# MAT 449 : Representation theory

Sophie Morel

April 26, 2019

# Contents

# I Representations of topological groups

## I.1 Topological groups

**Definition I.1.1.** A *topological group* is a topological set $G$ with the structure of a group such that the multiplication map $G \times G \to G$, $(x, y) \longmapsto xy$ and the inversion map $G \to G$, $x \longmapsto x^{-1}$ are continuous.

We usually will denote the unit of $G$ by $1$ or $e$.

**Example I.1.2.**

- Any group with the discrete topology is a topology group. Frequently used examples include finite groups, free groups (both commutative and noncommutative) and "arithmetic" matrix groups such as $\mathrm{GL}_n(\mathbb{Z})$ and $\mathrm{SL}_n(\mathbb{Z})$.
- The additive groups of $\mathbb{R}$ and $\mathbb{C}$ are topological groups.
- The group $\mathrm{GL}_n(\mathbb{C})$, with the topology given by any norm on the $\mathbb{C}$-vector space $M_n(\mathbb{C})$, is a topological group (see exercise I.5.1.1), hence so are all its subgroups if we put the induced topology on them. For example $S^1 := \{z \in \mathbb{C} | |z| = 1\}$, $\mathrm{GL}_n(\mathbb{R})$, $\mathrm{SU}(n)$, $\mathrm{SO}(n)$ etc.
- The additive group of $\mathbb{Q}_p$ and the group $\mathrm{GL}_n(\mathbb{Q}_p)$ are topological groups. (See exercise I.5.1.4.)

**Definition I.1.3.** We say that a topological space $X$ is *locally compact* if every point of $X$ has a compact neighborhood.

*Remark* I.1.4. If $X$ is Hausdorff, this is equivalent to the fact that every point of $X$ has a basis of compact neighborhoods. [1]

Note that we do not assume that neighborhoods of points in topological spaces are open.

**Notation I.1.5.** Let $G$ be a group, and let $A, B \subset G$, $x \in G$ and $n \geq 1$. We use the following notation :

$$xA = \{xy, y \in A\} \qquad \text{and} \qquad Ax = \{yx, y \in A\}$$

[1] reference ?

$$AB = \{yz, y \in A, z \in B\}$$

$$A^n = AA \dots A \qquad (n \text{ factors})$$

$$A^{-1} = \{y^{-1}, y \in A\}$$

**Definition I.1.6.** We say that a subset $A$ of $G$ is *symmetric* if $A = A^{-1}$.

**Proposition I.1.7.** *Let $G$ be a topological group.*

*(1). If $U$ is an open subset of $G$ and $A$ is any subset of $G$, then the sets $UA$, $AU$ and $U^{-1}$ are open.*

*(2). If $U$ is a neighborhood of $1$ in $G$, then there is an open symmetric neighborhood $V$ of $1$ such that $V^2 \subset U$.*

*(3). If $H$ is a subgroup of $G$, then its closure $\overline{H}$ is also a subgroup of $G$.*

*(4). If $H$ is an open subgroup of $G$, then it is also closed.*

*(5). If $A$ and $B$ are compact subsets of $G$, then the set $AB$ is also compact.*

*(6). Let $H$ be a subgroup of $G$. Then the quotient $G/H$ (with the quotient topology) is :*

*(a) Hausdorff if $H$ is closed;*

*(b) locally compact if $G$ is locally compact;*

*(c) a topological group if $H$ is normal.*

*Proof.* (1). For $x \in G$, we denote by $l_x : G \to G$ (resp. $r_x : G \to G$) left (resp. right) multiplication by $x$. We also denote by $\iota : G \to G$ the map $x \longmapsto x^{-1}$. By the axioms for topological groups, all these maps are continuous.

Now note that $U^{-1} = \iota^{-1}(U)$, $AU = \bigcup_{x \in A} l_{x^{-1}}^{-1}(U)$ and $UA = \bigcup_{x \in A} r_{x^{-1}}^{-1}(U)$. So $U^{-1}$, $AU$ and $UA$ are open.

(2). We may assume that $U$ is open. Let $m : G \times G \to G$, $(x, y) \longmapsto xy$. Then $m$ is continuous, so $W := s^{-1}(U)$ is open. We have $(1, 1) \in W$ because $1^2 = 1 \in U$. By definition of the product topology on $G \times G$, there exists an open subset $\Omega \ni 1$ of $G$ such that $\Omega \times \Omega \subset W$. We have $\Omega^2 \subset U$ by definition of $W$. Let $V = \Omega \cap \Omega^{-1}$. We know that $\Omega^{-1}$ is open by (a), so $V$ is open, and it is symmetric by definition. We clearly have $1 \in V$ and $V^2 \subset \Omega^2 \subset U$.

(3). Consider the map $u : G \times G \to G$, $(x, y) \longmapsto xy^{-1}$; then a nonempty subset $A$ of $G$ is a subgroup if and only if $u(A \times A) \subset A$. Alos, by the axioms of topological groups, the map $u$ is continuous. Hence, for every $Z \subset G \times G$, $u(\overline{Z}) \subset \overline{u(Z)})$. Applying this to $H \times H$ (whose closure is $\overline{H} \times \overline{H}$), we see that $\overline{H}$ is a subgroup of $G$.

(4). We have $G = H \sqcup ((G - H)H)$. If $H$ is open, then $(G - H)H$ is also open by (a), hence $H$ is closed.

(5). The multiplication map $m : G\times G \to G$ is continuous by hypothesis. As $AB = m(A\times B)$ and $A \times B$ is compact, the set $AB$ is also compact.

(6). (a) Let $x, y \in G$ be such that $xH \neq yH$. By question (a), $x(G - H)y^{-1}$ is open, so its complement $xHy^{-1}$ is closed. Also, by the assumption that $xH \neq yH$, the unit 1 is not in $xHy^{-1}$. By (b), there exists a symmetric open set $1 \in U$ such that $U^2 \subset G - xHy^{-1}$. Let's show that $UxH \cap UyH = \varnothing$, which will prove the result because $UxH$ (resp. $UyH$) is an open neighborhood of $xH$ (resp. $yH$) in $G/H$. If $UxH \cap UyH \neq \varnothing$, then we can find $u_1, u_2 \in U$ and $h_1, h_2 \in H$ such that $u_1xh_1 = u_2yh_2$. But then $xh_1h_2^{-1}y^{-1} = u_1^{-1}u_2 \in xHy^{-1}\cap U^2$, which is not possible.

(b) Let $xH \in G/H$. If $K$ is a compact neighborhood of $x$ in $G$, then its image in $G/H$ is a compact neighborhood of $xH$ in $G/H$.

(c) If $H$ is normal, then $G/H$ is a group. Let's show that its multiplication is continuous. Let $x, y \in G$. Any open neighborhood of $xyH$ in $G/H$ is of the form $UxyH$, with $U$ an open neighborhood of $xy$ in $G$. By the continuity of multiplication on $G$, there exists open neighborhoods $V$ and $W$ of $x$ and $y$ in $G$ such that $VW \subset U$. Then $VH$ and $WH$ are open neighborhoods of $xH$ and $yH$ in $G/H$, and we have $(VH)(WH) \subset UH$. (Remember that, as $H$ is normal, $AH = HA$ for every subset $A$ of $G$.) Let's show that inversion is continuous on $G/H$. Let $x \in G$. Any open neighborhood of $x^{-1}H$ in $G/H$ is of the form $UH$, with $U$ an open neighborhood of $x^{-1}$ in $G$. By question (a), the set $U^{-1}$ is open, so $U^{-1}H$ is an open neighborhood of $xH$ in $G/H$, and we have $(U^{-1}H)^{-1} = HU = UH$.

□

*Remark* I.1.8. In particular, if $G$ is a topological group, then $G/\overline{\{1\}}$ is a Hausdorff topological group. We are interested in continuous group actions of $G$ on vector spaces, so we could replace $G$ by $G/\overline{\{1\}}$ to study them. Hence, **in what follows, we will only consider Hausdorff topological groups (unless otherwise specified).**

**Definition I.1.9.** A *compact group* (resp. a *locally compact group*) is a Hausdorff and compact (resp. locally compact) topological group.

**Example I.1.10.** Among the groups of example I.1.2, finite discrete groups and the groups $S^1$, $\mathrm{SU}(n)$ and $\mathrm{SO}(n)$ are compact. All the other groups are locally compact. We get a non-locally compact group by considering the group of invertible bounded linear endomorphisms of an infinite-dimensional Banach space (see exercise I.5.1.1).

Translation operators : Let $G$ be a group, $x \in G$ and $f : G \to \mathbb{C}$ be a function. We define two functions $L_xf, R_xf : G \to \mathbb{C}$ by :

$$L_xf(y) = f(x^{-1}y) \qquad \text{and} \qquad R_xf(y) = f(yx).$$

We chose the convention so that $L_{xy} = L_x \circ L_y$ and $R_{xy} = R_x \circ R_y$. Note that, if $G$ is a topological group and $f$ is continuous, then $L_xf$ and $R_xf$ are also continuous.

Function spaces : Let $X$ be a topological set. If $f : X \to \mathbb{C}$ is a function, we write

$$\|f\|_\infty = \sup_{x \in X} |f(x)| \in [0, +\infty].$$

We also us the following notation :

- $\mathscr{C}(X)$ for the set of continuous functions $f : X \to \mathbb{C}$;
- $\mathscr{C}_b(X)$ for the set of bounded continuous functions $f : X \to \mathbb{C}$ (i.e. elements $f$ of $\mathscr{C}(X)$ such that $\|f\|_\infty < +\infty$);
- $\mathscr{C}_0(X)$ for the set of continuous functions $X \to \mathbb{C}$ that vanish at infinity (i.e. such that, for every $\varepsilon > 0$, there exists a compact subset $K$ of $X$ such that $|f(x)| < \varepsilon$ for every $x \notin K$);
- $\mathscr{C}_c(X)$ for the set of continuous functions with compact support from $X$ to $\mathbb{C}$.

Note that we have $\mathscr{C}(X) \supset \mathscr{C}_b(X) \supset \mathscr{C}_0(X) \supset \mathscr{C}_c(X)$, with equality if $X$ is compact. The function $\|.\|_\infty$ is a norm on $\mathscr{C}_b(X)$ and its subspaces, and $\mathscr{C}_b(X)$ and $\mathscr{C}_0(X)$ are complete for this norm (but not $\mathscr{C}_c(X)$, unless $X$ is compact). [2]

**Definition I.1.11.** Let $G$ be a topological group. A function $f : G \to \mathbb{C}$ is called *left (resp. right) uniformly continuous* if $\|L_x f - f\|_\infty \to 0$ as $x \to 1$ (resp. $\|R_x f - f\|_\infty \to 0$ as $x \to 1$).

**Proposition I.1.12.** *If $f \in \mathscr{C}_c(G)$, then $f$ is both left and right uniformly continuous.*

*Proof.* We prove that $f$ is right uniformly continuous (the proof that it is left uniformly continuous is similar). Let $K$ be the support of $f$. Let $\varepsilon > 0$. For every $x \in K$, we choose a neighborhood $U_x$ of 1 such that $|f(xy) - f(x)| < \frac{\varepsilon}{2}$ for every $y \in U_x$; by proposition I.1.7, we can find a symmetric open neighborhood $V_x$ of 1 such that $V_x^2 \subset U_x$. We have $K \subset \bigcup_{x \in K} xV_x$. As $K$ is compact, we can find $x_1, \dots, x_n \in K$ such that $K \subset \bigcup_{i=1}^n x_i V_{x_i}$. Let $V = \bigcup_{i=1}^n V_{x_i}$, this is a symmetric open neighborhood of 1.

We claim that, if $y \in V$, then $\|R_y f - f\|_\infty < \varepsilon$. Indeed, let $y \in V$, and let $x \in G$. First assume that $x \in K$. Then there exists $i \in \{1, \dots, n\}$ such that $x \in x_i V_{x_i}$. Then we have $xy \in x_i V_{x_i} V_{x_i} \subset x_i U_{x_i}$, hence

$$|f(xy) - f(x)| \le |f(xy) - f(x_i)| + |f(x_i) - f(x)| < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon.$$

Now assume that $xy \in K$. Then there exists $i \in \{1, \dots, n\}$ such that $xy \in x_i V_{x_i}$, and we have $x = xyy^{-1} \in x_i V_{x_i} V_{x_i} \subset x_i U_{x_i}$. Hence

$$|f(xy) - f(x)| \le |f(xy) - f(x_i)| + |f(x_i) - f(x)| < \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon.$$

Finally, if $x, xy \notin K$, then $f(x) = f(xy) = 0$, and of course $|f(xy) - f(x)| < \varepsilon$.

$\square$

[2] reference ?

*Remark* I.1.13. We put the topology given by $\|.\|_\infty$ on $\mathscr{C}_b(G)$. Then a function $f \in \mathscr{C}_b(G)$ is left (resp. right) uniformly continuous if and only if the map $G \to \mathscr{C}_b(G)$, $x \longmapsto L_x f$ (resp. $x \longmapsto R_x f$) is continuous at the unit of $G$.

Using the fact that $L_{xy} = L_x \circ L_y$ and $R_{xy} = R_x \circ R_y$ and the operators $L_x$ and $R_x$ preserve $\mathscr{C}_c(G)$, we see that the proposition above implies that, if $f \in \mathscr{C}_c(G)$, then the two maps $G \to \mathscr{C}_c(G)$ sending $x \in G$ to $L_x f$ and to $R_x f$ are continuous.

## I.2 Haar measures

**Definition I.2.1.** Let $X$ be a topological space.

(1). The $\sigma$-algebra of *Borel sets* on $X$ is the $\sigma$-algebra on $X$ generated by the open subsets of $X$. A *Borel measure* on $X$ is a measure on this $\sigma$-algebra.

(2). A *regular Borel measure* on $X$ is a measure $\mu$ on the $\sigma$-algebra of Borel sets of $X$ satisfying the following properties :

   (a) For every compact subset $K$ of $X$, $\mu(K) < +\infty$;

   (b) $\mu$ is *outer regular* : for every Borel subset $E$ of $X$, we have $\mu(E) = \inf\{\mu(U), U \supset E \text{ open}\}$;

   (c) $\mu$ is *inner regular* : for every $E \subset X$ that is either Borel of finite measure or open, we have $\mu(E) = \sup\{\mu(K), K \subset E \text{ compact}\}$.

**Notation I.2.2.** We denote by $\mathscr{C}_c^+(X)$ the subset of nonzero $f \in \mathscr{C}_c(X)$ such that $f(X) \subset \mathbb{R}_{\geq 0}$.

**Theorem I.2.3** (Riesz representation theorem)**.** *Let $X$ be a locally compact Hausdorff space, and let $\Lambda : \mathscr{C}_c(X) \to \mathbb{C}$ be a linear functional such that $\Lambda(f) \geq 0$ for every $f \in \mathscr{C}_c^+(X)$.* [3] *Then there exists a unique regular Borel measure $\mu$ on $X$ such that, for every $f \in \mathscr{C}_c(X)$,*

$$\Lambda(f) = \int_X f d\mu.$$

[4]

**Definition I.2.4.** Let $G$ be a locally compact group. A *left (resp. right) Haar measure* on $G$ is a nonzero regular Borel measure $\mu$ on $G$ such that, for every Borel set $E$ of $G$ and every $x \in G$, we have $\mu(xE) = \mu(E)$ (resp. $\mu(Ex) = \mu(E)$).

**Example I.2.5.** (1). If $G$ is a discrete group, then the counting measure is a left and right Haar measure on $G$.

[3] Such a linear functional is called *positive*.
[4] Reference ?

(2). Lebesgue measure is a left and right Haar measure on the additive group of $\mathbb{R}$.

**Proposition I.2.6.** *Let $G$ be a locally compact group and $\mu$ be a regular Borel measure on $G$.*

*(1). Let $\widetilde{\mu}$ be the Borel measure on $G$ defined by $\widetilde{\mu}(E) = \mu(E^{-1})$. Then $\mu$ is a left Haar measure if and only $\widetilde{\mu}$ is a right Haar measure.*

*(2). The measure $\mu$ is a left Haar measure on $G$ if and only if we have : for every $f \in \mathscr{C}_c(G)$, for every $y \in G$, $\int_G L_y f d\mu = \int_G f d\mu$.*

*(3). If $\mu$ is a left Haar measure on $G$, then $\mu(U) > 0$ for every nonempty open subset of $G$ and $\int_G f d\mu > 0$ for every $f \in \mathscr{C}_c^+(G)$.*

*Proof.* (1). First, note that $\widetilde{\mu}$ is a regular Borel measure on $G$ because $x \longmapsto x^{-1}$ is a homeomorphism from $G$ to itself.

If $E \subset G$ is a Borel set and $x \in E$, then $\widetilde{\mu}(Ex) = \mu(x^{-1}E^{-1})$. This implies the statement.

(2). Let $x \in G$, and let $\mu_x$ be the Borel measure on $G$ defined by $\mu_x(E) = \mu(xE)$. (This is indeed a regular Borel measure on $G$, because $y \longmapsto xy$ is a homeomorphism from $G$ to itself.) Then, for every measurable function $f : G \to \mathbb{C}$, we have $\int_G f d\mu_x = \int_G L_x f d\mu$. (This is obvious for characteristic functions of Borel subsets, and we get the general case by approximating $f$ by linear combinations of characteristic functions.)

On the one hand, the measure $\mu$ is a left Haar measure if and only if $\mu = \mu_x$ for every $x \in G$. On the other hand, by the uniqueness in the Riesz representation theorem (and the paragraph above), for $x \in G$, we have $\mu = \mu_x$ if and only $\int_G f d\mu = \int_G L_x f d\mu$ for every $f \in \mathscr{C}_c(G)$. The statement follows.

(3). Suppose that there exists a nonempty open subset $U$ of $G$ such that $\mu(U) = 0$. Then $\mu(xU) = 0$ for every $x \in G$, so we may assume that $1 \in U$. Let $K$ be a compact subset of $G$. Then $K \subset \bigcup_{x \in K} xU$, so there exist $x_1, \ldots, x_n \in K$ such that $K \subset \bigcup_{i=1}^n x_i U$. As $\mu(x_i U) = 0$ for every $i$, this implies that $\mu(K) = 0$. But then, by inner regularity of $\mu$, we get $\mu(G) = 0$, which contradicts the fact that $\mu$ is nonzero.

Let $f \in \mathscr{C}_c^+(G)$. Then $U := \{x \in G | f(x) > \frac{1}{2}\|f\|_\infty\}$ is a nonempty open subset of $G$, so $\mu(U) > 0$. But we have $f \geq \frac{1}{2}\|f\|_\infty \mathbb{1}_U$, hence $\int_G f d\mu \geq \frac{1}{2}\|f\|_\infty \mu(U) > 0$.

$\square$

**Theorem I.2.7.** *Let $G$ be a locally compact group. Then :*

*(1). There exists a left Haar measure on $G$.*

*(2). If $\mu_1$ and $\mu_2$ are two left Haar measures on $G$, then there exists $c \in \mathbb{R}_{>0}$ such that $\mu_2 = c\mu_1$.*

By proposition I.2.6, this theorem implies the similar result for right Haar measures.

*Proof.* We first prove existence. The idea is very similar to the construction of Lebesgue measure on $\mathbb{R}$. Suppose that $c > 0$, and that $\varphi \in C_c^+(\mathbb{R})$ is bounded by 1 and very close to the characteristic function of the interval $[0, c]$. If $f \in \mathscr{C}_c(\mathbb{R})$ does not vary too quickly on intervals of length $c$, then we can approximate $f$ by a linear combination of left translates of $\varphi$ : $f \simeq \sum c_i L_{x_i}\varphi$, and then $\int f d\mu \simeq \sum c_i L_{x_i} \int \varphi d\mu$. As $c \to 0$, we will be able to approximate every $f \in \mathscr{C}_c(\mathbb{R})$ (because we know that these functions are uniformly continuous), and we'll be able to define $\int f d\mu$ by going to the limit. On a general locally compact group, we replace the intervals by smaller and smaller compact neighborhoods of 1.

Now here is the rigorous proof. Let $f, \varphi \in C_c^+(G)$. Then $U := \{x \in G | \varphi(x) > \frac{1}{2}\|\varphi\|_\infty\}$ is a nonempty open subset of $G$ and we have $\varphi \geq \frac{1}{2}\|\varphi\|_\infty \mathbb{1}_U$. As the support of $f$ is compact, it can be covered by a finite number of translates of $U$, so there exist $x_1, \dots, x_n \in G$ and $c_1, \dots, c_n \in \mathbb{R}_{\geq 0}$ such that $f \leq \sum_{i=1}^n c_i L_{x_i}\varphi$. Hence, if we define $(f : \varphi)$ to be the infimum of all finite sums $\sum_{i=1}^n c_i$ with $c_1, \dots, c_n \in \mathbb{R}_{\geq 0}$ and such that there exist $x_1, \dots, x_n \in G$ with $f \leq \sum_{i=1}^n c_i L_{x_i}\varphi$, we have $(f : \varphi) < +\infty$. We claim that :

(I.2.0.0.1) $\quad (f : \varphi) = (L_x f : \varphi) \quad \forall x \in G$

(I.2.0.0.2) $\quad (f_1 + f_2 : \varphi) \leq (f_1 : \varphi) + (f_2 + \varphi)$

(I.2.0.0.3) $\quad (cf : \varphi) = c(f : \varphi) \quad \forall c \geq 0$

(I.2.0.0.4) $\quad (f_1 : \varphi) \leq (f_2 : \varphi) \quad \text{if } f_1 \leq f_2$

(I.2.0.0.5) $\quad (f : \varphi) \geq \frac{\|f\|_\infty}{\|\varphi\|_\infty}$

(I.2.0.0.6) $\quad (f : \varphi) \leq (f : \psi)(\psi : \varphi) \quad \forall \psi \in \mathscr{C}_c^+(G) - \{0\}$

The first four properties are easy. For the fifth property, note that, if $f \leq \sum_{i=1}^n c_i L_{x_i}\varphi$, then

$$\|f\|_\infty \leq \sum_{i=1}^n c_i \|L_{x_i}\varphi\|_\infty = \left(\sum_{i=1}^n c_i\right) \|\varphi\|_\infty.$$

Finally, the last property is a consequence of the following fact : Let $\psi \in \mathscr{C}_c^+(G)$. If we have $f \leq \sum_{i=1}^n c_i L_{x_i}\psi$ and $\psi \leq \sum_{j=1}^m d_j L_{y_j}\varphi$, then $f \leq \sum_{i=1}^n \sum_{j=1}^n c_i d_j L_{x_i y_j}\varphi$.

Now we fix $f_0 \in \mathscr{C}_c^+(G)$. By I.2.0.0.5, we know that $(f_0 : \varphi) > 0$. We define $I_\varphi : \mathscr{C}_c^+(G) \to \mathbb{R}_{\geq 0}$ by

$$I_\varphi(f) = \frac{(f:\varphi)}{(f_0:\varphi)}.$$

By I.2.0.0.1-I.2.0.0.4, we have

$$\begin{aligned} I_\varphi(f) &= I_\varphi(L_x f) \quad \forall x \in G \\ I_\varphi(f_1 + f_2) &\leq I_\varphi(f_1) + I_\varphi(f_2) \\ I_\varphi(cf) &= c I_\varphi(f) \quad \forall c \geq 0 \\ I_\varphi(f_1) &\leq I_\varphi(f_2) \quad \text{if } f_1 \leq f_2 \end{aligned}$$

If the second inequality were an equality (that is, if $I_\varphi$ were additive), we could extend $I_\varphi$ to a positive linear functional on $\mathscr{C}_c(G)$ and apply the Riesz representation theorem. This is not quite true, but we have the following result :

Claim : For all $f_1, f_2 \in \mathscr{C}_c^+(G)$ and $\varepsilon > 0$, there exists a neighborhood $V$ of $1$ in $G$ such that we have $I_\varphi(f_1) + I_\varphi(f_2) \leq I_\varphi(f_1 + f_2) + \varepsilon$ whenever $\mathrm{supp}(\varphi) \subset V$.

Let's first prove the claim. Choose a function $g \in \mathscr{C}_c^+(G)$ such that $g(x) = 1$ for every $x \in \mathrm{supp}(f_1 + f_2)$, and let $\delta$ be a positive real number. Let $h = f_1 + f_2 + \delta g$. We define functions $h_1, h_2 : G \to \mathbb{R}_{\geq 0}$ by

$$h_i(x) = \begin{cases} \frac{f_i(x)}{h(x)} & \text{if } f_i(x) \neq 0 \\ 0 & \text{if } f_i(x) = 0. \end{cases}$$

Note that $h_i$ is equal to $\frac{f_i}{h}$, hence continuous on the open subset $\{x \in G | h(x) \neq 0\}$. As $G$ is the union of this open subset and of the open subset $G - \mathrm{supp}(f_i)$ (on which $h_i$ is also continuous), this shows that $h_i$ is continuous, hence $h_i \in \mathscr{C}_c^+(G)$. Note also that we have $f_i = h_i h$.

By proposition I.1.12, there exists a neighborhood $V$ of $1$ such that, for $i \in \{1, 2\}$ and $x, y \in G$ with $y^{-1}x \in V$, we have $|h_i(x) - h_i(y)| < \delta$. Let $\varphi \in \mathscr{C}_c^+(G)$ be such that $\mathrm{supp}(\varphi) \subset V$. If $c_1, \ldots, c_n \in \mathbb{R}_{\geq 0}$ and $x_1, \ldots, x_n \in G$ are such that $h \leq \sum_{j=1}^m c_j L_{x_j}\varphi$, then, for every $x \in G$ and $i \in \{1, 2\}$,

$$f_i(x) = h(x)h_i(x) \leq \sum_{j=1}^n c_j \varphi(x_j^{-1}x)h_i(x) \leq \sum_{j=1}^n c_j \varphi(x_j^{-1}x)(h_i(x_j) + \delta),$$

because $\varphi(x_j^{-1}x) = 0$ unless $x_j^{-1}x \in V$. Hence

$$(f_1 : \varphi) + (f_2 : \varphi) \leq \sum_{j=1}^n c_j(h_1(x_j) + h_2(x_j) + 2\delta).$$

Since $h_1 + h_2 \leq 1$, we get

$$(f_1 : \varphi) + (f_2 : \varphi) \leq (1 + 2\delta) \sum_{j=1}^n c_j,$$

hence, taking the infimum over the families $(c_1, \ldots, c_n)$ and dividing by $(f_0 : \varphi)$, we get

$$I_\varphi(f_1) + I_\varphi(f_2) \leq (1 + 2\delta)I_\varphi(h) \leq (1 + 2\delta)(I_\varphi(f_1 + f_2) + \delta I_\varphi(g)).$$

The right-hand side of this tends to $I_\varphi(f_1 + f_2)$ as $\delta$ tends to $0$, so we get the desired inequality by taking $\delta$ small enough. This finishes the proof of the claim.

We come back to the construction of a left Haar measure on $G$. For every $f \in \mathscr{C}_c^+(G)$, let $X_f = [(f_0 : f)^{-1}, (f : f_0)] \subset \mathbb{R}$. Let $X = \prod_{f \in \mathscr{C}_c^+(G)} X_f$, endowed with the product topology. Then, by Tychonoff's theorem, [5] $X$ is a compact Hausdorff space. It is the space of functions $I : \mathscr{C}_c^+(G) \to \mathbb{R}$ such that $I(f) \in X_f$ for every $f$ (with the topology of pointwise convergence). Also, by I.2.0.0.6, we have $I_\varphi \in X$ for every $\varphi \in \mathscr{C}_c^+(G)$. For every neighborhood $V$ of $1$ in

[5] reference ?

$G$, let $K(V)$ be the closure of $\{I_\varphi | \operatorname{supp}(\varphi) \subset V\}$ in $X$. We have $K(V) \neq \varnothing$ for every $V$, so $K(V_1) \cap \ldots K(V_n) \supset K(\bigcap_{i=1}^n V_i) \neq \varnothing$ for every finite family $V_1, \ldots, V_n$ of neighborhoods of $1$ in $G$. As $X$ is compact, this implies that the intersection of all the sets $K(V)$ is nonempty. We choose an element $I$ of this intersection.

Let's show that $I$ is invariant by left translations, additive and homogenous of degree $1$. (That is, it has the same properties as $I_\varphi$, but it is also additive instead of just subadditive.) Let $f_1, f_2 \in \mathscr{C}_c^+(G)$, $c \in \mathbb{R}_{\geq 0}$, $x \in G$ and $\varepsilon > 0$. Choose a neighborhood $V$ of $1$ in $G$ such that $I_\varphi(f_1) + I_\varphi(f_2) \leq I_\varphi(f_1 + f_2) + \varepsilon$ whenever $\operatorname{supp}(\varphi) \subset V$; this exists by the claim. By definition of $I$, it is in the closure $\{I_\varphi | \operatorname{supp}(\varphi) \subset V\}$, which means that there exists $\varphi \in \mathscr{C}_c^+(G)$ such that $\operatorname{supp}(\varphi) \subset V$ and $|I(aL_y g) - I_\varphi(aL_y g)| < \varepsilon$ for $g \in \{f_1, f_2, f_1 + f_2\}$, $y \in \{1, x\}$ and $a \in \{1, c\}$. Then we get :

$$|I(L_x f_1) - I(f_1)| \leq |I(L_x f_1) - I_\varphi(L_x f_1)| + |I_\varphi(L_x f_1) - I_\varphi(f_1)| + |I_\varphi(f_1) - I(f_1)| < 2\varepsilon,$$

$$|I(cf_1) - cI(f_1)| \leq |I(cf_1) - I_\varphi(cf_1)| + |I_\varphi(cf_1) - cI_\varphi(f_1)| + |cI_\varphi(f_1) - cI(f_1)| < \varepsilon(1 + c)$$

and

$$|I(f_1 + f_2) - I(f_1) - I(f_2)| \leq |I_\varphi(f_1 + f_2) - I_\varphi(f_1) - I_\varphi(f_2)|$$
$$+|I(f_1 + f_2) - I_\varphi(f_1 + f_2)| + |I(f_1) - I_\varphi(f_1)| + |I(f_2) - I_\varphi(f_2)| < 4\varepsilon.$$

As $\varepsilon$ is arbitrary, this implies that $I(L_x f_1) = I(f_1)$, $I(cf_1) = cI(f_1)$ and $I(f_1 + f_2) = I(f_1) + I(f_2)$.

Now we extend $I$ to a linear functional $\mathscr{C}_c(G) \to \mathbb{C}$, that we will still denote by $I$. Let $f \in \mathscr{C}_c(G)$. Then we can write $f = (f_1 - f_2) + i(g_1 - g_2)$, with $f_1, f_2, g_1, g_2 \in \mathscr{C}_c^+(G) \cup \{0\}$ (for example, take $f_1 = \max(0, \operatorname{Re}(f))$, $f_2 = \max(0, -\operatorname{Re}(f))$, $g_1 = \max(0, \operatorname{Im}(f))$ and $g_2 = \max(0, \operatorname{Im}(f))$). We set $I(f) = I(f_1) - I(f_2) + i(I(g_1) - I(g_2))$ (with the convention that $I(0) = 0$). If $f = (F_1 - F_2) + i(G_1 - G_2)$, with $F_1, F_2, G_1, G_2 \in \mathscr{C}_c^+(G) \cup \{0\}$, then $F_1 + f_2 = F_2 + f_1$ and $G_1 + g_2 = G_2 + g_1$, so we get the same result for $I(f)$. Also, it is easy to check that $I$ is a linear functional from $\mathscr{C}_c(G)$ to $\mathbb{C}$, and it is positive by construction. By the Riesz representation theorem, there exists a regular Borel measure $\mu$ on $G$ such that $I(f) = \int_G f d\mu$. By proposition I.2.6, this measure is a left Haar measure.

We now prove the second statement of the theorem (uniqueness of left Haar measure up to a constant). Let $\mu_1, \mu_2$ be two left Haar measures on $G$. By the uniqueness in the Riesz representation theorem (and the fact that $\mathscr{C}_c^+(G)$ generates $\mathscr{C}_c(G)$) it suffices to find a positive real number $c$ such that $\int f d\mu_1 = c \int f d\mu_2$ for every $f \in \mathscr{C}_c^+(G)$. By proposition I.2.6, we have $\int_G f d\mu_2 > 0$ for every $f \in \mathscr{C}_c^+(G)$. So it suffices to show that, if $f, g \in \mathscr{C}_c^+(G)$, we have

$$\frac{\int f d\mu_1}{\int f d\mu_2} = \frac{\int g d\mu_1}{\int g d\mu_2} \qquad (*).$$

Let $f, g \in \mathscr{C}_c^+(G)$. Let $V_0$ be a symmetric compact neighborhood of $1$, and set

$$A = (\operatorname{supp}(f))V_0 \cup V_0(\operatorname{supp}(f))$$

and
$$B = (\mathrm{supp}(g))V_0 \cup V_0(\mathrm{supp}(g)).$$
Then $A$ and $B$ are compact by proposition I.1.7. If $y \in V_0$, the functions $x \longmapsto f(xy) - f(yx)$ and $x \longmapsto g(xy) - g(yx)$ are supported on $A$ and $B$ respectively.

Let $\varepsilon > 0$. By proposition I.1.12, there exists a symmetric neighborhood $V \subset V_0$ of $1$ such that, for every $x \in G$ and every $y \in V$, we have $|f(xy) - f(yx)| < \varepsilon$ and $|g(xy) - g(yx)| < \varepsilon$. Let $h \in \mathscr{C}_c^+(G)$ be such that $\mathrm{supp}(h) \subset V$ and $h(x) = h(x^{-1})$ for every $x \in G$. Then
$$\begin{aligned}(\int_G h d\mu_2)(\int_G f d\mu_1) &= \int_{G\times G} h(y)f(x)d\mu_1(x)d\mu_2(y) \\ &= \int_{G\times G} h(y)f(yx)d\mu_1(x)d\mu_2(y).\end{aligned}$$
(We use the left invariance of $\mu_1$. Also, we can apply Fubini's theorem, because all the functions are supported on compact sets, and compact sets have finite measure.) Similarly, we have
$$\begin{aligned}(\int_G h d\mu_1)(\int_G f d\mu_2) &= \int_{G\times G} h(x)f(y)d\mu_1(x)d\mu_2(y) \\ &= \int_{G\times G} h(y^{-1}x)f(y)d\mu_1(x)d\mu_2(y) \\ &= \int_{G\times G} h(x^{-1}y)f(y)d\mu_1(x)d\mu_2(y) \\ &= \int_{G\times G} h(y)f(xy)d\mu_1(x)d\mu_2(y).\end{aligned}$$
Hence
$$\begin{aligned}\left|(\int_G h d\mu_1)(\int_G f d\mu_2) - (\int_G h d\mu_2)(\int_G f d\mu_1)\right| &= \left|\int_{G\times G} h(y)(f(xy) - f(yx))d\mu_1(x)\mu_2(y)\right| \\ &\leq \varepsilon\mu_1(A)\int_G h d\mu_2,\end{aligned}$$
as $\mathrm{supp}(h) \subset V$. Dividing by $(\int_G f d\mu_2)(\int_G h d\mu_2)$, we get
$$\left|(\int_G h d\mu_1)(\int_G h d\mu_2)^{-1} - (\int_G f d\mu_1)(\int_G f d\mu_2)^{-1}\right| \leq \varepsilon\mu_1(A)(\int_G f d\mu_2)^{-1}.$$
Similarly, we have
$$\left|(\int_G h d\mu_1)(\int_G h d\mu_2)^{-1} - (\int_G g d\mu_1)(\int_G g d\mu_2)^{-1}\right| \leq \varepsilon\mu_1(B)(\int_G g d\mu_2)^{-1}.$$
Taking the sum gives
$$\left|\frac{\int_G f d\mu_1}{\int_G f d\mu_2} - \frac{\int_G g d\mu_1}{\int_G g d\mu_2}\right| \leq \varepsilon\left(\frac{\mu_1(A)}{\int_G f d\mu_2} + \frac{\mu_1(B)}{\int_G f d\mu_2}\right).$$

As $\varepsilon$ is arbitrary, this gives the desired equality (*).

□

We now want to compare left and right Haar measures.

**Proposition I.2.8.** *Let $G$ be a locally compact group. Let $x \in G$. Then there exists $\Delta(x) \in \mathbb{R}_{>0}$ such that, for every left Haar measure $\mu$ on $G$, we have $\mu(Ex) = \Delta(x)\mu(E)$. Moreover, $\Delta : G \to \mathbb{R}_{>0}$ is a continuous group homomorphism (where the group structure on $\mathbb{R}_{>0}$ is given by multiplication) and, for every left Haar measure $\mu$ on $G$, every $x \in G$ and every $f \in L^1(G, \mu)$, we have*

$$\int_G R_x f d\mu = \Delta(x^{-1}) \int_G f d\mu.$$

*Proof.* Let $x \in G$, and $\mu$ be a left Haar measure on $G$. Then the measure $\mu_x$ defined by $\mu_x(E) = \mu(Ex)$ is also a left Haar measure on $G$, so, by the uniqueness statement in theorem I.2.7, there exists $\Delta(x) \in \mathbb{R}_{>0}$ such that $\mu_x = \Delta(x)\mu$, that is, $\mu(Ex) = \Delta(x)\mu(E)$ for every Borel subset $E$ of $G$. Suppose that $\lambda$ is another left Haar measure on $G$. Then, again by theorem I.2.7, there exists $c > 0$ such that $\lambda = c\mu$, and so we get, fo every Borel subset $E$ of $G$,

$$\lambda(Ex) = c\mu(Ex) = c\Delta(x)\mu(E) = \Delta(x)\lambda(E).$$

This proves the first statement.

We prove that $\Delta$ is a morphism of groups. Let $x, y \in G$, and let $E$ be a Borel subset of $G$ such that $\mu(E) \neq 0$. Then

$$\Delta(xy)\mu(E) = \mu(Exy) = \Delta(y)\mu(Ex) = \Delta(y)\Delta(x)\mu(E),$$

hence $\Delta(xy) = \Delta(x)\Delta(y)$.

We now prove the last statement. If $E$ is a Borel subset of $G$ and $x \in G$, then $R_x \mathbb{1}_E = \mathbb{1}_{Ex^{-1}}$, so we get

$$\int_G R_x \mathbb{1}_E d\mu = \mu(Ex^{-1}) = \Delta(x^{-1})\mu(E) = \Delta(x)^{-1} \int_G \chi_E d\mu$$

by definition of $\Delta$. This proves the result for $f = \chi_E$. The general case follows by approximating $f$ by linear combinations of functions $\mathbb{1}_E$.

Finally, we prove that $\Delta$ is continuous. Let $f \in \mathscr{C}_c^+(G)$. We know that the function $G \to \mathscr{C}_c(G)$, $x \longmapsto R_{x^{-1}} f$ is continuous (see remark I.1.13), so the function $G \to \mathbb{C}$, $x \longmapsto \int_G R_{x^{-1}} f d\mu$ is also continuous. But we have just seen that $\int_G R_{x^{-1}} f d\mu = \Delta(x) \int_G f d\mu$, and we know that $\int_G f d\mu > 0$ by proposition I.2.6. Hence $\Delta$ is continuous.

□

**Definition I.2.9.** The function $\Delta$ of the previous proposition is called the *modular function* of $G$. We say that the group $G$ is *unimodular* if $\Delta = 1$ (that is, if some (or any) left Haar measure on $G$ is also a right Haar measure).

*Remark* I.2.10. Suppose that $\alpha : G \to G$ is a homeomorphism such that for every $x \in G$, we have $\beta(x) \in G$ satisfying : for every $y \in G$, $\alpha(xy) = \beta(x)\alpha(y)$. (For example, $\alpha$ could be right translation by a fixed element of $G$, or a continuous group isomorphism with continuous inverse.) Then we can generalize the construction of proposition I.2.8 to get a $\Delta(\alpha) \in \mathbb{R}_{>0}$ satisfying : for every $f \in \mathscr{C}_c(G)$, for every left Haar measure $\mu$ on $G$,

$$\Delta(\alpha) \int_G f(\alpha(x))d\mu(x) = \int_G f(x)d\mu(x)$$

(or equivalently $\mu(\alpha(E)) = \Delta(\alpha)\mu(E)$ for every Borel subset $E$ of $G$). Moreover, if $\beta : G \to G$ satisfies the same conditions as $\alpha$, then so does $\alpha \circ \beta$ and we have $\Delta(\alpha \circ \beta) = \Delta(\alpha)\Delta(\beta)$.

**Example I.2.11.** (1). Any compact group is unimodular. Indeed, if $G$ is compact, then $\Delta(G)$ is a compact subgroup of $\mathbb{R}_{>0}$, but the only compact subgroup of $\mathbb{R}_{>0}$ is $\{1\}$. In particular, a compact group $G$ has a unique left and right Haar measure $\mu$ such that $\mu(G) = 1$; we call this measure the *normalized Haar measure* of $G$.

(2). Any discrete group is unimodular. Indeed, we have a left Haar measure on $G$ that is also a right Haar measure : the counting measure.

(3). If $G$ is commutative, then left and right translations are equal on $G$, so $G$ is unimodular.

(4). The groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ are unimodular. (This is proved in exercise I.5.3.2(c) for $\mathrm{GL}_n(\mathbb{R})$, and the same proof works for $\mathrm{GL}_n(\mathbb{C})$.)

(5). The group of invertible upper triangular matrices in $M_2(\mathbb{R})$ is not unimodular (see exercise I.5.3.2(d)). In fact, its modular function is

$$\Delta : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \longmapsto |ac^{-1}|.$$

(6). Remember the commutator subgroup $[G, G]$ is the subgroup generated by all the $xyx^{-1}y^{-1}$, for $x, y \in G$. It is a normal subgroup of $G$, and every group morphism from $G$ to a commutative group is trivial on $[G, G]$. In particular, the modular function $\Delta$ is trivial on $[G, G]$, so $G$ is unimodular if $G = \overline{[G, G]}$. More generally, using the first example, we see that $G$ is unimodular if the quotient group $G/\overline{[G, G]}$ is compact.

**Proposition I.2.12.** *Let $G$ be a locally compact group, and let $\mu$ be a left Haar measure on $G$. We define a right Haar measure $\nu$ on $G$ by $\nu(E) = \mu(E^{-1})$ (see proposition I.2.6).*

*Then, for every $f \in \mathscr{C}_c(G)$, we have*

$$\int_G f(x^{-1})d\mu_G(x) = \int_G f(x)d\nu(x) = \int_G \Delta(x^{-1})f(x)d\mu(x).$$

We also write this property as $d\nu(x) = \Delta(x^{-1})d\mu(x)$, or $d\mu(x^{-1}) = \Delta(x^{-1})d\mu(x)$.

*Proof.* We prove the first equality. It is actually true for every $f \in L^1(G,\mu)$. If $f$ is characteristic function of a Borel subset $E$, then $x \longmapsto f(x^{-1})$ is the characteristic function of $E^{-1}$, so $\int f(x^{-1})d\mu(x) = \int f d\nu$ by definition of $\nu$. We get the general result by approximation $f$ by linear combination of characteristic functions of Borel subsets.

We prove the second equality. Consider the linear function $\Lambda : \mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_G \Delta(x^{-1})f(x)d\mu(x)$. As $\Delta$ takes its values in $\mathbb{R}_{>0}$, $\Lambda$ is positive. Also, for every $y \in G$, we have

$$\begin{aligned}\Lambda(R_y f) = \int_G f(xy)\Delta(x^{-1})d\mu(x) &= \Delta(y)\int_G f(xy)\Delta((xy)^{-1})d\mu(x) \\ &= \int_G f(x)\Delta(x^{-1})d\mu(x) = \Lambda(f)\end{aligned}$$

(using the left invariance of $\mu$ and the fact that $\Delta$ is a morphism of groups). So the unique regular Borel measure $\rho$ that corresponds to $\Lambda$ by the Riesz representation theorem is a right Haar measure (see proposition I.2.6). By theorem I.2.7, there exists $c > 0$ such that $\rho = c\nu$. To finish the proof, it suffices to show that $c = 1$. Suppose that $c \neq 1$. Then we can find a compact symmetric neighborhood $U$ of $1$ such that, for every $x \in U$, we have $|\Delta(x^{-1}) - 1| \leq \frac{1}{2}|c-1|$. As $U$ is symmetric, we have $\mu(U) = \nu(U)$, hence

$$|c-1|\mu(U) = |c\nu(U) - \mu(U)| = \left|\int_U (\Delta(x^{-1}) - 1)d\mu(x)\right| \leq \frac{1}{2}|c-1|\mu(U),$$

which contradicts the fact that $\mu(U) \neq 0$ (by proposition I.2.6).

□

# I.3 Representations

In this section, $G$ is a topological group.

## I.3.1 Continuous representations

**Definition I.3.1.1.** If $V$ and $W$ are normed $\mathbb{C}$-vector spaces, we denote by $\operatorname{Hom}(V,W)$ the $\mathbb{C}$-vector space of bounded linear operators from $V$ to $W$, and we put on it the topology given by the operator norm $\|.\|_{op}$. We also write $\operatorname{End}(V)$ for $\operatorname{Hom}(V,V)$, and $\operatorname{GL}(V)$ for $\operatorname{End}(V)^\times$, with the topology induced by that of $\operatorname{End}(V)$.

**Definition I.3.1.2.** Let $V$ be a normed $\mathbb{C}$-vector space. Then a *(continuous) representation* of $G$ on $V$ is a group morphism $\rho$ from $G$ to the group of $\mathbb{C}$-linear automorphisms of $V$ such that the action map $G \times V \to V$, $(g,v) \longmapsto \rho(g)(v)$, is continuous.

We refer to the representation by $(\rho, V)$, $\rho$ or often simply by $V$. Sometimes, we don't explicitely name the map $\rho$ and write the action of $G$ on $V$ as $(g, v) \longmapsto gv$.

*Remark* I.3.1.3. - The definition makes sense if $V$ is any topological vector space (over a topological field).

- If $(\rho, V)$ is a continuous representation of $G$, then the action of every $g \in G$ on $V$ is a continuous endomorphism of $V$, so we get a group morphism $\rho : G \to \mathrm{GL}(V)$. But this morphism is not necessarily continuous, unless $V$ is finite-dimensional (see proposition I.3.5.1). An example of this is given by the regular representations of $G$ on $L^p(G)$ defined in example I.3.1.11.
- If $\rho : G \to \mathrm{GL}(V)$ is a morphism of groups that is continuous for the weak* topology on $\mathrm{End}(V)$, then it is not necessarily a continuous representation. (For example, take $G = \mathrm{GL}(V)$, with the topology induced by the weak* topology on $\mathrm{End}(V)$, and $\rho = \mathrm{id}$. This is not a continuous representation of $G$ on $V$ if $V$ is infinite-dimensional.)

**Example I.3.1.4.** - The *trivial representation* of $G$ on $V$ is the representation given by $\rho(x) = \mathrm{id}_V$ for every $x \in G$. (It is a continuous representation.)

- If $V$ is finite-dimensional, then the identity map of $\mathrm{GL}(V)$ is a continuous representation of $\mathrm{GL}(V)$ on $V$.
- If $G = S^1$ and $n \in \mathbb{Z}$, the map $G \to \mathbb{C}$, $z \longmapsto z^n$ is a continuous representation of $G$ on $\mathbb{C}$.
- The map $\rho : \mathbb{R} \to \mathrm{GL}_2(\mathbb{C})$, $x \longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is a continuous representation of $\mathbb{R}$ on $\mathbb{C}^2$.
- See example I.3.1.11 for the representations of $G$ on its function spaces.

**Definition I.3.1.5.** Let $(\rho_1, V_1)$ and $(\rho_2, V_2)$ be two representations of $G$. An *intertwining operator* (or *G-equivariant map*) from $V_1$ to $V_2$ is a bounded $\mathbb{C}$-linear map $T : V_1 \to V_2$ such that, for every $g \in G$ and every $v \in V_1$, we have $T(\rho_1(g)v) = \rho_2(g)T(v)$.

We write $\mathrm{Hom}_G(V_1, V_2)$ for the space of intertwining operators from $V_1$ to $V_2$, and $\mathrm{End}_G(V_1)$ for the space of intertwining operators from $V_1$ to itself.

We say that the representations $(\rho_1, V_1)$ and $(\rho_2, V_2)$ are *isomorphic* (or *equivalent*) if there exists intertwining operators $T : V_1 \to V_2$ and $T' : V_2 \to V_1$ such that $T' \circ T = \mathrm{id}_{V_1}$ and $T \circ T' = \mathrm{id}_{V_2}$.

**Definition I.3.1.6.** Let $(\rho, V)$ be a representation of $V$.

(1). A *subrepresentation* of $V$ (or *G-invariant subspace*) is a linear subspace $W$ such that, for every $g \in G$, we have $\rho(g)(W) \subset W$.

(2). The representation $(\rho, V)$ is called *irreducible* if $V \neq 0$ and if its only *closed* $G$-invariant subspaces are $0$ and $V$. Otherwise, the representation is called *reducible*.

(3). The representation $(\rho, V)$ is called *indecomposable* if, whenever $V = W_1 \oplus W_2$ with $W_1$ and $W_2$ two closed $G$-invariant subspaces of $V$, we have $W_1 = 0$ or $W_2 = 0$.

(4). The representation $(\rho, V)$ is called *semisimple* if there exists a family $(W_i)_{i \in I}$ of closed $G$-invariant subspaces of $V$ that are in direct sum and such that $\bigoplus_{i \in I} W_i$ is dense in $V$. (If $I$ is finite, the direct sum is also closed in $V$, so this implies that $V = \bigoplus_{i \in I} W_i$.)

*Remark* I.3.1.7. If $(\rho, V)$ is a representation of $G$ and $W \subset V$ is a $G$-stable subspace, then its closure $\overline{W}$ is also stable by $G$.

**Example I.3.1.8.** The representation $\rho$ of $\mathbb{R}$ on $\mathbb{C}^2$ given by $\rho(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ is indecomposable but not irreducible.

**Lemma I.3.1.9.** *Let $(\rho_1, V_1)$ and $(\rho_2, V_2)$ be two representations of G, and let $T : V_1 \to V_2$ be an intertwining operator. Then* $\mathrm{Ker}(T)$ *is a subrepresentation of $V_1$, and* $\mathrm{Im}(T)$ *is a subrepresentation of $V_2$.*

*Proof.* Let $v \in \mathrm{Ker}(T)$ and $g \in G$. Then $T(\rho_1(g)(v)) = \rho_2(g)(T(v)) = 0$, so $\rho_1(g)(v) \in \mathrm{Ker}(T)$.

Now let $w \in \mathrm{Im}(T)$, and choose $v \in V_1$ such that $w = T(v)$. Then $\rho_2(g)(w) = T(\rho_1(g)(v)) \in \mathrm{Im}(T)$.

□

**Proposition I.3.1.10.** *Let $V$ be a normed vector space and $\rho : G \to \mathrm{End}(V)$ be a multiplicative map. We denote by $\|.\|_{op}$ the operator norm on $\mathrm{End}(V)$. Suppose that :*

*(a) For every $g \in G$, we have $\|\rho(g)\|_{op} \leq 1$;*

*(b) For every $v \in V$, the map $G \to V$, $g \longmapsto \rho(g)(v)$ is continuous.*

*Then $(\rho, V)$ is a continuous representation of G.*

*Proof.* Let $g_0 \in G$, $v_0 \in V$, and $\varepsilon > 0$. We want to find a neighborhood $U$ of $g$ in $G$ and a $\delta > 0$ such that : $g \in U$ and $\|v - v_0\| < \delta \Rightarrow \|\rho(g)(v) - \rho(g_0)(v_0)\| < \varepsilon$.

Choose a neighborhood $U$ of $g$ in $G$ such that : $g \in U \Rightarrow \|\rho(g)(v_0) - \rho(g_0)(v_0)\| < \varepsilon/2$, and take $\delta = \varepsilon/2$. Then, if $g \in U$ and $\|v - v_0\| < \delta$, we have

$$\begin{aligned} \|\rho(g)(v) - \rho(g_0)(v_0)\| &\leq \|\rho(g)(v) - \rho(g)(v_0)\| + \|\rho(g)(v_0) - \rho(g_0)(v_0)\| \\ &< \|\rho(g)\|_{op}\|v - v_0\| + \varepsilon/2 \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon, \end{aligned}$$

because $\|\rho(g)\|_{op} \leq 1$.

□

**Example I.3.1.11.** (1). We have defined, for every $x \in G$, two endomorphisms $L_x$ and $R_x$ of the space of functions on $G$, and these endomorphisms preserve $\|.\|_\infty$. So, by proposition I.3.1.10 and remark I.1.13, they define two representations of $G$ on $\mathscr{C}_c(G)$.

(2). Suppose that $G$ is locally compact Hausdorff. We fix a left Haar measure $dx$ on $G$, and we denote $L^p(G)$ the $L^p$ spaces for this measure, for $1 \leq p \leq \infty$. The left invariance of the measure implies that the operators $L_x$ preserve the $L^p$ norm, so we get a $\mathbb{C}$-linear left action of $G$ on $L^p(G)$, and, by proposition I.3.1.10, to show that it is a representation, we just need to show that, if $f \in L^p(G)$, the map $G \to L^p(G)$, $x \longmapsto L_x f$ is continuous. This is not necessarily true if $p = \infty$, but it is for $1 \leq p < \infty$, by proposition I.3.1.13 below. So we get a representation of $G$ on $L^p(G)$ for $1 \leq p < \infty$.

If we chose instead a right Haar measure on $G$, then the operators $R_x$ would define a representation of $G$ on $L^p(G)$ for $1 \leq p < \infty$. So, if $G$ is unimodular, we get two commuting representations of $G$ on $L^p(G)$.

**Definition I.3.1.12.** Let $G$ be a locally compact group with a left (resp. right) Haar measure $dx$, and let $L^2(G)$ be the corresponding $L^2$ space. The representation of $G$ on $L^2(G)$ given by the operators $L_x$ (resp. $R_x$) is called the *left* (resp. *right*) regular representation of $G$.

**Proposition I.3.1.13.** *Let $G$ be a locally compact group, let $\mu$ be a left Haar measure on G, and let $L^p(G)$ be the corresponding $L^p$ space. Suppose that $1 \leq p < \infty$.*

*Then, for every $f \in L^p(G)$, we have $\|L_x f - f\|_p \to 0$ and $\|R_x f - f\|_p \to 0$ as $x \to 1$.*

*Proof.* Suppose first that $f \in \mathscr{C}_c(G)$, and fix a compact neighborhood $V$ of 1. Then $K := V(\operatorname{supp} f) \cup (\operatorname{supp} f)V$ is compact by proposition I.1.7, so $\mu(K) < +\infty$. For every $x \in V$, we have $\operatorname{supp}(f), \operatorname{supp}(L_x f), \operatorname{supp}(R_x f) \subset K$, so $\|L_x f - f\|_p \leq \mu(K)^{1/p}\|L_x - f\|_\infty$ and $\|R_x f - f\|_p \leq \mu(K)^{1/p}\|R_x f - f\|_\infty$. The result then follows from proposition I.1.12.

Now let $f$ be any element of $L^p(G)$. We still fix a compact neighborhood $V$ of 1, and we set $C = \sup_{x\in V} \Delta(x)^{-1/p}$. Let $\varepsilon > 0$. There exists $g \in \mathscr{C}_c(G)$ such that $\|f - g\|_p < \varepsilon$. Then we have, for $x \in V$,

$$\|L_x f - f\|_p \leq \|L_x(f - g)\|_p + \|L_x g - g\|_p + \|g - f\|_p \leq 2\varepsilon + \|L_x g - g\|_p$$

(as $\|L_x(f - g)\|_p = \|f - g\|_p$) and

$$\|R_x f - f\|_p \leq \|R_x(f - g)\|_p + \|R_x g - g\|_p + \|g - f\|_p \leq (1 + C)\varepsilon + \|R_x g - g\|_p$$

(as $\|R_x(f-g)\|_p = \Delta(x)^{-1/p}\|f-g\|_p$). We have seen in the first part of the proof that $\|L_x g-g\|_p$ and $\|R_x g - g\|_p$ tend to 0 as $x$ tends to 1, so we can find a neighborhood $U \subset V$ of 1 such that $\|L_x f - f\|_p \leq 3\varepsilon$ and $\|R_x f - f\|_p \leq (2 + C)\varepsilon$ for $x \in U$.

□

## I.3.2 Unitary representations

Remember that a *(complex) Hilbert space* is a $\mathbb{C}$-vector space $V$ with a Hermitian inner product[6] such that $V$ is complete for the corresponding norm. If $V$ is a finite-dimensional $\mathbb{C}$-vector space with a Hermitian inner product, then it is automatically complete, hence a Hilbert space. We will usually denote the inner product on all Hermitian inner product spaces by $\langle .,. \rangle$ (unless otherwise specified).

**Notation I.3.2.1.** Let $V$ and $W$ be Hermitian inner product spaces. For every continuous $\mathbb{C}$-linear map $T : V \to W$, we write $T^* : W \to V$ for the adjoint of $T$, if it exists. Remember that we have $\langle T(v), w\rangle = \langle v, T^*(w)\rangle$ for every $v \in V$ and $w \in W$, and that $T^*$ always exists if $V$ and $W$ are Hilbert spaces.

If $V'$ is a subspace of $V$, we write $V'^{\perp}$ for the orthogonal of $V'$; it is defined by

$$(V')^{\perp} = \{v \in V | \forall v' \in V',\ \langle v, v'\rangle = 0\}.$$

Finally, we write $\mathrm{U}(V)$ for the group of unitary endomorphisms of $V$, that is, of endomorphisms $T$ of $V$ that preserve the inner product ($\langle T(v), T(w)\rangle = \langle v, w\rangle$ for all $v, w \in V$). A unitary endomorphism $T$ is automatically bounded and invertible (with inverse equal to $T^*$).

The following result is an immediate corollary of proposition I.3.1.10 (and of the fact that unitary operators have norm 1).

**Corollary I.3.2.2.** *If $V$ is a Hilbert space and $\rho : G \to \mathrm{U}(V)$ is a morphism of groups, then the following are equivalent :*

*(1). The map $G \times V \to V$, $(g, v) \longmapsto \rho(g)(v)$, is continuous.*

*(2). For every $v \in V$, the map $G \to V$, $g \longmapsto \rho(g)(v)$, is continuous.*

**Definition I.3.2.3.** If $V$ is a Hilbert space, a *unitary representation* of $G$ on $V$ is a morphism of groups $\rho : G \to \mathrm{U}(V)$ satisfying the conditions of corollary I.3.2.2.

These representations are our main object of study.

**Example I.3.2.4.** If $(X, \mu)$ is any measure space, then $L^2(X)$ is a Hilbert space, with the following inner product :

$$\langle f, g\rangle = \int_X f(x)\overline{g(x)}d\mu(x).$$

So if $G$ is a locally compact group, then the left regular representation and right regular representations of $G$ are unitary representations of $G$ (on the same space if $G$ is unimodular).

[6] We will always assume Hermitian inner products to be $\mathbb{C}$-linear in the first variable.

*Remark* I.3.2.5. Note that $\rho$ is still not necessarily a continuous map in general. (Unless $\dim_{\mathbb{C}} V < +\infty$.) For example, it is not continuous for the left regular representation of $S^1$.

Also, note that we don't need the completeness of $V$ in the proof, so corollary I.3.2.2 is actually true for any Hermitian inner product space.

**Lemma I.3.2.6.** *Let $(\rho, V)$ be a unitary representation of $G$. Then, for every $G$-invariant subspace $W$ of $V$, the subspace $W^\perp$ is also $G$-invariant.*

In particular, if $W$ is a *closed* $G$-invariant subspace of $V$, then we have $V = W \oplus W^\perp$ with $W^\perp$ a closed $G$-invariant subspace.

*Proof.* Let $v \in W^\perp$ and $g \in G$. Then, for every $w \in W$, we have

$$\langle \rho(g)(v), w\rangle = \langle v, \rho(g)^{-1}w\rangle = 0$$

(the last equality comes from the fact that $\rho(g)^{-1}w \in W$), hence $\rho(g)(v) \in W^\perp$.

$\square$

**Lemma I.3.2.7.** *Let $(\rho_1, V_1)$ and $(\rho_2, V_2)$ be two unitary representations of $G$, and let $T : V_1 \to V_2$ be an intertwining operator. Then $T^* : V_2 \to V_1$ is also an intertwining operator.*

*Proof.* Let $w \in V_2$ and $g \in G$. Then, for every $v \in V_1$, we have

$$\langle v, T^*(\rho_2(g)(w))\rangle = \langle T(v), \rho_2(g)(w)\rangle = \langle \rho_2(g)^{-1}T(v), w\rangle = \langle T(\rho_1(g)^{-1}(v)), w\rangle =$$

$$\langle \rho_1(g)^{-1}(v), T^*(w)\rangle = \langle v, \rho_1(g)T^*(w)\rangle.$$

So $T^*(\rho_2(g)(w)) = \rho_1(g)(T^*(w))$.

$\square$

**Theorem I.3.2.8.** *Assume that the group $G$ is compact Hausdorff. Let $(V, \langle.,.\rangle_0)$ be a Hilbert space and $\rho : G \to \mathrm{GL}(V)$ be a continuous representation of $G$ on $V$. Then there exists a Hermitian inner product $\langle.,.\rangle$ on $V$ satisfying the following properties :*

*(1). There exist real numbers $c, C > 0$ such that, for every $v \in V$, we have $c|\langle v, v\rangle_0| \leq |\langle v, v\rangle| \leq C|\langle v, v\rangle_0|$. In other words, the norms coming from the two inner products are equivalent, and so $V$ is still a Hilbert space for the inner product $\langle.,.\rangle$.*

*(2). The representation $\rho$ is unitary for the inner product $\langle.,.\rangle$.*

*Remark* I.3.1. (a) If $V$ is irreducible, it follows from Schur's lemma (see theorem I.3.4.1) that this inner product is unique up to a constant.

(b) This is false for noncompact groups. For example, consider the representation $\rho$ of $\mathbb{R}$ on $\mathbb{C}^2$ given by $\rho(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. There is no inner product on $\mathbb{C}^2$ that makes this representation unitary (otherwise $\rho(\mathbb{R})$ would be a closed subgroup of the unitary group of this inner product, hence compact, but this impossible because $\rho(\mathbb{R}) \simeq \mathbb{R}$).

*Proof of the theorem.* We define $\langle .,. \rangle : V \times V \to \mathbb{C}$ by the following formula : for all $v, w \in V$,

$$\langle v, w \rangle = \int_G \langle \rho(g)v, \rho(g)w \rangle_0 dg,$$

where $dg$ is a normalized Haar measure on $G$. This defines a Hermitian form on $V$, and we have $\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$ for every $v, w \in V$ and $g \in G$ by left invariance of the measure.

If we prove property (1), it will also imply that $\langle .,. \rangle$ is definite (hence an inner product), and so we will be done. Let $v \in V$. Then the two maps $G \to V$ sending $v$ to $\rho(g)(v)$ and to $\rho(g)^{-1}(v)$ are continuous. As $G$ is compact, they are both bounded. By the uniform boundedness principle (theorem I.3.2.11), there exist $A, B \in \mathbb{R}_{>0}$ such that $\|\rho(g)^{-1}\|_{op} \leq A$ and $\|\rho(g)\|_{op} \leq B$ for every $g \in G$. By the submultiplicativity of the operator norm, the first inequality implies that $\|\rho(g)\| \leq A^{-1}$ for every $g \in G$. So the definition of $\langle .,. \rangle$ (and the fact that $G$ has volume 1) gives property (1), with $c = A^{-2}$ and $C = B^2$.

□

**Corollary I.3.2.9.** *If $G$ is compact Hausdorff, then every nonzero finite-dimensional continuous representation of $G$ is semisimple.*

*Proof.* We may assume that the representation is unitary by the theorem. We prove the corollary by induction on $\dim V$. The result is obvious if $\dim V \leq 1$, so assume that $\dim V \geq 2$ and that we know the result for all spaces of strictly smaller dimension. If $V$ is irreducible, we are done. Otherwise, there is a $G$-invariant subspace $W \subsetneq V$ such that $W \neq 0$. This subspace is closed because it is finite-dimensional, and we have $V = W \oplus W^\perp$ with $W^\perp$ invariant by lemma I.3.2.6. As $\dim(W), \dim(W^\perp) < \dim(V)$, we can apply the induction hypothesis to $W$ and $W^\perp$ and conclude that they are semisimple. But then their direct sum $V$ is also semisimple.

□

*Remark* I.3.2.10. This is still true (but harder to prove) for infinite-dimensional unitary representations of compact groups (see theorem IV.2.1), but it is false for infinite-dimensional unitary representations of noncompact groups (if for example $G$ is abelian and not compact, its regular representation is not semisimple by corollary I.3.4.4 and exercise III.6.1.2(c)), or for finite-dimensional (non-unitary) representations of noncompact groups (see example I.3.1.8).

**Theorem I.3.2.11** (Uniform boundedness principle or Banach-Steinhaus theorem)**.** *Let $V$ and $W$ be normed vector spaces, and suppose that $V$ is a Banach space (i.e. that it is complete for* *the metric induced by its norm). Let $(T_i)_{i\in I}$ be a family of bounded linear operators from $V$ to $W$.*

*If the family $(T_i)_{i\in I}$ is pointwise bounded (that is, if $\sup_{i\in I}\|T_i(v)\|<+\infty$ for every $v\in V$), then it is bounded (that is, $\sup_{i\in I}\|T_i\|_{op}<+\infty$).*

*Proof.* [7] [8] Suppose that $\sup_{i\in I}\|T_i\|_{op}=+\infty$, and choose a sequence $(i_n)_{n\geq 0}$ of elements of $I$ such that $\|T_{i_n}\|_{op}\geq 4^n$. We define a sequence $(v_n)_{n\geq 0}$ of elements of $V$ in the following way :

- $v_0=0$;
- For $n\geq 1$, we can find, thanks to lemma I.3.2.12 below, an element $v_n$ of $V$ such that $\|v_n-v_{n-1}\|\leq 3^{-n}$ and $\|T_{i_n}(v_n)\|\geq\frac{2}{3}3^{-n}\|T_{i_n}\|_{op}$.

We have $\|v_n-v_m\|\leq\frac{1}{2}3^{-n}$ for $m\geq n$, so the sequence $(v_n)_{n\geq 0}$ is a Cauchy sequence; as $V$ is complete, it has a limit $v$, and we have $\|v_n-v\|\leq\frac{1}{2}3^{-n}$ for every $n\geq 0$. The inequality $\|T_{i_n}(v_n)\|\geq\frac{2}{3}3^{-n}\|T_{i_n}\|_{op}$ and the triangle inequality now imply that $\|T_{i_n}(x)\|\geq\frac{1}{6}3^{-n}\|T_{i_n}\|_{op}\geq\frac{1}{6}(\frac{4}{3})^n$, and so the sequence $(\|T_{i_n}(x)\|)_{n\geq 0}$ is unbounded, which contradicts the hypothesis.

□

**Lemma I.3.2.12.** *Let $V$ and $W$ be two normed vector spaces, and let $T:V\to W$ be a bounded linear operator. Then for any $v\in V$ and $r>0$, we have*

$$\sup_{v'\in B(v,r)}\|T(v')\|\geq r\|T\|_{op},$$

*where $B(v,r)=\{v'\in V|\|v-v'\|<r\}$.*

*Proof.* For every $x\in V$, we have

$$\|T(x)\|\leq\frac{1}{2}(\|T(v+x)\|+T(v-x)\|)\leq\max(\|T(v+x)\|,\|T(v-x)\|).$$

Taking the supremum over $x\in B(0,r)$ gives the inequality of the lemma.

□

Finally, we have the following result, whose proof uses Schur's lemma (theorem I.3.4.1) and is given in exercise I.5.5.9.

**Theorem I.3.2.13.** *If $G$ is a compact group, then every irreducible unitary representation of $G$ is finite-dimensional.*

[7] Taken from a paper of Alan Sokal.
[8] Precise ref.

## I.3.3 Cyclic representations

**Definition I.3.3.1.** Let $(\rho, V)$ be a continuous representation of $G$, and let $v \in V$. Then the closure $W$ of $\mathrm{Span}\{\rho(g)(v), g \in G\}$ is a subrepresentation of $V$, called the *cyclic subspace* generated by $v$.

If $V = W$, we say that $V$ is a *cyclic representation* and that $v$ is a *cyclic vector* for $V$.

**Example I.3.3.2.** An irreducible representation is cyclic, and every nonzero vector is a cyclic vector for it.

The converse is not true. For example, consider the representation $\rho$ of the symmetric group $\mathfrak{S}_n$ on $\mathbb{C}^n$ defined by $\rho(\sigma)(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$, and let $v = (1, 0, \ldots, 0) \in \mathbb{C}^n$. Then the set $\rho(\mathfrak{S}_n)(v)$ is the canonical basis of $\mathbb{C}^n$, hence it generates $\mathbb{C}^n$, and so $v$ is a cyclic vector for $\rho$. But $\rho$ is not irreducible, because $\mathbb{C}(1, 1, \ldots, 1)$ is a subrepresentation.

**Proposition I.3.3.3.** *Every unitary representation of G is a direct sum of cyclic representations.*

If the indexing set is infinite, we understand the direct sum to be the closed direct sum (that is, the closure of the algebraic direct sum).

*Proof.* Let $(\pi, V)$ be a unitary representation of $G$. By Zorn's lemma, we can find a maximal collection $(W_i)_{i\in I}$ of pairwise orthogonal cyclic subspaces of $V$. Suppose that $V$ is not the direct sum of the $W_i$, then there exists a nonzero vector $v \in (\bigoplus_{i\in I} W_i)^\perp$. By lemma I.3.2.6, the cyclic subspace generated by $v$ is included in $(\bigoplus_{i\in I} W_i)^\perp$, which contradicts the maximality of the family $(W_i)_{i\in I}$. Hence $V = \overline{\bigoplus_{i\in I} W_i}$.

□

## I.3.4 Schur's lemma

The following theorem is fundamental. We will not be able to prove it totally until we have the spectral theorem for normal endomorphisms of Hilbert spaces (theorem II.4.1).

**Theorem I.3.4.1** (Schur's lemma)**.** *Let $(\rho_1, V_1)$ and $(\rho_2, V_2)$ be two representations of G, and let $T : V_1 \to V_2$ be an intertwining operator.*

*(1). If $V_1$ is irreducible, then $T$ is either zero or injective.*

*(2). If $V_2$ is irreducible, then $T$ is zero or has dense image.*

*(3). Suppose that $V_1$ is unitary. Then it is irreducible if and only if $\mathrm{End}_G(V_1) = \mathbb{C} \cdot \mathrm{id}_{V_1}$.*

*(4). Suppose that $V_1$ and $V_2$ are unitary and irreducible. Then $\mathrm{Hom}_G(V_1, V_2)$ is of dimension zero (if $V_1$ and $V_2$ are not isomorphic) or $1$ (if $V_1$ and $V_2$ are isomorphic).*

*Proof.* We prove the first two points. By lemma I.3.1.9, $\mathrm{Ker}(T)$ and $\mathrm{Im}(T)$ are $G$-invariant subspaces of $V_1$ and $V_2$. Moreover, $\mathrm{Ker}(T)$ is a closed subspace of $V_1$. If $V_1$ is irreducible, then its only closed invariant subspaces are $0$ and $V_1$; this gives the first point. If $V_2$ is irreducible, then its only closed invariant subspaces are $0$ and $V_2$; this gives the second point.

We prove the third point. Suppose first that $V_1$ is not irreducible. Then it has a closed invariant subspace $W$ such that $0 \neq W \neq V_1$, and orthogonal projection on $W$ is a $G$-equivariant endomorphism by lemma I.3.4.3. So $\mathrm{End}_G(V_1)$ strictly contains $\mathbb{C} \cdot \mathrm{id}_{V_1}$.

Now suppose that $V_1$ is irreducible, and let $T \in \mathrm{End}_G(V_1)$. We want to show that $T \in \mathbb{C}\mathrm{id}_{V_1}$. If $V_1$ is finite-dimensional, then $T$ has an eigenvalue $\lambda$, and then $\mathrm{Ker}(T - \lambda\mathrm{id}_{V_1})$ is a nonzero $G$-invariant subspace of $V_1$, hence equal to $V_1$, and we get $T = \lambda\mathrm{id}_{V_1}$. In general, we still know that every $T \in \mathrm{End}(V)$ has a nonempty spectrum (by theorem II.1.1.3), but, if $\lambda$ is in the spectrum of $T$, we only know that $T - \lambda\mathrm{id}_V$ is not invertible, not that $\mathrm{Ker}(T - \lambda\mathrm{id}_V) \neq 0$. So we cannot apply the same strategy. Instead, we will use a corollary of the spectral theorem (theorem II.4.1). Note that the subgroup $\rho_1(G)$ of $\mathrm{End}(V_1)$ satisfies the hypothesis of corollary II.4.4 because $V_1$ is irreducible, so its centralizer in $\mathrm{End}(V_1)$ is equal to $\mathbb{C}\mathrm{id}_{V_1}$; but this centralizer is exactly $\mathrm{End}_G(V_1)$, so we are done.

We prove the fourth point. Let $T : V_1 \to V_2$ be an intertwining operator. Then $T^* : V_2 \to V_1$ is also an intertwining operator by lemma I.3.2.7, so $T^*T \in \mathrm{End}_G(V_1)$ and $TT^* \in \mathrm{End}_G(V_2)$. By the third point, there exists $c \in \mathbb{C}$ such that $T^*T = c\mathrm{id}_{V_1}$. If $c \neq 0$, then $T$ is injective and $\mathrm{Im}(T)$ is closed (because $\|T(v)\| \geq \frac{|c|}{\|T^*\|_{op}}\|v\|$ for every $v \in V_1$, see lemma I.3.4.2), so $T$ is an isomorphism by the second point, and its inverse $c^{-1}T^*$; hence $V_1$ and $V_2$ are isomorphic, and $\mathrm{Hom}_G(V_1, V_2) \simeq \mathrm{End}_G(V_1)$ is 1-dimensional. Suppose that $c = 0$. If $T \neq 0$, then it has dense image by the second point, but then $T^* = 0$ by the first point, hence $T = (T^*)^* = 0$, which is absurd; so $T = 0$. So we have proved that, if $\mathrm{Hom}_G(V_1, V_2) \neq 0$, then $V_1$ and $V_2$ must be isomorphic; this finishes the proof of the fourth point.

□

**Lemma I.3.4.2.** *Let $V$, $W$ be two normed vector spaces, and let $T : V \to W$ be a bounded linear operator. Suppose that $V$ is complete. If there exists $c > 0$ such that $\|T(v)\| \geq c\|v\|$ for every $v \in V$, then $\mathrm{Im}(T)$ is closed.*

*Proof.* Let $(v_n)_{n\in\mathbb{N}}$ be a sequence of elements of $V$ such that the sequence $(T(v_n))_{n\in\mathbb{N}}$ converges to a $w \in W$. We want to show that $w \in \mathrm{Im}(T)$. Note that, for all $n, m \in \mathbb{N}$, we have $\|v_n - v_m\| \leq c^{-1}\|T(v_n) - T(v_m)\|$. This implies that $(v_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, so it has a limit $v \in V$ because $V$ is complete. As $T$ is continuous, we have $w = \lim_{n\to+\infty} T(v_n) = T(v)$, so $w \in \mathrm{Im}(T)$.

□

**Lemma I.3.4.3.** *Let $(\rho, V)$ be a unitary representation of $G$, let $W$ be a closed subspace of $V$, and let $\pi$ be the orthogonal projection on $W$, seen as a linear endomorphism of $V$.*

*Then $W$ is $G$-invariant if and only if $\pi$ is $G$-equivariant.*

*Proof.* Suppose that $\pi$ is $G$-equivariant. Let $w \in W$ and $g \in G$. Then $\rho(g)(w) = \rho(g)(\pi(w)) = \pi(\rho(g)(w)) \in W$. So $W$ is invariant by $G$.

Conversely, suppose that $W$ is $G$-invariant. By lemma I.3.2.6, its orthogonal $W^\perp$ is also invariant by $G$. Let $v \in V$ and $g \in G$. We write $w = \pi(g)$ and $w' = g - \pi(g)$. Then $\rho(g)(v) = \rho(g)(w) + \rho(g)(w')$ with $\rho(g)(w) \in W$ and $\rho(g)(w') \in W^\perp$, so $\pi(\rho(g)(v)) = \rho(g)(w)$.

□

**Corollary I.3.4.4.** *If $G$ is commutative, then every irreducible unitary representation of $G$ is $1$-dimensional.*

So each unitary irreducible representation of $G$ is equivalent to one (and only one) continuous group morphism $G \to S^1$.

*Proof.* Let $(\rho, V)$ be an irreducible unitary representation. As $G$ is commutative, the operators $\rho(x)$ and $\rho(y)$ commute for all $x, y \in G$, so we have $\rho(x) \in \mathrm{End}_G(V)$ for every $x \in G$. By Schur's lemma, this implies that $\rho(x) \in \mathbb{C} \cdot \mathrm{id}_V$ for every $x \in G$. In particular, every linear subspace of $V$ is invariant by $G$. As $V$ is irreducible, it has no nontrivial closed invariant subspaces, so it must be $1$-dimensional.

□

**Example I.3.4.5.** Let $G = \mathbb{R}$. Then every irreducible unitary representation of $G$ is of the form $\rho_y : x \longmapsto e^{ixy}$, for $y \in \mathbb{R}$. The representation $\rho_y$ factors through $S^1 \simeq \mathbb{R}/\mathbb{Z}$ if and only $y \in 2\pi\mathbb{Z}$. (See exercise I.5.4.1(c) and (d).)

## I.3.5 Finite-dimensional representations

Remember that, if $V$ is a finite-dimensional $\mathbb{C}$-vector space, then all norms on $V$ are equivalent. [9] So $V$ has a canonical topology, and so does $\mathrm{End}(V)$ (as it is also a finite-dimensional vector space).

**Proposition I.3.5.1.** *Let $V$ be a normed $\mathbb{C}$-vector space and $\rho : G \to \mathrm{GL}(V)$ be a morphism of groups. Consider the following conditions.*

*(i) The map $G \times V \to V$, $(g, v) \longmapsto \rho(g)(v)$, is continuous (i.e. $\rho$ is a continuous representation of $G$ on $V$).*

*(ii) For every $v \in V$, the map $G \to V$, $g \longmapsto \rho(g)(v)$, is continuous.*

*(iii) The map $\rho : G \to \mathrm{GL}(V)$ is continuous.*

[9] reference ?

*Then we have (iii)⇒(i)⇒(ii). If moreover $V$ is finite-dimensional, then all three conditions are equivalent.*

*Proof.*

(i)⇒(ii) is obvious.

(ii)⇒(iii) : Suppose that $V$ is finite-dimensional, and let $(e_1, \dots, e_n)$ be a basis of $V$, and let $\|.\|$ be the norm on $V$ defined by $\|\sum_{i=1}^{x} x_i e_i\| = \sup_{1\leq i\leq n} |x_i|$. We use the corresponding operator norm on $\mathrm{End}(V)$ and still denote it by $\|.\|$. Let $g_0 \in G$ and let $\varepsilon > 0$; we are looking for a neighborhoord $U$ of $g_0 \in G$ such that : $g \in U \Rightarrow \|\rho(g) - \rho(g_0)\| \leq \varepsilon$.

For every $i \in \{1, \dots, n\}$, the function $G \to V$, $g \longmapsto \rho(g)(e_i)$, is continuous by assumption, so there exists a neighborhood $U_i$ of $g_0$ in $G$ such that : $g \in U \Rightarrow \|\rho(g)(e_i) - \rho(g_0)(e_i)\| \leq \varepsilon/n$. Let $U = \bigcap_{i=1}^{n} U_i$. Then if $g \in U$, for every $v = \sum_{i=1}^{n} x_i e_i \in V$, we have

$$\|\rho(g)(v) - \rho(g_0)(v)\| \leq \sum_{i=1}^{n} \|x_i\| \|\rho(g)(e_i) - \rho(g_0)(e_i)\| < \sum_{i=1}^{n} |x_i|\varepsilon/n \leq \varepsilon\|v\|,$$

which means that $\|\rho(g) - \rho(g_0)\| \leq \varepsilon$.

(iii)⇒(i) : Let $g_0 \in G$, $v_0 \in V$, and $\varepsilon > 0$. We want to find a neighborhood $U$ of $g$ and $G$ and a $\delta > 0$ such that : $g \in U$ and $\|v - v_0\| < \delta \Rightarrow \|\rho(g)(v) - \rho(g_0)(v_0)\| < \varepsilon$.

Choose a $\delta$ such that $0 < \delta \leq \frac{\varepsilon}{2\|\rho(g_0)\|}$, and let $U$ be a neighborhood of $g_0$ in $G$ such that : $g \in G \Rightarrow \|\rho(g) - \rho(g_0)\| < \frac{\varepsilon}{2(\|v_0\|+\delta)}$. Then, if $g \in U$ and $\|v - v_0\| < \delta$, we have $\|v\| \leq \|v_0\| + \delta$, and hence

$$\begin{array}{rcl} \|\rho(g)(v) - \rho(g_0)(v_0)\| & \leq & \|\rho(g)(v) - \rho(g_0)(v)\| + \|\rho(g_0)(v) - \rho(g_0)(v_0)\| \\ & \leq & \|\rho(g) - \rho(g_0)\|\|v\| + \|\rho(g_0)\|\|v - v_0\| \\ & < & \dfrac{\varepsilon}{2(\|v_0\| + \delta)}(\|v_0\| + \delta) + \|\rho(g_0)\|\delta \\ & \leq & \varepsilon/2 + \varepsilon/2 = \varepsilon. \end{array}$$

□

## I.4 The convolution product and the group algebra

Let $G$ be a locally compact group, and let $dx$ be a left Haar measure on $G$. We denote by $L^p(G)$ the $L^p$ spaces for this measure. We also denote by $\Delta$ the modular function of $G$.

## I.4.1 Convolution on $L^1(G)$ and the group algebra of $G$

**Definition I.4.1.1.** Let $f$ and $g$ be functions from $G$ to $\mathbb{C}$. The *convolution* of $f$ and $g$, denoted by $f * g$, is the function $x \longmapsto \int_G f(y)g(y^{-1}x)dy$ (if it makes sense).

**Proposition I.4.1.2.** *Let $f, g \in L^1(G)$. Then the integral $\int_G f(y)g(y^{-1}x)dy$ is absolutely convergent for almost every $x$ in G, so $f * g$ is defined almost everywhere, and we have $f * g \in L^1(G)$ and*

$$\|f * g\|_1 \leq \|f\|_1 \|g\|_1.$$

*Proof.* By the Fubini-Tonelli theorem and the left invariance of the measure on $G$, the function $G \times G \to \mathbb{C}$, $(x, y) \longmapsto f(y)g(y^{-1}x)$ is integrable and we have

$$\int_{G\times G} |f(y)g(y^{-1}x)|dxdy = \int_{G\times G} |f(y)||g(x)|dxdy = \|f\|_1 \|g\|_1.$$

So the first statement also follows from Fubini's theorem, and the second statement is obvious.

□

Note that the convolution product is clearly linear in both arguments.

**Proposition I.4.1.3.** *Let $f, g \in L^1(G)$.*

*(1). For almost every $x \in G$, we have*

$$\begin{aligned} f * g(x) &= \int_G f(y)g(y^{-1}x)dy \\ &= \int_G f(xy)g(y^{-1})dy \\ &= \int_G f(y^{-1})g(yx)\Delta(y^{-1})dy \\ &= \int_G f(xy^{-1})g(y)\Delta(y^{-1})dy \\ &= \int_G f(y)L_y g(x)dy \\ &= \int_G g(y^{-1})R_y f(x)dy. \end{aligned}$$

*(2). For every $h \in L^1(G)$, we have*

$$(f * g) * h = f * (g * h).$$

*(In other words, the convolution product is associative.)*

(3). *For every $x \in G$, we have*
$$L_x(f * g) = (L_x f) * g$$
*and*
$$R_x(f * g) = f * (R_x g).$$

(4). *If $G$ is abelian, then $f * g = g * f$.*

*Proof.* (1). We get the equalities of the first four lines by using the substitutions $y \longmapsto xy$ and $y \longmapsto y^{-1}$, the left invariance of $dy$ and proposition I.2.12. The last two lines are just reformulations of the first two.

(2). For almost every $x \in G$, we have

$$\begin{aligned}
((f * g) * h)(x) &= \int_G (f * g)(y) h(y^{-1}x) dy \\
&= \int_{G \times G} f(z) g(z^{-1}y) h(y^{-1}x) dz dy \\
&= \int_G f(z) \left( \int_G g(z^{-1}y) h(y^{-1}x) dy \right) dz \\
&= \int_G f(z) \left( \int_G g(y) h(y^{-1}z^{-1}x) dy \right) dz \\
&= \int_G f(z) (g * h)(z^{-1}x) dz \\
&= (f * (g * h))(x).
\end{aligned}$$

(3). This follows immediately from the definition and the equality of the first two lines in point (1).

(4). This follows from (1) and from the fact that $\Delta = 1$.

□

**Definition I.4.1.4.** A *Banach algebra* (over $\mathbb{C}$) is an associative $\mathbb{C}$-algebra $A$ with a norm $\|.\|$ making $A$ a Banach space (i.e. a complete normed vector space) and such that, for every $x, y \in A$, we have $\|xy\| \leq \|x\|\|y\|$ (i.e. the norm is submultiplicative). If $A$ has a unit $e$, we also require that $\|e\| = 1$.

Note that we do not assume that $A$ has a unit. If it does, we say that $A$ is *unital*.

**Example I.4.1.5.** (a) If $V$ is a Banach space, then $\mathrm{End}(V)$ is a unital Banach algebra.

(b) By propositions I.4.1.2 and I.4.1.3, the space $L^1(G)$ with the convolution product is a Banach algebra. We call it the *($L^1$) group algebra* of $G$.

*Remark* I.4.1.6. If the group $G$ is discrete and $dx$ is the counting measure, then $\delta_1 := \mathbb{1}_{\{1\}}$ is a unit for the convolution product. In general, $L^1(G)$ does not always have a unit. (It does if and only if $G$ is discrete.)[10] We can actually see it as a subalgebra of a bigger Banach algebra that does have a unit, the *measure algebra* $\mathscr{M}(G)$ of $G$ (see for example section 2.5 of [11]) :

Remember that a *(complex) Radon measure* on $G$ is a bounded linear functional on $\mathscr{C}_0(G)$ (with the norm $\|.\|_\infty$). We denote by $\mathscr{M}(G)$ the space of Radon measures and by $\|.\|$ its norm (which is the operator norm); this is a Banach space. If $\mu$ is a Radon measure, we write $f \longmapsto \int_G f(x)d\mu(x)$ for the corresponding linear functional on $\mathscr{C}_0(G)$. We define the convolution product $\mu * \nu$ of two Radon measures $\mu$ and $\nu$ to be the linear functional

$$f \longmapsto \int_{G\times G} f(xy)d\mu(x)d\nu(y).$$

Then it is not very hard to check that $\|\mu * \nu\| \leq \|\mu\|\|\nu\|$ and that the convolution product is associative on $\mathscr{M}(G)$. This makes $\mathscr{M}(G)$ into a Banach algebra, and the Dirac measure at $1$ is a unit element of $\mathscr{M}(G)$.

Note also that $\mathscr{M}(G)$ is commutative if and only if $G$ is abelian. Indeed, it is obvious on the definition of $*$ that $\mathscr{M}(G)$ is commutative if $G$ is abelian. To show the converse, we denote by $\delta_x$ the Dirac measure at $x$ (so $\int_G f d\delta_x = f(x)$). Then we clearly have $\delta_x * \delta_y = \delta_{xy}$ for every $x, y \in G$. So, if $\mathscr{M}(G)$ is commutative, then $\delta_{xy} = \delta_{yx}$ for every $x, y \in G$, and this implies that $G$ is abelian.

Even though $L^1(G)$ does not contain the unit of $\mathscr{M}(G)$, we have families of functions called "approximate identities" that will be almost as good as $\delta_1$ in practice. In particular, we will be able to prove that $L^1(G)$ is commutative if and only if $G$ is abelian (see corollary I.4.1.10).

**Definition I.4.1.7.** A (symmetric, continuous) approximate identity with supports in a basis of neighborhoods $\mathscr{U}$ of $1$ in $G$ is a family of functions $(\psi_U)_{U\in\mathscr{U}}$ in $\mathscr{C}_c^+(G)$ such that, for every $U \in \mathscr{U}$, we have

- $\operatorname{supp}(\psi_U) \subset U$;
- $\psi_U(x^{-1}) = \psi_U(x), \forall x \in G$;
- $\int_G \psi_U(x)dx = 1$.

For some results, we don't need the continuity of the $\psi_U$ or the fact that $\psi_U(x^{-1}) = \psi_U(x)$.

**Proposition I.4.1.8.** *For every basis of neighborhoods $\mathscr{U}$ of $1$ in $G$, there exists an approximate identity with supports in $\mathscr{U}$.*

*Proof.* Let $U \in \mathscr{U}$. Then $U$ contains a symmetric neighborhood $V \subset U$ of $1$ and a compact neighborhood $K \subset V$ of $1$, and, by corollary A.3.1, there exists a continuous function

[10] reference ?

$f : X \to [0,1]$ with compact support contained in $V$ such that $f_{|K} = 1$. In particular, $f \neq 0$, so $f \in \mathscr{C}_c^+(X)$. Define $g : X \to [0,2]$ by $g(x) = f(x) + f(x^{-1})$. Then $g \in \mathscr{C}_c^+(X)$ (because $g_{|K} = 2$) and $\operatorname{supp}(g) \subset V \subset U$. Now take $\psi_U = \frac{1}{\int_G g(x)dx} g$.

□

**Proposition I.4.1.9.** *Let $\mathscr{U}$ be a basis of neighborhoods of* $1$ *in G, and let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity with supports in $\mathscr{U}$.*

*(1). For every $f \in L^1(G)$, we have $\|\psi_U * f - f\|_1 \to 0$ and $\|f * \psi_U - f\|_1 \to 0$ as $U \to \{1\}$. In fact, we have :*

$$\|\psi_U * f - f\|_1 \leq \sup_{y\in U} \|L_Y f - f\|_1$$

*and*

$$\|f * \psi_U - f\|_1 \leq \sup_{y\in U} \|R_Y f - f\|_1.$$

*(2). If $f \in L^\infty(G)$ and $f$ is left (resp. right) uniformly continuous, then $\|\psi_U * f - f\|_\infty \to 0$ (resp. $\|f * \psi_U - f\|_\infty \to 0$) as $U \to \{1\}$. In fact, we have :*

$$\|\psi_U * f - f\|_\infty \leq \sup_{y\in U} \|L_Y f - f\|_\infty$$

*and*

$$\|f * \psi_U - f\|_\infty \leq \sup_{y\in U} \|R_Y f - f\|_\infty.$$

In point (2), note that if $f : G \to \mathbb{C}$ is bounded and $g \in \mathscr{C}_c(G)$, then the integral defining $(f * g)(x)$ converges absolutely for every $x \in G$.

*Proof.* (1). Let $U \in \mathscr{U}$. For every $x \in G$, we have

$$(\psi_U * f)(x) - f(x) = \int_G \psi_U(y)(L_y f(x) - f(x))dy$$

(because $\int_G \psi_U(y)dy = 1$). So

$$\begin{aligned}\|\psi_U * f - f\|_1 &= \int_G |\int_G \psi_U(y)(L_y f(x) - f(x))dy|dx \\ &\leq \int_{G\times G} \psi_U(y)|L_y f(x) - f(x)|dydx \\ &\leq \int_G \psi_U(y)\|L_y - f\|_1 dy \\ &\leq \sup_{y\in U} \|L_y f - f\|_1.\end{aligned}$$

The first convergence result then follows from the fact that $\|L_y f - f\|_1 \to 0$ as $y \to 1$, which is proposition I.3.1.13.

The proof of the second convergence result is similar (we get that $\|f * \psi_U - f\|_1 \leq \sup_{y\in U} \|R_y f - f\|_1$ and apply proposition I.3.1.13).

(2). Let $U \in \mathscr{U}$. Then for every $x \in G$,

$$|(\psi_U * f)(x) - f(x)| \leq \int_G \psi_U(y)|L_y f(x) - f(x)|dy.$$

As $\psi_U(y) = 0$ for $y \notin U$, this implies that

$$|(\psi_U * f)(x) - f(x)| \leq (\sup_{y\in U} |L_y f(x) - f(x)|)(\int_G \psi_U(y)dy) = \sup_{y\in U} |L_y f(x) - f(x)|.$$

Taking the supremum over $x \in G$ gives

$$\|\psi_U * f - f\|_\infty \leq \sup_{y\in U} \|L_y f - f\|_\infty.$$

So the first statement follows immediately from the definition of left uniform continuity. The proof of the second statement is similar.

□

**Corollary I.4.1.10.** *(1). The Banach algebra $L^1(G)$ is commutative if and only if the group $G$ is abelian.*

*(2). Let $\mathscr{I}$ be a closed linear subspace of $L^1(G)$. Then $\mathscr{I}$ is a left (resp. right) ideal if and only if it is stable under the operators $L_x$ (resp. $R_x$), $x \in G$.*

*Proof.* (1). If $G$ is abelian, then we have already seen that $L^1(G)$ is commutative. Conversely, suppose that $L^1(G)$ is commutative. Let $x, y \in G$. Let $f \in \mathscr{C}_c(G)$, and choose an approximate identity $(\psi_U)_{U\in\mathscr{U}}$. By proposition I.4.1.3, we have, for every $U \in \mathscr{U}$,

$$(R_x f) * (R_y \psi_U) = R_y((R_x f) * \psi_U) = R_y(\psi_U * (R_x f)) = R_y R_x(\psi_U * f) = R_{yx}(f * \psi_U)$$

and

$$(R_x f) * (R_y \psi_U) = (R_y \psi_U) * (R_x f) = R_x(f * (R_y \psi_U)) = R_x R_y(f * \psi_U) = R_{xy}(f * \psi_U).$$

Evaluating at 1 gives $(f*\psi_U)(xy) = (f*\psi_U)(yx)$. But proposition I.4.1.9 (and proposition I.1.12) implies that $\|f * \psi_U - f\|_\infty \to 0$ as $U \to \{1\}$, so we get

$$f(xy) = \lim_{U\to\{1\}} (f * \psi_U)(xy) = \lim_{U\to\{1\}} (f * \psi_U)(yx) = f(yx).$$

As this is true for every $f \in \mathscr{C}_c(G)$, we must have $xy = yx$ (this follows from local compactness and Urysohn's lemma). [11]

[11] reference ?

(2). We prove the result for left ideals (the proof for right ideals is similar). Suppose that $\mathscr{I}$ is a left ideal, and let $x \in G$. Choose an approximate identity $(\psi_U)_{U \in \mathscr{U}}$. We know that $\psi_U * f \to f$ in $L^1(G)$ as $U \to \{1\}$, and so $L_x(\psi_U * f) \to L_x f$ as $U \to \{1\}$ (because $L_x$ preserves the $L^1$ norm). But $L_x(\psi_U * f) = (L_x\psi_U) * f$ by proposition I.4.1.3; as $\mathscr{I}$ is a left ideal, we have $(L_x\psi_U) * f \in \mathscr{I}$ for every $U \in \mathscr{U}$, and as $\mathscr{I}$ is closed, this finally implies that $L_x f \in \mathscr{I}$.

Conversely, suppose that $\mathscr{I}$ is stable by all the operators $L_x$, $x \in G$. Let $f \in L^1(G)$ and $g \in \mathscr{I}$. By proposition I.4.1.3, we have $f * g = \int_G f(y) L_y g dy$. By the definition of the integral, the function $f * g$ is in the closure of the span of the $L_y g$, $y \in G$, and so it is in $\mathscr{I}$ by hypothesis (and because $\mathscr{I}$ is closed).

□

## I.4.2 Representations of $G$ vs representations of $L^1(G)$

**Definition I.4.2.1.** A *Banach $*$-algebra* is a Banach algebra $A$ with an involutive anti-automorphism $*$. (That is, for every $x, y \in A$ and $\lambda \in \mathbb{C}$, we have $(x+y)^* = x^* + y^*$, $(\lambda x)^* = \overline{\lambda} x^*$, $(xy)^* = y^* x^*$ and $(x^*)^* = x$.)

The anti-automorphism $*$ is called an *involution* on the Banach algebra $A$.

**Example I.4.2.2.** (a) $\mathbb{C}$, with the involution $z^* = \overline{z}$.

(b) If $G$ is a locally compact group with a left Haar measure, then $L^1(G)$ with the convolution product and the involution $*$ defined by $f^*(x) = \Delta(x)^{-1}\overline{f(x^{-1})}$ is a Banach $*$-algebra (note that $f^*$ is in $L^1(G)$ and that we have $\int_G f^*(x)dx = \int_G \overline{f(x)}dx$ and $\int_G |f^*(x)|dx = \int_G |f(x)|dx$ by proposition I.2.12; so $\|f^*\|_1 = \|f\|_1$). It is commutative if and only $G$ is abelian, and it has a unit if and only $G$ is discrete.

(c) If $X$ is a locally compact Hausdorff space, the space $\mathscr{C}_0(X)$ with the norm $\|.\|_\infty$, the usual (pointwise) multiplication and the involution $*$ defined by $f^*(x) = \overline{f(x)}$ is a commutative Banach $*$-algebra. It has a unit if and only if $X$ is compact (and the unit is the constant function 1).

(d) Let $H$ be a Hilbert space. Then $\mathrm{End}(H)$, with the operator norm and the involution $T \longmapsto T^*$ (where $T^*$ is the adjoint of $T$ as above) is a unital Banach $*$-algebra. It is commutative if and only if $\dim_{\mathbb{C}}(H) = 1$.

**Definition I.4.2.3.** (i) If $A$ and $B$ are two Banach $*$-algebras, a *$*$-homomorphism* from $A$ to $B$ is a morphism of $\mathbb{C}$-algebras $u : A \to B$ that is bounded as a linear operator and such that $u(x^*) = u(x)^*$, for every $x \in A$.

(ii) A *representation* of a Banach $*$-algebra $A$ on a Hilbert space $H$ is a $*$-homomorphism $\pi$ from $A$ to $\mathrm{End}(H)$. We say that the representation is *nondegenerate* if, for every $v \in H - \{0\}$, there exists $x \in A$ such that $\pi(x)(v) \neq 0$.

We will need the following result, which we will prove in the next section. (See corollary II.3.9.)

**Proposition I.4.2.4.** *Let $V$ be a Hilbert space. Then, for every $T \in \mathrm{End}(H)$ such that $TT^* = T^*T$, we have*

$$\|T\|_{op} = \lim_{n\to\infty} \|T^n\|_{op}^{1/n}.$$

**Corollary I.4.2.5.** *Let $A$ be a Banach $*$-algebra such that $\|x^*\| = \|x\|$ for every $x \in A$, and let $\pi$ be a representation of $A$ on a Hilbert space $V$. Then $\|\pi\|_{op} \leq 1$.*

*Proof.* By definition, the operator $\pi$ is bounded; let $C = \|\pi\|_{op}$. Let $x \in A$, and let $T = \pi(x^*x) \in \mathrm{End}(H)$. Note that $T = T^*$. For every $n \geq 1$, we have

$$\|T^n\| \leq C\|(x^*x)\|_1^n \leq C\|x\|^{2n}$$

(because $\|x^*\| = \|x\|$). On the other hand, we have

$$\|T\|_{op} = \lim_{n\to+\infty} \|T^n\|^{1/n}$$

by proposition I.4.2.4, hence

$$\|\pi(x)\|_{op} = \|\pi(x)^*\pi(x)\|_{op}^{1/2} = \|T\|_{op}^{1/2} \leq (\lim_{n\to+\infty} C^{1/n}\|x\|^{2n/n})^{1/2} = \|x\|.$$

In other words, $\|\pi\|_{op} \leq 1$.

□

We now fix a locally compact group $G$ as before. We will use vector-valued integrals, as defined in exercise I.5.6.1, and the properties proved in exercises I.5.6.2 and I.5.6.3.

**Theorem I.4.2.6.** *(1). Let $(\pi, V)$ be a unitary representation of $G$. We define a map from $L^1(G)$ to the space of linear endomorphisms of $V$, still denoted by $\pi$, in the following way : if $f \in L^1(G)$, we set*

$$\pi(f) = \int_G f(x)\pi(x)dx,$$

*by which we mean that*

$$\pi(f)(v) = \int_G f(x)\pi(x)(v)dx$$

*for every $v \in V$ (the integral converges by exercise I.5.6.3). Then this is a nondegenerate representation of the Banach $*$-algebra $L^1(G)$ on $V$, and moreover we have, for every $x \in G$ and every $f \in L^1(G)$,*

$$\pi(L_x f) = \pi(x)\pi(f) \quad \textit{and} \quad \pi(R_x f) = \Delta(x)^{-1}\pi(f)\pi(x)^{-1}.$$

*(2). Every nondegenerate representation $\pi$ of the Banach $*$-algebra $L^1(G)$ on a Hilbert space $V$ comes from a unitary representation $\pi$ of the group $G$ as in point (1).*

*Moreover, if $(\psi_U)_{U\in\mathscr{U}}$ is an approximate identity, then, for every $x \in G$ and every $v \in V$, we have*

$$\pi(x)(v) = \lim_{U\to\{1\}} \pi(L_x\psi_U)(v).$$

*(3). Let $(\pi, V)$ be a unitary representation of $G$, and $\pi : L^1(G) \to \mathrm{End}(V)$ be the associated $*$-homomorphism. Then a closed subspace $W$ of $V$ is $G$-invariant if and only if $\pi(f)(W) \subset W$ for every $f \in L^1(G)$.*

*(4). Let $(\pi_1, V_1)$ and $(\pi_2, V_2)$ be unitary representations of $G$, and $\pi_i : L^1(G) \to \mathrm{End}(V_i)$, $i = 1, 2$, be the associated $*$-homomorphisms. Then a bounded linear map $T : V_1 \to V_2$ is $G$-equivariant if and only if $T \circ \pi_1(f) = \pi_2(f) \circ T$ for every $f \in L^1(G)$.*

*Proof.* (1). If $f \in L^1(G)$, then the map $\pi(f) : V \to V$ is clearly $\mathbb{C}$-linear, and we have for every $v \in V$ :

$$\|\pi(f)(v)\| = \|\int_G f(x)\pi(x)(v)dx\| \le \int_G |f(x)|\|v\|dx \le \|v\|\|f\|_1,$$

so the endomorphism $\pi(f)$ of $V$ is bounded and $\|\pi(f)\|_{op} \le \|f\|_1$. Also, it is easy to see that the map $\pi : L^1(G) \to \mathrm{End}(H)$ sending $f$ to $\pi(f)$ is $\mathbb{C}$-linear, and the equality $\|\pi(f)\|_{op} \le \|f\|_1$ implies that it is also bounded (we also see that $\|\pi\|_{op}$ is bounded by 1, as it should according to corollary I.4.2.5).

Let $f, g \in L^1(G)$. Then, for every $v \in V$,

$$\begin{aligned}\pi(f * g)(v) &= \int_{G\times G} f(y)g(y^{-1}x)\pi(x)(v)dxdy \\ &= \int_G f(y)\left(\int_G g(y^{-1}x)\pi(x)(v)dx\right)dy \\ &= \int_G f(y)\left(\int_G g(x)\pi(yx)(v)dx\right)dy \\ &= \int_G f(y)\pi(y)(\pi(g)(v))dy \\ &= \pi(f)(\pi(g)(v)).\end{aligned}$$

So $\pi(f * g) = \pi(f) \circ \pi(g)$. Also,

$$\begin{aligned}\pi(f^*)(v) &= \int_G \Delta(x)^{-1}\overline{f(x^{-1})}\pi(x)(v)dx \\ &= \int_G \overline{f(x)}\pi(x^{-1})(v)dx \quad \text{by proposition I.2.12} \\ &= \int_G \overline{f(x)}\pi(x)^*(v)dx,\end{aligned}$$

so that, if $w \in V$,

$$\langle \pi(f^*)(v), w\rangle = \int_G \langle \overline{f(x)}\pi(x)^*(v), w\rangle dx = \int_G \langle v, f(x)\pi(x)(w)\rangle = \langle v, \pi(f)(w)\rangle.$$

This means that $\pi(f^*) = \pi(f)^*$. So we have proved that $\pi$ is a $*$-homomorphism.

Let $f \in L^1(G)$ and $x \in G$. Then, for every $v \in V$,

$$\begin{aligned}\pi(x)(\pi(f)(v)) &= \int_G f(y)\pi(x)(\pi(y)(v))dy \\ &= \int_G f(x^{-1}y)\pi(y)(v)dy \\ &\pi(L_x f)(v)\end{aligned}$$

and

$$\begin{aligned}\pi(f)(\pi(x)^{-1}(v)) &= \int_G f(y)\pi(y)(\pi(x^{-1})(v))dy \\ &= \Delta(x)\int_G f(yx)\pi(y)(v)dy \\ &= \Delta(x)\pi(R_x f)(v).\end{aligned}$$

Finally, we show that the representation $\pi : L^1(G) \to \mathrm{End}(V)$ is nondegenerate. Let $v \in V - \{0\}$, and choose a compact neighborhood $K$ of $1$ in $G$ such that $\|\pi(x)(v) - v\| \leq \frac{1}{2}\|v\|$ for every $x \in K$. Let $f = \mathrm{vol}(K)^{-1}\mathbb{1}_K$. Then

$$\|\pi(f)(v) - v\| = \frac{1}{\mathrm{vol}(K)}\|\int_K (\pi(x)(v) - v)dx\| \leq \frac{1}{2}\|v\|,$$

and in particular $\pi(f)(v) \neq 0$.

(2). Let $\pi$ be a nondegenerate representation of the Banach $*$-algebra $L^1(G)$ on a Hilbert space $V$. Choose an approximate identity $(\psi_U)_{U\in\mathscr{U}}$ of $G$. The idea of the proof is that $\pi(x)$ should be the limit of the $\pi(L_x\psi_U)$ as $U$ tends to $\{1\}$.

We now make the idea of proof above more rigorous. Note that, by corollary I.4.2.5, we have $\|\pi\|_{op} \leq 1$. Let $W$ be the span of the $\pi(f)(v)$, for $f \in L^1(G)$ and $v$. I claim thet $W$ is dense in $V$. Indeed, let $v \in W^\perp$. Then, for every $f \in L^1(G)$, we have $\langle \pi(f)(v), v'\rangle = \langle v, \pi(f^*)(v')\rangle = 0$ for all $v' \in V$, hence $\pi(f)(v) = 0$. As $\pi$ is nondegenerate, this is only possible if $v = 0$. Hence $W^\perp = 0$, which means that $W$ is dense in $V$.

Let $x \in G$. We want to define an element $\widetilde{\pi}(x) \in \mathrm{End}(V)$ such that, for every $f \in L^1(G)$, we have $\widetilde{\pi}(x)\pi(f) = \pi(L_x f)$. This forces us to define $\widetilde{\pi}(x)$ on an element $w = \sum_{j=1}^n \pi(f_j)(v_j)$ of $W$ ($f_j \in L^1(G)$, $v_j \in V$) as

$$\widetilde{\pi}(x)(w) = \sum_{j=1}^n \pi(L_x f_j)(v_j).$$

This is well-defined because, for every $\geq 1$, and for all $f_1, \ldots, f_n \in L^1(G)$ and $v_1, \ldots, v_n \in V$, we have

$$\begin{aligned}\sum_{j=1}^n \pi(L_x f_j)(v_j) &= \lim_{U \to \{1\}} \sum_{j=1}^n \pi(L_x(\psi_U * f_j))(v_j) \\ &= \lim_{U \to \{1\}} \sum_{j=1}^n \pi((L_x \psi_U) * f_j))(v_j) \\ &= \lim_{U \to \{1\}} \pi(L_x \psi_U) \left( \sum_{j=1}^n \pi(f_j)(v_j) \right)\end{aligned}$$

so $\sum_{j=1}^n \pi(L_x f_j)(v_j) = 0$ if $\sum_{j=1}^n \pi(f_j)(v_j) = 0$.

Moreover, as $\|\pi(L_x \psi_U)\|_{op} \leq \|\pi\|_{op} \|\psi_U\|_1 \leq 1$ for every $U \in \mathscr{U}$, we have $\|\widetilde{\pi}(x)(w)\| \leq \|w\|$ for every $w \in W$, so $\widetilde{\pi}(x)$ is a bounded linear operator of norm $\leq 1$ on $W$, hence extends by continuity to a bounded linear operator $\widetilde{\pi}(x) \in \mathrm{End}(V)$ of norm $\leq 1$.

Next, using the fact that $L_{xy} = L_x \circ L_y$, we see that, for all $x, y \in G$, $\widetilde{\pi}(xy) = \widetilde{\pi}(x)\widetilde{\pi}(y)$ on $W$, hence on all of $V$. Similarly, the fact that $L_1 = \mathrm{id}_{L^1(G)}$ implies that $\widetilde{\pi}(1) = \mathrm{id}_V$. Also, for every $x \in G$, we have, if $v \in V$,

$$\|v\| = \|\widetilde{\pi}(x^{-1})\widetilde{\pi}(x)(v)\| \leq \|\widetilde{\pi}(x^{-1})\|_{op} \|\widetilde{\pi}(x)(v)\| \leq \|\widetilde{\pi}(x)(v)\| \leq \|v\|,$$

so $\|\widetilde{\pi}(x)(v)\| = \|v\|$, i.e., $\widetilde{\pi}(x)$ is a unitary operator.

Let $v \in V$. We want to show that the map $G \to V$, $x \longmapsto \widetilde{\pi}(x)(v)$ is continuous. By proposition I.3.1.10, this will imply that $\widetilde{\pi} : G \to \mathrm{End}(V)$ is a unitary representation of $G$ on $V$. We first suppose that $v = \pi(f)(v')$, with $f \in L^1(G)$ and $v' \in V$. Then $\widetilde{\pi}(x)(v) = \pi(L_x f)(v')$, so the result follows from the continuity of the map $G \to L^1(G)$, $x \longmapsto L_x f$ (see proposition I.3.1.13), of $\pi$ and of the evaluation map $\mathrm{End}(V) \to V$, $T \longmapsto T(v')$. As finite sums of continuous functions $G \to V$ are continuous, we get the result for every $v \in W$. Now we treat the general case. Let $x \in G$ and $\varepsilon > 0$. We must find a neighborhood $U$ of $x$ in $G$ such that, for every $y \in U$, we have $\|\widetilde{\pi}(y)(v) - \widetilde{\pi}(x)(v)\| < \varepsilon$. Choose $w \in W$ such that $\|v - w\| < \varepsilon/3$, and a neighborhood $U$ of $x$ in $G$ such that, for every $y \in U$, we have $\|\widetilde{\pi}(y)(w) - \widetilde{\pi}(x)(w)\| < \varepsilon/3$ (this is possible by the first part of this paragraph). Then, for every $y \in U$, we have

$$\begin{aligned}\|\widetilde{\pi}(y)(v) - \widetilde{\pi}(x)(v)\| &\leq \|\widetilde{\pi}(y)(v) - \widetilde{\pi}(y)(w)\| + \|\widetilde{\pi}(y)(w) - \widetilde{\pi}(x)(w)\| + \|\widetilde{\pi}(x)(w) - \widetilde{\pi}(x)(v)\| \\ &< \|v - w\| + \varepsilon/3 + \|v - w\| \text{ (because } \widetilde{\pi}(x) \text{ and } \widetilde{\pi}(y) \text{ are unitary)} \\ &< \varepsilon,\end{aligned}$$

as desired.

We show that the representation $\widetilde{\pi}$ of $L^1(G)$ induced by $\widetilde{\pi}$ is the representation $\pi$ that we started from. Let $f, g \in L^1(G)$. Then, for every $v \in V$,

$$\begin{aligned}
\widetilde{\pi}(f)\pi(g)(v) &= \int_G f(x)\widetilde{\pi}(x)\pi(g)(v)dx \\
&= \int_G f(x)\pi(L_x g)(v)dx \\
&= \int_G \pi(f(x)L_x g)(v)dx \\
&= \pi\left(\int_G f(x)L_x g dx\right)(v) \\
&= \pi(f * g)(v) \\
&= \pi(f)\pi(g)(v).
\end{aligned}$$

So, if $f \in L^1(G)$, then $\widetilde{\pi}(f)$ and $\pi(f)$ are equal on $W$. As $W$ is dense in $V$, this implies that $\widetilde{\pi}(f) = \pi(f)$.

Finally, we show the last statement. Let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity as above. Let $x \in G$. We have already seen that, for every $v \in W$, we have

$$\widetilde{\pi}(x)(v) = \lim_{U\to\{1\}} \pi(L_x\psi_U)(v).$$

As both sides are continuous functions of $v \in V$ (for the right hand side, we use the fact that $\|\pi(L_x\psi_U)\|_{op} = 1$, this identity extends to all $v \in V$.

(3). Suppose that $W$ is $G$-invariant. Let $f \in L^1(G)$ and $w \in W$. As $\pi(f)(w) = \int_G f(x)\pi(x)(w)dx$ is a limit of linear combinations of elements of the form $\pi(x)(w)$, $x \in G$, it is still in $W$.

Conversely, suppose that $\pi(f)(W) \subset W$ for every $f \in L^1(G)$. Let $x \in G$, and let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity. Then, by the last statement of (2), for every $w \in W$, we have

$$\pi(x)(w) = \lim_{U\to\{1\}} \pi(L_x\psi_U)(w) \in W.$$

So $W$ is $G$-invariant.

(4). Let $T : V_1 \to V_2$ be a bounded linear map, and let $W \subset V_1 \times V_2$ be the graph of $T$; this is a closed linear subspace of $V_1 \times V_2$. Then $T$ is $G$-equivariant if and only $W$ is $G$-invariant, and $T$ is $L^1(G)$-equivariant if and only $W$ is stable by all the $\pi_1(f) \times \pi_2(f)$, $f \in L^1(G)$. So the conclusion follows from point (3).

□

**Example I.4.2.7.** Let $\pi$ be the representation of $G$ given by $\pi(x)(f) = L_x f$ (see example I.3.1.11). Then, for every $f, g \in L^1(G)$, we have $\pi(f)(g) = f * g$. Indeed, we have $\pi(f)(g) = \int_G f(x)L_x g dx$ by definition of $\pi(f)$, so the statement follows from exercise I.5.6.4.

## I.4.3 Convolution on other $L^p$ spaces

We will only see a few results that we'll need later to prove the Peter-Weyl theorem for compact groups. The most important case is that of $L^2(G)$.

Most of the results are based on Minkowski's inequality, which is proved in exercise I.5.6.7. Here, we only state it for functions on $G$.

**Proposition I.4.3.1** (Minkowski's inequality). *Let $p \in [1, +\infty)$, and let $\varphi$ be a function from $G \times G$ to $\mathbb{C}$. Then*

$$\left(\int_G \left|\int_G \varphi(x,y)d\mu(y)\right|^p d\mu(x)\right)^{1/p} \leq \int_G \left(\int_G |\varphi(x,y)|^p d\mu(x)\right)^{1/p} d\mu(y),$$

*in the sense that if the right hand side is finite, then $\int_G \varphi(x,y)d\mu(y)$ converges absolutely for almost all $x \in G$, the left hand side is finite and the inequality holds.*

**Corollary I.4.3.2.** *Let $p \in [1, +\infty)$, and let $f \in L^1(G)$ and $g \in L^p(G)$.*

*(1). The integral defining $f * g(x)$ converges absolutely for almost every $x \in G$, and we have $f * g \in L^p(G)$ and $\|f * g\|_p \leq \|f\|_1 \|g\|_p$.*

*(2). If $G$ is unimodular, then the same conclusions hold with $f * g$ replaced by $g * f$.*

*Proof.* (1). we apply Minkowski's inequality to the function $\varphi(x,y) = f(y)g(y^{-1}x)$. For every $y \in G$, we have

$$\int_G |\varphi(x,y)|^p d\mu(x) = |f(y)|^p \int_G |g(x)|^p d\mu(x) = |f(y)|^p \|g\|_p^p$$

by left invariance of $\mu$, so

$$\int_G \left(\int_G |\varphi(x,y)|^p d\mu(x)\right)^{1/p} d\mu(y) = \|g\|_p \int_G |f(y)| d\mu(y) = \|f\|_1 \|g\|_p.$$

Minkowski's inequality first says that $\int_G \varphi(x,y)d\mu(y) = f * g(x)$ converges absolutely for almost all $x \in G$, which is the first statement. The rest of Minkowski's inequality is exactly the fact that $\|f * g\|_p \leq \|f\|_1 \|g\|_p$.

(2). Suppose that $G$ is unimodular. Then

$$g * f(x) = \int_G g(y) f(y^{-1}x) d\mu(x) = \int_G g(xy^{-1}) f(y) d\mu(y).$$

So the proof is the same as in (1), by applying Minkowski's ineqality to the function $\varphi(x,y) = g(xy^{-1})f(y)$.

□

Now we generalize proposition I.4.1.9 to other $L^p$ spaces.

**Corollary I.4.3.3.** *Let $\mathscr{U}$ be a basis of neighborhoods of $1$ in $G$, and let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity with supports in $\mathscr{U}$. Then, for every $1 \leq p < +\infty$, if $f \in L^p(G)$, we have $\|\psi_U * f - f\|_p \to 1$ and $\|f * \psi_U - f\|_p \to 1$ as $U \to \{1\}$.*

*Proof.* Let $U \in \mathscr{U}$ and $f \in L^p(G)$. Then we have, for every $x \in G$,

$$\psi_U * f(x) - f(x) = \int_G \psi_U(y)(L_y f(x) - f(x))d\mu(y)$$

(because $\int_G \psi_U d\mu = 1$). Applying Minkowski's inequality to the function $\varphi(x,y) = \psi_U(y)(L_y f(x) - f(x))$, we get

$$\|\psi_U * f - f\|_p \leq \int_G \|L_y f - f\|_p \psi_U(y) d\mu(y) \leq \sup_{y\in U} \|L_y f - f\|_p.$$

Similarly, we have

$$\begin{aligned} f * \psi_U(x) - f(x) &= \int_G f(xy)\psi_U(y^{-1})d\mu(y) - f(x)\int_G \psi_U(y)d\mu(y) \\ &= \int_G (R_y f(x) - f(x))\psi_U(y)d\mu(y). \end{aligned}$$

So applying Minkowski's inequality to the function $\varphi(x,y) = (R_y f(x) - f(x))\psi_U(y)$ gives

$$\|f * \psi_U - f\|_p \leq \int_G \|R_y - f\|_p \psi_U(y) d\mu(y) \leq \sup_{y\in U} \|R_y f - f\|_p.$$

Hence both statements follow from proposition I.3.1.13.

□

Finally, we prove that the convolution product makes functions more regular in some cases. The most important case (for us) in the following proposition is when $G$ is compact and $p = q = 2$.

**Proposition I.4.3.4.** *Suppose that $G$ is unimodular. Let $p, q \in (1, +\infty)$ such that $p^{-1} + q^{-1} = 1$ and let $f \in L^p(G)$, $g \in L^q(G)$.*

*Then $f * g$ exists, $f * g \in \mathscr{C}_0(G)$ and $\|f * g\|_\infty \leq \|f\|_p \|g\|_q$.*

*Proof.* Let $x \in G$. We have

$$f * g(x) = \int_G f(y) R_x g(y^{-1}) d\mu(y).$$

As $G$ is unimodular, the function $y \longmapsto R_x g(y^{-1})$ is still in $L^q(G)$ and has the same $L^q$ norm as $g$. So, by Hölder's inequality,[12] the integral above converges absolutely and we have $|f * g(x)| \leq \|f\|_p \|g\|_q$. This proves the existence of $f * g$ and the result about its norm. It also shows that the bilinear map $L^p(G) \times L^q(G) \to L^\infty(G)$, $(f,g) \longmapsto f * g$ is continuous. As $\mathscr{C}_0(G)$ is closed in $L^\infty(G)$ and $\mathscr{C}_c(G)$ is dense in both $L^p(G)$ and $L^q(G)$, it suffices to prove that $f * g \in \mathscr{C}_0(G)$ if $f, g \in \mathscr{C}_c(G)$.

So let $f, g \in \mathscr{C}_c(G)$. Let $x \in G$, let $\varepsilon > 0$, and choose a neighborhood $U$ of $x$ such that, for every $y \in G$ and $x' \in U$, we have $|g(yx) - g(yx')| \leq \varepsilon$. Then, if $x' \in U$,

$$|f * g(x) - f * g(x')| \leq \int_G |f(y)||g(y^{-1}x) - g(y^{-1}x')| d\mu(y) \leq \varepsilon \int_G |f(y)| d\mu(y).$$

This shows that $f * g$ is continuous. Let $K = (\operatorname{supp} g)(\operatorname{supp} f)$; this is a compact subset of $G$. We want to show that $\operatorname{supp}(f * g) \subset K$, which will finish the proof. Let $x \in G$, and suppose that $f * g(x) \neq 0$. Then there exists $y \in G$ such that $f(y) g(y^{-1}x) \neq 0$. We must have $y \in \operatorname{supp} f$ and $y^{-1}x \in \operatorname{supp} g$, so $x \in y(\operatorname{supp} g) \subset K$.

$\square$

# I.5 Exercises

## I.5.1 Examples of topological groups

**Exercise I.5.1.1.** Let $V$ be a Banach space over $\mathbb{C}$. (That is, $V$ is a normed $\mathbb{C}$-vector space which is complete for the metric given by its norm.) We denote by $\operatorname{End}(V)$ the space of bounded linear operators from $V$ to itself, equipped with the operator norm. Remember that, if $\|.\|$ is the norm on $V$, then the operator norm $\|.\|_{op}$ is defined by : for every $f \in \operatorname{End}(V)$,

$$\|f\|_{op} = \inf\{c \in \mathbb{R}_{\geq 0} | \forall v \in V,\ \|f(v)\| \leq c\|v\|\} = \sup_{v \in V,\ \|v\|=1} \|f(v)\|$$

Let $\operatorname{GL}(V)$ be the group of invertible elements in $\operatorname{End}(V)$, with the topology induced by that of $\operatorname{End}(V)$.

(a). Show that $\operatorname{GL}(V)$ is an open subset of $\operatorname{End}(V)$.

(b). Show that $\operatorname{GL}(V)$ is a topological group.

(c). Show that $\operatorname{GL}(V)$ is locally compact if and only if $V$ is finite-dimensional.

*Solution.*

[12] Which reduces to the Cauchy-Schwarz inequality when $p = q = 2$.

(a). Note that, by definition of the operator norm, we have $\|xy\|_{op} \leq \|x\|_{op}\|y\|_{op}$ for all $x, y \in \mathrm{End}(V)$. (This property is called "submultiplicativity".) So, if $x \in \mathrm{End}(V)$ is such that $\|x\|_{op} < 1$, then the series $\sum_{n\geq 0} x^n$ converges (we take $x^0 = \mathrm{id}_V$ by convention), and we have $(\mathrm{id}_V - x)(\sum_{n\geq 0} x^n) = (\sum_{n\geq 0} x^n)(\mathrm{id}_V - x) = \mathrm{id}_V$. Hence, if $\|x\|_{op} < 1$, then $\mathrm{id}_V - x \in \mathrm{GL}(V)$.

Now let $x \in \mathrm{GL}(V)$. We want to show that $GL(V)$ contains a neighborhood of $x$ in $\mathrm{End}(V)$. Let $y \in \mathrm{End}(V)$ be such that $\|y\|_{op} < \|x^{-1}\|_{op}$. Then $\|x^{-1}y\|_{op} < 1$, so $\mathrm{id}_V - x^{-1}y$ is invertible, hence so is $x - y = x(\mathrm{id}_V - x^{-1}y)$. So every element $x'$ of $\mathrm{End}(V)$ such that $\|x - x'\|_{op} < \|x^{-1}\|_{op}$ is in $\mathrm{GL}(V)$, which proves the result.

If $V$ is finite-dimensional, we can also use tha fact that the determinant is a continuous map $\det : \mathrm{End}(V) \to \mathbb{C}$, and that $\mathrm{GL}(V)$ is the inverse image of the open subset $\mathbb{C}^\times$ of $\mathbb{C}$.

(b). Let's show that multiplication is a continuous map from $\mathrm{End}(V) \times \mathrm{End}(V)$ to $\mathrm{End}(V)$. (This implies immediately that multiplication is continuous on $\mathrm{GL}(V)$.) This follows immediately from the submultiplicativity of the operator norm. Indeed, if $x, x', y, y' \in \mathrm{End}(V)$, then we have

$$\|xy - x'y'\|_{op} = \|x(y - y') + (x - x')y'\|_{op} \leq \|x\|_{op}\|y - y'\|_{op} + \|x - x'\|_{op}\|y'\|_{op}.$$

Using the fact that

$$\|y'\|_{op} = \|y + (y' - y)\|_{op} \leq \|y\|_{op} + \|y - y'\|_{op},$$

we see that, if we fix $x$ and $y$, then $\|xy - x'y'\|_{op}$ tends to $0$ as $(\|x - x'\|_{op}, \|y - y'\|_{op})$ tends to $(0, 0)$.

Let's show that inversion is continuous on $\mathrm{GL}(V)$. Let $x \in \mathrm{GL}(V)$. Let $y \in \mathrm{End}(V)$, and write $h = x - y$ and $c = \|h\|_{op}\|x^{-1}\|_{op}$. Then $y = x - h = x(\mathrm{id}_V - x^{-1}h)$. We have seen in the answer of (a) that, if $c < 1$, then $y$ is invertible and $y^{-1} = (\sum_{n\geq 0}(x^{-1}h)^n)x^{-1} = x^{-1} + \sum_{n\geq 1}(x^{-1}h)^n x^{-1}$; in particular, we also have

$$\|y^{-1} - x^{-1}\|_{op} \leq \sum_{n\geq 1} \|(x^{-1}h)^n x^{-1}\|_{op} = \|x^{-1}\|_{op} \sum_{n\geq 1} c^n = \tfrac{c}{1-c}\|x^{-1}\|_{op}.$$

This shows that, if $x$ is fixed, then $\|x^{-1} - y^{-1}\|_{op}$ tends to $0$ as $\|x - y\|_{op}$ tends to $0$, which implies the result.

There is another way to prove the second point if $V$ is finite-dimensional. Indeed, in that case, we may assume that $V = \mathbb{C}^n$ for some $n \in \mathbb{N}$, so $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{C})$. Then we use the fact that, if $x \in \mathrm{GL}_n(\mathbb{C})$, the inverse of $x$ is equal to $(\det x)^{-1}y^T$, where $y$ is the matrix of cofactors of $x$. As the coefficients of $y$ are continuous functions of $x$ (because they are $\pm 1$ times determinants of submatrices of $x$), this shows that the coefficients of $x^{-1}$ are continuous functions of $x$.

(c). By (1)(a), a topological group is locally compact if and only its unit has a compact neighborhood. As $\mathrm{GL}(V)$ is open in $\mathrm{End}(V)$ by question (a), this implies that $\mathrm{GL}(V)$ is locally compact if and only if $e$ has an open neighborhood in $\mathrm{End}(V)$. As the topology of $\mathrm{End}(V)$ is defined by a norm, this is equivalent to the fact that closed balls in $\mathrm{End}(V)$ are compact. By Riesz's lemma, this is equivalent to the fact that $\mathrm{End}(V)$ is finite-dimensional. If $V$ is finite-dimensional, then $\mathrm{End}(V)$ is also finite-dimensional. If $V$ is infinite-dimensional, then it follows from the Hahn-Banach theorem that $\mathrm{End}(V)$ is also infinite-dimensional.

$\square$

**Exercise I.5.1.2.** Let $(G_i)_{i\in I}$ be a family of topological groups.

(a). Show that $\prod_{i\in I} G_i$ is a topological group (for the product topology).

(b). If all the $G_i$ are locally compact, is $\prod_{i\in I} G_i$ always locally compact ? (Give a proof or a counterexample.)

*Solution.*

(a). Let's show that multiplication is continuous. Let $(x_i),(y_i) \in \prod_{i\in I} G_i$. Let $U$ be a neighborhood of $(x_i y_i)$ in $\prod_{i\in I} G_i$. By the definition of the product topology, there exists a finite subset $J$ of $I$ and open neighborhoods $U_i$ of $x_i y_i$ in $G$, for $i \in J$, such that $U \supset (\prod_{i\in J} U_i) \times (\prod_{i\in I-J} G_i)$. By continuity of multiplication on the $G_i$ for $i \in J$, we can find, for every $i \in J$, open neighborhoods $V_i$ and $W_i$ of $x_i$ and $y_i$ such that $V_i W_i \subset U_i$. Let $V = (\prod_{i\in J} V_i) \times (\prod_{i\in I-J} G_i)$ and $W = (\prod_{i\in J} W_i) \times (\prod_{i\in I-J} G_i)$. Then $V$ and $W$ are open neighborhoods of $(x_i)$ and $(y_i)$ in $\prod_{i\in I} G_i$, and we have $VW \subset U$.

Let's show that inversion is continuous. (The proof is similar.) Let $(x_i) \in \prod_{i\in I} G_i$. Let $U$ be a neighborhood of $(x_i^{-1})$ in $\prod_{i\in I} G_i$. By the definition of the product topology, there exists a finite subset $J$ of $I$ and open neighborhoods $U_i$ of $x_i y_i$ in $G$, for $i \in J$, such that $U \supset (\prod_{i\in J} U_i) \times (\prod_{i\in I-J} G_i)$. By continuity of inversion on the $G_i$ for $i \in J$, we can find, for every $i \in J$, an open neighborhood $V_i$ of $x_i$ such that $V_i^{-1} \subset U_i$. Let $V = (\prod_{i\in J} V_i) \times (\prod_{i\in I-J} G_i)$. Then $V$ is an open neighborhood of $(x_i)$ in $\prod_{i\in I} G_i$, and we have $V^{-1} \subset U$.

(b). The answer is "no", as soon as infinitely many of $G_i$ are not compact. Indeed, let us denote by $p_j : \prod_{i\in I} G_i \to G_j$ the projection maps. These are continuous maps, so they send compact sets to compact sets. Now suppose that the set of $i \in I$ such that $G_i$ is not compact is infinite. If $\prod_{i\in I} G_i$ is locally compact, then its unit has a a compact neighborhood $K$. By the definition of the product topology, $K$ must contain a set $U$ of the form $(\prod_{i\in J} U_i) \times (\prod_{i\in I-J} G_i)$, where $J$ is a finite subset of $I$ and, for every $i \in J$, $U_i$ is a neighborhood of $e$ in $G_i$. By hypothesis, there exists $i \in I - J$ such that $G_i$ is not compact. But we have $G_i \supset p_i(K) \supset p_i(U) = G_i$, so $G_i = p_i(J)$ is compact, which is absurd.

Conversely, suppose that there exists a finite subset $J$ of $I$ such that $G_i$ is compact for every $i \in I - J$. Then $\prod_{i\in I} G_i$ is locally compact. Indeed, we have $\prod_{i\in I} G_i = (\prod_{i\in J} G_i) \times (\prod_{i\in I-J} G_i)$ and $\prod_{i\in I-J} G_i$ is compact by Tychonoff's theorem, so it suffices to prove that $\prod_{i\in J} G_i$ is locally compact. In other words, we may assume that $I$ is finite. But then, if $(x_i) \in \prod_{i\in I} G_i$ and $K_i$ is a compact neighborhood of $x_i$ for every $i \in I$, the product $\prod_{i\in I} K_i$ is a compact neighborhood of $(x_i)$.

□

**Exercise I.5.1.3.** Let $(I, \leq)$ be an ordered set. Consider a family $(X_i)_{i\in I}$ of sets and a family $(u_{ij} : X_i \to X_j)_{i\geq j}$ of maps such that :

- For every $i \in I$, we have $u_{ii} = \mathrm{id}_{X_i}$;
- For all $i \geq j \geq k$, we have $u_{ik} = u_{ij} \circ u_{jk}$.

This is called a *projective system of sets indexed by the ordered set $I$*. The *projective limit* of this projective system is the subset $\varprojlim_{i\in I} X_i$ of $\prod_{i\in I} X_i$ defined by :

$$\varprojlim_{i\in I} X_i = \{(x_i)_{i\in I} \in \prod_{i\in I} X_i | \forall i, j \in I \text{ such that } i \geq j,\ u_{ij}(x_i) = x_j\}.$$

(a). If all the $X_i$ are Hausdorff topological spaces and all the $u_{ij}$ are continuous maps, show that $\varprojlim_{i\in I} X_i$ is a closed subset of $\prod_{i\in I} X_i$. From now on, we will always put the induced topology on $\varprojlim_{i\in I} X_i$.

(b). If all the $X_i$ are compact Hausdorff topological spaces and all the $u_{ij}$ are continuous maps, show that $\varprojlim_{i\in I} X_i$ is also compact Hausdorff. (Hint : Tychonoff's theorem.)

(c). If all the $X_i$ are groups (resp. rings) and all the $u_{ij}$ are morphisms of groups (resp. of rings), show that $\varprojlim_{i\in I} X_i$ is a subgroup (resp. a subgroup) of $\prod_{i\in I} X_i$.

(d). If all the $X_i$ are topological groups and all the $u_{ij}$ are continuous group morphisms, show that $\varprojlim_{i\in I} X_i$ is a topological group.

(e). Let $p$ be a prime number. Take $I = \mathbb{N}$, with the usual order, $X_n = \mathbb{Z}/p^n\mathbb{Z}$ and $u_{nm} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ be the reduction modulo $p^m$ map. Show that $\mathbb{Z}_p := \varprojlim_{i\in I} X_i$ is a ring, and a compact topological group for the addition.

*Solution.*

(a). We write $X = \prod_{i\in I} X_i$ and $X' = \varprojlim_{i\in I} X_i$. For every $i \in I$, let $p_i : X \to X_i$ be the projection; this is a continuous map. Hence, if $i, j \in I$ are such that $i \geq j$, the subset $\{x \in X | u_{ij} \circ p_i(x) = p_j(x)\}$ of $X$ is closed (because it is the inverse image of the diagonal by the continuous map $(u_{ij} \circ p_i, p_j) : X \to X_j \times X_j$, and the diagonal of $X_j \times X_j$ is closed as $X_j$ is Hausdorff). But, by definition of the projective limit, we have

$$X' = \bigcap_{i,j\in I,\ i\geq j} \{x \in X | u_{ij} \circ p_i(x) = p_j(x)\}.$$

So $X'$ is also closed.

(b). If all the $X_i$ are compact Hausdorff topological spaces, then $X$ is compact Hausdorff by Tychonoff's theorem. By (a), the projective limit is a closed subspace of $X$, so it is also compact Hausdorff.

(c). We keep the notation of (a). Then all the projections $p_i$ are morphisms of groups (resp. rings), so, for all $i, j \in I$ such that $i \geq j$, the subset $\{x \in X | u_{ij} \circ p_i(x) = p_j(x)\}$ of $X$ is a subgroup (resp. subring). By definition of the projective limit, we have

$$X' = \bigcap_{i,j \in I,\ i \geq j} \{x \in X | u_{ij} \circ p_i(x) = p_j(x)\}.$$

So $X'$ is also a subgroup (resp. subring).

(d). By I.5.1.2(a), the direct product is a topological group. By question (c), the projective limit $X'$ is a subgroup of $X$. Hence $X'$ is a topological group.

(e). The set $\mathbb{Z}_p$ is a ring by question (c) and a topological group by question (d). It is compact by question (b) (note that finite sets with the discrete topology are compact Hausdorff).

□

**Exercise I.5.1.4.** Let $p$ be a prime number. We define the *$p$-adic norm* $|.|_p$ on $\mathbb{Q}$ in the following way :

- $|0|_p = 0$;
- if $x$ is a nonzero rational number, we write $x = p^n y$ with $y$ a rational number whose numerator and denominator are prime to $p$, and we set $|x|_p = p^{-n}$.

(a). Show that we have, for every $x, y \in \mathbb{Q}$ :

  - $|x + y|_p \leq \max(|x|_p, |y|_p)$, with equality if $|x|_p \neq |y|_p$;
  - $|xy|_p = |x|_p |y|_p$.

In particular, the $p$-adic distance function $d(x, y) = |x - y|_p$ is a metric on $\mathbb{Q}$. We denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ for this metric.

(a). Show that the $p$-adic norm $|.|_p$, the addition and the multiplication of $\mathbb{Q}$ extend to $\mathbb{Q}_p$ by continuity, that $\mathbb{Q}_p$ is a field (called the *field of $p$-adic numbers*), and that the statements of (a) extend to $\mathbb{Q}_p$.

(b). Show that the additive group of $\mathbb{Q}_p$ is a topological group.

(c). Calculate the subset $|\mathbb{Q}_p|_p$ of $\mathbb{R}$.

(d). Show that every open ball in $\mathbb{Q}_p$ is also a closed ball, and that every closed ball of positive radius in $\mathbb{Q}_p$ is also an open ball.

(e). Show that $\mathbb{Q}_p$ is totally disconnected (i.e. its only nonempty connected subsets are the singletons) but not discrete.

(f). Show that a series $\sum_{n\geq 0} x_n$ is convergent if and only if $\lim_{n\to+\infty} |x_n|_p = 0$.

(g). If $m \in \mathbb{Z}$ and $(c_n)_{n\geq m}$ is a family of integers, show that the series $\sum_{n\geq m} c_n p^n$ converges in $\mathbb{Q}_p$, and that its $p$-adic absolute value is $\leq p^{-m}$, with equality if $c_m$ is prime to $p$.

(h). Let $x \in \mathbb{Q}_p - \{0\}$. Show that there exists a unique $m \in \mathbb{Z}$ and a unique family $(c_n)_{n\geq m}$ of elements of $\{0, 1, \dots, p-1\}$ such that $x_m \neq 0$ and $x = \sum_{n\geq m} c_n p^n$, and that $|x|_p = p^{-m}$.

(i). Let $B = \{x \in \mathbb{Q}_p | \|x\|_p \leq 1\}$. Show that this is a subring of $\mathbb{Q}_p$, and the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

(j). We define a map $u$ from $B$ to $\prod_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z}$ in the following way : If $x \in B$, then, by question (e), we can find a Cauchy sequence $(x_n)_{n\geq 0}$ of elements of $\mathbb{Z}$ converging to $x$. After replacing it by a subsequence, we may assume that $|x - x_n|_p \leq p^{-n}$ for every $n$. We set $u(x) = (x_n \mod p^n\mathbb{Z})_{n\geq 0}$.

Show that $u$ is well-defined, a homeomorphism from $B$ to $\mathbb{Z}_p$, and that it is also a morphism of rings. We will use this to identify $B$ and $\mathbb{Z}_p$.

(k). We identify $M_n(\mathbb{Q}_p)$ with $\mathbb{Q}_p^{n^2}$, we put the product topology on it, and we use the induced topology on $\mathrm{GL}_n(\mathbb{Q}_p)$. Show that $\mathrm{GL}_n(\mathbb{Q}_p)$ is a locally compact topological group.

(l). Show that $\mathrm{GL}_n(\mathbb{Z}_p)$ is an open compact subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$. (Hint : Show that $\mathbb{Z}_p^\times$ is closed in $\mathbb{Z}_p$.)

*Solution.*

(a). We first note that, if $x \in \mathbb{Z} - \{0\}$, then we can write $x = p^m x'$ with $m \geq 0$ and $x' \in \mathbb{Z}$ prime to $p$, so $|x|_p = p^m \leq 1$. Of course, if $x = 0$, we also have $|x|_p \leq 1$.

We also note that it follows immediately from the definition of $|.|_p$ that, if $x \in \mathbb{Q}^\times$, we have $|x^{-1}|_p = |x|_p^{-1}$.

Let $x, y \in \mathbb{Q}_p$. If $x = 0$, then $x + y = y$ and $xy = 0$, so both points are obvious; the case $y = 0$ is similar. So we assume that both $x$ and $y$ are nonzero, and we write $x = p^n x'$ and $y = p^m y'$, with $x'$ and $y'$ rational numbers whose numerator and denominator are prime to $p$. Then the numerator and denominator of $x'y'$ are also prime to $p$, and $xy = p^{n+m}x'y'$, so

$$|xy|_p = p^{-n-m} = p^{-n}p^{-m} = |x|_p|y|_p.$$

To prove the first identity, note that, as the identity is symmetric in $x$ and $y$, we may assume that $n \leq m$. (Note that then we have $p^{-n} = |x|_p = \max(|x|_p, |y|_p)$.) We write $x' = \frac{a}{b}$ and $y' = \frac{c}{d}$, with $a, b, c, d \in \mathbb{Z}$ prime to $p$. Then

$$x + y = p^n(x' + p^{m-n}y) = p^n \frac{ad + p^{m-n}cb}{bd},$$

hence, by what we already proved,

$$|x + y|_p = |p^n|_p |ad + p^{m-n}bc|_p |bd|_p^{-1}.$$

As $bd$ is prime to $p$, we have $|bd|_p = 1$ (by definition of $|.|_p$). As $ad + p^{m-n}bc \in \mathbb{Z}$, we have $|ad + p^{m-n}cb|_p \leq 1$ by the remark at the beginning. Finally, we get

$$|x+y|_p \leq |p^n|_p = p^{-n} = \max(|x|_p, |y|_p).$$

Finally, if $|x|_p \neq |y|_p$, we have $n < m$, hence $ad + p^{m-n}cb$ is prime to $p$, and the definition of $|.|_p$ gives $|x+y|_p = p^{-n}$.

(b). By definition, $\mathbb{Q}_p$ is the set of Cauchy sequences $(x_n)_{n\geq 0}$ of elements of $\mathbb{Q}$ (for the metric given by the $p$-adic distance), modulo the equivalence relation $\sim$ defined by : $(x_n)_{n\geq 0} \sim (y_n)_{n\geq 0}$ if and only if $|x_n - y_n|_p \to 0$ as $n \to +\infty$.

Note that the second identity of (a) imply the triangle inequality : for all $x, y \in \mathbb{Q}$, we have $|x+y|_p \leq |x|_p + |y|_p$.

Let $x \in \mathbb{Q}_p$, and let $(x_n)_{n\geq 0}$ be a Cauchy sequence representing $x$. By the triangle inequality, we have, for all $n, m \in \mathbb{N}$, $||x_n|_p - |x_m|_p| \leq |x_n - x_m|_p$. So $(|x_n|_p)_{n\geq 0}$ is a Cauchy sequence in $\mathbb{R}$, and, as $\mathbb{R}$ is complete, it has a limit. Let $(y_n)_{n\geq 0}$ be another Cauchy sequence representing $x$. By the triangle inequality, we have $||x_n|_p - |y_n|_p| \leq |x_n - y_n|_p$ for every $n \geq 0$, so the limits of $(|x_n|_p)_{n\geq 0}$ and $(|y_n|_p)_{n\geq 0}$ are equal. Hence we can define $|x|_p$ by $|x|_p = \lim_{n\to+\infty} |x_n|_p$.

Now let $x, y \in \mathbb{Q}_p$, and choose Cauchy sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ representing $x$ and $y$. First note that the sequences $(|x_n|_p)_{n\geq 0}$ and $(|y_n|_p)_{n\geq 0}$ are bounded (for example because they converge, as we have seen above). Now, using (a), we get for all $n, m \in \mathbb{N}$ :

$$|(x_n + y_n) - (x_m + y_m)|_p \leq \max(|x_n - x_m|_p, |y_n + y_m|_p)$$

and

$$|x_n y_n - x_m y_m|_p = |x_n(y_n - y_m) + (x_n - x_m)y_m|_p \leq \max(|x_n|_p |y_n - y_m|_p, |y_m|_p |x_n - x_m|_p).$$

Hence the sequences $(x_n + y_n)_{n\geq 0}$ and $(x_n y_n)_{n\geq 0}$ are Cauchy sequences (for the second one, we use the fact that $(|x_n|_p)_{n\geq 0}$ and $(|y_n|_p)_{n\geq 0}$ are bounded), so they represent elements of $\mathbb{Q}_p$. We want to call these elements $x+y$ and $xy$, but first we have to check that they are independent of the choice of the Cauchy sequences representing $x$ and $y$. So let $(x'_n)_{n\geq 0}$ and $(y'_n)_{n\geq 0}$ be two other Cauchy sequences representing $x$ and $y$ respectively. Then we have, for every $n \geq 0$,

$$|(x_n + y_n) - (x'_n + y'_n)|_p \leq \max(|x_n - x'_n|_p, |y_n, y'_n|_p)$$

and

$$|x_n y_n - x'_n y'_n|_p = |x_n(y_n - y'_n) + (x_n - x'_n)y'_n|_p \leq \max(|x_n|_p |y_n - y'_n|_p, |y'_n|_p |x_n - x'_n|_p).$$

So both sequences $((x_n + y_n) - (x'_n + y'_n))_{n\geq 0}$ and $(x_n y_n - x'_n y'_n)_{n\geq 0}$ converge to $0$, which means that the sequences $(x_n + y_n)_{n\geq 0}$ and $(x'_n + y'_n)_{n\geq 0}$ (resp. $(x_n y_n)_{n\geq 0}$ and $(x'_n y'_n)_{n\geq 0}$) have the same limit, and so the definition of $x+y$ and $xy$ makes sense.

