VOORTGEZETTE GETALTHEORIE

P. Stevenhagen

Universiteit Leiden
2017

Disclaimer

These notes are being polished and extended as we go...
Readers who come across typos and inaccuracies or have suggestions for improvements: please send e-mail to psh@math.leidenuniv.nl!

Table of contents

Introduction

In the first part of these notes ('Number rings'), we proved the basic theorems on the arithmetic of algebraic number fields. The first part of the theory, dealing with ideal factorization in number rings, was completely algebraic, and used only ring theoretic arguments. The second part made specific use of the fact that number rings allow embeddings in Euclidean spaces, and the resulting theorems on the finiteness of the class group and the structure of the unit group of the ring of integers are particular for number rings. Although the terminology from commutative algebra we employed is of a more recent nature, the results we have proved so far are mostly classical, going back to 19-th century mathematicians as Kummer, Dirichlet, Kronecker and Dedekind.

The theory to be developed in this second half of the notes concerns some important extensions of the theory that were obtained during the period 1895–1950. We start with the valuation theory introduced by Hensel in the early 20-th century, which yields a more 'topological' or 'analytic' approach to the theory of ideal factorization. This leads in a natural way to the notion of a complete field, and for number fields the process of completion gives rise to *local fields* like the field $\mathbf{R}$ of real numbers and the fields $\mathbf{Q}_p$ of p-adic numbers. As was shown by Hasse, it is often fruitful to develop the global theory from the local case, since local fields are in many ways 'easier' than number fields, somewhat in the same way as localized number rings tend to be 'easier' than general number rings. The interplay between local and global fields finds its ultimate form in Chevalley's definition of adèles and idèles.

The power and esthetic impact of these more modern concepts is particularly visible in the *class field theory*, which allows a classical ideal theoretic and a more recent idelic formulation. Although it has its roots in the 19th century work of Kronecker, Weber and Hilbert, it is a 20th century theory that was developed by Takagi, Artin, Hasse and Chevalley during the period 1915–1945, and was reformulated once more in cohomological terms, in the second half of the twentieth century. We will apply class field theory to very classical problems such as the representation of integers by binary quadratic forms and the derivation of higher (than quadratic) reciprocity laws.

1 Valued fields

Valuation theory provides an approach to the arithmetic of number fields by methods reminiscent of those in complex function theory, which describe functions by locally convergent Laurent series expansions. More precisely, one considers the field $\mathcal{M}$ of meromorphic functions on $\mathbf{C}$ obtained as the field of fractions of the ring $\mathcal{O}$ of holomorphic functions on $\mathbf{C}$, and writes $f \in \mathcal{M}$ in the neighborhood of a point $\alpha \in \mathbf{C}$ as a convergent series

$$f(z) = \sum_{k \gg -\infty}^{\infty} a_k (z - \alpha)^k$$

with complex coefficients a_k that are zero for almost all $k < 0$. The 'local variable' $z - \alpha$ is not unique in the sense that we can write f as a Laurent series in any variable $w \in \mathcal{M}$ that has a simple zero at α. If f is not identically zero, the lowest index k with $a_k \neq 0$ does not depend on the choice of the local variable and is known as the order $\mathrm{ord}_\alpha(f)$ of f at α. A function $f \in \mathcal{M}^*$ is determined up to multiplication by a function without zeroes and poles by the values $\mathrm{ord}_\alpha(f)$ for $\alpha \in \mathbf{C}$. These functions are precisely the units in $\mathcal{O}$. One often encounters subfields of $\mathcal{M}$ instead of $\mathcal{M}$, such as the rational function field $\mathbf{C}(X) \subset \mathcal{M}$ consisting of those $f \in \mathcal{M}$ that allow a meromorphic extension to the Riemann sphere $\mathbf{P}^1(\mathbf{C})$. Finite extensions of $\mathbf{C}(X)$ inside $\mathcal{M}$ arise as function fields associated to algebraic curves.

Exercise 1. Show that $\mathbf{C}(X) \subset \mathcal{M}$ satisfies $\mathbf{C}(X) \cap \mathcal{O} = \mathbf{C}[X]$ and $\mathbf{C}(X) \cap \mathcal{O}^* = \mathbf{C}^*$.

In the early 20th century, the German mathematician Hensel observed that every non-zero element of a number field K can be viewed in a similar way as a function on the set of primes of the ring of integers $\mathcal{O}_K$ of K, since every non-zero element x has an order $\mathrm{ord}_\mathfrak{p}(x) \in \mathbf{Z}$ at each prime $\mathfrak{p}$. The subring of 'holomorphic elements' $x \in K$ that have $\mathrm{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p}$ is the ring of integers $\mathcal{O}_K$, and an element $x \in K^*$ is determined up to multiplication by an element in $\mathcal{O}_K^*$ by the values $\mathrm{ord}_\mathfrak{p}(x)$. If $\pi \in K$ is an element of order 1 at $\mathfrak{p}$, we can try to write x like the function f above as a Laurent series

$$x = \sum_{k \gg -\infty}^{\infty} a_k \pi^k$$

that converges 'locally at $\mathfrak{p}$'. Apart from the fact that we have to specify which coefficients $a_k \in K$ can occur in this series, we need to define a notion of 'convergence around $\mathfrak{p}$' for series in K in order for this statement to make sense.

▶ Valuations

Valuations, which can be thought of as 'absolute values' on arbitrary fields K, provide a tool to introduce a metric topology on K. We will see in Theorem 2.7 that '$\mathfrak{p}$-adic valuations' on a number field K lead to $\mathfrak{p}$-adic expansions of elements in K, and in the $\mathfrak{p}$-adic *completions* $K_\mathfrak{p}$ of K.

1.1. Definition. *A valuation on a field K is a function $\phi : K \to \mathbf{R}_{\geq 0}$ satisfying*
(1) *$\phi(x) = 0$ if and only if $x = 0$;*
(2) *$\phi(xy) = \phi(x)\phi(y)$ for $x, y \in K$;*
(3) *there exists $C \in \mathbf{R}_{>0}$ such that $\phi(x + y) \leq C \max\{\phi(x), \phi(y)\}$ for all $x, y \in K$.*

Conditions (1) and (2) describe the absolute value ϕ as the extension of a homomorphism $K^* \to \mathbf{R}_{>0}$ to all of K, obtained by putting $\phi(0) = 0$. Condition (3) expresses its 'continuity' with respect to addition. The smallest possible constant C in (3) is the *norm* $||\phi||$ of the valuation ϕ. It cannot be smaller than 1, and by (2) it equals

$$||\phi|| = \sup_{x:\ \phi(x)\leq 1} \phi(1 + x).$$

This supremum is actually a maximum and, as will become clear, it is actually assumed for $x \in \{0, 1\}$ (exercise 9). If ϕ is a valuation and r a positive real number, then $x \mapsto \phi(x)^r$ defines a valuation of norm $||\phi||^r$.

The valuations that are implicit in the two situations described above are the valuation $\phi_\alpha : \mathcal{M} \to \mathbf{R}_{\geq 0}$ defined by

$$\phi_\alpha(f) = c^{\mathrm{ord}_\alpha(f)} \qquad \text{for some } c \in (0, 1)$$

for $f \neq 0$ and the valuation $\phi_\mathfrak{p} : K \to \mathbf{R}_{\geq 0}$ defined by

$$\phi_\mathfrak{p}(x) = c^{\mathrm{ord}_\mathfrak{p}(x)} \qquad \text{for some } c \in (0, 1)$$

for $x \neq 0$. These definitions also make sense for $f = 0$ and $x = 0$ if we symbolically set $\mathrm{ord}_\alpha(0) = \mathrm{ord}_\mathfrak{p}(0) = +\infty$. From the obvious identities

$$\mathrm{ord}_\alpha(f_1 + f_2) \geq \min\{\mathrm{ord}_\alpha(f_1), \mathrm{ord}_\alpha(f_2)\}$$
$$\mathrm{ord}_\mathfrak{p}(x_1 + x_2) \geq \min\{\mathrm{ord}_\mathfrak{p}(x_1), \mathrm{ord}_\mathfrak{p}(x_2)\}$$

we see that the norm of ϕ_α and $\phi_\mathfrak{p}$ equals 1. The value of the constant c in their definition is irrelevant for most purposes, and in 1.8 we will introduce a corresponding notion of equivalence of valuations. A valuation ϕ of norm 1 satisfies the *ultrametric inequality*

$$\phi\left(\textstyle\sum_{k=1}^n x_i\right) \leq \max_{k=1,2,\ldots,n} \phi(x_k) \tag{1.2}$$

and is called *non-archimedean*. If (1.2) holds, a sum of small elements will never be large, so in this case the Archimedean postulate, which states that a 'small but non-zero' quantity becomes arbitrarily large when repeatedly added to itself, does not hold. When quantities of unequal size are added under a non-archimedean valuation, the ultrametric inequality becomes an equality:

$$\phi(x_1) \neq \phi(x_2) \Rightarrow \phi(x_1 + x_2) = \max\{\phi(x_1), \phi(x_2)\}. \tag{1.3}$$

To see this, one supposes $\phi(x_1) > \phi(x_2)$ and concludes from the inequalities

$$\phi(x_1) = \phi(x_1 + x_2 - x_2) \leq \max\{\phi(x_1 + x_2), \phi(-x_2)\} \leq \max\{\phi(x_1), \phi(x_2)\} = \phi(x_1)$$

that we have $\phi(x_1 + x_2) = \phi(x_1)$. The value $\phi(-1) = 1$ used here is immediate from the fact that its square equals $\phi(1) = 1$. The ultrametric inequality is much stronger than the more familiar *triangle inequality*

$$\phi(\textstyle\sum_{k=1}^{n} x_i) \leq \sum_{k=1}^{n} \phi(x_i),$$

and this has amusing consequences for the geometry of the underlying space (exercise 8). A trivial example of a non-archimedean valuation that exists on any field K is the *trivial valuation* on K, obtained by extending the trivial homomorphism $\phi : K^* \to \{1\}$.

