Adeles

William Stein

November 26, 2015

Contents

Preface

??????????????????
- ????????
- ????????????
- ??????????????????????
- ???????????????????
- ????????????????????????????????

Chapter 1

Introduction

??????????????????
- ????????
- ????????????
- ??????????????????????
- ??????????????????
- ????????????????????????????????

Chapter 2

Valuations

The rest of this book is a partial rewrite of [Cas67] meant to make it more accessible. I have attempted to add examples and details of the implicit exercises and remarks that are left to the reader.

2.1 Valuations

Definition 2.1.1 (Valuation)**.** A *valuation* $|\cdot|$ on a field K is a function defined on K with values in $\mathbb{R}_{\geq 0}$ satisfying the following axioms:

(1) $|a| = 0$ if and only if $a = 0$,

(2) $|ab| = |a|\,|b|$, and

(3) there is a constant $C \geq 1$ such that $|1 + a| \leq C$ whenever $|a| \leq 1$.

The *trivial valuation* is the valuation for which $|a| = 1$ for all $a \neq 0$. We will often tacitly exclude the trivial valuation from consideration.

From (2) we have

$$|1| = |1| \cdot |1|\,,$$

so $|1| = 1$ by (1). If $w \in K$ and $w^n = 1$, then $|w| = 1$ by (2). In particular, the only valuation of a finite field is the trivial one. The same argument shows that $|-1| = |1|$, so

$$|-a| = |a| \qquad \text{all } a \in K.$$

Definition 2.1.2 (Equivalent)**.** Two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field are *equivalent* if there exists $c > 0$ such that

$$|a|_2 = |a|_1^c$$

for all $a \in K$.

Note that if $|\cdot|_1$ is a valuation, then $|\cdot|_2 = |\cdot|_1^c$ is also a valuation. Also, equivalence of valuations is an equivalence relation.

If $|\cdot|$ is a valuation and $C > 1$ is the constant from Axiom (3), then there is a $c > 0$ such that $C^c = 2$ (i.e., $c = \log(2)/\log(C)$). Then we can take 2 as constant for the equivalent valuation $|\cdot|^c$. Thus every valuation is equivalent to a valuation with $C = 2$. Note that if $C = 1$, e.g., if $|\cdot|$ is the trivial valuation, then we could simply take $C = 2$ in Axiom (3).

Proposition 2.1.3. *Suppose $|\cdot|$ is a valuation with $C \le 2$. Then for all $a, b \in K$ we have*

$$|a + b| \le |a| + |b| \qquad \textit{(triangle inequality).} \tag{2.1.1}$$

Proof. Suppose $a_1, a_2 \in K$ with $|a_1| \ge |a_2|$. Then $a = a_2/a_1$ satisfies $|a| \le 1$. By Axiom (3) we have $|1 + a| \le 2$, so multiplying by a_1 we see that

$$|a_1 + a_2| \le 2|a_1| = 2 \cdot \max\{|a_1|, |a_2|\}.$$

Also we have

$$|a_1 + a_2 + a_3 + a_4| \le 2 \cdot \max\{|a_1 + a_2|, |a_3 + a_4|\} \le 4 \cdot \max\{|a_1|, |a_2|, |a_3|, |a_4|\},$$

and inductively we have for any $r > 0$ that

$$|a_1 + a_2 + \cdots + a_{2^r}| \le 2^r \cdot \max |a_j|.$$

If n is any positive integer, let r be such that $2^{r-1} \le n \le 2^r$. Thenn

$$|a_1 + a_2 + \cdots + a_n| \le 2^r \cdot \max\{|a_j|\} \le 2n \cdot \max\{|a_j|\},$$

since $2^r \le 2n$. In particular,

$$|n| \le 2n \cdot |1| = 2n \qquad (\text{for } n > 0). \tag{2.1.2}$$

Applying (2.1.2) to $\left|\binom{n}{j}\right|$ and using the binomial expansion, we have for any $a, b \in K$ that

$$\begin{aligned}
|a + b|^n &= \left|\sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}\right| \\
&\le 2(n+1) \max_j \left\{\left|\binom{n}{j}\right| |a|^j \, |b|^{n-j}\right\} \\
&\le 2(n+1) \max_j \left\{2\binom{n}{j} |a|^j \, |b|^{n-j}\right\} \\
&\le 4(n+1) \max_j \left\{\binom{n}{j} |a|^j \, |b|^{n-j}\right\} \\
&\le 4(n+1)(|a| + |b|)^n.
\end{aligned}$$

Now take nth roots of both sides to obtain

$$|a+b| \leq \sqrt[n]{4(n+1)} \cdot (|a|+|b|).$$

We have by elementary calculus that

$$\lim_{n\to\infty} \sqrt[n]{4(n+1)} = 1,$$

so $|a+b| \leq |a|+|b|$. (The "elementary calculus": We instead prove that $\sqrt[n]{n} \to 1$, since the argument is the same and the notation is simpler. First, for any $n \geq 1$ we have $\sqrt[n]{n} \geq 1$, since upon taking nth powers this is equivalent to $n \geq 1^n$, which is true by hypothesis. Second, suppose there is an $\varepsilon > 0$ such that $\sqrt[n]{n} \geq 1+\varepsilon$ for all $n \geq 1$. Then taking logs of boths sides we see that $\frac{1}{n}\log(n) \geq \log(1+\varepsilon) > 0$. But $\log(n)/n \to 0$, so there is no such ε. Thus $\sqrt[n]{n} \to 1$ as $n \to \infty$.) □

Note that Axioms (1), (2) and Equation (2.1.1) imply Axiom (3) with $C = 2$. We take Axiom (3) instead of Equation (2.1.1) for the technical reason that we will want to call the square of the absolute value of the complex numbers a valuation.

Lemma 2.1.4. *Suppose $a, b \in K$, and $|\cdot|$ is a valuation on K with $C \leq 2$. Then*

$$\Big||a|-|b|\Big| \leq |a-b|\,.$$

(Here the big absolute value on the outside of the left-hand side of the inequality is the usual absolute value on real numbers, but the other absolute values are a valuation on an arbitrary field K.)

Proof. We have

$$|a| = |b+(a-b)| \leq |b|+|a-b|,$$

so $|a|-|b| \leq |a-b|$. The same argument with a and b swapped implies that $|b|-|a| \leq |a-b|$, which proves the lemma. □

2.2 Types of Valuations

We define two important properties of valuations, both of which apply to equivalence classes of valuations (i.e., the property holds for $|\cdot|$ if and only if it holds for a valuation equivalent to $|\cdot|$).

Definition 2.2.1 (Discrete)**.** A valuation $|\cdot|$ is *discrete* if there is a $\delta > 0$ such that for any $a \in K$

$$1-\delta < |a| < 1+\delta \implies |a| = 1.$$

Thus the absolute values are bounded away from 1.

To say that $|\cdot|$ is discrete is the same as saying that the set

$$G = \big\{\log|a| : a \in K, a \neq 0\big\} \subset \mathbb{R}$$

forms a discrete subgroup of the reals under addition (because the elements of the group G are bounded away from 0).

Proposition 2.2.2. *A nonzero discrete subgroup G of $\mathbb{R}$ is free on one generator.*

Proof. Since G is discrete there is a positive $m \in G$ such that for any positive $x \in G$ we have $m \leq x$. Suppose $x \in G$ is an arbitrary positive element. By subtracting off integer multiples of m, we find that there is a unique n such that

$$0 \leq x - nm < m.$$

Since $x - nm \in G$ and $0 < x - nm < m$, it follows that $x - nm = 0$, so x is a multiple of m. □

By Proposition 2.2.2, the set of $\log|a|$ for nonzero $a \in K$ is free on one generator, so there is a $c < 1$ such that $|a|$, for $a \neq 0$, runs precisely through the set

$$c^{\mathbb{Z}} = \{c^m : m \in \mathbb{Z}\}$$

(Note: we can replace c by c^{-1} to see that we can assume that $c < 1$).

Definition 2.2.3 (Order)**.** If $|a| = c^m$, we call $m = \mathrm{ord}(a)$ the *order* of a.

Axiom (2) of valuations translates into

$$\mathrm{ord}(ab) = \mathrm{ord}(a) + \mathrm{ord}(b).$$

Definition 2.2.4 (Non-archimedean)**.** A valuation $|\cdot|$ is *non-archimedean* if we can take $C = 1$ in Axiom (3), i.e., if

$$|a + b| \leq \max\big\{|a|, |b|\big\}. \tag{2.2.1}$$

If $|\cdot|$ is not non-archimedean then it is *archimedean*.

Note that if we can take $C = 1$ for $|\cdot|$ then we can take $C = 1$ for any valuation equivalent to $|\cdot|$. To see that (2.2.1) is equivalent to Axiom (3) with $C = 1$, suppose $|b| \leq |a|$. Then $|b/a| \leq 1$, so Axiom (3) asserts that $|1 + b/a| \leq 1$, which implies that $|a + b| \leq |a| = \max\{|a|, |b|\}$, and conversely.

We note at once the following consequence:

Lemma 2.2.5. *Suppose $|\cdot|$ is a non-archimedean valuation. If $a, b \in K$ with $|b| < |a|$, then $|a + b| = |a|$.*

Proof. Note that $|a+b| \leq \max\{|a|,|b|\} = |a|$, which is true even if $|b| = |a|$. Also,

$$|a| = |(a+b)-b| \leq \max\{|a+b|,|b|\} = |a+b|,$$

where for the last equality we have used that $|b| < |a|$ (if $\max\{|a+b|,|b|\} = |b|$, then $|a| \leq |b|$, a contradiction).

□

Definition 2.2.6 (Ring of Integers)**.** Suppose $|\cdot|$ is a non-archimedean absolute value on a field K. Then

$$\mathcal{O} = \{a \in K : |a| \leq 1\}$$

is a ring called the *ring of integers* of K with respect to $|\cdot|$.

Lemma 2.2.7. *Two non-archimedean valuations $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if they give the same $\mathcal{O}$.*

We will prove this modulo the claim (to be proved later in Section 3.1) that valuations are equivalent if (and only if) they induce the same topology.

Proof. Suppose suppose $|\cdot|_1$ is equivalent to $|\cdot|_2$, so $|\cdot|_1 = |\cdot|_2^c$, for some $c > 0$. Then $|c|_1 \leq 1$ if and only if $|c|_2^c \leq 1$, i.e., if $|c|_2 \leq 1^{1/c} = 1$. Thus $\mathcal{O}_1 = \mathcal{O}_2$.

Conversely, suppose $\mathcal{O}_1 = \mathcal{O}_2$. Then $|a|_1 < |b|_1$ if and only if $a/b \in \mathcal{O}_1$ and $b/a \notin \mathcal{O}_1$, so

$$|a|_1 < |b|_1 \iff |a|_2 < |b|_2. \tag{2.2.2}$$

The topology induced by $|\ |_1$ has as basis of open neighborhoods the set of open balls

$$B_1(z,r) = \{x \in K : |x-z|_1 < r\},$$

for $r > 0$, and likewise for $|\ |_2$. Since the absolute values $|b|_1$ get arbitrarily close to 0, the set $\mathcal{U}$ of open balls $B_1(z,|b|_1)$ also forms a basis of the topology induced by $|\ |_1$ (and similarly for $|\ |_2$). By (2.2.2) we have

$$B_1(z,|b|_1) = B_2(z,|b|_2),$$

so the two topologies both have $\mathcal{U}$ as a basis, hence are equal. That equal topologies imply equivalence of the corresponding valuations will be proved in Section 3.1. □

The set of $a \in \mathcal{O}$ with $|a| < 1$ forms an ideal $\mathfrak{p}$ in $\mathcal{O}$. The ideal $\mathfrak{p}$ is maximal, since if $a \in \mathcal{O}$ and $a \notin \mathfrak{p}$ then $|a| = 1$, so $|1/a| = 1/|a| = 1$, hence $1/a \in \mathcal{O}$, so a is a unit.

Lemma 2.2.8. *A non-archimedean valuation $|\cdot|$ is discrete if and only if $\mathfrak{p}$ is a principal ideal.*

Proof. First suppose that $|\cdot|$ is discrete. Choose $\pi \in \mathfrak{p}$ with $|\pi|$ maximal, which we can do since

$$S = \{\log |a| : a \in \mathfrak{p}\} \subset (-\infty, 1],$$

so the discrete set S is bounded above. Suppose $a \in \mathfrak{p}$. Then

$$\left|\frac{a}{\pi}\right| = \frac{|a|}{|\pi|} \leq 1,$$

so $a/\pi \in \mathcal{O}$. Thus

$$a = \pi \cdot \frac{a}{\pi} \in \pi\mathcal{O}.$$

Conversely, suppose $\mathfrak{p} = (\pi)$ is principal. For any $a \in \mathfrak{p}$ we have $a = \pi b$ with $b \in \mathcal{O}$. Thus

$$|a| = |\pi| \cdot |b| \leq |\pi| < 1.$$

Thus $\{|a| : |a| < 1\}$ is bounded away from 1, which is exactly the definition of discrete. □

Example 2.2.9. For any prime p, define the p-adic valuation $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ as follows. Write a nonzero $\alpha \in K$ as $p^n \cdot \frac{a}{b}$, where $\gcd(a, p) = \gcd(b, p) = 1$. Then

$$\left|p^n \cdot \frac{a}{b}\right|_p := p^{-n} = \left(\frac{1}{p}\right)^n.$$

This valuation is both discrete and non-archimedean. The ring $\mathcal{O}$ is the local ring

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q} : p \nmid b\right\},$$

which has maximal ideal generated by p. Note that $\operatorname{ord}(p^n \cdot \frac{a}{b}) = n$.

Exercise 2.2.10. Give an example of a non-archimedean valuation on a field that is not discrete.

We will use the following lemma later (e.g., in the proof of Corollary 3.2.4 and Theorem 2.3.2).

Lemma 2.2.11. *A valuation $|\cdot|$ is non-archimedean if and only if $|n| \leq 1$ for all n in the ring generated by 1 in K.*

Note that we cannot identify the ring generated by 1 with $\mathbb{Z}$ in general, because K might have characteristic $p > 0$.

Proof. If $|\cdot|$ is non-archimedean, then $|1| \leq 1$, so by Axiom (3) with $a = 1$, we have $|1 + 1| \leq 1$. By induction it follows that $|n| \leq 1$.

Conversely, suppose $|n| \leq 1$ for all integer multiples n of 1. This condition is also true if we replace $|\cdot|$ by any equivalent valuation, so replace $|\cdot|$ by one with

$C \leq 2$, so that the triangle inequality holds. Suppose $a \in K$ with $|a| \leq 1$. Then by the triangle inequality,

$$\begin{aligned} |1+a|^n &= |(1+a)^n| \\ &\leq \sum_{j=0}^{n} \left| \binom{n}{j} \right| |a|^j \\ &\leq 1 + 1 + \cdots + 1 = n+1. \end{aligned}$$

Now take nth roots of both sides to get

$$|1+a| \leq \sqrt[n]{n},$$

and take the limit as $n \to \infty$ to see that $|1+a| \leq 1$. This proves that one can take $C = 1$ in Axiom (3), hence that $|\cdot|$ is non-archimedean. □

2.3 Examples of Valuations

The archetypal example of an archimedean valuation is the absolute value on the complex numbers. It is essentially the only one:

Theorem 2.3.1 (Gelfand-Tornheim)**.** *Any field K with an archimedean valuation is isomorphic to a subfield of $\mathbb{C}$, the valuation being equivalent to that induced by the usual absolute value on $\mathbb{C}$.*

We do not prove this here as we do not need it. For a proof, see [Art59, pg. 45, 67].

There are many non-archimedean valuations. On the rationals $\mathbb{Q}$ there is one for every prime $p > 0$, the p-adic valuation, as in Example 2.2.9.

Theorem 2.3.2 (Ostrowski)**.** *The nontrivial valuations on $\mathbb{Q}$ are those equivalent to $|\cdot|_p$, for some prime p, and the usual absolute value $|\cdot|_\infty$.*

Remark 2.3.3. Before giving the proof, we pause with a brief remark about Ostrowski. According to

`http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Ostrowski.html`

Ostrowski was a Ukrainian mathematician who lived 1893–1986. Gautschi writes about Ostrowski as follows: "... you are able, on the one hand, to emphasise the abstract and axiomatic side of mathematics, as for example in your theory of general norms, or, on the other hand, to concentrate on the concrete and constructive aspects of mathematics, as in your study of numerical methods, and to do both with equal ease. *You delight in finding short and succinct proofs, of which you have given many examples* ..." [italics mine]

We will now give an example of one of these short and succinct proofs.

Proof. Suppose $|\cdot|$ is a nontrivial valuation on $\mathbb{Q}$.

Nonarchimedean case: Suppose $|c| \leq 1$ for all $c \in \mathbb{Z}$, so by Lemma 2.2.11, $|\cdot|$ is nonarchimedean. Since $|\cdot|$ is nontrivial, the set

$$\mathfrak{p} = \{a \in \mathbb{Z} : |a| < 1\}$$

is nonzero. Also $\mathfrak{p}$ is an ideal and if $|ab| < 1$, then $|a|\,|b| = |ab| < 1$, so $|a| < 1$ or $|b| < 1$, so $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}$. Thus $\mathfrak{p} = p\mathbb{Z}$, for some prime number p. Since every element of $\mathbb{Z}$ has valuation at most 1, if $u \in \mathbb{Z}$ with $\gcd(u, p) = 1$, then $u \notin \mathfrak{p}$, so $|u| = 1$. Let $\alpha = \log_{|p|} \frac{1}{p}$, so $|p|^\alpha = \frac{1}{p}$. Then for any r and any $u \in \mathbb{Z}$ with $\gcd(u, p) = 1$, we have

$$|up^r|^\alpha = |u|^\alpha\,|p|^{\alpha r} = |p|^{\alpha r} = p^{-r} = |up^r|_p\,.$$

Thus $|\cdot|^\alpha = |\cdot|_p$ on $\mathbb{Z}$, hence on $\mathbb{Q}$ by multiplicativity, so $|\cdot|$ is equivalent to $|\cdot|_p$, as claimed.

Archimedean case: By replacing $|\cdot|$ by a power of $|\cdot|$, we may assume without loss that $|\cdot|$ satisfies the triangle inequality. We first make some general remarks about any valuation that satisfies the triangle inequality. Suppose $a \in \mathbb{Z}$ is greater than 1. Consider, for any $b \in \mathbb{Z}$ the base-a expansion of b:

$$b = b_m a^m + b_{m-1} a^{m-1} + \cdots + b_0,$$

where

$$0 \leq b_j < a \qquad (0 \leq j \leq m),$$

and $b_m \neq 0$. Since $a^m \leq b$, taking logs we see that $m \log(a) \leq \log(b)$, so

$$m \leq \frac{\log(b)}{\log(a)}.$$

Let $M = \max\limits_{1 \leq d < a} |d|$. Then by the triangle inequality for $|\cdot|$, we have

$$\begin{aligned} |b| &\leq |b_m|\,|a|^m + \cdots + |b_1|\,|a| + |b_0| \\ &\leq M \cdot (|a|^m + \cdots + |a| + 1) \\ &\leq M \cdot (m+1) \cdot \max(1, |a|^m) \\ &\leq M \cdot \left(\frac{\log(b)}{\log(a)} + 1\right) \cdot \max\left(1, |a|^{\log(b)/\log(a)}\right), \end{aligned}$$

where in the last step we use that $m \leq \frac{\log(b)}{\log(a)}$. Setting $b = c^n$, for $c \in \mathbb{Z}$, in the above inequality and taking nth roots, we have

$$\begin{aligned} |c| &\leq \left(M \cdot \left(\frac{\log(c^n)}{\log(a)} + 1\right) \cdot \max(1, |a|^{log(c^n)/\log(a)})\right)^{1/n} \\ &= M^{1/n} \cdot \left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n} \cdot \max\left(1, |a|^{\log(c^n)/\log(a)}\right)^{1/n}. \end{aligned}$$

The first factor $M^{1/n}$ converges to 1 as $n \to \infty$, since $M \geq 1$ (because $|1| = 1$). The second factor is

$$\left(\frac{\log(c^n)}{\log(a)} + 1\right)^{1/n} = \left(n \cdot \frac{\log(c)}{\log(a)} + 1\right)^{1/n}$$

which also converges to 1, for the same reason that $n^{1/n} \to 1$ (because $\log(n^{1/n}) = \frac{1}{n}\log(n) \to 0$ as $n \to \infty$). The third factor is

$$\max\left(1, |a|^{\log(c^n)/\log(a)}\right)^{1/n} = \begin{cases} 1 & \text{if } |a| < 1, \\ |a|^{\log(c)/\log(a)} & \text{if } |a| \geq 1. \end{cases}$$

Putting this all together, we see that

$$|c| \leq \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right).$$

Our assumption that $|\cdot|$ is archimedean implies that there is $c \in \mathbb{Z}$ with $c > 1$ and $|c| > 1$. Then for all $a \in \mathbb{Z}$ with $a > 1$ we have

$$1 < |c| \leq \max\left(1, |a|^{\frac{\log(c)}{\log(a)}}\right), \tag{2.3.1}$$

so $1 < |a|^{\log(c)/\log(a)}$, so $1 < |a|$ as well (i.e., any $a \in \mathbb{Z}$ with $a > 1$ automatically satisfies $|a| > 1$). Also, taking the $1/\log(c)$ power on both sides of (2.3.1) we see that

$$|c|^{\frac{1}{\log(c)}} \leq |a|^{\frac{1}{\log(a)}}. \tag{2.3.2}$$

Because, as mentioned above, $|a| > 1$, we can interchange the roll of a and c to obtain the reverse inequality of (2.3.2). We thus have

$$|c| = |a|^{\frac{\log(c)}{\log(a)}}.$$

Letting $\alpha = \log(2) \cdot \log_{|2|}(e)$ and setting $a = 2$, we have

$$|c|^{\alpha} = |2|^{\frac{\alpha}{\log(2)} \cdot \log(c)} = \left(|2|^{\log_{|2|}(e)}\right)^{\log(c)} = e^{\log(c)} = c = |c|_{\infty}.$$

Thus for all integers $c \in \mathbb{Z}$ with $c > 1$ we have $|c|^{\alpha} = |c|_{\infty}$, which implies that $|\cdot|$ is equivalent to $|\cdot|_{\infty}$. □

Let k be any field and let $K = k(t)$, where t is transcendental. Fix a real number $c > 1$. If $p = p(t)$ is an irreducible polynomial in the ring $k[t]$, we define a valuation by

$$\left|p^a \cdot \frac{u}{v}\right|_p = c^{-\deg(p) \cdot a}, \tag{2.3.3}$$

where $a \in \mathbb{Z}$ and $u, v \in k[t]$ with $p \nmid u$ and $p \nmid v$.