The ring axioms for $\mathbb{Q}_p$ follow immediately from the definition of the operations. Let's check that $\mathbb{Q}_p$ is a field. Let $x \in \mathbb{Q}_p - \{0\}$, and choose a Cauchy sequence $(x_n)_{n\geq 0}$ representing $x$. As $x \neq 0$, the sequence $(|x_n|_p)_{n\geq 0}$ cannot converge to $0$, so its limit (which is $|x|_p$) is nonzero. So we have $|x_n - x_m|_p \leq |x|_p/2$ for $n, m$ big enough, and, up to replacing $(x_n)_{n\geq 0}$ by an equivalent Cauchy sequence, we can assume that it is true for all $n, m \geq 0$. Let $n, m \geq 0$. By (a), we have $|x_n|_p \leq \max(|x_m|_p, |x_n - x_m|_p)$. Going to the limit as $m \to +\infty$, we get $|x_n|_p \leq |x|_p$. Similarly, going to the limit as $n \to +\infty$ and using the fact that $|x|_p > |x|_p/2 \geq \lim_{n\to+\infty} |x_n - x_m|_p$ gives $|x|_p \leq |x_m|_p$. This implies that $|x|_p = |x_n|_p$ for every $n \geq 0$. Now, if we can show that the sequence $(x_n^{-1})_{n\geq 0}$ is a Cauchy sequence, then the element of $\mathbb{Q}_p$ that it represents will clearly be an inverse of $x$. But we have, for all $n, m \geq 0$,

$$|x_n^{-1} - x_m^{-1}|_p = |x_n^{-1}x_m^{-1}|_p |x_m - x_n|_p = |x|_p^{-2} |x_m - x_n|_p,$$

so $|x_n^{-1} - x_m^{-1}|_p$ does converge to $0$ as $n, m \to +\infty$.

We finally prove that the identities of (a) stay true in $\mathbb{Q}_p$. If $x, y \in \mathbb{Q}_p - \{0\}$, then we just saw that we can find Cauchy sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ converging to $x$ and $y$ such that, for every $n \geq 0$, $|x|_p = |x_n|_p$ and $|y| = |y_n|_p$. Of course, this is also true if $x$ or $y$ is $0$. Then the identities follow immediately from (a) and from the definition of the operations on $\mathbb{Q}_p$.

(c). The addition on $\mathbb{Q}_p$ is continuous by definition (it is defined as the extension by continuity of a map). The inversion map $x \longmapsto -x$ is continuous because $|x|_p = |-x|_p$.

(d). We have seen that, if $x \in \mathbb{Q}_p$, then there is a Cauchy sequence of $\mathbb{Q}$ converging to $x$ and such that $|x|_p = |x_n|_p$ for every $n \geq 0$. So $|\mathbb{Q}_p|_p = |\mathbb{Q}|_p = \{0\} \cup p^{\mathbb{Z}}$.

(e). If $x \in \mathbb{Q}_p$ and $r \in \mathbb{R}$, we write $B(x, r)$ and $\overline{B}(x, r)$ for the open and closed balls of center $x$ and radius $r$.

Let $x \in \mathbb{Q}_p$. Let $r \in \mathbb{R}$. If $r \leq 0$, then $B(x, r) = \varnothing = \overline{B}(x, -1)$. Suppose that $r > 0$, and let $n$ be the unique integer such that $p^n < r \leq p^{n+1}$. By the previous question, if $a \in \mathbb{Q}_p$ is such that $|a|_p < r$, then $|a|_p \leq p^n$, and obviously the converse is true. So $B(x, r) = \overline{B}(x, p^n)$. Now let $m$ be the unique integer such that $p^m \leq r < p^{m+1}$. Then we see similarly that $\overline{B}(x, r) = B(x, p^{m+1})$.

(f). Let $x, y \in \mathbb{Q}_p$ such that $x \neq y$. Then $|x - y|_p > 0$, so we can choose $r > 0$ such that $r < |x - y|_p$. Then $B(x, r)$ is an open and closed subset of $\mathbb{Q}_p$ containing $x$ and not $y$, so $x$ and $y$ cannot be in the same connected subset of $\mathbb{Q}_p$. This shows that $\mathbb{Q}_p$ is totally disconnected.

To show that $\mathbb{Q}_p$ is not discrete, it suffices to show that its subset $\{0\}$ is not open. This follows from the fact that the sequence $(p^n)_{n\geq 0}$ converges to $0$ in $\mathbb{Q}_p$, and that $p^n \neq 0$ for every $n \in \mathbb{Z}$.

(g). Define a sequence $(S_n)_{n\geq 0}$ of rational numbers by $S_n = \sum_{i=0}^{n} x_n$. Then the series $\sum_{\geq 0} x_n$ converges if and only if the sequence $(S_n)_{n\geq 0}$. In particular, if the series converges, then

$|x_n|_p = |S_{n+1} - S_n|_p$ tends to $0$ as $n \to +\infty$.

Conversely, suppose that $\lim_{n\to+\infty} |x_n|_p = 0$. For all $n, n' \in \mathbb{N}$, if $n \le n'$, then (using (b)) :

$$|S_{n'} - S_n|_p = |\sum_{i=n+1}^{n'} x_i|_p \le \max_{n+1\le i\le n'} |x_i|_p \le \sup_{i\ge n+1} |x_i|_p.$$

This tends to $0$ as $n \to +\infty$, so $(S_n)_{n\ge0}$ is a Cauchy sequence, hence it converges in $\mathbb{Q}_p$, and so does the series $\sum_{n\ge0} x_n$.

(h). The convergence follows from the previous question and from the fact, noted in the proof of (b), that $|c|_p \le 1$ for every $c \in \mathbb{Z}$. Let $x = \sum_{n\ge m} c_m p^m$. By definition, we have

$$x = \lim_{n\to+\infty} \sum_{i=m}^{n} c_i p^i.$$

For every $n \ge m$, we have

$$|\sum_{i=m}^{n} c_i p^i|_p \le \max_{m\le i\le n} |c_i|_p |p^i|_p = p^{-m},$$

so $|x|_p \le p^{-m}$. Suppose that $c_m$ is prime to $p$; then $|c_m|_p = 1$. Hence $|c_m p^m|_p = p^{-m} > |c_i p^i|_p$ for every $i > m$, so, using (b) again, for every $n \ge m$,

$$|\sum_{i=m}^{n} c_i p^i|_p = p^{-m}.$$

This gives $|x|_p = p^{-m}$.

(i). Let's show existence. We may assume $x \ne 0$ (otherwise the result is trivial). We know that $|x|_p = p^{-m}$ for some $m \in \mathbb{Z}$. Choose a Cauchy sequence $(x_n)_{n\ge0}$ converging to $x$. After replacing $(x_n)_{n\ge0}$ by a subsequence, we may assume that $|x - x_n|_p < p^{-n}$ for every $n \ge 0$.

Let $n \ge 0$. We write $x_n$ in base $p$ as $x_n = \sum_{i=a_n}^{b_n} c_{i,n} p^i$, with $a_n, b_n \in \mathbb{Z}$ and $c_{i,n} \in \{0, 1, \dots, p-1\}$. We may assume that $c_{a_n,n} \ne 0$. Then $c_{a_n,n}$ is prime to $p$, so $|c_{a_n,n} p^{a_n}|_p = p^{-a_n} > |c_{i,n} p^i|$ for every $i > a_n$, and so (b) gives

$$p^{-m} = |x_n|_p = p^{-a_n},$$

hence finally $m = a_n$.

Also, we can replace $b_n$ by $+\infty$ in the expression for $x_n$, by setting $c_{i,n} = 0$ for $i > b_n$.

Let $n, n' \in \mathbb{N}$, and suppose that $n \ge n'$. Then $|x_n - x_{n'}|_p \le \max(|x_n - x|_p, |x - x_{n'}|_p) < p^{-n'}$. On the other hand, we have $x_n - x_{n'} = \sum_{i\ge m} (c_{i,n} - c_{i,n'}) p^i$. Note that the $c_{i,n} - c_{i,n'}$ are in $\{1-p, \dots, p-1\}$, so they are either $0$ or prime to $p$. By (h), this implies that $|x_n - x_{n'}|_p = p^{-r}$, where $r$ is the smallest integer such that $c_{r,n} - c_{r,n'} \neq 0$. This implies in turn that $n' < r$, that is, that $c_{i,n} = c_{i,n'}$ for $m \leq i \leq n'$.

We now define integers $c_i$, $i \geq m$, by $c_i = c_{0,i}$ if $i \leq 0$ and $c_i = c_{i,i}$ if $i \geq 0$. By the previous paragraph, $c_i = c_{i,n}$ if $0 \leq i \leq n$. For every $n \geq 0$, let $y_n = \sum_{i=m}^{n} c_i p^i$. Then

$$x_n - y_n = \sum_{i \geq m} (c_{i,n} - c_i) p^i = \sum_{i \geq n+1} (c_{i,n} - c_i) p^i,$$

so $|x_n - y_n|_p \leq p^{-n-1}$ by (h). Hence the sequence $(y_n)_{n \geq 0}$ also converges to $x$, and this shows that $x = \sum_{i \geq m} c_i p^i$.

Let's show uniqueness. Suppose that we have two sequences of integers $(c_n)_{n \geq m}$, $(d_n)_{n \geq m}$ such that $x = \sum_{n \geq m} c_n p^n = \sum_{n \geq m} d_n p^n$ and $c_n, d_n \in \{0, \dots, p-1\}$ for every $n$. Then $0 = \sum_{n \geq m} (c_n - d_n) p^n$. Also, for every $n$, $c_n - d_n$ is in $\{1-p, \dots, p-1\}$, so it is 0 or prime to $p$. If we had a $n$ such that $c_n - d_n \neq 0$, then this would imply $|0|_p \neq 0$ by (h), and this is impossible. So $c_n = d_n$ for every $n$.

(j). The fact that $B$ is a subring follows from (b) (and the fact that $|-x|_p = |x|_p$, which is obvious on the definition), and we have seen in the proof of (b) that $\mathbb{Z} \subset B$. Also, $B$ is a closed ball, so it is closed in $\mathbb{Q}_p$, and so it contains the closure of $\mathbb{Z}$.

Let $x \in B$. By (i), we can write $x = \sum_{n \geq 0} c_n p^n$, with $c_n \in \{0, \dots, p-1\}$. This means that $x$ is the limit of the sequence of integers $(\sum_{i=0}^{n} c_i p^i)_{n \geq 0}$, hence that $x$ is in the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

(k). We show that $u$ is well-defined. Let $x \in B$, and let $(x_n)_{n \geq 0}$, $(x'_n)_{n \geq 0}$ be two sequences as in the statement. Let $n \geq 0$. Then $|x_n - x'_n|_p \leq \max(|x_n - x|_p, |x - x'_n|_p) \leq p^{-n}$, which means that $p^n$ divides $x_n - x'_n$, and so $x_n$ and $x'_n$ have the same image in $\mathbb{Z}/p^n\mathbb{Z}$. This proves that $u(x)$ is well-defined.

The fact that $u$ is a morphism of rings follows immediately from the definition of the ring operations on $\mathbb{Q}_p$ and the fact that reduction modulo $p^n$ is a morphism of rings from $\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$ for every $n$.

We show that $u$ is injective. Let $x, y \in B$ such that $u(x) = u(y)$, and choose sequences $(x_n)_{n \geq 0}$, $(y_n)_{n \geq 0}$ converging to $x, y$ and satisfying the conditions of the statement. Then, for every $n \geq 0$, we have $x_n = y_n \mod p^n$, so $p^n$ divides $x_n - y_n$, i.e., $|x_n - y_n|_p \leq p^{-n}$. Going to the limit as $n \to +\infty$, we get $|x - y|_p = 0$. But we have seen in (b) that the only element of $\mathbb{Q}_p$ with $p$-adic norm 0 is 0, so $x = y$.

We show that $u$ is surjective. Let $(x_n + p^n\mathbb{Z})_{n \geq 0}$ be an element of $\mathbb{Z}_p$. For every $n \geq 0$, we choose a representative in $\{0, \dots, p^n - 1\}$ for $x_n + p^n\mathbb{Z}$, and we denote it by $x_n$. We also write $x_n$ in base $p$ as $x_n = \sum_{i=0}^{n-1} c_{i,n} p^i$, with $0 \leq c_{i,n} \leq p-1$. Let $m \geq n$. We know that $x_m = x_n \mod p^n$, so $c_{i,m} = c_{i,n}$ for $0 \leq i \leq n$. We define a sequence $(c_i)_{i \geq 0}$ by $c_i = c_{i,0} = c_{i,1} = \ldots = c_{i,i}$, and we set $x = \sum_{i \geq 0} c_i p^i \in \mathbb{Q}_p$. Then $x \in B$ by (c), and it is easy to check that $(x_n)_{n\geq 0}$ is a Cauchy sequence of integers converging to $x$ and satisfying the conditions of the statement. Hence $u(x) = (x_n + p^n\mathbb{Z})_{n\geq 0}$.

We show that $u$ is continuous. Every open set in $\mathbb{Z}_p$ is a union of open sets of the form $\mathbb{Z}_p \cap ((\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \ldots, x_0)\})$, with $m \geq 0$ and $x_i \in \mathbb{Z}/p^i\mathbb{Z}$ for $0 \leq i \leq m$. So it suffices to show that the inverse image of a set of that form is open in $B$. Write $A = (\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \ldots, x_0)\}$. Choose $x \in \mathbb{Z}$ such that $x = x_m \mod p^m$. Then we have $x = x_n \mod p^n$ for $0 \leq n \leq m$ (because $x_n = x_m \mod p^n$). We will show that $y \in B$ is in $u^{-1}(A)$ if and only if $|x - y|_p < p^{-m+1}$, which shows that $u^{-1}(A)$ is open. First note that, as the values of $|.|_p$ are always 0 or integer powers of $p$, the condition that $|x - y|_p < p^{-m+1}$ is equivalent to $|x - y|_p \leq p^{-m}$. [13] Let $y \in B$, and let $(y_n)_{n\geq 0}$ a Cauchy sequence converging to $y$ as in the definition of $u$. Suppose that $|x - y|_p \leq p^{-m}$. Then, for $n \in \{0, \ldots, m\}$, we have $|y_n - x|_p \leq \max(|y_n - y|_p, |y - x|_p) \leq p^{-n}$, hence $y_n = x = x_n \mod p^n$. So $u(y) \in A$. Conversely, suppose that $u(y) \in A$. Then $y_m = x_m = x \mod p^m$, so $|y_m - x|_p \leq p^{-m}$. As $|y - y_m|_p \leq p^{-m}$, this implies that $|x - y|_p \leq p^{-m}$.

Finally, we show that $u$ is open. As $u$ is bijctive, it suffices to show that the image of an open ball is open. We have more or less already done this : let $x \in B$, let $r \in \mathbb{R}_{>0}$, and let $A'$ be the open ball of center $x$ and radius $r$. If $m$ is the smallest integer such that $p^{-m} < r$, then $A'$ is also the closed ball of center $x$ and radius $p^{-m}$ (because $|.|_p$ has values in $\{0\} \cup p^{\mathbb{Z}}$). Let $y$ be an integer such that $|x - y|_p < p^{-m}$. Then the second identity of (a) implies that, for $z \in \mathbb{Q}_p$, we have $|x - z|_p \leq p^{-m}$ if and only if $|y - z|_p \leq p^{-m}$, which means that we can replace $x$ by $y$ in the definition of $A'$. Then we have already seen above that $u(A') = (\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \ldots, x_0)\}$, where $x_n = y + p^n\mathbb{Z}$ for $0 \leq n \leq m$.

(l). The proof that $\mathrm{GL}_n(\mathbb{Q}_p)$ is a topological group is the same as in I.5.1.2(b) (the finite-dimensional case). It is also open in $M_n(\mathbb{Q}_p)$, because it is the inverse image by the continuous function $\det$ of the open subset $\mathbb{Q}_p^\times$ of $\mathbb{Q}_p$. So to show that $\mathrm{GL}_n(\mathbb{Q}_p)$ is locally compact, it suffices to show that $M_n(\mathbb{Q}_p)$ is locally compact, which will follow if we know that $\mathbb{Q}_p$ is locally compact. But for every $x \in \mathbb{Q}_p$, the closed ball of radius 1 centered at $x$, which is $x + \mathbb{Z}_p$, is a compact neighborhood of $x$ : it is compact because $\mathbb{Z}_p$ is compact and translation by $x$ is continuous (by definition of the metric), and it is open because it is equal to the open ball of center $x$ and radius $p$.

(m). Remember that $\mathrm{GL}_n(\mathbb{Z}_p)$ is the group of invertible elements of $M_n(\mathbb{Z}_p)$, so we have

$$\mathrm{GL}_n(\mathbb{Z}_p) = \{A \in \mathrm{GL}_n(\mathbb{Q}_p) \mid A \text{ and } A^{-1} \in M_n(\mathbb{Z}_p)\}.$$

In other words, $\mathrm{GL}_n(\mathbb{Z}_p)$ is the inverse image by the continuous map $\mathrm{GL}_n(\mathbb{Q}_p) \to M_n(\mathbb{Q}_p) \times M_n(\mathbb{Q}_p)$, $A \longmapsto (A, A^{-1})$ of the open subset $M_n(\mathbb{Z}_p) \times M_n(\mathbb{Z}_p)$ of $M_n(\mathbb{Q}_p) \times M_n(\mathbb{Q}_p)$, so it is open in $\mathrm{GL}_n(\mathbb{Q}_p)$. As $M_n(\mathbb{Z}_p)$ is compact (because $\mathbb{Z}_p$ is), to show that $\mathrm{GL}_n(\mathbb{Z}_p)$ is compact, it suffices to show that it is closed in $M_n(\mathbb{Z}_p)$. As it is the inverse image of $\mathbb{Z}_p^\times$ by the continuous map $\det : M_n(\mathbb{Z}_p) \to \mathbb{Z}_p$, it suffices to show

[13] So, in $\mathbb{Q}_p$, every open ball is a closed ball and vice versa.

that $\mathbb{Z}_p^\times$ is closed in $\mathbb{Z}_p$. But $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \| x|_p = 1\}$ (which implies that it is closed). Indeed, let $x \in \mathbb{Z}_p$. If $x$ has an inverse in $\mathbb{Z}_p$, then $|x^{-1}|_p = |x|_p^{-1} \leq 1$, so $|x|_p \geq 1$, hence $|x|_p = 1$. Conversely, if $|x|_p = 1$, then $|x^{-1}|_p = 1$, so $x^{-1} \in \mathbb{Z}_p$.

□

## I.5.2 Van Dantzig's theorem

[14]

**Exercise I.5.2.1.** In this problem, $X$ is a compact Hausdorff totally disconnected topological space. (Remember that "totally disconnected" means that the only nonempty connected subsets of $X$ are the singletons.)

Let $x \in X$, and let $A$ be the intersection of all the open and closed subsets of $X$ containing $x$. Show that $A = \{x\}$. (Hint : This is equivalent to showing that $A$ is connected. And remember also that disjoint closed sets can be separated by open sets in any compact Hausdorff space.)

*Solution.* Note that $A$ is closed in $X$. Suppose that we have $A = A_1 \cup A_2$, with $A_1$ and $A_2$ closed in $X$ and disjoint and $x \in A_1$. As any compact Hausdorff space is normal, we can find open subsets $U_1 \supset A_1$ and $U_2 \supset A_2$ of $X$ such that $U_1 \cap U_2 = \varnothing$. Let's find a closed and open neighborhood $V$ of $x$ such that $V \cap \partial U_2 = \varnothing$. For every $y \in \partial U_2$, as $y \notin A$, we can find a closed and open neighborhood $V_y$ of $x$ such that $y \notin V_y$. Note that the $X - V_y$, $y \in \partial U_2$, form a family of open subsets of $X$ covering $\partial U_2$; as $\partial U_2$ is compact, this family has a finite subfamily that still covers $\partial U_2$, say $(X - V_{y_1}, \dots, X - V_{y_n})$. Let $V = V_{y_1} \cap \dots \cap V_{y_n}$; then $V$ is still open and closed, $x \in V$ and $V \cap \partial U_2 = \varnothing$. The last property implies that $B := V - U_2$ is also equal to $V - \overline{U}_2$, so it still open and closed. Also, we have $x \in B$ (because $x \notin U_2$), and $A_2 \cap B = \varnothing$. But $A$ must be contained in $B$ by definition, so $A_2 = \varnothing$. This proves that $A$ is connected, hence a singleton, hence equal to $\{x\}$.

□

**Exercise I.5.2.2.** In this problem, $G$ is a locally compact totally disconnected topological group.

(a). Show that the unit of $G$ has a compact open neighborhood $K$.

(b). Show that there exists an open subgroup $G'$ of $G$ contained in $K$. (Hint : Any open subset of $G$ will generate an open subgroup. Choose your open subset wisely.)

(c). Show that the compact open subgroups of $G$ form a basis of neighborhoods of $1$ in $G$.

(d). Let $G$ be the group $\mathrm{GL}_n(\mathbb{Q}_p)$ of exercise I.5.1.4. Find a basis of neighborhoods of $1$ in $G$ that is composed of compact open subgroups.

[14]From Terry Tao's blog.

*Solution.*

(a). Let $V$ be a compact neighborhood of $1$. Then $\partial V$ is also compact and doesn't contain $1$. By problem I.5.2.1, for every $y \in \partial V$, there exists an open and closed neighborhood $B_y$ of $1$ such that $B_y \cap \partial V = \varnothing$. As $\partial V \subset \bigcup_{y \in \partial V}(X - B_y)$ and the $X - B_y$ are open, there exist $y_1, \dots, y_n \in \partial V$ such that $\partial V \cap B = \varnothing$, with $B = \bigcap_{i=1}^{n} B_{y_i}$. Note that $B$ is still open and closed, and that $1 \in B$. Also, as $\partial V \cap B = \varnothing$, we have $B \cap V = B \cap \overset{\circ}{V}$, and so $K := B \cap V$ is open and compact (because it is closed in $V$) and contains $1$.

(b). Let $U$ be an open symmetric neighborhood of $1$ such that $UK \subset K$, and let $G'$ be the subgroup of $G$ generated by $U$. Let's show that $G'$ is an open compact subgroup of $G$ and that $G' \subset K$. First we show that $G'$ is open. Let $g \in G'$; then $gU \subset G'$ and $gU$ is open in $G$, so $G'$ contains a neighborhood of $G$. As every open subgroup of a topological group is also closed, we also get that $G'$ is closed. So, to show that is compact, it suffices to show that it is contained in $K$. Note that, as $U$ is symmetric and contains $1$, we have $G' = \bigcup_{n \geq 1} U^n$. As $U \subset K$ (because $1 \in K$) and $UK \subset K$, an easy induction shows that $U^n \subset K$ for every $n \geq 1$. So $G' \subset K$.

(c). The argument in the solution of question (a) actually shows that every compact neighborhood of $1$ contains an open compact neighborhood of $1$, and then question (b) implies that it also contains a compact open subgroup of $G$. Hence, as $G$ is locally compact, every neighborhood of $1$ in $G$ contains a compact open subgroup of $G$.

(d). Let's choose a norm on $M_n(\mathbb{Q}_p)$ that induces the product topology. For example, the norm $\|.\|$ defined by

$$\|(a_{ij})_{1 \leq i,j \leq n} - (b_{ij})_{1 \leq i,j \leq n}\| = \sup_{1 \leq i,j \leq n} |a_{ij} - b_{ij}|_p$$

works. For every integer $m \geq 1$, let $K_m = I_n + p^m M_n(\mathbb{Z}_p)$. With our choice of norm, this is just the open ball of center $I_n$ and radius $p^{-m+1}$ in $M_n(\mathbb{Q}_p)$ (and also the closed ball of center $I_n$ and radius $p^{-m}$). In particular, the sets $K_m$, for $m \geq 1$, form a family of open neighborhoods of $I_n$ in $M_n(\mathbb{Q}_p)$, and hence the sets $K_m$ for $m >> 0$ form a family of open neighborhoods of $I_n$ in $\mathrm{GL}_n(\mathbb{Q}_p)$ (because $\mathrm{GL}_n(\mathbb{Q}_p)$ is open in $M_n(\mathbb{Q}_p)$, as the preimage by the continuous map $\det$ of the open subset $\mathbb{Q}_p^\times$ of $\mathbb{Q}_p$).

Note also that $K_m$ is homeomorphic to $M_n(\mathbb{Z}_p) \simeq \mathbb{Z}_p^{n^2}$ (by the map $I_n + p^m X \longmapsto X$), so it is also compact.

At this point, we have our basis of neighborhoods consisting of compact open subgroups. We can actually be more precise and show that $K_m \subset \mathrm{GL}_n(\mathbb{Q}_p)$ for every $m \geq 1$ (and not just for $m$ big enough), which just means that $K_1 \subset \mathrm{GL}_n(\mathbb{Q}_p)$. In fact, we even have $K_1 \subset \mathrm{GL}_n(\mathbb{Z}_p)$. Indeed, it is clear that $K_1 \subset M_n(\mathbb{Z}_p)$. Moreover, if $X \in K_1$, then it is easy to see that $\det(X) \in 1 + p\mathbb{Z}_p \subset \mathbb{Q}_p$, which implies that $|\det(X)|_p = 1$ (by question I.5.1.4(a)), hence that $\det(X)^{-1}$ is also in $\mathbb{Z}_p$, i.e., that $\det(X) \in \mathbb{Z}_p^\times$.

$\square$

## I.5.3 Examples of Haar measures

**Exercise I.5.3.1.** Let $G$ be a topological group. Suppose that we have a homeomorphism of $G$ with an open subset of some $\mathbb{R}^N$ (not necessarily compatible with any groups structures), such that left translations on $G$ are given by affine maps. That is, if we identify $G$ with its image in $\mathbb{R}^N$ (as a topological space only !), then, for every $x \in G$, there is a $N \times N$ matrix $A(x) \in M_N(\mathbb{R})$ and an element $b(x) \in \mathbb{R}^N$ such that, for every $y \in G$, we have $xy = A(x)y + b(x)$.

Show that $|\det A(x)|^{-1}dx$ is a left Haar measure on $G$, where $dx$ denotes the Lebesgue measure on $\mathbb{R}^N$. (Hint : The change-of-variable formula. Also, start by proving that $x$ uniquely determines $A(x)$ and $b(x)$, and that $x \longmapsto A(x)$ is a morphism of groups from $G$ to $\mathrm{GL}_N(\mathbb{R})$.)

*Solution.* Let $x \in G$. Suppose that we have $A, A' \in M_N(\mathbb{R})$ and $b, b' \in \mathbb{R}^N$ such that, for every $y \in G$, $xy = Ay + b = A'y + b'$. Then $(A - A')y = b' - b$ for every $y \in G$. But the set of solutions the equation $(A - A')y = b' - b$ is an affine subspace of $\mathbb{R}^N$ (i.e. a translate of a linear subspace), so it has empty interior unless it is equal to $\mathbb{R}^N$. As $G$ is open in $\mathbb{R}^N$, this means that we must have $(A - A')y = b' - b$ for every $y \in \mathbb{R}^N$. The only way this is possible is if $\mathrm{Ker}(A - A') = \mathbb{R}^N$, hence $A = A'$, and then we also have $b = b'$. So $x$ determines $A(x)$ and $b(x)$.

We prove that $A(x)$ is invertible for every $x \in G$. Indeed, if $A(x)$ is not invertible, then the image of the map $G \to G$, $y \longmapsto xy$ is contained in $b(x) + \mathrm{Im}(A(x))$, which is the translate by $b(x)$ of a proper linear subspace of $\mathbb{R}^N$, and hence it has empty interior. But this image must be equal to $G$, hence be an open subset of $\mathbb{R}^N$, so we get a contradiction, and so $A(x)$ must be invertible.

We prove that $x \longmapsto A(x)$ is a morphism of groups. Let $x_1, x_2 \in G$. For every $y \in G$, we have

$$A(x_1x_2)y + b(x_1x_2) = x_1x_2y = A(x_1)A(x_2)y + A(x_1)b(x_2) + b(x_1).$$

By the first paragraph, this implies that $A(x_1x_2) = A(x_1)A(x_2)$ and $b(x_1x_2) = A(x_1)b(x_2) + b(x_1)$.

Now remember that the change of variable formula implies that, if $U$ is a measurable subset of $\mathbb{R}^N$, if $A \in \mathrm{GL}_N(\mathbb{R})$ and $b \in \mathbb{R}^N$, and if $V$ is the image of $U$ by the transformation $y \longmapsto Ay+b$, then we have, for every $f \in L^1(V)$,

$$\int_V f(v)dv = |\det A| \int_U f(Ay + b)dy.$$

Applying this to $U = V = G$, $A = A(y)$ and $b = b(y)$ for some $y \in G$, we get, for every $f \in L^1(G)$,

$$\int_G f(x)dx = |\det A(y)| \int_G f(yx)dx.$$

Let $f \in \mathscr{C}_c(G)$. Then the function $x \longmapsto |\det A(x)|^{-1} f(x)$ is also in $\mathscr{C}_c(G)$, so we can apply the previous paragraph to it. We get, for every $y \in G$,

$$\int_G f(yx)|\det A(yx)|^{-1} dx = |\det A(y)|^{-1} \int_G f(x)|\det A(x)|^{-1} dx.$$

Using the fact that $\det(A(xy)) = \det(A(x))\det(A(y))$, we can divide both sides by $|\det(A(y))|^{-1}$, and we get

$$\int_G f(yx)|\det A(x)|^{-1} dx = \int_G f(x)|\det A(x)|^{-1} dx,$$

which is the desired result.

□

**Exercise I.5.3.2.** In this problem, $dx$ will always be the Lebesgue measure on $\mathbb{R}$.

(a). Show that $\frac{dx}{|x|}$ is a Haar measure on the multiplicative group $\mathbb{R}^\times$.

(b). Show that $\frac{dxdy}{x^2+y^2}$ is a Haar measure on the multiplicative group $\mathbb{C}^\times$, with coordinates $z = x + iy$.

(c). Let $dT$ be the Lebesgue measure on $M_n(\mathbb{R})$. Show that $|\det T|^{-n} dT$ is a left and right Haar measure on $\mathrm{GL}_n(\mathbb{R})$.

(d). Let $G = \{\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} | x, z \in \mathbb{R}^\times, y \in \mathbb{R}\}$. Show that $\frac{dxdydz}{x^2|z|}$ is a left Haar measure on $G$. Is it a right Haar measure ?

*Solution.* Of course, we will use the previous exercise to solve every question.

(a). The obvious inclusion $\mathbb{R}^\times \subset \mathbb{R}$ makes $\mathbb{R}^\times$ an open subset of $\mathbb{R}$. Let $x \in \mathbb{R}\times$. Then, for every $y \in \mathbb{R}^\times$, we have $xy = A(x)y + b(x)$ with $A(x) = x \in \mathrm{GL}_1(\mathbb{R})$ and $b(x) = 0$. So the result follows from the fact that $\det(A(x)) = x$.

(b). We embed $\mathbb{C}^\times$ into $\mathbb{R}^2$ by the map $z \longmapsto (\mathrm{Re}(z), \mathrm{Im}(z))$. This makes $\mathbb{C}^\times$ into an open subset of $\mathbb{R}^2$. Let $z = x + iy \in \mathbb{C}^\times$, with $x, y \in \mathbb{R}$. Then left translation by $z$ on $\mathbb{C}^\times$ is given by left multiplication by the $2 \times 2$ matrix $A(z) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ (this is just the formula $(x + iy)(a + ib) = (xa - yb) + i(ya + xb)$). So the result follows from the fact that $\det(A(z)) = x^2 + y^2$.

(c). The group $\mathrm{GL}_n(\mathbb{R})$ is an open subset of $M_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$ (because it is given by the equation $\det(x) \neq 0$). Let $x \in \mathrm{GL}_n(\mathbb{R})$. Then left translation by $x$ on $M_n(\mathbb{R})$ is a linear transformation, and we need to calculate its determinant. Note that $M_n(\mathbb{R}) = \mathbb{R}^n \oplus \ldots \oplus \mathbb{R}^n$, where we have $n$ summands, correponding to the $n$ columns of a $n \times n$ matrix. Left multiplication by $x$ preserves this decomposition, and the determinant of its action on each summand is the determinant of the usual action of $x$ on $\mathbb{R}^n$,i.e., $\det(x)$. So the determinant of left translation by $x$ on $M_n(\mathbb{R})$ is $\det(x)^n$.

To see that $|\det(T)|^{-n} dT$ is also a right Haar measure, we use the obvious analogue of the previous problem with left translations replaced by right translations, and we see as above that the determinant of the action of $x \in \mathrm{GL}_n(\mathbb{R})$ by right translation on $M_n(\mathbb{R})$ is $\det(x)^n$.

(d). We embed $G$ as a open subset of $\mathbb{R}^3$ by sending $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ to $(x, y, z)$. Let $g = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in G$. Using the fact that

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xb + yc \\ 0 & zc \end{pmatrix},$$

we see that we are in the situation of the previous problem, with

$$A(g) = \begin{pmatrix} x & 0 & 0 \\ 0 & x & y \\ 0 & 0 & z \end{pmatrix}$$

and $b(g) = 0$. So $\det(A(g)) = x^2 z$, and we get the result.

As in (c), using the analogue previous problem for right translations, we see that the action of $g$ on $G$ by right translation is linear and given by the matrix

$$\begin{pmatrix} x & 0 & 0 \\ y & z & 0 \\ 0 & 0 & z \end{pmatrix},$$

whose determinant is $xz^2$. So $\frac{dxdydz}{|x|z^2}$ is a right Haar measure on $G$. It is not of the form $c\frac{dxdydz}{x^2|z|}$ with $c$ a constant, hence $\frac{dxdydz}{x^2|z|}$ cannot be a right Haar measure.

□

**Exercise I.5.3.3.** Consider the group $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$.

(a). Show that there exists a Haar measure $\mu$ on $G$ such that $\mu(G) = 1$.

(b). Show that every open subset of $G$ is a countable union of set of the form $U = V \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}}$, with $n \in \mathbb{N}$ and $V \subset (\mathbb{Z}/2\mathbb{Z})^{\{0,\ldots,n\}}$, and that we have $\mu(U) = \frac{|V|}{2^{n+1}}$.

(c). Consider the map $u : G \to [0, 1]$ sending $(x_n)_{n\in\mathbb{N}} \in G$ to $\sum_{n\geq 0} x_n 2^{-n-1}$. (We identify $\mathbb{Z}/2\mathbb{Z}$ with $\{0, 1\}$ in the defintion of $u$.) Show that $u$ is measurable and maps $\mu$ to Lebesgue measure $\lambda$ on $[0, 1]$. That is, show that, if $B \subset [0, 1]$ is a Borel set, then $u^{-1}(B)$ is a

Borel set and $\lambda(B) = \mu(u^{-1}(B))$. (Hint : Show that the half-open intervals of the form $[j2^{-k}, (j+1)2^{-k}]$ generate the Borel $\sigma$-algebra on $[0,1]$, and calculate their inverse images by $u$.)

*Solution.*

(a). Let $\mu$ be a left Haar measure on $G$. As $G$ is commutative, $\mu$ is also a right Haar measure. Also, by I.5.1.3(b), the group $G$ is compact, so $\mu(G) < +\infty$, and, after multiplying $\mu$ by $\mu(G)^{-1}$, we may assume that $\mu(G) = 1$.

(b). By definition of the product topology, every open subset of $G$ is a union of sets $U$ of the form $V \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}-I}$, with $I \subset \mathbb{N}$ finite and $V \subset (\mathbb{Z}/2\mathbb{Z})^I$. As every finite subset of $\mathbb{N}$ is included in a set of the form $\{0,1,\dots,n\}$, we may assume that $I = \{0,1,\dots,n\}$ for some $n \in \mathbb{N}$. We still need to show that we can the union to be countable. Suppose that we have an open set $\Omega$ of $G$ of the form $\bigcup_{i\in I} U_i$, with $U_i = V_i \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n_i+1}}$ and $V_i \subset (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n_i\}}$. For every $n \in \mathbb{N}$, let $I_n = \{i \in I | n_i = n\}$. Then

$$\bigcup_{i\in I_n} U_i = V_n \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}},$$

with

$$V_n = \bigcup_{i\in I_n} V_i \subset (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}.$$

Hence $\Omega = \bigcup_{n\in\mathbb{N}} V_n \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}}$.

Now we calculate $\mu(U)$, for $U = V \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}}$, with $V \subset (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}$. We write $W = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}}$. If $v, v' \in (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}$, then $\{v\} \times W = (v' - v) + \{v'\} \times W$, so $\mu(\{v\} \times W) = \mu(\{v'\} \times W)$. As $G = \coprod_{v\in(\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}} \{v\} \times W$, this implies that, for every $v \in (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}$,

$$1 = \mu(G) = |(\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}| \mu(\{v\} \times W),$$

hence $\mu(\{v\}) = \frac{1}{2^{n+1}}$. On the other hand, we have $U = \coprod_{v\in V} \{v\} \times W$, so we get $\mu(U) = \frac{|V|}{2^{n+1}}$.

(c). Write $I_{j,k} = [j2^{-k}, (j+1)2^{-k}]$. We first show that the $I_{j,k}$, for $k \geq 0$ and $0 \leq j \leq 2^k - 1$, generate the Borel $\sigma$-algebra on $[0,1]$. Every open subset of $[0,1]$ is a countable union of open intervals $(a,b)$ with $0 \leq a < b \leq 1$, and optionally of one or both of the half-open intervals $[0,b)$, $0 < b \leq 1$, and $(a,1]$, $0 \leq a < 1$. So we just need to check that any of these can be written as a countable union of $I_{j,k}$'s.

Suppose that $0 \leq a < b \leq 1$. If $b - a > 2^{-k}$, and if $i = 1 + \lfloor 2^k a \rfloor$ and $i' = -1 + \lceil 2^k b \rceil$ (where $\lfloor . \rfloor$ and $\lceil . \rceil$ are the floor and ceiling functions), then $0 < i2^{-k} - a \leq 2^{-k}$ and $0 < b - i'2^{-k} \leq 2^{-k}$. This implies that

$$(a,b) = \bigcup_{k > -\log_2(b-a)} \bigcup_{j=1+\lfloor 2^k a \rfloor}^{-2+\lceil 2^k b \rceil} I_{j,k}$$

(where $\log_2$ is the base 2 logarithm). Similarly, if $0 < b \leq 1$ and $0 \leq a < 1$, then

$$[0,b) = \bigcup_{k>-\log_2(b)} \bigcup_{j=0}^{-2+\lceil 2^k b\rceil} I_{j,k}$$

and

$$(a,1] = \bigcup_{k>-\log_2(1-a)} \bigcup_{j=1+\lfloor 2^k a\rfloor}^{2^k-1} I_{j,k}.$$

This proves the statement about the Borel $\sigma$-algebra of $[0,1]$. To finish the problem, we just need to prove that, for all $k \leq 0$ and all $j \in \{0,\ldots,2^k-1\}$, the inverse image $u^{-1}(I_{j,k})$ is a Borel set in $G$ and $\mu(u^{-1}(I_{j,k})) = 2^{-k}$. So we calculate these inverse images.

First note that, if $x \in [0,1]$, then $u^{-1}(x)$ is a singleton unless $x$ is of the form $j2^{-k}$ for $0 < j < 2^k$; in that last case, $x$ as second expression in base 2, where all the coefficients are 1 after a certain rank.

Now let $k \geq 0$ and $j \in \{0,1,\ldots,2^k-1\}$. If $k = 0$, then $j = 0$ and $I_{j,k} = [0,1]$, so $u^{-1}(I_{j,k}) = G$ and $\mu(G) = \lambda([0,1]) = 1$ by the choice of $\mu$. Suppose that $k \geq 1$. As $0 \leq j \leq 2^k - 1$, we can write $j$ in base 2 as $j = \sum_{i=0}^{k-1} a_{k-1-i}2^i$, with the $a_i$ in $\{0,1\}$. If $0 < j$, we also write $j-1 = \sum_{i=0}^{k-1} b_{k-1-i}2^i$, with the $b_i$ in $\{0,1\}$. If $j+1 < 2^k$, we also write $j+1 = \sum_{i=0}^{k-1} c_{k-1-i}2^i$, with the $c_i$ in $\{0,1\}$. Then we have

$$j2^{-k} = \sum_{i=0}^{k-1} a_i 2^{-(i+1)},$$

$$j2^{-k} = \sum_{i=0}^{k-1} b_i 2^{-(i+1)} + \sum_{i=k}^{+\infty} 2^{-i} \quad \text{if } j > 0$$

and

$$(j+1)2^{-k} = \sum_{i=0}^{k-1} c_i 2^{-(i+1)} \quad \text{if } j+1 < 2^k,$$

so $u^{-1}(I_{j,k}) = X \cup Y$, where

$$Y = \left(\{(a_0,\ldots,a_{k-1})\} \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq k}}\right)$$

and

$$X = \begin{cases} \{(b_0,\ldots,b_{k-1},1,1,\ldots),(c_0,\ldots,c_{k-1})\} & \text{if } 0 < j < 2^k-1 \\ \{(b_0,\ldots,b_{k-1},1,1,\ldots)\} & \text{if } j = 2^k-1 \\ \{(c_0,\ldots,c_{k-1})\} & \text{if } j = 0. \end{cases}$$

As $X$ is closed and $Y$ is open, this is a Borel subset of $G$. We also know by question (b) that $\mu(Y) = 2^{-k} = \lambda(I_{j,k})$, so it remains to show that $\mu(X) = 0$. That is, we want to show that singletons in have volume $0$ in $G$. As all singletons are translates of each others, it suffices to treat the case of $\{0\}$. This follows from the fact that

$$\{0\} \subset (\{0\})^{\{0,1,\dots,n\}} \times (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}_{\geq n+1}}$$

for every $n \geq 0$, because the right-hand side has volume $2^{-(n+1)}$ by question (b).

□

**Exercise I.5.3.4.** For $x \in \mathbb{Q}_p$ and $r \in \mathbb{R}$, write $B(x,r) = \{y \in \mathbb{Q}_p | |x-y|_p \leq r\}$ (the closed ball of center $x$ and radius $r$). Let $\lambda$ be the Haar measure on $\mathbb{Q}_p$ such that $\lambda(\mathbb{Z}_p) = 1$.

(a). If $x \in \mathbb{Q}_p$ and $m \in \mathbb{Z}$, show that $\lambda(B(x,p^m)) = p^m$.

(b). For every Borel set $X \subset \mathbb{Q}_p$, show that

$$\lambda(X) = \inf\{\sum_{i\geq 0} p^{m_i} | \exists x_0, x_1, \ldots \in \mathbb{Q}_p \text{ with } X \subset \bigcup_{i\geq 0} B(x_i, p^{m_i})\}.$$

*Solution.*

(a). First we note that, if $x, y \in \mathbb{Q}_p$, we have $B(x,p^m) = B(y,p^m) + x - y$, so $\lambda(B(x,p^m)) = \lambda(B(y,p^m))$. Note also that

$$B(0,p^m) = \{x \in \mathbb{Q}_p | |x|_p \leq p^m\} = \{x \in \mathbb{Q}_p | |p^m x|_p \leq 1\} = p^{-m}\mathbb{Z}_p$$

for every $m \in \mathbb{Z}$. So, for every $x \in \mathbb{Q}_p$ and evey $m \in \mathbb{Z}$, we have

$$B(x,p^m) = x + p^{-m}\mathbb{Z}_p.$$

Also, by question (i) of problem I.5.1.4, we have

$$\mathbb{Z}_p = \coprod_{i=0}^{p-1} (i + p\mathbb{Z}_p).$$

Multiplying by $p^{-m}$ gives

$$B(0,p^m) = \coprod_{i=0}^{p-1} B(p^{-m}i, p^{m-1}),$$

hence $\lambda(B(0,p^m)) = p\lambda(B(0,p^{m-1}))$. As $\lambda(B(0,1)) = \lambda(\mathbb{Z}_p) = 1$ by hypothesis, the result follows by an induction on $|m|$.

(b). First, by question (f) of problem I.5.1.4, the balls $B(x,r)$ form a base of (open !) sets for the topology of $\mathbb{Q}_p$, so every open subset of $\mathbb{Q}_p$ is a union of balls $B(x,r)$. As $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and countable, every open subset of $\mathbb{Q}_p$ is a countable union of balls $B(x,r)$ (and we can take the $x$ in $\mathbb{Q}$, but it doesn't matter). Also, note that, by question (b) of problem I.5.1.4, if $y \in B(x,r)$, then $B(y,r) = B(x,r)$. Hence, if two closed balls of $\mathbb{Q}_p$ intersect, then one of them must contain the other. This implies that every open subset of $\mathbb{Q}_p$ is a countable disjoint union of balls $B(x,r)$. The result now follows immediately from (a) and from outer regularity of $\lambda$.

$\square$

**Exercise I.5.3.5.** Let $G$ be a locally compact group, and let $H$ be a closed subgroup of $G$. We write $\pi$ for the quotient map from $G$ to $G/H$. We denote by $\Delta_G$ (resp. $\Delta_H$) the modular function of $G$ (resp. $H$), and we assume that $\Delta_{G|H} = \Delta_H$. We fix left Haar measures $\mu_G$ and $\mu_H$ on $G$ and $H$.

(a). Show that, for every compact subset $K'$ of $G/H$, there exists a compact subset $K$ of $G$ such $\pi(K) = K'$.

(b). Let $f \in L^1(G)$. Show that the function $G \to \mathbb{C}$, $x \longmapsto \int_H f(xh)d\mu_H(h)$ is invariant by right translations by elements of $H$. Hence it defines a function $G/H \to \mathbb{C}$, that we will denote by $f^H$.

(c). If $f \in \mathscr{C}_c(G)$, show that $f^H \in \mathscr{C}_c(G/H)$.

(d). Show that the map $\mathscr{C}_c(G) \to \mathscr{C}_c(G/H)$, $f \longmapsto f^H$ is surjective. (Hint : You may use the fact that, for every compact subset $K$ of $G$, there exists a function $\varphi \in \mathscr{C}_c^+(G)$ such that $\varphi(x) > 0$ for every $x \in K$.)

(e). If $f \in \mathscr{C}_c(G)$ is such that $f^H = 0$, show that $\int_G f(x)d\mu_G(x) = 0$. (Hint : use a function in $\mathscr{C}_c(G/H)$ that is equal to $1$ on $\pi(\mathrm{supp}(f))$, and proposition I.2.12.)

(f). Show that there exists a unique regular Borel measure $\mu_{G/H}$ on $G/H$ that is invariant by left translations by elements of $G$ and such that, for every $f \in \mathscr{C}_c(G)$, we have $\int_G f(x)d\mu_G(x) = \int_{G/H} f^H(y)d\mu_{G/H}(y)$.

(g). If $P$ is a closed subgroup of $G$ such that $\pi$ induces a homeomorphism $P \overset{\sim}{\to} G/H$, show that the inverse image of $\mu_{G/H}$ by this homeomorphism is a left Haar measure on $P$.

(h). If $P$ is a closed subgroup of $G$ such that the map $P \times H \to G$, $(p,h) \longmapsto ph$ is a homeomorphism, and if $d\mu_P$ is a left Haar measure on $P$, show that the linear functional $\mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_H \int_P f(ph)d\mu_P(p)d\mu_H(h)$ defines a left Haar measure on $G$.

*Solution.*

(a). Let $V$ be a compact neighborhood of $1$ in $G/H$. Then $\pi(V)$ is a compact neighborhood of $\pi(1)$ in $G/H$. We have $K' \subset \bigcup_{x \in \pi^{-1}(K')} \pi(xV)$. As $K'$ is compact, we can find $x_1, \ldots, x_n$

such that $K' \subset \bigcup_{i=1}^n \pi(x_i V)$. Let $K = \pi^{-1}(K') \cap (\bigcup_{i=1}^n x_i V)$. Then $K$ is a closed subset of the compact set $\bigcup_{i=1}^n x_i V$, hence it is compact, and we have $\pi(K) = K'$.

(b). Let $x \in H$. Then, for every $g \in G$, we have

$$\int_H f(gxh) d\mu_H(h) = \int_H f(gh) d\mu_H(h)$$

by the left invariance of $\mu_H$.

(c). We need to show that $f^H$ is continuous and that it has compact support.

Fix a symmetric compact neighborhood $V_0$ of 1, and note that $A := \operatorname{supp} f \cup V_0(\operatorname{supp} f)$ is compact. Let $\varepsilon > 0$. As $f$ is left uniformly continuous, there exists a neighborhood $V \subset V_0$ of 1 such that, for every $x \in G$ and every $y \in V$, we have $|f(yx) - f(x)| \leq \varepsilon$. Then, for every $x \in G$ and every $y \in V$, we have

$$|f^H(\pi(yx)) - f^H(x)| = |\int_H (f(yxh) - f(xh)) d\mu_H(h)| \leq \varepsilon \mu_H(x^{-1}A \cap H),$$

because $f(yxh) = f(xh) = 0$ unless $y \in (x^{-1} \operatorname{supp} f) \cup (x^{-1}y^{-1} \operatorname{supp} f) \subset x^{-1}A$. As $x^{-1}A \cap H$ is compact, it has finite measure, and the calculation above implies that $f^H$ is continuous at the point $\pi(x)$.

Now we show that $f^H$ has compact support. By definition of $f^H$, we have $f^H(\pi(x)) = 0$ if $x \notin KH$. So the support of $f^H$ is contained in $\pi(KH) = \pi(K)$, hence it is compact.

(d). Let $g \in \mathscr{C}_c(G/H)$, and let $K'$ be its support. By question (a), there exists a compact subset $K$ of $G$ such that $\pi(K) = K'$. Let $\varphi \in \mathscr{C}_c^+(G)$ be such that $\varphi(x) > 0$ for every $x \in K$. We show that $\varphi^H(y) > 0$ for every $y \in K'$. Let $y \in K'$, write $y = \pi(x)$ with $x \in K$. As $\varphi(x) > 0$ and $\varphi$ is continuous, we can find an open neighborhood $V$ of 1 in $G$ and a $c \in \mathbb{R}_{>0}$ such that $\varphi(x') \geq c$ for every $x' \in xV$. In particular,

$$\varphi^H(y) = \int_H \varphi(xh) d\mu_H(h) \geq \int_{H \cap V} \varphi(xh) d\mu_H(h) \geq c \cdot \mu_H(U \cap H) > 0$$

(as $U \cap H$ is a nonempty open subset of $H$, we have $\mu_H(U \cap H) > 0$).

We define a function $F : G \to \mathbb{C}$ in the following way :

$$F(x) = \begin{cases} \frac{g(\pi(x))}{\varphi^H(\pi(x))} & \text{if } \varphi^H(\pi(x)) > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Note that $F$ is continuous on the open subsets $U_1 = \{x \in G | \varphi^H(\pi(x)) > 0\}$ and $U_2 = G - \operatorname{supp}(g \circ \pi)$ (on the second subset, it is identically zero). As $U_1 \supset \pi^{-1}(K')$ and $\pi^{-1}(K') = \operatorname{supp}(g \circ \pi)$, we have $U_1 \cup U_2 = G$, the function $F$ is continuous on $G$. Finally, we take $f = F\varphi$. Then $f \in \mathscr{C}_c(G)$, and we just need to show that $f^H = g$.

Let $x \in G$. If $\varphi^H(\pi(x)) = 0$, then $f(xh) = 0$ for every $h \in H$, so $f^H(\pi(x)) = 0$. We have seen that $\varphi^H$ takes positive values on $K' = \operatorname{supp}(g)$, so we also have $x \notin \operatorname{supp}(g)$, i.e., $g(x) = 0 = f^H(x)$. Now assume that $\varphi^H(\pi(x)) > 0$. Note that the function $H \to \mathbb{C}$, $h \longmapsto F(xh)$ is constant. So

$$f^H(\pi(x)) = F(x)\int_H \varphi(xh)d\mu_H(h) = \tfrac{g(\pi(x))}{\varphi^H(\pi(x))}\varphi^H(\pi(x)) = g(\pi(x)).$$

Finally, note that $f \in \mathscr{C}_c^+(G)$ if $g \in \mathscr{C}_c^+(G/H)$, and that we also proved along the way that $f^H \in \mathscr{C}_c^+(G/H)$ if $f \in \mathscr{C}_c^+(G)$ (we proved this for $\varphi$).

(e). Let $\psi \in \mathscr{C}_c(G/H)$ be such that $\psi(y) = 1$ for every $y \in \pi(\operatorname{supp} f)$. By question (d), there exists $\varphi \in \mathscr{C}_c(G)$ such that $\varphi^H = \psi$. We have

$$\begin{aligned}
\int_G f(x)d\mu_G(x) &= \int_G f(x)\varphi^H(\pi(x))d\mu_G(x) \\
&= \int_{G\times H} f(x)\varphi(xh)d\mu_G(x)d\mu_H(h) \\
&= \int_H (\int_G f(x)\varphi(xh)d\mu_G(x))d\mu_H(h) \\
&= \int_H (\Delta_G(h)^{-1}\int_G f(xh^{-1})\varphi(x)d\mu_G(x))d\mu_H(h) \\
&= \int_G \varphi(x)(\int_H \Delta_H(h)^{-1}f(xh^{-1})d\mu_H(h))d\mu_G(x) \\
&= \int_G \varphi(x)(\int_H f(xh)d\mu_H(h))d\mu_G(x) \quad \text{(by proposition I.2.12)} \\
&= 0 \quad \text{(because } f^H = 0\text{)}.
\end{aligned}$$

(f). By question (e), the positive linear function $\mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_G f d\mu_G$ factors through the linear map $\mathscr{C}_c(G) \to \mathscr{C}_c(G/H)$, $f \longmapsto f^H$. By question (d) (and the remark at the end of its solution), it defines a positive linear functional $\mathscr{C}_c(G/H) \to \mathbb{C}$. By the Riesz representation theorem, this comes from a regular Borel measure $\mu_{G/H}$ on $G/H$. Unravelling the definition, we get, for every $f \in \mathscr{C}_c(G)$,

$$\int_G f d\mu_G = \int_{G/H} f^H d\mu_{G/H}.$$

By the left invariance of $\mu_G$ and question (d), we have, if $f \in \mathscr{C}_c(G/H)$ and $x \in G$,

$$\int_{G/H} f(xy)d\mu_{G/H}(y) = \int_{G/H} f(y)d\mu_{G/H}.$$

Using the uniqueness part of the Riesz representation theorem (as we did in class), we see that $\mu_{G/H}(xE) = \mu_{G/H}(E)$ for every Borel subset $E$ of $G/H$.

(g). Let $\nu$ be the inverse image of $\mu_{G/H}$ by the homeomorphism $\alpha : P \overset{\sim}{\to} G/H$. It is a regular Borel measure because $\alpha$ is a homeomorphism. Also, note that $\alpha(xy) = x\alpha(y)$ for every $x \in P$ (this is obvious on the definition of $\alpha$). As $\mu_{G/H}$ is invariant by left translations by elements of $P$, so is $\nu$.

(h). The hypothesis implies that $\pi$ induces a homeomorphism $P \overset{\sim}{\to} G/H$, hence we get a left Haar measure $\nu$ on $P$ as in question (g). By the uniqueness of left Haar measures, we have $\mu_P = c\nu$ for some $c \in \mathbb{R}_{>0}$. Hence, for every $f \in \mathscr{C}_c(G)$,

$$\int_H \int_P f(ph) d\mu_P(p) d\mu_H(h) = c \int_P ( \int_H f(ph) d\mu_H(h)) d\nu(p) =$$

$$c \int_{G/H} f^H(y) d\mu_{G/H}(y) = c \int_G f(x) d\mu_G(x).$$

So the functional $f \longmapsto \int_H \int_P f(ph) d\mu_P(p) d\mu_H(h)$ is positive and corresponds to the left Haar measure $c\mu_G$ on $G$.

□

**Exercise I.5.3.6.** Let $G$ be a locally compact group. Let $A$ and $N$ be two closed subgroups of $G$ such that $A \times N \to G$, $(a, n) \longmapsto an$ is a homeomorphism and that $A$ normalizes $N$ (i.e. for every $a \in A$ and $n \in N$, we have $ana^{-1} \in N$).

(a). If $\mu_A$ and $\mu_N$ are left Haar measures on $A$ and $N$, show that the linear functional $\mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_A \int_N f(an) d\mu_A(a) d\mu_N(n)$ defines a left Haar measure on $G$.

(b). Let $a \in A$. Show that there exists $\alpha(a) \in \mathbb{R}_{>0}$ such that, for every $f \in \mathscr{C}_c(N)$, we have

$$\int_N f(ana^{-1}) d\mu_N(n) = \alpha(a) \int_N f(n) d\mu_N(n).$$

(c). If $\Delta_G$, $\Delta_A$ and $\Delta_N$ are the modular functions of $G$, $A$ and $N$ respectively, show that $\Delta_G(an) = \alpha(a)\Delta_A(a)\Delta_N(n)$ if $a \in A$ and $n \in N$.

*Solution.*

(a). The setup is very similar to that of problem I.5.3.5 (with for example $N$ playing the role of $H$), with the difference that we don't make any assumption on the modular functions. Still, the results questions (a)-(d) of problem I.5.3.5 stay true, since their proof doesn't use the assumption on the modular functions. In particular, we get a surjective linear transformation $f \longmapsto f^N$ from $\mathscr{C}_c(G)$ to $\mathscr{C}_c(G/N) \simeq \mathscr{C}_c(A)$, and it sends $\mathscr{C}_c^+(G)$ onto $\mathscr{C}_c^+(A)$. The linear functions of the statement sends $f \in \mathscr{C}_c(G)$ to $\int_A f^N(a) d\mu_A(a)$, so it is positive, and the Riesz representation theorem says that there is a unique regular Borel measure $\mu_G$ on $G$ such that, for every $f \in \mathscr{C}_c(G)$, we have

$$\int_G f d\mu_G = \int_A \int_N f(an) d\mu_A(a) d\mu_N(n).$$

As $\mu_A$ is a left Haar measure on $A$, the formula above implies that $\int_G L_a f d\mu_G = \int_G f d\mu_G$ for every $f \in \mathscr{C}_c(G)$ and every $a \in A$. We show that $\mu_G$ is left invariant by $N$. Let $x \in N$ and $f \in \mathscr{C}_c(G)$. Then we have

$$\begin{aligned}\int_G L_x f d\mu_G &= \int_A \int_N f(xan) d\mu_A(a) d\mu_N(n) = \int_A (\int_N f(a(a^{-1}xa)n) d\mu_N(n)) d\mu_A(a) \\ &= \int_A (\int_N f(an) d\mu_N(n)) d\mu_A(a) \quad \text{because } a^{-1}xa \in N \text{ and } \mu_N \text{ is left invariant} \\ &= \int_G f d\mu_G.\end{aligned}$$

As $G = AN$, this implies that $\int_G L_x g d\mu_G = \int_G f d\mu_G$ for every $x \in G$ and every $f \in \mathscr{C}_c(G)$. By proposition I.2.6, $\mu_G$ is a left Haar measure on $G$.

(b). Note that the map $N \to N$, $n \longmapsto a^{-1}na$ is a homeomorphism. Hence the formula $E \longmapsto \mu_N(a^{-1}Ea)$ defines a regular Borel measure on $N$, which we denote by $\nu$. If $E$ is a Borel subset and $n \in N$, then

$$\nu(nE) = \mu(a^{-1}nEa) = \mu((a^{-1}na)a^{-1}Ea) = \mu(a^{-1}Ea) = \nu(E).$$

Hence $\nu$ is a left Haar measure on $N$, and so there exists $\alpha(a) \in \mathbb{R}_{>0}$ such that $\nu = \alpha(a)\mu_N$. Now, if $E$ is Borel subset of $N$ and $f = \mathbb{1}_E$, the function $n \longmapsto f(ana^{-1})$ is the characteristic function of $a^{-1}Ea$, so

$$\int_N f(ana^{-1}) d\mu_N(n) = \mu(a^{-1}Ea) = \alpha(a)\mu(E) = \alpha(a) \int_N f d\mu_N.$$

This extends in the usual way to all the functions $f \in L^1(N)$, and in particular to $f \in \mathscr{C}_c(N)$.

(c). Let $a \in A$ and $n \in N$, and fix $f \in \mathscr{C}_c^+(G)$. Then we have

$$\begin{aligned}\Delta_G(an)^{-1} \int_G f d\mu_G = \int_G R_{an}(f) d\mu_G &= \int_A \int_N f(bman) d\mu_A(b) d\mu_N(m) \\ &= \int_A (\int_N f(ba(a^{-1}ma)n) d\mu_N(m)) d\mu_A(b) \\ &= \alpha(a)^{-1} \int_A (\int_N f(bamn) d\mu_N(m)) d\mu_A(b) \text{ by question (b)} \\ &= \alpha(a)^{-1}\Delta_N(n)^{-1} \int_A (\int_N f(bam) d\mu_N(m)) d\mu_A(b) \text{ by definition of } \Delta_N \\ &= \alpha(a)^{-1}\Delta(n)^{-1} \int_N (\int_A f(bam) d\mu_A(b)) d\mu_N(m) \\ &= \alpha(a)^{-1}\Delta_N(n)^{-1}\Delta_A(a)^{-1} \int_N (\int_A f(bm) d\mu_A(b)) d\mu_N(m) \text{ by definition of } \Delta_A \\ & \alpha(a)^{-1}\Delta_N(n)^{-1}\Delta_A(a)^{-1} \int_G f d\mu_G.\end{aligned}$$

As $\int_G f d\mu_G > 0$, this implies that $\Delta_G(an) = \alpha(a)\Delta_A(a)\Delta_N(n)$.

□

**Exercise I.5.3.7.** Let $G = \mathrm{SL}_n(\mathbb{R})$, $H = \mathrm{SO}(n)$, and let $P \subset G$ be the subgroup of upper triangular matrices with positive entries on the diagonal (and determinant 1).

(a). Show that the map $P \times H \to G$, $(p, h) \longmapsto ph$ is a homeomorphism. (Hint : Gram-Schmidt.)

(b). Give a formula for a left Haar measure on $P$ similar to the formula in question I.5.3.2(d).

(c). Calculate the modular function of $P$.

(d). Show that $G$ is unimodular. (There are several ways to do this.)

(e). If $n = 2$, show that $\mathrm{SO}(n) \simeq S^1$ (the circle group), and give a left Haar measure on $G$.

*Solution.*

(a). In this problem, we denote the usual Euclidian inner product on $\mathbb{R}^n$ by $\langle ., . \rangle$, and the associated norm by $\|.\|$.

We denote the map $P \times H \to G$ of the statement by $\alpha$. This map is continuous because $\mathrm{SL}_n(\mathbb{R})$ is a topological group. We first show that it is injective. Suppose that we have $p, p' \in P$ and $h, h' \in H$ such that $ph = p'h'$. Then $p^{-1}p' = h(h')^{-1} \in P \cap H$ is a special orthogonal matrix that is upper triangular with positive entries on the diagonal. Such a matrix has to be the identity. Indeed, let $(v_1, \dots, v_n)$ be its columns, and let $(e_1, \dots, e_n)$ be the canonical basis of $\mathbb{R}^n$. We want to show that $(v_1, \dots, v_n) = (e_1, \dots, e_n)$. As $v_1$ is a norm 1 vector and a positive multiple of $e_1$, we must have $v_1 = e_1$. As the vectors $v_2, \dots, v_n$ are orthogonal to $v_1$, their first entries are all 0. So $v_2$ is a positive multiple of $e_2$; as $v_2$ is norm 1, we must have $v_2 = e_2$. Now the vectors $v_3, \dots, v_n$ are orthogonal to $v_2$, so their second entries are zero, so $v_3$ is a positive multiple of $e_3$ etc.

Now remember the Gram-Schmidt orthonormalization process. If $(v_1, \dots, v_n)$ is a basis of $\mathbb{R}^n$, it produces an orthogonal basis $(w_1, \dots, w_n)$ and an orthonormal basis $(u_1, \dots, u_n)$ in the following way :

- $w_1 = v_1$ and $u_1 = \frac{1}{\|w_1\|} w_1$;
- For $1 \leq k \leq n-1$, $u_{k+1} = \frac{1}{\|w_{k+1}\|} w_{k+1}$, where $w_{k+1} = v_{k+1} - \sum_{i=1}^{k} \frac{\langle w_i, v_{k+1} \rangle}{\langle w_i, w_i \rangle} w_i$.

In particular, if $A$ (resp. $B$, resp. $C$) is the matrix with columns $(v_1, \dots, v_n)$ (resp. $(w_1, \dots, w_n)$, resp. $(u_1, \dots, u_n)$), then we have $B = AN$ and $C = AND$, where $N$ is an upper triangular matrix with ones on the diagonal and $D$ is the diagonal matrix with diagonal entries $(\|w_1\|^{-1}, \dots, \|w_n\|^{-1})$. Note also that the entries of $N$ and of $D$ are continuous functions of $v_1, \dots, v_n$, hence also the entries of $B$ and $C$, and that $C$ is an orthogonal matrix. If $x \in \mathrm{SL}_n(\mathbb{R})$, applying this process to the columns of $x$, we get an orthogonal matrix $h$ and a matrix $p \in P$, both depending continuously on $x$, such that $h = xp$, i.e. $x = hp^{-1}$. Also, $\det(h) = \det(xp) = \det(p) > 0$, so $h$ is actually in $\mathrm{SO}(n)$. As $g \longmapsto g^{-1}$ is a continuous function on $\mathrm{GL}_n(\mathbb{R})$ (hence on its subgroup $P$), we have constructed a continuous map $\beta : G \to P \times H$ such that $\alpha \circ \beta = \mathrm{id}_G$. In particular, the map $\alpha$ is surjective, so it si bijective. Then its inverse must be $\beta$, and we know that $\beta$ is continuous. So $\alpha$ is a homeomorphism.

(b). Note that $P$ is an open subset of the $\mathbb{R}$-vector space $V$ of upper triangular matrices in $M_n(\mathbb{R})$. Moreover, for every $p \in P$, left translation by $p$ on $P$ is the restriction of the linear endomorphism $T_p : V \to V$, $x \longmapsto px$. So we can apply problem I.5.3.1 to define a Haar measure on $P$ as $|\det(T_p)|^{-1} d_V(p)$, where $d_V$ is Lebesgue measure on $V$.

We still need to calculate $\det(T_p)$ for $p \in P$. Let $p \in P$, and let $a_1, \dots, a_n$ be its diagonal entries. Let $(e_1, \dots, e_n)$ be the canonical basis of $\mathbb{R}^n$ as before, and let $V_i = \mathrm{Span}(e_1, \dots, e_i) \subset \mathbb{R}^n$ for $1 \le i \le n$. Note that the action of $p \in \mathrm{GL}_n(\mathbb{R})$ preserves the subspace $V_1, \dots, V_n$, and that ther determinant of the endormophism of $V_i$ induced by $p$ is $a_1 \dots a_i$. By decomposing $V$ using the columns of the matrices (as in the solution of I.5.3.2(c)), we get an isomorphism $V \simeq V_1 \oplus V_2 \oplus \dots \oplus V_n$ such that the endomorphism $T_p$ corresponds to the action of $p$ on each $V_i$. So we get

$$\det(T_p) = \prod_{i=1}^{n} \prod_{r=1}^{i} a_r = a_1^n a_2^{n-2} \dots a_{n-1}^2 a_n = \prod_{i=1}^{n} a_i^{n+1-i}.$$

(c). We will use problem I.5.3.6, with $G = P$, $N$ the group of unipotent upper triangular matrices (i.e. of upper triangular matrices with ones on the diagonal) and $A$ the group of diagonal matrices with positive diagonal entries. Let $\alpha : A \times N \to P$ be the map defined by $\alpha(a, n) = an$. Let's show that $\alpha$ is a homeomorphism. The map $\alpha$ is obviously continuous, and it is injective because $N \cap A = \{1\}$. Let $x \in P$, and let $a \in A$ be the matrix with the same diagonal entries as $x$. Then $n := a^{-1}x$ is in $N$, and $\alpha(a, n) = x$. Hence $\alpha$ is bijective. Moreover, the matrix $a$ depends continuously on $x$, hence so does $n$, so the inverse of $\alpha$ is continuous, and finally $\alpha$ is a homeomorphism.

We want to apply question I.5.3.6(c). For this, we need to calculate the modular functions of $A$ and $N$ and the function $\alpha : A \to \mathbb{R}_{>0}$.

First, as $A$ is commutative, we have $\Delta_A = 1$.

For $N$, there are several ways to proceed. For example, you may notice that $N$ is obviously homeomorphic (as a topological space only) to the $\mathbb{R}$-vector space $W$ of upper triangular matrices in $M_n(\mathbb{R})$ with zeroes on the diagonal. (Just forget the diagonal terms of the matrices.) Moreover, for $n \in N$, left translation by $n$ on $N$ corresponds to the linear endomorphism $U_n$ of $W$ given by $U_n(X) = nX$, for $X \in W$. Note that $W$ is a subspace of the space $V$ of the previous question, and that $U_n$ is the restriction of $T_n$. So we can use the same method as in the previous question to calculate $\det(U_n)$, and we get $\det(U_n) = 1$.

Hence Lebesgue measure on $W$ is a left Haar measure on $N$. We can redo everything using right translations instead of left translations, and we get that Lebesgue measure on $W$ is also a right Haar measure on $N$. This means that $N$ is unimodular, so $\Delta_N = 1$.

Finally, we need to calculate the function $\alpha$. Remember that it is defined by

$$\int_N f(ana^{-1})dn = \alpha(a) \int_N f(n)dn$$

for every $f \in \mathscr{C}_c(N)$, where $dn$ is Lebesgue measure on $W$ (which we have just seen is a Haar measure on $N$). Note that $c_a : X \longmapsto aXa^{-1}$ is a linear endomorphism of $W$, so we can calculate $\int_N f(ana^{-1})dn$ using the change of variables formula once we know $\det(c_a)$. We get $\det(c_a) \int_N f(ana^{-1})dn = \int_N f(n)dn$, hence $\alpha(a) = \det(c_a)^{-1}$. But is is easy to see that, if the diagonal entries of $a$ are $(a_1, \dots, a_n)$, then

$$\det(c_a) = a_1^{n-1} a_2^{n-3} \dots a_n^{1-n} = \prod_{i=1}^n a_i^{n-2i+1}.$$

Hence finally, for $p \in P$,

$$\Delta_P(p) = a_1^{1-n} a_2^{3-n} \dots a_n^{n-1} = \prod_{i=1}^n a_i^{2i-n-1},$$

where $a_1, \dots, a_n$ are the diagonal entries of $p$.

(d). If you know (or know how to prove) that $\mathrm{SL}_n(\mathbb{R})$ is equal to its commutator subgroup, then this isn easy. Here is another way : Let $\mathrm{GL}_n(\mathbb{R})^+$ be the group of $n \times n$ matrices with positive determinant. This is an open subgroup of $\mathrm{GL}_n(\mathbb{R})$ (it's the inverse image of $\mathbb{R}_{>0}$ by the continuous group morphism $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$), so, if $\mu$ is a Haar measure on $\mathrm{GL}_n(\mathbb{R})$ (remember that $\mathrm{GL}_n(\mathbb{R})$ is unimodular by question I.5.3.2(c)), its restriction to $\mathrm{GL}_n(\mathbb{R})^+$ is a nonzero regular Borel measure, and it is obviously a left and right Haar measure on $\mathrm{GL}_n(R)^+$. Now note that we have an isomorphism of topological groups $\mathbb{R}_{>0} \times \mathrm{SL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})^+$, $(\lambda, x) \longmapsto \lambda x$ (whose inverse is given by $x \longmapsto (\det(x)^{1/n}, \det(x)^{-1/n} x)$), so we can apply problem I.5.3.6 with $G = \mathrm{GL}_n(\mathbb{R})^+$, $A = \mathbb{R}_{>0} I_n$ and $N = \mathrm{SL}_n(\mathbb{R})$. As $A$ and $N$ commute, we have $\alpha = 1$. We know that $A$ is unimodular because it is commutative, and we have just seen that $\mathrm{GL}_n(\mathbb{R})^+$ is unimodular, hence I.5.3.6(c) implies that $\mathrm{SL}_n(\mathbb{R})$ is also unimodular.

(e). It is well-known that the group of rotations in $\mathbb{R}^2$ (i.e. $\mathrm{SO}(2)$) is isomorphic to the circle group $S^1$. The isomorphism sends $e^{2i\pi\theta} \in S^1$ to the matrix $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Also, we have seen in class that we can define a Haar measure on $S^1$ by the linear functional sending $f \in \mathscr{C}_c(S^1)$ to $\int_0^1 f(e^{2i\pi\theta})d\theta$, where $d\theta$ is Lebesgue measure on $\mathbb{R}$.

The point of this, of course, is that exercise I.5.3.5 now allows you to define a Haar measure on $\mathrm{SL}_2(\mathbb{R})$. To treat the case of $\mathrm{SL}_n(\mathbb{R})$, we need a Haar measure on $\mathrm{SO}(n)$. An example of such a measure is given in problem I.5.3.9

$\square$

**Exercise I.5.3.8.** (Remember problems I.5.1.4, I.5.3.1, I.5.3.2 and I.5.3.4). We denote by $dx$ a Haar measure on the additive group $\mathbb{Q}_p$. We also denote by $dx$ (resp. $dA$) the product measure on $\mathbb{Q}_p^n$ (resp. $M_n(\mathbb{Q}_p) \simeq \mathbb{Q}_p^{n^2}$); note that it is a Haar measure for the corresponding additive group.

(a). Show that, for every $f \in L^1(\mathbb{Q}_p)$ and every $a \in \mathbb{Q}_p^\times$, $b \in \mathbb{Q}_p$, we have

$$\int_{\mathbb{Q}_p} f(x)dx = |a|_p \int_{\mathbb{Q}_p} f(ax+b)dx.$$

(b). Let $n \geq 1$. Show that, if $f \in L^1(\mathbb{Q}_p^n)$, $A \in \mathrm{GL}_n(\mathbb{Q}_p)$ and $b \in \mathbb{Q}_p^n$, we have

$$\int_{\mathbb{Q}_p^n} f(x)dx = |\det(A)|_p \int_{\mathbb{Q}_p^n} f(Ax+b)dx.$$

(c). Show that $|\det(A)|_p^{-n} dA$ is a left and right Haar measure on $\mathrm{GL}_n(\mathbb{Q}_p)$.

(d). Let $B$ be the group of upper triangular matrices in $\mathrm{GL}_n(\mathbb{Q}_p)$. Find a left Haar measure on $B$ and calculate the modular function of $B$.

*Solution.*

(a). First, using the invariance by translation of $dx$, we see that

$$\int_{\mathbb{Q}_p} f(ax+b)dx = \int_{\mathbb{Q}_p} f(ax)dx$$

for every $f \in L^1(\mathbb{Q}_p)$ and $a, b \in \mathbb{Q}_p$.

Let $a \in \mathbb{Q}_p^\times$. We use the notation of problem I.5.3.4. If $x \in \mathbb{Q}_p$ and $m \in \mathbb{Z}$, then

$$aB(x,p^m) = \{ay \text{ with } |x-y|_p \leq p^m\} = \{y \in \mathbb{Q}_p | |ax-y|_p \leq |a|_p p^m\} = B(ax, |a|_p p^m),$$

and so, by I.5.3.4(a), $\mathrm{vol}(aB(x,p^m)) = |a|_p \mathrm{vol}(B(x,p^m))$. Using question (b) of the same problem, we get $\mathrm{vol}(aE) = |a|_p \mathrm{vol}(E)$ for every Borel subset $E$ of $\mathbb{Q}_p$. Suppose that $f = \mathbb{1}_E$, with $E$ a Borel subset of $\mathbb{Q}_p$. Then

$$\int_{\mathbb{Q}_p} f(ax)dx = \mathrm{vol}(a^{-1}E) = |a|_p^{-1} \int_{\mathbb{Q}_p} f(x)dx,$$

so we get the desired result for this function $f$. The result now follows for every $f \in L^1(\mathbb{Q}_p)$ by linearity and continuity of the integral.

(b). Using the translation invariance of $dx$ as in question (a), we see that it suffices to prove the result in the case $b = 0$. Let $A \in \mathrm{GL}_n(\mathbb{Q}_P)$. First note that $A = A_1A_2$ and if we know the result for $A_1$ and $A_2$, then we know it for $A$; indeed, for every $f \in L^1(\mathbb{Q}_p^n)$, we'll have

$$\int_{\mathbb{Q}_p^n} f(x)dx = |\det(A_1)|_p \int_{\mathbb{Q}_p^n} f(A_1x)dx =$$

$$|\det(A_1)|_p|\det(A_2)|_p \int_{\mathbb{Q}_p^n} f(A_1(A_2x))dx = |\det(A)|_p \int_{\mathbb{Q}_p^n} f(Ax)dx.$$

The Gauss algorithm (for solving systems of linear equations) says that we can make $A$ upper triangular by elementary row operations (with correspond to multiplying on the left by a lower triangular matrix) and permutations of rows (with correspond to multiplying on the left by a permutation matrix). So, by the observation above, it suffices to prove the result for upper and lower triangular matrices and for permutation matrices.

Suppose first that $A$ is a permutation matrix. So there exists a permutation $\sigma \in \mathfrak{S}_n$ such that, for every $x = (x_1 \dots, x_n) \in \mathbb{Q}_p^n$, $Ax = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$. As $dx$ is the product of identical measures on the $n$ factors $\mathbb{Q}_p$ of $\mathbb{Q}_p^n$, we have, for every $f \in L^1(\mathbb{Q}_p)$, $\int_{\mathbb{Q}_p^n} f(Ax)dx = \int_{\mathbb{Q}_p^n} f(x)dx$. The result now follows from the fact that $\det(A) = \pm + 1$.

Suppose that $A$ is upper triangular, and write $A = (a_{ij})_{1,\leq i,j \leq n}$. Let $f \in L^1(\mathbb{Q}_p)$. Then

$$\int_{\mathbb{Q}_p^n} f(A(x_1, \dots, x_n)) =$$

$$\int_{\mathbb{Q}_p} \dots \int_{\mathbb{Q}_p} f(a_{11}x_1 + \dots + a_{1n}x_n, \dots, a_{n-1,n-1}x_{n-1} + a_{n-1,n}x_n, a_{nn}x_n)dx_n dx_{n-1} \dots dx_1.$$

Using question (a), we see that this last integral is equal to

$$|a_{11}|_p^{-1} \dots |a_{n-1,n-1}|_p^{-1}|a_{nn}|_p^{-1} \int_{\mathbb{Q}_p^n} f(x)dx = |\det(A)|_p^{-1} \int_{\mathbb{Q}_p^n} f(x)dx.$$

The case of lower triangular matrices is similar (just put the $dx_i$ reverse order).

(c). Once we have the change of variables formula of question (b), we can replace $\mathbb{R}$ by $\mathbb{Q}_p$ in problems I.5.3.1 and I.5.3.2 and all the results will stay true, with exactly the same proofs. (Except I.5.3.2(b), which doesn't make sense for $\mathbb{Q}_p$.) In particular, we get that $|\det(A)|_p^{-n}dA$ is a left and right Haar measure on $\mathrm{GL}_n(\mathbb{Q}_p)$.

(d). Again, we can just apply the proofs of questions (b) and (c) of problem I.5.3.7 (and the analogue for $\mathbb{Q}_p$ of problem I.5.3.1) to get the result. Assuming that there is no sign mistake in problem I.5.3.7, a left Haar measure on $B$ is $\prod_{i=1}^n |a_{ii}|_p^{i-n-1}dA$, where $dA$ is the product measure on the $\mathbb{Q}_p$-vector space $V \simeq \mathbb{Q}_p^{n(n+1)/2}$ of upper triangular matrices and the $a_{ij}$ are the entries of the matrix. And the modular function of $B$ is given by

$$\Delta(A) = \prod_{i=1}^n |a_{ii}|_p^{2i-n-1}.$$

$\square$

**Exercise I.5.3.9.** [15] The goal of this problem is to give a formula for a Haar measure on $\mathrm{SO}(n)$. (We could do something similar for the unitary group $\mathrm{U}(n)$.)

(a). For $X \in M_n(\mathbb{R})$, we set $\Phi(X) = (I_n - X)(I_n + X)^{-1}$. Show that this is well-defined if $-1$ is not an eigenvalue of $X$, and that we have $\Phi(\Phi(X)) = X$ whenever this makes sense.

(b). We denote by $A_n$ the $\mathbb{R}$-vector space of $n \times n$ antisymmetric matrices (i.e. of $X \in M_n(\mathbb{R})$ such that $X^T = -X$) and by $U$ the set of elements of $\mathrm{SO}(n)$ that don't have $-1$ as an eigenvalue. Show that $U$ is an open dense subset of $\mathrm{SO}(n)$, and that $\Phi$ induces a homeomorphism $A_n \xrightarrow{\sim} U$.

(c). Let $X \in A_n$. Show that there exist open dense subsets $V$ and $W$ of $A_n$ such that the formula $\Phi(L_X Y) = \Phi(X)\Phi(Y)$ defines a diffeomorphism $L_X : V \xrightarrow{\sim} W$, and that $0 \in V$.

(d). Let $dX$ be Lebesgue measure on $A_n$. For every $X \in A_n$ and every $Y \in A_n$ on which $L_X$ is defined, we denote by $L'_X(Y)$ the differential at $Y$ of $L_X$. It is a linear transformation from $A_n$ to $A_n$ such that, for every $H \in A_n$,

$$L_X(Y + tH) = L_X(Y) + tL'_X(Y)(H) + o(t).$$

Fix $X \in A_n$. We want to compute $\det(L'_X(0))$. Remember that $L'_X(0)$ is a linear endomorphism of $A_n$, and note that $A_n \otimes_{\mathbb{R}} \mathbb{C}$ is the space of antisymmetric matrices in $M_n(\mathbb{C})$.

(i) Show that $\det(L'_X(0))$ is well-defined and nonzero.

(ii) Show that we have
$$L'_X(0)(H) = (I_n - X)H(I_n + X),$$
for every $H \in A_n$.

(iii) Show that $X$ has a basis of (complex) eigenvectors $(v_1, \dots, v_n)$ such that the corresponding eigenvalues are of the form $i\lambda_1, \dots, i\lambda_n$, with $\lambda_1, \dots, \lambda_n \in \mathbb{R}$.

(iv) For $j, k \in \{1, \dots, n\}$, we set $Y_{jk} = v_j v_k^T - v_k v_j^T$. Show that $Y_{jk} \in A_n \otimes_{\mathbb{R}} \mathbb{C}$, and that it is an eigenvector for $L'_X(0)$, with corresponding eigenvalue $(1 - i\lambda_j)(1 - i\lambda_k)$.

(v) Show that $(Y_{jk})_{1 \le j < k \le n}$ is a basis of $A_n \otimes_{\mathbb{R}} \mathbb{C}$.

(vi) Show that $\det(L'_X(0)) = \det(I_n - iX)^{n-1}$.

(e). Show that the linear functional sending $f \in \mathscr{C}_c(\mathrm{SO}(n))$ to

$$\int_{A_n} f(\Phi(X)) \frac{1}{|\det L'_X(0)|} dX$$

defines a left Haar measure on $\mathrm{SO}(n)$. (Hint : Note that $(L_X \circ L_Y)(0) = L_X(Y)$, and use the chain rule.)

[15] Somewhat incomplete proof here.

*Solution.*

(a). If $X \in M_n(\mathbb{R})$, then $-1$ is not an eigenvalue of $X$ if and only if $I_n + X$ is invertible, i.e. if and only if the formula defining $\Phi(X)$ makes sense. So the set of definition of $\Phi$ is the open set defined by the equation $\det(I_n + X) \neq 0$. Note also that $I_n - X$ and $I_n + X$ commute, so $I_n - X$ and $(I_n + X)^{-1}$ commute (if the second is defined), so we also have $\Phi(X) = (I_n + X)^{-1}(I_n - X)$.

Let $X \in M_n(\mathbb{R})$ such that $\Phi(X)$ is defined. Then we have

$$I_n + \Phi(X) = ((I_n + X) + (I_n - X))(I_n + X)^{-1} = 2(I_n + X)^{-1}$$

and

$$I_n - \Phi(X) = ((I_n + X) - (I_n - X))(I_n + X)^{-1} = 2X(I_n + X)^{-1}.$$

In particular, $I_n + \Phi(X)$ is invertible, so $\Phi(\Phi(X))$ makes sense, and we have

$$\Phi(\Phi(X)) = (I_n - \Phi(X))(I_n + \Phi(X))^{-1} = 2X(I_n + X)^{-1}(2(I_n + X)^{-1})^{-1} = X.$$

(b). Let $g \in \mathrm{SO}(n)$. Then we can find $P \in \mathrm{GL}_n(\mathbb{R})$ such that

$$PgP^{-1} = \begin{pmatrix} r_1 & 0 & \dots & 0 \\ 0 & r_2 & 0 & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & \dots & 0 & r_m \end{pmatrix},$$

where :

- if $n$ is even, then $m = n/2$ and $r_1, \dots, r_m$ are $2 \times 2$ matrices of the form $\begin{pmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{pmatrix}$, with $\theta_i \in [0, 2\pi)$;
- if $n$ is odd, then $m = (n+1)/2$, the matrix $r_m$ is the $1 \times 1$ matrix 1 and $r_1, \dots, r_{m-1}$ are $2 \times 2$ matrices of the form $\begin{pmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{pmatrix}$, with $\theta_i \in [0, 2\pi)$.

In both cases, $-1$ is an eigenvalue of $g$ if and only if one at least one of the $\theta_i$ is equal to $\pi$. So, by varying the $\theta_i$, we can find a sequence of elements of $\mathrm{SO}(n)$ that converge to $g$ and don't have $-1$ as an eigenvalue. This proves that $U$ is dense in $\mathrm{SO}(n)$.

Next, as antisymmetric matrices have only imaginary eigenvalues, the function $\Phi$ is defined on $A_n$. Note also that it is clear on the definition of $\Phi$ that $\Phi$ is continuous on its open set of definition. By the second part of question (a), $\Phi$ is injective and, to show that $\Phi$ is a homeomorphism from $A_n$ to $U$, it suffices to show that is a bijection from $A_n$ to $U$ (because then its inverse will be $\Phi$). So we just need to show that $\Phi(A_n) = U$. Using again the fact that $\Phi(\Phi(X)) = X$ whenever this makes sense, we see that it suffices to prove that $\Phi(A_n) \subset U$ and $\Phi(U) \subset A_n$.

Let $X \in A_n$. Then $X^T = -X$, so $\Phi(X)^T = (I_n+X^T)^{-1}(I_n-X^T) = (I_n-X)^{-1}(I_n+X)$, and hence $\Phi(X)^T\Phi(X) = I_n$, which means that $\Phi(X) \in \mathbf{O}(n)$. As $\Phi$ is continuous and $A_n$ is connected, $\Phi(A_n)$ is connected. But $I_n = \Phi(0) \in \Phi(A_n)$, so $\Phi(A_n)$ is contained in $\mathrm{SO}(n)$.

Let $X \in \mathrm{SO}(n)$ such that $-1$ is not an eigenvalue of $X$. Then $X^T = X^{-1}$, so

$$\Phi(X)^T = (I_n-X^T)(I_n+X^T)^{-1} = (I_n-X^{-1})(I_n+X^{-1})^{-1} = (X-I_n)(X+I_n)^{-1} = -\Phi(X).$$

So we have $\Phi(U) \subset A_n$.

(c). Fix $X \in A_n$. Note that the formula $\Phi(L_XY) = \Phi(X)\Phi(Y)$ can also be written $L_XY = \Phi(\Phi(X)\Phi(Y))$, by (a).

For $Y \in A_n$, $\Phi(X)\Phi(Y)$ has animage by $\Phi$ (which will automatically be in $A_n$ by (b)) if and only if $\Phi(Y) \in \Phi(X)^{-1}U$. So we can take $V = \Phi(U \cap (\Phi(X)^{-1}U))$; this is dense in $A_n$ because $U \cap (\Phi(X)^{-1}U)$ is dense in $\mathrm{SO}(n)$ by (b). Then the image of $V$ by the map $L_X : Y \longmapsto \Phi(\Phi(X)\Phi(Y))$ is $W := \Phi((\Phi(X)U) \cap U)$.

The map $L_X : V \to W$ is continuous and surjective. In fact, as $\Phi$ is infinitely differentiable (it is given by rational functions in the entries of its arguments, by the formula saying that $A^{-1}$ is $\det(A)^{-1}$ times the transpose of its cofactor matrix, for every $A \in \mathrm{GL}_n(\mathbb{R})$), the map $L_X$ is also infinitely differentiable.

Let $X' = \Phi(\Phi(X)^{-1}) \in A_n$. Then we get as above a continuous and surjective map $L_{X'} : W \to V$, defined by the formula $L_{X'}(Y) = \Phi(\Phi(X)^{-1}\Phi(Y))$. The maps $L_X$ and $L_{X'}$ are inverses of each other, and in particular they are both diffeomorphisms.

Finally, if $Y = 0$, then $\Phi(Y) = I_n$. So $\Phi(Y) \in U$, and we also have $\Phi(Y) \in \Phi(X)^{-1}U$, because $\Phi(X)\Phi(Y) = \Phi(X) \in U$. This shows that $0 \in V$.

(d). (i) Let $X \in A_n$. As $L_X$ is defined at the point $0$, the differential $L'_X(0)$ makes sense; also, as $L_X$ is a diffeomorphism, $\det(L'_X(0)) \neq 0$.

(ii) Note that, for $Y \in A_n$,

$$(I_n+X+Y)^{-1} = (I_n+X)^{-1}(I_n+(I_n+X)^{-1}Y) = (I_n+X)^{-1}(I_n-Y(I_n+X)^{-1}+o(Y)),$$

hence

$$\begin{aligned}\Phi(X+Y) &= (I_n - X - Y)(I_n + X + Y)^{-1} \\ &= ((I_n - X) - Y)(I_n + X)^{-1}(I_n - Y(I_n + X)^{-1} + o(Y)) \\ &= \Phi(X) - \Phi(X)Y(I_n + X)^{-1} - Y(I_n + X)^{-1} + o(Y).\end{aligned}$$

In particular (taking $X = 0$), we have

$$\Phi(Y) = I_n - 2Y + o(Y).$$

So

$$\Phi(X)\Phi(Y) = \Phi(X) - 2\Phi(X)Y + o(Y),$$

and

$$L_X(Y) = \Phi(\Phi(X)\Phi(Y)) = \Phi(\Phi(X) - 2\Phi(X)Y + o(Y)) =$$

$$\Phi(\Phi(X)) - \Phi(\Phi(X))(-2\Phi(X)Y)(I_n + \Phi(X))^{-1} - (-2\Phi(X)Y)(I_n + \Phi(X))^{-1} + o(Y).$$

Using $\Phi(\Phi(X)) = X$ and $I_n + \Phi(X) = 2(I_n + X)^{-1}$ (see (a)), we can simplify this last expression to

$$\begin{aligned} X + X\Phi(X)Y(I_n + X)^{-1} + \Phi(X)Y(I_n + X) + o(Y) &= X + (I_n + X)\Phi(X)Y(I_n + Y) + o(Y) \\ &= X + (I_n - X)Y(I_n + X) + o(Y). \end{aligned}$$

But then the conclusion that $L'_X(0)(Y) = (I_n - X)Y(I_n + X)$ follows immediately from the definition of the differential.

(iii) As $X$ is antisymmetric and has real entries, it is normal, so the spectral theorem says that $X$ is diagonalizable in an orthonormal basis of $\mathbb{C}^n$; in other words, there exists a unita matrix $P$ such that $PXP^{-1}$ is diagonal. We have already used the fact that the eigenvalues of $X$ are imaginary, but it is easy to recheck it quickly : we have $X^* = -X$ and $P^* = P^{-1}$, and $(PXP^{-1})^* = (P^*)^{-1}X^*P^* = -PXP^{-1}$. As $PXP^{-1}$ is diagonal, this means that its diagonal entries (which are the eigenvalues of $X$) are all imaginary.

(iv) It follows directly from the definition of $Y_{jk}$ that $Y_{jk}^T = -Y_{jk}$, so $Y_{jk} \in A_n \otimes_{\mathbb{R}} \mathbb{C}$. Furthermore, by (ii), we have

$$\begin{aligned} L'_X(0)(Y_{ij}) &= (I_n - X)Y_{ij}(I_n + X) \\ &= (I_n - X)(v_j v_k^T)(I_n - X^T) - (I_n - X)(v_k v_j^T)(I_n - X^T) \\ &= (1 - i\lambda_j)(v_j v_k^T)(1 - i\lambda_k) - (1 - i\lambda_k)(v_k v_j^T)(1 - i\lambda_j \\ &= (1 - i\lambda_j)(1 - i\lambda_k)Y_{ij}. \end{aligned}$$

(v) As $(v_1, \dots, v_n)$ is a basis of $\mathbb{C}^n$, the matrices $v_j v_k^T$, for $1 \leq j, k \leq n$, form a basis of $M_n(\mathbb{C})$. So the matrices $Y_{jk} = (v_j v_k^T) - (v_j v_k^T)^T$, for $1 \leq j, k \leq n$, generate $A_n \otimes_{\mathbb{R}} \mathbb{C}$. Note that $Y_{jj} = 0$ and $Y_{kj} = -Y_{jk}$, so $A_n \otimes_{\mathbb{R}} \mathbb{C}$ is actually spanned by the matrices $Y_{jk}$, for $1 \leq j < k \leq n$. As there are $n(n-1)/2$ such matrices and $\dim_{\mathbb{C}}(A_n \otimes_{\mathbb{R}} \mathbb{C}) = \dim_{\mathbb{R}}(A_n) = n(n-1)/2$, they form a basis of $A_n \otimes_{\mathbb{R}} \mathbb{C}$.

(vi) By (iv) and (v), we have

$$\det(L'_X(0)) = \prod_{1 \leq j < k \leq n} (1 - i\lambda_j)(1 - i\lambda_k) = \prod_{r=1}^{n} (1 - i\lambda_r)^{n-1}$$

(because each $1 - i\lambda_r$ appears $n - 1$ times in the first big product : $(n - r)$ times as the first factor $(1 - i\lambda_j)$, and $(r - 1)$ times as the second factor $(1 - i\lambda_k)$). To get the result, we just need to note that the eigenvalues of $I_n - iX$ are $1 - i\lambda_1, \dots, 1 - i\lambda_n$, so that

$$\det(I_n - X) = \prod_{r=1}^{n} (1 - i\lambda_r).$$

(e). Let us denote this functional by $\Lambda$. First, by question (e), the function $X \longmapsto \frac{1}{|\det(L'_X(0))|}$ is defined everywhere on $A_n$ and continuous, so the integral defining $\Lambda$ makes sense.

We need to check that $\Lambda$ is positive and invariant by left translations. We first check the positivity. Let $f \in \mathscr{C}_c^+(\mathrm{SO}(n))$. Then we can find $\varepsilon > 0$ and a nonempty open subset $\Omega$ of $\mathrm{SO}(n)$ such that $f_{|\Omega} \geq \varepsilon$. As $U$ is open dense in $\mathrm{SO}(n)$, its intersection with $\Omega$ is open and nonempty, so $\Phi(U \cap \Omega)$ is open and nonempty in $A_n$, and we have

$$\Lambda(f) \geq \varepsilon \int_{\Phi(U\cap\Omega)} \frac{1}{|\det(L'_X(0))|} dX > 0$$

(because the function $X \longmapsto \frac{1}{|\det(L'_X(0))|}$ is continuous and positive on $\Phi(U \cap \Omega)$).

Now we check the left invariance. Fix $f \in \mathscr{C}_c(\mathrm{SO}(n))$. Let $g \in U$. Then $\Lambda(L_g f) = \int_{A_n} f(g^{-1}\Phi(Y)) \frac{1}{|\det(L'_Y(0))|} dY$. Choose $X, X' \in A_n$ such that $\Phi(X) = g^{-1}$ and $\Phi(X') = g$. Then

$$\begin{aligned}
\Lambda(L_g f) &= \int_{A_n} f(\Phi(X)\Phi(Y)) \frac{1}{|\det(L'_Y(0))|} dY \\
&= \int_V f(\Phi(X)\Phi(Y)) \frac{1}{|\det(L'_Y(0))|} dY \text{ (because } \mathrm{vol}(A_n - V) = 0) \\
&= \int_V f(\Phi(L_X Y)) \frac{1}{|\det(L'_Y(0))|} dY.
\end{aligned}$$

Now note that, if $Y \in V$, then so does $L_Y(0) = Y$, so $L_X(Y) = L_X \circ L_Y(0) = L_{L_X Y}(0)$ makes sense, and we have by the chain rule

$$L'_{L_X Y}(0) = L'_X(Y) \circ L'_Y(0),$$

hence in particular

$$\frac{1}{|\det(L'_Y(0))|} = \frac{|\det(L'_X(Y))|}{|\det(L'_{L_X Y}(0))|}.$$

This implies that

$$\Lambda_g(f) = \int_V f(\Phi(L_X Y)) \frac{|\det(L'_X(Y))|}{|\det(L'_{L_X Y}(0))|} dY.$$

Using the substitution $Z = L_X Y$, we see that this is equal to

$$\int_W f(\Phi(Z)) \frac{1}{|\det(L'_Z(0))|} dZ.$$

As $\mathrm{vol}(A_N - W) = 0$, the last integral is equal to $\int_{A_n} f(\Phi(Z)) \frac{1}{|\det(L'_Z(0))|} dZ$, i.e. to $\Lambda(f)$.

So we have shown that the function $\mathrm{SO}(n) \to \mathbb{C}$, $g \longmapsto \Lambda(L_g f)$ is constant on the open dense subset $U$. As this function is continuous (it is the composition of the continuous function $\mathrm{SO}(n) \to \mathscr{C}_c(\mathrm{SO}(n))$, $g \longmapsto L_g f$ and of the continuous linear function $\Lambda : \mathscr{C}_c(\mathrm{SO}(n)) \to \mathbb{C}$), it is constant on the whole $\mathrm{SO}(n)$, which means that $\Lambda(L_g f) = \Lambda(f)$ for every $g \in \mathrm{SO}(n)$.

□

**Exercise I.5.3.10.** Let $G = \mathrm{SU}(2)$.

(a). Show that every element of $G$ is of the form $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$, with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$.

If we identify $\mathbb{C}$ and $\mathbb{R}^2$ in the usual way, the previous question gives a homeomorphism $\alpha$ between $\mathrm{SU}(2)$ and $S^3$ (the unit sphere in $\mathbb{R}^4$).

(a). If $g \in \mathrm{SU}(2)$, show that left translation by $g$ on $\mathrm{SU}(2)$ corresponds by $\alpha$ to the restriction to $S^3$ of the action of an element of $\mathrm{SO}(4)$ on $\mathbb{R}^4$ (i.e. there exists $A \in \mathrm{SO}(4)$ such that, for every $h \in \mathrm{SU}(2)$, we have $gh = A\alpha(h)$).

(b). Let $\mu$ be the usual spherical measure on $S^3$; that is, if $\lambda$ is Lebesgue measure on $\mathbb{R}^4$, we have by definition, for every Borel subset $E$ of $S^3$,

$$\mu(E) = \tfrac{2}{\pi^2}\lambda(\{tx, t \in [0,1], x \in E\})$$

(note that the volume of the unit ball in $\mathbb{R}^4$ is $\frac{\pi^2}{2}$).

Show that the inverse image by $\alpha$ of $\mu$ is a left and right Haar measure on $\mathrm{SU}(2)$.

(c). We use the following (hyperspherical) coordinates on $S^3$ : if $(x_1, x_2, x_3, x_4) \in S^3$, we write

$$\begin{cases} x_1 = \cos\theta \\ x_2 = \sin\theta\cos\psi \\ x_3 = \sin\theta\sin\psi\cos\phi \\ x_4 = \sin\theta\sin\psi\sin\phi \end{cases}$$

with $0 \leq \theta \leq \pi$, $0 \leq \psi \leq \pi$ and $0 \leq \phi \leq 2\pi$. Show that, for every $f \in \mathscr{C}_c(S^3)$, we have $\int_{S^3} f d\mu =$

$$\frac{1}{2\pi^2}\int_0^\pi\int_0^\pi\int_0^{2\pi} f(\cos\theta, \sin\theta\cos\psi, \sin\theta\sin\psi\cos\phi, \sin\theta\sin\psi\sin\phi)\sin^2\theta\sin\psi d\theta d\psi d\phi.$$

(Feel free to use a computer to calculate any big determinants.)

*Solution.*

(a). It is clear that every matrix as in the statement is in $\mathrm{SU}(2)$. Let's show the converse. Let $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{C})$. Then $A \in \mathrm{U}(2)$ if and only if $A^*A = I_2$, which means that the two column vectors of $A$ are orthogonal and norm 1 for the usual Hermitian inner product on $\mathbb{C}^2$. As the orthogonal of a line in $\mathbb{C}^2$ is one-dimensional, it implies that there exists $\lambda \in \mathbb{C}^\times$ such that $\begin{pmatrix} c \\ d \end{pmatrix} = \lambda \begin{pmatrix} -\overline{b} \\ \overline{a} \end{pmatrix}$. The condition on the norm of the columns gives

$a\overline{a} + b\overline{b} = \lambda\overline{\lambda}(a\overline{a} + b\overline{b}) = 1$, and the condition that $\det(A) = 1$ gives $\lambda(a\overline{a} + b\overline{b}) = 1$. So we get $\lambda = 1$, as desired.

(b). Let $V$ be the space of matrices of the form $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$, with $a, b \in \mathbb{C}$. Then $\alpha$ extends to a $\mathbb{C}$-linear isomorphism from $V$ to $\mathbb{C}^2$, hence to a $\mathbb{R}$-linear isomorphism from $V$ to $\mathbb{R}^4$, sending $\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$ to $(\mathrm{Re}(a), \mathrm{Im}(a), \mathrm{Re}(b), \mathrm{Im}(b))$. If $A \in \mathrm{SU}(2)$, then the action by left multiplication of $A$ on $V$ is the usual action of $A$ on $\mathbb{C}^2$, so it corresponds to a linear automorphism of $\mathbb{R}^4$ which preserves the usual Euclidian norm, i.e. is in $\mathbf{O}(4)$. Also, the determinant of this action is just $\det(A) = 1$, so the corresponding automorphism of $\mathbb{R}^4$ is in $\mathrm{SO}(4)$.

(c). First, note that $\mu$ is a regular Borel measure on $S^3$ (a subset $E$ of $S^3$ is a Borel subset if and only $\{tx, t \in [0,1], x \in E\}$ is a Borel subset of $\mathbb{R}^4$, it is compact if and only if $\{tx, t \in [0,1], x \in E\}$ is compact and openif and only if $\{tx, t \in (0,1], x \in E\}$ (which has the same measure as $\{tx, t \in [0,1], x \in E\}$) is open).

By the change of variables formula in $\mathbb{R}^4$, the measure $\mu$ is invariant by the action of $\mathrm{SO}(4)$ on $S^3$. By question (b), its inverse image by $\alpha$ is invariant by left translations on $\mathrm{SU}(2)$, hence a left Haar measure. But the group $\mathrm{SU}(2)$ is compact, so every left Haar measure is also a right Haar measure.

(d). Let $B^4$ be the closed unit ball in $\mathbb{R}^4$. Let $f \in \mathscr{C}_c(S^3)$. We define a function $g \in L^1(B^4)$ by

$$g(r\cos\theta, r\sin\theta\cos\psi, r\sin\theta\sin\psi\cos\phi, r\sin\theta\sin\psi\sin\phi) =$$

$$f(\cos\theta, \sin\theta\cos\psi, \sin\theta\sin\psi\cos\phi, \sin\theta\sin\psi\sin\phi)$$

for $0 \leq r \leq 1$. (Note : $g$ might not be well-defined at $0$, but it doesn't matter because $\{0\}$ has volume $0$.) Then, by definition of $\mu$, we have $\int_{S^3} f d\mu = \frac{2}{\pi^2}\int_{B^4} g d\lambda$. We can calculate this last integral using the change of variables formula (and avoiding the set where this change of variables is not bijective, which is of volume $0$ anyway). If $\beta$ is the map sending $(r, \theta, \varphi, \psi)$ to $(r\cos\theta, r\sin\theta\cos\psi, r\sin\theta\sin\psi\cos\phi, r\sin\theta\sin\psi\sin\phi)$, then we have

$$D\beta(r, \theta, \varphi, \psi) = r^3(\sin\theta)^2\sin\psi,$$

so $\int_{B^4} g d\lambda$ is equal to

$$\int_0^1\int_0^\pi\int_0^\pi\int_0^{2\pi} f(\cos\theta, \sin\theta\cos\psi, \sin\theta\sin\psi\cos\phi, \sin\theta\sin\psi\sin\phi) r^3\sin^2\theta\sin\psi dr d\theta d\psi d\phi =$$

$$\frac{1}{4}\int_0^\pi\int_0^\pi\int_0^{2\pi} f(\cos\theta, \sin\theta\cos\psi, \sin\theta\sin\psi\cos\phi, \sin\theta\sin\psi\sin\phi)\sin^2\theta\sin\psi d\theta d\psi d\phi.$$

We get the result by multiplying by $\frac{2}{\pi^2}$.

□

## I.5.4 The dual of a locally compact abelian group

**Exercise I.5.4.1.** Let $G$ be an abelian topological group. We write $\widehat{G}$ for the set of continuous group morphisms $G \to S^1$.

As the product of two continuous morphisms from $G$ is $S^1$ is also a continuous morphism from $G$ to $S^1$ (because $S^1$ is commutative), the set $\widehat{G}$ has a natural group structure. We put the topology of compact convergence on $\widehat{G}$; that is, if $\chi \in \widehat{G}$, then a basis of neighborhoods of $\chi$ is given by $\{\psi \in \widehat{G} | \sup_{x \in K} |\chi(x) - \psi(x)| < c\}$, for all compact subsets $K$ of $G$ and all $c > 0$.

(a). Show that $\widehat{G}$ is a topological group. This is called the *dual group* of $G$.

(b). Suppose that $G = \mathbb{R}$.

  (i) Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a continuous group morphism. Show that there exists a unique $A \in M_n(\mathbb{C})$ such that, for every $t \in \mathbb{R}$, $\rho(t) = \exp(tA)$. (There are several ways to do this. One way is to notice that, if the conclusion is true, then $c'(0)$ must exist and be equal to $A$, and to work backwards from there.)

  (ii) Show that the image of $\rho$ is contained in $\mathrm{U}(n)$ if and only if $A^* = -A$.

  (iii) Show that the map $\mathbb{R} \to \widehat{G}$ sending $x \in \mathbb{R}$ to the group morphism $G \to S^1, t \longmapsto e^{ixt}$ is an isomorphism of topological groups (i.e. a group isomorphism that is also a homeomorphism).

(c). Show that there is an isomorphism of topological groups $\widehat{S^1} \simeq \mathbb{Z}$ that sends $\mathrm{id}_{S^1}$ to $1$.

(d). What is the topological group $\widehat{\mathbb{Z}}$ ?

(e). Suppose that $G = \mathbb{Q}_p$ (cf. exercise I.5.1.4). We define a map $\chi_1 : \mathbb{Q}_p \to S^1$ in the following way : If $x \in \mathbb{Q}_p$, we can write $x = \sum_{n=-\infty}^{+\infty} c_n p^n$, with $0 \leq c_n \leq p-1$ and $c_n = 0$ for $n$ small enough, and this uniquely determines the $c_n$ (see question I.5.1.4(i)). We set

$$\chi_1(x) = \exp\left(2\pi i \sum_{n=-\infty}^{-1} c_n p^n\right).$$

  (i) Show that $\chi_1 : \mathbb{Q}_p \to S^1$ is a continuous group morphism and that $\mathrm{Ker}(\chi_1) = \mathbb{Z}_p$.

  (ii) For every $y \in \mathbb{Q}_p$, we define $\chi_y : \mathbb{Q}_p \to S^1$ by $\chi_y(x) = \chi(xy)$. Show that this is also a continuous group morphism, and find its kernel.

  (iii) Let $\chi \in \widehat{\mathbb{Q}_p}$. Show that there exists $k \in \mathbb{Z}$ such that $\chi = 1$ on $\{x \in \mathbb{Q}_p | |x|_p \leq p^{-k}\}$.

  (iv) Let $\chi \in \widehat{\mathbb{Q}_p}$ such that $\chi(1) = 1$ and $\chi(p^{-1}) \neq 1$. Show that there exists a sequence of integers $(c_r)_{r \geq 0}$ such that $1 \leq c_0 \leq p-1$ and $0 \leq c_r \leq p-1$ for $r \geq 1$ and that, for every $k \in \mathbb{Z}_{\geq 1}$,

$$\chi(p^{-k}) = \exp\left(2\pi i \sum_{r=1}^{k} c_{k-r} p^{-r}\right).$$

(v) Let $\chi \in \widehat{\mathbb{Q}_p}$ such that $\chi(1) = 1$ and $\chi(p^{-1}) \neq 1$. Show that there exists $y \in \mathbb{Q}_p$ such that $|y|_p = 1$ and $\chi = \chi_y$.

(vi) Show that the map $\mathbb{Q}_p \to \widehat{\mathbb{Q}_p}$, $y \longmapsto \chi_y$ is an isomorphism of topological groups.

(vii) Show that $\chi_{y|\mathbb{Z}_p} = \chi_{y'|\mathbb{Z}_p}$ if and only $y - y' \in \mathbb{Z}_p$, and that the map $y \longmapsto \chi_y$ induces an isomorphism of topological groups $\mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{\to} \widehat{\mathbb{Z}_p}$, where $\mathbb{Q}_p/\mathbb{Z}_p$ has the discrete topology.

*Solution.*

(a). We need to check the group operations of $\widehat{G}$ are continuous. Let's start with multiplication. Let $\chi_1, \chi_2 \in \widehat{G}$, and choose a neighborhood $U$ of $\chi_1\chi_2$ of the form $\{\psi \in \widehat{G} | \sup_{x\in K} |\chi(x) - \psi(x)| < c\}$, with $K \subset G$ compact and $c > 0$. We need to find neighborhoods $U_1$ of $\chi_1$ and $U_2$ of $\chi_2$ such that $U_1U_2 \subset U$. Take

$$U_i = \{\psi \in \widehat{G} | \sup_{x\in K} |\chi_i(x) - \psi(x)| < c/2\}$$

for $i = 1, 2$. Let $\psi_1 \in U_1$ and $\psi_2 \in U_2$. Then, if $x \in K$, we have

$$\begin{aligned}
|(\psi_1\psi_2)(x) - (\chi_1\chi_2)(x)| &= |\psi_1(x)(\psi_2(x) - \chi_2(x)) + \chi_2(x)(\psi_1(x) - \chi_1(x))| \\
&\leq |\psi_1(x)||\psi_2(x) - \chi_2(x)| + |\chi_2(x)||\psi_1(x) - \chi_1(x)| \\
&= |\psi_2(x) - \chi_2(x)| + |\psi_1(x) - \chi_1(x)| \text{ (because } \psi_1 \text{ and } \chi_2 \text{ are unitary)} \\
&< c.
\end{aligned}$$

So $\psi_1\psi_2 \in U$.

The proof for inversion is similar. Let $\chi \in \widehat{G}$, and choose a neighborhood $U$ of $\chi^{-1}$ of the form $\{\psi \in \widehat{G} | \sup_{x\in K} |\chi^{-1}(x) - \psi(x)| < c\}$, with $K \subset G$ compact and $c > 0$. We need to find a neighborhood $V$ of $\chi$ such that $V^{-1} \subset U$. Take $V = \{\psi \in \widehat{G} | \sup_{x\in K} |\chi(x) - \psi(x)| < c\}$. Let $\psi \in V$. Then, for every $x \in K$, we have

$$|\psi^{-1}(x) - \chi^{-1}(x)| = |\psi^{-1}(x)||\chi^{-1}||\chi(x) - \psi(x)| = |\chi(x) - \psi(x)| < c.$$

So $\psi^{-1} \in U$.

(b). (i) Choose a norm $\|.\|$ on $M_n(\mathbb{C})$. As $\mathrm{GL}_n(\mathbb{C})$ is open in $M_n(\mathbb{C})$, we can choose a nonempty open ball $B$ center of $I_n$ such that $B \subset \mathrm{GL}_n(\mathbb{C})$. We only care about the fact that $B$ is a convex subset of $M_n(\mathbb{C})$. As $\rho$ is continuous and $\rho(0) = I_n$, we can find $c > 0$ such that $\rho([0, c]) \subset B$. Then

$$\int_0^1 \rho(cx)dx = c\int_0^c \rho(x)dx \in B,$$

so $X := \int_0^c \rho(x)dx \in \mathrm{GL}_n(\mathbb{C})$. For every $t \in \mathbb{R}$, we have

$$X\rho(t) = \int_0^c \rho(x+t)dx = \int_t^{t+c} \rho(x)dx.$$

In particular, $\rho$ is continuously differentiable, and

$$\rho'(t) = X^{-1}(\rho(t+c) - \rho(t)) = X^{-1}(\rho(c) - I_n)\rho(t).$$

The only solution of this differential equation satisfying the initial condition $\rho(0) = I_n$ is $\rho(t) = \exp(tA)$, with $A = X^{-1}(\rho(c) - I_n)$. Finally, the matrix is uniquely determined by $\rho$, because we must have $A = \rho'(0)$.

(ii) If $A^* = -A$, then, for every $t \in \mathbb{R}$,

$$\rho(t)\rho(t)^* = \exp(tA)\exp(tA^*) = \exp(t(A + A^*)) = \exp(0) = I_n$$

(we use the fact that $tA$ and $tA^*$ commute to get the equality $\exp(tA)\exp(tA^*) = \exp(tA + tA^*)$), so $\rho(t) \in \mathrm{U}(n)$.

Conversely, suppose that $\rho(\mathbb{R}) \subset \mathrm{U}(n)$. Note that $A = \lim_{t\to 0} \frac{1}{t}(\rho(t) - I_n)$, so $A^* = \lim_{t\to 0} \frac{1}{t}(\rho(t)^* - I_n)$. As

$$\rho(t)^* - I_n = \rho(t)^{-1} - I_n = -\rho(t)^{-1}(\rho(t) - I_n)$$

and $\rho(t)^{-1} \to I_n$ as $t \to 0$, this implies that $A^* = -A$.

(iii) Let's denote by $\alpha$ the map $\mathbb{R} \to \widehat{G}$ of the statement.

We have seen in (i) and (ii) that every continuous group morphism $\rho : \mathbb{R} \to S^1$ is of the form $\rho(t) = e^{zt}$, for a unique $z \in \mathbb{C}$ such that $\overline{z} = -z$; that last condition means that $z = ix$ for some $x \in \mathbb{R}$. This means that $\alpha$ is bijective. It is also easy to see that $\alpha$ is a morphism of groups, so we just need to show that $\alpha$ is a homeomorphism.

We first show that $\alpha$ is continuous. Let $x \in \mathbb{R}$, and consider a neighborhood $U$ of $\alpha(x)$ of the form $\{\rho \in \widehat{G} | \forall t \in K,\ |\alpha(x)(t) - \rho(t)| < c\}$, where $K \subset \mathbb{R}$ is a compact subset and $c > 0$. Then, for every $y, t \in \mathbb{R}$, we have

$$|\alpha(x)(t) - \alpha(y)(t)|^2 = |e^{ixt} - e^{iyt}|^2 = |1 - e^{it(x-y)}|^2 = (1 - \cos(t(x-y)))^2 + (\sin(t(x-y)))^2.$$

Choose $\varepsilon > 0$ such that, for every $t \in K$ and $z \in (-\varepsilon, \varepsilon)$, we have $(1 - \cos(tz))^2 + (\sin(tz))^2 < c^2$. Then, if $|x - y| < \varepsilon$, we have $\alpha(y) \in U$.

Now we show that $\alpha$ is open. Let $x \in \mathbb{R}$, and choose a neighborhood $V$ of $x$ of the form $(x-\varepsilon, x+\varepsilon)$, with $\varepsilon$ (these form a basis of neighborhoods). We want to show that $\alpha(V)$ contains a neighborhood of $\alpha(x)$. Choose $\delta > 0$ such that the functions $t \longmapsto \sin(t)$ and $t \longmapsto 1-\cos(t)$ are both increasing on $[0, 2\delta\varepsilon]$, and let

$$U = \{\rho \in \widehat{G} | \forall t \in K,\ |\alpha(x)(t) - \rho(t)| < c\},$$

where $K = [-\delta, \delta]$ and $c = \left(\sup_{t\in[0,\varepsilon\delta/2]}(1-\cos(t))^2 + (\sin(t))^2\right)^{1/2}$ (note that this is also the sup on $[-\varepsilon\delta/2, \varepsilon\delta/2]$, because the function we are bounding is even). Let $y \in \mathbb{R}$ such that $|x-y| \geq \varepsilon$. We want to show that $\alpha(y) \notin U$. We can find $t \in K$ such that $\varepsilon\delta \leq t(x-y) \leq 2\varepsilon\delta$. Then we have

$$|\alpha(x)(t) - \alpha(y)(t)| = \left((1-\cos(t(x-y)))^2 + (\sin(t(x-y)))^2\right)^{1/2} > c,$$

by the choice of $\delta$ and $c$. So $\alpha(y) \notin U$.

(c). Note that we have an isomorphism of topological groups $\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} S^1$ given by $t \longmapsto e^{it}$. So we get an isomorphism of groups

$$\widehat{S^1} \simeq \{\rho \in \widehat{\mathbb{R}} | \rho(2\pi\mathbb{Z}) = \{1\}\} \simeq \{x \in \mathbb{R} | \forall t \in 2\pi\mathbb{Z},\ e^{ixt} = 1\} = \mathbb{Z}$$

(where the second isomorphism comes from question (b)). It remains to show that this is an isomorphism of topological groups, i.e. that $\widehat{S^1}$ is discrete. If you have read ahead, you know that this is a particular case of question I.5.4.2(e) (and I don't know a simpler proof in the case of $S^1$).

(d). As $\mathbb{Z}$ is discrete, a continuous group morphism from $\mathbb{Z}$ to $S^1$ is just a group morphism from $\mathbb{Z}$ to $S^1$. As $\mathbb{Z}$ is the free abelian group generated by $1 \in \mathbb{Z}$, the map $\rho \longmapsto \rho(1)$ is an isomorphism between the set of group morphisms $\mathbb{Z} \to S^1$ and $S^1$. So, as a group, $\widehat{\mathbb{Z}}$ is isomorphic to $S^1$. Let's denote this isomorphism by $\beta : S^1 \to \widehat{\mathbb{Z}}$ (so $\beta$ sends $z \in S^1$ to the morphism $\mathbb{Z} \to S^1$, $n \longmapsto z^n$). If we show that $\beta$ is continuous, then it will automatically be a homeomorphism because $S^1$ is compact. But the compact subsets of $\mathbb{Z}$ are its finite subsets, so the continuity of $\beta$ follows immediately from the continuity of the maps $S^1 \to S^1$, $z \longmapsto z^n$.

(e). (i) Let $x, x' \in \mathbb{Q}_p$, and write $x = \sum_{n=-\infty}^{+\infty} c_n p^n$ $x' = \sum_{n=-\infty}^{+\infty} c'_n p^n$ (with the same conditions on the $c_n$ and $c'_n$ as in the statement). Then, by I.5.1.4(h), we have, for every $N \in \mathbb{Z}$, $|x - x'|_p \leq p^{-N}$ if $c_n = c'_n$ for every $n \leq N-1$. In particular, $\chi_1(x) = \chi_1(x')$ if $|x-x'|_p \leq 1$, so $\chi_1$ is continuous and sends every $x \in \mathbb{Z}_p$ to $1 = \chi_1(0)$.

We still need to show that $\chi_1$ is a morphism of groups. Let $G'$ be the subgroup of $\mathbb{Q}_p$ whose elements are the $x \in \mathbb{Q}_p$ that can be writte $x = \sum_{n=-\infty}^{+\infty} a_n p^n$, with $a_n \in \mathbb{Z}$ and $a_n = 0$ for $|n|$ big enough. This is a dense subgroup (because $\sum_{n=-\infty}^{+\infty} c_n p^n$ is the limit as $N \to +\infty$ of $\sum_{n=-\infty}^{N} c_n p^n$), and it is contained in $\mathbb{Q}$. As we know that

$\chi_1$ is continuous, it suffices to prove that $\chi_1(x+y) = \chi_1(x)\chi_1(y)$ $x, y \in G'$. But note that, if $x \in G'$, then $\chi_1(x) = \exp(2\pi i x)$, where we see $x$ as an element of $\mathbb{Q}$. This implies the result.

Finally, we have to show that $\operatorname{Ker}(\chi_1) = \mathbb{Z}_p$. We have already seen that $\mathbb{Z}_p \subset \operatorname{Ker}(\chi_1)$. Conversely, let $x \in \mathbb{Q}_p$, and write $x = \sum_{n=-\infty}^{+\infty} c_n p^n$ as above. Suppose that $x \notin \mathbb{Z}_p$, then there exists $m < 0$ such that $c_m \neq 0$. Choose such a $m$. We have

$$p^{-m} \leq c_m p^{-m} < \sum_{n=-\infty}^{-1} c_n p^n \leq (p-1) \sum_{r \geq 1} p^{-r} = 1$$

(the second inequality is strict because the $c_n$ are 0 for $n$ small enough). So $\sum_{n=-\infty}^{-1} c_n p^n \in (0,1)$, and $\chi_1(x) = \exp(2\pi i \sum_{n=-\infty}^{-1} c_n p^n) \neq 1$.

(ii) The map $\chi_y$ is a continuous group morphism because it is the composition of the continuous group morphisms $\chi_1$ and $m_y : \mathbb{Q}_p \to \mathbb{Q}_p,\ x \longmapsto xy$. An element $x \in \mathbb{Q}_p$ is in the kernel of $\chi_y$ if and only if $xy \in \operatorname{Ker}(\chi_1) = \mathbb{Z}_p$. So, if $y = 0$, we have $\operatorname{Ker}(\chi_y) = \mathbb{Q}_p$, and if $y \neq 0$, we have

$$\operatorname{Ker}(\chi_y) = y^{-1}\mathbb{Z}_p = |y|_p \mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq |y|_p^{-1}\}.$$

(iii) Choose a neighborhood $U$ of 1 in $\mathbb{C}^\times$ such that the only subgroup of $\mathbb{C}^\times$ contained in $U$ is the trivial group. (See 3(b).) Then $\chi^{-1}(U \cap S^1)$ is a neighborhood of 1 in $\mathbb{Q}_p$, so there exists $k \in \mathbb{Z}$ such that $\chi^{-1}(U \cap S^1) \supset \{x \in \mathbb{Q}_p | |x|_p \leq p^k\}$. But as $\{x \in \mathbb{Q}_p | |x|_p \leq p^k\}$ is a subgroup of $\mathbb{Q}_p$, its image by $\chi$ is a subgroup of $S^1$ contained in $U$, hence is equal to $\{1\}$.

(iv) Write, for every integer $r \geq 0$, $z_r = \chi(p^{-r})$. Then $z_r \in S^1$ and, for every $r \geq 0$, we have

$$z_{r+1}^p = \chi(p^{-r-1})^p = \chi(p^{-r}) = z_r.$$

We will construct the integers $c_r$ by induction on $r \geq 0$. Note first that $z_1 \neq 1 = z_0$ by hypothesis, so we can find $c_0 \in \{1, \ldots, p-1\}$ such that $z_1 = \exp(2\pi i c_0 p^{-1})$. Suppose that we have found $c_0, \ldots, c_{r-1}$ (with $r \geq 1$) such that, for $1 \leq s \leq r$, we have

$$\chi(p^{-s}) = z_s = \exp(2\pi i \sum_{k=1}^{s} c_{s-k} p^{-k}).$$

We have to find $c_r \in \{0, \ldots, p-1\}$ such that

$$z_{r+1} = \exp(2\pi i \sum_{k=1}^{r+1} c_{r+1-k} p^{-k}) = \exp(2\pi i p^{-(r+1)} \sum_{s=0}^{r} c_s p^s).$$

As $z_{r+1}^p = z_r$, we have

$$\left( z_{r+1} \exp(2\pi i p^{-r-1} \sum_{s=0}^{r-1} c_s p^s) \right)^p = 1,$$

so there exists $c_r \in \{0, \ldots, p-1\}$ such that

$$z_{r+1} \exp(2\pi i p^{-r-1} \sum_{s=0}^{r-1} c_s p^s) = \exp(2\pi i p^{-1} c_r),$$

i.e.

$$z_{r+1} = \exp(2\pi i p^{-(r+1)} \sum_{s=0}^{r} c_s p^s).$$

(v) Let $(c_r)_{r\geq 0}$ be as in (iv), and set $y = \sum_{r=0}^{+\infty} c_r p^r$. As $c_0 \in \{1, \ldots, p-1\}$, we have $|y|_p = 1$. Also, for every $r \geq 1$, we have

$$\chi(p^{-r}) = \exp(2\pi i p^{-(r+1)} \sum_{k=-r}^{-1} c_{r+k} p^k) = \chi_1(p^{-r} y) = \chi_y(1),$$

because

$$p^{-r} y = \sum_{s\geq 0} c_s p^{r-s} = \sum_{n=-r}^{+\infty} c_{r+n} p^n.$$

On the other hand, if $r \geq 0$, then

$$\chi(p^r) = \chi(1)^{p^r} = 1 = \chi_y(p^r).$$

As $\chi$ and $\chi_y$ are continuous morphisms of groups, and as the family $(p^r)_{r\in\mathbb{Z}}$ generates a dense subgroup of $\mathbb{Q}_p$, this implies that $\chi = \chi_y$.

(vi) Let us denote the map $\mathbb{Q}_p \to \widehat{\mathbb{Q}_p}$, $y \longmapsto \chi_y$ by $\alpha$. It is easy to see that $\alpha$ is a morphism of groups (this follows immediately from the fact that $\chi_1$ is a morphism of groups and the distributivity of multiplication on $\mathbb{Q}_p$.)

We first show that $\operatorname{Ker}(\alpha) = \{0\}$. Let $y \in \mathbb{Q}_p - \{0\}$. Then we have $y = \sum_{n=m}^{+\infty} c_n p^n$ with $m \in \mathbb{Z}$, $0 \leq c_n \leq p-1$ and $c_m \geq 1$. So

$$p^{-m-1} y = c_m p^{-1} + \sum_{n\geq 0} c_{n+m+1} p^n,$$

and $\chi_y(p^{-m-1}) = \exp(2\pi i p^{-1} c_m) \neq 1$. This shows that $y \notin \operatorname{Ker}(\alpha)$.

Now we show that $\alpha$ is surjective. Let $\chi \in \widehat{\mathbb{Q}_p}$. If $\chi = 1$, then $\chi = \chi_0$, so we assume that $\chi \neq 1$. By (iii), there exists $k \in \mathbb{Z}$ such that $\chi = 1$ on $\{x \in \mathbb{Q}_p | |x|_p \leq p^{-k}\}$. Choose $k$ minimal for this property (this is possible because otherwise $\chi$ would be 1 on all of $\mathbb{Q}_p$, which contradicts our hypothesis that $\chi \neq 1$). Then there exists $a \in \mathbb{Q}_p$ such that $|a|_p = p^{-k+1}$ and $\chi(a) \neq 1$. Define $\psi \in \widehat{\mathbb{Q}_p}$ by $\psi(x) = \chi(pax)$. Then $\psi(p^{-1}) = \chi(a) \neq 1$ and $\psi(1) = \chi(pa) = 1$ (because $|pa|_p = p^{-k}$). By (v), there exists $y \in \mathbb{Z}_p$ such that $\psi = \chi_y$. In other words, for every $x \in \mathbb{Q}_p$,

$$\chi(x) = \psi(p^{-1} a^{-1} x) = \chi_1(p^{-1} a^{-1} y x),$$

i.e. $\chi = \alpha(p^{-1}a^{-1}y)$.

We show that $\alpha$ is continuous. Let $y \in \mathbb{Q}_p$, and choose a neighborhood $U$ of $\alpha(y)$ of the form

$$U = \{\chi \in \widehat{\mathbb{Q}_p} | \forall x \in K,\ |\chi(x) - \chi_y(x)| < c\},$$

where $K$ is a compact subset of $\mathbb{Q}_p$ and $c > 0$. We are looking for a neighborhood $V$ of $y$ in $\mathbb{Q}_p$ such that $\alpha(V) \subset U$.

As $\mathbb{Q}_p = \bigcup_{k\in\mathbb{Z}} p^k\mathbb{Z}_p$, we may assume that $K = p^N\mathbb{Z}_p$ for some $N \in \mathbb{Z}$. We know that $\chi_1$ is constant on the cosets of $\mathbb{Z}_p$ in $\mathbb{Q}_p$, so, if $x \in p^N\mathbb{Z}_p$, then $\chi_x$ is constant on the cosets of $p^{-N}\mathbb{Z}_p$ in $\mathbb{Q}_p$. Hence, if $y' \in y + p^{-N}\mathbb{Z}_p$, then, for every $x \in K = p^N\mathbb{Z}_p$,

$$|\chi_{y'}(x) - \chi_y(x)| = |\chi_x(y') - \chi_x(y)| = 0 < c.$$

In other words, $\alpha(y + p^{-N}\mathbb{Z}_p) \subset U$.

Finally, we show that $\alpha$ is open. Let $y \in \mathbb{Q}_p$, and let $V$ be a neighborhood of $y$. We may assume that $V$ is of the form $y + p^N\mathbb{Z}_p = \{y' \in \mathbb{Q}_p | |y' - y|_p \leq p^{-N}\}$ for some $N \in \mathbb{Z}$. We want to show that $\alpha(V)$ contains a neighborhood of $\alpha(y)$. As $\alpha$ is a morphism of groups, we may assume that $y = 0$. Let

$$U = \{\chi \in \widehat{\mathbb{Q}_p} | \forall x \in p^{-N}\mathbb{Z}_p,\ |\chi(x) - \chi_y(x)| < c\},$$

where $c = \min_{1\leq r\leq p-1} |1 - e^{2\pi i r p^{-1}}|$, and let's show that $\alpha(p^N\mathbb{Z}_p) \supset U$. Let $y' \notin p^N\mathbb{Z}_p$, we want to show that $\chi_{y'} \notin U$. We write $y' = \sum_{n=m}^{+\infty} c_n p^n$ with $c_n \in \{0, \dots, p-1\}$ for every $n \geq m$ and $c_m \geq 1$. Then the hypothesis on $y'$ says that $m < N$. Let $x = p^{-m-1}$. Then $x \in p^{-N}\mathbb{Z}_p$, and

$$\chi_{y'}(x) = \chi_1(xy') = \exp(2\pi i p^{-1} c_m),$$

so $|\chi_{y'}(x) - 1| \geq c$ and $\chi_{y'} \notin U$.

(vii) As the map $y \longmapsto \chi_y$ is a morphism of groups, the first statement is equivalent to the fact that $\chi_{y|\mathbb{Z}_p} = 1$ if and only if $y \in \mathbb{Z}_p$. We know that $\operatorname{Ker}(\chi_1) = \mathbb{Z}_p$, so $\operatorname{Ker}(\chi_y) \supset \mathbb{Z}_p$ for every $y \in \mathbb{Z}_p$. Conversely, let $y \in \mathbb{Q}_p - \mathbb{Z}_p$. Then $|y|_p > 1$, so $|y|_p \geq p$, so $|py|_p \geq 1$, and $p^{-1}y^{-1} \in \mathbb{Z}_p$. As $\chi_y(p^{-1}y^{-1}) = \chi_1(p^{-1}) = \exp(2\pi i p^{-1}) \neq 1$, $\operatorname{Ker}(\chi_y) \not\supset \mathbb{Z}_p$.

So the map $y \longmapsto \chi_y$ induces an injective morphism of groups from $\mathbb{Q}_p/\mathbb{Z}_p$ to $\widehat{\mathbb{Z}_p}$. We know (or will soon know) that $\widehat{\mathbb{Z}_p}$ is discrete by I.5.4.2(e), so it just remains to show that every element of $\widehat{\mathbb{Z}_p}$ is of the form $\chi_{y|\mathbb{Z}_p}$ for some $y \in \mathbb{Q}_p$.

Let $\chi \in \widehat{\mathbb{Z}_p}$. As in (iii), we can find $k \in \mathbb{N}$ such that $\operatorname{Ker}(\chi) \supset p^k\mathbb{Z}_p$. Let $z = \chi(1)$. Then $z^{p^k} = \chi(p^k) = 1$, so we can find $c \in \{0, \dots, p^k - 1\}$ such that $z = e^{2\pi i c p^{-k}}$. Write $c = \sum_{r=0}^{k-1} c_r p^r$, with $c_r \in \{0, \dots, p-1\}$. Then

$$\chi(1) = \exp(2\pi i \sum_{r=0}^{k-1} c_r p^{r-k}) = \exp(2\pi i \sum_{n=-k}^{-1} c_{k+n} p^n).$$

Let $y = \sum_{n=-k}^{-1} c_{k+n}p^n$. Then $\chi(1) = \chi_y(1)$. As $\chi_{y|\mathbb{Z}_p}$ and $\chi$ are continuous group morphisms on $\mathbb{Z}_p$, and as $1$ generates a dense subgroup of $\mathbb{Z}_p$, this implies that $\chi = \chi_{y|\mathbb{Z}_p}$.

$\square$

**Exercise I.5.4.2.** We use the notation of the previous exercise, and we suppose that $G$ is an abelian locally compact group and fix a Haar measure $\mu$ on $G$.

Remember that we have an isomorphism $L^\infty(G) \to L^1(G)^\vee := \mathrm{Hom}(L^1(G), \mathbb{C})$ sending $f \in L^\infty(G)$ to the bounded operator $g \longmapsto \int_G fgd\mu$ on $L^1(G)$. (This does not use the fact that $G$ is an abelian group.) So we can consider the weak* topology (or topology of pointwise convergence) on $L^\infty(G)$ : for $f \in L^\infty(G)$, a basis of neighborhoods of $f$ is given by the sets $U_{g_1,\dots,g_n,c} = \{f' \in L^\infty(G) || \int_G (f - f')g_i d\mu| < c,\ 1 \leq i \leq n\}$, for $n \in \mathbb{Z}_{\geq 1}$, $g_1, \dots, g_n \in L^1(G)$ and $c > 0$.

(a). Show that $\widehat{G} \subset L^\infty(G)$, and that the topology of $\widehat{G}$ is induced by the weak* topology of $L^\infty(G)$. [16]

(b). Show that the subset $\widehat{G} \cup \{0\}$ of $L^\infty(G)$ is closed for the weak* topology. (Hint : Identify it to the set of representations of the Banach $*$-algebra $L^1(G)$ on $\mathbb{C}$.)

(c). Show that $\widehat{G}$ is a locally compact topological group. (Hint : Alaoglu's theorem.)

(d). If $G$ is discrete, show that $\widehat{G}$ is compact.

(e). If $G$ is compact, show that $\widehat{G}$ is discrete.

*Solution.*

(a). An element of $\widehat{G}$ is a continuous function from $G$ to $S^1$, hence a continuous bounded function on $\widehat{G}$, hence an element of $L^\infty(G)$. Now we have to show that the two topologies on $\widehat{G}$ coincide.

Let $\chi \in \widehat{G}$. First, let $f_1, \dots, f_n \in L^1(G)$, and let $c > 0$. This defines a weak* open neighborhood

$$U = \{\psi \in \widehat{G} | \forall i \in \{1, \dots, n\},\ |\int_G \chi f_i d\mu - \int_G \psi f_i d\mu| < c\}$$

of $\chi$. We want to find an open neighborhood $V$ of $\chi$ for the topology of compact convergence such that $V \subset U$. Let $\varepsilon > 0$. Choose a compact subset $K$ of $G$ such that $\int_{G-K} |f_i| d\mu < \varepsilon$ for every $i \in \{1, \dots, n\}$ (this is possible by inner regularity of $\mu$). Let

$$V = \{\psi \in \widehat{G} | \forall x \in K,\ |\chi(x) - \psi(x)| < \varepsilon\}.$$

[16] Hard question.

Then, if $\psi \in V$ and $i \in \{1, \dots, n\}$, we have

$$\begin{aligned}|\int_G \chi f_i d\mu - \int_G \psi f_i d\mu| &\leq \int_K |f_i(x)||\chi(x) - \psi(x)| d\mu(x) + \int_{G-K} |f_i(x)||\chi(x) - \psi(x)| dx \\ &\leq \varepsilon \int_K |f_i(x)| d\mu(x) + 2 \int_{G-K} |f_i(x)| d\mu(x) \\ &\leq \varepsilon(\|f_i\|_1 + 2)\end{aligned}$$

So, if we take $\varepsilon$ small enough, we'll get $V \subset U$.

Now we prove the converse. Let $\chi \in \widehat{G}$, let $K$ be a compact subset of $G$ and let $c > 0$. We consider the neighborhood

$$V = \{\psi \in \widehat{G} | \forall x \in K,\ |\chi(x) - \psi(x)| < \varepsilon\}$$

of $\chi$ in the topology of compact convergence. We have to find a weak* neighborhood included in it. Let $\eta > 0$ (to be fiddled with later), and choose a compact neighborhood $A$ of $1$ such that, for every $y \in A$, we have $|\chi(y) - 1| < \eta$. Let $f = \mathbb{1}_A$; this is in $L^1(G)$ because $A$ is compact. Note that, for every $x \in G$,

$$\begin{aligned}|\mu(A)\chi(x) - f * \chi(x)| &= \left| \int_A (\chi(x) - \chi(y^{-1}x)) dy \right| \\ &\leq \int_A |1 - \overline{\chi(y)}| dy \\ &\leq \eta \mu(A).\end{aligned}$$

Now we try to find a weak* neighborhood of $\chi$ in $\widehat{G}$ whose elements $\psi$ will satisfy a similar inequality, but for $x \in K$. Note that, if $\psi \in \widehat{G}$ and $x \in G$, then

$$\begin{aligned}f * \psi(x) &= \int_A \chi(y^{-1}x) dy \\ &= \chi(x) \int_A \overline{\chi(y)} dy \\ &= \int_G \psi(y^{-1}) f(xy) dy \\ &= \int_G \overline{\psi(y)} L_{x^{-1}} f(y) dy\end{aligned}$$

(we use that $G$ is commutative and that $\psi$ is a morphism of groups from $G$ to $S^1$). Now remember that the map $G \to L^1(G)$, $x \longmapsto L_{x^{-1}} f$ is continuous (proposition I.3.1.13). As $K$ is compact, we can find $x_1, \dots, x_n$ such that, for every $x \in K$, there exists $i \in \{1, \dots, n\}$ with $\|L_{x^{-1}} f - L_{x_i^{-1}} f\|_1 < \eta\mu(A)$. Consider the following weak* neighborhood of $\chi$ :

$$U = \{\psi \in \widehat{G} | \forall x \in \{1, x_1^{-1}, \dots, x_n^{-1}\},\ \left| \int_G \overline{\chi(y)} L_x f(y) dy - \int_G \overline{\psi(y)} L_x f(y) dy \right| < \eta\mu(A)\}.$$

Let $\psi \in U$. First, we have, for every $x \in G$,

$$\begin{aligned}
|\mu(A)\psi(x) - f * \psi(x)| &= \left| \int_A (\psi(x) - \psi(y^{-1}x) dy \right| \\
&= \left| \int_A (1 - \overline{\psi(y)}) dy \right| \\
&\leq \left| \int_A (1 - \overline{\chi(y)}) dy \right| + \left| \int_A (\overline{\chi(y)} - \overline{\psi(y)}) dy \right| \\
&\leq 2\eta\mu(A).
\end{aligned}$$

Second, we want to bound $|f*\chi(x) - f*\psi(x)|$ for $x \in K$. So fix $x \in K$. Let $i \in \{1, \dots, n\}$ be such that $\|L_{x^{-1}} f - L_{x_i^{-1}} f\|_1 \leq \eta\mu(A)$. Then :

$$\begin{aligned}
|f * \chi(x) - f * \psi(x)| &= \left| \int_G (\overline{\chi(y)} - \overline{\psi(y)}) L_{x^{-1}} f(y) dy \right| \\
&\leq \left| \int_G (\overline{\chi(y)} - \overline{\psi(y)}) L_{x_i^{-1}} f(y) dy \right| \\
&+ \left| \int_G (\overline{\chi(y)} - \overline{\psi(y)}) (L_{x_i^{-1}} f(y) - L_{x^{-1}} f(y)) dy \right| \\
&< \eta\mu(A) + 2 \int_G |L_{x_i^{-1}} f(y) - L_{x^{-1}} f(y)| dy \\
&\leq 3\eta\mu(A).
\end{aligned}$$

Putting everything together, we get, for $x \in K$,

$$|\mu(A)\chi(x) - \mu(A)\psi(x)| < 6\eta\mu(A),$$

i.e. $|\chi(x) - \psi(x)| < 6\eta$. Choosing $\eta$ at the beginning such that $6\eta \leq c$, we get $U \subset V$, as desired.

(b). We have seen in class that $\widehat{G} \subset L^\infty(G) \simeq L^1(G)^\vee$ is the set of nondegenerate representations of the Banach $*$-algebra $L^1(G)$. Let $\pi : L^1(G) \to \mathbb{C}$ be a representation of $L^1(G)$ on $\mathbb{C}$, and assume that it is not nondegenerate. Then there exists $v \in \mathbb{C} - \{0\}$ such that $\pi(f)v = 0$ for every $f \in L^1(G)$. But this implies that $\pi = 0$. So we see that $\widehat{G} \cup \{0\} \subset L^\infty(G)$ is indeed the set of representation of $L^1(G)$ on $\mathbb{C}$. But the conditions saying that a bounded linear functional $\Lambda : L^1(G) \to \mathbb{C}$ is a representation are all closed conditions in the weak* topology (because they all assert that the values of $\Lambda$ at some points of $L^1(G)$ are equal), so the set of representations of $L^1(G)$ is a weak* closed subset of $L^\infty(G)$.

(c). Alaoglu's theorem[17] says that the closed unit ball of $L^\infty(G)$ (for the operator norm coming from $\|.\|_1$, which is just $\|.\|_\infty$) is compact Hausdorff for the weak* topology. But $\widehat{G} \cup \{0\}$ is

[17] ref ?

clearly included in this closed unit ball (this is easy even if we don't know that the operator norm is $\|.\|_\infty$), so is compact Hausdorff for the weak* topology. Hence its open subset $\widehat{G}$ is locally compact for the weak* topology, and we have seen in (i) that the weak* topology on $\widehat{G}$ is equal to the topology of compact convergence, so we are done.

(d). Consider the map $\alpha : \widehat{G} \to (S^1)^G$ sending $\chi$ to the family $(\chi(x))_{x\in G}$. This is obviously injective. As $G$ is discrete, its compact subsets are exactly its finite subsets, so the topology of compact convergence is exactly the topology induced by the product topology on $(S^1)^G$. Also, by Tychonoff's theorem, $(S^1)^G$ is compact Hausdorff. So, to get the result, we only need to show that the image of $\alpha$ is closed in $(S^1)^G$. But the image of $\alpha$ is the intersection of the subsets

$$\{(a_x)_{x\in G} \in (S^1)^G | a_{x_0}a_{y_0} = a_{x_0y_0}\}$$

for all $x_0, y_0 \in G$, and each of these subsets is closed, so $\mathrm{Im}(\alpha)$ is closed.