Exercise 2. Show that every valuation on a finite field is trivial.

Valuations of norm larger than 1 are called *archimedean*. Characteristic examples are the valuations $\phi_\sigma : K \to \mathbf{R}_{\geq 0}$ obtained from embeddings $\sigma : K \to \mathbf{C}$ as

$$\phi_\sigma(x) = |\sigma(x)|. \tag{1.4}$$

Valuations of this form have norm 2 and satisfy the triangle inequality.

▶ Metrics and topology

Although valuations are not required to satisfy the triangle inequality, they do when raised to a suitable power. This is a consequence of the following lemma.

1.5. Lemma. *A valuation on a field K satisfies the triangle inequality if and only if its norm does not exceed 2.*

Proof. It is clear that a valuation satisfying the triangle inequality has norm at most 2. Conversely, if ϕ has norm at most 2, we can repeatedly apply condition (3) in Definition 1.1 to obtain $\phi(\sum_{i=1}^{2^m} x_i) \leq 2^m \max_i \phi(x_i)$. Taking some of the x_i in this inequality equal to 0, we see that a sum of k terms can be bounded by $\phi(\sum_{i=1}^{k} x_i) \leq 2k \max_i \phi(x_i)$. In particular, we have $\phi(k \cdot 1) \leq 2k$ for $k \in \mathbf{Z}_{\geq 1}$. We now use the multiplicativity of ϕ to obtain the estimate

$$\begin{aligned}\phi(x+y)^n = \phi(\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}) &\leq 2(n+1) \max_i \{\phi(\binom{n}{i} x^i y^{n-i})\} \\ &\leq 4(n+1) \sum_{i=0}^{n} \binom{n}{i} \phi(x)^i \phi(y)^{n-i} = 4(n+1)(\phi(x) + \phi(y))^n.\end{aligned}$$

The resulting inequality $\phi(x+y) \leq \sqrt[n]{4(n+1)}(\phi(x) + \phi(y))$ is valid for all $x, y \in K$ and implies the triangle inequality if we let n tend to infinity. □

An argument similar to that given in the preceding proof shows that it is possible to decide whether a valuation is non-archimedean by looking at its values on multiples of the unit element only.

1.6. Proposition. *A valuation on a field K is non-archimedean if and only if it is bounded on the set $\{n \cdot 1 : n \in \mathbf{Z}\}$.*

Proof. It is clear from the ultrametric inequality 1.2 that we have $\phi(\pm n \cdot 1) \leq \phi(1) = 1$ if ϕ is non-archimedean. For the converse, we assume that ϕ is a valuation that is bounded by M on $\{n \cdot 1 : n \in \mathbf{Z}\}$ and—after replacing ϕ by a suitable power if necessary—that it satisfies the triangle inequality. Taking n-th roots of both sides of the estimate

$$\phi(x+y)^n = \phi(\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}) \leq (n+1)M \max\{\phi(x), \phi(y)\}^n$$

and letting n tend to infinity, we see that ϕ is non-archimedean. □

We see from 1.6 that we can always take the upper bound $M = 1$ for a valuation bounded on $\mathbf{Z}$. This is also immediate from the multiplicativity of valuations.

For a field K of positive characteristic, the set $\{n \cdot 1 : n \in \mathbf{Z}\}$ in 1.6 is finite set.

1.7. Corollary. *A valuation on a field of positive characteristic is non-archimedean.* □

Let ϕ be a valuation on a field K. Then there is a natural valuation topology $\mathcal{T}_\phi$ on K in which a basis of open neighborhoods of a point $x \in K$ is given by the collection of open balls

$$U_\varepsilon(x) = \{y \in K : \phi(x-y) < \varepsilon\} \qquad (\varepsilon \in \mathbf{R}_{>0})$$

of radius ε around x. As all powers of ϕ induce the same topology, the topology $\mathcal{T}_\phi$ is metrizable by 1.5.

Exercise 3. Show that $\mathcal{T}_\phi$ is the discrete topology on K if and only if ϕ is trivial.

Just as for the ordinary absolute value on $\mathbf{R}$ or $\mathbf{C}$, one shows for the valuation topology that the addition map $(x, y) \mapsto x+y$ and the multiplication map $(x, y) \mapsto xy$ are continuous maps from $K \times K$ to K, and that the inversion map $x \mapsto x^{-1}$ is continuous on K^*. These continuity properties can be summarized by stating that the valuation topology $\mathcal{T}_\phi$ on K makes K into a *topological field*.

By the ultramatric property (1.3), a non-archimedean topological field K is topologically rather different from archimedean topological fields such as $\mathbf{R}$ and $\mathbf{C}$. For instance, given points $x, y, z \in K$ for which $x - y$ and $y - z$ have different valuation, the sum $x - z = (x - y) + (y - z)$ has the same valuation as either $x - y$ or $y - z$: every triangle in K is isosceles. In the same vein, it follows from the fact that every two points x, y in an open ball $U_\varepsilon(x_0)$ have distance

$$\phi(x-y) = \phi(x - x_0 + x_0 - y) \leq \max\{\phi(x-x_0), \phi(x_0-y)\} < \varepsilon$$

that every point in this open ball is a center: $U_\varepsilon(x) = U_\varepsilon(x_0) = U_\varepsilon(y)$.

▶ Independence of valuations

Two valuations ϕ and ψ on a field K are said to be *equivalent* if they induce the same topology on K. Equivalence can easily be decided using the following proposition.

1.8. Proposition. *Let ϕ and ψ be two non-trivial valuations on a field K. Then the following conditions are equivalent.*
(1) *$\phi = \psi^r$ for some constant $r > 0$;*
(2) *ϕ and ψ are equivalent;*
(3) *the topology $\mathcal{T}_\phi$ is stronger than $\mathcal{T}_\psi$;*
(4) *$\phi(x) < 1$ implies $\psi(x) < 1$ for all $x \in K$.*

Proof. The implications (1) ⇒ (2) and (2) ⇒ (3) are clear. As the inequality $\phi(x) < 1$ amounts to saying that the sequence $\{x^n\}_n$ converges to 0 in the corresponding valuation topology, we also have (3) ⇒ (4).

In order to prove (4) ⇒ (1), we take an element $a \in K$ with $0 < \phi(a) < 1$. Such an element exists because ϕ is non-trivial. We claim that we actually have an equivalence

$$\phi(x) < 1 \Longleftrightarrow \psi(x) < 1.$$

Indeed, take $x \in K$ with $\psi(x) < 1$. If we had $\phi(x) > 1$ then x^{-1} would violate (4), and if we had $\phi(x) = 1$ then ax^{-k} would violate (4) for large k. Thus $\phi(x) < 1$ as desired.

Next, let $x \in K^*$ be arbitrary and define $\alpha, \beta \in \mathbf{R}$ by $\phi(x) = \phi(a)^\alpha$ and $\psi(x) = \psi(a)^\beta$. We want to show that $\alpha = \beta$, since this implies that $r = \log \phi(x)/\log \psi(x) = \log \phi(a)/\log \psi(a)$ does not depend on x, i.e. that we have $\phi = \psi^r$ for this r. The desired equality follows from the fact that for $m, n \in \mathbf{Z}$ with $n > 0$ we have

$$\tfrac{m}{n} < \alpha \Longleftrightarrow \phi(x) < \phi(a)^{m/n} \Longleftrightarrow \phi(x^n a^{-m}) < 1 \Longleftrightarrow \psi(x^n a^{-m}) < 1 \Longleftrightarrow \tfrac{m}{n} < \beta.$$

This finishes the proof of the proposition. □

If ϕ and ψ are non-trivial valuations on K that are not equivalent, the proof of 1.8 shows that we can find $a \in K$ satisfying $\phi(a) < 1$ and $\psi(b) \geq 1$, and also $b \in K$ satisfying $\phi(a) \geq 1$ and $\psi(b) < 1$. The element $x = a/b$ then satisfies $\phi(x) < 1$ and $\psi(x) > 1$, and this means that the elements

$$x_k = \frac{x^k}{1 + x^k}$$

converge for $k \to \infty$ to 0 in $\mathcal{T}_\phi$, and to 1 in T_ψ. For $k \to \infty$ the limits are 1 and 0, respectively. This 'unrelated behavior' leads to an independence of non-equivalent valuations that can be phrased in the following way for any number $n \geq 2$ of valuations.