Remark 2.3.4. This definition differs from the one page 46 of [Cassels-Frohlich, Ch. 2] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Also, we write $c^{-\deg(p)\cdot a}$ instead of c^{-a}, so that the product formula will hold. (For more about the product formula, see Section 7.1.)

In addition there is a a non-archimedean valuation $|\cdot|_\infty$ defined by

$$\left|\frac{u}{v}\right|_\infty = c^{\deg(u)-\deg(v)}. \tag{2.3.4}$$

This definition differs from the one in [Cas67, pg. 46] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Here's why: Recall that Axiom 3 for a non-archimedean valuation on K asserts that whenever $a \in K$ and $|a| \leq 1$, then $|a+1| \leq 1$. Set $a = p - 1$, where $p = p(t) \in K[t]$ is an irreducible polynomial. Then $|a| = c^0 = 1$, since $\mathrm{ord}_p(p-1) = 0$. However, $|a+1| = |p-1+1| = |p| = c^{-1} > 1$, since $\mathrm{ord}_p(p) = 1$. If we take $c > 1$ instead of $c < 1$, as I propose, then $|p| = c^{-1} < 1$, as required.

Note the (albeit imperfect) analogy between $K = k(t)$ and $\mathbb{Q}$. If $s = t^{-1}$, so $k(t) = k(s)$, the valuation $|\cdot|_\infty$ is of the type (2.3.3) belonging to the irreducible polynomial $p(s) = s$.

The reader is urged to prove the following lemma as a homework problem.

Lemma 2.3.5. *The only nontrivial valuations on $k(t)$ which are trivial on k are equivalent to the valuation (2.3.3) or (2.3.4).*

For example, if k is a finite field, there are no nontrivial valuations on k, so the only nontrivial valuations on $k(t)$ are equivalent to (2.3.3) or (2.3.4).

Exercise 2.3.6. Let k be any field. Prove that the only nontrivial valuations on $k(t)$ which are trivial on k are equivalent to the valuation (2.3.3) or (2.3.4) of page 17.

Chapter 3

Topology and Completeness

3.1 Topology

A valuation $|\cdot|$ on a field K induces a topology in which a basis for the neighborhoods of a are the *open balls*

$$B(a,d) = \{x \in K : |x-a| < d\}$$

for $d > 0$.

Lemma 3.1.1. *Equivalent valuations induce the same topology.*

Proof. If $|\cdot|_1 = |\cdot|_2^r$, then $|x-a|_1 < d$ if and only if $|x-a|_2^r < d$ if and only if $|x-a|_2 < d^{1/r}$ so $B_1(a,d) = B_2(a,d^{1/r})$. Thus the basis of open neighborhoods of a for $|\cdot|_1$ and $|\cdot|_2$ are identical. □

A valuation satisfying the triangle inequality gives a metric for the topology on defining the distance from a to b to be $|a-b|$. Assume for the rest of this section that we only consider valuations that satisfy the triangle inequality.

Lemma 3.1.2. *A field with the topology induced by a valuation is a* topological field*, i.e., the operations sum, product, and reciprocal are continuous.*

Proof. For example (product) the triangle inequality implies that

$$|(a+\varepsilon)(b+\delta) - ab| \le |\varepsilon|\,|\delta| + |a|\,|\delta| + |b|\,|\varepsilon|$$

is small when $|\varepsilon|$ and $|\delta|$ are small (for fixed a, b). □

Exercise 3.1.3. Prove the previous lemma, i.e., prove that the operations sum, product, and reciprocal are continuous.

Lemma 3.1.4. *Suppose two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field K induce the same topology. Then for any sequence $\{x_n\}$ in K we have*

$$|x_n|_1 \to 0 \iff |x_n|_2 \to 0.$$

Proof. It suffices to prove that if $|x_n|_1 \to 0$ then $|x_n|_2 \to 0$, since the proof of the other implication is the same. Let $\varepsilon > 0$. The topologies induced by the two absolute values are the same, so $B_2(0,\varepsilon)$ can be covered by open balls $B_1(a_i, r_i)$. One of these open balls $B_1(a,r)$ contains 0. There is $\varepsilon' > 0$ such that

$$B_1(0,\varepsilon') \subset B_1(a,r) \subset B_2(0,\varepsilon).$$

Since $|x_n|_1 \to 0$, there exists N such that for $n \geq N$ we have $|x_n|_1 < \varepsilon'$. For such n, we have $x_n \in B_1(0,\varepsilon')$, so $x_n \in B_2(0,\varepsilon)$, so $|x_n|_2 < \varepsilon$. Thus $|x_n|_2 \to 0$. □

Proposition 3.1.5. *If two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field induce the same topology, then they are equivalent in the sense that there is a positive real α such that $|\cdot|_1 = |\cdot|_2^{\alpha}$.*

Proof. If $x \in K$ and $i = 1, 2$, then $|x^n|_i \to 0$ if and only if $|x|_i^n \to 0$, which is the case if and only if $|x|_i < 1$. Thus Lemma 3.1.4 implies that $|x|_1 < 1$ if and only if $|x|_2 < 1$. On taking reciprocals we see that $|x|_1 > 1$ if and only if $|x|_2 > 1$, so finally $|x|_1 = 1$ if and only if $|x|_2 = 1$.

Let now $w, z \in K$ be nonzero elements with $|w|_i \neq 1$ and $|z|_i \neq 1$. On applying the foregoing to

$$x = w^m z^n \qquad (m, n \in \mathbb{Z})$$

we see that

$$m \log |w|_1 + n \log |z|_1 \geq 0$$

if and only if

$$m \log |w|_2 + n \log |z|_2 \geq 0.$$

Dividing through by $\log |z|_i$, and rearranging, we see that for every rational number $\alpha = -n/m$,

$$\frac{\log |w|_1}{\log |z|_1} \geq \alpha \iff \frac{\log |w|_2}{\log |z|_2} \geq \alpha.$$

Thus

$$\frac{\log |w|_1}{\log |z|_1} = \frac{\log |w|_2}{\log |z|_2},$$

so

$$\frac{\log |w|_1}{\log |w|_2} = \frac{\log |z|_1}{\log |z|_2}.$$

Since this equality does not depend on the choice of z, we see that there is a constant c $(= \log |z|_1 / \log |z|_2)$ such that $\log |w|_1 / \log |w|_2 = c$ for all w. Thus $\log |w|_1 = c \cdot \log |w|_2$, so $|w|_1 = |w|_2^c$, which implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$. □

3.2 Completeness

We recall the definition of metric on a set X.

Definition 3.2.1 (Metric)**.** A *metric* on a set X is a map

$$d : X \times X \to \mathbb{R}$$

such that for all $x, y, z \in X$,

1. $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$,
2. $d(x, y) = d(y, x)$, and
3. $d(x, z) \leq d(x, y) + d(y, z)$.

A *Cauchy sequence* is a sequence (x_n) in X such that for all $\varepsilon > 0$ there exists M such that for all $n, m > M$ we have $d(x_n, x_m) < \varepsilon$. The *completion* of X is the set of Cauchy sequences (x_n) in X modulo the equivalence relation in which two Cauchy sequences (x_n) and (y_n) are equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$. A metric space is *complete* if every Cauchy sequence converges, and one can show that the completion of X with respect to a metric is complete.

For example, $d(x, y) = |x - y|$ (usual archimedean absolute value) defines a metric on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to this metric is the field $\mathbb{R}$ of real numbers. More generally, whenever $|\cdot|$ is a valuation on a field K that satisfies the triangle inequality, then $d(x, y) = |x - y|$ defines a metric on K. Consider for the rest of this section only valuations that satisfy the triangle inequality.

Definition 3.2.2 (Complete)**.** A field K is *complete* with respect to a valuation $|\cdot|$ if given any Cauchy sequence a_n, $(n = 1, 2, \ldots)$, i.e., one for which

$$|a_m - a_n| \to 0 \qquad (m, n \to \infty, \infty),$$

there is an $a^* \in K$ such that

$$a_n \to a^* \qquad \text{w.r.t. } |\cdot|$$

(i.e., $|a_n - a^*| \to 0$).

Theorem 3.2.3. *Every field K with valuation $v = |\cdot|$ can be embedded in a complete field K_v with a valuation $|\cdot|$ extending the original one in such a way that K_v is the closure of K with respect to $|\cdot|$. Further K_v is unique up to a unique isomorphism fixing K.*

Proof. Define K_v to be the completion of K with respect to the metric defined by $|\cdot|$. Thus K_v is the set of equivalence classes of Cauchy sequences, and there is a natural injective map from K to K_v sending an element $a \in K$ to the constant Cauchy

sequence (a). Because the field operations on K are continuous, they induce well-defined field operations on equivalence classes of Cauchy sequences componentwise. Also, define a valuation on K_v by

$$|(a_n)_{n=1}^{\infty}| = \lim_{n\to\infty} |a_n|,$$

and note that this is well defined and extends the valuation on K.

To see that K_v is unique up to a unique isomorphism fixing K, we observe that there are no nontrivial continuous automorphisms $K_v \to K_v$ that fix K. This is because, by denseness, a continuous automorphism $\sigma : K_v \to K_v$ is determined by what it does to K, and by assumption σ is the identity map on K. More precisely, suppose $a \in K_v$ and n is a positive integer. Then by continuity there is $\delta > 0$ (with $\delta < 1/n$) such that if $a_n \in K_v$ and $|a - a_n| < \delta$ then $|\sigma(a) - \sigma(a_n)| < 1/n$. Since K is dense in K_v, we can choose the a_n above to be an element of K. Then by hypothesis $\sigma(a_n) = a_n$, so $|\sigma(a) - a_n| < 1/n$. Thus $\sigma(a) = \lim_{n\to\infty} a_n = a$. □

Corollary 3.2.4. *The valuation $|\cdot|$ is non-archimedean on K_v if and only if it is so on K. If $|\cdot|$ is non-archimedean, then the set of values taken by $|\cdot|$ on K and K_v are the same.*

Proof. The first part follows from Lemma 2.2.11 which asserts that a valuation is non-archimedean if and only if $|n| < 1$ for all integers n. Since the valuation on K_v extends the valuation on K, and all n are in K, the first statement follows.

For the second, suppose that $|\cdot|$ is non-archimedean (but not necessarily discrete). Suppose $b \in K_v$ with $b \neq 0$. First I claim that there is $c \in K$ such that $|b - c| < |b|$. To see this, let $c' = b - \frac{b}{a}$, where a is some element of K_v with $|a| > 1$, note that $|b - c'| = \left|\frac{b}{a}\right| < |b|$, and choose $c \in K$ such that $|c - c'| < |b - c'|$, so

$$|b - c| = \left|b - c' - (c - c')\right| \leq \max\left(\left|b - c'\right|, \left|c - c'\right|\right) = \left|b - c'\right| < |b|.$$

Since $|\cdot|$ is non-archimedean, we have

$$|b| = |(b - c) + c| \leq \max(|b - c|, |c|) = |c|,$$

where in the last equality we use that $|b - c| < |b|$. Also,

$$|c| = |b + (c - b)| \leq \max(|b|, |c - b|) = |b|,$$

so $|b| = |c|$, which is in the set of values of $|\cdot|$ on K. □

3.2.1 p-adic Numbers

This section is about the p-adic numbers $\mathbb{Q}_p$, which are the completion of $\mathbb{Q}$ with respect to the p-adic valuation. Alternatively, to give a p-adic *integer* in $\mathbb{Z}_p$ is the same as giving for every prime power p^r an element $a_r \in \mathbb{Z}/p^r\mathbb{Z}$ such that if $s \leq r$ then a_s is the reduction of a_r modulo p^s. The field $\mathbb{Q}_p$ is then the field of fractions of $\mathbb{Z}_p$.

Exercise 3.2.5. Prove that the field $\mathbb{Q}_p$ of p-adic numbers is uncountable.

We begin with the definition of the N-adic numbers for any positive integer N. Section 3.2.1 is about the N-adics in the special case $N = 10$; these are fun because they can be represented as decimal expansions that go off infinitely far to the left. Section 3.2.3 is about how the topology of $\mathbb{Q}_N$ is nothing like the topology of $\mathbb{R}$. Finally, in Section 3.2.4 we state the Hasse-Minkowski theorem, which shows how to use p-adic numbers to decide whether or not a quadratic equation in n variables has a rational zero.

The N-adic Numbers

Lemma 3.2.6. *Let N be a positive integer. Then for any nonzero rational number α there exists a unique $e \in \mathbb{Z}$ and integers a, b, with b positive, such that $\alpha = N^e \cdot \frac{a}{b}$ with $N \nmid a$, $\gcd(a, b) = 1$, and $\gcd(N, b) = 1$.*

Proof. Write $\alpha = c/d$ with $c, d \in \mathbb{Z}$ and $d > 0$. First suppose d is exactly divisible by a power of N, so for some r we have $N^r \mid d$ but $\gcd(N, d/N^r) = 1$. Then

$$\frac{c}{d} = N^{-r} \frac{c}{d/N^r}.$$

If N^s is the largest power of N that divides c, then $e = s - r$, $a = c/N^s$, $b = d/N^r$ satisfy the conclusion of the lemma.

By unique factorization of integers, there is a smallest multiple f of d such that fd is exactly divisible by N. Now apply the above argument with c and d replaced by cf and df. □

Definition 3.2.7 (N-adic valuation)**.** Let N be a positive integer. For any positive $\alpha \in \mathbb{Q}$, the *N-adic valuation* of α is e, where e is as in Lemma 3.2.6. The N-adic valuation of 0 is ∞.

We denote the N-adic valuation of α by $\mathrm{ord}_N(\alpha)$. (Note: Here we are using "valuation" in a different way than in the rest of the text. This valuation is not an absolute value, but the logarithm of one.)

Definition 3.2.8 (N-adic metric)**.** For $x, y \in \mathbb{Q}$ the *N-adic distance* between x and y is

$$d_N(x, y) = N^{-\mathrm{ord}_N(x-y)}.$$

We let $d_N(x, x) = 0$, since $\mathrm{ord}_N(x - x) = \mathrm{ord}_N(0) = \infty$.

For example, $x, y \in \mathbb{Z}$ are close in the N-adic metric if their difference is divisible by a large power of N. E.g., if $N = 10$ then 93427 and 13427 are close because their difference is 80000, which is divisible by a large power of 10.

Proposition 3.2.9. *The distance d_N on $\mathbb{Q}$ defined above is a metric. Moreover, for all $x, y, z \in \mathbb{Q}$ we have*

$$d(x,z) \leq \max(d(x,y), d(y,z)).$$

(This is the "nonarchimedean" triangle inequality.)

Proof. The first two properties of Definition 3.2.1 are immediate. For the third, we first prove that if $\alpha, \beta \in \mathbb{Q}$ then

$$\mathrm{ord}_N(\alpha+\beta) \geq \min(\mathrm{ord}_N(\alpha), \mathrm{ord}_N(\beta)).$$

Assume, without loss, that $\mathrm{ord}_N(\alpha) \leq \mathrm{ord}_N(\beta)$ and that both α and β are nonzero. Using Lemma 3.2.6 write $\alpha = N^e(a/b)$ and $\beta = N^f(c/d)$ with a or c possibly negative. Then

$$\alpha+\beta = N^e\left(\frac{a}{b} + N^{f-e}\frac{c}{d}\right) = N^e\left(\frac{ad+bcN^{f-e}}{bd}\right).$$

Since $\gcd(N, bd) = 1$ it follows that $\mathrm{ord}_N(\alpha+\beta) \geq e$. Now suppose $x, y, z \in \mathbb{Q}$. Then

$$x - z = (x-y) + (y-z),$$

so

$$\mathrm{ord}_N(x-z) \geq \min(\mathrm{ord}_N(x-y), \mathrm{ord}_N(y-z)),$$

hence $d_N(x,z) \leq \max(d_N(x,y), d_N(y,z))$. □

We can finally define the N-adic numbers.

Definition 3.2.10 (The N-adic Numbers)**.** The set of *N-adic numbers*, denoted $\mathbb{Q}_N$, is the completion of $\mathbb{Q}$ with respect to the metric d_N.

The set $\mathbb{Q}_N$ is a ring, but it need not be a field as you will show in Exercises 3.2.11 and **??**. It is a field if and only if N is prime. Also, $\mathbb{Q}_N$ has a "bizarre" topology, as we will see in Section 3.2.3.

Exercise 3.2.11. Let $N > 1$ be an integer.

1. Prove that $\mathbb{Q}_N$ is equipped with a natural ring structure.

2. If N is prime, prove that $\mathbb{Q}_N$ is a field.

Exercise 3.2.12.

1. Let p and q be distinct primes. Prove that $\mathbb{Q}_{pq} \cong \mathbb{Q}_p \times \mathbb{Q}_q$.

2. Is $\mathbb{Q}_{p^2}$ isomorphic to either of $\mathbb{Q}_p \times \mathbb{Q}_p$ or $\mathbb{Q}_p$?

The 10-adic Numbers

It's a familiar fact that every real number can be written in the form

$$d_n \dots d_1 d_0 . d_{-1} d_{-2} \dots = d_n 10^n + \cdots + d_1 10 + d_0 + d_{-1} 10^{-1} + d_{-2} 10^{-2} + \cdots$$

where each digit d_i is between 0 and 9, and the sequence can continue indefinitely to the right.

The 10-adic numbers also have decimal expansions, but everything is backward! To get a feeling for why this might be the case, we consider Euler's nonsensical series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$

One can prove (see Exercise **??**) that this series converges in $\mathbb{Q}_{10}$ to some element $\alpha \in \mathbb{Q}_{10}$.

Exercise 3.2.13. Let $N > 1$ be an integer. Prove that the series

$$\sum_{n=1}^{\infty} (-1)^{n+1} n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$

converges in $\mathbb{Q}_N$.

What is α? How can we write it down? First note that for all $M \geq 5$, the terms of the sum are divisible by 10, so the difference between α and $1! - 2! + 3! - 4!$ is divisible by 10. Thus we can compute α modulo 10 by computing $1! - 2! + 3! - 4!$ modulo 10. Likewise, we can compute α modulo 100 by compute $1! - 2! + \cdots + 9! - 10!$, etc. We obtain the following table:

α	$\bmod 10^r$
1	$\bmod 10$
81	$\bmod 10^2$
981	$\bmod 10^3$
2981	$\bmod 10^4$
22981	$\bmod 10^5$
422981	$\bmod 10^6$

Continuing we see that

$$1! - 2! + 3! - 4! + \cdots = \dots 637838364422981 \qquad \text{in } \mathbb{Q}_{10} \text{ !}$$

Here's another example. Reducing $1/7$ modulo larger and larger powers of 10 we see that

$$\frac{1}{7} = \dots 857142857143 \qquad \text{in } \mathbb{Q}_{10}.$$

Here's another example, but with a decimal point.

$$\frac{1}{70} = \frac{1}{10} \cdot \frac{1}{7} = \dots 85714285714.3$$

We have

$$\frac{1}{3} + \frac{1}{7} = \ldots 66667 + \ldots 57143 = \frac{10}{21} = \ldots 23810,$$

which illustrates that addition with carrying works as usual.

Fermat's Last Theorem in $\mathbb{Z}_{10}$

An amusing observation, which people often argued about on USENET news back in the 1990s, is that Fermat's last theorem is false in $\mathbb{Z}_{10}$. For example, $x^3 + y^3 = z^3$ has a nontrivial solution, namely $x = 1$, $y = 2$, and $z = \ldots 60569$. Here z is a cube root of 9 in $\mathbb{Z}_{10}$. Note that it takes some work to prove that there is a cube root of 9 in $\mathbb{Z}_{10}$ (see Exercise **??**).