(e). Suppose that $G$ is compact. Then the topology of $\widehat{G}$ is the topology of uniform convergence (induced by the norm $\|.\|_\infty$). To show that $\widehat{G}$ is discrete, it suffices to show that its subset $\{1\}$ is open (because $\widehat{G}$ is a topological group). Let $c > 0$ be such that the only subgroup of $\mathbb{C}^\times$ included in $\{z \in \mathbb{C}^\times ||1 - z| < c\}$ is the trivial group (see 3(b)). Let $U = \{\chi \in \widehat{G} | \|\chi - 1\|_\infty < c\}$. This is an open neighborhood of 1 in $\widehat{G}$. On the other hand, if $\chi \in U$, we have $\chi(G) \subset \{z \in \mathbb{C}^\times ||1-z| < c\}$; as $\chi(G)$ is a subgroup of $\mathbb{C}^\times$, this means that $\chi(G) = \{1\}$, i.e. $\chi = 1$, and so $U = \{1\}$.

□

## I.5.5 Representations

If $G$ is a group, we say that a representation $(\pi, V)$ of $G$ is *faithful* if $\pi : G \to \mathrm{GL}(V)$ is injective.

**Exercise I.5.5.1.** Let $G = \mathrm{SU}(2)$. The group $G$ acts on $\mathbb{C}^2$ via the inclusion $G \subset \mathrm{GL}_2(\mathbb{C})$, and we just denote this action by $(g, (z_1, z_2)) \longmapsto g(z_1, z_2)$. (This is called the *standard representation* of $G$.)

For every integer $n \geq 0$, let $V_n$ be the space of polynomials $P \in \mathbb{C}[t_1, t_2]$ that are homogeneous of degree $n$ (i.e. $P(t_1, t_2) = \sum_{r=0}^n a_r t_1^r t_2^{n-r}$, with $a_0, \dots, a_n \in \mathbb{C}$).

(a). If $P \in V_n$ and $g \in G$, show that the function $\mathbb{C}^2 \to \mathbb{C}$, $(z_1, z_2) \longmapsto P(g^{-1}(z_1, z_2))$ is still given by a polynomial in $V_n$, and that this defines a continuous representation of $G$ on $V_n$.

(b). Show that the representation $V_n$ of $G$ is irreducible for every $n \geq 0$.

(c). For which values of $n$ is the representation $V_n$ faithful ?

*Remark.* We will see later (see problem IV.9.1) that every irreducible unitary representation of $\mathrm{SU}(2)$ is isomorphic to one of the $V_n$.

*Solution.*

(a). First take $P = t_1^r t_2^{n-r}$, with $0 \leq r \leq n$. Let $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SU}(2)$. As $\det(x) = 1$, we have $x^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. So

$$P(x^{-1}(z_1, z_2)) = (dz_1 - bz_2)^r(-cz_1 + az_2)^{n-r}.$$

This is still a homogeneous polynomial of degree $n$ in $z_1$ and $z_2$, let's call it $P \circ x^{-1}$. Also, it is clear on the formula above that the map $G \to V_n$, $x \longmapsto P \circ x^{-1}$ is continuous (which means that the coefficients of $P \circ x^{-1}$ are continuous functions of the entries of the matrix $x$).

As the monomials $t_1^r t_2^{n-r}$, $0 \leq r \leq n$, generate $V_n$, the previous paragraph implies that, for every $P \in V_n$ and every $x \in \mathrm{SU}(2)$, the function $\mathbb{C}^2 \to \mathbb{C}$, $(z_1, z_2) \longmapsto P(x^{-1}(z_1, z_2))$ is still given by an element of $V_n$, that we will denote by $P \circ x^{-1}$; it also implies that the map $G \to V_n$, $x \longmapsto P \circ x^{-1}$ is continuous.

For every $x \in G$, the map $V_n \to V_n$, $P \longmapsto P \circ x^{-1}$ is clearly $\mathbb{C}$-linear in $P$. (In fact, we have already used that fact.) We also have $P \circ (xy)^{-1} = (P \circ y^{-1}) \circ x^{-1}$ for every $P \in V_n$ and all $x, y \in G$. So it follows from proposition I.3.5.1 that the map $G \times V_n \to V_n$, $(x, P) \longmapsto P \circ x^{-1}$ is continuous, i.e. defines a continuous representation of $G$ on $V_n$.

(b). Let $W$ be a $G$-invariant subspace of $V$. Let $P = \sum_{r=0}^n c_r t_1^r t_2^{n-r} \in W$. We show that, for every $r \in \{0, \dots, n\}$ such that $c_r \neq 0$, we have $t_1^r t_2^{n-r} \in W$. We prove this by induction on the number of nonzero coefficents of $P$. If $P$ has 0 or 1 nonzero coefficients, we are done. Suppose that $P$ has at least 2 nonzero coefficients. Fix $r \in \{0, \dots, n\}$ such that $c_r \neq 0$. It suffices to find another element $Q$ of $W$ such that the coefficient of $t_1^r t_2^{n-r}$ is nonzero, and such that $Q$ has fewer nonzero coefficients than $P$; then we can apply the induction hypothesis to $Q$. Pick $s \in \{0, \dots, n\} - \{r\}$ such that $c_s \neq 0$. Consider $x_a = \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$, with $a \in S^1$. Then $x_a \in \mathrm{SU}(2)$, and

$$P \circ x_a^{-1} = \sum_{i=0}^n \overline{a}^i a^{n-i} c_i t_1^i t_2^{n-i} = \sum_{i=0}^n a^{n-2i} c_i t_1^i t_2^{n-i}.$$

Choose $a, a' \in S^1$ such that $a^{n-2s}c_s - (a')^{n-2s}c_s = 0$ and $a^{n-2r}c_r - (a')^{n-2r}c_r \neq 0$. Then $Q := P \circ x_a^{-1} - P \circ x_{a'}^{-1} \in W - \{0\}$ has the desired properties.

Now suppose that $W \neq 0$. By the previous paragraph, we can find $r \in \{0, \dots, n\}$ such that $P := t_1^t t_2^{n-r} \in W$. Let $x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$, with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. Then $x \in \mathrm{SU}(2)$ and $P \circ x^{-1} = (\overline{a}t_1 - bt_2)^r(\overline{b}t_1 + at_2)^{n-r} \in W$. If we write $P \circ x^{-1} = \sum_{i=0}^n c_i t_1^i t_2^{n-i}$, then

$$c_i = \sum_{j=\max(0,i-n+r)}^{\min(i,r)} (-1)^{r-j} \binom{r}{j} \binom{n-r}{i-j} \overline{a}^j a^{n-r+j-i} b^{r-j} \overline{b}^{i-j}.$$

If we take $a = \frac{1}{\sqrt{1+t^2}}$ and $b = \frac{t}{\sqrt{1+t^2}}$ with $t \in [-1, 1]$, then each $c_i$ is the quotient of a nonzero polynomial in $t$ by $(1 + t^2)^{n/2}$, so there are only finitely many values of $t$ for which $c_i = 0$. Hence we can choose $x \in \mathrm{SU}(2)$ such that $P \circ x^{-1}$ has all its coefficients nonzero. By the first paragraph, this implies that every monomial $t_1^i t_2^{n-i}$, $0 \leq i \leq n$, is in $W$. So $W = V_n$.

(c). Let's write $\pi_n$ for the map $\mathrm{SU}(2) \to \mathrm{GL}(V_n)$. If $n = 0$, then $V_n$ is the trivial representation of $\mathrm{SU}(2)$, so $\mathrm{Ker}(\pi_n) = \mathrm{SU}(2)$. Suppose that $n \geq 1$, and let $x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{Ker}(\pi_n)$. In particular, if $P = t_1^n$, we must have $P \circ x^{-1} = P$. As $P \circ x^{-1} = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i} \overline{a}^i b^{n-i} t_1^i t_2^{n-i}$, this implies that $\overline{a}^n = 1$ and $\overline{a}^i b^{n-1} = 0$ for $0 \leq i \leq n-1$. In particular, $a \neq 0$, so we must have $b = 0$. Then $a \in S^1$, and, for every $r \in \{0, \ldots, n\}$, $(t_1^r t_2^{n-r}) \circ x^{-1} = a^{n-2r} t_1^r t_2^{n-r}$, hence $a^{n-2r} = 1$. If $n$ is odd, this implies that $a = 1$, so $x = I_2$ is the only element of $\mathrm{Ker}(\pi_n)$. If $n$ is even, this only implies that $a = \pm 1$, so $x = \pm I_2$. In fact, if $n$ is even and nonzero, it is easy to check that $-I_2$ acts trivially on $V_n$, so $\mathrm{Ker}(\pi_n) = \{\pm I_2\}$.

So to answer the question, the representation $V_n$ is faithful if and only if $n$ is odd.

□

**Exercise I.5.5.2.** Let $(\pi, V)$ be a finite-dimensional unitary representation of $G := \mathrm{SL}_2(\mathbb{R})$. We want to show that $V$ is trivial (i.e. $\pi(x) = \mathrm{id}_V$ for every $x \in G$).

(a). Consider the morphism of groups $\alpha : \mathbb{R} \to G$ sending $t \in \mathbb{R}$ to the matrix $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$.

Show that there exist a basis $\mathscr{B}$ of $V$ and $y_1, \ldots, y_n \in \mathbb{R}$, where $n = \dim V$, such that, for every $t \in \mathbb{R}$, the endormophism $\pi(\alpha(t))$ is diagonal in $\mathscr{B}$ with diagonal entries $e^{ity_1}, \ldots, e^{ity_n}$.

(b). Show that $\pi(\alpha(t)) = \mathrm{id}_V$ for every $t \in \mathbb{R}$. (Hint : If $u \in \mathbb{R}^\times$ and $x = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$, consider the action of $x\alpha(t)x^{-1}$ on $V$.)

(c). Show that $\pi(x) = \mathrm{id}_V$ for every $x \in G$.

(d). If $n \geq 3$, show that every finite-dimensional unitary representation of $\mathrm{SL}_n(\mathbb{R})$ is trivial.

*Solution.*

(a). The subgroup $\pi(\alpha(\mathbb{R}))$ of $\mathrm{GL}(V)$ is commutative, and all its elements are diagonalizable (because they are all unitary), so we can find a basis $\mathscr{B} = (v_1, \ldots, v_n)$ of $V$ in which all the elements of $\pi(\alpha(\mathbb{R}))$ are diagonal, and even an orthonormal basis if we want. (If you don't like simultaneously diagonalizing an infinite subset of $\mathrm{GL}(V)$, just choose $A_1, \ldots, A_m \in \pi(\alpha(\mathbb{R}))$ that generate $\mathrm{Span}(\pi(\alpha(\mathbb{R})))$ and simultanesouly diagonalize them.)

For every $j \in \{1, \ldots, n\}$, the subspace $\mathbb{C}v_j$ is stable by the action of $\alpha(\mathbb{R}) \subset G$ (by the choice of the basis), so we get a 1-dimensional representation of $\mathbb{R}$ on $\mathbb{C}v_j$, and we know by I.5.4.1(b) that such a representation is of the form $t \longmapsto e^{ity_j}v_j$, for a $y_j \in \mathbb{C}$.

(b). We have $x\alpha(t)x^{-1} = \alpha(u^2t)$, so $\pi(x\alpha(t)x^{-1})$ is diagonal in the basis $\mathscr{B}$ with diagonal entries $e^{iu^2ty_1}, \ldots, e^{iu^2ty_n}$. On the other hand, we have $\mathrm{Tr}(\pi(x\alpha(t)x^{-1})) = \mathrm{Tr}(\pi(x)\pi(\alpha(t))\pi(x)^{-1}) = \mathrm{Tr}(\pi(\alpha(t))$, hence, for every $t \in \mathbb{R}$ and every $u \in \mathbb{R}^\times$,

$$\sum_{j=1}^{n} e^{ity_j} = \sum_{j=1}^{n} e^{iu^2ty_j}.$$

Suppose that we know that the subset $\widehat{\mathbb{R}}$ of $L^\infty(\mathbb{R})$ is linearly independent. Then the equality tells us that, for every $u \in \mathbb{R}^\times$, the sets $\{y_1, \ldots, y_n\}$ and $\{u^2y_1, \ldots, u^2y_n\}$ are equal. This is only possible if $y_1 = \ldots = y_n = 0$, which in turn implies that $\alpha(t)$ acts trivially on $V$ for every $t \in \mathbb{R}$.

Now let's show the statement about $\widehat{\mathbb{R}}$. Let $y_1, \ldots, y_m \in \mathbb{R}$ be pairwise distinct and $c_1, \ldots, c_m \in \mathbb{C}$ be such that $\sum_{j=1}^m c_je^{ity_j} = 0$ for every $t \in \mathbb{R}$. We want to show that $c_1 = \ldots = c_m = 0$. Let $r \in \mathbb{R}$. Taking $t = 0, r, \ldots, r(m-1)$, and using the calculation of the Vandermonde determinant, we see that we must have $e^{iry_1} = \ldots = e^{iry_m}$. As this is true for every $r \in \mathbb{R}$, it implies that $y_1 = \ldots = y_m$ (for example by taking the derivative with respect to $r$ of the previous equalities and then evaluating at $r = 0$). So $m = 1$, and then the fact that $c_1e^{ity_1} = 0$ for every $t \in \mathbb{R}$ implies that $c_1 = 0$.

(c). If $x \in \mathrm{SL}_2(\mathbb{R})$ is a transvection (aka shear) matrix, then we have $x = y\alpha(t)y^{-1}$ for some $t \in \mathbb{R}$ and some $y \in \mathrm{SL}_2(\mathbb{R})$, so $\pi(x) = \pi(y)\pi(\alpha(t))\pi(y)^{1} = \pi(y)\pi(y)^{-1} = \mathrm{id}_V$ by (b). As $\mathrm{SL}_2(\mathbb{R})$ is generated by transvection matrices, this implies that $\pi(x) = \mathrm{id}_V$ for every $x \in \mathrm{SL}_2(\mathbb{R})$.

(d). Let $\pi : \mathrm{SL}_n(\mathbb{R}) \to \mathrm{GL}(V)$ be a finite-dimensional unitary representation. Let $x \in \mathrm{SL}_n(\mathbb{R})$ be a transvection matrix. We could imitate (a) and (b) to prove that $\pi(x) = \mathrm{id}_V$, but we can also do the following thing : Choose a basis $(v_1, \ldots, v_n)$ of $\mathbb{R}^n$ in which the matrix of the linear endomorphism of $\mathbb{R}^n$ corresponding to $x$ is $\begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & \ldots & 0 & \ddots & 0 \\ 0 & & \ldots & & 1 \end{pmatrix}$. Consider the subset $G$ of $\mathrm{SL}_n(\mathbb{R})$ composed of the elements whose matrix in $(v_1, \ldots, v_n)$ is of the form $\begin{pmatrix} a & b & 0 & \ldots & 0 \\ c & d & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & \ldots & 0 & \ddots & 0 \\ 0 & & \ldots & & 1 \end{pmatrix}$, with $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$. Then $G$ is a subgroup, and it is isomorphic to $\mathrm{SL}_2(\mathbb{R})$. As $\pi_{|G}$ is a unitary representation of $G$ on $V$, we have

$G \subset \mathrm{Ker}(\pi)$ by (c). In particular, $\pi(x) = \mathrm{id}_V$.

Now we use the fact that $\mathrm{SL}_n(\mathbb{R})$ is generated by transvections matrices to conclude that $\pi(x) = \mathrm{id}_V$ for every $x \in \mathrm{SL}_n(\mathbb{R})$.

□

**Exercise I.5.5.3.** (a). Let $G$ be a compact subgroup of $\mathrm{GL}_n(\mathbb{C})$. Show that there exists $x \in \mathrm{GL}_n(\mathbb{C})$ such that $xGx^{-1} \subset \mathrm{U}(n)$.

(b). Put your favorite norm on $M_n(\mathbb{C})$ (they are all equivalent anyway). Show that there exists $c > 0$ such that the only subgroup of $\mathrm{GL}_n(\mathbb{C})$ included in the ball $\{x \in \mathrm{GL}_n(\mathbb{C}) \| \|x - I_n\| < c\}$ is the trivial group.

(c). Show that, for every continuous representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ on a finite-dimensional $\mathbb{C}$-vector space, there exists an integer $m \geq 0$ such that the subgroup $I_n + p^m M_n(\mathbb{Z}_p)$ of $\mathrm{GL}_n(\mathbb{Q}_p)$ acts trivially.

(d). Show that, if $(\pi, V)$ is an irreducible unitary representation of $\mathrm{GL}_n(\mathbb{Z}_p)$, then there exists $m \geq 1$ such that $\pi(I_n + p^m M_n(\mathbb{Z}_p)) = \{1\}$.

(e). More generally, show that, if $G$ is a profinite group (i.e. a projective limit of finite discrete groups, see problem I.5.1.3), then $G$ has a faithful irreducible unitary representation only if $G$ is finite.

*Solution.*

(a). Consider the representation $\rho$ of $G$ on $\mathbb{C}^n$ given by the inclusion $G \subset \mathrm{GL}_n(\mathbb{C})$. We know by theorem I.3.2.8 that there exists a Hermitian inner product on $\mathbb{C}^n$ for which this representation is unitary. Let $A$ be the matrix of this Hermitian inner product in the canonical basis of $\mathbb{C}^n$. Then $A$ is a Hermitian positive matrix, so we can write it $A = B^*B$ with $B \in \mathrm{GL}_n(\mathbb{C})$. (This is an easy consequence of the spectral theorem. As $A$ is Hermitian, we have a unitary matrix $P$ and a diagonal matrix $D$ such that $A = P^*DP$. As $A$ is positive, the diagonal entries of $D$ are positive real numbers, so we can write $D = C^2$ with $C$ another diagonal matrix with positive diagonal entries. Take $B = P^*CP$, then $B$ is Hermitian positive and $A = B^2 = B^*B$.)

The fact that $\rho$ is unitary for $A$ means that $X^*AX = A$ for every $X \in G$. As $A = B^*B$, this is equivalent to $(BXB^{-1})^*(BXB^{-1}) = I_n$. So $BGB^{-1} \subset \mathrm{U}(n)$.

(b). Let $G$ be a subgroup of $\mathrm{GL}_n(\mathbb{C})$ contained in a ball of the form $\{x \in \mathrm{GL}_n(\mathbb{C}) \| \|x - I_n\| < c\}$. Then the closed subgroup $\overline{G}$ is contained in the closed ball $\{x \in \mathrm{GL}_n(\mathbb{C}) \| \|x - I_n\| \leq c\}$, so it is compact, so it is contained in a subgroup of the form $PU(n)P^{-1}$ by question (a). In particular, every element of $G$ is diagonalizable and has all its eigenvalues of modulus 1.

Fix any norm on $\mathbb{C}^n$, and consider the corresponding operator norm $\|.\|$ on $M_n(\mathbb{C})$. We will use this norm. Note that, if $X \in M_n(\mathbb{C})$ and if $\lambda$ is an eigenvalue of $X$, then we have a norm 1 vector $v \in \mathbb{C}^n$ such that $Xv = \lambda v$, hence $\|X\| \geq |\lambda|$. Now let's show that every subgroup of $\mathrm{GL}_n(\mathbb{C})$ included in the open ball $B := \{x \in \mathrm{GL}_n(\mathbb{C}) | \|x - I_n\| < \sqrt{2}\}$ is trivial. Let $G$ be such a subgroup, and let $X \in G$. Let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of $X$. We just saw that $|\lambda_1| = \dots = |\lambda_n| = 1$. Suppose that we have a $r \in \{1, \dots, n\}$ such that $\lambda_r$ is not equal to 1, then we can write $\lambda_r = e^{i\theta}$ with $-\pi/2 < \theta < \pi/2$, because $|\lambda_r - 1| \leq \|X - I_n\| < \sqrt{2}$; but then, if we choose an integer $m \geq 1$ such that $\pi/2 \leq m|\theta| \leq \pi$, we'll have $\|X^m - I_n\| \geq |\lambda_r^m - 1| \geq \sqrt{2}$, which contradicts the fact that $X^m \in G$. So we must have $\lambda_1 = \dots = \lambda_n = 1$, which means that $X = I_n$.

(c). We have seen in the solution of I.5.2.2(d) that $K_m := I_n + p^m M_n(\mathbb{Z}_p)$ is indeed a subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$. We have also put a norm on $M_n(\mathbb{Q}_p)$ such that $K_m$ is the open ball with center $I_n$ and radius $p^{-m+1}$.

Let $\rho : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ be a continuous representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ on a finite-dimensional vector space $V$. By proposition I.3.5.1, the morphism $\rho$ is continuous. Let $U$ be an open neighborhood of $\mathrm{id}_V$ in $\mathrm{GL}(V)$ such that the only subgroup of $\mathrm{GL}(V)$ contained in $U$ is $\{1\}$ (this exists by question (b)). Then $\rho^{-1}(U)$ is an open neighborhood of $I_n$ in $\mathrm{GL}_n(\mathbb{Q}_p)$, so it contains $K_m$ for $m >> 0$. But $K_m$ is a subgroup of $\mathrm{GL}_n(\mathbb{Q}_p)$, so $\rho(K_m)$ is a subgroup of $\mathrm{GL}(V)$, so $\rho(K_m) = \{1\}$ as soon as $\rho(K_m) \subset U$.

(d). By I.5.1.4(m), the group $\mathrm{GL}_n(\mathbb{Z}_p)$ is compact. Hence, by problem I.5.5.9, the space $V$ is finite-dimensional. Now the proof of the statement is exactly as in I.5.5.3(c).

(e). We know that $G$ is compact Hausdorff by problem I.5.1.3 (note that finite discrete groups are comact Hausdorff). So, by problem I.5.5.9, every irreducible unitary representation of $G$ is finite-dimensional.

Suppose that we know that $G$ is totally disconnected. Let $(\pi, V)$ be a continuous finite-dimensional representation of $G$. By I.5.2.2(c), the compact open subgroups of $G$ form a basis of neighborhoods of 1. By I.5.5.3(b), we can find a neighborhood $U$ of $\mathrm{id}_v$ in $\mathrm{GL}(V)$ such that the only subgroup of $\mathrm{GL}(V)$ contained in $U$ is $\{\mathrm{id}_V\}$. So, if we choose a compact open subgroup $K$ of $G$ such that $\pi(K) \subset U$, we must have $K \subset \mathrm{Ker}(\pi)$. Hence $\mathrm{Ker}(\pi) = \bigcup_{x \in \mathrm{Ker}(\pi)} xK$ is an open subgroup of $G$, and so the group $G/\mathrm{Ker}(\pi)$ is discrete. As it is also compact, it is a finite group. This shows that $G$ cannot have a faithful irreducible unitary representation unless it is finite.

So it remains to show that $G$ is totally disconnected, i.e. that the only nonempty connected subsets of $G$ are the singletons. Take a projective system $((G_i)_{i \in I}, (u_{ij} : G_i \to G_j)_{i \geq j})$ of finite groups such that $G = \varprojlim_{i \in I} G_i$. Let $C \subset G$ be a nonempty connected subset. Then the image of $G$ in each $G_i$ is connected nonempty, hence a singleton $\{g_i\}$. This implies that the only element of $C$ is the family $(g_i)_{i \in I} \in \prod_{i \in I} G_i$ (this family is automatically in the projective limit).

□

*Remark.* It is not true that a finite group always has a faithful irreducible unitary representation. For example, if $G$ is a finite abelian group, then every irreducible unitary representation of $G$ is 1-dimensional by Schur's lemma. Take $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and let $\pi : G \to \mathbb{C}$ be a 1-dimensional representation. As $(1.0)$ and $(0,1)$ are of order 2 in $G$, we must have $\pi(1,0), \pi(0,1) \in \{\pm 1\}$. If we want $\pi$ to be faithful, we need to have $\pi(1,0) = \pi(0,1) = -1$, but then $\pi(1,1) = (-1)^2 = 1$, so $\pi$ cannot be faithful. (More generally, a finite abelian group has a faithful 1-dimensional representation if and only if it is cyclic.)

**Exercise I.5.5.4.** The goal of this exercise is to define the Lie algebra of a closed subgroup $G$ of $\mathrm{GL}_n(\mathbb{C})$, and to show that the matrix exponential induces a homeomorphism between the Lie algebra and the group in a neighborhood of their identities.

Consider the function $\exp : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ defined by $\exp(X) = \sum_{n \geq 0} \frac{1}{n!} X^n$; we also write $e^X$ for $\exp(X)$. You may assume the basic properties of this function, i.e. that the series defining it converges absolutely, that it is infinitely derivable, and that we can calculate its derivatives term by term in the sum. You may also assume that $\exp(A+B) = \exp(A)\exp(B)$ for any $A, B \in M_n(\mathbb{C})$ such that $AB = BA$; in particular, $\exp(X) \in \mathrm{GL}_n(\mathbb{C})$ for every $X \in M_n(\mathbb{C})$, and $\exp(X)^{-1} = \exp(-X)$.

We also fix a closed subgroup $G$ of $\mathrm{GL}_n(\mathbb{C})$.

(a). Calculate the differential of $\exp$ at the point $0 \in M_n(\mathbb{C})$. (Remember that this is a linear operator from $M_n(\mathbb{C})$ to itself.)

(b). Show that $\exp$ induces a diffeomorphism from a neighborhood of $0$ in $M_n(\mathbb{C})$ to a neighborhood of $1$ in $\mathrm{GL}_n(\mathbb{C})$.

(c). Let $L = \{X \in M_n(\mathbb{C}) | \forall t \in \mathbb{R},\ \exp(tX) \in G\}$. Show that $L$ is a $\mathbb{R}$-linear subspace of $M_n(\mathbb{C})$. (Hint : For all $X, Y \in M_n(\mathbb{C})$, show that $\exp(X+Y) = \lim_{k \to +\infty} (\exp(\frac{1}{k}X)\exp(\frac{1}{k}Y))^k$.) [18]

(d). If $G = \mathrm{U}(n)$, show that $L = \{X \in M_n(\mathbb{C}) | X^* = -X\}$.

(e). If $G = \mathrm{SO}(n)$, show that $L = \{X \in M_n(\mathbb{C}) | X^T = -X\}$.

(f). Assume again that $G$ is any closed subgroup of $\mathrm{GL}_n(\mathbb{C})$. The goal of this question is to show the following statement : (*) There exists a neighborhood $U$ of $0$ in $L$ such that $\exp(U)$ is a neighborhood of $1$ in $G$ and that $\exp$ induces a homeomorphism $U \xrightarrow{\sim} \exp(U)$.

  (i) Let $L'$ be a $\mathbb{R}$-linear subspace of $M_n(\mathbb{C})$ such that $M_n(\mathbb{C}) = L \oplus L'$, and consider the function $\varphi : M_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ defined by $\varphi(A+B) = e^A e^B$, for every $A \in L$ and every $B \in L'$. Show that there exist neighborhoods $U_0$ of $0$ in $L$, $V$ of $0$ in $L'$ and $W$ of $1$ in $\mathrm{GL}_n(\mathbb{C})$ such that $\varphi$ induces a diffeomorphism $U_0 \times V \xrightarrow{\sim} W$.

  (ii) Suppose that (*) is not true. Show that there exists a decreasing sequence

[18] This $L$ is called the *Lie algebra* of $G$. It is also easy to prove that it stable by the commutator bracket $[X,Y] = XY - YX$.

$U_0 \supset U_1 \supset \dots$ of neighborhoods of $0$ in $L$, a sequence $(A_k)_{k\geq 0}$ of elements of $L$ and a sequence $(B_k)_{k\geq 0}$ of elements of $L'$ such that :

- for every $k \geq 0$, we have $A_k \in U_k$;
- for every $k \geq 0$, we have $B_k \neq 0$;
- for every $k \geq 0$, we have $\varphi(A_k + B_k) \in G$;
- the limit of the sequence $(B_k)_{k\geq 0}$ is $0$;
- for every neighborhood $U$ of $0$ in $L$, we have $U_k \subset U$ for $k$ big enough.

(iii) Show that the sequence $(\frac{1}{\|B_k\|} B_k)_{k\geq 0}$ has a convergent subsequence, and that the limit $B$ of this subsequence is not $0$.

(iv) For every $t \in \mathbb{R}$, show that $\lfloor \frac{t}{\|B_k\|} \rfloor \|B_k\| \to t$ as $k \to +\infty$. (Where, for every $c \in \mathbb{R}$, we write $\lfloor c \rfloor$ for the biggest integer that is $\leq c$.)

(v) Show that $B \in L$.

(g). Let $(\rho, V)$ be a continuous finite-dimensional representation of $G$. For every $X \in L$, show that there exists a unique element $u(X) \in \mathrm{End}(V)$ such that $\rho(e^{tX}) = e^{tu(X)}$ for every $t \in \mathbb{R}$. Show also that the function $u : L \to \mathrm{End}(V)$ is $\mathbb{R}$-linear. [19]

*Solution.*

(a). Let $d\exp_0$ be the differential of $\exp$ at the point $0$. By definition of the differential, for every $H \in M_n(\mathbb{C})$, we have

$$d\exp_0(H) = \lim_{t\to 0} \frac{1}{t}(e^{tH} - e^0) = \lim_{t\to 0} \frac{1}{t}(e^{tH} - I_n) = \frac{d}{dt} e^{tH}\Big|_{t=0}.$$

But we have

$$\frac{d}{dt} e^{tH} = \sum_{n\geq 0} \frac{1}{n!} \frac{d}{dt} (tH)^n = H \exp(tH) = \exp(tH) H,$$

so $d\exp_0(H) = H$. Finally, we get $d\exp_0 = \mathrm{id}_{M_n(\mathbb{C})}$.

(b). As $\mathrm{GL}_n(\mathbb{C})$ is open in $M_n(\mathbb{C})$, neighborhoods of $1$ in $\mathrm{GL}_n(\mathbb{C})$ are the same as small enough neighborhoods of $1$ in $M_n(\mathbb{C})$. So the result follows from the fact that $d\exp_0$ is invertible and from the inversion function theorem.

(c). Let's first prove the hint. Let $U$ be a neighborhood of $0$ in $M_n(\mathbb{C})$ and $V$ be a neighborhood of $1$ in $\mathrm{GL}_n(\mathbb{C})$ such that $\exp$ is a diffeomorphism from $U$ to $V$. We write $\log : V \to U$ for its inverse. As $\exp(H) = 1 + H + o(H)$ as $H \to 0$, we have $\log(1 + H) = H + o(H)$ as $H \to 0$.

[19] The function $u : L \to \mathrm{End}(V)$ is called the *differential* of $\rho$ at $0$. With a little more effort, you can show that it preserves commutator brackets.

Let $X, Y \in M_n(\mathbb{C})$. Then $\exp(\frac{1}{k}X) = 1 + \frac{1}{k}X + O(\frac{1}{k^2})$ and $\exp(\frac{1}{k}X) = 1 + \frac{1}{k}X + O(\frac{1}{k^2})$, so $\exp(\frac{1}{k}X)\exp(\frac{1}{k}Y) = 1 + \frac{1}{k}(X+Y) + O(\frac{1}{k^2})$. If $k$ is big enough, we have $\exp(\frac{1}{k}X)\exp(\frac{1}{k}Y) \in V$, and $\log(\exp(\frac{1}{k}X)\exp(\frac{1}{k}Y)) = \frac{1}{k}(X+Y) + o(\frac{1}{k})$. So finally

$$(\exp(\tfrac{1}{k}X)\exp(\tfrac{1}{k}Y))^k = \exp(k\log(\exp(\tfrac{1}{k}X)\exp(\tfrac{1}{k}Y))) = \exp(X+Y+o(1)) \to \exp(X+Y)$$

as $k \to +\infty$.

The set $L$ is stable by scalar multiplication by definition. Let $X, Y \in L$. Then $c(t) := e^{tX}e^{tY} \in G$ for every $t \in \mathbb{R}$. As $G$ is closed in $\mathrm{GL}_n(\mathbb{C})$, this implies that, for every $t \in \mathbb{R}$,

$$\exp(t(X+Y)) = \lim_{k \to +\infty} (\exp(\tfrac{t}{k}X)\exp(\tfrac{t}{k}Y))^k \in G.$$

So $X + Y \in L$.

(d). Let $X \in M_n(\mathbb{C})$ such that $X = -X^*$. Then, for every $t \in \mathbb{R}$, we have $tX = -(tX)^*$ (in particular, $tX$ and $tX^*$ commute), hence

$$e^{tX}(e^{tX})^* = e^{tX}e^{tX^*} = e^{tX+tX^*} = e^0 = I_n,$$

i.e., $e^{tX} \in \mathrm{U}(n)$. So $X \in L$.

Conversely, let $X \in L$. Then, for every $t \in \mathbb{R}$, we have $e^{tX}e^{tX^*} = I_n$. Deriving this expression (and using the expression for the derivative from the proof of (a)) gives

$$0 = Xe^{tX}e^{tX^*} + e^{tX}e^{tX^*}X^* = X + X^*.$$

(e). This is exactly the same proof as in (d), replacing "$*$" by "$T$".

(f). (i) By the inverse function theorem, it suffices to prove that the differential of $\varphi$ at $0 \in M_n(\mathbb{C})$ is invertible. If $A \in L$ and $B \in L'$, we have, by definition of the differential

$$d\varphi_0(A+B) = \lim_{t \to 0} \frac{1}{t}(\varphi(tA+tB) - \varphi(0)) = \lim_{t \to 0} \frac{1}{t}(e^{tA}e^{tB} - 1) = A + B$$

(by the calculation in (a)), so $d\varphi_0 = \mathrm{id}_{M_n(\mathbb{C})}$, and this is certainly invertible.

(ii) Choose a sequence of neighborhoods $U_0 \supset U_1 \supset \ldots$ (resp. $V = V_0 \supset V_1 \supset \ldots$) of $0$ in $L$ (resp. $L'$) such that every neighborhood $U$ (resp. $V'$) of $0$ in $L$ contains $U_k$ (resp. $V_k$) for $k$ big enough. (For example, we could take balls with radii tending to $0$ in $L$ and in $L'$.) For every $k \geq 0$, the function $\varphi$ is a diffeomorphism from $U_k \times V_k$ to $\varphi(U_k \times V_k)$, and in particular $\varphi(U_k \times V_k) \cap G$ is a neighborhood of $1$ in $G$, containing $\exp(U_k)$. If (*) is not true, them $\varphi(U_k \times V) \cap G$ strictly contains $\exp(U_k)$ for every $k$, so we can find $A_k \in U_k$ and $B_k \in V_k$ such that $\varphi(A_k + B_k) \in G$ and $\varphi(A_k + B_k) \notin \exp(U_k)$, i.e. $B_k \neq 0$. Also, we have $B_k \to 0$ as $k \to +\infty$ because of the condition on the neighborhoods $V_k$.

(iii) The sequence $(\frac{1}{\|B_k\|}B_k)_{k\geq 0}$ is a sequence of elements of the unit ball of $L'$, and this unit ball is compact, so it has a convergent subsequence, whose limit is still in the unit ball (and in particular nonzero).

(iv) For every $k \geq 0$, we have

$$0 \leq \frac{t}{\|B_k\|} - \lfloor \frac{t}{\|B_k\|} \rfloor < 1,$$

hence

$$0 \leq t - \lfloor \frac{t}{\|B_k\|} \rfloor \|B_k\| < \|B_k\|.$$

As $B_k \to 0$, we have $\|B_k\| \to 0$, which implies that

$$\lfloor \frac{t}{\|B_k\|} \rfloor \|B_k\| \to t.$$

(v) After passing to a subsequence, we may assume that $B = \lim_{k\to+\infty} \frac{1}{\|B_k\|}B_k$. We must show that $e^{tB} \in G$ for every $t \in \mathbb{R}$. Let $t \in \mathbb{R}$. By question (iv) and the definition of $B$, we have

$$e^{tB} = \lim_{k\to+\infty} \exp\left(\lfloor \tfrac{t}{\|B_k\|} \rfloor \|B_k\| \tfrac{1}{\|B_k\|} B_k\right) = \exp\left(\lfloor \tfrac{t}{\|B_k\|} \rfloor B_k\right).$$

But, for every $k \geq 0$, we have $\varphi(A_k + B_k) = e^{A_k}e^{B_k} \in G$ and $e^{A_k} \in G$ because $A_k \in L$, so $e^{B_k} \in G$; as $N := \lfloor \frac{t}{\|B_k\|} \rfloor$ is an integer, this implies that $e^{NB} = (e^B)^N \in G$. Finally, as $G$ is closed in $\mathrm{GL}_n(\mathbb{C})$, we deduce that $e^{tB} \in G$.

(g). Let $X \in L$. Consider the map $\mathbb{R} \to \mathrm{GL}(V)$, $t \longmapsto \rho(e^{tX})$. This a continuous morphism of groups, hence, by I.5.4.1(b)(i), there exists a unique $u(X) \in \mathrm{End}(V)$ such that $\rho(e^{tX}) = \exp(tu(X))$ for every $t \in \mathbb{R}$.

Let $X, Y \in L$ and $a \in \mathbb{R}$. For every $t \in \mathbb{R}$, we have

$$e^{tu(aX)} = \rho(e^{taX}) = e^{tau(X)}.$$

Taking derivatives at $t = 0$, we get $u(aX) = au(X)$. Now consider $c : \mathbb{R} \to \mathrm{GL}(V)$, $t \longmapsto \rho(e^{tX})\rho(e^{tY})\rho(e^{-t(X+Y)})$. We have $c(t) = e^{tu(X)}e^{tu(Y)}e^{-tu(X+Y)}$, so $c$ is $C^\infty$ and $c'(0) = u(X) + u(Y) - u(X+Y)$. On the other hand, using the fact that $c$ is $C^\infty$, we can prove as in (c) that, for every $t \in \mathbb{R}$, we have

$$\lim_{k\to+\infty} c(\tfrac{t}{k})^k = e^{tc'(0)}.$$

So we just need to prove that this limit is equal to $\mathrm{id}_V$ for every $t \in \mathbb{R}$. An easy calculation with infinitesimals shows that (if $t$ is fixed)

$$e^{\frac{t}{k}X}e^{\frac{t}{k}Y}e^{-\frac{t}{k}(X+Y)} = I_n + O(\tfrac{1}{k^2}),$$

so
$$(e^{\frac{t}{k}X}e^{\frac{t}{k}Y}e^{-\frac{t}{k}(X+Y)})^k = I_n + O(\tfrac{1}{k}),$$
and
$$c(\tfrac{t}{k}) = \rho((e^{\frac{t}{k}X}e^{\frac{t}{k}Y}e^{-\frac{t}{k}(X+Y)})^k) \xrightarrow[k\to+\infty]{} \rho(I_n) = \mathrm{id}_V.$$

□

We will now see how to find discrete groups that have no faithful finite-dimensional representations at all, over any field.

Let $\Gamma$ be a (discrete) group. We say that $\Gamma$ is *residually finite* if, for every $x \in \Gamma - \{1\}$, there exists a normal subgroup $\Delta$ of $\Gamma$ such that $\Gamma/\Delta$ is finite (we say that $\Delta$ is of *finite index* in $\Gamma$) and that the image of $x$ in $\Gamma/\Delta$ is not trivial.

The goal of the following two exercises is to prove that, if $k$ is a field and $\Gamma \subset \mathrm{GL}_n(k)$ is a finitely generated subgroup, then $\Gamma$ is residually finite. [20] [21]

**Exercise I.5.5.5.** Let $R$ be a finitely generated $\mathbb{Z}$-algebra that is also a domain. We fix an integer $n \geq 1$. For every ideal $I$ of $R$, we set
$$\Gamma(I) = \mathrm{Ker}(\mathrm{GL}_n(R) \to \mathrm{GL}_n(R/I)).$$

(a). Show that $R$ is a field if and only if $R$ is finite.

(b). If $\mathfrak{m}$ is a maximal ideal of $R$, show that $\Gamma(\mathfrak{m})$ is a normal subgroup of finite index in $\mathrm{GL}_n(R)$.

(c). Show that the intersection of all the maximal ideals of $R$ is $0$. (Hint : We may assume that $R$ is not a field. If $a \in R - \{0\}$, show that the localization $R[1/a]$ is not a field, take a maximal ideal in $R[1/a]$, and intersect it with $R$.)

(d). Show that $\mathrm{GL}_n(R)$ is residually finite.

*Solution.*

(a). It's a classical fact that a finite integral domain has to be a field. Here is the proof. Suppose that $R$ is finite, and let $a \in R - \{0\}$. Then multiplication by $a$ is an additive map from $R$ to itself, and its kernel is $\{0\}$ (because $R$ is an integral domain), so it is injective; as $R$ is finite, it is also surjective, which means that there exists $b \in R$ such that $ab = 1$, i.e. that $a \in R^\times$.

[20] In fact, we can use similar ideas to show that, if $\mathrm{char}(k) = 0$, such a $\Gamma$ has to be virtually residually $p$-finite (i.e. it has a finite index subgroup $\Gamma'$ such that, for every $x \in \Gamma' - \{1\}$, there exists a finite index normal subgroup $\Delta \not\ni x$ of $\Gamma'$ such that $\Gamma'/\Delta$ is a $p$-group) for almost every prime number $p$, but the only proof I know uses the Noether normalization theorem.

[21] Add a reference !

The converse follows from two classical results of commutative algebra (see for example exercises 4.30 and 4.32 of Eisenbud's [9]) :

- If $K \subset L$ is a field extension such that $L$ is finitely generated as a $K$-algebra, then $L$ is a finite-dimensional $K$-vector space (Zariski's lemma).
- If $R$ is a Noetherian ring, $S$ is a finitely generated $R$-algebra and $T \subset S$ is a $R$-subalgebra such that $S$ is a finite $T$-algebra (i.e. finitely generated as a $T$-module), then $T$ is a finitely generated $R$-algebra (Artin-Tate).

Indeed, if $R$ is a field, consider its prime field $k$. Then $R$ is a finitely generated $k$-algebra, hence a finite dimension $k$-vector space by Zariski's lemma, which implies that $k$ is a finitely generated $\mathbb{Z}$-algebra by the second result. Note that $k$ is either $\mathbb{Q}$ or one of the finite fields $\mathbb{F}_p$. But $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra (if $x_1, \dots, x_n \in \mathbb{Q} - \{0\}$, and if $\mathscr{P}$ is the (finite) set of prime numbers that divide the denominator of one of the $x_i$, then the prime numbers dividing the denominator of a nonzero element of the $\mathbb{Z}$-subalgebra generated by $x_1, \dots, x_n$ has to also be in $\mathscr{P}$, so this $\mathbb{Z}$-subalgebra cannot be equal to $\mathbb{Q}$). So $k$ is a finite field; as $R$ is a finite-dimensional $k$-vector space, it is also a finite field.

For completeness, let's give a proof of the part of the commutative algebra results that we actually need. Suppose that we know the following :
(*) Let $L/K$ be a field extension such that :

- there exists $u \in L$ such that $L = K(u)$ (i.e. $L$ is generated by $u$ as a field);
- $L$ is a finitely generated $\mathbb{Z}$-algebra,

the extension is finite and $K$ is also a finitely generated $\mathbb{Z}$-algebra.

Then we can prove in the same way that, if $R$ is a field, it has to be finite. (Just choose elements $x_1, \dots, x_n \in R$ generating $R$ over its prime field $k$ and apply (*) to the extensions $k(x_1, \dots, x_{i-1}) \subset k(x_1, \dots, x_i)$ to show that $k$ is a finitely generated $\mathbb{Z}$-algebra. The end of the proof is as before.)

We now prove (*). Let $x_1, \dots, x_n \in L^\times$ generating $L$ as a $\mathbb{Z}$-algebra. Assume that $u$ is transcendental over $K$; then $L$ is isomorphic to the field of rational fractions of $K$. Write $x_i = \frac{P_i}{Q_i}$, with $P_i, Q_i \in K[u]$. As $(1 + u \prod_{i=1}^n Q_i)^{-1} = L = \mathbb{Z}[a_1, \dots, a_n]$, we can write

$$(1 + u \prod_{i=1}^{n} Q_i)^{-1} = \frac{R}{Q_1^{d_1} \dots Q_n^{d_n}},$$

with $R \in K[u]$ coprime to all the $Q_i$ and $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$. We get $Q_1^{d_1} \dots Q_n^{d_n} = R(1 + u \prod_{i=1}^n Q_i)$, which contradicts the fact that $R$ is coprime to all the $Q_i$. So $u$ is algebraic over $K$. Let $X^d + a_1 X^{d-1} + \dots + a_d \in K[X]$ be the minimal polynomial of $u$ over $K$. For every $i \in \{1, \dots, n\}$, write $x_i = \sum_{j=0}^{d-1} b_{ij} u^j$, with $b_{ij} \in K$. Let $A$ be the $\mathbb{Z}$-algebra of $K$ generated by $a_1, \dots, a_d$ and by the $b_{ij}$, and let's show that $A = K$. Let $y \in K$. Then $y$ can be written as a polynomial in $x_1, \dots, x_d$ with coefficients in $\mathbb{Z}$, so it is also a polynomial in $u$ with coefficients in $A$, which can be taken of degree $\leq d-1$ (we can use the relation $u^d = -a_1u^{d-1} - \ldots - a_d$ to replace any terms of degree $\geq d$ with terms of lower degree). In other words, we can write $y = \sum_{i=0}^{d-1} c_i u^i$, with $c_0, \ldots, c_{d-1} \in A$. As the family $(1, u, \ldots, u^{d-1})$ is linearly independent over $K$, we must have $c_1 = \ldots = c_{d-1} = 0$ and $y = c_0 \in A$.

(b). First, the group $\Gamma(I)$ is a normal subgroup of $\mathrm{GL}_n(R)$ for any ideal, because it is the kernel of a morphism of groups. Suppose that $\mathfrak{m}$ is a maximal ideal. Then $R/\mathfrak{m}$ is a finite field by (a). As $\mathrm{GL}_n(R)/\Gamma(\mathfrak{m})$ injects into $\mathrm{GL}_n(R/\mathfrak{m})$, this implies that $\Gamma(\mathfrak{m})$ has finite index in $\mathrm{GL}_n(R)$.

(c). If $R$ is a field, then $(0)$ is a maximal ideal of $R$ and we are done. Suppose that $R$ is not a field; in particular, by (a), it is not finite. Let $a \in R - \{0\}$. The localization $R[1/a] := R[X]/(aX-1)$ is a finitely generated $\mathbb{Z}$-algebra because $R$ is, so it can only be a field if it is finite, by (a). But the obvious map $R \to R[1/a]$ is injective because $a$ is not a divisor of $0$ (remember that $R$ is an integral domain), and $R$ is infinite, so $R[1/a]$ is also infinite, hence it is not a field. Let $\mathfrak{m}'$ be a maximal ideal of $R[1/a]$, and let $\mathfrak{m}$ be its inverse image in $R$. Then the map $R/\mathfrak{m} \to R[1/a]/\mathfrak{m}'$ is injective (because $R \to R[1/a]$ is), and $R[1/a]/\mathfrak{m}'$ is finite because it is a field (by (a)), so $R/\mathfrak{m}$ is finite and an integral domain, so it is a field (by (a) again !), and $\mathfrak{m}$ is a maximal ideal of $R$. Note also that, as $a$ is invertible in $R[1/a]$, it cannot be in $\mathfrak{m}'$, and so it cannot be in $\mathfrak{m}$. So we have found a maximal ideal of $R$ that doesn't contain $a$.

(d). Let $x = (x_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(R)$ such that $x \neq I_n$. Choose $i, j \in \{1, \ldots, n\}$ such that $x_{ij} \neq 0$ and $i \neq j$, or such that $x_{ij} \neq 1$ and $i = j$. By (c), we can find a maximal ideal $\mathfrak{m}$ of $R$ such that $x_{ij} \notin \mathfrak{m}$ if $i \neq j$, and such that $x_{ij} - 1 \notin \mathfrak{m}$ if $i = j$. In other words, the image of $x$ in $\mathrm{GL}_n(R)/\Gamma(\mathfrak{m})$ is not the unit element. As $\Gamma(\mathfrak{m})$ is a normal subgroup of $\mathrm{GL}_n(R)$ of finite index by (b), we are done.

□

**Exercise I.5.5.6.** Let $k$ be a field, and let $\Gamma$ be a finitely generated subgroup of $\mathrm{GL}_n(k)$.

(a). Show that there exists a finitely generated $\mathbb{Z}$-subalgebra $R$ of $k$ such that $\Gamma \subset \mathrm{GL}_n(R)$.

(b). Show that $\Gamma$ is residually finite.

*Solution.*

(a). Let $\gamma_1, \ldots, \gamma_n$ be generators of $\Gamma$, and let $R$ be the $\mathbb{Z}$-subalgebra of $k$ generated by the entries of the $\gamma_i$ and of their inverses; this is a finitely generated $\mathbb{Z}$-algebra by definition. As each element of $\Gamma$ is a product of the elements $\gamma_i^{\pm 1}$, we have $\Gamma \subset \mathrm{GL}_n(R)$.

(b). This follows immediately from I.5.5.5(d) : If $\gamma \in \Gamma - \{1\}$, choose a normal subgroup of finite index $\Delta$ of $\mathrm{GL}_n(R)$ such that the image of $\gamma$ in $\mathrm{GL}_n(R)/\Delta$ is not trivial. Then $\Gamma \cap \Delta$

is a normal subgroup of $\Gamma$, and $\Gamma/(\Gamma\cap\Delta)$ injects into $\mathrm{GL}_n(R)/\Delta$, so $\Gamma\cap\Delta$ is of finite index in $\Gamma$ and the image of $\gamma$ in $\Gamma/(\Gamma\cap\Delta)$ is not trivial.

□

Of course, the result of the previous exercise would not be very interesting if we could not give any example of a finitely generated non residually finite group. We do that in the next two exercises.

**Exercise I.5.5.7.** Let $\Gamma$ be the quotient of the free group on the generators $a$ and $b$ by the relation $a^{-1}b^2a = b^3$. In this problem, we will assume that $b_1 := a^{-1}ba$ and $b$ do not commute in $\Gamma$, and deduce that $\Gamma$ is not residually finite.

Let $u:\Gamma\to\Gamma'$ be a morphism of groups, with $\Gamma'$ finite.

(a). Let $n$ be the order of $u(a)$ in $\Gamma'$. Show that the order of $u(b)$ divides $3^n-2^n$.

(b). Show that there exists an integer $N\geq 0$ such that $u(b_1)=u(b_1^2)^N$. (Note that the order of $u(b)$ is prime to both 2 and 3.)

(c). Show that $u(b_1)$ and $u(b)$ commute.

(d). Show that $\Gamma$ is not residually finite.

*Solution.*

(a). We first prove that, for every $r\in\mathbb{Z}_{\geq 0}$, we have $b^{2^r}=a^rb^{3^r}a^{-r}$. The case $r=0$ is obvious, and the case $r=1$ is the relation defining $\Gamma$. Let $r\geq 1$, suppose the result know for $r$, and let's prove it for $r+1$. We have

$$b^{2^{r+1}}=(b^2)^{2^r}=(ab^3a^{-1})^{2^r}=(ab^{2^r}a^{-1})^3=(a^{r+1}b^{3^r}a^{-(r+1)})^3=a^{r+1}b^{3^{r+1}}a^{-(r+1)}.$$

Applying to $r=n$ gives $b^{2^n}=a^nb^{3^n}a^{-n}$, hence $u(b)^{3^n-2^n}=1$, so the order of $u(b)$ divides $3^n-2^n$.

(b). Note that the order of $u(b)$ is odd, because it divides the odd number $3^n-2^n$. So there exists $N\geq 1$ such that $u(b)^{2N}=u(b)$. As $b_1=a^{-1}ba$, we have $b_1^r=a^{-1}b^ra$ for every $r\geq 0$, so $u(b_1)^{2N}=u(b_1)$, as desired.

(c). We have $b_1^2=b^3$ by the relation defining, so $u(b_1)=u(b)^{3N}$ by (b). This implies that $u(b)$ and $u(b_1)$ commute.

(d). Let $c=b_1^{-1}b^{-1}b_1b\in\Gamma$. Then we have assumed that $c\neq 1$, but question (c) shows that, for every normal subgroup of finite index $\Delta$ of $\Gamma$, the image of $c$ in $\Gamma/\Delta$ is trivial. So $\Gamma$ is not residually finite.

□

**Exercise I.5.5.8.** Let $\Gamma$ be the quotient of the free group on the generators $a$ and $b$ by the relation $a^{-1}b^2a = b^3$. The goal of this problem is to show that $b_1 := a^{-1}ba$ and $b$ do not commute in $\Gamma$, i.e. that $b_1bb_1^{-1}b^{-1}$ is not trivial in $\Gamma$. [22]

Let $F$ be the free group on the generators $a$ and $b$. Remember that elements of $F$ are reduced words in the letters $a, a^{-1}, b, b^{-1}$. (A reduced words is a word that contains no redundant pair $aa^{-1}$, $a^{-1}a$, $bb^{-1}$ or $b^{-1}b$.) We write an element of $F$ as $a^{n_1}b^{m_1}\dots a^{n_r}b^{m_r}$, with $n_1, m_1, \dots, n_r, m_r \in \mathbb{Z}$ and $m_1, n_2, m_2, \dots, n_{r-1}, m_{r-1}, n_r \neq 0$.

Let $\Omega$ be the set of reduced words of the form $b^{r_1}a^{s_1}\dots b^{r_m}a^{s_m}b^r$, with :

(i) $m \in \mathbb{Z}_{\geq 0}$ and $r_i, s_i, r \in \mathbb{Z}$;

(ii) $s_i \neq 0$ for every $i \in \{1, \dots, m\}$;

(iii) $r_i \neq 0$ for every $i \in \{2, \dots, m\}$;

(iv) for every $i \in \{1, \dots, m\}$, if $s_i > 0$, then $0 \leq r_i \leq 1$;

(v) for every $i \in \{1, \dots, m\}$, if $s_i < 0$, then $0 \leq r_i \leq 2$.

By definition of $\Gamma$, we have a surjective group morphism $F \to \Gamma$, that we will denote by $\varphi$.

(a). Show that $\varphi(\Omega) = \Gamma$.

(b). For every $w \in \Omega$ and every $s \in \{a, a^{-1}, b, b^{-1}\}$, find a word $w' \in \Omega$ such that $\varphi(w') = \varphi(ws)$. We will denote this $w'$ by $w \cdot s$ in what follows.

(c). For every $w \in \Omega$ and every $s \in \{a, a^{-1}, b, b^{-1}\}$, show that $(w \cdot s) \cdot s^{-1} = w$.

(d). Show that $(w, s) \longmapsto w \cdot s$ extends to a right action of $\Gamma$ on $\Omega$.

(e). Show that $\varphi$ induces a bijection $\Omega \xrightarrow{\sim} \Gamma$.

(f). Show that $b_1bb_1^{-1}b^{-1} \neq 1$ in $\Gamma$.

*Solution.*

(a). By definition of the free group, we can write every element $w$ of $F$ as a reduced word $b^{r_1}a^{s_1}\dots b^{r_m}a^{s_m}b^r$ satisfying conditions (i), (ii) and (iii). We define $N(w)$ to be the max of all $s_i > 0$ such that $r_i \notin \{0, 1\}$; so if $w$ satisfies condition (iv), we have $N(w) = 0$. We define $M(w)$ to be the max of all $|s_i|$, for $s_i < 0$ such that $r_i \notin \{0, 1, 2\}$; so if $w$ satisfies condition (v), we have $M(w) = 0$. We prove by induction on $N(w) + M(w)$ that there exists $w_0 \in \Omega$ such that $\varphi(w) = \varphi(w_0)$. If $N(w) + M(w) = 0$, then $w$ satisfies conditions (iv) and (v), so it is in $\Omega$ and the conclusion is obvious.

Suppose that $N(w) + M(w) > 0$. If $N(w) > 0$, choose $i \in \{1, \dots, m\}$ such that $s_i > 0$ and $r_i \notin \{0, 1\}$. Note that the relation defining $\Gamma$ says that $\varphi(b^2a) = \varphi(ab^3)$, hence also

[22] The easiest way to show this would to find a finite-dimensional representation of $\Gamma$ on which $b_1bb_1^{-1}b$ acts non-trivially, but we can't. Still, some variant of this idea will work.

that $\varphi(b^{-2}a) = \varphi(ab^{-3})$, which implies that $\varphi(b^{2k}a) = \varphi(ab^{3k})$ for every $k \in \mathbb{Z}$. Write $r_i = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$, and let

$$w' = b^{r_1}a^{s_1} \dots b^{r_{i-1}}a^{s_{i-1}}b^l ab^{3k}a^{s_i-1}b^{r_{i+1}}a^{s_{i+1}} \dots b^{r_m}a^{s_m}b^r.$$

Then $\varphi(w) = \varphi(w')$ by the observation above, and $N(w') < N(w)$, $M(w') = M(w)$. Similarly, if $M(w) > 0$, choose $i \in \{1, \dots, m\}$ such that $s_i < 0$ and $r_i \notin \{0, 1, 2\}$. For $k \in \mathbb{Z}$, the equality $\varphi(b^{2k}a) = \varphi(ab^{3k})$ can also be written $\varphi(a^{-1}b^{2k}) = \varphi(b^{3k}a^{-1})$. Write $r_i = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$, and let

$$w' = b^{r_1}a^{s_1} \dots b^{r_{i-1}}a^{s_{i-1}}b^l a^{-1}b^{2k}a^{s_i+1}b^{r_{i+1}}a^{s_{i+1}} \dots b^{r_m}a^{s_m}b^r.$$

Then $\varphi(w) = \varphi(w')$ by the observation above, and $N(w') = N(w)$, $M(w') < M(w)$. As one of $N(w)$ or $M(w)$ has to be $> 0$, we can always find $w' \in F$ such that $\varphi(w') = \varphi(w)$ and $N(w') + M(w') < N(w) + M(w)$. Applying the induction hypothesis to $w'$ gives the result.

(b). Let $w = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^r \in \Omega$; we assume that conditions (i)-(v) are satisfied. If $s = b$ (resp. $s = b^{-1}$), then $w' = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^{r+1}$ (resp. $w' = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^{r-1}$) works. If $s = a$, write $r = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$ and take $w' = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l ab^{3k}$. If $s = a^{-1}$, write $r = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$ and take $w' = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}b^{2k}$.

(c). The conclusion is obvious if $s \in \{b, b^{-1}\}$. Suppose that $s = a$ and write $r = 2k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1\}$. Then $w \cdot a = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l ab^{3k}$, so

$$(w \cdot a) \cdot a^{-1} = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l aa^{-1}b^{2k} = w.$$

If $s = a^{-1}$, write $r = 3k + l$ with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$. Then $w \cdot a = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}b^{2k}$, so

$$(w \cdot a^{-1}) \cdot a = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}ab^{3k} = w.$$

(d). By (c), $(w, s) \longmapsto w \cdot s$ extends to a right action of $F$ on $\Omega$. To prove that this factors through a right action of $\Gamma$ on $\Omega$, it suffices to show that $b^{-3}a^{-1}b^2a$ acts trivially. Let $w = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^r \in \Omega$; we assume that conditions (i)-(v) are satisfied. Write $r = 3k + l$, with $k \in \mathbb{Z}$ and $l \in \{0, 1, 2\}$. Then

$$w \cdot b^{-3} = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^{r-3} = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^{l+3(k-1)},$$

so

$$w \cdot (b^{-3}a^{-1}) = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}b^{2(k-1)},$$

hence

$$w \cdot (b^{-3}a^{-1}b^2) = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}b^{2k},$$

and finally

$$w \cdot (b^{-3}a^{-1}b^2a) = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^l a^{-1}ab^{3k} = b^{r_1}a^{s_1} \dots b^{r_m}a^{s_m}b^{l+3k} = w.$$

(e). We already know that $\varphi(\Omega) = \Gamma$ by (a), so we just need to show that $\varphi_{|\Omega}$ is injective. By the explicit formulas for the action given in the proof of (b), if $w \in \Omega$, then we have $1 \cdot w = w$. As $1 \cdot w$ only depends on $\varphi(w)$ by (d), this shows that $\varphi(w)$ determines $w$.

(f). By (e), we just need to show that the unique preimage of $\varphi(b_1 b b_1^{-1} b^{-1})$ in $\Omega$ is not trivial. We have seen in the proof of (a) an algorithm to transform a reduced word into an element of $\Omega$ having the same image by $\varphi$. Applying it to $b_1 b b_1^{-1} b^{-1} = a^{-1}baba^{-1}b^{-1}ab^{-1}$, we get $a^{-1}baba^{-1}bab^{-4} \neq 1$ (modulo easy-to-make mistakes), so we are done.

□

**Exercise I.5.5.9.** The goal of this problem it to prove I.3.2.13, i.e. the fact that every irreducible unitary representation of a compact group is finite-dimensional.

Let $G$ be a compact group, let $dx$ be the normalized Haar measure on $G$, and let $(\pi, V)$ be a nonzero unitary representation of $G$. Fix $u \in V - \{0\}$, and define $T : V \to V$ by

$$T(v) = \int_G \langle v, \pi(x)(u)\rangle \pi(x)(u) dx.$$

(a). Show that $T$ is well-defined and that $T \in \mathrm{End}(V)$.

(b). Show that $T$ is $G$-equivariant.

(c). Show that $\langle T(v), v\rangle \geq 0$ for every $v \in V$.

(d). Show that $T \neq 0$.

(e). Show that $T$ is in the closure (for $\|.\|_{op}$) of $\{T' \in \mathrm{End}(V) | \dim_{\mathbb{C}}(\mathrm{Im}(T')) < +\infty\}$; in other words, $T$ is in the closure of the space of endomorphisms of finite rank. (Hint : $G \to V$, $x \longmapsto \pi(x)(u)$ is uniformly continuous.)

(f). Let $B$ be the closed unit ball in $V$. Show that $\overline{T(B)}$ is compact. (In other words, the operator $T$ is a compact operator. Problem I.5.6.5 can help shorten the proof.)

(g). If $V$ is an irreducible representation of $V$, show that $V$ is finite-dimensional.

*Solution.*

(a). We must show that the integral defining $T(v)$ converges for every $v \in V$. Let $v \in V$. Then the function $G \to V$, $\langle v, \pi(x)(u)\rangle \pi(x)(u)$ is continuous (because $x \longmapsto \pi(x)(u)$ is continuous); as $G$ is compact, the integral exists by problem I.5.6.3, and moreover we have

$$\|T(v)\| \leq \int_G |\langle v, \pi(x)(u)\rangle| \|\pi(x)(u)\| dx \leq \|v\| \|u\|^2.$$

The function $T : V \to V$ is $\mathbb{C}$-linear (because addition and multiplication by a scalar are continuous on $V$, so they commute with the integral by I.5.6.1(b)), and the inequality above shows that $T$ is bounded and that $\|T\|_{op} \leq \|u\|^2$.

(b). Let $v \in V$ and $x \in G$.

$$\begin{aligned} T(\pi(x)(v)) &= \int_G \langle \pi(x)(v), \pi(y)(u)\rangle \pi(y)(u)dy \\ &= \int_G \langle v, \pi(x)^*\pi(y)(u)\rangle \pi(y)(u)dy \\ &= \int_G \langle v, \pi(x^{-1}y)(u)\rangle \pi(y)(u)dy \\ &= \int_G \langle v, \pi(y)(u)\rangle \pi(x)\pi(y)(u)dy \end{aligned}$$

(by left invariance of the Haar measure for the last equality). As $\pi(x) : V \to V$ is continuous and linear, I.5.6.1(b) implies that the last line is equal to

$$\pi(x)\left(\int_G \langle v, \pi(y)(u)\rangle \pi(y)(u)dy\right) = \pi(x)(T(v)),$$

which is what we wanted.

(c). Let $v \in V$. As $\overline{\langle v, .\rangle}$ is continuous and linear on $V$, we have

$$\begin{aligned} \langle T(v), v\rangle &= \int_G \langle \pi(x)(u), v\rangle \langle v, \pi(x)(u)\rangle dx \\ &= \int_G |\langle v, \pi(x)(u)\rangle|^2 dx \\ &\geq 0. \end{aligned}$$

(d). Take $v = u$. As $\langle u, \pi(x)(u)\rangle = \|u\|^2 > 0$ and $x \longmapsto \langle u, \pi(x)(u)\rangle$ is a continuous function from $G$ to $\mathbb{C}$, there exists $\varepsilon > 0$ and an open neighborhood $U$ of 1 in $G$ such that $|\langle u, \pi(x)(u)\rangle|^2 \geq \varepsilon$ for $x \in U$. Then, by the calculation in the proof of (c), we have

$$\langle T(u), u\rangle = \int_G |\langle u, \pi(x)(u)\rangle|^2 dx \geq \varepsilon\mu(U) > 0.$$

So $T \neq 0$.

(e). Let $\varepsilon > 0$. As $G$ is compact, the continuous function $G \to \mathbb{C}$, $x \longmapsto \pi(x)(u)$ is uniformly continuous, so there exists a neighborhood $U$ of 1 such that, for $x \in G$ and $y \in xU$, we have $\|\pi(x)(u) - \pi(y)(u)\| \leq \varepsilon$. As $G$ is compact and the family $(xU)_{x\in G}$ covers $G$, we can $x_1, \dots, x_n \in G$ such that $G = \bigcup_{i=1}^n x_iU$. Choose Borel subsets $E_1, \dots, E_n$ of $X$ such that $x_i \in E_i \subset x_iU$ for every $i \in \{1, \dots, n\}$ and $X = E_1 \sqcup \dots \sqcup E_n$ (as sets). If $x \in E_i$ and $v \in V$, then we have

$$\begin{aligned} &\|\langle v, \pi(x)(u)\rangle \pi(x)(u) - \langle v, \pi(x_i)(u)\rangle \pi(x_i)(u)\| \\ &\qquad \leq \|\langle v, (\pi(x) - \pi(x_i))(u)\rangle \pi(x)(u)\| + \|\langle v, \pi(x_i)(u)\rangle (\pi(x) - \pi(x_i)))(u)\| \\ &\qquad \leq \|v\|\varepsilon\|u\| + \|v\|\|u\|\varepsilon = 2\varepsilon\|v\|\|u\|. \end{aligned}$$

Define $U \in \mathrm{End}(V)$ by

$$T(v) = \sum_{i=1}^{n} \mu(E_i)\langle v, \pi(x_i)(u)\rangle \pi(x_i)(u) = \sum_{i=1}^{n} \int_{E_i} \langle v, \pi(x_i)(u)\rangle \pi(x_i)(u) dx.$$

This operator $U$ has finite rank, because its image is contained $\mathrm{Span}(\pi(x_1)(u), \dots, \pi(x_n)(u))$. Also, by the calculation above (and exercise I.5.6.2), for every $v \in V$, we have

$$\begin{aligned}\|T(v) - U(v)\| &\le \sum_{i=1}^{n} \left| \int_{E_i} \langle v, \pi(x)(u)\rangle \pi(x)(u) dx - \int_{E_i} \langle v, \pi(x_i)(u)\rangle \pi(x_i)(u) dx \right| \\ &\le \sum_{i=1}^{n} \mu(E_i) 2\varepsilon \|v\| \|u\| \\ &= 2\varepsilon \|v\| \|u\|.\end{aligned}$$

So $\|T - U\|_{op} \le 2\varepsilon\|u\|$. As $\varepsilon > 0$ was arbitrary, this shows that $T$ is a limit of operators of finite rank.

(f). By I.5.6.5(e), it suffices to show that $T(B)$ is totally bounded. Let $U$ be a neighborhoof of $0$, which we may assume to be an open ball of radius $\varepsilon > 0$. We must find $x_1, \dots, x_n \in B$ such that every point of $T(B)$ is at distance $< \varepsilon$ from one of the $T(x_i)$.

By (e), we know that $T$ is a limit of operators of finite rank, so we can find $U \in \mathrm{End}(V)$ of finite rank such that $\|T - U\|_{op} \le \varepsilon/4$. As $U$ has finite rank, $\overline{U(B)}$ is a closed bounded subset of the finite-dimensional space $\mathrm{Im}(U)$, so it is compact. In particular, we can find $x_1, \dots, x_n \in B$ such that, for every $y \in B$, there exists $i \in \{1, \dots, n\}$ such that $\|U(y) - U(x_i)\| < \varepsilon/2$.

Now let $y \in B$, and choose $i \in \{1, \dots, n\}$ such that $\|U(y) - U(x_i)\| < \varepsilon/2$. Then

$$\begin{aligned}\|T(y) - T(x_i)\| &\le \|T(y) - U(y)\| + \|U(y) - U(x_i)\| + \|U(x_i) - T(x_i)\| \\ &< \|y\|\varepsilon/4 + \varepsilon/2 + \|x_i\|\varepsilon/4 \\ &\le \varepsilon.\end{aligned}$$

(Remember that $y, x_i$ are in the closed unit ball of $V$.)

(g). Now we put everything together. Suppose that $V$ is an irreducible unitary representation of $G$. Then the operator $T \in \mathrm{End}(V)$ that we constructed is $G$-equivariant, so, by Schur's lemma, there exists $\lambda \in \mathbb{C}$ such that $T = \lambda \mathrm{id}_V$. As $T \ne 0$, $\lambda \ne 0$. So $T(\lambda B)$ is the closed unit ball in $V$. Part (f) says that this is compact, which, by Riesz's lemma, implies that $V$ is finite-dimensional.

□

## I.5.6 Vector-valued integrals and Minkowski's inequality

Note : You are allowed to use without proof the following results :

- The Hahn-Banach theorem.
- The fact that every continuous linear functional on a Hilbert space $V$ is of the form $\langle ., v\rangle$, with $v \in V$.
- Hölder's inequality.
- The fact that, if $(X, \mu)$ is a measure space, and if $1 \leq p < +\infty$ and $1 < q \leq +\infty$ are such that $p^{-1}+q^{-1} = 1$, then the map $L^p(X, \mu) \to \mathrm{Hom}(L^q(X, \mu), \mathbb{C})$, $f \longmapsto (g \longmapsto \int_X fgd\mu)$ is an isomorphism that preserves the norm ($L^p$ norm on the left, operator norm on the right). [23]

**Exercise I.5.6.1.** Let $(X, \mu)$ be a measure space and $V$ be a Banach space. We write $V^\vee$ for $\mathrm{Hom}(V, \mathbb{C})$. We say that a function $f : X \to V$ is *weakly integrable* if, for every $T \in V^\vee$, the function $T \circ f : X \to \mathbb{C}$ is in $L^1(X, \mu)$. If $f$ is weakly integrable and if there exists an element $v$ of $V$ such that $T(v) = \int_X T \circ f(x)d\mu(x)$ for every $T \in V^\vee$, we say that $v$ is the *integral* of $f$ on $X$ and write $v = \int_X f(x)d\mu(x) = \int_X fd\mu$.

(a). Show that the integral of $f$ is unique if it exists.

(b). Let $W$ be another Banach space and $u \in \mathrm{Hom}(V, W)$. If $f : X \to V$ is weakly integrable and has an integral $v$, show that $u \circ f : X \to W$ is weakly integrable and has an integral, which is equal to $u(v)$.

(c). Give an example of a weakly intergrable function that doesn't have an integral.

*Solution.*

(a). By the Hahn-Banach theorem, for every $v \in V$, there exists $T \in \mathrm{Hom}(V, \mathbb{C})$ such that $T(v) = \|v\|$ and $\|T\|_{op} \leq 1$. In particular, an element $v$ of $V$ is zero if and only if $T(v) = 0$ for every $T \in \mathrm{Hom}(V, \mathbb{C})$, or, in other words, two elements $v, w \in V$ are equal if and only if $T(v) = T(w)$ for every $T \in \mathrm{Hom}(V, \mathbb{C})$. This implies that the integral of $f$ is unique if it exists.

(b). We first show that $u \circ f$ is weakly integrable. Let $T \in \mathrm{Hom}(W, \mathbb{C})$. Then $T \circ u \in \mathrm{Hom}(V, \mathbb{C})$, so the function $T \circ u \circ f : X \to \mathbb{C}$ is integrable.

Now suppose that $f$ has an integral $v$. Then, for every $T \in \mathrm{Hom}(W, \mathbb{C})$, we have $T \circ \mathrm{Hom}(V, \mathbb{C})$, so $\int_X T \circ u \circ fd\mu = T \circ u(v)$. This means that $u(v)$ is the integral of $u \circ f$.

[23] Technical note : This is not true in general for $p = 1$, $q = +\infty$ if $\mu$ is not $\sigma$-finite, but it can be salvaged for a regular Borel measure on a locally compact Hausdorff space by slightly modifying the definition of $L^\infty$. You can ignore this.

(c). Let $X = \mathbb{N}$ with the counting measure $\mu$, and

$$V = c_0(\mathbb{N}) := \{(x_n)_{n\geq 0} \in \mathbb{C}^{\mathbb{N}} | \lim_{n\to+\infty} x_n = 0\}.$$

We will use the fact that $\ell^1(\mathbb{N})$ is the continuous dual of $c_0(\mathbb{N})$, via the map $\ell^1(\mathbb{N}) \times c_0(\mathbb{N}) \to \mathbb{C}$, $((x_n), (y_n)) \longmapsto \sum_{n\geq 0} x_n y_n$, and that the continuous dual of $\ell^1(\mathbb{N})$ is $\ell^\infty(\mathbb{N})$ (by a similar map). The map from $c_0(\mathbb{N})$ into its bidual is the usual embedding $c_0(\mathbb{N}) \subset \ell^\infty(\mathbb{N})$.

We define $f : X \to V$ by $f(n) = \mathbb{1}_{\{n\}}$. Then, for every $(x_n)_{n\geq 0} \in \ell^1(\mathbb{N})$, if $T : c_0(\mathbb{N}) \to \mathbb{C}$ is the corresponding linear functional, we have

$$\int_X T(f(x))d\mu(x) = \sum_{n\geq 0} x_n,$$

which converges because $(x_n)_{n\geq 0}$ is in $\ell^1(\mathbb{N})$. Hence $f$ is weakly integrable. But $f$ does not have an integral (at least in $c_0(\mathbb{N})$), because the continuous linear functional it defines on $\ell^1(\mathbb{N})$ is representable by an element of $\ell^\infty(\mathbb{N})$ which is not in $c_0(\mathbb{N})$ (the constant sequence 1). As evaluating on points of $\ell^1(\mathbb{N})$ separates the elements of $\ell^\infty(\mathbb{N})$, there cannot be any element of $c_0(\mathbb{N})$ giving the same linear functional on $\ell^1(\mathbb{N})$.

□

**Exercise I.5.6.2.** In this problem, $X$ is a locally compact Hausdorff space and $\mu$ is a regular Borel measure on $X$. Let $V$ be a Banach space, and let $f : X \to V$ be a continuous function with compact support.

(a). Show that $f$ is weakly integrable.

(b). If $\mu(\operatorname{supp} f) = 0$, show that $\int_X f d\mu$ exists and is equal 0.

The goal of this problem is to show that:

(i) $f$ has an integral $v$;

(ii) $\|v\| \leq \int_X \|f(x)\| d\mu(x)$;

(iii) if $\mu(\operatorname{supp} f) \neq 0$, then $\mu(\operatorname{supp} f)^{-1} v$ is in the closure of the convex hull of $f(X)$.

By question (b), we may (and will) assume that $\mu(\operatorname{supp} f) \neq 0$.

(a). Show that we may assume that $X = \operatorname{supp} f$ (in particular, $X$ is compact) and that $\mu(X) = 1$.

From now on, we assume that $X$ is compact and that $\mu(X) = 1$.

(a). Let $T_1, \ldots, T_n : V \to \mathbb{R}$ be bounded $\mathbb{R}$-linear functionals (we see $V$ as a $\mathbb{R}$-vector space in the obvious way), and define $a_1, \ldots, a_n \in \mathbb{R}$ by $a_i = \int_X T_i \circ f d\mu$. Show that $(a_1, \ldots, a_n)$ is in the convex hull of the compact subset $((T_1, \ldots, T_n) \circ f)(X)$ of $\mathbb{R}^n$. (Hint : What happens if it is not ?)

Let $K$ be the closure of the convex hull of $f(X)$. This is a compact subset of $V$ by problem I.5.6.7. For every finite subset $\Omega$ of $\mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})$ (the space of bounded $\mathbb{R}$-linear functionals from $V$ to $\mathbb{R}$), we denote by $I_\Omega$ the set of $v \in K$ such that, for every $T \in \Omega$, we have $T(v) = \int_X T \circ f d\mu$.

(a). Show that $I_\Omega$ is compact for every $\Omega \subset \mathrm{Hom}_{\mathbb{R}}(V,\mathbb{R})$.

(b). Show that $I_\Omega$ is nonempty if $\Omega$ is finite.

(c). Show that the integral of $f$ exists and is in $K$.

(d). Show that :

$$\| \int_X f d\mu \| \leq \int_X \|f(x)\| d\mu(x).$$

(Hint : Hahn-Banach.)

*Solution.*

(a). Let $T \in \mathrm{Hom}(V,\mathbb{C})$. Then $T \circ f : X \to \mathbb{C}$ is a continuous, and its support is contained in $\mathrm{supp}(f)$, hence compact. Hence $T \circ f$ is integrable.

(b). Suppose that $\mu(\mathrm{supp}\, f) = 0$. If $T \in \mathrm{Hom}(V,\mathbb{C})$, then $T \circ f : X \to \mathbb{C}$ is continuous and $\mu(\mathrm{supp}(T \circ f)) = 0$, so $\int_X T \circ f(f) d\mu = 0$. This shows that 0 is the integral of $f$.

(c). Suppose that we know the conclusion if $X = \mathrm{supp}\, f$ and $\mu(X) = 1$. Let $f : X \to V$ be continuous with compact support. We have already seen that we may assume $\mu(\mathrm{supp}\, f) \neq 0$, so let's do that. Let $X' = \mathrm{supp}\, f$, and consider the measure $\mu'$ on $X'$ that is $\mu(\mathrm{supp}\, f)^{-1}$ times the restriction of $\mu$. By our assumption, $\int_{X'} f_{|X'} d\mu'$ exists, let's call it $v$, we have $\|v\| \leq \int_{X'} \|f(x)\| d\mu'(x)$ and $v$ is in the closure of the convex hull of $f(X')$.

Let's show that $w := \mu(\mathrm{supp}\, f)v$ is the integral of $f$. Note that $\mu(\mathrm{supp}\, f)^{-1}w$ is in the convex hull of $f(X') = f(X)$ and that

$$\|w\| \leq \mu(\mathrm{supp}\, f) \int_{X'} |f(x')| d\mu'(x) = \int_X |f(x)| d\mu(x),$$

so this proves the conclusion for $f$.

Let $T \in \mathrm{Hom}(V,\mathbb{C})$. Then $\mathrm{supp}(T \circ f) \subset X'$, so

$$\int_X T \circ f(x) d\mu(x) = \mu(\mathrm{supp}\, f) \int_{X'} T \circ f(x) d\mu'(x) = w.$$

So $w = \int_X f d\mu$.

(d). Let $L = ((T_1, \dots, T_n) \circ f)(X)$. Suppose that $(a_1, \dots, a_n)$ is not in the convex hull of $L$. Then, by the hyperplane separation theorem, there exists a linear functional $\lambda : \mathbb{R}^n \to \mathbb{R}$

and $c > 0$ such that $\lambda(a_1, \dots, a_n) \geq c + \lambda(v)$, for every $v \in L$. Let $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ be the images by $\lambda$ of the vectors of the canonical basis of $\mathbb{R}^n$. Then we have, for every $x \in X$,

$$\sum_{i=1}^{n} \lambda_i a_i = \lambda(a_1, \dots, a_n) \geq c + \lambda \circ (T_1, \dots, T_n) \circ f(x) = c + \sum_{i=1}^{n} \lambda_i T_i(f(x)).$$

Taking the integral over $X$ (and using $\mu(X) = 1$) gives

$$\sum_{i=1}^{n} \lambda_i a_i \geq c + \sum_{i=1}^{n} \lambda_i \int_X T_i \circ f(x) d\mu(x) = c + \sum_{i=1}^{n} \lambda_i a_i,$$

a contradiction.

(e). For every $T \in \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$, the set of $v \in K$ such that $T(v) = \int_X T \circ f d\mu$ is a closed subset of $K$. As the set $I_\Omega$ is an intersection of sets of this form, it is also a closed subset of $K$, hence compact because $K$ is compact.

(f). If $\Omega$ is finite, write $\Omega = \{T_1, \dots, T_n\}$ and $T_\Omega = (T_1, \dots, T_n) : V \to \mathbb{R}^n$. We have seen in question (d) that $a := \int_X T_\Omega(f(x)) d\mu(x)$ is in the convex hull of $T_\Omega(f(X))$, so there exists $v \in V$ such that $v$ is in the convex hull of $f(X)$ (hence in $K$) and $T_\Omega(v) = a = \int_V T_\Omega(f(x)) d\mu(x)$. The second condition says exactly that $v \in I_\Omega$.

(g). The subsets $(I_{\{T\}})_{T \in \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})}$ of $K$ have the finite intersection property by question (f). As $K$ is compact, this implies that $\cap_{T \in \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})} I_{\{T\}}$ is nonempty. Choose a vector $v$ in it. Let $T \in \mathrm{Hom}(V, \mathbb{C})$. As $\mathrm{Re}(T)$ and $\mathrm{Im}(T)$ are in $\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$, we have

$$\begin{aligned} T(v) &= \mathrm{Re}(T(v)) + i\,\mathrm{Im}(T(v)) \\ &= \int_X \mathrm{Re}(T(f(x))) d\mu(x) + i \int_X \mathrm{Im}(T(f(x))) d\mu(x) \\ &= \int_X T(f(x)) d\mu(x), \end{aligned}$$

so $v = \int_X f d\mu$. Also, $v \in K$ because all the $I_{\{T\}}$ are contained in $K$ by definition.

(h). By the Hahn-Banach theorem, there exists $T \in \mathrm{Hom}(V, \mathbb{C})$ such that $T(v) = \|v\|$ and $\|T\|_{op} \leq 1$. Then

$$\|v\| = |T(v)| = |\int_X T(f(x)) d\mu(x)| \leq \int_X |T(f(x))| d\mu(x) \leq \int_X \|f(x)\| d\mu(x).$$

$\square$

**Exercise I.5.6.3.** In this problem, $X$ is a locally compact Hausdorff space and $\mu$ is a regular Borel measure on $X$. Let $V$ be a Banach space, let $f : X \to \mathbb{C}$ be a function in $L^1(X, \mu)$, and let $G : X \to V$ be a bounded continuous function.

The goal of this problem is to show that :

(i) the function $fG : X \to V$ has an integral $v$;

(ii) $\|v\| \leq (\sup_{x\in X} \|G(x)\|) \left(\int_X |f(x)|d\mu(x)\right)$;

(iii) $v \in \overline{\mathrm{Span}(G(X))}$.

(a). Show that $fG$ is weakly integrable.

(b). Let $(f_n)_{n\geq 0}$ be a sequence of functions of $\mathscr{C}_c(X)$ that converges to $f$ in $L^1(X,\mu)$. Show that $\int f_n G d\mu$ exists for each $n \geq 0$, and that $(\int_X f_n G d\mu)_{n\geq 0}$ is a Cauchy sequence.

(c). Prove assertions (i), (ii) and (iii) above.

*Solution.*

(a). Let $T \in \mathrm{Hom}(V,\mathbb{C})$. Then, for every $x \in X$,

$$|T(f(x)G(x))| \leq |f(x)||T(G(x))| \leq |f(x)|\|T\|_{op}\|G(x)\| \leq |f(x)|\|T\|_{op} \sup_{y\in X} \|G(y)\|.$$

As $\sup_{y\in X} \|G(y)\| < +\infty$ and $f \in L^1(X, mu)$, the function $T \circ (fG)$ is integrable. So $fG$ is weakly integrable.

(b). For every $h \in \mathscr{C}_c(X)$, the function $hG : X \to V$ is continuous and has support contained in $\mathrm{supp}(h)$, hence compact. By problem I.5.6.2, this function is integrable, and we have

$$\|\int_X (hG)(x)d\mu(x)\| \leq \int_X |h(x)|\|G(x)\|d\mu(x) \leq \sup_{y\in X} \|G(y)\|\|h\|_1.$$

Applying this to $f_n$ shows that $f_n G$ is integrable, and applying it to $f_n - f_m$ shows that

$$\|\int_X (f_n G)d\mu(x) - \int_X (f_m G)d\mu\| \leq \sup_{y\in X} \|G(y)\|\|f_n - f_m\|_1 \xrightarrow[n,m\to+\infty]{} 0$$

because $(f_n)_{n\geq 0}$ converges in $L^1(X,\mu)$.

(c). As $V$ is complete, the Cauchy sequence $(\int_X (f_n G)d\mu)$ has a limit in $V$, that we'll call $v$. For every $T \in \mathrm{Hom}(V,\mathbb{C})$, we have

$$T(v) = \lim_{n\to+\infty} T\left(\int_X (f_n G)d\mu\right) = \lim_{n\to+\infty} \int_X T(f_n(x)G(x))d\mu(x).$$

As in (a), we have

$$\|\int_X T(f_n(x)G(x))d\mu(x) - \int_X T(f(x)G(x))d\mu(x)\| \leq \sup_{y\in X} \|G(y)\|\|T\|_{op}\|f_n - f\|_1,$$

so this converges to 0 as $n \to +\infty$, and we get

$$T(v) = \int_X T(f(x)G(x))d\mu(x).$$

This shows that $x$ is the integral of $fG$.

Moreover, by problem I.5.6.2, $\int_X (f_n G) d\mu$ is in the closure of the span $G(X)$ for every $n \geq 0$. As $v$ is the limit of these vectors, it is also in the close of $\mathrm{Span}(G(X))$.

Finally, to show the bound on $\|v\|$, we could use the Hahn-Banach theorem and the property characterising $v$ as in question I.5.6.2(h), or use the fact that

$$\| \int_X (f_n G) d\mu \| \leq \int_X |f_n(x)| \|G(x)\| d\mu(x) \leq \sup_{x \in X} \|G(x)\| \|f_n\|_1$$

for every $n \geq 0$ and that this sequence of integrals converges to $v$.

□

**Exercise I.5.6.4.** Let $G$ be a locally compact group, $\mu$ be a left Haar measure on $G$, and $L^1(G) = L^1(G, \mu)$. Let $f, g \in L^1(G)$.

(a). Show that the function $G \to L^1(G)$, $y \longmapsto f(y) L_y g$ is weakly integrable and has an integral.

(b). Show that

$$f * g = \int_G f(y) L_y g d\mu(y).$$

*Solution.*

(a). Note that the function $G \to L^1(G)$, $y \longmapsto L_y g$ is continuous and that $\sup_{y \in G} \|L_y g\|_1 = \|g\|_1 < +\infty$. So the conclusion follows from problem I.5.6.3.

(b). Let $F = \int_G f(y) L_y g d\mu(y) \in L^1(G)$. By definition of the intergral, for every $h \in L^\infty(G)$, we have

$$\int_G h(x) F(x) d\mu(x) = \int_{G \times G} h(x) f(y) g(y^{-1} x) d\mu(y) d\mu(x) = \int_G h(x) (f * g)(x) d\mu(x).$$

As $L^\infty(G)$ is the continuous dual of $L^1(G)$, we have $f * g = F$ by question I.5.6.1(a).

□

**Exercise I.5.6.5.** Let $V$ be a normed vector space. A subset $A$ is $V$ is called *totally bounded* if, for every neighborhood $U$ of $0$ in $V$, there is a finite set $F$ such that $A \subset F + U$.

(a). Show that the convex hull of a finite subset of $V$ is compact.

(b). Show that every compact subset of $V$ is totally bounded.

(c). If $A \subset V$ is totally bounded, show that $\overline{A}$ is totally bounded.

(d). If $A$ is a totally bounded subset of $V$, show that its convex hull is totally bounded. (Hint : Open balls are convex.)

(e). If $V$ is complete and $A$ is totally bounded, show that $\overline{A}$ is compact.

(f). If $V$ is complete and $K \subset V$ is compact, show that the closure of the convex hull of $K$ is compact.

*Solution.*

(a). Let $F$ be a finite subset subset of $V$. Then its convex hull is contained in $\mathrm{Span}(F)$, which is finite-dimensional. In a finite-dimensional vector space, the convex hull of any compact set is compact, so the convex hull of the finite set $F$ is compact.

(b). Let $K$ be compact subset of $V$, and let $U$ be a neighborhood of $0$ in $V$. We may assume that $U$ is open. Then $K \subset \bigcup_{x\in K}(x+U)$. As $K$ is compact, there exists a finite subset $F$ of $K$ such that $K \subset \bigcup_{x\in F}(x+U) = F+U$.

(c). Let $A \subset V$ be a totally bounded subset, and let $U$ be a neighborhood of $0$ in $V$. We may assume that $U$ is an open ball centered at $0$ and of positive radius, say $c$. Let $U'$ be the open ball centered at $0$ of radius $c/2$. As $A$ is totally bounded, there exists a finite set $F$ such that $A \subset F+U'$. As $F$ is finite, the set $F+\overline{U'}$ is closed, so it contains $\overline{A}$. But $U \supset \overline{U'}$, so $\overline{A} \subset F+U$.

(d). Let $U$ be a neighborhood of $0$ in $V$. Choose a convex open neighborhood $U'$ of $0$ (a ball for example) such that $U'+U' \subset U$, and let $F$ be a finite set such that $A \subset F+U'$. Let $K$ be the convex hull of $F$, then $A \subset K+U'$. As $K$ and $U'$ are convex, so is $K+U'$, so the convex hull of $A$ is contained in $K+U'$. On the other hand, the set $K$ is compact by question (a), hence totally bounded by question (b), so there exists a finite set $F'$ such that $K \subset F'+U'$, hence $K+U' \subset F'+U'+U' \subset F'+U$. So we have found a finite set $F'$ such that the convex hull of $A$ is contained in $F'+U$.

(e). Write $K=\overline{A}$. For every $x \in V$ and $c>0$, let $B(x,c)$ be the closed ball of radius $c$ center at $x$.

Let $(U_i)_{i\in I}$ be a family of open subsets of $K$ such that $K \subset \bigcup_{i\in I} U_i$, and assume that no finite subfamily of $(U_i)_{i\in I}$ covers $K$. We know that $K$ is totally bounded by question (c). We will construct by induction on $n$ a decreasing sequence $(K_n)_{n\geq 1}$ of nonempty closed subsets of $K$ such that $K_n$ is contained in a ball of radius $1/n$ and $K_n$ cannot be covered by a finite subfamily of $(U_i)_{i\in I}$.

First, as $K$ is totally bounded, there exists a finite set $F$ such that $K \subset F+B(0,1) = \bigcup_{x\in F} B(x,1)$. We choose $x \in F$ such that $K \cap B(x,1)$ is nonempty and cannot be covered by a finite number of the $U_i$, and take $K_1 = K \cap B(x,1)$.

Now suppose that we have constructed $K_1,\dots,K_n$, with $n \geq 1$. Then, as $K_n$ is totally bounded (as a subset of $K$), there exists a finite set $F$ such that $K_n \subset F+B(0,(n+1)^{-1})$.

Again, as $K_n$ cannot be covered by a finite number of the $U_i$, there must exist $x \in F$ such that $K_n \cap B(x, (n+1)^{-1})$ is nonempty and can also not be covered by a finite number of the $U_i$, and we take $K_{n+1} = K_n \cap B(x, (n+1)^{-1})$.

Choose $x_n \in K_n$ for every $n \geq 1$. By the condition that $K_n$ is contained in a ball of radius $1/n$, the sequence $(x_n)_{n\geq 0}$ is a Cauchy sequence. As $V$ is complete, $(x_n)_{n\geq 1}$ has a limit, say $x$. As $x \in K$, there exists $i \in I$ such that $U_i$. But then $B(x, c) \subset U_i$ for $c > 0$ small enough, so $K_n \subset U_i$ for $n$ big enough, which contradicts the properties of $K_n$.

(f). By question (d), the convex hull of $K$ is totally bounded, so its closure is compact by question (e).

□

**Exercise I.5.6.6.** Let $G$ be a locally compact group, let $dx$ be a left Haar measure on $G$, and let $UCB(G)$ be the subspace of $L^\infty(G)$ composed of the left uniformly continuous bounded functions on $G$.

Let $f \in L^1(G)$ and $\varphi \in L^\infty(G)$.

(a). Show that $f * \varphi$ exists and is left uniformly continuous and bounded.

(b). If $\varphi \in UCB(G)$, show that the integral $\int_G f(y) L_y \varphi dy$ exists and is equal to $f * \varphi$.

*Solution.*

(a). Let $x \in G$. Then the integral defining $f * \varphi(x)$ is

$$\int_G f(y)\varphi(y^{-1}x)d\mu(y),$$

which converges because $|f(y)\varphi(y^{-1}x)| \leq \|\varphi\|_\infty |f(y)|$ for every $y \in G$. This also shows that

$$|f * \varphi(x)| \leq \|\varphi\|_\infty \|f\|_1$$

for every $x \in G$, so $f * \varphi$ is bounded and

$$\|f * \varphi\|_\infty \leq \|\varphi\|_\infty \|f\|_1,$$

Now we show that $f * \varphi$ is left uniformly continuous. Let $x \in G$. By proposition I.4.1.3, we have $L_x(f * \varphi) = (L_x f) * \varphi$, so

$$\|L_x(f * \varphi) - f * \varphi\|_\infty = \|(L_x f - f) * \varphi\|_\infty \leq \|L_x f - f\|_1 \|\varphi\|_\infty.$$

By proposition I.3.1.13, this tends to 0 as $x$ tends to 1 in $G$, which exactly means that $f * \varphi$ is left uniformly continuous.

(b). Suppose that $\varphi \in UCB(G)$. Then the map $G \to UCB(G)$, $y \longmapsto L_y\varphi$ is continuous (see remark I.1.13), so the integral $\int_G f(y)L_y\varphi d\mu(y)$ exists in $UCB(G)$ by problem I.5.6.3. Let $h = \int_G f(y)L_y\varphi d\mu(y)$.

For every $g \in L^1(G)$, the map $\psi \longmapsto \int_G g\psi d\mu$ is a continuous linear functional on $UCB(G)$. So, by definition of the integral, we have

$$\int_G ghd\mu = \int_{G\times G} h(x)f(y)\varphi(y^{-1}x)d\mu(x)d\mu(y) = \int_G g(f*\varphi)d\mu.$$

As the linear functionals defined by the elements of $L^1(G)$ separate points on $L^\infty(G)$, this implies that $h = f * \varphi$.

□

**Exercise I.5.6.7** (Minkowski's inequality)**.** Let $(X,\mu)$ and $(Y,\nu)$ be measure spaces, which we will take $\sigma$-finite to simplify. [24] Let $p \in (1,+\infty)$. [25] Let $\varphi : X \times Y \to \mathbb{C}$ be a measurable function. We assume that

$$\int_Y \left(\int_X |\varphi(x,y)|^p d\mu(x)\right)^{1/p} d\nu(y) < \infty.$$

(a). Show that the function $\varphi(.,y)$ is in $L^p(X,\mu)$ for almost every $y \in Y$.

(b). Let $Y'$ be a measurable subset of $Y$ such that $\nu(Y - Y') = 0$ and $\varphi(.,y) \in L^p(X,\mu)$ for every $y \in Y'$. Show that the function $Y' \to L^p(X,\mu)$, $y \longmapsto \varphi(.,y)$ is weakly integrable.

(c). Show that the integral $h \in L^p(X,\mu)$ of the function of (b) exists, and that we have

$$h(x) = \int_Y \varphi(x,y)d\nu(y)$$

for almost all $x \in X$.

(d). Show Minkowski's inequality :

$$\left(\int_X \left|\int_Y \varphi(x,y)d\nu(y)\right|^p d\mu(x)\right)^{1/p} \le \int_Y \left(\int_X |\varphi(x,y)|^p d\mu(x)\right)^{1/p} d\nu(y).$$

*Solution.*

(a). The function $y \longmapsto \left(\int_X |\varphi(x,y)|^p d\mu(x)\right)^{1/p}$ is integrable by hypothesis, so it must take finite values for almost all $y \in Y$, which means that $\int_X |\varphi(x,y)|^p d\mu(x) < +\infty$ for almost every $y \in Y$.

[24] There is a way to extend the results to not necessarily $\sigma$-compact locally compact groups with their Haar measures.

[25] Minkowski's inequality is still true for $p = 1$, but it follows immediately from the Fubini-Torelli theorem in that case.

(b). Let $q \in (1,+\infty)$ be such that $\frac{1}{p}+\frac{1}{q}$. We want to check that, for every $f \in L^q(X,\mu)$, the integral $\int_{Y'}\int_X f(x)\varphi(x,y)d\mu(x)d\mu(y)$ converges. Let $f \in^q (X,\mu)$. By Hölder's inequality, for every $y \in Y'$, $\int_X f(x)\varphi(x,y)d\mu(x)$ converges absolutely, and

$$\int_X |f(x)\varphi(x,y)|d\mu(x) \leq \|f\|_q \|\varphi(.,y)\|_p.$$

As $\int_{Y'} \|\varphi(.,y)\|_p d\nu(y)$ converges by hypothesis, this gives the convergence of $\int_{Y'}\int_X f(x)\varphi(x,y)d\mu(x)d\mu(y)$, and even its absolute convergence.

(c). We have seen in question (b) that $\int_X\int_Y |f(x)\varphi(x,y)|d\mu(x)d\nu(y) < +\infty$ for every $f \in L^1(X,\mu)$. By Fubini's theorem, this implies that, for every $f \in L^q(X,\mu)$, $\int_Y |f(x)\varphi(x,y)|d\nu(y) = |f(x)|\int_Y |\varphi(x,y)|d\nu(y) < +\infty$ for almost all $x \in X$. As $f$ is arbitrary (and $\mu$ is $\sigma$-finite), we get that $\int_Y |\varphi(x,y)|d\nu(y) < +\infty$ for almost all $x \in X$, say for $x \in X'$ with $\mu(X - X') = 0$.

We define a function $h : X' \to \mathbb{C}$ by $h(x) = \int_Y \varphi(x,y)d\nu(y)$. We want to show that this is the integral of $y \longmapsto \varphi(.,y)$. If $f \in L^q(X,\mu)$, we have

$$\int_X f(x)h(x)d\mu(x) = \int_X f(x)\varphi(x,y)d\mu(x)d\mu(y),$$

so, using Hölder's inequality as in question (b),

$$\left|\int_X f(x)h(x)d\mu(x)\right| \leq \int_{X\times Y} |f(x)\varphi(x,y)|d\mu(x) \leq C\|f\|_q,$$

where

$$C = \int_Y \left(\int_X |\varphi(x,y)|^p\right)^{1/p} d\nu(y).$$

This shows that $f \longmapsto \int_X f(x)h(x)d\mu(x)$ is a bounded linear functional on $L^q(X,\mu)$, and that its operator norm is bounded by $C$. As the continuous dual of $L^q(X,\mu)$ is $L^p(X,\mu)$, we must have $h \in L^p(X,\mu)$ and $\|h\|_p \leq C$. The first property, together with the formula for $\int_X f(x)h(x)d\mu(x)$, says that $h$ is indeed the integral of $y \longmapsto \varphi(.,y)$.

(d). The second property of $h$ proved above is exactly Minkowski's inequality.

$\square$

# II Some Gelfand theory

## II.1 Banach algebras

In this section, $A$ will be a Banach algebra. (See definition I.4.1.4.) Note that the submultiplicativity of the norm implies that the multiplication is a continuous map from $A \times A$ to $A$.

We suppose for now that $A$ has a unit $e$ and denote by $A^\times$ the group of invertible elements of $A$.

### II.1.1 Spectrum of an element

**Definition II.1.1.1.** Let $x \in A$.

(i) The *spectrum* of $x$ in $A$ is

$$\sigma(x) = \sigma_A(x) = \{\lambda \in \mathbb{C} | \lambda e - x \notin A^\times\}.$$

(ii) The *spectral radius* of $x$ is

$$\rho(x) = \inf_{n \geq 1} \|x^n\|^{1/n}.$$

We will see below how that $\rho(x)$ is equal to $\sup\{|\lambda|,\ \lambda \in \sigma(x)\}$ (which justifies the name "spectral radius").

We start by proving some basic properties of invertible elements and the spectral radius. (Note that point (i) does not use the completeness of $A$, so it stays true in any normed algebra.)

**Proposition II.1.1.2.** *(i) If $x, y \in A^\times$ are such that $\|x - y\| \leq \frac{1}{2}\|x^{-1}\|^{-1}$, then we have*

$$\|x^{-1} - y^{-1}\| \leq 2\|x^{-1}\|^2 \|y - x\|.$$

*In particular, the map $x \longmapsto x^{-1}$ is a homeomorphism from $A^\times$ onto itself.*

*(ii) For every $x \in A$, we have*

$$\rho(x) = \lim_{n \to +\infty} \|x^n\|^{1/n}$$

*(Gelfand's formula).*

(iii) *Let $x \in A$. If $\rho(x) < 1$ (for example if $\|x\| < 1$), then $e - x \in A^\times$ and $(e-x)^{-1} = \sum_{n\geq 0} x^n$, with the convention that $x^0 = e$. (In particular, the series converges.)*

(iv) *The group $A^\times$ is open in $A$.*

*Proof.* (i) We have

$$\|y^{-1}\| - \|x^{-1}\| \leq \|y^{-1} - x^{-1}\| = \|y^{-1}(x-y)x^{-1}\| \leq \|y^{-1}\|\|x-y\|\|x^{-1}\| \leq \frac{1}{2}\|y^{-1}\|.$$

In particular, $\|y^{-1}\| \leq 2\|x^{-1}\|$. Combining this with the inequality above gives

$$\|y^{-1} - x^{-1}\| \leq \|y^{-1}\|\|x-y\|\|x^{-1}\| \leq 2\|x^{-1}\|^2\|x-y\|,$$

which is the first statement. This also show that the map $x \longmapsto x^{-1}$ is continuous. As this map is equal to its own inverse, it is a homeomorphism.

(ii) Let $\varepsilon > 0$. We want to find $N \in \mathbb{Z}_{\geq 1}$ such that $\|x^n\|^{1/n} \leq \rho(x) + \varepsilon$ for $n \geq N$. (We already know that $\|x^n\|^{1/n} \geq \rho(x)$ by definition of $\rho(x)$, so this is enough to establish the result.) By definition of $\rho(x)$, we can find $m \geq 1$ such that $\|x^m\|^{1/m} \leq \rho(x) + \frac{1}{2}\varepsilon$. For every integer $n \geq 1$, we can write $n = mq(n) + r(n)$, with $q(n), r(n) \in \mathbb{N}$ and $0 \leq r(n) \leq m-1$. Note that

$$\frac{q(n)}{n} = \frac{1}{m}\left(1 - \frac{r(n)}{n}\right) \xrightarrow[n\to+\infty]{} \frac{1}{m},$$

hence

$$\|x^m\|^{q(n)/n}\|x\|^{r(n)/n} \xrightarrow[n\to+\infty]{} \|x^m\|^{1/m}.$$

Choose $N \geq 1$ such that, for $n \geq 1$, we have

$$\|x^m\|^{q(n)/n}\|x\|^{r(n)/n} \leq \|x^m\|^{1/m} + \frac{\varepsilon}{2} \leq \rho(x)\varepsilon.$$

Then, if $n \geq N$, we have

$$\|x^n\|^{1/n} = \|x^{mq(n)}x^{r(n)}\|^{1/n} \leq \|x^m\|^{q(n)/n}\|x\|^{r(n)/n} \leq \rho(x) + \varepsilon,$$

as desired. [1]

(iii) Fix $r \in \mathbb{R}$ such that $\rho(x) < r < 1$. Then, by (ii), we have $\|x^n\| \leq r^n$ for $n$ big enough. For every $n \in \mathbb{N}$, we write $S_n = \sum_{k=0}^n x^k$. Then, if $m \geq n$ are big enough, we have

$$\|S_m - S_n\| = \left\|\sum_{k=n+1}^m x^k\right\| \leq r^{n+1}\sum_{k\geq 0} r^k = r^{n+1}\frac{1}{1-r}.$$

[1] The reasoning used in this proof is sometimes called *Fekete's lemma*. See `https://en.wikipedia.org/wiki/Subadditivity`.

So the sequence $(S_n)_{n\geq 0}$ is a Cauchy sequence, and it converges because $A$ is complete. This means that the series $\sum_{n\geq 0} x^n$ converges. Moreover, for every $n \geq 0$, we have

$$(e-x)S_n = S_n(e-x) = \sum_{k=0}^{n} x^k - \sum_{k=1}^{n+1} x^k = e - x^{n+1}.$$

This tends to $e$ as $n \to +\infty$, so $\sum_{n\geq 0} x^n$ is the inverse of $e-x$.

(iv) Let $x \in A^\times$. If $y \in A$ is such that $\|y-x\| < \|x^{-1}\|^{-1}$, then we have $\|e - x^{-1}y\| \leq \|x^{-1}\|\|x-y\| < 1$. So, by (iii), $x^{-1}y \in A^\times$, hence $y \in A^\times$.

□

**Theorem II.1.1.3.** *For every $x \in A$, the spectrum $\sigma_A(x)$ is a nonempty compact subset of $\mathbb{C}$, and we have*

$$\rho(x) = \max\{|\lambda|,\ \lambda \in \sigma_A(x)\}.$$

This explains the name "spectral radius" for $\rho(x)$. Note in particular that, although the spectrum of $x$ depends on $A$ (for example, if we consider a Banach subalgebra $B$ of $A$ containing $x$, then we have $\sigma_B(x) \supset \sigma_A(x)$, but this may not be an equality), the spectral radius of $x$ does not.

*Proof.* Consider the map $F : \mathbb{C} \to A$ sending $\lambda \in \mathbb{C}$ to $\lambda e - x$. Then $F$ is continuous, and $\sigma_A(x)$ is the inverse of the closed subset $A - A^\times$ of $A$, so $\sigma_A(x)$ is closed in $\mathbb{C}$.

Next, let $\lambda \in \mathbb{C}$ such that $|\lambda| > \rho(x)$. Then $\rho(\lambda^{-1}x) < 1$, so, by (iii) of proposition II.1.1.2, we have $e - \lambda^{-1}x = \lambda^{-1}(\lambda e - x) \in A^\times$, which immediately implies that $\lambda \notin \sigma_A(x)$. So we have shown that

$$\rho(x) \geq \sup\{|\lambda|,\ \lambda \in \sigma_A(x)\}.$$

In particular, $\sigma_A(x)$ is a closed and bounded subset of $\mathbb{C}$, so it is compact.

Let's show that $\sigma_A(x)$ is not empty. Let $T : A \to \mathbb{C}$ be a bounded linear functional, and define $f : \mathbb{C} - \sigma_A(x) \to \mathbb{C}$ by $f(\lambda) = T((\lambda e - x)^{-1})$. If $\lambda, \mu \in \mathbb{C} - \sigma_A(x)$, then

$$(\lambda e - x)^{-1} - (\mu e - x)^{-1} = (\lambda e - x)^{-1}((\mu e - x) - (\lambda e - x))(\mu e - x)^{-1} = -(\lambda - \mu)(\lambda e - x)^{-1}(\mu e - x)^{-1},$$

so, if $\lambda \neq \mu$, we get

$$\frac{f(\lambda) - f(\mu)}{\lambda - \mu} = -T((\lambda e - x)^{-1}(\mu e - x)^{-1}).$$

Using the continuity of the function $y \longmapsto y^{-1}$ (see (i) of proposition II.1.1.2), we get, for every $\lambda \in \mathbb{C} - \sigma_A(x)$,

$$\lim_{\mu \to \lambda} \frac{f(\lambda) - f(\mu)}{\lambda - \mu} = -T((\lambda e - x)^{-2}).$$

In particular, the function $f$ is holomorphic on $\mathbb{C} - \sigma_A(x)$. Let's prove that $f$ vanishes at $\infty$, i.e. that $f(\lambda)$ tends to $0$ when $|\lambda| \to +\infty$. Let $\lambda \in \mathbb{C}$ such that $|\lambda| > \rho(x)$. Then, by (iii) of proposition II.1.1.2,

$$(\lambda e - x)^{-1} = \lambda^{-1}(e - \lambda^{-1}x)^{-1} = \frac{1}{\lambda}\sum_{n\geq 0}\frac{1}{\lambda^n}x^n,$$

so

$$\|(\lambda e - x)^{-1}\| \leq \frac{1}{|\lambda|}\sum_{n\geq 0}\frac{\|x\|^n}{|\lambda|^n} = \frac{1}{|\lambda|}\frac{1}{1 - |\lambda|^{-1}\|x\|}.$$

This tends to $0$ as $|\lambda| \to +\infty$; as $T$ is continuous, so does $f(\lambda)$.

Now suppose that $\sigma_A(x) = \varnothing$. Then $f$ is an entire function, and $f(\lambda) \to 0$ as $|\lambda| \to +\infty$. By Liouville's theorem, this implies that $f = 0$, i.e. that $T((\lambda e - x)^{-1}) = 0$ for every $\lambda \in \mathbb{C}$. But this is true for every $T \in \operatorname{Hom}(A, \mathbb{C})$ and bounded linear functionals on $A$ separate points by the Hahn-Banach theorem, so we get that $(\lambda e - x)^{-1} = 0$ for every $\lambda \in \mathbb{C}$. This is impossible, because $(\lambda e - x)^{-1} \in A^\times$. So $\sigma_A(x) \neq \varnothing$.

Finally, we prove that

$$\rho(x) \leq \max\{|\lambda|,\ \lambda \in \sigma_A(x)\}.$$

Let $r = \max\{|\lambda|,\ \lambda \in \sigma_A(x)\}$. We already know that $r \leq \rho(x)$. Assume that $r < \rho(x)$, and pick $r'$ such that $r < r' < \rho(x)$. Let $T \in \operatorname{Hom}(A, \mathbb{C})$ and define $f : \mathbb{C} - \sigma_A(x) \to \mathbb{C}$ as before. Then we have seen that $f$ is holomorphic on $\mathbb{C} - \sigma_A(x) \supset \{\lambda \in \mathbb{C} | |\lambda| > r\}$. We have also seen that, if $|\lambda| > \rho(x)$, then

$$(\lambda e - x)^{-1} = \sum_{n\geq 0}\frac{1}{\lambda^{n+1}}x^n,$$

hence

$$f(\lambda) = \sum_{n\geq 0}\frac{T(x^n)}{\lambda^{n+1}}.$$

By uniqueness of the power series expansion, this is still valid for $|\lambda| > r$. In particular, the series $\sum_{n\geq 0}\frac{T(x^n)}{(r')^{n+1}}$ converges, so the sequence $(\frac{T(x^n)}{(r')^{n+1}})_{n\geq 0}$ converges to $0$, and in particular it is bounded. Consider the sequence $(\alpha_n)_{n\geq 0}$ of bounded linear functionals on $\operatorname{Hom}(A, \mathbb{C})$ defined by $\alpha_n(T) = \frac{T(x^n)}{(r')^{n+1}}$. We just saw that, for every $T \in \operatorname{Hom}(A, \mathbb{C})$, the sequence $(\alpha_n(T))_{n\geq 0}$ is bounded. By the uniform boundedness principle (theorem I.3.2.11), this implies that the sequence $(\|\alpha_n\|_{op})_{n\geq 0}$ is bounded. But note that, by the Hahn-Banch theorem, we have $\|\alpha_n\|_{op} = \left\|\frac{x^n}{(r')^{n+1}}\right\|$. So the sequence $(\frac{\|x^n\|}{(r')^{n+1}})_{n\geq 0}$ is bounded. Choose a real number $C$ bounding it. Then we get

$$\rho(x) = \lim_{n\to+\infty}\|x^n\|^{1/n} \leq \lim_{n\to+\infty} C^{1/n}(r')^{(n+1)/n} = r',$$

a contradiction. So $r \geq \rho(x)$.

□

## II.1.2 The Gelfand-Mazur theorem

It is a well-known fact that every finite-dimensional $\mathbb{C}$-algebra that is a field is isomorphic to $\mathbb{C}$. This is the Banach algebra analogue.

**Corollary II.1.2.1** (Gelfand-Mazur theorem)**.** *Let $A$ be a Banach algebra in which every nonzero element is invertible. Then $A$ is isomorphic to $\mathbb{C}$ (i.e. $A = \mathbb{C}e$).*

*Proof.* Let $x \in A$. By theorem II.1.1.3, $\sigma_A(x) \neq \varnothing$. Let $\lambda \in \sigma_A(x)$, then $\lambda e - x$ is not invertible, so $x = \lambda e$ by hypothesis.

□

**Definition II.1.2.2.** We say that a subset $I$ of $A$ is an *ideal* if it is an ideal in the usual algebraic sense, i.e. if $I$ is a $\mathbb{C}$-subspace of $A$ that is stable by left and right multiplication by every element of $A$. We say that $I$ is a *proper ideal* of $A$ if $I$ is an ideal of $A$ and $I \neq A$.

If $I$ is an ideal of $A$, then it is easy to see that $\overline{I}$ is also an ideal.

Remember also the definition of the quotient norm.

**Definition II.1.2.3.** Let $V$ be a normed vector space and $W \subset V$ be a closed subspace. Then the *quotient norm* on $V/W$ is defined by

$$\|x + W\| = \inf_{w \in W} \|v + w\|.$$

If $V$ is a Banach space, then so is $V/W$ (for the quotient norm).

**Proposition II.1.2.4.** *(i) If $I$ is a closed ideal of $A$, then $A/I$ is a Banach algebra for the quotient norm.*

*(ii) If $I$ is a proper ideal of $A$, then so is its closure $\overline{I}$.*

*Proof.* (i) We already know that $A/I$ is a Banach space and an algebra, so we just need to check that its norm is submultiplicative. Let $x, y \in A$. Then

$$\begin{aligned}
\|x + I\|\|y + I\| &= \inf_{a,b \in I} \|x + a\|\|y + b\| \\
&\geq \inf_{a,b \in I} \|(x + a)(y + b)\| \\
&= \inf_{a,b \in I} \|xy + (ay + xb + ab)\| \\
&\geq \inf_{c \in I} \|xy + c\| \text{ (because } ay + xb + ab \in I \text{ if } a, b \in I) \\
&= \|xy + I\|.
\end{aligned}$$

(ii) Consider the open ball $B = \{x \in A | \|e - x\| < 1\}$. Then $B \subset A^\times$ by proposition II.1.1.2, so $B \cap I = \varnothing$. As $B$ is open, this implies that $B \cap \overline{I} = \varnothing$, so $\overline{I} \neq A$.

□

**Corollary II.1.2.5.** *Let $A$ be a commutative unital Banach algebra. If $\mathfrak{m}$ is a maximal ideal of $A$, then $\mathfrak{m}$ is closed, and $A/\mathfrak{m} = \mathbb{C}$.*

This is the Banach algebra analogue of the Nullstellensatz.

*Proof.* By proposition II.1.2.4, the ideal $\overline{\mathfrak{m}}$ is also proper; as $\mathfrak{m}$ is maximal, we must have $\mathfrak{m} = \overline{\mathfrak{m}}$, i.e. $\mathfrak{m}$ is closed. By the same proposition, $A/\mathfrak{m}$ is a Banach algebra. Also, every nonzero element of $A/\mathfrak{m}$ is invertible because $\mathfrak{m}$ is maximal, so $A/\mathfrak{m} = \mathbb{C}$ by the Gelfand-Mazur theorem.

□

## II.2 Spectrum of a Banach algebra

In this section, $A$ is still a Banach algebra, but we don't assume that it has a unit.

**Definition II.2.1.** A *multiplicative functional* on $A$ is a nonzero linear functional $\varphi : A \to \mathbb{C}$ such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in A$

The set of all multiplicative functionals on $A$ is called the *spectrum* of $A$ and denoted by $\sigma(A)$. We put the weak* topology on $\sigma(A)$. In other words, if $\varphi \in \sigma(A)$, then a basis of open neighborhoods of $\varphi$ is given by the sets $\{\psi \in \sigma(A) | \forall i \in \{1, \dots, n\},\ |\varphi(x_i) - \psi(x_i)| < c_i\}$, for $n \in \mathbb{Z}_{\geq 1}$, $x_1, \dots, x_n \in A$ and $c_1, \dots, c_n \in \mathbb{R}_{>0}$.

Note that we do not assume that $\varphi$ is continuous; in fact, this is automatically the case, as we will see below.

**Lemma II.2.2.** *If $A$ is unital, then, for every $\varphi \in \sigma(A)$, we have $\varphi(e) = 1$ and $\varphi(A^\times) \subset \mathbb{C}^\times$.*

*Proof.* Let $x \in A$ be such that $\varphi(x) \neq 0$. Then $\varphi(x) = \varphi(xe) = \varphi(x)\varphi(e)$, so $\varphi(e) = 1$. Also, if $y \in A^\times$, then $1 = \varphi(e) = \varphi(y)\varphi(y^{-1})$, so $\varphi(y) \in \mathbb{C}^\times$.

□

**Definition II.2.3.** Let $A$ be a Banach algebra. Then we define a unital Banach algebra $A_e$ by taking the $\mathbb{C}$-vector space $A \oplus \mathbb{C}e$, defining the multiplication on $A_e$ by $(x + \lambda e)(y + \mu e) = (xy + \lambda y + \mu x) + \lambda\mu e$ (for $x, y \in A$ and $\lambda, \mu \in \mathbb{C}$) and the norm by $\|x + \lambda e\| = \|x\| + |\lambda|$ (for $x \in A$ and $\lambda \in \mathbb{C}$). If $A$ is a Banach $*$-algebra, we make $A_e$ into a Banach $*$-algebra by setting $(x + \lambda e)^* = x^* + \overline{\lambda} e$ (for $x \in A$ and $\lambda \in \mathbb{C}$).

This construction is called *adjoining an identity* to $A$.

*Remark* II.2.4. If $A$ already has a unit, then $A_e$ is not equal to $A$. In fact, if we denote by $e_A$ the unit of $A$, then the map $A_e \to A \times \mathbb{C}$ sending $x + \lambda e$ to $(x + \lambda e_A, \lambda)$ is an isomorphism of $\mathbb{C}$-algebras (and a homeomorphism).

**Proposition II.2.5.** *For every $\varphi \in \sigma(A)$, we get an element $\widetilde{\varphi} \in \sigma(A_e)$ by setting $\widetilde{\varphi}(x + \lambda e) = \varphi(x) + \lambda$. This defines an injective map $\sigma(A) \to \sigma(A_e)$, whose image is $\sigma(A_e) - \{\varphi_\infty\}$, with $\varphi_\infty$ defined by $\varphi_\infty(x + \lambda e) = \lambda$.*

Later, we will identify $\varphi$ and $\widetilde{\varphi}$ and simply write $\sigma(A_e) = \sigma(A) \cup \{\varphi_\infty\}$.

*Proof.* The fact that $\widetilde{\varphi}$ is a multiplicative functional follows directly from the definition of the multiplication on $A_e$, and $\widetilde{\varphi}$ obviously determines $\varphi$. So we just need to check the statement about the image of $\sigma(A) \to \sigma(A_e)$.

Let $\psi \in \sigma(A_e)$ such that $\psi \neq \varphi_\infty$, and let $\varphi = \psi_{|A}$. Then we have $\psi(x + \lambda e) = \varphi(x) + \lambda$ for all $x \in A$ and $\lambda \in \mathbb{C}$; as $\psi \neq \varphi_\infty$, the linear functional $\varphi : A \to \mathbb{C}$ cannot be zero, so $\varphi$ is a multiplicative functional on $A$, and we clearly have $\psi = \widetilde{\varphi}$.

□

**Corollary II.2.6.** *Let $\varphi \in \sigma(A)$. Then $\varphi$ is a bounded linear function on $A$, and we have $\|\varphi\|_{op} \leq 1$, with equality if $A$ is unital.*

*Proof.* By proposition II.2.5, the multiplicative functional extends to a multiplicative functional $\widetilde{\varphi}$ on $A_e$. Let $x \in A$. For every $\lambda \in \mathbb{C}$ such that $|\lambda| > \|x\|$, the element $x - \lambda e$ of $A_e$ is invertible by proposition II.1.1.2, so $\varphi(x) - \lambda = \widetilde{\varphi}(x - \lambda e) \neq 0$. This implies that $|\varphi(x)| \leq \|x\|$, i.e. that $\varphi$ is bounded and $\|\varphi\|_{op}$.

If $A$ is unital, then $\|e\| = 1$ and $\varphi(e) = 1$, so $\|\varphi\|_{op} = 1$.

□

**Theorem II.2.7.** *Let $A$ be a Banach algebra.*

*(i) If $A$ is unital, then the space $\sigma(A)$ is compact Hausdorff.*

*(ii) In general, the space $\sigma(A)$ is locally compact Hausdorff, and $\sigma(A_e)$ is its Alexandroff compactification (a.k.a. one-point compactification).*

Remember that, if $X$ is a Hausdorff locally compact topological space, then its Alexandroff compactification is the space $X \cup \{\infty\}$ (i.e. $X$ with one point added), and that its open subsets are the open subsets of $X$ and the complements in $X \cup \{\infty\}$ of compact subsets of $X$.

*Proof.* By corollary II.2.6, the spectrum $\sigma(A)$ is a subset of the closed unit ball of $\mathrm{Hom}(A, \mathbb{C})$. We know that this closed unit ball is compact Hausdorff for the weak* topology on $\mathrm{Hom}(A, \mathbb{C})$ (this is Alaoglu's theorem), and $\sigma(A) \cup \{0\}$ is closed in this topology, because it is defined by the closed conditions $\varphi(xy) = \varphi(x)\varphi(y)$, for all $x, y \in A$. So $\sigma(A) \cup \{0\}$ is compact (for the weak* topology), and its open subset $\sigma(A)$ is locally compact. If $A$ is unital, then $\sigma(A)$ is closed in $\sigma(A) \cup \{0\}$ because it is cut out by the condition $\varphi(e) = 1$, so $\sigma(A)$ is compact.

Now we show the last statement of (ii). If $\varphi \in \sigma(A)$ (resp. $\sigma(A_e)$), $x \in A$ and $c > 0$, we set

$$U(\varphi, x, c) = \{\psi \in \sigma(A) | |\varphi(x) - \psi(x)| < c\}$$

$$\text{(resp. } \widetilde{U}(\varphi, x, c) = \{\psi \in \sigma(A_e) | |\varphi(x) - \psi(x)| < c\}).$$

These form a basis for the topology of $\sigma(A)$ (resp. $\sigma(A_e)$).

If $\varphi \in \sigma(A)$, $x \in A$ and $c > 0$, we have

$$\widetilde{U}(\widetilde{\varphi}, x, c) = \begin{cases} U(\varphi, x, c) \cup \{\varphi_\infty\} & \text{if } |\varphi(x)| < c \\ U(\varphi, x, c) & \text{otherwise.} \end{cases}$$

For the neighborhoods of $\varphi_\infty$, we get that, if $x \in A$ and $c > 0$, then

$$\begin{aligned} \widetilde{U}(\varphi_\infty, x, c) &= \{\varphi_\infty\} \cup \{\varphi \in \sigma(A) | |\varphi(x)| < c\} \\ &= \sigma(A_e) - \{\psi \in \sigma(A_e) | |\psi(x)| \geq c\}. \end{aligned}$$

So the topology of $\sigma(A)$ is induced by the topology of $\sigma(A_e)$. Also, as $\{\psi \in \sigma(A_e) | |\psi(x)| \geq c\}$ is closed in $\sigma(A_e)$, hence compact, for all $x \in A$ and $c > 0$, the open neighborhoods of $\varphi_\infty$ in $\sigma(A_e)$ are exactly the complements of the compact subsets of $\sigma(A)$. This means that $\sigma(A_e)$ is the Alexandroff compactification of $\sigma(A)$.

□

**Definition II.2.8.** Let $A$ be a Banach algebra. For every $x \in A$, the map $\widehat{x} : \sigma(A) \to \mathbb{C}$ defined by $\widehat{x}(\varphi) = \varphi(x)$ is called the *Gelfand transform* of $x$.

Note that each $\widehat{x}$ is continuous on $\sigma(A)$ by definition of the topology of $\sigma(A)$. The resulting map $\Gamma : A \to \mathscr{C}(\sigma(A))$, $x \longmapsto \widehat{x}$ is called the *Gelfand representation* of $A$ (or sometimes also the Gelfand transform).

Note that $\Gamma$ is a morphism of $\mathbb{C}$-algebras by definition of the algebra operations on $\mathscr{C}(\sigma(A))$.

**Theorem II.2.9.** *(i) The map $\Gamma$ maps $A$ into $\mathscr{C}_0(\sigma(A))$, and we have $\|\widehat{x}\|_\infty \leq \|x\|$ for every $x \in A$.*

*(ii) The image of $\Gamma$ separates the points of $\sigma(A)$.*

*(iii) If $A$ is unital, then $\widehat{e}$ is the constant function $1$ on $\sigma(A)$.*

*Proof.* (i) If $A$ is unital, then $\sigma(A)$ is compact, so $\mathscr{C}_0(\sigma(A)) = \mathscr{C}(\sigma(A))$. In general, as $\sigma(A_e)$ is the Alexandroff compactification of $\sigma(A)$, we just need to check that $\widehat{x}(\varphi_\infty) = 0$ for every $x \in A$; but this follows immediately from the definitions.

Let $x \in A$. Then
$$\|\widehat{x}\|_\infty = \sup_{\varphi\in\sigma(A)} |\widehat{x}(\varphi)| = \sup_{\varphi\in\sigma(A)} |\varphi(x)| \leq \|x\|$$
by corollary II.2.6.

(ii) Let $\varphi, \varphi' \in \sigma(A)$ such that $\varphi \neq \varphi'$. Then there exists $x \in A$ such that $\varphi(x) \neq \varphi'(x)$, i.e. $\widehat{x}(\varphi) \neq \widehat{x}(\varphi')$.

(iii) This follows immediately from lemma II.2.2.

□

For a general Banach algebra (even a unital one), the spectrum can be empty (see exercise II.5.1). But this cannot occur for commutative Banach algebras.

**Theorem II.2.10.** *Let $A$ be a commutative unital Banach algebra. Then the map $\varphi \longmapsto \mathrm{Ker}(\varphi)$ induces a bijection from $\sigma(A)$ to the set of maximal ideals of $A$.*

If you have seen another definition of the spectrum (for example in algebraic geometry), this theorem shows how it is related to our definition.

*Proof.* If $\varphi \in \sigma(A)$, then $A/\mathrm{Ker}(\varphi) \simeq \mathbb{C}$ (note that $\varphi$ is surjective because it is nonzero), so $\mathrm{Ker}(\varphi)$ is a maximal ideal of $A$. This shows that the map is well-defined.

If $\mathfrak{m}$ is a maximal ideal, then it follows from the Gelfand-Mazur theorem that $A/\mathfrak{m} \simeq \mathbb{C}$ (see corollary II.1.2.5), so the map $\varphi : A \to A/\mathfrak{m} \simeq \mathbb{C}$ is an element of $\sigma(A)$ such that $\mathrm{Ker}(\varphi) = \mathfrak{m}$. This shows that the map is surjective.

Now we need to check injectivity. Let $\varphi, \psi \in \sigma(A)$ such that $\mathfrak{m} := \mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi)$. Let $x \in A$. As $A/\mathfrak{m} \simeq \mathbb{C}$, we can write $x = \lambda e + y$, with $\lambda \in \mathbb{C}$ and $y \in \mathfrak{m}$. Then we have
$$\varphi(x) = \lambda = \psi(y).$$
So $\varphi = \psi$.

□

**Corollary II.2.11.** *Let $A$ be a commutative unital Banach algebra. Then, for every $x \in A$ :*

*(i) $x \in A^\times$ if and only if $\widehat{x}$ never vanishes;*

*(ii) $\widehat{x}(\sigma(A)) = \sigma_A(x)$;*

*(iii) $\|\widehat{x}\|_\infty = \rho(x)$.*

*Proof.* (i) If $x \in A^\times$, then $\widehat{x}$ cannot vanish, because we have $\widehat{x}\widehat{x^{-1}} = \widehat{e} = 1$. Conversely, suppose that $x$ is not invertible. Then there exists a maximal ideal containing $x$, so, by theorem II.2.10, there exists $\varphi \in \sigma(A)$ such that $0 = \varphi(x) = \widehat{x}(\varphi)$.

(ii) By (i), we have

$$\sigma_A(x) = \{\lambda \in \mathbb{C} | x - \lambda e \notin A^\times\} = \{\lambda \in \mathbb{C} | \widehat{x} - \lambda \text{ vanishes at at least one point}\} = \widehat{x}(\sigma(A)).$$

(iii) This follows from (ii) and from theorem II.1.1.3.

□

## II.3 $C^*$-algebras and the Gelfand-Naimark theorem

**Definition II.3.1.** A Banach $*$-algebra $A$ is called a $C^*$*-algebra* if we have $\|x^*x\| = \|x\|^2$ for every $x \in A$.

*Remark* II.3.2. Everybody calls this a $C^*$-algebra, except Bourbaki who says “stellar algebra” (“algèbre stellaire”).

**Lemma II.3.3.** *If $A$ is a $C^*$-algebra, then $\|x\| = \|x^*\|$ for every $x \in A$.*

.

*Proof.* Let $x \in A - \{0\}$. Then

$$\|x\|^2 = \|x^*x\| \leq \|x^*\|\|x\|,$$

so $\|x\| \leq \|x^*\|$. Applying this to $x^*$ and using that $(x^*)^* = x$ gives $\|x^*\| \leq \|x\|$.

□

**Example II.3.4.** Most of the examples of example I.4.2.2 are actually $C^*$-algebras.

(a) $\mathbb{C}$ is a $C^*$-algebra because, for every $\lambda \in \mathbb{C}$, we have $|\lambda\overline{\lambda}| = |\lambda|^2$.

(b) Let $G$ be a locally compact group. Then $L^1(G)$ is not a $C^*$-algebra in general, though it does satisfy the conclusion of lemma II.3.3. [2]

(c) Let $X$ be a locally compact Haudorff space. Then $\mathscr{C}_0(X)$ is a $C^*$-algebra, because, for every $f \in \mathscr{C}_0(X)$, we have

$$\|f^*f\|_\infty = \sup_{x\in X} |\overline{f(x)}f(x)| = \sup_{x\in X} |f(x)|^2 = \|f\|_\infty^2.$$

(d) Let $V$ be a Hilbert space. Then $\mathrm{End}(V)$ is a $C^*$-algebra. Indeed, let $T \in \mathrm{End}(V)$. We want to prove that $\|T^*T\|_{op} = \|T\|_{op}^2$. First note that

$$\|T^*\|_{op} = \sup_{v,w\in V,\ \|v\|=\|w\|=1} |\langle T^*(v), w\rangle| = \sup_{v,w\in V,\ \|v\|=\|w\|=1} |\langle v, T(w)\rangle| = \|T\|_{op},$$

[2] There is a way to modify the norm on $L^1(G)$ to make the completion for the new norm a $C^*$-algebra, but we won’t need this here.

so $\|T^*T\|_{op} \leq \|T^*\|_{op}\|T\|_{op} = \|T\|_{op}^2$. On the other hand,

$$\|T^*T\|_{op} = \sup_{v\in V,\ \|v\|=1} \|T^*T(v)\| \geq \sup_{v\in V,\ \|v\|=1} |\langle T^*T(v), v\rangle| = \sup_{v\in V,\ \|v\|=1} |\langle T(v), T(v)\rangle| = \|T\|_{op}^2.$$

**Proposition II.3.5.** *Let $A$ be a $C^*$-algebra. Then the Gelfand representation $\Gamma : A \to \mathscr{C}_0(\sigma(A))$ is a $*$-homomorphism.*

*Remark* II.3.6. The proposition says that everybody multiplicative functional on $A$ is a $*$-homomorphism. A Banach $*$-algebra satisfying this condition is called *symmetric*. Every $C^*$-algebra is symmetric, but the converse is not true. (For example, if $G$ is a locally compact commutative group, then $L^1(G)$ is symmetric, see exercise II.5.4.)

*Proof.* By adjoining an identity to $A$, we may reduce to the case where $A$ is unital. (See exercise II.5.6 for the correct choice of norm on $A_e$. Note that changing the norm on $A_e$ does not affect $\sigma(A_e)$, because the definition of the spectrum does not involve the norm.)

Let $x \in A$ and $\varphi \in \sigma(A)$. We want to prove that $\varphi(x^*) = \widehat{x^*}(\varphi) = \overline{\widehat{x}}(\varphi) = \overline{\varphi(x)}$. Write $\varphi(x) = a + ib$ and $\varphi(x^*) = c + id$, with $a, b, c, d \in \mathbb{R}$.

Suppose that $b + d \neq 0$. Let

$$y = \frac{1}{b+d}(x + x^* - (a+c)e) \in A.$$

Note that $y = y^*$, and that

$$\varphi(y) = \frac{1}{b+d}(a + ib + c + id - (a+c)) = i,$$

so, for every $t \in \mathbb{R}$, we have $\varphi(y + ite) = (1+t)i$, hence

$$|1+t| = |\varphi(y+ite)| \leq \|y + ite\|$$

(by corollary II.2.6). Using the defining property of $C^*$-algebras and the fact that $y = y^*$ gives, for every $t \in \mathbb{R}$,

$$(1+t)^2 \leq \|y+ite\|^2 = \|(y+ite)(y+ite)^*\| = \|(y+ite)(y-ite)\| = \|y^2 + t^2 e\| \leq \|y^2\| + t^2,$$

i.e. $1 + 2t \leq \|y\|^2$. But this implies that $\|y\|$ is infinite, which is not possible. So $b + d = 0$, i.e. $d = -b$.

Applying the same reasoning to $ix$ and $(ix)^* = -ix^*$ (and nothing that $\varphi(ix) = \overline{-b + ia}$ and $\varphi((ix^*)) = d - ic$) gives $a - c = 0$, i.e. $a = c$. This finishes the proof that $\varphi(x^*) = \overline{\varphi(x)}$.

$\square$

**Proposition II.3.7.** *Let $A$ be a commutative unital $C^*$-algebra. Then, for every $x \in A$, we have $\|x\| = \rho(x)$.*

*Proof.* If $x \in A$ is such that $x = x^*$, then $\|x\|^2 = \|x^*x\| = \|x^2\|$, so $\|x^{2^n}\| = \|x\|^{2^n}$ for every $n \in \mathbb{N}$.

Now let $x$ be any element of $A$. Then $(xx^*)^* = xx^*$, so the first part applies to $xx^*$. Also, for every $n \in \mathbb{N}$, $(xx^*)^n = x^n(x^*)^n$ (because $A$ is commutative). So, if $n \geq 0$,

$$\|x\|^{2^{n+1}} = \|xx^*\|^{2^n} = \|(xx^*)^{2^n}\| = \|x^{2^n}(x^*)^{2^n}\| = \|x^{2^n}\|^2.$$

This implies that

$$\rho(x) = \lim_{x\to+\infty} \|x^{2^n}\|^{2^{-n}} = \|x\|.$$

□

**Definition II.3.8.** If $A$ is a Banach $*$-algebra, an element $x$ of $A$ is called *normal* if $xx^* = x^*x$.

**Corollary II.3.9.** *Let $A$ be a unital $C^*$-algebra, and let $x \in A$ be a normal element of $A$. Then $\rho(x) = \|x\|$.*

In particular, if $V$ is a Hilbert space and $T \in \mathrm{End}(V)$ is normal, then $\|T\|_{op} = \rho(T)$.

*Proof.* Indeed, as $x$ commutes with $x^*$, the closure of the smallest unital $\mathbb{C}$-algebra $A'$ of $A$ containing $x$ and $x^*$ is a commutative $C^*$-algebra, and $\rho(x)$ and $\|x\|$ don't change when we see $x$ as an element of $A'$.

□

**Theorem II.3.10** (Gelfand-Naimark theorem)**.** *Let $A$ be a commutative unital $C^*$-algebra. Then the Gelfand representation $\Gamma : A \to \mathscr{C}(\sigma(A))$ is an isometric $*$-isomorphism.*

*Proof.* We know that $\Gamma$ is a $*$-homomorphism by proposition II.3.5, and that it is an isometry by corollary II.2.11(iii) and proposition II.3.7. In particular, $\Gamma$ is injective. So it just remains to show that it is surjective. As $\Gamma$ is an isometry and $A$ is complete, the image $\Gamma(A)$ is closed in $\mathscr{C}(\sigma(A))$; but it separates points by theorem II.2.9(ii) and contains the constant functions because $\Gamma(e) = 1$, so it is equal to $\mathscr{C}(\sigma(A))$ by the Stone-Weierstrass theorem.

□

It is easy to see that the Gelfand-Naimark theorem implies the following result (but we won't need it).

**Corollary II.3.11.** *Let $A$ be a commutative $C^*$-algebra. Then the Gelfand representation $\Gamma : A \to \mathscr{C}_0(\sigma(A))$ is an isometric $*$-isomorphism.*

# II.4 The spectral theorem

**Theorem II.4.1.** *Let $V$ a Hilbert space, and let $T \in \mathrm{End}(V)$ be normal. We denote by $A_T$ the closure of the unital subalgebra of $\mathrm{End}(V)$ generated by $T$ and $T^*$; it is commutative because $T$ and $T^*$ commute.*

*Then there exists an isometric $*$-isomorphism $\Phi : \mathscr{C}(\sigma(T)) \xrightarrow{\sim} A_T$ such that, if $\iota$ is the injection of $\sigma(T)$ into $\mathbb{C}$, we have $\Phi(\iota) = T$.*

Note that we just write $\sigma(T)$ for $\sigma_{\mathrm{End}(T)}(T)$ (this is the usual spectrum of $T$).

This theorem doesn't look a lot like the spectral theorem of finite-dimensional linear algebra. See exercise II.5.2 for a way to pass between the two.

*Proof.* Let $A = A_T$. First we will prove the result with $\sigma_A(T)$ instead of $\sigma(T)$, then we'll show that $\sigma(T) = \sigma_A(T)$. Note that we automatically have $\sigma(T) \subset \sigma_A(T)$ (because, if $\lambda \mathrm{id}_V - T$ is not invertible in $\mathrm{End}(T)$, then it certainly won't be invertible in a subalgebra).

Consider the Gelfand transform of $T$ (seen as an element of $A$), this is a continuous map $\widehat{T} : \sigma(A) \to \mathbb{C}$. Let's show that $\widehat{T}$ is injective. Consider $\varphi_1, \varphi_2 \in \sigma(A)$, i.e. two multiplicative functionals on $A$, such that $\widehat{T}(\varphi_1) = \widehat{T}(\varphi_2)$, i.e. $\varphi_1(T) = \varphi_2(T)$. We have seen that the Gelfand representation is a $*$-homomorphism, so we have

$$\widehat{T^*}(\varphi_1) = \overline{\widehat{T}(\varphi_1)} = \overline{\widehat{T}(\varphi_2)} = \widehat{T^*}(\varphi_2),$$

i.e. $\varphi_1(T^*) = \varphi_2(T^*)$. The multiplicative functionals $\varphi_1$ and $\varphi_2$ are equal on $e$, $T$ and $T^*$, and they are continuous, so they are equal on all of $A$, which is what we wanted.

Now remember that $\sigma(A)$ is compact Hausdorff, because $A$ is unital. So $\widehat{T}$ induces a homeomorphism from $\sigma(A)$ to its image in $\mathbb{C}$, which is $\sigma_A(T)$ by corollary II.2.11. Hence composing with $\widehat{T}$ gives an isometric $*$-isomorphism $\Psi : \mathscr{C}(\sigma_A(T)) \xrightarrow{\sim} \mathscr{C}(\sigma(A))$.

Remember that we also have the Gelfand representation of $A$, which is an isometric $*$-isomorphism $\Gamma : A \xrightarrow{\sim} \mathscr{C}(\sigma(A))$. So we get an isometric $*$-isomorphism $\Phi : \mathscr{C}(\sigma_A(T)) \xrightarrow{\sim} A$ by setting $\Phi = \Gamma^{-1} \circ \Psi$.

Let's show that $\Phi(\iota) = T$. As $\Gamma : A \to \mathscr{C}(\sigma(A))$ is an isomorphism, it suffices to check that $\widehat{T} = \widehat{\Phi(\iota)}$, i.e. that $\widehat{T} = \Psi(\iota)$. Let $\varphi \in \sigma(A)$. We have $\Psi(\iota)(\varphi) = \iota(\widehat{T}(\varphi)) = \widehat{T}(\varphi)$, as desired.

Finally, we show that the inclusion $\sigma(T) \subset \sigma_A(T)$ is an equality. Let $\lambda \in \sigma_A(T)$, and suppose that $\lambda \notin \sigma(T)$. Let $\varepsilon > 0$, and choose $f \in \mathscr{C}(\sigma_A(T))$ such that $\|f\|_\infty = 1$, $f(\lambda) = 1$ and $f(\mu) = 0$ if $|\lambda - \mu| \geq \varepsilon > 0$. Let $U = \Phi(f) \in A$, then $\|U\|_{op} = \|f\|_\infty = 1$. Note that $\Phi(1) = \mathrm{id}_V$ (where $1$ is the constant function with value $1$), because $\Phi$ is an isomorphism of algebras. So $T - \lambda \mathrm{id}_V = \Phi(\iota - \lambda)$, and $(T - \lambda \mathrm{id}_V) \circ U = \Phi((\iota - \lambda) f)$. As $\Phi$ is an isometry, this implies that

$$\|(T - \lambda \mathrm{id}_V) \circ U\|_{op} = \|(\iota - \lambda) f\|_\infty \leq \varepsilon$$

(because $f$ is bounded by 1, and $f(\mu) = 0$ if $|\lambda - \mu| \geq \varepsilon$). On the other hand, as $\lambda \notin \sigma(T)$, the operator $T - \lambda \mathrm{id}_V$ is invertible in $\mathrm{End}(V)$, so we get

$$1 = \|f\|_\infty = \|U\|_{op} = \|(T - \lambda \mathrm{id}_V)^{-1}(T - \lambda \mathrm{id}_V)U\|_{op} \leq \varepsilon \|(T - \lambda \mathrm{id}_V)^{-1}\|_{op}.$$

This is true for every $\varepsilon > 0$, so it implies that $1 = 0$, which is a contradiction.

□

**Corollary II.4.2.** *Let $V$ be a Hilbert space and $T \in \mathrm{End}(V)$ be normal. Then the following conditions are equivalent :*

*(i)* $\sigma(T)$ *is a singleton;*

*(ii)* $T \in \mathbb{C}\mathrm{id}_V$*;*

*(iii)* $A_T = \mathbb{C}\mathrm{id}_V$.

*Proof.*

(i)⇒(ii) If $\sigma(T) = \{\lambda\}$, then $\iota$ is $\lambda$ times the unit of $\mathscr{C}(\sigma(T))$, so $T = \Phi(\iota) = \lambda \mathrm{id}_V$.

(ii)⇒(iii) If $T \in \mathbb{C}\mathrm{id}_V$, then $\mathbb{C}\mathrm{id}_V$ is a closed unital subalgebra of $A$ containing $T$ and $T^*$, so it is equal to $A_T$.

(ii)⇒(iii) Suppose that $A_T = \mathbb{C}\mathrm{id}_V$. Let $\lambda, \mu \in \sigma(T)$. If $\lambda \neq \mu$, then we can find $f_1, f_2 \in \mathscr{C}(\sigma(T))$ such that $f_1(\lambda) = 1$, $f_2(\mu) = 1$ and $f_1 f_2 = 0$. But then $\Phi(f_1)\Phi(f_2) = 0$ and $\Phi(f_1), \Phi(f_2) \neq 0$, which contradicts the fact that $\mathbb{C}$ is a domain.

□

**Definition II.4.3.** If $A$ is a $\mathbb{C}$-algebra and $E \subset A$ is a subset, we set $Z_A(E) = \{x \in A | \forall y \in E,\ xy = yx\}$. This is called the *centralizer* of $E$ in $A$.

It is easy to see that the centralizer is always a subalgebra of $A$.

**Corollary II.4.4.** *Let $V$ be a Hilbert space, and let $E$ be a subset of $\mathrm{End}(V)$ such that $E^* = E$. Suppose that the only closed subspaces of $V$ stable by all the elements of $E$ are $\{0\}$ and $V$. Then $Z_{\mathrm{End}(V)}(E) = \mathbb{C}\mathrm{id}_V$.*

*Proof.* Let $A = Z_{\mathrm{End}(V)}(E)$. It is a closed subalgebra of $\mathrm{End}(V)$. We show that $A$ is stable by $*$ : If $T \in A$, then, for every $U \in E$, we have $U^* \in E$, hence

$$T^* \circ U = (U^* \circ T)^* = (T \circ U^*)^* = U \circ T^*,$$

so $T^* \in A$. In particular, the subalgebra $A$ is generated by its normal elements; indeed, for every $T \in A$, we have $T = \frac{1}{2}((T + T^*) + (T - T^*))$, and both $T + T^*$ and $T - T^*$ are normal.