1.9. Approximation theorem. *Let $\phi_1, \phi_2, \ldots, \phi_n$ be n non-trivial valuations on K, and suppose that no two of them are equivalent. Write K_i for the field K equipped with the topology $\mathcal{T}_{\phi_i}$, and $\Delta = K \cdot (1, 1, \ldots, 1)$ for the image of K under the diagonal embedding $K \longrightarrow \prod_{i=1}^n K_i$. Then Δ is dense in $\prod_{i=1}^n K_i$.*

Proof. We may and will assume $n \geq 2$, the case $n = 1$ being trivial.

By the continuity of the field operations in the valuation topologies T_{ϕ_i}, the closure $\overline{\Delta}$ of Δ is a K-vector subspace of the n-dimensional K-vector space $\prod_{i=1}^n K_i$. For $n = 2$, we observed just before the theorem that $\overline{\Delta}$ that contains the basis vectors $(0, 1)$ and $(1, 0)$ as limits of elements $x^n/(1 + x^n) \cdot (1, 1) \in \Delta$. This implies $\overline{\Delta} = K_1 \times K_2$, as desired.

In order to prove the general case by induction, we assume that the theorem holds for $n - 1 \geq 2$ valuations. This implies that we can find $a \in K$ satisfying $\phi_1(a) > 1$ and $\phi_i(a) < 1$ for $2 \leq i \leq n - 1$, and also $b \in K$ satisfying $\phi_1(b) > 1$ and $\phi_n(b) < 1$.

If we have $\phi_n(a) \leq 1$, then $x = a^m b$ with m sufficiently large will be an element for which $x^n/(1 + x^n) \cdot (1, 1, \ldots, 1)$ converges to the basis vector $(1, 0, \ldots, 0)$. If we have $\phi_n(a) > 1$, then $x = a^m b/(1 + a^m)$ with m sufficiently large has this property. Thus $\overline{\Delta}$ contains $(1, 0, \ldots, 0)$, and therefore all basis vectors, yielding $\overline{\Delta} = \prod_{i=1}^n K_i$. □

In less formal terms, the approximation theorem states that given ϕ_i as above and any choice of elements $a_i \in K$ for $1 \leq i \leq n$, there exists $x \in K$ such that x is arbitrarily close to a_i in the topology $\mathcal{T}_{\phi_i}$ for all i.

▶ Prime divisors

An equivalence class of non-trivial valuations on K is known as a *place* or *prime divisor* of K, often shortened to *prime* of K. By the proposition, the prime divisor corresponding to a non-trivial valuation ϕ is the equivalence class $\{\phi^r : r > 0\}$. Depending on the type of valuations it contains, a prime divisor is said to be archimedean or non-archimedean. Archimedean prime divisors are also known as *infinite primes*, as opposed to the *finite primes* denoting the non-archimedean prime divisors.

The terminology 'prime' to denote an equivalence class of valuations stems from the fact that, at least in the non-archimedean case, they are closely related to the prime ideals in subrings of K. The most classical case is the classification of the prime divisors of the rational number field $\mathbf{Q}$, due to Ostrowski.

1.10. Theorem. *A non-trivial valuation on* $\mathbf{Q}$ *is either equivalent to the* p*-adic valuation* $\phi_p : \mathbf{Q} \to \mathbf{R}$ *given by*

$$\phi_p(x) = p^{-\operatorname{ord}_p(x)}$$

for a prime number p*, or to the ordinary absolute value on* $\mathbf{Q}$ *given by*

$$\phi_\infty(x) = |x|.$$

Proof. Let ϕ be a non-archimedean valuation on $\mathbf{Q}$. Then ϕ is bounded by 1 on $\mathbf{Z}$, and the set $\mathfrak{p} = \{x \in \mathbf{Z} : \phi(x) < 1\}$ is easily seen to be a prime ideal of $\mathbf{Z}$. It is non-zero as ϕ is non-trivial, so we have $\mathfrak{p} = p\mathbf{Z}$ for some prime number p. As all elements in $\mathbf{Z} \setminus p\mathbf{Z}$ have valuation 1, the valuation ϕ assumes the value 1 on all fractions $u = \frac{a}{b}$ with $p \nmid ab$. Writing arbitrary $x \in \mathbf{Q}^*$ as $x = up^k$ with u as above and $k = \operatorname{ord}_p(x) \in \mathbf{Z}$, we find that we have $\phi(x) = c^{\operatorname{ord}_p(x)}$ with $c = \phi(p) \in (0, 1)$, and that ϕ is equivalent to ϕ_p.

Suppose now that ϕ is an archimedean valuation on $\mathbf{Q}$. We may assume that it satisfies the triangle inequality, implying $\phi(k) \leq |k|$ for $k \in \mathbf{Z}$. Given two integers $m, n > 1$, we can write all powers of m in base n as $m^t = \sum_{i=0}^{s} a_i n^i$ with $a_i \in \{0, 1, \ldots, n-1\}$ and $a_s \neq 0$. As the number of digits s is the entier of $\log(m^t)/\log n$, we have $s/t \leq \log m/\log n$. The triangle inequality implies $\phi(m)^t \leq (s+1)n \max\{1, \phi(n)^s\}$, so we can take t-th roots and let t tend to infinity to obtain the estimate

$$\phi(m) \leq \max\{1, \phi(n)\}^{\log m/\log n}.$$

This shows that we must have $\phi(n) > 1$, since otherwise ϕ would be bounded on $\mathbf{Z}$ and therefore non-archimedean. The resulting inequality $\phi(m)^{1/\log m} \leq \phi(n)^{1/\log n}$ is in fact an equality, as we can interchange the roles of m and n. Thus $a = \phi(n)^{1/\log n} > 1$ does not depend on the value of $n > 1$, and we have $\phi(n) = |n|^{\log a}$ for all $n \in \mathbf{Z}$. This implies $\phi(x) = |x|^{\log a}$ for all $x \in \mathbf{Q}$, showing ϕ to be equivalent to the ordinary absolute value ϕ_∞ on $\mathbf{Q}$. □

The normalization of the p-adic valuation ϕ_p in 1.10 is standard, and chosen in such a way that we have have the *product formula*

$$\prod_{p \leq \infty} \phi_p(x) = 1 \qquad \text{for} \quad x \in \mathbf{Q}^*.$$

Here the product is taken over all prime divisors of $\mathbf{Q}$, including the unique infinite prime. It shows that the approximation theorem 1.9 does not necessarily hold for an *infinite* collection of non-equivalent valuations.

Exercise 4. Show that Chinese remainder theorem for $\mathbf{Z}$ can be obtained as a special case of the approximation theorem.

The argument used to classify the non-archimedean primes of $\mathbf{Q}$ can be used in more general situations. For any non-archimedean valuation ϕ on a field K, the ultrametric property of ϕ implies that

$$A_\phi = \{x \in K : \phi(x) \leq 1\}$$

is a subring of K, the *valuation ring* of ϕ. We have $x \in A_\phi$ or $x^{-1} \in A_\phi$ for every $x \in K^*$. In particular, A_ϕ has field of fractions K. The valuation ring A_ϕ is a local ring with unit group $A_\phi^* = \{x \in K : \phi(x) = 1\}$ and maximal ideal

$$\mathfrak{m}_\phi = \{x \in K : \phi(x) < 1\}.$$

The quotient $k_\phi = A_\phi/\mathfrak{m}_\phi$ is known as the *residue class field* of ϕ.

Exercise 5. Which possibilities are there for the pair $(\mathrm{char}(K), \mathrm{char}(k_\phi))$ of field characteristics?

Just as for $K = \mathbf{Q}$, the finite primes of a number field 'are' the primes of its ring of integers.

1.11. Theorem. *Every non-trivial non-archimedean valuation on a number field K is of the form*

$$\phi_\mathfrak{p}(x) = c^{\mathrm{ord}_\mathfrak{p}(x)} \qquad \textit{with} \quad c \in (0,1)$$

for some non-zero prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K. In this way, the finite primes of K correspond bijectively to the non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_K$.

