Chapter 13
p-Adic Numbers and Adeles

The majority of the examples of topological groups in this book given so far, are locally euclidean, meaning that the groups are locally homeomorphic to $\mathbb{R}^n$. In this chapter the reader will see some examples which are not of this type. These examples, the p-adic numbers and the adeles, resp. ideles, are not only interesting as examples of this theory, but they also carry great importance for other areas of mathematics, in particular number theory.

13.1 p-Adic Numbers

The set $\mathbb{R}$ of real numbers is the completion of $\mathbb{Q}$ with respect to the usual absolute value

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

We shall see, that there are more "absolute values" defined on $\mathbb{Q}$. But first we have to give this notion a precise meaning.

Absolute Values

By an *absolute value* on a field K we mean a map $|\cdot| : K \to [0, \infty)$, such that for all $a, b \in K$ one has

- $|a| = 0 \Leftrightarrow a = 0$, (definiteness)
- $|ab| = |a||b|$, (multiplicativity)
- $|a + b| \leq |a| + |b|$. (triangle inequality)

Remark Every absolute value maps ± 1 to 1, i.e., one has $|1| = |-1| = 1$. For a proof consider $|1| = |1 \cdot 1| = |1|^2$ so $|1| = 1$ and $|-1|^2 = |(-1)^2| = |1| = 1$ so that $|-1| = 1$.

A. Deitmar, S. Echterhoff, *Principles of Harmonic Analysis,* Universitext,
DOI 10.1007/978-3-319-05792-7_13, © Springer International Publishing Switzerland 2014

Lemma 13.1.1 *If* $|\cdot|$ *is an absolute value on the field* K*, then* $d(x,y) = |x-y|$ *is a metric on* K*.*

Proof The map d is positive definite. It is symmetric, too, since

$$d(y,x) = |y-x| = |(-1)(x-y)| = |-1||x-y| = |x-y| = d(x,y).$$

Finally. it satisfies the triangle inequality, since for $x, y, z \in K$ one has

$$d(x,y) = |x-z+z-y| \le |x-z| + |z-y| = d(x,z) + d(z,y). \qquad \square$$

Examples 13.1.2

- For $K = \mathbb{Q}$ the usual absolute value $|\cdot|_\infty$ is an example.
- The *discrete absolute value* exists for every field and is given by

$$|x|_{\text{triv}} = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

  The metric generated by this absolute value is the *discrete metric*

$$d(x,y) = \begin{cases} 0 & \text{if } x = y \\ 1, & \text{if } x \neq y. \end{cases}$$

  The discrete metric induces the discrete topology, as for every $x \in K$ the open ball $B_{1/2}(x)$ of radius $1/2$ equals the set $\{x\}$, which therefore is open.

Definition Consider the field $K = \mathbb{Q}$ of rational numbers and fix a prime number p. Every rational can be written in the form

$$r = p^k \frac{m}{n}, \qquad n \neq 0,$$

where $m, n \in \mathbb{Z}$ are coprime to p. The exponent $k \in \mathbb{Z}$ is uniquely determined by r, if $r \neq 0$. We define the *p-adic absolute value* by

$$|r|_p = \left| p^k \frac{m}{n} \right|_p := \begin{cases} p^{-k} & \text{if } r \neq 0, \\ 0 & \text{if } r = 0. \end{cases}$$

Lemma 13.1.3 *Let p be a prime number. Then* $|\cdot|_p$ *is an absolute value on* $\mathbb{Q}$*, which satisfies the* strong triangle inequality

$$|x+y|_p \ \le \ \max(|x|_p, |y|_p).$$

Here we have equality, if $|x|_p \neq |y|_p$*.*

Proof Definiteness follows from the definition. To show multiplicativity, write $x = p^k \frac{m}{n}$ and $y = p^{k'} \frac{m'}{n'}$, where m, n, m', n' are coprime to p. Then $xy = p^{k+k'} \frac{mm'}{nn'}$, and this yields $|xy|_p = |x|_p |y|_p$ in the case $xy \neq 0$. The case $xy = 0$ is trivial. For a proof of the strong triangle inequality, we can assume $xy \neq 0$ and $k \le k'$. Then we have

$$x + y = p^k \left(\frac{m}{n} + p^{k'-k} \frac{m'}{n'} \right) = p^k \frac{mn' + p^{k'-k} nm'}{nn'}.$$

If $|x|_p \neq |y|_p$, i.e., $k' - k > 0$, then the number $mn' + p^{k'-k} nm'$ is coprime to p and we have $|x + y| = p^{-k} = \max(|x|_p, |y|_p)$. If on the other hand $|x|_p = |y|_p$, then the enumerator $mn' + p^{k'-k} nm' = mn' + nm'$ is of the form $p^l N$, where $l \ge 0$ and N is coprime to p. This means that $|x+y|_p = |p^{k+l} \frac{N}{nn'}|_p = p^{-k-l} \le \max(|x|_p, |y|_p)$. □

In what follows we denote by $R^\times$ the group of units in a ring R. Of course, if K is a field, we have $K^\times = K \smallsetminus \{0\}$.

Proposition 13.1.4 *For every $x \in \mathbb{Q}^\times$ we have the* product formula

$$\prod_{p \le \infty} |x|_p = 1.$$

The product is extended over all prime numbers and $p = \infty$. For a given number $x \in \mathbb{Q}^\times$, almost all factors in the product are equal to 1.

Remark When we say *almost all*, we mean *all, up to finitely many exceptions*.

Proof Write x as a fraction of coprime integers and write these integers as product of primes. Then one has $x = \pm p_1^{k_1} \cdots p_n^{k_n}$ for pairwise different primes $p_1, \dots, p_n$ and $k_1, \dots, k_n \in \mathbb{Z}$. The p-adic absolute value $|x|_p$ equals 1, if p is a prime not occurring among the above. So the product indeed has only finitely many factors $\neq 1$. Further one has $|x|_{p_j} = p_j^{-k_j}$ and $|x|_\infty = p_1^{k_1} \cdots p_n^{k_n}$. Hence

$$\prod_{p \le \infty} |x|_p = \left(\prod_{j=1}^n p_j^{-k_j} \right) \cdot p_1^{k_1} \cdots p_n^{k_n} = 1.$$ □

Remark One can show that every non-trivial absolute value $|\cdot|$ on $\mathbb{Q}$ is of the form $|x| = |x|_p^a$ for a uniquely determined $p \le \infty$ and a uniquely determined real number $a > 0$.

$\mathbb{Q}_p$ *as Completion of* $\mathbb{Q}$

We now give the first construction of the set $\mathbb{Q}_p$ of p-adic numbers. This set is the completion of $\mathbb{Q}$ in the p-adic metric

$$d_p(x, y) = |x - y|_p.$$

Proposition 13.1.5 *Let $p \le \infty$. Then $\mathbb{Q}$ is not complete in the metric d_p. We denote the completion by $\mathbb{Q}_p$. Addition and Multiplication of $\mathbb{Q}$ can be extended in a unique way to continuous maps $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$. With these operations, $\mathbb{Q}_p$ is a field, called the field of p-adic numbers. The absolute value $|\cdot|_p$ can be extended in a unique way to a continuous map on $\mathbb{Q}_p$, which is an absolute value, again.*

Proof We consider this proposition known for $p = \infty$. In this case one has $\mathbb{Q}_p = \mathbb{Q}_\infty = \mathbb{R}$. We now let $p < \infty$. We write $|\cdot| = |\cdot|_p$. The non-completeness of $\mathbb{Q}$ follows from another description of $\mathbb{Q}_p$, which will be shown in the next section. We now extend the operations. Let $x, y \in \mathbb{Q}_p$. As $\mathbb{Q}$ is dense in the metric space $\mathbb{Q}_p$, there are sequences (x_n) and (y_n) in $\mathbb{Q}$, converging to x, resp. y in $\mathbb{Q}_p$. These sequences are Cauchy sequences in $\mathbb{Q}$. The estimate

$$|(x_n + y_n) - (x_m + y_m)| \le |x_n - x_m| + |y_n - y_m|$$

implies that $(x_n + y_n)$ is a Cauchy sequence as well. So it converges in $\mathbb{Q}_p$ to an element z. This element does not depend on the choice of the sequences, since if (x'_n) and (y'_n) is another choice, then the sequence $\left(x'_n + y'_n\right)$ also is a Cauchy sequence, which differs from $(x_n + y_n)$ only by a sequence converging to zero, hence gives the same element in the completion. We set $x+y = z$ and have thus extended the addition to $\mathbb{Q}_p$. It is easy to see that addition is a continuous map from $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$. The multiplication is extended analogously and it is not difficult to show that $\mathbb{Q}_p$ is a field with these operations and that the absolute value extends as well. We leave the details as an exercise. □

The strong triangle inequality $|x + y| \le \max(|x|, |y|)$ still holds on $\mathbb{Q}_p$. It has astonishing consequences, for example, the set

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\},$$

which contains $\mathbb{Z}$, is a subring of the field $\mathbb{Q}_p$. This ring is called the *ring of p-adic integers*.

