MAT 449 : Problem Set 1

Due Thursday, September 20

In this problem set, $\mathbb{N}$ is the set of nonnegative integers.

Examples of topological groups

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 $\mathcal{L}(V)$ 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 $f \in \mathcal{L}(V)$,

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

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

You can do this problem assuming that V is finite-dimensional. You'll get one point of extra credit for every question where you treat the general case (i.e. without any assumption on the dimension of V).

a) (1) Show that $\mathbf{GL}(V)$ is an open subset of $\mathcal{L}(V)$.

b) (2) Show that $\mathbf{GL}(V)$ is a topological group.

c) (1) Show that $\mathbf{GL}(V)$ is locally compact if and only if V is finite-dimensional.

Solution.

a) Note that, by definition of the operator norm, we have $\|xy\|_{op} \leq \|x\|_{op}\|y\|_{op}$ for all $x, y \in \mathcal{L}(V)$. (This property is called "submultiplicativity".) So, if $x \in \mathcal{L}(V)$ 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 $\mathrm{id}_V - x \in \mathbf{GL}(V)$.

Now let $x \in \mathbf{GL}(V)$. We want to show that $GL(V)$ contains a neighborhood of x in $\mathcal{L}(V)$. Let $y \in \mathcal{L}(V)$ 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 $\mathcal{L}(V)$ such that $\|x - x'\|_{op} < \|x^{-1}\|_{op}$ is in $\mathbf{GL}(V)$, which proves the result.

If V is finite-dimensional, we can also use tha fact that the determinant is a continuous map $\det : \mathcal{L}(V) \to \mathbb{C}$, and that $\mathbf{GL}(V)$ 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 $\mathcal{L}(V) \times \mathcal{L}(V)$ to $\mathcal{L}(V)$. (This implies immediately that multiplication is continuous on $\mathbf{GL}(V)$.) This follows immediately from the submultiplicativity of the operator norm. Indeed, if $x, x', y, y' \in \mathcal{L}(V)$, 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 $\mathbf{GL}(V)$. Let $x \in \mathbf{GL}(V)$. Let $y \in \mathcal{L}(V)$, 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 $\mathbf{GL}(V) = \mathbf{GL}_n(\mathbb{C})$. Then we use the fact that, if $x \in \mathbf{GL}_n(\mathbb{C})$, 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 ± 1 times determinants of submatrixes 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 $\mathbf{GL}(V)$ is open in $\mathcal{L}(V)$ by question (a), this implies that $\mathbf{GL}(V)$ is locally compact if and only if e has an open neighborhood in $\mathcal{L}(V)$. As the topology of $\mathcal{L}(V)$ is defined by a norm, this is equivalent to the fact that closed balls in $\mathcal{L}(V)$ are compact. By Riesz's lemma, this is equivalent to the fact that $\mathcal{L}(V)$ is finite-dimensional. If V is finite-dimensional, then $\mathcal{L}(V)$ is also finite-dimensional. If V is infinite-dimensional, then it follows from the Hahn-Banach theorem that $\mathcal{L}(V)$ is also infinite-dimensional.

□

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

a) (2) Show that $\prod_{i\in I} G_i$ is a topological group (for the product topology).

b) (2, extra credit) 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).

□

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 *projctive 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) (1) 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) (1) 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) (2) 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) (2) 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) (2) 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 (3)(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).

□

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) (2) 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.

b) (4) 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 $\mathbb{Q}_p$.

c) (1) Show that the additive group of $\mathbb{Q}_p$ is a topological group.

d) (1) Calculate the subset $|\mathbb{Q}_p|_p$ of $\mathbb{R}$.

e) (1) 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.

f) (1) Show that $\mathbb{Q}_p$ is totally disconnected (i.e. its only nonempty connected subsets are the singletons) but not discrete.

g) (1) Show that a series $\sum_{n\geq 0} x_n$ is convergent if and only if $\lim_{n\to+\infty} |x_n|_p = 0$.

h) (1) 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.

i) (2) 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 $|x|_p = p^{-m}$.

j) (2) 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 $\mathbb{Q}_p$.

k) (2) 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 $\mathbb{Z}_p$.

l) (2) 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 $\mathbf{GL}_n(\mathbb{Q}_p)$. Show that $\mathbf{GL}_n(\mathbb{Q}_p)$ is a locally compact topological group.

m) (2) Show that $\mathbf{GL}_n(\mathbb{Z}_p)$ is an open compact subgroup of $\mathbf{GL}_n(\mathbb{Q}_p)$. (Hint : Show that $\mathbb{Z}_p^\times$ is closed in $\mathbb{Z}_p$.)

Solution.