Proof. If ϕ is a non-archimedean valuation on a number field K, then the ring of integers $\mathcal{O}_K$ is contained in the valuation ring A_ϕ. To see this, one observes that every $x \in \mathcal{O}_K$ satisfies some equation $x^n = \sum_{i=0}^{n-1} a_i x^i$ with $n \geq 1$ and coefficients $a_i \in \mathbf{Z}$. We have $\phi(a_i) \leq 1$, so $\phi(x) > 1$ would imply $\phi(x^n) > \max_{i=1,2\cdots,n-1} \phi(a_i x^i)$, contradicting (1.2).

If ϕ is non-trivial, then $\mathfrak{m}_\phi \cap \mathcal{O}_K$ is a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and ϕ is identically 1 on $\mathcal{O}_K \setminus \mathfrak{p}$. The local ring $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring, say with maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$, and we have $\phi[\mathcal{O}_\mathfrak{p}^*] = 1$. Writing $x \in K^*$ as $x = u\pi^k$ with $u \in \mathcal{O}_\mathfrak{p}^*$ and $k = \mathrm{ord}_\mathfrak{p}(x)$, we find $\phi_\mathfrak{p}(x) = c^{\mathrm{ord}_\mathfrak{p}(x)}$ with $c = \phi(\pi) \in (0,1)$.

As $\phi_\mathfrak{p}$ and $\phi_{\mathfrak{p}'}$ are clearly inequivalent for $\mathfrak{p} \neq \mathfrak{p}'$, this shows that the finite primes of K correspond bijectively to the non-zero prime ideals $\mathfrak{p} \subset \mathcal{O}_K$. □

The valuation ring corresponding to a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is the ring

$$\mathcal{O}_{K,\mathfrak{p}} = \{\frac{a}{b} : a \in \mathcal{O}_K, b \in \mathcal{O}_K \setminus \mathfrak{p}\}$$

defined in [Number rings, §2] by localizing the ring of integers $\mathcal{O}_K$ at the prime $\mathfrak{p}$.

If $K = F(X)$ is the field of rational functions over a field F, the argument used in proving 1.11 yields the following.

1.12. Theorem. *Let $R = F[X]$ be the polynomial ring over a field F and ϕ a non-trivial valuation on its field of fractions $K = F(X)$ that is trivial on F. Then ϕ is either a P-adic valuation ϕ_P given by*

$$\phi_P(x) = c^{\mathrm{ord}_P(x)} \qquad \textit{with } c \in (0,1)$$

for some non-constant monic irreducible polynomial $P \in R$, or the degree valuation ϕ_∞ given by

$$\phi_\infty(x) = c^{-\deg(x)} \qquad \textit{with } c \in (0,1)$$

for $x \neq 0$. Here deg *is the multiplicative extension to K^* of the degree map $R \setminus \{0\} \to \mathbf{Z}$.*

Proof. As ϕ is trivial on F, it is non-archimedean by 1.6. Suppose first that we have $\phi(X) \leq 1$. Then $R = F[X]$ is a subring of the valuation ring K_ϕ, so so $\mathfrak{p} = \mathfrak{m}_\phi$ is a prime ideal of $R = F[X]$. It is non-zero as ϕ is non-trivial, so $\mathfrak{p} = (P)$ for some non-constant monic irreducible polynomial $P \in R$. All elements in $R \setminus \mathfrak{p}$ have valuation 1, and ϕ assumes the value 1 on all units of the localized ring $R_\mathfrak{p}$. As before, K is the field of fractions of the discrete valuation ring $R_\mathfrak{p}$, and any $x \in K^*$ can be written as $x = uP^k$ with $u \in R_\mathfrak{p}^*$ and $k = \mathrm{ord}_P(x) \in \mathbf{Z}$. In this situation we have $\phi(x) = \phi(P)^k$, so we find $\phi = \phi_P$ with constant $c = \phi(P) \in (0,1)$.

Suppose now that we have $\phi(X) > 1$. Then we have $\phi(X^{-1}) < 1$, so the previous argument can be repeated with the ring $F[X^{-1}]$ in the role of R. This time the prime ideal $\mathfrak{p} \subset F[X^{-1}]$ contains X^{-1}, so we have $\mathfrak{p} = X^{-1}F[X^{-1}]$. To finish the proof we note the equality $\mathrm{ord}_{X^{-1}}(x) = -\deg(x)$, which yields $\phi = \phi_\infty$ with constant $c = \phi(X^{-1})$. □

▶ Finite and infinite primes

If F is finite, then *all* valuations of $F(X)$ are trivial on F and 1.12 provides all valuations on $F(X)$. If F is algebraically closed, then the monic irreducibles in $F[X]$ are of the form $X - \alpha$ with $\alpha \in F$, and the primes ϕ_P in 1.12 correspond to the 'points' of F. One can view $-\deg(x)$ as the order of the zero of x at the 'point at infinity' $\infty = 1/0$. In geometric terms, $K = F(X)$ is the function field of the projective line $\mathbf{P}^1(F)$, and primes of K are the points of $\mathbf{P}^1(F)$. This point of view is fundamental in the theory of algebraic curves, as it neatly generalizes to arbitrary projective curves.

It is a standard fact from algebraic geometry that the most elegant and uniform results are usually obtained for projective curves, which provide a 'compactification' of the more familiar affine curves by the addition of finitely many 'points at infinity'. In the same way the consideration of *all* primes of a number field, not just the finite ones, is in many ways the 'right' way to approach number fields. This point of view was introduced by Weil and Chevalley, who incorporated it around 1940 in their construction of ideles. It was further developed by Arakelov and others.

For projective curves, the notion of being a point 'at infinity' is not canonical, and the degree valuation ϕ_∞, which corresponds to the discrete valuation ring $F[X^{-1}]_{(X^{-1})}$, is in no intrinsic way different from the valuation ϕ_X with valuation ring $F[X]_{(X)}$: it also corresponds to a finite prime of $F(X)$. Number fields are different from function fields in the sense that they have 'intrinsically' infinite primes, i.e., non-archimedean primes. We will prove in 2.4 that the infinite primes of a number field are of the type given in (1.4), and come from the finitely many complex embeddings of the field.

▶ Discrete valuation rings

The proofs of 1.10, 1.11 and 1.12 show that non-archimedean valuations on K often come from discrete valuation rings $R \subset K$, and as their name indicates such rings provide valuations on their field of fractions. In line with this terminology, we call a valuation $\phi : K \to \mathbf{R}_{\geq 0}$ *discrete* if $\phi[K^*]$ is a discrete subgroup of $\mathbf{R}_{>0}$. An archimedean valuation on a field K can not be discrete as it follows from 1.6 and 1.7 that we have $\mathbf{Q} \subset K$ with ϕ non-trivial on $\mathbf{Q}$, and then from 1.10 that $\phi[K^*]$ contains the dense subgroup $\phi[\mathbf{Q}^*] \subset \mathbf{R}_{>0}$. As expected, discrete valuation rings are indeed the valuation rings coming from non-trivial discrete valuations.

1.13. Proposition. *Let ϕ be a non-trivial non-archimedean valuation on a field K and A_ϕ the valuation ring of ϕ. Then ϕ is discrete if and only if A_ϕ is a discrete valuation ring.*

Proof. Suppose that A is a discrete valuation ring and π a generator of its maximal ideal. Then every $x \in K^*$ has a unique representation as $x = u\pi^k$ with $u \in A^*$ and $k \in \mathbf{Z}$. Units in A have valuation 1, so $\phi(x) = \phi(\pi)^k$ and $\phi[K^*]$ is the discrete subgroup of $\mathbf{R}_{>0}$ generated by $\phi(\pi)$.

Conversely, let $\phi[K^*] \neq \{1\}$ be discrete in $\mathbf{R}_{>0}$. Then $\phi[K^*]$ is infinite cyclic (cf. exercise 11), so we can find $\pi \in A$ such that $\phi[K^*]$ is generated by $\phi(\pi)$. For any $x \in K^*$

there exists $k \in \mathbf{Z}$ with $\phi(x) = \phi(\pi)^k$, so we have $x = u\pi^k$ for some $u \in A^*$. It follows that A is a discrete valuation ring with maximal ideal πA. □

Let ϕ be a non-trivial discrete valuation on K with valuation ring A. If $\pi \in A$ generates the maximal ideal $\mathfrak{p}$ of A, we say that π is a *prime element* for ϕ, or a *uniformizer* or *local parameter* at the corresponding prime. The function $\nu : K \to \mathbf{Z} \cup \{\infty\}$ sending $x \in K^*$ to $\mathrm{ord}_{\mathfrak{p}}(x) \in \mathbf{Z}$ and $0 \in K$ to ∞ is the (normalized) *exponential valuation* corresponding to ϕ. It is a homomorphism on K^* that fits in a natural exact sequence

$$0 \to A^* \longrightarrow K^* \xrightarrow{\nu} \mathbf{Z} \to 0.$$

Every choice of π leads to a splitting of this exact sequence, and an isomorphism

$$K^* = \langle \pi \rangle \times A^*. \tag{1.14}$$

A fundamental system of neighborhoods of $0 \in K$ in the valuation topology $\mathcal{T}_\phi$ is given by the integral powers $\pi^k A$ of the maximal ideal of K. Note that these are additive subgroups of K. Analogously, the subgroups $1 + \pi^k A \subset K^*$ form a fundamental system of neighborhoods of 1 inside A^*, when k ranges over the positive integers. Note that these neighborhoods are both open and closed, and that the topological groups K and K^* are therefore totally disconnected. This shows that the topology of K is different from what we are used to for the archimedean fields $\mathbf{R}$ and $\mathbf{C}$.