Remember that we want to show that each element of $A$ is in $\mathbb{C}\mathrm{id}_V$; by what we just showed, it suffices to prove it for the normal elements of $A$. So let $T \in A$ be normal. By corollary II.4.2, it suffices to show that the spectrum $\sigma(T)$ of $T$ is a singleton. By the spectral theorem (theorem II.4.1), we have an isometric $*$-isomorphism $\Phi : \mathscr{C}(\sigma(T)) \xrightarrow{\sim} A_T$, where $A_T$ is the closure of the unital subalgebra of $\mathrm{End}(V)$ generated by $T$ and $T^*$, such that $\Phi$ sends the embedding $\iota : \sigma(T) \hookrightarrow \mathbb{C}$ to $T$. Note that $A_T \subset A$. Now suppose that $\sigma(T)$ is not a singleton. Then we can find two nonzero functions $f_1, f_2 \in \mathscr{C}(\sigma(T))$ such that $f_1 f_2 = 0$, and $\Phi(f_1), \Phi(f_2)$ are nonzero elements of $\mathrm{End}_G(V)$ such that $\Phi(f_1)\Phi(f_2) = 0$. Let $W = \overline{\mathrm{Im}(\Phi(f_2))}$; then $W \neq \{0\}$ because $\Phi(f_2)$ is nonzero. Also, as $\Phi(f_2)$ commutes with every element of $E$, the subspace $W$ is stable by all the elements of $E$, so $W = V$ by hypothesis. But we also have $\Phi(f_1)(W) = 0$ because $\Phi(f_1)\Phi(f_2) = 0$, so $\Phi(f_1) = 0$, which contradicts the choice of $f_1, f_2$. So $\sigma(T)$ is a singleton, and we are done.

□

## II.5 Exercises

**Exercise II.5.1.** (a). Let $V$ be a finite-dimensional $\mathbb{C}$-vector space such that $\dim_{\mathbb{C}}(V) \geq 2$. Show that $\sigma(\mathrm{End}(V)) = \varnothing$.

(b). Let $V$ be an infinite-dimensional Hilbert space. Show that $\sigma(\mathrm{End}(V)) = \varnothing$.

(Hint : Look at nilpotent endomorphisms.)

*Solution.*

(a). We may assume that $V = \mathbb{C}^n$, so that $\mathrm{End}(V) = M_n(\mathbb{C})$. Let $\varphi : M_n(\mathbb{C}) \to \mathbb{C}$ be a multiplicative linear functional. We want to prove that $\varphi = 0$. Let $(E_{ij})_{1 \leq i,j \leq n}$ be the canonical basis of $M_n(\mathbb{C})$ (so $E_{ij}$ is the matrix with all entry $0$, except for a $1$ at the $(i, j)$-entry). Then $E_{ij}E_{kl}$ is equal to $0$ unless $j = k$, and $E_{ij}E_{jl} = E_{il}$. In particular, if $i \neq j$, then $E_{ij}^2 = 0$, hence $0 = \varphi(E_{ij}^2) = \varphi(E_{ij})^2$, and $\varphi(E_{ij}) = 0$. Also, for every $i \in \{1, \dots, n\}$, if we choose $j$ such that $j \neq i$ (this is possible because $n \geq 2$), then $E_{ii} = E_{ij}E_{ji}$, so $\varphi(E_{ii}) = \varphi(E_{ij})\varphi)E_{ji}) = 0$. To sum up, we have shown that $\varphi$ is $0$ on a basis of $M_n(\mathbb{C})$, so $\varphi = 0$.

(b). Let $\varphi : \mathrm{End}(V) \to \mathbb{C}$ be a multiplicative linear functional. As in (a), as the key is to note that, if $T \in \mathrm{End}(V)$ is such that $T^2 = 0$, then we have $\varphi(T)^2 = 0$, hence $\varphi(T) = 0$. Now choose two closed subspaces $V_1$ and $V_2$ such that $V = V_1 \oplus V_2$ and that $V_1$ and $V_2$ are isomorphic. (This is possible because $V$ is infinite-dimensional. For example, choose a Hilbert basis $(e_i)_{i \in I}$ of $V$. As $I$ is infinite, we can find $I_1, I_2 \subset I$ such that $I = I_1 \sqcup I_2$ and that there exists a bijection between $I_1$ and $I_2$. Take $V_r = \overline{\bigoplus_{i \in I_r} \mathbb{C}e_i}$, for $r = 1, 2$.)

Choose isomorphisms $U_1 : V_1 \xrightarrow{\sim} V_2$ and $U_2 : V_2 \xrightarrow{\sim} V_1$. Let $T_1 \in \mathrm{End}(V)$ be defined by $T_1(v+w) = U_1(v)$ if $v \in V_1$ and $w \in V_2$, and $T_2 \in \mathrm{End}(V)$ be defined by $T_2(v+w) = U_2(w)$ if $v \in V_1$ and $w \in V_2$. Then $T_1^2 = T_2^2 = 0$, so $\varphi(T_1) = \varphi(T_2) = 0$, and also $\varphi(T_1 + T_2) = 0$. But $T := T_1 + T_2$ is an automorphism of $V$, so, for every $T' \in \mathrm{End}(V)$, we have $T' = T(T^{-1}T')$, hence $\varphi(T') = \varphi(T)\varphi(T^{-1}T') = 0$.

$\square$

**Exercise II.5.2.** Let $V$ be a finite-dimensional Hilbert space. The goal of this problem is to relate the spectral theorem of the notes (theorem II.4.1) with the usual finite-dimensional spectral theorem (which says that a normal endomorphism of $V$ is diagonalizable in an orthonormal basis).

Remember that, if $R$ is a commutative ring, we say that $x \in R$ is *nilpotent* if there exists an integer $n \geq 1$ such that $x^n = 0$, and we say that $R$ is *reduced* if the only nilpotent element of $R$ is $0$.

(a). Show that the usual finite-dimensional spectral theorem (as stated above) implies theorem II.4.1 for $V$.

(b). Let $T \in \mathrm{End}(V)$, and let $A$ be the unital subalgebra of $\mathrm{End}(V)$ generated by $T$ (i.e. the space of polynomials in $T$). Show that $T$ is diagonalizable if and only if $A$ is reduced.

(c). Let $A$ be a commutative unital subalgebra of $\mathrm{End}(V)$. If $A$ is reduced, show that there exist subspaces $V_1, \dots, V_r$ of $V$, uniquely determined up to ordering, such that $V = \bigoplus_{i=1}^r V_i$ and that

$$A = \{T \in \mathrm{End}(V) | \forall i \in \{1, \dots, r\},\ T(V_i) \subset V_i \text{ and } T_{|V_i} \in \mathbb{C} \cdot \mathrm{id}_{V_i}\}.$$

(d). Let $A$ be as in question (c). Show that $A$ is stable by the map $T \longmapsto T^*$ if and only the $V_i$ are pairwise orthogonal.

(e). Show that theorem II.4.1 implies the usual finite-dimensional spectral theorem (as stated above).

*Solution.*

(a). Let $T \in \mathrm{End}(V)$ be a normal endomorphism. By the finite-dimensional spectral theorem, we can find an orthonormal basis $(e_1, \dots, e_n)$ of $V$ and $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ such that $T(e_i) = \lambda_i e_i$ for every $i \in \{1, \dots, n\}$. As the basis is orthonormal, we also have $T^*(e_i) = \overline{\lambda}_i e_i$ for every $i \in \{1, \dots, n\}$. After rearranging the $e_i$, we may also assume that we have $1 \leq n_0 \leq \ldots \leq n_r = n+1$ such that $\lambda_i = \lambda_j$ if there exists $s \in \{0, \dots, r-1\}$ with $n_s \leq i, j \leq n_{s+1} - 1$ and $\lambda_i \neq \lambda_j$ otherwise.

In particular, we may assume that $V = \mathbb{C}^n$ and that $T$ is the diagonal matrix with diagonal entries $\lambda_1, \dots, \lambda_n$, with the same conditions on the $\lambda_i$. I claim that $A_T$ is the subalgebra of diagonal matrices in $M_n(\mathbb{C})$ with diagonal entries $x_1, \dots, x_n$ satisfying : $x_i = x_j$ if there exists $s \in \{0, \ldots, r-1\}$ with $n_s \leq i, j \leq n_{s+1} - 1$. First, this does define a subalgebra of $M_n(\mathbb{C})$. It is also clear that every matrix in $A_T$ is of this form, because $A_T$ is generated (as an algebra) by $I_n$, $T$ and $T^*$, and all three of these matrices satisfy the condition defining $A_T$. Finally, let $X \in A_T$, and let $x_1, \ldots, x_n$ be its diagonal entries. By Lagrange interpolation, there exists a polynomial $P \in \mathbb{C}[t]$ such that $P(\lambda_{n_s}) = x_{n_s}$ for $s \in \{0, \ldots, r-1\}$, and then $P(T)$ is the diagonal matrix with entries $x_1, \ldots, x_n$, i.e. $X$.

(b). Let $P \in \mathbb{C}[t]$ be the minimal polynomial of $T$. Then $\mathbb{C}[t] \to M_n(\mathbb{C})$, $f(t) \longmapsto f(T)$ is a morphism of $\mathbb{C}$-algebra with image $A$ and kernel the ideal generated by $P$, by definition of the minimal polynomial. So $A \simeq \mathbb{C}[t]/(P)$. If we write $P(t) = \prod_{i=}^{r}(t - a_i)^{n_i}$ with $a_1, \ldots, a_r \in \mathbb{C}$ pairwise distinct and $n_1, \ldots, n_r \geq 1$, then, by the Chinese remainder theorem, $A \simeq \prod_{i=1}^{n} \mathbb{C}[t]/(t - a_i)^{n_i}$. So $A$ is reduced if and only if all the $n_i$ are equal to $1$, i.e., if and only if $P$ has only simple roots, which is equivalent to the fact that $T$ is diagonalizable.

(c). if $T \in A$, then the unital subalgebra of $\mathrm{End}(V)$ generated by $T$ is contained in $A$, and in particular it is reduced; by question (b), this implies that $T$ is diagonalizable. As $A$ by a finite number of elements (because it is a finite-dimensional $\mathbb{C}$-vector space), and these are diagonalizable and commute with each other, we can find a basis $(e_1, \ldots, e_n)$ in which every element of $A$ is diagonal. For $i \in \{1, \ldots, n\}$, define $\varphi_i : A \to \mathbb{C}$ by $T(e_i) = \varphi_i(T)e_i$, for $T \in A$. Then $\varphi_1, \ldots, \varphi_n$ are multiplicative functionals on $A$. After reordering the $e_i$, we may assume that we have $1 \leq n_0 \leq \ldots \leq n_r = n + 1$ such that $\varphi_i = \varphi_j$ if there exists $s \in \{0, \ldots, r-1\}$ with $n_s \leq i, j \leq n_{s+1} - 1$ and $\varphi_i \neq \varphi_j$ otherwise.

Note that all the $\varphi_i$ are nonzero (because they send $I_n$ to 1), so they are surjective. I claim that $\varphi_{n_0}, \varphi_{n_1} \ldots, \varphi_{n_{r-1}}$ are linearly independent (as function $A \to \mathbb{C}$). This is a classical result, but let's prove it quickly. Suppose that it is not true, and choose a nontrivial relation of linear dependence $\sum_{i=0}^{r-1} a_i \varphi_{n_i} = 0$, with $a_i \in \mathbb{C}$, such that the number of nonzero $a_i$ is minimal. There are at least two nonzero $a_i$, so, up to reordering, we may assume that $a_0, a_1 \neq 0$. Choose $x_0 \in A$ such that $\varphi_{n_1}(x_0) \neq \varphi_{n_1}(x_0)$. Then, for every $x \in A$,

$$0 = \varphi_{n_0}(x_0) \sum_{i=0}^{r-1} a_i \varphi_{n_i}(x) - \sum_{i=0}^{r-1} a_i \varphi_{n_i}(x_0 x) = \sum_{i=1}^{r-1} a_i (\varphi_{n_0}(x_0) - \varphi_{n_i}(x_0)) \varphi_{n_i}(x).$$

So $\sum_{i=1}^{r-1} a_i(\varphi_{n_0}(x_0) - \varphi_{n_i}(x_0))\varphi_{n_i} = 0$, with $a_1(\varphi_{n_1}(x_0) - \varphi_{n_1}(x_0)) \neq 0$. So we have another nontrivial relation of linear dependence among the $\varphi_{n_i}$, and it has fewer nonzero coefficients than the first one, which is a contradiction.

Now that we know that $\varphi_{n_0}, \varphi_{n_1} \ldots, \varphi_{n_{r-1}}$ are linearly independent, we also know that $(\varphi_{n_0}, \varphi_{n_1} \ldots, \varphi_{n_{r-1}}) : A \to \mathbb{C}^r$ is surjective. For $i \in \{1, \ldots, r\}$, let $V_i = \mathrm{Span}(e_{n_{i-1}}, \ldots, e_{-1+n_i}) \subset V$. Then, if $T$ is in $A$, $T$ acts as a multiple of $\mathrm{id}$ on each $V_i$, and the surjectivity of $(\varphi_{n_0}, \varphi_{n_1} \ldots, \varphi_{n_{r-1}}) : A \to \mathbb{C}^r$ implies that the converse is true. (If $(a_1, \ldots, a_r) \in \mathbb{C}^r$, choose $T \in A$ such that $\varphi_{n_i} = a_{i+1}$ for $0 \leq i \leq r-1$. Then $T$ acts on each $V_i$ by multiplication by $\varphi_{n_{i+1}}(T) = a_i$).

Finally, let's show that $V_1, \ldots, V_r$ are uniquely determined. Let $V = V_1' \oplus \ldots \oplus V_s'$ be another decomposition satisfying the same property. Choose $a_1, \dots, a_r \in \mathbb{C}$ pairwise distinct, and let $T \in A$ such that $T_{|V_i} = a_i \mathrm{id}_{V_i}$ for every $i$. Then $V_1, \dots, V_r$ are the eigenspaces of $T$, and $T$ acts by a multiple of identity on each $V'_j$, so we must have a partition $I_1, \dots, I_s$ of $\{1, \dots, r\}$ such that $V'_j = \bigoplus_{i \in I_j} V_i$ for every $j \in \{1, \dots, s\}$. But the roles of the $V_i$ and the $V'_j$ are symmetric, so we have a similar property with $V_i$ and $V'_j$ exchanged. This implies that $r = s$ and that $V'_1, \dots, V'_r$ are equal to $V_1, \dots, V_r$ up to reordering.

(d). For $i \in \{1, \dots, r\}$, we define a linear endomorphism $\pi_i : V \to V$ by $\pi_i(v_1 \dots + v_r) = v_i$ if $v_j \in V_j$ for $j \in \{1, \dots, r\}$. Then $\mathrm{Im}(\pi_i) = V_i$, $\mathrm{Ker}(\pi_i) = \bigoplus_{j \neq i} V_j$ and $\pi_1 + \dots + \pi_r = \mathrm{id}_V$. Note that $A$ is exactly the subalgebra $\{\sum_{i=1}^r \lambda_i \pi_i,\ \lambda_1, \dots, \lambda_r \in \mathbb{C}\}$ of $\mathrm{End}(T)$.

If $V_1, \dots, V_r$ are pairwise orthogonal, then $\pi_1, \dots, \pi_r$ are orthogonal projections, so they are self-adjoint, and so $A$ is stable by $T \longmapsto T^*$.

Conversely, suppose that $A$ is stable by $T \longmapsto T^*$. If $v \in V$ and $w \in V_1^\perp$, then

$$0 = \langle \pi_1(v), w \rangle = \langle v, \pi_1^*(w) \rangle.$$

This implies that $V_1^\perp \subset \mathrm{Ker}(\pi_1^*)$. As $\mathrm{rk}(\pi_1^*) = \mathrm{rk}(\pi_1) = \dim(V_1)$, we actually have $\mathrm{Ker}(\pi_1^*) = V_1^\perp$. But $\pi_1^* \in A$, so every eigenspace of $\pi_1^*$ is a sum of $V_i$'s, so there exists $I \subset \{1, \dots, r\}$ such that $\mathrm{Ker}(\pi_1^*) = \bigoplus_{i \in I} V_i$. As $V_1^\perp \cap V_1 = \{0\}$, the set $I$ cannot contain $1$. But then the only way that $\ker(\pi_1^*)$ can have dimension $\dim(V) - n_1$ is if $I = \{2, \dots, r\}$. Finally, we have shown that

$$V_1^\perp = \mathrm{Ker}(\pi_1^*) = V_2 \oplus \dots \oplus V_r.$$

Repeating this procedure with the other $\pi_i$'s, we see that, for every $i \in \{a, \dots, r\}$,

$$V_i^\perp = \bigoplus_{j \neq i} V_j.$$

(e). Let $T \in \mathrm{End}(V)$, and let $\Phi : \mathscr{C}(\sigma(T)) \xrightarrow{\sim} A_T$ be as in theorem II.4.1. In particular, $A_T$ is a commutative reduced subalgebra of $\mathrm{End}(V)$ (because $\mathscr{C}(\sigma(T))$ is reduced), and it is stable by $*$ (by definition), so, by (c) and (d), we have a decomposition $V = V_1 \oplus \dots \oplus V_r$ of $V$ into pairwise orthogonal subspaces such that every element of $A_T$ preserves this decomposition and acts as a scalar on each $V_i$. If we choose an orthonormal basis for each $V_i$ and put these together, we'll get an orthonormal basis on $V$ in which each element of $A_T$ is diagonal. Now just remember that $T \in A_T$.

□

**Exercise II.5.3.** This problem is meant to be solved without any of the results of sections and II.3 and II.4. [3]

[3] Compare Nullstellensatz.

Let $X$ be a locally compact Hausdorff topological space. Let $\overline{X}$ be the Alexandroff compactification of $X$. This means that $\overline{X} = X \cup \{\infty\}$, and that the open sets of $\overline{X}$ are the open subsets and the sets of the form $(X - K) \cup \{\infty\}$, where $K$ is a compact subset of $X$.

(a). Show that $\overline{X}$ is a compact Hausdorff topological space, that $X$ is open in $\overline{X}$, and that $X$ is dense in $\overline{X}$ if and only if $X$ is not compact.

(b). Show that $\mathscr{C}(\overline{X})$ is isomorphic to the Banach $*$-algebra that you get by adjoining a unit to $\mathscr{C}_0(X)$. (Don't forget to compare the topologies.)

(c). If $X$ is compact, show that every proper ideal of $\mathscr{C}(X)$ is contained in one of the ideals $\mathfrak{m}_x = \{f \in \mathscr{C}(X) | f(x) = 0\}$, $x \in X$.

(d). In general, show that the map $X \to \sigma(\mathscr{C}_0(X))$, $x \longmapsto (\varphi_x : f \longmapsto f(x))$ is a homeomorphism.

Let $A$ be a commutative Banach algebra. If $I$ is an ideal of $A$, we set

$$V(I) = \{x \in \sigma(A) | \forall f \in A, \widehat{f}(x) = 0\}.$$

If $N$ is a subset of $\sigma(A)$, we set

$$I(N) = \{f \in A | \forall x \in N, \widehat{f}(x) = 0\}.$$

(a). Suppose that $X$ is compact. Show that, for every closed ideal $I$ of $\mathscr{C}(X)$ and every closed subset $N$ of $\sigma(\mathscr{C}(X)) \simeq X$, we have

$$I(V(I)) = I \text{ and } V(I(N)) = N.$$

*Remark.* The result is still true without the assumption that $X$ is compact (use $\mathscr{C}_0(X)$ everywhere).

*Solution.*

(a). First we show that the definition does give a topology on $\overline{X}$. Let $(U_i)_{i \in I}$ be a family of open subsets of $\overline{X}$. Then we can write $I = I' \sqcup I''$, with $U_i \subset X$ open and $i \in I'$ and $U_i = \overline{X} - K_i$ with $K_i$ compact if $i \in I''$. We have

$$\bigcup_{i \in I} U_i = \left(\bigcup_{i \in I'} U_i\right) \cup \left(\overline{X} - \bigcap_{i \in I''} K_i\right).$$

If $I''$ is empty, this is an open subset of $X$, hence an open subset of $\overline{X}$. Otherwise, this is the complement on the compact subset $\bigcap_{i \in I''} K_i - \bigcup_{i \in I'} U_i$ of $X$, so it is again an open subset of $\overline{X}$. On the other hand, we have

$$\bigcap_{i \in I} U_i = \left(\bigcap_{i \in I'} U_i\right) \cap \left(\overline{X} - \bigcup_{i \in I''} K_i\right).$$

Suppose that $I$ is finite. Then, if $I'' = \varnothing$, the set $\bigcap_{i \in I} U_i$ is the open subset $\bigcap_{i \in I'} U_i$ of $X$, hence it is an open subset of $\overline{X}$. Otherwise, it is the complement of the compact subset $\bigcup_{i \in I''} K_i - \bigcap_{i \in I'} U_i$ of $X$, hence it is again an open subset of $\overline{X}$.

Let's show that $\overline{X}$ is Hausdorff. Let $x, y \in \overline{X}$ such that $x \neq y$. We want to find disjoint open neighborhoods of $x$ and $y$. If $x, y \in X$, then there exists open subsets $U$ and $V$ of $X$ such that $x \in U$, $y \in V$ and $U \cap V = \varnothing$. These sets are still open in $\overline{X}$, so we are done. If one of $x$ or $y$ is $\infty$, we may assume that it is $x$. As $X$ is locally compact, we can find a compact subset $K$ of $X$ and an open subset $V$ of $X$ such that $y \in V \subset K$. Then $U := \overline{X} - K$ is an open subset of $\overline{X}$ containing $x = \infty$, and we have $U \cap V = \varnothing$.

Let's show that $\overline{X}$ is compact. Let $(U_i)_{i \in I}$ be a family of open subsets of $\overline{X}$ such that $\overline{X} = \bigcup_{i \in I} U_i$. Let $i_0 \in I$ be such that $\infty \in U_{i_0}$, and write $K = \overline{X} - U_{i_0}$. This is a compact subset of $X$, and it is covered by the open subsets $U_i \cap X$, $i \in I - \{i_0\}$. So there exists a finite subset $J$ of $I - \{i_0\}$ such that $K \subset \bigcup_{i \in J} U_i$, and then we have $\overline{X} = \bigcup_{i \in J \cup \{i_0\}} U_i$.

The set $X$ is open in $\overline{X}$ by definition of the topology of $\overline{X}$.

Suppose that $X$ is not compact. Then, if $U$ is an open neighborhood of $\infty$ in $\overline{X}$, the compact subset $\overline{X} - U$ of $X$ cannot be equal to $X$, which means that $U \cap X \neq \varnothing$. So $\infty$ is in the closure of $X$ in $\overline{X}$. Conversely, suppose that $X$ is compact. Then $\{\infty\} = \overline{X} - X$ is an open subset of $\overline{X}$, so $\infty$ is an isolated point of $\overline{X}$.

(b). Let $A$ be the Banach $*$-algebra that you get by adjoining a unit to $\mathscr{C}_0(X)$. We have $A = \mathscr{C}_0(X) \oplus \mathbb{C}e$, with $\|f + \lambda e\| = \|f\|_\infty + |\lambda|$ and $(f + \lambda e)^* = \overline{f} + \overline{\lambda} e$ (for $f \in \mathscr{C}_0(X)$ and $\lambda \in \mathbb{C}$).

Note that we can extend every $f \in \mathscr{C}_0(X)$ to a continuous function $f$ on $\overline{X}$ by setting $f(\infty) = 0$. (The condition that $f$ is 0 at infinity exactly says that the extended function is continuous, by definition of the topology on $\overline{X}$.) This gives an injective $\mathbb{C}$-algebra map $\mathscr{C}_0(X) \to \mathscr{C}(\overline{X})$. So we get a map $\alpha : A \to \mathscr{C}(\overline{X})$ sending $f + \lambda e$ to $f + \lambda$, where the second "$\lambda$" is the constant function on $\overline{X}$. This $\alpha$ is a morphism of $\mathbb{C}$-algebras by definition of the multiplication on $A$, and it is a $*$-homomorphism by definition of $*$ on $A$. Also, $\alpha$ is bounded, because, if $f \in \mathscr{C}_0(X)$ and $\lambda \in \mathbb{C}$, we have

$$\|f + \lambda\|_\infty \leq \|f\|_\infty + |\lambda| = \|f + \lambda e\|.$$

Finally, note that $\alpha$ is surjective, because it has an inverse sending $f \in \mathscr{C}(\overline{X})$ to $(f_{|X} - \lambda) + \lambda e$. By the open mapping theorem (also known as the Banach-Schauder theorem), the inverse of $\alpha$ is also bounded, so $\alpha$ is a homeomorphism.

(c). Let $I$ be an ideal of $\mathscr{C}(X)$, and suppose that $I$ is not contained in any $\mathfrak{m}_x$. Then, for every $x \in X$, we can find $f_x \in I$ such that $f_x(x) \neq 0$; as $f_x$ is continuous, we can also find an open neighborhood $U_x$ of $x$ such that $f_x(y) \neq 0$ for every $y \in U_x$. We have $X = \bigcup_{x \in X} U_x$ and $X$ is compact, so there exist $x_1, \ldots, x_n \in X$ such that $X = \bigcup_{i=1}^n U_{x_i}$. Let $f = \sum_{i=1}^n |f_{x_i}|^2 = \sum_{i=1}^n \overline{f_{x_i}} f_{x_i}$. Then $f \in I$ because $I$ is an ideal, and $f$ doesn't vanish on $X$; indeed, if $x \in X$, we can find $i \in \{1, \ldots, x\}$ such that $x \in U_{x_i}$, and then

$f(x) \geq |f_{x_i}(x)|^2 > 0$. So the function $g : x \longmapsto f(x)^{-1}$ exists and is continuous on $X$, and we have $gf = 1$, which implies that $1 \in I$, hence that $I = \mathscr{C}(X)$.

(d). Let's call this map $\alpha$. First we show that $\alpha$ is injective. If $x, y \in X$ are such that $x \neq y$, then there exists $f \in \mathscr{C}_0(X)$ such that $f(x) \neq f(y)$ (by Urysohn's lemma), so $\varphi_x \neq \varphi_y$.

Let's show that $\alpha$ is surjective. Let $\varphi : \mathscr{C}_0(X) \to \mathbb{C}$ be a multiplicative functional. We can extend it to a multiplicative functional $\widetilde{\varphi}$ on $\mathscr{C}_0(X)_e$, and we have seen in (b) that $\mathscr{C}_0(X)_e$ is isomorphic to $\mathscr{C}(\overline{X})$. Let $I = \mathrm{Ker}(\widetilde{\varphi})$. This is a maximal ideal of $\mathscr{C}(\overline{X})$, hence, by (c), there exists $x \in X$ such that $I \subset \mathfrak{m}_x$, and we must have $I = \mathfrak{m}_x$ because $I$ is maximal. Also, note that the isomorphism $\mathscr{C}_0(X)_e \simeq \mathscr{C}(\overline{X})$ constructed in (b) identities $\mathscr{C}_0(X)$ to $\mathfrak{m}_\infty$. Hence, as $\varphi$ is not 0 on $\mathscr{C}_0(X)$,w e cannot have $x = \infty$, so $x \in X$, and we have $\mathrm{Ker}(\varphi) = \{f \in \mathscr{C}_0(X) | f(x) = 0\} = \mathrm{Ker}(\varphi_x)$. As in the proof of theorem II.2.10, this easily implies that $\varphi = \varphi_x$.

The map $\alpha$ is continuous by definition of the topology on $\sigma(\mathscr{C}_0(X))$. If $X$ is compact, this implies that $\alpha$ is a homeomorphism. In general, the analogue of $\alpha$ for the Alexandroff compactification $\overline{X}$ of $X$ is a homeomorphism because $\overline{X}$ is compact, and its restriction to $X$ is $\alpha$ (if we identify $\mathscr{C}_0(X)$ to a subalgebra of $\mathscr{C}(\overline{X})$ as in (b)), so $\alpha$ is open, and we are done.

(e). Note that, if $N$ is a closed subset of $X$, then $I(N) = \bigcap_{x \in N} \mathfrak{m}_x$, so $I(N)$ is an ideal of $\mathscr{C}(X)$.

Let $I$ be a closed ideal of $\mathscr{C}(X)$, and let $N = N(I)$. For every $x \in N$ and every $f \in I$, we have $f(x) = 0$ by definition of $N(I)$. So $I \subset \bigcap_{x \in N} \mathfrak{m}_x = I(N)$. Conversely, let $f \in \bigcap_{x \in N} \mathfrak{m}_x$; we want to show that $f \in I$. By assumption, $f(x) = 0$ for every $x \in N$, so $\mathrm{supp}(f) \cap N = \varnothing$. For every $y \in \mathrm{supp}(f)$, choose $f_y \in I$ such that $f_y(y) \neq 0$; as $f_y$ is continuous, we can find an open subset $U_y \ni y$ of $X$ such that $f_y(z) \neq 0$ for every $z \in U_y$. We have $\mathrm{supp}(f) \subset \bigcup_{y \in \mathrm{supp}(f)} U_y$ and $\mathrm{supp}(f)$ is compact, so we can find $y_1, \ldots, y_n \in \mathrm{supp}(f)$ such that $\mathrm{supp}(f) \subset \bigcup_{i=1}^n U_{y_i}$. Let $g = \sum_{i=1}^n |f_{y_i}|^2$. Then $g \in I$, and $g(y) > 0$ for every $y \in \mathrm{supp}(f)$. Define a function $h : X \to \mathbb{C}$ by

$$h(x) = \begin{cases} f(x)g(x)^{-1} & \text{if } x \in \mathrm{supp}(f) \\ 0 & \text{otherwise.} \end{cases}$$

Let $U = \{x \in X | g(x) \neq 0\}$ and $V = X - \mathrm{supp}(f)$. Then $U$ and $V$ are open subsets of $X$ and $X = U \cup V$. On $U$, the function $h$ is equal to $fg^{-1}$, hence continuous; on $V$, it is equal to 0, hence also continuous. So $h \in \mathscr{C}(X)$, and we have $f = gh$ by definition of $h$. As $g \in I$, this shows that $f \in I$, as desired.

Now let $N$ be a closed subset of $X$, and let $I = I(N)$. For every $x \in N$ and every $f \in I$, we have $f(x) = 0$ by definition of $I(N)$, so $N \subset V(I)$. Conversely, if $x \notin N$, then, by Urysohn's lemma, we can find $f \in \mathscr{C}(X)$ such that $f_{|N} = 0$ and $f(x) \neq 0$. Then $f \in I$ by definition of $I(N)$, so $x \notin V(I)$.

□

**Exercise II.5.4.** Consider the Banach $*$-algebra $\ell^1(\mathbb{Z})$ (i.e. $L^1(G)$ for the discrete group $G = \mathbb{Z}$, with the convolution product and the involution defined in class). We write elements of $\ell^1(\mathbb{Z})$ as sequences $a = (a_n)_{n \in \mathbb{Z}}$ in $\mathbb{C}^{\mathbb{Z}}$.

(a). Show that $\ell^1(\mathbb{Z})$ is not a $C^*$-algebra.

(b). Show that there is a homeomorphism $\sigma(\ell^1(\mathbb{Z})) \xrightarrow{\sim} S^1$ such that the Gelfand transform of $a = (a_n)_{n \in \mathbb{Z}}$ is the function $S^1 \to \mathbb{C}$, $e^{i\theta} \longmapsto \sum_{n=-\infty}^{+\infty} a_n e^{in\theta}$. [4]

(c). More generally, if $G$ is a commutative locally compact group, show that the map $\widehat{G} \to \sigma(L^1(G))$ sending $\chi$ to the morphism $L^1(G) \to \mathbb{C}$, $f \longmapsto \int_G f(x)\chi(x)dx$ is a homeomorphism. (Hint : What is the dual of $L^1(G)$ ?)

*Solution.*

(a) Let $a = (a_n)_{n \in \mathbb{Z}}$. Then $a^* = (\overline{a}_{-n})_{n \in \mathbb{Z}}$ (remember that $\mathbb{Z}$ is unimodular, because it is commutative (or because it is discrete)). Let $b = a^* * a$. We have, for every $n \in \mathbb{Z}$,

$$b_n = \sum_{m \in \mathbb{Z}} a^*_m a_{n-m} = \sum_{m \in \mathbb{Z}} \overline{a}_{-m} a_{n-m}.$$

Take $a$ defined by $a_0 = i$, $a_1 = 1$, $a_2 = i$ and $a_n = 0$ for $n \in \mathbb{Z} - \{0, 1, 2\}$. Then $a^*_0 = -i$, $a^*_{-1} = 1$, $a^*_2 = -i$, and $a^*_n = 0$ if $n \in \mathbb{Z} - \{-2, -1, 0\}$. So $b_n = 0$ if $n \notin \{-2, -1, 0, 1, 2\}$, and we have

$$b_{-2} = a^*_{-2} a_0 = 1,$$

$$b_{-1} = a^*_{-1} a_0 + a^*_{-2} a_1 = i - i = 0,$$

$$b_0 = a^*_{-2} a_2 + a^*_{-1} a_1 + a^*_0 a_0 = 3,$$

$$b_1 = a^*_0 a_1 + a^*_{-1} a_2 = -i + i = 0,$$

and

$$b_2 = a^*_0 a_2 = 1.$$

So $|b|_1 = 5 \neq |a|_1^2 = 9$.

(c) Let $G$ be a commutative locally compact group. Let $\varphi \in \sigma(L^1(G))$. We want to show that $\varphi$ comes from an element $\chi$ of $\widehat{G}$. As $\varphi$ is a continuous linear functional on $L^1(G)$, there exists $\chi \in L^\infty(G)$ such that $\varphi(f) = \int_G f(x)\chi(x)dx$ for every $f \in L^1(G)$.

[4] This means that the Gelfand transform is a $*$-homomorphism, i.e. the Banach $*$-algebra $L^1(G)$ is symmetric, even though it is not a $C^*$-algebra.

For every $f, g \in L^1(G)$, we have

$$\begin{aligned}
\varphi(f)\int_G g(y)\chi(y)dy &= \varphi(f)\varphi(g) \\
&= \varphi(g * f) \\
&= \int_{G\times G} g(y)f(y^{-1}x)\chi(x)dxdy \\
&= \int_G g(y)\varphi(L_y f)dy.
\end{aligned}$$

As this is true for every $g \in L^1(G)$, the functions $\varphi(f)\chi$ and $y \longmapsto \varphi(L_y f)$ (both in $L^\infty(G)$ are equal almost everywhere. Hence, if we choose $f \in L^1(G)$ such that $\varphi(f) \neq 0$, we can replace $\chi$ by $y \longmapsto \varphi(f)^{-1}\varphi(L_y f)$. As the functions $\varphi : L^1(G) \to \mathbb{C}$ and $G \to L^1(G)$, $y \longmapsto L_y f$ are continuous (the second by proposition I.3.1.13), this new $\chi$ is continuous. Also, we have $\varphi(g)\chi(y) = \varphi(L_y g)$ for every $g \in L^1(G)$ and every $y \in G$.

Let $x, y \in G$. As $L_{xy}f = L_x(L_y f)$, we have

$$\begin{aligned}
\varphi(L_{xy}f) &= \chi(xy)\varphi(f) \\
&= \chi(x)\varphi(L_y f) \\
&= \chi(x)\chi(y)\varphi(f),
\end{aligned}$$

so $\chi(xy) = \chi(x)\chi(y)$. So $\chi \in \widehat{G}$, and we have shown that the map $\widehat{G} \to \sigma(L^1(G))$ of the problem is surjective. Note that this map is also injective, because a continuous function on $G$ is determined by the linear functional it defines on $L^1(G)$. Also, the topology on $\sigma(L^1(G)) \subset L^\infty(G)$ is the weak* topology by definition, and we have seen in question I.5.4.2(a) that this coincides with the topology on compact convergence on $\widehat{G}$, so the map $\widehat{G} \to \sigma(L^1(G))$ is a homeomorphism.

(b) We know that $\widehat{\mathbb{Z}} \simeq S^1$ by I.5.4.1(d), so we get a homeomorphism $S^1 = \widehat{\mathbb{Z}} \xrightarrow{\sim} \sigma(\ell^1(\mathbb{Z}))$ by question (c). Unpacking the formulas, we see that it sends $z \in S^1$ to the multiplicative functional $a = (a_n)_{n\in\mathbb{Z}} \longmapsto \sum_{n\in\mathbb{Z}} a_n z^n$ on $\ell^1(\mathbb{Z})$, which is exactly what we wanted.

□

**Exercise II.5.5.** Let $A$ be a unital $\mathbb{C}$-algebra with an involutive anti-isomorphism $*$. Show that there is at most one norm on $A$ that makes $A$ into a $C^*$-algebra.

*Solution.* Let $\|.\|$ be a norm on $A$ that makes $A$ into a $C^*$-algebra. Let $x \in A$. Note that $(x^*x)^* = x^*x$, so $x^*x$ is normal. By definition of a $C^*$-algebra and corollary II.3.9, we have

$$\|x\| = \|x^*x\|^{1/2} = \rho(x^*x)^{1/2}.$$

But, by theorem II.1.1.3,

$$\rho(x^*x) = \max\{|\lambda|,\ \lambda \in \mathbb{C},\ x^*x - \lambda e \notin A^\times\}.$$

This last quantity only depends on the algebra structure of $A$ and on $*$, and it determines $\|x\|$.

□

**Exercise II.5.6.** Let $A$ be a $C^*$-algebra. Then $A_e$ is a Banach $*$-algebra, but it is not always a $C^*$-algebra with the norm defined by $\|x + \lambda e\| = \|x\| + |\lambda$. (See question II.5.3 (b) for an example of this phenomenon.)

We define a new norm $\|.\|'$ on $A_e$ by :

$$\|x + \lambda e\|' = \sup\{\|xy + \lambda y\|,\ y \in A,\ \|y\| \leq 1\}.$$

We now suppose that $A$ does *not* have a unit and that $A \neq \{0\}$.

(a). Show that $\|.\|'$ is a submultiplicative norm on $A_e$.

(b). Show that $\|.\|'$ agrees with $\|.\|$ on $A$, that $A$ is closed in $A_e$ and that $A_e$ is complete for $\|.\|'$.

(c). Show that $A_e$ is a $C^*$-algebra for the norm $\|.\|'$.

*Solution.*

(a). Let $x_1 = y_1 + \lambda_1 e$, $x_2 = y_2 + \lambda_2 e$ be elements of $A_e$ ($y_1, y_2 \in A$ and $\lambda_1, \lambda_2 \in \mathbb{C}$) and $c \in \mathbb{C}$. Then

$$\begin{aligned}\|x_1 + x_2\|' &= \sup\{\|y_1 y + \lambda_1 y + y_2 y + \lambda_2 y\|,\ y \in A, \|y\| = 1\}\\ &\leq \sup\{\|y_1 y + \lambda_1 y\|,\ y \in A,\ \|y\| \leq 1\} + \sup\{\|y_2 y + \lambda_2 y\|,\ y \in A,\ \|y\| \leq 1\}\\ &= \|x_1\|' + \|x_2\|',\end{aligned}$$

$$\begin{aligned}\|cx_1\| &= \sup\{\|cy_1 y + c\lambda_1 y\|,\ y \in A,\ \|y\| \leq 1\}\\ &= |c| \sup\{\|y_1 y + \lambda_1 y\|,\ y \in A,\ \|y\| \leq 1\}\\ &= |c|\|x_1\|',\end{aligned}$$

and

$$\begin{aligned}\|x_1 x_2\|' &= \sup\{\|(y_1 y_2 + \lambda_2 y_1 + \lambda_1 y_2)y + \lambda_1\lambda_2 y\|,\ y \in A, \|y\| = 1\}\\ &= \sup\{\|y_1(y_2 y + \lambda_2 y) + \lambda_1(y_2 y + \lambda_2 y)\|,\ y \in A, \|y\| = 1\}\\ &\leq \sup\{\|y_1 + \lambda_1 e\|'\|y_2 y + \lambda_2 y\|,\ y \in A,\ \|y\| \leq 1\}\\ &= \|x_1\|'\|x_2\|'.\end{aligned}$$

To show that $\|.\|'$ is a norm on $A_e$, we still need to show that $\|x + \lambda e\|' \neq 0$ if $x + \lambda e \neq 0$. Suppose that $\|x + \lambda e\|' = 0$, then $xy + \lambda y = 0$ for every $y \in A$ such that $\|y\| = 1$, hence for every $y \in A$. If $x = 0$, then $\lambda = 0$. If $x \neq 0$, then, taking $y = x^*$ (and noting that $xx^* \neq 0$ because $\|xx^*\| = \|x^*\|^2 \neq 0$), we see that $\lambda \neq 0$. Let, so $\lambda^{-1}xy = y$ for every $y \in A$, i.e. $\lambda^{-1}x$ is a left unit for $A$. This implies that $(\lambda^{-1}y)^*$ is a right unit for $A$, so $A$ has a unit, contradicting our assumption. So $x = 0$.

(b). If $x \in A$, then we have

$$\|x\|' = \sup\{\|xy\|,\ y \in A,\ \|y\| = 1\} \leq \|x\|.$$

If $x = 0$, then $\|x\|' = \|x\| = 0$. Otherwise, we also have $x^* \neq 0$; taking $y = \frac{1}{\|x^*\|}x^*$, we get

$$\|x\|' \geq \frac{1}{\|x^*\|}\|xx^*\| = \|x^*\| = \|x\|.$$

Hence $A$ is complete for $\|.\|'$, so it is closed in $A_e$. In particular, the quotient map $A_e \to A_e/A \simeq \mathbb{C}$, $x + \lambda e \longmapsto \lambda$ is continuous.

Now we show that $A_e$ is complete for $\|.\|'$. Let $(x_n + \lambda_n e)_{n\geq 0}$ be a Cauchy sequence in $A_e$, with $x_n \in A$ and $\lambda_n \in \mathbb{C}$. By the previous paragraph, the sequence $(\lambda_n)_{n\geq 0}$ is Cauchy, so the sequence $(x_n)_{n\geq 0}$ in $A$ is also Cauchy. As the two norms coincide on $A$, the sequence $(x_n)_{n\geq 0}$ converges to some $x \in A$, and of course $(\lambda_n)_{n\geq 0}$ converges to some $\lambda \in \mathbb{C}$. It is now clear (using the obvious fact that $\|z + \mu e\|' \leq \|z\| + |\mu|$ for $z \in A$ and $\mu \in \mathbb{C}$) that the sequence $(x_n + \lambda_n e)_{n\geq 0}$ converges to $x + \lambda e$ in $A_e$.

(c). Finally, we show that $A_e$ is a $C^*$-algebra. Let $x \in A$ and $\lambda \in \mathbb{C}$. We want to show that $\|(x + \lambda e)^*(x + \lambda e)\|' = (\|x + \lambda e\|')^2$. We may assume that $x + \lambda e \neq 0$. Let $\varepsilon > 0$. Then we can find $y \in A$ such that $\|y\| = 1$ and

$$\|xy + \lambda y\| \geq \|x + \lambda e\|'(1 - \varepsilon).$$

Note that $xy + \lambda y = (x + \lambda e)y$ (in $A_e$). So

$$\begin{aligned}
(1-\varepsilon)^2(\|x + \lambda e\|')^2 &\leq \|xy + \lambda y\|^2 \\
&= \|(xy + \lambda y)^*(xy + \lambda y)\| \\
&= \|y^*(x + \lambda e)^*(x + \lambda e)y\|' \\
&\leq \|y\|^2\|(x + \lambda e)^*(x + \lambda e)\|' \\
&= \|(x + \lambda e)^*(x + \lambda e)\|'.
\end{aligned}$$

As this is true for every $\varepsilon$, we get

$$\|(x + \lambda e)^*(x + \lambda e)\|' \geq (\|x + \lambda e\|')^2.$$

Using the submultiplicativity of the norm, we deduce that

$$\|x + \lambda e\|' \leq \|(x + \lambda e)^*\|'.$$

As $*$ is bijective on $A_e$, the last inequality is actually an equality, and so we also get

$$(\|x+\lambda e\|')^2 \leq \|(x+\lambda e)^*(x+\lambda e)\|' \leq (\|x+\lambda e\|')^2,$$

which finishes the proof.

$\square$

# III The Gelfand-Raikov theorem

The goal of this chapter is to prove the Gelfand-Raikov theorem, which says that irreducible unitary representations of locally groups separate point (i.e., if $G$ is alocally compact group and $x \in G - \{1\}$, then there exists an irreducible unitary representation of $G$ such that $\pi(x) \neq 1$).

In this chapter, $G$ is a locally compact group and $\mu$ (or just "$dx$") is a left Haar measure on $G$.

## III.1 $L^\infty(G)$

You can safely ignore this section and assume that all groups are $\sigma$-compact.

We will be using $L^\infty(G)$ more seriously in this chapter, and we want it to be the continuous dual of $L^1(G)$, which is not true if $G$ is not $\sigma$-compact. So we change the definition of $L^\infty(G)$ to make it true. See section 2.3 of [11].

More generally, let $X$ be a locally compact Hausdorff topological space and let $\mu$ be a regular Borel measure. We say that $E \subset X$ is *locally Borel* if, for every Borel subset $F$ of $X$ such that $\mu(F) < +\infty$, we have that $E \cap F$ is a Borel subset of $X$. If $E$ is locally Borel, we say that $E$ is *locally null* if, for every Borel subset $F$ of $X$ such that $\mu(F) < +\infty$, we have $\mu(E \cap F) = 0$. We say that an assertion about points of $X$ is true *locally almost everywhere* if it is true outside of a locally null subset. We saw that a function $f : X \to \mathbb{C}$ is *locally measurable* if, for every Borel subset $A$ of $\mathbb{C}$, the set $f^{-1}(A)$ is locally Borel. Now we set $L^\infty(X)$ to be the space of locally measurable functions $X \to \mathbb{C}$ that are bounded locally almost everywhere, modulo the equivalence relation : $f \sim g$ if $f - g = 0$ locally almost everywhere. The norm on $L^\infty(X)$ is given by

$$\|f\|_\infty = \inf\{c \in \mathbb{R}_{\geq 0} | |f(x)| \text{ locally almost everywhere}\}.$$

## III.2 Functions of positive type

**Definition III.2.1.** A *function of positive type* on $G$ is a function $\varphi \in L^\infty(G)$ such that, for every $f \in L^1(G)$, we

$$\int_G (f^* * f)(x)\varphi(x)dx \geq 0.$$

Note that $f^* * f \in L^1(G)$ if $f \in L^1(G)$, so the integral converges.

*Remark* III.2.2. For every $\varphi \in L^\infty(G)$ and every $f, g \in L^1(G)$, we have

$$\begin{aligned}\int_G (f^* * g)(x)\varphi(x)dx &= \int_{G\times G} f^*(y)g(y^{-1}x)\varphi(x)dxdy \\ &= \int_{G\times G} \Delta(y)^{-1}\overline{f(y^{-1})}g(y^{-1}x)\varphi(x)dxdy \\ &= \int_{G\times G} \overline{f(y)}g(yx)\varphi(x)dxdy \\ &= \int_{G\times G} \overline{f(y)}g(x)\varphi(y^{-1}x)dxdy.\end{aligned}$$

**Example III.2.3.** (1) $0$ is a function of positive type.

(2) If $\varphi : G \to S^1 \subset \mathbb{C}$ is a 1-dimensional representation (i.e. $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$), then it is a function of positive type. Indeed, for every $f \in L^1(G)$, we have by remark III.2.2

$$\begin{aligned}\int_G (f^* * f)(x)\varphi(x)dx &= \int_{G\times G} \overline{f(y)}f(yx)\varphi(y^{-1}x)dxdy \\ &= \int_{G\times G} \overline{f(y)}f(x)\overline{\varphi(y)}\varphi(x)dxdy \\ &= \left|\int_G \varphi(x)f(x)dx\right|^2 \geq 0.\end{aligned}$$

We will generalize the second example in point (ii) of the following proposition.

**Proposition III.2.4.** *(i) If $\varphi : G \to \mathbb{C}$ is a function of positive type, then so is $\overline{\varphi}$.*

*(ii) If $(\pi, V)$ is a unitary representation of $G$ and $v \in V$, then $\varphi : G \to \mathbb{C}$, $x \longmapsto \langle \pi(x)(v), v\rangle$ is a continuous function of positive type.*

*(iii) Let $f \in L^2(G)$, and define $\widetilde{f} : G \to \mathbb{C}$ by $\widetilde{f}(x) = \overline{f(x^{-1})}$. Then $f * \widetilde{f}$ makes sense, it is in $L^\infty(G)$, and it is a function of positive type.*

*Proof.* (i) Let $f \in L^1(G)$. Then, by remark III.2.2,

$$\begin{aligned}\int_G (f^* * f)\overline{\varphi}d\mu &= \int_{G\times G} \overline{f(y)}f(yx)\overline{\varphi(x)}dxdy \\ &= \overline{\int_{G\times G} f(y)\overline{f(yx)}\varphi(x)dxdy} \\ &= \overline{\int (\overline{f}^* * \overline{f})\varphi d\mu} \geq 0.\end{aligned}$$

(ii) The function $\varphi$ is continuous because $G \to V$, $x \longmapsto \pi(x)(v)$ is continuous. Let's show that it is of positive type. Note that, for all $x, y \in G$, we have

$$\varphi(y^{-1}x) = \langle \pi(y^{-1}x)(v), v\rangle = \langle \pi(x)(v), \pi(y)(v)\rangle.$$

Let $f \in L^1(G)$. Then, by remark III.2.2,

$$\begin{aligned}\int (f^* * f)\varphi d\mu &= \int_{G\times G} f(x)\overline{f(y)}\varphi(y^{-1}x)dxdy \\ &= \int_{G\times G} \langle f(x)\pi(x)(v), f(y)\pi(y)(v)\rangle dxdy \\ &= \langle \pi(f)(v), \pi(f)(v)\rangle \geq 0.\end{aligned}$$

(iii) Let $x \in G$. Then the integral defining $f * \widetilde{f}(x)$ is

$$\int_G f(y)\overline{f(x^{-1}y)}dy.$$

This integral converges, because both $f$ and $L_x\overline{f} : y \longmapsto \overline{f(x^{-1}y)}$ are in $L^2(G)$ (by left invariance of $\mu$). Also, by the Cauchy-Schwarz inequality, we have

$$|f * \widetilde{f}(x)| \leq \|f\|_2 \|L_x\overline{f}\|_2 = \|f\|_2^2.$$

So $f * \widetilde{f} \in L^\infty(G)$.

Let's show that $f * \widetilde{f}$ is of positive type. Let $\pi_L$ be the left regular representation of $G$, i.e. the unitary representation of $G$ on $L^2(G)$ given by $\pi_L(x) = L_x$. Then, for every $x \in G$, we have

$$\langle \pi_L(x)(f), f\rangle = \int_G f(x^{-1}y)\overline{f(y)}dy = \int_G \overline{\widetilde{f}(y^{-1}x)}\overline{f(y)}dy = \overline{f * \widetilde{f}(x)}.$$

So the result follows from (i) and (ii).

□

The main result of this function is that the example in (ii) above is the only one.

**Theorem III.2.5.** *Let $\varphi : G \to \mathbb{C}$ be a function of positive type. Then there exists a cyclic unitary representation $(\pi, V)$ of $G$ and a cyclic vector $v$ for $V$ such that $\varphi(x) = \langle \pi(x)(v), v\rangle$ locally almost everywhere.*

*Moreover, the representation $\pi$ and the vector $v$ are uniquely determined by $\varphi$, in the following sense : if $(\pi', V')$ is another cyclic unitary representation of $G$ and if $v' \in V'$ is a cyclic vector such that $\varphi(x) = \langle \pi'(x)(v'), v'\rangle$ locally almost everywhere, then there exists a $G$-equivariant isometry $T : V \to V'$ such that $T(v) = v'$.*

In fact, we will give a somewhat explicit construction of $(\pi, V)$ during the proof.

Before proving the theorem, let's see some easy corollaries.

**Corollary III.2.6.** *Let $\varphi : G \to \mathbb{C}$ be a function of positive type. Then $\varphi$ agrees with a continuous function locally almost everywhere, $\|\varphi\|_\infty = \varphi(1)$ and, for every $x \in G$, we have $\varphi(x^{-1}) = \overline{\varphi(x)}$.*

*Proof.* The first statement follows from (ii) of proposition III.2.4. To prove the other statements, choose a cyclic unitary representation $(\pi, V)$ of $G$ and $v \in V$ such that $\varphi(x) = \langle \pi(x)(v), v\rangle$. Then, for every $x \in G$,

$$|\varphi(x)| \leq \|\pi(x)(v)\|\|v\| = \|v\|^2 = \varphi(1)$$

and

$$\varphi(x^{-1}) = \langle \pi(x^{-1})(v), v\rangle = \langle \pi(x)^*(v), v\rangle = \langle v, \pi(x)(v)\rangle = \overline{\varphi(x)}.$$

□

Now we come back to the proof of the theorem. Let $\varphi : G \to \mathbb{C}$ be a function of positive type. Define a Hermitian form $\langle ., .\rangle_\varphi$ on $L^1(G)$ by :

$$\langle f, g\rangle_\varphi = \int (g^* * f)\varphi = \int_{G\times G} f(x)\overline{g(y)}\varphi(y^{-1}x)dxdy$$

(see remark III.2.2). In particular, we clearly have, for all $f, g \in L^1(G)$,

$$|\langle f, g\rangle_\varphi| \leq \|f\|_1\|g\|_1\|\varphi\|_\infty.$$

As $\varphi$ is of positive type, we have $\langle f, f\rangle_\varphi \geq 0$, that is, the Hermitian form we just defined is positive semi-definite; in particular, the Cauchy-Schwarz inequality applies to it, and it gives, for all $f, g \in L^1(G)$,

$$|\langle f, g\rangle_\varphi|^2 \leq \langle f, f\rangle_\varphi \langle g, g\rangle_\varphi.$$

Let $\mathscr{N}$ be the kernel (or radical) of the form $\langle ., .\rangle_\varphi$, that is, the orthogonal of $L^1(G)$, i.e. the space of $f \in L^1(G)$ such that $\langle f, g\rangle_\varphi = 0$ for every $g \in L^1(G)$. By the Cauchy-Schwarz inequality, we have $f \in \mathscr{N}$ if and only if $\langle f, f\rangle_\varphi = 0$. Hence the form $\langle ., .\rangle_\varphi$ defines a positive definite Hermitian form on $L^1(G)/\mathscr{N}$, that we will still denote by $\langle ., .\rangle_\varphi$; we denote the associated norm by $\|.\|_\varphi$. For every $f \in L^1(G)$, we have

$$\|f + \mathscr{N}\|_\varphi^2 \leq \|\varphi\|_\infty \|f\|_1^2.$$

Let $V_\varphi$ be the completion of $L^1(G)/\mathscr{N}$ for the norm $\|.\|_\varphi$; this is a Hilbert space.

We want to construct a unitary action of $G$ on $V_\varphi$. We already have a continuous representation of $G$ on $L^1(G)$, using the operators $L_x$. This will magically give our unitary representation. Note first that, for every $L^1(G)$, the map $G \to L^1(G)$, $x \longmapsto L_x f$ is continuous for the semi-norm $\|.\|_\varphi$ because of the inequality $\|.\|_\varphi \le \|\varphi\|_\infty^{1/2}\|.\|_1$ that we just proved.

Let's prove that $\langle .,.\rangle_\varphi$ is invariant by the action of $G$. Let $x \in G$ and $f, g \in L^1(G)$. Then

$$\begin{aligned}\langle L_x f, L_x g\rangle_\varphi &= \int_{G\times G} f(x^{-1}y)\overline{g(x^{-1}z)}\varphi(z^{-1}y)dydz \\ &= \int_{G\times G} f(y)\overline{g(z)}\varphi((xz)^{-1}(xy))dydz \\ &= \int_{G\times G} f(y)\overline{g(z)}\varphi(z^{-1}y)dydz = \langle f, g\rangle_\varphi.\end{aligned}$$

In particular, the radical $\mathscr{N}$ of the form $\langle .,.\rangle_\varphi$ is a $G$-invariant subspace of $L^1(G)$, so we get an action of $G$ on $L^1(G)/\mathscr{N}$, which preserves the Hermitian inner product and is a continuous representation by proposition I.3.1.10. We extend this action to $V_\varphi$ by continuity. This gives a unitary representation of $G$ on $V_\varphi$, which we will denote by $\pi_\varphi$.

Let $f, g \in L^1(G)$. Then, by example I.4.2.7, we have

$$\pi_\varphi(f)(g + \mathscr{N}) = f * g + \mathscr{N}.$$

The following lemma will imply the first statement of theorem III.2.5.

**Lemma III.2.7.** *There exists a cyclic vector $v = v_\varphi$ for $V_\varphi$ such that :*

*(i) for $f \in L^1(G)$, we have $\pi_\varphi(f)(v) = f + \mathscr{N}$;*

*(ii) we have $\varphi(x) = \langle \pi_\varphi(x)(v), v\rangle_\varphi$ locally almost everywhere on $G$.*

*Proof.* By the calculation of $\pi_\varphi(f)(g + \mathscr{N})$ for $f, g \in L^1(G)$ (see above), we see that $v$ would be the image in $L^1(G)/\mathscr{N}$ of a unit element for $*$ (i.e. a Dirac measure at $1 \in G$), if such a unit element existed. In general, it doesn't, but we can approximate it, and hope that we will get a Cauchy sequence in $L^1(G)/\mathscr{N}$.

So let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity (see definition I.4.1.7). Note that $(\psi_U^*)_{U\in\mathscr{U}}$ is also an approximate identity, so, by proposition I.4.1.9, we have $\psi_U^* * f \xrightarrow[U\to\{1\}]{} f$ in $L^1(G)$ for every $f \in L^1(G)$. So, for every $f \in L^1(G)$, we have

$$\langle f, \psi_U\rangle_\varphi = \int (\psi_U^* * f)\varphi d\mu \xrightarrow[U\to\{1\}]{} \int f\varphi d\mu.$$

Hence $f \longmapsto \int_G f\varphi d\mu$ is a bounded (for $\|.\|_1$ and $\|.\|_\varphi$) linear functional on $L^1(G)$ whose kernel contains $\mathscr{N}$. We can descend this bounded linear functional to $L^1(G)/\mathscr{N}$ and extend it to $V_\varphi$ by continuity, and we get a bounded linear functional on $V_\varphi$, which must be of the form $\langle ., v\rangle_\varphi$ for

some $v \in V_\varphi$ (uniquely determined), because $V_\varphi$ is a Hilbert space. By definition of $v$, we have, for every $f \in L^1(G)$,
$$\langle f + \mathscr{N}, v\rangle_\varphi = \int_G f\varphi d\mu,$$
and this determines $v$ because the image of $L^1(G)$ is dense in $V_\varphi$.

Now we prove properties (i) and (ii). Let $f, g \in L^1(G)$. Then
$$\begin{aligned}
\langle g, f\rangle_\varphi &= \int_G (f^* * g)\varphi d\mu \\
&= \int_{G\times G} g(x)\overline{f(y)}\varphi(y^{-1}x)dxdy \\
&= \int_{G\times G} g(yx)\overline{f(y)}\varphi(x)dxdy \\
&= \int_{G\times G} \overline{f(y)}L_{y^{-1}}g(x)\varphi(x)dxdy \\
&= \int_G \overline{f(y)}\langle \pi_\varphi(y^{-1})(g+\mathscr{N}), v\rangle_\varphi dx \\
&= \int_G \langle g+\mathscr{N}, f(y)\pi_\varphi(y)(v)\rangle_\varphi dx \\
&= \langle g+\mathscr{N}, \pi_\varphi(f)(v)\rangle_\varphi.
\end{aligned}$$
As this is true for every $g \in L^1(G)$ and as the image of $L^1(G)$ is dense in $V_\varphi$, we get $\pi_\varphi(f)(v) = f + \mathscr{N}$. In particular, the span of $\{\pi_\varphi(f)(v),\ f \in L^1(G)\}$ is dense in $V_\varphi$, so $v$ is a cyclic vector (by (iii) of theorem I.4.2.6).

Also, for $f \in L^1(G)$, by what we have just seen :
$$\begin{aligned}
\int_G f(x)\langle \pi_\varphi(x)(v), v\rangle_\varphi dx &= \langle \int_G f(x)\pi_\varphi(x)(v)dx, v\rangle_\varphi \\
&= \langle \pi_\varphi(f)(v), v\rangle_\varphi \\
&= \langle f+\mathscr{N}, v\rangle_\varphi \\
&= \int_G f(x)\varphi(x)dx.
\end{aligned}$$
As this is true for every $f \in L^1(G)$, it implies that $\varphi(x) = \langle \pi_\varphi(x)(v), v\rangle_\varphi$ locally almost everywhere.

□

To finish the proof of theorem III.2.5, we just need to establish the following lemma.

**Lemma III.2.8.** *Let $(\pi, V)$ and $(\pi, V')$ be two cyclic unitary representations of $G$ and $v \in V$, $v' \in V'$ be two cyclic vectors such that, for every $x \in G$, we have*
$$\langle \pi(x)(v), v\rangle = \langle \pi'(x)(v'), v'\rangle.$$

*Then there exists a $G$-equivariant isometry $T : V \to V'$ such that $T(v) = v'$.*

*Proof.* Of course, we want to define $T : V \to V'$ by the formula $T(\pi(x)(v)) = \pi'(x)(v')$, for every $x \in G$. We need to make sense of this. Let $W = \mathrm{Span}\{\pi(x)(v),\ x \in G\}$. By the assumption that $v$ is cyclic, the subspace $W$ is dense in $V$. Let's check that the formula above defines an isometry $T : W \to V'$. Let $x_1, \dots, x_n \in G$ amd $\lambda_1, \dots, \lambda_n \in \mathbb{C}$. Then

$$\begin{aligned}\left\| \sum_{i=1}^n \lambda_i \pi(x_i)(v) \right\|^2 &= \sum_{i=1}^n \sum_{j=1}^n \lambda_i \overline{\lambda}_j \langle \pi(x_j^{-1} x_i)(v), v \rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n \lambda_i \overline{\lambda}_j \langle \pi'(x_j^{-1} x_i)(v'), v' \rangle \\ &= \left\| \sum_{i=1}^n \lambda_i \pi'(x_i)(v') \right\|^2.\end{aligned}$$

In particular, if $\sum_{i=1}^n \lambda_i \pi(x_i)(v) = 0$, then we also have $\sum_{i=1}^n \lambda_i \pi'(x_i)(v') = 0$. So we can define $T : W \to V'$ by $T(\sum_{i=1}^n \lambda_i \pi(x_i)(v)) = \sum_{i=1}^n \lambda_i \pi'(x_i)(v')$, and then the calculation above shows that $T$ is an isometry. Hence $T$ is continuous, and so we can extend to a continuous linear operator $T : V \to V'$, which is still an isometry, hence injective and with closed image. Also, if $x \in G$ and $w \in W$, then we have $T(\pi(x)(w)) = \pi'(x)(T(w))$ by definition of $T$. As $T$ is continuous and $W$ is dense in $V$, this stays true for every $w \in W$; in other words, $T$ is $G$-equivariant. Finally, $T(v) = v'$ by definition of $T$, so the image of $T$ is dense in $V'$, hence equal to $V'$.

□

## III.3 Functions of positive type and irreducible representations

We have seen that cyclic unitary representations of $G$ (together with a fixed cyclic vector) are parametrized by functions of positive type. The next natural question is "which functions of positive type correspond to the irreducible representations ?"

**Definition III.3.1.** We denote by $\mathscr{P}(G)$ or $\mathscr{P}$ the set of continuous functions of positive type on $G$. This is a convex cone in $\mathscr{C}_b(G)$. [1]

Let

$$\mathscr{P}_1 = \{\varphi \in \mathscr{P} | \|\varphi\|_\infty = 1\} = \{\varphi \in \mathscr{P} | \varphi(1) = 1\}$$

and

$$\mathscr{P}_0 = \{\varphi \in \mathscr{P} | \|\varphi\|_\infty \leq 1\} = \{\varphi \in \mathscr{P} | \varphi(1) \leq 1\}.$$

[1] "Cone" means that it is stable by multiplication by elements of $\mathbb{R}_{\geq 0}$.

(Remember that, by corollary III.2.6, we have $\|\varphi\|_\infty = \varphi(1)$ for every $\varphi \in \mathscr{P}$.)

Then $\mathscr{P}_1$ and $\mathscr{P}_0$ are convex subsets of $\mathscr{C}_b(G)$. We denote by $\mathscr{E}(\mathscr{P}_1)$ and $\mathscr{E}(\mathscr{P}_0)$ their sets of extremal points.

**Theorem III.3.2.** *Let $\varphi \in \mathscr{P}_1$. Then the unitary representation $(V_\varphi, \pi_\varphi)$ constructed in the previous section is irreducible if and only if $\varphi \in \mathscr{E}(\mathscr{P}_1)$.*

*Remark* III.3.3. If $\varphi \in \mathscr{P}$ and $c \in \mathbb{R}_{>0}$, then we have $\langle .,. \rangle_{c\varphi} = c\langle .,. \rangle_\varphi$, so $V_{c\varphi} = V_\varphi$, $\pi_{c\varphi} = \pi_\varphi$ and $v_{c\varphi} = v_\varphi$. (But the identity of $V_\varphi$ is not an isometry, because we are using two different inner products, i.e. $\langle .,. \rangle_\varphi$ and $\langle .,. \rangle_{c\varphi}$). As each nonzero $\varphi \in \mathscr{P}$ is a of the form $c\varphi'$ for a unique $\varphi' \in \mathscr{P}_1$ (we have $c = \varphi(1)$), the theorem does answer the question at the beginning of the section.

*Remark* III.3.4. If $G$ is commutative, the theorem says that $\widehat{G} = \mathscr{E}(\mathscr{P}_1)$.

*Proof.* In this proof, we will denote the inner form and norm of $V = V_\varphi$ by $\langle .,. \rangle$ and $\|.\|$, and we will write $\pi = \pi_\varphi$. (Unless this introduces confusion.)

We first suppose that $\pi$ is not irreducible. Let $0 \neq W \subsetneq V$ be a closed $G$-invariant subspace. As $\pi$ is unitary, $W^\perp$ is also $G$-invariant, and we have $V = W \oplus W^\perp$. Let $v \in V$ be the cyclic vector of lemma III.2.7. As $v$ is cyclic, it cannot be contained in $W$ or in $W^\perp$ (otherwise we would have $W = V$ or $W^\perp = V$). So we can write $v = v_1 + v_2$, with $v_1 \in W$, $v_2 \in W^\perp$, and $v_1, v_2 \neq 0$. Define $\varphi_1, \varphi_2 : G \to \mathbb{C}$ by $\varphi_i(x) = \langle \pi(x)(v_i), v_i \rangle$. Then $\varphi_1, \varphi_2 \in \mathscr{P}$ by (ii) of proposition III.2.4, and we have $\varphi = \varphi_1 + \varphi_2$. Let $c_1 = \|v_1\|^2$ and $c_2 = \|v_2\|^2$; we have $c_1 + c_2 = \|v\|^2 = \varphi(1) = 1$ by the Pythagorean theorem, so $c_1, c_2 \in (0,1)$. Let $\psi_i = \frac{1}{c_i}\varphi_i$, for $i = 1,2$. Then $\varphi = c_1\psi_1 + c_2\psi_2$, and $\psi_1, \psi_2 \in \mathscr{P}_1$ (because $\psi_1(1) = \psi_2(1) = 1$). To conclude that $\varphi$ is not an extremal point of $\mathscr{P}_1$, we still need to prove that $\psi_1 \neq \psi_2$, i.e. that $\varphi_2$ is not of the form $c\varphi_1$ for $c \in \mathbb{R}_{>0}$.

Let $c \in \mathbb{R}_{>0}$. Choose $\varepsilon > 0$ such that $\varepsilon < \frac{c\|v_1\|^2}{\|v_2\| + c\|v_1\|}$, i.e. such that $\varepsilon\|v_2\| < c\|v_1\|^2 - \varepsilon c\|v_1\|$. As $v$ is a cyclic vector for $V$, we can find $x_1, \dots, x_n \in G$ and $a_1, \dots, a_n \in \mathbb{C}$ such that

$$\left\| \sum_{i=1}^n a_i \pi(x_i)(v) - v_1 \right\| < \varepsilon.$$

As $v = v_1 + v_2$ with $v_1 \in W$ and $v_2 \in W^\perp$, and as both $W$ and $W^\perp$ are stable by the action of $G$, we have, for $x \in G$,

$$\langle \pi(x)(v), v_1 \rangle = \langle \pi(x)(v_1) + \pi(x)(v_2), v_1 \rangle = \langle \pi(x)(v_1), v_1 \rangle.$$

Hence

$$
\begin{aligned}
\left|\sum_{i=1}^{n} a_i\langle\pi(x_i)(v_1), v_1\rangle - \langle v_1, v_1\rangle\right| &= \left|\sum_{i=1}^{n} a_i\langle\pi(x_i)(v), v_1\rangle - \langle v_1, v_1\rangle\right| \\
&= \left|\langle\sum_{i=1}^{n} a_i\pi(x_i)(v) - v_1, v_1\rangle\rangle\right| \\
&< \varepsilon\|v_1\|,
\end{aligned}
$$

which implies that

$$
\|v_1\|^2 - \varepsilon\|v_1\| < \left|\sum_{i=1}^{n} a_i\langle\pi(x_i)(v_1), v_1\rangle\right| = \left|\sum_{i=1}^{n} a_i\varphi_1(x_i)\right|.
$$

On the other hand (using the fact that $\langle\pi(x)(v), v_2\rangle = \langle\pi(x)(v_2), v_2\rangle$ for every $x \in G$), we have

$$
\begin{aligned}
\left|\sum_{i=1}^{n} a_i\langle\pi(x_i)(v_2), v_2\rangle\right| &= \left|\sum_{i=1}^{n} a_i\langle\pi(x_i)(v), v_2\rangle - \langle v_1, v_2\rangle\right| \\
&= \left|\langle\sum_{i=1}^{n} a_i\pi(x_i)(v) - v_1, v_2\rangle\right| \\
&\leq \left\|\sum_{i=1}^{n} a_i\pi(x_i)(v) - v_1\right\| \|v_2\| \\
&< \varepsilon\|v_2\| \\
&< c\|v_1\|^2 - \varepsilon c\|v_1\| \\
&< c\left|\sum_{i=1}^{n} a_i\varphi_1(x_i)\right|
\end{aligned}
$$

i.e.

$$
\left|\sum_{i=1}^{n} a_i\varphi_2(x_i)\right| < c\left|\sum_{i=1}^{n} a_i\varphi_1(x_i)\right|.
$$

So we cannot have $\varphi_2 = c\varphi_1$. As $c$ was arbitrary, this finishes the proof that $\psi_1 \neq \psi_2$, hence that $\varphi$ is not an extremal point of $\mathscr{P}_1$.

Conversely, we want to show that $\varphi$ is extremal in $\mathscr{P}_1$ if $\pi_\varphi$ is irreducible. Suppose that $\varphi = \varphi_1 + \varphi_2$, with $\varphi_1, \varphi_2 \in \mathscr{P}$. For every $f \in L^1(G)$, we have

$$
\langle f, f\rangle_{\varphi_1} = \langle f, f\rangle_\varphi - \langle f, f\rangle_{\varphi_2} \leq \langle f, f\rangle_\varphi.
$$

In particular, the kernel of $\langle ., \rangle_\varphi$ is contained in the kernel of $\langle ., .\rangle_{\varphi_1}$, so the identity of $L^1(G)$ extends to a continuous surjective map $T : V_\varphi \to V_{\varphi_1}$, and that map is $G$-equivariant because the action of $G$ on both $V_\varphi$ and $V_{\varphi_1}$ comes from its action on $L^1(G)$ by left translations. Also, as $v_\varphi$

(resp. $v_{\varphi_1}$) is just the limit in $V_\varphi$ (resp. $V_{\varphi_1}$) of the image of an approximate identity, the operator $T$ sends $v_\varphi$ to $v_{\varphi_1}$. As $\operatorname{Ker} T$ is a $G$-invariant subspace of $V_\varphi$, so is $(\operatorname{Ker} T)^\perp$, so $T$ defines a $G$-equivariant isomorphism $(\operatorname{Ker} T)^\perp \overset{\sim}{\to} V_{\varphi_1}$, so $V_{\varphi_1}$ is isomorphic to a subrepresentation of $V_\varphi$.

Now suppose that $\pi_\varphi$ is irreducible. Then $T^*T \in \operatorname{End}(V_\varphi)$ is $G$-equivariant, so it is equal to $c\mathrm{id}_{V_\varphi}$ for some $c \in \mathbb{C}$ by Schur's lemma (theorem I.3.4.1). As $T(v_\varphi) = v_{\varphi_1}$, for every $x \in G$, we have

$$\begin{aligned}
\varphi_1(x) &= \langle \pi_{\varphi_1}(x)(v_{\varphi_1}), v_{\varphi_1}\rangle_{\varphi_1} \\
&= \langle \pi_{\varphi_1}(x)(T(v_\varphi)), T(v_\varphi)\rangle_{\varphi_1} \\
&= \langle T(\pi_\varphi(x)(v_\varphi)), T(v_\varphi)\rangle_{\varphi_1} \\
&= \langle T^*T(\pi_\varphi(x)(v_\varphi)), v_\varphi\rangle_{\varphi} \\
&= c\varphi(x).
\end{aligned}$$

As $\varphi_1$ and $\varphi$ are of positive type, we must have $c \in \mathbb{R}_{\geq 0}$. We see similarly that $\varphi_2$ must be in $\mathbb{R}_{\geq 0}\varphi$. So $\varphi$ is extremal.

□

## III.4 The convex set $\mathscr{P}_1$

We have seen in the previous two sections that irreducible unitary representations of $G$ are parametrized by extremal points of $\mathscr{P}_1$. Remember that we are trying to show that there enough irreducible unitary representations to separate points on $G$. So we want to show that $\mathscr{P}_1$ has a lot of extremal points. A natural ideal is to use the Krein-Milman theorem (theorem B.5.2, that says that a compact convex set is the closed convex hull of its extremal points), but $\mathscr{P}_1$ is not compact in general. However, the set $\mathscr{P}_0$ is convex and weak* compact and closely related to $\mathscr{P}_1$; this will be enough to extend the conclusion of the Krein-Milman theorem to $\mathscr{P}_1$.

Remember that $\mathscr{P}$ is a subset of $L^\infty(G)$. We identify $L^\infty(G)$ with the continuous dual of $L^1(G)$ and consider the weak* topology on it and on its subsets $\mathscr{P}$, $\mathscr{P}_0$ and $\mathscr{P}_1$. For $f \in L^\infty(G)$, a basis of neighborhoods of $f$ is given by the sets $U_{g_1,\dots,g_n,c} = \{f' \in L^\infty(G) | |\int_G (f-f')g_i d\mu| < c,\ 1 \leq i \leq n\}$, for $n \in \mathbb{Z}_{\geq 1}$, $g_1,\dots,g_n \in L^1(G)$ and $c > 0$. The second main result of this section is that the weak* topology coincides with the topology of compact convergence on $\mathscr{P}_1$.

**Theorem III.4.1.** *The convex hull of $\mathscr{E}(\mathscr{P}_1)$ is dense in $\mathscr{P}_1$ for the weak* topology.*

**Lemma III.4.2.** *We have $\mathscr{E}(\mathscr{P}_0) = \mathscr{E}(\mathscr{P}_1) \cup \{0\}$.*

*Proof.* First we show that every point of $\mathscr{E}(\mathscr{P}_1) \cup \{0\}$ is extremal in $\mathscr{P}_0$. Let $\varphi_1, \varphi_2 \in \mathscr{P}_0$ and $c_1, c_2 \in (0,1)$ such that $c_1 + c_2 = 1$. If $c_1\varphi_1 + c_2\varphi_2 = 0$, then $0 = c_1\varphi_1(1) + c_2\varphi_2(1)$, so $\varphi_1(1) = \varphi_2(1) = 0$, so $\|\varphi_1\|_\infty = \|\varphi_2\|_\infty = 0$, i.e. $\varphi_1 = \varphi_2 = 0$. This shows that 0 is extremal. Suppose that $\varphi := c_1\varphi_1 + c_2\varphi_2 \in \mathscr{E}(\mathscr{P}_1)$. Then $1 = \varphi(1) = c_1\varphi(1) + \varphi_2(1)$, so $\varphi_1(1) = \varphi_2(1) = 1$, so $\varphi_1, \varphi_2 \in \mathscr{P}_1$; as $\varphi$ is extremal in $\mathscr{P}_1$, this implies that $\varphi_1 = \varphi_2$. So $\varphi$ is also extremal in $\mathscr{P}_0$.

Now we show that every extremal point of $\mathscr{P}_0$ is in $\mathscr{E}(\mathscr{P}_1) \cup \{0\}$. Let $\varphi \in \mathscr{P}_0 - (\mathscr{E}(\mathscr{P}_1) \cup \{0\})$. If $\varphi \in \mathscr{P}_1$, it is not extremal. If $\varphi \notin \mathscr{P}_1$, then $0 < \varphi(1) < 1$, so $\varphi = (1-c)0 + c\frac{1}{\varphi(1)}\varphi$, with $c = \varphi(1) \in (0,1)$ and $\frac{1}{\varphi(1)}\varphi \in \mathscr{P}_0$; this shows that $\varphi$ is not extremal.

$\square$

*Proof of the theorem.* Note that the conditions defining $\mathscr{P}$ in $L^\infty(G)$ are weak* closed conditions, so $\mathscr{P}$ is a weak* closed subset of $L^\infty(G)$. As $\mathscr{P}_0$ is the intersection of $\mathscr{P}$ with the closed unit ball of $L^\infty(G)$, it is weak* closed in this closed unit ball, hence weak* compact by the Banach-Alaoglu theorem (theorem B.4.1). As $\mathscr{P}_0$ is also convex, the Krein-Milman theorem (theorem B.5.2) says that the convex hull of $\mathscr{E}(\mathscr{P}_0)$ is weak* dense in $\mathscr{P}_0$. Also, the lemma above says that $\mathscr{E}(\mathscr{P}_0) = \mathscr{E}(\mathscr{P}_1) \cup \{0\}$.

Let $\varphi \in \mathscr{P}_1$, and let $U$ be a weak* neighborhood of $\varphi$ of the form $\{\psi \in \mathscr{P}_1 | |\int_G (\varphi - \psi) g_i d\mu| < c,\ 1 \leq i \leq n\}$, with $n \in \mathbb{Z}_{\geq 1}$, $g_1, \dots, g_n \in L^1(G)$ and $c > 0$. We want to find a point of $U$ that is in the convex hull of $\mathscr{E}(\mathscr{P}_1)$. Choose $\varepsilon > 0$ (we will see later how small it needs to be). By the first paragraph and the fact that closed balls in $L^\infty(G)$ are weak* closed (a consequence of the Hahn-Banach theorem), we can find $\psi$ in the convex hull of $\mathscr{E}(\mathscr{P}_1) \cup \{0\}$ such that, for every $i \in \{1, \dots, n\}$, we have $|\int_G (\varphi - \psi) g_i d\mu| < c/2$ and such that $\|\psi\|_\infty \geq 1 - \varepsilon$. Write $\psi = c_1\psi_1 + \dots + c_r\psi_r$, with $c_1, \dots, c_r \in [0,1]$, $\psi_1, \dots, \psi_r \in \mathscr{E}(\mathscr{P}_1)$ and $c_1 + \dots + c_r \leq 1$. Let $a = \frac{1}{\|\psi\|_\infty}$. Then $a\psi = (ac_1)\psi_1 + \dots + (ac_r)\psi_r$ and $ac_1 + \dots + ac_r = 1$, so $a\psi$ is in the convex hull of $\mathscr{E}(\mathscr{P}_1)$. Let's show that $a\psi \in U$. If $i \in \{1, \dots, n\}$, we have

$$\begin{aligned} \left| \int_G (\varphi - a\psi) g_i d\mu \right| &\leq \left| \int_G (\varphi - \psi) g_i d\mu \right| \left| \int_G (\psi - a\psi) g_i d\mu \right| \\ &< c/2 + |1-a| \left| \int_G \psi g_i d\mu \right| \\ &< c/2 + \varepsilon \left( c/2 + \left| \int_G \varphi g_i d\mu \right| \right). \end{aligned}$$

So, if we choose $\varepsilon$ small enough so that $\varepsilon \left( c/2 + \left| \int_G \varphi g_i d\mu \right| \right) < c/2$ for every $1 \in \{1, \dots, n\}$, the function $a\psi$ will be in $U$.

$\square$

As $\mathscr{P}$ is a subspace of the space $\mathscr{C}(G)$, we can also consider the topology of compact convergence on $\mathscr{P}$, that is, of convergence on compact subsets of $G$. If $\varphi \in \mathscr{P}$, a basis of neighborhoods of $\varphi$ for this topology is given by $\{\psi \in \mathscr{P} | \sup_{x \in K} |\varphi(x) - \psi(x)| < c\}$, for all compact subsets $K$ of $G$ and all $c > 0$.

**Theorem III.4.3.** *(Raikov) On the subset $\mathscr{P}_1$ of $\mathscr{P}$, the topology of compact convergence and the weak* topology coincide.*

*Remark* III.4.4. This theorem generalizes question (a) of exercise I.5.4.2. (See remark III.3.4.)

Note that the theorem is *not* true for $\mathscr{P}_0$. For example, if $G = \mathbb{R}$, then the topology of compact convergence and the weak* topology do not coincide on $\widehat{G} \cup \{0\}$. For example, consider the elements $\chi_y : x \longmapsto e^{ixy}$ of $\widehat{G}$. I claim that the family $(\chi_y)_{y\in\mathbb{R}}$ converges weakly to $0$ when $|y| \to +\infty$. (Obviously, it does not converge to $0$ for the topology of compact convergence; in fact, it has no limit in this topology.) Remember the this statement means that, for every $f \in L^1(\mathbb{R})$, we have

$$\lim_{|y|\to+\infty} \int_{\mathbb{R}} f(x)e^{ixy}dx = 0.$$

Suppose first that $f$ is the characteristic function of a compact interval $[a, b]$. Then

$$\int_{\mathbb{R}} f(x)e^{ixy}dy = \frac{1}{y}(e^{iby} - e^{iay}) \xrightarrow[|y|\to+\infty]{} 0.$$

So, if $f$ is a (finite) linear combination of characteristic functions of compact intervals, the conclusion still holds. Now let $f$ be any element of $L^1(\mathbb{R})$, and let $\varepsilon > 0$. We can find a linear combination $g$ of characteristic functions of compact intervals $g$ such that $\|f - g\|_1 \leq \varepsilon$. By what we just saw, we can also find $A \in \mathbb{R}$ such that $|\int_{\mathbb{R}} g(x)e^{ixy}dy| \leq \varepsilon$ for $|x| \geq A$. Then, if $|y| \geq A$, we have

$$\begin{aligned}\left|\int_{\mathbb{R}} f(x)e^{ixy}dx\right| &\leq \left|\int_{\mathbb{R}} g(x)e^{ixy}dx\right| + \left|\int_{\mathbb{R}} (f(x) - g(x))e^{ixy}dx\right| \\ &\leq \varepsilon + \int_{\mathbb{R}} |f(x) - g(x)|dx \\ &\leq 2\varepsilon.\end{aligned}$$

So $\int_{\mathbb{R}} f(x)e^{ixy}dx$ converges to 0 as $|y| \to +\infty$.

**Corollary III.4.5.** *The convex hull of $\mathscr{E}(\mathscr{P}_1)$ is dense in $\mathscr{P}_1$ for the topology of compact convergence.*

*Proof of the theorem.* We first show that the topology of compact convergence on $\mathscr{P}_1$ is finer than the weak* topology (this is the easier part). Let $\varphi \in \mathscr{P}_1$. Let $f \in L^1(G)$ and $c > 0$, and let $U = \{\psi \in \mathscr{P}_1 | \left|\int_G f(\varphi - \psi)d\mu\right| < c\}$. We want to find a neighborhood of $\varphi$ in the topology of compact convergence that is contained in $U$. Let $K \subset G$ be a compact subset such that $\int_{G\setminus K} |f|d\mu < c/3$, and let $V = \{\psi \in \mathscr{P}_1 | \sup_{x\in K} |\varphi(x) - \psi(x)| \leq \frac{c}{3\|f\|_1+1}\}$. Then, if

$\psi \in V$, we have

$$\begin{aligned}\left|\int_G f(\varphi-\psi)d\mu\right| &\leq \left|\int_K f(\varphi-\psi)d\mu\right| + \left|\int_{G\setminus K} f(\varphi-\psi)d\mu\right| \\ &\leq \|f\|_1 \sup_{x\in K}|\varphi(x)-\psi(x)| + 2\int_{G\setminus K}|f|d\mu \\ &< c\end{aligned}$$

so $\psi \in U$ (on the second line, we use the fact that $\|\varphi\|_\infty = \|\psi\|_\infty = 1$).

Now let's prove the hard direction, i.e. the fact that the weak* topology on $\mathscr{P}_1$ is finer than the topology of compact convergence. Let $\varphi \in \mathscr{P}_1$, and let $V = \{\psi \in \mathscr{P}_1 | \sup_{x\in K}|\varphi(x)-\psi(x)| < c\}$, with $K \subset G$ compact and $c > 0$. Let $\delta > 0$ be such that $\delta + 4\sqrt{\delta} < c$. Let $Q$ be a compact neighborhood of $1$ in $G$ such that

$$\sup_{x\in Q}|\varphi(x)-1| \leq \delta.$$

(Such a $Q$ exists because $\varphi$ is continuous and $\varphi(1) = 1$.) As $Q$ contains an open set, we have $\mu(Q) \neq 0$. Let $f = \frac{1}{\mu(Q)}\mathbb{1}_Q$. By the first lemma below (applied to $V = L^1(G)$ and $B = \mathscr{P}_1$) and the fact that $G \to L^1(G)$, $x \longmapsto L_{x^{-1}}f$ is continuous (hence $\{L_{x^{-1}}f,\ x \in K\} \subset L^1(G)$ is compact), we can find a weak* neighborhood $U_1$ of $\varphi$ in $\mathscr{P}_1$ such that, for every $x \in K$ and every $\psi \in U_1$, we have

$$\left|\int_G (\overline{\varphi-\psi})L_{x^{-1}}f\right| \leq \delta.$$

Then, for every $x \in K$ and every $\psi \in U_1$, we have

$$\begin{aligned}|f*\varphi(x) - f*\psi(x)| &= \left|\int_G f(xy)(\varphi(y^{-1})-\psi(y^{-1}))dy\right| \\ &= \left|\int_G L_{x^{-1}}f(y)(\overline{\varphi(y)-\psi(y)})dy\right| \quad \text{(see corollary III.2.6)} \\ &\leq \delta.\end{aligned}$$

Let $U_2 = \{\psi \in \mathscr{P}_1 | \left|\int_G(\varphi-\psi)fd\mu\right| < \delta\}$. (This is a weak* neighborhood of $\varphi$.) Let $\psi \in U_1 \cap U_2$. Then

$$\begin{aligned}\left|\int_G(1-\psi)fd\mu\right| &\leq \left|\int_G(1-\varphi)fd\mu\right| + \left|\int_G(\varphi-\psi)fd\mu\right| \\ &\leq \frac{1}{\mu(Q)}\left|\int_Q(1-\varphi(x))dx\right| + \delta \\ &\leq \sup_{x\in Q}|1-\varphi(x)| + \delta \\ &\leq 2\delta.\end{aligned}$$

On the other hand, for every $x \in G$, we have

$$\begin{aligned}
|f * \psi(x) - \psi(x)| &= \left| \frac{1}{\mu(Q)} \int_G \mathbb{1}_Q(y)\psi(y^{-1}x)dy - \frac{1}{\mu(Q)} \int_Q \psi(x)dy \right| \\
&= \frac{1}{\mu(Q)} \left| \int_Q (\psi(y^{-1}x) - \psi(x))dy \right| \\
&\le \frac{1}{\mu(Q)} \int_Q |\psi(y^{-1}x) - \psi(x)|dy \\
&\le \frac{1}{\mu(Q)} \int_Q \sqrt{2(1 - \mathrm{Re}(\psi(y)))}dy \text{ (see the second lemma below)} \\
&\le \frac{\sqrt{2}}{\mu(Q)} \left( \int_Q (1 - \mathrm{Re}(\psi(y)))dy \right)^{1/2} \left( \int_Q dy \right)^{1/2} \quad \text{(Cauchy-Schwarz)} \\
&\le \frac{\sqrt{2}}{\sqrt{\mu(Q)}} \left| \int_Q (1 - \psi(y))dy \right|^{1/2} \\
&= \sqrt{2} \left| \int_G (1 - \psi) f d\mu \right|^{1/2}
\end{aligned}$$

As $\psi \in U_2$, the previous calculation shows that this is $\le 2\sqrt{\delta}$. Note that this also applies to $\psi = \varphi$, because of course $\varphi$ is in $U_1 \cap U_2$. Putting all these bounds together, we get, is $\psi \in U_1 \cap U_2$ and $x \in K$,

$$\begin{aligned}
|\psi(x) - \varphi(x)| &\le |\psi(x) - f * \psi(x)| + |f * \psi(x) - f * \varphi(x)| + |f * \varphi(x) - \varphi(x)| \\
&\le \delta + 4\sqrt{\delta} \\
&< c.
\end{aligned}$$

So $U_1 \cap U_2 \subset V$, and we are done.

□

**Lemma III.4.6.** *Let $V$ be a Banach space, and let $B$ be a norm-bounded subset of* $\mathrm{Hom}(V, \mathbb{C})$. *Then the topology of compact convergence (i.e. of uniform convergence on compact subsets of $V$) and the weak* topology coincide on $B$.*

*Proof.* We want to compare the topology of pointwise convergence on $V$ (i.e. the weak* topology) and the topology of compact convergence on $V$. The second one is finer than the first one on all of $\mathrm{Hom}(V, \mathbb{C})$, so we just need to show that the first one is finer than the second on $B$.

Let $T_0 \in B$, let $K \subset V$ be compact and let $c > 0$. We want to find a weak* neighborhood of $T_0$ in $B$ contained in $\{T \in B | \sup_{x \in K} |T(x) - T_0(x)| < c\}$. Let $M = \sup_{T \in B} \|T\|_{op}$ (this is finite because $B$ is bounded). Let $x_1, \dots, x_n \in K$ such that $K$ is contained in the union of the open balls centered at the $x_i$ with radius $\frac{c}{3M}$. Let $T \in B$ be such that $|(T - T_0)(x_i)| < c/3$

for $i = 1, \dots, n$ (this defines a weak* neighborhood of $T$). For every $x \in K$, there exists $i \in \{1, \dots, n\}$ such that $\|x - x_i\| < \frac{c}{3M}$, and then we have

$$\begin{aligned}|T(x) - T_0(x)| &\leq |T(x - x_i)| + |(T - T_0)(x_i)| + |T_0(x - x_i)| \\ &\leq \|T\|_{op}\|x - x_i\| + c/3 + \|T_0\|_{op}\|x - x_i\| \\ &< c/3 + 2M\frac{c}{3M} = c.\end{aligned}$$

So $T \in U$.

□

**Lemma III.4.7.** *Let $\varphi \in \mathscr{P}_1$. Then, for all $x, y \in G$, we have*

$$|\varphi(x) - \varphi(y)|^2 \leq 2 - 2\,\mathrm{Re}(\varphi(yx^{-1})).$$

*Proof.* By theorem III.2.5, we can find a unitary representation $(\pi, V)$ of $G$ and $v \in V$ such that $\varphi(x) = \langle \pi(x)(v), v\rangle$ for every $x \in G$. Also, as $\varphi(1) = 1$, we have $\|v\| = 1$. So, for all $x, y \in G$, we have

$$\begin{aligned}|\varphi(x) - \varphi(y)|^2 &= |\langle (\pi(x) - \pi(y))(v), v\rangle| \\ &= |\langle v, (\pi(x^{-1}) - \pi(y^{-1}))(v)\rangle|^2 \\ &\leq \|(\pi(x^{-1}) - \pi(y^{-1}))(v)\|^2 \\ &= \|\pi(x^{-1})(v)\|^2 + \|\pi(x^{-1})(v)\|^2 - 2\,\mathrm{Re}(\langle \pi(x^{-1})(v), \pi(y^{-1})(v)\rangle) \\ &= 2 - 2\,\mathrm{Re}(\langle \pi(x^{-1})(v), \pi(y^{-1})(v)\rangle) \\ &= 2 - 2\,\mathrm{Re}(\langle \pi(yx^{-1})(v), v\rangle) \\ &= 2 - 2\,\mathrm{Re}(\varphi(yx^{-1})).\end{aligned}$$

□

# III.5 The Gelfand-Raikov theorem

**Theorem III.5.1.** *(Gelfand-Raikov) Let $G$ be a locally compact group. Then, for all $x, y \in G$ such that $x \neq y$, there exists an irreducible unitary representation $\pi$ of $G$ such that $\pi(x) \neq \pi(y)$.*

*More precisely, there exists an irreducible unitary representation $(\pi, V)$ of $G$ and a vector $v \in V$ such that $\langle \pi(x)(v), v\rangle \neq \langle \pi(y)(v), v\rangle$.*

*Proof.* Let $x, y \in G$. Suppose that $\langle \pi(x)(v), v\rangle = \langle \pi(y)(v), v\rangle$ for every irreducible unitary representation $(\pi, V)$ of $G$ and every $v \in V$. By theorem III.3.2, this implies that $\varphi(x) = \varphi(y)$ for every $\varphi \in \mathscr{E}(\mathscr{P}_1)$, hence for every $\varphi \in \mathscr{P}_1$ by corollary III.4.5 (and the fat that $\{x, y\}$ is a compact subset of $G$), hence for every $\varphi \in \mathscr{P}$ because $\mathscr{P} = \mathbb{R}_{\geq 0} \cdot \mathscr{P}_1$.

Let $\pi_L$ be the left regular representation of $G$, i.e. the representation of $G$ on $L^2(G)$ defined by $\pi_L(z)(f) = L_z f$ for $z \in G$ and $f \in L^2(G)$. This is a unitary representation of $G$, so, by the first paragraph and by proposition III.2.4, we have $\langle \pi_L(x)(f), f\rangle = \langle \pi_L(y)(f), f\rangle$ for every $f \in L^2(G)$. Let $f_1, f_2 \in L^2(G)$. Then

$$\langle \pi_L(x)(f_1+f_2), f_1+f_2\rangle = \langle \pi_L(x)(f_1), f_1\rangle + \langle \pi_L(f_2), f_2\rangle + \langle \pi_L(x)(f_1), f_2\rangle + \langle \pi_L(x)(f_2), f_1\rangle$$

and

$$\langle \pi_L(x)(f_1+if_2), f_1+if_2\rangle = \langle \pi_L(x)(f_1), f_1\rangle + \langle \pi_L(f_2), f_2\rangle - i\langle \pi_L(x)(f_1), f_2\rangle + i\langle \pi_L(x)(f_2), f_1\rangle,$$

so

$$\begin{aligned} 2\langle \pi_L(x)(f_1), f_2\rangle &= \langle \pi_L(x)(f_1+f_2), f_1+f_2\rangle + i\langle \pi_L(x)(f_1+if_2), f_1+if_2\rangle \\ &\quad - (1+i)(\langle \pi_L(x)(f_1), f_1\rangle + \langle \pi_L(x)(f_2), f_2\rangle). \end{aligned}$$

We have a similar identity for $\pi_L(y)$, and this shows that

$$\langle \pi_L(x)(f_1), f_2\rangle = \langle \pi_L(y)(f_1), f_2\rangle.$$

Now note that

$$\begin{aligned} \langle \pi_L(x)(f_1), f_2\rangle &= \int_G L_x f_1(z)\overline{f_2(z)}dz \\ &= \int_G f_1(x^{-1}z)\overline{f_2(z)}dz \\ &= \int_G \overline{f_2(z)}\overline{\widetilde{f_1}(z^{-1}x)}dz \\ &= \overline{f_2 * \widetilde{f_1}(x)} \end{aligned}$$

(remember that $\widetilde{f_1} \in L^2(G)$ is defined by $\widetilde{f_1}(z) = \overline{f_1(z^{-1})}$), so $f_2 * \widetilde{f_1}(x) = f_2 * \widetilde{f_1}(y)$. This calculation also shows that $f_2 * \widetilde{f_1}$ makes sense and is continuous.

As $f \longmapsto \widetilde{f}$ is an involution on $L^2(G)$, we deduce that $f_1 * f_2(x) = f_1 * f_2(y)$ for all $f_1, f_2 \in L^2(G)$, and in particular for all $f_1, f_2 \in \mathscr{C}_c(G)$. Let $f \in \mathscr{C}_c(G)$, and let $(\psi_U)_{U\in\mathscr{U}}$ be an approximate identity. We have $\psi_U \in \mathscr{C}_c(G)$ for every $U \in \mathscr{U}$, and $\psi_U * f \xrightarrow[U\to\{1\}]{} f$ for $\|.\|_\infty$ by proposition I.4.1.9 (and the fact that $f$ is uniformly continuous, which is proposition I.1.12). As $\psi_U * f(x) = \psi_U * f(y)$ for every $U \in \mathscr{U}$, this implies that $f(x) = f(y)$. But then we must have $x = y$ (by Urysohn's lemma).

□

# III.6 Exercises

Let $G$ be a topological group and $(\pi, V)$ be a unitary representation of $G$. A *matrix coefficient* of $\pi$ is a function $G \to \mathbb{C}$ of the form $x \longmapsto \langle \pi(x)(v), w\rangle$, with $v, w \in V$. Note that these functions are all continuous.

Remember also that, if $G$ is locally compact (and $\mu$ is a left Haar measure on $G$), then the *left regular representation* $\pi_L$ is the representation of $G$ on $L^2(G) := L^2(G,\mu)$ given by $\pi_L(x)(f) = L_x f$, for $x \in G$ and $f \in L^2(G)$. In this section, we'll just call $\pi_L$ the *regular representation* of $G$.

## III.6.1 The regular representation

**Exercise III.6.1.1.** Let $G$ be a discrete group, and let $\varphi = \mathbb{1}_{\{1\}}$.

(a). (1) Show that $\varphi$ is a function of positive type on $G$.

(b). (2) Show that $V_\varphi$ is equivalent to the regular representation of $G$.

*Solution.*

(a). The counting measure $\mu$ is a left Haar measure on $G$, so we use this measure. For every $f \in L^1(G)$, we have $\int_G f\varphi d\mu = f(1)$. So

$$\int_G (f^* * f)\varphi d\mu = (f^* * f)(1) = \sum_{y\in G} \overline{f(y^{-1})} f(y^{-1}) \in \mathbb{R}_{\geq 0}.$$

(b). For all $f, g \in L^1(G)$, we have

$$\begin{aligned} \langle f, g\rangle_\varphi &= \int_G (g^* * f)\varphi d\mu \\ &= (g^* * f)(1) \\ &= \sum_{y\in G} \overline{g(y^{-1})} f(y^{-1}) \\ &= \langle f, g\rangle_{L^2(G)}. \end{aligned}$$

So the kernel of $\langle .,.\rangle_\varphi$ is equal to $\{0\}$, and the Hilbert space $V_\varphi$ is the completion of $L^1(G)$ for the norm $\|.\|_2$, that is, $L^2(G)$. The action of $G$ on $V_\varphi$ is the extension by continuity of its action by left translations on $L^1(G)$, so we get the action of $G$ by left translations on $L^2(G)$.

□

**Exercise III.6.1.2.** Let $G$ be a locally compact group.

(a). If $f, g \in \mathscr{C}_c(G)$, show that $f * g \in \mathscr{C}_c(G)$.

(b). Show that every matrix coefficient of the regular representation of $G$ vanishes at $\infty$.

(c). Suppose that $G$ is not compact. If $(\pi, V)$ is a finite-dimensional unitary representation of $G$, show that it has a matrix coefficient that does not vanish at $\infty$.

(d). If $G$ is not compact, show that its regular representation has no finite-dimensional subrepresentation. [2]

*Solution.*

(a). First, we know that $f * g$ exists, because $f$ and $g$ are in $L^1(G)$. If $x, x' \in G$, then

$$\begin{aligned}|f * g(x) - f * g(x')| &= \left|\int_G f(y)(g(y^{-1}x) - g(y^{-1}x'))dy\right| \\ &\leq \|f\|_1 \operatorname{supp}_{y \in \operatorname{supp}(f)} |g(y^{-1}x) - g(y^{-1}x')|.\end{aligned}$$

As $g$ is right uniformly continuous (see proposition I.1.12), this tends to $0$ as $x'$ tends to $x$, so $f * g$ is continuous.

Let $x \in G$ such that $f * g(x) \neq 0$. We have

$$f * g(x) = \int_G f(y)g(y^{-1}x)dy,$$

so there exists $y \in \operatorname{supp}(f)$ such that $y^{-1}x \in \operatorname{supp}(g)$. In other words, $x \in \operatorname{supp}(f)\operatorname{supp}(g)$. As both $\operatorname{supp}(f)$ and $\operatorname{supp}(g)$ are compact, their product $\operatorname{supp}(f)\operatorname{supp}(g)$ is also compact, so $f * g$ has compact support.

(b). Remember that, if $f \in L^2(G)$, we define $\widetilde{f} : G \to \mathbb{C}$ by $\widetilde{f}(x) = \overline{f(x^{-1})}$.

Every matrix coefficient of the left regular representation of $G$ is of the form

$$x \longmapsto \langle L_{x^{-1}} f, g\rangle_{L^2(G)},$$

with $f, g \in L^2(G)$. We have (see proposition III.2.4(iii))

$$\begin{aligned}\langle L_{x^{-1}} f, g\rangle_{L^2(G)} &= \int_G f(x^{-1}y)\overline{g(y)}dy \\ &= \int_G \overline{\widetilde{f}(y^{-1}x)}\overline{g(y)}dy \\ &= \overline{g} * \overline{\widetilde{f}}(x).\end{aligned}$$

Moreover, if $f', g' \in L^2(G)$, then we have (using the Cauchy-Schwarz inequality)

$$\begin{aligned}|\langle L_{x^{-1}} f, g\rangle_{L^2(G)} - \langle L_{x^{-1}} f', g\rangle_{L^2(G)}| &\leq \int_G |g(y)||f(x^{-1}y - f'(x^{-1}y)|dy \\ &\leq \|g\|_2 \|L_{x^{-1}}(f - f')\|_2 \\ &= \|g\|_2 \|f - f'\|_2\end{aligned}$$

[2] Compare with Peter-Weyl.

and

$$\begin{aligned}|\langle L_{x^{-1}}f, g\rangle_{L^2(G)} - \langle L_{x^{-1}}f, g'\rangle_{L^2(G)}| &\leq \int_G |g(y) - g'(y)||f(x^{-1}y|dy \\ &\leq \|g - g'\|_2 \|L_{x^{-1}}f\|_2 \\ &= \|g - g'\|_2 \|f'\|_2.\end{aligned}$$

Suppose that $f, g \in \mathscr{C}_c(G)$. Then $\overline{g}, \overline{\widetilde{f}} \in \mathscr{C}_c(G)$, so, by question (a), $\overline{g} * \overline{\widetilde{f}} \in \mathscr{C}_c(G)$, and in particular this function vanishes at $\infty$.

In the general case, let $\varepsilon > 0$ and let $f', g' \in \mathscr{C}_c(G)$ such that $\|f - f'\|_2 \leq \varepsilon$ and $\|g - g'\|_2 \leq \varepsilon$. Then, by the two inequality above, we have, for every $x \in G$,

$$|\overline{g} * \overline{\widetilde{f}}(x) - \overline{g}' * \overline{\widetilde{f}}'(x)| \leq \varepsilon(\|f\|_2 + \|g\|_2).$$

But we have just seen that $\overline{g}' * \overline{\widetilde{f}}'$ has compact support, so there exists a compact subset $K$ of $G$ such that, for every $x \notin K$¡ we have

$$|\overline{g} * \overline{\widetilde{f}}(x)| \leq \varepsilon(\|f\|_2 + \|g\|_2).$$

This shows that the matrix coefficient $\overline{g} * \overline{\widetilde{f}}$ vanishes at $\infty$.

(c). Let $(e_1, \dots, e_n)$ be an orthonormal basis of $V$. For every $i \in \{1, \dots, n\}$, let $f_i$ be the matrix coefficient $x \longmapsto \langle \pi(x)(e_1), e_i \rangle$. Then we have, for every $x \in G$,

$$\sum_{i=1}^{n} |f_i(x)|^2 = \sum_{i=1}^{n} |\langle \pi(x)(e_1), e_i\rangle|^2 = \|\pi(x)(e_1)\|^2 = 1.$$

This shows that at least one of the $f_i$ does not vanish at $\infty$.

(d). This follows directly from (c) and (d).

□

## III.6.2 Weak containment

Let $G$ be a topological group and $(\pi, V)$ be a unitary representation of $G$. We say that the functions $G \to \mathbb{C}$, $x \longmapsto \langle \pi(x)(v), w\rangle$ (with $v, w \in V$) is a *diagonal matrix coefficient* if $v = w$; a diagonal matrix coefficient is a function of positive type by proposition III.2.4, and we call it a *function of positive type associated to* $\pi$. We say that a function of positive type is *normalized* if it is of the form $x \longmapsto \langle \pi(x)(v), v\rangle$ with $\|v\| = 1$. We denote by $\mathscr{P}(\pi)$ the set of functions of positive type associated to $\pi$.

We will see soon [3] that, if $G$ is compact, then the regular representation of $G$ contains all the irreducible representations of $G$ (which are all finite-dimensional); in fact, it is the closure of the direct sum of all its irreducible subrepresentations. On the other hand, if $G$ is abelian, then its regular representation is the direct integral of all the irreducible representations of $G$ (which are all 1-dimensional), even though it does not contain any of them if $G$ is not compact. We will not rigorously define direct integrals here, but we will introduce a weaker definition of containment, for which irreducible representations of an abelian locally compact group are contained in the regular representation, and start studying it.

Let $(\pi, V)$ and $(\pi', V')$ be unitary representations of $G$. We say that $\pi$ is *weakly contained* in $\pi'$, and write $\pi \prec \pi'$, if $\mathscr{P}(\pi)$ is contained in the closure of the set of finite sums of elements of $\mathscr{P}(\pi')$ for the topology of convergence on compact subsets of $G$. In other words, $\pi \prec \pi'$ if, for every $v \in V$, for every $K \subset G$ compact and every $c > 0$, there exist $v'_1, \ldots, v'_n \in V'$ such that

$$\sup_{x \in K} |\langle \pi(x)(v), v \rangle - \sum_{i=1}^{n} \langle \pi'(x)(v'_i), v'_i \rangle| < c.$$

**Exercise III.6.2.1.** Let $(\pi_1, V_1)$, $(\pi_2, V_2)$ be unitary representations of $G$.

(a). Show that the algebraic tensor product $V_1 \otimes_{\mathbb{C}} V_2$ has a Hermitian inner product, uniquely determined by $\langle v_1 \otimes v_2, w_1 \otimes w_2 \rangle = \langle v_1, w_1 \rangle \langle v_2, w_2 \rangle$.

(b). We denote the completion of $V_1 \otimes_C V_2$ for this inner form by $V_1 \hat{\otimes}_{\mathbb{C}} V_2$. Show that the formula $(x, v_1 \otimes v_2) \longmapsto \pi_1(x)(v_1) \otimes \pi_2(x)(v_2)$ defines a unitary representation of $G$ on $V_1 \hat{\otimes}_{\mathbb{C}} V_2$. (This is called the tensor product representation and usually denoted by $\pi_1 \otimes \pi_2$.)

(c). If $V_1$ and $V_2$ are finite-dimensional, show that, for every $x \in G$, we have

$$\mathrm{Tr}(\pi_1 \otimes \pi_2(x)) = \mathrm{Tr}(\pi_1(x))\mathrm{Tr}(\pi_2(x)).$$

*Solution.*

(a). As pure tensors span $V_1 \otimes_{\mathbb{C}} V_2$, there is at most one sesquilinear form $B$ on $V_1 \otimes_{\mathbb{C}} V_2$ such that $B(v_1 \otimes v_2, w_1 \otimes w_2) = \langle v_1, w_1 \rangle \langle v_2, w_2 \rangle$. Let's show that such a form exists. Let $w_1 \in V_1$ and $w_2 \in V_2$. Then the map on $V_1 \times V_2 \to \mathbb{C}$, $(v_1, v_2) \longmapsto \langle v_1, w_1 \rangle \langle v_2, w_2 \rangle$ is a bilinear form, hence it corresponds to a unique linear form on $V_1 \otimes_{\mathbb{C}} V_2$, say $B_{w_1,w_2}$. Next, the map on $V_1 \times V_2$ sending $(w_1, w_2)$ to the antilinear form $v \longmapsto \overline{B_{w_1,w_2}(v)}$ is bilinear, so it corresponds to a unique linear functional $T$ on $V_1 \otimes_{\mathbb{C}} V_2$. Finally, the map $B : (V_1 \otimes_{\mathbb{C}} V_2) \times (V_1 \otimes_{\mathbb{C}} V_2) \to \mathbb{C}$ sending $(v, w)$ to $\overline{T(w)(v)}$ is linear in $v$ and antilinear in $w$, so it is a sesquilinear form, and it sends pure tensors where we want by definition.

Now we show that $B$ is Hermitian, i.e. that $B(w, v) = \overline{B(v, w)}$ for all $v, w \in V_1 \otimes_{\mathbb{C}} V_2$. As $B$ is sesquilinear, it suffices to check this property for $v$ and $w$ pure tensors, but then it follows immediately from the analogous property of the inner products of $V_1$ and $V_2$.

[3] Add ref.

Finally, we show that $B$ is definite positive. Let $v \in V_1 \otimes_{\mathbb{C}} V_2$, and write $v = \sum_{i=1}^n v_{1,i} \otimes v_{2,i}$, $v_{1,i} \in V_1$ and $v_{2,i} \in V_2$. Then $v$ is in $V_1' \otimes_{\mathbb{C}} V_2'$, where $V_1' = \mathrm{Span}(v_{1,1}, \dots, v_{1,n})$ and $V_2' = \mathrm{Span}(v_{2,1}, \dots, v_{2,n})$. So we may replace $V_1$ and $V_2$ by $V_1'$ and $V_2'$, and so may assume that $V_1$ and $V_2$ are finite-dimensional. If this is the case, let $(e_1, \dots, e_r)$ (resp. $(e_1', \dots, e_s')$) be an orthonormal basis of $V_1$ (resp. $V_2$). Then $(e_i \otimes e_j')_{1 \le i \le r, 1 \le j \le s}$ is a basis of $V_1 \otimes_{\mathbb{C}} V_2$, and it is clear from the definition of the Hermitian form $B$ on $V_1 \otimes_{\mathbb{C}} V_2$ that it is an orthonormal basis for $B$ . But the existence of an orthonomal basis forces the form to be positive definite (if $v = \sum_{i=1}^r \sum_{j=1}^s a_{ij} e_i \otimes e_j'$, then $B(v, v) = \sum_{i,j} |a_{ij}|^2$).

(b). First note that, if $v_1 \in V_1$ and $v_2 \in V_2$, then we have $\|v_1 \otimes v_2\| = \|v_1\| \|v_2\|$.

Let $x \in G$. Then the map $V_1 \times V_2 \to V_1 \otimes_{\mathbb{C}} V_2$ sending $(v_1, v_2)$ to $\pi_1(x)(v_1) \otimes \pi_2(x)(v_2)$ is bilinear, so it induces a $\mathbb{C}$-linear map $\pi_1 \otimes \pi_2(x)$ from $V_1 \otimes_{\mathbb{C}} V_2$ to itself. We show that this map is an isometry (hence continuous). Let $(e_i)_{i \in I}$ (resp. $(f_j)_{j \in J}$) be a Hilbert basis of $V_1$ (resp. $V_2$). If $v_1 \in V_1$ and $v_2 \in V_2$, we can write $v_1 = \sum_{i \in I} a_i e_i$ and $v_2 = \sum_{j \in J} b_j f_j$, and then, by the remark above, the series $\sum_{i,j} a_i b_i e_i \otimes f_j$ converges to $v_1 \otimes v_2$ in $V_1 \otimes_{\mathbb{C}} V_2$. As every element of $V_1 \otimes_{\mathbb{C}} V_2$ is a finite sum of elements of the form $v_1 \otimes v_2$, this proves that every element $v$ of $V_1 \otimes_{\mathbb{C}} V_2$ can be written as the limit of a convergent series $\sum_{i \in I, j \in J} a_i b_j e_i \otimes f_j$, with $a_i, b_j \in \mathbb{C}$. Then $\pi_1 \otimes \pi_2(x)(v) = \sum_{i,j} a_i b_j \pi_1(x)(e_i) \otimes \pi_2(x)(f_j)$. As the families $(e_i \otimes f_j)$ and $(\pi_1(x)(e_i) \otimes \pi_2(x)(f_j))$ are both orthogonal in $V_1 \otimes_{\mathbb{C}} V_2$, we get $\|v\|^2 = \sum_{i,j} |a_i|^2 |b_j|^2 = \|\pi_1 \otimes \pi_2(x)(v)\|^2$.

As the map $\pi_1 \otimes \pi_2(x)$ is continuous, it extends to a continuous endormophism of $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$, which is also an isometry and will still be denoted by $\pi_1 \otimes \pi_2(x)$.

If $y$ is another element of $G$, the endomorphisms $\pi_1 \otimes \pi_2(xy)$ and $(\pi_1 \otimes \pi_2(x)) \circ (\pi_1 \otimes \pi_2(y))$ of $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$ are equal on pure tensors, hence they are equal because pure tensors generate a dense subspace of $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$.

To check that this defines a unitary representation of $G$ on $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$, we still need to check that, for every $v \in V_1 \widehat{\otimes}_{\mathbb{C}} V_2$, the map $G \to V_1 \widehat{\otimes}_{\mathbb{C}} V_2$, $x \longmapsto \pi_1 \otimes \pi_2(x)(v)$ is continuous. This is true for $v$ a pure tensor : if $v = v_1 \otimes v_2$, then, for $x, y \in G$, we have

$$\begin{aligned}
\|(\pi_1 \otimes \pi_2(x) - \pi_1 \otimes \pi_2(y))(v)\| &\le \|\pi_1(x)(v_1) \otimes (\pi_2(x) - \pi_2(y))(v_2)\| \\
&\quad + \|(\pi_1(x) - \pi_1(y))(v_1) \otimes \pi_2(y)(v_2)\| \\
&= \|v_1\| \|(\pi_2(x) - \pi_2(y))(v_2)\| + \|(\pi_1(x) - \pi_1(y))(v_1)\| \|v_2\|,
\end{aligned}$$

which implies the result. So it is still true for a finite sum of pure tensors, and then a standard shows that it is true for every element of $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$.

(c). Let $(e_1, \dots, e_n)$ (resp. $(f_1, \dots, f_j)$) be an orthonormal basis of $V_1$ (resp. $V_2$). Then $(e_i \otimes f_j)_{1 \le i \le n, 1 \le j \le m}$ is an orthonormal basis of $V_1 \otimes_{\mathbb{C}} V_2$. Let $x \in G$. Then

$$\mathrm{Tr}(\pi_1(x)) = \sum_{i=1}^n \langle \pi_1(x)(e_i), e_i \rangle$$

and

$$\mathrm{Tr}(\pi_2(x)) = \sum_{j=1}^{m} \langle \pi_2(x)(f_j), f_j \rangle,$$

so

$$\begin{aligned}\mathrm{Tr}(\pi_1 \otimes \pi_2(x)) &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \pi_1 \otimes \pi_2(x)(e_i \otimes f_j), e_i \otimes f_j \rangle \\ &= \left( \sum_{i=1}^{n} \langle \pi_1(x)(e_i), e_i \rangle \right) \left( \sum_{j=1}^{m} \langle \pi_2(x)(f_j), f_j \rangle \right) \\ &= \mathrm{Tr}(\pi_1(x))\mathrm{Tr}(\pi_2(x)).\end{aligned}$$

□

**Exercise III.6.2.2.** Let $V$ be a locally convex topological $\mathbb{C}$-vector space, $K$ be a compact convex subset of $V$, and $F \subset K$ be such that $K$ is the closure of the convex hull of $F$. Show that every extremal point of $K$ is in the closure of $F$. (This is known as *Milman's theorem*.)

*Solution.* If $0 \in X$ is an open convex subset of $V$, then we have $\overline{X} \subset 2X$. Indeed, if $p : V \to \mathbb{R}_{\geq 0}$ be the gauge of $X$ (see lemma B.3.8), then $X = \{v \in V | p(v) < 1\}$, so

$$\overline{X} \subset \{v \in V | p(v) \leq 1\} \subset \{v \in V | p(v) < 2\} = 2X.$$

Let $v$ be an extremal of $K$, and suppose that $v \notin \overline{F}$. Then we can find a convex neighborhood $X$ of 0 in $V$ such that $X = -X$ and $(v + X) \cap \overline{F} = \varnothing$. Replacing $X$ by $\frac{1}{2}X$, we may assume that we have $(v + \overline{X}) \cap \overline{F} = \varnothing$.

As $\overline{F}$ is compact (as a closed subset of $K$), we can find $x_1, \dots, x_n \in F$ such that $\overline{F} \subset \bigcup_{i=1}^{n} (x_i + X)$. For every $i \in \{1, \dots, n\}$, let $K_i$ be the closure of the convex hull of $\overline{F} \cap (x_i + X)$; this is a compact convex subset of $V$ (it is compact because it is closed in $K$). As $K$ is the closure of the convex hull of $\overline{F}$, we have $K \supset K_1 \cup \ldots \cup K_n$, so $K$ contains the convex hull $L$ of $K_1 \cup \ldots \cup K_n$. Let's show that $K = L$. As $L \supset F$ and $L$ is convex, it suffices to show that $L$ is compact. Let

$$S = \{(x_1, \dots, x_n) \in [0,1]^n | x_1 + \ldots + x_n = 1\},$$

and consider the function

$$f : S \times K_1 \times \ldots \times K_n \to L$$

sending $((x_1, \dots, x_n), v_1, \dots, v_n)$ to $\sum_{i=1}^{m} x_i v_i$. This map is continuous, so its image is compact. If we show that this image is convex, then it will equal to $L$ by definition of $L$, and we will be done. So let $a = ((x_1, \dots, x_n), v_1, \dots, v_n)$ and $a' = ((x'_1, \dots, x'_n), v'_1, \dots, v'_n)$ be elements of $S \times K_1 \times \dots\dots K_n$ and $t \in [0, 1]$. Then

$$tf(a) + (1-t)f(a') = \sum_{i=1}^{n} (tx_i v_i + (1-t)x'_i v'_i)$$

Let $i \in \{1, \dots, n\}$. If $tx_i + (1-t)x_i \neq 0$, we set $y_i = tx_i + (1-t)x_i$ and $w_i = \frac{1}{y_i}(tx_i v_i + (1-t)x'_i v'_i)$. Otherwise, we set $w_i = v_i$ and $y_i = 0$. Then we have $w_i \in K_i$ for every $i$ because $K_i$ is convex, $y_i \geq 0$ for every $i$, and

$$\sum_{i=1}^{n} y_i = t\sum_{i=1}^{n} x_i + (1-t)\sum_{i=1}^{n} x'_i = 1.$$

So

$$tf(a) + (1-t)f(a') = f((y_1 \dots, y_n), w_1, \dots, w_n)$$

is in the image of $f$, and we are done.

Now we derive a contradiction. As $K = L$, we can write $v = \sum_{i=1}^{n} t_i v_i$, with $(t_1, \dots, t_n) \in S$ and $v_i \in K_i$ for every $i$. As $v$ is extremal in $K$, there exists $i \in \{1, \dots, n\}$ such that $v = v_i$. But then $v \in K_i \subset (x_i + \overline{X})$ (because $K_i$ is contained in the closure of the convex hull of $x_i + X$, and this is $x_i + \overline{X}$ because $X$ is convex). As $x_i \in F$ and $X = -X$, this implies that $x_i \in (v + \overline{V}) \cap F$, contradicting the choice of $X$.

□

**Exercise III.6.2.3.** Let $(\pi, V)$ and $(\pi', V')$ be unitary representations of $G$. Let $C \subset V$ such that $\mathrm{Span}(\pi(x)(v),\ x \in G,\ v \in C)$ is dense in $V$.[4] Suppose that every function $x \longmapsto \langle \pi(x)(v), v \rangle$, for $v \in C$, is in the closure of the set of finite sums of elements of $\mathscr{P}(\pi')$ (still for the topology of convergence on compact subsets of $G$). The goal of this problem is to show that this implies $\pi \prec \pi'$.

Let $X$ be the set of $v \in V$ such that $x \longmapsto \langle \pi(x)(v), v \rangle$ is in the closure of the set of finite sums of elements of $\mathscr{P}(\pi')$ (for the same topology as above).

(a). Show that $X$ is stable by all the $\pi(x)$, $x \in G$, and under scalar multiplication.

(b). If $v \in X$ and $x_1, x_2 \in G$, show that $\pi(x_1)(v) + \pi(x_2)(v) \in X$.

(c). Show that $X$ is closed in $V$.

(d). If $v \in X$, show that the smallest closed $G$-invariant subspace of $V$ containing $v$ is contained in $X$.

(e). Let $v_1, v_2 \in X$, and let $W_1$ (resp. $W_2$) be the smallest closed $G$-invariant subspace of $V$ containing $v_1$ (resp. $v_2$). Let $W = \overline{W_1 + W_2}$, and denote by $T : W \to W_1^{\perp}$ the orthogonal projection, where we take the orthogonal complement of $W_1$ in $W$.

[4]For example, if $V$ is cyclic, $C$ could just contain a cyclic vector for $V$.

(i) Show that $T$ is $G$-equivariant and that $T(W_2)$ is dense in $W_1^\perp$.

(ii) Show that $W_1^\perp \subset X$.

(iii) Show that $v_1 + v_2 \in X$. (Hint : Use $T(v_1 + v_2)$ and $(v_1 + v_2) - T(v_1 + v_2)$.)

(f). Show that $\pi \prec \pi'$.

*Solution.*

(a). For every $v \in V$ (resp. $v \in V'$), we write $\varphi_v$ for the matrix coefficient $x \longmapsto \langle \pi(x)(v), v\rangle$ (resp. $x \longmapsto \langle \pi'(x)(v), v\rangle$). We also write $\sum \mathscr{P}(\pi')$ for the set of finite sums of elements of $\mathscr{P}(\pi')$.

Let $v \in X$, let $y \in G$ and let $\lambda \in \mathbb{C}$. We want to show that $\pi(y)(v)$ and $\lambda v$ are in $X$, that is, that $\varphi_{\pi(y)(v)}$ and $\varphi_{\lambda v}$ are in $\overline{\sum \mathscr{P}(\pi')}$. If $\lambda = 0$, the conclusion is obvious for $\lambda v$ (note that $0$ is a matrix coefficient of every representation of $G$), so we may assume that $\lambda \neq 0$. Let $K$ be a compact subset of $G$ $\varepsilon > 0$. Choose $v'_1, \ldots, v'_n$ such that $\sup_{x \in K \cup y^{-1}Ky} |\varphi_v(x) - \sum_{i=1}^n \varphi_{v'_i}(x)| \leq \min(\varepsilon, |\lambda|^{-2}\varepsilon)$. Then, for every $x \in K$, we have

$$\begin{aligned}
|\varphi_{\pi(y)v}(x) - \sum_{i=1}^n \varphi_{\pi'(y)(v'_i)}(x)| &= |\langle \pi(xy)(v), \pi(y)(v)\rangle - \sum_{i=1}^n \langle \pi'(xy)(v'_i), \pi'(y)(v'_i)\rangle| \\
&= |\langle \pi(y^{-1}xy)(v), v\rangle - \sum_{i=1}^n \langle \pi'(y^{-1}xy)(v'_i), v'_i\rangle| \\
&= |\varphi_v(y^{-1}xy) - \sum_{i=1}^n \varphi_{v'_i}(y^{-1}xy)| \\
&\leq \varepsilon
\end{aligned}$$

and

$$|\varphi_{\lambda v}(x) - \sum_{i=1}^n \varphi_{\lambda v'_i}(x)| = |\lambda|^2 |\varphi_v(x) - \sum_{i=1}^n \varphi_{v'_i}(x)| \leq \varepsilon.$$

So $\varphi_{\pi(y)(v)}$ and $\varphi_{\lambda v}$ are in the closure of $\mathscr{P}(\pi')$.

(b). Let $v \in X$ and let $x_1, x_2 \in G$. For every $y \in G$, we have

$$\begin{aligned}
\varphi_{\pi(x_1)(v)+\pi(x_2)(v)}(y) &= \langle \pi(y)(\pi(x_1)(v) + \pi(x_2)(v)), \pi(x_1)(v) + \pi(x_2)(v)\rangle \\
&= \langle \pi(x_1^{-1}yx_1)(v), v\rangle + \langle \pi(x_2^{-1}yx_1)(v), v\rangle + \langle \pi(x_1^{-1}yx_2)(v), v\rangle \\
&\quad + \langle \pi(x_2^{-1}yx_2)(v), v\rangle.
\end{aligned}$$

In other words,

$$\varphi_{\pi(x_1)(v)+\pi(x_2)(v)} = \sum_{i,j=1}^2 L_{x_i} R_{x_j} \varphi_v.$$

Let $K$ be a compact subset of $G$ and let $\varepsilon > 0$. Choose $v'_1, \dots, v'_n \in V'$ such that

$$\sup_{x \in \bigcup_{i,j=1}^{2} x_i^{-1} K x_j} |\varphi_v(x) - \sum_{i=1}^{n} \varphi_{v'_i}(x)| \leq \varepsilon.$$

Then, by the calculation above (and its analogue for the functions $\varphi_{v'_i}$), we have, for every $x \in K$,

$$|\varphi_{\pi(x_1)(v)+\pi(x_2)(v)}(x) - \sum_{i=1}^{n} \varphi_{\pi(x_1)(v_i)+\pi(x_2)(v_i)}(x)| \leq \varepsilon.$$

This shows that $\varphi_{\pi(x_1)(v)+\pi(x_2)(v)}$ is in the closure of $\mathscr{P}(\pi')$, that is, that $\pi(x_1)(v) + \pi(x_2)(v) \in X$.

(c). It suffices to show that the map $V \to \mathscr{P}(\pi)$, $v \longmapsto \varphi_v$ is continuous if we use the topology of compact convergence on $\mathscr{P}(\pi)$. Let $v, v' \in V$. Then, for every $x \in G$,

$$\begin{aligned} |\varphi_v(x) - \varphi_{v'}(x)| &= |\langle \pi(x)(v), v\rangle - \langle \pi(x)(v'), v'\rangle \\ &\leq |\langle \pi(x)(v - v'), v\rangle| + |\langle \pi(x)(v'), v - v'\rangle| \\ &\leq \|v - v'\|\|v\| + \|v'\|\|v - v'\|. \end{aligned}$$

So the map $v \longmapsto \varphi_v$ is continuous even for the topology on $\mathscr{P}(\pi)$ given by $\|.\|_\infty$.

(d). Let $v \in X$. By (a) and (b), for every $n \geq 1$ and all $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ and $x_1, \dots, x_n$, we have $\sum_{i=1}^{n} \lambda_i \pi(x_i)(v) \in X$. So the smallest $G$-invariant subspace of $V$ containing $v$ (i.e. $\sum_{x \in G} \pi(x)(\mathbb{C}v)$) is contained in $X$. The conclusion now follows from (c).

(e). (i) As $W_1$ is $G$-invariant, the operator $T$ is $G$-equivariant by lemma I.3.4.3. As $W = \overline{W_1 + W_2}$, the image of $W_1 + W_2$ by $T$ is dense in $\mathrm{Im}(T) = W_1^\perp$. As $\mathrm{Ker}(T) = W_1$, we have $T(W_1 + W_2) = T(W_2)$, so $T(W_2)$ is dense in $W_1^\perp$.

(ii) As $W = W_1 \oplus W_1^\perp$, we deduce that $T(W_1^\perp \cap W_2) = W_1^\perp \cap W_2$ is dense in $W_1^\perp$. As $W_2 \subset X$, question (c) implies that $W_1^\perp \subset X$.

(iii) We set $v = T(v_1 + v_2)$ and $w = v_1 + v_2 - v$. Then $v \in W_1^\perp \subset X$ and $w \in \mathrm{Ker}(T) = W_1 \subset X$, so $v, w \in X$. On other hand, for every $x \in G$, we have

$$\begin{aligned} \varphi_{v_1+v_2}(x) &= \langle \pi(x)(v_1 + v_2), v_1 + v_2\rangle \\ &= \pi(x)(v + w), v + w\rangle \\ &= \varphi_v(x) + \varphi_w(x). \end{aligned}$$

As $\overline{\mathscr{P}(\pi')}$ is stable by sums, this implies that $v_1 + v_2 \in X$.

(f). By (a), (c) and (e), the set $X$ is closed $G$-invariant subspace of $V$, so it is equal to $V$ by the hypothesis on $C$. This means that $\pi \prec \pi'$.

$\square$

**Exercise III.6.2.4.** Let $(\pi, V)$ and $(\pi', V')$ be two unitary representations of $G$ such that $\pi \prec \pi'$. Let $C$ be the closure in the weak* topology on $L^\infty(G)$ of the convex hull of the set of normalized functions of positive type associated to $\pi'$.

(a). Show that every normalized function of positive type associated to $\pi$ is in $C$.

(b). If $\pi$ is irreducible, show that every normalized function of positive type associated to $\pi$ is a limit in the topology of convergence on compact subsets of $G$ of normalized functions of positive type associated to $\pi'$. (Hint : problem III.6.2.2.)

(c). If $\pi$ is the trivial representation of $G$, show that, for every compact subset $K$ of $G$ and every $c > 0$, there exists $v' \in V'$ such that $\|v'\| = 1$ and that

$$\sup_{x \in K} \|\pi'(x)(v') - v'\| < c.$$

(d). Conversely, suppose that, for every compact subset $K$ of $G$ and every $c > 0$, there exists $v' \in V'$ such that $\|v'\| = 1$ and that

$$\sup_{x \in K} \|\pi'(x)(v') - v'\| < c.$$

Show that the trivial representation is weakly contained in $\pi'$.

*Solution.*

(a). Let $\varphi$ be a normalized function of positive type associated to $\pi$. Let $f \in L^1(G)$ and $\varepsilon > 0$. We want to find a convex combination $\psi$ of normalized functions of positive type associated to $\pi'$ such that $\left|\int_G f(\varphi - \psi)d\mu\right| \leq \varepsilon$. Pick $\delta > 0$; we will see later how small it needs to be. Let $K \ni 1$ be a compact subset of $G$ such that $\int_{G-K} |f| d\mu \leq \delta$. As $\pi \prec \pi'$, we can find $v_1, \ldots, v_n \in V'$ such that $\sup_{x \in K} |\varphi(x) - \sum_{i=1}^n \varphi_{v_i}(x)| \leq \delta$. In particular, evaluating at 1, we get $|1 - \sum_{i=1}^n \|v_i\|^2| \leq \delta$. Let $c_i = \|v\|_i^2$, $c = c_1 + \ldots + c_n$, $\varphi_i = \frac{1}{c_i}\varphi_{v_i} = \varphi_{\frac{1}{\|v_i\|}}\varphi_{v_i}$ and $\psi = \frac{1}{c}\sum_{i=1}^n \varphi_{v_i} = \frac{1}{c}\sum_{i=1}^n c_i \varphi_i$. Then $\varphi_1, \ldots, \varphi_n$ are normalized functions of positive type associated to $\pi'$, and $\psi$ is a convex combination of $\varphi_1, \ldots, \varphi_n$. In particular, $\|\psi\|_\infty \leq 1 = \|\varphi\|_\infty$.

For every $x \in K$, we have

$$\begin{aligned}|\varphi(x) - \psi(x)| &\leq |\varphi(x) - \sum_{i=1}^n \varphi_{v_i}(x)| + |1 - c||\psi(x)| \\ &\leq 2\delta.\end{aligned}$$

So

$$\begin{aligned}\left|\int_G f(\varphi - \psi)d\mu\right| &\leq \sup_{x \in K} |\varphi(x) - \psi(x)| \int_K |f| d\mu + \sup_{x \in G-K} |\varphi(x) - \psi(x)| \int_{G-K} |f| d\mu \\ &\leq 2\delta\|f\|_1 + 2\delta.\end{aligned}$$

We can make this $\leq \varepsilon$ by taking $\delta$ small enough.

(b). Let $F$ be the set of normalized functions of positive type associated to $\pi'$, and let $K$ be the weak* closure of its convex hull. Then $F$ is contained in the convex set $\mathscr{P}_1$ of all normalized functions of positive type on $G$, so $K \subset \mathscr{P}_1$. Let $\varphi$ be a normalized function of positive type associated to $\pi$. By question (a), we have $\varphi \in K$. By theorem III.3.2, the function $\varphi$ is extremal in $\mathscr{P}_1$, hence also in $K$. By problem III.6.2.2, this implies that $\varphi$ is in the closure of $F$ in the weak* topology. But $F$ and $\varphi$ are in $\mathscr{P}_1$, and the weak* topology on $\mathscr{P}_1$ coincides with the topology of convergence on compact subsets of $G$ (by Raikov's theorem, i.e. theorem III.4.3), so $\varphi$ is also in the closure of $F$ in the topology of convergence on compact subsets of $G$.

(c). As $\pi$ is the trivial representation, the only normalized function of positive type associated to $\pi$ is the constant function 1. By question (c), there exists $v' \in V'$ such that $\|v'\| = 1$ and

$$\sup_{x \in K} |1 - \langle \pi'(x)(v'), v' \rangle| \leq c^2/3.$$

Let $x \in G$. Then

$$\|\pi'(x)(v') - v'\|^2 = \|\pi'(x)(v')\|^2 + \|v'\|^2 - 2\operatorname{Re}(\langle \pi'(x)(v'), v' \rangle) \leq 2|1 - \langle \pi'(x)(v'), v' \rangle| \leq 2c^2/3,$$

so

$$\sup_{x \in K} \|\pi'(x)(v') - v'\| < c.$$

(d). Let $\pi$ be the trivial representation of $G$. Then $\mathscr{P}(\pi)$ is the set of nonnegative constant functions, so, to show that $\pi \prec \pi'$, it suffices to show that the constant function 1 is a limit of finite sums of functions of $\mathscr{P}(\pi')$ (in the topology of convergence on compact subsets of $G$). Let $K$ be a compact subset of $G$ and $c > 0$. Choose $v' \in V'$ such that $\|v'\| = 1$ and $\sup_{x \in K} \|\pi'(x)(v') - v'\| < c$, and define $\varphi'$ by $\varphi'(x) = \langle \pi'(x)(v'), v' \rangle$. Then, for every $x \in K$, we have

$$|1 - \varphi'(x)| = |\langle v', v' \rangle - \langle \pi'(x)(v'), v' \rangle| = |\langle v' - \pi'(x)(v'), v' \rangle| \leq \|v' - \pi'(x)(v')\| < c.$$

□

**Exercise III.6.2.5.** Let $G$ be a finitely generated discrete group, and let $S$ be a finite set of generators for $G$. Show that the trivial representation of $G$ is weakly contained in the regular representation of $G$ if and only, for every $\varepsilon > 0$, there exists $f \in L^2(G)$ such that

$$\sup_{x \in S} \|L_x f - f\|_2 < \varepsilon \|f\|_2.$$

*Solution.* We use the criterion of III.6.2.4(c) and (d), that says that the trivial representation of $G$ is weakly contained in the regular representation if and only if, for every compact (i.e. finite) subset $K$ of $G$ and every $\varepsilon > 0$, there exists $f \in L^2(G)$ such that $\|f\|_2 = 1$ and

$$\sup_{x \in K} \|L_x f - f\|_2 < \varepsilon.$$

First, as $S$ is finite, we see immediately that, if the trivial representation is contained in the regular representation, then the condition of the statement is satisfied.

Conversely, suppose that the condition of the statement is satisfied. Let $K$ be a finite subset of $G$, and let $\varepsilon > 0$. Let $T = S \cup S^{-1} \cup \{1\}$. We have $G = \bigcup_{n \geq 1} T^n$ because $S$ generates $G$, and this is an increasing union. As $K$ is finite, there exists $n \geq 1$ such that $T^n$. By assumption, we can find $f \in L^2(G)$ such that $\|f\|_2 = 1$ and

$$\sup_{x \in S} \|L_x f - f\|_2 \leq \tfrac{1}{n}\varepsilon.$$

We want to show that

$$\sup_{x \in K} \|L_x f - f\|_2 \leq \varepsilon.$$

It suffices to show it for $\sup_{x \in T^n}$. Let $x \in T^n$, and write $x = x_1 \ldots x_n$, with $x_1, \ldots, x_n \in T$. We show by induction on $i \in \{1, \ldots, n\}$ that $\|L_{x_1 \ldots x_i} f - f\|_2 \leq \frac{i}{n}\varepsilon$. If $i = 1$, we want to show that $\|L_{x_1} f - f\|_2 \leq \frac{1}{n}\varepsilon$. This is true by the choice of $f$ if $x_1 \in S$, it is obvious if $x_1 = 1$, and, if $x_1 \in S^{-1}$, it follows from the fact that

$$\|L_{x_1} f - f\|_2 = \|f - L_{x_1^{-1}} f\|_2.$$

Now suppose the result known for $i \in \{1, \ldots, n-1\}$, and let's prove it for $i+1$. We have

$$\begin{aligned}\|L_{x_1 \ldots x_{i+1}} f - f\|_2 &\leq \|L_{x_1 \ldots x_i}(L_{x_{i+1}} f - f)\|_2 + \|L_{x_1 \ldots x_i} f - f\|_2 \\ &= \|L_{x_{i+1}} f - f\|_2 + \|L_{x_1 \ldots x_i} f - f\|_2 \\ &\leq \tfrac{i}{n}\varepsilon + \tfrac{1}{n}\varepsilon = \tfrac{i+1}{n}\varepsilon.\end{aligned}$$

□

**Exercise III.6.2.6.** Let $G = \mathbb{Z}$. Show that the trivial representation of $G$ is weakly contained in the regular representation of $G$.

*Solution.* We apply the result of problem III.6.2.5, with $S = \{1\}$. So, for every $\varepsilon > 0$, we must find $f \in L^2(\mathbb{Z})$ such that $\|f\|_2 = 1$ and $\|L_1 f - f\|_2 \leq \varepsilon$. The first condition says that $\sum_{n \in \mathbb{Z}} |f(n)|^2 = 1$, and the second condition that $\sum_{n \in \mathbb{Z}} |f(n-1) - f(n)|^2 \leq \varepsilon^2$. Let $N \in \mathbb{Z}_{\geq 0}$, and consider the function $g_N = \mathbb{1}_{[0,N]} \in L^2(\mathbb{Z})$. Then $\|g_N\|_2^2 = N+1$, and $\sum_{n \in \mathbb{Z}} |g(n-1) - g(n)|^2 = 2$. So, if $f_N = \frac{1}{\sqrt{N+1}}$, we have $\|f\|_2 = 1$ and $\|L_1 f - f\|_2 = \frac{\sqrt{2}}{\sqrt{N+1}}$. Taking $N$ big enough, we see that $f_N$ has the desired properties.

□

**Exercise III.6.2.7.** Let $G = \mathbb{R}$.

(a). Show that the trivial representation of $G$ is weakly contained in the regular representation of $G$.

(b). Show that every irreducible unitary representation of $G$ is weakly contained in the regular representation of $G$. [5] [6]

*Solution.*

(a). If $a, b \in \mathbb{R}$ are such that $a < b$, let $f = (b-a)^{-1/2}\mathbb{1}_{[a,b]}$. Then $f \in L^2(\mathbb{R})$ and we have $\|f\|_2 = 1$. Moreover, for every $t \in \mathbb{R}$, we have $L_t f = (b-a)^{-1/2}\mathbb{1}_{[a+t,b+t]}$, so

$$\|L_t f - f\|_2^2 \leq \frac{2|t|}{b-a}.$$

Let $K$ be a compact subset of $\mathbb{R}$, and let $\varepsilon > 0$. If we choose $a, b \in \mathbb{R}$ such that $b - a \geq 2\varepsilon^{-2}\sup_{t\in K}|t|$, then the construction above gives a $f \in L^2(\mathbb{R})$ such that $\|f\|_2 = 1$ and $\sup_{x\in K}\|L_t f - f\|_2 \leq \varepsilon$. By 6(d), the trivial representation of $\mathbb{R}$ is contained in its regular representation.

(b). As $\mathbb{R}$ is abelian, every irreducible unitary representation is 1-dimensional by Schur's lemma (theorem I.3.4.1). Let $\chi : \mathbb{R} \to S^1$ be such a representation. Let $K$ be a compact subset of $\mathbb{R}$ and $\varepsilon > 0$. By (a), there exists $f \in L^2(\mathbb{R})$ such that $\|f\|_2 = 1$ and $\sup_{t\in K}\|L_t f - f\|_2 \leq \varepsilon$. Let $g = \overline{\chi} f$. Then, for every $t \in \mathbb{R}$, we have

$$\langle L_t g, g\rangle_{L^2(\mathbb{R})} = \int_{\mathbb{R}} g(x-t)\overline{g(x)}dx = \chi(t)\langle L_t f, f\rangle_{L^2(\mathbb{R})},$$

hence

$$|\chi(t) - \langle L_t g, g\rangle_{L^2(\mathbb{R})}| = |1 - \langle L_t f, f\rangle_{L^2(\mathbb{R})}| = |\langle f - L_t f, f\rangle_{L^2(\mathbb{R})}| \leq \|L_t f - f\|_2.$$

So

$$\sup_{t\in K}|\chi(t) - \langle L_t g, g\rangle_{L^2(\mathbb{R})}| \leq \varepsilon.$$

This implies the desired result by III.6.2.4(d).

□

**Exercise III.6.2.8.** Let $G$ be the free (nonabelian) group on two generators, with the discrete topology. Show that the trivial representation of $G$ is not weakly contained in the regular representation of $G$.

[7]

*Solution.* Let $a, b \in G$ be the two generators of $G$, and let $S = \{1, a, b, a^{-1}, b^{-1}\}$. We have $G = \bigcup_{n\geq 1} S^n$, and this is an increasing union. Suppose that the trivial representation of $G$ is

[5] We will see later that this is true for every abelian locally compact group.
[6] Where ?
[7] Should be in the next section.

weakly contained in the regular representation. Then, by III.6.2.4(c), for every $n \geq 1$, there exists $f_n \in L^2(G)$ such that $\|f_n\|_2 = 1$ and

$$\sup_{x \in S_n} \|L_x f_n - f_n\|_2 \leq \tfrac{1}{n}.$$

Let $g_n = |f_n|^2$. Then $g_n \in L^1(G)$, $\|g_n\|_1 = 1$, and, for every $x \in S_n$, the Cauchy-Schwarz inequality gives

$$\|L_x g_n - g_n\|_1 \leq \|L_x f_n - f_n\|_2 \|L_x f_n + f_n\|_2 \leq \frac{2}{n}.$$

For every $n \geq 1$, we define a continuous linear functional $\Lambda_n$ on $L^\infty(G)$ by $\Lambda_n(\varphi) = \sum_{x \in G} g_n(x)\varphi(x)$. Then $\|\Lambda_n\|_{op} = \|g_n\|_1 = 1$, so, by the Banach-Alaoglu theorem, there is a subsequence $(\Lambda_{n_k})_{k \geq 0}$ of $(\Lambda_n)_{n \geq 1}$ that converges for the weak* topology on $\mathrm{Hom}(L^\infty(G), \mathbb{C})$. Let $\Lambda$ be its limit. Let $\varphi \in L^\infty(G)$. We have

$$\Lambda(\varphi) = \lim_{k \to +\infty} \Lambda_{n_k}(\varphi).$$

Let $y \in G$. There exists $n \geq 1$ such that $y^{-1} \in S_n$. Then, if $k$ is such that $n_k \geq n$, we have

$$\begin{aligned}
|\Lambda_{n_k}(L_y\varphi) - \Lambda_{n_k}(\varphi)| &= |\sum_{x \in G} L_{y^{-1}} g_{n_k}(x)\varphi(x) - \sum_{x \in G} g_{n_k}(x)\varphi(x)| \\
&\leq \|L_{y^{-1}} g_{n_k} - g_{n_k}\|_1 \|\varphi\|_\infty \\
&\leq \frac{2}{n_k}\|\varphi\|_\infty.
\end{aligned}$$

Taking the limit as $k \to +\infty$, we see that $\Lambda(L_y\varphi) = \Lambda(\varphi)$. As, note that $\Lambda(1) = 1$, and that $\Lambda(\varphi) \geq 0$ if $\varphi$ takes nonnegative values.