Dan : I tried to be very thorough in the solution. If they are a bit sketchier but got the idea, you don't have to take points off.

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

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

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 $x \mapsto -x$ 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 $n \leq n'$, then (using (b)) :

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

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

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

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

For every $n \geq m$, we have

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

so $|x|_p \leq p^{-m}$. 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 $n \geq m$,

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

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

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

Let $n \geq 0$. 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 $c_{a_n,n} \neq 0$. 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 $n \geq n'$. Then $|x_n - x_{n'}|_p \leq \max(|x_n - x|_p, |x - x_{n'}|_p) < p^{-n'}$. On the other hand, we have $x_n - x_{n'} = \sum_{i\geq m}(c_{i,n} - c_{i,n'})p^i$. 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 $\mathbb{Z}_p \cap ((\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \dots, x_0)\})$, 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 $A = (\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \dots, x_0)\}$. 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 $|x - y|_p \leq p^{-m}$. [1] 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 $n \in \{0, \dots, m\}$, 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 $u(A') = (\prod_{n\geq m+1} \mathbb{Z}/p^n\mathbb{Z}) \times \{(x_m, \dots, x_0)\}$, where $x_n = y + p^n\mathbb{Z}$ for $0 \leq n \leq m$.

l) The proof that $\mathbf{GL}_n(\mathbb{Q}_p)$ is a topological group is the same as in (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 $\mathbf{GL}_n(\mathbb{Q}_p)$ 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) First, $\mathbf{GL}_n(\mathbb{Z}_p)$ is open in $\mathbf{GL}_n(\mathbb{Q}_p)$ because it is the intersection of $\mathbf{GL}_n(\mathbb{Q}_p)$ with the open subset $M_n(\mathbb{Z}_p)$ of $M_n(\mathbb{Q}_p)$ (we have seen in the previous question that $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$). As $M_n(\mathbb{Z}_p)$ is compact (because $\mathbb{Z}_p$) is, to show that $\mathbf{GL}_n(\mathbb{Z}_p)$ 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 that $Z_p^\times$ 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 $x^{-1} \in \mathbb{Z}_p$.

□

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

Examples of Haar measures

5. (6) 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 $x \mapsto A(x)$ is a morphism of groups from G to $\mathbf{GL}_N(\mathbb{R})$.)

   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 $\operatorname{Ker}(A - A') = \mathbb{R}^N$, 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 $G \to G$, $y \mapsto xy$ is contained in $b(x) + \operatorname{Im}(A(x))$, 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 $x \mapsto A(x)$ 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 $A \in \mathbf{GL}_N(\mathbb{R})$ and $b \in \mathbb{R}^N$, and if V is the image of U by the transformation $y \mapsto Ay + b$, 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 $f \in \mathcal{C}_c(G)$. Then the function $x \mapsto |\det A(x)|^{-1}f(x)$ is also in $\mathcal{C}_c(G)$, 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.

□

6. In this problem, dx will always be the Lebesgue measure on $\mathbb{R}$.

   a) (1) Show that $\frac{dx}{|x|}$ is a Haar measure on the multiplicative group $\mathbb{R}^\times$.

   b) (1) 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) (3) 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 $\mathbf{GL}_n(\mathbb{R})$.

   d) (2) 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 problem 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 $A(x) = x \in \mathbf{GL}_1(\mathbb{R})$ 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 $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$. 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 2×2 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 $\mathbf{GL}_n(\mathbb{R})$ 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 $x \in \mathbf{GL}_n(\mathbb{R})$. 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 $x \in \mathbf{GL}_n(\mathbb{R})$ 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.

□

7. (extra credit) Consider the group $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$.

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

b) (2) 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 $V \subset (\mathbb{Z}/2\mathbb{Z})^{\{0,\dots,n\}}$, and that we have $\mu(U) = \frac{|V|}{2^{n+1}}$.

c) (4) 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 μ to Lebesgue measure λ 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 σ-algebra on $[0,1]$, and calculate their inverse images by u.)

Solution.

a) Let μ be a left Haar measure on G. As G is commutative, μ is also a right Haar measure. Also, by problem 3(b), the group G is compact, so $\mu(G) < +\infty$, and, after multiplying μ 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 Ω 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 σ-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 σ-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 μ. 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

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

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

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

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

□

8. 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 λ be the Haar measure on $\mathbb{Q}_p$ such that $\lambda(\mathbb{Z}_p) = 1$.

   a) (1) If $x \in \mathbb{Q}_p$ and $m \in \mathbb{Z}$, show that $\lambda(B(x, p^m)) = p^m$.

   b) (2) 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 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 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 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 λ.

□