Exercises

6. An *exponential valuation* on a field K is a map $\nu : K \to \mathbf{R} \cup \{\infty\}$ satisfying
   (1) $\nu(x) = \infty$ if and only if $x = 0$;
   (2) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K$;
   (3) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K$.
   Show that there is a natural bijective correspondence between exponential valuations and non-archimedean valuations on K. What does it mean for exponential valuations to be 'non-trivial', 'discrete' or 'equivalent'?

7. Let L/K be an algebraic extension and ϕ a valuation on L. Show that ϕ is trivial if and only if its restriction to K is trivial.

8. Show that the norm of a valuation ϕ on a field K equals $\max\{\phi(1), \phi(2)\}$.

9. Let F be a field and H a subgroup of $\mathbf{R}_{>0}$. Recall that the group ring $F[H]$ consists of *finite* formal sums $\sum_{h \in H} f_h[h]$ with $f_h \in F$, with addition and multiplication being derived from addition and multiplication in F and the relations $[h_1][h_2] = [h_1 h_2]$ for $h_1, h_2 \in H$. For non-zero $x \in F[H]$ we set

$$\phi\Big(\sum_{h \in H} f_h[h]\Big) = \max\{h \in H : f_h \neq 0\}.$$

Show that $F[H]$ is a domain, and that ϕ induces a non-archimedean valuation on the field of fractions K of $F[H]$ with image $\phi[K^*] = H$. What is the residue class field of this valuation?

10. Let ϕ be a valuation on a field K. Show that the value group $\phi[K^*]$ is either a discrete or a dense subgroup of $\mathbf{R}_{>0}$, and that it is cyclic if and only if it is discrete.

11. Do there exist a field K and a non-trivial valuation ϕ on K for which we can strengthen the implication (1.3) to an equivalence

$$\phi(x+y) = \max\{\phi(x), \phi(y)\} \Longleftrightarrow \phi(x) \neq \phi(y)$$

valid for all $x, y \in K^*$?

12. Show that there is a unique valuation on $\mathbf{C}$ that extends the ordinary absolute value on $\mathbf{R}$.

13. Let ϕ be a non-trivial discrete valuation, A its valuation ring, and $k_\mathfrak{p} = A/\mathfrak{p}$ its residue class field. Write $U_k = 1 + \mathfrak{p}^k$ for $k \in \mathbf{Z}_{>0}$.
    a. Show that $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ is a 1-dimensional vector space over $k_\mathfrak{p}$;
    b. Show that the map $x \mapsto x - 1$ induces a group isomorphism $U_k/U_{k+1} \xrightarrow{\sim} \mathfrak{p}^k/\mathfrak{p}^{k+1}$.

14. Let ϕ be a non-archimedean valuation on K. For $c \in \mathbf{R}_{>0}$, define $\psi_c : K[X] \to \mathbf{R}_{>0}$ by

$$\psi_c(\textstyle\sum_i a_i X^i) = \max_i \phi(a_i) c^i.$$

    a. Show that ψ_c gives rise to a valuation on the field of fractions $K(X)$ of $K[X]$ that extends ϕ.
    b. Show that ψ_{c_1} and ψ_{c_2} are not equivalent for ϕ non-trivial and $c_1 \neq c_2$.
    c. Which prime divisors are obtained when ϕ is trivial on K?

15. *(Gauss's lemma.)* Let A be the valuation ring of a non-archimedean valuation on a field K. Prove that if the product of two monic polynomials $f, g \in K[X]$ is in $A[X]$, then f and g are in $A[X]$. How does the classical Gauss lemma (with $A = \mathbf{Z}$ and $K = \mathbf{Q}$) follow from this? [Hint: you can use the valuation ψ_1 from the preceding exercise.]

16. Let K be a field and $\sigma, \tau : K \to \mathbf{C}$ two embeddings of K in the field of complex numbers. Show that the induced archimedean valuations ϕ_σ and ϕ_τ on K are equivalent if and only if we have $\sigma = \tau$ or $\sigma = \overline{\tau}$.

17. Let F be a finite field, and $K = F(X)$ the rational functional field over F. Show every $x \in K^*$ satisfies a 'sum formula'

$$\sum_\nu \nu(x) = 0$$

analogous to the product formula for $K = \mathbf{Q}$, when ν ranges over all *suitably* normalized exponential valuations on K.

2 Complete fields

In calculus, one learns that the right setting to study functions defined over the rational number field $\mathbf{Q}$ is not $\mathbf{Q}$ itself: in order to obtain a satisfactory theory, one uses a completion process to pass from $\mathbf{Q}$ to the real number field $\mathbf{R}$, or the algebraic closure $\mathbf{C}$ of $\mathbf{R}$. In the same way, functions on a valued field K are studied most conveniently over the *completion* of K with respect to the valuation, or an algebraic extension of this completion.

▶ Completions

A valued field K is said to be *complete* if every Cauchy sequence in K has a limit in K. Given K with valuation ϕ, we can construct its *completion* with respect to ϕ. The construction is similar to Cantor's construction of $\mathbf{R}$ from $\mathbf{Q}$, but uses the existence of the complete field $\mathbf{R}$ containing the values of ϕ.

2.1. Theorem. *Let ϕ be a valuation on K. Then there exists a field extension $K \subset K_\phi$ and an extension of ϕ to a valuation on K_ϕ such that K_ϕ is a complete valued field containing K as a dense subfield.*
For every field extension F of K that is complete with respect to a valuation extending ϕ, there exists a unique continuous K-homomorphism $K_\phi \to F$.

Proof. Let $\mathfrak{R}$ be the K-algebra of Cauchy sequences in K with componentwise addition and multiplication, and extend ϕ to $\mathfrak{R}$ by putting

$$\phi((a_i)_{i=1}^\infty) = \lim_{i\to\infty} \phi(a_i).$$

The ideal $\mathfrak{m} = \{a \in \mathfrak{R} : \phi(a) = 0\}$ of null-sequences is a maximal $\mathfrak{R}$-ideal as $a = (a_i)_{i=1}^\infty \notin \mathfrak{m}$ implies $a_i \neq 0$ for i sufficiently large, making a invertible in $\mathfrak{R}/\mathfrak{m}$. The composition $K \to \mathfrak{R} \to \mathfrak{R}/\mathfrak{m} = K_\phi$ yields a field inclusion $K \subset K_\phi = \mathfrak{R}/\mathfrak{m}$, and ϕ is descends to a map $K_\phi \to \mathbf{R}_{\geq 0}$ that is easily checked to be a valuation on K_ϕ extending ϕ. The subfield K is dense in K_ϕ, as the element $(a_i)_{i=1}^\infty \bmod \mathfrak{m} \in K_\phi$ is the limit of the sequence $(a_i)_{i=1}^\infty$ in K. Moreover, K_ϕ is complete as we can choose, for any given Cauchy sequence $(x_i)_{i=1}^\infty$ in K_ϕ, a sequence of elements $a_i \in K \subset K_\phi$ such that $\overline{\phi}(x_i - a_i) < 1/i$ holds. Then $x = (a_i)_{i=1}^\infty$ is a Cauchy sequence in K, and $x \bmod \mathfrak{m} \in K_\phi$ is the limit of $(x_i)_{i=1}^\infty$.

Finally, if $F \supset K$ is complete with respect to a valuation extending ϕ, the canonical map $\mathfrak{R} \to F$ sending $(a_i)_{i=1}^\infty$ to $\lim_{i\to\infty} a_i$ gives rise to a topological embedding $K_\phi = \mathfrak{R}/\mathfrak{m} \to F$. As K is dense in K_ϕ, there can be at most one continuous K-homomorphism $K_\phi \to F$, so this embedding is unique. □

▶ Complete archimedean fields

The last statement in theorem 2.1 implies that the completion K_ϕ is uniquely determined up to topological isomorphism. It also implies that a complete archimedean field, which contains the prime field $\mathbf{Q}$ on which the valuation is non-trivial by 1.6 and equal to a

power of the ordinary absolute value by Ostrowski's earlier theorem 1.10, contains the real number field $\mathbf{R}$ as a topological subfield. The following lemma allows us to focus on the case were K also contains the complex number field $\mathbf{C}$ as a topological subfield.