Remember that every element of $G$ can be written in a unique way as a reduced word in $a$, $b$, $a^{-1}$ and $b^{-1}$. Let $A$ be the set of elements of $G$ whose reduced expression begins with a nonzero power of $a$. The, for every $x \in G$, if $x \notin A$, we have $a^{-1}x \in A$ and then $x \in aA$. In other words, $G = A \cup aA$, so $\mathbb{1}_A + \mathbb{1}_{aA} - \mathbb{1}_G$ takes nonnegative values, hence

$$\Lambda(\mathbb{1}_A) = \frac{1}{2}(\Lambda(\mathbb{1}_A) + \Lambda(\mathbb{1}_{aA})) \geq \frac{1}{2}\Lambda(\mathbb{1}_G) = \frac{1}{2}.$$

On the other hand, the group $G$ is the disjoint union of the subset $b^nA$, $n \in \mathbb{Z}$, so we have in particular

$$1 = \Lambda(\mathbb{1}_G) \geq \Lambda(\mathbb{1}_A) + \Lambda(\mathbb{1}_{bA}) + \Lambda(\mathbb{1}_{b^2A}) = 3\Lambda(\mathbb{1}_A),$$

that is, $\Lambda(\mathbb{1}_A) \leq \frac{1}{3}$. So we get a contradiction.

□

**Exercise III.6.2.9.** If $\pi_1, \pi_2, \pi_1', \pi_2'$ are unitary representations of $G$ such that $\pi_1 \prec \pi_1'$ and $\pi_2' \prec \pi_2$, show that $\pi_1 \otimes \pi_2 \prec \pi_1' \otimes \pi_2'$.

*Solution.* We use the same notation $\varphi_v$ for functions of positive type as in the solution of problem III.6.2.3. For $i = 1, 2$, we denote by $V_i$ (resp. $V_i'$) the space of $\pi_i$ (resp. $\pi_i'$).

If $v_1 \in V_1$ and $v_2 \in V_2$, then, by definition of the inner product on $V_1 \otimes_{\mathbb{C}} V_2$, we have $\varphi_{v_1 \otimes v_2} = \varphi_{v_1}\varphi_{v_2}$. There is similar result for pure tensors in $V_1' \otimes_{\mathbb{C}} V_2'$. So $\varphi_{v_1\otimes v_2}$ is in $\overline{\mathscr{P}(\pi_1' \otimes \pi_2')}$. As $\overline{\mathscr{P}(\pi_1' \otimes \pi_2')}$ is stable by finite sums, and as every element of $V_1 \otimes_{\mathbb{C}} V_2$ can be written as a finite sum of an orthogonal family of pure tensors (see the proof of 1(a)), this implies that $\varphi_v \in \overline{\mathscr{P}(\pi_1' \otimes \pi_2')}$ for every $v \in V_1 \otimes_{\mathbb{C}} V_2$. Finally, we have proved in 5(c) that the map $v \longmapsto \varphi_v$ is continuous, and $V_1 \otimes_{\mathbb{C}} V_2$ is dense in $V_1 \widehat{\otimes}_{\mathbb{C}} V_2$, so $\varphi_v \in \overline{\mathscr{P}(\pi_1' \otimes \pi_2')}$ for every $v \in V_1 \widehat{\otimes}_{\mathbb{C}} V_2$.

□

**Exercise III.6.2.10.** Suppose that $G$ is discrete. For every $x \in G$, we denote by $\delta_x \in L^2(G)$ the characteristic function of $\{x\}$.

Let $(\pi, V)$ be a unitary representation of $G$, and let $(\pi_0, V)$ be the trivial representation of $G$ on $V$ (i.e. $\pi_0(x) = \mathrm{id}_V$ for every $x \in G$).

(a). Show that the formula $v \otimes f \longmapsto \sum_{x\in G} f(x)(\pi(x)^{-1}(v)) \otimes \delta_x$ gives a well-defined and continuous $\mathbb{C}$-linear transformation from $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$ to itself.

(b). Show that the representations $\pi \otimes \pi_L$ and $\pi_0 \otimes \pi_L$ are equivalent (remember that $\pi_L$ is the left regular representation of $G$).

*Solution.*

(a). First, the map $V \times L^2(G) \to V \otimes_{\mathbb{C}} L^2(G)$, $(v, f) \longmapsto \sum_{x\in G} f(x)(\pi(x)^{-1}(v)) \otimes \delta_x$ is bilinear, so it defines a linear map $\alpha : V \otimes_{\mathbb{C}} L^2(G) \to V \otimes_{\mathbb{C}} L^2(G)$. For every $v, v' \in V$ and $f, f' \in L^2(G)$, we have (observing that the family $(v_x \otimes \delta_x)_{x\in G}$ is orthogonal for every family $(v_x)_{x\in G}$ of elements of $V$)

$$\begin{aligned}\langle \alpha(v \otimes f), \alpha(v' \otimes f')\rangle &= \sum_{x\in G} f(x)\overline{f'(x)}\langle \pi(x)^{-1}(v), \pi(x)^{-1}(v')\rangle \\ &= \sum_{x\in G} f(x)\overline{f'(x)}\langle v, v'\rangle \\ &= \langle v \otimes f, v' \otimes f'\rangle.\end{aligned}$$

Using the fact that every element of $V \otimes_{\mathbb{C}} L^2(G)$ can be written as a finite sum or pairwise orthogonal pure tensors (see the proof of 1(a)), this implies that $\|\alpha(v)\| = \|v\|$ for every $v \in V \otimes_{\mathbb{C}} L^2(G)$. In particular, $\alpha$ is continuous, so it extends to a continuous endomorphism of $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$, which is still an isometry.

(b). We still call $\alpha$ the endomorphism of $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$ constructed in (a). We show that it is a $G$-equivariant map from $\pi \otimes \pi_L$ to $\pi_0 \otimes \pi_L$. As pure tensors generates a dense subspace of $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$, it suffices to check the $G$-equivariance on them. So let $v \in V$ and $f \in L^2(G)$, and let $x \in G$. We have

$$\alpha(\pi \otimes \pi_L(x)(v \otimes f)) = \alpha(\pi(x)(v) \otimes L_x f) = \sum_{y \in G} f(x^{-1}y)\pi(y^{-1}x)(v) \otimes \delta_y.$$

On the other hand,

$$\begin{aligned}
\pi_0 \otimes \pi_L(x)(\alpha(v \otimes f)) &= \pi_0 \otimes \pi_L(x) \left( \sum_{y \in G} f(y)\pi(y)^{-1}(v) \otimes \delta_y \right) \\
&= \sum_{y \in G} f(y)\pi(y)^{-1}(v) \otimes L_x \delta_y \\
&= \sum_{y \in G} f(y)\pi(y)^{-1}(v) \otimes \delta_{xy} \\
&= \sum_{y \in G} f(x^{-1}z)\pi(z^{-1}x)(v) \otimes \delta_z \\
&= \alpha(\pi \otimes \pi_L(x)(v \otimes f)).
\end{aligned}$$

We still need to check that $\alpha$ is an isomorphism of vector spaces. This follows from the fact that is has an inverse $\beta$, given by the formula $\beta(v \otimes f) = \sum_{x \in G} f(x)\pi(x)(v) \otimes \delta_x$. (We can check as in (a) that $\beta$ is well-defined and continuous, and then we can check on pure tensors that it is the inverse of $\alpha$, which is an easy verification.)

Note that the isomorphism betweem $\pi \otimes \pi_L$ and $\pi_0 \otimes \pi_L$ is an isometry, so these representations have the same functions of positive type.

□

**Exercise III.6.2.11.** Generalize the result of III.6.2.10(b) to non-discrete locally compact groups.

*Solution.* Let $(\pi, V)$ be a unitary representation of $G$. We write $V_0$ for $V$ with the trivial action of $G$.

First we define a Hilbert space $L^2(G, V_0)$ with a unitary action of $G$. (This is also often denoted by $\mathrm{Ind}_{\{1\}}^G V_0$.) Consider the space $\mathscr{C}_c(G, V_0)$ of continuous functions with compact support from $G$ to $V_0$, with the norm $\|.\|_\infty$ defined by $\|f\|_\infty = \sup_{x \in G} \|f(x)\|$. We make $G$ act on this space by $(x, f) \longmapsto L_x f$, for $x \in G$ and $f \in \mathscr{C}_c(G, V_0)$. Looking at proposition I.1.12, we see that its proof generalizes to functions from $G$ to $V_0$ and show that every element of $\mathscr{C}_c(G, V_0)$ is left and right uniformly continuous. In particular, for every $f \in \mathscr{C}_c(G, V_0)$, the map $G \to \mathscr{C}_c(G, V_0)$, $x \longmapsto L_x f$ is continuous.

Now we define a Hermitian sesquilinear form on $\mathscr{C}_c(G, V_0)$ by

$$\langle f, g \rangle = \int_G \langle f(x), g(x) \rangle_{V_0} dx.$$

It is easy to see that this is an inner form, and that the action of $G$ on $\mathscr{C}_c(G, V_0)$ preserves this inner form and is continuous in the first variable $x \in G$ for the topology on $\mathscr{C}_c(G, V_0)$ defined by the associated norm. We denote by $L^2(G, V_0)$ the completion of $\mathscr{C}_c(G, V_0)$ for $\langle ., . \rangle$. This is a Hilbert space, and we show as in the case $V_0 = \mathbb{C}$ that the action of $G$ on $\mathscr{C}_c(G, V_0)$ extends to a unitary action of $G$ on $L^2(G, V_0)$.

We now construct a $G$-equivariant isometry $V \widehat{\otimes}_{\mathbb{C}} L^2(G) \to L^2(G, V_0)$. Consider the map $V \times \mathscr{C}_c(G) \to L^2(G, V_0)$ sending $(v, f)$ to the function $x \longmapsto f(x)\pi(x^{-1})(v)$. This is a bilinear map, so it induces a $\mathbb{C}$-linear operator $\alpha : V \otimes_{\mathbb{C}} \mathscr{C}_c(G) \to L^2(G, V_0)$. We check that $\alpha$ is $G$-equivariant. It suffices to check it on pure tensors, because they generate $V \otimes_{\mathbb{C}} \mathscr{C}_c(G)$. If $y \in G$, $v \in V$ and $f \in \mathscr{C}_c(G)$, then, for every $x \in G$,

$$\begin{aligned} \alpha(\pi(y)(v) \otimes L_y f)(y) &= f(y^{-1}x)\pi(xy^{-1}v) \\ &= L_y(\alpha(v \otimes f))(x). \end{aligned}$$

We also check that $\alpha$ preserves the inner forms. As before, by bilinearity, it suffices to check it on pure tensors. Let $v, w \in V$ and $f, g \in \mathscr{C}_c(G)$. Then

$$\begin{aligned} \langle \alpha(v \otimes f), \alpha(w \otimes g) \rangle &= \int_G \langle f(x)\pi(x)^{-1}(v), g(x)\pi(x)^{-1}(w) \rangle_{V_0} dx \\ &= \int_G f(x)\overline{g(x)} \langle v, w \rangle_{V_0} dx \\ &= \langle f, g \rangle_{L^2(G)} \langle v, w \rangle_{V_0}. \end{aligned}$$

This implies that $\alpha$ is an isometry, hence that it extends by continuity to an isometry $V \widehat{\otimes}_{\mathbb{C}} L^2(G) \to L^2(G, V_0)$ (we use the fact that $\mathscr{C}_c(G)$ is dense in $L^2(G)$), which is still $G$-equivariant.

We define a $G$-equivariant isometry $\alpha' : V_0 \widehat{\otimes}_{\mathbb{C}} L^2(G) \to L^2(G, V_0)$ in a way similar to $\alpha$, but, for $v \in V_0$ and $f \in \mathscr{C}_c(G)$, we take $\alpha'(v \otimes f)$ to be the function $x \longmapsto f(x)v$. The proof that this does define the deisred $G$-equivariant isometry is the same as in the case of $\alpha$.

Finally, we show that $\alpha$ and $\alpha'$ are isomorphisms. We already know that they are injective and have closed image because they are isometries, so we just need to show that they have dense image.

Let $(e_i)_{i \in I}$ be a Hilbert basis of $V_0$. Consider the subspace $W$ of $L^2(G, V_0)$ whose elements are continuous functions with compact support $f : G \to V_0$ such that there exists $J \subset I$ finite with $f(G) \subset \mathrm{Span}(e_j, j \in J)$. Let's show that $W$ is dense in $L^2(G, V_0)$. It suffices to show that $W$ is dense in $\mathscr{C}_c(G, V_0)$. Let $f \in \mathscr{C}_c(G, V_0)$. As $f$ has compact support, the subset $f(G)$ of $V_0$ is compact. Let $\varepsilon > 0$. For every $x \in K$, there exists a finite subset $J$ of $I$ such that the closed ball centered at $x$ and of radius $\varepsilon$ intersects $\mathrm{Span}(e_j, j \in J)$. As $K$ is compact, it can be covered by a finite number of these balls, so we can find s finite subset $J$ of $I$ such that the distance between $x$ and $\mathrm{Span}(e_j, j \in J)$ is $\leq \varepsilon$ for every $x \in K$. In other words, if $\pi_J$ is the orthogonal projection on $\mathrm{Span}(e_j, j \in J)$, then $\|\pi_J(x) - x\| \leq \varepsilon$ for every $x \in K$. Then $\pi_J \circ f \in W$, and

$\|f - \pi_J \circ f\|_\infty \leq \varepsilon$, so $\|f - \pi_J \circ f\|_2 \leq \mathrm{vol}(\mathrm{supp}\, f)\varepsilon$. This shows that $W$ is dense in $\mathscr{C}_c(G, V_0)$ for both topologies on $\mathscr{C}_c(G, V_0)$ (the one induced by $\|.\|_\infty$ and the one induced by $\|.\|_2$; only the second one is relevant here). To finish, it suffices to show that $W$ is contained in the images of $\alpha$ and $\alpha'$. Let $f \in W$. We can find a finite subset $J$ of $I$ such that $f(G) \subset \mathrm{Span}(e_j, j \in J)$, and then we have $f(x) = \sum_{j \in J} f_j(x) e_j$, with the $f_j$ in $\mathscr{C}_c(G)$. (Just take coordinates in the orthonormal basis $(e_j)_{j \in J}$ of $\mathrm{Span}(e_j, j \in J)$). In particular, $f = \alpha'(\sum_{j \in J} e_j \otimes f_j)$, so $f \in \mathrm{Im}(\alpha')$. This shows that $\alpha'$ is an isomorphism.

For $\alpha$, we consider instead the subspace $W'$ of $f \in \mathscr{C}_c(G, V_0)$ such that there exists $J \subset I$ finite such that, for every $x \in G$, the vector $\pi(x)(f(x))$ is in $\mathrm{Span}(e_j, j \in J)$. We show as before that $W'$ is dense in $\mathscr{C}_c(G, V_0)$ (for both $\|.\|_\infty$ and $\|.\|_2$) : Let $f \in \mathscr{C}_c(G, V_0)$ and $\varepsilon > 0$. As $f$ has compact support, the subset $\{\pi(x)(f(x)),\ x \in G\}$ of $V_0$ is compact, so we can find a finite subset $J$ of $I$ such that, for every $x \in G$, the distance between $\pi(x)(f(x))$ and $\mathrm{Span}(e_j, j \in J)$ is at most $\varepsilon$. Let $\pi_J$ be the orthogonal projection on $\mathrm{Span}(e_j, j \in J)$, and define $g \in W'$ by $g(x) = \pi(x)^{-1} \circ \pi_J \circ \pi(x)(f(x))$. For every $x \in G$,

$$\|g(x) - f(x)\| = \|\pi(x)(g(x) - f(x))\| = \|\pi_J(\pi(x)(f(x))) - \pi(x)(f(x))\| \leq \varepsilon,$$

so $\|g - f\|_\infty \leq \varepsilon$ and $\|g - f\|_2 \leq \mathrm{vol}(\mathrm{supp}\, f)\varepsilon$. Finally, we show that $W'$ is contained in the image of $\alpha$. Let $f \in W'$, and define $g \in \mathscr{C}_c(G, V_0)$ by $g(x) = \pi(x)(f(x))$. Choose a finite subset $J$ of $I$ such that $g(G) \subset \mathrm{Span}(e_j, j \in J)$, and write $g = \sum_{j \in J} g_j e_j$, with $g_j \in \mathscr{C}_c(G)$. Then, for every $x \in G$, we have

$$f(x) = \sum_{j \in J} g_j(x) \pi(x)^{-1}(e_j).$$

In other words, we have $f = \alpha(\sum_{j \in J} e_j \otimes g_j)$.

□

**Exercise III.6.2.12.** Show that the following are equivalent :

(i) The trivial representation of $G$ is weakly contained in $\pi_L$.

(ii) Every unitary representation of $G$ is weakly contained in $\pi_L$.

*Solution.* The fact that (ii) implies (i) is obvious. So let's show that (i) implies (ii). Let $(\pi, V)$ be a unitary representation of $G$, let $\pi_0$ be the trivial representation of $G$ on $V$, and let $\mathbb{1}$ be the trivial representation of $G$ on $\mathbb{C}$. We know that $\mathbb{1} \prec \pi_L$, so, by exercises III.6.2.9 and III.6.2.10, we have $\pi \simeq \pi \otimes \mathbb{1} \prec \pi \otimes \pi_L \simeq \pi_0 \otimes \pi_L$.

As in the solution of exercise III.6.2.3, for every unitary representation $\pi'$ of $G$, we denote by $\overline{\sum \mathscr{P}(\pi')}$ the set of finite sums of functions of positive type associated to $\pi$. Let's show that $\overline{\sum \mathscr{P}(\pi_L)} = \overline{\sum \mathscr{P}(\pi_0 \otimes \pi_L)}$, which will finish the proof, because we already know that $\mathscr{P}(\pi) \subset \overline{\sum \mathscr{P}(\pi_0 \otimes \pi_L)}$.

As $\pi_L$ is a subrepresentation of $\pi_0 \otimes \pi_L$ (for every $v \in V - \{0\}$, the subspace $\mathbb{C}v \otimes L^2(G)$ of $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$ is $G$-invariant and equivalent to the representation $\pi_L$ by the map $v \otimes f \longmapsto f$), we have $\mathscr{P}(\pi_L) \subset \mathscr{P}(\pi_0 \otimes \pi_L)$, so $\overline{\sum \mathscr{P}(\pi_L)} \subset \overline{\sum \mathscr{P}(\pi_0 \otimes \pi_L)}$. Conversely, let $(e_i)_{i\in I}$ be an orthonormal basis of $V$, and let $v \in V \widehat{\otimes}_{\mathbb{C}} L^2(G)$. Then we can write $v = \sum_{i\in I} e_i \otimes f_i$, where the sum converges in $V \widehat{\otimes}_{\mathbb{C}} L^2(G)$ (i.e. $\sum_{i\in I} \|f_i\|^2$ converges). Then, for every $x \in G$, we have

$$\langle \pi_0 \otimes \pi_L(x)(v), v\rangle = \sum_{i\in I} \langle L_x f_i, f_i\rangle_{L^2(G)},$$

so the function $x \longmapsto \langle \pi_0 \otimes \pi_L(x)(v), v\rangle$ is in $\overline{\sum \mathscr{P}(\pi_L)}$.

□

## III.6.3 Amenable groups

Let $(X, \mu)$ be a measure space. and let $E$ be a closed linear subspace of $L^\infty(X)$ containing the constant functions and closed under the map $\varphi \longmapsto \overline{\varphi}$. A *mean* on $E$ is a linear functional $M : E \to \mathbb{C}$ such that :

(i) $M(\mathbb{1}_X) = 1$;

(ii) if $f \geq 0$ (locally) almost everywhere, then $M(f) \geq 0$.

If $X = G$ is a locally compact group, we say that a mean $M$ on $E$ is *$G$-invariant* if for every $f \in E$ and every $x \in G$, we have $L_x f \in E$ and $M(L_x f) = M(f)$.

The group $G$ is called *amenable* is there exists a $G$-invariant mean on $L^\infty(G)$.

Let $V$ be a locally convex topological vector space (see definition B.3.5), let $K$ be a convex subset of $V$. We say that a map $f : K \to K$ is *affine* if, for all $v, w \in K$ and every $t \in [0, 1]$, we have $f(tv + (1-t)w) = tf(v) + (1-t)f(w)$. Let $G \times K \to K$, $(x, v) \longmapsto x \cdot v$ be a continuous left action of $G$ on $X$. We say that this action is an *affine action* if, for every $x \in G$, the map $K \to K$, $v \longmapsto x \cdot v$ is affine.

We say that the group $G$ has the *fixed point property* if every affine action of $G$ on a nonempty compact convex subset of a locally convex topological vector space has a fixed point.

Note : The Hahn-Banach theorem is your friend in this series of problems. Also the fact that, if $V$ is a topological vector space, then any weak* continuous linear functional on $\mathrm{Hom}(V, \mathbb{C})$ is of the form $\Lambda \longmapsto \Lambda(v)$, for some $v \in V$. (See theorem 3.10 of Rudin's [20].)

**Exercise III.6.3.1.** (a). If $(X, \mu)$ is a measure space and $E$ is a subspace of $L^\infty(X)$ containing the constant functions, show that any mean $M$ on $E$ is automatically continuous (for the topology given by the norm $\|.\|_\infty$) and that $\|M\|_{op} = 1$.

We now suppose that $G$ is a locally compact group.

(a). If $G$ is compact, show that left invariant means on $\mathscr{C}(G)$ are in natural bijection with normalized Haar measures on $G$.

(b). Let $L^1(G)_{1,+}$ be the convex subset of $f \in L^1(G)$ such that $f \geq 0$ almost everywhere and $\|f\|_1 = 1$. We identify $L^1(G)$ to a subspace of the continuous dual of $L^\infty(G)$ in the usual way (i.e. a function $f \in L^1(G)$ corresponds to the continuous linear functional $\varphi \longmapsto \int_G f\varphi d\mu$ on $L^\infty(G)$). Show that $L^1_{1,+}(G)$ is weak* dense in the set of means on $L^\infty(G)$.

(c). Let $UCB(G)$ be the subspace of $L^\infty(G)$ composed of the left uniformly continuous bounded functions on $G$. For every $x \in G$, we write $\delta_x$ for the linear functional $\mathscr{C}(G) \to \mathbb{C}$, $f \longmapsto f(x)$. Show that the set of convex combinations of functionals $\delta_x$ (that is, the set of sums $\sum_{i=1}^n a_i\delta_{x_i}$, with $x_1, \dots, x_n \in G$ and $a_1, \dots, a_n \in [0,1]$ such that $a_1 + \dots + a_n = 1$) is weak* dense in the set of means on $UCB(G)$.

*Solution.*

(a). Let $M$ be a mean on $E$. Let $\varphi \in E$, and suppose that $\varphi(x) \in \mathbb{R}$ for almost every $x$. We have $\|\varphi\|_\infty \mathbb{1}_X \in E$, because it is a multiple of the constant function $\mathbb{1}_X$, and the functions $\|\varphi\|_\infty \mathbb{1}_X - \varphi$ and $\|\varphi\|_\infty \mathbb{1}_X + \varphi$ are $\geq 0$ almost everywhere, so their image by $M$ is $\geq 0$, that is, $M(\varphi) \in \mathbb{R}$ and
$$-\|\varphi\|_\infty \leq M(\varphi) \leq \|\varphi\|_\infty,$$
i.e. $|M(\varphi)| \leq \|\varphi\|_\infty$.

Now let $\varphi$ be any element of $E$. Choose $c \in \mathbb{C}$ such that $|c| = 1$ and $M(c\varphi) \in \mathbb{R}$. Let $\varphi_1 = \frac{1}{2}(c\varphi + \overline{c\varphi})$ and $\varphi_2 = \frac{1}{2i}(c\varphi - \overline{c\varphi})$. Then $\varphi_1, \varphi_2$ have real values and $c\varphi = \varphi_1 + i\varphi_2$. We have
$$|\varphi(x)| = \sqrt{\varphi_1(x)^2 + \varphi_2(x)^2} \geq \max(|\varphi_1(x)|, |\varphi_2(x)|)$$
for every $x \in X$, so $\|\varphi\|_\infty \geq \max(\|\varphi_1\|_\infty, \|\varphi_2\|_\infty)$. On the other hand, $M(c\varphi) = M(\varphi_1) + iM(\varphi_2)$ and $M(\varphi_1), M(\varphi_2) \in \mathbb{R}$, so $M(\varphi_2) = 0$, and
$$|M(\varphi)| = |M(c\varphi)| = |M(\varphi_1)| \leq \|\varphi_1\|_\infty \leq \|\varphi\|_\infty.$$

This shows that $M$ is continuous and that $\|M\|_{op} \leq 1$. As $M(\mathbb{1}_X) = 1 = \|\mathbb{1}_X\|_\infty$, we have $\|M\|_{op} = 1$.

(b). This is just the Riesz representation theorem (theorem I.2.3) and proposition I.2.6.

(c). Let $\mathscr{M}$ be the set of means on $L^\infty(G)$. It is clearly a convex subset of $\mathrm{Hom}(L^\infty(G), \mathbb{C})$. By question (a), the set $\mathscr{M}$ is contained in the closed unit ball of $\mathrm{Hom}(L^\infty(G), \mathbb{C})$. Also, as the conditions characterizing a mean are all closed for the weak* topology, the set $\mathscr{M}$ is weak* closed in $\mathrm{Hom}(L^\infty(G), \mathbb{C})$. So $\mathscr{M}$ is weak* compact.

By definition of $L^1(G)_{1,+}$, for every $f \in L^1(G)_{1,+}$, the corresponding linear form on $L^\infty(G)$ is an element of $\mathscr{M}$. Note also that $L^1(G)_{1,+}$ is a convex subset of $L^1(G)$, so its image in $\mathrm{Hom}(L^\infty(G), \mathbb{C})$ is also convex. Let $\mathscr{M}'$ be the weak* closure of this image. We have $\mathscr{M}' \subset \mathscr{M}$, so $\mathscr{M}'$ is convex and weak* compact. Suppose that $\mathscr{M}' \neq \mathscr{M}$. Then, by the Hahn-Banach theorem (second geometric form), there exists

$M \in \mathscr{M}$ and a weak* continuous $\mathbb{R}$-linear operator $\Lambda : \mathrm{Hom}(L^\infty(G), \mathbb{C}) \to \mathbb{R}$ such that $\Lambda(M) > \sup_{M' \in \mathscr{M}'} \Lambda(M')$. Note that the linear operator $\Lambda' : M' \longmapsto \Lambda(M) + \frac{1}{i}\Lambda(iM')$ is weak* continuous and $\mathbb{C}$-linear, so there exists $\varphi \in L^\infty(G)$ such that $\Lambda'(M') = M'(\varphi)$ for every $M' \in \mathrm{Hom}(L^\infty(G), \mathbb{C})$, which gives $\Lambda(M') = \mathrm{Re}(M'(\varphi))$. Then we have

$$\mathrm{Re}\, M(\varphi) > \sup_{f \in L^1(G)_{1,+}} \left( \mathrm{Re} \int_G f \varphi d\mu \right).$$

Write $\varphi = \varphi_1 + i\varphi_2$, with $\varphi_1 = \mathrm{Re}\,\varphi$ and $\varphi_2 = \mathrm{Im}\,\varphi$. Then

$$M(\varphi_1) > \sup_{f \in L^1(G)_{1,+}} \int_G f \varphi_1 d\mu$$

(because $M(\varphi_1), M(\varphi_2) \in \mathbb{R}$ by the solution of question (a)). Let

$$c = \inf\{d \in \mathbb{R} | \varphi_1 \leq d\mathbb{1}_G \text{ locally almost everywhere}\}.$$

If $\varphi_1 \leq d\mathbb{1}_G$ locally almost everywhere, then $M(\varphi_1) \leq M(d\mathbb{1}_G) = d$. So $M(\varphi_1) \leq c$. Let $\delta > 0$ such that $M(\varphi_1) - \delta > \sup_{f \in L^1(G)_{1,+}} \int_G f \varphi_1 d\mu$. By definition of $c$, there exists a measurable subset $A$ of $G$ such that $\mu(A) > 0$ and $\varphi_{1|A} \geq (c + \delta)\mathbb{1}_A$. Let $f = \mu(A)^{-1}\mathbb{1}_A$. Then $f \in L^1(G)_{1,+}$ and $\int_G \varphi_1 f d\mu \geq c + \delta \geq M(\varphi_1) + \delta$, a contradiction.

(d). Let $\mathscr{M}$ be the set of means on $UCB(G)$. We see as in the solution of (c) that $\mathscr{M}$ is a convex and weak* compact subset of $\mathrm{Hom}(UCB(G), \mathbb{C})$. Let $\mathscr{M}'$ be the weak* closure of the convex hull of the $\delta_x$, $x \in G$; then $\mathscr{M}' \subset \mathscr{M}$ because each $\delta_x$ is in $\mathscr{M}$. If $\mathscr{M}' \neq \mathscr{M}$, then, by the Hahn-Banach theorem (second geometric version), there exists an element $M$ of $\mathscr{M}$ and a continuous $\mathbb{R}$-linear functional $\Lambda : \mathrm{Hom}(UCB(G), \mathbb{C}) \to \mathbb{R}$ such that

$$\Lambda(M) > \sup_{M' \in \mathscr{M}'} \Lambda(M').$$

As in the solution of (c), we see that we can find a function $\varphi \in UCB(G)$ having real values and such that $\Lambda(M') = M'(\varphi)$ for every $M' \in \mathscr{M}$. So we have

$$M(\varphi) > \sup_{M' \in \mathscr{M}'} M'(\varphi) \geq \sup_{x \in G} \delta_x(\varphi) = \sup_{x \in G} \varphi(x).$$

Let $\delta > 0$ be such that $M(\varphi) - \delta \geq \sup_{x \in G} \varphi(x)$. Then $\varphi \leq (M(\varphi) - \delta)\mathbb{1}_G$, and so $M(\varphi) \leq M(\varphi) - \delta$, a contradiction.

□

**Exercise III.6.3.2.** Let $G$ be an amenable locally compact group. The goal of this problem is to prove that $G$ has the fixed point property.

So let $V$ be a locally convex topological vector space, let $K$ be a nonempty compact convex subset of $V$, and let $G \times K \to K$, $(x, v) \longmapsto x \cdot v$ be a continuous affine action.

(a). Show that there exists a left invariant mean on $UCB(G)$.

(b). Fix a point $v_0 \in K$ and define $t : G \to K$ by $t(x) = x \cdot v_0$. If $M$ is a mean on $UCB(G)$, show that there exists a unique regular Borel measure $\mu_M$ on $K$ such that, for every $f \in \mathscr{C}(K)$, we have

$$\int_K f d\mu_M = M(f \circ t).$$

(c). Show that the integral $b_M = \int_K v d\mu_M(v)$ exists and that $b_M \in K$.

(d). Let $\mathscr{M}$ be the set of all means on $UCB(G)$, equipped with the weak* topology (where the topology on $UCB(G)$ is given by $\|.\|_\infty$). Show that, for every continuous linear functional $\Lambda : V \to \mathbb{C}$, the map $\mathscr{M} \to K$, $M \longmapsto \Lambda(b_M)$ is continuous.

(e). If $M = \delta_x$ for some $x \in G$, calculate $b_M$.

(f). Show that, for every $M \in \mathscr{M}$ and every $x \in G$, we have $b_{M \circ L_{x^{-1}}} = x \cdot b_M$. (Hint : question III.6.3.1(d). Also, you may assume the fact that the formation of vector-valued integrals commutes with continuous affine maps.) [8]

(g). Show that the action of $G$ on $K$ has a fixed point.

*Solution.*

(a). Just take the restriction of a left invariant mean on $L^\infty(G)$.

(b). We first show that $f \circ t \in UCB(G)$ for every $f \in \mathscr{C}(K)$, and that the linear operator $\mathscr{C}(K) \to UCB(G)$, $f \longmapsto f \circ t$ is continuous. So let $f \in \mathscr{C}(K)$. Note that the function $t : G \to K$ is continuous by assumption, so $f \circ t$ is continuous. Also, we clearly have $\|f \circ t\|_\infty \leq \|f\|_\infty$. It remains to show that $f \circ t$ is left uniformly continuous. We denote by $a : G \times K \to K$ the action map. Let $\varepsilon > 0$. For every $v \in K$, there exists an open neighborhood $\Omega$ of $a^{-1}(v)$ such that $|f(x \cdot w) - f(v)| < \varepsilon$ for every $(x, w) \in \Omega$; as $(1, v) \in a^{-1}(v)$, we may assume that $\Omega = U_v \times V_v$, with $U_v$ an open neighborhood of $1$ in $G$ and $V_v$ an open neighborhood of $v$ in $K$. As $K$ is compact, we can find $v_1, \ldots, v_n \in K$ such that $K = \bigcup_{i=1}^n V_{v_i}$. Let $U = \bigcap_{i=1}^n U_{v_i}$. Let $x \in U$ and $v \in K$. Then there exists $i \in \{1, \ldots, n\}$ such that $v \in V_{v_i}$, and we have

$$|f(x \cdot v) - f(v)| \leq |f(x \cdot v) - f(v_i)| + |f(v_i) - f(1 \cdot v)| < 2\varepsilon.$$

So, for every $x \in U$ and every $y \in G$, we have

$$|f \circ t(xy) - f \circ t(y)| = |f(x \cdot t(y)) - f(t(y))| < 2\varepsilon.$$

This shows that $f \circ t$ is uniformly continuous.

[8] Virer le hint ?

Let $M$ be a mean on $UCB(G)$. Composing $M$ with the continuous linear operator $\mathscr{C}(K) \to UCB(G)$, $f \longmapsto f \circ t$, we get a mean on $\mathscr{C}(K)$. By the Riesz representation theorem, there is a unique regular Borel measure $\mu_M$ on $K$ such that $M(f \circ t) = \int_K f d\mu_M$ for every $f \in \mathscr{C}(K)$.

(c). Note that $\mu(K) = \int_K 1 d\mu_K = M(\mathbb{1}_G) = 1$. The function $\mathrm{id}_K$ is a continuous function with compact on $K$, so, by problem I.5.6.2, its integral $b_M = \int_K v d\mu_M$ with respect to $\mu_M$ exists, and $\mu(K)^{-1} b_M = b_M$ is in closure of the convex hull of $K$, i.e. in $K$.

(d). By definition of the integral, for every $\Lambda \in \mathrm{Hom}(V, \mathbb{C})$ and every mean $M$ on $UCB(G)$, we have

$$\Lambda(b_M) = \int_G \Lambda(v) d\mu_M = M(\Lambda \circ t).$$

This is continuous in $M$ for the weak* topology by the very definition of the weak* topology.

(e). Let $x \in G$, and let $M = \delta_x$. Then, for every $f \in Cf(K)$, we have

$$\int_K f d\mu_M = M(f \circ t) = f(x \cdot v_0).$$

Taking $f = \mathrm{id}_K$, we get

$$b_M = \int_K v d\mu_M = x \cdot v_0.$$

(f). Let $\mathscr{M}$ be the set of means on $UCB(G)$. Fix $M \in \mathscr{M}$. Let $x \in G$, and let $\Lambda \in \mathrm{Hom}(V, \mathbb{C})$. The map $L_{x^{-1}}$ sends $UCB(G)$ to itself, so $M \circ L_{x^{-1}}$ makes sense. For every $M \in \mathscr{M}$, using the fact that the map $K \to K$, $x \longmapsto x \cdot v$ is continuous and affine, we get

$$\begin{aligned}\Lambda(x \cdot b_M) = \Lambda\left(\int_K x \cdot v d\mu_M\right) &= \int_K \Lambda(x \cdot v) d\mu_M = M(\Lambda(x \cdot t)) \\ &= M(L_{x^{-1}}(\Lambda \circ t)) \\ &= \Lambda(b_{M \circ L_{x^{-1}}}).\end{aligned}$$

As continuous linear functionals separate points (by the Hahn-Banach theorem), this implies that $x \cdot b_M = b_{M \circ L_{x^{-1}}}$.

(g). Let $M$ be an invariant mean on $UCB(G)$ (this exists by question (a)). Then, by question (f), the point $b_M \in K$ is a fixed point for the action of $G$.

$\square$

**Exercise III.6.3.3.** Let $G$ be a locally compact group, and suppose that $G$ has the fixed point property. The goal of this problem is to show that $G$ is amenable. (You might find exercise I.5.6.6 useful.)

(a). Let $\mathscr{M}$ be the set of all means on $UCB(G)$. Show that this is a nonempty weak* compact convex subset of the continuous dual of $UCB(G)$, and that the action of $G$ on $\mathscr{M}$ given by $x \cdot M(f) = M(L_{x^{-1}}f)$ for $x \in G$, $M \in \mathscr{M}$ and $f \in UCB(G)$, is continuous and affine. (For the weak* topology on $\mathscr{M}$.)

(b). Show that there exists a left invariant mean $m$ on $UCB(G)$. [9] [10]

(c). Show that, if $f \in L^1(G)_{1,+}$ and $\varphi \in UCB(G)$, then $m(f * \varphi) = m(\varphi)$.

(d). Show that, if $f, f' \in L^1(G)_{1,+}$ and $\varphi \in L^\infty(G)$, then $m(f * \varphi) = m(f' * \varphi)$.

(e). Let $f_0 \in L^1(G)_{1,+}$. Show that the formula $\varphi \longmapsto m(f_0 * \varphi)$ defines a mean $\widetilde{m}$ on $L^\infty(G)$, and that we have $\widetilde{m}(f * \varphi) = \widetilde{m}(\varphi)$ for every $f \in L^1(G)_{1,+}$ and every $\varphi \in L^\infty(G)$.

Let $E = \prod_{f \in L^1(G)_{1,+}} L^1(G)$. We consider two topologies on $E$ :

- The product of the weak* topology on $L^1(G)$ (that we get by seeing $L^1(G)$ as a subspace of the continuous dual of $L^\infty(G)$). We will call this the *weak topology* on $E$.
- The product of the topology on $L^1(G)$ defined by the norm $\|.\|_1$. We will call this the *strong topology* on $E$.

(a). Let
$$\Sigma = \{(f * g - g)_{f \in L^1(G)_{1,+}},\ g \in L^1(G)_{1,+}\} \subset E.$$
Show that the closure of $\Sigma$ in the weak topology contains $0$.

(b). Show that the closure of $\Sigma$ in the strong topology contains $0$. (Hint : Any strongly continuous linear functional $\Lambda$ on $E$ can be written as $\Lambda((g_f)_{f \in L^1(G)_{1,+}}) = \sum_{f \in L^1(G)_{1,+}} \int_G g_f \varphi_f d\mu$, with the $\varphi_f$ in $L^\infty(G)$ and $\varphi_f = 0$ for all but a finite number of $f$.)

(c). Let $Q \ni 1$ be a compact subset of $G$, $\varepsilon > 0$ and $f \in L^1(G)_{1,+}$. Show that there exists $g \in L^1(G)_{1,+}$ such that
$$\sup_{x \in Q} \|(L_x f) * g - g\|_1 \le \varepsilon.$$

(d). Find a function $h \in L^1(G)_{1,+}$ such that
$$\sup_{x \in Q} \|L_x h - h\|_1 \le 2\varepsilon.$$

(e). Show that there exists a left invariant mean on $L^\infty(G)$. (If you are uncomfortable with nets, you may assume that $G$ is $\sigma$-compact, i.e. a countable union of compact subsets.)

*Solution.*

[9] If $G$ is a general topological group, it is called amenable if such a mean exists. One of the things we prove in this problem is that, for $G$ locally compact, this is equivalent to the other definition.

[10] reference

(a). We already saw that $\mathscr{M}$ is a weak* compact convex subset of $\operatorname{Hom}(UCB(G), \mathbb{C})$ in the solution of 1(d), and $\mathscr{M}$ is not empty because it contains all the linear functionals $\delta_x$, $x \in G$.

If $x \in G$, the morphism $\Lambda \longmapsto \Lambda \circ L_{x^{-1}}$ from $\operatorname{Hom}(UCB(G), \mathbb{C})$ to itself is linear, and it clearly preserves $\mathscr{M}$, so its restriction to $\mathscr{M}$ is affine.

It remains to show that the map $G \times \mathscr{M} \to \mathscr{M}$, $(x, M) \longmapsto M \circ L_{x^{-1}}$ is continuous. As we are using the weak* topology on $\mathscr{M}$, this means that, for every $\varphi \in UCB(G)$, the map $G \times \mathscr{M} \to \mathbb{C}$, $(x, M) \longmapsto M(L_{x^{-1}}\varphi)$ is continuous. Fix $\varphi \in UCB(G)$, and let $\varepsilon > 0$. As $\varphi$ is left uniformly continuous, there exists an open neighborhood $U$ of $1$ in $G$ such that, for every $y \in U$, we have $\|L_{y^{-1}}\varphi - \varphi\|_\infty < \varepsilon$. Note that, for every $y \in U$ and every $x \in G$, we have

$$\|L_{x^{-1}y^{-1}}\varphi - L_{x^{-1}}\varphi\|_\infty = \|L_{y^{-1}}\varphi - \varphi\|_\infty < \varepsilon.$$

Let $(x, M) \in G \times \mathscr{M}$. Let $V = \{M' \in \mathscr{M} | |M(L_{x^{-1}}\varphi) - M'(L_{x^{-1}}\varphi)| < \varepsilon\}$. This is weak* neighborhood of $M$, so $Ux \times V$ is a neighborhood of $(x, M)$ in $G \times \mathscr{M}$. If $y \in U$ and $M' \in V$, we have

$$\begin{aligned} |M(L_{x^{-1}}\varphi) - M'(L_{(yx)^{-1}}\varphi)| &\leq |M(L_{x^{-1}}\varphi) - M'(L_{x^{-1}}\varphi)| + |M'(L_{x^{-1}}\varphi) - M'(L_{x^{-1}y^{-1}}\varphi)| \\ &< \varepsilon + \|M'\|_{op}\|L_{x^{-1}}\varphi - L_{x^{-1}y^{-1}}\varphi\|_\infty \\ &< 2\varepsilon \end{aligned}$$

(using III.6.3.1(a) to see that $\|M'\|_{op} = 1$). This shows the desired result.

(b). A left invariant mean on $UCB(G)$ is exactly a fixed point of the action of $G$ on $\mathscr{M}$ defined by $x \cdot M = M \circ L_{x^{-1}}$. So the existence of such a mean follows from (a) and from the fact that $G$ has the fixed point property.

(c). By problem I.5.6.6, we have $f * \varphi = \int_G f(y) L_y \varphi dy$. By problem I.5.6.6, the linear functional $m$ on $UCB(G)$ is continuous. Applying the definition of the integral and the left invariance of $m$, we get

$$m(f * \varphi) = \int_G f(y) m(L_y \varphi) dy = \int_G f(y) m(\varphi) dy = m(\varphi) \int_G f d\mu = m(\varphi).$$

(d). Let $(\psi_U)_{U \in \mathscr{U}}$ be an approximate identity on $G$. Note that $\psi_U \in L^1(G)_{1,+}$ for every $U \in \mathscr{U}$. Let $\varphi \in L^\infty(G)$ and $f, f' \in L^1(G)_{1,+}$. By question I.5.6.6(a), we have $\psi_U * \varphi \in UCB(G)$ for every $U \in \mathscr{U}$, so, by question (c), we get

$$m(f * \psi_U * \varphi) = m(\psi_U * \varphi) = m(f' * \psi_U * \varphi).$$

Also, by proposition I.4.1.9, we have $\lim_{U \to \{1\}} f * \psi_U = f$ and $\lim_{U \to \{1\}} f' * \psi_U = f'$. Taking the limit as $U \to \{1\}$ in the equality above (forgetting the middle term) and using the fact that the convolution product from $L^1(G) \times L^\infty(G)$ to $UCB(G)$ is continuous in both variables (by the solution of I.5.6.6(a)) and that $m$ is continuous, we get that $m(f * \varphi) = m(f' * \varphi)$.

(e). The map $\widetilde{m}$ is well-defined by I.5.6.6(a), and it is clearly $\mathbb{C}$-linear. If $\varphi = \mathbb{1}_G$, then, for every $x \in G$,

$$f_0 * \varphi(x) = \int_G f_0(y)d\mu(y) = 1,$$

so $\widetilde{m}(\varphi) = m(\mathbb{1}_G) = 1$. If $\varphi \geq 0$ locally almost everywhere, then $f_0 * \varphi \geq 0$ almost everywhere, so $\widetilde{m}(\varphi) \geq 0$. This shows that $\widetilde{m}$ is a mean on $L^\infty(G)$.

Let $f \in L^1(G)_{1,+}$ and $\varphi \in L^\infty(G)$. Then

$$\widetilde{m}(f * \varphi) = m(f * f_0 * \varphi) \quad \text{and} \quad \widetilde{m}(\varphi) = m(f_0 * \varphi).$$

By (d), to show that these are equal, it suffices to show that $f * f_0 \in L^1(G)_{1,+}$. We already know that $f * f_0 \in L^1(G)$ by proposition I.4.1.2, and the fact that $f * f_0 \geq 0$ almost everywhere is clear from the formula defining $f * f_0$. Finally, we have

$$\begin{aligned}\int_G f * f_0(x)dx = \int_{G\times G} f(y)f_0(y^{-1}x)dxdy &= \int_G f(y)\left(\int_G f_0(y^{-1}x)dx\right)dy \\ &= \int_G f(y)dy = 1.\end{aligned}$$

(f). A piece of useful notation : for every $f \in L^1(G)$, we will denote by $M_f$ the linear functional $\varphi \longmapsto \int_G f\varphi d\mu$ on $L^\infty(G)$.

We want to show the following statement : For every $n \geq 1$, for all $f_1, \dots, f_n \in L^1(G)_{1,+}$, if $U_1, \dots, U_n$ are weak* neighborhoods of 0 in $\mathrm{Hom}(L^\infty(G), \mathbb{C})$, then there exists $g \in L^1(G)_{1,+}$ such that $M_{f_i * g} - M_g$ is in $U_i$ for $i \in \{1, \dots, n\}$.

If $f \in L^1(G)_{1,+}$, the map $c_f : \Lambda \longmapsto \Lambda(f * (.))$ from $\mathrm{Hom}(L^\infty(G), \mathbb{C})$ to itself is weak* continuous (because $\varphi \longmapsto f * \varphi$ is continuous on $L^\infty(G)$ by I.5.6.6(a)). Moreover, if $\Lambda = M_g$ with $g \in L^1(G)$, then, for every $\varphi \in L^\infty(G)$, we have

$$\begin{aligned}(c_{f'}\Lambda)(\varphi) &= \int_G g(y)(f' * \varphi)(y)dy \\ &= \int_{G\times G} g(y)\Delta(x)^{-1}f(x^{-1})\varphi(x^{-1}y)dxdy \\ &= \int_{G\times G} \Delta(x)^{-1}f(x^{-1})g(xz)\varphi(z)dxdz \\ &= \int_G (f * g)\varphi d\mu \quad \text{(see proposition I.4.1.3)},\end{aligned}$$

where $f' \in L^1(G)$ is defined by $f'(x) = \Delta(x)^{-1}f(x^{-1})$. In other words, $c_{f'}M_g = M_{f*g}$.

Fix $n$, $f_1, \dots, f_n$ and $U_1, \dots, U_n$ as above. Then $U := U_1 \cap \dots \cap U_n$ is a weak* neighborhood of 0 in $\mathrm{Hom}(L^\infty(G), \mathbb{C})$. Choose another weak* neighborhood $V$ of 0 such that $V = -V$ and $V + V \subset U$.

Then $\widetilde{m}+V$ is a weak* neighborhood of $\widetilde{m}$, so, by 1(c) and the previous paragraph, there exists $g \in L^1(G)_{1,+}$ such that $M_g - \widetilde{m}$ and all the $M_{f_i * g} - c_{f_i'}\widetilde{m}$, $1 \leq i \leq n$, are in $V$. Note that $c_{f_i'}\widetilde{m} = \widetilde{m}$ by (e), so, for $1 \leq i \leq n$, we have

$$M_{f_i * g} - M_g = (M_{f_i * g} - \widetilde{m}) + (\widetilde{m} - M_g) \in V - V \subset U_i.$$

(g). Note that $\Sigma$ is a convex subset of $E$. Let $\overline{\Sigma}$ be the closure of $\Sigma$ for the strong topology. If $0 \notin \overline{\Sigma}$, then, by the Hahn-Banach theorem (second geometric version), there exists a strongly continuous $\mathbb{R}$-linear functional $\Lambda' : E \to \mathbb{R}$ such that $0 = \Lambda'(0) > \sup_{x\in\Sigma} \Lambda'(x)$. As in the solution of III.6.3.1(c) and (d), we can write $\Lambda' = \operatorname{Re}\Lambda$, for $\Lambda : E \to \mathbb{C}$ a strongly continuous $\mathbb{C}$-linear functional (defined by $\Lambda(x) = \Lambda'(x) + \frac{1}{i}\Lambda'(ix)$).

Now an important remark is that, as we are using the product topology on $E$, the direct sum $\bigoplus_{f\in L^1(G)_{1,+}} L^1(G)$ is dense in $E$.

For every $f_0 \in L^1(G)_{1,+}$, consider the linear functional $\Lambda_{f_0} : L^1(G) \to \mathbb{C}$ that is the composition of $\Lambda$ and of the inclusion of the factor indexed by $f_0$ in $\prod_{f\in L^1(G)_{1,+}} L^1(G) = E$. This is a continuous linear functional on $L^1(G)$, so there exists a unique $\varphi_{f_0} \in L^\infty(G)$ such that $\Lambda_{f_0}$ is integration against $\varphi_{f_0}$.

Now consider an increasing family $(X_n)_{n\geq 0}$ of subsets of $L^1(G)_{1,+}$ such that $L^1(G)_{1,+} = \bigcup_{n\geq 0} X_n$. For every $x = (g_f)_{f\in L^1(G)_{1,+}} \in E$, the sequence $((g_f)_{f\in X_n})_{n\geq 0}$ converges to $x$ in the strong topology, so

$$\Lambda(x) = \lim_{n\to+\infty} \Lambda((g_f)_{f\in X_n}) = \lim_{n\to+\infty} \sum_{f\in X_n} \int_G g_f \varphi_f d\mu = \sum_{f\in L^1(G)_{1,+}} \int_G g_f \varphi_f d\mu.$$

As the sum converges for any $(g_f) \in E$, we must have $\varphi_f = 0$ for all but a finite number of $f \in L^1(G)_{1,+}$.

But then, if we consider any real number $c$ such that $0 > c > \sup_{x\in\Sigma} \operatorname{Re}(\Lambda(x))$, the set $\{x \in E | \operatorname{Re}(\Lambda(x)) \leq c\}$ is weakly closed in $E$, hence contains the weak closure of $\Sigma$, hence contains $0$ by (f), contradiction.

(h). For every $x \in Q$, let $U_x$ be a neighborhood of $x$ in $G$ such that, for $y \in U_x$, we have $\|L_y f - L_x f\|_1 \leq \varepsilon/2$. (See proposition I.3.1.13). As $Q$ is compact, we can find $x_1, \ldots, x_n \in Q$ such that $Q \subset \bigcup_{i=1}^n U_{x_i}$. By question (f), there exists $g \in L^1(G)_{1,+}$ such that, for every $i \in \{1, \ldots, n\}$, we have $\|(L_{x_i} f) * g - g\|_1 \leq \varepsilon/2$.

Let's show that this $g$ works. Let $x \in Q$. Then there exists $i \in \{1, \ldots, n\}$ such that $x \in U_{x_i}$, and we have

$$\begin{aligned}\|(L_x f) * g - g\|_1 &\leq \|(L_x f) * g - (L_{x_i} f) * g\|_1 + \|(L_{x_i} f) * g - g\|_1 \\ &\leq \|L_x f - L_{x_i} f\|_1 \|g\|_1 + \|(L_{x_i} f) * g - g\|_1 \\ &\leq \varepsilon.\end{aligned}$$

(The second equality uses proposition I.4.1.2).

(i). Let $h = f * g$. We have $h \in L^1(G)_{1,+}$ (see the solution of question (e)), and, as $1 \in Q$, for every $x \in Q$,

$$\|L_x h - h\|_1 \leq \|L_x h - g\|_1 + \|g - h\|_1 \leq \|(L_x f) * g - g\|_1 + \|(L_1 f) * g - g\|_1 \leq 2\varepsilon.$$

(j). Suppose that $G$ is $\sigma$-compact, and write $G = \subset_{n \geq 0}$, where each $Q_n$ is a compact subset of $G$ containing 1. For every $n \in \mathbb{Z}_{\geq 0}$, we can find by (h) a function $h_n \in L^1(G)_{1,+}$ such that $\sup_{x \in Q_n} \|L_x h_n - h_n\|_1 \leq 2^{-n}$. The sequence $(M_{h_n})_{n \geq 0}$ of elements of the weak* compact subset of means on $L^\infty(G)$ (we have seen in III.6.3.1(c) that this set is weak* compact) has a convergent subsequence, so we may assume that it is convergent. Let $M = \lim_{n \geq 0} M_{h_n}$. We show that $M$ is left invariant. Let $x \in G$. Then $x^{-1} \in Q_n$ for $n >> 0$, so, for every $\varphi \in L^\infty(G)$,

$$\begin{aligned} M(L_x \varphi) &= \lim_{n \to +\infty} M_{h_n}(L_x \varphi) \\ &= \lim_{n \to +\infty} \int_G h_n(y) \varphi(x^{-1} y) dy \\ &= \lim_{n \to +\infty} \int_G h_n(xy) \varphi(y) dy \\ &= \lim_{n \to +\infty} \int_G L_{x^{-1}} h_n \varphi d\mu, \end{aligned}$$

and

$$\begin{aligned} |M(L_x \varphi) - M(\varphi)| &= \lim_{n \to +\infty} \left| \int_G (L_{x^{-1}} h_n - h_n) \varphi d\mu \right| \\ &\leq \lim_{n \to +\infty} \|L_{x^{-1}} h_n - h_n\|_1 \|\varphi\|_\infty \\ &= 0, \end{aligned}$$

that is, $M(L_x \varphi) = M(\varphi)$.

Assume that $G$ is not $\sigma$-compact. Then we write $G = \bigcup_{Q \in \mathscr{Q}} Q$, where $Q$ is a family of compact subsets of $G$ such that, if $Q_1, Q_2 \in \mathscr{Q}$, then $Q_1 \cup Q_2 \in \mathscr{Q}$. That is, $\mathscr{Q}$ is a directed set for the order relation given by inclusion. For every $Q \in \mathscr{Q}$, we can find by (i) a function $h_Q \in L^1(G)_{1,+}$ such that $\sup_{x \in Q} \|L_x h_Q - h_Q\|_1 \leq (1 + \mu(Q))^{-1}$. If $G$ is not compact, then $\mu(G) = +\infty$, so $\lim_{Q \in \mathscr{Q}} (1 + \mu(Q))^{-1} = 0$. Let $M$ be a weak* limit point of $(M_{h_Q})_{Q \in \mathscr{Q}}$, which exists because the set of means on $L^\infty(G)$ is weak* compact. Then we see exactly as above that $M$ is left invariant.

□

**Exercise III.6.3.4.** Let $G$ be a locally compact group. Remember problem III.6.2.4.

(a). If $G$ is amenable, show that the trivial representation is weakly contained in the left regular representation of $G$. (Hint : For all $a, b \in \mathbb{R}_{\geq 0}$, we have $|a - b|^2 \leq |a^2 - b^2|$.)

(b). If the trivial representation is weakly contained in the left regular representation of $G$, show that $G$ is amenable. (Hint : For all $a, b \in \mathbb{C}$, prove that $||a|^2 - |b|^2| \leq |a+b||a-b|$.)

*Solution.*

(a). Let's first prove the inequality in the hint. Let $a, b \in \mathbb{R}_{\geq 0}$. We may assume that $a \geq b$. Then

$$|a-b|^2 = (a-b)^2 = a^2 + b^2 - 2ab \leq a^2 + b^2 - 2b^2 = a^2 - b^2 = |a^2 - b^2|.$$

Suppose that $G$ is amenable. Let $K$ be a compact subset of $G$ and let $c > 0$. By III.6.3.3(i), there exists $h \in L^1(G)_{1,+}$ such that $\sup_{x \in K} \|L_x h - h\|_1 < c^2$. Let $f = \sqrt{h}$. Then, by the inequality above, for every $x \in K$, we have

$$\begin{aligned} \|L_x f - f\|_2^2 &= \int_G |f(x^{-1}y) - f(y)|^2 dy \\ &\leq \int_G |h(x^{-1}y) - h(y)| dy \\ &= \|L_x h - h\|_1 \\ &< c^2, \end{aligned}$$

so $\|L_x f - f\|_2 < c$.

By III.6.2.4(d), this implies that the trivial representation of $G$ is weakly contained in the regular representation.

(b). We check that the result of III.6.3.3(i) holds, i.e. that, for every compact subset $Q$ of $G$ and every $\varepsilon > 0$, there exists $h \in L^1(G)_{1,+}$ such that $\sup_{x \in Q} \|L_x h - h\|_1 \leq \varepsilon$. Indeed, we have seen in III.6.3.3(j) that this implies the existence of a left invariant mean on $L^\infty(G)$.

Let $Q$ be a compact subset of $G$ and $\varepsilon > 0$. By III.6.2.4(c), there exists $f \in L^2(G)$ such that $\|f\|_2 = 1$ and $\sup_{x \in Q} \|L_x f - f\|_2 \leq \varepsilon/2$. Let $h = |f|^2$. Then $\|h\|_1 = \|f\|_2^2 = 1$, so $h \in L^1(G)_{1,+}$. Note that, for all $a, b \in \mathbb{C}$, we have $|a^2 - b^2| \geq ||a|^2 - |b|^2|$ by the triangle inequality, so

$$|a+b|^2 |a-b|^2 = (a^2 - b^2)(\overline{a}^2 - \overline{b}^2) = |a^2 - b^2|^2 \geq ||a|^2 - |b|^2|^2.$$

Now, if $x \in Q$, we get

$$\begin{aligned} \|L_x h - h\|_1 &= \int_G ||L_x f(y)|^2 - |f(y)|^2| dy \\ &\leq \int_G (|L_x f(y) + f(y)|)|L_x f(y) - f(y)| dy \\ &\leq \|L_x f - f\|_2 \|L_x + f\|_2 \quad \text{(Cauchy-Schwarz)} \\ &\leq \varepsilon \end{aligned}$$

(because $\|L_x f + f\|_2 \leq \|L_x f\|_2 + \|f\|_2 = 2\|f\|_2 = 2$).

□

**Exercise III.6.3.5.** Let $G$ be an abelian locally compact group. The goal of this problem is to show that $G$ has the fixed point property (hence is amenable).

Let $V$ be a locally convex topological vector space, $K$ be a nonempty compact convex subset of $V$ and $G \times K \to K$, $(x, v) \longmapsto x \cdot v$ be an affine action of $G$ on $K$.

For every $n \in \mathbb{Z}_{\geq 0}$ and every $x \in G$, we define a continuous affine map $A_n(x) : K \to K$ by

$$A_n(x)(v) = \frac{1}{n+1} \sum_{i=0}^{n} x^i \cdot v.$$

Let $\mathscr{G}$ be the semigroup of continuous affine maps $K \to K$ generated by all the $A_n(x)$, for $n \geq 0$ and $x \in G$. (That is, the semigroup whose elements are finite compositions of morphisms $A_n(x)$, where the semigroup operation is the composition of maps $K \to K$.)

(a). Let $v \in \bigcap_{\gamma \in \mathscr{G}} \gamma(K)$. Show that $v$ is a fixed point of the action of $G$. (Hint : For every continuous linear functional $\Lambda$ on $V$ and every $x \in G$, show that $\Lambda(v) = \Lambda(x \cdot v)$.)

(b). For all $\gamma_1, \ldots, \gamma_n \in \mathscr{G}$, show that $\bigcap_{i=1}^{n} \gamma_i(K) \neq \varnothing$.

(c). Show that $G$ has a fixed point in $K$.

*Solution.*

(a). Let $x \in G$. Let $\Lambda$ be a continuous linear functional on $V$. As $K$ is compact, $C := \sup_{w \in K} |\Lambda(w)| < +\infty$. If $n \geq 0$, we have $x \in A_n(x)(K)$, so there exists $w \in K$ such that $v = A_n(x)(w)$. As the action of $G$ is affine, this implies that

$$x \cdot v = \frac{1}{n+1} \sum_{i=0}^{n} x^{i+1} \cdot w,$$

so $v - x \cdot v = \frac{1}{n+1}(w - x^{n+1} \cdot w)$, so $|\Lambda(v - x \cdot v)| \frac{2C}{n+1}$. As this is true for every $n \geq 0$, we have $|\Lambda(v) - \Lambda(x \cdot v)|$, i.e. $\Lambda(v) = \Lambda(x \cdot v)$. As continuous linear functional on $V$ separate points, we finally get $x \cdot v = v$.

(b). Note that, if $x, y \in G$ and $n, m \in \mathbb{Z}_{\geq 0}$, then, for every $v \in K$,

$$\begin{aligned}
A_n(x) \circ A_m(y)(v) &= \frac{1}{n+1} \sum_{i=1}^{n} x^i \cdot A_m(y)(v) \\
&= \frac{1}{(n+1)(m+1)} \sum_{i=0}^{n} \sum_{j=0}^{m} x^i \cdot (y^j \cdot v) \\
&= \frac{1}{(n+1)(m+1)} \sum_{i=0}^{n} \sum_{j=0}^{m} y^j \cdot (x^i \cdot v) \quad \text{(because } G \text{ is commutative)} \\
&= A_m(y) \circ A_n(x)(v).
\end{aligned}$$

This implies that the semigroup $\mathscr{G}$ is commutative.

Now let $\gamma_1, \ldots, \gamma_n \in \mathscr{G}$. Then, for every $i \in \{1, \ldots, n\}$,

$$\gamma_i(K) \supset \gamma_i(\gamma_1 \circ \ldots \circ \gamma_{i-1} \circ \ldots \circ \gamma_n(K)) = \gamma_1 \circ \ldots \circ \gamma_n(K).$$

So

$$\bigcap_{i=1}^{n} \gamma_i(K) \supset \gamma_1 \circ \ldots \circ \gamma_n(K) \neq \varnothing.$$

(c). As $K$ is compact and each $\gamma \in \mathscr{G}$ is continuous, the subset $\gamma(K)$ of $K$ is compact, hence closed in $K$, for every $\gamma \in \mathscr{G}$. By (b), the family $(\gamma(K))_{\gamma \in \mathscr{G}}$ has the finite intersection property. By compactness of $K$, we have $\bigcap_{\gamma \in \mathscr{G}} \gamma(K) \neq \varnothing$. By (a), any point of this intersection is a fixed point of $G$ on $K$.

□

**Exercise III.6.3.6.** (a). Let $\mathscr{P}(\mathbb{Z})$ be the set of subsets of $\mathbb{Z}$. Show that there exists a finitely additive left-invariant probability measure on $\mathbb{Z}$, that is, a function $\mu : \mathscr{P}(\mathbb{Z}) \to \mathbb{R}_{\geq 0}$ such that :

(i) If $A_1, \ldots, A_n \in \mathscr{P}(\mathbb{Z})$ are such that $A_i \cap A_j = \varnothing$ for $i \neq j$, then $\mu(A_1 \cup \ldots \cup A_n) = \mu(A_1) + \ldots + \mu(A_n)$.

(ii) $\mu(\mathbb{Z}) = 1$.

(iii) For every $A \in \mathscr{P}(Z)$ and $n \in \mathbb{Z}$, we have $\mu(n + A) = \mu(A)$.

(b). Is the measure of question (a) unique ? (Hint : You need a somewhat explicit way to construct invariant means on $\mathbb{Z}$. You can for example try to exploit the sequence of (non-invariant) means $M_n : L^\infty(\mathbb{Z}) \to \mathbb{C}$, $(x_k)_{k \in \mathbb{Z}} \longmapsto \frac{1}{2k+1} \sum_{k=-n}^{n} x_k$.)

*Solution.*

(a). As $\mathbb{Z}$ is an abelian locally compact group, it is amenable by problems III.6.3.3 and III.6.3.5. This means that there exists a left-invariant mean $M$ on $L^\infty(\mathbb{Z})$. We define $\mu$ by $\mu(A) = M(\mathbb{1}_A)$; this function does take its values in $\mathbb{R}_{\geq 0}$ by definition of a mean. Then $\mu$ satisfies (i) because $M$ is linear, it satisfies (ii) because $M(1) = 1$ and it satisfies (iii) because $M$ is left-invariant.

Conversely, note that the existence of a $\mu$ as in the statement implies the existence of an invariant mean.

(b). No.

Let $V = L^\infty(\mathbb{Z})$, and consider the family of linear functionals $M_n : L^\infty(\mathbb{Z}) \to \mathbb{C}$ defined by

$$M_n((x_k)_{k\in\mathbb{Z}}) = \frac{1}{2n+1}\sum_{k=-n}^{n} x_k,$$

for $n \in \mathbb{N}$. We have $|M_n(x)| \leq \|x\|_\infty$ for every $x \in V$, so $M_n$ is continuous. Also, it is clear on the definition that $M_n$ is a mean. If $a \in \mathbb{Z}$, then, for every $x \in V$ and every $n \in \mathbb{N}$, we have

$$|M_n(L_a x) - M_n(x)| \leq \frac{2|a|}{2n+1}\|x\|_\infty.$$

So, if we could make the sequence $(M_n)_{n\geq 0}$ converge in the weak* topology of $\mathrm{Hom}(V,\mathbb{C})$, then its limit would be an invariant mean, and it would define an invariant finitely additive probability measure as in question (a). We can always find a convergent subsequence of $(M_n)_{n\geq 0}$ converge in the weak* using the Banach-Alaoglu theorem, but we would also like to show that we can get two different limits.

Consider the element $x = (x_n)_{n\in\mathbb{Z}}$ of $V$ defined by $x_n = 0$ for $n \leq 0$, and $x_n = (-1)^k$ if we have $2^k \leq n \leq 2^{k+1} - 1$ with $k \in \mathbb{Z}_{\geq 0}$. Then, if $n = 2^k - 1$ with $k \geq 0$, we have

$$\sum_{r=-n}^{n} x_n = \sum_{s=0}^{k-1}(-1)^s 2^s = \frac{1-(-2)^k}{3},$$

so

$$M_n(x) = \frac{1-(-2)^k}{3(2^{k+1}-1)}.$$

In particular, the sequence $(M_{2^{2l}-1}(x))_{l\geq 0}$ converges to $-\frac{1}{6}$, and the sequence $(M_{2^{2l+1}-1}(x))_{l\geq 0}$ converges to $\frac{1}{6}$.

By the Banach-Alaoglu theorem,[11] the sequences $(M_{2^{2l}-1})_{l\geq 0}$ $(M_{2^{2l+1}-1})_{l\geq 0}$ both have weak* limit points, say $M$ and $M'$. Both $M$ and $M'$ are left invariant means on $V$, but we have $M(x) = -\frac{1}{6}$ and $M'(x) = \frac{1}{6}$ by the calculation above, so $M \neq M'$.

$\square$

**Exercise III.6.3.7.** (a). Let $G$ be a group acting on a set $X$. Suppose that we have subgroups $G_1, G_2$ of $G$ and subsets $X_1, X_2$ of $X$ such that :

- The sets $X_1$ and $X_2$ are not empty, and $X_1 \neq X_2$;
- For every $x \in G_1 - \{1\}$, we have $x \cdot X_1 \subset X_2$;
- For every $x \in G_2 - \{1\}$, we have $x \cdot X_2 \subset X_1$;
- The cardinality of $G_2$ is at least 3.

Show that we cannot have an equality $1 = h_1 \dots h_n$ with $h_i$ in $G_1 - \{1\}$ for $i$ odd, $h_i$ in $G_2 - \{1\}$ for $i$ even and $n \geq 1$.

[11] ref ?

(b). Let $a_1, a_2 \in \mathbb{C}$ such that $|a_1| \geq 2$ and $|a_2| \geq 2$. Define $x, y \in \mathrm{SL}_2(\mathbb{C})$ by

$$x = \begin{pmatrix} 1 & a_1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 \\ a_2 & 1 \end{pmatrix}.$$

Show that the subgroup of $\mathrm{SL}_2(\mathbb{C})$ generated by $x$ and $y$ is isomorphic to the free group on two generators. (Hint : Let $\mathrm{SL}_2(\mathbb{C})$ act on $\mathbb{C}^2$ in the usual way. Look at the subsets $\{(z_1, z_2) \in \mathbb{C}^2 | |z_1| > |z_2|\}$ and $\{(z_1, z_2) \in \mathbb{C}^2 | |z_1| < |z_2|\}$.)

(c). Let $G = \mathrm{SL}_2(\mathbb{R})$ with the discrete topology. Show that $G$ is not amenable.

*Solution.*

(a). If $G_1 = \{1\}$, the result if obvious. So we may assume $G_1 \neq \{1\}$.

Suppose that we have $1 = h_1 \dots h_n$ with $h_i$ in $G_1 - \{1\}$ for $i$ odd, $h_i$ in $G_2 - \{1\}$ for $i$ even and $n \geq 1$.

We first assume that $n$ is even. As $|G_2| \geq 3$, we can find $h \in G_2 - \{1\}$ such that $h \neq h_n$. Note that $1 = hh^{-1} = hh_1 \dots (h_n h^{-1})$, with $h_n h^{-1} \in G_2 - \{1\}$. Let $g \in G_1 - \{1\}$. We also have $1 = gg^{-1} = ghh_1 \dots (h_n h^{-1}) g^{-1}$. So, for every $x \in X_2$, we have

$$x = hh_1 \dots h_{n-1}(h_n h^{-1})(x) \in X_1,$$

hence $X_2 \subset X_1$. On the other hand, for every $y \in X_1$, we get

$$y = ghh_1 \dots (h_n h^{-1}) g^{-1}(y) \in X_2,$$

so $X_1 \subset X_2$. This contradicts the fact that $X_1 \neq X_2$.

Now suppose that $n$ is odd. Let $h \in G_2 - \{1\}$. Then $1 = hh^{-1} = hh_1 \dots h_n h^{-1}$. So, for every $x \in X_2$, we have

$$x = hh^{-1} = hh_1 \dots h_n h^{-1}(x) \in X_1,$$

hence $X_2 \subset X_1$. On the other hand, for every $y \in X_1$, we have

$$y = h_1 \dots h_n(y) \in X_2,$$

so $X_1 \subset X_2$. Again, this contradicts the fact that $X_1 \neq X_2$.

(b). We want to apply question (a) with $X = \mathbb{C}^2$, $X_1 = \{(z_1, z_2) \in \mathbb{C}^2 | |z_1| < |z_2|\}$, $X_2 = \{(z_1, z_2) \in \mathbb{C}^2 | |z_1| > |z_2|\}$, $G_1 = \langle x \rangle$ and $G_2 = \langle y \rangle$. We have to check that these subsets and subgroups satisfy the conditions of (a).

Let $g \in G_1 - \{1\}$ and $(z_1, z_2) \in X_1$. We have $g = x^n$, with $n \in \mathbb{Z} - \{0\}$, so $g = \begin{pmatrix} 1 & na_1 \\ 0 & 1 \end{pmatrix}$, and $g \cdot (z_1, z_2) = (z_1 + na_1 z_2, z_2)$. Hence

$$|z_1 + na_1 z_2| \geq |n||a_1||z_2| - |z_1| \geq 2|z_2| - |z_1| > |z_2|,$$

that is, $g\cdot(z_1, z_2) \in X_2$. (We have used the fact that $|n| \geq 1$.) The proof that $g\cdot(z_1, z_2) \in X_1$ for $g \in G_2 - \{1\}$ and $(z_1, z_2) \in X_2$ is similar.

Let $G$ be the subgroup of $\mathrm{SL}_2(\mathbb{C})$ generated by $x$ and $y$, and let $F$ be the free group on two generators $a$ and $b$. We have a surjective morphisms of groups $\varphi : F \to G$ sending an element $a^{n_1}b^{m_1} \ldots a^{n_r}b^{m_r}$ of $F$ (with $r \geq 0$ and $n_1, m_1, \ldots, n_r, m_r \in \mathbb{Z}$) to $x^{n_1}y^{m_1} \ldots x^{n_r}y^{m_r} \in G$. We want to check that $\varphi$ is injective. This means that its kernel is trivial, i.e. that it sends reduced words in $F$ to nontrivial elements of $G$. But this property is exactly the conclusion of (a).

(c). Suppose that $G$ is amenable. Then, by problem III.6.3.4, the trivial representation $\mathbb{1}$ of $G$ on $\mathbb{C}$ is contained in its regular representation $\pi_L$. Let $H$ be a subgroup of $G$. It follows immediately from the definition of weak containment that the representation $\mathbb{1}_{|H}$ of $H$ (which is just its trivial representation) is weakly contained in $\pi_{L|H}$. Let $\pi$ be the regular representation of $H$, and let's show that $\pi_{L|H}$ is weakly contained in $\pi$. This will imply that the trivial representation of $H$ is contained in its regular representation.

Let $(x_i)_{i\in I}$ be a system of representatives of the quotient $H\backslash G$; we have $G = \coprod_{i\in I} Hx_i$. Let $\varphi$ be a function of positive type associated to $\pi_{L|H}$. This means that we have $f \in L^2(G)$ such that, for every $x \in H$,

$$\varphi(x) = \langle L_x f, f\rangle_{L^2(G)}.$$

For every $i \in I$, let $f_i = f_{|Hx_i} \in L^2(G)$. Then the series $\sum_{i\in I} f_i$ converges to $f$ in $L^2(G)$, and, if $i \neq j$, then $\langle L_x f_i, f_i\rangle_{L^2(G)} = 0$ for every $x \in H$ (because $L_x f_i$ and $f_j$ have disjoint supports). In particular, $\|f\|_2^2 = \sum_{i\in I} \|f_i\|_2^2$. So, for every $x \in H$,

$$\varphi(x) = \sum_{i\in I} \langle L_x f_i, f_i\rangle_{L^2(G)},$$

and this sums converges uniformly on $x \in H$ (because $|\langle L_x f_i, f_i\rangle_{L^2(G)}| \leq \|f_i\|_2^2$). For every $i \in I$, we define $g_i \in L^2(H)$ by $g_i(y) = f_i(yx_i)$. Then $\langle L_x g_i, g_i\rangle_{L^2(H)} = \langle L_x f_i, f_i\rangle_{L^2(G)}$ for every $x \in H$. So we have written $\varphi$ as a limit of finite sums of functions of positive type associated to the regular representation of $H$, which is what we wanted.

In summary, we have shown that, if $G$ is amenable, then, for every subgroup $H$ of $G$, the trivial representation of $H$ is contained in its regular representation (i.e. $H$ is also amenable). Note that we only used the fact that $G$ is discrete so far.

Now if $G = \mathrm{SL}_2(\mathbb{R})$, question (b) says that $G$ has a subgroup $H$ isomorphic to the free group on two generators (just take $a_1, a_2 \in \mathbb{R}$ in (b)). Then the result above contradicts problem III.6.2.8.

□

# IV The Peter-Weyl theorem

## IV.1 Compact operators

**Definition IV.1.1.** Let $V$ and $W$ be Banach spaces, and let $B$ be the closed unit ball in $V$. A continuous linear operator $T : V \to W$ is called *compact* if $\overline{T(B)}$ is compact.

**Example IV.1.2.** (1) If $\mathrm{Im}(T)$ is finite-dimensional (i.e. if $T$ has finite rank), then $T$ is compact.

(2) If $T$ is a limit of operators of finite rank, then $T$ is compact; more generally, any limit of compact operators is compact (see exercise I.5.5.9).

Conversely, if $W$ is a Hilbert space, then every compact operator $T : V \to W$ is a limit of operators of finite rank. [1]

(3) The identity of $V$ is compact if and only if $V$ is finite-dimensional. (This is a consequence of Riesz's lemma, see theorem B.4.2.)

In this class, we will only need to use self-adjoint compact endormophisms of Hilbert space. A much simpler version of the spectral theorem holds for them.

**Theorem IV.1.3.** *Let $V$ be a Hilbert space over $\mathbb{C}$, and let $T : V \to V$ be a continuous endomorphism of $V$. Assume that $T$ is compact and self-adjoint, and write $V_\lambda = \mathrm{Ker}(T - \lambda \mathrm{id}_V)$ for every $\lambda \in \mathbb{C}$.*

*Then :*

*(i) If $V_\lambda \neq 0$, then $\lambda \in \mathbb{R}$.*

*(ii) If $\lambda, \mu \in \mathbb{C}$ and $\lambda \neq \mu$, then $V_\mu \subset V_\lambda^\perp$.*

*(iii) If $\lambda \in \mathbb{C} - \{0\}$, then $\dim_\mathbb{C} V_\lambda < +\infty$.*

*(iv) $\{\lambda \in \mathbb{C} | V_\lambda \neq 0\}$ is finite or countable, and its only possible limit point is $0$.*

*(v) $\bigoplus_{\lambda \in \mathbb{C}} V_\lambda$ is dense in $V$.*

*Proof.* We prove (i). Let $\lambda \in \mathbb{C}$ such that $V_\lambda \neq 0$, and choose $v \in V_\lambda$ nonzero. Then

$$\lambda \|v\|^2 = \langle \lambda v, v \rangle = \langle T(v), v \rangle = \langle v, T^*(v) \rangle = \langle v, T(v) \rangle = \overline{\lambda} \|v\|^2.$$

[1] This is not true in general, see Enflo's article [10] for a counterexample.

As $\|v\| \neq 0$, this implies that $\lambda \in \mathbb{R}$.

We prove (ii). Let $\lambda, \mu \in \mathbb{C}$ such that $\lambda \neq \mu$, and let $v \in V_\lambda$ and $w \in V_\mu$. We want to prove that $\langle v, w\rangle = 0$. By (i), it suffices to treat the case where $\lambda, \mu \in \mathbb{R}$ (otherwise $v = w = 0$). In that case, we have

$$\lambda\langle v, w\rangle = \langle T(v), w\rangle = \langle v, T(w)\rangle = \overline{\mu}\langle v, w\rangle = \mu\langle v, w\rangle,$$

so $\langle v, w\rangle = 0$.

Let $r > 0$. Let $W = \overline{\bigoplus_{|\lambda|\geq r} V_\lambda}$. We want to show that $\dim W < +\infty$, which will imply (iii) and (iv). Choose a Hilbert basis $(e_i)_{i\in I}$ of $W$ made up of eigenvectors of $T$, i.e. such that, for every $i \in I$, we have $T(e_i) = \lambda_i e_i$ with $|\lambda_i| \geq r$. If $I$ is infinite, then the family $(T(e_i))_{i\in I}$ cannot have a convergent (non-stationary) subsequence. Indeed, if we had an injective map $\mathbb{N} \to I$, $n \longmapsto i_n$, such that $(T(e_{i_n}))_{n\geq 0}$ converges to some vector $v$ of $V$, then $\lambda_{i_n} e_{i_n} \to v$, so $v$ is in the closure of $\operatorname{Span}(e_{i_n}, n \geq 0)$. But on the other hand, for every $n \geq 0$, $\langle v, e_{i_n}\rangle = \lim_{m\to+\infty}\langle \lambda_{i_m} e_{i_m}, e_{i_n}\rangle = 0$, so $v \in \operatorname{Span}(e_{i_n}, n \geq 0)^\perp$. This forces $v = 0$. But $\|v\| = \lim_{n\to+\infty}\|\lambda_{i_n} e_{i_n}\| \geq r > 0$, contradiction. As $T$ is compact, this show that $I$ cannot be infinite, i.e. that $\dim(W) < +\infty$.

Let's prove (v). Let $W' = \bigoplus_{\lambda\in\mathbb{C}} V_\lambda$, and $W = W'^\perp$. We want to show that $W = 0$. So suppose that $W \neq 0$. As $T$ is self-adjoint and $W'$ is clearly stable by $T$, we have $T(W) \subset W$. (If $v \in W$, then for every $w \in W'$, $\langle T(v), w\rangle = \langle v, T(w)\rangle = 0$.) By definition of $W$, we have $\operatorname{Ker}(T_{|W}) = \{0\}$, hence $\|T_{|W}\|_{op} > 0$. Let $B = \{x \in W | \|x\| = 1\}$. As $\|T_{|W}\|_{op} = \sup_{x\in B} |\langle T(x), x\rangle|$ by the lemma below, there exists a sequence $(x_n)_{n\geq 0}$ of elements of $B$ such that $\langle T(x_n), x_n\rangle \to \lambda$ as $n \to +\infty$, where $\lambda = \pm\|T_{|W}\|_{op}$. Then

$$0 \leq \|T(x_n) - \lambda x_n\|^2 = \|T(x_n)\|^2 + \lambda^2\|x_n\|^2 - 2\lambda\langle T(x_n), x_n\rangle \leq 2\lambda^2 - 2\lambda\langle T(x_n), x_n\rangle$$

converges to $0$ as $n \to +\infty$, so $T(x_n) - \lambda x_n$ itself converges to $0$. As $T$ is compact, we may assume that the sequence $(T(x_n))_{n\geq 0}$ has a limit in $W$, say $w$. Then $T(w) - \lambda w = 0$. By definition of $W$, we must have $w = 0$. But then $T(x_n) \to 0$, so $\langle T(x_n), x_n\rangle \to 0$, so $\lambda = 0 = \|T_{|W}\|_{op}$, a contradiction.

□

**Lemma IV.1.4.** *Let $V$ be a Hilbert space, and let $T \in \operatorname{End}(V)$ be self-adjoint. Then*

$$\|T\|_{op} = \sup_{x\in V,\ \|x\|=1} |\langle T(x), x\rangle|.$$

*Proof.* Let $c = \sup_{x\in V,\ \|x\|=1} |\langle T(x), x\rangle|$. We have $c \leq \|T\|_{op}$ by definition of $\|T\|_{op}$. As $\|T\|_{op} = \sup_{x,y\in V, \|x\|=\|y\|=1} |\langle T(x), y\rangle|$, to prove the other inequality, it suffices to show that $|\langle T(x), y\rangle| \leq c$ for all $x, y \in V$ such that $\|x\| = \|y\| = 1$. Let $x, y \in V$. After mutliplying $y$ by a norm $1$ element of $\mathbb{C}$ (which doesn't change $\|y\|$), we may assume that $\langle T(x), y\rangle \in \mathbb{R}$. Then

$$\langle T(x), y\rangle = \frac{1}{4}(\langle T(x+y), x+y\rangle - \langle T(x-y), x-y\rangle),$$

so

$$|\langle T(x), y\rangle| \leq \frac{c}{4}(\|x+y\|^2 + \|x-y\|^2) = \frac{c}{2}(\|x\|^2 + \|y^2\|)$$

(the last equality is the parallelogram identity). This shows the desired result.

□

Here are some results that are true for compact operators in greater generality (see [20] 4.16-4.25).

**Theorem IV.1.5.** *Let $V$ be a Banach space, and let $T \in \mathrm{End}(V)$ be a* compact *endomorphism. We write $\sigma(T)$ for the spectrum of $T$ in $\mathrm{End}(V)$, i.e.*

$$\sigma(T) = \{\lambda \in \mathbb{C} | \lambda \mathrm{id}_V - T \not\in \mathrm{End}(V)^\times\}.$$

*Then :*

*(i) For every $\lambda \neq 0$, the image of $T - \lambda \mathrm{id}_V$ is closed.*

*(ii) For every $\lambda \in \sigma(T) - \{0\}$, we have $\mathrm{Im}(T - \lambda \mathrm{id}_V) \neq V$ and $\dim(\mathrm{Ker}(T - \lambda \mathrm{id}_V)) = \dim(V/\mathrm{Im}(T - \lambda \mathrm{id}_V))$.* [2] *In particular,* $\mathrm{Ker}(T - \lambda \mathrm{id}_V) \neq \{0\}$.

*(iii) For every $\lambda \neq 0$, the increasing sequence $(\mathrm{Ker}((T - \lambda \mathrm{id}_V)^n))_{n \geq 1}$ stabilizes, and its limit is finite-dimensional.*

*(iv) If $\dim_{\mathbb{C}} V = +\infty$, then $0 \in \sigma(T)$.*

*(v) The subset $\sigma(T) - \{0\}$ of $\mathbb{C} - \{0\}$ is discrete. In particular, for every $r > 0$, there are only finitely many $\lambda \in \sigma(T)$ such that $|\lambda| \geq r$.*

In particular, if $V$ is a Hilbert space and $T$ is self-adjoint, then (v) of theorem IV.1.3 become

$$V = \overline{\bigoplus_{\lambda \in \sigma(T)} \mathrm{Ker}(T - \lambda \mathrm{id}_V)}.$$

## IV.2 Semisimplicity of unitary representations of compact groups

The goal of this section is to prove the following theorem. (Compare with proposition I.3.3.3.)

[2]Note that this generalizes the rank-nullity theorem.

**Theorem IV.2.1.** *Let $G$ be a compact group, and let $V$ be a unitary representation of $G$. Then there exists a family $(W_i)_{i\in I}$ of pairwise orthogonal subrepresentations of $V$ such that each $W_i$ is irreducible and that*

$$V = \overline{\bigoplus_{i\in I} W_i}.$$

We already saw the crucial construction in problem I.5.5.9. Let's summarize it in a proposition.

**Proposition IV.2.2.** *(See problem I.5.5.9.) Let $G$ be a compact group, let $dx$ be the normalized Haar measure on $G$, and let $(\pi, V)$ be a unitary representation of $G$. If $u \in V$, then the formula*

$$T(v) = \int_G \langle v, \pi(x)(u)\rangle \pi(x)(u)dx$$

*defines a continuous $G$-equivariant self-adjoint compact endormophism of $V$, and we have $T = 0$ if and only if $u = 0$.*

In fact, we even know that $T$ is positive, i.e. that $\langle T(v), v\rangle \geq 0$ for every $v \in V$.

**Corollary IV.2.3.** *Let $V$ be a nonzero unitary representation of a compact group $G$. Then $V$ contains an irreducible representation of $G$.*

*Proof.* If $V$ is finite-dimensional, then any nonzero $G$-invariant subspace of $V$ of minimal dimension has to be irreducible.

In the general case, choose $u \in V - \{0\}$, and let $T \in \mathrm{End}(V)$ be the endomorphism of $V$ constructed in the proposition. By the spectral theorem for self-adjoint compact operators (theorem IV.1.3), we have

$$V = \overline{\bigoplus_{\lambda\in\mathbb{C}} \mathrm{Ker}(T - \lambda \mathrm{id}_V)}.$$

As $T \neq 0$, the closed subspace $\mathrm{Ker}(T)$ of $V$ is not equal to $V$. By the equality above, there exists $\lambda \in \mathbb{C} - \{0\}$ such that $W := \mathrm{Ker}(T - \lambda \mathrm{id}_V) \neq 0$. Then $W$ is a nonzero closed subspace of $V$, and it is $G$-invariant because $T$ is $G$-equivariant, and stable by $T$ by definition. Also, the space $W$ is finite-dimensional by (iii) of theorem IV.1.3. So $W$ has an irreducible subrepresentation by the beginning of the proof, and we are done.

□

*Proof of the theorem.* By Zorn's lemma, we can find a maximal collection $(W_i)_{i\in I}$ of pairwise orthogonal irreducible subrepresentations of $V$. Suppose that the direct sum of the $W_i$ is not dense in $V$, then $W := \left(\bigoplus_{i\in I} W_i\right)^\perp$ is a nonzero closed invariant subspace of $V$ (see lemma I.3.2.6). By the corollary above, the representation $W$ has an irreducible subrepresentation, which contradicts the maximality of the family $(W_i)_{i\in I}$. Hence $V = \overline{\bigoplus_{i\in I} W_i}$.

□

We finish this section with a remark on two different notions of equivalence for unitary representations. Remember that two continuous representations $V_1$ and $V_2$ of a topological group $G$ are called *equivalent* (or *isomorphic*) if there exists a continuous $G$-equivariant isomorphism $V_1 \to V_2$ with a continuous inverse.

**Definition IV.2.4.** Two unitary representations $V_1$ and $V_2$ of a topological group $G$ are called *unitarily equivalent* if there exists a $G$-equivariant isomorphism $V_1 \to V_2$ that is an isometry.

Two unitarily equivalent representations are clearly equivalent.

**Example IV.2.5.** Let $G$ be a locally compact group, let $\mu$ be a left Haar measure on $G$, and let $\nu$ be the right Haar measure defined by $\nu(E) = \mu(E^{-1})$.

Then the left and right regular representations of $G$ are unitarily equivalent, by sending $f \in L^2(G, \mu)$ to the element $x \longmapsto \Delta(x)^{-1/2} f(x^{-1})$ of $L^2(G, \nu)$. (See proposition I.2.12.)

**Proposition IV.2.6.** *Suppose that $V_1$ and $V_2$ are irreducible unitary representations of $G$. Then they are equivalent if and only if they are unitarily equivalent.*

*Proof.* Suppose that $V_1$ and $V_2$ are equivalent, and let $U : V_1 \to V_2$ be a $G$-equivariant isomorphism. We denote by $\langle .,. \rangle_1$ and $\langle .,. \rangle_2$ the inner products of $V_1$ and $V_2$. Let $B : V_1 \times V_1 \to \mathbb{C}$, $(v, w) \longmapsto \langle U(v), U(w) \rangle_2$. This is a Hermitian sesquilinear form on $V_1$, and it is bounded because $U$ is bounded. By the lemma below, there exists a self-adjoint endomorphism $T \in \operatorname{End}(V_1)$ such that, for all $v, w \in V$, we have $B(v, w) = \langle T(v), w \rangle_1$. Let's prove that $T$ is $G$-equivariant. Let $v \in V$ and $x \in G$. For every $w \in V$, we have

$$\begin{aligned}
\langle T(\pi_1(x)(v)), w \rangle_1 &= B(\pi_1(x)(v), w) \\
&= \langle U(\pi_1(x)(v)), U(w) \rangle_2 \\
&= \langle \pi_2(x)(U(v)), U(w) \rangle_2 \\
&= \langle U(v), \pi_2(x^{-1}) U(w) \rangle_2 \\
&= \langle U(v), U(\pi_1(x)^{-1}(w)) \rangle_2 \\
&= B(v, \pi_1(x^{-1})(w)) \\
&= \langle T(v), \pi_1(x)^{-1}(w) \rangle_1 \\
&= \langle \pi_1(x)(T(v)), w \rangle_1,
\end{aligned}$$

so $T(\pi_1(x)(v)) = \pi_1(x)(T(v))$. As $V_1$ is irreducible, Schur's lemma (theorem I.3.4.1) implies that $T = \lambda \mathrm{id}_{V_1}$ for some $\lambda \in \mathbb{C}$. As $\langle T(v), v \rangle_1 = \langle U(v), U(v) \rangle_2 > 0$ for every nonzero $v \in V_1$, we must have $\lambda \in \mathbb{R}_{>0}$. Then $\lambda^{-1/2} U$ is an isometry, so $V_1$ and $V_2$ are unitarily equivalent.

□

**Lemma IV.2.7.** *Let $V$ be a Hilbert space, and let $B : V \times V \to \mathbb{C}$ be a bounded sesquilinear form (i.e. $B$ is $\mathbb{C}$-linear in the first variable and $\mathbb{C}$-antilinear in the second variable; the boundedness conditions means that $\sup_{v,w \in V,\ \|v\| = \|w\| = 1} |B(v, w)| < +\infty$).*

*Then there exists a unique $T \in \mathrm{End}(V)$ such that, for all $v, w \in V$,*

$$B(v, w) = \langle T(v), w \rangle.$$

*Moreover, $T$ is self-adjoint if and only if $B$ is Hermitian (which means that $B(w, v) = \overline{B(v, w)}$ for all $v, w \in V$).*

*Proof.* The uniqueness of $T$ is clear (it follows from the fact that $V^\perp = \{0\}$.)

If $v \in V$, then the map $V \to \mathbb{C}$, $w \longmapsto \overline{B(v, w)}$ is a continuous linear functional on $V$, so there exists a unique $T(v) \in V$ such that $B(v, w) = \langle T(v), w \rangle$ for every $w \in V$. The linearity of $T$ follows from the fact that $B$ is linear in the first variable. Moreover, for every $v \in V$, we have

$$\|T(v)\| = \sup_{w \in V,\ \|w\|=1} |\langle T(v), w \rangle| = \sup_{w \in V,\ \|w\|=1} |B(v, w)| \leq C\|v\|,$$

where

$$C = \sup_{x, y \in V,\ \|x\|=\|y\|=1} |B(x, y)|.$$

So $T$ is bounded.

Finally, $T$ is self-adjoint if and only, for all $v, w \in V$, we have

$$B(v, w) = \langle T(v), w \rangle = \langle v, T(w) \rangle = \overline{B(w, v)}.$$

This proves the last statement.

□

**Definition IV.2.8.** We denote by $\widehat{G}$ the set of equivalence (or unitary equivalence) classes of irreducible unitary representations of $G$, and call it the *unitary dual* of $G$.

If $(\pi, V) \in \widehat{G}$, we write $\dim(\pi)$ and $\mathrm{End}(\pi)$ for $\dim(V)$ and $\mathrm{End}(\pi)$.

Note that this notation agrees with the one used in exercise I.5.4.1 for a commutative group.

## IV.3 Matrix coefficients

**Definition IV.3.1.** Let $(\pi, V)$ be a unitary representation of a topological group $G$. A *matrix coefficient* of $(\pi, V)$ is a function $G \to \mathbb{C}$ of the form $x \longmapsto \langle \pi(x)(u), v \rangle$, where $u, v \in V$.

Note that matrix coefficients are continuous functions. We denote by $\mathscr{E}_\pi$ or $\mathscr{E}_V$ the subspace of $\mathscr{C}(G)$ spanned by the matrix coefficients of $\pi$.

We start by proving some general results that are true for any group $G$.

**Proposition IV.3.2.** *Let $(\pi, V)$ be a unitary representation of $G$.*

*(i) The subspace $\mathscr{E}_\pi$ of $\mathscr{C}(G)$ only depends on the unitary equivalence class of $\pi$, and it is invariant by the operators $L_x$ and $R_x$, for every $x \in G$.*

*(ii) If $V$ is finite-dimensional, then $\mathscr{E}_\pi$ is finite-dimensional and $\dim(\mathscr{E}_\pi) \leq (\dim V)^2$.*

*(iii) If $V = V_1 \oplus \ldots \oplus V_n$ with the $V_i$ $G$-invariant and pairwise orthogonal, then $\mathscr{E}_\pi = \sum_{i=1}^n \mathscr{E}_{V_i}$.*

*(iv) We have $\mathscr{E}_{\pi^*} = \overline{\mathscr{E}_\pi}$.*

In particular, we get an action of $G \times G$ on $\mathscr{E}_\pi$ by making $(x, y) \in G \times G$ act by $L_x \circ R_y = R_y \circ L_x$.

*Proof.* (i) The first statement is obvious. To prove the second statement, let $v, w \in V$ and $x \in G$. Then, for every $y \in G$,

$$\langle \pi(x^{-1}y)(v), w\rangle = \langle \pi(y)(v), \pi(x)(w)\rangle$$

and

$$\langle \pi(yx)(v), w\rangle = \langle \pi(y)(\pi(x)(v)), w\rangle,$$

so the functions $y \longmapsto \langle \pi(x^{-1}y)(v), w\rangle$ and $y \longmapsto \langle \pi(yx)(v), w\rangle$ are also matrix coefficients of $\pi$.

(ii) Let $(e_1, \ldots, e_n)$ be a basis of $V$. For $i, j \in \{1, \ldots, n\}$, write $\varphi_{ij}$ for the function $G \to \mathbb{C}$, $x \longmapsto \langle \pi(x)(e_i), e_j\rangle$. If $v, w \in V$, we can write $v = \sum_{i=1}^n a_i e_i$ and $w = \sum_{j=1}^n b_j e_j$, and then we have, for every $x \in G$,

$$\langle \pi(x)(v), w\rangle = \sum_{i,j=1}^n a_i \overline{b}_j \varphi_{ij}(x).$$

So the family $(\varphi_{ij})_{1 \leq i,j \leq n}$ spans $\mathscr{E}_\pi$.

(iii) For every $i \in \{1, \ldots, n\}$, we clearly have $\mathscr{E}_{V_i} \subset \mathscr{E}_\pi$. So $\sum_{i=1}^n \mathscr{E}_{V_i} \subset \mathscr{E}_\pi$. Conversely, let $v, w \in V$, and write $v = \sum_{i=1}^n v_i$ and $w = \sum_{i=1}^n w_i$, with $v_i, w_i \in V_i$. Then, for every $x \in G$,

$$\langle \pi(x)(v), w\rangle = \sum_{i,j=1}^n \langle \pi(x)(v_i), w_j\rangle = \sum_{i=1}^n \langle \pi(x)(v_i), w_i\rangle.$$

So the function $x \longmapsto \langle \pi(x)(v), w\rangle$ is in $\sum_{i=1}^n \mathscr{E}_{V_i}$.

□

**Definition IV.3.3.** Let $(\pi, V)$ and $(\pi', V')$ be continuous representation of $V$. We define an action $\rho$ of $G \times G$ on $\mathrm{Hom}(V, V')$ by

$$\rho(x, y)(T) = \pi'(y) \circ T \circ \pi(x)^{-1},$$

for $T \in \mathrm{Hom}(V, V')$ and $x, y \in G$.

**Proposition IV.3.4.** *We have*

$$\mathrm{Hom}_G(V, V') = \{T \in \mathrm{Hom}(V, V') | \forall x \in G,\ \rho(x, x)(T) = T\}.$$

*Moreover, if the maps $G \to \mathrm{End}(V)$, $x \longmapsto \pi(x)$ and $G \to \mathrm{End}(V')$, $x \longmapsto \pi'(x)$ are continuous (for example if $V$ and $V'$ are finite-dimensional, see proposition I.3.5.1), then the action defined above is a continuous representation of $G \times G$ on* $\mathrm{Hom}(V, V')$.

*Proof.* The first statement is obvious. The second statement follows from the continuity of the composition on $\mathrm{Hom}$ spaces, and of inversion on $G$.

□

In particular, we get actions of $G \times G$ on $\mathrm{End}(V)$ and $V^* := \mathrm{Hom}(V, \mathbb{C})$ (using the trivial action of $G$ on $\mathbb{C}$); the second one gives an action of $G$ on $V^*$ by restriction to the first factor (if $x \in G$ and $\Lambda \in V^*$, then $(x, \Lambda)$ is sent to $\Lambda \circ \pi(x)^{-1}$). This will be the default action on these spaces.

**Definition IV.3.5.** Let $(\pi, V)$ and $(\pi', V')$ be continuous representations of $V$. We define an action $\rho$ of $G \times G$ on the algebraic tensor product $V \otimes_{\mathbb{C}} V'$ by

$$\rho(x, y)(v \otimes w) = \pi(x)(v) \otimes \pi'(y)(w),$$

for $x, y \in G$, $v \in V$ and $w \in V'$.

This action is well-defined because, for all $x, y \in G$, the map $V \times V' \to V \otimes_{\mathbb{C}} V'$, $(v, w) \longmapsto \pi(x)(v) \otimes \pi'(y)(w)$ is bilinear, hence induces a map $\rho(x, y) : V \otimes_{\mathbb{C}} V' \to V \otimes_{\mathbb{C}} V'$. If $V$ and $V'$ are finite-dimensional, the resulting action of $G \times G$ on $V \otimes_{\mathbb{C}} V'$ is continuous by proposition I.3.5.1.

Note that, if we restrict the action of $G \times G$ on $V \otimes_{\mathbb{C}} W$ to the first (resp. the second) factor, we get a representation equivalent to $V^{\oplus \dim(W)}$ (resp. $W^{\oplus \dim(V)}$).

**Proposition IV.3.6.** *Let $V, W$ be continuous representations of $G$.*

*(i) The map $V^* \otimes_{\mathbb{C}} W \to \mathrm{Hom}(V, W)$ sending $\Lambda \otimes w$ (with $\Lambda \in V^*$, $w \in W$) to the linear operator $V \to W$, $v \longmapsto \Lambda(v)w$ is well-defined and $G \times G$-equivariant. If $V$ and $W$ are finite-dimensional, it is an equivalence of continuous representations.*

*(ii) The map $V^* \otimes_{\mathbb{C}} V \to \mathscr{C}(G)$ sending $\Lambda \otimes v$ (with $\Lambda \in V^*$, $v \in V$) to the function $G \to \mathbb{C}$, $x \longmapsto \Lambda(\pi(x)(v))$ is well-defined and $G \times G$-equivariant, and its image is $\mathscr{E}_V$ if $V$ is unitary.*

In particular, if $V$ is finite-dimensional and unitary, we get a surjective $G \times G$-equivariant map $\mathrm{End}(V) \to \mathscr{E}_V$.

*Remark* IV.3.7. Point (ii) suggests a way to generalize the definition of a matrix coefficients to the non-unitary case : just define a matrix coefficient as the image of a pure tensor by the map $V^* \otimes_{\mathbb{C}} V \to \mathscr{C}(G)$.

*Proof.* In this proof, we will denote all the actions of $G$ and $G \times G$ by a $\cdot$ (this should not cause confusion, as each space has at most one action).

(i) The map is well-defined, because the map $V^* \otimes_{\mathbb{C}} W \to \mathrm{Hom}(V, W)$ sending $(\Lambda, w)$ to $(v \longmapsto \Lambda(v)w)$ is bilinear. Let's denote it by $\varphi$. To check that it is $G \times G$-equivariant, it suffices to check it on pure tensors (because they generate $V^* \otimes_{\mathbb{C}} W$). So let $\Lambda \in V^*$, $w \in W$, $x, y \in G$. For every $v \in V$, we have

$$\varphi((x,y) \cdot (\Lambda \otimes w))(v) = \varphi((y \cdot \Lambda) \otimes (x \cdot w))(v) = \Lambda(y^{-1} \cdot v)(x \cdot w)$$

and

$$((x,y) \cdot \varphi(\Lambda \otimes w))(v) = x \cdot (\varphi(\Lambda \otimes w)(y^{-1} \cdot v)) = x \cdot (\Lambda(y^{-1} \cdot)w) = \Lambda(y^{-1} \cdot v)(x \cdot w).$$

So

$$\varphi(x \cdot (\Lambda \otimes w)) = x \cdot \varphi(\Lambda \otimes w).$$

Suppose that $V$ is finite-dimensional, let $(e_1, \ldots, e_n)$ be a basis of $V$, and let $(e_1^*, \ldots, e_n^*)$ be the dual basis. Define $\psi : \mathrm{Hom}(V, W) \to V^* \otimes_{\mathbb{C}} W$ by sending $T$ to $\sum_{i=1}^n e_i^* \otimes T(e_i)$. Let's show that $\psi$ is the inverse of $\varphi$.

If $j \in \{1, \ldots, m\}$ and $w \in W$, then

$$\psi(\varphi(e_j^* \otimes w)) = \sum_{i=1}^n e_i^* \otimes (\varphi(e_j^* \otimes w)(e_i)) = e_j^* \otimes w.$$

As the elements $e_j^* \otimes w$, for $j \in \{1, \ldots, n\}$ and $w \in W$, generate $V^* \otimes_{\mathbb{C}} W$, this shows that $\psi \circ \varphi = \mathrm{id}$.

Conversely, if $T \in \mathrm{Hom}(V, W)$, then, for every $v \in V$,

$$\varphi(\psi(T)) = \sum_{i=1}^n \varphi(e_i^* \otimes T(e_i))(v) = \sum_{i=1}^n e_i^*(v) T(e_i) = T(v),$$

because $v = \sum_{i=1}^n e_i^*(v) v$. So $\varphi(\psi(T)) = T$.

This shows that, if $V$ is finite-dimensional, the map $V^* \otimes_{\mathbb{C}} W \to \mathrm{Hom}(V, W)$ is an isomorphism. The last statement follows immediately.

(ii) The map is well-defined because the map $V^* \times V \to \mathscr{C}(G)$ sending $(\Lambda, v)$ to the function $x \longmapsto \Lambda(\pi(x)(v))$ is bilinear. Let's denote it by $\alpha$. We show that $\alpha$ is $G \times G$-equivariant.

As before, it suffices to check it on pure tensors. So let $\Lambda \in V^*$, $v \in V$ and $x, y \in G$. For every $z \in G$, we have

$$\alpha((x,y)\cdot(\Lambda\otimes v))(z) = \Lambda(x^{-1}\cdot(z\cdot(y\cdot v))) = \Lambda((x^{-1}zy)\cdot v) = ((L_x \circ R_y)(\alpha(\Lambda\otimes v)))(z),$$

hence $\alpha((x,y)\cdot(\Lambda\otimes v)) = (L_x \circ R_y)(\alpha(\Lambda\otimes v))$.

Finally, we show that the image of $\alpha$ is $\mathscr{E}_V$ if $V$ is unitary. Let $\Lambda \in V^*$. As $V$ is a Hilbert space, there exists a unique $v \in V$ such that $\Lambda = \langle ., v\rangle$. So, for every $w \in V$ and every $x \in G$, we have

$$\alpha(\Lambda \otimes w)(v) = \langle \pi(x)(w), v\rangle.$$

This shows that $\alpha(\Lambda \otimes w)$ is a matrix coefficient of $\pi$, and also that we get all the matrix coefficients of $\pi$ in this way.

□

Now we prove stronger results that are only true for compact groups. If $G$ is a compact group, we fix a normalized Haar measure on $G$, and we denote by $L^p(G)$ the $L^p$ space for this measure. Note that we have $\mathscr{C}(G) \subset L^p(G)$ for every $p$.

**Theorem IV.3.8.** *Let $G$ be a compact group, and let $(\pi, V)$ be an irreducible unitary representation of $G$. Remember that $V$ is finite-dimensional (by exercise I.5.5.9).*

*(i) (Schur orthogonality) If $(\pi', V')$ is another irreducible unitary representation of $G$ that is not equivalent to $(\pi, V)$, then $\mathscr{E}_\pi$ and $\mathscr{E}_{\pi'}$ are orthogonal as subspaces of $L^2(G)$.*

*(ii) We have $\dim(\mathscr{E}_\pi) = (\dim V)^2$. More precisely, if $(e_1, \dots, e_d)$ is an orthonormal basis of $V$ and if we denote by $\varphi_{ij}$ the function $G \to \mathbb{C}$, $x \longmapsto \langle \pi(x)(e_j), e_i\rangle$, then $\{\sqrt{d}\varphi_{ij},\ 1 \le i,j \le d\}$ is an orthonormal basis of $\mathscr{E}_\pi$ for the $L^2$ inner product.*

*(iii) The $G \times G$-equivariant map $\mathrm{End}(V) \to \mathscr{E}_\pi$ defined above is an isomorphism.*

*Proof.* Note that (iii) follows immediately from (ii), because $\mathrm{End}(V) \to \mathscr{E}_\pi$ is surjective and (ii) says that $\dim(\mathscr{E}_\pi) = (\dim V)^2 = \dim(\mathrm{End}(V))$.

We prove (i) and (ii). Let $(\pi', V')$ be an irreducible unitary representation of $G$, that could be equal to $(\pi, V)$. If $A \in \mathrm{Hom}(V, V')$, we define $\widetilde{A} \in \mathrm{Hom}(V, V')$ by

$$\widetilde{A} = \int_G \pi'(x)^{-1} \circ A \circ \pi(x) dx$$

(note that there is no problem with the integral, because the representations are finite-dimensional). Then, for every $y \in G$, we have

$$\begin{aligned}\widetilde{A} \circ \pi(y) &= \int_G \pi'(x)^{-1} \circ A \circ \pi(xy) dx \\ &= \int_G \pi'(xy^{-1})^{-1} \circ A \circ \pi(x) dx \quad \text{(right invariance of } dx\text{)} \\ &= \pi'(y) \circ \widetilde{A}.\end{aligned}$$

In other words, $\widetilde{A}$ is $G$-equivariant.

Let $v \in V$ and $v' \in V'$, and define $A \in \mathrm{Hom}(V, V')$ by $A(u) = \langle u, v\rangle v'$. Then, for all $u \in V$ and $u' \in V$, we have

$$\begin{aligned}\langle \widetilde{A}(u), u'\rangle &= \int_G \langle (\pi'(x)^{-1} \circ A \circ \pi(x))(u), u'\rangle dx \\ &= \int_G \langle \langle \pi(x)(u), v\rangle \pi'(x)^{-1}(v'), u'\rangle dx \\ &= \int_G \langle \pi(x)(u), v\rangle \overline{\langle \pi'(x)(u'), v'\rangle} dx.\end{aligned}$$

Suppose that $\pi$ and $\pi'$ are not equivalent. Then, by Schur's lemma, we have $\widetilde{A} = 0$ for every $A \in \mathrm{Hom}(V, V')$, and so, by the calculation above, for all $u, v \in V$ and $u', v' \in V'$,

$$\int_G \langle \pi(x)(u), v\rangle \overline{\langle \pi'(x)(u'), v'\rangle} dx = 0.$$

This proves (i).

Suppose that $\pi = \pi'$, and use the notation of (ii). Take $v = e_i$ and $v' = e_{i'}$ with $i, i' \in \{1, \ldots, d\}$, and define $A$ as above. By Schur's lemma again, there exists $c \in \mathbb{C}$ such that $\widetilde{A} = c\mathrm{id}_V$. So, taking $u = e_j$ and $u' = e_{j'}$, we get from the calculation above that

$$\langle \varphi_{i,j}, \varphi_{i',j'}\rangle_{L^2(G)} = \langle ce_j, e_{j'}\rangle = \begin{cases} c & \text{if } j = j' \\ 0 & \text{otherwise.}\end{cases}$$

On the other hand, we have

$$cd = \mathrm{Tr}(\widetilde{A}) = \int_G \mathrm{Tr}(\pi(x)^{-1} \circ A \circ \pi(x)) dx = \int_G \mathrm{Tr}(A) dx = \mathrm{Tr}(A).$$

As $A$ is defined by $A(w) = \langle w, e_i\rangle e_{i'}$, we have $\mathrm{Tr}(A) = 0$ if $i \neq i'$, and $\mathrm{Tr}(A) = 1$ if $i = i'$. This finishes the proof that $\{\sqrt{d}\varphi_{ij},\ 1 \leq i, j \leq d\}$ is an orthonormal basis of $\mathscr{E}_\pi$.

□

## IV.4 The Peter-Weyl theorem

Let $G$ be a compact group. We see $L^2(G)$ as a representation of $G \times G$ by making $(x, y) \in G \times G$ act by $L_x \circ R_y = R_y \circ L_x$. The restriction of this to the first (resp. second) factor is the left (resp. rigth) regular representation of $G$.

**Definition IV.4.1.** Let $G$ be a compact group. We denote by $\mathscr{E}$ the subspace of matrix coefficients in $\mathscr{C}(G)$.

By theorem IV.3.8, we have $\mathscr{E} = \bigoplus_{\pi \in \widehat{G}} \mathscr{E}_\pi$.

**Theorem IV.4.2.** *If $G$ is compact, then $\mathscr{E}$ is a dense subalgebra of $\mathscr{C}(G)$. (For the usual pointwise multiplication and the norm $\|.\|_\infty$.)*

*Proof.* Let's prove that $\mathscr{E}$ is stable by multiplication. Note that, by (iii) of proposition IV.3.2 and theorem IV.2.1, for every finite-dimensional unitary representation $\pi$ of $G$, we have $\mathscr{E}_\pi \subset \mathscr{E}$. Let $(\pi, V)$ and $(\pi', V')$ be irreducible unitary representations of $G$, and let $v, w \in V$ and $v', w' \in V'$. Remember that we have defined an action $\pi \otimes \pi'$ of $G$ on $V \otimes_{\mathbb{C}} V'$[3] and an inner product on $V \otimes_{\mathbb{C}} V'$ in exercise III.6.2.1. [4] By definition of these, for every $x \in G$, we have

$$\langle (\pi \otimes \pi')(x)(v \otimes w), v' \otimes w' \rangle = \langle \pi(x)(v), w \rangle \langle \pi'(x)(v'), w \rangle.$$

This proves that the product of a matrix coefficient of $\pi$ and a matrix coefficient of $\pi'$ is a matrix coefficient of $\pi \otimes \pi'$. By the observation above, every matrix coefficient of $\pi \otimes \pi'$ is in $\mathscr{E}$, and we are done.

Now we prove that $\mathscr{E}$ is dense in $\mathscr{C}(G)$. We have shown that $\mathscr{E}$ is a subalgebra, it is stable by complex conjugation by proposition IV.3.2(iv), it contains the constants (they are the matrix coefficients of the trivial representation of $G$ on $\mathbb{C}$) and it separates points on $G$ by the Gelfand-Raikov theorem (theorem III.5.1). So it is dense in $\mathscr{E}$ by the Stone-Weierstrass theorem.

∎

**Corollary IV.4.3.** *For every $p \in [1, +\infty)$, the subspace $\mathscr{E}$ of $L^p(G)$ is dense for the $L^p$ norm.*

*In particular, we have a canonical $G \times G$-equivariant isomorphism*

$$L^2(G) = \overline{\bigoplus_{(\pi,V) \in \widehat{G}} \operatorname{End}(V)}.$$

The last statement is what is usually called the Peter-Weyl theorem. It implies that the left and right regular representations of $G$ are both isomorphic to the completion of $\bigoplus_{\pi \in \widehat{G}} \pi^{\oplus \dim(\pi)}$.

*Remark* IV.4.4. The Peter-Weyl theorem actually predates the Gelfand-Raikov theorem, and the original proof uses the fact that the operators $f * .$ are compact on $L^2(G)$, for $f \in L^2(G)$.

[3] This is just the restriction to the diagonal of $G \times G$ of the action defined above.

[4] We don't need to complete the tensor product here, because $V$ and $V'$ are finite-dimensional.

## IV.5 Characters

**Definition IV.5.1.** Let $(\pi, V)$ be a continuous finite-dimensional representation of a topological group $G$. The *character* of $\pi$ is the continuous map $\chi_V = \chi_\pi : G \to \mathbb{C}$, $x \longmapsto \mathrm{Tr}(\pi(x))$.

*Remark* IV.5.2. If $(\pi, V)$ is a finite-dimensional representation of $G$ and $(e_1, \dots, e_n)$ is an orthonormal basis of $V$, then, for every $x \in G$, we have

$$\chi_\pi(x) = \sum_{i=1}^{n} \langle \pi(x)(e_i), e_i \rangle.$$

So $\chi_\pi \in \mathscr{E}_\pi$.

**Definition IV.5.3.** We say that a function $f : G \to \mathbb{C}$ is a *central function* or a *class function* if $f(xyx^{-1}) = f(y)$ for all $x, y \in G$.

These functions are called central because they are central for the convolution product, as we will see in section IV.7.

**Proposition IV.5.4.** *Let $G$ be a topological group, and let $(\pi, V)$ and $(\pi', V')$ be continuous finite-dimensional representations of $G$. Then :*

*(i)* $\chi_\pi$ *is a central function, and it only depends on the equivalence class of* $\pi$.

*(ii)* $\chi_{V \oplus V'} = \chi_V + \chi_{V'}$.

*(iii) For every* $x \in G$, $\chi_{V^*}(x) = \chi(x^{-1})$.

*(iv) For all* $x, y \in G$, *we have*

$$\chi_{V \otimes_{\mathbb{C}} V'}(x, y) = \chi_V(x)\chi_{V'}(y) \quad \textit{and} \quad \chi_{\mathrm{Hom}(V,V')}(x, y) = \chi_V(x^{-1})\chi_{V'}(y).$$

*(v) If* $(\pi, V)$ *is unitarizable (for example if* $G$ *is compact), then* $\chi_V(x^{-1}) = \overline{\chi_V(x)}$ *for every* $x \in G$.

*Proof.* Point (i) just follows from the properties of the trace, i.e. the fact that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for all $A, B \in M_n(\mathbb{C})$.

Put arbitrary Hermitian inner products on $V$ and $V'$. Let $(e_1, \dots, e_n)$ (resp. $(e'_1, \dots, e'_m)$) be an orthonormal basis of $V$ (resp. $V'$). Then $(e_1, \dots, e_n, e'_1, \dots, e'_m)$ is an orthonormal basis of $V \oplus V'$, so, for every $x \in G$,

$$\chi_{V \oplus V'}(x) = \sum_{i=1}^{n} \langle \pi(x)(e_i), e_i \rangle + \sum_{j=1}^{m} \langle \pi'(x)(e'_j), e'_j \rangle = \chi_V(x) + \chi_{V'}(x).$$

This proves (ii).

Let $(e_1^*, \dots, e_n^*)$ be the dual basis of $(e_1, \dots, e_n)$. Let $x \in G$. Then, if $A$ is the matrix of $\pi(x^{-1})$ in the basis $(e_1, \dots, e_n)$, the matrix of the endomorphism $\Lambda \longmapsto \Lambda \circ \pi(x^{-1})$ in the basis $(e_1^*, \dots, e_n^*)$ is $A^T$, and we have

$$\chi_{V^*}(x) = \mathrm{Tr}(A^T) = \mathrm{Tr}(A) = \chi_V(x^{-1}).$$

This proves (iii).

We prove the formula for $\chi_{V \otimes_{\mathbb{C}} V'}$. We have seen in exercise III.6.2.1 how to put an inner product on $V \otimes_{\mathbb{C}} V'$ for which $(e_i \otimes e'_j)_{1 \le i \le n, 1 \le j \le m}$ is an orthonormal basis. So, for all $x, y \in G$, we have

$$\begin{aligned}\chi_{V \otimes_{\mathbb{C}} V'}(x, y) &= \sum_{i=1}^n \sum_{j=1}^m \langle \pi(x)(e_i) \otimes \pi'(y)(e'_j), e_i \otimes e'_j \rangle \\ &= \sum_{i=1}^n \sum_{j=1}^m \langle \pi(x)(e_i), e_i \rangle \langle \pi'(y)(e'_j), e'_j \rangle \\ &= \chi_V(x) \chi_{V'}(y).\end{aligned}$$

Now the formula for $\chi_{\mathrm{Hom}(V,V')}$ follows from this, from (iii) and from proposition IV.3.6(i).

Finally, we prove (v). If $V$ is unitarizable, we can choose the Hermitian inner form on $V$ to be invariant by $G$. Then, for every $x \in G$, we have

$$\chi_V(x^{-1}) = \sum_{i=1}^n \langle \pi(x)^{-1}(e_i), e_i \rangle = \sum_{i=1}^n \langle e_i, \pi(x)(e_i) \rangle = \sum_{i=1}^n \overline{\langle \pi(x)(e_i), e_i \rangle} = \overline{\chi_V(x)}.$$

$\square$

**Notation IV.5.5.** If $(\pi, V)$ is a representation of a topological group $G$ (continuous or not), we write

$$V^G = \{v \in V | \forall x \in G,\ \pi(x)(v) = v\}.$$

This is a closed $G$-invariant subspace of $V$.

**Example IV.5.6.** If $V$ and $W$ are two representations of $G$, then

$$\mathrm{Hom}(V, W)^G = \mathrm{Hom}_G(V, W).$$

**Theorem IV.5.7.** *Let $G$ be a compact group and $(\pi, V)$ be a finite-dimensional continuous representation of $G$. Then*

$$\int_G \chi_V(x) dx = \dim(V^G).$$

*Proof.* As $V$ is finite-dimensional, we can find a finite family $(V_i)_{i\in I}$ of irreducible subrepresentations of $V$ such that $V = \bigoplus_{i\in I} V_i$. (Cf. corollary I.3.2.9.) We have $\chi_V = \sum_{i\in I} \chi_{V_i}$ by proposition IV.5.4, and $V^G = \bigoplus_{i\in I} V_i^G$. So it suffices to prove the theorem for $V$ irreducible.

Suppose that $V$ is an irreducible representation of $V$. As $V^G$ is a $G$-invariant subspace of $V$, we have $V^G = V$ or $V^G = \{0\}$. If $V^G = V$, then $G$ acts trivially on $V$, so every linear subspace of $V$ is invariant by $G$, so we must have $\dim V = 1$. On the other hand, we have $\chi_V(x) = \mathrm{Tr}(1) = 1$ for every $x \in G$, so $\int_G \chi_V(x)dx = 1$. Suppose that $V$ is irreducible and that $V^G = \{0\}$. Let $\pi_0$ be the trivial representation of $G$ on $\mathbb{C}$. Then, by theorem IV.3.8(i), the subspaces $\mathscr{E}_\pi$ and $\mathscr{E}_{\pi_0}$ of $L^2(G)$ are orthogonal. But $\mathscr{E}_{\pi_0}$ is the subspace of constant functions, and we saw above (remark IV.5.2) that $\chi_V \in \mathscr{E}_\pi$. So $\chi_V$ is orthogonal to the constant function 1, which means exactly that $\int_G \chi_V(x)dx = 0$.

□

**Corollary IV.5.8.** *Let $G$ be a compact group, and let $(\pi, V)$ and $(\sigma, W)$ be two continuous finite-dimensional representations of $G$.*

*(i) We have $\langle \chi_W, \chi_V \rangle_{L^2(G)} = \dim_{\mathbb{C}}(\mathrm{Hom}_G(V, W))$.*

*(ii) If $V$ and $W$ are irreducible and not equivalent, then $\langle \chi_V, \chi_W \rangle_{L^2(G)} = 0$.*

*(iii) The representation $V$ is irreducible if and only $\|\chi\|_{L^2(G)} = 1$.*

*Proof.* (i) Make $G$ act on $\mathrm{Hom}(V, W)$ by $x \cdot T = \rho(x) \circ T \circ \pi(x)^{-1}$. We know (cf. proposition IV.3.4) that $\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G$. Applying the theorem to the representation $\mathrm{Hom}(V, W)$ and using points (iv) and (v) of proposition IV.5.4 to calculate the character of this representation, we get :

$$\begin{aligned}\dim_{\mathbb{C}}(\mathrm{Hom}_G(V, W)) &= \dim_{\mathbb{C}}(\mathrm{Hom}(V, W)^G) \\ &= \int_G \chi_{\mathrm{Hom}(V,W)}(x)dx \\ &= \int_G \overline{\chi_V(x)}\chi_W(x)dx \\ &= \langle \chi_W, \chi_V \rangle_{L^2(G)}.\end{aligned}$$

(ii) This follows from (i) and from Schur's lemma (theorem I.3.4.1), or from the fact that $\chi_V \in \mathscr{E}_V$, $\chi_W \in \mathscr{E}_W$ and $\mathscr{E}_V$ and $\mathscr{E}_W$ are orthogonal in $L^2(G)$ (see theorem IV.3.8).

(iii) If $V$ is irreducible, then Schur's lemma implies that $\mathrm{End}_G(V)$ is 1-dimensional, so we have $\|\chi_V\|_{L^2(G)} = 1$ by (i). Conversely, suppose that $\|\chi_V\|_{L^2(G)} = 1$. We write $V = \bigoplus_{i\in I} V_i$, where $I$ is finite and the $V_i$ are irreducible subrepresentations of $V$. By (ii), the characters of non-isomorphic irreducible representations of $G$ are orthogonal in $L^2(G)$, so we have

$$\|\chi_V\|^2_{L^2(G)} = \sum_{W\in\widehat{G}} n_W \|\chi_W\|^2_{L^2(G)} = \sum_{W\in\widehat{G}} n_W,$$

where, for every $W \in \widehat{G}$,

$$n_W = \mathrm{card}(\{i \in I | V_i \simeq W\}).$$

As $\|\chi_V\|_{L^2(G)} = 1$, there is a unique $W \in \widehat{G}$ such that $n_W \neq 0$, and we must have $n_W = 1$. By the definition of the integers $n_W$, this means that $V \simeq W$, so $V$ is irreducible.

□

**Corollary IV.5.9.** *Let $G$ be a compact group. Then the family $(\chi_V)_{V \in \widehat{G}}$ of elements of $L^2(G)$ (or $\mathscr{C}(G)$) is linearly independent.*

*Proof.* This follows from (ii) of the previous corollary.

□

**Corollary IV.5.10.** *Let $\pi$ and $\pi'$ be two continuous finite-dimensional representations of a compact group $G$. Then $\pi$ and $\pi'$ are equivalent if and only if $\chi_\pi = \chi_{\pi'}$.*

*Proof.* If $\pi$ and $\pi'$ are equivalent, we already know that $\chi_\pi = \chi_{\pi'}$. Conversely, suppose that $\chi_\pi = \chi_{\pi'}$. We decompose $\pi$ and $\pi'$ as direct sums of irreducible representations :

$$\pi \simeq \bigoplus_{\rho \in \widehat{G}} \rho^{n_\rho}$$

and

$$\pi' \simeq \bigoplus_{\rho \in \widehat{G}} \rho^{m_\rho},$$

with $n_\rho, m_\rho \in \mathbb{Z}_{\geq 0}$ and $n_\rho = m_\rho = 0$ for all but a finite number of $\rho \in \widehat{G}$. By corollary IV.5.8, we have $\chi_\pi = \sum_{\rho \in \widehat{G}} n_\rho \chi_\rho$ and $\chi_{\pi'} = \sum_{\rho \in \widehat{G}} m_\rho \chi_\rho$ (and these are finite sums). By the linear independence of the $\chi_\rho$, the equality $\chi_\pi = \chi_{\pi'}$ implies that $n_\rho = m_\rho$ for every $\rho \in \widehat{G}$, which in turn implies that $\pi$ and $\pi'$ are equivalent.

□

## IV.6 The Fourier transform

We still assume that $G$ is a compact group.

By propositions I.4.3.4 and I.4.1.3, the space $L^2(G)$ is actually a Banach algebra for the convolution product. This section answers the question "how can we see the algebra structure in the decomposition given by the Peter-Weyl theorem ?".

**Definition IV.6.1.** Let $f \in L^2(G)$. For every $(\pi, V) \in \widehat{G}$, the *Fourier transform of $f$ at $\pi$* is the endomorphism

$$\widehat{f}(\pi) = \int_G f(x)\pi(x^{-1})dx = \int_G f(x)\pi(x)^* dx$$

of $V$.

This is clearly a $\mathbb{C}$-linear endomorphism of $V$.

**Example IV.6.2.** Suppose that $G = S^1$. Then we have seen in exercise I.5.4.1 that $\widehat{G} \simeq \mathbb{Z}$, where $n \in \mathbb{Z}$ corresponds to the representation $G \to \mathbb{C}^\times$, $e^{2i\pi t} \longmapsto e^{2i\pi nt}$ (with $t \in \mathbb{R}$). So, if $f \in L^1(G)$, its Fourier transform is the function $\widehat{f} : \mathbb{Z} \to \mathbb{C}$ sending $n$ to

$$\widehat{f}(n) = \int_0^1 f(e^{2i\pi t})e^{-2i\pi nt}dt.$$

**Theorem IV.6.3.** *(i) For every $\pi \in \widehat{G}$, the map $L^2(G) \to \mathrm{End}(\pi)$, $f \longmapsto \widehat{f}(\pi)$ is a $G \times G$-equivariant $*$-homomorphism from $L^2(G)$ to the opposite algebra of $\mathrm{End}(\pi)$. (Note that $L^2(G) \subset L^1(G)$, because $G$ is compact. The involution of $L^1(G)$ defined in example I.4.2.2 restricts to an involution of $L^2(G)$.)*

*In other words, we have, for $f, g \in L^2(G)$ and $x \in G$ :*

$$\widehat{f * g}(\pi) = \widehat{g}(\pi) \circ \widehat{f}(\pi),$$

$$\widehat{f^*}(\pi) = (\widehat{f}(\pi))^*,$$

$$\widehat{L_x f}(\pi) = \widehat{f}(\pi) \circ \pi(x)^{-1} \text{ and } \widehat{R_x f}(\pi) = \pi(x) \circ \widehat{f}(\pi).$$

*(Compare with (i) of theorem I.4.2.6.)*

*(ii) Let $f \in L^2(G)$. Then, for every $\pi \in \widehat{G}$, the function $\dim(\pi)\mathrm{Tr}(\widehat{f}(\pi) \circ \pi(.)) \in L^2(G)$ is the orthogonal projection of $f$ on $\mathscr{E}_\pi$, and the series*

$$\sum_{\pi \in \widehat{G}} \dim(\pi)\mathrm{Tr}(\widehat{f}(\pi) \circ \pi(.))$$

*converges to $f$ in $L^2(G)$ (Fourier inversion formula).*

*(iii) For every $f \in L^2(G)$, we have*

$$\|f\|_2^2 = \sum_{\pi \in \widehat{G}} \dim(\pi)\mathrm{Tr}(\widehat{f}(\pi)^* \circ \widehat{f}(\pi))$$

*(Parseval formula).*

**Example IV.6.4.** Take $G = S^1$. Then (ii) and (iii) say that, for every $f \in L^2(S^1)$, the series $\sum_{n \in \mathbb{Z}} \widehat{f}(n)e^{2i\pi nt}$ converges to $f$ in $L^1(S^1)$ and that

$$\int_0^1 |f(e^{2i\pi t})|^2 dy = \sum_{n \in \mathbb{Z}} |\widehat{f}(n)|^2.$$

*Proof.* (i) We have

$$\begin{aligned}
\widehat{f * g}(\pi) &= \int_G (f*g)(x)\pi(x^{-1})dx \\
&= \int_{G\times G} f(y)g(y^{-1}x)\pi(x^{-1})dxdy \\
&= \int_{G\times G} f(y)g(x)\pi(x^{-1}y^{-1})dxdy \quad \text{(change of variable } x' = y^{-1}x\text{)} \\
&= \widehat{g}(\pi)\circ\widehat{f}(\pi).
\end{aligned}$$

Remember that $f^*(x) = \overline{f(x^{-1})}$, because $\Delta = 1$. So

$$\begin{aligned}
\widehat{f^*}(\pi) &= \int_G \overline{f(x^{-1})}\pi(x)^* dx \\
&= \int_G \overline{f(x)}\pi(x^{-1})^* dx \\
&= (\widehat{f}(\pi))^*.
\end{aligned}$$

Finally,

$$\begin{aligned}
\widehat{L_x f}(\pi) &= \int_G f(x^{-1}y)\pi(y^{-1})dy \\
&= \int_G f(y)\pi(y^{-1}x^{-1})dy \\
&= \widehat{f}(\pi)\circ\pi(x^{-1})
\end{aligned}$$

and

$$\begin{aligned}
\widehat{R_x f}(\pi) &= \int_G f(yx)\pi(y^{-1})dy \\
&= \int_G f(y)\pi(xy^{-1})dy \\
&= \pi(x)\circ\widehat{f}(\pi).
\end{aligned}$$

(ii) It is enough to prove the first statement (the second will follow by the Peter-Weyl theorem). Let $(\pi, V) \in \widehat{G}$. As in theorem IV.3.8, fix an orthonormal basis $(e_1, \dots, e_d)$ of $V$ and denote by $\varphi_{ij}$ the function $G \to \mathbb{C}$, $x \longmapsto \langle \pi(x)(e_j), e_i\rangle$. Then we have seen (in (ii) of theorem IV.3.8) that $\{\sqrt{d}\varphi_{ij},\ 1 \le i,j \le d\}$ is an orthonormal basis of $\mathscr{E}_\pi$ for the $L^2$ inner product. So the orthogonal projection of $f$ on $\mathscr{E}_\pi$ is

$$d\sum_{i,j=1}^{d} \langle f, \varphi_{ij}\rangle_{L^2(G)}\varphi_{ij}.$$

For all $i, j \in \{1, \dots, d\}$, we have

$$\begin{aligned}\langle f, \varphi_{i,j}\rangle_{L^2(G)} &= \int_G f(x)\langle e_i, \pi(x)(e_j)\rangle dx \\ &= \int_G f(x)\langle \pi(x)^*(e_i), e_j\rangle dx \\ &= \langle \widehat{f}(\pi)(e_i), e_j\rangle.\end{aligned}$$

Let $y \in G$, and let $(\widehat{\pi}(f)_{i,j})$ and $(\pi(y)_{i,j})$ be the matrices of $\widehat{f}(\pi)$ and $\pi(y)$ in the basis $(e_1, \dots, e_d)$. Then

$$\widehat{f}(\pi)_{i,j} = \langle \widehat{f}(\pi)(e_j), e_i\rangle = \langle f, \varphi_{j,i}\rangle_{L^2(G)}$$

and

$$\pi(y)_{i,j} = \langle \pi(y)(e_j), e_i\rangle = \varphi_{ij}(y),$$

so

$$\mathrm{Tr}(\widehat{f}(\pi) \circ \pi(y)) = \sum_{i,j=1}^{d} \widehat{f}(\pi)_{j,i}\pi(y)_{i,j} = \sum_{i,j=1}^{d} \langle \widehat{f}(\pi), \varphi_{i,j}\rangle_{L^2(G)}\varphi_{i,j}(y).$$

This gives the desired formula for the orthogonal projection of $f$ on $\mathscr{E}_\pi$.

(iii) Let $\pi \in \widehat{G}$, and use the notation of the proof of (ii). Let $g = d\mathrm{Tr}(\widehat{f}(\pi)^* \circ \widehat{f}(\pi))$. It suffices to show that $\|g\|_2^2 = d\mathrm{Tr}(\widehat{f}(\pi)^* \circ \widehat{f}(\pi))$ (because the $\mathscr{E}_\pi$ for non-isomorphic $\pi$ are orthogonal, by theorem IV.3.8). We have

$$\mathrm{Tr}(\widehat{f}(\pi)^* \circ \widehat{f}(\pi)) = \sum_{i,j=1}^{d} |\widehat{f}(\pi)_{i,j}|^2 = \sum_{i,j=1}^{d} |\langle f, \varphi_{i,j}\rangle_{L^2(G)}|^2.$$

On the other hand, as $g = d\sum_{i,j=1}^{d}\langle f, \varphi_{ij}\rangle_{L^2(G)}\varphi_{ij}$, we get

$$\|g\|_{L^2(G)}^2 = d^2 \sum_{i,j=1}^{d} |\langle f, \varphi_{i,j}\rangle_{L^2(G)}|^2 = d \cdot d\mathrm{Tr}(\widehat{f}(\pi)^* \circ \widehat{f}(\pi)).$$

□

## IV.7 Characters and Fourier transforms

To finish this chapter, we relate characters and the Fourier transform, and give an explanation of the name “central function”.

**Proposition IV.7.1.** *Let $f \in L^2(G)$. Then, for every $x \in G$, we have*

$$\mathrm{Tr}(\widehat{f}(\pi) \circ \pi(x)) = f * \chi_\pi(x).$$

By theorem IV.6.3, this says that the orthogonal projection of $f$ in $\mathscr{E}_\pi$ is $\dim(\pi) f * \chi_\pi$, so we have
$$f = \sum_{\pi \in \widehat{G}} \dim(\pi) f * \chi_\pi$$
in $L^2(G)$.

*Proof.* We have
$$\begin{aligned} \operatorname{Tr}(\widehat{f}(\pi) \circ \pi(x)) &= \int_G f(y) \operatorname{Tr}(\pi(y)^{-1}\pi(x)) dy \\ &= \int_G f(y) \chi_\pi(y^{-1}x) \\ &= f * \chi_\pi(x). \end{aligned}$$

□

**Corollary IV.7.2.** *For all $\pi, \pi' \in \widehat{G}$, we have*
$$\chi_\pi * \chi_{\pi'} = \begin{cases} \dim(\pi)^{-1}\chi_\pi & \textit{if } \pi \simeq \pi' \\ 0 & \textit{otherwise.} \end{cases}$$

*Proof.* We know that $\chi_\pi \in \mathscr{E}_\pi$ for every $\pi \in \widehat{G}$, that $\mathscr{E}_\pi$ and $\mathscr{E}_{\pi'}$ are orthogonal for $\pi \not\simeq \pi'$, and the proposition says that $\dim(\pi)\chi_\pi * \chi_{\pi'}$ is the orthogonal projection of $\chi_\pi$ on $\mathscr{E}_{\pi'}$. This immediately implies the formula of the corollary.

□

**Definition IV.7.3.** For $1 \leq p < +\infty$, we denote by $ZL^p(G)$ the subspace of central functions in $L^p(G)$. We also denote by $Z\mathscr{C}(G)$ the subspace of central functions in $\mathscr{C}(G)$.

**Proposition IV.7.4.** *The space $L^p(G)$, $1 \leq p < +\infty$ (resp. $\mathscr{C}(G)$) is a Banach algebra for the convolution product, and $ZL^p(G)$ (resp. $Z\mathscr{C}(G)$) is its center.*

*Proof.* Let $p \in [1, +\infty)$, and let $q \in [1, +\infty)$ be such that $p^{-1} + q^{-1} = 1$. As $G$ is compact, the constant function 1 is in $L^q(G)$ and has $L^q$ norm equal to 1, so, by Hölder's inequality, $f = f \cdot 1$ is in $L^1(G)$, and $\|f\|_1 \leq \|f\|_p$. Now corollary I.4.3.2 says that, for every $g \in L^p(G)$, the function $f * g$ exists and is in $L^p(G)$, and that we have $\|f * g\|_p \leq \|f\|_1 \|g\|_p \leq \|f\|_p \|g\|_p$. This shows that $L^p(G)$ is a Banach algebra for $*$.

We show that $\mathscr{C}(G)$ is also a Banach algebra for $*$. If $f, g \in \mathscr{C}(G)$, then $f * g$ clearly exists, and, for every $x \in G$,
$$|f * g(x)| \leq \int_G |f(y)| g(y^{-1})| dy \leq \|f\|_\infty \|g\|_\infty \int_G 1 dy = \|f\|_\infty \|g\|_\infty.$$

So $\|f * g\|_\infty \leq \|f\|_\infty \|g\|_\infty$.

Finally, we show the statement about the centers. Let $f \in L^p(G)$, and suppose that $f*g = g*f$ for every $g \in L^p(G)$. Then, for every $x \in G$ and every $g \in L^p(G)$, we have

$$\int_G f(xy)g(y^{-1})dy = \int_G g(y)f(y^{-1}x)dy = \int_G f(yx)g(y^{-1})dy.$$

This holds if and only if $f(xy) = f(yx)$ almost everywhere on $G \times G$. The proof for $f \in \mathscr{C}(G)$ is the same.

□

**Corollary IV.7.5.** *The family $(\chi_\pi)_{\pi \in \widehat{G}}$ is an orthonormal basis of $ZL^2(G)$.*

*Proof.* We already know that the $\chi_\pi$ are in $ZL^2(G)$ and that they are pairwise orthogonal, so it just remains to show that a central function orthogonal to all the $\chi_\pi$ has to 0. Let $f \in ZL^2(G)$. By the lemma below, we have $(\dim \pi) f * \chi_\pi = \langle f, \chi_\pi \rangle_{L^2(G)} \chi_\pi$ for every $\pi \in \widehat{G}$, so, if $f$ is orthogonal to every $\chi_\pi$, then its projection on all the spaces $\mathscr{E}_\pi$ is 0 by proposition IV.7.1, hence $f = 0$ by theorem IV.4.2.

□

**Lemma IV.7.6.** *If $f \in ZL^1(G)$ and $\pi \in \widehat{G}$, then $(\dim \pi) f * \chi_\pi = \langle f, \chi_\pi \rangle_{L^2(G)} \chi_\pi$.*

*Proof.* We know that $f * \chi_\pi = \mathrm{Tr}(\widehat{f}(\pi) \circ \pi(.))$ by proposition IV.7.1. For every $x \in G$, we have

$$\begin{aligned}
\widehat{f}(\pi) \circ \pi(x) &= \int_G f(y)\pi(y^{-1}x)dy \\
&= \int_G f(xy^{-1})\pi(y)dy \\
&= \int_G f(y^{-1}x)\pi(y)dy \quad \text{(because } f \text{ is central)} \\
&= \int_G f(y)\pi(xy^{-1})dy \\
&= \pi(x) \circ \widehat{f}(\pi).
\end{aligned}$$

So $\widehat{f}(\pi) \in \mathrm{End}(\pi)$ is $G$-equivariant. By Schur's lemma, this implies that $\widehat{f}(\pi) = c\mathrm{id}$, with $c \in \mathbb{C}$. Taking the trace gives

$$c(\dim \pi) = \mathrm{Tr}(\widehat{f}(\pi)) = \int_G f(y)\mathrm{Tr}(\pi(y^{-1}))dy = \langle f, \chi_\pi \rangle_{L^2(G)}.$$

So

$$\langle f, \chi_\pi \rangle_{L^2(G)} \chi_\pi = (\dim \pi)\mathrm{Tr}(\widehat{f}(\pi) \circ \pi(.)) = (\dim \pi) f * \chi_\pi.$$

□

*Remark* IV.7.7. In fact, we can even show that the family $(\chi_\pi)_{\pi\in\widehat{G}}$ spans a dense subspace in $ZL^p(G)$ for every $p \in [1, +\infty)$ and in $Z\mathscr{C}(G)$. (See proposition 5.25 of [11].)

*Remark* IV.7.8. If $G$ is finite, then $L^2(G)$ is the space of all functions from $G$ to $\mathbb{C}$, and $ZL^2(G)$ is the space of functions that are constant on the conjugacy classes of $G$. So the proposition above says that $|\widehat{G}|$ is equal to the number of conjugacy classes in $G$, and the Peter-Weyl theorem says that $|G| = \sum_{\pi\in\widehat{G}}(\dim\pi)^2$.

*Remark* IV.7.9. We have shown in particular that the Banach algebras $(ZL^p(G), *)$ (for $1 \leq p < +\infty$) and $(Z\mathscr{C}(G), *)$ are commutative. We could ask what their spectrum is. In fact, the answer is very simple (see theorem 5.26 of [11]) : For every $\pi \in \widehat{G}$, the formula $f \longmapsto (\dim\pi)\int_G f\overline{\chi_\pi}d\mu$ defines a multiplicative functional on $ZL^p(G)$ (resp. $Z\mathscr{C}(G)$), and this induces a homeomorphism from the *discrete* set $\widehat{G}$ to the spectrum of $ZL^p(G)$ (resp. $Z\mathscr{C}(G)$).

## IV.8 The classical proof of the Peter-Weyl theorem

In section IV.4, we gave a proof of the Peter-Weyl theorem that uses the Gelfand-Raikov and Stone-Weierstrass theorems. We will now explain the original proof. We fix a compact group $G$. Remember that this implies that $L^2(G) \subset L^1(G)$.

By corollary I.4.3.2, if $f \in L^1(G)$ and $g \in L^2(G)$, then the integrals defining $f * g$ and $g * f$ converge and define functions of $L^2(G)$ such that $\|f*g\|_2 \leq \|f\|_1\|g\|_2$ and $\|g*f\|_2 \leq \|f\|_1\|g\|_2$.

**Definition IV.8.1.** If $f \in L^1(G)$, we define continuous linear endomorphisms $L_f$ and $R_f$ of $L^2(G)$ by $L_f(g) = f * g$ and $R_f(g) = g * f$.

In fact, by exercise I.5.6.4 (and its obvious analogue for right multiplication), these actions of $L^1(G)$ on $L^2(G)$ are just the extensions to the group algebra $L^1(G)$ of the left and right regular representations of $G$ on $L^2(G)$, as defined in theorem I.4.2.6. In particular, we have $\|L_f\|_{op} \leq \|f\|_1$ and $\|R_f\|_{op} \leq \|f\|_1$, which we also knew by corollary I.4.3.2.