Power Series

Let p be a prime. We now give a second construction of p-adic numbers. Every integer $n \ge 0$ can be written in the *p-adic expansion*,

$$n = \sum_{j=0}^{N} a_j p^j,$$

with uniquely determined coefficients $a_j \in \{0, 1, \dots, p-1\}$. The sum of n and a second number $m = \sum_{i=0}^{M} b_i p^i$ is

$$n + m = \sum_{j=0}^{\max(M,N)+1} c_j p^j,$$

where each c_j only depend on $a_0, \dots, a_j$ and $b_0, \dots, b_j$. More precisely, these coefficients are computed as follows: First one sets $c'_j = a_j + b_j$. Then one has $0 \le c'_j \le 2p - 2$ and it may happen, then $c'_j \ge p$. Let j be the smallest index, for which this happens. One replaces c'_j by the remainder modulo p and increases c'_{j+1} by one. Then one repeats this step until all coefficients are $\le p - 1$.

For the multiplication one has

$$nm = \sum_{j=0}^{M+N+1} d_j p^j,$$

where again the coefficient d_j only depends on $a_0, \dots, a_j$ and $b_0, \dots, b_j$.

These properties of multiplication and addition make it possible, to extend them to the set Z of formal power series

$$\sum_{j=0}^{\infty} a_j p^j,$$

with $0 \le a_j < p$. A *formal power series* may be considered simply as the sequence of its coefficients $(a_0, a_1, \dots)$. The multiplicative unit 1 is represented by the sequence $(1, 0, 0, \dots)$. One only uses the notation of a series for convenience.

Lemma 13.1.6 *With these operations, the set Z is a ring. An element* $x = \sum_{j=0}^{\infty} a_j p^j$ *is invertible in Z if and only if* $a_0 \neq 0$.

Proof Associativity and distributivity are inherited from $\mathbb{Z}$, as it suffices to check them on finite parts of the series. To show that Z is a ring, we are left with showing that an additive inverse exists. So let $x = \sum_{j=0}^{\infty} a_j p^j$ in Z. We have to show the existence of some $y = \sum_{j=0}^{\infty} b_j p^j$ in Z, such that $x + y = 0$. We construct the coefficients b_j inductively. In the case $a_0 = 0$ we set $b_0 = 0$ and $b_0 = p - a_0$ otherwise. Assume $b_0, \dots, b_n$ already constructed with the property, that the element $y_n = \sum_{j=0}^{n} b_j p^j$ satisfies

$$x + y_n = \sum_{j=n+1}^{\infty} c_j p^j, \qquad 0 \le c_j < p.$$

If $c_{n+1} = 0$, then one sets $b_{n+1} = 0$. Otherwise one sets $b_{n+1} = p - c_{n+1}$. In this way one gets an element $y = \sum_{j=0}^{\infty} b_j p^j$, which satisfies $x + y = 0$.

We show the second assertion. If $x = \sum_{j=0}^{\infty} a_j p^j$ is invertible, then $a_0 \neq 0$, since otherwise the series xy would have vanishing zeroth coefficient for every $y \in Z$. For the converse direction, let $x = \sum_{j=0}^{\infty} a_j p^j$ with $a_0 \neq 0$. We construct a multiplicative inverse $y = \sum_{j=0}^{\infty} b_j p^j$ by giving the coefficients b_j successively. Since $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field, there exists exactly one $1 \le b_0 < p$ such that $a_0 b_0 \equiv 1 \bmod p$. Assume next that $0 \le b_0, \dots, b_n < p$ are already constructed with the property that

$$\underbrace{\left(\sum_{0\le j} a_j p^j\right)}_{=A} \underbrace{\left(\sum_{0\le j\le n} b_j p^j\right)}_{=B} \equiv 1 \mod p^{n+1}.$$

Then one has $\frac{AB-1}{p^{n+1}} \in \mathbb{Z}$, so there exists exactly one $0 \le b_{n+1} < p$, such that $\frac{AB-1}{p^{n+1}} + a_0 b_{n+1} = pc$, $c \in \mathbb{Z}$, or $AB - 1 + a_0 b_{n+1} p^{n+1} = p^{n+2}c$. In other words, one has

$$\left(\sum_{0\le j} a_j p^j\right) \left(\sum_{0\le j\le n+1} b_j p^j\right) \equiv 1 \mod p^{n+2}.$$

The element $y = \sum_{j=0}^\infty b_j p^j$ constructed in this way satisfies the equation $xy = 1$. □

Lemma 13.1.7 *Let (a_j) be a sequence in $\{0, 1, \dots, p-1\}$. Then the series $\sum_{j=0}^\infty a_j p^j$ converges in $\mathbb{Q}_p$. We map the formal series to this limit and get a map $\psi : Z \to \mathbb{Q}_p$. This map is an isomorphism of rings*

$$Z \xrightarrow{\cong} \mathbb{Z}_p.$$

Proof Let $x_n = \sum_{j=0}^n a_j p^j$. We have to show that (x_n) is a Cauchy sequence in $\mathbb{Q}_p$. For $m \ge n \ge n_0$ one has

$$|x_m - x_n| = \left|\sum_{j=n+1}^m a_j p^j\right| \le \max_{n<j\le m} |a_j|_p |p^j|_p \le p^{-n_0}.$$

Therefore the sequence is Cauchy, so the map ψ is well-defined. It is easy to show that ψ is a ring homomorphism. It remains to show bijectivity of $\phi : Z \to \mathbb{Z}_p$.

Injectivity: Let $x = \sum_{j=0}^\infty a_j p^j \ne 0$. Then there is a minimal j_0 such that $a_{j_0} \ne 0$. We have

$$|\psi(x)| = \left|a_{j_0} p^{j_0} + \sum_{j=j_0+1}^\infty a_j p^j\right| = p^{-j_0},$$

since $\left|\sum_{j=j_0+1}^\infty a_j p^j\right| \le \max_{j>j_0} |a_j| p^{-j} < p^{-j_0}$ (use continuity of $|\cdot|_p$). So it follows $\psi(x) \ne 0$ and therefore ψ has trivial kernel, thus is injective.

Surjectivity: We define an absolute value on Z by

$$|z| = |\psi(z)|_p.$$

We claim that Z is complete in this absolute value. Let (z_j) be a Cauchy-sequence in Z. For each $k \in \mathbb{N}$ there exists a $j_0(k) \in \mathbb{N}$, such that for all $i, j \ge j_0(k)$ one has

$|z_i - z_j| \le p^{-k}$, which means, that $\psi(z_i) - \psi(z_j) \in p^k\mathbb{Z}_p$, so $z_i - z_j \in p^k Z$. We conclude, that the coefficients of the power series z_i and z_j coincide up to the index $k-1$. Therefore there are coefficients a_ν for $\nu = 0, 1, 2, \dots$, such that for every $k \in \mathbb{N}$ and every $j \ge j_0(k)$ one has $z_j \equiv \sum_{\nu=0}^{k-1} a_\nu p^\nu \bmod p^k Z$. Set $z = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in Z$. The sequence (z_j) converges to z, so Z is complete. To finish the proof, it suffices to show that $\psi(Z)$ contains a dense subset of $\mathbb{Z}_p$. Such a set is given by the set of all rational numbers in $\mathbb{Z}_p$, i.e., the set of all $q = \pm p^k \frac{m}{n}$ where $k \ge 0$ and m, n coprime to p. As Z is a ring, it suffices to show that $\frac{1}{n} \in Z$, if $n \in \mathbb{N}$ is coprime to p. But for n coprime to p the zeroth coefficient of the p-adic expansion is non-zero and therefore n is invertible in Z. □

We now can identify $\mathbb{Z}_p$ with the set of all power series in p. As $\mathbb{Z}_p$ equals the set of all $z \in \mathbb{Q}_p$ with $|z| \le 1$, the set $p^{-j}\mathbb{Z}_p$ is the set of all $z \in \mathbb{Q}_p$ with $|z| \le p^j$. Therefore,

$$\mathbb{Q}_p = \bigcup_{j=0}^{\infty} p^{-j}\mathbb{Z}_p.$$

So we can write $\mathbb{Q}_p$ as the set of all Laurent-series in p with only finitely many negative entries, i.e.,

$$\mathbb{Q}_p = \left\{ \sum_{j=-N}^{\infty} a_j p^j \,:\, N \in \mathbb{N},\ 0 \le a_j < p \right\}.$$

This also implies that $\mathbb{Q}_p$ is uncountable. In particular, $\mathbb{Q} \ne \mathbb{Q}_p$ and therefore $\mathbb{Q}$ is not complete in the p-adic metric.