Exercise 3.2.14. Prove that 9 has a cube root in $\mathbb{Q}_{10}$ using the following strategy (this is a special case of Hensel's Lemma, which you can read about in an appendix to Cassel's article).

1. Show that there is an element $\alpha \in \mathbb{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

2. Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbb{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbb{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b \cdot 10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

3. Conclude that 9 has a cube root in $\mathbb{Q}_{10}$.

3.2.2 The Field of p-adic Numbers

The ring $\mathbb{Q}_{10}$ of 10-adic numbers is isomorphic to $\mathbb{Q}_2 \times \mathbb{Q}_5$ (see Exercise **??**), so it is not a field. For example, the element $\ldots 8212890625$ corresponding to $(1, 0)$ under this isomorphism has no inverse. (To compute n digits of $(1, 0)$ use the Chinese remainder theorem to find a number that is 1 modulo 2^n and 0 modulo 5^n.)

If p is prime then $\mathbb{Q}_p$ is a field (see Exercise **??**). Since $p \neq 10$ it is a little more complicated to write p-adic numbers down. People typically write p-adic numbers in the form

$$\frac{a_{-d}}{p^d} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where $0 \leq a_i < p$ for each i.

Exercise 3.2.15. Compute the first 5 digits of the 10-adic expansions of the following rational numbers:

$$\frac{13}{2}, \quad \frac{1}{389}, \quad \frac{17}{19}, \quad \text{the 4 square roots of 41.}$$

3.2.3 The Topology of $\mathbb{Q}_N$ (is Weird)

Definition 3.2.16 (Connected)**.** Let X be a topological space. A subset S of X is *disconnected* if there exist open subsets $U_1, U_2 \subset X$ with $U_1 \cap U_2 \cap S = \emptyset$ and $S = (S \cap U_1) \cup (S \cap U_2)$ with $S \cap U_1$ and $S \cap U_2$ nonempty. If S is not disconnected it is *connected*.

The topology on $\mathbb{Q}_N$ is induced by d_N, so every open set is a union of open balls

$$B(x, r) = \{y \in \mathbb{Q}_N : d_N(x, y) < r\}.$$

Recall Proposition 3.2.9, which asserts that for all x, y, z,

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

This translates into the following shocking and bizarre lemma:

Lemma 3.2.17. *Suppose $x \in \mathbb{Q}_N$ and $r > 0$. If $y \in \mathbb{Q}_N$ and $d_N(x, y) \geq r$, then $B(x, r) \cap B(y, r) = \emptyset$.*

Proof. Suppose $z \in B(x, r)$ and $z \in B(y, r)$. Then

$$r \leq d_N(x, y) \leq \max(d_N(x, z), d_N(z, y)) < r,$$

a contradiction. □

You should draw a picture to illustrates Lemma 3.2.17.

Lemma 3.2.18. *The open ball $B(x, r)$ is also closed.*

Proof. Suppose $y \notin B(x, r)$. Then $r \leq d(x, y)$ so

$$B(y, d(x, y)) \cap B(x, r) \subset B(y, d(x, y)) \cap B(x, d(x, y)) = \emptyset.$$

Thus the complement of $B(x, r)$ is a union of open balls. □

Exercise 3.2.19. Prove that the polynomial $f(x) = x^3 - 3x^2 + 2x + 5$ has all its roots in $\mathbb{Q}_5$, and find the 5-adic valuations of each of these roots. (You might need to use Hensel's lemma, which we don't discuss in detail in this book. See [Cas67, App. C].)

The lemmas imply that $\mathbb{Q}_N$ is *totally disconnected*, in the following sense.

Proposition 3.2.20. *The only connected subsets of $\mathbb{Q}_N$ are the singleton sets $\{x\}$ for $x \in \mathbb{Q}_N$ and the empty set.*

Proof. Suppose $S \subset \mathbb{Q}_N$ is a nonempty connected set and x, y are distinct elements of S. Let $r = d_N(x, y) > 0$. Let $U_1 = B(x, r)$ and U_2 be the complement of U_1, which is open by Lemma 3.2.18. Then U_1 and U_2 satisfies the conditions of Definition 3.2.16, so S is not connected, a contradiction. □

3.2.4 The Local-to-Global Principle of Hasse and Minkowski

Section 3.2.3 might have convinced you that $\mathbb{Q}_N$ is a bizarre pathology. In fact, $\mathbb{Q}_N$ is omnipresent in number theory, as the following two fundamental examples illustrate.

In the statement of the following theorem, a *nontrivial solution* to a homogeneous polynomial equation is a solution where not all indeterminates are 0.

Theorem 3.2.21 (Hasse-Minkowski)**.** *The quadratic equation*

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 0, \tag{3.2.1}$$

with $a_i \in \mathbb{Q}^\times$, has a nontrivial solution with $x_1, \ldots, x_n$ in $\mathbb{Q}$ if and only if (3.2.1) has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

This theorem is very useful in practice because the p-adic condition turns out to be easy to check. For more details, including a complete proof, see [Ser73, IV.3.2].

The analogue of Theorem 3.2.21 for cubic equations is false. For example, Selmer proved that the cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution other than $(0, 0, 0)$ in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p but has no solution other than $(0, 0, 0)$ in $\mathbb{Q}$ (for a proof see [Cas91, §18]).

Open Problem. Give an algorithm that decides whether or not a cubic

$$ax^3 + by^3 + cz^3 = 0$$

has a nontrivial solution in $\mathbb{Q}$.

This open problem is closely related to the Birch and Swinnerton-Dyer Conjecture for elliptic curves. The truth of the conjecture would follow if we knew that "Shafarevich-Tate Groups" of certain elliptic curves are finite.

3.3 Weak Approximation

The following theorem asserts that inequivalent valuations are in fact almost totally independent. For our purposes it will be superseded by the strong approximation theorem (Theorem 7.4.4).

Theorem 3.3.1 (Weak Approximation)**.** *Let $|\cdot|_n$, for $1 \le n \le N$, be inequivalent nontrivial valuations of a field K. For each n, let K_n be the topological space consisting of the set of elements of K with the topology induced by $|\cdot|_n$. Let Δ be the image of K in the topological product*

$$A = \prod_{1 \le n \le N} K_n$$

equipped with the product topology. Then Δ is dense in A.

The conclusion of the theorem may be expressed in a less topological manner as follows: given any $a_n \in K$, for $1 \le n \le N$, and real $\varepsilon > 0$, there is an $b \in K$ such that simultaneously

$$|a_n - b|_n < \varepsilon \qquad (1 \le n \le N).$$

If $K = \mathbb{Q}$ and the $|\cdot|$ are p-adic valuations, Theorem 3.3.1 is related to the Chinese Remainder Theorem (Theorem **??**), but the strong approximation theorem (Theorem 7.4.4) is the real generalization.

Proof. We note first that it will be enough to find, for each n, an element $c_n \in K$ such that

$$|c_n|_n > 1 \quad \text{and} \quad |c_n|_m < 1 \quad \text{for } n \ne m,$$

where $1 \le n, m \le N$. For then as $r \to +\infty$, we have

$$\frac{c_n^r}{1+c_n^r} = \frac{1}{1+\left(\frac{1}{c_n}\right)^r} \to \begin{cases} 1 & \text{with respect to } |\cdot|_n \text{ and} \\ 0 & \text{with respect to } |\cdot|_m, \text{ for } m \ne n. \end{cases}$$

It is then enough to take

$$b = \sum_{n=1}^{N} \frac{c_n^r}{1+c_n^r} \cdot a_n$$

By symmetry it is enough to show the existence of $c = c_1$ with

$$|c|_1 > 1 \qquad \text{and} \qquad |c|_n < 1 \quad \text{for} \quad 2 \le n \le N.$$

We will do this by induction on N.

First suppose $N = 2$. Since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent (and all absolute values are assumed nontrivial) there is an $a \in K$ such that

$$|a|_1 < 1 \qquad \text{and} \qquad |a|_2 \ge 1 \tag{3.3.1}$$

and similarly a b such that

$$|b|_1 \ge 1 \qquad \text{and} \qquad |b|_2 < 1.$$

Then $c = \dfrac{b}{a}$ will do.

Remark 3.3.2. It is not completely clear that one can choose an a such that (3.3.1) is satisfied. Suppose it were impossible. Then because the valuations are nontrivial, we would have that for any $a \in K$ if $|a|_1 < 1$ then $|a|_2 < 1$. This implies the converse statement: if $a \in K$ and $|a|_2 < 1$ then $|a|_1 < 1$. To see this, suppose there is an $a \in K$ such that $|a|_2 < 1$ and $|a|_1 \ge 1$. Choose $y \in K$ such that $|y|_1 < 1$. Then for any integer $n > 0$ we have $|y/a^n|_1 < 1$, so by hypothesis $|y/a^n|_2 < 1$. Thus $|y|_2 < |a|_2^n < 1$ for all n. Since $|a|_2 < 1$ we have $|a|_2^n \to 0$ as $n \to \infty$, so $|y|_2 = 0$, a contradiction since $y \ne 0$. Thus $|a|_1 < 1$ if and only if $|a|_2 < 1$, and we have proved before that this implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$.

Next suppose $N \geq 3$. By the case $N-1$, there is an $a \in K$ such that

$$|a|_1 > 1 \qquad \text{and} \qquad |a|_n < 1 \quad \text{for} \quad 2 \leq n \leq N-1.$$

By the case for $N = 2$ there is a $b \in K$ such that

$$|b|_1 > 1 \qquad \text{and} \qquad |b|_N < 1.$$

Then put

$$c = \begin{cases} a & \text{if } |a|_N < 1 \\ a^r \cdot b & \text{if } |a|_N = 1 \\ \dfrac{a^r}{1+a^r} \cdot b & \text{if } |a|_N > 1 \end{cases}$$

where $r \in \mathbb{Z}$ is sufficiently large so that $|c|_1 > 1$ and $|c|_n < 1$ for $2 \leq n \leq N$. □

Example 3.3.3. Suppose $K = \mathbb{Q}$, let $|\cdot|_1$ be the archimedean absolute value and let $|\cdot|_2$ be the 2-adic absolute value. Let $a_1 = -1$, $a_2 = 8$, and $\varepsilon = 1/10$, as in the remark right after Theorem 3.3.1. Then the theorem implies that there is an element $b \in \mathbb{Q}$ such that

$$|-1-b|_1 < \frac{1}{10} \qquad \text{and} \qquad |8-b|_2 < \frac{1}{10}.$$

As in the proof of the theorem, we can find such a b by finding a $c_1, c_2 \in \mathbb{Q}$ such that $|c_1|_1 > 1$ and $|c_1|_2 < 1$, and a $|c_2|_1 < 1$ and $|c_2|_2 > 1$. For example, $c_1 = 2$ and $c_2 = 1/2$ works, since $|2|_1 = 2$ and $|2|_2 = 1/2$ and $|1/2|_1 = 1/2$ and $|1/2|_2 = 2$. Again following the proof, we see that for sufficiently large r we can take

$$\begin{aligned} b_r &= \frac{c_1^r}{1+c_1^r} \cdot a_1 + \frac{c_2^r}{1+c_2^r} \cdot a_2 \\ &= \frac{2^r}{1+2^r} \cdot (-1) + \frac{(1/2)^r}{1+(1/2)^r} \cdot 8. \end{aligned}$$

We have $b_1 = 2$, $b_2 = 4/5$, $b_3 = 0$, $b_4 = -8/17$, $b_5 = -8/11$, $b_6 = -56/55$. None of the b_i work for $i < 6$, but b_6 works.

Exercise 3.3.4. In this problem you will compute an example of weak approximation, like I did in the Example 3.3.3. Let $K = \mathbb{Q}$, let $|\cdot|_7$ be the 7-adic absolute value, let $|\cdot|_{11}$ be the 11-adic absolute value, and let $|\cdot|_\infty$ be the usual archimedean absolute value. Find an element $b \in \mathbb{Q}$ such that $|b - a_i|_i < \frac{1}{10}$, where $a_7 = 1$, $a_{11} = 2$, and $a_\infty = -2004$.

Exercise 3.3.5. Find the 3-adic expansion to precision 4 of each root of the following polynomial over $\mathbb{Q}_3$:

$$f = x^3 - 3x^2 + 2x + 3 \in \mathbb{Q}_3[x].$$

Your solution should conclude with three expressions of the form

$$a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3 + O(3^4).$$

Exercise 3.3.6. Prove that every finite extension of $\mathbb{Q}_p$ "comes from" an extension of $\mathbb{Q}$, in the following sense. Given an irreducible polynomial $f \in \mathbb{Q}_p[x]$ there exists an irreducible polynomial $g \in \mathbb{Q}[x]$ such that the fields $\mathbb{Q}_p[x]/(f)$ and $\mathbb{Q}_p[x]/(g)$ are isomorphic. [Hint: Choose each coefficient of g to be sufficiently close to the corresponding coefficient of f, then use Hensel's lemma to show that g has a root in $\mathbb{Q}_p[x]/(f)$.]

Exercise 3.3.7. Suppose that K is a finite extension of $\mathbb{Q}_p$ and L is a finite extension of $\mathbb{Q}_q$, with $p \neq q$ and assume that K and L have the same degree. Prove that there is a polynomial $g \in \mathbb{Q}[x]$ such that $\mathbb{Q}_p[x]/(g) \cong K$ and $\mathbb{Q}_q[x]/(g) \cong L$. [Hint: Combine your solution to exercise 3.3.6 with the weak approximation theorem.]

Chapter 4

Adic Numbers: The Finite Residue Field Case

4.1 Finite Residue Field Case

Let K be a field with a non-archimedean valuation $v = |\cdot|$. Recall that the set of $a \in K$ with $|a| \leq 1$ forms a ring $\mathcal{O}$, the ring of integers for v. The set of $u \in K$ with $|u| = 1$ are a group U under multiplication, the group of units for v. Finally, the set of $a \in K$ with $|a| < 1$ is a maximal ideal $\mathfrak{p}$, so the quotient ring $\mathcal{O}/\mathfrak{p}$ is a field. In this section we consider the case when $\mathcal{O}/\mathfrak{p}$ is a finite field of order a prime power q. For example, K could be $\mathbb{Q}$ and $|\cdot|$ could be a p-adic valuation, or K could be a number field and $|\cdot|$ could be the valuation corresponding to a maximal ideal of the ring of integers. Among other things, we will discuss in more depth the topological and measure-theoretic nature of the completion of K at v.

Suppose further for the rest of this section that $|\cdot|$ is discrete. Then by Lemma 2.2.8, the ideal $\mathfrak{p}$ is a principal ideal (π), say, and every $a \in K$ is of the form $a = \pi^n \varepsilon$, where $n \in \mathbb{Z}$ and $\varepsilon \in U$ is a unit. We call

$$n = \mathrm{ord}(a) = \mathrm{ord}_\pi(a) = \mathrm{ord}_\mathfrak{p}(a) = \mathrm{ord}_v(a)$$

the ord of a at v. (Some authors, including me (!) also call this integer the *valuation* of a with respect to v.) If $\mathfrak{p} = (\pi')$, then π/π' is a unit, and conversely, so $\mathrm{ord}(a)$ is independent of the choice of π.

Let $\mathcal{O}_v$ and $\mathfrak{p}_v$ be defined with respect to the completion K_v of K at v.

Lemma 4.1.1. *There is a natural isomorphism*

$$\varphi : \mathcal{O}_v/\mathfrak{p}_v \to \mathcal{O}/\mathfrak{p},$$

and $\mathfrak{p}_v = (\pi)$ *as an* $\mathcal{O}_v$*-ideal.*

Proof. Since we are assuming that $|\cdot|$ is discrete, we may view $\mathcal{O}_v$ as the set of equivalence classes of Cauchy sequences (a_n) in K such that $a_n \in \mathcal{O}$ for n sufficiently

large, and similarly $\mathfrak{p}_v$ as those such that $a_n \in \mathfrak{p}$ for n sufficiently large. For any ε, given such a sequence (a_n), there is N such that for $n, m \geq N$, we have $|a_n - a_m| < \varepsilon$. In particular, we can choose N such that $n, m \geq N$ implies that $a_n \equiv a_m \pmod{\mathfrak{p}}$. Let $\varphi((a_n)) = a_N \pmod{\mathfrak{p}}$, which is well-defined. The map φ is surjective because the constant sequences are in $\mathcal{O}_v$. Its kernel is the set of Cauchy sequences whose elements are eventually all in $\mathfrak{p}$, which is exactly $\mathfrak{p}_v$. This proves the first part of the lemma. The second part is true because any element of $\mathfrak{p}_v$ is a sequence all of whose terms are eventually in $\mathfrak{p}$, hence all a multiple of π (we can set to 0 a finite number of terms of the sequence without changing the equivalence class of the sequence). □

Assume for the rest of this section that K is complete with respect to $|\cdot|$.

Lemma 4.1.2. *Then ring $\mathcal{O}$ is precisely the set of infinite sums*

$$a = \sum_{j=0}^{\infty} a_j \cdot \pi^j \tag{4.1.1}$$

where the a_j run independently through some set $\mathcal{R}$ of representatives of $\mathcal{O}$ in $\mathcal{O}/\mathfrak{p}$.

By (4.1.1) is meant the limit of the Cauchy sequence $\sum_{j=0}^{n} a_j \cdot \pi^j$ as $j \to \infty$.

Proof. There is a uniquely defined $a_0 \in \mathcal{R}$ such that $|a - a_0| < 1$. Then $a' = \pi^{-1} \cdot (a - a_0) \in \mathcal{O}$. Now define $a_1 \in \mathcal{R}$ by $|a' - a_1| < 1$. And so on. □

Example 4.1.3. Suppose $K = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$ is the p-adic valuation, for some prime p. We can take $\mathcal{R} = \{0, 1, \ldots, p-1\}$. The lemma asserts that

$$\mathcal{O} = \mathbb{Z}_p = \left\{ \sum_{j=0}^{\infty} a_n p^n : 0 \leq a_n \leq p-1 \right\}.$$

Notice that $\mathcal{O}$ is uncountable since there are p choices for each p-adic "digit". We can do arithmetic with elements of $\mathbb{Z}_p$, which can be thought of "backwards" as numbers in base p. For example, with $p = 3$ we have

$$\begin{aligned}
&(1 + 2 \cdot 3 + 3^2 + \cdots) + (2 + 2 \cdot 3 + 3^2 + \cdots) \\
&= 3 + 4 \cdot 3 + 2 \cdot 3^2 + \cdots \qquad \text{not in canonical form} \\
&= 0 + 2 \cdot 3 + 3 \cdot 3 + 2 \cdot 3^2 + \cdots \qquad \text{still not canonical} \\
&= 0 + 2 \cdot 3 + 0 \cdot 3^2 + \cdots
\end{aligned}$$

Here is an example of doing basic arithmetic with p-adic numbers in Sage:

```
sage: a = 1 + 2*3 + 3^2 + O(3^3)
sage: b = 2 + 2*3 + 3^2 + O(3^3)
sage: a + b
```

```
2*3 + O(3^3)
sage: sqrt(a)
1 + 3 + O(3^3)
sage: sqrt(a)^2
1 + 2*3 + 3^2 + O(3^3)
sage: a * b
2 + O(3^3)
```

Type `Zp?` and `Qp?` in Sage for much more information about the various computer models of p-adic arithmetic that are available.

Theorem 4.1.4. *Under the conditions of the preceding lemma, $\mathcal{O}$ is compact with respect to the $|\cdot|$-topology.*

Proof. Let V_λ, for λ running through some index set Λ, be some family of open sets that cover $\mathcal{O}$. We must show that there is a finite subcover. We suppose not.

Let $\mathcal{R}$ be a set of representatives for $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}$ is the union of the finite number of cosets $a + \pi\mathcal{O}$, for $a \in \mathcal{R}$. Hence for at lest one $a_0 \in \mathcal{R}$ the set $a_0 + \pi\mathcal{O}$ is not covered by finitely many of the V_λ. Then similarly there is an $a_1 \in \mathcal{R}$ such that $a_0 + a_1\pi + \pi^2\mathcal{O}$ is not finitely covered. And so on. Let

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots \in \mathcal{O}.$$

Then $a \in V_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since V_{λ_0} is an open set, $a + \pi^J \cdot \mathcal{O} \subset V_{\lambda_0}$ for some J (since those are exactly the open balls that form a basis for the topology). This is a contradiction because we constructed a so that none of the sets $a + \pi^n \cdot \mathcal{O}$, for each n, are not covered by any finite subset of the V_λ. □

Definition 4.1.5 (Locally compact)**.** A topological space X is *locally compact* at a point x if there is some compact subset C of X that contains a neighborhood of x. The space X is locally compact if it is locally compact at each point in X.