In example I.4.2.2(b), we defined an involution $*$ on $L^1(G)$; as the modular function of $G$ is 1, this involution sends $f \in L^1(G)$ to the function $f^*$ defined by $f^*(x) = \overline{f(x^{-1})}$. By theorem I.4.2.6, we have $(L_f)^* = L_{f^*}$ and $(R_f)^* = R_{f^*}$, for every $f \in L^1(G)$.

**Theorem IV.8.2.** *For every $f \in L^1(G)$, the endomorphisms $R_f$ and $L_f$ of $L^2(G)$ are compact.*

*Remark* IV.8.3. We could also show that $L_f$ and $R_f$ are trace class operators (with trace $\int_G f(x)dx$) for $f \in L^1(G)$, and that they are Hilbert-Schmidt operators (with Hilbert-Schmidt norm $\|f\|_2$) for $f \in L^2(G)$, but we will not need this.

**Lemma IV.8.4.** *For every $F \in L^2(G \times G)$, the formula*

$$T_F(h)(x) = \int_G F(x,y)h(y)dy$$

*defines a continuous linear operator $T_F : L^2(G) \to L^2(G)$, and we have $\|T_F\| \leq \|F\|_2$.* [5]

*Proof.* Let $h \in L^2(G)$. By Minkowski's inequality and the Cauchy- Schwarz inequality, we have

$$\begin{aligned}\left(\int_G \left|\int_G F(x,y)h(y)dy\right|^2 dx\right)^{1/2} &\leq \int_G \left(\int_G |F(x,y)|^2|h(y)|^2 dx\right)^{1/2} dy \\ &\leq \int_G |h(y)| \left(\int_G |F(x,y)|^2 dx\right)^{1/2} dy \\ &\leq \|h\|_2 \left(\int_G \left(\int_G |F(x,y)|^2 dx\right)^{1/2\times 2} dy\right)^{1/2} = \|h\|_2\|F\|_2.\end{aligned}$$

This proves that $T_F(h)$ is well-defined, in $L^2(G)$, and that $\|T_F(h)\|_2 \leq \|h\|_2\|F\|_2$.

$\square$

**Lemma IV.8.5.** *If $f_1, f_2 : G \to \mathbb{C}$, define a function $u(f_1 \otimes f_2) : G \times G \to \mathbb{C}$ by $(f_1 \otimes f_2)(x_1, x_2) = f_1(x_1)f_2(x_2)$. This induces a $\mathbb{C}$-linear isometry $u : L^2(G) \otimes_{\mathbb{C}} L^2(G) \to L^2(G \times G)$, which is injective with dense image, hence gives an isometric isomorphism $L^2(G)\widehat{\otimes}_{\mathbb{C}} L^2(G) \xrightarrow{\sim} L^2(G \times G)$.*

After we prove this lemma, we will just identify $L^2(G)\widehat{\otimes}_{\mathbb{C}} L^2(G)$ and $L^2(G \times G)$ and write $f_1 \otimes f_2$ instead of $u(f_1 \otimes f_2)$.

*Proof.* The existence of the $\mathbb{C}$-linear map $u$ follows from the properties of the tensor product. If $f_1, f_2, g_1, g_2 \in L^2(G)$, then we have

$$\begin{aligned}\langle u(f_1 \otimes f_2), u(g_1 \otimes g_2)\rangle_{L^2(G\times G)} &= \int_{G\times G} u(f_1 \otimes f_2)(x_1,x_2)\overline{u(g_1 \otimes g_2)(x_1,x_2)}dx_1dx_2 \\ &= \int_{G\times G} f_1(x_1)f_2(x_2)\overline{g_1(x_1)g_2(x_2)}dx_1dx_2 \\ &= \langle f_1, g_1\rangle_{L^2(G)}\langle f_2, g_2\rangle_{L^2(G)}.\end{aligned}$$

This implies that $u$ is an isometry.

Take a Hilbert basis $(e_i)_{i\in I}$ of $L^2(G)$. Then the family $(u(e_i \otimes e_j))_{i,j\in I}$ of $L^2(G \times G)$ is orthonormal by the calculation, and its span is the image of $u$. So we just need to show that a function in $L^2(G \times G)$ that is orthogonal to every $u(e_i \otimes e_j)$ is 0. Let $F \in L^2(G \times G)$ be such a function. Let $i \in I$, and consider the function $f_i : G \to \mathbb{C}$ defined by $f_i(x) = \int_G F(x,y)e_i(y)dy$. Then $f_i \in L^2(G)$ by lemma IV.8.4, and $f_i$ is orthogonal to all the $e_j$ by the choice of $F$. As $(e_j)_{j\in I}$ is a Hilbert basis of $L^2(G)$, we must have $f_i = 0$. This is true for every $i \in I$, so, using again the

[5] In fact, we can prove that $T_F$ is a Hilbert-Schmidt operator and that its Hilbert-Schmidt norm is equal to $\|F\|_2$.

fact that $(e_i)_{i\in I}$ is a Hilbert basis of $L^2(G)$, we see that the function $F(x,.)$ is almost every zero for almost every $x$, i.e., that $F = 0$ in $L^2(G\times G)$.

□

**Lemma IV.8.6.** *For every $F \in L^2(G\times G)$, the operator $T_F : L^2(G) \to L^2(G)$ of lemma IV.8.4 is compact.*

*Proof.* By lemma IV.8.5, there exist families of functions $(g_i)_{i\in I}$ and $(h_i)_{i\in I}$ in $L^2(G)$ such that the sum $\sum_{i\in I} g_i \otimes h_i$ converges to $F$ in $L^2(G\times G)$.

For every finite subset $J$ of $I$, let $S_J = \sum_{i,j\in J} g_i \otimes h_j \in L^2(G\times G)$ and $T_J = T_{S_J}$. Then, for every $h \in L^2(G)$, for every $x \in G$,

$$(T_J h)(x) = \sum_{(i,j)\in J^2} \int_G h(y) g_i(x) h_j(y) dy = \sum_{i\in J} (\sum_{j\in J} \int_G h(y) h_j(y) dy) g_i(x).$$

In other words, for every $h \in L^2(G)$, $T_J h$ is in the finite-dimensional subspace of $L^2(G)$ spanned by the $g_i$, $i \in J$. Hence the operator $T_J$ has finite rank.

To show that $T_F$ is compact, it suffices by problem 6 of problem set 5 to show that it is the limit of the operators $T_J$ as $J$ becomes bigger. But this follows from lemma IV.8.4 and from the fact that $K$ is the limit of the $S_J$ in $L^2(G\times G)$.

□

*Proof of theorem IV.8.2.* We prove the result for $L_f$; the proof for $R_f$ is similar.

Suppose first that $f \in L^2(G)$. Consider the function $K : G\times G \to \mathbb{C}$, $(x,y) \longmapsto f(xy^{-1})$. Then $K \in L^2(G\times G)$, and $L_f = T_K$. So the result follows from lemma IV.8.6.

In general, the result follows from the fact that a limit of compact operators is compact (see exercise I.5.5.9(f)), that $L^2(G)$ is dense in $L^1(G)$, and that $f \longmapsto L_f$ (resp. $f \longmapsto R_f$) is a continuous map from $L^1(G)$ to $\mathrm{End}(L^2(G))$.

□

Remember that the subspace $\mathscr{E}$ of $\mathscr{C}(G)$ was defined in IV.4.1; this is the space of matrix coefficients of finite-dimensional representations of $G$.

**Proposition IV.8.7.** *Let $f \in L^2(G)$. Then the following conditions are equivalent :*

*(i)* $\mathrm{Span}\{L_x f,\ x \in G\}$ *is finite-dimensional;*

*(ii)* $\mathrm{Span}\{R_x f,\ x \in G\}$ *is finite-dimensional;*

*(iii)* $f \in \mathscr{E}$.

*Proof.* We first prove that (i) implies (ii) and (iii). If $f \in \mathscr{E}$, then $f$ is a finite sum $\sum_{\pi \in \widehat{G}} f_\pi$, with $f_\pi \in \mathscr{E}_\pi$. So it suffices to show that every element of $\mathscr{E}_\pi$ generates a finite-dimensional subspace of the left (resp. right) regular representation for $\pi \in \widehat{G}$; but this follows immediately from the fact that $\mathscr{E}_\pi$ is finite-dimensional and stable by the operators $L_x$ (resp. $R_x$), $x \in G$.

We now prove that (ii) implies (i). (The proof that (iii) implies (i) is similar.) So let $f \in L^2(G)$, and suppose that there exists a finite-dimensional subspace $V \ni f$ of $L^2(G)$ that is stable by all the $L_x$, $x \in G$. We will show that $f$ is a matrix coefficient of $V^*$. Let $\langle .,. \rangle_V$ be the restriction to $V$ of the inner product of $L^2(G)$, let $\rho : G \to \mathrm{GL}(V)$ be the action of $G$ on $V$, and let $\Pi : L^2(G) \to V$ be the orthogonal projection. Suppose that $\psi \in \mathscr{C}(G)$ has real values and is such that $\psi(x^{-1}) = \psi(x)$ for every $x \in G$. In particular, $\psi \in L^2(G)$, so, by proposition I.4.3.4, $f * \psi$ is continuous. For every $x \in G$, we have

$$\begin{aligned} f * \psi(x) &= L_{x^{-1}}(f * \psi)(1) \\ &= (L_{x^{-1}} f) * \psi(1) \quad \text{(by proposition I.4.1.3)} \\ &= \int_G (L_{x^{-1}} f)(y)\overline{\psi(y)}dy \quad \text{(because } \psi \text{ has real values and } \psi(y^{-1}) = \psi(y)) \\ &= \langle L_{x^{-1}} f, \psi \rangle_{L^2(G)} \\ &= \langle \rho(x^{-1})\Pi(f), \Pi(\psi) \rangle_V \quad \text{(because } L_{x^{-1}} f \in V) \\ &= \overline{\langle \rho(x)\Pi(\psi), \Pi(f) \rangle_V}. \end{aligned}$$

By proposition IV.3.2(iv), $f * \psi$ is a matrix coefficient of $V^*$, i.e. $f * \psi \in \mathscr{E}_{V^*}$. Now we choose an approximate identity $(\psi_U)_{U \in \mathscr{U}}$ (definition I.4.1.7, this exists by proposition I.4.1.8). By the calculation we just did, $f * \psi_U \in \mathscr{E}_{V^*}$ for every $U \in \mathscr{U}$. But, by corollary I.4.3.3, $f$ is the limit in $L^2(G)$ of the family $(f * \psi_U)_{U \in \mathscr{U}}$. As $\mathscr{E}_{V^*}$ is finite-dimensional (by proposition IV.3.2(ii)), it is a closed subspace of $L^2(G)$, so $f$ is also in $\mathscr{E}_{V^*}$.

□

We now explain how to prove theorem IV.4.2 (that is, the fact that $\mathscr{E}$ is dense in $\mathscr{C}(G)$) without using the Gelfand-Raikov theorem. It suffices to prove that $\mathscr{E}$ is dense in $L^2(G)$. Consider the left regular representation of $G$ on $L^2(G)$. By proposition IV.8.7, $\mathscr{E}$ contains every finite-dimensional representation of $L^2(G)$, and in fact it is the sum of all the finite-dimensional subrepresentations of $L^2(G)$. As $L^2(G)$ is a Hilbert space, to show that $\mathscr{E}$ is dense in $L^2(G)$, it suffice to show that $\mathscr{E}^\perp = \{0\}$. So let $f \in \mathscr{E}^\perp$. Choose an approximate identity $(\psi_U)_{U \in \mathscr{U}}$ (definition I.4.1.7, this exists by proposition I.4.1.8). If $U \in \mathscr{U}$, then $\psi_U^* = \psi_U$, so $R_{\psi_U}$ is self-adjoint, and it is a compact operator by theorem IV.8.2. So, by the spectral theorem for self-adjoint compact operators (theorem IV.1.3), $\mathrm{Ker}(R_{\psi_U})$ is the orthogonal of the closure of the sum $\bigoplus_{\lambda \in \mathbb{C}^\times} \mathrm{Ker}(R_{\psi_U} - \lambda \mathrm{id})$, and $\mathrm{Ker}(R_{\psi_U} - \lambda \mathrm{id})$ is finite-dimensional for every $\lambda \in \mathbb{C}^\times$. Also, $R_{\psi_U}$ commutes with the left action of $G$ by proposition I.4.1.3, so each space $\mathrm{Ker}(R_{\psi_U} - \lambda\mathrm{id})$ is a subrepresentation of $L^2(G)$. As $f$ is orthogonal to every finite-dimensional subrepresentation of $L^2(G)$ by assumption, this implies that $f \in \mathrm{Ker}(R_{\psi_U})$, i.e. that $f * \psi_U = 0$. But $f$ is the limit of $(f * \psi_U)_{U\in\mathscr{U}}$ in $L^2(G)$ by corollary I.4.3.3, so we conclude that $f = 0$.

## IV.9 Exercises

**Exercise IV.9.1.** Let $d$ be a positive integer.

(a). Let $T$ be the intersection of $\mathrm{U}(d)$ with the set of diagonal matrices. Show that

$$T = \left\{ \begin{pmatrix} z_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & z_d \end{pmatrix}, z_1, \dots, z_d \in S^1 \right\}.$$

(b). Show that every element of $\mathrm{U}(d)$ is conjugated in $\mathrm{U}(d)$ to an element of $T$.

(c). Show that every element of $\mathrm{SU}(d)$ is conjugated in $\mathrm{SU}(d)$ to an element of $T_0 := T \cap \mathrm{SU}(d)$.

(d). Show that a finite-dimensional representation $V$ of $\mathrm{SU}(d)$ is uniquely determined up to equivalence by $\chi_{V|T_0}$.

We now take $d = 2$. Remember the irreducible representations $V_n$ ($n \geq 0$) of $\mathrm{SU}(2)$ defined in problem I.5.5.1

(a). Calculate the restriction of $\chi_{V_n}$ to $T_0$.

(b). Let $(\rho, V)$ be a finite-dimensional representation of $\mathrm{SU}(2)$. Show that there exists $m \geq 1$ and nonnegative integers $a_0, \dots, a_m$ such that, for every $z \in S^1$, we have

$$\chi_V \left( \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix} \right) = a_0 + \sum_{i=1}^{m} a_i (z^i + z^{-i}).$$

(c). Show that there exist integers $c_n \in \mathbb{Z}$, $n \geq 0$, such that $c_n = 0$ for $n$ big enough and $\chi_V = \sum_{n\geq 0} c_n \chi_{V_n}$.

(d). Show that the integers $c_n$ of (f) are all nonnegative.

(e). If $V$ is irreducible, show that there exists $n \geq 0$ such that $V \simeq V_n$.

*Solution.*

(a). Let $x = \begin{pmatrix} z_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & z_d \end{pmatrix} \in M_d(\mathbb{C})$, with $z_1, \dots, z_d \in \mathbb{C}$. Then $x$ is in $T$ if and only if $xx^* = I_d$. As $x^* = \begin{pmatrix} \overline{z}_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & \overline{z}_d \end{pmatrix}$, this condition is equivalent to $|z_1| = \dots = |z_d| = 1$.

(b). Let $x \in \mathrm{U}(d)$. Then $x$ is normal, so, by the spectral theorem, it can be diagonalized in an orthonormal basis of $\mathbb{C}^n$. This means that there exists $y \in \mathrm{U}(d)$ such that $yxy^{-1}$ is diagonal, i.e., $yxy^{-1} \in$.

(c). Let $x \in \mathrm{SU}(d)$. By question (b), there exists $y \in \mathrm{U}(d)$ such that $yxy^{-1} \in T$. We have $\det(yxy^{-1}) = \det(x) = 1$, so $yxy^{-1}$ is actually in $T_0$. Let $c = \det(y) \in \mathbb{C}^\times$. We choose $c' \in \mathbb{C}$ such that $(c')^d = c$; as $|c| = 1$, we also have $|c'| = 1$. Then $y' := (c')^{-1}y$ has determinant 1, hence is in $\mathrm{SU}(d)$, and $y'x(y')^{-1} = yxy^{-1}$.

(d). Let $V, W$ be two finite-dimensional representations of $\mathrm{SU}(d)$, and suppose that $\chi_V = \chi_W$ on $T_0$. By question (c) and the fact that $\chi_V$ and $\chi_W$ are central functions, this implies that $\chi_V = \chi_W$ on all of $\mathrm{SU}(d)$. But then $V$ and $W$ are equivalent by corollary IV.5.10.

(e). Let $x = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \in T_0$. Note that $x_1x_2 = 1$, so $x_2 = x_1^{-1} = \overline{x}_1$. We calculate the action of $x$ on the basis $(t_1^k t_2^{n-k})_{0 \le k \le n}$ of $V_n$. For $0 \le k \le n$, we have

$$x \cdot t_1^l t_2^{n-k} = (x_1^{-1}t_1)^k (x_2^{-1}t_2)^{n-k} = x_1^{n-2k} t_1^k t_2^{n-k}.$$

So

$$\chi_{V_n}(x) = \sum_{k=0}^{n} x_1^{n-2k}.$$

(f). We embed $S^1$ in $\mathrm{SU}(1)$ by the continuous group morphism $z \longmapsto \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$. Note that this induces an isomorphism of topological groups $S^1 \xrightarrow{\sim} T_0$. Then $\rho_{|S^1}$ is a finite-dimensional representation of $S^1$, so it is a finite direct sum of irreducible representations. We know (from problem I.5.4.1) that every irreducible representation of $S^1$ is of the form $\rho_m : z \longmapsto z^m$ with $m \in \mathbb{Z}$, so there exist nonnegative integers $a_m$, $m \in \mathbb{Z}$, that are 0 for all but a finite number of $m$, and such that $\rho_{|S^1} \simeq \bigoplus_{m \in \mathbb{Z}} \rho_m^{a_m}$. In particular, for every $z \in S^1$,

$$\chi_V\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}\right) = \sum_{m \in \mathbb{Z}} a_m z^m.$$

Let $y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Then $y \in \mathrm{SU}(2)$ and, for every $z \in S^1$, we have $y \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} y^{-1} = \begin{pmatrix} z^{-1} & 0 \\ 0 & z \end{pmatrix}$. As $V$ is a representation of $\mathrm{SU}(2)$, the function $\chi_V$ is central on $\mathrm{SU}(2)$, and so $\chi_V\left(\begin{pmatrix} z & 0 \\ 0 & z^{-1}\end{pmatrix}\right) = \chi_V\left(\begin{pmatrix} z^{-1} & 0 \\ 0 & z\end{pmatrix}\right)$. This implies that $a_{-m} = a_m$ for every $m \in \mathbb{Z}$, so we get the desired statement.

(g). Let $M$ be the $\mathbb{Z}$-module of functions $\chi : S^1 \to \mathbb{Z}$ that can be written $\chi(z) = a_0 + \sum_{m\geq 1} a_m(z^m + z^{-m})$, with $a_0, a_1, \ldots \in \mathbb{Z}$ and $a_m = 0$ for $m$ big enough. By question (f), the restriction to $S^1$ of $\chi_V$ is in $M$.

A basis of $M$ over $\mathbb{Z}$ is formed by the function $(\chi_0 = 1, \chi_1 = z + z^{-1}, \chi_2 = z^2 + z_2^{-2}, \ldots)$. On the other hand, we have seen in question (e) that $\chi_{V_n} = \sum_{\substack{0\leq k\leq n \\ k=n \mod n}} \chi_k$. So the (infinite) matrix representing $(\chi_{V_n})_{n\geq 0}$ in the basis $(\chi_n)_{n\geq 0}$ is upper triangular with ones on the diagonal, which means that it can be inverted, i.e., that $(\chi_{V_n})_{n\geq 0}$ is also a basis of $M$ over $\mathbb{Z}$. (If you don't like that, it is also very easy from the formula expressing $\chi_{V_n}$ in the basis $(\chi_m)_{m\geq 0}$ to show by induction over $n$ that $(\chi_{V_0}, \ldots, \chi_{V_n})$ is linearly independent and spans the same $\mathbb{Z}$-submodule as $(\chi_0, \ldots, \chi_n)$.)

The conclusion of the question follows immediately from this.

(h). We know that the functions $\chi_{V_n}$ are pairwise orthogonal in $L^2(\mathrm{SU}(2))$ (by corollary IV.5.8). So, for every $n \geq 0$,

$$c_n = \langle \chi_V, \chi_{V_n}\rangle_{L^2(\mathrm{SU}(2))}.$$

By the same corollary, the right-hand side is also equal to $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathrm{SU}(2)}(V, V_n))$, which is a nonnegative integer.

(i). If $V$ is irreducible, then, by the last formula in the proof of (h) (and Schur's lemma), we have $c_n = 0$ unless $V \simeq V_n$. So, if there were no $n \geq 0$ such that $V \simeq V_n$, we would have $\chi_V = 0$, hence $V = 0$, which is impossible.

□

**Exercise IV.9.2.** Let $G$ be a compact group, and let $(\pi, V)$ be a faithful finite-dimensional continuous representation of $G$. (Remember that this means that $\pi : G \to \mathrm{GL}(V)$ is injective.) The goal of this problem is to show that, if $G$ is finite, then every irreducible representation of $G$ is a direct summand of a representation of the form $V^{\otimes n} \otimes (V^*)^{\otimes m}$ (for some $n, m \geq 1$), where the notation $V^{\otimes n}$ means $\underbrace{V \otimes \ldots \otimes V}_{n \text{ times}}$, and similarly for $(V^*)^{\otimes m}$.

(a). Let $\mathbb{1}$ be the trivial representation of $G$ on $\mathbb{C}$. Show that it suffices to show that every irreducible representation of $G$ is a direct summand of a representation of the form $(V \oplus V^* \oplus \mathbb{1})^{\otimes N}$, for some $N \geq 1$.

(b). Let $W$ be an irreducible representation of $G$. Show that $W$ is a direct summand of $(V \oplus V^* \oplus \mathbb{1})^{\otimes N}$ if and only if $\int_G (1 + 2\,\mathrm{Re}\,\chi_V(x))^N \overline{\chi_W(x)} dx \neq 0$.

From now on, we assume that $G$ is finite, we fix a finite-dimensional representation $W$ of $G$, and we write, for every $N \in \mathbb{Z}_{\geq 0}$,

$$S_N = \sum_{x \in G} (1 + 2\operatorname{Re}\chi_V(x))^N \overline{\chi_W(x)}.$$

Let $d = \dim V$.

(c). If $x \neq 1$, show that $(1 + 2\operatorname{Re}\chi_V(x))^N \overline{\chi_W(x)} = o((1+2d)^N)$ as $N \to +\infty$.

(d). If $W \neq 0$, show that $S_N \neq 0$ for $N$ big enough.

*Solution.*

(a). Let's show by induction on $N$ that, for every $N \in \mathbb{Z}_{\geq 1}$, we have a $G$-equivariant isomorphism

$$(\mathbb{1} \oplus V \oplus V^*)^{\otimes N} \simeq \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l}\right)^{\frac{N!}{k!l!m!}}.$$

This clearly implies the result of (a).

For $N = 1$, it follows from the fact that $\mathbb{1} \otimes W \simeq W$ for every representation $W$ of $G$. Suppose the result know for $N$, and let's prove it for $N+1$. We have

$$\begin{aligned}
(\mathbb{1} \oplus V \oplus V^*)^{\otimes N+1} &\simeq (\mathbb{1} \oplus V \oplus V^*)^{\otimes N} \otimes (\mathbb{1} \oplus V \oplus V^*) \\
&\simeq (\mathbb{1} \oplus V \oplus V^*) \otimes \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l}\right)^{\frac{N!}{k!l!m!}} \\
&\simeq \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l}\right)^{\frac{N!}{k!l!m!}} \oplus \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N}} \left(V^{\otimes k+1} \otimes (V^*)^{\otimes l}\right)^{\frac{N!}{k!l!m!}} \\
&\quad \oplus \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l+1}\right)^{\frac{N!}{k!l!m!}} \\
&\simeq \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N+1}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l}\right)^{\frac{N!}{k!l!(m-1)!} + \frac{N!}{(k-1)!l!m!} + \frac{N!}{k!(l-1)!m!}} \\
&\simeq \bigoplus_{\substack{k,l,m \geq 0 \\ k+l+m=N+1}} \left(V^{\otimes k} \otimes (V^*)^{\otimes l}\right)^{\frac{(N+1)!}{k!l!m!}}.
\end{aligned}$$

(b). By the semisimplicity of finite-dimensional representations of $G$ (corollary I.3.2.9) and Schur's lemma (theorem I.3.4.1), the representation $W$ is a direct summand of $(\mathbb{1} \oplus V \oplus V^*)^{\otimes N}$ if and only if $\operatorname{Hom}_G((\mathbb{1} \oplus V \oplus V^*)^{\otimes N}, W) \neq 0$. By corollary IV.5.8, this is the case if and only $\langle \chi_{(\mathbb{1} \oplus V \oplus V^*)^{\otimes N}}, \chi_W \rangle_{L^2(G)} \neq 0$. So the conclusion follows from the fact that $\chi_{(\mathbb{1} \oplus V \oplus V^*)^{\otimes N}} = (1 + \chi_V + \overline{\chi}_V)^N = (1 + 2\operatorname{Re}\chi_V)^N$, which is an immediate consequence of proposition IV.5.4.

(c). As $G$ is compact, the representation $(\pi, V)$ is unitarizable, so we can choose an isomorphism $V \simeq \mathbb{C}^d$ such that $\pi(G) \subset \mathrm{U}(d)$. Let $z_1, \ldots, z_d$ be the eigenvalues of $\pi(x)$. As $\pi$ is faithful, we have $\pi(x) \neq 1$, so at least one the $z_i$ is not equal to $1$ (we are using the fact that $\pi(x)$ is diagonalizable); so we may assume that $z_1 \neq 1$. As $|z_1| = 1$, this implies that $-1 \leq \operatorname{Re} z_1 < 1$, so $1-2d \leq 1+2\sum_{i=1}^d \operatorname{Re}(z_i) < 1+2d$, and $\left|1+2\sum_{i=1}^d \operatorname{Re} z_i\right| < 1+2d$. Finally, we get

$$|(1+2\operatorname{Re}\chi_V(x))^N \chi_W(x)| \leq (\dim W)\left|1+2\sum_{i=1}^d \operatorname{Re} z_i\right|^N = o((1+2d)^N).$$

(d). As $G$ is finite, question (c) implies that

$$\sum_{x \in G-\{1\}} (1+2\operatorname{Re}\chi_V(x))^N \chi_W(x) = o((1+2d)^N).$$

On the other hand, $(1+2\operatorname{Re}\chi_V(1))\chi_W(1) = (\dim W)(1+2d)^N$. So $S_n = (\dim W)(1+2d)^N + o((1+2d)^N)$, which implies that $S_n \neq 0$ for $N$ big enough.

□

**Exercise IV.9.3.** The goal of this problem is to generalize exercise IV.9.2 to an arbitrary compact group $G$, assuming something about the Haar measure. In the next problem, we give another approach to the same result using matrix coefficients.

Let $(\rho, V)$ be a faithful finite-dimensional continuous representation of $G$. We want to show that any irreducible representation of $G$ is a direct summand of some $V^{\otimes N} \otimes (V^*)^{\otimes M}$. We fix a normalized Haar measure $\mu$ on $G$.

(a). Show that there exists an isomorphism $V \simeq \mathbb{C}^n$ such that $\rho$ induces an isomorphism (of topological groups) between $G$ and a closed subgroup of $\mathrm{U}(n)$.

From now on, we assume that $G$ is a closed subgroup of $\mathrm{U}(n)$, that $V = \mathbb{C}^n$ and that $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ is the inclusion. Let $(\pi, W)$ be a continuous nonzero finite-dimensional representation of $G$. Define $f : \mathrm{U}(n) \to \mathbb{C}$ and $g : G \to \mathbb{C}$ by $f(x) = 1 + \operatorname{Tr}(x) + \overline{\operatorname{Tr}(x)}$ and $g(x) = \overline{\chi_W(x)}$.

As in exercise I.5.5.4, we define

$$L_0 = \{X \in M_n(\mathbb{C}) | \forall t \in \mathbb{R},\ e^{tX} \in \mathrm{U}(n)\}$$

and

$$L = \{X \in M_n(\mathbb{C}) | \forall t \in \mathbb{R},\ e^{tX} \in G\}.$$

Remember that we proved in problem I.5.5.4 that, if $\Omega$ is a small enough neighborhood of $0$ in $L$, then $\exp$ induces a homeomorphism between $\Omega$ and $\exp(\Omega)$, and $\exp(\Omega)$ is a neighborhood of $1$ in $G$. Choose an isomorphism $L_0 \simeq \mathbb{R}^m$, and let $dX$ be the Lebesgue measure on $L_0$ given by this isomorphism. We assume the following : (**) For $\Omega$ small enough, there exists $c \in \mathbb{R}_{>0}$ such that the inverse image by the homeomorphism $\exp : \Omega \xrightarrow{\sim} \exp(\Omega)$ of the Haar measure $\mu$ is of the form $h(X)dX$, where $h(X) = c + O(\|X\|)$ as $X \to 0$.

*Remark.* This is always true, but we don't have the tools to prove it. Indeed, a closed subgroup $G$ of $\mathrm{GL}_n(\mathbb{C})$ is a Lie group, so the Haar measure is given by a left-invariant differential form $\omega$ on $G$, that is, $\omega_g$ is the pullback of $\omega_1$ by left translation by $g$. This and some effort will give the desired asymptotic formula.

It would actually be much simpler to use the Weyl integration formula (see for example theorem 7.16 of [22]) to prove all the estimates in this exercise, since the function that we integrate are central functions. However, this requires some more theory (maximal tori in particular).

(a). Show that, for every $x \in \mathrm{U}(n)$, we have $f(x) = 1 + 2\sum_{i=1}^n \cos\theta_i$, where $e^{i\theta_1}, \dots, e^{i\theta_n}$ are the eigenvalues of $x$.

(b). If $\Omega$ is a neighborhood of $0$ in $L_0$, show that there exists $\delta > 0$ such that, for every $x \notin \exp(\Omega)$ and every $N \geq 1$, we have

$$|f(x)^N| \leq (1 + 2n - \delta)^N.$$

(c). If $\Omega$ is a neighborhood of $0$ in $L$ and $U = \exp(\Omega)$, show that there exists $\delta > 0$ and $C \in \mathbb{R}_{>0}$ such that, for every $N \geq 1$, we have

$$\left| \int_{G-U} f(x)^N g(x) d\mu(x) \right| \leq C(1 + 2n - \delta)^N.$$

(d). Show that

$$f(e^X) = (2n+1)e^{-K(X) + O(\|X\|^4)}$$

as $X \to 0$ in $L_0$, where $K(X) = \frac{1}{1+2n}\|X\|^2 = \frac{1}{1+2n}\mathrm{Tr}(X^*X)$.

(e). Show that, if $\Omega$ is a ball (of finite radius) centered at $0$ in $L$, there exists $D \in \mathbb{R}_{>0}$ such that

$$\int_\Omega e^{-NK(X)} g(e^X) dX \sim D \cdot N^{-\frac{1}{2}\dim L}$$

as $N \to +\infty$. (Hint : Show that we have $g(e^X) = \dim W + O(\|X\|)$ as $X \to 0$ in $L$.)

(f). Show that there exists a neighborhood $U$ of $1$ in $G$ and $E \in \mathbb{R}_{>0}$ such that

$$\int_U f(x)^N g(x) d\mu(x) \sim E \frac{(2n+1)^N}{N^{\frac{1}{2}\dim L}}$$

as $N \to +\infty$.

(g). Show that $\int_G f(x)^N g(x) d\mu(x) \neq 0$ if $N$ is big enough.

*Solution.*

(a). As $G$ is compact, the representation $(\rho, V)$ is unitarizable. This means that there exists an isomorphism $V \simeq \mathbb{C}^n$ such that $\rho(G) \subset \mathrm{U}(n)$. As the representation $(\rho, V)$ is faithful, the morphism $\rho$ is injective, so $\rho : G \to \mathrm{U}(n)$ is an injective and continuous map. As $G$ is compact, this map is a homeomorphism onto its image.

(b). Let $D$ be the diagonal matrix with diagonal entries $e^{i\theta_1}, \ldots, e^{i\theta_n}$. As $x$ commutes with $x^* = x^{-1}$, the spectral theorem implies that there exists $A \in \mathrm{U}(n)$ such that $D = AxA^{-1}$. As $f$ is clearly a central function on $\mathrm{U}(n)$ (and even on $\mathrm{GL}_n(\mathbb{C})$), we have $f(x) = f(D)$. But $f(e^D) = 1 + \sum_{j=1}^n \mathrm{Re}(e^{i\theta_j}) = 1 + 2\sum_{j=1}^n \cos(\theta_j)$.

(c). By question (b), we have, for every $x \in \mathrm{U}(n)$, $f(x) \in \mathbb{R}$ and $1 - 2n \leq f(x) \leq 1 + 2n$. Moreover, the equality $f(x) = 1 + 2n$ is possible only if all te eigenvalues of $x$ are equal to 1, which in turn implies that $x = 1$, because $x$ is diagonalizable.

By question I.5.5.4(f), we know that $\exp(\Omega)$ contains an open neighborhood $V$ of 1 in $\mathrm{U}(n)$. As $\mathrm{U}(n)$, the continuous function $f$ attains its supremum on $\mathrm{U}(n) - V$, and this supremum is $< 1 + 2n$ by the previous paragraph. So $\sup_{x \in \mathrm{U}(n) - \exp(\Omega)} |f(x)| < 1 + 2n$, and this implies the desired result.

(d). For every $x \in G$, we have $|g(x)| \leq \dim W$. So we can take $C = \mathrm{vol}(G - U)(\dim W)$ and apply question (c).

(e). Let $i\theta_1, \ldots, i\theta_n$ be the eigenvalues of $X$. As $X$ commutes with $X^* = -X$, there exists $A \in \mathrm{U}(n)$ such that $AXA^{-1} = D$, where $D$ is the diagonal matrix with diagonal entries $i\theta_1, \ldots, i\theta_n$. Then $Ae^XA^{-1} = e^D$ is the diagonal matrix with diagonal entries $e^{i\theta_1}, \ldots, e^{i\theta_n}$, so the eigenvalues of $e^X$ are $e^{i\theta_1}, \ldots, e^{i\theta_n}$, and $f(e^X) = 1 + 2\sum_{j=1}^n \cos(\theta_j) = 1 + 2n - \sum_{j=1}^n \theta_j^2 + O(\sum_{j=1}^n \theta_j^4)$.

We have $X = A^{-1}DA$, so $X^* = -X = -A^{-1}DA$, hence $X^*X = -A^{-1}D^2A$, and finally $\mathrm{Tr}(X^*X) = -\mathrm{Tr}(D^2) = \sum_{j=1}^n \theta_j^2$. So $f(e^X) = 1 + 2n - \sum_{j=1}^n \theta_j^2 + O(\|X\|^4)$. On the other hand,

$$(2n+1)e^{-K(X)+O(\|X\|^4)} = (2n+1)(1 - \tfrac{1}{2n+1}\|X\|^2 + O(\|X\|^4)) = 2n+1 - \sum_{j=1}^n \theta_j^2 + O(\|X\|^4).$$

(f). We first prove the hint. By question I.5.5.4(g), there exists a $\mathbb{R}$-linear map $u : L \to \mathrm{End}(W)$ such that, for every $X \in L$, we have $\pi(e^X) = e^{tu(X)}$. As $u$ is $\mathbb{R}$-linear, it is $C^\infty$, and so the map $U : L \to \mathbb{C}$, $X \longmapsto g(e^X) = \mathrm{Tr}(e^{u(X)})$ is also $C^\infty$. We also have $U(0) = \mathrm{Tr}(\mathrm{id}_W) = \dim W$. So we get $U(X) = \dim W + O(\|X\|)$.

Now we evaluate the integral. Doing the change of variable $Y = N^{1/2}X$ (and observing that $NK(X) = K(Y)$), we get

$$\int_\Omega e^{-NK(X)}U(X)dX = N^{-\frac{1}{2}\dim L}\int_{N^{1/2}\Omega} e^{-K(Y)}U(N^{-1/2}Y)dY.$$

It remains to show that $\int_{N^{1/2}\Omega} e^{-K(Y)}U(N^{-1/2}Y)dY$ converges to a positive real number as $N \to +\infty$. First note that, as $\int_L e^{-K(Y)}dY$ converges and as the function $g$ is bounded by $\dim W$, we have

$$\left|\int_{N^{1/2}\Omega - N^{1/4}\Omega} e^{-K(Y)}U(N^{-1/2}Y)dY\right| \le \left|\int_{L-N^{1/4}\Omega} e^{-K(Y)}U(N^{-1/2}Y)dY\right| \xrightarrow[N\to+\infty]{} 0.$$

On the other hand, using the fact that $U(N^{-1/2}Y) = \dim W + O(N^{-1/4})$ for $Y \in N^{1/4}\Omega$, we get

$$\begin{aligned}\lim_{N\to+\infty}\int_{N^{1/4}\Omega} e^{-K(Y)}U(N^{-1/2}Y)dY &= \lim_{N\to+\infty}(\dim W)\int_{N^{1/4}\Omega} e^{-K(Y)}dY \\ &= (\dim W)\int_L e^{-K(Y)}dY.\end{aligned}$$

As the function $Y \longmapsto e^{-K(Y)}$ takes positive real values on $L$, the last integral is positive and real.

(g). If there exists a neighborhood $\Omega$ of $0$ in $L$ such that $\exp$ is a diffeomorphism from $\Omega$ to $U$ (which we can always assume by making $U$ small enough), then

$$\int_U f(x)^N g(x)dx = (2n+1)^N \int_\Omega e^{-NK(X)+NO(\|X\|^4)}g(e^X)h(X)dX,$$

with $h(X) = c + O(\|X\|)$, $c \in \mathbb{R}_{>0}$. This is equal to

$$\frac{(2n+1)^N}{(\dim L)^{N/2}}\int_{N^{1/2}\Omega} e^{-K(Y)+O(N^{-1}\|Y\|^4)}U(N^{-1/2}Y)h(N^{-1/2}Y)dY.$$

We can prove as in question (f) that, if we choose $\Omega$ to be a ball centered at $0$ (which we can), then the integral converges to $c(\dim W)\int_L e^{-K(Y)}dY$ as $N \to +\infty$, which gives the conclusion.

(h). By questions (d) and (f), we can decompose $\int_G f(x)^N g(x)dx$ as a sum of two terms, one of which is equivalent to a positive multiple of $\frac{(2n+1)^N}{(\dim L)^{N/2}}$ and one of which is dominated by $(1+2n-\delta)^N$, for some $\delta > 0$. As $N$ tends to $+\infty$, the second term will become negligible with respect to the first, so the sum of the two terms cannot be $0$ for $N$ big enough.

□

**Exercise IV.9.4.** The goal of this exercise is also to generalize exercise IV.9.2 to a compact group $G$ admitting a faithful finite-dimensional representation $(\rho, V)$. As in the beginning of IV.9.3, we may assume that $G$ is a closed subgroup of $\mathrm{U}(N)$, that $V = \mathbb{C}^N$, and that $\rho : G \to U(N) \subset \mathrm{GL}_N(\mathbb{C})$ is the inclusion.

Remember that the algebra $\mathscr{E} \subset \mathscr{C}(G)$ of all matrix coefficients of $G$ was defined in IV.4.1. As in section IV.4, we see $\mathscr{C}(G)$ and $\mathscr{E}$ as representations of $G \times G$ by making $(x, y) \in G \times G$ act by $L_x \circ R_y$.

For $i, j \in \{1, \dots, N\}$, we denote by $e_{ij} : G \to \mathbb{C}$ the function sending $x \in G \subset \mathrm{GL}_N(\mathbb{C})$ to its $(i, j)$th entry.

(a). Let $\mathscr{E}'$ be the subalgebra of $\mathscr{E}$ generated by $1$ and by the function $e_{ij}$ and $\overline{e}_{ij}$, for $1 \leq i, j \leq N$. Show that $\mathscr{E}'$ is stable by the action of $G \times G$.

(b). Show that there exists a subset $A$ of $\widehat{G}$ such that $\mathscr{E}' = \bigoplus_{\pi \in A} \mathscr{E}_\pi$.

(c). Show that $\mathscr{E}' = \mathscr{E}$.

(d). Show that every irreducible representation of $G$ is a direct summand of a representation of the form $V^{\otimes n} \otimes (V^*)^{\otimes m}$ (for some $n, m \geq 1$).

*Solution.*

(a). Let $x \in G$, and write $x^{-1} = (a_{ij})_{1 \leq i,j \leq N}$. Then $L_x e_{ij} = \sum_{k=1}^N a_{ik} e_{kj}$ for all $i, j \in \{1, \dots, N\}$, so $L_x e_{ij} \in \mathscr{E}'$. The proof that $\mathscr{E}'$ is stable by the operators $R_y$ is similar.

(b). Remember that, by theorem IV.3.8, $\mathscr{E} = \bigoplus_{\pi \in \widehat{G}} \mathscr{E}_\pi$, and, if we write $\pi : G \to \mathrm{GL}(V_\pi)$, then $\mathscr{E}_\pi$ is isomorphic to $\mathrm{End}(V_\pi)$ as a representation of $G \times G$. We show that the $\mathscr{E}_\pi$ are irreducible and mutually non isomorphic as representation of $G \times G$. Let $\pi, \pi' \in \widehat{G}$. Then, for $(x, y) \in G \times G$, we have $\chi_{\mathscr{E}_\pi}(x, y) = \chi_\pi(y)\overline{\chi_\pi(x)}$ by proposition IV.5.4, and similarly for $\pi'$, so

$$\langle \chi_{\mathscr{E}_\pi}, \chi_{\mathscr{E}_{\pi'}} \rangle_{L^2(G \times G)} = \int_{G^4} \chi_\pi(x_1)\overline{\chi_\pi(x_2)}\chi_{\pi'}(x_3)\overline{\chi_{\pi'}(x_4)} dx_1 dx_2 dx_3 dx_4.$$

By Schur orthogonality for characters (corollary IV.5.8(ii)), this is $0$ if $\pi \not\simeq \pi'$, and by corollary IV.5.8(iii), this is $1$ if $\pi \simeq \pi'$. The irreducibility of $\mathscr{E}_\pi$ follows from this and corollary IV.5.8(iii), and the fact that $\mathscr{E}_\pi \not\simeq \mathscr{E}_{\pi'}$ if $\pi \not\simeq \pi'$ also follows.

For every $\pi \in \widehat{G}$, let $W_\pi$ be the image $W$ of $\mathscr{E}'$ by the orthogonal projection $L^2(\mathrm{G}) \to \mathscr{E}_\pi$. As $\mathscr{E}'$ is stable by the action of $G \times G$, so is $W_\pi$, hence $W$ is $\{0\}$ of $\mathscr{E}_\pi$ because $\mathscr{E}_\pi$ is an irreducible representation of $G \times G$. So, if $A = \{\pi \in \widehat{G} \mid W_\pi \neq \{0\}\}$, then $\mathscr{E}' = \bigoplus_{\pi \in A} \mathscr{E}_\pi$.

(c). The subalgebra $\mathscr{E}'$ of $\mathscr{E}$ is stable by complex conjugation, it clearly separates points on $G$ and it contains the constant function $1$, so it is dense in $\mathscr{C}(G)$ by the Stone-Weierstrass theorem. In particular, it is dense in $\mathscr{E}$. But, if $A \subset \widehat{G}$ is the subset of (b), we have $\mathscr{E} = \mathscr{E}' \bigoplus_{\pi \in \widehat{G} \setminus A} \mathscr{E}_\pi$, so the fact that $\mathscr{E}'$ is dense in $\mathscr{E}$ implies that $A = \widehat{G}$, i.e. that $\mathscr{E}' = \mathscr{E}$.

(d). Let $W$ be an irreducible representation of $G$, and suppose that it is not a direct summand of any representation of the form $V^{\otimes n} \otimes (V^*)^{\otimes m}$ (for $n, m \geq 1$). By IV.9.2(a), this implies that $W$ is not a direct summand of any $(\mathbb{1} \oplus V \oplus V^*)^{\otimes n}$, $n \geq 1$, i.e., by Schur orthogonality (theorem IV.3.8(i)), that $\chi_W$ is orthogonal to any matrix coefficient of a $(\mathbb{1} \oplus V \oplus V^*)^{\otimes n}$, for $n \geq 1$. But the space of matrix coefficients of $(\mathbb{1} \oplus V \oplus V^*)^{\otimes n}$ is exactly the subspace of $\mathscr{E}$ generated by the products of at most $n$ of the functions $e_{ij}$ and $\overline{e_{ij}}$, for $1 \leq i, j \leq N$, so the space generated by the matrix coefficients of all these representations is $\mathscr{E}'$, which we have just seen is equal to $\mathscr{E}$. It is not possible for $\chi_W$ to be orthogonal to every element of $\mathscr{E}'$, so we get the result.

$\square$

# V Gelfand pairs

In this chapter, $G$ will always be a locally compact group, and $K$ a compact subgroup of $G$. We fix a left Haar measure $\mu = \mu_G$ on $G$ and a normalized Haar measure $\mu_K$ on $K$.

## V.1 Invariant and bi-invariant functions

**Definition V.1.1.** A function $f$ on $G$ is called *left invariant* (resp. *right invariant*, resp. *bi-invariant*) by $K$ if, for every $x \in K$, we have $L_x f = f$ (resp. $R_x f = f$, resp. $L_x f = R_x f = f$).

If $\mathscr{F}(G)$ is a space of functions on $G$ (for example $\mathscr{C}_c(G)$), we denote by $\mathscr{F}(K \backslash G)$ (resp. $\mathscr{F}(G/K)$, resp. $\mathscr{F}(K \backslash G/K)$) its subspace of left invariant (resp. right invariant, resp. bi-invariant) functions.

Let $\Delta_G$ be the modular function of $G$. As $K$ is compact, we have $\Delta_{G|K} = 1$, so we can use the results of exercise I.5.3.5. In particular :

**Proposition V.1.2.** *Let $f \in \mathscr{C}(G)$, and define two functions $f^K : G \to \mathbb{C}$ and ${}^K f : G \to \mathbb{C}$ by setting*

$$f^K(x) = \int_K f(xk)dk$$

*and*

$${}^K f(x) = \int_K f(kx)dk.$$

*Then $f^K$ is right invariant and ${}^K f$ is left invariant.*

**Proposition V.1.3.** *There exists a unique regular Borel measure $\mu_{G/K}$ (resp. $\mu_{K\backslash G}$) on $G/K$ (resp. $K \backslash G$) such that, for every $f \in \mathscr{C}_c(G)$, we have*

$$\int_G f(x)dx = \int_{G/K} f^K(x)d\mu_{G/K}(x)$$

$$(\textit{resp.} \quad \int_G f(x)dx = \int_{K\backslash G} {}^K f(x)d\mu_{K\backslash G}(x)).$$

**Definition V.1.4.** If $f$ is a continuous function on $G$, we write

$$^K f^K = {}^K(f^K) = ({}^K f)^K.$$

In other words, this is the continuous function on $G$ defined by :

$$^K f^K(x) = \int_{K\times K} f(kxk')dkdk'.$$

Note that $^K f^K$ is obviously a bi-invariant function.

**Proposition V.1.5.** *Let $f \in \mathscr{C}(G)$. Then $f$ is left invariant (resp. right invariant, resp. bi-invariant) if and only if $f = {}^K f$ (resp. $f = f^K$, resp. $f = {}^K f^K$).*

*Proof.* This follows immediately from proposition V.1.2 and from the fact that the measure on $K$ is normalized.

□

**Lemma V.1.6.** *For every $f \in \mathscr{C}_c(G)$, we have*

$$\int_G f(x)dx = \int_G {}^K f^K(x)dx.$$

*Proof.* We have

$$\int_G {}^K f^K(x)dx = \int_{G\times K^2} f(kxk')dxdkdk' = \int_G f(x)dx,$$

because, for all $k, k' \in K$,

$$\int_G f(kxk')dx = \Delta(k')^{-1}\int_G f(x)dx = \int_G f(x)dx$$

(by proposition I.2.8).

□

**Proposition V.1.7.** *Let $(\pi, V)$ be a unitary representation of $G$, and let $P_K : V \to V$ be the orthogonal projection on $V^K$. Then we have, for every $v \in V$,*

$$P_K(v) = \int_K \pi(k)(v)dk.$$

*Moreover, if $f \in \mathscr{C}_c(G)$ and $v \in V$, then $\pi(f)(P_K(v)) = \pi(f^K)(v)$ and $P_K(\pi(f)(v)) = \pi({}^K f)(v)$. In particular :*

*(i) If $f \in \mathscr{C}_c(G)$ and $v \in V^K$, we have $\pi(f)(v) = \pi(f^K)(v)$.*

*(ii) If $f \in \mathscr{C}_c(K\backslash G)$ and $v \in V$, then $\pi(f)(v) \in V^K$.*

*(Remember that $\pi : L^1(G) \to \mathrm{End}(V)$ is defined in theorem I.4.2.6.)*

*Proof.* Let $v \in V$. The existence of the integral $w := \int_K \pi(k)(v)dk$ follows from exercise I.5.6.2. If $x \in K$, then we have

$$\pi(x)(w) = \int_K \pi(xk)(v)dk = \int_K \pi(k)(v)dk = w,$$

so $w \in V^K$. Also, if $w' \in V^K$, then

$$\langle w, w'\rangle = \int_K \langle \pi(k)(v), w'\rangle dk = \int_K \langle v, \pi(k^{-1})(w')\rangle dk = \int_K \langle v, w'\rangle dk = \langle v, w'\rangle.$$

So $w$ is the orthogonal projection of $v$ on $V^K$.

Now we prove the last statement. Let $f \in \mathscr{C}_c(G)$ and $v \in V$. Then :

$$\begin{aligned}
\pi(f^K)(v) = \int_G f^K(x)\pi(x)(v)dx &= \int_G \int_K f(xk)\pi(x)(v)dxdk \\
&= \int_G \int_K f(x)\pi(x)\pi(k)^{-1}(v)dxdk \\
&= \int_G \int_K f(x)\pi(x)\pi(k)(v)dxdk \quad (K \text{ is unimodular}) \\
&= \pi(f)(P_K(v)).
\end{aligned}$$

On the other hand :

$$\begin{aligned}
P_K(\pi(f)(v)) &= \int_K \int_G f(x)\pi(kx)(v)dkdx \\
&= \int_K \int_G f(k^{-1}x)\pi(x)(v)dkdx \\
&= \int_K \int_G f(kx)\pi(x)(v)dkdx \\
&= \pi({}^K f)(v).
\end{aligned}$$

□

The same proof gives :

**Proposition V.1.8.** *Let $f, g \in \mathscr{C}_c(G)$. Then*

$${}^K(f * g) = ({}^K f) * g \quad \textit{and} \quad (f * g)^K = f * (g^K).$$

*In particular, if $f$ and $g$ are bi-invariant, then $f * g$ is also bi-invariant, so $\mathscr{C}_c(K\backslash G/K)$ is a subalgebra of $\mathscr{C}_c(G)$ for the convolution product.*

*Remark* V.1.9. Let $L^p(K\backslash G/K)$ be the subspace of bi-invariant functions in $L^p(G)$. Then, if $1 \leq p < +\infty$, if $f \in L^1(K\backslash G/K)$ and $g \in L^p(K\backslash G/K)$, then their convolution product $f * g$ is in $L^p(K\backslash G/K)$. This is clear on the formulas defining $f * g$ (see proposition I.4.1.3); indeed, we have

$$f * g(x) = \int_G f(y)g(y^{-1}x)dx = \int_G f(xy^{-1})g(y)dy$$

(the first formula shows that $f * g$ is right invariant, and the second that $f * g$ is left invariant).

In particular, the subspace $L^1(K\backslash G/K)$ of $L^1(G)$ is a subalgebra, and we have a similar result for the $L^2$ spaces if $G$ is compact.

*Remark* V.1.10. All this is easier to remember if we extend the convolution product and the representation $\pi$ to the space $\mathscr{M}(G)$ of Radon measures on $G$. (See remark I.4.1.6.) We can see $\mu_K$ as an element of $\mathscr{M}(G)$ by identifying it to the Radon measure $\mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_K f(x)d\mu_K(x)$. Then we have $\mu_K * \mu_K = \mu_K$, $f^K = f * \mu_K$, ${}^K f = \mu_K * f$ and $P_K = \pi(\mu_K)$, so, for example, the last part of proposition V.1.7 just follows from the fact that $\pi$ is a $*$-homomorphism.

## V.2 Definition of a Gelfand pair

**Definition V.2.1.** We say that $(G, K)$ is a *Gelfand pair* if the algebra $\mathscr{C}_c(K\backslash G/K)$ is commutative for the convolution product.

*Remark* V.2.2. If $p \in [1, +\infty)$, $f \in L^p(K\backslash G/K)$ and $g \in \mathscr{C}_c(G)$, then

$$\begin{aligned}\|f - {}^K g^K\|_p^p &= \int_G \left| f(x) - \int_{K\times K} g(kxk')dkdk' \right|^p dx \\ &= \int_G \left| \int_{K\times K} (f(kxk') - g(kxk'))dkdk' \right|^p dx.\end{aligned}$$

So, by Minkowski's formula (see exercise **??**), we have

$$\|f - {}^K g^K\|_p \leq \int_{K\times K} \|L_k R_{k'} f - L_k R_{k'} f\|_p dkdk' = \|f - g\|_p.$$

As $\mathscr{C}_c(G)$ is dense in $L^p(G)$, every function of $L^p(K\backslash G/K)$ can be approximated by elements of $\mathscr{C}_c(G)$, hence, by the calculation above, by elements of $\mathscr{C}_c(K\backslash G/K)$. In other words, the space $\mathscr{C}_c(K\backslash G/K)$ is dense in $L^p(K\backslash G/K)$. So, in the definition of a Gelfand pair, we could have replaced the condition "$\mathscr{C}_c(K\backslash G/K)$ is commutative for the convolution product" by the condition "$L^1(K\backslash G/K)$ is commutative for the convolution product" (or, for $G$, we could have used "$L^2(K\backslash G/K)$ is commutative for the convolution product").

**Example V.2.3.** If $G$ is abelian, then $(G, \{1\})$ is a Gelfand pair.

Here are other examples (but we will not prove yet that they are Gelfand pairs) :

- $(\mathrm{SO}(n+1), \mathrm{SO}(n))$, where $\mathrm{SO}(n)$ is identified to a subgroup of $\mathrm{SO}(n+1)$ by sending $x \in \mathrm{SO}(n)$ to the $(n+1)\times(n+1)$ matrix $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$;
- $(\mathfrak{S}_{n+m}, \mathfrak{S}_n \times \mathfrak{S}_m)$;
- $(\mathrm{GL}_n(\mathbb{Q}_p), \mathrm{GL}_n(\mathbb{Z}_p))$.

**Proposition V.2.4.** *Let $(G, K)$ be a Gelfand pair. Then $G$ is unimodular.*

*Proof.* By proposition I.2.12, we have, for every $f \in \mathscr{C}_c(G)$,

$$\int_G f(x)dx = \int_G \Delta(x)^{-1} f(x^{-1})dx.$$

So it suffices to prove that $\int_G f(x)dx = \int_G f(x^{-1})dx$ for every $f \in \mathscr{C}_c(G)$. First note that

$$\int_G {}^K f^K(x)dx = \int_G f(x)dx$$

and

$$\int_G {}^K f^K(x^{-1})dx = \int_G f(x^{-1})dx,$$

by lemma V.1.6. So it suffices to show that $\int_G f(x)dx = \int_G f(x^{-1})dx$ for every $f \in \mathscr{C}_c(K\backslash G/K)$. Fix $f \in \mathscr{C}_c(K\backslash G/K)$. We can find $g \in \mathscr{C}_c(K\backslash G/K)$ such that $g$ is equal to $1$ on $(\operatorname{supp} f) \cup (\operatorname{supp} f)^{-1}$ (because $\operatorname{supp} f = K(\operatorname{supp} f)K$). Then

$$f * g(1) = \int_G f(y)g(y^{-1})dy = \int_{\operatorname{supp} f} f(y)dy = \int_G f(y)dy$$

and

$$g * f(1) = \int_G g(y)f(y^{-1})dy = \int_{(\operatorname{supp} f)^{-1}} f(y^{-1})dy = \int_G f(y^{-1})dy.$$

But $f * g = g * f$ because $(G, K)$ is a Gelfand pair, so this implies the desired result.

□

The following criterion will allow us to find more Gelfand pairs.

**Proposition V.2.5.** *Suppose that there exists a continuous automorphism $\theta : G \to G$ such that :*

*(a) $\theta^2 = \mathrm{id}_G$ (i.e. $\theta$ is an involution);*

*(b) for every $x \in G$, we have $\theta(x) \in Kx^{-1}K$.*

*Then $(G, K)$ is Gelfand pair.*

*Proof.* Consider the linear functional $\mathscr{C}_c(G) \to \mathbb{C}$, $f \longmapsto \int_G f(\theta(x))dx$. This is a left-invariant positive linear functional on $\mathscr{C}_c(G)$, so, by the uniqueness statement in theorem I.2.7, there exists $c \in \mathbb{R}_{>0}$ such that, for every $f \in \mathscr{C}_c(G)$, we have

$$\int_G f(\theta(x))dx = c \int_G f(x)dx.$$

As $\theta^2 = \mathrm{id}_G$, we must have $c^2 = 1$, so $c = 1$.

Let $f, g \in \mathscr{C}_c(G)$. On the one hand, we have, for every $x \in G$,

$$\begin{aligned}(f \circ \theta) * (g \circ \theta)(x) &= \int_G f(\theta(y))g(\theta(y)^{-1}\theta(x))dy \\ &= \int_G f(y)g(y^{-1}\theta(x))dy \\ &= (f * g) \circ \theta(x)\end{aligned}$$

(the second equality follows from the first paragraph of this proof). On the other hand, for every $x \in G$, we have

$$(g * f)(x^{-1}) = \int_G g(x^{-1}y)f(y)dy = \int_G f'(y^{-1})g'(yx)dy = (f' * g')(x),$$

where $f'(z) = f(z^{-1})$ and $g'(z) = g(z^{-1})$. (We used the fact that $G$ is unimodular to do the change of variables $y \longmapsto y^{-1}$.)

Suppose that $f$ and $g$ are bi-invariant. Then we have $f(\theta(x)) = f(x^{-1})$ and $g(\theta(x)) = g(x^{-1})$ by condition (b), and a similar equality for $g * f$ because $g * f$ is also bi-invariant, so, for every $x \in G$,

$$(f * g)(\theta(x)) = ((f \circ \theta) * (g \circ \theta))(x) = (f' * g')(x) = (g * f)(x^{-1}) = (g * f)(\theta(x)).$$

As $\theta$ is an automorphism, this implies that $f * g = g * f$.

□

**Example V.2.6.** (1) If $G$ is abelian, then we can take $\theta : x \longmapsto x^{-1}$, so $(G, K)$ is a Gelfand pair for any compact subgroup $K$, and in particular for $K = \{1\}$.

(2) If $G$ is compact, then $(G \times G, \{(x, x),\ x \in G\})$ is a Gelfand pair. Indeed, it suffices to apply the proposition above with $\theta(x, y) = (y, x)$. Indeed, for every $(x, y) \in G \times G$, we have $\theta(x, y) = (x, x)(x^{-1}, y^{-1})(y, y)$.

## V.3 Gelfand pairs and representations

In this section, we will give two representation-theoretic criteria for $(G, K)$ to be a Gelfand pair, one valid in general and one for $G$ compact.

## V.3.1 Gelfand pairs and vectors fixed by $K$

**Theorem V.3.1.1.** *The couple $(G, K)$ is a Gelfand pair if and only if, for every irreducible unitary representation $(\pi, V)$ of G, we have $\dim(V^K) \leq 1$.*

We will need the following variant of the Gelfand-Raikov theorem.

**Lemma V.3.1.2.** *Let $f \in \mathscr{C}_c(G)$. If $f \neq 0$, then there exists $\varphi \in \mathscr{E}(\mathscr{P}_1)$ (see section III.3) such that $\int_G f(x)\varphi(x)dx \neq 0$.*

*Proof.* Suppose that $\int_G f\varphi d\mu = 0$ for every $\varphi \in \mathscr{E}(\mathscr{P}_1)$. By theorem III.4.1, we have $\int_G f\varphi d\mu = 0$ for every function of positive type $\varphi$. By theorem III.2.5, for every unitary representation $(\pi, V)$ of $G$ and any $v \in V$, we have $\langle \pi(f)(v), v\rangle = 0$. Applying this to the left regular representation of $G$, we get that, for every $g \in L^2(G)$, we have $\langle f * g, g\rangle_{L^2(G)} = 0$. As in the proof of theorem III.5.1, we see that this implies that $\langle f * g_1, g_2\rangle_{L^2(G)} = 0$ for all $g_1, g_2 \in L^2(G)$. Again as in the proof of that theorem, we see that, for all $g_1, g_2 \in L^2(G)$, we have $\langle f * g_1, g_2\rangle_{L^2(G)} = \langle f, g_2 * \widetilde{g}_1\rangle_{L^2(G)}$, where $\widetilde{g}_1(x) = \overline{g_1(x^{-1})}$. So we get $\langle f, g_1 * g_2\rangle_{L^2(G)} = 0$ for all $g_1, g_2 \in L^2(G)$. Applying this to $g_1 = f$ and to $g_2 = \psi_U$, where $(\psi_U)_{U\in\mathscr{U}}$ is an approximate identity, we finally get $\langle f, f\rangle_{L^2(G)} = 0$, hence $f = 0$.

□

We also need the following variant of Schur's lemma.

**Lemma V.3.1.3.** *Let $A$ be a commutative Banach $*$-algebra, and let $u : A \to \mathrm{End}(V)$ be a representation of $A$ on a nonzero Hilbert space $V$. Suppose that the only closed subspaces of $V$ that are fixed by all the $u(x)$, $x \in A$ are $\{0\}$ and $V$. Then $\dim V = 1$.*

*Proof.* By assumption, the subset $u(A)$ satisfies the hypothesis of corollary II.4.4, so its centralizer in $\mathrm{End}(V)$ is equal to $\mathbb{C}\mathrm{id}_V$. But as $A$ is commutative, even element of $u(A)$ is in the centralizer in $u(A)$, so this implies that $\mathrm{Im}(u) \subset \mathbb{C}\mathrm{id}_V$. In particular, every subspace of $V$ is invariant by all the elements of $u(A)$, so $V$ has no nontrivial closed subspaces, which is only possible if $\dim V \leq 1$.

□

**Lemma V.3.1.4.** *Let $(\pi, V)$ be a unitary representation of G. Then $\pi(f)$ sends $V^K$ to itself for every $f \in L^1(K\backslash G/K)$. If moreover $\pi$ is irreducible, then the only closed subspaces of $V^K$ stable by all the $\pi(f)$, $f \in L^1(K\backslash G/K)$, are $\{0\}$ and $V^K$.*

*Proof.* By proposition V.1.7, for every $f \in \mathscr{C}_c(K \backslash G/K)$ and every $v \in V^K$, we have $\pi(f)(v) \in V^K$. The first statement follows from the fact that $\mathscr{C}_c(K \backslash G/K)$ is dense in $L^1(K\backslash G/K)$.

To prove the second statement, it suffices to show that, for every $v \in V^K - \{0\}$, the space $\{\pi(f)(v),\ f \in \mathscr{C}_c(K\backslash G/K)\}$ is dense in $V^K$. Let $w \in V^K$, and let $\varepsilon > 0$. As $V$ is irreducible, the space $\{\pi(f)(v),\ f \in L^1(G)\}$ is dense in $V$. As $\mathscr{C}_c(G)$ is dense in $L^1(G)$, there exists $f \in \mathscr{C}_c(G)$ such that $\|\pi(f)(v) - w\| \leq \varepsilon$. By proposition V.1.7 again, we have $\pi(f)(v) = \pi(f^K)(v)$, and so $\pi({}^K f^K)(v) = P_K(\pi(f)(v))$, where $P_K$ is the orthogonal projection of $V$ on $V^K$. As $w \in V^K$, we get $\|\pi({}^K f^K)(v) - w\| = \|P_k(\pi(f)(v)) - w\| \leq \|\pi(f)(v) - w\| \leq \varepsilon$.

$\square$

*Proof of theorem V.3.1.1.* Suppose that $(G, K)$ is a Gelfand pair. Let $(\pi, V)$ be an irreducible unitary representation of $G$. By lemma V.3.1.4, $\pi$ defines a $*$-homomorphism from $L^1(K\backslash G/K)$ to $\mathrm{End}(V^K)$, and the only closed subspaces of $V^K$ stable by all the elements of $L^1(K\backslash G/K)$ are $\{0\}$ and $V^K$. As $L^1(K\backslash G/K)$ is commutative, lemma V.3.1.3 implies that $\dim(V^K) \leq 1$.

We prove the converse. Suppose that $\dim(V^K) \leq 1$ for every irreducible unitary representation $(\pi, V)$ of $G$. Let $f \in \mathscr{C}_c(K\backslash G/K)$ be nonzero. By lemma V.3.1.2, there exists $\varphi \in \mathscr{E}(\mathscr{P}_1)$ such that $\int_G f\varphi d\mu \neq 0$. Let $(\pi, V)$ be a cyclic unitary representation of $G$ and $v \in V$ be a cyclic vector such that $\varphi(x) = \langle \pi(x)(v), v\rangle$ for every $x \in G$ (see theorem III.2.5). Then we have

$$\int_G f(x)\varphi(x)dx = \int_G f(x)\langle \pi(x)(v), v\rangle dx = \langle \pi(f)(v), v\rangle,$$

so $\pi(f)(v) \neq 0$. By theorem III.3.2, the representation $(\pi, V)$ is irreducible. By lemma V.3.1.4, the endomorphism $\pi(f)$ of $V$ preserves $V^K$ and, by proposition V.1.7, if $w$ is the orthogonal projection of $v$ on $V^K$, then $\pi(f)(w) = \pi(f)(v) \neq 0$. In particular, the subspace $V^K$ of $V$ is nonzero, so $\dim(V^K) = 1$ by assumption. Hence $\mathrm{End}(V^K) = \mathbb{C}$, which means that we have found a $*$-homomorphism $u : \mathscr{C}_c(K\backslash G/K) \to \mathbb{C}$ (sending $g$ to $\pi(g)_{|V^k}$) such that $u(f) \neq 0$.

Now let $f_1, f_2 \in \mathscr{C}_c(K \setminus G/K)$. As $\mathbb{C}$ is commutative, we have $u(f_1 * f_2 - f_2 * f_1) = u(f_1)u(f_2) - u(f_2)u(f_1) = 0$ for every morphism of algebras $u : \mathscr{C}_c(K\backslash G/K) \to \mathbb{C}$. By the preceding paragraph, this implies that $f_1 * f_2 - f_2 * f_1 = 0$, and we are done.

$\square$

## V.3.2 Gelfand pairs and multiplicity-free representations

**Definition V.3.2.1.** Let $(\pi, V)$ be a unitary representation of $G$, and suppose that we can write $V = \overline{\bigoplus_{i\in I} V_i}$, with the $V_i$ closed $G$-invariant subspaces of $V$ that are irreducible as representations of $V$.[1] Then we say that $(\pi, V)$ is *multiplicity-free* if, for every irreducible unitary representation $W$ of $G$, the set of $i \in I$ such that $V_i$ and $W$ are equivalent has cardinality $\leq 1$.

Note that the group $G$ acts by left translations on the homogenous space $G/K$, so, if $x \in G$ and $f$ is a function on $G/K$, we can define $L_x f$ by $L_x f(y) = f(x^{-1}y)$.

[1] This is always the case if $G$ is compact, see theorem IV.2.1.

**Definition V.3.2.2.** The *quasiregular representation* of $G$ on $L^2(G/K)$ is the representation defined by $x \cdot f = L_x f$, for every $x \in G$ and every $f \in L^2(G/K)$.

**Proposition V.3.2.3.** *The definition above makes sense, and gives a unitary representation of $G$.*

*Proof.* By definition of the measure on $G/K$, we have $\int_{G/K} f d\mu_{G/K} = \int_{G/K} L_x f d\mu_{G/K}$ for every $f \in \mathscr{C}_c(G/K)$ and every $x \in G$. As $\mathscr{C}_c(G/K)$ is dense in $L^2(G/K)$, this implies that the operators $L_x$ preserve $L^2(G/K)$ and are isometries. By proposition I.3.1.10, it suffices to prove that, for every $f \in L^2(G/K)$, the map $G \to L^2(G/K)$, $x \longmapsto L_x f$ is continuous. As in the proof of proposition I.3.1.13, it suffices to prove this for $f \in \mathscr{C}_c(G/K)$, in which case it follows from proposition I.1.12.

□

*Remark* V.3.1. If we make $G$ act on $L^2(G)$ by the right regular representation, then $L^2(G/K)$ is the space of $K$-invariant vectors in $L^2(G)$. The quasi-regular regular representation is then the restriction of the left regular representation to $L^2(G/K)$

We could also define a quasiregular representation on $L^2(K \setminus G)$ (this is the space of $K$-invariant vectors in $L^2(G)$ if $K$ acts via the left regular representation, and it gets an action of $G$ via the right regular representation). The representation we get is unitarily equivalent to the quasiregular representation on $L^2(G/K)$.

**Theorem V.3.2.4.** *Assume that $G$ is compact. Then $(G, K)$ is a Gelfand pair if and only if the quasiregular representation of $G$ on $L^2(G/K)$ is multiplicity-free.*

*Also, if $(G, K)$ is a Gelfand pair, then we have a $G$-equivariant isomorphism*

$$L^2(G/K) \simeq \widehat{\bigoplus_{\substack{(\pi,V)\in\widehat{G} \\ V^K\neq 0}} V}.$$

*Proof.* First observe that $L^2(G/K)$ is the space of vectors of $L^2(G)$ that are $K$-invariant if $K$ acts by the right regular representation. The Peter-Weyl theorem (corollary IV.4.3) says that, as a representation of $G \times G$, the space $L^2(G)$ is isomorphic to the completion of $\bigoplus_{(\pi,V)\in\widehat{G}} \operatorname{End}(V) = \bigoplus_{(\pi,V)\in\widehat{G}} V^* \otimes_{\mathbb{C}} V$. So $L^2(G/K)$ is isomorphic as a representation of $G$ to the completion of

$$\bigoplus_{\substack{(\pi,V)\in\widehat{G} \\ V^K\neq 0}} (V^*)^{\dim(V^K)}.$$

Note that, for every $(\pi, V) \in \widehat{G}$, the representation $V^*$ is also irreducible; this follows for example from (iii) of corollary IV.5.8, because $\chi_{V^*} = \overline{\chi}_V$, so $\|\chi_{V^*}\|_2 = \|\chi_V\|_2$. So the representation $L^2(G/K)$ is multiplicity-free if and only if, for every irreducible unitary representation $(\pi, V)$ of $G$, we have either $V^K = 0$ or $\dim(V^K) = 1$. Hence the first statement of the theorem follows from theorem V.3.1.1.

We now prove the second statement. We have already seen that

$$L^2(G/K) \simeq \widehat{\bigoplus_{\substack{(\pi,V)\in\widehat{G} \\ V^K\neq 0}}} V^*,$$

so we just need to show that, if $(\pi, V)$ is a finite-dimensional representation of $G$, then $V^K \neq 0$ if and only if $(V^*)^K \neq 0$. Applying theorem IV.5.7 to the restrictions of the representations $V$ and $V^*$ to $K$, we get

$$\dim(V^K) = \int_K \chi_V(k)dk$$

and

$$\dim((V^*)^K) = \int_K \chi_{V^*}(k)dk = \int_K \overline{\chi_V(k)}dk = \overline{\dim(V^K)} = \dim(V^K).$$

□

## V.4 Spherical functions

In this section, we assume that $(G, K)$ is a Gelfand pair.

**Definition V.4.1.** Let $\varphi \in \mathscr{C}(K\backslash G/K)$. We say that $\varphi$ is a *spherical function* if the linear functional $\chi_\varphi : \mathscr{C}_c(K\backslash G/K) \to \mathbb{C}$, $f \longmapsto f * \varphi(1) = \int_G f(x)\varphi(x^{-1})dx$ is a multiplicative functional, where the multiplication on $\mathscr{C}_c(K\backslash G/K)$ is the convolution product.

In other words, the function $\varphi$ is spherical if $\varphi \neq 0$ and if, for all $f, g \in \mathscr{C}_c(K\backslash G/K)$, we have $\chi_\varphi(f * g) = \chi_\varphi(f)\chi_\varphi(g)$.

**Example V.4.2.** If $G$ is commutative and $K = \{1\}$, then every continuous morphism of groups $\varphi : G \to \mathbb{C}^\times$ is a spherical function. Indeed, let $f, g \in \mathscr{C}_c(G)$. Then :

$$\begin{aligned}
\int_G (f * g)(x)\varphi(x^{-1})dx &= \int_{G\times G} f(y)g(y^{-1}x)\varphi(x^{-1})dx \\
&= \int_{G\times G} f(y)g(z)\varphi(z^{-1}y^{-1})dydz \\
&= \left(\int_G f(y)\varphi(y^{-1})dy\right)\left(\int_G g(z)\varphi(z^{-1})dz\right).
\end{aligned}$$

These are actually the only spherical functions in this case. (This follows immediately from the next proposition.)

**Proposition V.4.3.** *Let $\varphi \in \mathscr{C}(K\backslash G/K)$. The following conditions are equivalent :*

*(i) The function $\varphi$ is spherical.*

*(ii) The function $\varphi$ is nonzero and, for all $x, y \in G$, we have*

$$\int_K \varphi(xky)dk = \varphi(x)\varphi(y).$$

*(iii) We have :*

*(a) $\varphi(1) = 1$;*

*(b) for every $f \in \mathscr{C}_c(K\backslash G/K)$, there exists $\chi(f) \in \mathbb{C}$ such that $f * \varphi = \chi(f)\varphi$.*

*Proof.* We can extend $\chi_\varphi$ to $\mathscr{C}_c(G)$ by using the same formula, i.e., $\chi_\varphi(f) = \int_G f(x)\varphi(x^{-1})dx$. Note that, for all $f, g \in \mathscr{C}_c(G)$, we have

$$\begin{aligned}\chi_\varphi(f * g) &= \int_{G\times G} f(y)g(y^{-1}x)\varphi(x^{-1})dx \\ &= \int_{G\times G} f(y)g(z)\varphi(z^{-1}y^{-1})dydz,\end{aligned}$$

hence

$$\chi_\varphi(f * g) - \chi_\varphi(f)\chi_\varphi(g) = \int_{G\times G} f(y)g(z)(\varphi(z^{-1}y^{-1}) - \varphi(z^{-1})\varphi(y^{-1}))dydz.$$

Let $f, g \in \mathscr{C}_c(G)$. Applying the calculation above to $f' := {}^K f^K$ and $g' := {}^K g^K$ and using the bi-invariance of $\varphi$ (and the fact that the measure on $K$ is normalized), we get that $\chi_\varphi(f' * g') - \chi_\varphi(f')\chi_\varphi(g')$ is equal to

$$\begin{aligned}&\int_{G^2\times K^4} f(k_1xk_2)g(k_3yk_4)(\varphi(y^{-1}x^{-1}) - \varphi(y^{-1})\varphi(x^{-1}))dxdydk_1dk_2dk_3dk_4 \\ =&\int_{G^2\times K^2} f(x)g(y)(\varphi(y^{-1}k_3k_2x^{-1}) - \varphi(x^{-1})\varphi(y^{-1}))dxdydk_2dk_3 \\ =&\int_{G^2} f(x)g(y)\left(\int_K \varphi(y^{-1}kx^{-1})dk - \varphi(x^{-1})\varphi(y^{-1})\right)dxdy.\end{aligned}$$

This shows that $\chi_\varphi$ is multiplicative if and only $\int_G \varphi(y^{-1}kx^{-1})dk = \varphi(y^{-1})\varphi(x^{-1})$ for all $x, y \in G$. As $\chi_\varphi \neq 0$ if and only if $\varphi \neq 0$, this proves that (i) and (ii) are equivalent.

Suppose that $\varphi$ satisfies conditions (a) and (b) of (iii). Then, for every $f \in \mathscr{C}_c(K\backslash G/K)$, we have

$$\chi_\varphi(f) = f * \varphi(1) = \chi(f).$$

As $f \longmapsto \chi(f)$ is multiplicative (by the associativity of the convolution product), this implies that $\varphi$ is spherical.

Finally, suppose that $\varphi$ is spherical. We want to prove that conditions (a) and (b) of (iii) are satisfied. Let $f \in \mathscr{C}_c(K\backslash G/K)$. Then we have, for every $x \in G$,

$$\begin{aligned} f * \varphi(x) &= \int_G f(y)\varphi(y^{-1}x)dy \\ &= \int_{G\times K} f(y)\varphi(y^{-1}kx)dydk \quad \text{(by left invariance of } f) \\ &= \int_G f(y)\varphi(y)^{-1}\varphi(x)dy \quad \text{(by (ii))} \\ &= \chi_\varphi(f)\varphi(x). \end{aligned}$$

This shows condition (b). Choosing $f \in \mathscr{C}_c(K\backslash G/K)$ such that $\chi_\varphi(f) \neq 0$, and applying the equality above to $x = 1$, we get $\chi_\varphi(f) = \chi_\varphi(f)\varphi(1)$, hence $\varphi(1) = 1$.

□

Remember that $L^1(G)$ is a Banach $*$-algebra, for the convolution product and the involution given by $f^*(x) = \overline{f(x^{-1})}$. [2] We have seen that $L^1(K\backslash G/K)$ is a commutative Banach subalgebra of $L^1(G)$, and it is clear that it is also preserved by the involution. So it is natural to ask what the spectrum of $L^1(K\backslash G/K)$ is.

If $\varphi \in \mathscr{C}_b(K\backslash G/K)$ (note the boundedness condition), then the integral $\int_G f(x)\varphi(x^{-1})dx$ converges for every $f \in L^1(G)$, so we can extend the linear functional $\chi_\varphi$ on $\mathscr{C}_c(K\backslash G/K)$ to a bounded linear functional on $L^1(K\backslash G/K)$, that we will still denote by $\chi_\varphi$.

**Theorem V.4.4.** *The map $\varphi \longmapsto \chi_\varphi$ identifies the set of* bounded *spherical functions to $\sigma(L^1(K\backslash G/K))$.*

**Example V.4.5.** If $G$ is commutative and $K = \{1\}$, a bounded spherical function is a bounded continuous morphism of groups $G \to \mathbb{C}^\times$, that is, a continuous morphism of groups $G \to S^1$, i.e. an irreducible unitary representation of $G$. So we get a canonical bijection $\widehat{G} \overset{\sim}{\to} \sigma(L^1(G))$. In particular, every multiplicative functional on $L^1(G)$ is a $*$-homomorphism in this case, that is, the Banach $*$-algebra $L^1(G)$ is symmetric. This recovers the result of question II.5.4(c).

If $G$ is compact, we will see (in theorem V.7.1) that it is still true that every spherical function defines a $*$-homomorphism of $L^1(K\backslash G/K)$, i.e. that $L^1(K\backslash G/K)$. But in general, this is not true.

*Proof of theorem V.4.4.* If $\varphi$ is a bounded spherical function, then $\chi_\varphi$ is multiplicative on $\mathscr{C}_c(K\backslash G/K)$, hence also on $L^1(K\backslash G/K)$ because $\mathscr{C}_c(K\backslash G/K)$ is dense in $L^1(K\backslash G/K)$.

Conversely, let $\chi : L^1(K\backslash G/K) \to \mathbb{C}$ be a multiplicative functional. By corollary II.2.6, the linear functional $\chi$ is continuous and has norm $\leq 1$.

[2] As $(G, K)$ is a Gelfand pair, the group $G$ is automatically unimodular by proposition V.2.4, so we don't need the factor $\Delta(x)^{-1}$.

By remark V.2.2, the linear operator $\mathscr{C}_c(G) \to \mathscr{C}_c(K\backslash G/K)$, $f \longmapsto {}^K f^K$ decreases the $L^1$ norm, so it extends to a continuous linear operator $L^1(G) \to L^1(K\backslash G/K)$, that we will still denote by $f \longmapsto {}^K f^K$. Then $f \longmapsto \chi({}^K f^K)$ is a continuous linear functional on $L^1(G)$, and its norm is equal to that of $\chi$, so there exists a unique $\varphi \in L^\infty(G)$ such that $\|\varphi\|_\infty = \|\chi\|_{op}$ and that, for every $f \in L^1(G)$, we have

$$\int_G f(x)\varphi(x^{-1})dx = \chi({}^K f^K).$$

In particular, for all $k, k' \in K$ and every $f \in L^1(G)$, we have

$$\begin{aligned}\int_G f(x)\varphi(kx^{-1}k')dx &= \int_G f((k')^{-1}xk^{-1})\varphi(x^{-1})dx \\ &= \chi({}^K(L_{k'}R_{k^{-1}}f)^K) \\ &= \chi({}^K f^K) \\ &= \int_G f(x)\varphi(x^{-1})dx.\end{aligned}$$

So $\varphi$ is bi-invariant.

Let $f, g \in L^1(K\backslash G/K)$. We have

$$\begin{aligned}\chi(f * g) &= \int_G (f * g)(x)\varphi(x^{-1})dx \\ &= \int_{G\times G} f(y)g(y^{-1}x)\varphi(x^{-1})dxdy \\ &= \int_{G\times G} f(y)\varphi(y^{-1}z)g(z^{-1})dydz \\ &= \int_G (f * \varphi)(z)g(z^{-1})dz.\end{aligned}$$

As $\chi(f * g) = \chi(f)\chi(g) = \chi(f)\int_G \varphi(z)g(z^{-1})dz$, this implies that

$$\int_G ((f * \varphi) - \chi(f)\varphi)(z)g(z^{-1})dz = 0.$$

Hence, for every $f \in L^1(K\backslash G/K)$, we have $f * \varphi = \chi(f)\varphi$. Choose $f \in \mathscr{C}_c(K\backslash G/K)$ such that $\chi(f) \neq 0$. Then $\chi(f) = f * \varphi(1) = \chi(f)\varphi(1)$, so $\varphi(1) = 1$. Also, the function $f * \varphi$ is continuous, because it is left uniformly continuous (note that, for every $x \in G$, we have $\|L_x(f*\varphi) - f*\varphi\|_\infty = \|(L_x f - f)*\varphi\|_\infty \leq \|L_x f - f\|_1\|\varphi\|_\infty$ and apply proposition I.3.1.13). So $\varphi$ is locally almost everywhere equal to a bi-invariant continuous bounded function, and this continuous bounded function is spherical by proposition V.4.3.

Finally, let $\varphi'$ be another bounded spherical function such that, for every $f \in L^1(K\backslash G/K)$, we have

$$\int_G f(x)\varphi'(x^{-1})dx = \int_G f(x)\varphi(x^{-1})dx.$$

We have seen above that, for every $f \in L^1(G)$, we have

$$\int_G f(x)\varphi(x^{-1})dx = \chi({}^K f^K) = \int_G {}^K f^K(x)\varphi(x^{-1})dx,$$

and we have a similar equality for $\varphi'$. So

$$\int_G f(x)\varphi'(x^{-1})dx = \int_G f(x)\varphi(x^{-1})dx$$

for every $f \in L^1(G)$, and this implies that $\varphi' = \varphi$.

□

## V.5 Spherical functions of positive type

For the first result, we don't need to assume that $(G, K)$ is a Gelfand pair.

**Proposition V.5.1.** *Let $\varphi$ be a function of positive type on G, and let $(\pi_\varphi, V_\varphi)$ and $v_\varphi \in V_\varphi$ be the unitary representation of G and the cyclic vector associated to $\varphi$. (See section III.2.)*

*Then $v_\varphi \in V_\varphi^K$ if and only if $\varphi$ is bi-invariant.*

*Proof.* For all $k, k' \in K$ and $x \in G$, we have

$$\varphi(kxk') = \langle \pi_\varphi(kxk')(v_\varphi), v_\varphi \rangle = \langle \pi_\varphi(x)(\pi_\varphi(k')(v_\varphi)), \pi_\varphi(k^{-1})(v_\varphi) \rangle.$$

So, if $v_\varphi \in V_\varphi^K$, we get $\varphi(kxk') = \varphi(x)$. Conversely, suppose that $\varphi$ is bi-invariant. Taking $k' = 1$ in the equation above, we see that, for every $k \in K$ and every $x \in G$,

$$\varphi(x) = \langle \pi_\varphi(x)(v_\varphi), v_\varphi \rangle = \varphi(k^{-1}x) = \langle \pi_\varphi(x)(v_\varphi), \pi_\varphi(k)(v_\varphi) \rangle.$$

As $v_\varphi$ is a cyclic vector, the span of $\{\pi_\varphi(x)(v_\varphi),\ x \in G\}$ is dense in $V_\varphi$, and so this implies that $\pi_\varphi(k)(v_\varphi) = v_\varphi$, for every $k \in K$.

□

**Theorem V.5.2.** *Assume again that $(G, K)$ is a Gelfand pair. Let $\varphi$ be a continuous bi-invariant function on G.*

*If $\varphi$ is a normalized function of positive type (i.e. $\varphi \in \mathscr{P}_1$), then $\varphi$ is spherical if and only $\varphi \in \mathscr{E}(\mathscr{P}_1)$, that is, if and only if the representation $(\pi_\varphi, V_\varphi)$ is irreducible.*

*Proof.* We write $(\pi, V)$ and $v$ for $(\pi_\varphi, V_\varphi)$ and $v_\varphi$. As $\varphi$ is bi-invariant, we know that $v \in V^K$ by proposition V.5.1. Suppose first that $\varphi \in \mathscr{E}(\mathscr{P}_1)$, i.e., that $\pi$ is irreducible. By theorem V.3.1.1, we have $\dim(V^K) = 1$. Let $f \in \mathscr{C}_c(K\backslash G/K)$. Then we have, for every $x \in G$,

$$\begin{aligned} f * \varphi(x) &= \int_G f(y)\langle \pi(y^{-1}x)(v), v\rangle dy \\ &= \int_G f(y)\langle \pi(x)(v), \pi(y)v\rangle dy \\ &= \langle \pi(x)(v), \pi(f)(v)\rangle. \end{aligned}$$

As $\pi(f)(v) \in V^K$, we can write $\pi(f)(v) = \overline{\chi(f)}v$, with $\chi(f) \in \mathbb{C}$, and we get, for every $x \in G$,

$$f * \varphi(x) = \chi(f)\langle \pi(x)(v), v\rangle = \chi(f)\varphi(x).$$

By proposition V.4.3, this implies that $\varphi$ is spherical.

Conversely, assume that $\varphi$ is spherical. Then, by proposition V.4.3 again, there exists a map $\chi : \mathscr{C}_c(K\backslash G/K) \to \mathbb{C}$ such that, for every $f \in \mathscr{C}_c(K\backslash G/K)$, we have $f * \varphi = \chi(f)\varphi$. In other words, for every $f \in \mathscr{C}_c(K\backslash G/K)$ and every $x \in G$, we have

$$\begin{aligned} f * \varphi(x) = \int_G f(y)\langle \pi(y^{-1}x)(v), v\rangle dy &= \langle \pi(x)(v), \pi(f)(v)\rangle \\ &= \chi(f)\varphi(x) \\ &= \chi(f)\langle \pi(x)(v), v\rangle. \end{aligned}$$

As $v$ is a cyclic vector, this implies that $\pi(f)(v) = \overline{\chi(f)}v \in V^K$. But we have seen in the proof of lemma V.3.1.4 that the space $\{\pi(f)(v),\ f \in \mathscr{C}_c(K\backslash G/K)\}$ is dense in $V^K$ (if $v$ is cyclic), so $\dim(V^K) = 1$. By lemma V.5.3, this implies that $(\pi, V)$ is irreducible.

□

**Lemma V.5.3.** *We don't assume that $(G, K)$ is a Gelfand pair. Let $(\pi, V)$ be a unitary representation of G, and suppose that there is a cyclic vector in $V^K$. If $\dim(V^K) \leq 1$, then $(\pi, V)$ is irreducible.*

*Proof.* It suffices to prove that $\mathrm{End}_G(V) = \mathbb{C}\mathrm{id}_V$. Indeed, if $V$ has a closed $G$-invariant subspace $W$ such that $W \neq \{0\}, V$, then the orthogonal projection on $W$ is a $G$-equivariant endomorphism of $V$ (by lemma I.3.4.3) that is not a multiple of $\mathrm{id}_V$.

So let $T \in \mathrm{End}_G(V)$. Then, by proposition V.1.7, the operator $T$ commutes with the orthogonal projection on $V^K$, so it preserves $V^K$. Choose a cyclic vector $v \in V^K$. As $\dim(V^K) = 1$, we have $T(v) = \lambda v$, with $\lambda \in \mathbb{C}$. As $T$ is $G$-equivariant, we get that $T(\pi(x)(v)) = \lambda\pi(x)(v)$ for every $x \in G$. As $v$ is cyclic, this implies that $T = \lambda \mathrm{id}_V$.

□

**Corollary V.5.4.** *Assume that $(G, K)$ is a Gelfand pair. Then $\varphi \longmapsto (\pi_\varphi, V_\varphi)$ induces a bijection from the set of spherical functions in $\mathscr{E}(\mathscr{P}_1)$ to the set of unitary equivalence classes of irreducible unitary representations $(\pi, V)$ of G such that $V^K \neq \{0\}$.*

*Proof.* The only statement that doesn't follows immediately from proposition V.5.1 and theorem V.5.2 is the fact that, if two spherical functions in $\mathscr{E}(\mathscr{P}_1)$ give rise to unitarily equivalent representations, then they must be equal. Let $\varphi_1, \varphi_2 \in \mathscr{E}(\mathscr{P}_1)$ be spherical, and suppose that there is an isometric $G$-equivariant isomorphism $T : V_{\varphi_1} \to V_{\varphi_2}$. By proposition V.5.1, the vectors $v_{\varphi_1}$ and $v_{\varphi_2}$ are $K$-invariant. Also, as $(G, K)$ is a Gelfand pair, the spaces $V_{\varphi_1}^K$ and $V_{\varphi_2}^K$ are both of dimension $\leq 1$, hence of dimension 1 because they contain nonzero vectors. But $T$ is $G$-equivariant, so we have $T(V_{\varphi_1}^K) \subset V_{\varphi_2}^K$, which implies that $T(v_{\varphi_1}) = \lambda v_{\varphi_2}$ for some $\lambda \in \mathbb{C}$. As $\|v_{\varphi_1}\| = \|v_{\varphi_2}\| = 1$, we must have $|\lambda| = 1$. So, for every $x \in G$, we get

$$\begin{aligned}\varphi_2(x) &= \langle \pi_{\varphi_2}(x)(v_{\varphi_2}), v_{\varphi_2} \rangle \\ &= \langle \pi_{\varphi_2}(x)(\lambda^{-1} T(v_{\varphi_1})), \lambda^{-1} T(v_{\varphi_1}) \rangle \\ &= \langle T(\pi_{\varphi_1}(x)(v_{\varphi_1})), T(v_{\varphi_1}) \rangle \\ &= \langle \pi_{\varphi_1}(x)(v_{\varphi_1}), v_{\varphi_1} \rangle.\end{aligned}$$

□

## V.6 The dual space and the spherical Fourier transform

In this section, we suppose that $(G, K)$ is a Gelfand pair. We will state a few results on the (spherical) Fourier transform without proof. In the next section, we will give proofs of some version of these results if $G$ is compact.

**Definition V.6.1.** The *dual space* of $(G, K)$ is the set $Z$ of spherical functions in $\mathscr{E}(\mathscr{P}_1)$, with the weak* topology coming from the embedding $\mathscr{E}(\mathscr{P}_1) \subset L^\infty(G) \simeq \mathrm{Hom}(L^1(G), \mathbb{C})$.

**Example V.6.2.** If $G$ is commutative and $K = \{1\}$, then $Z = \widehat{G}$, the dual group of $G$. (See exercise I.5.4.1.)

**Proposition V.6.3.** *The space $Z$ is locally compact, and its topology coincides with the topology of convergence on compact subsets of $G$.*

*Proof.* For the first statement, note first that $\mathscr{P}_0 = \{\psi \text{ of positive type} | \psi(1) \leq 1\}$ is weak* compact, because it is weak* closed in the closed unit ball of $L^\infty(G)$. By the proof of theorem V.4.4, the subset $\mathscr{P}_0 \cap \mathscr{C}(K \setminus G/K)$ is the set of $\varphi \in \mathscr{P}_0$ such that, for every $f \in L^1(G)$, we have $\int_G f(x)\varphi(x^{-1})dx = \int_G {}^K f^K(x)\varphi(x^{-1})dx$. These are weak* closed conditions, so $\mathscr{P}_0 \cap \mathscr{C}(K \setminus G/K)$ is weak* closed in $\mathscr{P}_0$, hence weak* compact. Finally, by theorem V.5.2, the set $Z \cup \{0\}$ is the set of $\varphi \in \mathscr{P}_0 \cap \mathscr{C}(K \setminus G/K)$ such that $\int_G (f * g)(x)\varphi(x^{-1})dx = \left(\int_G f(x)\varphi(x^{-1})dx\right)\left(\int_G g(x)\varphi(x^{-1})dx\right)$ for all $f, g \in L^1(K \setminus G/K)$. This is a weak* closed condition, so $Z \cup \{0\}$ is weak* compact, and $Z$ is locally compact. Note that this also proves that $Z \cup \{0\}$ is the Alexandroff compactification of $Z$.

The second statement follows immediately from Raikov's theorem (theorem III.4.3).

□

**Definition V.6.4.** Let $f \in L^1(K\backslash G/K)$. The *(spherical) Fourier transform* of $f$ is the function $\widehat{f} : Z \to \mathbb{C}$ defined by

$$\widehat{f}(\varphi) = \int_G f(x)\varphi(x^{-1})dx = \chi_\varphi(f).$$

**Proposition V.6.5.** *The Fourier transform has the following properties :*

*(i) For every $f \in L^1(K\backslash G/K)$, the function $\widehat{f}$ is in $\mathscr{C}_0(Z)$, and we have $\|\widehat{f}\|_\infty \leq \|f\|_1$.*

*(ii) The map $L^1(K\backslash G/K) \to \mathscr{C}_0(Z)$, $f \longmapsto \widehat{f}$ is $\mathbb{C}$-linear and it has dense image.*

*(iii) For all $f, g \in L^1(K\backslash G/K)$, we have $\widehat{f * g} = \widehat{f}\widehat{g}$.*

*(iv) For every $f \in L^1(K\backslash G/K)$, we have $\widehat{f^*} = \overline{\widehat{f}}$.*

*Proof.* (i) The continuity $\widehat{f}$ follows immediately from the definition of the weak* topology. In fact, we can extend $\widehat{f}$ (by the same formula) to a continuous linear functional on the whole space $L^\infty(G)$. But have seen in the proof of proposition V.6.3 that $Z \cup \{0\}$ is the Alexandroff compactification of $Z$, so this implies that $\widehat{f} \in \mathscr{C}(Z)$ vanishes at $\infty$. The inequality $\|\widehat{f}\|_\infty \leq \|f\|_1$ just follows from the fact that $\|\varphi\|_\infty = 1$ for every $\varphi \in Z$.

(iii) and (iv) This is just expressing the fact that $\chi_\varphi$ is a $*$-homomorphism from $L^1(K\backslash G/K)$ to $\mathbb{C}$, for every $\varphi \in Z$.

(ii) The linearity is clear. The second statement follows from the Stone-Weierstrass theorem : indeed, the image of the spherical Fourier transform is a $\mathbb{C}$-subalgebra of $\mathscr{C}_0(Z)$ by (iii), it is stable by complex conjugation by (iv), it separates points (because, by theorem V.4.4, the map $Z \to \sigma(L^1(K\backslash G/K))$, $\varphi \longmapsto (f \longmapsto \widehat{f}(\varphi))$ is injective), and it vanishes nowhere (for every $\varphi \in Z$, the map $f \longmapsto \widehat{f}(\varphi)$ is a multiplicative functional on $L^1(K\backslash G/K)$, so it is nonzero).

□

**Theorem V.6.6.** *(Fourier inversion)* [3] *Let $\mathscr{V}^1(K\backslash G/K)$ be the space of $L^1$ functions that are complex linear combinations of bi-invariant functions of positive type on G.*

*Then there exists a unique measure $\nu$ on $Z$, called the* Plancherel measure*, such that, for every $f \in \mathscr{V}^1(K\backslash G/K)$, we have $\widehat{f} \in L^1(Z, \nu)$ and, for every $x \in G$,*

$$f(x) = \int_Z \varphi(x)\widehat{f}(\varphi)d\nu.$$

**Theorem V.6.7.** *(Plancherel formula)* [4] *For every $f \in \mathscr{C}_c(K\backslash G/K)$, we have $\widehat{f} \in L^2(Z, \nu)$, and*

$$\int_G |f(x)|^2dx = \int_Z |\widehat{f}(\varphi)|^2 d\nu(\varphi).$$

[3] See [25] Theorem 6.4.5.
[4] See [25] Theorem 6.4.6.

*In particular, the map $f \longmapsto \widehat{f}$ extends to an isometry $L^2(K\backslash G/K) \to L^2(Z,\nu)$, and this is an isomorphism.*

*Remark* V.6.8. If $G$ is commutative and $K = \{1\}$, then $Z = \widehat{G}$ is a locally compact group, the measure $\nu$ is a Haar measure on $\widehat{G}$, and the Pontrjagin duality theorem says that the canonical map $G \to \widehat{\widehat{G}}$, $x \longmapsto (\varphi \longmapsto \varphi(x))$ is an isomorphism of topological groups. (See for example [11] Theorems 4.22 and 4.32, or [25] Theorems 5.5.1 and 5.7.1.)

But in general, the Plancherel measure $\nu$ could be supported on a strict subset of $Z$.

## V.7 The case of compact groups

In this section, we assume that $(G,K)$ is a Gelfand pair, and that $G$ is compact. We also assume that the Haar measure on $G$ is normalized.

**Theorem V.7.1.** *(i) The dual space $Z$ of $(G,K)$ is discrete, and it is an orthogonal subset of $L^2(G)$.*

*(ii) Every spherical function on $G$ is of positive type (hence in $\mathscr{E}(\mathscr{P}_1)$ by theorem V.5.2). In other words, the set $Z$ is in canonical bijection (via $\varphi \longmapsto (\pi_\varphi, V_\varphi)$) with the set of equivalence classes of irreducible unitary representations of $G$ such that $\dim(V_\varphi^K) = 1$.*

*(iii) For every $\varphi \in Z$, we have*

$$\varphi(x) = \int_K \chi_{\pi_\varphi}(xk)dk$$

*for $x \in G$, and*

$$\int_G |\varphi(x)|^2 = \frac{1}{\dim V_\varphi}.$$

*(iv) If $f \in L^2(K\backslash G/K)$ and $(\pi, V) \in \widehat{G}$, then $f * \chi_\pi = 0$ if $V^K = \{0\}$, and otherwise $f * \chi_\pi$ is a multiple of the element $\varphi_\pi$ of $Z$ corresponding to $\pi$ by corollary V.5.4.*

*Proof.* Let $\varphi, \varphi' \in Z$ such that $\varphi \neq \varphi'$. We know by corollary V.5.4 (and proposition IV.2.6) that the representations $V_\varphi$ and $V_{\varphi'}$ are unitary and not equivalent. We also know (by construction of the representation) that $\varphi$ and $\varphi'$ are matrix coefficients of $V_\varphi$ and $V_{\varphi'}$, respectively. By Schur orthogonality (theorem IV.3.8), this implies that $\langle \varphi, \varphi' \rangle_{L^2(G)} = 0$.

We prove that $Z$ is discrete. Let $\varphi \in Z$, and consider $U = \{\varphi' \in Z | \|\varphi - \varphi'\|_\infty < \|\varphi\|_2\}$. This is open in the topology of convergence on compact subsets of $G$ (because $G$ is compact), hence is an open subset of $Z$ by Raikov's theorem (theorem III.4.3). Also, if $\varphi' \in U$, then we have

$$\begin{aligned}|\langle \varphi, \varphi' \rangle_{L^2(G)}| &= |\langle \varphi, \varphi \rangle_{L^2(G)} - \langle \varphi, \varphi' - \varphi \rangle_{L^2(G)}| \\ &\geq \|\varphi\|_2^2 - \|\varphi\|_2 \|\varphi - \varphi'\|_2 \\ &\geq \|\varphi\|_2^2 - \|\varphi\|_2 \|\varphi - \varphi'\|_\infty \\ &> 0,\end{aligned}$$

hence, by the first paragraph, $\varphi' = \varphi$. This means that $U = \{\varphi\}$, i.e., that $\varphi$ is an isolated point of $Z$.

Let $(\pi, V)$ be an irreducible unitary representation of $G$ and let $f \in L^2(K\backslash G/K)$. We want to calculate $f * \chi_\pi$. Let $(v_1, \dots, v_d)$ be an orthonomal basis; then, for every $x \in G$, we have $\chi_\pi(x) = \sum_{i=1}^d \langle \pi(x)(e_i), e_i \rangle$. Hence, for every $x \in G$,

$$f * \chi_\pi(x) = \int_G f(y) \sum_{i=1}^d \langle \pi(y^{-1}x)(e_i), e_i \rangle = \sum_{i=1}^d \langle \pi(x)(e_i), \pi(\overline{f})(e_i) \rangle.$$

Let $P_K \in \mathrm{End}(V)$ be the orthogonal projection on $V^K$. As $\overline{f}$ is bi-invariant, we have $\pi(\overline{f}) = P_K \circ \pi(\overline{f}) \circ P_K$ by proposition V.1.7. Suppose first that $V^K = \{0\}$. Then the formula above gives $f * \chi_\pi = 0$. Now suppose that $V^K \neq \{0\}$. Then, by corollary V.5.4, there is a unique spherical function of positive type $\varphi_\pi$ whose associated representation is $(\pi, V)$, and a unitary cyclic vector $v \in V^K$ such that $\varphi_\pi(x) = \langle \pi(x)(v), v \rangle$. We may choose the orthonormal basis such that $v_1 = v$. Then $P_K(v_i) = 0$ for $i \geq 2$ and $P_K(v_1) = v_1$, for every $x \in G$, we have

$$f * \chi_\pi(x) = \sum_{i=1}^d \langle \pi(x)(v_i), P_K(\pi(\overline{f})(P_K(v_i))) \rangle = \langle \pi(x)(v_1), P_K(\pi(\overline{f})(v_1)) \rangle.$$

As $V^K$ is 1-dimensional, the vector $P_K(\pi(\overline{f})(v_1))$ is a multiple of $v_1$, and so $f * \chi_\pi$ is a multiple of $\varphi_\pi$. This proves (iv). Note also that, for every $x \in G$, we have

$$\begin{aligned}\int_K \chi_\pi(kx)dk &= \int_K \sum_{i=1}^d \langle \pi(kx)(v_i), v_i \rangle dk \\ &= \sum_{i=1}^d \left\langle \pi(x)(v_i), \int_K \pi(k^{-1})(v_i)dk \right\rangle \\ &= \sum_{i=1}^d \langle \pi(x)(v_i), P_K(v_i) \rangle \quad \text{(by proposition V.1.7)} \\ &= \langle \pi(x)(v_1), v_1 \rangle \\ &= \varphi_\pi(x),\end{aligned}$$

which gives the first part of (iii). The second part of (iii) is contained in point (ii) of proposition IV.3.8.

Now consider a spherical function $\varphi$ on $G$. By proposition IV.7.1 (i.e. the Fourier inversion formula), we have an equality (in $L^2(G)$)

$$\varphi = \sum_{\pi \in \widehat{G}} \dim(\pi) \varphi * \chi_\pi.$$

By the calculations above, only the $\pi \in \widehat{G}$ with nonzero $K$-invariant vectors appear in the sum above, and then $\varphi * \chi_\pi$ is a multiple of the function that was denoted by $\varphi_\pi$ in the previous paragraph. In other words, using corollary V.5.4 again, we get

$$\varphi = \sum_{\psi \in Z} c_\psi \psi,$$

for some $c_\psi \in \mathbb{C}$. If we denote by $\chi_\varphi$ (resp. $\chi_\psi$) the linear functional $f \longmapsto f * \varphi(1)$ (resp. $f \longmapsto f * \psi(1)$) on $L^1(K \backslash G/K)$, we know that it is multiplicative (for $\chi_\psi$, this uses theorem V.5.2). Also, as $\varphi = \sum_{\psi \in Z} c_\psi \psi$, we have $\chi_\varphi = \sum_{\psi \in Z} c_\psi \chi_\psi$. Let $\psi, \psi' \in Z$ such that $\psi \neq \psi'$. Then $\psi * \psi' = \psi' * \psi$ is a multiple of both $\psi$ and $\psi'$ (by proposition V.4.3), so $\psi * \psi' = 0$. In particular, we have $\chi_\psi(\psi') = \chi_{\psi'}(\psi) = 0$. This implies that $\chi_\varphi(\psi) = c_\psi \chi_\psi(\psi)$ for every $\psi \in Z$; note also that

$$\chi_\psi(\psi) = \int_G \psi(x)\psi(x^{-1})dx = \int_G \psi(x)\overline{\psi(x)}dx > 0.$$

Hence, if $\psi, \psi' \in Z$ and $\psi \neq \psi'$, then

$$0 = \chi_\varphi(\psi * \psi') = \chi_\varphi(\psi)\chi_\varphi(\psi') = c_\psi c'_\psi \chi_\psi(\psi)\chi_{\psi'}(\psi'),$$

so $c_\psi c_{\psi'} = 0$. So at most of one the $c_\psi$ can be nonzero, i.e., there exists $\psi \in Z$ such that $\varphi = c_\psi \psi$. As $\varphi(1) = 1 = \psi(1)$, we must also have $c_\psi = 1$, so finally we see that $\varphi = \psi$ is of positive type. This finishes the proof of (ii).

□

**Corollary V.7.2.** *(i) We have a G-equivariant isomorphism*

$$L^2(G/K) \simeq \widehat{\bigoplus_{\varphi \in Z} V_\varphi}.$$

*(ii) The family* $((\dim V_\varphi)^{1/2}\varphi)_{\varphi \in Z}$ *is a Hilbert basis of* $L^2(K \backslash G/K)$.

*(iii) For every* $f \in L^2(K \backslash G/K)$, *we have*

$$f = \sum_{\varphi \in Z} \dim(V_\varphi) \widehat{f}(\varphi) \varphi$$

*(Fourier inversion formula) and*

$$\|f\|^2_{L^2(G)} = \sum_{\varphi \in Z} \dim(V_\varphi) |\widehat{f}(\varphi)|^2$$

*(Parseval formula).*

*Proof.* Point (i) is just a reformulation of the last statement of theorem V.3.2.4.

For (ii), we already know that the family $(\sqrt{\dim(V_\varphi)}\varphi)_{\varphi\in Z}$ is orthonormal in $L^2(G)$. Also, if $f \in L^2(K\backslash G/K)$, we have

$$f = \sum_{(\pi,V)\in\widehat{G}} \dim(V) f * \chi_\pi$$

by proposition IV.7.1, so $f$ is in the closure of $\mathrm{Span}(Z)$ by point (iv) of the theorem, which means that $\mathrm{Span}(Z)$ is dense in $L^2(K\backslash G/K)$.

The second formula of (iii) follows from the first formula and from (ii). To prove the first formula, it only remains to show that, for every $f \in L^2(K\backslash G/K)$ and every $\varphi \in Z$, we have $f * \chi_{\pi_\varphi} = \widehat{f}(\varphi)\varphi$. As we already know that $f * \chi_{\pi_\varphi}$ is a multiple of $\varphi$, we just need to check that $f * \chi_{\pi_\varphi}(1) = \widehat{f}(\varphi)$. By point (iii) of the theorem, we have $\varphi(x) = \int_K \chi_{\pi_\varphi}(kx)dk$ for every $x \in G$. So :

$$\begin{aligned}
f * \chi_{\pi_\varphi}(1) &= \int_G f(x)\chi_{\pi_\varphi}(x^{-1})dx \\
&= \int_{G\times K} f(k^{-1}x)\overline{\chi_{\pi_\varphi}(x)}dxdk \quad (f \text{ is left invariant and } \mathrm{vol}(K) = 1) \\
&= \int_{G\times K} f(x)\overline{\chi_{\pi_\varphi}(kx)}dxdk \\
&= \int_G f(x)\overline{\varphi(x)}dx \\
&= \int_G f(x)\varphi(x^{-1})dx \\
&= \widehat{f}(\varphi).
\end{aligned}$$

□

*Remark* V.7.3. The corollary says in particular that the Plancherel measure $\nu$ on $Z$ is given by $|\nu(\{\varphi\})| = \dim(V_\varphi)$.

# V.8 Exercises

## V.8.1 The Gelfand pair $(\mathrm{SO}(n), \mathrm{SO}(n-1))$

The material in this series of exercises is classical, but the exposition here ows a lot to section 2.3.2 of [22] and section 7.3 of [25].

**Exercise V.8.1.1.** Fix a positive integer $n$. For every $m \in \mathbb{Z}_{\geq 0}$, we denote by $V_m(\mathbb{R}^n)$ the vector space of complex-valued polynomial functions on $\mathbb{R}^n$ that are homogenous of degree $m$. We define an action of $\mathrm{O}(n)$ on $V_m(\mathbb{R}^n)$ by $(x \cdot f)(v) = f(x^{-1}v)$ if $x \in \mathrm{O}(n)$, $f \in V_m(\mathbb{R}^n)$ and $v \in \mathbb{R}^n$ (in other words, $x \cdot f = L_x f$).

For $i \in \{1, \ldots, n\}$, we denote by $\partial_{x_i}$ the endomorphism $f \longmapsto \frac{\partial}{\partial x_i} f$ of $C^\infty(\mathbb{R}^n)$ (the space of smooth functions from $\mathbb{R}^n$ to $\mathbb{C}$), and we set $\Delta = \sum_{i=1}^n (\partial_{x_i})^2$ (this is called the Laplacian operator).

The space of harmonic polynomials of degree $m$ on $\mathbb{R}^n$ is the space

$$\mathscr{H}_m(\mathbb{R}^n) = \{f \in V_m(\mathbb{R}^n) | \Delta(f) = 0\}.$$

(a). Calculate $\dim(V_m(\mathbb{R}^n))$.

(b). Show that the action of $\mathrm{O}(n)$ on $V_m(\mathbb{R}^n)$ is a continuous representation.

(c). Show that, for every $x \in \mathrm{O}(n)$ and every $f \in C^\infty(\mathbb{R}^n)$, we have $\Delta(L_x f) = L_x(\Delta(f))$. (Using V.8.1.2 can help with this question.)

(d). Show that the subspace $\mathscr{H}_m(\mathbb{R}^n)$ of $V_m(\mathbb{R}^n)$ is $\mathrm{O}(n)$-invariant.

*Solution.*

(a). For every $i \in \{1, \ldots, n\}$, denote by $x_i \in V_1(\mathbb{R}^n)$ the function $(z_1, \ldots, z_n) \longmapsto z_i$. Then $\{x_1^{i_1} \ldots x_n^{i_n}, i_1, \ldots, i_n \in \mathbb{Z}_{\geq 0}, i_1 + \ldots + i_n = m\}$ is a basis of $V_m(\mathbb{R}^n)$. So

$$\dim(V_m(\mathbb{R}^n)) = |\{(i_1, \ldots, i_n) \in (\mathbb{Z}_{\geq 0})^n | i_1 + \ldots + i_n = m\}|.$$

This is also equal to

$$|\{(j_1, \ldots, j_n) \in (\mathbb{Z}_{\geq 1})^n | j_1 + \ldots + j_n = m + n\}|$$

(take $j_r = i_r + 1$). Choosing $(j_1, \ldots, j_n)$ in the set above is equivalent to choosing the numbers $j_1, j_1 + j_2, \ldots, j_1 + \ldots + j_{n-1}$, which form a subset of $\{1, \ldots, n + m - 1\}$ of cardinality $n - 1$. So we get

$$\dim(V_m(\mathbb{R}^n)) = \binom{n+m-1}{n-1} = \binom{n+m-1}{m}.$$

(b). If we use the basis of $V_m(\mathbb{R}^n)$ from (a), the action of $x \in \mathrm{O}(n)$ is given by a matrix with coefficients polynomial functions in the entries of $x$. So, for every $f \in V_m(\mathbb{R}^n)$, the map $\mathrm{O}(n) \to V_m(\mathbb{R}^n)$, $x \cdot f$ is continuous. As $V_m(\mathbb{R}^n)$ is finite-dimensional, this implies that the action is continuous.

(c). To avoid doing the calculation, let's use V.8.1.2(c). Note that $\Delta = \partial_{x_1^2 + \ldots + x_n^2}$. So, by V.8.1.2(c), for every $f \in C^\infty(\mathbb{R}^n)$ and every $x \in G$, we have

$$\Delta(x \cdot f) = x \cdot (\partial_g f),$$

where $g = L_{x^T}(x_1^2 + \ldots + x_n)$. So we just need to show that $x_1^2 + \ldots + x_n^2 \in V_2(\mathbb{R}^n)$ is invariant by all the elements of $\mathrm{O}(n)$, which follows directly from the definition of $\mathrm{O}(n)$.

(d). Question (c) implies that $\Delta : V_m(\mathbb{R}^n) \to V_{m-2}(\mathbb{R}^n)$ is $\mathrm{O}(n)$-equivariant, and $\mathscr{H}_m(\mathbb{R}^n)$ is its kernel.

$\square$

**Exercise V.8.1.2.** We keep the notation of problem V.8.1.1. For $i \in \{1, \ldots, n\}$, we denote by $x_i$ the $i$th coordinate function on $\mathbb{R}^n$.

(a). Show that the map $x_i \to \partial_{x_i}$ extends to a unique morphism of $\mathbb{C}$-algebras from $\bigoplus_{m\geq 0} V_m(\mathbb{R}^n)$ (the algebra of complex-valued polynomial functions on $\mathbb{R}^n$) to $\mathrm{End}(\mathscr{C}^\infty(\mathbb{R}^n))$. We will denote this morphism by $f \longmapsto \partial_f$.

If $f, g \in V_m(\mathbb{R}^n)$, we set $\langle f, g\rangle = \partial_{\overline{g}}(f)$. (Note that $\overline{g}$ is still a polynomial function on $\mathbb{R}^n$.)

(a). Show that $\langle ., . \rangle$ is an inner form on $V_m(\mathbb{R}^n)$. (Hint : Can you find an orthogonal basis ?)

(b). Show that, for every $f \in V_m(\mathbb{R}^n)$ and every $y \in \mathrm{O}(n)$, we have $\partial_f \circ L_y = L_y \circ \partial_{L_{y^T} f}$ in $\mathrm{End}(C^\infty(\mathbb{R}^n))$.

(c). Show that the continuous representation of $\mathrm{O}(n)$ on $V_m(\mathbb{R}^n)$ defined in problem V.8.1.1 is unitary for the inner product $\langle ., . \rangle$.

(d). If $m \leq 1$, show that $V_m(\mathbb{R}^n) = \mathscr{H}_m(\mathbb{R}^n)$.

(e). If $m \geq 2$, show that $\mathscr{H}_m(\mathbb{R}^n)^\perp = |x|^2 V_{m-2}(\mathbb{R}^n)$, where $|x|^2$ is the function $\sum_{i=1}^n x_i^2 \in V_2(\mathbb{R}^n)$.

(f). Show that

$$V_m(\mathbb{R}^n) = \bigoplus_{k=0}^{\lfloor m/2 \rfloor} |x|^{2k} \mathscr{H}_{m-2k}(\mathbb{R}^n),$$

and that this induces a $\mathrm{O}(n)$-equivariant isomorphism

$$V_m(\mathbb{R}^n) = \bigoplus_{k=0}^{\lfloor m/2 \rfloor} \mathscr{H}_{m-2k}(\mathbb{R}^n).$$

(g). If $S \subset \mathbb{R}^n$ is the unit sphere, show that the map $\bigoplus_{m\geq 0} \mathscr{H}_m(\mathbb{R}^n) \to \mathscr{C}(S)$, $f \longmapsto f_{|S}$ is injective.

(h). Show that, for every $f \in V_m(\mathbb{R}^n)$, there is a unique $g \in \bigoplus_{k=0}^{\lfloor m/2 \rfloor} \mathscr{H}_{m-2k}(\mathbb{R}^n)$ such that $f_{|S} = g_{|S}$.

*Solution.*

(a). Note that $\bigoplus_{m\geq 0} V_m(\mathbb{R}^n)$ is isomorphic to the polynomial algebra $\mathbb{C}[x_1, \ldots, x_n]$. So we just need to check that $\partial_{x_i}$ and $\partial_{x_j}$ commute for all $i, j \in \{1, \ldots, n\}$. But this is a well-known property of partial derivatives of $C^2$ functions.

(b). First, it is clear from the definition that $\langle .,. \rangle$ is linear in the first variable and antilinear in the second variable. We calculate the matrix of this form in the basis of V.8.1.1(a).

Let $f = x_1^{i_1} \dots x_n^{i_n}$, with $i_1, \dots, i_n \in \mathbb{Z}_{\geq 0}$ and $i_1 + \dots + i_n = m$. If $r \in \{1, \dots, n\}$ and $a \in \mathbb{Z}_{\geq 0}$, we have

$$\partial_{x_r^a} f = \begin{cases} 0 & \text{if } a > i_r \\ i_r(i_r - 1) \dots (i_r - a + 1) x_r^{i_r - a} \prod_{s \neq r} x_s^{i_s} & \text{if } a \leq i_r. \end{cases}$$

Let $g = x_1^{j_1} \dots x_n^{j_n}$, with $j_1, \dots, j_n \in \mathbb{Z}_{\geq 0}$ and $j_1 + \dots + j_n = m$. As $i_1 + \dots + i_n = j_1 + \dots + j_n$, either there exists $r \in \{1, \dots, n\}$ such that $j_r > i_r$, or $i_r = j_r$ for every $r \in \{1, \dots, n\}$. In the first case, we have $\langle f, g \rangle = \partial_{\overline{g}} f = 0$. In the second case, we have

$$\langle f, g \rangle = \partial_{\overline{g}} f = i_1! i_2! \dots i_n!.$$

So the matrix of $\langle .,. \rangle$ in the basis $\{x_1^{i_1} \dots x_n^{i_n}, i_1, \dots, i_n \in \mathbb{Z}_{\geq 0}, i_1 + \dots + i_n = m\}$ of $V_m(\mathbb{R}^n)$ is diagonal with real positive entries, and in particular Hermitian definite positive. This implies that $\langle .,. \rangle$ is an inner product.

(c). The statement is actually true for every $y \in \mathrm{GL}_n(\mathbb{R})$, and we will prove this.

First note that the identity of the statement makes sense for $f$ in the algebra $V(\mathbb{R}^n) := \bigoplus V_m(\mathbb{R}^n)$, and it is linear in $f$. Also, if it is true for $f, g \in V(\mathbb{R}^n)$, then we have, for $y \in \mathrm{GL}_n(\mathbb{R})$,

$$\begin{aligned} \partial_{fg} \circ L_y &= \partial_f \circ \partial_g \circ L_y \\ &= \partial_f \circ L_y \circ \partial_{L_{y^T} g} \\ &= L_y \circ \partial_{L_{y^T} f} \circ \partial_{L_{y^T} g} \\ &= L_y \circ \partial_{L_{y^T} f L_{y^T} g} \\ &= L_y \circ \partial_{L_{y^T}(fg)}, \end{aligned}$$

that is, the identity also holds for $fg$. In conclusion, we only need to prove it for the functions $x_1, \dots, x_n$.

Let $i \in \{1, \dots, n\}$, and, let $y \in \mathrm{GL}_n(\mathbb{R})$, and write $y^{-1} = a = (a_{ij}) \in \mathrm{GL}_n(\mathbb{R})$. Then for every $(z_1, \dots, z_n) \in \mathbb{R}^n$, we have

$$(L_{y^T} x_i)(z_1, \dots, z_n) = x_i(a^T(z_1, \dots, z_n)) = \sum_{j=1}^n a_{ji} z_j.$$

In other words, we have

$$L_{y^T} x_i = \sum_{j=1}^n a_{ji} x_j,$$

so

$$\partial_{L_{y^T} x_i} = \sum_{j=1}^n a_{ji} \partial_{x_j}.$$

Let $\varphi \in C^\infty(\mathbb{R}^n)$ and $z = (z_1, \dots, z_n) \in \mathbb{R}^n$. We have

$$\partial_{L_{y^T} x_i} \varphi = \sum_{j=1}^n a_{ji} \frac{\partial \varphi}{\partial x_j},$$

so

$$L_y \partial_{L_{y^T} x_i} \varphi(z) = \sum_{j=1}^n a_{ji} \frac{\partial \varphi}{\partial x_j}(az).$$

On the other hand, $L_y \varphi(z) = \varphi(az)$, with

$$az = (\sum_{j=1}^n a_{rj} z_r)_{1 \leq r \leq n},$$

so

$$(\partial_{x_i} L_y \varphi)(z) = \sum_{r=1}^n a_{ri} \partial_{x_r} \varphi(az).$$

We see that we do get the same result for $L_y \partial_{L_{y^T} x_i} \varphi(z)$ and $(\partial_{x_i} L_y \varphi)(z)$.

(d). Let $f, g \in V_m(\mathbb{R}^n)$ and $y \in \mathrm{O}(n)$. By (c), we have

$$\langle L_y f, L_y g \rangle = \partial_{\overline{L_y g}} L_y f = L_y \partial_{L_{y^T} L_y \overline{g}} f = L_y \partial_{\overline{g}} f.$$

As $\partial_{\overline{g}} f$ is a constant function, we have

$$L_y \partial_{\overline{g}} f = \partial_{\overline{g}} f = \langle f, g \rangle,$$

which is what we wanted.

(e). If $m \geq 1$, then $\Delta = 0$ on $V_m(\mathbb{R}^n)$, so $\mathscr{H}_m(\mathbb{R}^n) = \ker(\Delta) = V_m(\mathbb{R}^n)$.

(f). Note that $\Delta = \partial_{|x|^2}$. So, if $f \in V_m(\mathbb{R}^n)$ and $g \in V_{m-2}(\mathbb{R}^n)$, we have

$$\langle f, |x|^2 g \rangle = \partial_{|x|^2 \overline{g}} f = \partial_{\overline{g}}(\partial_{|x|^2} f) = \langle \Delta f, g \rangle.$$

In other words, the map $V_{m-2}(\mathbb{R}^n) \to V_m(\mathbb{R}^n)$, $g \longmapsto |x|^2 g$ is the adjoint of $\Delta : V_m(\mathbb{R}^n) \to V_{m-2}(\mathbb{R}^n)$, and so its image is the orthogonal of $\operatorname{Ker} \Delta = \mathscr{H}_m(\mathbb{R}^n)$.

(g). The first formula just follows from (f) by an easy induction. For the second formula, we note that, for every $k \in \{0, \dots, \lfloor \frac{m}{2} \rfloor\}$, the injective linear transformation $V_{m-2}(\mathbb{R}^n) \to V_m(\mathbb{R}^n)$, $g \longmapsto |x|^{2k} g$ is $\mathrm{O}(n)$-equivariant, because the function $|x|^{2k}$ is invariant by $\mathrm{O}(n)$.

(h). We will use polar coordinates on $\mathbb{R}^n$ : a point $z$ of $\mathbb{R}^n$ can be written as $z = rs$, with $r \in \mathbb{R}_{\geq 0}$ and $s \in S$, and $r$ and $s$ are uniquely determined if $z \neq 0$.

Let $f \in \mathscr{H}_m(\mathbb{R}^n)$ and $g \in \mathscr{H}_p(\mathbb{R}^n)$. Then, if $r \geq \mathbb{R}_{\geq 0}$ and $s \in S$, we have $f(rs) = r^m f(s)$ and $g(rs) = r^p g(s)$. By Green's second formula, we have

$$\int_B (f\Delta g - g\Delta f) d\lambda = c\int_S (f\frac{\partial g}{\partial r} - g\frac{\partial f}{\partial r}) d\mu,$$

where $B$ is the closed unit ball, $\lambda$ is Lebesgue measure on $\mathbb{R}^n$, $c$ is a positive constant and and $\mu$ is the measure on $S$ defined in 4(g). As $f$ and $g$ are in the kernel of $\Delta$, this gives

$$0 = c(p-m)\int_S f(s)g(s)d\mu(s).$$

If $m \neq p$, we get $\int_S f(s)g(s)d\mu(s) = 0$. So, for $m \neq p$, the subspaces $\mathscr{H}_m(\mathbb{R}^n)_{|S}$ and $\mathscr{H}_p(\mathbb{R}^n)_{|S}$ are orthogonal for the inner product of $L^2(S,\mu)$. In particular, if $f \in \bigoplus_{m\geq 0} \mathscr{H}_m(\mathbb{R}^n)$ is such that $f_{|S} = 0$, then, writing $f = \sum_{m\geq 0} f_m$ with $f_m \in \mathscr{H}_m(\mathbb{R}^n)$, we must have $f_{m|S} = 0$ for every $m \geq 0$. But $f_m$ is homogeneous of degree $m$, so $f_m(rs) = r^m f_m(s)$ for every $r \in \mathbb{R}_{\geq 0}$ and $s \in S$, so $f_{m|S} = 0$ implies $f_m = 0$.

(i). The existence follows from the first identity of (g) (because $|x|^2 = 1$ on $S$), and the uniqueness from (h).

□

**Exercise V.8.1.3.** Let $n \geq 2$, and embed $\mathrm{O}(n-1)$ into $\mathrm{O}(n)$ by using the map $x \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$. Let $G = \mathrm{SO}(n)$, and let $K$ be the image of $\mathrm{SO}(n-1)$ in $G$ by the embedding we just defined.

(a). Let $A$ be the subset of $\mathrm{SO}(n)$ consisting of matrices of the form

$$\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & I_{n-2} & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix},$$

with $\theta \in \mathbb{R}$.

Show that $A$ is a subgroup of $G$ and that we have $G = KAK$.

(b). Show that $(G,K)$ is a Gelfand pair. (You might want to use the involution $\theta$ of $G$ defined by $\theta(x) = JxJ$, where $J$ is the diagonal matrix with diagonal coefficients $-1, 1, \ldots, 1$.)

*Solution.*

(a). For every $\theta \in \mathbb{R}$, we write $A_\theta = \begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & I_{n-2} & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$. We have $A = \{A_\theta,\ \theta \in \mathbb{R}\}$. We check easily that $A_\theta A_{\theta'} = A_{\theta+\theta'}$, so $A$ is a subgroup of $G$.

Let $v_0 = (1, 0, \ldots, 0) \in S$. Then the action of $\mathrm{O}(n)$ on $\mathbb{R}^n$ preserves $S$ (and $\mathrm{O}(n)$ acts transitively on $S$), and $K$ is the stabilizer of $v_0$ in $\mathrm{O}(n)$. Let $x \in \mathrm{O}(n)$, and write $z = x \cdot v_0 = (z_1, \ldots, z_n)$. We can find $y \in K$ such that $y \cdot z = (z_1, 0, \ldots, 0, c)$, with $c^2 = z_2^2 + \ldots + z_n^2$, and then we can find $a \in A$ such that $a \cdot (y \cdot z) = (1, 0, \ldots, 0) = v_0$. Then we have $(ayx) \cdot v_0 = v_0$, so $ayx \in K$, and $x \in Ka^{-1}y^{-1} \subset KAK$.

(b). We want to apply proposition V.2.5 to $\theta$, where $\theta$ sends $x \in G$ to $JxJ$, with $J = \begin{pmatrix} -1 & 0 \\ 0 & I_{n-1} \end{pmatrix}$. Note that $J^2 = I_n$, so $J = J^{-1}$, so $\theta$ is a morphism of groups and an involution. It is also clear that $\theta(K) = K$. We need to check that $\theta(x) \in Kx^{-1}K$ for every $x \in G$. Let $x \in G$, and write $x = kak'$, with $k, k' \in K$ and $a \in A$. Then $\theta(x) = \theta(k)\theta(a)\theta(k')$ and $\theta(k), \theta(k') \in K$, and, if $a = A_\theta$, we have $\theta(a) = A_{-\theta} = a^{-1}$. So $\theta(x) = \theta(k)k'x^{-1}k\theta(k') \in Kx^{-1}K$.

□

**Exercise V.8.1.4.** We use the notation of problems V.8.1.1 and V.8.1.2, and the embedding $\mathrm{O}(n-1) \subset \mathrm{O}(n)$ defined in problem V.8.1.3.

(a). Show that we have a $\mathrm{O}(n-1)$-equivariant isomorphism

$$V_m(\mathbb{R}^n) \simeq \bigoplus_{k=0}^{m} V_{m-k}(\mathbb{R}^{n-1}).$$

(b). Show that we have a $\mathrm{O}(n-1)$-equivariant isomorphism

$$\mathscr{H}_m(\mathbb{R}^n) \simeq \bigoplus_{k=0}^{m} \mathscr{H}_{m-k}(\mathbb{R}^{n-1}).$$

(c). If $m \geq 2$, show that $\mathscr{H}_m(\mathbb{R}^2)$ is an irreducible representation of $\mathrm{O}(2)$, but that it is not irreducible as a representation of $\mathrm{SO}(2)$.

From now on, we assume that $n \geq 3$.

(a). If $m \geq 1$, show that $\mathscr{H}_m(\mathbb{R}^n)^{\mathrm{SO}(n)} = \{0\}$.

(b). Show that, for every $m \geq 0$, the space $\mathscr{H}_m(\mathbb{R}^n)^{\mathrm{SO}(n-1)}$ is 1-dimensional.

(c). Let $S \subset \mathbb{R}^n$ be the unit sphere, and let $v_0 = (1, 0, \ldots, 0) \in S$. Show that the map $\mathrm{SO}(n) \to S$, $x \longmapsto x \cdot v_0$ induces a homeomorphism $\mathrm{SO}(n)/\mathrm{SO}(n-1) \xrightarrow{\sim} S$.

(d). Show that the measure $\mu$ on $S$ defined in I.5.3.5(f) (using the normalized Haar measures on $\mathrm{SO}(n)$ and $\mathrm{SO}(n-1)$) is given by $\mu(E) = c\lambda(\{tx,\ t \in [0,1],\ x \in E\})$ for every Borel subset $E$ of $S$, where $\lambda$ is Lebesgue measure on $\mathbb{R}^n$ and $c^{-1}$ is the volume of the unit ball (for $\lambda$).

(e). By the previous question, we have the quasi-regular representation of $\mathrm{SO}(n)$ on $L^2(S)$, and it preserves the subspace of continuous functions. If $V \subset \mathscr{C}(S)$ is a nonzero finite-dimensional $\mathrm{SO}(n)$-stable subspace, show that $V^{\mathrm{SO}(n-1)} \neq \{0\}$. (Hint : Start with a function $f \in V$ such that $f(v_0) \neq 0$.)

(f). Show that the representation $\mathscr{H}_m(\mathbb{R}^n)$ of $\mathrm{SO}(n)$ is irreducible.

(g). Show that the representations $\mathscr{H}_m(\mathbb{R}^n)$ and $\mathscr{H}_{m'}(\mathbb{R}^n)$ of $\mathrm{SO}(n)$ are not equivalent if $m \neq m'$. (Hint : Compare the dimensions.)

(h). If $m \geq 2$, show that $\mathscr{H}_m(\mathbb{R}^n)$ is spanned by the functions $(z_1, \dots, z_n) \longmapsto (a_1 z_1 + \dots a_n z_n)^m$, with $a_1, \dots, a_n \in \mathbb{C}$ such that $a_1^2 + \dots + a_n^2 = 0$.

*Solution.*

(a). If $f \in V_m(\mathbb{R}^n)$, then we can write $f = \sum_{k=0}^m x_1^k f_k$, for uniquely determined $f_k \in V_{m-k}(\mathbb{R}^{n-1})$. As $\mathrm{O}(n-1) \subset \mathrm{O}(n)$ acts trivially on $x_1$, this gives an $\mathrm{O}(n-1)$-equivariant isomorphism $V_m(\mathbb{R}^n) \simeq \bigoplus_{k=0}^m V_{m-k}(\mathbb{R}^{n-1})$.

(b). In this proof, we will use the convention that $V_m(\mathbb{R}^n) = 0$ if $m < 0$. Fix $n$ and $m$. By V.8.1.2(f) and (g), we have an $\mathrm{O}(n)$-equivariant isomorphism $V_m(\mathbb{R}^n) \simeq \mathscr{H}_m(\mathbb{R}^n) \oplus V_{m-2}(\mathbb{R}^n)$. Using (a), we deduce from this an $\mathrm{O}(m-1)$-equivariant isomorphism

$$V_m(\mathbb{R}^n) \simeq \mathscr{H}_m(\mathbb{R}^n) \oplus \bigoplus_{k=0}^{m-2} V_{m-2-k}(\mathbb{R}^{n-1}).$$

On the other hand, applying (a) to $V_m(\mathbb{R}^n)$ gives an $\mathrm{O}(n-1)$-equivariant isomorphism $V_m(\mathbb{R}^n) \simeq \bigoplus_{k=0}^m V_{m-k}(\mathbb{R}^{n-1})$. Using V.8.1.2(f) or (g) on each summand, we get an $\mathrm{O}(n-1)$-equivariant isomorphism

$$\begin{aligned} V_m(\mathbb{R}^n) &\simeq \bigoplus_{k=0}^m (\mathscr{H}_{m-k}(\mathbb{R}^{n-1}) \oplus V_{m-2-k}(\mathbb{R}^{n-1})) \\ &= \left( \bigoplus_{k=0}^m \mathscr{H}_{m-k}(\mathbb{R}^{n-1}) \right) \oplus \left( \bigoplus_{k=0}^{m-2} V_{m-2-k}(\mathbb{R}^{n-1}) \right). \end{aligned}$$

Define representations $V_1$, $V_2$ and $V_3$ of $\mathrm{O}(n-1)$ by $V_1 = \mathscr{H}_m(\mathbb{R}^n)$, $V_2 = \bigoplus_{k=0}^m \mathscr{H}_{m-k}(\mathbb{R}^{n-1})$ and $V_3 = \bigoplus_{k=0}^{m-2} V_{m-2-k}(\mathbb{R}^{n-1})$. We have just seen that $V_1 \oplus V_3 \simeq V_2 \oplus V_3$, so $\chi_{V_1} + \chi_{V_3} = \chi_{V_2} + \chi_{V_3}$, so $\chi_{V_1} = \chi_{V_2}$. By corollary IV.5.10, this implies that $V_1$ and $V_2$ are equivalent.

(c). Note that $\mathrm{SO}(2)$ is a commutative group (it is isomorphic to $S^1$), so its irreducible representations are all 1-dimensional. On the other hand, by V.8.1.2(f) and V.8.1.2(a), we have

$$\dim \mathscr{H}_m(\mathbb{R}^2) = \dim V_m(\mathbb{R}^2) - \dim V_{m-2}(\mathbb{R}^2) = \binom{m+1}{m} - \binom{m-1}{m-2} = 2 > 1$$

if $m \geq 2$, so $\mathscr{H}_m(\mathbb{R}^n)$ cannot be an irreducible representation of $\mathrm{SO}(2)$.

If $m = 2$, then a basis of $\mathscr{H}_m(\mathbb{R}^2)$ is given by the functions $x_1^2 - x_2^2$ and $x_1x_2$, and they both span lines that are stable by the action of $\mathrm{O}(2)$, so $\mathscr{H}_2(\mathbb{R}^2)$ is not an irreducible representation of $\mathrm{O}(2)$.

Suppose that $m \geq 3$. As $\dim \mathscr{H}_m(\mathbb{R}^2) = 2$, if $\mathscr{H}_m(\mathbb{R}^2)$ is not an irreducible representation of $\mathrm{O}(2)$, we must have a nonzero $f \in \mathscr{H}_m(\mathbb{R}^2)$ such that $L_x f \in \mathbb{C}f$ for every $x \in \mathrm{O}(2)$. We identify $\mathbb{R}^2$ with the complex plane $\mathbb{C}$ in the usual way. Then $f(z)$, for $z \in \mathbb{C}$, can be written as $f(z) = \sum_{r=0}^m a_r z^r \overline{z}^{m-r}$, with $a_0, \ldots, a_m \in \mathbb{C}$. The action of $\mathrm{SO}(2)$ becomes the action of $S^1$ on $\mathbb{C}$ by multiplication, and the action of $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ corresponds to complex conjugation. By the assumption on $f$, for every" $u \in S^1$, the function $f(uz) = \sum_{r=0}^m a_r u^{2r-m} z^r \overline{z}^{m-r}$ is a multiple of $f$. This is only possible if there exists $r \in \{0, \ldots, m\}$ such that $a_s = 0$ for $s \neq r$. So we may assume that $f(z) = z^r \overline{z}^{m-r}$. The function $f(\overline{z}) = z^{m-r}\overline{z}^r$ is also a multiple of $f$, so we must have $m = 2r$ and $f = |x|^m$. Then $\Delta f = m(m-1)|x|^{m-2}$, which contradicts the fact that $\Delta f = 0$.

(d). Let $f \in V_m(\mathbb{R}^n)^{\mathrm{SO}(n)}$. As $f$ is invariant by $\mathrm{SO}(n)$, it is constant on the sphere with center 0, so $f(z) = f(\|z\| v_0)$ for every $z \in \mathbb{R}^n$. As $f$ is homogeneous of degree $m$, we get that $f(z) = \|z\|^m f(v_0)$, for every $z \in \mathbb{R}^n$. So $f$ is a polynomial if and only if $m$ is even. Also, we check easily that $\Delta f = m(m-1)|x|^{-2} f$, so $f \in \mathscr{H}_m(\mathbb{R}^n)$ if and only if $f = 0$ or $m = 0$.

(e). By (b), we have a $\mathrm{SO}(n-1)$-equivariant isomorphism $\mathscr{H}_m(\mathbb{R}^n) \simeq \bigoplus_{k=0}^m Hf_{m-k}(\mathbb{R}^{n-1})$. So, by (d), we get

$$\mathscr{H}_m(\mathbb{R}^n)^{\mathrm{SO}(n-1)} \simeq \mathscr{H}_0(\mathbb{R}^{n-1})^{\mathrm{SO}(n-1)} \simeq \mathbb{C}.$$

(f). Let us denote the map $\mathrm{SO}(n) \to S$, $x \longmapsto x \cdot v_0$ by $\varphi$. First, this map is clearly continuous, and it is surjective because $\mathrm{SO}(n)$ acts transitively on $S$. (If we have $v_1, v_1' \in S$, we want to find $x \in \mathrm{SO}(n)$ such that $x \cdot v_1 = v_1'$. We can complete $v_1$ and $v_1'$ to two orthonormal bases $(v_1, \ldots, v_n)$ and $(v_1', \ldots, v_n')$ of $\mathbb{R}^n$. The change of basis matrix between these two bases is in $\mathrm{O}(n)$. If it is in $\mathrm{SO}(n)$, we are done. Otherwise, the change of basis matrix between $(v_1, \ldots, v_n)$ and $(v_1', \ldots, v_{n-1}', -v_n')$ will be in $\mathrm{SO}(n)$.)

Also, the stabilizer of $v_0$ in $\mathrm{SO}(n)$ is the subgroup of $\mathrm{SO}(n)$ whose elements have $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ as their first column, and we see easily that this is $\mathrm{SO}(n-1)$. So $\varphi$ induces a continuous bijective map $\mathrm{SO}(n)/\mathrm{SO}(n-1) \xrightarrow{\sim} S$. As $\mathrm{SO}(n)/\mathrm{SO}(n-1)$ is compact, this map is a homeomorphism.

(g). Define a regular Borel measure $\nu$ on $S$ by

$$\nu(E) = c\lambda(\{tx,\ t \in [0,1],\ x \in E\}).$$

Define a linear functional $I : \mathscr{C}(\mathrm{SO}(n)) \to \mathbb{C}$ by

$$I(f) = \int_S f^{\mathrm{SO}(n-1)}(s) d\nu(s),$$

where

$$f^{\mathrm{SO}(n-1)}(x) = \int_{\mathrm{SO}(n-1)} f(xy) dy$$

(we are using the normalized Haar measure on $\mathrm{SO}(n-1)$) for every $s \in \mathrm{SO}(n)$; the function $f^{\mathrm{SO}(n-1)}$ is right invariant by $\mathrm{SO}(n-1)$, hence can be identified to a function on $S$ by (f).

This is a positive functional on $\mathscr{C}(\mathrm{SO}(n))$, so it comes from a regular Borel measure on $\mathrm{SO}(n)$, say $\rho$. We want to show that $\rho$ is the normalized Haar measure on $\mathrm{SO}(n)$.

Note that, if $f$ is the constant function 1, then $I(f) = 1$. So, to show that $\rho$ is the normalized Haar measure on $\mathrm{SO}(n)$, it suffices to show that it is left invariant. Let $f \in \mathscr{C}(\mathrm{SO}(n))$ and $y \in \mathrm{SO}(n)$. Then it follows immediately from the definition that $(L_y f)^{\mathrm{SO}(n-1)} = L_y(f^{\mathrm{SO}(n-1)})$, so we only need to show that the measure $\nu$ on $S$ is left invariant by the action of $\mathrm{SO}(n)$. But this follows immediately from the fact that Lebesgue measure $\lambda$ is left invariant by the action of $\mathrm{SO}(n)$ (which we can see using the change of variables formula).

(h). Let $V$ be as in the question. As $\mathrm{SO}(n)$ acts transitively on $S$ and $V$ is stable by $\mathrm{SO}(n)$, we can find $f \in V$ such that $f(v_0) \neq 0$. Let $(f_1, \dots, f_r)$ be a basis of $V$. As $V$ is stable by $\mathrm{SO}(n)$ and as the action of $\mathrm{SO}(n)$ on $V$ is continuous, we can find continuous functions $c_1, \dots, c_r : \mathrm{SO}(n) \to \mathbb{C}$ such that, for every $x \in \mathrm{SO}(n)$ and every $s \in S$, we have $f(x \cdot s) = \sum_{i=1}^r c_i(x) f_i(s)$. Define $\widetilde{f} : S \to \mathbb{C}$ by

$$\widetilde{f}(s) = \int_{\mathrm{SO}(n-1)} f(x \cdot s) dx.$$

Then $\widetilde{f} = \sum_{i=1}^r \left( \int_{\mathrm{SO}(n-1)} c_i(x) dx \right) f_i$, so $\widetilde{f} \in V$. Also, $\widetilde{f}$ is $\mathrm{SO}(n-1)$-invariant by construction. Finally, as $x \cdot v_0 = v_0$ for every $x \in \mathrm{SO}(n-1)$, we have $\widetilde{f}(v_0) = f(v_0) \neq 0$, so $\widetilde{f} \neq 0$.

(i). By V.8.1.2(h), restriction from $\mathbb{R}^n$ to $S$ is injective on $\mathscr{H}_m(\mathbb{R}^n)$, so $\mathscr{H}_m(\mathbb{R}^n)$ is irreducible as a representation of $\mathrm{SO}(n)$ if and only if $H_m = \mathscr{H}_m(\mathbb{R}^n)_{|S} \subset \mathscr{C}(S)$ is irreducible as a representation of $\mathrm{SO}(n)$. As $\mathrm{SO}(n)$ is compact, if $H_m$ is not irreducible, then we can write $H_m = V \oplus V'$ with $V$ and $V'$ nonzero $\mathrm{SO}(n)$-invariant subspaces of $H_m$. By (h), this implies that $\dim(H_m^{\mathrm{SO}(n)}) \geq 2$ and contradicts (d). So $H_m$ is irreducible.

(j). Let $d_m = \dim \mathscr{H}_m(\mathbb{R}^n)$. We will show that $d_{m+1} > d_m$ for every $m \in \mathbb{Z}_{\geq 0}$, which implies that $d_m \neq d_{m'}$ if $m \neq m'$, hence that $\mathscr{H}_m(\mathbb{R}^n)$ and $\mathscr{H}_{m'}(\mathbb{R}^n)$ are not equivalent.