Proposition 13.1.8 (a) *The topological spaces $\mathbb{Q}_p$ and $\mathbb{Q}_p^\times$ are locally compact and totally disconnected. So together with Proposition 13.1.5 this implies that these are totally disconnected LCA-groups.*

(b) *The open compact subgroups $p^n\mathbb{Z}_p$, $n \in \mathbb{N}$ form a basis of the unit-neighborhoods of the additive group* $(\mathbb{Q}_p, +)$.

(c) *The compact open subgroups $1 + p^n\mathbb{Z}_p$, $n \in \mathbb{N}$ form a basis of the unit-neighborhoods of the multiplictive group* $(\mathbb{Q}_p^\times, \times)$.

Proof It suffices to show (b) and (c), for these imply (a) as well. The subgroup $p^n\mathbb{Z}_p$ coincides with the open ball $B_r(0)$ for any $r > 0$ with $p^{-n} < r < p^{-n+1}$, so these sets clearly form a neighborhood basis of zero. Likewise, the set $1 + p^n\mathbb{Z}_p$ equals the open Ball $B_r(1)$ around 1 of radius $r > 0$, if $p^{-n} < r < p^{-n+1}$. Hence the claim follows as soon as we have shown that $\mathbb{Z}_p$, and hence $p^n\mathbb{Z}_p$, is compact. But if (x_n) is a sequence in $\mathbb{Z}_p$ and if we write each x_n as a power series $\sum_{j=0}^{\infty} a_j^n p^j$ with $a_j^n \in \{0, \dots, p-1\}$ we may pass inductively to subsequences $\left(x_{n_k}^l\right)$ of (x_n) such that the first l coefficients $a_1, \dots, a_l$ of all elements in the l-th subsequence agree. It is then easy to check that the diagonal subsequence $\left(x_{n_l}^l\right)$ of (x_n) converges in $\mathbb{Z}_p$. □

p-Adic Numbers as Limits

Fix a prime p and let $m, n \in \mathbb{N}$ with $m \geq n$. Then the natural projection

$$\pi_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

is a ring homomorphism. The family $\left(\pi_m^n\right)_{m,n}$ satisfies the axioms of a projective system of rings as in Sect. 1.8.

Proposition 13.1.9 *The ring $\mathbb{Z}_p$ is canonically isomorphic with the projective limit of the $\mathbb{Z}/p^n\mathbb{Z}$.*

Proof If we view $\mathbb{Z}_p$ as ring of power series, we get natural projections $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ by cutting off a power series beyond its n-th entry. These projections are compatible with the projections $\pi_m^n : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, so these maps fit together to give a ring homomorphism

$$\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Interpreting the right hand side as set of compatible elements in the product $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ easily shows that this map is a bijection. □

13.2 Haar Measures on *p*-adic Numbers

The absolute value $|\cdot|_p$ defines a metric, which yields a topology on $\mathbb{Q}_p$. We showed above that with this topology the groups $\left(\mathbb{Q}_p, +\right)$ and $\left(\mathbb{Q}_p^\times, \cdot\right)$ are locally compact abelian groups. We now determine their Haar measures.

Note that the group of units $\mathbb{Z}_p^\times$ in $\mathbb{Z}_p$ is exactly the set of all $x \in \mathbb{Q}_p$, which satisfy $|x|_p = 1$.

Let μ be the Haar measure on the group $\left(\mathbb{Q}_p, +\right)$, which gives the compact open subgroup $\mathbb{Z}_p$ the volume 1, so $\mu(\mathbb{Z}_p) = 1$. Invariance of μ means $\mu(x + A) = \mu(A)$ for every measurable $A \subset \mathbb{Q}_p$ and every $x \in \mathbb{Q}_p$.

Lemma 13.2.1 *For every measurable subset $A \subset \mathbb{Q}_p$ and every $x \in \mathbb{Q}_p$ one has $\mu(xA) = |x|_p\mu(A)$. In particular, for every integrable function f and $x \neq 0$ one has*

$$\int_{\mathbb{Q}_p} f\left(x^{-1}y\right) d\mu(y) = |x|_p \int_{\mathbb{Q}_p} f(y)\, d\mu(y).$$

Proof Let $x \in \mathbb{Q}_p \setminus \{0\}$. The measure μ_x, defined by $\mu_x(A) = \mu(xA)$, is a Haar measure again, as is easily seen. By uniqueness of Haar measures, there exists some $M(x) > 0$ such that $\mu_x = M(x)\mu$. We show that $M(x) = |x|_p$. It suffices to show

$\mu(x\mathbb{Z}_p) = |x|_p$. Assume that $|x|_p = p^{-k}$. Then $x = p^k y$ for some $y \in \mathbb{Z}_p^\times$, and so $x\mathbb{Z}_p = p^k\mathbb{Z}_p$. Therefore it suffices to show $\mu\left(p^k\mathbb{Z}_p\right) = p^{-k}$. We start with the case $k \geq 0$. Then $[\mathbb{Z}_p : p^k\mathbb{Z}_p] = p^k$, so there is a disjoint decomposition of $\mathbb{Z}_p$, $\mathbb{Z}_p = \bigcup_{j=1}^{p^k} (x_j + p^k\mathbb{Z}_p)$. By invariance of Haar measure we have

$$1 = \mu(\mathbb{Z}_p) = \sum_{j=1}^{p^k} \mu\left(x_j + p^k\mathbb{Z}_p\right) = p^k\mu\left(p^k\mathbb{Z}_p\right),$$

which implies the claim. If $k < 0$, then one uses $\left[p^k\mathbb{Z}_p : \mathbb{Z}_p\right] = p^{-k}$ in an analogous way. □

For simplification, we write integration according to a Haar measure as dx, so

$$\int_{\mathbb{Q}_p} f(x)\, d\mu(x) = \int_{\mathbb{Q}_p} f(x)\, dx.$$

Proposition 13.2.2 *The measure $\frac{dx}{|x|_p}$ is a Haar measure of the multiplicative group $\mathbb{Q}_p^\times$.*

Proof Let $f \in C_c(\mathbb{Q}_p^\times)$ and $y \in \mathbb{Q}_p^\times$. Then one has

$$\int_{\mathbb{Q}_p^\times} f\left(y^{-1}x\right) \frac{dx}{|x|_p} = |y|_p^{-1} \int_{\mathbb{Q}_p^\times} f\left(y^{-1}x\right) \frac{1}{|y^{-1}x|_p}\, dx = \int_{\mathbb{Q}_p^\times} f(x) \frac{dx}{|x|_p}$$

by Lemma 13.2.1. □

The subgroup $\mathbb{Z}_p^\times$ of $\mathbb{Q}_p^\times$ is the kernel of the group homomorphism $\mathbb{Q}_p^\times \to \mathbb{Z}$; $x \mapsto \frac{\log(|x|_p)}{\log p}$. Hence $\mathbb{Q}_p^\times$ can be written as disjoint union: $\mathbb{Q}_p^\times = \bigcup_{k\in\mathbb{Z}} p^k\mathbb{Z}_p^\times$. One has $\mathrm{vol}_{\frac{dx}{|x|_p}}\left(p^k\mathbb{Z}_p^\times\right) = \mathrm{vol}_{\frac{dx}{|x|_p}}\left(\mathbb{Z}_p^\times\right)$. It is therefore of interest, to compute the measure $\mathrm{vol}_{\frac{dx}{|x|_p}}\left(\mathbb{Z}_p^\times\right)$. One has $\mathrm{vol}_{\frac{dx}{|x|_p}}\left(\mathbb{Z}_p^\times\right) = \int_{\mathbb{Z}_p^\times} \frac{dx}{|x|_p} = \int_{\mathbb{Z}_p^\times} dx = \mathrm{vol}_{dx}\left(\mathbb{Z}_p^\times\right)$. Consider the power series representation of $\mathbb{Z}_p$ and order the elements of $\mathbb{Z}_p^\times$ by their first coefficient. We get a disjoint decomposition

$$\mathbb{Z}_p^\times = \dot{\bigcup_{\substack{a \mod p \\ a\not\equiv 0 \mod p}}} \left(a + p\mathbb{Z}_p\right).$$

This means that the subgroup $1 + p\mathbb{Z}_p$ of $\mathbb{Z}_p^\times$ has index $p - 1$, so

$$\mathrm{vol}_{dx}\left(\mathbb{Z}_p^\times\right) = (p-1)\mathrm{vol}_{dx}\left(p\mathbb{Z}_p\right) = \frac{p-1}{p}.$$

We define the *normalized multiplicative Haar measure* on $\mathbb{Q}_p$ by

$$d^\times x = \frac{p}{p-1}\frac{dx}{|x|_p}.$$

This Haar measure is determined by the property that the volume of the compact open subgroup $\mathbb{Z}_p^\times$ is one.