2.2. Lemma. *Let K be a field that is complete with respect to a valuation ϕ, and $L = K(i)$ the extension of K obtained by adjoining a root i of X^2+1. Then L is complete with respect to the valuation $\psi : L \to \mathbf{R}_{\geq 0}$ defined by*

$$\psi(x) = \phi(N_{L/K}(x))^{1/[L:K]}.$$

Proof. For $i \in K$, we have $L = K(i) = K$ and $\psi = \phi$, so there is nothing to prove.

Assume $i \notin K$. Then the map ψ is multiplicative and non-zero on L^*, and on the K-basis $\{1, i\}$ of L we have $\psi(a+bi) = \phi(a^2+b^2)^{1/2}$ for $a, b \in K$. Replacing ϕ if necessary by a power, we can assume that ϕ satisfies the triangle inequality. In order to show that ψ is a valuation, we need to show that $\psi(x) \leq 1$ implies $\psi(1+x) \leq C$ for some $C \in \mathbf{R}_{>0}$. Writing $x = a + bi$, we see that it suffices to show that $\phi(a)$ and $\phi(b)$ remain bounded when $a, b \in K$ satisfy the inequality $\phi(a^2 + b^2) \leq 1$.

We argue by contradiction, and assume that $\phi(a)$ is unbounded under the inequality $\phi(1 + (b/a)^2) < \phi(a)^{-2}$. This yields elements $x_n \in K$ satisfying $\phi(1 + x_n^2) < 4^{-n}$, and therefore, by the triangle inequality for ϕ,

$$\phi(x_{n+1} - x_n)\phi(x_{n+1} + x_n) = \phi((1 + x_{n+1}^2) - (1 + x_n^2)) < 2 \cdot 4^{-n}.$$

Upon changing the sign of x_{n+1} where necessary, we obtain $\phi(x_{n+1} - x_n) < 2^{-n}$ for all $n \geq 1$, making $(x_n)_n$ into a Cauchy sequence in the complete field K. Its limit $x \in K$ satisfies $x^2 + 1 = 0$, contrary to the assumption $i \notin K$.

The argument above also shows that if $\phi(a^2+b^2)$ tends to 0, then so do $\phi(a)$ and $\phi(b)$. Indeed, if $\phi(a)$ would be bounded away from zero, then $\phi(1 + (b/a)^2) = \phi(a)^{-2}\phi(a^2 + b^2)$ would tend to zero, leading to the same contradiction. This implies that L is complete with respect to ψ, as convergence in L amounts to convergence of the coefficients on the K-basis $\{1, i\}$. □

Lemma 2.2 does not assume that ϕ is archimedean, and the formula it gives to extend ϕ to a finite extension is a generality that we will encounter again in 3.3.

We will now show that no complete archimedean fields exist beyond the familiar examples $\mathbf{R}$ and $\mathbf{C}$. This theorem, which goes by the name of Ostrowski in valuation theory, is also known as the Gelfand-Mazur theorem in Banach algebras.

2.3. Theorem. *A complete archimedean field is topologically isomorphic to either $\mathbf{R}$ or $\mathbf{C}$.*

Proof. We already saw that a complete archimedean field K contains $\mathbf{R}$ as a topological subfield. By Lemma 2.2, the (possibly trivial) extension $L = K(i)$ is a complete archimedean field containing $\mathbf{C}$ as a topological subfield. It now suffices to show that L equals $\mathbf{C}$, as we then have $\mathbf{R} \subset K \subset L = \mathbf{C}$, leaving no further choice for K.

Write ψ for the valuation on L, and scale it to satisfy the triangle inequality. Suppose there exists $\alpha \in L \setminus \mathbf{C}$. Then the function $\mathbf{C} \to \mathbf{R}$ defined by $z \mapsto \psi(z-\alpha)$ is positive on all of $\mathbf{C}$, and as $\psi(z-\alpha) \geq \psi(z)(1-\psi(\alpha/z))$ tends to infinity with $\psi(z)$, there exists an element $z_0 \in \mathbf{C}$ where $\psi(z-\alpha)$ attains its minimum value $r > 0$. If $z \in \mathbf{C}$ satisfies $\psi(z-z_0) < r$, we can use *Ostrowski's identity*

$$\psi(z-\alpha) = \frac{\psi((z-z_0)^n - (\alpha - z_0)^n)}{\prod_{\zeta^n=1, \zeta \neq 1} \psi(\zeta(z-z_0) - (\alpha - z_0))}$$

to obtain, for all integers $n \geq 1$, an inequality

$$\psi(z-\alpha) \leq r^{1-n}\psi(z_0-\alpha)^n \psi(1 - \frac{(z-z_0)^n}{(\alpha-z_0)^n}) \leq r(1 + (\frac{\psi(z-z_0)}{r})^n).$$

Letting n tend to infinity, we find $\psi(z-\alpha) = r$ for all z satisfying $\psi(z-z_0) < r$. Repeating the argument, we see that $\psi(z-\alpha)$ is constant on $\mathbf{C}$. This contradiction shows that no element $\alpha \in L \setminus \mathbf{C}$ exists, and finishes the proof. □

2.4. Corollary. *Let ϕ be an archimedean valuation on K. Then there exist an embedding $\sigma : K \to \mathbf{C}$ and $r \in \mathbf{R}_{>0}$ such that $\phi(x) = |\sigma(x)|^r$ holds for $x \in K$.*

Proof. Theorems 2.1 and 2.3 show that we have an embedding $\sigma : K \to \mathbf{C}$ of topological fields, so the topology T_ϕ coincides with the topology of the valuation ϕ_σ from (1.4) that is induced by σ. By 1.8, this implies $\phi = \phi_\sigma^r$. □

If two embeddings $\sigma_1, \sigma_2 : K \to \mathbf{C}$ induce the same valuation on K, there is by 2.1 an induced topological isomorphism on the completions. As $\mathbf{R}$ has no automorphisms and $\mathbf{C}$ no continuous automorphisms besides the identity and complex conjugation, we conclude that σ_1 and σ_2 are either equal or complex conjugates of each other. This immediately yields the following archimedean counterpart of theorem 1.11.

2.5. Corollary. *The infinite primes of a number field K correspond bijectively to the complex embeddings $\sigma : K \to \mathbf{C}$, when taken up to complex conjugation.* □

An infinite prime of a number field K is called *real* if it comes from a real embedding $K \to \mathbf{R}$, and *complex* if it comes from an embedding $K \to \mathbf{C}$ with non-real image. We see that in contrast to the situation for non-archimedean primes in 1.11, a number field has only a finite number of archimedean prime divisors: for K of degree n, the number r of real and s of complex primes satisfies the relation

$$r + 2s = n$$

that we already encountered in [NR, (5.3)].

▶ Non-archimedean completions

For non-archimedean valued fields K, the residue class field $\overline{K}$ can be any field, and the value group $\phi[K^*]$ any subgroup of $\mathbf{R}_{>0}$ (cf. exercise 1.10). The same is true for complete archimedean fields, by the following lemma.

2.6. Lemma. *Let K_ϕ be the completion of a field K with respect to a non-archimedean valuation ϕ. Then we have $\phi[K^*] = \phi[K_\phi^*]$ and $\overline{K} = \overline{K_\phi}$.*

For $x \in K_\phi^*$ we can find $a \in K^*$ with $\phi(a-x) < \phi(x)$, so the ultrametric inequality (1.3) gives $\phi(a) = \phi(a-x+x) = \phi(x)$, proving $\phi(x) \in \phi[K]$ and $\phi[K] = \phi[K_\phi]$.

Similarly, if $x \in K_\phi^*$ satisfies $\phi(x) \leq 1$ and $a \in K$ is chosen satisfying $\phi(a-x) < 1$, then we have $\overline{x} = \overline{a} \in \overline{K} = \overline{K_\phi}$. □

Given the large variety of complete non-archimedean fields, no classification result of the simplicity of Theorem 2.3 exists for them. On the other hand, they all share 'analytic properties' that are in some ways easier than those of $\mathbf{R}$ and $\mathbf{C}$.

By the ultrametric inequality (1.2), which bounds finite sums by the maximum of their terms, converging sums $\sum_{k\geq 0} a_k$ in a complete non-archimedean field with valuation ϕ can simply be characterized as sums for which $\phi(a_k)$ tends to 0 for $k \to \infty$.

Exercise 1. Prove this, and show that the value of the sum is the same for each reordering of the terms.

In non-archimedean fields, all open balls $U_\varepsilon = \{x \in K : \phi(x) < \varepsilon\}$ and closed balls $B_\varepsilon = \{x \in K : \phi(x) \leq \varepsilon\}$ are additive subgroups of K. For $\varepsilon = 1$ we obtain the valuation ring $A = A_\phi = B_1$ and its maximal ideal $\mathfrak{m} = \mathfrak{m}_\phi = U_1$. Open and closed balls are the same thing in case we are dealing with the *discrete* valuations from 1.13, which frequently arise in number theory and geometry.