Corollary 4.1.6. *The complete local field K is locally compact.*

Proof. If $x \in K$, then $x \in C = x + \mathcal{O}$, and C is a compact subset of K by Theorem 4.1.4. Also C contains the neighborhood $x + \pi\mathcal{O} = B(x, 1)$ of x. Thus K is locally compact at x. □

Remark 4.1.7. The converse is also true. If K is locally compact with respect to a non-archimedean valuation $|\cdot|$, then

1. K is complete,
2. the residue field is finite, and
3. the valuation is discrete.

For there is a compact neighbourhood C of 0. Let π be any nonzero with $|\pi| < 1$. Then $\pi^n \cdot \mathcal{O} \subset C$ for sufficiently large n, so $\pi^n \cdot \mathcal{O}$ is compact, being closed. Hence $\mathcal{O}$ is compact. Since $|\cdot|$ is a metric, $\mathcal{O}$ is sequentially compact, i.e., every fundamental sequence in $\mathcal{O}$ has a limit, which implies (1). Let a_λ (for $\lambda \in \Lambda$) be a set of representatives in $\mathcal{O}$ of $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}_\lambda = \{z : |z - a_\lambda| < 1\}$ is an open covering of $\mathcal{O}$. Thus (2) holds since $\mathcal{O}$ is compact. Finally, $\mathfrak{p}$ is compact, being a closed subset of $\mathcal{O}$. Let S_n be the set of $a \in K$ with $|a| < 1 - 1/n$. Then S_n (for $1 \leq n < \infty$) is an open covering of $\mathfrak{p}$, so $\mathfrak{p} = S_n$ for some n, i.e., (3) is true.

If we allow $|\cdot|$ to be archimedean the only further possibilities are $k = \mathbb{R}$ and $k = \mathbb{C}$ with $|\cdot|$ equivalent to the usual absolute value.

We denote by K^+ the commutative topological group whose points are the elements of K, whose group law is addition and whose topology is that induced by $|\cdot|$. General theory tells us that there is an invariant Haar measure defined on K^+ and that this measure is unique up to a multiplicative constant.

Definition 4.1.8 (Haar Measure)**.** A *Haar measure* on a locally compact topological group G is a translation invariant measure such that every open set can be covered by open sets with finite measure.

Lemma 4.1.9. *Haar measure of any compact subset C of G is finite.*

Proof. The whole group G is open, so there is a covering U_α of G by open sets each of which has finite measure. Since C is compact, there is a finite subset of the U_α that covers C. The measure of C is at most the sum of the measures of these finitely many U_α, hence finite. □

Remark 4.1.10. Usually one defined Haar measure to be a translation invariant measure such that the measure of compact sets is finite. Because of local compactness, this definition is equivalent to Definition 4.1.8. We take this alternative viewpoint because Haar measure is constructed naturally on the topological groups we will consider by defining the measure on each member of a basis of open sets for the topology.

We now deduce what any such measure μ on $G = K^+$ must be. Since $\mathcal{O}$ is compact (Theorem 4.1.4), the measure of $\mathcal{O}$ is finite. Since μ is translation invariant,

$$\mu_n = \mu(a + \pi^n \mathcal{O})$$

is independent of a. Further,

$$a + \pi^n \mathcal{O} = \bigcup_{1 \leq j \leq q} a + \pi^n a_j + \pi^{n+1} \mathcal{O}, \qquad \text{(disjoint union)}$$

where a_j (for $1 \leq j \leq q$) is a set of representatives of $\mathcal{O}/\mathfrak{p}$. Hence

$$\mu_n = q \cdot \mu_{n+1}.$$

If we normalize μ by putting

$$\mu(\mathcal{O}) = 1$$

we have $\mu_0 = 1$, hence $\mu_1 = q^{-1}$, and in general

$$\mu_n = q^{-n}.$$

Conversely, without the theory of Haar measure, we could *define* μ to be the necessarily unique measure on K^+ such that $\mu(\mathcal{O}) = 1$ that is translation invariant. This would have to be the μ we just found above.

Everything so far in this section has depended not on the valuation $|\cdot|$ but only on its equivalence class. The above considerations now single out one valuation in the equivalence class as particularly important.

Definition 4.1.11 (Normalized valuation)**.** Let K be a field equipped with a discrete valuation $|\cdot|$ and residue class field with $q < \infty$ elements. We say that $|\cdot|$ is *normalized* if

$$|\pi| = \frac{1}{q},$$

where $\mathfrak{p} = (\pi)$ is the maximal ideal of $\mathcal{O}$.

Example 4.1.12. The normalized valuation on the p-adic numbers $\mathbb{Q}_p$ is $|u \cdot p^n| = p^{-n}$, where u is a rational number whose numerator and denominator are coprime to p.

Next suppose $K = \mathbb{Q}_p(\sqrt{p})$. Then the p-adic valuation on $\mathbb{Q}_p$ extends uniquely to one on K such that $\left|\sqrt{p}\right|^2 = |p| = 1/p$. Since $\pi = \sqrt{p}$ for K, this valuation is not normalized. (Note that the ord of $\pi = \sqrt{p}$ is $1/2$.) The normalized valuation is $v = |\cdot|' = |\cdot|^2$. Note that $|p|' = 1/p^2$, or $\mathrm{ord}_v(p) = 2$ instead of 1.

Finally suppose that $K = \mathbb{Q}_p(\sqrt{q})$ where $x^2 - q$ has no root mod p. Then the residue class field degree is 2, and the normalized valuation must satisfy $\left|\sqrt{q}\right| = 1/p^2$.

The following proposition makes clear why this is the best choice of normalization.

Theorem 4.1.13. *Suppose further that K is complete with respect to the normalized valuation $|\cdot|$. Then*

$$\mu(a + b\mathcal{O}) = |b|,$$

where μ is the Haar measure on K^+ normalized so that $\mu(\mathcal{O}) = 1$.

Proof. Since μ is translation invariant, $\mu(a + b\mathcal{O}) = \mu(b\mathcal{O})$. Write $b = u \cdot \pi^n$, where u is a unit. Then since $u \cdot \mathcal{O} = \mathcal{O}$, we have

$$\mu(b\mathcal{O}) = \mu(u \cdot \pi^n \cdot \mathcal{O}) = \mu(\pi^n \cdot u \cdot \mathcal{O}) = \mu(\pi^n \cdot \mathcal{O}) = q^{-n} = |\pi^n| = |b|.$$

Here we have $\mu(\pi^n \cdot \mathcal{O}) = q^{-n}$ by the discussion before Definition 4.1.11. □

Exercise 4.1.14. 1. Find the normalized Haar measure of the following subset of $\mathbb{Q}_7^+$:

$$U = B\left(28, \frac{1}{50}\right) = \left\{x \in \mathbb{Q}_7 : |x - 28| < \frac{1}{50}\right\}.$$

2. Find the normalized Haar measure of the subset $\mathbb{Z}_7^*$ of $\mathbb{Q}_7^*$.

We can express the result of the theorem in a more suggestive way. Let $b \in K$ with $b \neq 0$, and let μ be a Haar measure on K^+ (not necessarily normalized as in the theorem). Then we can define a new Haar measure μ_b on K^+ by putting $\mu_b(E) = \mu(bE)$ for $E \subset K^+$. But Haar measure is unique up to a multiplicative constant and so $\mu_b(E) = \mu(bE) = c \cdot \mu(E)$ for all measurable sets E, where the factor c depends only on b. Putting $E = \mathcal{O}$, shows that the theorem implies that c is just $|b|$, when $|\cdot|$ is the normalized valuation.

Remark 4.1.15. The theory of locally compact topological groups leads to the consideration of the dual (character) group of K^+. It turns out that it is isomorphic to K^+. We do not need this fact for class field theory, so do not prove it here. For a proof and applications see Tate's thesis or Lang's *Algebraic Numbers*, and for generalizations see Weil's *Adeles and Algebraic Groups* and Godement's Bourbaki seminars 171 and 176. The determination of the character group of K^* is local class field theory.

The set of nonzero elements of K is a group K^* under multiplication. Multiplication and inverses are continuous with respect to the topology induced on K^* as a subset of K, so K^* is a topological group with this topology. We have

$$U_1 \subset U \subset K^*$$

where U is the group of units of $\mathcal{O} \subset K$ and U_1 is the group of 1-units, i.e., those units $\varepsilon \in U$ with $|\varepsilon - 1| < 1$, so

$$U_1 = 1 + \pi\mathcal{O}.$$

The set U is open because of the discreteness of the metric, and U is closed because $U = \mathcal{O} \setminus \mathfrak{p}$ and we already proved that $\mathcal{O}$ is closed and $\mathfrak{p}$ is open in this case. Likewise, U_1 is both open and closed.

The quotient $K^*/U = \{\pi^n \cdot U : n \in \mathbb{Z}\}$ is isomorphic to the additive group $\mathbb{Z}^+$ of integers with the discrete topology, where the map is

$$\pi^n \cdot U \mapsto n \qquad \text{for } n \in \mathbb{Z}.$$

The quotient U/U_1 is isomorphic to the multiplicative group $\mathbb{F}^*$ of the nonzero elements of the residue class field $\mathbb{F} = \mathcal{O}/\mathfrak{p}$, where the finite group $\mathbb{F}^*$ has the discrete topology. Note that $\mathbb{F}^*$ is cyclic of order $q-1$, and Hensel's lemma implies that K^* contains a primitive $(q-1)$th root of unity ζ. Thus K^* has the following structure:

$$K^* = \{\pi^n \zeta^m \varepsilon : n \in \mathbb{Z}, m \in \mathbb{Z}/(q-1)\mathbb{Z}, \varepsilon \in U_1\} \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times U_1.$$

(How to apply Hensel's lemma: Let $f(x) = x^{q-1} - 1$ and let $a \in \mathcal{O}$ be such that a mod $\mathfrak{p}$ generates K^*. Then $|f(a)| < 1$ and $|f'(a)| = 1$. By Hensel's lemma there is a $\zeta \in K$ such that $f(\zeta) = 0$ and $\zeta \equiv a \pmod{\mathfrak{p}}$.)

Since U is compact and the cosets of U cover K, we see that K^* is locally compact.

Lemma 4.1.16. *The additive Haar measure μ on K^+, when restricted to U_1 gives a measure on U_1 that is also invariant under multiplication, so gives a Haar measure on U_1.*

Proof. It suffices to show that

$$\mu(1 + \pi^n\mathcal{O}) = \mu(u \cdot (1 + \pi^n\mathcal{O})),$$

for any $u \in U_1$ and $n > 0$. Write $u = 1 + a_1\pi + a_2\pi^2 + \cdots$. We have

$$\begin{aligned} u \cdot (1 + \pi^n\mathcal{O}) &= (1 + a_1\pi + a_2\pi^2 + \cdots) \cdot (1 + \pi^n\mathcal{O}) \\ &= 1 + a_1\pi + a_2\pi^2 + \cdots + \pi^n\mathcal{O} \\ &= a_1\pi + a_2\pi^2 + \cdots + (1 + \pi^n\mathcal{O}), \end{aligned}$$

which is an additive translate of $1 + \pi^n\mathcal{O}$, hence has the same measure. □

Thus μ gives a Haar measure on K^* by translating U_1 around to cover K^*.

Lemma 4.1.17. *The topological spaces K^+ and K^* are totally disconnected (the only connected sets are points).*

Proof. The proof is the same as that of Proposition 3.2.20. The point is that the non-archimedean triangle inequality forces the complement of an open disc to be open, hence any set with at least two distinct elements "falls apart" into a disjoint union of two disjoint open subsets. □

Remark 4.1.18. Note that K^* and K^+ are locally isomorphic if K has characteristic 0. We have the exponential map

$$a \mapsto \exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

defined for all sufficiently small a with its inverse

$$\log(a) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(a-1)^n}{n},$$

which is defined for all a sufficiently close to 1.

Chapter 5

Normed Spaces and Tensor Products

Much of this chapter is preparation for what we will do later when we will prove that if K is complete with respect to a valuation (and locally compact) and L is a finite extension of K, then there is a *unique* valuation on L that extends the valuation on K. Also, if K is a number field, $v = |\cdot|$ is a valuation on K, K_v is the completion of K with respect to v, and L is a finite extension of K, we'll prove that

$$K_v \otimes_K L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j are the completions of L with respect to the equivalence classes of extensions of v to L. In particular, if L is a number field defined by a root of $f(x) \in \mathbb{Q}[x]$, then

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j correspond to the irreducible factors of the polynomial $f(x) \in \mathbb{Q}_p[x]$ (hence the extensions of $|\cdot|_p$ correspond to irreducible factors of $f(x)$ over $\mathbb{Q}_p[x]$).

In preparation for this clean view of the local nature of number fields, we will prove that the norms on a finite-dimensional vector space over a complete field are all equivalent. We will also explicitly construct tensor products of fields and deduce some of their properties.

5.1 Normed Spaces

Definition 5.1.1 (Norm)**.** Let K be a field with valuation $|\cdot|$ and let V be a vector space over K. A real-valued function $\|\cdot\|$ on V is called a *norm* if

1. $\|v\| > 0$ for all nonzero $v \in V$ (positivity).

2. $\|v+w\| \leq \|v\| + \|w\|$ for all $v, w \in V$ (triangle inequality).

3. $\|av\| = |a| \, \|v\|$ for all $a \in K$ and $v \in V$ (homogeneity).

Note that setting $\|v\| = 1$ for all $v \neq 0$ does *not* define a norm unless the absolute value on K is trivial, as $1 = \|av\| = |a| \, \|v\| = |a|$. We assume for the rest of this section that $|\cdot|$ is not trivial.

Definition 5.1.2 (Equivalent)**.** Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on the same vector space V are *equivalent* if there exists positive real numbers c_1 and c_2 such that for all $v \in V$

$$\|v\|_1 \leq c_1 \|v\|_2 \qquad \text{and} \qquad \|v\|_2 \leq c_2 \|v\|_1 .$$

Exercise 5.1.3. ex:normed1 Suppose $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent norms on a finite-dimensional vector space V over a field K (with valuation $|\cdot|$). Carefully prove that the topology induced by $\|\cdot\|_1$ is the same as that induced by $\|\cdot\|_2$.

Lemma 5.1.4. *Suppose that K is a field that is complete with respect to a valuation $|\cdot|$ and that V is a finite dimensional K vector space. Then any two norms on V are equivalent.*

Remark 5.1.5. As we shall see soon (see Theorem 6.1.8), the lemma is usually false if we do not assume that K is complete. For example, when $K = \mathbb{Q}$ and $|\cdot|_p$ is the p-adic valuation, and V is a number field, then there may be several extensions of $|\cdot|_p$ to inequivalent norms on V.

If two norms are equivalent then the corresponding topologies on V are equal, since very open ball for $\|\cdot\|_1$ is contained in an open ball for $\|\cdot\|_2$, and conversely. (The converse is also true, since, as we will show, all norms on V are equivalent.)

Proof. Let $v_1, \ldots, v_N$ be a basis for V. Define the max norm $\|\cdot\|_0$ by

$$\left\| \sum_{n=1}^{N} a_n v_n \right\|_0 = \max \{ |a_n| : n = 1, \ldots, N \} .$$

It is enough to show that any norm $\|\cdot\|$ is equivalent to $\|\cdot\|_0$. We have

$$\begin{aligned} \left\| \sum_{n=1}^{N} a_n v_n \right\| &\leq \sum_{n=1}^{N} |a_n| \, \|v_n\| \\ &\leq \sum_{n=1}^{N} \max |a_n| \, \|v_n\| \\ &= c_1 \cdot \left\| \sum_{n=1}^{N} a_n v_n \right\|_0 , \end{aligned}$$

where $c_1 = \sum_{n=1}^{N} \|v_n\|$.

To finish the proof, we show that there is a $c_2 \in \mathbb{R}$ such that for all $v \in V$,

$$\|v\|_0 \leq c_2 \cdot \|v\| .$$

We will only prove this in the case when K is not just merely complete with respect to $|\cdot|$ but also locally compact. This will be the case of primary interest to us. For a proof in the general case, see the original article by Cassels (page 53).

By what we have already shown, the function $\|v\|$ is continuous in the $\|\cdot\|_0$-topology, so by local compactness it attains its lower bound δ on the unit circle $\{v \in V : \|v\|_0 = 1\}$. (Why is the unit circle compact? With respect to $\|\cdot\|_0$, the topology on V is the same as that of a product of copies of K. If the valuation is archimedean then $K \cong \mathbb{R}$ or $\mathbb{C}$ with the standard topology and the unit circle is compact. If the valuation is non-archimedean, then we saw (see Remark 4.1.7) that if K is locally compact, then the valuation is discrete, in which case we showed that the unit disc is compact, hence the unit circle is also compact since it is closed.) Note that $\delta > 0$ by part 1 of Definition 5.1.1. Also, by definition of $\|\cdot\|_0$, for any $v \in V$ there exists $a \in K$ such that $\|v\|_0 = |a|$ (just take the max coefficient in our basis). Thus we can write any $v \in V$ as $a \cdot w$ where $a \in K$ and $w \in V$ with $\|w\|_0 = 1$. We then have

$$\frac{\|v\|_0}{\|v\|} = \frac{\|aw\|_0}{\|aw\|} = \frac{|a| \, \|w\|_0}{|a| \, \|w\|} = \frac{1}{\|w\|} \leq \frac{1}{\delta}.$$

Thus for all v we have

$$\|v\|_0 \leq c_2 \cdot \|v\| ,$$

where $c_2 = 1/\delta$, which proves the theorem. □

5.2 Tensor Products

We need only a special case of the tensor product construction. Let A and B be commutative rings containing a field K and suppose that B is of finite dimension N over K, say, with basis

$$1 = w_1, w_2, \ldots, w_N.$$

Then B is determined up to isomorphism as a ring over K by the multiplication table $(c_{i,j,n})$ defined by

$$w_i \cdot w_j = \sum_{n=1}^{N} c_{i,j,n} \cdot w_n.$$

We define a new ring C containing K whose elements are the set of all expressions

$$\sum_{n=1}^{N} a_n \underline{w}_n$$

where the $\underline{w}_n$ have the same multiplication rule

$$\underline{w}_i \cdot \underline{w}_j = \sum_{n=1}^{N} c_{i,j,n} \cdot \underline{w}_n$$

as the w_n.

There are injective ring homomorphisms

$$i : A \hookrightarrow C, \qquad i(a) = a\underline{w}_1 \qquad \text{(note that } \underline{w}_1 = 1)$$

and

$$j : B \hookrightarrow C, \qquad j\left(\sum_{n=1}^{N} c_n w_n\right) = \sum_{n=1}^{N} c_n \underline{w}_n.$$

Moreover C is defined, up to isomorphism, by A and B and is independent of the particular choice of basis w_n of B (i.e., a change of basis of B induces a canonical isomorphism of the C defined by the first basis to the C defined by the second basis). We write

$$C = A \otimes_K B$$

since C is, in fact, a special case of the ring tensor product.

Exercise 5.2.1. Prove that the ring C defined in Section 5.2 really is the tensor product of A and B, i.e., that it satisfies the defining universal mapping property for tensor products. Part of this problem is for you to look up a functorial definition of tensor product.

Let us now suppose, further, that A is a topological ring, i.e., has a topology with respect to which addition and multiplication are continuous. Then the map

$$C \to A \oplus \cdots \oplus A, \qquad \sum_{m=1}^{N} a_m \underline{w}_m \mapsto (a_1, \ldots, a_N)$$

defines a bijection between C and the product of N copies of A (considered as sets). We give C the product topology. It is readily verified that this topology is independent of the choice of basis $w_1, \ldots, w_N$ and that multiplication and addition on C are continuous, so C is a topological ring. We call this topology on C the *tensor product topology*.

Now drop our assumption that A and B have a topology, but suppose that A and B are not merely rings but fields. Recall that a finite extension L/K of fields is *separable* if the number of embeddings $L \hookrightarrow \overline{K}$ that fix K equals the degree of L over K, where $\overline{K}$ is an algebraic closure of K. The primitive element theorem from Galois theory asserts that any such extension is generated by a single element, i.e., $L = K(a)$ for some $a \in L$.

Lemma 5.2.2. *Let A and B be fields containing the field K and suppose that B is a separable extension of finite degree $N = [B : K]$. Then $C = A \otimes_K B$ is the direct sum of a finite number of fields K_j, each containing an isomorphic image of A and an isomorphic image of B.*

Proof. By the primitive element theorem, we have $B = K(b)$, where b is a root of some separable irreducible polynomial $f(x) \in K[x]$ of degree N. Then $1, b, \ldots, b^{N-1}$ is a basis for B over K, so

$$A \otimes_K B = A[\underline{b}] \cong A[x]/(f(x))$$

where $1, \underline{b}, \underline{b}^2, \ldots, \underline{b}^{N-1}$ are linearly independent over A and $\underline{b}$ satisfies $f(\underline{b}) = 0$.

Although the polynomial $f(x)$ is irreducible as an element of $K[x]$, it need not be irreducible in $A[x]$. Since A is a field, we have a factorization

$$f(x) = \prod_{j=1}^{J} g_j(x)$$

where $g_j(x) \in A[x]$ is irreducible. The $g_j(x)$ are distinct because $f(x)$ is separable (i.e., has distinct roots in any algebraic closure).

For each j, let $\underline{b}_j \in \overline{A}$ be a root of $g_j(x)$, where $\overline{A}$ is a fixed algebraic closure of the field A. Let $K_j = A(\underline{b}_j)$. Then the map

$$\varphi_j : A \otimes_K B \to K_j \tag{5.2.1}$$

given by sending any polynomial $h(\underline{b})$ in $\underline{b}$ (where $h \in A[x]$) to $h(\underline{b}_j)$ is a ring homomorphism, because the image of $\underline{b}$ satisfies the polynomial $f(x)$, and $A \otimes_K B \cong A[x]/(f(x))$.