Self-duality

The group $\mathbb{R}$ is self-dual in the way that there is a character $\chi_0(x) = e^{2\pi i x}$ such that every character χ can be written as $\chi(x) = \chi_0(ax)$ for a unique $a \in \mathbb{R}$. Actually, the choice of χ_0 was arbitrary, so, given any non-trivial character ω, any character can uniquely be written as $x \mapsto \omega(ax)$. We will now find that $\mathbb{Q}_p$ is self-dual as well.

Theorem 13.2.3 (Self-duality of $\mathbb{Q}_p$). *Fix any non-trivial character $\omega \in \widehat{\mathbb{Q}_p}$. Then the map $\Phi : \mathbb{Q}_p \to \widehat{\mathbb{Q}_p}$, given by $\Phi(a) = \omega_a$, where $\omega_a(x) = \omega(ax)$, is an isomorphism of LCA groups.*

Proof The computation

$$\omega_{a+b}(x) = \omega(ax + bx) = \omega(ax)\omega(bx) = \omega_a(x)\omega_b(x)$$

shows that Φ is a group homomorphism. For injectivity, assume $\Phi(a) = 1$, then $\omega(ax) = 1$ for every $x \in \mathbb{Q}_p$ and as ω is non-trivial, this implies $a = 0$.

For surjectivity, we construct a standard character $\chi_0 : \mathbb{Q}_p \to \mathbb{T}$ and show that $\chi(x) = \chi_0(ax)$ for some $a \in \mathbb{Q}_p$. Since the same holds for ω we get $\omega(x) = \chi_0(bx)$ and as ω is non-trivial, it follows $b \neq 0$. Then we infer $\chi(x) = \chi_0(ax) = \chi_0(bb^{-1}ax) = \omega(b^{-1}ax)$. We use the power series representation of elements of $\mathbb{Q}_p$ to define χ_0 as follows

$$\chi_0\left(\sum_{k=-N}^{\infty} a_k p^k\right) = e^{2\pi i \sum_{k=-N}^{-1} a_k p^k}.$$

This is easily seen to be a character with $\chi_0(\mathbb{Z}_p) = 1$ and $\chi_0\left(p^{-N}\right) = e^{2\pi i p^{-N}}$. Let now χ be any character. By continuity, there exists $k \in \mathbb{Z}$ such that the open subgroup $p^k\mathbb{Z}_p$ is mapped into the open unit-neighborhood $\{\mathrm{Re}(z) > 0\}$ in $\mathbb{T}$. The latter set contains only one subgroup of $\mathbb{T}$, the trivial group. So we get $\chi\left(p^k\mathbb{Z}_p\right) = 1$. Replacing $\chi(x)$ with $\chi(p^k x)$, we can assume $\chi(\mathbb{Z}_p) = 1$. Let $N \in \mathbb{N}$. Then we have $\chi\left(p^{-N}\right)^{p^N} = 1$, so there are uniquely determined coefficients $a_k \in \{0, \dots, p-1\}$, such that

$$\chi\left(p^{-N}\right) = e^{2\pi i \left(\sum_{k=0}^{N-1} a_k p^k\right) p^{-N}}.$$

Since $\chi(p^{-N}) = \chi\left(p^{-(N+1)}p\right) = \chi\left(p^{-(N+1)}\right)^p$, these coefficients do not depend on N, so there is a number $a = \sum_{k=0}^{\infty} a_k p^k$ in $\mathbb{Z}_p$ with $\chi(p^{-N}) = \chi_0(ap^{-N})$ for every $N \in \mathbb{N}$. We apply this to varying N to conclude

$$\begin{aligned}\chi\left(\sum_{k=-N}^{\infty} a_k p^k\right) &= \chi\left(\sum_{k=-N}^{-1} a_k p^k\right) = \prod_{k=-N}^{-1} \chi(a_k p^k) = \prod_{k=-N}^{-1} \chi(p^k)^{a_k} \\ &= \prod_{k=-N}^{-1} \chi_0(ap^k)^{a_k} = \prod_{k=-N}^{-1} \chi_0(aa_k p^k) = \chi_0\left(a \sum_{k=-N}^{\infty} a_k p^k\right).\end{aligned}$$

To establish continuity of ϕ, recall that the topology of $\widehat{\mathbb{Q}_p}$ is the topology of the structure space of $L^1(\mathbb{Q}_p)$. So it suffices to show that the map $a \mapsto \hat{f}(\omega_a)$ is continuous for every $f \in L^1(\mathbb{Q}_p)$. This map, however, is $\hat{f}(\omega_a) = \int_{\mathbb{Q}_p} f(x)\overline{\omega(ax)}\,dx$, and is seen to be continuous by means of the Theorem on Dominated Convergence, as for a sequence $a_j \to a$ the sequence $\hat{f}(\omega_{a_j})$ converges dominatedly to $\hat{f}(\omega_a)$.

The continuity of the inverse map follows from the Open Mapping Theorem 4.2.10. □

13.3 Adeles and Ideles

In this section, we compose all the completions $\mathbb{Q}_p$ to a big ring, called the adele ring, which contains number theoretical information on all primes. The naive idea would be to simply take the product of all $\mathbb{Q}_p$. This, however, will not give a locally compact space, as we show in the first section. The construction has to be refined to the so-called restricted product.

Restricted Products

By the Theorem of Tychonov, direct products of compact spaces are compact. For "locally compact", this does not hold in general, as Lemma 1.8.10 shows. Let $(X_i)_{i\in I}$ be a family of locally compact spaces and for each $i \in I$ let there be given a compact open subset $K_i \subset X_i$. Define the *restricted product* as

$$X = \widehat{\prod_{i\in I}}^{K_i} X_i := \left\{ x \in \prod_{i\in I} X_i : x_i \in K_i \text{ for almost all } i \in I \right\}$$
$$= \bigcup_{\substack{E\subset I\\ \text{finite}}} \left\{ \prod_{i\in E} X_i \times \prod_{i\notin E} K_i . \right\}$$

If it is clear, which sets K_i to take, one leaves them out of the notation and simply writes $X = \widehat{\prod}_{i\in I} X_i$.

On the restricted product we introduce the *restricted product topology* as follows. A *restricted open rectangle* is a subset of the restricted product of the form $\prod_{i\in E} U_i \times \prod_{i\notin E} K_i$, where $E \subset I$ is a finite subset and for each $i \in E$ the set $U_i \subset X_i$ is an arbitrary open subset of X_i. A subset $A \subset \widehat{\prod}_{i\in I} X_i$ is called open, if it can be written as a union of restricted open rectangles. Note that the intersection of two restricted open rectangles is again a restricted open rectangle, since the sets K_i have been assumed to be open.

Lemma 13.3.1 (a) *If I is finite, then $\prod_i X_i = \widehat{\prod}_i X_i$ and the restricted product topology is the usual product topology.*

(b) *For every disjoint decomposition of the index set $I = A \dot{\cup} B$ one has a homeomorphism*

$$\widehat{\prod}_{i\in I} X_i \cong \left(\widehat{\prod}_{i\in A} X_i\right) \times \left(\widehat{\prod}_{i\in B} X_i\right).$$

(c) *The inclusion map $\widehat{\prod}_i X_i \hookrightarrow \prod_i X_i$ is continuous, but the restricted product topology only equals the subspace topology, if $X_i = K_i$ for almost all $i \in I$.*

(d) *If all the spaces X_i are locally compact, then so is $X = \widehat{\prod}_i X_i$.*

Proof (a) is trivial. For (b) note that both sides of the equation describe the same set. The definition of the restricted product topology implies that the left hand side carries the product topology of the two factors on the right.

(c) For continuity we have to show that the pre-image of a set of the form $\prod_{i\in E} U_i \times \prod_{i\notin E} X_i$ is open in $\widehat{\prod}_i X_i$, where $E \subset I$ is a finite subset and every $U_i \subset X_i$ is open. This follows from (a) and (b). The second assertion is clear.

We finally show (d). Let $x \in X$. Then there exists a finite set $E \subset I$ such that $x_i \in K_i$, if $i \notin E$. For every $i \in E$ choose a compact neighborhood U_i of x_i. Then $\prod_{i\in E} U_i \times \prod_{i\notin E} K_i$ is a compact neighborhood of x, so X is locally compact. $\square$

Adeles

By a *place* of $\mathbb{Q}$ we either mean a prime number or ∞, the latter we call the *infinite place*. Write $p < \infty$, if p is a prime and $p \le \infty$ if p is an arbitrary place. This manner of speaking comes from algebraic geometry, as these "places" behave in many ways like points on a curve. We write $\mathbb{Q}_\infty = \mathbb{R}$.