Let ϕ be non-trivial and discrete on K. Then the value group $\phi[K^*]$ is an infinite cyclic group $\langle \phi(\pi) \rangle \subset \mathbf{R}_{>0}$ generated by the largest value $\phi(\pi) \in (0,1)$ assumed by ϕ. A *uniformizer* $\pi \in K^*$ for the corresponding prime divisor $\mathfrak{p}$, on which ϕ assumes this largest value, is unique up to multiplication by units in the valuation ring A, and by (1.14) every $x \in K^*$ can be written as

$$x = u \cdot \pi^{\mathrm{ord}_\mathfrak{p}(x)}, \tag{2.7}$$

where $u \in A^*$ is a $\mathfrak{p}$-adic unit having $\phi(u) = 1$ and $\mathrm{ord}_\mathfrak{p}(x) \in \mathbf{Z}$ denotes the valuation of x at the prime $\mathfrak{p}$. We also write $\mathfrak{p}$ for the maximal ideal πA of the valuation ring A.

In a complete discretely valued field K, with π a uniformizer for the prime $\mathfrak{p}$, every element admits a $\mathfrak{p}$-adic expansion

$$x = \sum_{k \geq \mathrm{ord}_\mathfrak{p}(x)} a_k \pi^k, \tag{2.8}$$

with a_k from some subset $S \subset A$ of $\mathfrak{p}$-*adic digits*. For S one can pick any set of representatives in A of the residue classes modulo $\mathfrak{p}$, where it is customary to pick $0 \in S$ for

the representative of the class $\mathfrak{p}$ itself. In view of the application in 3.7, we include in the statement below a version in which the powers π^k are replaced by arbitrary elements π_k that generate the same ideal as π^k.

2.9. Theorem. *Let K be a complete non-archimedean field, with A and $\mathfrak{p} = \pi A$ as above. Let $\pi_k \in K$ be a generator of $\mathfrak{p}^k$, for $k \geq 1$, and $S \subset A$ a set of representatives of $A/\mathfrak{p}$ containing 0. Then we have*

$$A = \{\sum_{k=0}^{\infty} a_k \pi_k : a_k \in S \text{ for } k \geq 0\},$$

and every $x \in K^*$ has a unique $\mathfrak{p}$-adic expansion $x = \sum_{k \geq \mathrm{ord}_{\mathfrak{p}}(x)} a_k \pi^k$.

Proof. If $(a_k)_{k\geq 0}$ is any sequence in S, the sum $\sum_{k\geq 0} a_k\pi_k$ has terms tending to 0, and is therefore convergent in K. Assume that not all a_k are zero. As all non-zero terms have different valuations, the value $x = \sum_k a_k\pi_k$ has valuation $\phi(x) = \phi(\pi_N)$, with $N = \mathrm{ord}_{\mathfrak{p}}(x)$ the smallest k with $a_k \neq 0$. This not only shows that the value lies in A, but also that any difference $\sum_k^{\infty} a_k\pi_k - \sum_k^{\infty} b_k\pi_k$ of two distinct sums with coefficients in S is non-zero: it has non-zero valuation $\phi(\pi_N)$ with $N = \min\{k : a_k \neq b_k\}$.

Conversely, given $x \in A$, there exists $a_0 \in S$ with $x \equiv a_0 \bmod \mathfrak{p}$. We have $x = a_0 + \pi_1 x_1$ with $x_1 \in A$, and taking $a_1 \in S$ satisfying $x_1 \equiv a_1 \bmod \mathfrak{p}$ yields $x - a_0 - a_1\pi_1 \in \pi_1\mathfrak{p} = \mathfrak{p}^2$. Thus $x = a_0 + a_1\pi_1 + x_2\pi_2$ for some $x_2 \in A$, and continuing inductively we construct elements a_k for $k \geq 0$ such that we have $x \equiv \sum_{k=0}^{n} a_k\pi_n \bmod \mathfrak{p}^{n+1}$, and therefore $x = \sum_{k=0}^{\infty} a_k\pi_n$. We already know that the expansion is unique, proving the first statement.

For the second statement, we use (2.7) to reduce to the case $\mathrm{ord}_{\mathfrak{p}}(x) = 0$, and then apply the first statement with $\pi_k = \pi^k$. □

If the complete field K in the preceding theorem is obtained by completion of a subfield $K_0 \subset K$, the elements π_k and the coefficients a_k can be taken from K_0 by Lemma 2.6. This applies in particular to the completions of $\mathbf{Q}$ arising from the p-adic valuations in Theorem 1.10.

▶ p-ADIC NUMBERS

The p-adic number field $\mathbf{Q}_p$ is the field obtained by completing the rational number field $\mathbf{Q}$ under the p-adic valuation ϕ_p from 1.10. The valuation ring of $\mathbf{Q}_p$ is denoted by $\mathbf{Z}_p$, and its residue class field is the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p/p\mathbf{Z}_p$. Making the obvious choices $\pi = p$ and $S = \{0, 1, 2, \ldots, p-1\}$ for $K = \mathbf{Q}_p$ in Theorem 2.9, we see that p-adic numbers have a unique p-adic expansion

$$x = \sum_k a_k p^k \qquad \text{with} \qquad a_i \in \{0, 1, 2, \ldots, p-1\}.$$

These expansions are in many ways similar to the well known decimal expansions $x = \sum_k a_k 10^{-k}$ with $a_i \in \{0, 1, 2, \ldots, 9\}$ that are used in the archimedean completion $\mathbf{R}$ of $\mathbf{Q}$.

Note that the ambiguity of decimal expansions (1=.9999999999...) does not occur in the p-adic case.

Arithmetical operations in $\mathbf{Q}_p$ are performed in almost the same way as operations on real numbers given by a decimal expansion. An addition $\sum_k a_k p^k + \sum_k b_k p^k$ is performed as an addition of formal power series in p followed by a transport of 'carries', for i ranging from $-\infty$ to ∞, from coefficients $a_i + b_i$ not in S to the next higher coefficient. A carry at the i-th coefficient $a_i + b_i \notin S$ gives a new i-th coefficient $a_i + b_i - p \in S$ and replaces the $(i+1)$-st coefficient by $a_{i+1} + b_{i+1} + 1$. Similar remarks can be made for the multiplication of p-adic numbers, and for subtraction one transports 'carries' in the other direction. As an example for the addition, one can consider the representation

$$-1 = \sum_{k \geq 0} (p-1) p^k \in \mathbf{Q}_p$$

for $-1 \in \mathbf{Z}_p$: both sides yield 0 when 1 is added. As this example makes clear, the natural (total) ordering on $\mathbf{Z}$ or $\mathbf{Q}$ has no natural extension to $\mathbf{Z}_p$ or $\mathbf{Q}_p$.

Division in $\mathbf{Q}_p$ can be treated in various ways. If one needs $a = x/y \in \mathbf{Q}_p$, one can find the expansion of a by equating coefficients in a 'power series identity' $ay = x$. However, one can also perform long division as for real numbers. In this case one obtains the quotient $a = x/y = \sum_k a_k p^k$ of two elements $x, y \in \mathbf{Z}_p^*$ by successively subtracting suitable multiples $a_k p^k y$ (with $a_k \in S$) of y from x that eliminate the lowest coefficient, i.e. that leave a smaller remainder. As an example, one can check that the quotient $\frac{1}{7} \in \mathbf{Z}_3$ has a 3-adic expansion

$$7^{-1} = 1\,102120\,102120\,102120\ldots \in \mathbf{Q}_3$$

that is periodic with period length 6, just like the decimal expansion

$$7^{-1} = .142857\,142857\,142857\ldots \in \mathbf{R}.$$

The equality of the period lengths is no coincidence, see exercise 6.

There are other convenient choices for the set S of digits in $\mathbf{Q}_p$, such as the multiplicatively closed set of Teichmüller representatives (exercise 7).

▶ Local fields

For K as in theorem 2.9, the representation of elements of A by their expansions $\sum_{k \geq 0} a_k \pi_k$ establishes a bijection of A with a countable infinite product $\prod_{k \geq 0} S$ of 'digit sets' S that is actually an isomorphism of topological spaces if we give S the discrete topology: elements are close if their first N digits coincide for some large N. If the cardinality of S, which equals the cardinality of the residue class field $A/\mathfrak{p}$, is finite, then Tychonoff's theorem from topology implies that $\prod_{k \geq 0} S$, and therefore A and all open balls $\mathfrak{p}^n$ are compact, making the valuation topology on K into a *locally compact* topology.

A field equipped K with a non-discrete valuation is said to be a *local field* if the valuation topology on K is locally compact.