By the Chinese Remainder Theorem, the maps from (5.2.1) combine to define a ring isomorphism

$$A \otimes_K B \cong A[x]/(f(x)) \cong \bigoplus_{j=1}^{J} A[x]/(g_j(x)) \cong \bigoplus_{j=1}^{J} K_j.$$

Each K_j is of the form $A[x]/(g_j(x))$, so contains an isomorphic image of A. It thus remains to show that the ring homomorphisms

$$\lambda_j : B \xrightarrow{b \mapsto 1 \otimes b} A \otimes_K B \xrightarrow{\varphi_j} K_j$$

are injections. Since B and K_j are both fields, λ_j is either the 0 map or injective. However, λ_j is not the 0 map since $\lambda_j(1) = 1 \in K_j$. □

Example 5.2.3. If A and B are finite extensions of $\mathbb{Q}$, then $A \otimes_{\mathbb{Q}} B$ is an algebra of degree $[A : \mathbb{Q}] \cdot [B : \mathbb{Q}]$. For example, suppose A is generated by a root of $x^2 + 1$ and B is generated by a root of $x^3 - 2$. We can view $A \otimes_{\mathbb{Q}} B$ as either $A[x]/(x^3 - 2)$ or $B[x]/(x^2 + 1)$. The polynomial $x^2 + 1$ is irreducible over $\mathbb{Q}$, and if

it factored over the cubic field B, then there would be a root of x^2+1 in B, i.e., the quadratic field $A = \mathbb{Q}(i)$ would be a subfield of the cubic field $B = \mathbb{Q}(\sqrt[3]{2})$, which is impossible. Thus x^2+1 is irreducible over B, so $A \otimes_{\mathbb{Q}} B = A.B = \mathbb{Q}(i, \sqrt[3]{2})$ is a degree 6 extension of $\mathbb{Q}$. Notice that $A.B$ contains a copy A and a copy of B. By the primitive element theorem the composite field $A.B$ can be generated by the root of a single polynomial. For example, the minimal polynomial of $i + \sqrt[3]{2}$ is $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$, hence $\mathbb{Q}(i + \sqrt[3]{2}) = A.B$.

Example 5.2.4. The case $A \cong B$ is even more exciting. For example, suppose $A = B = \mathbb{Q}(i)$. Using the Chinese Remainder Theorem we have that

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i) \cong \mathbb{Q}(i)[x]/(x^2+1) \cong \mathbb{Q}(i)[x]/((x-i)(x+i)) \cong \mathbb{Q}(i) \oplus \mathbb{Q}(i),$$

since $(x-i)$ and $(x+i)$ are coprime. The last isomorphism sends $a+bx$, with $a, b \in \mathbb{Q}(i)$, to $(a+bi, a-bi)$. Since $\mathbb{Q}(i) \oplus \mathbb{Q}(i)$ has zero divisors, the tensor product $\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i)$ must also have zero divisors. For example, $(1,0)$ and $(0,1)$ is a zero divisor pair on the right hand side, and we can trace back to the elements of the tensor product that they define. First, by solving the system

$$a + bi = 1 \qquad \text{and} \qquad a - bi = 0$$

we see that $(1,0)$ corresponds to $a = 1/2$ and $b = -i/2$, i.e., to the element

$$\frac{1}{2} - \frac{i}{2}x \in \mathbb{Q}(i)[x]/(x^2+1).$$

This element in turn corresponds to

$$\frac{1}{2} \otimes 1 - \frac{i}{2} \otimes i \in \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i).$$

Similarly the other element $(0,1)$ corresponds to

$$\frac{1}{2} \otimes 1 + \frac{i}{2} \otimes i \in \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i).$$

As a double check, observe that

$$\begin{aligned}\left(\frac{1}{2} \otimes 1 - \frac{i}{2} \otimes i\right) \cdot \left(\frac{1}{2} \otimes 1 + \frac{i}{2} \otimes i\right) &= \frac{1}{4} \otimes 1 + \frac{i}{4} \otimes i - \frac{i}{4} \otimes i - \frac{i^2}{4} \otimes i^2 \\ &= \frac{1}{4} \otimes 1 - \frac{1}{4} \otimes 1 = 0 \in \mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}(i).\end{aligned}$$

Clearing the denominator of 2 and writing $1 \otimes 1 = 1$, we have $(1 - i \otimes i)(1 + i \otimes i) = 0$, so $i \otimes i$ is a root of the polynomimal $x^2 - 1$, and $i \otimes i$ is not ± 1, so $x^2 - 1$ has more than 2 roots.

In general, to understand $A \otimes_K B$ explicitly is the same as factoring either the defining polynomial of B over the field A, or factoring the defining polynomial of A over B.

Exercise 5.2.5. Find a zero divisor pair in $\mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{5})$.

Exercise 5.2.6. 1. Is $\mathbb{Q}(\sqrt{5}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-5})$ a field?

2. Is $\mathbb{Q}(\sqrt[4]{5}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[4]{-5}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1})$ a field?

Exercise 5.2.7. Suppose ζ_5 denotes a primitive 5th root of unity. For any prime p, consider the tensor product $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5) = K_1 \oplus \cdots \oplus K_{n(p)}$. Find a simple formula for the number $n(p)$ of fields appearing in the decomposition of the tensor product $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_5)$. To get full credit on this problem your formula must be correct, but you do *not* have to prove that it is correct.

Corollary 5.2.8. *Let $a \in B$ be any element and let $f(x) \in K[x]$ be the characteristic polynomials of a over K and let $g_j(x) \in A[x]$ (for $1 \leq j \leq J$) be the characteristic polynomials of the images of a under $B \to A \otimes_K B \to K_j$ over A, respectively. Then*

$$f(x) = \prod_{j=1}^{J} g_j(X). \tag{5.2.2}$$

Proof. We show that both sides of (5.2.2) are the characteristic polynomial $T(x)$ of the image of a in $A \otimes_K B$ over A. That $f(x) = T(x)$ follows at once by computing the characteristic polynomial in terms of a basis $\underline{w}_1, \ldots, \underline{w}_N$ of $A \otimes_K B$, where $w_1, \ldots, w_N$ is a basis for B over K (this is because the matrix of left multiplication by b on $A \otimes_K B$ is exactly the same as the matrix of left multiplication on B, so the characteristic polynomial doesn't change). To see that $T(X) = \prod g_j(X)$, compute the action of the image of a in $A \otimes_K B$ with respect to a basis of

$$A \otimes_K B \cong \bigoplus_{j=1}^{J} K_j \tag{5.2.3}$$

composed of basis of the individual extensions K_j of A. The resulting matrix will be a block direct sum of submatrices, each of whose characteristic polynomials is one of the $g_j(X)$. Taking the product gives the claimed identity (5.2.2). □

Exercise 5.2.9. Suppose K and L are number fields (i.e., finite extensions of $\mathbb{Q}$). Is it possible for the tensor product $K \otimes_{\mathbb{Q}} L$ to contain a nilpotent element? (A nonzero element a in a ring R is *nilpotent* if there exists $n > 1$ such that $a^n = 0$.)

Corollary 5.2.10. *For $a \in B$ we have*

$$\mathrm{Norm}_{B/K}(a) = \prod_{j=1}^{J} \mathrm{Norm}_{K_j/A}(a),$$

and

$$\mathrm{Tr}_{B/K}(a) = \sum_{j=1}^{J} \mathrm{Tr}_{K_j/A}(a),$$

Proof. This follows from Corollary 5.2.8. First, the norm is $\pm$ the constant term of the characteristic polynomial, and the constant term of the product of polynomials is the product of the constant terms (and one sees that the sign matches up correctly). Second, the trace is minus the second coefficient of the characteristic polynomial, and second coefficients add when one multiplies polynomials:

$$(x^n + a_{n-1}x^{n-1} + \cdots) \cdot (x^m + a_{m-1}x^{m-1} + \cdots) = x^{n+m} + x^{n+m-1}(a_{m-1} + a_{n-1}) + \cdots .$$

One could also see both the statements by considering a matrix of left multiplication by a first with respect to the basis of $\underline{w}_n$ and second with respect to the basis coming from the left side of (5.2.3).

□

Chapter 6

Extensions and Normalizations of Valuations

6.1 Extensions of Valuations

In this section we continue to tacitly assume that all valuations are nontrivial. We do not assume all our valuations satisfy the triangle inequality.

Suppose $K \subset L$ is a finite extension of fields, and that $|\cdot|$ and $\|\cdot\|$ are valuations on K and L, respectively.

Definition 6.1.1 (Extends)**.** We say that $\|\cdot\|$ *extends* $|\cdot|$ if $|a| = \|a\|$ for all $a \in K$.

Theorem 6.1.2. *Suppose that K is a field that is complete with respect to $|\cdot|$ and that L is a finite extension of K of degree $N = [L : K]$. Then there is precisely one extension of $|\cdot|$ to K, namely*

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right|^{1/N}, \tag{6.1.1}$$

where the Nth root is the non-negative real Nth root of the nonnegative real number $\left|\mathrm{Norm}_{L/K}(a)\right|$.

Proof. We may assume that $|\cdot|$ is normalized so as to satisfy the triangle inequality. Otherwise, normalize $|\cdot|$ so that it does, prove the theorem for the normalized valuation $|\cdot|^c$, then raise both sides of (6.1.1) to the power $1/c$. In the uniqueness proof, by the same argument we may assume that $\|\cdot\|$ also satisfies the triangle inequality.

Uniqueness. View L as a finite-dimensional vector space over K. Then $\|\cdot\|$ is a norm in the sense defined earlier (Definition 5.1.1). Hence any two extensions $\|\cdot\|_1$ and $\|\cdot\|_2$ of $|\cdot|$ are equivalent as norms, so induce the same topology on K. But as we have seen (Proposition 3.1.5), two valuations which induce the same topology are equivalent valuations, i.e., $\|\cdot\|_1 = \|\cdot\|_2^c$, for some positive real c. Finally $c = 1$ since $\|a\|_1 = |a| = \|a\|_2$ for all $a \in K$.

Existence. We do not give a proof of existence in the general case. Instead we give a proof, which was suggested by Dr. Geyer at the conference out of which [Cas67] arose. It is valid when K is locally compact, which is the only case we will use later.

We see at once that the function defined in (6.1.1) satisfies the condition (i) that $\|a\| \geq 0$ with equality only for $a = 0$, and (ii) $\|ab\| = \|a\| \cdot \|b\|$ for all $a, b \in L$. The difficult part of the proof is to show that there is a constant $C > 0$ such that

$$\|a\| \leq 1 \implies \|1 + a\| \leq C.$$

Note that we do not know (and will not show) that $\|\cdot\|$ as defined by (6.1.1) is a norm as in Definition 5.1.1, since showing that $\|\cdot\|$ is a norm would entail showing that it satisfies the triangle inequality, which is not obvious.

Choose a basis $b_1, \ldots, b_N$ for L over K. Let $\|\cdot\|_0$ be the max norm on L, so for $a = \sum_{i=1}^{N} c_i b_i$ with $c_i \in K$ we have

$$\|a\|_0 = \left\| \sum_{i=1}^{N} c_i b_i \right\|_0 = \max\{|c_i| : i = 1, \ldots, N\}.$$

(Note: in Cassels's original article he let $\|\cdot\|_0$ be *any* norm, but we don't because the rest of the proof does not work, since we can't use homogeneity as he claims to do. This is because it need not be possible to find, for any nonzero $a \in L$ some element $c \in K$ such that $\|ac\|_0 = 1$. This would fail, e.g., if $\|a\|_0 \neq |c|$ for any $c \in K$.) The rest of the argument is very similar to our proof from Lemma 5.1.4 of uniqueness of norms on vector spaces over complete fields.

With respect to the $\|\cdot\|_0$-topology, L has the product topology as a product of copies of K. The function $a \mapsto \|a\|$ is a composition of continuous functions on L with respect to this topology (e.g., $\mathrm{Norm}_{L/K}$ is the determinant, hence polynomial), hence $\|\cdot\|$ defines nonzero continuous function on the compact set

$$S = \{a \in L : \|a\|_0 = 1\}.$$

By compactness, there are real numbers $\delta, \Delta \in \mathbb{R}_{>0}$ such that

$$0 < \delta \leq \|a\| \leq \Delta \qquad \text{for all } a \in S.$$

For any nonzero $a \in L$ there exists $c \in K$ such that $\|a\|_0 = |c|$; to see this take c to be a c_i in the expression $a = \sum_{i=1}^{N} c_i b_i$ with $|c_i| \geq |c_j|$ for any j. Hence $\|a/c\|_0 = 1$, so $a/c \in S$ and

$$0 \leq \delta < \frac{\|a/c\|}{\|a/c\|_0} \leq \Delta.$$

Then by homogeneity

$$0 \leq \delta < \frac{\|a\|}{\|a\|_0} \leq \Delta.$$

Suppose now that $\|a\| \leq 1$. Then $\|a\|_0 \leq \delta^{-1}$, so

$$\begin{aligned}\|1+a\| &\leq \Delta \cdot \|1+a\|_0 \\ &\leq \Delta \cdot (\|1\|_0 + \|a\|_0) \\ &\leq \Delta \cdot \left(\|1\|_0 + \delta^{-1}\right) \\ &= C \quad \text{(say)},\end{aligned}$$

as required. □

Example 6.1.3. Consider the extension $\mathbb{C}$ of $\mathbb{R}$ equipped with the archimedean valuation. The unique extension is the ordinary absolute value on $\mathbb{C}$:

$$\|x+iy\| = \left(x^2+y^2\right)^{1/2}.$$

Example 6.1.4. Consider the extension $\mathbb{Q}_2(\sqrt{2})$ of $\mathbb{Q}_2$ equipped with the 2-adic absolute value. Since x^2-2 is irreducible over $\mathbb{Q}_2$ we can do some computations by working in the subfield $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}_2(\sqrt{2})$.

```
sage: K.<a> = NumberField(x^2 - 2); K
Number Field in a with defining polynomial x^2 - 2
sage: norm = lambda z: math.sqrt(2^(-z.norm().valuation(2)))
sage: norm(1 + a)
1.0
sage: norm(1 + a + 1)
0.70710678118654757
sage: z = 3 + 2*a
sage: norm(z)
1.0
sage: norm(z + 1)
0.35355339059327379
```

Remark 6.1.5. Geyer's existence proof gives (6.1.1). But it is perhaps worth noting that in any case (6.1.1) is a consequence of unique existence, as follows. Suppose L/K is as above. Suppose M is a finite Galois extension of K that contains L. Then by assumption there is a unique extension of $|\cdot|$ to M, which we shall also denote by $\|\cdot\|$. If $\sigma \in \mathrm{Gal}(M/K)$, then

$$\|a\|_\sigma := \|\sigma(a)\|$$

is also an extension of $|\cdot|$ to M, so $\|\cdot\|_\sigma = \|\cdot\|$, i.e.,

$$\|\sigma(a)\| = \|a\| \qquad \text{for all } a \in M.$$

But now

$$\mathrm{Norm}_{L/K}(a) = \sigma_1(a) \cdot \sigma_2(a) \cdots \sigma_N(a)$$

for $a \in L$, where $\sigma_1, \ldots, \sigma_N \in \mathrm{Gal}(M/K)$ extend the embeddings of L into M. Hence

$$\begin{aligned} \left|\mathrm{Norm}_{L/K}(a)\right| &= \left\|\mathrm{Norm}_{L/K}(a)\right\| \\ &= \prod_{1 \le n \le N} \|\sigma_n(a)\| \\ &= \|a\|^N, \end{aligned}$$

as required.

Corollary 6.1.6. *Let $w_1, \ldots, w_N$ be a basis for L over K. Then there are positive constants c_1 and c_2 such that*

$$c_1 \le \frac{\left\|\sum_{n=1}^{N} b_n w_n\right\|}{\max\{|b_n| : n = 1, \ldots, N\}} \le c_2$$

for any $b_1, \ldots, b_N \in K$ not all 0.

Proof. For $\left\|\sum_{n=1}^{N} b_n w_n\right\|$ and $\max |b_n|$ are two norms on L considered as a vector space over K.

I don't believe this proof, which I copied from Cassels's article. My problem with it is that the proof of Theorem 6.1.2 does not give that $C \le 2$, i.e., that the triangle inequality holds for $\|\cdot\|$. By changing the basis for L/K one can make any nonzero vector $a \in L$ have $\|a\|_0 = 1$, so if we choose a such that $|a|$ is very large, then the Δ in the proof will also be very large. One way to fix the corollary is to only claim that there are positive constants c_1, c_2, c_3, c_4 such that

$$c_1 \le \frac{\left\|\sum_{n=1}^{N} b_n w_n\right\|^{c_3}}{\max\{|b_n|^{c_4} : n = 1, \ldots, N\}} \le c_2.$$

Then choose c_3, c_4 such that $\|\cdot\|^{c_3}$ and $|\cdot|^{c_4}$ satisfies the triangle inequality, and prove the modified corollary using the proof suggested by Cassels. □

Corollary 6.1.7. *A finite extension of a completely valued field K is complete with respect to the extended valuation.*

Proof. By the proceeding corollary it has the topology of a finite-dimensional vector space over K. (The problem with the proof of the previous corollary is not an issue, because we can replace the extended valuation by an equivalent one that satisfies the triangle inequality and induces the same topology.) □

When K is no longer complete under $|\cdot|$ the position is more complicated:

Theorem 6.1.8. *Let L be a separable extension of K of finite degree $N = [L : K]$. Then there are at most N extensions of a valuation $|\cdot|$ on K to L, say $\|\cdot\|_j$, for $1 \le j \le J$. Let K_v be the completion of K with respect to $|\cdot|$, and for each j let L_j be the completion of L with respect to $\|\cdot\|_j$. Then*

$$K_v \otimes_K L \cong \bigoplus_{1 \le j \le J} L_j \tag{6.1.2}$$

algebraically and topologically, where the right hand side is given the product topology.

Proof. We already know (Lemma 5.2.2) that $K_v \otimes_K L$ is of the shape (6.1.2), where the L_j are finite extensions of K_v. Hence there is a unique extension $|\cdot|_j^*$ of $|\cdot|$ to the L_j, and by Corollary 6.1.7 the L_j are complete with respect to the extended valuation. Further, the ring homomorphisms

$$\lambda_j : L \to K_v \otimes_K L \to L_j$$

are injections. Hence we get an extension $\|\cdot\|_j$ of $|\cdot|$ to L_j by putting

$$\|b\|_j = |\lambda_j(b)|_j^* .$$

Further, $L \cong \lambda_j(L)$ is dense in L_j with respect to $\|\cdot\|_j$ because $L = K \otimes_K L$ is dense in $K_v \otimes_K L$ (since K is dense in K_v). Hence L_j is exactly the completion of L.

It remains to show that the $\|\cdot\|_j$ are distinct and that they are the only extensions of $|\cdot|$ to L.

Suppose $\|\cdot\|$ is any valuation of L that extends $|\cdot|$. Then $\|\cdot\|$ extends by continuity to a real-valued function on $K_v \otimes_K L$, which we also denote by $\|\cdot\|$. (We are again using that L is dense in $K_v \otimes_K L$.) By continuity we have for all $a, b \in K_v \otimes_K L$,

$$\|ab\| = \|a\| \cdot \|b\|$$

and if C is the constant in axiom (iii) for L and $\|\cdot\|$, then

$$\|a\| \le 1 \implies \|1 + a\| \le C.$$

(In Cassels, he inexplicable assume that $C = 1$ at this point in the proof.)

We consider the restriction of $\|\cdot\|$ to one of the L_j. If $\|a\| \ne 0$ for some $a \in L_j$, then $\|a\| = \|b\| \cdot \left\|ab^{-1}\right\|$ for every $b \ne 0$ in L_j so $\|b\| \ne 0$. Hence either $\|\cdot\|$ is identically 0 on L_j or it induces a valuation on L_j.

Further, $\|\cdot\|$ cannot induce a valuation on two of the L_j. For

$$(a_1, 0, \dots, 0) \cdot (0, a_2, 0, \dots, 0) = (0, 0, 0, \dots, 0),$$

so for any $a_1 \in L_1$, $a_2 \in L_2$,

$$\|a_1\| \cdot \|a_2\| = 0.$$

Hence $\|\cdot\|$ induces a valuation in precisely one of the L_j, and it extends the given valuation $|\cdot|$ of K_v. Hence $\|\cdot\| = \|\cdot\|_j$ for precisely one j.

It remains only to show that (6.1.2) is a topological homomorphism. For

$$(b_1, \ldots, b_J) \in L_1 \oplus \cdots \oplus L_J$$

put

$$\|(b_1, \ldots, b_J)\|_0 = \max_{1 \le j \le J} \|b_j\|_j .$$

Then $\|\cdot\|_0$ is a norm on the right hand side of (6.1.2), considered as a vector space over K_v and it induces the product topology. On the other hand, any two norms are equivalent, since K_v is complete, so $\|\cdot\|_0$ induces the tensor product topology on the left hand side of (6.1.2). □

Corollary 6.1.9. *Suppose $L = K(a)$, and let $f(x) \in K[x]$ be the minimal polynomial of a. Suppose that*

$$f(x) = \prod_{1 \le j \le J} g_j(x)$$

in $K_v[x]$, where the g_j are irreducible. Then $L_j = K_v(b_j)$, where b_j is a root of g_j.