If $m \leq 1$, then, by V.8.1.1(a) and V.8.1.2(e), we have $d_m = \dim V_m(\mathbb{R}^n) = \binom{m+n-1}{m}$. If $m \geq 2$, then, by V.8.1.1(a) and V.8.1.2(f), we have

$$\begin{aligned} d_m &= \dim V_m(\mathbb{R}^n) - \dim V_{m-2}(\mathbb{R}^n) \\ &= \binom{m+n-1}{m} - \binom{m+n-3}{m-2} \\ &= \frac{(m+n-3)!}{(m-2)!(n-1)!}\left(\frac{(m+n-1)(m+n-2)}{m(m-1)} - 1\right) \\ &= \frac{(2m+n-2)(m+n-3)!}{m!(n-2)!}. \end{aligned}$$

In particular, $d_0 = 1$, $d_1 = n$ and $d_2 = 2n-1$, so $d_2 > d_1 > d_0$. Let $m \geq 2$. Then

$$\begin{aligned} d_{m+1} - d_m &= \frac{(2(m+1)+n-2)(m+1+n-3)!}{(m+1)!(n-2)!} - \frac{(2m+n-2)(m+n-3)!}{m!(n-2)!} \\ &= \frac{(m+n-3)!}{m!(n-2)!}\left(\frac{(2m+n)(m+n-2)}{m+1} - (2m+n-2)\right) \\ &= \frac{(m+n-3)!}{m!(n-2)!}\frac{(2m+n)(m+n-2)-(2m+n-2)(m+1)}{m+1} \\ &> 0 \end{aligned}$$

(because $m+n-2 \geq m+1$ and $2m+n > 2m+n-2$).

(k). Let $a_1, \dots, a_n \in \mathbb{C}$, and consider $f = (a_1x_1 + \ldots + a_nx_n)^m \in V_m(\mathbb{R}^n)$. Then $\Delta f = m(m-1)(a_1^2 + \ldots + a_n^2)(a_1x_1 + \ldots + a_nx_n)^{m-2}$, so $f \in \mathscr{H}_m(\mathbb{R}^n)$ if and only if $a_1^2 + \ldots + a_n^2 = 0$. Let

$$W = \mathrm{Span}\{(a_1x_1 + \ldots + a_nx_n)^m,\ a_1, \dots, a_n \in \mathbb{C}, a_1^2 + \ldots + a_n^2 = 0\} \subset \mathscr{H}_m(\mathbb{R}^n).$$

As $W \neq 0$ and $\mathscr{H}_m(\mathbb{R}^n)$ is irreducible as a representation of $\mathrm{SO}(n)$, to show that $W = \mathscr{H}_m(\mathbb{R}^n)$, it suffices to show that $W$ is invariant by $\mathrm{SO}(m)$. Let $x \in \mathrm{SO}(n)$ and $a_1, \dots, a_n \in \mathbb{C}$, and let $f = (a_1x_1 + \ldots + a_nx_n)^m$. Write $(b_1, \dots, b_n) = (a_1, \dots, a_n)x^T$ (we see $(a_1, \dots, a_n)$ as a row vector). Then $b_1^2 + \ldots + b_n^2 = 0$ because $x \in \mathrm{O}(n)$, and $L_x f = (b_1x_1 + \ldots + b_nx_n)^m$, so $L_x f \in W$.

$\square$

**Exercise V.8.1.5.** We keep the notation of problems V.8.1.1-V.8.1.4, and we assume that $n \geq 3$.

(a). Show that the space $\sum_{m \geq 0} \mathscr{H}_m(\mathbb{R}^n)_{|S}$ is dense in $L^2(S)$ and that the sum is direct.

(b). Show that the subspaces $\mathscr{H}_m(\mathbb{R}^n)_{|S}$ and $\mathscr{H}_{m'}(\mathbb{R}^n)_{|S}$ of $L^2(S)$ are orthogonal (for the $L^2$ inner form) if $m \neq m'$.

(c). Show that every irreducible unitary representation of $\mathrm{SO}(n)$ having a nonzero $\mathrm{SO}(n-1)$-invariant vector is isomorphic to one of the $\mathscr{H}_m(\mathbb{R}^n)$.

*Solution.*

(a). By V.8.1.2(i), we have
$$\sum_{m\geq 0} \mathscr{H}_m(\mathbb{R}^n)_{|S} = \sum_{m\geq 0} V_m(\mathbb{R}^n)_{|S},$$
an the right hand side is dense in $\mathscr{C}(S)$ (hence in $L^2(S)$) by the Stone-Weierstrass theorem. Also, we have seen in the proof of V.8.1.2(h) that the spaces $\mathscr{H}_m(\mathbb{R}^n)_{|S}$ are pairwise orthogonal in $L^2(S)$, so they are in direct sum.

(b). See (a).

(c). Let $V$ be an irreducible unitary representation of $\mathrm{SO}(n)$ such that $V^{\mathrm{SO}(n-1)} \neq 0$. By theorem V.3.2.4, $V$ is a subrepresentation of $L^2(S)$. But we have seen that
$$L^2(S) = \overline{\bigoplus_{m\geq 0} \mathscr{H}_m(\mathbb{R}^n)_{|S}}$$
and that all these summands are irreducible, so $V$ is isomorphic to one of them.

□

**Exercise V.8.1.6.** We keep the notation of problems V.8.1.1-V.8.1.5. We say that a function $\varphi \in \mathscr{C}(S)$ is *zonal* if it is left invariant by $\mathrm{SO}(n-1)$. (As $S = \mathrm{SO}(n)/\mathrm{SO}(n-1)$, we can also see the function $\varphi$ as a bi-invariant function on $\mathrm{SO}(n)$.) Suppose that $n \geq 3$.

(a). Show that $\varphi \in \mathscr{C}(S)$ is zonal if and only if there exists a continuous function $f : [-1, 1] \to \mathbb{C}$ such that, for every $z = (z_1, \dots, z_n) \in S$, we have $\varphi(z) = f(z_1)$.

(b). Show that there exists $c \in \mathbb{R}_{>0}$ such that, for every zonal $\varphi \in \mathscr{C}(S)$, if we define $f : [-1, 1] \to \mathbb{C}$ as in (a), then
$$\int_S \varphi(z)d\mu(z) = c\int_{-1}^{1} f(t)(1-t^2)^{(n-3)/2}dt.$$
(Hint : You can try using spherical coordinates, as in `https://en.wikipedia.org/wiki/N-sphere#Spherical_coordinates`.)

(c). Let $m \geq 0$. If $t \in S$, let $f_t$ be the unique element of $\mathscr{H}_m(\mathbb{R}^n)$ such that, for every $g \in \mathscr{H}_m(\mathbb{R}^n)$, we have $\langle g, f_t\rangle = g(t)$. (Note that we are using the inner form of problem V.8.1.2.)

Show that the function $Z_m = f_{v_0|S}$ (where $v_0 = (1, 0, \dots, 0)$) is a zonal function.

(d). Let $f_m : [-1, 1] \to \mathbb{C}$ be the continuous function corresponding to $Z_m$ as in question (a). Show that $f_m$ is a polynomial function of degree $\leq m$.

(e). If $m \neq m'$, show that $\int_{-1}^{1} f_m(t)\overline{f_{m'}(t)}(1-t^2)^{(n-3)/2}dt = 0$.

(f). Show that the degree of $f_m$ is $m$.

(g). Show that $x \longmapsto \frac{1}{Z_m(v_0)} Z_m(x \cdot v_0)$ is a spherical function on $\mathrm{SO}(n)$, and that every spherical function is of this form.

The polynomials $\frac{1}{f_m(1)} f_m$ are called Gegenbauer polynomials (and also Legendre polynomials if $n = 3$).

We will now give a different formula for the spherical functions.

(h). Consider the function $h_m \in V_m(\mathbb{R}^n)$ defined by $h_m(z_1, \ldots, z_n) = (z_1 + iz_2)^m$. Show that $h_m \in \mathscr{H}_m(\mathbb{R}^n)$.

(i). Define a function $\psi_m : S \to \mathbb{C}$ by $\psi_m(z) = \int_{\mathrm{SO}(n-1)} h_m(k \cdot z)dk$. Show that $\psi_m$ is left invariant by $\mathrm{SO}(n-1)$, that $\psi_m \in \mathscr{H}_m(\mathbb{R}^n)_{|S}$ and that $\psi_m(v_0) = 1$.

(j). Show that every spherical function on $\mathrm{SO}(n)$ is of the form $x \longmapsto \psi_m(x \cdot v_0)$, for a unique $m \geq 0$.

We can calculate the integral defining $\psi_m$, and we get

$$\psi_m(\cos\varphi, z_2, \ldots, z_n) = \frac{\Gamma(\frac{n-1}{2})}{\sqrt{\pi}\Gamma(\frac{n-2}{2})} \int_0^\pi (\cos\varphi + i \sin\varphi\cos\theta)^m \sin^{n-3}\theta d\theta.$$

[5]

*Solution.*

(a). If there exists a continuous function $f : [-1, 1] \to \mathbb{C}$ such that $\varphi(z_1, \ldots, z_n) = f(z_1)$, then $\varphi$ is clearly zonal.

Conversely, suppose that $\varphi$ is zonal, and define $f : [-1, 1] \to \mathbb{C}$ by

$$(z_1) = \varphi(z_1, 0, \ldots, 0, \sqrt{1 - z_1^2}).$$

Then $f$ is clearly continuous. Let $s = (z_1, \ldots, z_n) \in S$. Then there exists $x \in \mathrm{SO}(n-1)$ such that $x \cdot s = (z_1, 0, \ldots, 0, \sqrt{1 - z_1^2})$ (we are using the fact that $\mathrm{SO}(n-1)$ acts transitively on any sphere in $\mathbb{R}^{n-1}$). As $\varphi$ is zonal, we have $\varphi(s) = f(z_1)$.

[5] Reference.

(b). We use spherical coordinates on $\mathbb{R}^n$. That is, given $(z_1, \dots, z_n) \in \mathbb{R}^n$, we write

$$\begin{aligned} z_1 &= r\cos\phi_1 \\ z_2 &= r\sin\phi_1\cos\phi_2 \\ &\dots \\ z_{n-1} &= r\sin\phi_1\sin\phi_2\dots\sin\phi_{n-2}\cos\phi_{n-1} \\ z_n &= r\sin\phi_1\sin\phi_2\dots\sin\phi_{n-2}\sin\phi_{n-1}, \end{aligned}$$

with $r = \sqrt{z_1^2 + \dots + z_n^2} \in \mathbb{R}_{\geq 0}$, $\phi_1, \dots, \phi_{n-2} \in [0, \pi]$ and $\phi_{n-1} \in [0, 2\pi)$ ($\phi_1, \dots, \phi_{n-1}$ are not uniquely determined in general, but they are if for example $z_1, \dots, z_n$ are all nonzero). If $dz$ is Lebesgue measure on $\mathbb{R}^n$, then we have

$$dz = r^{n-1}\sin^{n-2}\phi_1\sin^{n-3}\phi_2\dots\sin\phi_{n-2}drd\phi_1\dots d\phi_{n-1}.$$

Let $\varphi \in \mathscr{C}(S)$ be zonal. Up to a positive real constant, $\int_S \varphi(s)d\mu(s)$ is equal to $\int_{B-\{0\}}\psi(z)dz$, where $B$ is the closed unit ball and $\psi(z) = \varphi(\|z\|^{-1}z)$ for $z \neq 0$. This is equal to the product of $\int_0^1 r^{n-1}dr$ (another positive real constant) and of

$$\int_0^\pi \dots \int_0^\pi \int_0^{2\pi} \varphi(\cos\phi_1, \sin\phi_1\cos\phi_2, \dots, \sin\phi_1\dots\sin\phi_{n-2}\sin\phi_{n-1})$$
$$\sin^{n-2}\phi_1\sin^{n-3}\phi_2\dots\sin\phi_{n-2}d\phi_1\dots d\phi_{n-1}.$$

As $\varphi$ is zonal, the big integral above is equal to

$$\int_0^\pi \dots \int_0^\pi \int_0^{2\pi} f(\cos\phi_1)\sin^{n-2}\phi_1\sin^{n-3}\phi_2\dots\sin\phi_{n-2}d\phi_1\dots d\phi_{n-1}.$$

Up to the constant

$$\int_0^\pi \dots \int_0^\pi \int_0^{2\pi} \sin^{n-3}\phi_2\dots\sin\phi_{n-2}d\phi_2\dots d\phi_{n-1}$$

(which has to be positive because it calculates the integral of the constant function $1$ up to a positive constant), this is equal to

$$\int_0^\pi f(\cos\phi_1)\sin^{n-2}\phi_1 d\phi_1.$$

Finally, we use the change of variable $t = \cos\phi_1$. We have $dr = -\sin\phi_1 d\phi_1$, so

$$\begin{aligned} \int_0^\pi f(\cos\phi_1)\sin^{n-2}\phi_1 d\phi_1 &= \int_1^{-1} f(t)(-\sqrt{1-t^2}^{n-3})dt \\ &= \int_{-1}^1 f(1)(1-t^2)^{(n-3)/2}dt. \end{aligned}$$

(c). Let $y \in \mathrm{SO}(n-1)$. By definition of $f_{v_0}$, we have, for every $g \in \mathscr{H}_m(\mathbb{R}^n)$,

$$\langle g, L_y f_{v_0} \rangle = \langle L_{y^{-1}} g, f_{v_0} \rangle = L_y g(v_0) = g(y^{-1} v_0) = g(v_0) = \langle g, f_{v_0} \rangle$$

(because $\mathrm{SO}(n-1)$ is the stabilizer of $v_0$ in $\mathrm{SO}(n)$). So $f_{v_0} - L_y f_{v_0}$ is orthogonal to every element of $\mathscr{H}_m(\mathbb{R}^n)$, which implies that $f_{v_0} - L_y f_{v_0} = 0$, i.e. that $f_{v_0} = L_y f_{v_0}$. So $Z_m$ is zonal.

(d). The function $Z_m$ is the restriction of $f_{v_0}$, which is an element of $\mathscr{H}_m(\mathbb{R}^n)$, and in particular a polynomial function of degree $m$. As $f_m$ is defined by $f_m(t) = Z_m(t, 0, \dots, 0, \sqrt{1-t^2})$, we can write

$$f_m(t) = \sum_{k=0}^{m} c_k t^k (1-t^2)^{(m-k)/2},$$

with $c_0, \dots, c_m \in \mathbb{C}$. But we also have $f_m(t) = Z_m(t, 0, \dots, 0, -\sqrt{1-t^2})$, so

$$\sum_{k=0}^{m} c_k t^k (1-t^2)^{(m-k)/2} = \sum_{k=0}^{m} (-1)^{m-k} c_k t^k (1-t^2)^{(m-k)/2}.$$

This forces $c_k$ to be $0$ unless $m-k$ is even, and so $f(t)$ is indeed polynomial of degree $\leq m$ in $t$.

(e). The function $s \longmapsto Z_m(s)\overline{Z_{m'}(s)}$ is zonal, so we have

$$\int_S Z_m(s)\overline{Z_{m'}(s)} d\mu(s) = c \int_{-1}^{1} f_m(t)\overline{f_{m'}(t)}(1-t^2)^{(n-3)/2} dt$$

by (b). By V.8.1.5(b), the left hand side is $0$.

(f). For every $m \geq 0$, the function $Z_m$ is nonzero by definition (and because there exist functions $f \in \mathscr{H}_m(\mathbb{R}^n)$ such that $g(v_0) \neq 0$, see the proof of V.8.1.4(h)), so $f_m \neq 0$ by V.8.1.2(h). By (e), the functions $(f_m)_{m \geq 0}$ form an orthogonal family in $L^2([-1,1], (1-t^2)^{(n-3)/2} dt)$, so they also form a linearly independent family. Fix $m \geq 0$. The space $P_m$ of polynomials of degree $\leq m$ is of dimension $m+1$ and contains the linearly independent family $(f_0, \dots, f_m)$, so this family is a basis of $P_m$. But $f_0, \dots, f_{m-1}$ are of degree $\leq m-1$, so $f_m$ has to be of degree $m$.

(g). By corollary V.7.2, if $Z$ is the set of spherical functions on $\mathrm{SO}(n)$, then we have

$$L^2(S) = \widehat{\bigoplus_{\varphi \in Z} V_\varphi}$$

and $\varphi$ generates $V_\varphi^{\mathrm{SO}(n-1)}$. So, using problem V.8.1.5, we see that the spherical functions are exactly the generators of the spaces $(\mathscr{H}_m(\mathbb{R}^n)_{|S})^{\mathrm{SO}(n-1)}$ that send $v_0$ to 1.

For every $m \geq 0$, the function $Z_m \in \mathscr{H}_m(\mathbb{R}^n)_{|S}$ is invariant by $\mathrm{SO}(n-3)$, so it generates the space of $\mathrm{SO}(n-1)$-invariant vectors in $\mathscr{H}_m(\mathbb{R}^n)_{|S}$ and has a multiple which is a spherical functions. Because a spherical function must send $v_0$ to 1, this multiple is $x \longmapsto \frac{1}{Z_m(v_0)} Z_m(x \cdot v_0)$.

(h). This follows from V.8.1.4(k). It is also easy to prove it directly.

(i). This is exactly the same construction as in the proof of V.8.1.4(h) (with $V = \mathscr{H}_m(\mathbb{R}^n)_{|S}$). The same proof shows that $\psi_m \in \mathscr{H}_m(\mathbb{R}^n)_{|S}$, that $\psi_m$ is left invariant by $\mathrm{SO}(n-1)$ and that $\psi_m(v_0) = f_m(v_0) = 1$.

(j). Same idea as in the proof of (g) : we have one spherical function in each $\mathscr{H}_m(\mathbb{R}^n)_{|S}$, and it is the unique $\mathrm{SO}(n-1)$-invariant element of this space that sends $v_0$ to $1$. By (i), the function $\psi_m$ satisfies all the required properties.

□

## V.8.2 The Gelfand pair $(\mathfrak{S}_n, \mathfrak{S}_r \times \mathfrak{S}_{n-r})$

The goal of this series of exercises, which were extracted from sections 5.1, 6.1 and 6.2 of [7], is to study the Gelfand pair $(\mathfrak{S}_n, \mathfrak{S}_r \times \mathfrak{S}_{n-r})$. We will embed $\mathfrak{S}_r \times \mathfrak{S}_{n-r}$ in $\mathfrak{S}_n$ in the following way : If $\sigma \in \mathfrak{S}_r$ and $\tau\, \mathfrak{S}_{n-r}$, then $\sigma \times \tau \in \mathfrak{S}_n$ is given by

$$(\sigma \times \tau)(i) = \begin{cases} \sigma(i) & \text{if } 1 \leq i \leq r \\ \tau(i-r) + r & \text{if } r+1 \leq i \leq n. \end{cases}$$

If $E$ is a finite set, we will denote by $L(E)$ the space of functions $f : E \to \mathbb{C}$, with the $L^2$ inner product given by $\langle f, f' \rangle = \sum_{x \in E} f(x)\overline{f'(x)}$.

**Exercise V.8.2.1.** In this problem, we fix a finite group $G$ acting transitively (on the left) on a set $E$. Let $x_0 \in E$, and let $K \subset G$ be the stabilizer of $x_0$.

(a). Show that the following conditions are equivalent :

  (i) For all $x, y \in E$, there exists $g \in G$ such that $g \cdot (x, y) = (y, x)$.

  (ii) For every $g \in G$, we have $g^{-1} \in KgK$.

(b). If the conditions of (a) are satisfied, show that $(G, K)$ is a Gelfand pair.

We now assume that there is a metric $d : E \times E \to \mathbb{R}_{\geq 0}$, and that the group $G$ acts by isometries. Suppose that the action of $G$ on $E$ is *distance-transitive*, that is : for all $(x, y), (x', y') \in E \times E$ such that $d(x, y) = d(x', y')$, there exists $g \in G$ such that $g \cdot (x, y) = (x', y')$.

(c). Show that $(G, K)$ is a Gelfand pair.

(d). Show that the orbits of $K$ on $E$ are the spheres $\{x \in E | d(x, x_0) = j\}$, for $j \in \mathbb{R}_{\geq 0}$.

(e). Let $\Omega_r$ be the set of cardinality $r$ subsets of $\{1, \ldots, n\}$. Show that the formula $d(A, B) = r - |A \cap B|$ defines a metric on $\Omega_r$.

(f). Show that $(\mathfrak{S}_n, \mathfrak{S}_r \times \mathfrak{S}_{n-r})$ is a Gelfand pair.

*Solution.*

(a). Suppose that (i) holds. Let $g \in G$. By (i), there exists $h \in G$ such that $h \cdot (K, gK) = (gK, K)$. Then the equality of the first entries gives $g^{-1}h \in K$, and the equality of the second entries gives $g^{-1}hg \in g^{-1}K$, hence $g \in (g^{-1}h)^{-1}g^{-1}K \subset Kg^{-1}K$.

Suppose that (ii) holds. Let $g, h \in G$. By (i), we can find $k_1, k_2 \in K$ such that $g^{-1}h = k_1h^{-1}gk_2$, and then

$$\begin{aligned}(gK, hK) = g \cdot (K, g^{-1}hK) = g \cdot (K, k_1h^{-1}gK) &= gk_1^{-1} \cdot (K, h^{-1}gK) \\ &= gk_1^{-1}h^{-1} \cdot (hK, gK).\end{aligned}$$

(b). This follows from proposition V.2.5, taking $\theta = \mathrm{id}_G$.

(c). Let $x, y \in X$. Then $d(y, x) = d(x, y)$, so there exists $g \in G$ such that $g \cdot (x, y) = (y, x)$. In other words, condition (i) of (a) is satisfied, so condition (ii) is also satisfied. By (b), this implies that $(G, K)$ is a Gelfand pair.

(d). Write $S_j = \{x \in X | d(x, x_0) = j\}$, for $j \in \mathbb{Z}_{\geq 0}$. As $G$ acts by isometries on $X$ and $K$ fixes $x_0$, the sets $S_j$ are stable by $K$. To show that they are the orbits of $K$ on $X$, we need to show that $K$ acts transitively on each nonempty $S_j$. So let $j \geq 0$, and suppose that we have $x, y \in S_j$. Then $d(x_0, x) = d(x_0, y) = j$, so, by the hypothesis, there exists $g \in G$ such that $g \cdot (x_0, x) = (x_0, y)$. The fact that $g \cdot x_0 = x_0$ implies that $g \in K$, so $x$ and $y$ are in the same $K$-orbit.

(e). We clearly have $d(A, B) = d(B, A)$ for all $A, B \in \Omega_r$. Let $A, B, C \in \Omega_r$. First, if $d(A, B) = 0$, then $|A \cap B| = r = |A| = |B|$, so $A \cap B = A$ and $A \cap B = B$, and so $A = B$. Let's prove the triangle inequality. We have

$$|A \cap B| + |B \cap C| = |(A \cap B) \cup (B \cap C)| + |A \cap B \cap C| \leq |B| + |A \cap C| = r + |A \cap C|,$$

so

$$d(A, C) = r - |A \cap C| \leq 2r - |A \cap B| - |B \cap C| = d(A, B) + d(B, C).$$

(f). We make $\mathfrak{S}_n$ act by $\Omega_r$ by $\sigma \cdot A = \sigma(A)$. This action is transitive, and $\mathfrak{S}_r \times \mathfrak{S}_{n-r}$ is the stabilizer of $\{1, \ldots, r\}$. Also, it is clear that $\mathfrak{S}_n$ acts by isometries on $\Omega_r$. So, by (c), we just need to check that the action is distance-transitive. Let $A, B, A', B' \in \Omega_r$ such that $d(A, B) = d(A', B')$, i.e. $|A \cap B| = |A' \cap B'|$. Choose a bijection $\varphi : A \overset{\sim}{\to} A'$ that sends the subset $A \cap B$ of $A$ onto $A' \cap B'$; this is possible because $|A \cap B| = |A' \cap B'|$. Choose a bijection $\psi : B - (A \cap B) \overset{\sim}{\to} B' - (A' \cap B')$; this is also possible, because $|B - (A \cap B)| = r - |A \cap B| = |B' - (A' \cap B')|$. Putting $\varphi$ and $\psi$ together gives a bijection $A \cup B \overset{\sim}{\to} A' \cup B'$ that sends $A$ to $A'$ and $B$ to $B'$, and any extension of this to an element $\sigma$ of $\mathfrak{S}_n$ will satisfy $\sigma \cdot (A, B) = (A', B')$.

$\square$

**Exercise V.8.2.2.** Let $(\Omega_r, d)$ be the finite metric space of question V.8.2.1(e). Let $N$ be the *diameter* of $\Omega_r$, that is,

$$N = \max\{d(A, B),\ A, B \in \Omega_r\}.$$

For $i \in \{0, \dots, N\}$, we define a linear operator $\Delta_i : L(\Omega_r) \to L(\Omega_r)$ by

$$\Delta_i f(A) = \sum_{B \in \Omega_r,\ d(A,B)=i} f(B),$$

for every $f \in L(\Omega_r)$. We also denote by $\mathbb{A}_f$ the subalgebra of $\mathrm{End}(L(\Omega_r))$ generated by $\Delta_0, \dots, \Delta_N$.

(a). Show that $N = \min(r, n - r)$.

(b). Show that there exist integers $b_0, \dots, b_N, c_0, c_1, \dots, c_N$ such that, for every $i$ and all $A, B \in \Omega_r$ such that $d(A, B) = i$, we have

$$|\{C \in \Omega_r | d(A, C) = 1 \text{ and } d(B, C) = i + 1\}| = b_i$$

and

$$|\{C \in \Omega_r | d(A, C) = 1 \text{ and } d(B, C) = i - 1\}| = c_i.$$

(Of course, $c_0 = 0$ and $c_1 = 1$.) [6]

(c). Show that $c_2, \dots, c_N > 0$.

(d). If $i \in \{1, \dots, N\}$, show that

$$\Delta_i \Delta_1 = b_{i-1}\Delta_{i-1} + (b_0 - b_i - c_i)\Delta_i + c_{i+1}\Delta_{i+1},$$

with the convention that $\Delta_{N+1} = 0$.

(e). Show that there exist polynomials $p_0, \dots, p_N \in \mathbb{R}[t]$ such that $\deg(p_i) = i$ and $\Delta_i = p(\Delta_1)$.

(f). Show that $\mathbb{A}_f$ is the subalgebra of $\mathrm{End}(L(\Omega_r))$ generated by $\Delta_1$.

(g). Show that $\mathbb{A}_f$ is spanned as a $\mathbb{C}$-vector space by $\Delta_0, \dots, \Delta_N$.

(h). Show that $\dim_{\mathbb{C}} \mathbb{A}_f = N + 1$.

(i). Show that the endormorphism $\Delta_1$ of $L(\Omega_r)$ is self-adjoint.

(j). Show that we have a decomposition into pairwise orthogonal subspaces $L(\Omega_r) = \bigoplus_{i=0}^{N} V_i$, where $V_0, \dots, V_N$ are the eigenspaces of $\Delta_1$. (Hint : problem II.5.2.)

*Solution.*

[6] In other words, the graph with set of vertices $\Omega_r$ and an edge between any $A, B \in \Omega_r$ such that $d(A, B) = 1$ is *distance-regular*, see definition 5.1.1 of [7] .

(a). Note that $d(A,B) \leq r$ for all $A, B \in \Omega_r$ by definition of $d$, so $N \leq r$. Also, for all $A, B \in \Omega_r$, we have

$$d(A,B) = r - |A \cap B| = r - (|A| + |B| - |A \cup B|) = |A \cup B| - r \leq n - r,$$

so $N \leq n - r$, and $N \leq \min(r, n - r)$.

Now take $A = \{1, \ldots, r\}$ and $B = \{n - r + 1, \ldots, n\}$. Then $A, B \in \Omega_r$, and $|A \cap B| = \max(0, 2r - n)$. So $N \geq d(A,B) = r - \max(0, 2r - n) = \min(r, n - r)$.

(b). Fix $i \in \{0, \ldots, N\}$. For all $A, B \in \Omega_r$ such that $d(A,B) = i$, let

$$X_i(A,B) = \{C \in \Omega_r | d(A,C) = 1 \text{ and } d(B,C) = i + 1\}$$

and

$$Y_i(A,B) = \{C \in \Omega_r | d(A,C) = 1 \text{ and } d(B,C) = i - 1\}.$$

If $\sigma \in \mathfrak{S}_n$ is such that $\sigma(A,B) = (A', B')$, then $\sigma$ induces bijections $X_i(A,B) \xrightarrow{\sim} X_i(A', B')$ and $Y_i(A,B) \xrightarrow{\sim} Y_i(A', B')$, because $\mathfrak{S}_n$ acts on $\Omega_r$ by isometries. So the statement follows from the fact that the action of $\mathfrak{S}_n$ on $\Omega_r$ is distance-transitive, which we showed in the proof of V.8.2.1(f).

(c). Let $i \in \{2, \ldots, N\}$. Take $A = \{1, \ldots, r\}$ and $B = \{i + 1, i + 2, \ldots, i + r\}$. (Note that $i + r \leq N + r \leq n$ by (a).) We need to show that there exists at least one $C \in \Omega_r$ such that $d(A,C) = 1$ (i.e. $|A \cap C| = r - 1$) and $d(B,C) = i - 1$ (i.e. $|B \cap C| = r - i + 1$). This holds for $C = \{2, 3, \ldots, r + 1\}$.

(d). Let $f \in L(\Omega_r)$ and $A \in \Omega_r$. Then we have

$$\Delta_i \Delta_1 f(A) = \sum_{B \in \Omega_r, d(A,B) = i} \; \sum_{C \in \Omega_r, d(B,C) = 1} f(C).$$

Let $C \in \Omega_r$. If there exists $B \in \Omega_r$ such that $d(A,B) = i$ and $d(B,C) = 1$, then we must have $i - 1 \leq d(A,C) \leq i + 1$ by the triangle inequality.

Suppose that $d(A,C) = i + 1$. Then

$$\{B \in \Omega_r | d(A,B) = i \text{ and } d(B,C) = 1\} = Y_{i+1}(C, A)$$

(with the notation of the proof of (b)). Suppose that $d(A,C) = i - 1$. Then

$$\{B \in \Omega_r | d(A,B) = i \text{ and } d(B,C) = 1\} = X_{i-1}(C, A).$$

Finally, suppose that $d(A,C) = i$. Consider the set

$$\{B \in \Omega_r | d(A,B) = i \text{ and } d(B,C) = 1\} \cup \{B \in \Omega_r | d(A,B) = i + 1 \text{ and } d(B,C) = 1\}$$
$$\cup \{B \in \Omega_r | d(A,B) = i - 1 \text{ and } d(B,C) = 1\}.$$

The union is clearly disjoint. We are trying to calculate the cardinality of the first set, the second set is $X_i(C,A)$ and the third set is $Y_i(C,A)$. Also, by the triangle inequality, the union is simply

$$\{B \in \Omega_r | d(B,C) = 1\} = X_0(C,C).$$

So we get

$$|\{B \in \Omega_r | d(A,B) = i \text{ and } d(B,C) = 1\}| + b_i + c_i = b_).$$

Finally, we see that

$$\begin{aligned}\Delta_i \delta_1 f(A) &= c_{i+1} \sum_{C,\ d(A,C)=i+1} f(C) b_{i-1} \sum_{C,\ d(A,C)=i-1} f(C) + (b_0 - b_i - c_i) \sum_{C,\ d(A,C)=i} f(C) \\ &= c_{i+1}\Delta_{i+1} f(A) + b_{i-1}\Delta_{i-1} f(A) + (b_0 - b_i - c_i)\Delta_i f(A).\end{aligned}$$

(e). We prove the statement by induction on $i$. It is obvious $i = 0$ (note that $\Delta_0 = \mathrm{id}$, so we take $p_0 = 1$) and for $i = 1$ (take $p_1(t) = t$). Suppose the result known up to some $i \geq 1$, and let's prove it for $i + 1$. By (c) and (d), we have

$$\Delta_{i+1} = c_{i+1}^{-1}(\Delta_i \Delta_1 - b_{i-1}\Delta_{i-1} - (b_0 - b_i - c_i)\Delta_i),$$

so $\Delta_{i+1} = p_{i+1}(\Delta_1)$, with

$$p_{i+1}(t) = c_{i+1}^{-1}(t p_i(t) - p_{i-1}(t) - (b_0 - b_i - c_i) p_i(t)).$$

It is also clear that $\deg(p_{i+1}(t)) = i + 1$.

(f). Let $\mathbb{A}'_f$ be the subalgebra of $\mathrm{End}(L(\Omega_r))$ generated by $\Delta_1$. Then $\mathbb{A}'_f \subset \mathbb{A}_f$ by definition of $\mathbb{A}_f$. By (e), we have $\Delta_0, \ldots, \Delta_N \in \mathbb{A}'_f$, and so $\mathbb{A}_f \subset \mathbb{A}'_f$.

(g). We show by induction on $i \geq 0$ that $\Delta_1^i \in \mathrm{Span}(\Delta_0, \Delta_1, \ldots, \Delta_i)$. (The conclusion will follow by (f).) The assertion is clear for $i = 0$ and $i = 1$. Suppose that holds up to $i \geq 1$, and let's prove it for $i + 1$. By (e), there exist a nonzero $c \in \mathbb{R}$ and $c_0, \ldots, c_i \in \mathbb{R}$ such that $\Delta_{i+1} = a\Delta_1^{i+1} + \sum_{j=0}^{i} a_j \Delta_1^j$. As $\Delta_1^j \in \mathrm{Span}(\Delta_0, \ldots, \Delta_j)$ for every $j \in \{0, \ldots, i\}$ by the induction, we deduce that $\Delta_1^{i+1} \in \mathrm{Span}(\Delta_0, \ldots, \Delta_{i+1})$.

(h). We know that $\mathbb{A}_f = \mathrm{Span}(\Delta_0, \ldots, \Delta_N)$ by (g), so we must show that the family $(\Delta_0, \ldots . \Delta_N)$ is linearly independent. Let $c_0, \ldots, c_N \in \mathbb{C}$. If $A, B \in \Omega_r$, and if we denote by $\delta_A$ the indicator function of $\{A\}$, then $\Delta_i \delta_A(B) \neq 0$ only if $d(A,B) = i$, and we have

$$\sum_{i=0}^{N} c_i \Delta_i \delta_A(B) = c_{d(A,B)}.$$

As there are couples $(A,B) \in \Omega_r^2$ such that $d(A,B) = i$ for every $i \in \{0, \ldots, N\}$, we conclude that, if $\sum_{i=0}^{N} c_i \Delta_i = 0$, then $c_0 = \ldots = c_N = 0$.

(i). Let $f, g \in L(\Omega_r)$. Then

$$\begin{aligned}\langle f, \Delta_1 g\rangle &= \sum_{A\in\Omega_r} f(A)\overline{(\Delta_1 g)(A)}\\ &= \sum_{A\in\Omega_r} f(A) \sum_{B\in\Omega_r,\ d(A,B)=1} \overline{g(B)}\\ &= \sum_{A,B\in\Omega_r,\ d(A,B)=1} f(A)\overline{g(B)}\\ &= \sum_{B\in\Omega_r} (\Delta_1 f)(B)\overline{g(B)}\\ &= \langle \Delta_1 f, g\rangle.\end{aligned}$$

(j). As $\Delta_1$ is self-adjoint, the spectral theorem says that it is diagonalizable and that its eigenspaces are pairwise orthogonal. So the only thing we have to show is that there are $N+1$ eigenspaces. By II.5.2(b), we know that the subalgebra of $\mathrm{End}(L(\Omega_r))$ generated by $\Delta_1$, i.e. $\mathbb{A}_f$ (see (f)), is reduced. By II.5.2(c), we know that the number of eigenspaces of $\mathbb{A}_f$, i.e. of $\Delta_1$, is $\dim(\mathbb{A}_f)$, and by (h), we know that $\dim(\mathbb{A}_f) = N+1$.

$\square$

**Exercise V.8.2.3.** We use the notation of problem V.8.2.2. Note that we have an action of $G := \mathfrak{S}_n$ on $\Omega_r$, and that the stabilizer of $\{1, \ldots, r\}$ is $K := \mathfrak{S}_r \times \mathfrak{S}_{n-r}$. Let $M^{n-r,r} = L(\Omega_r)$, seen as a representation of $\mathfrak{S}_n$ via the quasi-regular representation (that is, if $g \in G$, $f \in M^{n-r,n}$ and $A \in \Omega_r$, we have $(g \cdot f)(A) = f(g^{-1}A)$).

We define $d : M^{n-r,r} \to M^{n-r+1,r-1}$ and $d^* : M^{n-r+1,r-1} \to M^{n-r,r}$ by

$$(df)(A) = \sum_{B\in\Omega_r|A\subset B} f(B)$$

and

$$(d^* f)(B) = \sum_{A\in\Omega_r|A\subset B} f(A).$$

(If $r = 0$, we take $d = 0$ and $d^* = 0$.)

We also denote by $\Delta$ the operator $\Delta_1$ of problem V.8.2.2; that is, for every $f \in M^{n-r,r}$, the function $\Delta f \in M^{n-r,r}$ is defined by

$$(\Delta f)(A) = \sum_{B\in\Omega_r|d(A,B)=1} f(B).$$

[7] Note that the functions $d$, $d^*$ and $\Delta$ are defined for every $r$; we will not indicate $r$ in the notation, it should be clear from the context.

[7] This is closely related to the *discrete Laplace operator*. In fact, the most common definition of the discrete Laplace operator on $M^{n-r,r}$ would be $\frac{1}{r}\Delta - \mathrm{id}$.

Finally, if $a \in \mathbb{C}$ and $i \in \mathbb{Z}_{\geq 0}$, we write

$$(a)_i = a(a+1)\dots(a+i-1).$$

For example, we have $(1)_n = n!$ and $\binom{n}{k} = \frac{(n-k+1)_k}{k!}$.

(a). Show that $A \longmapsto \{1,\dots,n\} - A$ induces a $G$-equivariant isomorphism $M^{r,n-r} \xrightarrow{\sim} M^{n-r,r}$.

(b). Show that $d$ and $\Delta$ are $G$-equivariant.

(c). Show that $d^*$ is the adjoint of $d$.

(d). If $f \in M^{n-r,r}$, show that

$$dd^*f = \Delta f + (n-r)f \quad \text{and} \quad d^*df = \Delta f + rf.$$

(e). Let $f \in M^{n-r,r}$ and $1 \leq p \leq q \leq n-r$. Show that

$$d(d^*)^q f = (d^*)^q df + q(n-2r-q+1)(d^*)^{q-1}f.$$

If moreover $df = 0$, show that

$$d^p(d^*)^q f = (q-p+1)_p(n-2r-q+1)_p(d^*)^{q-p}f.$$

Suppose that $0 \leq r \leq n/2$. If $r > 0$, set $S^{n-r,r} = \operatorname{Ker}(d : M^{n-r,r} \to M^{n-r+1,r-1})$; if $r = 0$, set $S^{n-r,r} = M^{n-r,r}$. This is a $G$-stable subspace of $M^{n-r,r}$.

(a). If $0 \leq m \leq n$ and $0 \leq r \leq \min(m, n-m)$, show that $(d^*)^{m-r} : S^{n-r,r} \to M^{n-m,m}$ is injective. (Hint : calculate $\|(d^*)^{m-r}f\|_2^2$).

(b). Under the hypothesis of (f), show that $(d^*)^{m-r}(S^{n-r,r})$ is contained in the eigenspace of $\Delta$ for the eigenvalue $m(n-m) - r(n-r+1)$.

(c). Show that the orthogonal of $S^{n-m,m}$ in $M^{n-m,m}$ is $d^*(M^{n-m+1,m-1})$, if $1 \leq m \leq n/2$.

(d). Show that $S^{n-r,r} \neq 0$ for every $r$ such that $0 \leq r \leq n/2$.

(e). If $0 \leq m \leq n$, show that we have

$$M^{n-m,m} = \bigoplus_{r=0}^{\min(m,n-m)} (d^*)^{m-r}(S^{n-r,r}),$$

where the summands are pairwise orthogonal and are exactly the eigenspaces of $\Delta$.

(f). Show that $\dim_{\mathbb{C}}(S^{n-r,n}) = \binom{n}{r} - \binom{n}{r-1}$ if $r > 0$.

(g). Show that the representations $S^{n-r,r}$, $0 \leq r \leq n/2$, are irreducible and pairwise inequivalent. (Hint : how many irreducible constituents does $M^{m,n-m}$ have ?)

*Solution.*

(a). The map $A \longmapsto \{1,\dots,n\} - A$ is a bijection from $\Omega_r$ to $\Omega_{n-r}$, and it commutes with the action of $G$ on these two sets. The conclusion follows immediately.

(b). Let $f \in M^{n-r,r}$ and $\sigma \in \mathfrak{S}_n$. If $A \in \Omega_{r-1}$, then

$$\begin{aligned}(dL_\sigma f)(A) &= \sum_{B\in\Omega_r,\ B\supset A} f(\sigma^{-1}(B)) \\ &= \sum_{B'\in\Omega_r,\ B'\supset\sigma^{-1}(A)} f(B') \\ &= (df)(\sigma^{-1}(A)) \\ &= L_\sigma(df)(A).\end{aligned}$$

If $A \in \Omega_r$, then

$$\begin{aligned}(\Delta L_\sigma f)(A) &= \sum_{B\in\Omega_r,\ d(A,B)=1} f(\sigma^{-1}(B)) \\ &= \sum_{B'\in\Omega_r,\ d(\sigma^{-1}(A),B')=1} f(B') \\ &= \Delta f(\sigma^{-1}(A)) \\ &= L_\sigma(\Delta f)(A).\end{aligned}$$

(c). Let $f \in M^{n-r,r}$ and $g \in M^{n-r+1,r-1}$. Then

$$\begin{aligned}\langle df, g\rangle &= \sum_{A\in\Omega_{r-1}} df(A)\overline{g(A)} \\ &= \sum_{A\in\Omega_{r-1},B\in\Omega_r,\ A\subset B} f(B)\overline{g(A)} \\ &= \sum_{B\in\Omega_r} f(B)\overline{d^*g(B)}.\end{aligned}$$

(d). Let $f \in M^{n-r,r}$ and $A \in \Omega_r$. Then

$$\begin{aligned}dd^*f(A) &= \sum_{B\in\Omega_{r+1},B\supset A} d^*f(B) \\ &= \sum_{B\in\Omega_{r+1},\ C\in\Omega_r\ C\subset B\supset A} f(C)\end{aligned}$$

Let $C \in \Omega_r$. If there exists $B \in \Omega_{r+1}$ such that $C \subset B \supset A$, then $d(A,C) \le 1$. If $C = A$, then

$$|\{B \in \Omega_{r+1} | C \subset B \supset A\}| = |\{B \in \Omega_{r+1} | A \subset B\}| = n - r\}.$$

If $d(A,C)=1$, then the only element of $\Omega_{r+1}$ that contains both $A$ and $C$ is $A\cup C$. Finally, we get

$$\begin{aligned} dd^* f(A) &= (n-r)f(A) + \sum_{C\in\Omega_r,\ d(A,C)=1} f(C) \\ &= (n-r)f(A) + \Delta f(A). \end{aligned}$$

Similarly, we have

$$\begin{aligned} d^* df(A) &= \sum_{B\in\Omega_{r-1}, B\subset A} df(B) \\ &= \sum_{C\in\Omega_r,\ B\in\Omega_{r-1}, C\supset B\subset A} f(C). \end{aligned}$$

Let $C\in\Omega_r$. If there exists $B\in\Omega_{r-1}$ such that $C\supset B\subset A$, then $d(A,C)\leq 1$. If $A=C$, then

$$|\{B\in\Omega_{r-1}|C\supset B\subset A\}| = r.$$

If $d(A,C)=1$, then the only $B\in\Omega_{r-1}$ that is contained in both $A$ and $C$ is $B=A\cap C$. So we get

$$\begin{aligned} d^* df(A) &= rf(A) + \sum_{C\in\Omega_r,\ d(A,C)=1} f(C) \\ &= rf(A) + \Delta f(A). \end{aligned}$$

(e). We show the first identity by induction on $q$. If $q=1$, then, by (d), we have

$$dd^* f = \Delta f + (n-r)f = \Delta f + rf + (n-2r)f = d^* df + q(n-2r-q+1)(d^*)^{q-1}f$$

for every $f\in M^{n-r,r}$. Now suppose the identity known for $q\in\{1,\dots,n-r-1\}$, every $s$ and every element of $M^{n-s,s}$, and let's show it for $q+1$. If $f\in M^{n-r,r}$, we have

$$\begin{aligned} d(d^*)^{q+1} f &= d(d^*)^q(d^* f) \\ &= (d^*)^q d(d^* f) + q(n-2(r+1)-q+1)(d^*)^{q-1}(d^* f) \\ &\qquad \text{(by the induction hypothesis for } d^* f\in M^{n-r-1,r+1}) \\ &= (d^*)^q(d^* df + (n-2r)f) + q(n-2r-q-1)(d^*)^q f \\ &\qquad \text{(by the case } q=1) \\ &= (d^*)^{q+1} df + (n-2r+q(n-2r-q-1))(d^*)^q f \\ &= (d^*)^{q+1} df + (q+1)(n-2r-(q+1)+1)(d^*)^q f. \end{aligned}$$

Now let's prove the second identity by induction on $p$. If $p=1$, it just reduce to the first identity (using that $df=0$). Suppose that we have proved it for some $p\in\{1,\dots,q-1\}$

(and all $s$ and all $f \in M^{n-s,s}$ such that $df = 0$), and let's prove it for $p+1$. Let $f \in M^{n-r,r}$ such that $df = 0$. Then we have

$$\begin{aligned}
d^{p+1}(d^*)^q f &= d(d^p(d^*)^q f) \\
&= d((q-p+1)_p(n-2r-q+1)_p(d^*)^{q-p} f) \\
&= (q-p+1)_p(n-2r-q+1)_p(q-p)(n-2r-(q-p)+1)(d^*)^{q-p-1} f \\
&\quad \text{(using the first identity and the fact that } df = 0) \\
&= (q-p)_{p+1}(n-2r-q+1)_{p+1}(d^*)^{q-p-1} f.
\end{aligned}$$

(f). Let $f \in S^{n-r,r}$, $f \neq 0$. Using (c) and then the second identity of (e), we see that

$$\begin{aligned}
\langle (d^*)^{m-r} f, (d^*)^{m-r} f \rangle &= \langle d^{m-r}(d^*)^{m-r} f, f \rangle \\
&= (1)_{m-r}(n-2r-(m-r)+1)_{m-r}\langle f, f \rangle \\
&\neq 0,
\end{aligned}$$

so $(d^*)^{m-r} f \neq 0$.

(g). Let $f \in S^{n-r,r}$. Using the second formula of (d) to calculate $\Delta$ on $M^{n-m,m}$ and the second formula of (e) (with $p = 1$), we get

$$\begin{aligned}
\Delta((d^*)^{m-r} f) &= d(d^*)^{m-r+1} f - (n-m)(d^*)^{m-r} f \\
&= (m-r+1)(n-2r-(m-r+1)+1)(d^*)^{m-r} f - (n-m)(d^*)^{m-r} f \\
&= (m(n-m) - r(n-r+1))(d^*)^{m-r} f.
\end{aligned}$$

(h). This is an immediate consequence of the definition of $S^{n-m,m}$ and of (c).

(i). The space $S^{n-r,r}$ is the kernel of $d : M^{n-r,r} \to M^{n-r+1,r-1}$, and $\dim(M^{n-r+1,r-1}) = \binom{n}{r-1} < \binom{n}{r} \dim(M^{n-r,r})$ because $r \leq n/2$, so $d$ cannot be injective.

(j). The subspaces $(d^*)^{m-r}(S^{n-r,r})$, for $0 \leq r \leq \min(m, n-m)$, are contained in eigenspaces of $\Delta$ for different eigenvalues by (g). They are all nonzero by (f) and (i). We know that $\Delta$ is seld-adjoint by V.8.2.2(i), so these spaces are pairwise orthogonal. Also, we know that $\Delta \in \mathrm{End}(M^{n-m,m})$ has exactly $1 + \min(m, n-m)$ eigenvalues by V.8.2.2(a) and V.8.2.2(j), so these eigenvalues have to be the numbers $m(n-m) - r(n-r+1)$, $0 \leq r \leq \min(m, n-m)$. It remains to show that

$$M^{n-m,m} = \bigoplus_{r=0}^{\min(m,n-m)} (d^*)^{m-r}(S^{n-r,r}).$$

We prove this by induction on $m$. It's obvious if $m = 0$. Suppose that we have the result for $m-1$, with $n/2 \geq m \geq 1$, and let's prove it for $m$. By (h), we have

$$M^{n-m,m} = S^{n-m,m} \oplus d^*(M^{n-m+1,m-1}).$$

By the induction hypothesis, we have

$$M^{n-m+1,m-1} = \bigoplus_{r=0}^{m-1} (d^*)^{m-1-r}(S^{n-r,r}).$$

The result for $m$ follows immediately from these two facts.

Finally, we treat the case $m \geq n/2$. Let $m' = n - m$. We have seen that

$$M^{n-m',m'} = \bigoplus_{r=0}^{m'} (d^*)^{m'-r}(S^{n-r,r}).$$

By (f), this implies that $\dim(M^{n-m'}, m') = \sum_{r=0}^{m'} \dim(S^{n-r,r})$. We have also seen that

$$M^{n-m,m} \supset \bigoplus_{r=0}^{m'} (d^*)^{m-r}(S^{n-r,r}),$$

and, again by (f), this implies that $\dim(M^{n-m,m}) \geq \sum_{r=0}^{m'} \dim(S^{n-r,r}) = \dim(M^{m',n-m'})$. But $\dim(M^{n-m,m}) = \dim(M^{n-m',m'})$ (by (a)), so the inequality above is an equality, and

$$M^{n-m,m} = \bigoplus_{r=0}^{m'} (d^*)^{m-r}(S^{n-r,r}).$$

(k). By (j) and (f), the map $d^* : M^{n-r+1,r-1} \to M^{n-r,r}$ is injective. By (h), this implies that

$$\dim(S^{n-r,r}) = \dim(M^{n-r,r}) - \dim(M^{n-r+1,r-1}) = \binom{n}{r} - \binom{n}{r-1}.$$

(l). Let $m = \lfloor n/2 \rfloor$. As the maps $d$ and $d^*$ are $\mathfrak{S}_n$-equivariant (see (b) for $d$, and $d^*$ is the adjoint of $d$ by (c) so it also equivariant), the subspace $S^{n-r,r} \subset M^{n-r,r}$ is $\mathfrak{S}_n$-stable for every $r \leq n/2$, and the decomposition of (j) is a decomposition into $\mathfrak{S}_n$-subspaces. Next, we know that $(\mathfrak{S}_n, \mathfrak{S}_m \times \mathfrak{S}_{n-m})$ is a Gelfand pair by V.8.2.1(f), so the corresponding quasi-regular representation, which is $M^{n-m,r}$, decomposes into a direct sum of distinct irreducible representations by theorem V.3.2.4. By corollary V.7.2, the number of irreducible summands in $M^{n-m,m}$ is the number of spherical functions for the Gelfand pair, which is the dimension of the space of bi-invariant functions on $\mathfrak{S}_n$ (because spherical functions form a basis for these bi-invariants functions by (iii) of the same corollary), i.e. the cardinality of $(\mathfrak{S}_m \times \mathfrak{S}_{n-m}) \setminus \mathfrak{S}_n / (\mathfrak{S}_m \times \mathfrak{S}_{n-m})$, and this is also equal to the number of orbits of $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ on $\Omega_m$. But we have seen in V.8.2.1(d) that the orbits of $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ on $\Omega_m$ are the spheres with center $A_0 := \{1, \ldots, m\}$. The possible radii for these spheres are $0, 1, \ldots, \min(m, n-m) = m$ by 2(a), and it is easy to see that all the spheres are nonempty (we already used this in the proof of V.8.2.2(f)). Finally, we get that the number of irreducible constituents of $M^{n-m,m}$ is $m+1$. As the decomposition of (j) is a decomposition of $M^{n-m,m}$ int $m+1$ nonzero subrepresentations, it must be its decomposition into irreducible constituents, and so we get the conclusion. (Note that $(d^*)^{m-r}(S^{n-r,r})$ is equivalent to $S^{n-r,r}$ as a representation of $\mathfrak{S}_n$ by (f).)

$\square$

**Exercise V.8.2.4.** We keep the notation of problem V.8.2.3. If $m, h \in \{0, \dots, n\}$, $A \in \Omega_m$, and $\max(0, h-m) \leq \ell \leq \min(n-m, h)$, we denote by $\sigma_{\ell,h-\ell}(A) \in L(\Omega_h)$ the characteristic function of the set $\{C \in \Omega_h | |A \cap C| = h - \ell\}$. We also write $\sigma_{-1,h+1}(A) = 0$. We fix $A \in \Omega_m$.

(a). If $h = m$, show that, for every $\ell \in \{0, \dots, \min(m, n-m)\}$, the function $\sigma_{\ell,m-\ell}(A)$ is the characteristic function of the sphere $\{C \in \Omega_m | d(A, C) = \ell\}$.

(b). Show that

$$d(\sigma_{\ell,h-\ell}(A)) = (n-m-\ell+1)\sigma_{\ell-1,h-\ell}(A) + (m-h+\ell+1)\sigma_{\ell,h-\ell-1}(A).$$

(c). If $k \leq h$ and $\max(0, k-m) \leq i \leq \min(k, n-m)$, show that

$$\frac{1}{(h-k)!}(d^*)^{h-k}\sigma_{i,k-i}(A) = \sum_{\ell=\max(i,h-m)}^{\min(h-k+i,n-m)} \binom{\ell}{i}\binom{h-\ell}{k-i}\sigma_{\ell,h-\ell}(A).$$

From now on, we take $A = \{1, \dots, m\}$.

(a). If $0 \leq h \leq \min(m, n-m)$, show that the space of $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$-invariant vectors in $M^{n-h,h}$ is spanned by the functions $\sigma_{\ell,h-\ell}(A)$, for $0 \leq \ell \leq h$.

(b). If $0 \leq h \leq \min(m, n-m)$, show that the space of $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$-invariant vectors in $S^{n-h.h}$ is spanned by the function

$$\sum_{\ell=0}^{h} \frac{(n-m-h+1)_{h-\ell}}{(-m)_{h-\ell}}\sigma_{\ell,h-\ell}(A).$$

(c). For $0 \leq h \leq \min(m, n-m)$, let $\varphi_h \in M^{n-m,m}$ be the unique spherical function contained in the summand $(d^*)^{m-h}(S^{n-h,h})$. Show that

$$\varphi_h = \sum_{\ell=0}^{\min(m,n-m)} \varphi(n, m, h; \ell)\sigma_{\ell,m-\ell}(A),$$

where

$$\varphi(n, m, h; \ell) = (-1)^h \frac{1}{\binom{n-m}{h}} \sum_{i=\max(0,\ell-m+h)}^{\min(\ell,h)} \binom{m-\ell}{h-i}\binom{\ell}{i}\frac{(n-m-h+1)_{h-i}}{(-m)_{h-i}}.$$

(d). Fix $h$ such that $0 \leq h \leq \min(m, n-m)$. Show that the coefficient of $\sigma_{1,m-1}(A)$ in $\varphi_h$ is $1 - \dfrac{h(n-h+1)}{m(n-m)}$. (Remark : there is a way to solve this question with minimal calculations.)

*Solution.*

(a). The function $\sigma_{\ell,m-\ell}(A)$ is the characteristic function of the set $\{C \in \Omega_m \| A \cap C| = m-\ell\}$. As $d(A,C) = m - |A \cap C|$, this set is exactly the sphere of radius $\ell$ with center $A$.

(b). Let $B \in \Omega_{h-1}$. We have

$$\begin{aligned} d(\sigma_{\ell,h-\ell}(A))(B) &= \sum_{C \in \Omega_h,\ C \supset B} \sigma_{\ell,h-\ell}(A)(C) \\ &= |\{C \in \Omega_h | C \supset B \text{ and } |A \cap C| = h - \ell\}|. \end{aligned}$$

If there exists at least one $C \in \Omega_h$ such that $C \supset B$ and $|A \cap C| = h - \ell$, then $A \cap C \supset A \cap B$ and these two sets differ by at most one element, so $|A \cap B| \in \{h-\ell, h-\ell-1\}$.

Suppose that $|A \cap B| = h - \ell$. Then, for every $C \in \Omega_h$ such that $C \supset B$ and $|A \cap C| = h - \ell$, we must have $A \cap C = A \cap B$. We get each such $C$ by adding an element of $\{1, \ldots, n\} - (A \cup B)$ to $B$, so the number of possibilities for $C$ is

$$n - |A \cup B| = n - (|A| + |B| - |A \cap B|) = n - (m + h - 1 - (h - \ell)) = n - m - \ell + 1.$$

Suppose that $|A \cap B| = h - \ell + 1$. Then, for every $C \in \Omega_h$ such that $C \supset B$ and $|A \cap C| = h - \ell$, the unique element of $C - B$ must be the element of $A \cap C - A \cap B$. So the number of possibilities for $C$ is

$$|A - A \cap B| = m - h + \ell - 1.$$

Finally, we get

$$d(\sigma_{\ell,h-\ell}(A))(B) = (n - m - \ell - 1)\sigma_{\ell-1,h-\ell}(B) + (m - h + \ell - 1)\sigma_{\ell,h-\ell-1}(B),$$

as desired.

(c). For every $i$ and every $D \in \Omega_i$, denote by $\delta_D \in L(\Omega_i)$ the characteristic function of $\{D\}$. Let $S$ be the set $\{C \in \Omega_k \| A \cap C| = k - i\}$. Then $\sigma_{i,k-i}(A)$ is the characteristic function of $S$. If $C \in S$, then, for every $D \in \Omega_h$, we have

$$(d^*)^{h-k}\delta_C(D) = \sum_{C \subset D_1 \subset \ldots \subset D_{h-k-1} \subset D_{h-k} = D,\ D_i \in \Omega_{k+i}} 1.$$

If $C \not\subset D$, the set $\{C \subset D_1 \subset \ldots \subset D_{h-k-1} \subset D_{h-k} = D,\ D_i \in \Omega_{k+i}\}$ is empty; if $C \subset D$, this set has $(h-k)!$ elements. So we see that

$$(d^*)^{h-k}\delta_C = (h-k)! \sum_{C \subset D \in \Omega_h} \delta_D.$$

So, if $D \in \Omega_h$, the coefficient of $\delta_D$ in $\frac{1}{(h-k)!}(d^*)^{h-k}\sigma_{i,k-i}(A)$ is the cardinality of the set $\{C \in S | C \subset D\}$. Write $|A \cap D| = h - \ell$, with $0 \leq \ell \leq h$; note that we have

$$h - \ell = |A \cap D| = |A| + |D| - |A \cup D| \geq m + h - |A \cup D|$$

and $h \leq |A \cup D| \leq n$, so $h - m \leq \ell \leq n - m$, and all the nonnegative $\ell$ in this range can occur. We get a $C \in S$ such that $C \subset D$ by removing $(h - \ell) - (k - i)$ elements from $A \cap D$ and $\ell - i$ elements from $D - (A \cap D)$. This is only possible if $h - \ell - (k - i) \geq 0$ and $0 \leq \ell - i$, and we have $\binom{h-\ell}{(h-\ell)-(k-i)}\binom{\ell}{\ell-i}$ different possible choices. Putting all this together, we see that, if $|A \cap D| = h - \ell$, then the coefficient of $\delta_D$ in $\frac{1}{(h-k)!}(d^*)^{h-k}\sigma_{i,k-i}(A)$ is $\binom{h-\ell}{k-i}\binom{\ell}{i}$ if $\max(h - m, i) \leq \ell \leq \min(n - m, h - k + i)$ and 0 otherwise. This gives the result.

(d). The statement is equivalent to the fact that the orbits $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ in $\Omega_h$ are the $S_\ell := \{C \in \Omega_h || A \cap C| = h - \ell\}$, for $0 \leq \ell \leq h$. Let's prove this fact. As $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ fixes $A$, the sets $S_\ell$ are invariant by $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$, so we just need to show that $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$ acts transitively on these sets. Fix $\ell \in \{0, \ldots, h\}$ and take $C, C' \in S_\ell$. As $|A \cap C| = |A \cap C'|$, we can find an element $\sigma \in \mathfrak{S}_m$ that sends $A \cap C$ to $A \cap C'$. Also, we have $|\{m + 1, \ldots, n\} \cap C| = |\{m + 1, \ldots, n\} \cap C'| = \ell$, so we can find an element $\tau \in \mathfrak{S}_{n-m}$ that sends $\{m+1, \ldots, n\} \cap C$ to $\{m+1, \ldots, n\} \cap C'$. Then $\sigma \times \tau \in \mathfrak{S}_m \times \mathfrak{S}_{n-m}$ sends $C$ and $C'$.

(e). Let $f \in S^{n-h,h}$ be a $\mathfrak{S}_m \times \mathfrak{S}_{n-m}$-invariant vector. By (d), the invariance condition is equivalent to the fact that we can write $f = \sum_{\ell=0}^{h} a_\ell \sigma_{\ell,h-\ell}(A)$, with $a_0, \ldots, a_h \in \mathbb{C}$. The fact that $f \in S^{n-h,h}$ means that $df = 0$. Using (b), we can rewrite this condition as

$$\begin{aligned} 0 &= \sum_{\ell=0}^{h} a_\ell((n - m - \ell + 1)\sigma_{\ell-1,h-\ell}(A) + (m - h + \ell + 1)\sigma_{\ell,h-1-\ell}(A)) \\ &= \sum_{\ell=0}^{h-1} a_{\ell+1}(n - m - \ell)\sigma_{\ell,h-\ell+1}(A) + \sum_{\ell=0}^{h} a_\ell(m - h + \ell + 1)\sigma_{\ell,h-1-\ell}(A). \end{aligned}$$

As the functions $\sigma_{\ell,h-1-\ell}(A)$, $0 \leq \ell \leq h - 1$, are linearly independent (because they have disjoint supports), this equality if equivalent to the fact that

$$a_\ell = a_{\ell+1}\frac{n - m - \ell}{-m + h - \ell - 1},$$

for every $\ell \in \{0, \ldots, h - 1\}$. A straightforward descending induction on $\ell$ shows that this is equivalent to

$$a_\ell = \frac{(n - m - h + 1)_{h-\ell}}{(-m)_{h-\ell}}a_h$$

for every $\ell \in \{0, \ldots, h\}$. This implies the desired result.

(f). By (e) (and the $\mathfrak{S}_n$-equivariance of $d^*$), the function $\varphi_h$ is a multiple of

$$\psi := \frac{1}{(m-h)!}(d^*)^{m-h}\left(\sum_{i=0}^{h}\frac{(n-m-h+1)_{h-i}}{(-m)_{h-i}}\sigma_{i,h-i}(A)\right).$$

We calculate $\psi$ using the formula of (c). We get

$$\begin{aligned}\psi &= \sum_{i=0}^{h}\frac{(n-m-h+1)_{h-i}}{(-m)_{h-i}}\sum_{\ell=i}^{\min(m-h+i,n-m)}\binom{\ell}{i}\binom{m-\ell}{h-i}\sigma_{\ell,m-\ell}(A)\\ &= \sum_{\ell=0}^{\min(m,n-m)}\sum_{i=\max(0,\ell-m+h)}^{\min(\ell,h)}\binom{\ell}{i}\binom{m-\ell}{h-i}\frac{(n-m-h+1)_{h-i}}{(-m)_{h-i}}\sigma_{\ell,m-\ell}(A).\end{aligned}$$

This is almost the formula we want, except for the constant $(-1)^h\frac{1}{\binom{n-m}{h}}$ at the beginning.

The spherical function $\varphi_h$ is normalized by the fact that $\varphi_h(A_0) = 1$, so we have $\varphi_h = \frac{1}{\psi(A_0)}\psi$. So to finish the proof, we just need to show that $\psi(A_0) = (-1)^h\binom{n-m}{h}$. Note that $\sigma_{\ell,m-\ell}(A)(A_0) = 0$ unless $\ell = 0$ and $\sigma_{0,m}(A)(A_0) = 1$, so

$$\begin{aligned}\psi(A_0) &= \binom{m}{h}\frac{(n-m-h+1)_h}{(-m)_h}\\ &= \frac{m!}{h!(m-h)!}\frac{(n-m)!}{(n-m-h)!}\frac{(-1)^h(m-h)!}{m!}\\ &= (-1)^h\binom{n-m}{h}.\end{aligned}$$

(g). Let's try and ignore questions (c), (d), (e) and (f).

The function $\varphi_h$ is spherical, so it is constant on the $\mathfrak{S}_m\times\mathfrak{S}_{n-m}$-orbits in $\Omega_m$, which are the spheres with center $A$ by V.8.2.1(d). By (a) and V.8.2.2(a), this means that $\varphi_h$ is a linear combination of the functions $\sigma_{\ell,m-\ell}(A)$, for $0\leq\ell\leq\min(m,n-m)$. Also, by V.8.2.3(g), the function $\varphi_h$ is an eigenvector of $\Delta$ with eigenvalue $m(n-m)-h(n-h+1)$. Let $S = \{B\in\Omega_m|d(A,B)=1\}$. Then $\sigma_{1,m-1}(A)$ is the characteristic function of $S$, and we have seen that $\varphi_h$ is constant on $S$, the coefficient of $\sigma_{1,m-1}(A)$ in $\varphi_h$ is $\frac{1}{|S|}\sum_{B\in S}\varphi_h(B)$. On the other hand, $\sum_{B\in S}\varphi_h(B)$ is equal to $\Delta\varphi_h(A)$ by definition of $\Delta$, and this is equal to $(m(n-m)-h(n-h+1))\varphi_h(A)$. Moreover, as $\varphi_h$ is spherical, we must have $\varphi_h(A)=1$. Finally, the coefficient of $\sigma_{1,m-1}(A)$ in $\varphi_h$ is $\frac{1}{|S|}(m(n-m)-h(n-h-1))$. To finish the calculation, we just need to show that $|S| = m(n-m)$. This just follows from the fact that we get every element $B$ of $S$ by removing one element of $A$ ($m$ choices) and adding an element of $\{1,\dots,n\}-A$ ($n-m$ choices).

□

## V.8.3 Problem : the Satake isomorphism

This probolem was extracted from Cartier's survey in Corvalley ([6]), especially chapter IV, and from unpublished notes of Kottwitz.

We will use the following conventions :

- If $G$ is a locally compact group, we denote by $\mu_G$ a left Haar measure on $G$ (sometimes normalized in a particular way). We then denote the corresponding $L^p$ spaces by $L^p(G)$.
- If $G$ is a locally compact group and $H \subset G$ is a closed subgroup, then we denote by $\mu_{G/H}$ (resp. $\mu_{H\backslash G}$) the left (resp. right) $G$-invariant measure on $G/H$ (resp. $H\backslash G$) induced by the measures $\mu_G$ and $\mu_H$. See proposition V.1.3. To construct the measure $\mu_{H\backslash G}$, we need $\mu_G$ to be right invariant.

To make things a bit more concrete, I wrote this problem for $\mathrm{GL}_3(\mathbb{Q}_p)$. Everything generalizes to $\mathrm{GL}_n(\mathbb{Q}_p)$ (for any $n \geq 1$), and in fact most questions have a solution that applies to $\mathrm{GL}_n(\mathbb{Q}_p)$ with minimal changes.

Let $\mathbf{n} = \mathbf{3}$. We write $G = \mathrm{GL}_3(\mathbb{Q}_p)$ and $K = \mathrm{GL}_3(\mathbb{Z}_p)$. We denote by $B$ the subgroup of upper triangular matrices in $G$, by $T$ the group of diagonal matrices in $G$ and by $N$ the group of unipotent upper triangular matrices in $G$ (i.e. upper triangular matrices with all their diagonal entries equal to 1). We write $X = \mathbb{Z}^3$ and

$$X^+ = \{(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}^3 | \lambda_1 \geq \lambda_2 \geq \lambda_3\}.$$

If $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in X$, we set

$$p^\lambda = \begin{pmatrix} p^{\lambda_1} & & 0 \\ & p^{\lambda_2} & \\ 0 & & p^{\lambda_3} \end{pmatrix} \in T.$$

We fix left Haar measures $\mu_G$, $\mu_B$, $\mu_T$, $\mu_N$ and $\mu_K$ on $G$, $B$, $T$, $N$ and $K$; if there is no risk of confusion, we will just write $dx$ instead of $d\mu_G(x)$ etc in the integrals. We normalize all the Haar measures by demanding that $\mathrm{vol}(H \cap K) = 1$ for $H \in \{G, B, T, N, K\}$. In this problem only, we will write $\mathscr{C}_c(X)$ for the space of *locally constant* functions $f : X \to \mathbb{C}$ with compact support. (Where "locally constant" means exactly what you would image : $f : X \to \mathbb{C}$ is locally constant if for every $x \in X$, there exists a neighborhood $U$ of $x$ in $X$ such that $f_{|U}$ is constant. Note that this implies that $f$ is continuous.)

Let $\mathscr{H} = \mathscr{C}_c(K\backslash G/K)$ and $\mathscr{H}_T = \mathscr{C}_c(T/(T \cap K))$, with the algebra structure given by the convolution product. (It is very easy to check that the convolution product respects the "locally constant" condition.) The goal of this problem is to understand the structure of the algebra $\mathscr{H}$.

(1) Define $\delta : B \to \mathbb{R}_{>0}$ by

$$\delta \begin{pmatrix} a_1 & * & * \\ 0 & a_2 & * \\ 0 & 0 & a_3 \end{pmatrix} = \prod_{i=1}^{n} |a_i|_p^{n+1-2i}.$$

Show that $\delta^{-1}$ is the modular function of $B$, and that we have

$$\int_B f(b_0 b b_0^{-1}) db = \delta^{-1}(b_0) \int_B f(b) db.$$

for every $f \in \mathscr{C}_c(B)$ and every $b_0 \in B$.

(2) Show that $G = BK$, and that we have

$$\int_G f(g) dg = \int_B \int_K f(bk) db dk = \int_T \int_N \int_K f(tnk) dt dn dk$$

for every $f \in \mathscr{C}_c(G)$.

(3) Let $(e_1, e_2, e_3)$ be the canonical basis of $\mathbb{Q}_p^3$. Show that the map $g \longmapsto \mathbb{Z}_p g(e_1) + \mathbb{Z}_p g(e_2) + \mathbb{Z}_p g(e_3)$ induces a bijection between $G/K$ and the set of free $\mathbb{Z}_p$-submodules of rank 3 of $\mathbb{Q}_p^3$.

(4) Show that

$$G = \coprod_{\lambda \in X^+} K p^\lambda K.$$

(This is called the *Cartan decomposition.*) .

(5) Show that $(G, K)$ is a Gelfand pair. (Hint : $\theta(x) = (x^T)^{-1}$.)

Let $z = (z_1, z_2, z_3) \in (\mathbb{C}^\times)^3$. We define a morphism $\chi_z : B \to \mathbb{C}^\times$ by

$$\chi_z \begin{pmatrix} a_1 & * & * \\ 0 & a_2 & * \\ 0 & 0 & a_3 \end{pmatrix} = \prod_{i=1}^n z_i^{v_p(a_i)},$$

where, for every $a \in \mathbb{Q}_p^\times$, we write $|a|_p = p^{-v_p(a)}$ (so that $v_p(a) \in \mathbb{Z}$). We denote by $V_z$ the space of functions $f : G \to \mathbb{C}$ such that :

(i) for every $b \in B$ and every $g \in G$, we have

$$f(bg) = \chi_z(b) \delta(b)^{1/2} f(g);$$

(ii) there exists an open compact subgroup $K_1$ of $G$ such that $f(gk) = f(g)$ for every $g \in G$ and every $k \in K_1$.

We make $G$ act on $V_z$ by $g \cdot f = R_g(f)$.

(6) Show that $V_z$ is a representation of $G$ (note that I am not saying anything about continuity) and that $\dim(V_z^K) = 1$.

*Remark.* (Not necessary to do the problem.) The elements of $V_z$ are locally constant but don't have compact support in general, because of condition (i). Also, we did not define a topology on $V_z$, so we cannot say that $V_z$ is a continuous representation of $G$. In fact, it is what is called a *smooth* representation, which means that every element of $V_z$ is fixed by an open compact subgroup of $G$ (this is automatic from condition (ii)). This means that the representation is continuous if we put the *discrete* topology on $V_z$, and it is a more natural condition for representations of totally disconnected groups. If we wanted a continuous representation on a Hilbert space, we would put the inner form $\langle f_1, f_2\rangle = \int_K f_1(k)\overline{f_1(k)}dk$ on $V_z$ and complete for this inner form. Note that, even then, the representation would not be unitary unless $|z_1| = |z_2| = |z_3| = 1$.

We denote by $\varphi_z$ the unique element of $V_z^K$ such that $\varphi_z(1) = 1$.[8] For every $f \in \mathscr{H}$, we denote by $f^\vee : (\mathbb{C}^\times)^3 \to \mathbb{C}$ the function[9]

$$z \longmapsto \int_G f(g)\varphi_z(g)dg.$$

If $f \in \mathscr{H}_T$, we define $f^\vee : (\mathbb{C}^\times)^3 \to \mathbb{C}$ by

$$f^\vee(z) = \int_T f(t)\chi_z(t)dt.$$

(7) Show that, for all $f_1, f_2 \in \mathscr{H}$, we have $(f_1 * f_2)^\vee = f_1^\vee f_2^\vee$.

(8) Show that
$$T = \coprod_{\lambda\in X}(T\cap K)p^\lambda.$$

(9) Show that $f \longmapsto f^\vee$ is a an isomorphism of $\mathbb{C}$-algebras from $\mathscr{H}_T$ to the algebra of functions on $(\mathbb{C}^\times)^3$ that are polynomial in $z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}$; we will identify this algebra to $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]$.

For every $f \in \mathscr{C}_c(G)$, we define a function $f^{(B)} : T \to \mathbb{C}$ by

$$f^{(B)}(t) = \delta(t)^{1/2}\int_N f(tn)dn.$$

(10) Show that $f^{(B)} \in \mathscr{C}_c(T)$ for every $f \in \mathscr{C}_c(G)$, and that $f^{(B)} \in \mathscr{H}_T$ if $f \in \mathscr{H}$.

(11) Show that, for every $f \in \mathscr{H}$ and every $z \in (\mathbb{C}^\times)^3$, we have $f^\vee(z) = (f^{(B)})^\vee(z)$.

Define $D : T \to \mathbb{R}_{>0}$ by

$$D\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3\end{pmatrix} = \prod_{i,j\in\{1,\dots,n\}, i\neq j} |1 - a_i a_j^{-1}|_p.$$

[8] It is a spherical function (except that it's not bounded in general), hence the notation. But you cannot use this fact unless you prove it first !

[9] This is morally the spherical Fourier transform, but unfortunately the usual convention for $p$-adic groups differs from the convention that we used in class.

If $f \in \mathscr{C}_c(G)$ and $t \in T$ is such that $D(t) \neq 0$, we set

$$O_t(f) = \int_{T\backslash G} f(g^{-1}tg) d\mu_{T\backslash G}.$$

(12) Show that, for every $f \in \mathscr{C}_c(N)$ and every $t \in T$ such that $D(t) \neq 0$, we have

$$\int_N f(n)dn = D(t)^{1/2}\delta(t)^{1/2} \int_N f(ntn^{-1}t^{-1})dn.$$

(Hint : Consider the subgroup $U \subset N$ defined by

$$U = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

and use the formula $\int_N f(n)dn = \int_{N/U} \int_U f(nu) d\mu_{N/U}(n) d\mu_U(u)$.)

(13) Show that, for every $f \in \mathscr{H}$ and every $t \in T$ such that $D(t) \neq 0$, we have

$$O_t(f) = D(t)^{-1/2} f^{(B)}(t).$$

(14) Show that, for every $f \in \mathscr{H}$, the function $f^\vee : (\mathbb{C}^\times)^3 \to \mathbb{C}$ is an element of $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$, the algebra of symmetric polynomial functions in $z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}$, i.e.

$$\{p(z_1, z_2, z_3) \in \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}] | \forall \sigma \in \mathfrak{S}_3,\ p(z_{\sigma(1)}, z_{\sigma(2)}, z_{\sigma(3)}) = p(z_1, z_2, z_3)\}.$$

We define a partial order on $X = \mathbb{Z}^3$ by saying that $(\mu_1, \mu_2, \mu_3) \leq (\lambda_1, \lambda_2, \lambda_3)$ if and only if $\mu_1 \leq \lambda_1$, $\mu_1 + \mu_2 \leq \lambda_1 + \lambda_2$ and $\mu_1 + \mu_2 + \mu_3 = \lambda_1 + \lambda_2 + \lambda_3$. (Note that the last relation is an equality !) For every $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in X$, we define $z^\lambda \in \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 2}, z_3^{\pm 1}]$ by

$$z^\lambda = z_1^{\lambda_1} z_2^{\lambda_2} z_3^{\lambda_3}$$

and $f_\lambda \in \mathscr{H}$ by

$$f_\lambda = \mathbb{1}_{Kp^\lambda K}.$$

(15) Show that $(f_\lambda)_{\lambda \in X^+}$ is a basis of $\mathscr{H}$.

(16) For every $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in X^+$, let

$$c_\lambda = \sum_{\sigma \in \mathfrak{S}_3} z^{(\lambda_{\sigma(1)}, \lambda_{\sigma(2)}, \lambda_{\sigma(3)})}.$$

Show that $(c_\lambda)_{\lambda \in X^+}$ is a basis of $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$.

(17) For every $\lambda \in X$, we write

$$(f_\lambda)^\vee = \sum_{\mu \in X} c_\lambda(\mu) z^\mu,$$

with the $c_\lambda(\mu) \in \mathbb{C}$. The goal of this question is to show the following two facts :

(i) If $\lambda, \mu \in X^+$ and $\mu \not\leq \lambda$, then $c_\lambda(\mu) = 0$.

(ii) For every $\lambda \in X^+$, we have

$$c_\lambda(\lambda) = p^{\frac{1}{2}\sum_{i=1}^{n}(n+1-2i)\lambda_i}.$$

If $\mu = (\mu_1, \mu_2, \mu_3) \in X$, we write $\overline{\mu} = (\mu_3, \mu_2, \mu_1)$.

(a). For every $g = (g_{ij}) \in M_3(\mathbb{Q}_p)$, let $\|g\| = \sup_{i,j} |g_{i,j}|_p$. Show that, for every $g \in M_3(\mathbb{Q}_p)$ and $k, k' \in K$, we have $\|g\| = \|kgk'\|$.

(b). Let $r \in \{1, \dots, n\}$, and let $\Omega_r$ be the set of cardinality $r$ subsets of $\{1, \dots, n\}$. If $g = (g_{ij}) \in M_3(\mathbb{Q}_p)$, we define $\Lambda^r g : \Omega_r \times \Omega_r \to \mathbb{Q}_p$ by

$$\Lambda^r(g)(A, A') = \det((g_{ij})_{i \in A, j \in A'}),$$

and $\|\Lambda^r g\|$ by

$$\|\Lambda^r g\| = \sup_{A, A' \in \Omega_r} |\Lambda^r g(A, A')|_p.$$

Show that, for every $g \in M_3(\mathbb{Q}_p)$ and $r \in \{1, \dots, n\}$ :

($\alpha$) If $k, k' \in K$, then $\|\Lambda^r(kgk')\| = \|\Lambda^r g\|$.

($\beta$) If $t \in T$ and $n \in N$, then $\|\Lambda^r(tn)\| \geq \|\Lambda^r(t)\|$.

($\gamma$) If $g = p^\lambda$ with $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in X^+$, then

$$\|\Lambda^r g\| = p^{-(\lambda_{3-r+1} + \dots + \lambda_3)}.$$

(c). For all $\lambda, \mu \in X$, show that

$$c_\lambda(\mu) = f_\lambda^{(B)}(p^\mu) = f_\lambda^{(B)}(p^{\overline{\mu}}).$$

(d). Let $\lambda, \mu \in X^+$. If there exists $n \in N$ such that $p^\mu n \in K p^\lambda K$, show that $\mu \leq \lambda$.

(e). Prove (i).

(f). Let $\lambda \in X^+$, and let $t = p^{\overline{\lambda}}$. For every $n \in N$, show that $tn \in KtK$ if and only if $n \in N \cap K$.

(g). Prove (ii).

(18) Show that $f \longmapsto f^\vee$ induces an isomorphism of $\mathbb{C}$-algebras $\mathscr{H} \xrightarrow{\sim} \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$. (This isomorphism is called the *Satake isomorphism*.)

*Solution.*

(1) We have seen that $\delta^{-1}$ is the modular function of $B$ in I.5.3.8(d). The second statement follows from the left invariance of $db$ and proposition I.2.8.

(2) Note that, as $B$ and $K$ are subgroups of $G$, it is equivalent to, prove that $G = BK$ and to prove that $G = KB$. (This decomposition of $G$ is called the *Iwasawa decomposition*.) We will prove the second statement, using a variant of the algorithm of Gaussian elimination (a.k.a. row reduction). In this algorithm, we apply three kinds of operations on a matrix of $\mathrm{GL}_3(\mathbb{Q}_p)$ :

   (a) swapping two rows;

   (b) multiplying a row by an element $\alpha$ of $\mathbb{Q}_p^\times$;

   (c) adding a multiple by an element $\beta$ of $\mathbb{Q}_p$ of a row to another row.

   Each of these operations corresponds to multiplication on the left by an elementary matrix. Moreover, this matrix is in $\mathrm{GL}_3(\mathbb{Z}_p)$ in case (a), in case (b) if $\alpha \in \mathbb{Z}_p^\times$, and in case (c) if $\beta \in \mathbb{Z}_p$. So it suffices to show that, if we apply a sequence of operations (a), (b), (c) with the restrictions just noted on the operations, we can always get an upper triangular matrix. So let $g = (g_{ij})$ be an element of $\mathrm{GL}_3(\mathbb{Q}_p)$. As $g$ is invertible, it has a nonzero entry in its first column. After permuting the rows of $g$ (operation (a)), we may assume that $g_{11} \neq 0$ and that, for $i = 2, 3$, we have $|g_{11}|_p \geq |g_{i1}|_p$. After adding $-g_{11}^{-1}g_{21}$ (resp. $-g_{11}^{-1}g_{31}$) times the first row of $g$ to the second (resp. third) row of $g$ (operation (b), note that we are multiplying the first row by an element of $\mathbb{Z}_p$ by the first step), we may assume that $g_{11}$ is the only nonzero element of the first column of $g$. Then at least one of $g_{22}$ and $g_{23}$ is nonzero (otherwise the rank of $g$ would be $\leq 2$), so, after possibly switching the last two rows of $g$, we may assume that $g_{22} \neq 0$ and that $|g_{22}|_p \geq |g_{23}|_p$. Then, after adding $-g_{22}^{-1}g_{23}$ times the second row to the third row, we may assume that $g_{23} = 0$. At this point, the matrix $g$ is upper triangular, so we are done.

   We now prove the second statement. Consider the group $G' = B \times K$, and its subgroup $H = \{(x, x),\ x \in B \cap K\}$. We consider the measure $\mu_{G'} = \mu_B \times \mu_K$ on $G'$; this is obviously a left Haar measure. We also put the normalized Haar measure $\mu_H$ on the compact group $H$. Consider the continuous action of $G'$ of $G$ given by $(b, k) \cdot g = bgk^{-1}$. By the first part of this question, this action is transitive. Also, the stabilizer of $1 \in G$ is clearly $H$, so we get a surjective continuous map $\varphi : G'/H \xrightarrow{\sim} G$. Let's show that $\varphi$ is also open. If $x \in G'/H$, then $((B \cap K) \times K)x$ is an open neighborhood of $x$ (because $B \cap K$ is open in $B$), and its image by $\varphi$ is $(B \cap K)\varphi(x)K$, which is open in $G$ because $K$ is an open subgroup of $G$. So $\varphi$ is open, hence it is a homeomorphism. Let $\mu$ be the image by $\varphi^{-1}$ of the fixed Haar measure on $G$. As $G$ is unimodular (by I.5.3.8(c)), the measure $\mu$ is left invariant by $G'$, so the positive linear functional $\mathscr{C}_c(G') \to \mathbb{C}$, $h \longmapsto \int_{G'/H} h^H(x)d\mu(x)$ is left invariant, so it is a positive multiple of $\mu_{G'}$, say $c\mu_{G'}$ with $c > 0$. Let $f \in \mathscr{C}_c(G)$. We define a function $h \in \mathscr{C}(G')$ by $h(b, k) = f(bk^{-1})$; we have $h(b, k) = 0$ if $b \notin (\operatorname{supp} f)K$, so $h$ has compact support. Applying problem I.5.3.6, we get

$$\int_{G'} h(b,k)d\mu_{G'}(b,k) = \int_B \int_K f(bk)dbdk = c^{-1} \int_{G'/H} h^H(x)d\mu(x).$$

Let $x \in G'/H$. We choose a preimage $(b,k) \in G'$ of $x$, so that $\varphi(x) = bk$. Then

$$h^H(x) = \int_H h((b,k)h)dh = \int_{B\cap K} f(bhh^{-1}k)dh = f(bk).$$

So

$$\int_B \int_K f(bk)dbdk = c^{-1} \int_G f(g)dg,$$

for every $f \in \mathscr{C}_c(G)$. To calculate $c$, we apply this to $f = \mathbb{1}_K$ (this is a continuous function with compact support, because $K$ is an open compact subgroup of $G$ by I.5.1.4(m)). The left hand side is $\mu_H(H)\mu_K(K) = 1$, and the right hand side is $\mu_G(K) = 1$ (by the choice of $\mu_G$). So $c = 1$.

Finally, we prove the last formula by applying I.5.3.6 to the subgroups $T$ and $N$ of $B$ : we get that a positive constant $c'$ such that, for every $f \in \mathscr{C}_c(B)$, we have

$$\int_B f d\mu_B = c' \int_T \int_N f(tn)d\mu_T(t)d\mu_N(n).$$

To show that $c' = 1$, it suffices to calculate both sides of this equality for $f = \mathbb{1}_{B\cap K}$ and to use the (easy) fact that $B \cap K = (T \cap K)(N \cap K)$.

(3) We first note the following easy fact : Let $(x_1, x_2, x_3)$ be a family of elements of $\mathbb{Q}_p^3$; then this family is linearly independent over $\mathbb{Z}_p$ if and only if it is linearly independent over $\mathbb{Q}_p$. Indeed, linear independence over $\mathbb{Q}_p$ clearly implies linear independence over $\mathbb{Z}_p$ (because $\mathbb{Z}_p \subset \mathbb{Q}_p$). Conversely, suppose that $(x_1, x_2, x_3)$ is linearly independent over $\mathbb{Z}_p$; if we have $a_1x_1 + a_2x_2 + a_3x_3 = 0$ with $a_1, a_2, a_3 \in \mathbb{Q}_p$, then there exists $m \in \mathbb{Z}$ such that $p^m a_1, p^m a_2, p^m a_3 \in \mathbb{Z}_p$, and the relation $p^m a_1 x_1 + p^m a_2 x_2 + p^m a_3 x_3 = 0$ implies that $p^m a_1 = p^m a_2 = p^m a_3 = 0$, hence $a_1 = a_2 = a_3 = 0$.

Let $\mathscr{L}$ be the set of free $\mathbb{Z}_p$-submodules of rank 3 of $\mathbb{Q}_p^3$, and let $L_0 = \mathbb{Z}_p e_1 + \mathbb{Z}_p e_2 + \mathbb{Z}_p e_3 = \mathbb{Z}_p^3 \in \mathscr{L}$. If $L \in \mathscr{L}$ and $g \in \mathrm{GL}_3(\mathbb{Q}_p)$, then $g(L)$ is also an element of $\mathscr{L}$. Indeed, if $(x_1, x_2, x_3)$ is a $\mathbb{Z}_p$-basis of $L$, then the family $(x_1, x_2, x_3)$ is also linearly independent over $\mathbb{Q}_p$, so the family $(g(x_1), g(x_2), g(x_3))$ of $\mathbb{Q}_p^3$ is linearly independent over $\mathbb{Q}_p$, hence over $\mathbb{Z}_p$, so the $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p^3$ that it generates is an element of $\mathscr{L}$. This shows that $(g, L) \longmapsto g(L)$ defines a left action of $G$ on $\mathscr{L}$. Moreover, the stabilizer of $L_0$ is clearly $\mathrm{GL}_3(\mathbb{Z}_p)$.

We show that this action if transitive, which will give the desired bijection $G/K \overset{\sim}{\to} \mathscr{L}$. Let $L \in \mathscr{L}$, and let $(x_1, x_2, x_3)$ be a basis of $L$ over $\mathbb{Z}_p$. Then we have seen that the family $(x_1, x_2, x_3)$ is also linearly independent over $\mathbb{Q}_p$. So $(x_1, x_2, x_3)$ is a basis of the $\mathbb{Q}_p$-vector space $\mathbb{Q}_p^3$, hence there exists $g \in \mathrm{GL}_3(\mathbb{Q}_p)$ such that $x_i = g(e_i)$ for $i = 1, 2, 3$, and then we have $L = g(L_0)$.

(4) We first prove that $G = \bigcup_{\lambda \in X^+} Kp^\lambda K$. Let $g \in G$. Let $x_1, x_2, x_3 \in \mathbb{Q}_p^3$ be the columns of $g$, and let let $L$ be the sub-$\mathbb{Z}_p$-module of $\mathbb{Q}_p^3$ generated by $(x_1, x_2, x_3)$; in the notation of the solution of (3), this is $g(L_0)$. As $\mathbb{Q}_p = p^{\mathbb{Z}}\mathbb{Z}_p$, we can choose $m \in \mathbb{Z}$ such that the entries of the matrix $p^m g$ are all in $\mathbb{Z}_p$. Then the sub-$\mathbb{Z}_p$-module $L'$ of $\mathbb{Q}_p^3$ generated by $(p^m x_1, p^m x_2, p^m x_3)$ satisfies $L_0 \supset L' = p^m L$. By Theorem 4 of chapter 12 of Dummit and Foote, there exists a basis $(y_1, y_2, y_3)$ of $L_0$ and elements $a_1, a_2, a_3 \in \mathbb{Z}_p - \{0\}$ such that $a_3 | a_2 | a_1$ and that $(a_1 y_1, a_2 y_2, a_3 y_3)$ is a basis of $L'$. As each element $a$ of $\mathbb{Z}_p - \{0\}$ can be written (in a unique way) $a = p^n u$ with $n\mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}_p^\times$, we may assume that $a_i = p^{n_i}$ with $n_1, n_2, n_3 \in \mathbb{Z}_{\geq 0}$ and $n_1 \geq n_2 \geq n_3$. Let $g'$ (resp. $k$) be the matrix with columns $a_1 y_1, a_2 y_2, a_3 y_3$ (resp. $y_1, y_2, y_3$) and $t$ the diagonal matrix with diagonal entries $a_1, a_2, a_2$; in other words, we have $t = p^{(n_1, n_2, n_3)}$. Then $k \in K$ and $g' = kt$. Also, as $L' = g'(L_0) = p^m L = p^m g(L_0)$, question (3) implies that there exists $k' \in K$ such that $p^m g = g'k'$. So we get

$$g = p^{-m} g' k' = kp^{(n_1 - m, n_2 - m, n_3 - m)} k' \in Kp^{(n_1 - m, n_2 - m, n_3 - m)} K.$$

Note that we have also shown that, if $m = 0$ (for example if all the entries of $g$ are already in $\mathbb{Z}_p$), so that $L \subset L_0$, then we have $L_0 / L \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times (\mathbb{Z}/p^{n_2}\mathbb{Z}) \times (\mathbb{Z}/p^{n_3}\mathbb{Z})$.

Now we show that the union is a disjoint union. Let $\lambda, \lambda' \in X^+$, and suppose that $Kp^\lambda K \cap Kp^{\lambda'} K \neq \varnothing$. After multiplying $p^\lambda$ and $p^{\lambda'}$ by $p^m$ with $m \in \mathbb{Z}$ big enough, we may assume that $\lambda$ and $\lambda'$ are in $\mathbb{Z}_{\geq 0}^3$. Let $g \in Kp^\lambda K \cap Kp^{\lambda'} K$, and let $L = g(L_0)$. As the entries of $g$ are elements of $\mathbb{Z}_p$ (by the assumption on $\lambda$), we have $L \subset L_0$. Write $\lambda = (n_1, n_2, n_3)$ and $\lambda' = (n_1', n_2', n_3')$, with $n_1 \geq n_2 \geq n_3$ and $n_1' \geq n_2' \geq n_3'$. By the previous paragraph, we have

$$L_0/L \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times (\mathbb{Z}/p^{n_2}\mathbb{Z}) \times (\mathbb{Z}/p^{n_3}\mathbb{Z}) \simeq (\mathbb{Z}/p^{n_1'}\mathbb{Z}) \times (\mathbb{Z}/p^{n_2'}\mathbb{Z}) \times (\mathbb{Z}/p^{n_3'}\mathbb{Z}).$$

By Theorem 9 of Chapter 12 of Dummit and Foote, this implies that $n_i = n_i'$ for $i = 1, 2, 3$, i.e. that $\lambda = \lambda'$.

(5) Consider the map $\theta : G \to G$, $x \longmapsto (x^T)^{-1}$. This is a continuous isomorphism of groups, hence a homeomorphism because $\theta^{-1} = \theta$. We also have $\theta(K) = K$. Let $g \in G$. By (4), we can write $g = kp^\lambda k'$, with $k, k' \in K$ and $\lambda \in \mathbb{Z}^3$. Then

$$\theta(g) = \theta(k) p^{-\lambda} \theta(k') = \theta(k) k' g^{-1} k \theta(k') \in K g^{-1} K.$$

So, by proposition V.2.5, $(G, K)$ is a Gelfand pair.

(6) The space of all functions $f : G \to \mathbb{C}$, with the action of $G$ given by $x \cdot f = R_x f$, is a representation of $G$. We check that $V_z$ is a subrepresentation of this space. First, it is a vector subspace :

- the function $0$ is in $V_z$;
- condition (i) is clearly stable by linear combinations;

- let $f, f' \in V_z$, and let $K_1$ and $K_1'$ be open compact subgroups of $G$ such that $f$ (resp. $f'$) is right $K_1$-invariant (resp. right $K_1'$-invariant); then $K_1 \cap K_1'$ is a compact subgroup of $G$, and any linear combination of $f$ and $f'$ is right $K_1 \cap K_1'$-invariant, so it satisfies condition (ii).

Now we check that $V_z$ is $G$-invariant. Let $f \in V_z$ and $x \in G$. For every $b \in B$ and every $g \in G$, we have

$$(R_x f)(bg) = f(bgx) = \chi_z(b)\delta(b)^{1/2} f(gx) = \chi_z(b)\delta(b)^{1/2} R_x f(g),$$

so $R_x f$ satisfies condition (i). Let $K_1$ be an open compact subgroup of $G$ such that $f$ is right $K_1$-invariant. Then, for every $g \in G$ and $k \in K_1$, we have

$$R_x f(gxkx^{-1}) = f(gxk) = f(gx) = R_x f(g),$$

so $R_x f$ is right invariant under the open compact subgroup $xK_1x^{-1}$ of $G$, and so it satisfies condition (ii).

Finally, we compute the dimension of $V_z^K$. Remember that the map $G' := B \times K \to G$, $(b,k) \longmapsto bk^{-1}$ identifies $G$ with the quotient $G'/H$, where $H = \{(x,x),\ x \in B \cap K\}$. Consider the function
$varphi'_z : G' \to \mathbb{R}_{>0}$, $(b,k) \longmapsto \chi_z(b)\delta(b)^{1/2}$. This is a continuous morphism of groups, so it is trivial on the compact subgroup $H$, and so it descends to the quotient $G'/H$ and defines a continuous function from $G$ to $\mathbb{R}_{>0}$, which we will denote by $\varphi_z$. By construction, the function $\varphi_z$ satisfies

$$\varphi_z(bk) = \chi_z(b)\delta(b)^{1/2}$$

for every $b \in B$ and every $k \in K$, so $\varphi_z(1) = 1$ and $\varphi_z \in V_z^K$. To finish the proof, we show that $V_z^K$ is generated by $\varphi_z$. Let $f \in V_z^K$. If $g \in G$, then, by question (2), we can find $b \in B$ and $k \in K$ such that $g = bk$, and then

$$f(g) = f(b) = \chi_z(b)\delta(b)^{1/2} f(1) = \varphi_z(g) f(1).$$

So $f$ is a multiple of $\varphi_z$.

(7) Fix $z \in (\mathbb{C}^\times)^3$.

Let $f \in \mathscr{H}$. We define $\widetilde{f} \in \mathscr{H}$ by $\widetilde{f}(x) = f(x^{-1})$. Let's show that $\varphi_z * \widetilde{f} = f^\vee(z)\varphi_z$. First note that $\varphi_z * \widetilde{f}$ is right $K$-invariant, because $\widetilde{f}$ is (this follows from proposition V.1.8). Let $x \in G$ and $b \in B$. Then

$$\varphi_z * \widetilde{f}(bx) = \int_G \varphi_z(bxy) f(y) dy = \int_G \chi_z(b)\delta(b)^{1/2} \varphi_z(xy) f(y) dy = \chi_z(b)\delta(b)^{1/2} \varphi_z * \widetilde{f}(x)$$

(because $\varphi_z \in V_z$). So $\varphi_z * \widetilde{f} \in V_z^K$, which implies that $\varphi_z * \widetilde{f}$ is a scalar multiple of $\varphi_z$ by question (6). To find the scalar, we evaluate both functions at $1$ : we have $\varphi_z(1) = 1$, and

$$\varphi_z * \widetilde{f}(1) = \int_G \varphi_z(y) f(y) dy = f^\vee(z).$$

Now let $f_1, f_2 \in \mathscr{H}$. Then, for every $x \in G$, we have

$$\begin{aligned}
\widetilde{f_1 * f_2}(x) &= f_1 * f_2(x^{-1}) \\
&= \int_G f_1(x^{-1}y^{-1}) f_2(y) dy \\
&= \int_G \widetilde{f}_1(yx)\widetilde{f}_2(y^{-1})dy = (\widetilde{f}_2 * \widetilde{f}_1)(x) \quad \text{(because } G \text{ is unimodular)} \\
&= (\widetilde{f}_1 * \widetilde{f}_2)(x) \quad \text{(because } (G,K) \text{ is a Gelfand pair),}
\end{aligned}$$

so $\widetilde{f_1 * f_2} = \widetilde{f}_1 * \widetilde{f}_2$. (Actually, the fact that $\widetilde{f_1 * f_2 -} = \widetilde{f}_2 * \widetilde{f}_1$ would be good enough for our purposes.) Using the calculation of the previous paragraph, we get

$$(f_1 * f_2)^\vee(z) = (\varphi_z * \widetilde{f_1 * f_2})(1) = (\varphi_z * \widetilde{f}_1 * \widetilde{f}_2)(1) = ((f_1^\vee(z)\varphi_z) * \widetilde{f}_2)(1) = f_1^\vee(z) f_2^\vee(z).$$

(8) Note that $T \cap K$ is the group of invertible diagonal matrices $t$ such that both $t$ and $t^{-1}$ have all their entries in $\mathbb{Z}_p$, i.e. such that all the entries of $t$ are in $\mathbb{Z}_p^\times$. So the statement follows from the fact that $\mathbb{Q}_p^\times = \coprod_{m \in \mathbb{Z}} p^m \mathbb{Z}_p^\times$ (applied to each diagonal entries of the matrices), and this fact follows from I.5.1.4(i).

(9) The map $f \longmapsto f^\vee$ is clearly linear in $f \in \mathscr{H}_T$. Let's show that it is a morphism of algebras. Let $f_1, f_2 \in \mathscr{H}_T$, and let $z \in (\mathbb{C}^\times)^3$. Then

$$\begin{aligned}
(f_1 * f_2)^\vee(z) &= \int_T (f_1 * f_2)(t)\chi_z(t) dt \\
&= \int_{T \times T} f_1(t') f_2((t')^{-1}t)\chi_z(t) dt dt' \\
&= \int_{T \times T} f_1(t') f_2(t) \chi_z(t't) dt dt' \\
&\left(\int_T f_1(t')\chi_z(t')dt'\right)\left(\int_T f_2(t)\chi_z(t)dt\right) \quad \text{(because } \chi_z \text{ is multiplicative)} \\
&= f_1^\vee(z) f_2^\vee(z),
\end{aligned}$$

as desired.

By question (8), the family $(\mathbb{1}_{(T\cap K)p^\lambda})_{\lambda \in X}$ is a basis of $\mathscr{H}_T$. Let $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in X$, and let $g_\lambda = \mathbb{1}_{(T\cap K)p^\lambda}$. Then, for every $z = (z_1, z_2, z_3) \in (\mathbb{C}^\times)^3$, we have

$$g_\lambda^\vee(z) = \int_{(T\cap K)p^\lambda} \chi_z(t) dt = \mathrm{vol}(T \cap K)\chi_z(p^\lambda) = z_1^{\lambda_1} z_2^{\lambda_2} z_3^{\lambda_3}.$$

As the functions of the form $(z_1, z_2, z_3) \longmapsto z_1^{\lambda_1} z_2^{\lambda_2} z_3^{\lambda_3}$, for $(\lambda_1, \lambda_2, \lambda_3) \in X$, for a basis of $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]$, this shows that the linear transformation $f \longmapsto f^\vee$ sends a basis of $\mathscr{H}_T$ to a basis of $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]$, so it is an isomorphism from $\mathscr{H}_T$ to $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]$.

(10) By I.5.2.2, the open compact subgroups of $G$ form a basis of neighborhoods of 1. Let $f \in \mathscr{C}_c(G)$. By definition of $\mathscr{C}_c(G)$, for every $x \in G$, there exists an open compact subgroup $K_x$ of $G$ such that $f$ is constant on $K_x^2 x K_x^2$. We have $\operatorname{supp} f \subset \bigcup_{x \in \operatorname{supp} x} K_x x K_x$ and $\operatorname{supp} f$ is compact, so there exist $x_1, \dots, x_m \in \operatorname{supp} f$ such that $\operatorname{supp} f \subset \bigcup_{i=1}^m K_{x_i} x_i K_{x_i}$. Let $L = \bigcap_{i=1}^m K_{x_i}$; this is an open compact subgroup of $G$. Let's show that $f$ is bi-$L$-invariant. Let $x \in G$. If $x \in \operatorname{supp} f$, then there exists $i \in \{1, \dots, m\}$ such that $x \in K_{x_i} x_i K_{x_i}$. Then $LxL \subset K_{x_i}^2 x_i K_{x_i}^2$, so $f$ is constant on $LxL$. If $x \notin \operatorname{supp} f$, we want to show that $LxL \cap (\operatorname{supp} f) = \varnothing$. But suppose that there exist $l, l' \in L$ such that $lxl' \in \operatorname{supp} f$, then we know that $f$ is constant on $L(lxl')L = LxL$ by what we have just seen, and in particular $f$ cannot vanish at $x$. So $LxL \cap (\operatorname{supp} f) = \varnothing$, and in particular $f$ is constant (and equal to 0) on $LxL$.

Now we show that $f^{(B)}$ is bi-invariant under $L \cap T$; this implies that $f^{(B)}$ is locally constant, as $L \cap T$ is an open compact subgroup of $T$. As $T$ is commutative, we only need to show that $f^{(B)}$ is left invariant under $K \cap T$, but then this follows immediately from the definition and from the fact that $\delta : T \to \mathbb{R}_{>0}$ is multiplicative (because then $\delta$ must be trivial on the compact subgroup $K \cap T$ of $T$).

Finally, we need to show that $f^{(B)}$ has compact support. Let $t \in T$ be such that $f^{(B)}(t) \neq 0$. Then there exists $n \in N$ such that $tn \in B \cap (\operatorname{supp} f)$. In particular, $t$ is in the image of the compact set $B \cap (\operatorname{supp} f)$ by the continuous projection map $B \to T \simeq B/N$. This image is compact and contains the support of $f^{(B)}$, so $f^{(B)}$ has compact support.

If $f \in \mathscr{H}$, then we can take $L = K$ in the proof of the first assertion, and we get that $f^{(B)}$ is bi-invariant under $K \cap T$, i.e. that $f^{(B)} \in \mathscr{H}_T$.

(11) Let $z \in (\mathbb{C}^\times)^3$. Note that the multiplicative functions $\delta$ and $\chi_z$ are both trivial on $N$. So, if $t \in T$ and $n \in N$, then we have $\varphi_z(tn) = \chi_z(t)\delta(t)^{1/2}$.

Let $f \in \mathscr{H}$. Then, using the integration formula of question (2), we get

$$\begin{aligned}
f^\vee(z) &= \int_T \int_N \int_K f(tnk)\varphi_z(tnk)dtdndk \\
&= \int_T \int_N f(tn)\varphi_z(tn)dtdn \quad \text{(because both } f \text{ and } \varphi_z \text{ are right } K\text{-invariant)} \\
&= \int_T \int_N f(tn)\chi_z(t)\delta(t)^{1/2}dtdn \\
&= \int_T f^{(B)}(t)\chi_z(t)dt \\
&= (f^{(B)})^\vee(z).
\end{aligned}$$

(12) We could actually do the calculation directly (by writing the formula for $ntn^{-1}t^{-1}$ and using the change of variables), but we'll take the hint, as it generalizes better to $\mathrm{GL}_n(\mathbb{Q}_p)$ for arbitrary $n$.

First we note that the subgroup $U$ of $N$ is normal (and even central) and isomorphic to the additive group $\mathbb{Q}_p$. In particular, we have the Haar measure $\mu_U = \lambda$ on $U$ given by I.5.3.4 (which is normalized by requiring that $\mathbb{Z}_p$ have volume 1).

Next, we note that the map $N \to \mathbb{Q}_p^2$, $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \longmapsto (a,c)$ induces an isomorphism of topological groups from $N/U$ to $\mathbb{Q}_p^2$, and that the action by left translations of $N$ on $N/U$ corresponds via this isomorphism to the action of $N$ on $\mathbb{Q}_p^2$ given by $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot (x,y) = (a+x, c+y)$. In particular, the measure $\lambda^2$ on $\mathbb{Q}_p^2$ gives a regular Borel measure $d\mu_{N/U}$ on $N/U$ that is left invariant by $N$. Then the positive linear function $\mathscr{C}_c(N) \to \mathbb{C}$, $f \longmapsto \int_{N/U}\int_U f(nu)d\mu_{N/U}(n)d\mu_U(u)$ is left invariant, hence it is a multiple of the Haar measure $\mu_N$. Also, by taking $f = \mathbb{1}_{K\cap N}$ (and using the fact that $K \cap U = \mathbb{Z}_p$ and $(K\cap N)/(K\cap U)$ corresponds to the subgroup $\mathbb{Z}_p^2$ of $\mathbb{Q}_p^2$ in the isomorphism above), we see that this positive linear functional is actually equal to $\mu_N$, which proves the integration formula of the hint.

In the calculation that follows, we will identify $U$ to $\mathbb{Q}_p$ and $N/U$ to $\mathbb{Q}_p^2$. Let $t = \begin{pmatrix} x_1 & 0 & 0 \\ 0 & x_2 & 0 \\ 0 & 0 & x_3 \end{pmatrix} \in T$. Note that the map $N \to N$, $n \longmapsto ntn^{-1}t^{-1}$ preserves $U$, so it induces maps $U \to U$ and $N/U \to N/U$. If $u \in U = \mathbb{Q}_p$, we have $utu^{-1}t^{-1} = (1-x_1x_3^{-1})u$. On the other hand, if $n \in N$ and if the image of $n$ in $N/U = \mathbb{Q}_p^2$ is $(a,b)$, then the image of $ntn^{-1}t^{-1}$ in $N/U$ is $(a(1-x_1x_2^{-1}), b(1-x_2x_3^{-1}))$.

Suppose that $D(t) \neq 0$. By the change of variable formula proved in I.5.3.8, we have :

- for every $f \in \mathscr{C}_c(U)$,

$$\int_U f(u)du = |1 - x_1x_3^{-1}|_p \int_U f(utu^{-1}t^{-1})du;$$

- for every $f \in \mathscr{C}_c(N/U)$,

$$\int_{N/U} f(n)dn = |1 - x_1x_2^{-1}|_p|1 - x_2x_3^{-1}|_p \int_{N/U} f(ntn^{-1}t^{-1})dn.$$

Also, using the fact that $U$ is central in $N$ and that $t^{-1}Ut = U$, we see that, for every $n \in N$ and every $u \in U$, we have

$$(ntn^{-1}t^{-1})(utu^{-1}t^{-1}) = ntn^{-1}(t^{-1}ut)u^{-1}t^{-1} = nt(t^{-1}ut)u^{-1}n^{-1}t^{-1} = nut(nu)^{-1}t^{-1}.$$

Let $f \in \mathscr{C}_c(N)$. Then

$$\begin{aligned}
\int_N f(n)dn &= \int_U \int_{N/U} f(nu)d\mu_{N/U}(n)d\mu_U(u) \\
&= |1 - x_1x_2^{-1}|_p|1 - x_2x_3^{-1}|_p|1 - x_1x_3^{-1}|_p \\
&\qquad \int_U \int_{N/U} f((ntn^{-1}t^{-1})(utu^{-1}t^{-1}))d\mu_{N/U}(n)d\mu_U(u) \\
&= |1 - x_1x_2^{-1}|_p|1 - x_2x_3^{-1}|_p|1 - x_1x_3^{-1}|_p \\
&\qquad \int_U \int_{N/U} f(nut(nu)^{-1}t^{-1})d\mu_{N/U}(n)d\mu_U(u) \\
&= |1 - x_1x_2^{-1}|_p|1 - x_2x_3^{-1}|_p|1 - x_1x_3^{-1}|_p \int_N f(ntn^{-1}t^{-1})dn.
\end{aligned}$$

To finish the proof, it suffices to notice that

$$|1 - x_1x_2^{-1}|_p|1 - x_2x_3^{-1}|_p|1 - x_1x_3^{-1}|_p = D(t)^{1/2}\delta(t)^{1/2}.$$

We will actually need a variant of the formula of this question in question (13), so let's prove it now. Define a function $\widetilde{f} \in \mathscr{C}_c(N)$ by $\widetilde{f}(n) = f(n^{-1})$. Applying the formula we just obtained to $\widetilde{f}$ and using the fact that $N$ is unimodular, we get :

$$\begin{aligned}
\int_N f(n)dn &= \int_N f(n^{-1})dn \\
&= D(t)^{1/2}\delta(t)^{1/2} \int_N \widetilde{f}(ntn^{-1}t^{-1})dn \\
&= D(t)^{1/2}\delta(t)^{1/2} \int_N f(tnt^{-1}n^{-1})dn \\
&= D(t)^{1/2}\delta(t)^{1/2} \int_N f(tn^{-1}t^{-1}n)dn
\end{aligned}$$

(13) Let $f \in \mathscr{H}$, and let $h \in \mathscr{C}_c(T \setminus G)$ be the function defined by $h(g) = f(g^{-1}tg)$. By I.5.1.1(d), we can find $h' \in \mathscr{C}_c(G)$ such that ${}^T h' = h$. By I.5.1.1(f), we have

$$O_t(f) = \int_{T\backslash G} h(g)d\mu_{T\backslash G}(g) = \int_G h'(g)dg.$$

Using question (2), we get :

$$\begin{aligned}
O_t(f) &= \int_T \int_N \int_K h'(tnk)dtdndk \\
&= \int_N \int_K h(nk)dndk \quad \text{(by definition of } {}^T h'\text{)} \\
&= \int_N \int_K f(k^{-1}n^{-1}tnk)dndk \\
&= \int_N f(n^{-1}tn)dn \quad \text{(because } f \text{ is bi-}K\text{-invariant)} \\
&= \int_N f(t(t^{-1}n^{-1}tn))dn \\
&= D(t^{-1})^{1/2}\delta(t^{-1})^{1/2} \int_N f(tn)dn \quad \text{(by the end of the proof of (12)} \\
&= D(t)^{-1/2} f^{(B)}(t),
\end{aligned}$$

where we used the facts that $\delta(t^{-1}) = \delta(t)^{-1}$ and $D(t^{-1}) = D(t)$, which are both obvious on the definitions.

(14) Let $f \in \mathscr{H}$. Then we have $f^\vee = (f^{(B)})^\vee$ by question (11), so $f^\vee \in \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]$ by question (9).

We want to show that $f^\vee$ is symmetric in the variables $z_1, z_2, z_3$. So let $\sigma \in \mathfrak{S}_3$; we write $\sigma^{-1}(z) = (z_{\sigma(1)}, z_{\sigma(2)}, z_{\sigma(3)})$. If $t \in T$ has diagonal entries $x_1, x_2, x_3$, then

$$\chi_{\sigma^{-1}(z)}(t) = z_{\sigma(1)}^{v_p(x_1)} z_{\sigma(2)}^{v_p(x_2)} z_{\sigma(3)}^{v_p(x_3)} = z_1^{v_p(x_{\sigma^{-1}(1)})} z_2^{v_p(x_{\sigma^{-1}(2)})} z_3^{v_p(x_{\sigma^{-1}(3)})} = \chi_z(A^{-1}tA),$$

where $A$ is the permutation matrix associated to $\sigma$. Applying this to the formula defining $(f^{(B)})^\vee(z)$, we get

$$f^\vee(\sigma^{-1}(z)) = \int_T f^{(B)}(t)\chi_z(A^{-1}tA)dt = \int_T f^{(B)}(AtA^{-1})\chi_z(t)dt,$$

where the second equality comes from the fact that $dt$ is the product of the Haar measures on the three factors $\mathbb{Q}_p^\times$ of $T$, so it is invariant by permutation of these factors. So, to show that $f^\vee(\sigma^{-1}(z)) = f^\vee(z)$, it suffices to prove that $f^{(B)}(AtA^{-1}) = f^{(B)}(t)$. We use the equality of question (14). First note that it is obvious on the definition of $D(t)$ that the value of $D(t)$ doesn't change if we permute the diagonal entries of $t$. So it suffices to prove that $O_t(f) = O_{AtA^{-1}}(f)$. Using the fact that $A \in \mathrm{GL}_3(\mathbb{Z}) \subset \mathrm{GL}_3(\mathbb{Z}_p)$ (hence $f$ is invariant by left and right translation by $A$ and $A^{-1}$), the fact that the Haar measure on $G$ is invariant by left and right translations (because $G$ is unimodular), and the fact (which we have just noted) that the Haar measure on $T$ is invariant by conjugation by $A^{\pm 1}$, we see that

$$O_{AtA^{-1}}(f) = \int_{T\backslash G} f(g^{-1}AtA^{-1}g)dg = \int_{T\backslash G} f((A^{-1}gA)^{-1}t(A^{-1}gA))dg$$
$$= \int_{T\backslash G} f(g^{-1}tg)dg = O_t(f).$$

(15) As $K$ is open and compact, every function $f_\lambda$ is in $\mathscr{C}_c(G)$; also, $f_\lambda$ is clearly bi-$K$-invariant, so it is in $\mathscr{H}$.

Now let $f \in \mathscr{H}$. By question (4), the function $f$ is constant on every set $Kp^\lambda K$, $\lambda \in X^+$; also, as all these sets are open and $f$ has compact support, the support of $f$ must be a finite union of sets of the form $Kp^\lambda K$. This shows that $f$ is a (finite) linear combination of functions $f_\lambda$, $\lambda \in X^+$, so the family $(f_\lambda)_{\lambda \in X^+}$ generates $\mathscr{H}$. As the supports of the $f_\lambda$ (for $\lambda \in X^+$) are disjoint (by question (4)) again, this family is linearly independent, so it is a basis of $\mathscr{H}$.

(16) First, the family $(c_\lambda)_{\lambda \in X^+}$ is linearly independent, because the sets of monomials that appear in its elements are pairwise disjoint.

Let's show that this family generates $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$ (it is clearly contained in this space). Let $f \in \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$. We can find a family of complex numbers $(a_\lambda)_{\lambda \in \mathbb{Z}^3}$ such that all but a finite number of the $a_\lambda$ are 0 and that $f = \sum_{\lambda \in I} a_\lambda z^\lambda$. Moreover, as $f$ is symmetric, we must have $a_{\sigma(\lambda)} = a_\lambda$ for every $\lambda \in I$ and every $\sigma \in \mathfrak{S}_3$. For every $\lambda \in \mathbb{Z}^3$, there is a unique element of $\{\sigma(\lambda),\ \sigma \in \mathfrak{S}_3\}$ that is in $X^+$. So $f$ is a linear combination of the $c_\lambda$; more precisely, we have $f = \sum_{\lambda \in X^+} b_\lambda c_\lambda$, where

$$b_\lambda = \frac{1}{|\{\sigma \in \mathfrak{S}_3 \mid \sigma(\lambda) = \lambda\}|} \sum_{\sigma \in \mathfrak{S}_3} a_\lambda.$$

(17) (a). Let $k = (k_{ij}) \in \mathrm{GL}_3(\mathbb{Z}_p)$. Then, for all $i, j \in \{1, 2, 3\}$, we have $(kg)_{ij} = \sum_{r=1}^3 k_{ir} g_{rj}$ and $(gk)_{ij} = \sum_{r=1}^3 g_{ir} k_{rj}$, so

$$|(kg)_{ij}|_p \leq \sup_{1 \leq r \leq 3} |k_{ir}|_p |g_{rj}|_p \leq \sup_{1 \leq r \leq 3} |g_{rj}|_p \leq \|g\|$$

and

$$|(gk)_{ij}|_p \leq \sup_{1 \leq r \leq 3} |g_{ir}|_p |k_{rj}|_p \leq \sup_{1 \leq r \leq 3} |g_{ir}|_p \leq \|g\|$$

(because all the entries of $k$, being elements of $\mathbb{Z}_p$, have $p$-adic absolute value $\leq 1$). This implies that $\|kg\| \leq \|g\|$ and $\|gk\| \leq \|g\|$. As $k^{-1}$ is also in $\mathrm{GL}_3(\mathbb{Z}_p)$, we can apply this result to $k^{-1}$ and $kg$ (resp. $gk$) to get $\|g\| \leq \|kg\|$ (resp. $\|g\| \leq \|gk\|$), so we have finally $\|kg\| = \|g\| = \|gk\|$. This implies the statement.

(b). ($\alpha$) What is hidden behind this proof if the fact that, for all $g, h \in \mathrm{GL}_3(\mathbb{Q}_p)$ and every $r$, we have $\Lambda^r(gh) = \Lambda^r(g)\Lambda^r(h)$; as $\Lambda^r(h)$ has coefficients in $\mathbb{Z}_p$ if $h$ does, we can then just use the same proof as in (a) to get the desired statement.

The reason for the compatibility of $\Lambda^r$ with products is that $\Lambda^r g$ is the matrix of the action of $g$ on the $r$th exterior power of $\mathbb{Q}_p^3$, but in our case, we can also prove it directly. There is nothing to prove if $r = 1$ (because $\Lambda^1 g = g$) or $r = 3$ (because $\Lambda^3 g = \det(g)$), so we may assume $r = 2$. Let $g, h \in \mathrm{GL}_3(\mathbb{Q}_p)$ and $A, A' \in \Omega_2$. We want to show that $\Lambda^2(gh)_{A,A'} = \sum_{A'' \in \Omega_2} \Lambda^2(g)_{A,A''} \Lambda^2(h)_{A'',A}$. We may assume that $A = A' = \{1, 2\}$ (the other cases are similar). Then $\sum_{A'' \in \Omega_2} \Lambda^2(g)_{A,A''} \Lambda^2(h)_{A'',A}$ is equal to

$$(g_{11}g_{22} - g_{12}g_{21})(h_{11}h_{22} - h_{12}h_{21}) + (g_{11}g_{23} - g_{13}g_{21})(h_{11}h_{23} - h_{13}h_{21}) \\ + (g_{12}g_{23} - g_{13}g_{22})(h_{12}h_{23} - h_{13}h_{22}),$$

while $\Lambda^2(gh)_{A,A'}$ is equal to

$$(g_{11}h_{11} + g_{12}h_{21} + g_{13}h_{31})(g_{21}h_{12} + g_{22}h_{22} + g_{23}h_{32}) \\ -(g_{11}h_{12} + g_{12}h_{22} + g_{13}h_{32})(g_{21}h_{11} + g_{22}h_{21} + g_{23}h_{31}).$$

It is easy to check that these two expressions are equal.

($\beta$) We have seen in the proof of ($\alpha$) that $\Lambda^r(tn) = \Lambda^r(t)\Lambda^r(n)$. As $\Lambda^r(t)$ is diagonal and the diagonal entries of $\Lambda^r(n)$ are all equal to 1, the diagonal entries of $\Lambda^r(tn)$ are equal to the diagonal entries $\Lambda^r(t)$. So $\|\Lambda^r(tn)\|$ is at least the supremum of the $p$-adic absolute values of the diagonal entries of $\Lambda^r t$, and this last number is $\|\Lambda^r t\|$.

($\gamma$) We already noted that $\Lambda^r g$ is diagonal. So

$$\|\Lambda^r g\| = \sup_{A \in \Omega_r} \left| p^{\sum_{i \in A} \lambda_i} \right|_p = p^{-\inf_{A \in \Omega_r} \sum_{i \in A} \lambda_i}.$$

As $\lambda_1 \geq \lambda_2 \geq \lambda_3$, we have

$$\inf_{A \in \Omega_r} \sum_{i \in A} \lambda_i = \lambda_{3-r+1} + \ldots + \lambda_3.$$

(c). First we note that we can prove as in question (15) that $(\mathbb{1}_{(K \cap T)p^\lambda})_{\lambda \in X}$ is a basis of the $\mathbb{C}$-vector space $\mathscr{H}_T$.

Now let's show that, for every $h \in \mathscr{H}_T$, we have $h^\vee = \sum_{\mu \in X} h(p^{\overline{\mu}}) z^\mu$. As both sides are linear in $h$, we may assume that $h = \mathbb{1}_{(K \cap T)p^\lambda}$ for some $\lambda \in X$. Then, for every $z \in (\mathbb{C}^\times)^3$, we have :

$$h^\vee(z) = \int_T h(t)\chi_z(t)dt = \int_{(T \cap K)p^\lambda} \chi_z(t)dt.$$

As $\chi_z$ is constant on the set $(K \cap T)p^\lambda$ (because $T \cap K$ is the group of diagonal matrices with entries in $\mathbb{Z}_p^\times$, and we have $|u|_p = 1$ for every $u \in \mathbb{Z}_p^\times$), and as this set has volume 1, we get

$$h^\vee(z) = \chi_z(p^\lambda) = z^\lambda = h(p^\lambda)z^\lambda = \sum_{\mu \in X} h(p^\mu) z^\mu$$

(for the last equality, note that $h(p^\mu) = 0$ for every $\mu \neq \lambda$, because the sets $(K \cap T)p^\mu$ are pairwise disjoint by question (8)).

Now let $f \in \mathscr{H}$. By applying the statement proved in the previous paragraph to $f^{(B)}$, we get $c_\lambda(\mu) = f_\lambda^{(B)}(p^\mu)$. But $p^{\overline{\mu}} = Ap^\mu A^{-1}$ where $A$ is the permutation matrix associated to $\sigma = (13)$ (i.e. the matrix with antidiagonal entries 1 and all other entries 0), and we have seen in the proof of question (14) that $f^{(B)}(AtA^{-1}) = f^{(B)}(t)$ for every $f \in \mathscr{H}$ and every $t \in T$. So we are done.

(d). Suppose that $p^\mu n \in Kp^\lambda K$ for some $n \in N$. Then $\det(p^\mu) = \det(p^\mu n) \in \mathbb{Z}_p^\times \det(p^\lambda)$ (because $\det(K) \subset \mathbb{Z}_p^\times$), so $\|\det(p^\mu)\|_p = \|\det(p^\lambda)\|_p$, which gives $\mu_1 + \mu_2 + \mu_3 = \lambda_1 + \lambda_2 + \lambda_3$. Also, by (b), we have, for every $r \in \{1, 2, 3\}$,

$$p^{-(\mu_{3+1-r}+\ldots+\mu_3)} = \|\Lambda^r p^{\overline{\mu}}\| \leq \|\Lambda^r(p^{\overline{\mu}}n)\| = \|\Lambda^r p^\lambda\| = p^{-(\lambda_{3-r+1}+\ldots+\lambda_3)}.$$

Taking $r = 1$ gives $\mu_3 \geq \lambda_3$, and taking $r = 2$ gives $\mu_2 + \mu_3 \geq \lambda_2 + \lambda_3$. Using this and the fact that $\mu_1 + \mu_2 + \mu_3 = \lambda_1 + \lambda_2 + \lambda_3$, we get $\mu_1 + \mu_2 \leq \lambda_1 + \lambda_2$ and $\mu_1 \leq \lambda_1$, as desired.

(e). Suppose that $c_\lambda(\mu) \neq 0$. By (c), we have

$$c_\lambda(\mu) = f_\lambda^{(B)}(p^\mu) = \delta(p^\mu)^{1/2} \int_N f_\lambda(p^\mu n) dn.$$

As this is nonzero, the set $p^\mu N$ must intersect $\operatorname{supp}(\lambda) = Kp^\lambda K$. By (d), this implies that $\mu \leq \lambda$.

(f). Let $n \in N$. If $n \in N \cap K$, then $tn \in t(K \cap N) \subset KtK$. Conversely, suppose that $tn \in KtK$. We write $n = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$; then $tn = \begin{pmatrix} p^{\lambda_3} & p^{\lambda_3}a & p^{\lambda_3}b \\ 0 & p^{\lambda_2} & p^{\lambda_2}c \\ 0 & 0 & p^{\lambda_1} \end{pmatrix}$. We want to show that $n \in N \cap K$, which means that $a, b, c \in \mathbb{Z}_p$. As $K \subset M_n(\mathbb{Z}_p)$ and as $\lambda_1 \geq \lambda_2 \geq \lambda_3$, the fact that $tn \in KtK$ implies that every entry of $tn$ is $p^{\lambda_3}$ times an element of $\mathbb{Z}_p$. In particular, $a, b \in \mathbb{Z}_p$. Moreover, we have $\|\Lambda^2(tn)\| = \|\Lambda^2 t\| = p^{-(\lambda_2+\lambda_3)}$ by (b). Applying this to the entry of $\Lambda^2(tn)$ indexed by $A = \{1, 2\}$ and $A' = \{1, 3\}$, we get

$$p^{-(\lambda_2+\lambda_3)} \geq \left| \det \begin{pmatrix} p^{\lambda_3} & p^{\lambda_3}b \\ 0 & p^{\lambda_2}c \end{pmatrix} \right|_p = p^{-(\lambda_2+\lambda_3)}|c|_p,$$

so $|c|_p \leq 1$, which means that $c \in \mathbb{Z}_p$.

(g). Let $\lambda \in X^+$. By (c), we have

$$c_\lambda(\lambda) = f_\lambda^{(B)}(p^{\overline{\lambda}}) = \delta(p^{\overline{\lambda}})^{1/2} \int_N f_\lambda(p^{\overline{\lambda}}n) dn.$$

As $f_\lambda = \mathbb{1}_{Kp^\lambda K} = \mathbb{1}_{Kp^{\overline{\lambda}}K}$ (because $p^\lambda$ and $p^{\overline{\lambda}}$ are conjugate under a permutation matrix, and permutation matrices are in $K$), question (f) implies that

$$c_\lambda(\lambda) = \delta(p^{\overline{\lambda}})^{1/2}\,\mathrm{vol}(K \cap N),$$

where the volume is taken for the Haar measure on $N$. By the choice of the Haar measure on $N$, we have $\mathrm{vol}(K \cap N) = 1$. So

$$c_\lambda(\lambda) = \delta(p^{\overline{\lambda}})^{1/2} = |p^{\lambda_3}|_p |p^{\lambda_1}|_p^{-1} = p^{\lambda_1-\lambda_3}.$$

This is the statement of (ii).

(18) We denote the map $\mathscr{H} \overset{\sim}{\to} \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$, $f \longmapsto f^\vee$ by $S$. We have seen in question (14) that this map is well-defined, and in question (7) that it is a morphism of $\mathbb{C}$-algebras. So we just need to show that it is an isomorphism of $\mathbb{C}$-vector spaces. We have given a basis $(f_\lambda)_{\lambda\in X^+}$ of $\mathscr{H}$ in question (15), and a basis $(c_\lambda)_{\lambda\in X^+}$ of $\mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3}$ in question (16). Moreover, the set $X^+$ is partially ordered, and the matrix of $S$ in the two bases is upper triangular (for this partial order) by question (17)(i) and has nonzero diagonal entries by 17(ii). So $S$ is invertible.

If we want to make the argument more explicit, we could say the following : By (17)(i) and (ii), we have, for every $\lambda \in X^+$,

$$S(f_\lambda) = \sum_{\mu\in X^+,\ \mu\leq\lambda} c_\lambda(\mu) c_\mu,$$

with $c_\lambda(\lambda) \in \mathbb{C}^\times$. We will try to construct the inverse $T : \mathbb{C}[z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}]^{\mathfrak{S}_3} \to \mathscr{H}$ of $S$. It suffices to give the value of $T$ on the basis elements $c_\lambda$, $\lambda \in X^+$. If there is no $\mu \in X^+$ such that $\mu \leq \lambda$ and $\mu \neq \lambda$, we set $T(c_\lambda) = c_\lambda(\lambda)^{-1} f_\lambda$. Otherwise, we define $T(c_\lambda)$ recursively by

$$T(c_\lambda) = c_\lambda(\lambda)^{-1} f_\lambda - c_\lambda(\lambda)^{-1} \sum_{\mu\in X^+-\{\lambda\},\ \mu\leq\lambda} c_\lambda(\mu) T(c_\mu).$$

As $\{\mu \in X^+ \mid \mu \leq \lambda\}$ is finite (indeed, if $\mu \in X^+$ and $\mu \leq \lambda$, then $\mu_3 = (\lambda_1+\lambda_2+\lambda_3) - (\mu_1+\mu_2) \geq \lambda_3$, so $\lambda_3 \leq \mu_3 \leq \mu_2 \leq \mu_1 \leq \lambda_1$), this process will always terminate.

$\square$

### V.8.4 Problem

10 11

[10] What is the name of this result ? And a reference ?

[11] H/t G. Dospinescu.

In this problem, we write $G = \mathrm{SL}_2(\mathbb{R})$ and $K = \mathrm{SO}(2)$. We denote the subgroup of upper triangular matrices in $G$ by $B$ and the subgroup of unipotent upper triangular matrices by $N$ ("unipotent upper triangular" means "upper triangular with diagonal entries all equal to 1"). [12] [13] We fix left Haar measures on all the groups. Remember that $G$ is unimodular.

(1) The goal of this question is to prove the following fact : (*) If $(\pi, V)$ is a unitary representation of $G$ and if $v \in V$ is a vector that is fixed by an element of $G$ of the form $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ with $u \neq 0$, then $v$ is fixed by every element of $G$.

We fix a unitary representation $(\pi, V)$ of $G$.

(a). Let $v \in V$, and suppose that there exists a continuous morphism of groups $\chi : \mathbb{R} \to S^1$ such that, for every $u \in \mathbb{R}$, we have $\pi \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} (v) = \chi(u)v$. Define $\varphi : G \to \mathbb{C}$ by $\varphi(x) = \langle \pi(x)(v), v \rangle$.

(i) Show that, if $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $x' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ are such that $c = c'$, then we have $|\varphi(x)| = |\varphi(x')|$.

(ii) Show that, if $x \in B$, then $|\varphi(x)| = |\varphi(1)|$.

(iii) Show that there exists a continuous group morphism $\psi : B \to S^1$ such that $\pi(x)(v) = \psi(x)v$ for every $x \in B$.

(iv) Show that the function $x \longmapsto |\varphi(x)|$ is constant on $G$.

(v) Show that $\pi(x)(v) = v$ for every $x \in G$.

(b). Prove (*).

(2) Let

$$A^+ = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \ a \in \mathbb{R}_{\geq 1} \right\} \subset G.$$

(a). Show that

$$G = \coprod_{a \in A^+} KaK.$$

(As sets, not as topological spaces.)

(b). Show that $(G, K)$ is a Gelfand pair.

(c). Generalize questions (a) and (b) to $\mathrm{SL}_n(\mathbb{R})$, where $K = \mathrm{SO}(n)$ and $A^+$ is the set of diagonal matrices with diagonal coefficients $a_1, \ldots, a_n$ satisfying $a_1 \geq a_2 \geq \ldots a_n > 0$.

[12] We could make everything in this problem work for $\mathrm{SL}_n(\mathbb{R})$, but the generalization is a bit more painful than in problem V.8.3.

[13] References.

(3) The goal of this question is to prove the following fact : (**) For every unitary representation $(\pi, V)$ of $G$ such that $V^G = \{0\}$, for all $v, w \in V$, we have $\lim_{x\to\infty}\langle \pi(x)(v), w\rangle = 0$, where $\infty$ is the point at infinity of the Alexandroff compactification of $G$. (So $\lim_{x\to\infty}\langle \pi(x)(v), w\rangle = 0$ means that for every $\varepsilon > 0$, there exists a compact subset $X$ of $G$ such that $|\langle \pi(x)(v), w\rangle| \leq \varepsilon$ for every $x \in G - X$.)

We fix a unitary representation $(\pi, V)$ of $G$, and we assume that it does not satisfy the conclusion of (**).

(a). Show that there exists $v, v' \in V$, a sequence $(a_n)_{n\geq 0}$ of elements of $\mathbb{R}_{\geq 1}$ and $\alpha \in \mathbb{C} - \{0\}$ such that :

- $a_n \to +\infty$ as $n \to +\infty$;
- $\langle \pi(t_n)(v), v'\rangle \to \alpha$ as $n \to +\infty$, where $t_n = \begin{pmatrix} a_n & 0 \\ 0 & a_n^{-1} \end{pmatrix}$.

(b). Show that, after replacing $(a_n)_{n\geq 0}$ by a subsequence, we may assume that there exists $v_0 \in V$ such that, for every $w \in V$, we have $\langle \pi(t_n)(v), w\rangle \to \langle v_0, w\rangle$ as $n \to +\infty$.

(c). Show that $v_0 \neq 0$ and that $v_0$ is fixed by every element of $N$. (Hint : If $x \in N$ and $w \in V$, what is the behavior of $\langle \pi(xt_n)(v), w\rangle - \langle \pi(t_n)(v), w\rangle \to 0$ as $n \to +\infty$ ?)

(d). Conclude.

(4) The goal of this question is to show that the quotient $\mathrm{SL}_2(\mathbb{Z})\backslash G$ has finite volume.

Let $\mathfrak{h} := \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$.

For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and $z \in \mathfrak{h}$, we set

$$g \cdot z = \frac{az+b}{cz+d}.$$

(a) Show that this defines a left action of $G$ on $\mathfrak{h}$.

(b) Show that the stabilizer of $i \in \mathfrak{h}$ is $K$, and that this induces a homeomorphism $G/K \xrightarrow{\sim} \mathfrak{h}$.

(c) Show that the homeomorphism of (b) sends the measure $\mu_{G/K}$ to a multiple of $\frac{dxdy}{y^2}$, where $x$ and $y$ are the real and imaginary parts of $z \in \mathfrak{h}$ and $dx$ and $dy$ are Lebesgue measure on $\mathbb{R}$.

(d) Let $\Omega = \{z \in \mathfrak{h} || \operatorname{Re}(z)| \leq \frac{1}{2} \text{ and } |z| \geq 1\}$. Show that, for every $z \in \mathfrak{h}$, there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $g \cdot z \in \Omega$.

(e) Show that $\int_{z=x+iy\in\Omega} \frac{dxdy}{y^2} < +\infty$.

(f) Show that $\operatorname{vol}(\mathrm{SL}_2(\mathbb{Z})\backslash G) < +\infty$.

(5) In this question, we fix a closed discrete subgroup $\Gamma$ of $G$ such that $\mathrm{vol}(\Gamma\backslash G) < +\infty$. Note that $G$ is unimodular by I.5.3.7, so the Haar measure on $G$ is also right invariant. We write $X = \Gamma\backslash G$ and we denote by $\mu$ the measure $\mu_{\Gamma\backslash G}$; we normalize the Haar measures on $G$ and $\Gamma$ so that $\mu(X) = 1$. We consider the space $L^2(X) = L^2(X, \mu)$ with the right quasi-regular representation $\pi$ of $G$ (i.e. we have $\pi(g)(f) = R_g f$ for $g \in G$ and $f \in L^2(X)$).

Show that, for all $f_1, f_2 \in L^2(X)$, we have

$$\lim_{g\to\infty} \int_X f_1(xg) f_2(x) d\mu(x) = \int_X f_1(x) d\mu(x) \int_X f_2(x) d\mu(x).$$

(Hint : what are the $G$-invariant vectors in $V := \{f \in L^2(X) | \int_X f(x) d\mu(x) = 0\}$ ?)

(6) We use the notation of question (5). Let $Y = (\Gamma \cap K) \setminus K$. We put the measure $\mu_Y = \mu_{(\Gamma\cap K)\backslash K}$ on $Y$, and we normalize the Haar measures on $\Gamma \cap K$ and $K$ so that $Y$ has volume 1.

The goal of this question is to prove the following statement : (***) For every $f \in \mathscr{C}_c(X)$, we have

$$\lim_{g\to\infty} \int_Y f(yg) d\mu_Y(y) = \int_X f(x) d\mu(x).$$

[14]

We think of $\mu_K$ as the continuous linear functional on $\mathscr{C}_c(G)$ given by

$$\mu_K(f) = \int_K f(x) d\mu_K(x),$$

for $f \in \mathscr{C}_c(G)$. Proving (***) would be relatively easy (from what we have already done) if $\mu_K$ were representable by an element of $\mathscr{C}_c(G)$ (i.e. if we had some $h \in \mathscr{C}_c(G)$ such that $\int_K f(x) d\mu_K(x) = \int_G f(x)h(x) d\mu_G(x)$ for every $f \in \mathscr{C}_c(G)$), but this is not the case. Nevertheless, we can try to approximate $\mu_K$ by elements of $\mathscr{C}_c(G)$. You might remember that we have used that kind of technique several times already to approximate Dirac measures.

(a). If $\psi \in \mathscr{C}_c(G)$, we define a continuous linear functional $\psi * \mu_K$ on $\mathscr{C}_c(G)$ by

$$\psi * \mu_K(f) = \int_{G\times K} f(xy)\psi(x) d\mu_G(x) d\mu_K(y).$$

Show that there exists $h \in \mathscr{C}_c(G)$ such that

$$\psi * \mu_K(f) = \int_G f(x)h(x) d\mu_G(x)$$

for every $f \in \mathscr{C}_c(G)$.

[14] In other words, the sets $Yg$ become equidistributed in $X$ as $g \to \infty$ in $G$. Note that $g \to \infty$ if and only if $g^{-1} \to \infty$.

(b). Show that there exists a sequence $(\psi_n)_{n\geq 0}$ of elements of $\mathscr{C}_c(G)$ such that $\mu_K$ is the limit of the sequence $(\psi_n * \mu_K)_{n\geq 0}$ in the weak* topology of $\mathrm{Hom}(\mathscr{C}_c(G), \mathbb{C})$.

(c). Prove (***).

*Solution.*

(1) (a). Note that, if $n = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, n' = \begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix} \in N$ and $x \in G$, then

$$|\varphi(nxn')| = |\langle \pi(x)(\pi(n')(v)), \pi(n)^{-1}(v)\rangle| = |\chi(u')\chi(u)\langle \pi(x)(v), v\rangle| = |\varphi(x)|.$$

(i) Suppose first that $c = c' \neq 0$. Let $n = \begin{pmatrix} 1 & c^{-1}(d'-d) \\ 0 & 1 \end{pmatrix}$ and $n' = \begin{pmatrix} 1 & c^{-1}(a'-a) \\ 0 & 1 \end{pmatrix}$. Then we have

$$n'xn = \begin{pmatrix} a' & w \\ c' & d' \end{pmatrix},$$

for some $w \in \mathbb{R}$. As $1 = \det(n'xn) = a'd' - wc' = a'd' - b'c'$ and $c' \neq 0$, we must have $w = b'$, so $n'xn = x'$, and the remark above implies that $|\varphi(x)| = |\varphi(x')|$.

Now suppose that $c = c' = 0$. Then we can sequence $(x_n)_{\geq 1}$ and $(x'_n)_{\geq 1}$ in $G$ such that $x_n \to x$, $x'_n \to x'$ and, for every $n \geq 1$, the $(2,1)$-entries of $x_n$ and $x'_n$ are both equal to $\frac{1}{n}$. For example, we can take $x_n = \begin{pmatrix} a + \frac{b}{nd} & b \\ \frac{1}{n} & d \end{pmatrix}$, which makes sense because $\det(x) = ad = 1$ implies that $d \neq 0$, and we can define $x'_n$ by a similar formula. Applying the first case to $x_n$ and $x'_n$ gives $|\varphi(x_n)| = |\varphi(x'_n)|$ for every $n \geq 1$; as $\varphi$ is continuous, we can go to the limit in $n$, and we get $|\varphi(x)| = |\varphi(x')|$.

(ii) This follows from the case "$c = c' = 0$" of question (i).

(iii) Let $x \in B$. We have $|\langle \pi(x)(v), v\rangle)| = |\langle v, v\rangle|$ by (ii), so, by the case of equality in the Cauchy-Schwartz formula, we must have $\pi(x)(v) = \psi(x)v$ for some $\psi(x) \in S^1$. As $x \longmapsto \pi(x)(v)$ is continuous in $x$ and $\psi(x) = \langle \pi(x)(v), v\rangle$, the function $x \longmapsto \psi(x)$ is also continuous. The fact that it is a morphism of groups follows immediately from the fact that $\pi(xy) = \pi(x) \circ \pi(y)$ for all $x, y \in B$.

(iv) Repeating what we did at the beginning of the proof of (a) and using (iii), we see that $|\varphi(bxb')| = |\varphi(x)|$ for every $x \in G$ and all $b, b' \in G$. Let $x_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Let $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. If $c \neq 0$, then

$$x = \begin{pmatrix} 1 & c^{-1}a \\ 0 & 1 \end{pmatrix} x_0 \begin{pmatrix} c & -d \\ 0 & b - c^{-1}ad \end{pmatrix},$$

so $|\varphi(x)| = |\varphi(x_0)|$. If $c = 0$, then we can approximate $x$ by elements of $G$ whose $(2,1)$-entry is nonzero (as in the proof of (i)), so, by the first case and continuity of $\varphi$, we also get $|\varphi(x)| = |\varphi(x_0)|$.

(v) We repeat the reasoning of (iii) to show that there exists a continuous group morphism $\psi : G \to S^1$ (extending the map $\psi$ of (iii)) such that $\pi(x)(v) = \psi(x)v$ for every $x \in G$. But there are no nontrivial group morphisms from $G$ to a commutative group (because $G$ is equal to its commutator subgroup, and a group morphism into a commutative is trivial on every commutator), so $\psi = 1$, so $v \in V^G$.

(b). We denote by $\pi'$ the unitary representation of $\mathbb{R}$ on $V$ defined by $\pi'(t) = \pi \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$, for every $t \in \mathbb{R}$. By hypothesis, we have $\pi'(u)(v) = v$. As $\mathbb{R}$ is commutative, this implies that $\pi(u)(w) = w$ for every $w$ in $\{\pi(t)(u),\ t \in \mathbb{R}\}$, hence (because both sides are linear and continuous in $w$) for every $w \in W := \overline{\mathrm{Span}\{\pi(t)(v),\ t \in \mathbb{R}\}}$. In other words, the unitary representation $\pi'_{|W}$ is trivial on the subgroup $\mathbb{Z}u$ of $\mathbb{R}$, so it induces a unitary representation of the compact group $\mathbb{R}/\mathbb{Z}u$ on $W$. By theorem IV.2.1 and corollary I.3.4.4, the space $W$ is the closure of a direct sum of 1-dimensional representations of $\mathbb{R}/\mathbb{Z}u$, that is, there exists a linearly independent family $(v_i)_{i\in I}$ generating a dense subspace of $W$ and such that every $v_i$ is an eigenvector of all the $\pi(n)$, $n \in N$. By question (a), this implies that all $v_i$ are in $V^G$, hence $W \subset V^G$, and in particular $v \in V^G$.

(2) (a). We prove the result directly for $\mathrm{SL}_n(\mathbb{R})$, so we will write $G = \mathrm{SL}_n(\mathbb{R})$ and $K = \mathrm{SO}(n)$.