The set of *finite adeles* is the restricted product

$$\mathbb{A}_{\text{fin}} = \widehat{\prod_{p<\infty}}^{\mathbb{Z}_p} \mathbb{Q}_p.$$

The set of *adeles* is the set $\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{R}$. We also write $\mathbb{A} = \widehat{\prod}_{p\le\infty} \mathbb{Q}_p$, although this is not a restricted product, as there is no restriction at the infinite place. For an arbitrary set of places S we write $\mathbb{A}_S = \widehat{\prod}_{p\in S} \mathbb{Q}_p$ and $\mathbb{A}^S = \widehat{\prod}_{p\notin S} \mathbb{Q}_p$. Note that $\mathbb{A} = \mathbb{A}_S \times \mathbb{A}^S$.

Theorem 13.3.2

(a) *For every set of places S the ring $\mathbb{A}_S$ is a locally compact topological ring.*

(b) *The set* $\mathbb{Q}$, *embedded diagonally into* $\mathbb{A}$, *is a discrete subgroup and the quotient of abelian groups* $\mathbb{A}/\mathbb{Q}$ *is compact.*

(c) $\mathbb{Q}$ *is dense in* $\mathbb{A}_{\text{fin}}$.

Proof The space $\mathbb{A}_S$ is locally compact by Lemma 13.3.1. For (a) we have to show that addition and multiplication are continuous maps from $\mathbb{A}_S \times \mathbb{A}_S$ to $\mathbb{A}_S$. We only show this for addition, as the proof for multiplication is analogous. Let $a, b \in \mathbb{A}_S$ and let U be an open neighborhood of $a + b$. We have to show that there are open neighborhoods V, W of a and b such that $V + W \subset U$. Choosing U smaller, we can assume that $U = \prod_{p \in E} U_p \times \prod_{p \in S \smallsetminus E} \mathbb{Z}_p$ for a finite set $E \subset S$. For given $p \in E$ the addition is continuous on $\mathbb{Q}_p$, so there are open neighborhoods $V_p, W_p \subset \mathbb{Q}_p$ of a_p and b_p, such that $V_p + W_p \subset U_p$. Set $V = \prod_{p \in E} V_p \times \prod_{p \in S \smallsetminus E} \mathbb{Z}_p$ and $W = \prod_{p \in E} W_p \times \prod_{p \in S \smallsetminus E} \mathbb{Z}_p$. Then V and W are open neighborhoods of a and b, and one has $V + W \subset U$ as claimed.

For part (b) let $U = \left(-\frac{1}{2}, \frac{1}{2}\right) \times \prod_{p<\infty} \mathbb{Z}_p$. The set U is an open neighborhood of zero in $\mathbb{A}$. For $r \in \mathbb{Q} \cap U$ one has $|r|_p \le 1$ for every $p < \infty$ and therefore $r \in \mathbb{Z}$. Further one has $|r|_\infty < \frac{1}{2}$ and so $r = 0$. We have thus found an open neighborhood of zero with $U \cap \mathbb{Q} = \{0\}$. As $\mathbb{Q}$ is a subgroup of the additive group $\mathbb{A}$, it is discrete in $\mathbb{A}$. For compactness it suffices to show, that the compact set $K = [0, 1] \times \prod_{p<\infty} \mathbb{Z}_p$ contains a set of representatives of $\mathbb{A}/\mathbb{Q}$, because then the projection $P : K \to \mathbb{A}/\mathbb{Q}$ is surjective, so $\mathbb{A}/\mathbb{Q}$ is the continuous image of a compact set, hence compact.

So let $x \in \mathbb{A}$. There is a finite set E of places with $\infty \in E$, such that $p \notin E \Rightarrow x_p \in \mathbb{Z}_p$. For $p \in E$ with $p < \infty$ we write $x_p = \sum_{j=-N}^{\infty} a_j p^j$. Then

$$x_p - \underbrace{\sum_{j=-N}^{-1} a_j p^j}_{=r \in \mathbb{Q}} \in \mathbb{Z}_p.$$

For a prime $q \neq p$ one has $|r|_q = \left|\sum_{j=-N}^{-1} a_j p^j\right|_q \le \max\{|a_j p^j|_q\} \le 1$. We replace x by $x - r$ and thus reduce E to $E \smallsetminus \{p\}$. Repeating this argument, we end up with $E = \{\infty\}$, so $x_p \in \mathbb{Z}_p$ for every prime number p. This means that $x \in \mathbb{R} \times \prod_{p<\infty} \mathbb{Z}_p$. Modulo $\mathbb{Z}$ one can move x to $[0, 1] \times \prod_{p<\infty} \mathbb{Z}_p = K$.

Note that the above argument implies in particular that $\mathbb{A}_{\text{fin}} = \mathbb{Q} + \widehat{\mathbb{Z}}$ for $\widehat{\mathbb{Z}} = \prod_{p<\infty} \mathbb{Z}_p$. Hence, for (c) it suffices to show that $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$. We have to show that $\mathbb{Z}$ meets every open subset of $\widehat{\mathbb{Z}}$. Every such set is a union of sets of the form $U = \prod_{p \in E} B_p \times \prod_{p \notin E} \mathbb{Z}_p$, where E is a finite set of places and every B_p is an open ball in $\mathbb{Z}_p$. This means that B_p is of the form $B_p = n_p + p^{k_p}\mathbb{Z}_p$ for some $n_p \in \mathbb{Z}$ and some $k_p \in \mathbb{N}_0$. We have to show that there is $l \in \mathbb{Z}$, such that for every $p \in E$ one has $l \in n_p + p^{k_p}\mathbb{Z}_p$, or $l \equiv n_p \mod p^{k_p}$. The existence of such l is a consequence of the Chinese Remainder Theorem. $\square$

The ring $\mathbb{A}$ is locally compact, so in particular a locally compact group with respect to addition, so there is an additive Haar measure dx on $\mathbb{A}$. To describe it, we need the following definition.

Definition A *simple function* f on $\mathbb{A}$ is a function of the form $f = \prod_{p\le\infty} f_p$ with $f_p = \mathbf{1}_{\mathbb{Z}_p}$ for almost all p. Likewise, a *simple function* on $\mathbb{A}_{\mathrm{fin}}$ is a function of the form $f = \prod_{p<\infty} f_p$ with $f_p = \mathbf{1}_{\mathbb{Z}_p}$ for almost all p.

Theorem 13.3.3 *The Haar measure dx on $(\mathbb{A}, +)$ can be chosen such that for every integrable simple function $f = \prod_p f_p$ one has the product formula*

$$\int_{\mathbb{A}} f(x)\,dx = \prod_p \int_{\mathbb{Q}_p} f_p(x_p)\,dx_p.$$

The Haar measure dx_p on *$\mathbb{Q}_p$ is normalized such that* $\mathrm{vol}(\mathbb{Z}_p) = 1$ for $p < \infty$ *and dx_∞ equals the Lebesgue measure. The product is alway finite, i.e., almost all factors are equal to* 1,

This theorem also holds for $\mathbb{A}_S$ for an arbitrary set of places S. In the sequel, we will always use the normalization of the theorem.

Proof Since $\mathbb{A} = \mathbb{A}_{\mathrm{fin}} \times \mathbb{R}$, any Haar measure on $\mathbb{A}$ is a product of the Lebesgue measure and some Haar measure on $\mathbb{A}_{\mathrm{fin}}$. It therefore suffices to show that the Haar measure on $\mathbb{A}_{\mathrm{fin}}$ can be normalized in a way that for every simple function f on $\mathbb{A}_{\mathrm{fin}}$ one has

$$\int_{\mathbb{A}_{\mathrm{fin}}} f(x)\,dx = \prod_p \int_{\mathbb{Q}_p} f_p(x_p)\,dx_p.$$

Lemma 13.3.4 *Let $f \in C_c(\mathbb{A}_{\mathrm{fin}})$ be a continuous function with compact support. Then there is a compact subset $K \subseteq \mathbb{A}_{\mathrm{fin}}$ and a sequence of simple functions* (f_n) on *$\mathbb{A}_{\mathrm{fin}}$ with supports in K which converges uniformly to f.*

Proof Let L be the support of f. Since f is uniformly continuous, we find a neighborhood U_n of zero of the form $\prod_{p<\infty} B_p$ with $B_p = p^{k_p}\mathbb{Z}_p$ for all $p < \infty$ with $k_p \in \mathbb{Z}$ for all p and $k_p = 0$ for almost all p such that $|f(x+y) - f(x)| < \frac{1}{n}$ for all $x \in \mathbb{A}_{\mathrm{fin}}$ and $y \in U_n$. Then U_n is a compact open subgroup of $\mathbb{A}_{\mathrm{fin}}$, so L can be covered by a disjoint union of a finite number of translates of U_n, so $L \subset \coprod_{i=1}^{l} (x_i + U_n)$ for suitable $x_i \in K$. Define $g_n(x) = f(x_i)$ if $x \in x_i + U_n$. Then $\mathrm{supp}\, g_n \subseteq \mathrm{supp} f + U_n$ and $\|f - g_n\|_{\mathbb{A}_{\mathrm{fin}}} \le \frac{1}{n}$. Doing this construction for all n and taking care that $U_{n+1} \subseteq U_n$ for all n, we obtain the desired sequence (g_n). □