Exercise 6.1.10. Let K be the number field $\mathbb{Q}(\sqrt[5]{2})$.

1. In how many ways does the 2-adic valuation $|\cdot|_2$ on $\mathbb{Q}$ extend to a valuation on K?

2. Let $v = |\cdot|$ be a valuation on K that extends $|\cdot|_2$. Let K_v be the completion of K with respect to v. What is the residue class field $\mathbb{F}$ of K_v?

6.2 Extensions of Normalized Valuations

Let K be a complete field with valuation $|\cdot|$. We consider the following three cases:

(1) $|\cdot|$ is discrete non-archimedean and the residue class field is finite.

(2i) The completion of K with respect to $|\cdot|$ is $\mathbb{R}$.

(2ii) The completion of K with respect to $|\cdot|$ is $\mathbb{C}$.

(Alternatively, these cases can be subsumed by the hypothesis that the completion of K is locally compact.)

In case (1) we defined the normalized valuation to be the one such that if Haar measure of the ring of integers $\mathcal{O}$ is 1, then $\mu(a\mathcal{O}) = |a|$ (see Definition 4.1.11). In case (2i) we say that $|\cdot|$ is normalized if it is the ordinary absolute value, and in (2ii) if it is the *square* of the ordinary absolute value:

$$|x + iy| = x^2 + y^2 \qquad \text{(normalized)}.$$

In every case, for every $a \in K$, the map

$$a : x \mapsto ax$$

on K^+ multiplies any choice of Haar measure by $|a|$, and this characterizes the normalized valuations among equivalent ones.

We have already verified the above characterization for non-archimedean valuations, and it is clear for the ordinary absolute value on $\mathbb{R}$, so it remains to verify it for $\mathbb{C}$. The additive group $\mathbb{C}^+$ is topologically isomorphic to $\mathbb{R}^+ \oplus \mathbb{R}^+$, so a choice of Haar measure of $\mathbb{C}^+$ is the usual area measure on the Euclidean plane. Multiplication by $x + iy \in \mathbb{C}$ is the same as rotation followed by scaling by a factor of $\sqrt{x^2 + y^2}$, so if we rescale a region by a factor of $x + iy$, the area of the region changes by a factor of the square of $\sqrt{x^2 + y^2}$. This explains why the normalized valuation on $\mathbb{C}$ is the square of the usual absolute value. Note that the normalized valuation on $\mathbb{C}$ does not satisfy the triangle inequality:

$$|1 + (1 + i)| = |2 + i| = 2^2 + 1^2 = 5 \not\leq 3 = 1^2 + (1^2 + 1^2) = |1| + |1 + i|\,.$$

The constant C in axiom (3) of a valuation for the ordinary absolute value on $\mathbb{C}$ is 2, so the constant for the normalized valuation $|\cdot|$ is $C \leq 4$:

$$|x + iy| \leq 1 \implies |x + iy + 1| \leq 4.$$

Note that $x^2 + y^2 \leq 1$ implies

$$(x + 1)^2 + y^2 = x^2 + 2x + 1 + y^2 \leq 1 + 2x + 1 \leq 4$$

since $x \leq 1$.

Lemma 6.2.1. *Suppose K is a field that is complete with respect to a normalized valuation $|\cdot|$ and let L be a finite extension of K of degree $N = [L : K]$. Then the normalized valuation $\|\cdot\|$ on L which is equivalent to the unique extension of $|\cdot|$ to L is given by the formula*

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right| \qquad \text{all } a \in L. \tag{6.2.1}$$

Proof. Let $\|\cdot\|$ be the normalized valuation on L that extends $|\cdot|$. Our goal is to identify $\|\cdot\|$, and in particular to show that it is given by (6.2.1).

By the preceding section there is a positive real number c such that for all $a \in L$ we have

$$\|a\| = \left|\mathrm{Norm}_{L/K}(a)\right|^c.$$

Thus all we have to do is prove that $c = 1$. In case 2 the only nontrivial situation is $L = \mathbb{C}$ and $K = \mathbb{R}$, in which case $\left|\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}(x + iy)\right| = \left|x^2 + y^2\right|$, which is the normalized valuation on $\mathbb{C}$ defined above.

One can argue in a unified way in all cases as follows. Let $w_1, \ldots, w_N$ be a basis for L/K. Then the map

$$\varphi : L^+ \to \bigoplus_{n=1}^{N} K^+, \qquad \sum a_n w_n \mapsto (a_1, \ldots, a_N)$$

is an isomorphism between the additive group L^+ and the direct sum $\oplus_{n=1}^N K^+$, and this is a homeomorphism if the right hand side is given the product topology. In particular, the Haar measures on L^+ and on $\oplus_{n=1}^N K^+$ are the same up to a multiplicative constant in $\mathbb{Q}^*$.

Let $b \in K$. Then the left-multiplication-by-b map

$$b : \sum a_n w_n \mapsto \sum b a_n w_n$$

on L^+ is the same as the map

$$(a_1, \ldots, a_N) \mapsto (ba_1, \ldots, ba_N)$$

on $\oplus_{n=1}^N K^+$, so it multiplies the Haar measure by $|b|^N$, since $|\cdot|$ on K is assumed normalized (the measure of each factor is multiplied by $|b|$, so the measure on the product is multiplied by $|b|^N$). Since $\|\cdot\|$ is assumed normalized, so multiplication by b rescales by $\|b\|$, we have

$$\|b\| = |b|^N .$$

But $b \in K$, so $\mathrm{Norm}_{L/K}(b) = b^N$. Since $|\cdot|$ is nontrivial and for $a \in K$ we have

$$\|a\| = |a|^N = \left|a^N\right| = \left|\mathrm{Norm}_{L/K}(a)\right| ,$$

so we must have $c = 1$ in (6.2.1), as claimed. □

In the case when K need not be complete with respect to the valuation $|\cdot|$ on K, we have the following theorem.

Theorem 6.2.2. *Suppose $|\cdot|$ is a (nontrivial as always) normalized valuation of a field K and let L be a finite extension of K. Then for any $a \in L$,*

$$\prod_{1 \le j \le J} \|a\|_j = \left|\mathrm{Norm}_{L/K}(a)\right|$$

where the $\|\cdot\|_j$ are the normalized valuations equivalent to the extensions of $|\cdot|$ to K.

Proof. Let K_v denote the completion of K with respect to $|\cdot|$. Write

$$K_v \otimes_K L = \bigoplus_{1 \le j \le J} L_j .$$

Then Theorem 6.2.2 asserts that

$$\mathrm{Norm}_{L/K}(a) = \prod_{1 \le j \le J} \mathrm{Norm}_{L_j/K_v}(a). \tag{6.2.2}$$

By Theorem 6.1.8, the $\|\cdot\|_j$ are exactly the normalizations of the extensions of $|\cdot|$ to the L_j (i.e., the L_j are in bijection with the extensions of valuations, so there are no other valuations missed). By Lemma 6.1.1, the normalized valuation $\|\cdot\|_j$ on L_j is $|a| = \left|\mathrm{Norm}_{L_J/K_v}(a)\right|$. The theorem now follows by taking absolute values of both sides of (6.2.2). □

What's next?! We're building up to give a new proof of finiteness of the class group, which uses that the class group naturally has the discrete topology and is the continuous image of a compact group.

Chapter 7

Global Fields and Adeles

7.1 Global Fields

Definition 7.1.1 (Global Field)**.** A *global field* is a number field or a finite separable extension of $\mathbb{F}(t)$, where $\mathbb{F}$ is a finite field, and t is transcendental over $\mathbb{F}$.

In this chapter, we will focus attention on number fields, and leave the function field case to the reader.

The following lemma essentially says that the denominator of an element of a global field is only "nontrivial" at a finite number of valuations.

Lemma 7.1.2. *Let $a \in K$ be a nonzero element of a global field K. Then there are only finitely many inequivalent valuations $|\cdot|$ of K for which*

$$|a| > 1.$$

Proof. If $K = \mathbb{Q}$ or $\mathbb{F}(t)$ then the lemma follows by Ostrowski's classification of all the valuations on K (see Theorem 2.3.2). For example, when $a = \frac{n}{d} \in \mathbb{Q}$, with $n, d \in \mathbb{Z}$, then the valuations where we could have $|a| > 1$ are the archimedean one, or the p-adic valuations $|\cdot|_p$ for which $p \mid d$.

Suppose now that K is a finite extension of $\mathbb{Q}$, so a satisfies a monic polynomial

$$a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0,$$

for some n and $c_0, \ldots, c_{n-1} \in \mathbb{Q}$. If $|\cdot|$ is a non-archimedean valuation on K, we have

$$\begin{aligned} |a|^n &= \left|-(c_{n-1}a^{n-1} + \cdots + c_0)\right| \\ &\leq \max(1, |a|^{n-1}) \cdot \max(|c_0|, \ldots, |c_{n-1}|). \end{aligned}$$

Dividing each side by $|a|^{n-1}$, we have that

$$|a| \leq \max(|c_0|, \ldots, |c_{n-1}|),$$

so in all cases we have

$$|a| \leq \max(1, |c_0|, \ldots, |c_{n-1}|)^{1/(n-1)}. \tag{7.1.1}$$

We know the lemma for $\mathbb{Q}$, so there are only finitely many valuations $|\cdot|$ on $\mathbb{Q}$ such that the right hand side of (7.1.1) is bigger than 1. Since each valuation of $\mathbb{Q}$ has finitely many extensions to K, and there are only finitely many archimedean valuations, it follows that there are only finitely many valuations on K such that $|a| > 1$. □

Any valuation on a global field is either archimedean, or discrete non-archimedean with finite residue class field, since this is true of $\mathbb{Q}$ and $\mathbb{F}(t)$ and is a property preserved by extending a valuation to a finite extension of the base field. Hence it makes sense to talk of normalized valuations. Recall that the normalized p-adic valuation on $\mathbb{Q}$ is $|x|_p = p^{-\operatorname{ord}_p(x)}$, and if v is a valuation on a number field K equivalent to an extension of $|\cdot|_p$, then the normalization of v is the composite of the sequence of maps

$$K \hookrightarrow K_v \xrightarrow{\text{Norm}} \mathbb{Q}_p \xrightarrow{|\cdot|_p} \mathbb{R},$$

where K_v is the completion of K at v.

Example 7.1.3. Let $K = \mathbb{Q}(\sqrt{2})$, and let $p = 2$. Because $\sqrt{2} \notin \mathbb{Q}_2$, there is exactly one extension of $|\cdot|_2$ to K, and it sends $a = 1/\sqrt{2}$ to

$$\left|\text{Norm}_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(1/\sqrt{2})\right|_2^{1/2} = \sqrt{2}.$$

Thus the normalized valuation of a is 2.

There are two extensions of $|\cdot|_7$ to $\mathbb{Q}(\sqrt{2})$, since $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}_7 \cong \mathbb{Q}_7 \oplus \mathbb{Q}_7$, as $x^2 - 2 = (x-3)(x-4) \pmod 7$. The image of $\sqrt{2}$ under each embedding into $\mathbb{Q}_7$ is a unit in $\mathbb{Z}_7$, so the normalized valuation of $a = 1/\sqrt{2}$ is, in both cases, equal to 1. More generally, for any valuation of K of characteristic an odd prime p, the normalized valuation of a is 1.

Since $K = \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{R}$ in two ways, there are exactly two normalized archimedean valuations on K, and both of their values on a equal $1/\sqrt{2}$. Notice that the product of the absolute values of a with respect to all normalized valuations is

$$2 \cdot \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \cdot 1 \cdot 1 \cdot 1 \cdots = 1.$$

This "product formula" holds in much more generality, as we will now see.

Theorem 7.1.4 (Product Formula)**.** *Let $a \in K$ be a nonzero element of a global field K. Let $|\cdot|_v$ run through the normalized valuations of K. Then $|a|_v = 1$ for almost all v, and*

$$\prod_{\text{all } v} |a|_v = 1 \qquad \text{(the product formula)}.$$

We will later give a more conceptual proof of this using Haar measure (see Remark 7.3.10).

Proof. By Lemma 7.1.2, we have $|a|_v \leq 1$ for almost all v. Likewise, $1/|a|_v = |1/a|_v \leq 1$ for almost all v, so $|a|_v = 1$ for almost all v.

Let w run through all normalized valuations of $\mathbb{Q}$ (or of $\mathbb{F}(t)$), and write $v \mid w$ if the restriction of v to $\mathbb{Q}$ is equivalent to w. Then by Theorem 6.2.2,

$$\prod_v |a|_v = \prod_w \left(\prod_{v|w} |a|_v \right) = \prod_w \left| \mathrm{Norm}_{K/\mathbb{Q}}(a) \right|_w ,$$

so it suffices to prove the theorem for $K = \mathbb{Q}$.

By multiplicativity of valuations, if the theorem is true for b and c then it is true for the product bc and quotient b/c (when $c \neq 0$). The theorem is clearly true for -1, which has valuation 1 at all valuations. Thus to prove the theorem for $\mathbb{Q}$ it suffices to prove it when $a = p$ is a prime number. Then we have $|p|_\infty = p$, $|p|_p = 1/p$, and for primes $q \neq p$ that $|p|_q = 1$. Thus

$$\prod_v |p|_v = p \cdot \frac{1}{p} \cdot 1 \cdot 1 \cdot 1 \cdots = 1,$$

as claimed. □

Exercise 7.1.5. Prove that the product formula holds for $\mathbb{F}(t)$ similar to the proof we gave in class using Ostrowski's theorem for $\mathbb{Q}$. You may use the analogue of Ostrowski's theorem for $\mathbb{F}(t)$, which you had on the previous homework assignment 2.3.6. (Don't give a measure-theoretic proof.)

If v is a valuation on a field K, recall that we let K_v denote the completion of K with respect to v. Also when v is non-archimedean, let

$$\mathcal{O}_v = \mathcal{O}_{K,v} = \{x \in K_v : |x| \leq 1\}$$

be the ring of integers of the completion.

Definition 7.1.6 (Almost All)**.** We say a condition holds for *almost all* elements of a set if it holds for all but finitely many elements.

We will use the following lemma later (see Lemma 7.3.3) to prove that formation of the adeles of a global field is compatible with base change.

Lemma 7.1.7. *Let $\omega_1, \ldots, \omega_n$ be a basis for L/K, where L is a finite separable extension of the global field K of degree n. Then for almost all normalized non-archimedean valuations v on K we have*

$$\omega_1 \mathcal{O}_v \oplus \cdots \oplus \omega_n \mathcal{O}_v = \mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g} \subset K_v \otimes_K L, \tag{7.1.2}$$

where $w_1, \ldots, w_g$ are the extensions of v to L. Here we have identified $a \in L$ with its canonical image in $K_v \otimes_K L$, and the direct sum on the left is the sum taken inside the tensor product (so directness means that the intersections are trivial).

Proof. The proof proceeds in two steps. First we deduce easily from Lemma 7.1.2 that for almost all v the left hand side of (7.1.2) is contained in the right hand side. Then we use a trick involving discriminants to show the opposite inclusion for all but finitely many primes.

Since $\mathcal{O}_v \subset \mathcal{O}_{w_i}$ for all i, the left hand side of (7.1.2) is contained in the right hand side if $|\omega_i|_{w_j} \leq 1$ for $1 \leq i \leq n$ and $1 \leq j \leq g$. Thus by Lemma 7.1.2, for all but finitely many v the left hand side of (7.1.2) is contained in the right hand side. We have just eliminated the finitely many primes corresponding to "denominators" of some ω_i, and now only consider v such that $\omega_1, \ldots, \omega_n \in \mathcal{O}_w$ for all $w \mid v$.

For any elements $a_1, \ldots, a_n \in K_v \otimes_K L$, consider the discriminant

$$D(a_1, \ldots, a_n) = \det(\mathrm{Tr}(a_i a_j)) \in K_v,$$

where the trace is induced from the L/K trace. Since each ω_i is in each $\mathcal{O}_w$, for $w \mid v$, the traces $\mathrm{Tr}(\omega_i \omega_j)$ lie in $\mathcal{O}_v$, so

$$d = D(\omega_1, \ldots, \omega_n) \in \mathcal{O}_v.$$

Also note that $d \in K$ since each ω_i is in L. Now suppose that

$$\alpha = \sum_{i=1}^{n} a_i \omega_i \in \mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g},$$

with $a_i \in K_v$. Then by properties of determinants for any m with $1 \leq m \leq n$, we have

$$D(\omega_1, \ldots, \omega_{m-1}, \alpha, \omega_{m+1}, \ldots, \omega_n) = a_m^2 D(\omega_1, \ldots, \omega_n). \tag{7.1.3}$$

The left hand side of (7.1.3) is in $\mathcal{O}_v$, so the right hand side is as well, i.e.,

$$a_m^2 \cdot d \in \mathcal{O}_v, \qquad (\text{for } m = 1, \ldots, n),$$

where $d \in K$. Since $\omega_1, \ldots, \omega_n$ are a basis for L over K and the trace pairing is nondegenerate, we have $d \neq 0$, so by Theorem 7.1.4 we have $|d|_v = 1$ for all but finitely many v. Then for all but finitely many v we have that $a_m^2 \in \mathcal{O}_v$. For these v, that $a_m^2 \in \mathcal{O}_v$ implies $a_m \in \mathcal{O}_v$ since $a_m \in K_v$, i.e., α is in the left hand side of (7.1.2). □

Example 7.1.8. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$. Let $\omega_1 = 1/3$ and $\omega_2 = 2\sqrt{2}$. In the first stage of the above proof we would eliminate $|\cdot|_3$ because ω_2 is not integral at 3. The discriminant is

$$d = D\left(\frac{1}{3}, 2\sqrt{2}\right) = \det \begin{pmatrix} \frac{2}{9} & 0 \\ 0 & 16 \end{pmatrix} = \frac{32}{9}.$$

As explained in the second part of the proof, as long as $v \neq 2, 3$, we have equality of the left and right hand sides in (7.1.2).

7.2 Restricted Topological Products

In this section we describe a topological tool, which we need in order to define adeles (see Definition 7.3.1).

Definition 7.2.1 (Restricted Topological Products)**.** Let X_λ, for $\lambda \in \Lambda$, be a family of topological spaces, and for almost all λ let $Y_\lambda \subset X_\lambda$ be an open subset of X_λ. Consider the space X whose elements are sequences $\mathbf{x} = \{x_\lambda\}_{\lambda\in\Lambda}$, where $x_\lambda \in X_\lambda$ for every λ, and $x_\lambda \in Y_\lambda$ for almost all λ. We give X a topology by taking as a basis of open sets the sets $\prod U_\lambda$, where $U_\lambda \subset X_\lambda$ is open for all λ, and $U_\lambda = Y_\lambda$ for almost all λ. We call X with this topology the *restricted topological product* of the X_λ with respect to the Y_λ.

Corollary 7.2.2. *Let S be a finite subset of Λ, including at least all λ for which Y_λ is not defined, and let X_S be the set of $\mathbf{x} \in X$ with $x_\lambda \in Y_\lambda$ for all $\lambda \notin S$, i.e.,*

$$X_S = \prod_{\lambda\in S} X_\lambda \times \prod_{\lambda\notin S} Y_\lambda \subset X.$$

Then X_S is an open subset of X, and the topology induced on X_S as a subset of X is the same as the product topology.

The restricted topological product depends on the totality of the Y_λ, but not on the individual Y_λ:

Lemma 7.2.3. *Let $Y'_\lambda \subset X_\lambda$ be open subsets, and suppose that $Y_\lambda = Y'_\lambda$ for almost all λ. Then the restricted topological product of the X_λ with respect to the Y'_λ is canonically isomorphic to the restricted topological product with respect to the Y_λ.*

Lemma 7.2.4. *Suppose that the X_λ are locally compact and that the Y_λ are compact. Then the restricted topological product X of the X_λ is locally compact.*

Proof. For any finite subset S of Λ, the open subset $X_S \subset X$ is locally compact, because by Lemma 7.2.2 it is a product of finitely many locally compact sets with an infinite product of compact sets. (Here we are using Tychonoff's theorem from topology, which asserts that an arbitrary product of compact topological spaces is compact (see Munkres's *Topology, a first course*, chapter 5).) Since $X = \cup_S X_S$, and the X_S are open in X, the result follows. □

The following measure will be extremely important in deducing topological properties of the ideles, which will be used in proving finiteness of class groups. See, e.g., the proof of Lemma 7.4.1, which is a key input to the proof of strong approximation (Theorem 7.4.4).

Definition 7.2.5 (Product Measure)**.** For all $\lambda \in \Lambda$, suppose μ_λ is a measure on X_λ with $\mu_\lambda(Y_\lambda) = 1$ when Y_λ is defined. We define the *product measure* μ on X to be that for which a basis of measurable sets is

$$\prod_\lambda M_\lambda$$

where each $M_\lambda \subset X_\lambda$ has finite μ_λ-measure and $M_\lambda = Y_\lambda$ for almost all λ, and where

$$\mu\left(\prod_\lambda M_\lambda\right) = \prod_\lambda \mu_\lambda(M_\lambda).$$

7.3 The Adele Ring

Let K be a global field. For each normalized valuation $|\cdot|_v$ of K, let K_v denote the completion of K. If $|\cdot|_v$ is non-archimedean, let $\mathcal{O}_v$ denote the ring of integers of K_v.