We will use the polar decomposition for elements of $\mathrm{GL}_n(\mathbb{R})$ (see Theorem 12.35 of Rudin's [20], [15] though that is overkill because we only need the finite-dimensional case) : for every $g \in \mathrm{GL}_n(\mathbb{R})$, there exists a unique couple $(u,p)$ such that $u$ is orthogonal, $p$ is symmetric positive definite and $g = up$; also, we have $p^2 = g^T g$. If $g \in G$, then $\det(p)^2 = \det(g^T g) = 1$; as $p$ is definite positive, we have $\det(p) > 0$, so $\det(p) = 1$, and then we also deduce that $\det(u) = 1$, i.e. that $u$ is in $K$.

We prove that $G = \bigcup_{a\in A^+} KaK$. Let $g \in G$. Let $g = up$ be the polar decomposition of $g$. As $p$ is symmetric, is is diagonalizable in an orthonormal basis by the spectral theorem, so we can write $p = kak^{-1}$ with $k \in \mathrm{O}(n)$ and $a$ diagonal. The diagonal entries of $a$ are the eigenvalues of $p$, and we may assume that they are in decreasing order, so that $a \in A^+$. Also, if $k$ is not in $\mathrm{SO}(n)$, then we can change the sign of the one of the vectors of the eigenbasis; this does not affect $a$, and the new $k$ is in $\mathrm{SO}(n)$. Finally, we get $g = (uk)ak^{-1} \in KaK$.

We also want to prove that the set $KaK$, $a \in A^+$, are pairwise disjoint. Let $a, a' \in A^+$, and suppose that $KaK \cap Ka'K \neq \varnothing$. Then there exist $k, l \in K$ such

[15] Better ref.

that $a' = kal$. So
$$(a')^2 = a'a'^T = kall^Tak^T = ka^2k^{-1},$$
which implies that the $(a')^2$ and $a^2$ have the same eigenvalues, i.e. they have the same diagonal entries up to reordering. As the diagonal entries of $(a')^2$ and $a^2$ are decreasing, these two matrices actually have the same diagonal entries, i.e. $(a')^2 = a^2$. Finally, as $a$ and $a'$ are diagonal with positive entries, the fact that $(a')^2 = a^2$ implies that $a' = a$.

(b). (We still take $G = \mathrm{SL}_n(\mathbb{R})$ and $K = \mathrm{SO}(n)$.) Consider the continuous group automorphism $\theta : G \to G$, $g \longmapsto (g^T)^{-1}$. We have $\theta^2 = \mathrm{id}_G$, and $\theta_{|K} = \mathrm{id}_K$. For every $g \in G$, if we write $g = kal$ with $k, l \in K$ and $a \in A^+$, then $\theta(g) = ka^{-1}l = klg^{-1}kl \in Kg^{-1}K$. By proposition V.2.5, $(G, K)$ is a Gelfand pair.

(3) Now we are back in $\mathrm{SL}_2(\mathbb{R})$, so that frees the letter $n$.

(a). As $V$ does not satisfy the conclusion of (**), there exists $v_1, v_2 \in V$ and $\varepsilon > 0$ such that, for every compact subset $X$ of $G$, there exists $x \in G - X$ such that $|\langle\pi(x)(v_1), v_2\rangle| > \varepsilon$.

For every $n \geq 1$, let $A_n^+$ be the set of $\begin{pmatrix} a & 0 \\ 0 & a^{-1}\end{pmatrix} \in A^+$ such that $a \leq n$.. Then $\bigcup_{t\in A_n^+} KtK$ is relatively compact in $G$, because, if $g \in KtK$ with $t \in A_n^+$, then all the entries of $g$ and of $g^{-1}$ are bounded by $4n$ in absolute value (note that, if $k \in K$, then the entries of $k$ are all bounded by $1$ in absolute value). So we can find $x_n \in G - \bigcup_{t\in A_n^+} KtK$ such that $|\langle\pi(x_n)(v_1), v_2\rangle| > \varepsilon$. Write $x_n = k_nt_nl_n$ with $k_n, l_n \in K$ and $t_n = \begin{pmatrix} a_n & 0 \\ 0 & a_n^{-1}\end{pmatrix} \in A_n^+$. As $K$ is compact, after replacing $(k_n)$ and $(l_n)$ by subsequences, we may assume that $(k_n)$ (resp. $(l_n)$) has a limit $k \in K$ (resp. $l \in L$). Let $v = \pi(l)(v_1)$ and $v' = \pi(k)^{-1}(v_2)$. As the sequence $(\langle\pi(t_n)(v), v'\rangle)$ of elements of $\mathbb{C}$ is bounded (by $\|v\|\|v'\|$), after going to a subsequence, we may assume that it converges to some $\alpha \in \mathbb{C}$. To finish the proof, we just need to show that $\alpha \neq 0$. Note that, for every $n \geq 1$, we have
$$\langle\pi(t_n)v, v'\rangle = \langle\pi(kk_n^{-1})\pi(k_nt_nl_n)\pi(l_n^{-1}l)v_1, v_2\rangle = \langle\pi(x_n)\pi(l_n^{-1}l)v_1, \pi(k_nk^{-1})v_2\rangle,$$
so
$$|\langle\pi(t_n)v, v'\rangle - \langle\pi(x_n)v_1, v_2\rangle| \leq \|v_1\|\|v_2\|((\|\pi(l_n^{-1}l) - \mathrm{id}\|_{op} + \|\pi(k_nk{-}1) - \mathrm{id}\|_{op}.$$
This tends to $0$ as $n \to 1$. As $|\langle\pi(x_n)v_1, v_2\rangle| \geq \varepsilon$ for every $n \geq 1$, the limit $\alpha$ of the sequence $(\langle\pi(t_n)(v), v'\rangle)$ cannot be $0$.

(b). The conclusion means that the sequence of bounded linear forms $(\Lambda_n : w \longmapsto \overline{\langle\pi(t_n)(v), w\rangle})_{n\geq 1}$ on $V$ converges to the bounded linear form $w \longmapsto \overline{\langle v_0, w\rangle}$ in the weak* topology of $V^*$. As each $\Lambda_n$ is in the closed unit ball of $V^*$ (for the operator norm), and as this closed unit ball is weak* compact by the Banach-Alaoglu theorem, we may indeed assume, after going to a subsequence, that the sequence $(\Lambda_n)_{n\geq 1}$ converges to some element $\Lambda \in V^*$ in the weak* topology. But we know that $\Lambda$ has to be of the form $w \longmapsto \overline{\langle v_0, w\rangle}$, for a uniquely determined $v_0 \in V$, so we are done.

(c). We have $\langle v_0, v'\rangle = \lim_{n\to+\infty}\langle \pi(t_n)(v), v'\rangle = \alpha \neq 0$, so $v_0 \neq 0$.

Let $x \in N$, and write $x = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$. Let $w \in V$. Then

$$\langle \pi(xt_n)(v), w\rangle - \langle \pi(t_n)(v), w\rangle = \langle \pi(t_n)(\pi(t_n^{-1}xt_n)(v) - v), w\rangle,$$

so

$$|\langle \pi(xt_n)(v), w\rangle - \langle \pi(t_n)(v), w\rangle| \leq \|(\pi(t_n^{-1}xt_n) - \pi(1))(v)\|\|w\|.$$

As $t_n^{-1}xt_n = \begin{pmatrix} 1 & a_n^{-2}u \\ 0 & 1 \end{pmatrix}$ and as $\lim_{n\to+\infty} a_n = +\infty$, we have $\lim_{n\to+\infty} t_n^{-1}xt_n = 1$. Using the continuity of the representation $\pi$, we deduce that $\lim_{n\to+\infty}(\pi(t_n^{-1}xt_n)(v) - v) = 0$, so that $\lim_{n\to+\infty} |\langle \pi(xt_n)(v), w\rangle - \langle \pi(t_n)(v), w\rangle| = 0$. But we know that $\lim_{n\to+\infty}\langle \pi(t_n)(v), w\rangle = \langle v_0, w\rangle$, so we get $\lim_{n\to+\infty}\langle \pi(xt_n)(v), w\rangle = \langle v_0, w\rangle$. On the other hand, we have

$$\lim_{n\to+\infty}\langle \pi(xt_n)(v), w\rangle = \lim_{n\to+\infty}\langle \pi(t_n)(v), \pi(x)^{-1}(w)\rangle = \langle v_0, \pi(x)^{-1}(w)\rangle = \langle \pi(x)(v_0), w\rangle.$$

As this holds for every $w \in V$, we deduce that $\pi(x)(v_0) = v_0$.

(d). By question (1), (d) implies that $v_0$ is fixed by every element of $G$. So $V^G \neq \{0\}$, which finishes the proof of the contrapositive of (**).

(4) (a). We first check that $g \cdot z$ is well-defined and in $\mathfrak{h}$ if $z \in \mathfrak{h}$. Write $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $c \neq 0$, then $\operatorname{Im}(cz + d) = c\operatorname{Im}(z) \neq 0$, so the quotient $\frac{az+b}{cz+d}$ makes sense. If $c = 0$, then $ad = \det(g) = 1$, so $d \neq 0$, so $cz + d = d \neq 0$, so once again the quotient $\frac{az+b}{cz+d}$ makes sense. We calculate the imaginary part of this quotient. We have

$$\frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{(cz+d)(c\overline{z}+d)} = \frac{acz\overline{z} + bd + adz + bc\overline{z}}{(cz+d)(c\overline{z}+d)},$$

so

$$\operatorname{Im}\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)(c\overline{z}+d)}(ac\operatorname{Im}(z) - bd\operatorname{Im}(z)) = \frac{\operatorname{Im}(z)}{(cz+d)(c\overline{z}+d)} > 0,$$

and $\frac{az+b}{cz+d} \in \mathfrak{h}$.

If $g = 1$, then clearly $g \cdot z = z$. Let $h = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be another element of $G$. We must check that $(gh) \cdot z = g \cdot (h \cdot z)$. This is a straightforward calculation.

(b). Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ such that $g \cdot i = i$. This is equivalent $ai + b = i(ci + d) = -c + id$, i.e. to the fact that $a = d$ and $b = -c$. If $a = d$ and $b = -c$, then $1 = ad - bc = a^2 + b^2 = d^2 + c^2$ and $ac + bd = 0$, so $g$ is an orthogonal matrix, hence $g \in K$ because $\det(g) = 1$. Conversely, if $g \in K$, then $g$ is of the form $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, so we do have $a = d$ and $b = -c$, hence $g \cdot i = i$.

If $z$ is an arbitrary element of $\mathfrak{h}$, we write $z = x + iy$ with $x \in \mathbb{R}$ and $y \in \mathbb{R}_{>0}$. Then $z = g(z) \cdot i$, with $g(z) = \begin{pmatrix} \sqrt{y} & \sqrt{y}^{-1}x \\ 0 & \sqrt{y}^{-1} \end{pmatrix} \in G$. So the action of $G$ on $\mathfrak{h}$ is transitive, and it induces a continuous bijection $\alpha : G/K \xrightarrow{\sim} \mathfrak{h}$. To show that $\alpha$ is a homeomorphism, we note that the map $\mathfrak{h} \to G$, $z \longmapsto g(z)$ that we just constructed is continuous, and that $z \longmapsto g(z)K$ is the inverse of $\alpha$.

(c). Let $\mu$ be the image by $\alpha^{-1}$ of the measure $\frac{dxdy}{y^2}$. Reasoning as in the proof of (2) of problem V.8.3, we see that it suffices to prove that $\mu$ is left invariant by $G$. In other words, it suffices to prove that the measure $\frac{dxdy}{y^2}$ is invariant by the action of $G$ on $\mathfrak{h}$. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, and let $z = x + iy \in \mathfrak{h}$. We have seen in the proof of (a) that

$$\operatorname{Im}(g \cdot z) = \frac{y}{(cz + d)(c\overline{z} + d)} = \frac{y}{c^2(x^2 + y^2) + 2cdx + d^2}.$$

Similarly,

$$\operatorname{Re}(g \cdot z) = \frac{ac(x^2 + y^2) + (ad + bc)x + bd}{c^2(x^2 + y^2) + 2cdx + d^2}.$$

If we write $x' = \operatorname{Re}(g \cdot z)$ and $y' = \operatorname{Im}(g \cdot z)$, we want to show that $\frac{dx'dy'}{y'^2} = \frac{dxdy}{y^2}$.

Let $g_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We saw in the proof of (1)(a)(iv) that $G = B \cup Bg_0B$, so it suffices to show that $\frac{dx}{dy}y^2$ is invariant under the action of an element of $B$ and of $g_0$. In both cases, we will use the usual change of variables on $\mathbb{R}^2$ to calculate $dx'dy'$.

If $g \in B$ (i.e. $c = 0$), then $x' = \frac{1}{d^2}(x + bd)$ and $y' = \frac{y}{d^2}$, so $dx'dy' = \frac{1}{d^4}dxdy$, and we get $\frac{dx'dy'}{y'^2} = \frac{dxdy}{y^2}$.

If $g = g_0$, then $x' = -\frac{x}{x^2+y^2}$ and $y' = \frac{y}{x^2+y^2}$, so

$$dx'dy' = \left|\det\begin{pmatrix} \frac{-(x^2+y^2)+2x^2}{(x^2+y^2)^2} & \frac{-2xy}{(x^2+y^2)^2} \\ \frac{2xy}{(x^2+y^2)^2} & \frac{(x^2+y^2)-2y^2}{(x^2+y^2)^2} \end{pmatrix}\right| dxdy = \frac{dxdy}{(x^2 + y^2)^2},$$

and again this implies immediately that $\frac{dx'dy'}{y'^2} = \frac{dxdy}{y^2}$.

(d). If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then we have $ad - bc = 1$, so $c$ and $d$ are relatively prime in $\mathbb{Z}$. Conversely, if $c$ and $d$ are relatively prime in $\mathbb{Z}$, then there exist $a, d \in \mathbb{Z}$ such that $ad - bc = 1$, and then $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $\mathrm{SL}_2(\mathbb{Z})$.

Let $z \in \mathfrak{h}$. Then the group $\mathbb{Z} + \mathbb{Z}z$ is discrete in $\mathbb{C}$ (because $z \notin \mathbb{R}$), so its intersection with every ball is finite. In particular, the infimum of $|cz+d|$ as $c, d \in \mathbb{Z}$ are relatively prime is attained. By the previous paragraph and the fact that $\mathrm{Im}(g \cdot z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}$ if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we see that $\sup\{|\mathrm{Im}(g \cdot z)|,\ g \in \mathrm{SL}_2(\mathbb{Z})\}$ is also attained. We want to show that there exists $g \in \mathrm{SL}_2(\mathbb{Z})$ such that $g \cdot z \in \Omega$. After replacing $z$ by some $g \cdot z$ with $g \in \mathrm{SL}_2(\mathbb{Z})$, we may assume that $|\mathrm{Im}(z)| = \sup\{|\mathrm{Im}(g \cdot z)|,\ g \in \mathrm{SL}_2(\mathbb{Z})\}$. In particular, taking $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we get $|\mathrm{Im}(z)| \geq \frac{|\mathrm{Im}(z)|}{|z|^2}$, so $|z| \geq 1$. If $g_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ with $n \in \mathbb{Z}$, then $g_n \cdot z = z + n$, so $\mathrm{Im}(g_n \cdot z) = \mathrm{Im}(z)$ and we still have $|\mathrm{Im}(g_n \cdot z)| = \sup\{|\mathrm{Im}((hg_n) \cdot z)|,\ h \in \mathrm{SL}_2(\mathbb{Z})\}$, and in particular we still have $|g \cdot z| \geq 1$. We can choose $n \in \mathbb{Z}$ such that $-\frac{1}{2} \leq \mathrm{Re}(z) + n \leq \frac{1}{2}$, and then we have $g_n \cdot z \in \Omega$ and we are done.

(e). We have :

$$\int_\Omega \frac{dxdy}{y^2} = \int_{-1/2}^{1/2} \int_{\sqrt{1-x^2}}^{+\infty} \frac{dxdy}{y^2} = \int_{-1/2}^{1/2} \frac{1}{\sqrt{1-x^2}} dx < +\infty.$$

(f). For every $\varepsilon \in (0, 1/4)$, let

$$\Omega_\varepsilon = \{z \in \mathfrak{h} \mid |z| > 1 - \varepsilon \text{ and } |\mathrm{Im}(z)| < \tfrac{1}{2} + \varepsilon\}.$$

As in (e), we see that

$$I_\varepsilon := \int_{\Omega_\varepsilon} \frac{dxdy}{y^2} = \int_{-1/2-\varepsilon}^{1/2+\varepsilon} \frac{1}{\sqrt{1 - x^2 - \varepsilon}} dx < +\infty.$$

Let

$$\Omega'_\varepsilon = \{g \in G \mid g \cdot i \in \Omega_\varepsilon\}.$$

This is the inverse image of $\Omega_\varepsilon$ by the continuous map $G \to G/K$. In particular, it is an open subset of $G$, so, by the definition of a regular Borel measure (and Urysohn's lemma), we have

$$\mu_G(\Omega'_\varepsilon) = \sup\left\{\int_G f d\mu_G,\ f \in \mathscr{C}_c(G),\ 0 \leq f \leq 1 \text{ and } \mathrm{supp}(f) \subset \Omega'_\varepsilon\right\}.$$

If $f \in \mathscr{C}_c(G)$ is such that $0 \leq f \leq 1$ and $\operatorname{supp}(\Omega'_\varepsilon)$, then, for every $g \in G$, we have $f^K(gK) = \int_K f(gk) d\mu_K(k) \in [0,1]$ (because the Haar measure $\mu_K$ has total volume 1), and $f^K(gK) = 0$ if $g \in \Omega'_\varepsilon$, i.e. if $gK \notin \Omega_\varepsilon$; so $\int_{G/K} f^K d\mu_{G/K} \leq \mu_{G/K}(\Omega_\varepsilon)$. As $\int_G f d\mu_G = \int_{G/K} f^K d\mu_{G/K}$ for every $f \in \mathscr{C}_c(G)$, and as $\mu_{G/K}$ is a multiple of the measure $\frac{dxdy}{y^2}$ by (c), we see that $\mu_G(\Omega_\varepsilon)$ is bounded by a multiple of $I_\varepsilon$, hence finite.

On the other hand, as $\Omega_\varepsilon \supset \Omega$, the restriction to $\Omega'_\varepsilon$ of the projection $\pi : G \to \mathrm{SL}_2(\mathbb{Z})\backslash G$ is surjective; indeed, if $g \in G$, then, by (d), there exists $h \in \mathrm{SL}_2(\mathbb{Z})$ such that $hg \cdot i \in \Omega$, and then $hg \in \Omega'_\varepsilon$ and $\pi(hg) = \pi(g)$. Again by the definition of a regular Borel measure and Urysohn's lemma, there exists $f \in \mathscr{C}_c^+(G)$ such that $f_{|\Omega'_\varepsilon} = 1$ and $\int_G f d\mu_G < +\infty$. Let $h = {}^{\mathrm{SL}_2(\mathbb{Z})}f \in \mathscr{C}_c(\mathrm{SL}_2(\mathbb{Z})\backslash G)$. We have $\int_{\mathrm{SL}_2(\mathbb{Z})\backslash G} h d\mu_{\mathrm{SL}_2(\mathbb{Z})\backslash G} = \int_G f d\mu_G < +\infty$. But if $x \in \mathrm{SL}_2(\mathbb{Z})\backslash G$ and $g$ is an element of $\Omega'_\varepsilon$ such that $\pi(g) = x$, then

$$h(x) = \sum_{h \in \mathrm{SL}_2(\mathbb{Z})} f(hg) \geq f(g) = 1$$

(using the fact that $f \geq 0$). So

$$\mathrm{vol}(\mathrm{SL}_2(\mathbb{Z})\backslash G) \leq \int_{\mathrm{SL}_2(\mathbb{Z})\backslash G} h d\mu_{\mathrm{SL}_2(\mathbb{Z})\backslash G} < +\infty.$$

(5) Let $V := \{f \in L^2(X) | \int_X f(x) d\mu(x) = 0\}$. This is a $G$-invariant subspace of $L^2(X)$ because the measure $\mu$ is left invariant by $G$. We show that $V^G = 0$. Let $f \in L^2(X)^G$. Then we have $\|R_g f - f\|_{L^2(X)} = 0$ for every $g \in G$. Applying Minkowski inequality (see I.5.6.7) to the function $\varphi : G \times X \to \mathbb{C}$, $(g,x) \longmapsto |f(xg) - f(x)|$, we see that

$$\int_X \left| \int_G |f(xg) - f(x)| dg \right|^2 dx = 0,$$

so the function $x \longmapsto \int_G |f(xg) - f(x)| dg$ is 0 almost everywhere on $x$. Choose $x_0 \in X$ such that $\int_G |f(x_0 g) - f(x_0)| dg = 0$. Then the function $g \longmapsto f(x_0 g) - f(x_0)$ is 0 almost everywhere on $G$, so $f$ is equal in $L^2(X)$ to the class of the constant function $f(x_0)$. If moreover $f \in V$, this forces $f$ to be 0.

Now we can apply question (4) to $V$. Its conclusion says that, for all$f_1, f_2 \in V$, we have

$$\lim_{g \to +\infty} \langle R_g f_1, f_2 \rangle = 0.$$

Let $f_1, f_2 \in L^2(X)$. We write $c_1 = \int_X f_1 d\mu$ and $c_2 = \int_X f_2 d\mu$. As $\mathrm{vol}(X) = 1$, the functions $f_1 - c_1$ and $\overline{f_2 - c_2}$ are in $V$, so, by what we have just seen, we have

$$\lim_{g \to +\infty} \langle R_g f_1 - c_1, \overline{f_2 - c_2} \rangle = 0.$$

For every $g \in G$, we have

$$\begin{aligned}\langle R_g f_1 - c_1, \overline{f_2 - c_2}\rangle &= \int_X (f_1(xg) - c_1)(f_2(x) - c_2)dx \\ &= \int_X f_1(xg)f_2(x)dx - c_1 \int_X f_2(x)dx - c_2 \int_X f_1(xg)dx + c_1c_2 \\ &= \int_X f_1(xg)f_2(x)dx - c_1c_2.\end{aligned}$$

Finally, we get

$$\lim_{g\to+\infty} \int_X f_1(xg)f_2(x)dx = c_1c_2,$$

as desired.

(6) (a). We define a function $h : G \to \mathbb{C}$ by

$$h(x) = \int_K \psi(xy^{-1})d\mu_K(y),$$

for every $y \in G$. Let's show that $h$ is continuous. Let $\varepsilon > 0$. As $\psi \in \mathscr{C}_c(G)$, proposition I.1.12 implies that $\psi$ is left uniformly continuous, so there exists a neighborhood $U$ of $1$ in $G$ such that $|\psi(x'x) - \psi(x)| \leq \varepsilon$ for every $x \in G$ and every $x' \in U$. Then, if $x \in G$ and $x' \in U$, we have

$$|h(x'x) - h(x)| \leq \int_K |\psi(x'xy^{-1}) - \psi(xy^{-1})|d\mu_K(y) \leq \int_K \varepsilon d\mu_K = \varepsilon,$$

so $h$ is also left uniformly continuous (and in particular continuous). Moreover, ince we have $\psi(xy^{-1}) = 0$ unless $x \in (\operatorname{supp}\psi)y \subset (\operatorname{supp}\psi)K$, the support of $\psi$ is contained in $(\operatorname{supp}\psi)K$, hence it is compact.

Finally, for every $f \in \mathscr{C}_c(G)$, we have :

$$\begin{aligned}\psi * \mu_K(f) &= \int_{G\times K} f(xy)\psi(x)d\mu_G(x)d\mu_K(y) \\ &= \int_{G\times K} f(x)\psi(xy^{-1})d\mu_G(x)d\mu_K(y) \quad \text{(because } \Delta_{G|K} = 1\text{)} \\ &= \int_G f(x)h(x)d\mu_G(x).\end{aligned}$$

(b). Let $(U_n)_{n\geq 0}$ be a decreasing sequence of neighborhoods of $1$ in $G$ that forms a basis of neighborhoods; for example, we can take for $U_n$ the intersection of $G$ with the ball of radius $2^{-n}$ in $M_2(\mathbb{R})$, for any choice of norm on $M_2(\mathbb{R})$. By proposition I.4.1.8, there exists an approximate identity $(\psi_n)_{n\geq 0}$ such that $\operatorname{supp}(\psi_n) \subset U_n$ for every $n$.

We prove as in proposition I.4.1.9 that this sequence $(\psi_n)_{n\geq 0}$ works. Let $f \in \mathscr{C}_c(G)$. Then $\mu_K(f) = \int_K f(y)d\mu_K(y) = \int_{G\times K} f(y)\psi_n(x)d\mu_G(x)d\mu_K(y)$ for every $n$, so

$$|\psi_n{*}\mu_K(f){-}\mu_K(f)| \leq \int_{G\times K} |f(xy){-}f(y)|\psi(x)d\mu_G(x)d\mu_K(y) \leq \sup_{x\in U_n} \|L_{x^{-1}}f{-}f\|_\infty.$$

As $f$ is left uniformly continuous, this tends to $0$ when $n \to +\infty$.

$\square$

# VI Application of Fourier analysis to random walks on groups

We will mostly be interested in the case of finite groups in this chapter, but we will give some results for more general groups in the last section.

## VI.1 Finite Markov chains

We fix once and for all a probability space $\Omega$ (i.e. a measure space with total volume one).

**Definition VI.1.1.** Let $X$ be a measurable space (i.e. a space with a $\sigma$-algebra). A *random variable* with values in $X$ is a measurable function $X : \Omega \to X$.

For every measurable subset $A$ of $X$, we write $\mathbb{P}(X \in A)$ for the measure of $X^{-1}(A)$. (We think of this as the probability that $X$ is in $A$.) The *distribution* of $X$ is the probability distribution $\mu$ on $X$ defined by $\mu(A) = \mathbb{P}(X \in A)$.

We think of random variables as representing the outcome of some experiment or observation. The probability space $\Omega$ is usually not specified (you can think of it as something like "all the possible universes"). For example, we could think of the outcome of flipping a coin as a random variable with values in the finite set $\{\text{heads}, \text{tails}\}$. If the coin is unbiased, the distribution of that random variable is given by $\mu(\{\text{heads}\}) = \mu(\{\text{tails}\}) = \frac{1}{2}$.

In this notes, we will only be concerned with the case where $X$ is finite and its $\sigma$-algebra is the set of all subsets of $X$. We can (and will) think of measures on $X$ as functions $\mu : X \to \mathbb{R}_{\geq 0}$.

**From now on, we assume that $X$ is finite.**

**Definition VI.1.2.** A matrix $P = (P_{i,j}) \in M_n(\mathbb{R})$ is called *stochastic* if $P_{i,j} \geq 0$ for all $i, j \in \{1, \ldots, n\}$ and $\sum_{j=1}^{n} P_{i,j} = 1$ for every $i \in \{1, \ldots, n\}$.

If $P : X \times X \to \mathbb{R}$ is a function, we think of it as a matrix of size $|X| \times |X|$ and we call is *stochastic* if $P(x, y) \geq 0$ for all $x, y \in X$ and $\sum_{y \in X} P(x, y) = 1$ for every $x \in X$.

**Definition VI.1.3.** Let $P : X^2 \to \mathbb{R}$ be a stochastic function and $\nu$ be a probability distribution on $X$ A (discrete-time homogeneous) *Markov chain* with *state space* $X$, *initial distribution* $\nu$ and *transition matrix* $P$ is a sequence $(X_n)_{n \geq 0}$ of random variables with values in $X$ such that :

(a) The distribution of $X_0$ is $\nu$.

(b) For every $n \geq 0$ and all $x_0, \dots, x_{n+1} \in X$, if $\mathbb{P}(X_n = x_n, \dots, X_0 = x_0) > 0$, then

$$\mathbb{P}(X_{n+1} = x_{n+1} | X_n = x_n, \dots, X_0 = x_0) = P(x_n, x_{n+1}).$$

Let $P, Q : X^2 \to \mathbb{R}$ be two functions. We write $PQ$ for the function $X^2 \to \mathbb{R}$ defined by

$$PQ(x, y) = \sum_{z \in X} P(x, z)Q(z, y).$$

(If we see functions on $X^2$ as matrices, this is the usual matrix product.)

In particular, we write $P^n$ for the product $PP \dots P$ ($n$ times); by convention, $P^0$ is the characteristic function of the diagonal.

**Lemma VI.1.4.** *Let $(X_n)_{n \geq 0}$ be a Markov chain on $X$ with initial distribution $\nu$ and transition matrix $P$. Then, for every $x \in X$, we have*

$$\mathbb{P}(X_n = x) = \sum_{y \in X} \nu(y) P^n(y, x).$$

In other words, if we see $P$ as a matrix and $\nu$ as a row vector, then the distribution of $X_n$ is $\nu P^n$.

*Proof.* We prove the result by induction on $n$. It is obvious for $n = 0$. Suppose that we know it for some $n$, and let's prove it for $n + 1$. Let $x \in X$. Then

$$\begin{aligned}
\mathbb{P}(X_{n+1} = x) &= \sum_{y \in X,\ \mathbb{P}(X_n = y) \neq 0} \mathbb{P}(X_{n+1} = x | X_n = y) \\
&= \sum_{y \in X} \mathbb{P}(X_n = y) \mathbb{P}(X_{n+1} = x | X_n = y) \\
&= \sum_{y \in X} \mathbb{P}(X_n = y) P(y, x).
\end{aligned}$$

Using the induction hypothesis, we get

$$\mathbb{P}(X_{n+1} = x) = \sum_{y \in X} P(y, x) \sum_{z \in X} \nu(z) P^n(z, y) = \sum_{z \in X} \nu(z) P^{n+1}(z, x).$$

□

**Example VI.1.5.** (1) Random walk on the discrete circle : We take $X = \mathbb{Z}/r\mathbb{Z}$, $\nu = \delta_0$ and $P$ defined by

$$P(x,y) = \begin{cases} \frac{1}{2} & \text{if } x-y \in \{\pm 1\} \\ 0 & \text{otherwise.} \end{cases}$$

The Markov chain is modeling a random walk on the "discrete circle" $\mathbb{Z}/n\mathbb{Z}$ where we start at $0$ with probability $1$, and then, at each time $n$, we have a 50% chance to go to the preceding point on the discrete circle and a 50% chance to go to the next point of the circle.

(2) Mixing a deck of cards using random transpositions : We are trying to understand the following situation : We have a deck of $N$ cards. At each time $n$, we randomly (uniformly and independently) choose two cards and switch their positions in the deck. How long will it take to mix the deck ?

This problem is modeled by a Markov chain with state space $\mathfrak{S}_N$ (representing all the possible orderings of the deck), initial distribution the Dirac measure supported at our starting position, and transition matrix $P$ given by

$$P(\tau\sigma,\sigma) = \begin{cases} \frac{1}{N} & \text{if } \tau = 1 \\ \frac{2}{N^2} & \text{if } \tau \text{ is a transposition} \\ 0 & \text{otherwise.} \end{cases}$$

(3) The Bernoulli-Laplace diffusion model : We have two urns labeled by $0$ and $1$. At the start, urn $0$ contains $r$ red balls and urn $1$ contains $b$ blue balls. At each time $n$, we choose a ball in each urn (uniformly and independently) and switch them. How long will it take to mix the balls ?

We model this problem using a Markov chain with state space $\mathfrak{S}_N / \mathfrak{S}_r \times \mathfrak{S}_b$, where $N = r + b$, and $\mathfrak{S}_r \times \mathfrak{S}_b$ is embedded in $\mathfrak{S}_N$ via the obvious bijection $\{1,\dots,r\} \times \{1,\dots,b\} \simeq \{1,\dots,N\}$. Indeed, we can think of the $N$ balls as the set $\{1,\dots,N\}$, where the first $r$ balls are red and the last $b$ balls are blue. A state of the process described above is a subset $A$ of $\{1,\dots,N\}$ such that $|A| = r$ (the content of urn $0$); note that switching two balls between the urns does not change the number of balls in each urn. The group $\mathfrak{S}_N$ acts transitively on the set $\Omega_r$ of cardinality $r$ subsets of $\{1,\dots,N\}$, and its subgroup $\mathfrak{S}_r \times \mathfrak{S}_b$ is the stabilizer of $\{1,\dots,r\}$, so the state set is indeed in bijection with $\mathfrak{S}_N / \mathfrak{S}_r \times \mathfrak{S}_b$. The initial distribution is the Dirac measure concentrated at $\{1,\dots,r\}$ The transition matrix $P$ is given by

$$P(A',A) = \begin{cases} \frac{(r-1)!(b-1)!}{(r+b)!} & \text{if } r - |A \cap A'| = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Indeed, we need the calculate the number of pairs $(A,A')$ of subsets of cardinality $r$ of $\{1,\dots,N\}$ such that $r - |A \cap A'| = 1$; note that the condition means that $A' - A$ and $A - A'$ both have exactly one element. There are $\frac{(r+b)!}{r!b!}$ choices for $A$, $b$ choicse for the element of $A' - A$ and $r$ choices for the element of $A - A'$.

We have been asking if the chains described in the examples converge, but the first question should be : to what distribution(s) can they converge ?

**Definition VI.1.6.** Consider a stochastic function $P : X^2 \to \mathbb{R}$. A *stationary distribution* for $P$ is a probability distribution $\mu$ on $X$ such that, for every $y \in X$, we have

$$\mu(y) = \sum_{x \in X} \mu(x) P(x, y).$$

If we think of $P$ as a $|X| \times |X|$ matrix and of $\mu$ as a row vector of size $|X|$, then the condition becomes $\mu P = \mu$.

If a Markov chain with transition matrix $P$ converges in any reasonable sense, then the distribution of its limit should be a stationary distribution of $P$.

Finally, we define the distance that we will use on random variables. Note that this definition makes just as much sense if $X$ is a general measure space, and the lemma following it stays true with essentially the same proof.

**Definition VI.1.7.** Let $\mu$ and $\nu$ be two probability distributions on $X$. Their *total variation distance* is

$$\|X - Y\|_{TV} = \max_{A \subset X} |\mu(A) - \nu(A)|.$$

This is clearly a metric on the set of probability distributions, and in fact it is closely related to the $L^1$ metric.

**Lemma VI.1.8.** *Let $\mu$ and $\nu$ be two probability distributions on $X$. Then we have*

$$\|\mu - \nu\|_{TV} = \frac{1}{2} \sum_{x \in X} |\mu(x) - \nu(x)|.$$

*Proof.* Let $B = \{x \in X | \mu(x) \geq \nu(x)\}$. For every $A \subset X$, we have

$$\begin{aligned}
\mu(A) - \nu(A) &= \mu(A \cap B) - \nu(A \cap B) + \sum_{x \in A - A \cap B} (\mu(x) - \nu(x)) \\
&\leq \mu(A \cap B) - \nu(A \cap B) \\
&= \mu(B) - \nu(B) - \sum_{x \in B - A \cap B} (\mu(x) - \nu(x)) \\
&\leq \mu(B) - \nu(B).
\end{aligned}$$

Similarly, we have

$$\nu(A) - \mu(A) \leq \nu(X - B) - \mu(X - B) = \mu(B) - \nu(B).$$

Hence $|\mu(A)-\nu(A)| \leq \mu(B)-\nu(B)$, with equality if $A=B$ or $A=X-B$, and we get

$$\begin{aligned}\|\mu-\nu\|_{TV} = \mu(B)-\nu(B) &= \frac{1}{2}(\mu(B)-\nu(B)+\nu(X-B)-\mu(X-B)) \\ &= \frac{1}{2}\sum_{x\in B}|\mu(x)-\nu(x)| + \frac{1}{2}\sum_{x\in X-B}|\mu(x)-\nu(x)| \\ &= \frac{1}{2}\|\mu-\nu\|_1.\end{aligned}$$

□

## VI.2 The Perron-Frobenius theorem and convergence of Markov chains

**Notation VI.2.1.** Let $A, B \in M_{nm}(\mathbb{R})$. We say that $A \geq B$ (resp. $A > B$) if $A_{ij} \geq B_{ij}$ (resp. $A_{ij} > B_{ij}$) for every $(i,j) \in \{1,\dots,n\}\times\{1,\dots,m\}$. We also denote by $|A|$ the $n\times m$ matrix $(|A_{ij}|)$.

**Definition VI.2.2.** We say that a matrix $P = (P_{ij}) \in M_n(\mathbb{R})$ is *positive* if $P > 0$.

**Definition VI.2.3.** We say that a stochastic matric $P \in M_n(\mathbb{R})$ is *ergodic* if there exists a positive integer $r$ such that $P^r$ is positive.

Remember the following classical theorem from linear algebra :

**Theorem VI.2.4** (Perron-Frobenius theorem)**.** *Let $P=(P_{ij}) \in M_n(\mathbb{R})$ be an ergodic stochastic matrix. Then :*

*(i) The matrix $P$ has $1$ as a simple eigenvalue, and every complex eigenvalue $\lambda$ of $P$ satisfies $|\lambda| < 1$.*

*(ii) The space of row vectors $w \in M_{1n}(\mathbb{R})$ such that $wP = w$ is $1$-dimensional, and it has a generator $v = (v_1,\dots,v_n)$ such that $v_i > 0$ for every $i$ and $v_1+\dots+v_n = 1$.*

*(iii) Let $P_\infty$ be the $n\times n$ matrix all of whose rows are equal to the vector $v$ of (ii). Then $P^r \to P_\infty$ as $r \to +\infty$. More precisely, let $\rho = \max\{|\lambda|,\ \lambda \neq 1$ eigenvalue of $P\}$; by (i), we know that $\rho < 1$. Fix any norm $\|.\|$ on $M_n(\mathbb{R})$. Then there exists a polynomial $f \in \mathbb{Z}[t]$ such that*

$$\|P^k - P_\infty\| \leq f(k)\rho^k.$$

**Lemma VI.2.5.** *Let $A = (A_{ij}) \in M_n(\mathbb{R})$ be a positive matrix, let*

$$Z = \{x = (x_1,\dots,x_n) \in \mathbb{R}^n | x \geq 0 \text{ and } x_1+\dots+x_n = 1\},$$

*and let*

$$\Lambda = \{\lambda \in \mathbb{R} | \exists x \in Z,\ Ax \geq \lambda x\}.$$

*Then the real number* $\lambda_0 = \sup \Lambda$ *is positive and a simple root of the characteristic polynomial of* $A$*, and it has an eigenvector all of whose entries are positive. Moreover, for any complex eigenvalue* $\lambda \neq \lambda_0$ *of* $A$*, we have* $|\lambda| < \lambda_0$*.*

*Proof.* Note that $\Lambda \neq \varnothing$ because $0 \in \Lambda$, and $\Lambda$ is bounded above by the sum of all the entries of $A$. So $\lambda_0$ is well-defined and nonnegative. Let $(\mu_n)_{n\geq 0}$ be a sequence of elements of $\Lambda$ converging to $\lambda_0$; for every $n \geq 0$, choose $x^{(n)} \in Z$ such that $Ax^{(n)} \geq \mu_n x^{(n)}$. As $Z$ is compact, we may assume that the sequence $(x^{(n)})_{n\geq 0}$ converges to some $x \in Z$, and then we have $Ax \geq \lambda_0 x$. Suppose that $Ax \neq \lambda_0 x$, then, as $A > 0$, we get $A(Ax) > \lambda_0 Ax$. As $Ax \geq 0$ and $Ax \neq 0$, we can multiply $Ax$ by a positive scalar to get a vector $y \in Z$ such that $Ay > \lambda_0 y$, which contradicts the definition of $\lambda_0$. So $Ax = \lambda_0 x$. Also, as $x$ has at least one positive entry and $A > 0$, the vector $\lambda_0 x = Ax$ has all its entries positive, which implies that $\lambda_0 > 0$ and $x > 0$.

Next we show that every complex eigenvalue $\lambda \neq \lambda_0$ of $A$ satisfies $|\lambda| < \lambda_0$. Let $\lambda$ be a complex eigenvalue of $A$. Then there exists a nonzero vector $y = (y_1, \ldots, y_n) \in \mathbb{C}^n$ such that $Ay = \lambda y$. For every $i \in \{1, \ldots, n\}$, we have

$$|\lambda||y_i| = \left|\sum_{j=1}^{n} A_{i,j} y_j\right| \leq \sum_{j=1} A_{i,j}|y_j|.$$

In other words, we have $A|y| \geq |\lambda||y|$. As we can normalize $|y|$ to get an element of $Z$, this shows that $|\lambda| \leq \lambda_0$. Suppose that $|\lambda| = \lambda_0$. As $A > 0$, there exists a positive real number $\delta$ such that $A' := A - \delta I_n > 0$. Then $\mu \longmapsto \mu - \delta$ induces a bijection between the eigenvalues and those of $A'$, and in particular $\lambda_0 - \delta$ is the biggest real eigenvalue of $A'$ (and it is positive because $A' > 0$). By applying the beginning of the paragraph to $A'$, we see that $|\lambda - \delta| \leq \lambda_0 - \delta$. But then

$$\lambda_0 = |\lambda| = |\lambda - \delta + \delta| \leq |\lambda - \delta| + \delta \leq \lambda_0,$$

so $|\lambda - \delta| + \delta = |\lambda|$, so $\lambda \in \mathbb{R}_{\geq \delta}$, and we must have $\lambda = \lambda_0$.

Let's show that the eigenspace $E_{\lambda_0} := \operatorname{Ker}(A - \lambda_0 I_n)$ has dimension 1. Suppose that there exists $y = (y_1, \ldots, y_n) \in E_{\lambda_0}$ (with real entries) such that the family $\{x, y\}$ is linearly independent. We may assume that $y$ has at least one positive entry. Write $x = (x_1, \ldots, x_n)$, and let $\mu = \sup\{\nu \in \mathbb{R} | \forall i \in \{1, \ldots, n\},\ x_i \geq \nu y_i\}$. Then $x - \nu y \geq 0$ and $x - \nu y \not> 0$. The vector $x - \nu y$ is nonzero because $x$ and $y$ are linearly independent, and we have $A(x - \nu y) = \lambda_0(x - \nu y)$. As $A > 0$, $x - \nu y \geq 0$ and $\lambda_0$, this implies $x - \nu y > 0$, contradicting the choice of $\nu$.

Now we show that $\lambda_0$ is a simple root of the characteristic polynomial $\chi_A(t)$ of $A$. We can find $g \in \mathrm{GL}_n(\mathbb{R})$ such that $g^{-1}Ag$ is of the form $\begin{pmatrix} \lambda_0 & * \\ 0 & B \end{pmatrix}$, with $B \in M_{n-1}(\mathbb{R})$. We have $\chi_A(t) = (t - \lambda_0)\chi_B(t)$. Suppose that the multiplicity of $\lambda_0$ as a root of $\chi_A(t)$ is $\geq 2$. Then $\lambda_0$

is a root of $\chi_B(t)$, so there exists $z \in \mathbb{R}^{n-1}$ such that $Bz = \lambda_0 z$. Let $y = g \begin{pmatrix} 0 \\ z \end{pmatrix} \in \mathbb{R}^n$, then $Ay = \lambda_0 y + \alpha x$ for some $\alpha \in \mathbb{R}$. As $\dim(E_{\lambda_0}) \neq 0$, the vector $y$ cannot be an eigenvector of $A$, so $\alpha \neq 0$. An easy induction (using the fact that $Ax = \lambda_0 x$) shows that, for every positive integer $r$, we have $A^r y = \lambda_0^r y + r\alpha\lambda_0^{r-1}x$. As $A^r > 0$, this implies that

$$A^r|y| \geq |A^r y| = |\lambda_0^r y + r\alpha\lambda_0^{r-1}x| \geq |r\alpha\lambda_0^{r-1}x| - \lambda_0^r|y| = \lambda_0^{r-1}(r|\alpha x| - \lambda_0|y|).$$

As $\alpha \neq 0$ and $x > 0$, there exists a positive integer $r$ such that $r|\alpha x| - \lambda_0|y| > \lambda_0|y|$, and then we have $A^r|y| > \lambda_0^r|y|$. As $A^r > 0$, applying the beginning of the proof to $A^r$, we see that this implies that $A^r$ has a real eigenvalue $> \lambda_0^r$. But this impossible, because the eigenvalues of $A^r$ are the $r$th powers of the eigenvalues of $A$, so they all absolute value $\leq \lambda_0^r$.

□

*Proof of the theorem.* We prove (i). Let $v_0 = (1, \dots, 1) \in \mathbb{R}^n$. Then the fact that $P$ is stochastic is equivalent to the fact $P \geq 0$ and $Pv_0 = v_0$. As all the matrices $P^r$ for $r \geq 1$ have nonnegative entries and satisfy $P^r v_0 = v_0$, they are all stochastic. Also, if $x = (x_1, \dots, x_n) \in (\mathbb{R}_{\geq 0})^n$ and $Q = (Q_{ij}) \in M_n(\mathbb{R})$ is stochastic, then, for every $i \in \{1, \dots, n\}$, we have

$$(Qx)_i = \sum_{j=1}^n Q_{ij}x_j \leq \sup_{1 \leq j \leq n} x_j.$$

Fix an integer $r \geq 1$ such that $P^r > 0$. By the lemma, the matrix $P^r$ has a simple real positive eigenvalue $\lambda_0$ such that every complex eigenvalue $\lambda \neq \lambda_0$ of $P^r$ satisfies $|\lambda| < \lambda_0$. By the definition of $\lambda_0$ in the lemma and the observation above about stochastic matrices, we have $\lambda_0 \leq 1$. On the other hand, we have $Pv_0 = v_0$, so $1$ is an eigenvalue of $P$, hence also of $P^r$, and so $\lambda_0 = 1$. Let $\lambda \in \mathbb{C}$ be an eigenvalue of $P$, and $y \in \mathbb{C}^n$ be an eigenvector for this eigenvalue. Then $P^r y = \lambda^r y$, so $\lambda^r$ is an eigenvalue of $P^r$. If $\lambda^r \neq 1$, then $|\lambda^r| < 1$ by the lemma, hence $|\lambda| < 1$. If $\lambda^r = 1$, then the eigenvector $y$ must be in $\mathrm{Ker}(P^r - I_n)$, and we know (again by the lemma) that this space is 1-dimensional. As $v_0 \in \mathrm{Ker}(P^r - I_n)$, the vector $y$ must be a multiple of $v_0$, and then $\lambda = 1$.

Finally, if the characteristic polynomial of $P$ is $\chi_P(t) = (t - \lambda_1) \dots (t - \lambda_n)$, then that of $P^r$ is $\chi_{P^r}(t) = (t - \lambda_1^r) \dots (t - \lambda_n^r)$. So the multiplicity of $1$ in $\chi_P(t)$ is at most its mutliplicity in $\chi_{P^r}(t)$, which we know is $1$ by the lemma. This finishes the proof of (i).

Let's prove (ii). As $P$ and $P^T$ have the same characteristic polynomial, we know that $1$ is a simple eigenvalue of $P^T$ by (i), so the space of row vectors $w$ such that $wP = w$ has dimension 1. Let $w = (w_1, \dots, w_n)$ be a nonzero vector in this space. Then we also have $|w|P = |w|$. Indeed, for every $j \in \{1, \dots, n\}$, we have

$$|w_j| = \left| \sum_{i=1}^n w_i P_{ij} \right| \leq \sum_{i=1}^n |w_i| P_{i,j}$$

(because all the $P_{ij}$ are nonnegative). Suppose that $|w| \neq |w|P$. Then there exists $j_0 \in \{1, \ldots, n\}$ such that $|w_{j_0}| < \sum_{i=1}^n |w_i| P_{ij_0}$, and this implies that

$$\sum_{i=1}^n |w_i| = \sum_{i,j=1}^n |w_i| P_{ij} > \sum_{j=1}^n |w_j|,$$

a contradiction. As $w \neq 0$, at least one of the $|w_i|$ is positive. If we choose as before $r \geq 1$ such that $P^r > 0$, then $|w| = P^r|w|$, so, for every $j \in \{1, \ldots, n\}$, we have $|w_j| = \sum_{i=1}^n (P^r)_{i,j} |w_i| > 0$. This finishes the proof of (ii).

We finally prove (iii). As all the norms on $M_n(\mathbb{R})$ are equivalent, it suffices to prove the statement for a particular norm. By the existence of the Jordan normal form (actually by the Jordan-Chevalley decomposition), there exists a matrix $g \in \mathrm{GL}_n(\mathbb{R})$ with $g^{-1}Pg = A = \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}$, with $B \in M_{n-1}(\mathbb{R})$ such that $B = D + N$, with $D$ a diagonal matrix, $N$ a nilpotent matrix and $DN = ND$. Choose the operator norm $\|.\|$ on $M_n(\mathbb{R})$ coming from the usual Euclidian norm on $\mathbb{R}^n$. The entries of $D$ are the eigenvalues of $P$ different from 1, so $\|D\| = \rho$. As $D$ and $N$ commute, we have, for every $k \in \mathbb{Z}_{\geq 0}$,

$$B^k = (D + N)^k = \sum_{j=0}^k \binom{k}{j} D^{k-j} N^j.$$

If $k \geq n$ (in fact, $k \geq n - 1$ suffices), then this simplifies to $\sum_{j=0}^n \binom{k}{j} D^{k-j} N^j$, because $N^j = 0$ for $j \geq n$. Hence, if $k \geq n$,

$$\|B^k\| \leq \sum_{j=0}^n \binom{k}{j} \|D\|^{k-j} \|N\|^j \leq \rho^{k-n} \sum_{j=0}^n k^j \|N\|^j.$$

Let $A_\infty = \begin{pmatrix} 1 & 0 \\ 0 & B_\infty \end{pmatrix}$, with $B_\infty = 0 \in M_{n-1}(\mathbb{R})$. Then $\|A^k - A_\infty\| = \|B^k\|$ for every $k \geq 0$, so $A^k \to A_\infty$ as $k \to +\infty$ (because $\rho < 1$). This implies that $P^k \to P' := gA_\infty g^{-1}$ as $k \to +\infty$. Also,

$$\|P^k - P'\| = \|g^{-1}(A^k - A_\infty)g\| \leq \|g\| \|g^{-1}\| \|B^k\|,$$

which is bounded by the product of $\rho^k$ and of a polynomial in $k$. So it only remains to show that $P' = P_\infty$. As $P' = \lim_{k \to +\infty} P^k$, we have $P'P = PP' = P'$. Remember that 1 is a simple eigenvalue of $P$ and of $P^T$. So all the rows of $P'$ are multiples of the corresponding eigenvector of $P^T$, i.e. of $v$. Also, as $P^k$ is stochastic for every $k \geq 0$, its limit $P'$ is stochastic. So all the rows of $P'$ have nonnegative entries whose sum is 1, which means that they are all equal to $v$, and that $P' = P_\infty$.

□

**Definition VI.2.6.** A Markov chain with transition matrix $P$ is called *ergodic* if $P$ is ergodic.

In example VI.1.5, all the chains are ergodic, except the Markov chain of (1) when $r$ is even.

**Corollary VI.2.7.** *Let $(X_n)_{n\geq 0}$ be an ergodic Markov chain with transition matrix $P$. Then $P$ has a unique stationary distribution $\mu$, and, if $\mu_n$ is the distribution of $X_n$, we have*

$$\|\mu_n - \mu\|_{TV} \leq f(n)\rho^n,$$

*where $f$ is a polynomial and $\rho = \max\{|\lambda|,\ \lambda \neq 1$ eigenvalue of $P\} < 1$.*

*Proof.* Let $\nu$ be the initial distribution of the Markov chain. By lemma VI.1.4, we have $\mu_n = \nu P^n$. Let $P_\infty$ be the limit of the sequence $(P^n)_{n\geq 0}$. All the rows of $P_\infty$ are equal to $\mu$, so $\nu P_\infty = \mu$. If we use the $L^1$ norm on the space of functions from $X$ to $\mathbb{R}$ (for the counting measure on $X$) to define the operator norm $\|.\|$ on the space of matrices, then we have

$$\|\mu_n - \mu\|_{TV} = \frac{1}{2}\|\mu_n - \mu\|_1 = \frac{1}{2}\|\nu P^n - \nu P_\infty\|_1 \leq \frac{1}{2}\|\nu\|_1\|P^n - P_\infty\|,$$

so the bound on $\|\mu_n - \mu\|_{TV}$ follows immediately from (iii) of the theorem.

□

*Remark* VI.2.8. Although the bound on $\|\mu_n - \mu\|_{TV}$ looks quite good (it is exponential), it is useless if we want to know when exactly $\mu_n$ becomes close to the stationary distribution. We need to analyse the problem more closely to answer that kind of question. This is what we will now try to do in some particular cases.

**Example VI.2.9.** The chain of example VI.1.5(2) is ergodic. Indeed, let $T \subset \mathfrak{S}_n$ be the union of $\{1\}$ and of the set of transpositions. Then, for $r \geq 1$ and $\sigma, \sigma' \in \mathfrak{S}_n$, we have $P^r(\sigma', \sigma) > 0$ if and only if $\sigma'\sigma^{-1}$ can be written as a product of exactly $r$ elements of $T$; as $1 \in T$, this is equivalent to the condition that $\sigma'\sigma^{-1}$ can be written as a product of $s$ transpositions, for some $s \leq r$. So if $r \geq \frac{n(n-1)}{2}$ (the length of the longest element of $\mathfrak{S}_n$), then $P^r(\sigma', \sigma) > 0$ for all $\sigma, \sigma' \in \mathfrak{S}_n$.

## VI.3 A criterion for ergodicity

The definitions and results ot this sectiona are not used in the next sections.

Remember the following definitions :

**Definition VI.3.1.** A (finite unoriented) graph is a pair $G = (X, E)$, where $X$ is a finite set and $E$ is a set of unordered pairs $\{x, y\}$ of distinct elements of $X$. We say that $X$ is the set of *vertices* of $G$ and that $E$ is the set of *edges*.

Let $x, y \in X$. A path connecting $x$ and $y$ in the graph $G$ is a sequence $p = (e_0, \dots, e_n)$ of edges of $G$ such that we can write $e_i = \{x_i, y_i\}$ with $x_0 = x$, $y_n = y$ and $y_i = x_{i+1}$ for every

$i \in \{0, \dots, n-1\}$. We call the integer $n+1$ the *length* of the path $p$ and denoted by $|p|$. If $x = y$, we say that the path if a *closed path* or a *loop* based at $x$.

We say that the graph $G$ is *connected* if for every $x, y \in X$, there exists a path connected $x$ and $y$. We say that $G$ is *bipartite* if there exists a surjective function $\phi : X \to \{-1, 1\}$ such that, for every edge $e = \{x, y\}$ of $G$, we gave $\phi(x) \neq \phi(y)$. (In other parts, we can partition $X$ into two nonempty subsets $X_0$ and $X_1$ such that every edge connects an element of $X_0$ to an element of $X_1$.)

For every $x, y \in X$, the *distance* $d(x, y)$ between $x$ and $y$ is the length of the shortest path connecting $x$ and $y$; if there is no such path, then we set $d(x, y) = +\infty$. Note that this defines a metric on $X$ if $G$ is connected.

The following result is classical.

**Proposition VI.3.2.** *Let $G = (X, E)$ be a connected graph such that $|X| \geq 2$. Then the following conditions are equivalent :*

*(i) $G$ is bipartite;*

*(ii) every loop in $G$ has even length;*

*(iii) there exists $x_0$ such that every loop based at $x_0$ has even length.*

*Proof.* We show that (i) implies (ii). Suppose that $G$ is bipartite, and let $\phi : X \to \{-1, 1\}$ be as in the definition above. Let $(e_0, \dots, e_n)$ be a loop in $G$. We write $e_i = \{x_i, y_i\}$ with $x_i = y_{i+1}$ for $0 \leq i \leq n-1$ and $y_n = x_0$. Then an easy induction on $i$ shows that, if $i$ is even, we have $\phi(x_i) = \phi(x_0)$ and $\phi(y_i) \neq \phi(x_0)$, and, if $i$ is odd, we have $\phi(x_i) \neq \phi(x_0)$ and $\phi(y_i) = \phi(x_0)$. But $y_n = x_0$, so $\phi(y_n) = \phi(x_0)$, so $n$ is odd, and the loop has even length.

It is obvious that (ii) implies (iii). Now assume (iii) and let's show (i). Pick $x_0 \in X$ such that every loop based at $x_0$ has even length. We want to define a function $\phi : X \to \{0, 1\}$. Let $y \in X$. As $G$ is connected, there exists a path $p = (e_0, \dots, e_n)$ connecting $x_0$ and $x$, and we set $\phi(x) = (-1)^{|p|}$. We need to show that this does not depend on the path. Let $q = (f_0, \dots, f_m)$ be another path connecting $x_0$ and $x$. Then $(e_0, \dots, e_n, f_m, \dots, f_0)$ is a loop based at $x_0$, so it has even length by assumption, so $|p| + |q|$ and even, and $(-1)^{|p|} = (-1)^{|q|}$. Note that $\phi(x_0) = 1$ and that $\phi(x) = -1$ if $\{x_0, x\}$ is an edge (such an edge must exist because $G$ is connected and $|X| \geq 2$). So $\phi$ is surjective. Let $e = \{x, y\}$ be an edge of $G$. Let $p = (e_0, \dots, e_n)$ be a path connecting $x_0$ and $x$. Then $p' := (e_0, \dots . e_n, e)$ is a path connecting $x_0$ and $y$, and $|p'| = |p| + 1$, so $\phi(x) \neq \phi(y)$. This shows that $G$ is bipartite.

$\square$

We now come to the connection with Markov chains.

**Proposition VI.3.3.** *Let $X$ be a finite set and $P : X \times X \to \mathbb{R}$ be a stochastic function. We define a graph $G = (X, E)$ in the following way : a pair $\{x, y\}$ of distinct elements of $X$ is an edge of $G$ if and only if $P(x, y) > 0$.*

*Suppose that $G$ is connected and that it is not bipartite. Then the function $P$ is ergodic.*

*Proof.* Note that, for every $x, y \in X$ and every $n \geq 1$, we have $P^n(x,y) > 0$ if and only if there exists a path of length $n$ connecting $x$ and $y$.

By proposition VI.3.2, for every $x \in X$, there exists a loop $p_x$ of odd length based at $x$. Write $2m+1 = \max_{x \in X} |p_x|$, with $m \in \mathbb{Z}_{\geq 0}$. Let $x \in X$. Let's show that, for every $n \geq 2m$, there is a loop of length $n$ based at $x$. Let $\{x, z\}$ be an edge. For every $r \geq 0$, write $q_{2r}$ for the loop of length $2r$ given by $q_{2r} = (\{x,z\}, \{z,x\}, \dots, \{x,z\}, \{z,x\})$. Let $n \geq 2m$. If $n$ is even, then $q_n$ is a loop of length $n$ based at $x$. If $n$ is odd, then $r := \frac{n - |p_x|}{2}$ is a nonnegative integer, and the loop obtained by concatening $p_x$ and $q_{2r}$ has length $n$ and contains $x$.

Let $\delta = \max_{x,y \in X} d(x,y)$. (This is called the *diameter* of the graph $G$.) Let $x, y \in X$ and $n \geq 2m + \delta$, and let's show that there is a path of length connecting $x$ and $y$ (this will finish the proof). Let $p$ be any path connecting $x$ and $y$. Then $|p| \leq \delta$, so, by the previous paragraph, there exists a loop $q$ of length $n - |p|$ based at $x$. The concatenation of $p$ and $q$ is the desired path.

□

**Corollary VI.3.4.** *(i) The chain of example VI.1.5(1) is ergodic if and only if r is odd.*

*(ii) The chain of example VI.1.5(3) is ergodic if $r \leq n-1$.*

We will reprove (ii) by a different method in section VI.5.

*Proof.* (i) The graph corresponding to the chain has $\mathbb{Z}/r\mathbb{Z}$ as set of vertices, and there is an edge between $a, b \in \mathbb{Z}/r\mathbb{Z}$ if and only if $a - b \in \{\pm 1\}$. This graph is obviously connected, and ti is easy to see that it is bipartite if and only if $r$ is even. In particular, if $r$ is odd, then the proposition implies that the chain is ergodic.

Now assume that $r$ is even. An easy induction on $n$ shows that, for every $n \geq 1$ and all $a, b \in \mathbb{Z}/r\mathbb{Z}$, we have $P^n(a,b) = 0$ if the image of $n + a + b$ in $\mathbb{Z}/2\mathbb{Z}$ is nonzero. Indeed, this follows from the definition of $P$ if $n = 1$. Suppose the result known up to some $n \geq 1$, and let's prove it for $n+1$. Let $a, b \in \mathbb{Z}/r\mathbb{Z}$ be such that $P^{n+1}(a,b) \neq 0$. As $P^{n+1}(a,b) = \sum_{c \in \mathbb{Z}/r\mathbb{Z}} P(a,c) P^n(c,b)$, there exists $c \in \mathbb{Z}/r\mathbb{Z}$ such that $P(a,c) \neq 0$ and $P^n(c,b) \neq 0$. By the induction hypothesis and the case $n = 1$, this implies that $a + c \neq 0 \mod 2$ and $n + c + b \neq 0 \mod 2$, and then $n + a + b + 2c = n + a + b = 0 \mod 2$.

(ii) The graph corresponding to the Markov chain has the set $\Omega_r$ of cardinality $r$ subsets of $\{1, \dots, n\}$ as its set of vertices, and there is an edge linking $A, A' \in \Omega_r$ if and only if $|A \cap A'| = r - 1$. Let $A_0 = \{1, \dots, r\}$. We first show that the graph is connected. Let $A \in \Omega_r$. We write $A = \{n_1, \dots, n_r\}$, and we choose the ordering of the elements such that $A \cap A_0 = \{1, \dots, n_s\}$, with $s = |A \cap A_0|$. Let $m_1, \dots, m_{r-s}$ be the elements of $A_0 - A$. For $0 \leq i \leq r - s$, let $B_i = \{n_1, \dots, n_{s+i}, m_{i+1}, \dots, m_{r-s}\}$. Then $B_0 = A_0$, $B_{r-s} = A$, and there is an edge between $B_i$ and $B_{i+1}$ for every $i \in \{0, \dots, r-s-1\}$. So the graph is connected.

Now we show that the graph is not bipartite, by finding a loop of odd length. Let $A = \{1, \dots, r-1, r+1\}$ and $B = \{2, \dots, r, r+1\}$. Then $\{A_0, A\}$, $\{A, B\}$ and $\{B, A_0\}$ are edges, so we have found a loop of length 3.

□

## VI.4 Random walks on homogeneous spaces

Now suppose that we have a finite group $G$ acting transitively (on the left) on the finite set $X$. Fix $x_0 \in X$, and let $K$ be the stabilizer of $x_0$ in $G$, so that we have a bijection $G/K \simeq X$, $g \longmapsto g \cdot x_0$.

Warning : We will be using the counting measure on $G$ to define convolution products and $L^p$ norms in this section. Beware constants ! (The reason for this choice is that we want the convolution of two probability distributions to be a probability distribution.)

**Definition VI.4.1.** If $\pi$ is a probability distribution on $G$, we denote by $P_\pi : X \times X \to \mathbb{R}$ the function defined by

$$P_\pi(xK, yK) = \pi(yKx^{-1}),$$

for all $x, y \in G$.

**Definition VI.4.2.** A *left-invariant random walk* on $X$ driven by $\pi$ and with initial distribution $\nu$ is a Markov chain with state space $X$, initial distribution $\nu$ and transition matrix $P_\pi$.

Here is the description of this Markov chain $(X_n)_{n\geq 0}$ in words : We choosing a starting point on $X$ according to the probability distribution $\nu$. At time $n$, we choose an element of $G$ using the probability distribution $\pi$ and act on our position by this element to get to the position at time $n+1$.

*Remark* VI.4.3. The matrix $P_\pi$ is actually *bistochastic*, i.e. both $P_\pi$ and its transpose are stochastic. Indeed, for every $y \in G$, we have

$$\begin{aligned}\sum_{x\in G/K} P_\pi(xK, yK) &= \sum_{x\in G/K} \pi(yKx^{-1}) \\ &= \sum_{x\in G} \pi(yx^{-1}) \\ &= 1.\end{aligned}$$

In particular, the uniform probability distribution on $X$ is an invariant distribution for $P_\pi$. If $P_\pi$ is ergodic, it is the only invariant distribution.

If the homogeneous space is $G$ itself, we can give a simple criterino for ergodicity. (See lemma 16.20 and proposition 16.21 of [1].)

**Proposition VI.4.4.** *Suppose that $X = G$, and let $S = \operatorname{supp}(\pi)$. Write $G_S$ for the set of elements of $G$ that can be written as $g_1 \dots g_{2r}$ for some $r \geq 0$, with exactly $r$ of the $g_i$ in $S$ and $r$ of the $g_i$ in $S^{-1}$.*

*Then $G_S$ is a subgroup of $G$, and the function $P_\pi$ is ergodic if and only if $G = G_S$.*

In particular, if $\pi(1) \neq 0$, then $P_\pi$ is ergodic if and only $S$ generates $G$. More generally, if $S$ generates $G$ and is not contained in a coset of a strict subgroup of $G$, then $P_\pi$ is ergodic. (Note that we have $S \subset gG_S$ for every $g \in S$.)

**Proposition VI.4.5.** *For every $n \geq 1$, we have $P_\pi^n = P_{\pi^{*n}}$, where $\pi^{*n}$ is the $n$-fold convolution product of $\pi$.*

*Proof.* We prove the result by induction on $n$. It is just the definition of $P_\pi$ if $n = 1$. Suppose the equality known for some $n \geq 1$, and let's prove it for $n+1$. Let $x, y \in X$. Then

$$\begin{aligned}
P_\pi^{n+1}(xK, yK) &= \sum_{z \in G/K} P_\pi(xK, zK) P_\pi^n(zK, yK) \\
&= \sum_{z \in G/K} \pi(zKx^{-1}) \pi^{*n}(yKz^{-1}) \\
&= \sum_{z \in G,\ h \in K} \pi(zx^{-1}) \pi^{*n}(yhz^{-1}) \\
&= \sum_{h \in K} \pi^{*(n+1)}(yhx^{-1}) \\
&= \pi^{*(n+1)}(x, y).
\end{aligned}$$

□

**Corollary VI.4.6.** *Let $\pi$ a probability measure on $G$, and suppose that $\pi$ is right invariant by $K$. Consider a left-invariant random walk $(X_n)_{n \geq 0}$ driven by $\pi$ and with initial distribution the Dirac measure concentrated at $x_0 \in X$. Let $\mu_n$ be the distribution of $X_n$, and let $\mu$ be the uniform probability distribution on $X$.*

*Then, for every $n \geq 0$, we have*

$$\|\mu_n - \mu\|_{TV}^2 \leq \frac{1}{4} \sum_{(\rho, V) \in \widehat{G} | V^K \neq 0 \text{ and } \rho \not\simeq \mathbb{1}} \dim(V) \operatorname{Tr}((\widehat{\pi}(\rho)^*)^n \circ \widehat{\pi}(\rho)^n),$$

*where we denote by $\mathbb{1}$ the trivial representation of $G$.*

Remember that, if $(\rho, V) \in \widehat{G}$ is an irreducible unitary representation of $G$ and $f : G \to \mathbb{C}$ is a function, then $\widehat{f}(\rho)$ is then endomorphism of $V$ defined by

$$\widehat{f}(\rho) = \sum_{x \in G} f(x) \rho(x^{-1}).$$

*Proof.* Fix $n \geq 0$. For every $x \in G$, we have

$$\mu_n(x) = P_\pi^n(x_0, x) = \pi^{*n}(xK)$$

by lemma VI.1.4 and proposition VI.4.5. Let $\pi_0$ be the uniform probability distribution on $G$. By lemma VI.1.8, we have

$$\begin{aligned}
\|\mu_n - \mu\|_{TV}^2 &= \frac{1}{4}\left(\sum_{x \in G/K} |\mu_n(x) - \mu(x)|\right)^2 \\
&= \frac{1}{4}\left(\sum_{x \in G} |\pi^{*n}(x) - \pi_0(x)|\right)^2 \\
&= \frac{1}{4}\|\pi^{*n} - \pi_0\|_1^2 \\
&\leq \frac{|G|}{4}\|\pi^{*n} - \pi_0\|_2^2,
\end{aligned}$$

where the last inequality is the Cauchy-Schwarz inequality. (Note that we are using the counting measure on $G$ to define the $L^p$ norms.) Let $f = \pi^{*n} - \pi_0 \in L^2(G)$. By the Parseval formula (theorem IV.6.3(iii), note the factor $\frac{1}{|G|}$ coming from the unnormalized Haar measure), we have

$$\|f\|^2 = \frac{1}{|G|} \sum_{(\rho,V) \in \widehat{G}} \dim(V) \mathrm{Tr}(\widehat{f}(\rho)^* \circ \widehat{f}(\rho)).$$

So we need to calculate the $\widehat{f}(\rho)$. Note that we have

$$\widehat{f}(\rho) = \widehat{\pi}(\rho)^n - \widehat{\mu}(\rho)$$

for every $\rho \in \widehat{G}$.

Suppose first that $\rho = \mathbb{1}$. Then $\widehat{\pi}(\rho) = \widehat{\mu}(\rho) = 1$, so $\widehat{f}(\rho) = 0$.

Let $(\rho, V) \in \widehat{G}$, and suppose that $\rho \not\simeq \mathbb{1}$. Then $\widehat{\mu}(\rho) = \sum_{x \in G} \rho(x^{-1})$ is an element of $\mathrm{End}(V)$ that is $G$-equivariant, hence a multiple of $\mathrm{id}_V$ by Schur's lemma, and has trace equal to $\frac{1}{|G|}\sum_{x \in G} \chi(x) = 0$ (by corollary IV.5.8). So $\widehat{\mu}(\rho) = 0$, and $\widehat{f}(\rho) = \widehat{\pi}(\rho)^n$. To finish the proof, we just need to show that $\widehat{\pi}(\rho) = 0$ if $V^K = 0$. Let $T = \widehat{\pi}(\rho) = \sum_{x \in G} \pi(x)\rho(x^{-1})$ and $P_K = \sum_{x \in K} \rho(x)$. As $\pi$ is right invariant by $K$, we have $\rho(x) \circ T = T$ for every $x \in K$, so $P_K \circ T = |K|T$. But $P_K$ is the orthogonal projection on $V^K$ by proposition V.1.7, so $\mathrm{Im}(T) \subset V^K$, and so $T = 0$ if $V^K = 0$.

□

**Corollary VI.4.7.** *With the notation of the previous corollary, suppose that $(G, K)$ is a Gelfand pair and that $\pi$ is bi-$K$-invariant. As in section V.6, let $Z$ be the dual space of $(G, K)$ (i.e. the set of spherical functions by theorem V.7.1).*

*Then, for every $n \geq 0$, we have*

$$|||\mu_n - \mu||^2_{TV} \leq \frac{1}{4} \sum_{\varphi \in Z,\ \varphi \neq 1} \dim(V_\varphi) |\widehat{\pi}(\varphi)|^{2n},$$

*where now, if $f \in \mathscr{C}(K \backslash G/K)$ and $\varphi \in Z$, the scalar $\widehat{f}(\varphi) \in \mathbb{C}$ is the spherical Fourier transform, defined by*

$$\widehat{f}(\varphi) = \sum_{x \in G} f(x) \varphi(x^{-1}).$$

*Proof.* The proof is almost the same as for the previous corollary, except that we use the Parseval formula of corollary V.7.2 to calculate $\|\pi^{*n} - \pi_0\|_2^2$. By this formula, we have

$$\|\pi^{*n} - \pi_0\|_2^2 = \frac{1}{|G|} \sum_{\varphi \in Z} \dim(V_\varphi) |\widehat{f}(\varphi)|^2,$$

where $f = \pi^{*n} - \pi_0$. If $\varphi = 1$ is the spherical function corresponding to the trivial representation, then $\widehat{\pi}(\varphi) = \widehat{\pi_0}(\varphi) = 1$, so $\widehat{f}(\varphi) = 0$. If $\varphi \neq 1$, then

$$\widehat{\pi_0}(\varphi) = \sum_{x \in G} \varphi(x^{-1}) = \langle 1, \varphi \rangle_{L^2(G)} = 0$$

(by (i) of theorem V.7.1 for example). So $\widehat{f}(\varphi) = \widehat{\pi}(\varphi)^n$, which finishes the proof.

□

## VI.5 Application to the Bernoulli-Laplace diffusion model

Remember that the Bernoulli-Laplace diffusion model was described in example VI.1.5(3). We have two positive integers $r$ and $b$. This model is a Markov chain $(X_n)_{n \geq 0}$ on the set $\Omega_r$ of subsets of cardinality $r$ of $\{1, \dots, r+b\}$ with initial distribution the Dirac distribution concentrated at $\{1, \dots, r\}$. The group $G := \mathfrak{S}_{r+b}$ acts transitively on $\Omega_r$, and the stabilizer of $A_0 := \{1, \dots, r\}$ is $K := \mathfrak{S}_r \times \mathfrak{S}_b$. The transition matrix $P$ of the chain is given by

$$P(A', A) = \begin{cases} \frac{(r-1)!(b-1)!}{(r+b)!} & \text{if } r - |A \cap A'| = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Remember that we have defined in exercise V.8.2.1(e) a metric $d$ on $\Omega_r$ by $d(A, A') = r - |A \cap A'|$, and that we have proved in V.8.2.1(d) (and V.8.2.1(f)) that the orbits of $K$ on $G/K \simeq \Omega_r$ are the spheres with center $A_0$ for this metric. Bi-invariant probability distributions $\pi$ on $G$ correspond bijectively to probability distributions on the set $K\backslash G/K$ of $K$-orbits on $G/K$, and the description of $P$ implies easily that $P = P_\pi$, where $\pi$ is the bi-invariant probability distribution that corresponding to the uniform distribution on the sphere with center $A_0$ and radius $1$.

If $\mu_n$ is the distribution of $X_n$ and $\mu$ is the uniform distribution of $\Omega_r$, then, by corollary VI.4.7, we have

$$\|\mu_n - \mu\|_{TV}^2 \leq \frac{1}{4} \sum_{\varphi \in Z - \{1\}} \dim(V_\varphi) |\widehat{\pi}(\varphi)|^{2n}.$$

We calculated all these terms in the exercises of section V.8.2. Suppose for example that $r \leq b$ (if not, we can just switch $r$ and $b$ and we get an equivalent problem). Then we saw how to decompose the quasi-regular representation of $G$ on $L^2(\Omega_r)$ into irreducible subrepresentations in exercise V.8.2.3 (see V.8.2.3(j) and V.8.2.3(k)), and we have exactly $r+1$ of them. We denote the corresponding spherical functions by $\varphi_0, \dots, \varphi_r$, as in exercise V.8.2.4. In particular, the function $\varphi_0$ is just the constant function $1$. We calculated these functions in V.8.2.3(f), but actually we only need V.8.2.3(g). Indeed, we only care about $\widehat{\pi}(\varphi_s)$, for $1 \leq s \leq r$. As $\pi$ corresponds to the uniform distribution on the sphere or radius $1$ centered at $A_0$, the number $\widehat{\pi}(\varphi_s)$ is just the coefficient of $\sigma_{1,r-1}(A_0)$ in $\varphi_s$ (with the notation of exercise V.8.2.3), that is,

$$\widehat{\pi}(\varphi_s) = 1 - \frac{s(r+b-s+1)}{rb}.$$

Also, V.8.2.3(f) says that

$$\dim(V_{\varphi_s}) = \binom{r+b}{s} - \binom{r+b}{s-1}$$

if $1 \leq s \leq r$.

So corollary VI.4.7 gives

$$\|\mu_n - \mu\|_{TV} \leq \frac{1}{4} \sum_{s=1}^{r} \left( \binom{r+b}{s} - \binom{r+b}{s-1} \right) \left( 1 - \frac{s(r+b-s+1)}{rb} \right)^{2n}.$$

With some more effort, we can get the following result.

**Theorem VI.5.1.** *(See theorem 10 of chapter 3F of [8].) There exists a universal constant $a \in \mathbb{R}_{>0}$ such that, if $n = \frac{r+b}{4}(\log(2(r+b)) + c)$ with $c \geq 0$, then we have*

$$\|\mu_n - \mu\|_{TV} \leq a e^{-c/2}.$$

A different calculation (still using spherical functions) gives the following theorem :

**Theorem VI.5.2.** *(See theorem 6.3.2 of [7].) If $r = b$ is large enough, then, for $n = \frac{r+b}{4}(\log(2(r+b)) - c)$ with $0 < c < \log(2(r+b))$, we have*

$$\|\mu_n - \mu\|_{TV} \geq 1 - 32 e^{-c}.$$

# VI.6 Random walks on locally compact groups

In this section, we will see a few results (mostly without proofs) about random walks on more general groups. A good reference for many questions that we did not touch on here is Breuillard's survey [5].

We fix a locally compact group $G$ and a left Haar measure on $G$.

## VI.6.1 Setup

**Definition VI.6.1.1.** (See remark I.4.1.6.) A (complex) Radon measure on $G$ is a bounded linear functional on $\mathscr{C}_0(G)$ (with the norm $\|.\|_\infty$). We denote by $\mathscr{M}(G)$ the space of Radon measures and by $\|.\|$ its norm (which is the operator norm); this is a Banach space. If $\mu$ is a Radon measure, we write $f \longmapsto \int_G f(x)d\mu(x)$ for the corresponding linear functional on $\mathscr{C}_0(G)$.

**Example VI.6.1.2.** (1) Any regular Borel measure is a Radon measure on $G$ (such measure are called "positive" when we want to distinguish them from general Radon measures).

(2) If $\varphi \in L^1(G)$, then the linear functional $f \longmapsto \int_G f(x)\varphi(x)dx$ is a Radon measure on $G$, often denoted by $\varphi(x)dx$ or $\varphi dx$.

(3) For every $x \in G$, the linear functional $\mathscr{C}_0(G) \to \mathbb{C}$, $f \longmapsto f(x)$ is a Radon measure on $G$, called the Dirac measure at $x$.

We define the convolution product $\mu * \nu$ of two Radon measures $\mu$ and $\nu$ to be the linear functional

$$f \longmapsto \int_{G\times G} f(xy)d\mu(x)d\nu(y).$$

Then it is not very hard to check that $\|\mu * \nu\| \leq \|\mu\|\|\nu\|$ and that the convolution product is associative on $\mathscr{M}(G)$. This makes $\mathscr{M}(G)$ into a Banach algebra, and the Dirac measure at $1$ is a unit element of $\mathscr{M}(G)$.

If $\mu = \varphi dx$ and $\mu' = \varphi' dx$, then it is easy to check that $\mu * \mu' = (\varphi * \varphi')dx$, where $\varphi * \varphi'$ is the usual convolution in $L^1(G)$.

We denote by $\widehat{G}$ the set of unitary equivalence classes of irreducible unitary representations of $G$. We can extend the Fourier transform (both the ordinary and the spherical versions) to $\mathscr{M}(G)$ :

(1) If $\mu \in \mathscr{M}(G)$ and $(\pi, V) \in \widehat{G}$, define $\widehat{\mu}(\pi) \in \operatorname{End}(V)$ by

$$\widehat{\mu}(\pi)(v) = \int_G \pi(x^{-1})(v)d\mu(x).$$

(2) Suppose that $G$ is the first entry of a Gelfand pair $(G, K)$, and that $\varphi$ is a spherical function of positive type on $G$. Then, for every $\mu \in \mathscr{M}(G)$, we define $\widehat{\mu}(f) \in \mathbb{C}$ by :

$$\widehat{\mu}(f) = \int_G \varphi(x^{-1})d\mu(x).$$

For both versions of the Fourier transform, the equality

$$\widehat{\mu * \mu'} = \widehat{\mu}\widehat{\mu'}$$

for all $\mu, \mu' \in \mathscr{M}(G)$ (where the product on the right is composition of endomorphisms in the first case and multiplication in the second case).

The following theorem is a generalization of Lévy's convergence criterion. We say that a sequence $(\mu_n)_{n\geq 0}$ of Radon measures converges weakly if it converges in the weak* topology of $\mathscr{M}(G)$.

**Theorem VI.6.1.3.** *(See [12], section 5.2, theorem 5.2.)*

*(i) If $\mu, \mu' \in \mathscr{M}(G)$ are such that $\widehat{\mu}(\pi)\widehat{\mu'}(\pi)$ for every $\pi \in \widehat{G}$, then $\mu = \mu'$.*

*(ii) Let $(\mu_n)_{n\geq 0}$ be a sequence of (positive) probability measures on G and $\mu$ be another probability measure on G. If $(\mu_n)_{n\geq 0}$ converges weakly to $\mu$, then, for every $(\pi, V) \in \widehat{G}$ and every $v \in V$, we have $\lim_{n\to+\infty} \widehat{\mu}_n(\pi)(v) = \widehat{\mu}(\pi)(v)$. Conversely, if, for every $(\pi, V) \in \widehat{G}$ and all $v, w \in V$, we have $\lim_{n\to+\infty}\langle\widehat{\mu}_n(\pi)(v), w\rangle = \langle\widehat{\mu}(\pi)(v), w\rangle$, then $(\mu_n)_{n\geq 0}$ converges weakly to $\mu$.*

## VI.6.2 Random walks

We fix a regular Borel probability measure $\mu$ on $G$, and we want to understand the behavior of $\mu^{*n}$ as $n \to +\infty$.

The connection with random walks is that $\mu^{*n}$ is the distribution of the $n$th step of a Markov chain with state space $G$, initial distribution $\delta_1$ and "transition matrix" $\mu(yx^{-1})$. (We are choosing $\delta_1$ as initial distribution to simplify the notation, but this is not really necessary for most results.) In other words, we consider a sequence $(g_n)_{n\geq 1}$ of independent random variables with values in $G$ and distribution $\mu$. The Markov chain $(X_n)_{n\geq 0}$ is defined by $X_n = g_1 n \dots g_1$ (so $X_0$ is the constant function 1). We could also consider random walks on a space $G/K$, where $K$ is a subgroup of $G$ : take $(g_n)_{n\geq 1}$ as before, fix some initial random variable $X_0$ with values in $G/K$ (for example a constant function) and set $X_n = g_n \dots g_1 X_0$.

## VI.6.3 Compact groups

In this section, we suppose that $G$ is compact. We start with a general convergence result, due to Ito and Kawada ([14], see also theorem 2.3 of [5]).

Remember that the support of $\mu$ is by definition the set of $x \in G$ such that, for every neighborhood $U$ of $x$, we have $\mu(U) > 0$.

**Theorem VI.6.3.1.** *Suppose that the support of $\mu$ generates a dense subgroup of $G$ and is not contained in any (left or right) coset of a proper closed subgroup of $G$. Then the sequence $(\mu^{*n})_{n\geq 0}$ converges weakly to the normalized Haar measure on $G$.*

The proof is based on the convergence criterion of theorem VI.6.1.3(ii). We must show that, for every $(\pi, V) \in \widehat{G}$ nontrivial, the sequence $\widehat{\mu^{*n}}(\pi) = \widehat{\mu}(\pi)^n$ converges to $0$ in $\mathrm{End}(V)$. Note that $V$ is finite-dimensional (because $G$ is compact), so all the notions of convergence in $\mathrm{End}(V)$ are equivalent, and we just need to prove that all the eigenvalues of $\widehat{\mu}(\pi)$ are $< 1$ in absolute value. Suppose that this not the case, then there exists a unit vector $v \in V$ such that

$$\int_G \pi(x^{-1})(v)d\mu(x) = \lambda v,$$

with $|\lambda| = 1$. It is not hard to see that this forces $\pi(x^{-1})(v)$ to be equal to $\lambda v$ $\mu$-almost everywhere and contradicts the hypothesis of the theorem.

Note that this result is much weaker that proposition VI.4.4 (and the Perron-Frobenius theorem), because it only guarantees the weak convergence of $(\mu^{*n})_{n\geq 0}$ and says nothing about convergence for other topologies (such as the one induced by the total variation distance) or about the speed of convergence. If $G$ is finite, all the notions of convergence on the set of probability measures on $G$ coincide (it's just a convex subset of the space of functions on $G$, which is finite-dimensional); also, it follows from the upper bound lemma (corollary VI.4.6) that the speed is convergence is exponential and controlled by the biggest eigenvalue of a $\widehat{\mu}(\pi)$ that is $\neq 1$. But if $G$ is infinite, then $\widehat{G}$ is also infinite, so, also $\widehat{\mu}(\pi)$ has all its eigenvalues $< 1$ (in absolute value), we can get eigenvalues that are arbitrarily close to $1$. In fact, there is a special name for when this doesn't happen :

**Definition VI.6.3.2.** We say that the probability measure $\mu$ on $G$ has a *spectral gap* if there exists $\varepsilon > 0$ such that, for every $\pi \in \widehat{G}$ nontrivial and for every eigenvalue $\lambda$ of $\widehat{\mu}(\pi)$, we have $|\lambda| < 1 - \varepsilon$.

Let's first look at some examples.

**Example VI.6.3.3.** If $\mu = \varphi dx$ with $\varphi \in L^2(G)$, then $\mu$ has a spectral gap. In fact, the upper bound lemma (corollary VI.4.6) holds with essentially the same proof : for every $n \geq 0$, we have

$$\|\mu^{*n} - \mu_G\|_{TV}^2 \leq \frac{1}{4} \sum_{(\rho,V)\in\widehat{G}|\rho\not\simeq\mathbb{1}} \dim(V)\mathrm{Tr}((\widehat{\pi}(\rho)^*)^n \circ \widehat{\pi}(\rho)^n),$$

where we denote by $\mathbb{1}$ the trivial representation of $G$ and by $\mu_G$ the normalized Haar measure on $G$. (We could also prove a version for random walks on spaces $G/K$.) So we have convergence in total variation distance and with exponential speed in this case.

At the other extreme, we have measures with finite support.

**Example VI.6.3.4.** Take $G = S^1$. Let $\lambda_1, \dots, \lambda_r \in \mathbb{R}$, and consider the measure

$$\mu = \frac{1}{2r}\sum_{s=1}^{r}(\delta_{e^{2i\pi\lambda_s}} + \delta_{e^{-2i\pi\lambda_s}})$$

on $G$. Remember that $\widehat{G} = \mathbb{Z}$ (where $n \in \mathbb{Z}$ corresponds to the representation $z \longmapsto z^n$ of $G$). For every $n \in \mathbb{Z}$, we have

$$\widehat{\mu}(n) = \frac{1}{2r}\sum_{s=1}^{r}(e^{2i\pi n\lambda_s} + e^{-2i\pi n\lambda_s}).$$

Suppose that the family $(1, \lambda_1, \dots, \lambda_r)$ is $\mathbb{Q}$-linearly independent. Then Kronecker's theorem (see for example chapter XXIII of [13]) says that the set $\{(e^{2i\pi n\lambda_1}, \dots, e^{2i\pi n\lambda_r}),\ n \in \mathbb{Z}\}$ is dense in $(S^1)^r$. So we can find $n \neq 0$ such that $\widehat{\mu}(n)$ is arbitrarily close to $1$. In other words, the measure $\mu$ has no spectral gap.

The question of which measures on nice groups like $\mathrm{SU}(d)$ have a spectral gap is a very difficult and an active area of research. We'll give some (difficult) recent results, due to Bourgain and Gamburd (cf. [4] and [3]) for $G = \mathrm{SU}(d)$ and to Benoist and de Saxcé (cf. [2]) for a general simple compact Lie group.

**Theorem VI.6.3.5.** *Let $G$ be a simple compact Lie group (for example $G = \mathrm{SU}(d)$ for $d \geq 2$ or $G = \mathrm{SO}(d)$ for $d = 3$ or $d \geq 5$), and let $\mu$ be a probability measure on $G$. We say that $\mu$ is almost Diophantine if there exists $c_1, c_2 > 0$ such that for every proper closed subgroup $H$ of $G$ and for every $n \in \mathbb{Z}_{\geq 0}$ big enough, we have $\mu^{*n}(\{x \in G | d(x, H) \leq e^{-c_1 n}\}) \leq e^{-c_2 n}$ (where $d$ is any metric on $G$).*

*Then $\mu$ has a spectral gap if and only if it is amost Diophantine.*

Although the next version has a generalization to any simple compact Lie group, we'll just state it for $\mathrm{SU}(d)$ for simplicity.

**Theorem VI.6.3.6.** *Let $G = \mathrm{SU}(d)$, and let $\mu$ be a probability measure on $G$ such that the support of $\mu$ generates a dense subgroup of $G$ (such a measure is sometimes called "adapted").*

*If every element of the support of $\mu$ has algebraic entries, then $\mu$ has a spectral gap.*

In fact, Benoist and de Saxcé conjecture that the algebraicity condition is not necessary (so every adapted measure should have a spectral gap), see the introduction of [2].

*Remark* VI.6.3.7. The spectral gap question is also connected to the Banach-Ruziewicz problem (see chapter 2 of Sarnak's book [21] for the connection; another good reference on the Banach-Ruziewicz problem is Lubotzky's book [15]). This problem asks whether Lebesgue measure is the only (up to a constant) finitely additive $\mathrm{SO}(n+1)$-invariant measure on Lebesgue measurable subsets of the sphere $S^n \subset \mathbb{R}^n$. The answer is known to be "no" for $n = 1$ and "yes" for $n \geq 2$. For $n \geq 4$, it is due to Margulis and Sullivan and uses the fact that $\mathrm{SO}(n+1)$ has a finitely generated dense subgroup that satisfies Kazhdan's property (T) for $n \geq 4$ (in fact, the same methods will show that Haar measure is the only left-invariant mean on any simple compact Lie group that is not $\mathrm{SO}(n)$ with $n \geq 4$). For $n = 2, 3$, the solution is originally due to Drinfeld and uses the Jacquet-Langlands correspondence and the Ramanujan-Petersson conjecture. (All this and more is explained in [15].)

## VI.6.4 Convergence of random walks with Fourier analysis

We now present some example of random walks on compact groups (or homogeneous spaces) that can be analyzed using Fourier analysis, in the spirit of section VI.5.

As we noted before (in example VI.6.3.3), the upper bound lemma (corollary VI.4.6) still holds for general compact groups.

As for finite groups, Fourier analysis works best if the measure $\mu$ is conjugation or if $\mu$ is bi-$K$-invariant and $(G, K)$ is a Gelfand pair.

### Random reflections in $\mathrm{SO}(n)$

The reference for this result is Rosenthal's paper [17]. Fix $n \geq 2$ and $\theta \in (0, 2\pi)$. Let

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta & & & 0 \\ -\sin\theta & \cos\theta & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \in \mathrm{SO}(n),$$

and let $\mu_\theta$ be the unique conjugation-invariant probability measure concentrated on the conjugacy class of $R_\theta$ (in other words, the measure $\mu_\theta$ is the image of the normalized Haar measure of $\mathrm{SO}(n)$ by the map $\mathrm{SO}(n) \to \mathrm{SO}(n)$, $x \longmapsto x R_\theta x^{-1}$).

**Theorem VI.6.4.1.** *(i) There exist $\Gamma, \Delta > 0$ (with $\Delta$ independent of $\theta$) such that, for every $n \geq 1$ and every $c > 0$, if $k = \frac{1}{2(1-\cos\theta)}(n \log n - cn)$, then*

$$\|\mu_\theta^{*k} - dx\|_{TV} \geq 1 - \Gamma e^{-2c} - \Delta \frac{\log n}{n}.$$

*(ii) Suppose that $\theta = \pi$. Then there exist $\Lambda, \gamma > 0$ such that, for every $n \geq 3$ and every $c > 0$, if $k = \frac{1}{4} n \log n + cn$, then*

$$\|\mu_\theta^{*k} - dx\|_{TV} \leq \Lambda e^{-\gamma c}.$$

### The Gelfand pair case

The reference for this result is Su's paper [24].

Fix $\theta \in (0, \pi)$ and consider the following random process on $S^2 \simeq \mathrm{SO}(3)/\mathrm{SO}(2)$ :

- $X_0$ is constant with value the North pole;
- to go from $X_n$ to $X_{n+1}$, choose a direction (independently and uniformly) and move a distance of $\theta$ following the geodesic (= big circle) in that direction.

This random walk is not driven by a measure on $\mathrm{SO}(3)$, but it is equivalent to one that is (see section 3 of [24]). Let $\mu_n$ be the distribution of $X_n$ and $\lambda$ be the unique $\mathrm{SO}(3)$-invariant probability measure on $\S^2$. Then we have the following result :

**Theorem VI.6.4.2.** *If $n = \frac{c}{\sin^2\theta}$ with $c \geq 0$, then*

$$0.433 e^{-c/2} \leq \|\mu_l - \lambda\|_{DD} \leq 4.442 e^{-c/8}.$$

In this theorem, $\|.\|_{DD}$ is the *discrepancy distance* : If $X$ is a metric space and $\mu, \mu'$ are two (Borel) probability measures on $X$, then

$$\|\mu - \mu'\|_{DD} = \sup_{B \subset X \text{ ball}} |\mu(B) - \mu'(B)|.$$

It is bounded above by the total variation distance, but it can see some phenomena that the total variation distance misses (see the next subsection).

### Remark about the different types of convergence

The reference for this subsection is Su's paper [23].

Consider a random walk $(X_n)_{n\geq 0}$ on the circle $S^1$ driven by the masure $\mu = \frac{1}{2}(\delta_{e^{2i\pi\alpha}} + \delta_{e^{-2i\pi\alpha}})$, for some $\alpha \in \mathbb{R}$ irrational, and let $\mu_n$ be the distribution of $X_n$. Then :

- The general convergence result of Ito-Kawada (theorem VI.6.3.1) says that $(\mu_n)_{n\geq 0}$ converges weakly to the normalized Haar measure $dx$ on $S^1$.
- On the other hand, we have seen in example VI.6.3.4 that $\mu$ has no spectral gap, so the convergence cannot be too good. In fact, $(\mu_n)_{n\geq 0}$ does not converge to $dx$ in total variation distance.
- On the third hand, $(\mu_n)_{n\geq 0}$ does converge to $dx$ (but not exponentially fast) in discrepancy distance in many cases. More precisely, we have :

**Theorem VI.6.4.3.** *Let $\eta$ be the type of $\alpha$, i.e.*

$$\eta = \sup\{\gamma > 0 | \lim \inf_{m \to +\infty} m^\gamma \{m\alpha\} = 0\}$$

*(where $\{.\}$ is the fractional part). Then we have, for every $\varepsilon > 0$,*

$$\|\mu_n - dx\|_{DD} = O(n^{-1/2\eta+\varepsilon})$$

*and*

$$\|\mu_n - dx\|_{DD} = \Omega(n^{-1/2\eta-\varepsilon}).$$

*If $\alpha$ is irrational quadratic, we can do better : there exist constants $c_1, c_2 > 0$ such that, for every $n \geq 1$, we have*

$$\frac{c_1}{\sqrt{n}} \leq \|\mu_n - dx\|_{DD} \leq \frac{c_2}{\sqrt{n}}.$$

It is known that $\eta = 1$ if $\alpha$ is algebraic, and also that the subset of type $1$ elements of $[0, 1]$ has Lebesgue measure $1$.

## VI.6.5 Random walks on noncompact groups

We don't assume that $G$ is compact anymore. We fix a probability measure $\mu$ on $G$. One of the many questions we can ask is whether a random walk on $G$ driven by $\mu$ goes to infinity, and if so, how fast.

A reference for this section are the excellent course notes of Quint ([16]).

First, we define a continuous linear operator $P_\mu : L^2(G) \to L^2(G)$ by setting

$$P_\mu(f)(x) = \int_G f(yx) d\mu(y)$$

if $f \in \mathscr{C}_c(G)$ and $x \in G$; this extends to $L^2(G)$ by continuity. (If $\mu = \varphi dx$ with $\varphi \in L^1(G)$, this is just the construction of theorem I.4.2.6(i) applied to the right regular representation of $G$.)

We denote by $\rho(P_\mu)$ the spectral radius of $P_\mu$, seen as an element of the Banach algebra $\mathrm{End}(L^2(G))$. We always have $\rho(P_\mu) \leq 1$ (because $\mu$ is a probability measure).

**Theorem VI.6.5.1.** *(Kesten's criterion, theorem 5.2 of [16].)*

*(i) If $G$ is amenable, then $\rho(P_\mu) = 1$.*

*(ii) Let $H$ be the closure of the subgroup of $G$ generated by the support of $\mu$. If $\rho(P_\mu) = 1$, then $H$ is amenable.*

**Definition VI.6.5.2.** We say that $G$ is *compactly generated* if there exists a compact subset $K$ of $G$ that generates $G$.

If $G$ is discrete, this just means that $G$ is finitely generated.

**Definition VI.6.5.3.** Suppose that $G$ is compactly generated, and let $K$ be a symmetric compact subset generating $G$. We define $j_K : G \to \mathbb{Z}$ by

$$j_K(x) = \min\{n \in \mathbb{Z}_{\geq 0} | x \in K^n\}$$

(with the convention that $K^0 = \{1\}$).

**Lemma VI.6.5.4.** *If $K$ and $L$ are two symmetric compact subsets generating $G$, then there exists $a > 0$ such that $j_L \leq a j_K$.*

**Corollary VI.6.5.5.** *(Corollary 7.3 of [16].) Suppose that $G$ is compactly generated, and let $K$ be a symmetric compact subset generating $G$. Let $\mu$ be a probability measure on $G$, and let $(g_n)_{n \geq 1}$ be a sequence of idenpendent random variables valued on $G$ with distribution $\mu$.*

*Let $H$ be the closure of the subgroup of $G$ generated by the support of $\mu$. If $H$ is not amenable, then there exist $\alpha, \varepsilon > 0$ such that, for every $n \geq 1$, we have*

$$\mathbb{P}(j_K(g_n \dots g_1) \leq \varepsilon n) = o(e^{-\alpha n}).$$

In particular, by the Borel-Cantelli lemma (see section 17.1 of [18]), if $n$ is large enough, we have $j_K(g_n \dots g_1) \geq \varepsilon n$ almost surely.

We finish with an example. We say that a subgroup $H$ of $\mathrm{SL}_2(\mathbb{R})$ is *non-elementary* if no conjugate of $H$ is contained in $\mathrm{SO}(2)$, in

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix},\ a \in \mathbb{R}^\times,\ b \in \mathbb{R} \right\}$$

or in

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},\ a \in \mathbb{R}^\times \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix},\ a \in \mathbb{R}^\times \right\}.$$

(An equivalent condition is that $H$ is not compact and does not fix a line in $\mathbb{R}^2$ or the union of two lines in $\mathbb{R}^2$. Here the action of $\mathrm{SL}_2(\mathbb{R})$ in $\mathbb{R}^2$ is the standard one, given by the inclusion $\mathrm{SL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R})$.)

**Proposition VI.6.5.6.** *(Proposition 8.6 of [16].) A closed subgroup of $\mathrm{SL}_2(\mathbb{R})$ is non-amenable if and only if it is non-elementary.*

**Example VI.6.5.7.** If $t \in \mathbb{R}^\times$, we set

$$a_t = \begin{pmatrix} t & 0 \\ t^{-1} & 0 \end{pmatrix}.$$

If $\theta \in \mathbb{R}$, we set

$$r_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Then, if $s, t > 1$ and $0 < \theta < \pi/2$, the subgroup of $\mathrm{SL}_2(\mathbb{R})$ spanned by $a_s$ and $r_\theta a_t r_\theta^{-1}$ is non-elementary, and so corollary VI.6.5.5 applies to a random walk driven by the measure $\mu = \frac{1}{2}(\delta_{a_t} + \delta_{r_\theta a_t r_\theta^{-1}})$.

## VI.7 Problem : Random walks on non-amenable groups

Let $G$ be a locally compact group. We fix a left invariant Haar measure $\mu_G$ on $G$. In this problem, all the measures on $G$ are assumed to be regular Borel measures, and you may assume that $G$ is $\sigma$-compact.[1]

(1) Let $H$ be a closed subgroup of $G$, and let $\mu_H$ be a left-invariant Haar measure on $H$. The goal of this question is to show that, if there exists a mean on $L^\infty(G)$ that is left invariant by $H$, then $H$ is amenable. [2]

(a). We want to show that, for every open neighborhood $U$ of $1$ in $G$, there exists a subset $T$ of $G/H$ such that :

- $G/H = \bigcup_{t\in T} Ut$;
- for every compact subset $K$ of $G/H$, the set $K \cap T$ is finite.

To simplify the proof (and because this is the only case we'll need later), we assume that $G$ is the union of a countable family of compact subsets. Choose an open neighborhood $V$ of $1$ in $G$ such that $V^{-1}V \subset U$.

(i) Show that, if $K$ is a compact subset of $G/H$, there is no infinite sequence $(t_n)_{n\geq 0}$ of elements of $K$ such that $Vt_n \cap Vt_m = \varnothing$ for $n \neq m$.

(ii) Write $G/H = \bigcup_{n\geq 0} K_n$ with the $K_n$ compact subsets of $G/H$ such that $K_n \subset K_{n+1}$ for every $n \geq 0$. Define a family $(T_n)_{n\geq 0}$ of finite subsets of $G/H$ inductively like so :

- $T_0 = \varnothing$;
- for $n \geq 1$, take for $T_n$ a maximal finite subset of $L_n := K_n - (UT_0 \cup \ldots \cup UT_{n-1})$ such that $Vt \cap Vt' = \varnothing$ for all $t, t' \in T_n$ such that $t \neq t'$.

Show that the definition makes sense and that we have $K_n \subset \bigcup_{i=0}^{n} UT_i$ for every $n \geq 1$.

(iii) Show that $T := \bigcup_{n\geq 0} T_n$ satisfies the two required properties.

(b). Show that there exists a bounded continuous function $\theta : G \to \mathbb{R}_{\geq 0}$ such that :

- for any compact subset $K$ of $G$, the function $\theta_{|KH}$ has compact support;
- for every $x \in G$, we have $\int_H \theta(xy)d\mu_H(y) = 1$.

(Hint : Take $T$ as in question (a) with $U$ relatively compact, take $\varphi \in \mathscr{C}_c^+(G)$ such that $\varphi_{|U} = 1$, define $\psi$ by $\psi(x) = \sum_{t\in T} \varphi(xg_t^{-1})$ where $g_t \in G$ is a lift of $t$, and

[1] We are mostly interested in compactly generated groups, and those are clearly $\sigma$-compact.
[2] The converse is also true and much easier to prove, but we won't need it.

modify $\psi$ a bit.)

(c). For every $\varphi \in L^\infty(H)$, define $\varphi_\theta : G \to \mathbb{C}$ by

$$\varphi_\theta(x) = \int_H \varphi(y)\theta(x^{-1}y)d\mu_H(y).$$

Show that $\varphi_\theta \in L^\infty(G)$.

(d). If $M$ is a mean on $L^\infty(G)$ that is left-invariant by $H$, show that $\varphi \longmapsto M(\varphi_\theta)$ is a left-invariant mean on $L^\infty(H)$.

(2) Let $T : V \to W$ be a bounded linear operator between two normed $\mathbb{C}$-vector spaces.

(a). If $V$ and $W$ are Hilbert spaces and if $\mathrm{Im}(T)$ is not dense in $W$, show that $T^*$ is not injective.

(b). If $V$ is complete and $\mathrm{Im}(T)$ is not closed in $W$, show that there exists a sequence $(v_n)_{n\geq 0}$ of norm $1$ vectors in $V$ such that $\lim_{n\to+\infty} T(v_n) = 0$.

(3) Let $\mu$ be a probability measure on $G$. For every $f \in \mathscr{C}_c(G)$, we define a function $P_\mu f : G \to \mathbb{C}$ by

$$(P_\mu f)(x) = \int_G f(yx)d\mu(y).$$

(a). For every $f \in \mathscr{C}_c(G)$, show that $P_\mu f$ is continuous and that $\|P_\mu f\|_2 \leq \|f\|_2$.

(b). Show that $P_\mu$ extends to a continuous linear operator $P_\mu : L^2(G) \to L^2(G)$ and that we have $\|P_\mu\|_{op} \leq 1$.

(c). Show that $(P_\mu)^* = P_\nu$, where $\nu$ is the probability measure defined by $\nu(E) = \mu(E^{-1})$.

(4) Suppose that $G$ is amenable, and let $\mu$ be a probability measure on $G$. We want to show that $\rho(P_\mu) = 1$. (Where $\rho(P_\mu)$ is the spectral radius of $P_\mu$, seen as an element of $\mathrm{End}(L^2(G))$.)

(a) For every $\varepsilon > 0$, show that there exists a compact subset $K$ of $G$ and a function $f \in L^2(G)$ such that :

* $\mu(K) \geq 1 - \varepsilon$;
* $\|f\|_2 = 1$;
* $\sup_{x\in K} \|L_x f - f\|_2 \leq \varepsilon$.

(b) For every $\varepsilon > 0$, show that there exists a function $f \in L^2(G)$ such that $\|f\|_2 = 1$ and $\|P_\mu f - f\|_2 \leq \varepsilon$.

(c) Show that $\rho(P_\mu) = 1$.

(5) Let $\mu$ be a probability measure on $G$. Suppose that $\rho(P_\mu) = 1$, and let $H$ be the closure of the subgroup generated by the support of $\mu$. (Where the support of $\mu$ is the set of $x \in G$

such that every open neighborhood of $x$ has positive volume for $\mu$.) We want to show that $H$ is amenable.

(a). Show that at least one of the following conditions holds :

($\alpha$) There exists $\lambda \in \mathbb{C}$ such that $|\lambda| = 1$ and $P_\mu - \lambda \mathrm{id}_{L^2(G)}$ is not injective.

($\beta$) There exists $\lambda \in \mathbb{C}$ such that $|\lambda| = 1$ and $\mathrm{Im}(P_\mu - \lambda \mathrm{id}_{L^2(G)})$ is not dense in $L^2(G)$.

($\gamma$) There exists $\lambda \in \mathbb{C}$ such that $|\lambda| = 1$ and $\mathrm{Im}(P_\mu - \lambda \mathrm{id}_{L^2(G)})$ is not closed in $L^2(G)$.

(b). Suppose that condition ($\alpha$) holds.

(i) Show that $P_\mu - \mathrm{id}_{L^2(G)}$ is not injective.

(ii) Show that there exists a nonzero element of $L^2(G)$ that is left $H$-invariant.

(iii) Show that $H$ is compact.

(c). If condition ($\beta$) holds, show that $H$ is compact.

(d). Suppose that condition ($\gamma$) holds.

(i) Show that there exists a sequence $(f_n)_{n\geq 0}$ of norm $1$ elements of $L^2(G)$ such that $\lim_{n\to+\infty} \|P_\mu f_n - \lambda f_n\|_2 = 0$.

(ii) Define $g_n : G \to \mathbb{R}_{\geq 0}$ by

$$g_n(x) = \|L_x f_n - \overline{\lambda} f_n\|_2^2.$$

Show that the sequence $(g_n)_{n\geq 0}$ converges to $0$ in $L^1(G, \mu)$ (note the measure !).

(iii) Show that we may assume that $\lim_{n\to+\infty} g_n(x) = 0$ $\mu$-almost everywhere on $G$.

(iv) Define $h_n : G \to \mathbb{R}_{\geq 0}$ by $h_n(x) = |f_n(x)|^2$. Show that $\int_G h_n(x) d\mu_G(x) = 1$ for every $n$ and that $\lim_{n\to+\infty} \|L_x h_n - h_n\|_1$ $\mu$-almost everywhere on $G$. (Note that we are back in $L^1(G)$.)

(v) Show that there exists a mean $M$ on $L^\infty(G)$ that is left invariant by $H$.

(6) If $K$ is a compact symmetric (i.e. $K^{-1} = K$) subset of $G$ that generates $G$, we define $j_K : G \to \mathbb{Z}_{\geq 0}$ by

$$j_K(x) = \min\{n \in \mathbb{Z}_{\geq 0} | x \in K^n\}$$

(with the convention that $K^0 = \{1\}$).

Show that, if $L$ is another compact symmetric subset that generates $G$, then there exists $a > 0$ such that $j_L \leq a j_K$.

- Let $K$ be a compact symmetric subset of $G$ with nonempty interior. The goal of this question is to show that the sequence $(\mu_G(K^n)^{1/n})_{n\geq 1}$ converges.

(a). If $A$, $B$ and $C$ are compact subsets of $G$, show that

$$\mu_G(AB)\mu_G(C) \leq \mu_G(AC)\mu_G(C^{-1}B).$$

(Hint : Look at $\mathbb{1}_{AC} * \mathbb{1}_{C^{-1}B}$.)

(b). Show that, for all $n, m \in \mathbb{Z}_{\geq 1}$, we have

$$\mu_G(K^{n+m}) \leq \mu_G(K)^{-1}\mu_G(K^{n+1})\mu_G(K^{m+1}).$$

(c). Conclude.

(7) Let $\mu$ be a probability measure on $G$. Suppose that the closure $H$ of the subgroup generated by the support of $\mu$ is not amenable, and that $G$ is compactly generated. Fix a symmetric compact subset $K$ of $G$ generating $G$. We want to show that there exist $\varepsilon, \alpha > 0$ such that, if $(g_n)_{n\geq 1}$ is a sequence of independent random variables valued in $G$ with distribution $\mu$, then, for every $n \geq 0$, we have

$$\mathbb{P}(j_K(g_n \dots g_1) \leq \varepsilon n) = o(e^{-\alpha n}).$$

In other words, we want to show that

$$\mu^{*n}(K^{\lfloor \varepsilon n \rfloor}) = o(e^{-\alpha n}),$$

where $\mu^{*n}$ is the image of the measure $\mu^n$ on $G^n$ by the multiplication map $(x_1, \dots, x_n) \longmapsto x_1 \dots x_n$. (The equivalence of these two statements is basically the definition of "independent", and you don't need to prove it.)

(a). Show that we may assume that $K$ has nonempty interior.

(b). Show that, for every compact subset $L$ of $G$ and every $n \geq 1$, we have

$$\mu^{*n}(L)\mu_G(K) \leq \langle P_\mu^n \mathbb{1}_{LK}, \mathbb{1}_K \rangle_{L^2(G)}.$$

(c). Let $\varepsilon > 0$. Show that there exists $\alpha > 0$ such that, for every $n \geq 1$, we have

$$\langle P_\mu^n \mathbb{1}_{K^{\lfloor \varepsilon n \rfloor + 1}}, \mathbb{1}_K \rangle_{L^2(G)} = o(e^{-\alpha n} \|\mathbb{1}_{K^{\lfloor \varepsilon n \rfloor + 1}}\|_{L^2(G)} \|\mathbb{1}_K\|_{L^2(G)}).$$

(d). Show that, if we choose $\varepsilon$ small enough in (c), then we have

$$\langle P_\mu^n \mathbb{1}_{K^{\lfloor \varepsilon n \rfloor + 1}}, \mathbb{1}_K \rangle_{L^2(G)} = o(e^{-\alpha n/2}).$$

(e). Conclude.

# A Urysohn's lemma and some consequences

## A.1 Urysohn's lemma

**Definition A.1.1.** A topological space $X$ is called *normal* if whenever we have two disjoint closed subsets $A$ and $B$ of $X$, there exist open subsets $U$ and $V$ of $X$ such that $A \subset U$ and $B \subset V$.

**Proposition A.1.2.** *Any topological space that is compact Hausdorff or metrizable is normal.*

**Theorem A.1.3** (Urysohn's lemma)**.** *Let $X$ be a normal topological space, and let $A$, $B$ be two disjoint closed subsets of $X$. Then there exists a continuous functions $f : X \to [0,1]$ such that $f(x) = 0$ for every $x \in A$ and $f(x) = 1$ for every $x \in B$.*

## A.2 The Tietze extension theorem

**Corollary A.2.1** (Tietze extension theorem)**.** *Let $X$ be a normal topological space, $A$ be a closed subset of $X$ and $f : A \to \mathbb{C}$ be a continuous function. Then there exists a continuous function $F : X \to \mathbb{R}$ such that $F_{|A} = f$ and that $\sup_{x\in X} |F(x)| = \sup_{x\in A} |f(x)|$.*

## A.3 Applications

**Corollary A.3.1.** *Let $X$ be a locally compact Hausdorff topological space, and let $K \subset U$ be two subsets of $X$ such that $K$ is compact and $U$ is open. Then there exists a continuous function with compact support $f : X \to [0,1]$ such that $f_{|K} = 1$ and $\operatorname{supp} f \subset U$.*

*Proof.* As $X$ is locally, for every $x \in K$, we can find an open neighborhood $V_x$ of $x$ such that $\overline{V}_x$ is compact and contained in $U$. We have $K \subset \bigcup_{x\in K} V_x$; as $K$ is compact, we can find $x_1, \dots, x_n \in K$ such that $K \subset \bigcup_{i=1}^n V_{x_i}$. Set $K' = \bigcup_{i=1}^n \overline{V}_{x_i}$. Then $K'$ is a compact subset of $X$, it is contained in $U$ and its interior contains $K$. Applying the same procedure to $K' subsetU$, we can find a compact subset $K'' \subset U$ of $X$ whose interiot contains $K'$.

The space $K''$ is compact, hence normal, and its subsets $K$ and $K''-\mathring{K}'$ are closed and disjoint, so, by Urysohn's lemma, we have a continuous function $f : K'' \to [0,1]$ such that $f_{|K} = 1$ and $f_{|K''-\mathring{K}'} = 0$. We extend $f$ to $X$ by setting $f(x) = 0$ if $x \in X - K''$. Then $f$ is equal to $0$ (hence comtinuous) on $X - K'$, and it is also continuous on $\mathring{K}''$. As $X - K'$ and $\mathring{K}''$ are open subset whose union is $X$, the function $f$ is continuous on $X$. It is clear from the construction of $f$ that it satisfies all the desired properties.

□

**Corollary A.3.2.** *Let $X$ be a locally compact Hausdorff topological space, and let $K \subset U$ be two subsets of $X$ such that $K$ is compact and $U$ is open. Then, for every continuous function $f : K \to \mathbb{C}$, there exists a continuous function with compact $F : X \to \mathbb{C}$ such that :*

*(a)* $\mathrm{supp}(F) \subset U$;

*(b)* $F_{|K} = f$;

*(c)* $\sup_{x\in X} |F(x)| = \mathrm{supp}_{x\in K} |f(x)|$.

*Proof.* By corollary A.3.1, we can find a continuous function with compact support $\psi : X \to [0,1]$ such that $\psi_{|K} = 1$ and $\mathrm{supp}(\psi) \subset U$. On the other hand, we can find, as in the proof of corollary A.3.1, a compact set $K' \subset U$ whose interior contains $\mathrm{supp}\,\psi$. Applying the Tietze extension to the normal space $K'$, we get a continuous function $f' : K' \to \mathbb{C}$ such that $f'_{|K} = f$ and $\mathrm{supp}_{x\in K'} |f'(x)| = \mathrm{supp}_{x\in K} |f(x)|$. We define a function $F : X \to \mathbb{C}$ by $F(x) = f'(x)\psi(x)$ if $x \in K'$, and $F(x) = 0$ if $x \in X - K'$. This functuion $F$ clearly satisfies conditions (a)-(c), so we just need to check that it is continuous. But this follows from the fact that $F$ is continuous on the open sets $X - \mathrm{supp}(\psi)$ (because it is zero on that set) and $\mathring{K}'$, and that the union of these open sets is $X$.

□

# B Useful things about normed vector spaces

## B.1 The quotient norm

See [19] 18.15 or [20] 1.40, 1.41.

**Definition B.1.1.** Let $V$ be a normed vector space and $W \subset V$ be a subspace. Then the *quotient seminorm* on $V/W$ is defined by

$$\|x + W\| = \inf_{w \in W} \|v + w\|.$$

If $W$ is closed, this is called the *quotient norm*.

**Proposition B.1.2.** *(i) The formula of the preceding definition gives a seminorm on $V/W$, which is a norm if and only if $W$ is closed in $V$.*

*(ii) If $V$ is a Banach space and $W$ is closed in $V$, then $V/W$ is a Banach space for the quotient norm.*

*Proof.* (i) Let $v, v' \in V$ and $\lambda \in \mathbb{C}$. Then we have

$$\|v+v'+W\| = \inf_{x \in W} \|v+v'+w\| \leq \inf_{w \in W} \|v+w\| + \inf_{w \in W} \|v'+w\| = \|v+W\| + \|v'+W\|.$$

If $\lambda = 0$, then $\lambda v \in W$, so $\|\lambda v + W\| = 0$; otherwise,

$$\|\lambda v + W\| = \inf_{w \in W} \|\lambda v + w\| = \inf_{w \in W} \|\lambda(v + w)\| = |\lambda| \inf_{w \in W} \|v + w\| = |\lambda| \|v + W\|.$$

This shows that the quotient seminorm is indeed a seminorm on $V/W$. Now let's prove that $\|v + W\| = 0$ if and only $v \in \overline{W}$, which will imply the last statement. By definition of $\|v + W\|$ (and the fact that $W$ is a subspace), we have $\|v + W\| = 0$ and and only if, for every $\varepsilon > 0$, there exists $w \in W$ such that $\|v - w\| < \varepsilon$. This is equivalent to $v \in \overline{W}$.

(ii) Let $(v_n)_{n \geq 0}$ be a sequence in $V$ such that $(v_n + W)_{n \geq 0}$ is a Cauchy sequence in $V/W$. Up to replacing $(v_n)_{n \geq 0}$ by a subsequence, we may assume that $\|v_{n+1} - v_n + W\| < 2^{-n}$ for every $n \geq 0$. We define another sequence $(v'_n)_{n \geq 0}$ such that $v'_n \in v_n + W$ for $n \geq 0$ and $\|v'_n - v'_{n-1}\| < 2^{-n+1}$ for $n \geq 1$, in the following way :

- Take $v'_0 = v_0$.
- Suppose that we have $v'_0, \dots, v'_n$ satisfying the two required conditions, with $n \geq 0$. Then we have $\|v_{n+1} - v'_n + W\| = \|v_{n+1} - v_n + W\| < 2^{-n}$, so, by definition of the quotient norm, we can find $w \in W$ such that $\|v_{n+1} - v'_n + w\| < 2^{-n}$. Take $v'_{n+1} = v_{n+1} + w$.

By the second condition, $(v'_n)_{n \geq 0}$ is a Cauchy sequence, so it has a limit $v$ in $V$. By the first condition, $v'_n + W = v_n + W$ for every $n \geq 0$, so $v + W$ is the limit of the sequence $(v_n + W)_{n \geq 0}$ in $V/W$.

□

## B.2 The open mapping theorem

This is also known as the Banach-Schauder theorem. See for example theorem 5.10 of [19].

**Theorem B.2.1.** *Let $V$ and $W$ be Banach spaces, and let $T : V \to W$ be a bounded linear transformation that is bijective. Then $T^{-1} : W \to V$ is also bounded.*

## B.3 The Hahn-Banach theorem

See [19] Theorem 5.16 or [20] Theorems 3.2-3.7.

**Theorem B.3.1** (Hahn-Banach theorem, analytic version, real case)**.** *Let $V$ be a vector space over $\mathbb{R}$, let $p : V \to \mathbb{R}$ such that :*

*(a) $p(v + v') \leq p(v) + p(v')$ for all $v, v' \in V$ (i.e. $p$ is subadditive);*

*(b) $p(\lambda v) = \lambda p(v)$ for every $v \in V$ and ever $\lambda \in \mathbb{R}_{>0}$.*

*Let $E \subset V$ be a $K$-subspace and let $f : E \to K$ be a linear functional such that, for every $x \in E$, we have $f(x) \leq p(x)$.*

*Then there exists a linear function $F : V \to K$ such that $F_{|W} = f$ and $F(x) \leq p(x)$ for every $x \in V$.*

Note that, in this version, there is no norm or topology or $V$ and no continuity condition on the linear functionals.

*Proof.* Consider the set $X$ of pairs $(W, g)$, where $W \supset E$ is a subspace of $V$ and $g : W \to \mathbb{R}$ is a linear functional such that $g_{|E} = f$ and $g(x) \leq p(x)$ for every $x \in W$. We order this set by saying that $(W, g) \leq (W', g')$ if $W \subset W'$ and $g = g'_{|W}$. Suppose that $(W_i, g_i)_{i \in I}$ is a nonempty totally ordered family in $X$, and let's show that it has an upper bound. We set $W = \bigcup_{i \in I} W_i$; this is a subspace of $V$ because $(W_i)_{i \in I}$ is totally ordered (so, for all $i, j \in I$, we have $W_i \subset W_j$ or $W_j \subset W_i$). We define $g : W \to \mathbb{R}$ in the following way : If $v \in W$, then there exists $i \in I$ such that $v \in W_i$, and we set $g(v) = g_i(v)$. We obviously have $g(v) \leq p(v)$. Also, if $j \in I$ is another element such that $v \in W_j$, then we have $(W_i, f_i) \leq (W_j, f_j)$ or $(W_j, f_j) \leq (W_i, f_i)$, and in both cases this forces $g_i(v) = g_j(v)$, so the definition makes sense. It is also easy to see that $g$ is $\mathbb{R}$-linear, so that $(W, g) \in X$. This is an upper bound for the family.

So we can apply Zorn's lemma to the set $X$. Let $(W, g)$ be a maximal element of $X$, and let's show that $W = V$. Suppose that $W \neq V$, and choose $v \in V - W$. We want to extend $g$ to a linear functional $h$ on on $W \oplus \mathbb{R}v$ such that $h \leq p$, which will contradict the maximality of $(W, g)$. This just means that we have to choose the value of $h(v)$, say $h(v) = \alpha \in \mathbb{R}$. The condition $h \leq p$ means that we want, for every $w \in W$ and every $t \in \mathbb{R}$ :

$$h(w + tv) = g(w) + t\alpha \leq p(w + tv).$$

If the inequality above is true for a $t \in \mathbb{R}$ and all $w \in W$, it is also true for all $ct$, $c \in \mathbb{R}_{>0}$, and for all $w \in W$ (because $W$ is a subspace and the values of both $g$ and $p$ are multiplied by $c$ when their argument is multiplied by $c$). So it suffices to check it for $t = \pm 1$, which means that we want, for every $w \in W$ :

$$g(w) + \alpha \leq p(w + v) \text{ and } g(w) - \alpha \leq p(w - v).$$

In other words, we want to have :

$$\sup_{w \in W} (g(w) - p(w - v)) \leq \alpha \leq \inf_{w \in W} (p(w + v) - g(w)).$$

We can find such a $\alpha$ because we have, for all $w, w' \in W$,

$$g(w) + g(w') = g(w + w') \leq p(w + w') \leq p(w + v) + p(w' - v),$$

i.e.

$$g(w') - p(w' - v) \leq p(w + v) - g(w).$$

So we get our contradiction, we can conclude that $W$ was equal to $V$ after all, and we are done.

□

**Theorem B.3.2** (Hahn-Banach theorem, analytic version, complex case)**.** *Let $V$ be a vector space over $\mathbb{C}$, let $p : V \to \mathbb{R}_{\geq 0}$ be a semi-norm,* [1] *let $E \subset V$ be a $\mathbb{C}$-subspace and let $f : E \to \mathbb{C}$ be a linear functional such that, for every $x \in E$, we have $|f(x)| \leq p(x)$.*

*Then there exists a linear function $F : V \to \mathbb{C}$ such that $F_{|W} = f$ and $|F(x)| \leq p(x)$ for every $x \in V$.*

[1] This means that, for all $x, y \in V$ and all $\lambda \in \mathbb{C}$, we have $p(x + y) \leq p(x) + p(y)$ and $p(\lambda x) = |\lambda| p(x)$.

*Proof.* We see $V$ and $E$ as $\mathbb{R}$-vector spaces, and define a $\mathbb{R}$-linear functional $h : E \to \mathbb{R}$ by

$$h(v) = \tfrac{1}{2}(f(v) + \overline{f(v)}).$$

Then we have, for every $v \in E$,

$$h(v) \leq \tfrac{1}{2}(|f(v)| + |\overline{f(v)}|) \leq p(v).$$

Note that satisfies conditions (a) and (b) of theorem B.3.1. By that theorem, we can find a $\mathbb{R}$-linear functional $H : V \to \mathbb{R}$ such that $H_{|E} = h$ and that $H(v) \leq p(v)$ for every $v \in V$. Define $F : V \to \mathbb{C}$ by

$$F(v) = H(v) + \frac{1}{i}H(iv),$$

and let's show that it has all the desired properties.

(i) $F$ is $\mathbb{R}$-linear by construction, and, for everey $v \in V$, we have

$$F(iv) = H(iv) + \frac{1}{i}H(i(iv)) = iF(v).$$

So $F$ is $\mathbb{C}$-linear.

(ii) If $v \in E$, then

$$F(v) = h(v) + \frac{1}{i}h(iv) = \frac{1}{2}(f(v) + \overline{f(v)} - if(iv) - i\overline{f(iv)}) = f(v)$$

(because $f$ is $\mathbb{C}$-linear), so $F_{|E} = E$.

(iii) Let $v \in V$ and choose $\theta \in \mathbb{R}$ such that $e^{i\theta}F(v) \in \mathbb{R}_{\geq 0}$. Then we have

$$|F(v)| = e^{i\theta}F(v) = F(e^{i\theta}v) = H(e^{i\theta}v) - iH(ie^{i\theta}v) \in \mathbb{R}.$$

As $H(e^{i\theta}v) \in \mathbb{R}$ and $iH(e^{i\theta}v) \in i\mathbb{R}$, we must have $iH(ie^{i\theta}v) = 0$. So

$$|F(v)| = H(e^{i\theta}v) \leq p(e^{i\theta}v) = p(v).$$

□

**Corollary B.3.3.** *Let $V$ be a normed vector space (over $\mathbb{R}$ or $\mathbb{C}$), let $W$ be a subspace of $V$, and let $T_W$ be a bounded linear functional on $W$. Then there exists a bounded linear functional $T$ on $V$ such that $T_{|W} = T_W$ and $\|T\|_{op} = \|T_W|_{op}$.*

*Proof.* Let $C = \|T_W\|_{op}$. Apply the Hahn-Banach with $p(v) = C\|V\|$. We get a linear functional $T : V \to \mathbb{C}$ extending $T_W$ and such that $|T(v)| \leq C\|v\|$ for every $v \in V$, which means that $T$ is bounded and $\|T\|_{op} \leq \|T_W\|_{op}$. As the inequality $\|T_W\|_{op} \leq \|T\|$ is obvious, we are done.

□

**Corollary B.3.4.** *(See Theorem 5.20 and Remark 5.21 of [19].) Let $V$ be a normed vector space over $K = \mathbb{R}$ or $\mathbb{C}$. We write $V^* = \mathrm{Hom}(V, K)$. Then the map $V \to V^{**}$ sending $v \in V$ to the linear functional $\widehat{v} : V^* \to \mathbb{C}$, $T \longmapsto T(v)$ is an isometry.*

In particular, this map is injective, which means that bounded linear functionals on $V$ separate points.

We can now deduce the geometric versions of the Hahn-Banach theorem. (In finite dimension, these are sometimes called "the hyperplane separation theorem").

**Definition B.3.5.** Let $V$ be a vector space over the field $K$, with $K = \mathbb{R}$ or $\mathbb{C}$. We say that $V$ is a *topological vector space* over $K$ if it has a topology such that :

- $(V, +)$ is a topological group;
- the map $K \times V \to V$, $(a, v) \longmapsto av$ is continuous.

We say that a topological vector space is *locally convex* if every point has a basis of convex neighborhoods.

**Example B.3.6.** (a) Any normed vector is a locally convex topological vector, as is its dual for the weak* topology.

(b) Let $(X, \mu)$ be a measure space, let $p \in (0, 1)$, and consider the space $L^p(X, \mu)$, with the metric given by

$$d(f, g) = \int_X |f(x) - g(x)|^p d\mu(x).$$

This makes $L^p(X, \mu)$ into a topological vector space, which is not locally convex if $\mu$ is atomless and finite (for example if $\mu$ is Lebesgue measure on a bounded subset of $\mathbb{R}^n$, or the Haar measure on a compact group).

**Theorem B.3.7** (Hahn-Banach theorem, first geometric version)**.** *Let $V$ be a topological $\mathbb{R}$-vector space, and let $A$ and $B$ be two nonempty convex subsets of $V$. Suppose that $A$ is open and that $A \cap B = \varnothing$.*

*Then there exists a continuous linear functional $f : V \to \mathbb{R}$ and $c \in \mathbb{R}$ such that, for every $x \in A$ and every $y \in B$, we have*

$$f(x) \leq c \leq f(y).$$

We are going to use as our function $p$ what is called the *gauge* of an open convex set $C \ni 0$.

**Lemma B.3.8.** *Let $C$ be a nonempty open convex subset of $V$, and suppose that $0 \in C$. We define the gauge $p : V \to \mathbb{R}_{\geq 0}$ of $C$ by*

$$p(v) = \inf\{\alpha > 0 | v \in \alpha C\}.$$

*Then $p$ satisfies conditions (a) and (b) of theorem B.3.1, and moreover :*

*(c) If $V$ is a normed vector space, then there exists $M \in \mathbb{R}_{\geq 0}$ such that, for every $v \in V$,*

$$0 \leq p(v) \leq M\|v\|.$$

*(d)* $C = \{v \in V | p(v) < 1\}$.

*Proof.* The fact that $p(\lambda v) = \lambda p(v)$ for every $\lambda \in \mathbb{R}_{>0}$ and every $v \in V$ follows immediately from the definition (and doesn't use the convexity or openness of $C$).

Let's prove (c). As $C$ is open and $0 \in C$, there exists $r > 0$ such that $C \supset \{v \in V | \|v\| < r\}$. Then, for every $v \in V - \{0\}$, we have $\frac{r}{\|v\|}v \in C$, so $p(v) \leq \frac{1}{r}\|v\|$.

Let's prove (d). Let $v \in C$. As $C$ is open, there exists $\varepsilon > 0$ such that $(1+\varepsilon)v \in C$. So $p(v) \leq \frac{1}{1+\varepsilon} < 1$. Conversely, let $v \in V$ such that $p(v) < 1$. Then there exists $\alpha \in (0,1)$ such that $x \in \alpha C$, i.e. $\frac{1}{\alpha}v \in C$, and then we have $v = \alpha(\frac{1}{\alpha}v) + (1-\alpha)0 \in C$, because $C$ is convex.

Finally, we prove that $p$ is subadditive, i.e. condition (b). Let $v, w \in V$. Let $\varepsilon > 0$. By (b) (and the first property we proved), we have $\frac{1}{p(v)+\varepsilon}v \in C$ and $\frac{1}{p(w)+\varepsilon}w \in C$. As $C$ is convex, this implies that, for every $t \in [0,1]$, we have

$$\tfrac{t}{p(v)+\varepsilon}v + \tfrac{1-t}{p(w)+\varepsilon}w \in C.$$

Taking $t = \frac{p(v)+\varepsilon}{p(v)+p(w)+2\varepsilon}$, we get that

$$\frac{1}{p(v)+p(w)+2\varepsilon}(v+w) \in C,$$

i.e. that $p(v+w) \leq p(v) + p(w) + 2\varepsilon$. As $\varepsilon > 0$ was arbitrary, this implies that $p(v+w) \leq p(v) + p(w)$.

□

**Lemma B.3.9.** *Let $C \subset V$ be a nonempty open convex subset, and let $v_0 \in V - C$.*

*Then there exists a continuous linear functional $F$ on $V$ such that, for every $v \in C$, we have $F(v) < F(v_0)$.*

*Proof.* We may assume $0 \in C$ (by translating the situation). Let $p : V \to \mathbb{R}_{\geq 0}$ be the gauge of $C$, i.e. the function defined in the preceding lemma.

Let $E = \mathbb{R}v_0$, and let $f : E \to \mathbb{R}$ be the linear functional defined by $f(\lambda v_0) = \lambda$, for every $\lambda \in \mathbb{R}$. Let's show that $f \leq p$. If $\lambda \leq 0$, then $f(\lambda v_0) \leq 0 \leq p(\lambda v_0)$. If $\lambda > 0$, then $\lambda = g(\lambda v_0) \leq p(\lambda v_0)$ because $\frac{1}{\lambda}(\lambda v_0) = v_0 \notin C$.

So we can apply the analytic form of the Hahn-Banach theorem to get a linear function $F : V \to \mathbb{R}$ such that $F(v) \leq p(v)$ for every $v \in V$. In particular, $F(v_0) = 1$, and, if $v \in C$, then $F(v) \leq p(v) < 1$ (by (d) in the first lemma).

Finally, we show that $F$ is continuous. Note that, if $v \in -C$, we have $-F(v) = F(-v) < 1$. So, for every $v$ in the open neighborhood $U := C \cap (-C)$ of $0$, we have $|F(v)| < 1$. If $\varepsilon > 0$, then $\varepsilon U$ is an open neighborhood of $0$ in $V$, and we have $|F(v)| < \varepsilon$ for every $v \in \varepsilon U$. So $F$ is continuous at $0$. As $F$ is linear and translations are continuous on $V$, this implies that $F$ is continous at every point of $V$.

□

*Proof of the theorem.* Let $C = A - B = \{x - y,\ x \in A, y \in B\}$. Then $C$ is clearly convex, $C$ is open because it is equal to $\bigcup_{y \in B}(A - y)$, and $0 \notin C$ because $A \cap B = \varnothing$. So we can apply the second lemma above to get a continuous linear functional $f : V \to \mathbb{R}$ such that $f(x) < 0$ for every $x \in C$. Then, for every $x \in A$ and every $y \in B$, we have $f(x) < f(y)$. So the conclusion is true for $f$ and for $c = \sup_{x \in A} f(x)$.

□

**Theorem B.3.10** (Hahn-Banach theorem, second geometric version)**.** *Let $V$ be a locally convex topological $\mathbb{R}$-vector space, and let $A$ and $B$ be two nonempty convex subsets of $V$. Suppose that $A$ is closed, that $B$ is compact, and that $A \cap B = \varnothing$.*

*Then there exists a continuous linear functional $f : V \to \mathbb{R}$ and $c \in \mathbb{R}$ such that, for every $x \in A$ and every $y \in B$, we have*

$$f(x) < c < f(y).$$

*Proof.* We first find a convex open neighborhood $U$ of $0$ in $V$ such that $(A + U) \cap (B + U) = \varnothing$. (Note : this only uses that $V$ is locally and that $A$ is closed and $B$ compact, but not the fact that $A$ and $B$ are convex.)

For every $x \in B$, choose a symmetric convex open neighborhood $U_x$ of $0$ such that $(x + U_x + U_x + U_x) \cap A = \varnothing$; as $U_x$ is symmetric, this is equivalent to saying that $(x + U_x + U_x) \cap (A + U_x) = \varnothing$. As $B$ is compact, we can find $x_1, \dots, x_n \in B$ such that $B \subset \bigcup_{i=1}^n (x_i + U_{x_i})$. Let $U = \bigcap_{i=1}^n U_{x_i}$. Then $U$ is a convex open neighborhood of $0$, and we have $B + U \subset \bigcup_{i=1}^n (x_i + U_{x_i} + U)$ and $A + U \subset \bigcap_{i=1}^n (A + U_{x_i})$, so $(B + U) \cap (A + U) = \varnothing$.

The sets $A + U$ and $B + U$ are convex and open, so, by theorem B.3.7, there exists a continuous linear functional $f : V \to \mathbb{R}$ and $c' \in \mathbb{R}$ such that $f(x) \le c' \le f(y)$ for every $x \in A + U$ and every $y \in B + U$. As $B$ is compact and $f$ continuous, there exists $y_0 \in B$ such that $f(y_0) = \min_{y \in B} f(y)$. In particular, $c' < \min_{y \in B} f(y)$. Choose $c \in \mathbb{R}$ such that $c' < c < \min_{y \in B} f(y)$. Then we have $f(x) < c < f(y)$ for every $x \in A$ and every $y \in B$.

□

## B.4 The Banach-Alaoglu theorem

See section 15.1 of [18] or Theorem 3.15 of [20]. This theorem is also called "Alaoglu's theorem".

**Theorem B.4.1.** *Let $V$ be a normed vector space. Then the closed unit ball in* $\mathrm{Hom}(V, \mathbb{C})$ *is compact Hausdorff for the weak* topology.*

Compare with the following results, usually called "Riesz's lemma" or "Riesz's theorem" (see section 13.3 of [18] or Theorem 1.22 of [20]) :

**Theorem B.4.2.** *Let $V$ be normed vector space. Then the closed unit ball of $V$ is compact if and only if $V$ is finite-dimensional.*

## B.5 The Krein-Milman theorem

See section 14.6 of [18] (or theorem 3.23 of [20]).

**Definition B.5.1.** Let $V$ be a $\mathbb{R}$-vector space and $C$ be a convex subset of $V$. We say that $x \in C$ is *extremal* if, whenever $x = ty + (1-t)z$ with $t \in (0, 1)$ and $y, z \in C$, we must have $y = z = x$.

**Theorem B.5.2.** *Let $V$ be a locally convex topological $\mathbb{R}$-vector space, and let $K$ be a nonempty compact convex subset of $V$. Then $K$ is the closure of the convex hull of its set of extremal points.*

**Lemma B.5.3.** *Let $V$ be a locally convex topological $\mathbb{R}$-vector space, and let $K$ be a nonempty compact convex subset of $V$. Then $K$ has an extremal point.*

*Proof.* We say that a subset $S$ of $K$ is extremal if for every $x \in S$, if we have $x = ty + (1 - t)z$ with $y, z \in K$ and $t \in (0, 1)$, then we must have $y, z \in S$. (Note that a point $x \in K$ is extremal if and only if $\{x\}$ is extremal.)

Let $X$ be the set of nonempty closed extremal subsets of $K$, ordered by reverse inclusion. Let $Y$ a nonempty totally ordered subset of $X$, and let's show that it has a maximal element. As $Y$ is totally ordered, for all $T_1, \dots, T_n \in Y$, there exists $i \in \{1, \dots, n\}$ such that $T_i \subset T_j$ for every $j \in \{1, \dots, n\}$, and then $T_1 \cap \dots \cap T_n \supset T_i \neq \varnothing$. As $K$ is compact, this implies that $S := \bigcap_{T \in Y} T$ is not empty. The set $S$ is clearly closed, so if we can show that it is extremal, we will be done. Let $x \in S$, and write $x = ty + (1 - t)z$, with $y, z \in K$ and $t \in (0, 1)$. For every $T \in Y$, as $T$ is extremal, we must have $y, z \in T$. So $y, z \in S$, and $S$ is indeed extremal.

By Zorn's lemma, the set $X$ has a maximal element, let's call it $S$. To finish the proof, we just need to show that $S$ is a singleton. If $|S| \geq 2$, let $x, y \in S$ such that $x \neq y$. By the geometric version of the Hahn-Banach theorem (theorem B.3.10), there exists a continuous linear functional $f : V \to \mathbb{R}$ such that $f(x) < f(y)$. As $S$ is compact, the continuous function $f$ reaches its minimum on $S$. Let $m = \min_{z \in S} f(z)$, and let $S' = \{z \in S | f(z) \leq m\}$. Then $S'$ is closed, it is nonempty by the observation we just made, and $S' \neq S$ because $y \notin S'$. Let's show that $S'$ is extremal, which will give a contradiction (and imply that $S$ had to be a singleton). Let $z \in S'$, and write $z = tz' + (1-t)z''$, with $z', z'' \in K$ and $t \in (0,1)$. As $S$, we have $z', z'' \in S$. By definition of $m$, we have $m = f(z) = tf(z') + (1-t)f(z'') \leq tm + (1-t)m$, which forces $m = f(z') = f(z'')$, i.e. $z', z'' \in S'$.

□

*Proof of the theorem.* Let $L$ be the closure of the convex hull of the set of extremal points of $K$. Then $L$ is convex, closed and contained in $K$; in particular, $L$ is also compact. Suppose that $L \neq K$, and let $x \in K \setminus L$. By the geometric version of the Hahn-Banach theorem (theorem B.3.10), there exists a continuous linear functional $f : V \to \mathbb{R}$ such that $\max_{y \in L} f(y) < f(x)$. Let $M = \max_{z \in K} f(z)$, and let $K' = \{z \in K | f(z) = M\}$. Then $K'$ is a closed convex subset of $K$ (hence it is compact), and $K' \cap L = \varnothing$. By the lemma, $K'$ must have an extremal point $z$, and it is easy to see (as in the proof of the lemma) that $z$ is also an extremal point of $K$. But then $z$ should be in $L$, contradiction.

□

## B.6 The Stone-Weierstrass theorem

See section 12.3 of [18] or theorem 5.7 of [20] for the case of a compact space.

**Theorem B.6.1.** *Let $X$ be a locally compact Hausdorff topological space, and let $A$ be a $\mathbb{C}$-subalgebra of $\mathscr{C}_0(X)$ such that :*

*(a) for every $f \in A$, the function $x \longmapsto \overline{f(x)}$ is also in $A$;*

*(b) for all $x, y \in X$ such that $x \neq y$, there exists $f \in A$ such that $f(x) \neq f(y)$ ("$A$ separates the points of $X$");*

*(c) for every $x \in X$, there exists $f \in A$ such that $f(x) \neq 0$ ("$A$ vanishes nowehere on $X$").*

*Then $A$ is dense in $\mathscr{C}_0(X)$.*

# Index

# Bibliography


[1] Ehrhard Behrends. *Introduction to Markov chains*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 2000. With special emphasis on rapid mixing.

[2] Yves Benoist and Nicolas de Saxcé. A spectral gap theorem in simple Lie groups. *Invent. Math.*, 205(2):337–361, 2016.

[3] J. Bourgain and A. Gamburd. A spectral gap theorem in $\mathrm{SU}(d)$. *J. Eur. Math. Soc. (JEMS)*, 14(5):1455–1511, 2012.

[4] Jean Bourgain and Alex Gamburd. On the spectral gap for finitely-generated subgroups of $\mathrm{SU}(2)$. *Invent. Math.*, 171(1):83–121, 2008.

[5] Emmanuel Breuillard. Random walks on lie groups. `https://www.math.u-psud.fr/~breuilla/part0gb.pdf`, 2004.

[6] P. Cartier. Representations of $p$-adic groups: a survey. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*, Proc. Sympos. Pure Math., XXXIII, pages 111–155. Amer. Math. Soc., Providence, R.I., 1979.

[7] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli. *Harmonic analysis on finite groups*, volume 108 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2008. Representation theory, Gelfand pairs and Markov chains.

[8] Persi Diaconis. *Group representations in probability and statistics*, volume 11 of *Institute of Mathematical Statistics Lecture Notes—Monograph Series*. Institute of Mathematical Statistics, Hayward, CA, 1988.

[9] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[10] Per Enflo. A counterexample to the approximation problem in Banach spaces. *Acta Math.*, 130:309–317, 1973.

[11] Gerald B. Folland. *A course in abstract harmonic analysis*. Textbooks in Mathematics. CRC Press, Boca Raton, FL, second edition, 2016.

[12] Ulf Grenander. *Probabilities on algebraic structures*. Second edition. Almqvist & Wiksell, Stockholm; John Wiley & Sons Inc., New York-London, 1968.

[13] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University

Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[14] Yukiyosi Kawada and Kiyosi Itô. On the probability distribution on a compact group. I. *Proc. Phys.-Math. Soc. Japan (3)*, 22:977–998, 1940.

[15] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. With an appendix by Jonathan D. Rogawski, Reprint of the 1994 edition.

[16] Jean-Fran cois Quint. An introduction to random walks on groups. `https://www.math.u-bordeaux.fr/~jquint/publications/CoursChili.pdf`, 2014.

[17] Jeffrey S. Rosenthal. Random rotations: characters and random walks on $\mathrm{SO}(N)$. *Ann. Probab.*, 22(1):398–423, 1994.

[18] H. L. Royden. *Real analysis*. Macmillan Publishing Company, New York, third edition, 1988.

[19] Walter Rudin. *Real and complex analysis*. McGraw-Hill Book Co., New York, third edition, 1987.

[20] Walter Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., New York, second edition, 1991.

[21] Peter Sarnak. *Some applications of modular forms*, volume 99 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1990.

[22] Mark R. Sepanski. *Compact Lie groups*, volume 235 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[23] Francis Edward Su. Convergence of random walks on the circle generated by an irrational rotation. *Trans. Amer. Math. Soc.*, 350(9):3717–3741, 1998.

[24] Francis Edward Su. Discrepancy convergence for the drunkard's walk on the sphere. *Electron. J. Probab.*, 6:no. 2, 20, 2001.

[25] Gerrit van Dijk. *Introduction to harmonic analysis and generalized Gelfand pairs*, volume 36 of *De Gruyter Studies in Mathematics*. Walter de Gruyter & Co., Berlin, 2009.