Proof of Theorem 13.3.3 If $f \in C_c(A_{\mathrm{fin}})$ choose a sequence (f_n) of simple functions as in the lemma. Then it is easy to check that $\left(\int_{\mathbb{A}_{\mathrm{fin}}} f_n(x)\,dx\right)$ is a Cauchy sequence in $\mathbb{C}$, and that the limit

$$\int_{\mathbb{A}} f(x)\,dx := \lim_n \int_{\mathbb{A}} f_n(x)\,dx$$

does not depend on the chosen sequence. Then $\int_{\mathbb{A}} : C_c(\mathbb{A}) \to \mathbb{C}$ is a positive Radon integral which is left invariant, since it is left invariant on the set of simple functions. □

We will finally show that $\mathbb{A}$ is self-dual as well. For this let χ be a character of the LCA-group $\mathbb{A}$. For $p \le \infty$, we define the character χ_p of $\mathbb{Q}_p$ as the composition $\mathbb{Q}_p \hookrightarrow \mathbb{A} \xrightarrow{\chi} \mathbb{T}$. If p is a prime, we say that χ_p is *unramified*, if $\chi_p(\mathbb{Z}_p) = 1$.

Lemma 13.3.5 *For almost all p, the character χ_p is unramified. For an adele a one has $\chi(a) = \prod_{p\le\infty} \chi_p(a_p)$, where the product is finite, i.e., almost all factors are equal to one.*

Proof As χ is continuous, there exists a unit-neighborhood U in $\mathbb{A}$ such that $\chi(U) \subset \{\mathrm{Re}(z) > 0\}$. Then U contains a restricted open rectangle, therefore U contains $\mathbb{Z}_p$ for almost all p. The image $\chi(\mathbb{Z}_p) = \chi_p(\mathbb{Z}_p)$ is a subgroup of $\mathbb{T}$ contained in $\{\mathrm{Re}(z) > 0\}$, hence trivial. So almost all χ_p are unramified. Finally, let $a \in \mathbb{A}$ and let S be a finite set of places outside which $a_p \in \mathbb{Z}_p$ and χ_p is unramified. This implies that outside S one has $\chi_p(a_p) = 1$. Let a_S be the product of all a_p with $p \in S$ and a^S the product of all a_p with $p \notin S$. Then $a = a_S a^S$ and we have $\chi(a^S) = 1$ as well as $\chi(a_S) = \prod_{p\in S} \chi_p(a_p)$ as the product is finite. □

Definition We say that a character ω is *nowhere trivial*, if $\omega_p \neq 1$ for every $p \le \infty$.

Theorem 13.3.6 (Self-duality of adeles). *There are characters ω* of $\mathbb{A}$ *which are nowhere trivial. For any such, the map $\Phi : \mathbb{A} \to \widehat{\mathbb{A}}$ given by $\Phi(a) = \omega_a$ with $\omega_a(x) = \omega(ax)$ is an isomorphism of locally compact groups.*

Proof At each $p \le \infty$, fix a non-trivial character ω_p in a way that ω_p is unramified for almost all p. One can, for instance, choose ω_p to be the standard character used in the proof of Theorem 13.2.3, which was called χ_0 there. It is easy to verify that the prescription

$$\omega(a) = \prod_{p\le\infty} \omega_p(a_p)$$

defines a nowhere trivial character.

As in the case of $\mathbb{Q}_p$ in Theorem 13.2.3, we observe that Φ is a group homomorphism. For injectivity, let $a \in \mathbb{A}$ with $\Phi(a) = 1$. Then $\omega(ax) = 1$ for every $x \in \mathbb{A}$, which implies $\omega_p(a_p x_p) = 1$ for every $x_p \in \mathbb{Q}_p$, hence $a_p = 0$ and so $a = 0$.

To show surjectivity, let χ be a character. By the corresponding local result, for each $p \le \infty$, there exists a unique $a_p \in \mathbb{Q}_p$ with $\chi_p(x_p) = \omega_p(a_p x_p)$ for every $x_p \in \mathbb{Q}_p$. At places p, where χ and ω are both unramified, we get $a_p \in \mathbb{Z}_p$. Hence the a_p are the coordinates of an adele a and we have $\chi(x) = \omega(ax)$ for all $x \in \mathbb{A}$.

Continuity and openness follows exactly as in the proof of the corresponding result for $\mathbb{Q}_p$ in Theorem 13.2.3. $\square$

The ring of adeles $\mathbb{A}$ can be used to describe the dual group $\widehat{\mathbb{Q}}$ of the discrete additive group $\mathbb{Q}$. For this recall that $\mathbb{Q}$ imbeds diagonally into $\mathbb{A}$ as a discrete subgroup. Thus we obtain a short exact sequence

$$0 \to \mathbb{Q} \xrightarrow{\iota} \mathbb{A} \xrightarrow{q} \mathbb{A}/\mathbb{Q} \to 0$$

which dualizes to the short exact sequence

$$0 \to \mathbb{Q}^{\perp} \to \widehat{\mathbb{A}} \xrightarrow{\mathrm{res}} \widehat{\mathbb{Q}} \to 0$$

For each $p < \infty$ let $e_p : \mathbb{Q}_p \to \mathbb{T}$ denote the standard character given by

$$e_p\left(\sum_{k=-N}^{\infty} a_k p^k\right) = e^{2\pi i \sum_{k=-N}^{-1} a_k p^k}$$

and let $e_\infty : \mathbb{R} \to \mathbb{T}$ be the character $e_\infty(x) = e^{-2\pi i x}$. Then the character $\omega = \prod_{p \le \infty} e_p : \mathbb{A} \to \mathbb{T}$ is nowhere trivial and by Theorem 13.3.6 we have an isomorphism $\mathbb{A} \cong \widehat{\mathbb{A}}$ given by $a \mapsto \omega_a$ with $\omega_a(x) = \omega(xa)$. If we compose this with the restriction map $\mathrm{res} : \widehat{\mathbb{A}} \to \widehat{\mathbb{Q}}$ we obtain a surjective homomorphism $\phi : \mathbb{A} \to \widehat{\mathbb{Q}}$ by $a \mapsto \omega_a|_{\mathbb{Q}}$.

Theorem 13.3.7 *The kernel* $\ker\phi \subseteq \mathbb{A}$ *is precisely the image of* $\mathbb{Q}$ *under the diagonal embedding. Therefore* ϕ *factors through an isomorphism of topological groups* $\mathbb{A}/\mathbb{Q} \cong \widehat{\mathbb{Q}}$ *given by* $a + \mathbb{Q} \mapsto \omega_a|_{\mathbb{Q}}$.

Proof An element $a \in \mathbb{A}$ lies in the kernel of ϕ if and only if $a\mathbb{Q} \subseteq \ker\omega$ with $\omega = \prod_{p \le \infty} e_p$ as above. We first show that $\mathbb{Q} \subseteq \ker\omega$, which then implies that $\mathbb{Q} \subseteq \ker\phi$. For this let $x \in \mathbb{Q}$. Let E be the finite set of primes p such that $|x|_p > 1$ and for $p \in E$ let $x_p = \sum_{k=-N}^{\infty} a_k p^k$ denote the p-adic expansion of x and let $r_p := \sum_{k=-N}^{-1} a_k p^k \in \mathbb{Q}$. Then $|r_p|_q \le \max_{k \le -1} |a_k p^k|_q \le 1$ for all $q \ne p$ and therefore $r_p \in \ker e_q$ for all primes $q \ne p$. It follows that

$$\omega(x - r_p) = \omega(x) e_\infty\left(-r_p\right) e_p\left(-r_p\right) = \omega(x) e^{-2\pi i r_p} e^{2\pi i r_p} = \omega(x).$$

Thus, replacing x by $x + \sum_{p \in E} r_p$, we may assume without loss of generality that $|x_p|_p \le 1$ for all $p < \infty$. But this implies that $x \in \mathbb{Z}$, hence $x_p \in \ker e_p$ for all $p \le \infty$ and $\omega(x) = 1$.