Definition 7.3.1 (Adele Ring)**.** The *adele ring* $\mathbb{A}_K$ of K is the topological ring whose underlying topological space is the restricted topological product of the K_v with respect to the $\mathcal{O}_v$, and where addition and multiplication are defined componentwise:

$$(\mathbf{xy})_v = \mathbf{x}_v\mathbf{y}_v \qquad (\mathbf{x}+\mathbf{y})_v = \mathbf{x}_v + \mathbf{y}_v \qquad \text{for } \mathbf{x},\mathbf{y} \in \mathbb{A}_K. \tag{7.3.1}$$

It is readily verified that (i) this definition makes sense, i.e., if $\mathbf{x},\mathbf{y} \in \mathbb{A}_K$, then $\mathbf{xy}$ and $\mathbf{x}+\mathbf{y}$, whose components are given by (7.3.1), are also in $\mathbb{A}_K$, and (ii) that addition and multiplication are continuous in the $\mathbb{A}_K$-topology, so $\mathbb{A}_K$ is a topological ring, as asserted. Also, Lemma 7.2.4 implies that $\mathbb{A}_K$ is locally compact because the K_v are locally compact (Corollary 4.1.6), and the $\mathcal{O}_v$ are compact (Theorem 4.1.4).

There is a natural continuous ring inclusion

$$K \hookrightarrow \mathbb{A}_K \tag{7.3.2}$$

that sends $x \in K$ to the adele every one of whose components is x. This is an adele because $x \in \mathcal{O}_v$ for almost all v, by Lemma 7.1.2. The map is injective because each map $K \to K_v$ is an inclusion.

Definition 7.3.2 (Principal Adeles)**.** The image of (7.3.2) is the ring of *principal adeles*.

It will cause no trouble to identify K with the principal adeles, so we shall speak of K as a subring of $\mathbb{A}_K$.

Formation of the adeles is compatible with base change, in the following sense.

Lemma 7.3.3. *Suppose L is a finite (separable) extension of the global field K. Then*

$$\mathbb{A}_K \otimes_K L \cong \mathbb{A}_L \tag{7.3.3}$$

both algebraically and topologically. Under this isomorphism,

$$L \cong K \otimes_K L \subset \mathbb{A}_K \otimes_K L$$

maps isomorphically onto $L \subset \mathbb{A}_L$.

Proof. Let $\omega_1, \ldots, \omega_n$ be a basis for L/K and let v run through the normalized valuations on K. The left hand side of (7.3.3), with the tensor product topology, is the restricted product of the tensor products

$$K_v \otimes_K L \cong K_v \cdot \omega_1 \oplus \cdots \oplus K_v \cdot \omega_n$$

with respect to the integers

$$\mathcal{O}_v \cdot \omega_1 \oplus \cdots \oplus \mathcal{O}_v \cdot \omega_n. \tag{7.3.4}$$

(An element of the left hand side is a finite linear combination $\sum \mathbf{x}_i \otimes a_i$ of adeles $\mathbf{x}_i \in \mathbb{A}_K$ and coefficients $a_i \in L$, and there is a natural isomorphism from the ring of such formal sums to the restricted product of the $K_v \otimes_K L$.)

We proved before (Theorem 6.1.8) that

$$K_v \otimes_K L \cong L_{w_1} \oplus \cdots \oplus L_{w_g},$$

where $w_1, \ldots, w_g$ are the normalizations of the extensions of v to L. Furthermore, as we proved using discriminants (see Lemma 7.1.7), the above identification identifies (7.3.4) with

$$\mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g},$$

for almost all v. Thus the left hand side of (7.3.3) is the restricted product of the $L_{w_1} \oplus \cdots \oplus L_{w_g}$ with respect to the $\mathcal{O}_{w_1} \oplus \cdots \oplus \mathcal{O}_{w_g}$. But this is canonically isomorphic to the restricted product of all completions L_w with respect to $\mathcal{O}_w$, which is the right hand side of (7.3.3). This establishes an isomorphism between the two sides of (7.3.3) as topological spaces. The map is also a ring homomorphism, so the two sides are algebraically isomorphic, as claimed. □

Corollary 7.3.4. *Let $\mathbb{A}_K^+$ denote the topological group obtained from the additive structure on $\mathbb{A}_K$. Suppose L is a finite seperable extension of K. Then*

$$\mathbb{A}_L^+ = \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+, \qquad ([L:K] \text{ summands}).$$

In this isomorphism the additive group $L^+ \subset \mathbb{A}_L^+$ of the principal adeles is mapped isomorphically onto $K^+ \oplus \cdots \oplus K^+$.

Proof. For any nonzero $\omega \in L$, the subgroup $\omega \cdot \mathbb{A}_K^+$ of $\mathbb{A}_L^+$ is isomorphic as a topological group to $\mathbb{A}_K^+$ (the isomorphism is multiplication by $1/\omega$). By Lemma 7.3.3, we have isomorphisms

$$\mathbb{A}_L^+ = \mathbb{A}_K^+ \otimes_K L \cong \omega_1 \cdot \mathbb{A}_K^+ \oplus \cdots \oplus \omega_n \cdot \mathbb{A}_K^+ \cong \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+.$$

If $a \in L$, write $a = \sum b_i \omega_i$, with $b_i \in K$. Then a maps via the above map to

$$x = (\omega_1 \cdot \{b_1\}, \ldots, \omega_n \cdot \{b_n\}),$$

where $\{b_i\}$ denotes the principal adele defined by b_i. Under the final map, x maps to the tuple

$$(b_1, \ldots, b_n) \in K \oplus \cdots \oplus K \subset \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+.$$

The dimensions of L and of $K \oplus \cdots \oplus K$ over K are the same, so this proves the final claim of the corollary. □

Theorem 7.3.5. *The global field K is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K^+/K^+$ of additive groups is compact in the quotient topology.*

At this point Cassels remarks

> "It is impossible to conceive of any other uniquely defined topology on K. This metamathematical reason is more persuasive than the argument that follows!"

Proof. Corollary 7.3.4, with K for L and $\mathbb{Q}$ or $\mathbb{F}(t)$ for K, shows that it is enough to verify the theorem for $\mathbb{Q}$ or $\mathbb{F}(t)$, and we shall do it here for $\mathbb{Q}$.

To show that $\mathbb{Q}^+$ is discrete in $\mathbb{A}_\mathbb{Q}^+$ it is enough, because of the group structure, to find an open set U that contains $0 \in \mathbb{A}_\mathbb{Q}^+$, but which contains no other elements of $\mathbb{Q}^+$. (If $\alpha \in \mathbb{Q}^+$, then $U + \alpha$ is an open subset of $\mathbb{A}_\mathbb{Q}^+$ whose intersection with $\mathbb{Q}^+$ is $\{\alpha\}$.) We take for U the set of $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_\mathbb{Q}^+$ with

$$|x_\infty|_\infty < 1 \qquad \text{and} \qquad |x_p|_p \leq 1 \quad (\text{all } p),$$

where $|\cdot|_p$ and $|\cdot|_\infty$ are respectively the p-adic and the usual archimedean absolute values on $\mathbb{Q}$. If $b \in \mathbb{Q} \cap U$, then in the first place $b \in \mathbb{Z}$ because $|b|_p \leq 1$ for all p, and then $b = 0$ because $|b|_\infty < 1$. This proves that K^+ is discrete in $\mathbb{A}_\mathbb{Q}^+$. (If we leave out one valuation, as we will see later (Theorem 7.4.4), this theorem is false—what goes wrong with the proof just given?)

Next we prove that the quotient $\mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$ is compact. Let $W \subset \mathbb{A}_\mathbb{Q}^+$ consist of the $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_\mathbb{Q}^+$ with

$$|x_\infty|_\infty \leq \frac{1}{2} \qquad \text{and} \qquad |x_p|_p \leq 1 \qquad \text{for all primes } p.$$

We show that every adele $\mathbf{y} = \{y_v\}_v$ is of the form

$$\mathbf{y} = a + \mathbf{x}, \qquad a \in \mathbb{Q}, \quad \mathbf{x} \in W,$$

which will imply that the compact set W maps surjectively onto $\mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$. Fix an adele $\mathbf{y} = \{y_v\} \in \mathbb{A}_\mathbb{Q}^+$. Since $\mathbf{y}$ is an adele, for each prime p we can find a rational number

$$r_p = \frac{z_p}{p^{n_p}} \qquad \text{with} \quad z_p \in \mathbb{Z} \quad \text{and} \quad n_p \in \mathbb{Z}_{\geq 0}$$

such that

$$|y_p - r_p|_p \leq 1,$$

and

$$r_p = 0 \qquad \text{almost all } p.$$

More precisely, for the finitely many p such that

$$y_p = \sum_{n \geq -|s|} a_n p^n \notin \mathbb{Z}_p,$$

choose r_p to be a rational number that is the value of an appropriate truncation of the p-adic expansion of y_p, and when $y_p \in \mathbb{Z}_p$ just choose $r_p = 0$. Hence $r = \sum_p r_p \in \mathbb{Q}$ is well defined. The r_q for $q \neq p$ do not mess up the inequality $|y_p - r|_p \leq 1$ since the valuation $|\cdot|_p$ is non-archimedean and the r_q do not have any p in their denominator:

$$|y_p - r|_p = \left| y_p - r_p - \sum_{q \neq p} r_q \right|_p \leq \max\left(|y_p - r_p|_p, \left| \sum_{q \neq p} r_q \right|_p \right) \leq \max(1, 1) = 1.$$

Now choose $s \in \mathbb{Z}$ such that

$$|y_\infty - r - s| \leq \frac{1}{2}.$$

Then $a = r + s$ and $\mathbf{x} = \mathbf{y} - a$ do what is required, since $\mathbf{y} - a = \mathbf{y} - r - s$ has the desired property (since $s \in \mathbb{Z}$ and the p-adic valuations are non-archimedean).

Hence the continuous map $W \to \mathbb{A}_{\mathbb{Q}}^+/\mathbb{Q}^+$ induced by the quotient map $\mathbb{A}_{\mathbb{Q}}^+ \to \mathbb{A}_{\mathbb{Q}}^+/\mathbb{Q}^+$ is surjective. But W is compact (being the topological product of the compact spaces $|x_\infty|_\infty \leq 1/2$ and the $\mathbb{Z}_p$ for all p), hence $\mathbb{A}_{\mathbb{Q}}^+/\mathbb{Q}^+$ is also compact. □

Exercise 7.3.6. Prove Theorem 7.3.5, that "The global field K is discrete in $\mathbb{A}_K$ and the quotient $\mathbb{A}_K^+/K^+$ of additive groups is compact in the quotient topology." in the case when K is a finite extension of $\mathbb{F}(t)$, where $\mathbb{F}$ is a finite field.

Corollary 7.3.7. *There is a subset W of $\mathbb{A}_K$ defined by inequalities of the type $|x_v|_v \leq \delta_v$, where $\delta_v = 1$ for almost all v, such that every $\mathbf{y} \in \mathbb{A}_K$ can be put in the form*

$$\mathbf{y} = a + \mathbf{x}, \qquad a \in K, \quad \mathbf{x} \in W,$$

i.e., $\mathbb{A}_K = K + W$.

Proof. We constructed such a set for $K = \mathbb{Q}$ when proving Theorem 7.3.5. For general K the W coming from the proof determines compenent-wise a subset of $\mathbb{A}_K^+ \cong \mathbb{A}_{\mathbb{Q}}^+ \oplus \cdots \oplus \mathbb{A}_{\mathbb{Q}}^+$ that is a subset of a set with the properties claimed by the corollary. □

As already remarked, $\mathbb{A}_K^+$ is a locally compact group, so it has an invariant Haar measure. In fact one choice of this Haar measure is the product of the Haar measures on the K_v, in the sense of Definition 7.2.5.

Corollary 7.3.8. *The quotient $\mathbb{A}_K^+/K^+$ has finite measure in the quotient measure induced by the Haar measure on $\mathbb{A}_K^+$.*

Remark 7.3.9. This statement is independent of the particular choice of the multiplicative constant in the Haar measure on $\mathbb{A}_K^+$. We do not here go into the question of finding the measure $\mathbb{A}_K^+/K^+$ in terms of our explicitly given Haar measure. (See Tate's thesis, [Cp86, Chapter XV].)

Proof. This can be reduced similarly to the case of $\mathbb{Q}$ or $\mathbb{F}(t)$ which is immediate, e.g., the W defined above has measure 1 for our Haar measure.

Alternatively, finite measure follows from compactness. To see this, cover $\mathbb{A}_K/K^+$ with the translates of U, where U is a nonempty open set with finite measure. The existence of a finite subcover implies finite measure. □

Remark 7.3.10. We give an alternative proof of the product formula $\prod |a|_v = 1$ for nonzero $a \in K$. We have seen that if $x_v \in K_v$, then multiplication by x_v magnifies the Haar measure in K_v^+ by a factor of $|x_v|_v$. Hence if $\mathbf{x} = \{x_v\} \in \mathbb{A}_K$, then multiplication by $\mathbf{x}$ magnifies the Haar measure in $\mathbb{A}_K^+$ by $\prod |x_v|_v$. But now multiplication by $a \in K$ takes $K^+ \subset \mathbb{A}_K^+$ into K^+, so gives a well-defined bijection of $\mathbb{A}_K^+/K^+$ onto $\mathbb{A}_K^+/K^+$ which magnifies the measure by the factor $\prod |a|_v$. Hence $\prod |a|_v = 1$ by Corollary 7.3.8. (The point is that if μ is the measure of $\mathbb{A}_K^+/K^+$, then $\mu = \prod |a|_v \cdot \mu$, so because μ is finite we must have $\prod |a|_v = 1$.)

7.4 Strong Approximation

We first prove a technical lemma and corollary, then use them to deduce the strong approximation theorem, which is an extreme generalization of the Chinese Remainder Theorem; it asserts that K^+ is dense in the analogue of the adeles with one valuation removed.

The proof of Lemma 7.4.1 below will use in a crucial way the normalized Haar measure on $\mathbb{A}_K$ and the induced measure on the compact quotient $\mathbb{A}_K^+/K^+$. Since I am not formally developing Haar measure on locally compact groups, and since I didn't explain induced measures on quotients well in the last chapter, hopefully the following discussion will help clarify what is going on.

The real numbers $\mathbb{R}^+$ under addition is a locally compact topological group. Normalized Haar measure μ has the property that $\mu([a,b]) = b - a$, where $a \leq b$ are real numbers and $[a,b]$ is the closed interval from a to b. The subset $\mathbb{Z}^+$ of $\mathbb{R}^+$ is discrete, and the quotient $S^1 = \mathbb{R}^+/\mathbb{Z}^+$ is a compact topological group, which thus has a Haar measure. Let $\overline{\mu}$ be the Haar measure on S^1 normalized so that the natural quotient $\pi : \mathbb{R}^+ \to S^1$ preserves the measure, in the sense that if $X \subset \mathbb{R}^+$ is a measurable set that maps injectively into S^1, then $\mu(X) = \overline{\mu}(\pi(X))$. This determine $\overline{\mu}$ and we have $\overline{\mu}(S^1) = 1$ since $X = [0,1)$ is a measurable set that maps bijectively onto S^1 and has measure 1. The situation for the map $\mathbb{A}_K \to \mathbb{A}_K/K^+$ is pretty much the same.

Lemma 7.4.1. *There is a constant $C > 0$ that depends only on the global field K with the following property:*

Whenever $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_K$ is such that

$$\prod_v |x_v|_v > C, \tag{7.4.1}$$

then there is a nonzero principal adele $a \in K \subset \mathbb{A}_K$ such that

$$|a|_v \le |x_v|_v \qquad \text{for all } v.$$

Proof. This proof is modelled on Blichfeldt's proof of Minkowski's Theorem in the Geometry of Numbers, and works in quite general circumstances.

First we show that (7.4.1) implies that $|x_v|_v = 1$ for almost all v. Because $\mathbf{x}$ is an adele, we have $|x_v|_v \le 1$ for almost all v. If $|x_v|_v < 1$ for infinitely many v, then the product in (7.4.1) would have to be 0. (We prove this only when K is a finite extension of $\mathbb{Q}$.) Excluding archimedean valuations, this is because the normalized valuation $|x_v|_v = |\mathrm{Norm}(x_v)|_p$, which if less than 1 is necessarily $\le 1/p$. Any infinite product of numbers $1/p_i$ must be 0, whenever p_i is a sequence of primes.

Let c_0 be the Haar measure of $\mathbb{A}_K^+/K^+$ induced from normalized Haar measure on $\mathbb{A}_K^+$, and let c_1 be the Haar measure of the set of $\mathbf{y} = \{y_v\}_v \in \mathbb{A}_K^+$ that satisfy

$$\begin{aligned} |y_v|_v &\le \frac{1}{2} && \text{if } v \text{ is real archimedean,} \\ |y_v|_v &\le \frac{1}{2} && \text{if } v \text{ is complex archimedean,} \\ |y_v|_v &\le 1 && \text{if } v \text{ is non-archimedean.} \end{aligned}$$

(As we will see, any positive real number $\le 1/2$ would suffice in the definition of c_1 above. For example, in Cassels's article he uses the mysterious 1/10. He also doesn't discuss the subtleties of the complex archimedean case separately.)

Then $0 < c_0 < \infty$ since $\mathbb{A}_K/K^+$ is compact, and $0 < c_1 < \infty$ because the number of archimedean valuations v is finite. We show that

$$C = \frac{c_0}{c_1}$$

will do. Thus suppose $\mathbf{x}$ is as in (7.4.1).

The set T of $\mathbf{t} = \{t_v\}_v \in \mathbb{A}_K^+$ such that

$$\begin{aligned} |t_v|_v &\le \frac{1}{2}\,|x_v|_v && \text{if } v \text{ is real archimedean,} \\ |t_v|_v &\le \frac{1}{2}\sqrt{|x_v|_v} && \text{if } v \text{ is complex archimedean,} \\ |t_v|_v &\le |x_v|_v && \text{if } v \text{ is non-archimedean} \end{aligned}$$

has measure

$$c_1 \cdot \prod_v |x_v|_v > c_1 \cdot C = c_0. \tag{7.4.2}$$

(Note: If there are complex valuations, then the some of the $|x_v|_v$'s in the product must be squared.)

Because of (7.4.2), in the quotient map $\mathbb{A}_K^+ \to \mathbb{A}_K^+/K^+$ there must be a pair of distinct points of T that have the same image in $\mathbb{A}_K^+/K^+$, say

$$\mathbf{t}' = \{t'_v\}_v \in T \quad \text{and} \quad \mathbf{t}'' = \{t''_v\}_v \in T$$

and

$$a = \mathbf{t}' - \mathbf{t}'' \in K^+$$

is nonzero. Then

$$|a|_v = \left|t'_v - t''_v\right|_v \leq \begin{cases} |t'_v| + |t''_v| \leq 2 \cdot \frac{1}{2} |x_v|_v \leq |x_v|_v & \text{if } v \text{ is real archimedean, or} \\ \max(|t'_v|, |t''_v|) \leq |x_v|_v & \text{if } v \text{ is non-archimedean,} \end{cases}$$

for all v. In the case of complex archimedean v, we must be careful because the normalized valuation $|\cdot|_v$ is the *square* of the usual archimedean complex valuation $|\cdot|_\infty$ on $\mathbb{C}$, so e.g., it does not satisfy the triangle inequality. In particular, the quantity $|t'_v - t''_v|_v$ is at most the square of the maximum distance between two points in the disc in $\mathbb{C}$ of radius $\frac{1}{2}\sqrt{|x_v|_v}$, where by distance we mean the usual distance. This maximum distance in such a disc is at most $\sqrt{|x_v|_v}$, so $|t'_v - t''_v|_v$ is at most $|x_v|_v$, as required. Thus a satisfies the requirements of the lemma. □

Corollary 7.4.2. *Let v_0 be a normalized valuation and let $\delta_v > 0$ be given for all $v \neq v_0$ with $\delta_v = 1$ for almost all v. Then there is a nonzero $a \in K$ with*

$$|a|_v \leq \delta_v \qquad (\text{all } v \neq v_0).$$

Proof. This is just a degenerate case of Lemma 7.4.1. Choose $x_v \in K_v$ with $0 < |x_v|_v \leq \delta_v$ and $|x_v|_v = 1$ if $\delta_v = 1$. We can then choose $x_{v_0} \in K_{v_0}$ so that

$$\prod_{\text{all } v \text{ including } v_0} |x_v|_v > C.$$

Then Lemma 7.4.1 does what is required. □

Remark 7.4.3. The character group of the locally compact group $\mathbb{A}_K^+$ is isomorphic to $\mathbb{A}_K^+$ and K^+ plays a special role. See Chapter XV of [Cp86], Lang's [Lan64], Weil's [Wei82], and Godement's Bourbaki seminars 171 and 176. This duality lies behind the functional equation of ζ and L-functions. Iwasawa has shown [Iwa53] that the rings of adeles are characterized by certain general topologico-algebraic properties.