Assume now that $a \in \mathbb{A}$ such that $\omega(ax) = 1$ for all $x \in \mathbb{Q}$. We need to show that $a \in \mathbb{Q}$. Let E be the finite set of primes p with $|a_p|_p = p^{k_p} > 1$. By passing from a to $a' = a \cdot \prod_{p \in E} p^{k_p}$ if necessary we may assume that $E = \emptyset$, hence $|a_p|_p \le 1$ for all $p < \infty$. It follows that $a_p \in \ker e_p$ for all $p \le \infty$ and $1 = \omega(a) = e_\infty(a_\infty)$, hence $a_\infty \in \mathbb{Z}$. Writing $a_\infty = \pm p_1^{k_1} \cdots p_l^{k_l}$ with $k_1, \ldots, k_l \ge 0$ and after passing to

$a'' = a \cdot (\pm p_1^{-k_1} \cdots p_l^{-k_l})$ we may even assume that $a_\infty = 1$. (Note that multiplication of a with $p_i^{-k_i}$ only alters the norm of a_{p_i}. But since $1 = e_\infty(a_\infty \cdot p_i^{-k_i})$ and $1 = \omega\left(a \cdot p_i^{-k_i}\right) = e_\infty\left(a_\infty \cdot p_i^{-k_i}\right) \cdot e_{p_i}\left(a_p \cdot p_i^{-k_i}\right)$ we still have $|a_{p_i} \cdot p_i^{-k_i}|_{p_i} \leq 1$, hence $|a''_p|_p \leq 1$ for all $p < \infty$.)

After these reductions we need to show that $a_p = 1$ for all $p < \infty$. To see this let $a_p = \sum_{k=0}^{\infty} b_k p^k$. We need to show that $b_0 = 1$ and $b_k = 0$ for all $k > 0$. To see this we consider for all $l \in \mathbb{N}$

$$\begin{aligned} 1 = \omega\left(a \cdot p^{-l}\right) &= e_\infty\left(p^{-k}\right) e_p\left(\sum_{k=0}^{l} b_k p^{k-l}\right) \\ &= \exp\left(\frac{2\pi i}{p^l}\left((b_0 - 1) + \sum_{k=1}^{l-1} b_k p^k\right)\right) \end{aligned}$$

which is only possible if $b_0 = 1$ and $b_k = 0$ for all $1 \leq k < l$. Since l is arbitrary, the result follows. □

Ideles

The group $\mathbb{A}^\times$ of invertible elements of the adele ring $\mathbb{A}$ can be described as follows

$$\mathbb{A}^\times = \left\{ a \in \mathbb{A} : \begin{array}{l} a_p \neq 0 \ \forall p \leq \infty \\ |a_p|_p = 1 \text{ for almost all } p \end{array} \right\}.$$

Equipping $\mathbb{A}^\times$ with the subspace topology makes the multiplication continuous, but not the map $x \mapsto x^{-1}$. In order to make $\mathbb{A}^\times$ a topological group, we need more open sets. We have to insist, that with each open set U, the set $U^{-1} = \{u^{-1} : u \in U\}$ is open as well. The topology of $\mathbb{A}$ is generated by all sets of the form $\prod_{p \in E} U_p \times \prod_{p \notin E} \mathbb{Z}_p$, where E is a finite set of places and U_p is open in $\mathbb{Q}_p$ for every $p \in E$. The subspace topology of $\mathbb{A}^\times$ therefore is generated by all sets of the form

$$U = \left\{ a \in \mathbb{A}^\times : \begin{array}{c} a_p \in U_p, \ p \in E \\ |a_p| \leq 1, p \notin E \end{array} \right\},$$

where we can insist, that every U_p lies in $\mathbb{Q}_p^\times$. So we have to ask that sets of the form

$$U^{-1} = \left\{ a \in \mathbb{A}^\times : \begin{array}{c} a_p^{-1} \in U_p, \ p \in E \\ |a_p| \geq 1, p \notin E \end{array} \right\}$$

be open as well. This implies that the intersection of sets of the form U and another of the form $(U')^{-1}$ be open. Such intersections are of the form

$$W = \left\{ a \in \mathbb{A}^\times : \begin{array}{c} a_p \in W_p, \ p \in E \\ |a_p| = 1, p \notin E \end{array} \right\},$$

where W_p is any open subset of $\mathbb{Q}_p^\times$. On the other hand, sets of the form U or U^{-1} above can be written as unions of sets of the form W.

Lemma 13.3.8 *The coarsest topology on $\mathbb{A}^\times$, which contains the subspace topology of $\mathbb{A}$ and makes $\mathbb{A}^\times$ a topological group is the topology generated by all sets of the form W above with W_p any open set in $\mathbb{Q}_p^\times$. This topology is a restricted product topology, i.e., one can write $\mathbb{A}^\times$ as restricted product*

$$\mathbb{A}^\times = \left(\widehat{\prod_{p<\infty}}^{\mathbb{Z}_p^\times} \mathbb{Q}_p^\times \right) \times \mathbb{R}^\times.$$

With this topology, $\mathbb{A}^\times$ is a locally compact group, called the idele group of $\mathbb{Q}$. The elements are referred to as ideles.

Proof This is clear by what we have said above. □

Definition The *absolute value of an idele* $a \in \mathbb{A}^\times$ is defined as $|a| = \prod_p |a_p|_p$. This product is well defined, since almost all factors are equal to 1. We extend the definition to all of $\mathbb{A}$ by setting $|a| = 0$, if $a \in \mathbb{A} \smallsetminus \mathbb{A}^\times$. Note that the identity $|a| = \prod_p |a_p|_p$ also holds in this case, if one interprets the product as $(|a_\infty|_\infty \lim_{N\to\infty} \prod_{p\le N} |a_p|_p)$. Let

$$\mathbb{A}^1 = \{a \in \mathbb{A}^\times : |a| = 1\}.$$

Proposition 13.1.4 says that $\mathbb{Q}^\times \subset \mathbb{A}^1$. Recall that we write

$$\widehat{\mathbb{Z}} = \prod_{p<\infty} \mathbb{Z}_p.$$

Then $\widehat{\mathbb{Z}}$ is a compact subring of $\mathbb{A}_{\text{fin}}$. Its unit group is $\widehat{\mathbb{Z}}^\times = \prod_{p<\infty} \mathbb{Z}_p^\times$.

Theorem 13.3.9 *The subgroup $\mathbb{Q}^\times$ is discrete in $\mathbb{A}^\times$, it lies in the closed subgroup $\mathbb{A}^1$, and the quotient $\mathbb{A}^1/\mathbb{Q}^\times$ is compact. More precisely, there is a canonical isomorphism*

$$\mathbb{A}^1/\mathbb{Q}^\times \;\cong\; \widehat{\mathbb{Z}}^\times.$$

The absolute value induces an isomorphism of topological groups: $\mathbb{A}^\times \cong \mathbb{A}^1 \times (0,\infty)$ given by $x \mapsto (\tilde{x}, |x|_\infty)$, where $\tilde{x} \in \mathbb{A}^1$ is defined by

$$\tilde{x}_p = \begin{cases} x_p & \text{if } p < \infty, \\ \frac{x_\infty}{|x|} & \text{if } p = \infty. \end{cases}$$

Further one has $\mathbb{A}^1 \cong \mathbb{A}_{\text{fin}}^\times \times \{\pm 1\}$.

Proof Choose $0 < \varepsilon < 1$ and set $U = (1-\varepsilon, 1+\varepsilon) \times \prod_{p<\infty} \mathbb{Z}_p^\times$. Then U is an open unit neighborhood in $\mathbb{A}^\times$. With $r \in \mathbb{Q} \cap U$ we get $|r|_p = 1$ for every prime number p, so $r \in \mathbb{Z}$ and $r^{-1} \in \mathbb{Z}$. We have $r \in (1-\varepsilon, 1+\varepsilon)$, so $r = 1$.

Consider the map $\eta : \prod_p \mathbb{Z}_p^\times \to \mathbb{A}^1/\mathbb{Q}^\times$ given by $x \mapsto (x, 1)\mathbb{Q}^\times$. We claim that η is an isomorphism of topological groups. The map η is a group homomorphism, and since the map $\prod_p \mathbb{Z}_p^\times \hookrightarrow \mathbb{A}^\times$ is continuous, η is continuous. The inverse map is given by $x = (x_{\text{fin}}, x_\infty) \mapsto \frac{1}{x_\infty} x_{\text{fin}}$, where we note, that for $x \in \mathbb{A}^1$ one has $x_\infty \in \mathbb{Q}^\times$.

We leave it as an exercise to check that the map $x \mapsto (\tilde{x}, |x|_\infty)$ gives an isomorphism $\mathbb{A}^\times \cong \mathbb{A}^1 \times (0, \infty)$. Finally, the map $\phi : \mathbb{A}_{\text{fin}}^\times \times \{\pm 1\} \to \mathbb{A}^1$ given by $\phi(a_{\text{fin}}, \varepsilon) = (a_{\text{fin}}, \varepsilon |a_{\text{fin}}|^{-1})$ is easily seen to be an isomorphism. □

Proposition 13.3.10 (a) *The set $\mathbb{A}_{\text{fin}}^\times$ is the disjoint union*

$$\mathbb{A}_{\text{fin}}^\times = \coprod_{q \in \mathbb{Q}_{>0}^\times} q \widehat{\mathbb{Z}}^\times.$$

The set $\widehat{\mathbb{Z}} \cap \mathbb{A}_{\text{fin}}^\times$ is the disjoint union

$$\widehat{\mathbb{Z}} \cap \mathbb{A}_{\text{fin}}^\times = \coprod_{k \in \mathbb{N}} k \widehat{\mathbb{Z}}^\times.$$

(b) *For every $s \in \mathbb{C}$ with* $\text{Re}(s) > 1$ *the integral $\int_{\widehat{\mathbb{Z}}} |x|^s \, d^\times x$ converges absolutely and equals the Riemann zeta function $\zeta(s)$. Here $d^\times x$ is the uniquely determined Haar measure on $\mathbb{A}_{\text{fin}}^\times$, which gives the compact open subgroup $\widehat{\mathbb{Z}}^\times$ the measure* 1. *We consider this measure also as a measure on $\mathbb{A}_{\text{fin}}$, which is zero outside $\mathbb{A}_{\text{fin}}^\times$.*

Proof For given $x \in \mathbb{A}_{\text{fin}}^\times$ the absolute value $|x|$ lies in $\mathbb{Q}_{>0}^\times$. Consider the element $|x|x \in \mathbb{A}_{\text{fin}}^\times$. Let p be a prime number. One has $x_p = p^k u$ for some $k \in \mathbb{Z}$ and some $u \in \mathbb{Z}_p^\times$. So one has $|x| = p^{-k} r$, where $r \in \mathbb{Q}$ is coprime to p. We infer that $||x|x_p|_p = 1$, so $|x|x \in \widehat{\mathbb{Z}}^\times$. With $q = |x|^{-1}$ we have $x \in q\widehat{\mathbb{Z}}^\times$. If $x \in \widehat{\mathbb{Z}}$ we have $k_p \geq 0$ for all p, which implies that $q \in \mathbb{Z}$. This concludes the proof of (a).

We use (a) to show (b) as follows

$$\begin{aligned} \int_{\widehat{\mathbb{Z}}} |x|^s \, d^\times x &= \sum_{k \in \mathbb{N}} \int_{k\widehat{\mathbb{Z}}^\times} |x|^s \, d^\times x \\ &= \sum_{k \in \mathbb{N}} \int_{\widehat{\mathbb{Z}}^\times} |kx|^s \, d^\times x = \sum_{k \in \mathbb{N}} k^{-s} \underbrace{\int_{\widehat{\mathbb{Z}}^\times} |x|^s \, d^\times x}_{=1}. \end{aligned}$$

The convergence follows from the convergence of the Dirichlet series $\zeta(s)$. □

13.4 Exercises

Exercise 13.1 For $a \in \mathbb{Q}_p$ and $r > 0$ let $B_r(a)$ be the open ball $B_r(a) = \{x \in \mathbb{Q}_p : |a - x|_p < r\}$. Show:

(a) If $b \in B_r(a)$, then $B_r(a) = B_r(b)$.

(b) Two open balls are either disjoint or one is contained in the other.

Exercise 13.2 Show that there is a canonical ring isomorphism $\mathbb{Q}_p \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Exercise 13.3 Show that $\sum_{j=-N}^{\infty} a_j p^j \mapsto \sum_{j=-N}^{\infty} a_j p^{-j}$, $0 \leq a_j < p$, defines a continuous map $\mathbb{Q}_p \to \mathbb{R}$. Is this a ring homomorphism? Describe its image.

Exercise 13.4 Let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ denote the circle group and let $\chi : \mathbb{Z}_p \to \mathbb{T}$ be a continuous group homomorphism, i.e., $\chi(a+b) = \chi(a)\chi(b)$.

Show that there exists $k \in \mathbb{N}$ with $\chi(p^k\mathbb{Z}_p) = 1$. It follows that χ factors through the finite group $\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$, so the image of χ is finite.
(Hint: Let $U = \{z \in \mathbb{T} : \mathrm{Re}(z) > 0\}$. Then U is an open neighborhood of the unit, so $\chi^{-1}(U)$ is an open neighborhood of zero.)

Exercise 13.5 Let $e_p : \mathbb{Q}_p \to \mathbb{T}$ be defined by

$$e_p\left(\sum_{j=-N}^{\infty} a_j p^j\right) = \exp\left(2\pi i \sum_{j=-N}^{-1} a_j p^j\right),$$

where $a_j \in \mathbb{Z}$ with $0 \leq a_j < p$. Show that e_p is a continuous group homomorphism.

Exercise 13.6 (For this exercise it helps to have some familiarity with number theory.) Let p be a prime number and let $\mathcal{O}$ be the polynomial ring $\mathbb{F}_p[t]$. As one can perform division with remainder, the ring $\mathcal{O}$ is a factorial principal domain. The prime ideals of $\mathcal{O}$ are the principal ideals of the form 0 or (η), where $\eta \neq 0$ is an irreducible polynomial in $\mathcal{O}$.

(a) For such η let $v_\eta : \mathcal{O} \to \mathbb{N}_0 \cup \{\infty\}$ be defined by $v_\eta(f) = \sup\{k : f \in (\eta^k)\}$. Show that $|f|_\eta = p^{-\deg(\eta)v_\eta(f)}$ defines an absolute value on the ring $\mathcal{O}$.

(b) Let $v_\infty(f) = -\deg(f)$. Show that $|f|_\infty = p^{-v_\infty(f)}$ is an absolute value.

(c) Prove the product formula $\prod_{\eta \leq \infty} |f|_\eta = 1$.

Exercise 13.7 (a) Show that the family $(N\widehat{\mathbb{Z}})_{N\in\mathbb{N}}$ is a neighborhood basis of zero in $\mathbb{A}_{\mathrm{fin}}$. That is, show that every $N\widehat{\mathbb{Z}}$ is a neighborhood of zero and that every zero neighborhood contains a set of the form $N\widehat{\mathbb{Z}}$ for some N.

(b) Show that the sets of the form $(1 + N\widehat{\mathbb{Z}}) \cap \widehat{\mathbb{Z}}^\times$, $N \in \mathbb{N}$ are a neighborhood basis of the unit 1 in $\mathbb{A}_{\mathrm{fin}}^\times$.

Exercise 13.8 Let p be a prime number, $n \in \mathbb{N}$ and let dx be the additive Haar measure on $\mathrm{M}_n(\mathbb{Q}_p)$, so

$$\int_{\mathrm{M}_n(\mathbb{Q}_p)} f(x)\,dx = \int_{\mathbb{Q}_p} \cdots \int_{\mathbb{Q}_p} f(x_{i,j})\,dx_{1,1} \cdots dx_{n,n}.$$

(a) Show that $\frac{dx}{|\det x|^n}$ is a left- and right-invariant Haar measure on the group $\mathrm{GL}_n(\mathbb{Q}_p)$. Conclude that the group $\mathrm{GL}_n(\mathbb{Q}_p)$ is unimodular.

(b) Show that the group $\mathrm{GL}_n(\mathbb{A})$ is unimodular.

Exercise 13.9 Let $n, N \in \mathbb{N}$ and let K_N be the set of all invertible $n \times n$ matrices g with entries in $\widehat{\mathbb{Z}}$ such that $g \equiv I \mod N$. Show

- K_N is a compact open subgroup of $\mathrm{GL}_n(\widehat{\mathbb{Z}})$,
- $K_N \subset K_d$ if $d|N$,
- the K_N form a neighborhood basis of the unit in $\mathrm{GL}_n(\widehat{\mathbb{Z}})$.

Exercise 13.10 Let U be a compact open subgroup of the locally compact group G. Show that for every $g \in G$ the set UgU/U is finite.

Exercise 13.11 Let G be a totally disconnected locally compact group. For a compact open subgroup U and a compact set K let $L(U, K)$ be the set of all functions $f : G \to \mathbb{C}$ with

- $\mathrm{supp} f \subset K$ and
- $f(ux) = f(x)$ for every $x \in G$ and every $u \in U$.

Further let $R(U, K)$ be the set of all functions $f : G \to \mathbb{C}$ with

- $\mathrm{supp} f \subset K$ and
- $f(xu) = f(x)$ for every $x \in G$ and every $u \in U$.

Show that in general one has $L(U, K) \neq R(U, K)$, but

$$\bigcup_{U,K} L(U, K) = \bigcup_{U,K} R(U, K).$$