We proved before that K is discrete in $\mathbb{A}_K$. If one valuation is removed, the situation is much different.

Theorem 7.4.4 (Strong Approximation)**.** *Let v_0 be any normalized nontrivial valuation of the global field K. Let $\mathbb{A}_{K,v_0}$ be the restricted topological product of the K_v with respect to the $\mathcal{O}_v$, where v runs through all normalized valuations $v \neq v_0$. Then K is dense in $\mathbb{A}_{K,v_0}$.*

Proof. This proof was suggested by Prof. Kneser at the Cassels-Frohlich conference.

Recall that if $\mathbf{x} = \{x_v\}_v \in \mathbb{A}_{K,v_0}$ then a basis of open sets about $\mathbf{x}$ is the collection of products

$$\prod_{v \in S} B(x_v, \varepsilon_v) \times \prod_{v \notin S,\ v \neq v_0} \mathcal{O}_v,$$

where $B(x_v, \varepsilon_v)$ is an open ball in K_v about x_v, and S runs through finite sets of normalized valuations (not including v_0). Thus denseness of K in $\mathbb{A}_{K,v_0}$ is equivalent to the following statement about elements. Suppose we are given (i) a finite set S of valuations $v \neq v_0$, (ii) elements $x_v \in K_v$ for all $v \in S$, and (iii) an $\varepsilon > 0$. Then there is an element $b \in K$ such that $|b - x_v|_v < \varepsilon$ for all $v \in S$ and $|b|_v \leq 1$ for all $v \notin S$ with $v \neq v_0$.

By the corollary to our proof that $\mathbb{A}_K^+/K^+$ is compact (Corollary 7.3.7), there is a $W \subset \mathbb{A}_K$ that is defined by inequalities of the form $|y_v|_v \leq \delta_v$ (where $\delta_v = 1$ for almost all v) such that ever $\mathbf{z} \in \mathbb{A}_K$ is of the form

$$\mathbf{z} = \mathbf{y} + c, \qquad \mathbf{y} \in W, \quad c \in K. \tag{7.4.3}$$

By Corollary 7.4.2, there is a nonzero $a \in K$ such that

$$\begin{aligned} |a|_v &< \frac{1}{\delta_v} \cdot \varepsilon \qquad \text{for } v \in S, \\ |a|_v &\leq \frac{1}{\delta_v} \qquad \text{for } v \notin S,\ v \neq v_0. \end{aligned}$$

Hence on putting $\mathbf{z} = \frac{1}{a} \cdot \mathbf{x}$ in (7.4.3) and multiplying by a, we see that every $\mathbf{x} \in \mathbb{A}_K$ is of the shape

$$\mathbf{x} = \mathbf{w} + b, \qquad \mathbf{w} \in a \cdot W, \quad b \in K,$$

where $a \cdot W$ is the set of $a\mathbf{y}$ for $\mathbf{y} \in W$. If now we let $\mathbf{x}$ have components the given x_v at $v \in S$, and (say) 0 elsewhere, then $b = \mathbf{x} - \mathbf{w}$ has the properties required. □

Remark 7.4.5. The proof gives a quantitative form of the theorem (i.e., with a bound for $|b|_{v_0}$). For an alternative approach, see [Mah64].

In the next chapter we'll introduce the ideles $\mathbb{A}_K^*$. Finally, we'll relate ideles to ideals, and use everything so far to give a new interpretation of class groups and their finiteness.

Chapter 8

Ideles and Ideals

In this chapter, we introduce the ideles $\mathbb{I}_K$, and relate ideles to ideals, and use what we've done so far to give an alternative interpretation of class groups and their finiteness, thus linking the adelic point of view with the classical point of view of the first part of this course.

8.1 The Idele Group

The invertible elements of any commutative topological ring R are a group R^* under multiplication. In general R^* is not a topological group if it is endowed with the subset topology because inversion need not be continuous (only multiplication and addition on R are required to be continuous). It is usual therefore to give R^* the following topology. There is an injection

$$x \mapsto \left(x,\ \frac{1}{x}\right) \tag{8.1.1}$$

of R^* into the topological product $R \times R$. We give R^* the corresponding subset topology. Then R^* with this topology is a topological group and the inclusion map $R^* \hookrightarrow R$ is continous. To see continuity of inclusion, note that this topology is finer (has at least as many open sets) than the subset topology induced by $R^* \subset R$, since the projection maps $R \times R \to R$ are continuous.

Example 8.1.1. This is a "non-example". The inverse map on $\mathbb{Z}_p^*$ is continuous with respect to the p-adic topology. If $a, b \in \mathbb{Z}_p^*$, then $|a| = |b| = 1$, so if $|a - b| < \varepsilon$, then

$$\left|\frac{1}{a} - \frac{1}{b}\right| = \left|\frac{b-a}{ab}\right| = \frac{|b-a|}{|ab|} < \frac{\varepsilon}{1} = \varepsilon.$$

Definition 8.1.2 (Idele Group)**.** The *idele group* $\mathbb{I}_K$ of K is the group $\mathbb{A}_K^*$ of invertible elements of the adele ring $\mathbb{A}_K$.

We shall usually speak of $\mathbb{I}_K$ as a subset of $\mathbb{A}_K$, and will have to distinguish between the $\mathbb{I}_K$ and $\mathbb{A}_K$-topologies.

Example 8.1.3. For a rational prime p, let $\mathbf{x}_p \in \mathbb{A}_{\mathbb{Q}}$ be the adele whose pth component is p and whose vth component, for $v \neq p$, is 1. Then $\mathbf{x}_p \to 1$ as $p \to \infty$ in $\mathbb{A}_{\mathbb{Q}}$, for the following reason. We must show that if U is a basic open set that contains the adele $1 = \{1\}_v$, the $\mathbf{x}_p$ for all sufficiently large p are contained in U. Since U contains 1 and is a basic open set, it is of the form

$$\prod_{v \in S} U_v \times \prod_{v \notin S} \mathbb{Z}_v,$$

where S is a finite set, and the U_v, for $v \in S$, are arbitrary open subsets of $\mathbb{Q}_v$ that contain 1. If q is a prime larger than any prime in S, then $\mathbf{x}_p$ for $p \geq q$, is in U. This proves convergence. If the inverse map were continuous on $\mathbb{I}_K$, then the sequence of $\mathbf{x}_p^{-1}$ would converge to $1^{-1} = 1$. However, if U is an open set as above about 1, then for sufficiently large p, *none* of the adeles $\mathbf{x}_p$ are contained in U.

Lemma 8.1.4. *The group of ideles $\mathbb{I}_K$ is the restricted topological project of the K_v^* with respect to the units $U_v = \mathcal{O}_v^* \subset K_v$, with the restricted product topology.*

We omit the proof of Lemma 8.1.4, which is a matter of thinking carefully about the definitions. The main point is that inversion is continuous on $\mathcal{O}_v^*$ for each v. (See Example 8.1.1.)

We have seen that K is naturally embedded in $\mathbb{A}_K$, so K^* is naturally embedded in $\mathbb{I}_K$.

Definition 8.1.5 (Principal Ideles)**.** We call K^*, considered as a subgroup of $\mathbb{I}_K$, the *principal ideles*.

Lemma 8.1.6. *The principal ideles K^* are discrete as a subgroup of $\mathbb{I}_K$.*

Proof. For K is discrete in $\mathbb{A}_K$, so K^* is embedded in $\mathbb{A}_K \times \mathbb{A}_K$ by (8.1.1) as a discrete subset. (Alternatively, the subgroup topology on $\mathbb{I}_K$ is finer than the topology coming from $\mathbb{I}_K$ being a subset of $\mathbb{A}_K$, and K is already discrete in $\mathbb{A}_K$.) □

Definition 8.1.7 (Content of an Idele)**.** The *content* of $\mathbf{x} = \{x_v\}_v \in \mathbb{I}_K$ is

$$c(\mathbf{x}) = \prod_{\text{all } v} |x_v|_v \in \mathbb{R}_{>0}.$$

Lemma 8.1.8. *The map $\mathbf{x} \to c(\mathbf{x})$ is a continuous homomorphism of the topological group $\mathbb{I}_K$ into $\mathbb{R}_{>0}$, where we view $\mathbb{R}_{>0}$ as a topological group under multiplication. If K is a number field, then c is surjective.*

Proof. That the content map c satisfies the axioms of a homomorphisms follows from the multiplicative nature of the defining formula for c. For continuity, suppose (a, b) is an open interval in $\mathbb{R}_{>0}$. Suppose $\mathbf{x} \in \mathbb{I}_K$ is such that $c(\mathbf{x}) \in (a, b)$. By considering small intervals about each non-unit component of $\mathbf{x}$, we find an open neighborhood $U \subset \mathbb{I}_K$ of $\mathbf{x}$ such that $c(U) \subset (a, b)$. It follows the $c^{-1}((a, b))$ is open.

For surjectivity, use that each archimedean valuation is surjective, and choose an idele that is 1 at all but one archimedean valuation. □

Remark 8.1.9. Note also that the $\mathbb{I}_K$-topology is that appropriate to a group of operators on $\mathbb{A}_K^+$: a basis of open sets is the $S(C,U)$, where $C, U \subset \mathbb{A}_K^+$ are, respectively, $\mathbb{A}_K$-compact and $\mathbb{A}_K$-open, and S consists of the $\mathbf{x} \in \mathbb{I}_J$ such that $(1-\mathbf{x})C \subset U$ and $(1-\mathbf{x}^{-1})C \subset U$.

Definition 8.1.10 (1-Ideles)**.** The subgroup $\mathbb{I}_K^1$ of 1-*ideles* is the subgroup of ideles $\mathbf{x} = \{x_v\}$ such that $c(\mathbf{x}) = 1$. Thus $\mathbb{I}_K^1$ is the kernel of c, so we have an exact sequence

$$1 \to \mathbb{I}_K^1 \to \mathbb{I}_K \xrightarrow{c} \mathbb{R}_{>0} \to 1,$$

where the surjectivity on the right is only if K is a number field.

Lemma 8.1.11. *The subset $\mathbb{I}_K^1$ of $\mathbb{A}_K$ is closed as a subset, and the $\mathbb{A}_K$-subset topology on $\mathbb{I}_K^1$ coincides with the $\mathbb{I}_K$-subset topology on $\mathbb{I}_K^1$.*

Proof. Let $\mathbf{x} \in \mathbb{A}_K$ with $\mathbf{x} \notin \mathbb{I}_K^1$. To prove that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, we find an $\mathbb{A}_K$-neighborhood W of $\mathbf{x}$ that does not meet $\mathbb{I}_K^1$.

1st Case. Suppose that $\prod_v |x_v|_v < 1$ (possibly $= 0$). Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and
2. $\prod_{v \in S} |x_v|_v < 1$.

Then the set W can be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\le 1 \qquad v \notin S \end{aligned}$$

for sufficiently small ε.

2nd Case. Suppose that $C := \prod_v |x_v|_v > 1$. Then there is a finite set S of v such that

1. S contains all the v with $|x_v|_v > 1$, and
2. if $v \notin S$ an inequality $|w_v|_v < 1$ implies $|w_v|_v < \frac{1}{2C}$. (This is because for a non-archimedean valuation, the largest absolute value less than 1 is $1/p$, where p is the residue characteristic. Also, the upper bound in Cassels's article is $\frac{1}{2}C$ instead of $\frac{1}{2C}$, but I think he got it wrong.)

We can choose ε so small that $|w_v - x_v|_v < \varepsilon$ (for $v \in S$) implies $1 < \prod_{v \in S} |w_v|_v < 2C$. Then W may be defined by

$$\begin{aligned} |w_v - x_v|_v &< \varepsilon \qquad v \in S \\ |w_v|_v &\le 1 \qquad v \notin S. \end{aligned}$$

This works because if $\mathbf{w} \in W$, then either $|w_v|_v = 1$ for all $v \notin S$, in which case $1 < c(\mathbf{w}) < 2c$, so $\mathbf{w} \notin \mathbb{I}_K^1$, or $|w_{v_0}|_{v_0} < 1$ for some $v_0 \notin S$, in which case

$$c(\mathbf{w}) = \left(\prod_{v \in S} |w_v|_v\right) \cdot |w_{v_0}| \cdots < 2C \cdot \frac{1}{2C} \cdots < 1,$$

so again $\mathbf{w} \notin \mathbb{I}_K^1$.

We next show that the $\mathbb{I}_K$- and $\mathbb{A}_K$-topologies on $\mathbb{I}_K^1$ are the same. If $\mathbf{x} \in \mathbb{I}_K^1$, we must show that every $\mathbb{A}_K$-neighborhood of $\mathbf{x}$ contains an $\mathbb{I}_K$-neighborhood and vice-versa.

Let $W \subset \mathbb{I}_K^1$ be an $\mathbb{A}_K$-neighborhood of $\mathbf{x}$. Then it contains an $\mathbb{A}_K$-neighborhood of the type

$$|w_v - x_v|_v < \varepsilon \qquad v \in S \tag{8.1.2}$$

$$|w_v|_v \leq 1 \qquad v \notin S \tag{8.1.3}$$

where S is a finite set of valuations v. This contains the $\mathbb{I}_K$-neighborhood in which $\leq$ in (8.1.2) is replaced by $=$.

Next let $H \subset \mathbb{I}_K^1$ be an $\mathbb{I}_K$-neighborhood. Then it contains an $\mathbb{I}_K$-neighborhood of the form

$$|w_v - x_v|_v < \varepsilon \qquad v \in S \tag{8.1.4}$$

$$|w_v|_v = 1 \qquad v \notin S, \tag{8.1.5}$$

where the finite set S contains at least all archimedean valuations v and all valuations v with $|x_v|_v \neq 1$. Since $\prod |x_v|_v = 1$, we may also suppose that ε is so small that (8.1.4) implies

$$\prod_v |w_v|_v < 2.$$

Then the intersection of (8.1.4) with $\mathbb{I}_K^1$ is the same as that of (8.1.2) with $\mathbb{I}_K^1$, i.e., (8.1.4) defines an $\mathbb{A}_K$-neighborhood. □

By the product formula we have that $K^* \subset \mathbb{I}_K^1$. The following result is of vital importance in class field theory.

Theorem 8.1.12. *The quotient $\mathbb{I}_K^1/K^*$ with the quotient topology is compact.*

Proof. After the preceeding lemma, it is enough to find an $\mathbb{A}_K$-compact set $W \subset \mathbb{A}_K$ such that the map

$$W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^*$$

is surjective. We take for W the set of $\mathbf{w} = \{w_v\}_v$ with

$$|w_v|_v \leq |x_v|_v\,,$$

where $\mathbf{x} = \{x_v\}_v$ is any idele of content greater than the C of Lemma 7.4.1.

Let $\mathbf{y} = \{y_v\}_v \in \mathbb{I}_K^1$. Then the content of $\mathbf{x}/\mathbf{y}$ equals the content of $\mathbf{x}$, so by Lemma 7.4.1 there is an $a \in K^*$ such that

$$|a|_v \leq \left|\frac{x_v}{y_v}\right|_v \qquad \text{all } v.$$

Then $a\mathbf{y} \in W$, as required. □

Remark 8.1.13. The quotient $\mathbb{I}_K^1/K^*$ is totally disconnected in the function field case. For the structure of its connected component in the number field case, see papers of Artin and Weil in the "Proceedings of the Tokyo Symposium on Algebraic Number Theory, 1955" (Science Council of Japan) or [AT90]. The determination of the character group of $\mathbb{I}_K/K^*$ is global class field theory.

8.2 Ideals and Divisors

Suppose that K is a finite extension of $\mathbb{Q}$. Let F_K be the the free abelian group on a set of symbols in bijection with the non-archimedean valuation v of K. Thus an element of F_K is a formal linear combination

$$\sum_{v \text{ non arch.}} n_v \cdot v$$

where $n_v \in \mathbb{Z}$ and all but finitely many n_v are 0.

Lemma 8.2.1. *There is a natural bijection between F_K and the group of nonzero fractional ideals of $\mathcal{O}_K$. The correspondence is induced by*

$$v \mapsto \wp_v = \{x \in \mathcal{O}_K : v(x) < 1\},$$

where v is a non-archimedean valuation.

Endow F_K with the discrete topology. Then there is a natural continuous map $\pi : \mathbb{I}_K \to F_K$ given by

$$\mathbf{x} = \{x_v\}_v \mapsto \sum_v \mathrm{ord}_v(x_v) \cdot v.$$

This map is continuous since the inverse image of a valuation v (a point) is the product

$$\pi^{-1}(v) = \pi\mathcal{O}_v^* \quad \times \prod_{w \text{ archimedean}} K_w^* \quad \times \prod_{w \neq v \text{ non-arch.}} \mathcal{O}_w^*,$$

which is an open set in the restricted product topology on $\mathbb{I}_K$. Moreover, the image of K^* in F_K is the group of nonzero principal fractional ideals.

Recall that the *class group* C_K of the number field K is by definition the quotient of F_K by the image of K^*.

Theorem 8.2.2. *The class group C_K of a number field K is finite.*

Proof. We first prove that the map $\mathbb{I}_K^1 \to F_K$ is surjective. Let ∞ be an archimedean valuation on K. If v is a non-archimedean valuation, let $\mathbf{x} \in \mathbb{I}_K^1$ be a 1-idele such that $x_w = 1$ at ever valuation w except v and ∞. At v, choose $x_v = \pi$ to be a generator for the maximal ideal of $\mathcal{O}_v$, and choose x_∞ to be such that $|x_\infty|_\infty = 1/|x_v|_v$. Then $\mathbf{x} \in \mathbb{I}_K$ and $\prod_w |x_w|_w = 1$, so $\mathbf{x} \in \mathbb{I}_K^1$. Also $\mathbf{x}$ maps to $v \in F_K$.

Thus the group of ideal classes is the continuous image of the compact group $\mathbb{I}_K^1/K^*$ (see Theorem 8.1.12), hence compact. But a compact discrete group is finite. □

8.2.1 The Function Field Case

When K is a finite separable extension of $\mathbb{F}(t)$, we define the divisor group D_K of K to be the free abelian group on all the valuations v. For each v the number of elements of the residue class field $\mathbb{F}_v = \mathcal{O}_v/\wp_v$ of v is a power, say q^{n_v}, of the number q of elements in $\mathbb{F}$. We call n_v the degree of v, and similarly define $\sum n_v d_v$ to be the degree of the divisor $\sum n_v \cdot v$. The divisors of degree 0 form a group D_K^0. As before, the principal divisor attached to $a \in K^*$ is $\sum \mathrm{ord}_v(a) \cdot v \in D_K$. The following theorem is proved in the same way as Theorem 8.2.2.

Theorem 8.2.3. *The quotient of D_K^0 modulo the principal divisors is a finite group.*

8.2.2 Jacobians of Curves

For those familiar with algebraic geometry and algebraic curves, one can prove Theorem 8.2.3 from an alternative point of view. There is a bijection between nonsingular geometrically irreducible projective curves over $\mathbb{F}$ and function fields K over $\mathbb{F}$ (which we assume are finite separable extensions of $\mathbb{F}(t)$ such that $\overline{\mathbb{F}} \cap K = \mathbb{F}$). Let X be the curve corresponding to K. The group D_K^0 is in bijection with the divisors of degree 0 on X, a group typically denoted $\mathrm{Div}^0(X)$. The quotient of $\mathrm{Div}^0(X)$ by principal divisors is denoted $\mathrm{Pic}^0(X)$. The *Jacobian* of X is an abelian variety $J = \mathrm{Jac}(X)$ over the finite field $\mathbb{F}$ whose dimension is equal to the genus of X. Moreover, assuming X has an $\mathbb{F}$-rational point, the elements of $\mathrm{Pic}^0(X)$ are in natural bijection with the $\mathbb{F}$-rational points on J. In particular, with these hypothesis, the class group of K, which is isomorphic to $\mathrm{Pic}^0(X)$, is in bijection with the group of $\mathbb{F}$-rational points on an algebraic variety over a finite field. This gives an alternative more complicated proof of finiteness of the degree 0 class group of a function field.

Without the degree 0 condition, the divisor class group won't be finite. It is an extension of $\mathbb{Z}$ by a finite group.

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \xrightarrow{\deg} n\mathbb{Z} \to 0,$$

where n is the greatest common divisor of the degrees of elements of $\mathrm{Pic}(X)$, which is 1 when X has a rational point.

Bibliography

[Art59] E. Artin, *Theory of algebraic numbers*, Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, vol. 1956/7, George Striker, Schildweg 12, Göttingen, 1959. MR 24 #A1884

[AT90] E. Artin and J. Tate, *Class field theory*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1990. MR 91b:11129

[Cas67] J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42–84.

[Cas91] ———, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991. MR 92k:11058

[Cp86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[Iwa53] K. Iwasawa, *On the rings of valuation vectors*, Ann. of Math. (2) **57** (1953), 331–356. MR 14,849a

[Lan64] S. Lang, *Algebraic numbers*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR 28 #3974

[Mah64] K. Mahler, *Inequalities for ideal bases in algebraic number fields*, J. Austral. Math. Soc. **4** (1964), 425–448. MR 31 #1243

[Ser73] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[Wei82] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono. MR 83m:10032