2.10. Theorem. *Let K be a local field. Then K is complete under the valuation topology, and either*

- *K is archimedean, and topologically isomorphic to $\mathbf{R}$ or $\mathbf{C}$, or*
- *K is non-archimedean, its valuation is discrete and its residue class field is finite.*

Proof. If K is archimedean, its completion is topologically isomorphic to either $\mathbf{R}$ or $\mathbf{C}$ by Theorem 2.3. As a locally compact subfield of $\mathbf{R}$ contains a closed interval $[-\varepsilon, \varepsilon]$, and a locally compact subfield of $\mathbf{C}$ a closed disk $\{z : |z| < \varepsilon\}$, we deduce that K is equal to either $\mathbf{R}$ or $\mathbf{C}$.

Suppose K is non-archimedean and locally compact for the topology $\mathcal{T}_\phi$ of a non-discrete valuation ϕ. Then $0 \in K$ has a compact neighborhood that contains the closed ball $\pi^n A = \{x \in K : \phi(x) \leq \phi(\pi^n)$ if we pick for $\pi \in K^*$ any element with $\phi(\pi) < 1$, and n a sufficiently large integer. It follows that the closed ball $\pi^n A$, and therefore A itself, is compact. As the cosets of the open unit ball $U_1 = \mathfrak{m} \subset A$ cover A, there are only finitely many different cosets, and the residue class field $A/\mathfrak{m}$ is finite. We also see that the complement of $\mathfrak{m}$ in the closed set A, and therefore in K, is open, and that $\mathfrak{m}$ is therefore closed and compact. As $\mathfrak{m} = \cup_{n \geq 2} U_{1-1/n}$ is covered by finitely many open balls of radius $1 - 1/n$, it is contained in $U_{1-1/n}$ for n sufficiently large, showing that the valuation is discrete. □

Combining Theorem 1.11 with Lemma 2.6, we see that the completions of a number field at its primes, both finite and infinite, are local fields.

Exercise 2. Let F be a finite field. Show that every completion of the rational function field $F(X)$ at one of its primes is a local field.

▶ Hensel's lemma

In complete fields, one can often 'refine' approximate solutions to polynomial equations to actual solutions. There are several results of this nature that all go under the same name.

2.11. Hensel's lemma. *Let K be complete with respect to a non-archimedean valuation and A the valuation ring of K. Suppose that $f \in A[X]$ is a primitive polynomial that factors over the residue class field $\overline{K}$ as*

$$\overline{f} = \overline{g} \cdot \overline{h} \in \overline{K}[X]$$

with $\overline{g}, \overline{h} \in \overline{K}[X]$ coprime. Then there is a factorization $f = g \cdot h$ of f in $K[X]$ such that $\deg(g) = \deg(\overline{g})$ and $g, h \in A[X]$ have reduction $\overline{g}$ and $\overline{h}$ in $\overline{K}[X]$.

Proof. The required polynomials g and h are obtained by an inductive refinement of initial lifts of $\overline{g}$ and $\overline{h}$ to $A[X]$. More precisely, set $r = \deg f$ and $s = \deg(\overline{g})$ and suppose we have $\pi \in \mathfrak{p}$ and polynomials g_0, h_0, a_0 and b_0 in $A[X]$ such that

$$\begin{aligned} \deg(g_0) &= s & f &\equiv g_0 h_0 \bmod \pi A[X] \\ \deg(h_0) &\leq r - s & a_0 g_0 + b_0 h_0 &\equiv 1 \bmod \pi A[X]. \end{aligned}$$

By assumption, such polynomials can be found when π is taken to be a generator of $\mathfrak{p}$. We will show how to construct g_1, h_1, a_1 and b_1 in $A[X]$ that are congruent to g_0, h_0, a_0 and b_0 modulo $\pi A[X]$ and satisfy

$$\begin{aligned} \deg(g_1) &= \deg(g_0) & f &\equiv g_1 h_1 \bmod \pi^2 A[X] \\ \deg(h_1) &= \deg(h_0) & a_1 g_1 + b_1 h_1 &\equiv 1 \bmod \pi^2 A[X]. \end{aligned}$$

Once we can do this, it suffices to iterate the construction. One obtains sequences $(g_k)_k$ and $(h_k)_k$ of polynomials in $A[X]$ that satisfy $\deg(g_k) = \deg(\overline{g})$ and $f \equiv g_k h_k \bmod \pi^{2^k} A[X]$. Moreover, these sequences converge *quadratically* to polynomials $g, h \in A[X]$ as we have congruences

$$\begin{aligned} g_k &\equiv g_{k-1} \bmod \pi^{2^k} A[X] \\ h_k &\equiv h_{k-1} \bmod \pi^{2^k} A[X], \end{aligned}$$

and their limit yields the factorization $f = gh$ in $K[X]$.

We now construct polynomials $u, v \in A[X]$ of degree $\deg(u) < s$ and $\deg(v) \leq r - s$ such that $g_1 = g_0 + \pi u$ and $h_1 = h_0 + \pi v$ provide a factorization $f \equiv g_1 h_1 \bmod \pi^2 A[X]$. Writing $f = g_0 h_0 + \pi r_0$ for some $r_0 \in A[X]$, we need to achieve the congruence

$$v g_0 + u h_0 \equiv r_0 \bmod \pi A[X].$$

By assumption we have $a_0 g_0 + b_0 h_0 \equiv 1 \bmod \pi A[X]$, and we take $u \in A[X]$ to be the polynomial of degree smaller than $s = \deg(g_0)$ that satisfies $u \equiv b_0 r_0 \bmod g_0 A[X]$. Then the congruence $u h_0 \equiv r_0 \bmod \pi A[X] + g_0 A[X]$ shows that we can find $v \in A[X]$ of degree at most $r - s$ satisfying $u h_0 \equiv r_0 - v g_0 \bmod \pi A[X]$, as desired.

The polynomials g_1 and h_1 satisfy $a_0 g_1 + b_0 h_1 = 1 + \pi t$ for some $t \in A[X]$, so we can define $a_1 = (1 - \pi t) a_0$ and $b_1 = (1 - \pi t) b_0$ to achieve the desired congruence $a_1 g_1 + b_1 h_1 = (1 - \pi t)(1 + \pi t) \equiv 1 \bmod \pi^2 A[X]$. □

In the special case that $\bar{g}$ is a simple linear factor of $\bar{f}$, the proof reduces to the iterative approximation of a root of f by a process known as Newton iteration (exercise 8). As this special case will be used frequently, we state it separately. For some immediate consequences of the result we refer to the exercises.

2.12. Corollary. *Let $f \in A[X]$ be a polynomial. Then every simple zero of the polynomial $\overline{f} = f \bmod \mathfrak{p}[X]$ in $A/\mathfrak{p}$ can be lifted to a zero of f in A.* □

A more general version of the lifting of zeroes from $\overline{K}$ to K is given in exercise 9.

Exercises

3. Let K be a field that is locally compact in some valuation topology T_ϕ and E a finite extension of K. Show that the function ψ on E given by

$$\psi(x) = \phi(N_{E/K}(x))^{1/[E:K]} \qquad (x \in E)$$

is a valuation on E, and that E is complete with respect to this valuation. Deduce that $\mathbf{C}$ is the algebraic closure of $\mathbf{R}$.
[Hint: Define an appropriate vector norm $||.||$ on the K-vector space E and use the continuity of ψ on the norm-compact unit ball in E to show that there are positive constants c_1, c_2 such that $c_1||x|| \leq \psi(x) \leq c_2||x||$ for all $x \in E$.]

4. Show that the completion of the rational function field $\mathbf{C}(X)$ with respect to the discrete valuation ϕ_α corresponding to $\alpha \in \mathbf{C}$ is the field

$$\mathbf{C}((X-\alpha)) = \{\textstyle\sum_{i \gg -\infty}^{\infty} c_i (X-\alpha)^i : c_i \in \mathbf{C}\}$$

of Laurent series in $X - \alpha$.

5. Show that $\mathbf{Q}_p$ is transcendental over $\mathbf{Q}$. What is its transcendence degree?

6. *(Periodic expansions.)* Show that a p-adic number $x \in \mathbf{Q}_p$ is rational if and only if its p-adic expansion $x = \sum_i a_i p^i$ is periodic, i.e. if there exists an integer $N > 0$ such that $a_{i+N} = a_i$ for all sufficiently large i. The smallest such N is called the period of x. Determine how the period of x depends on x, and find all $x \in \mathbf{Q}_p$ having period 1. State and prove analogous results for $x \in \mathbf{Q}_\infty = \mathbf{R}$ in terms of the decimal expansion of x.

7. *(Teichmüller representatives.)* Let p be a prime number. Show that $\mathbf{Q}_p$ contains a primitive $(p-1)$-st root of unity ζ_{p-1} and that there is a natural isomorphism

$$\mathbf{Z}_p^* \cong \langle \zeta_{p-1} \rangle \times (1 + p\mathbf{Z}_p).$$

Deduce that $S = \langle \zeta_{p-1} \rangle \cup \{0\}$ is a set of representatives of $\mathbf{F}_p$ in $\mathbf{Z}_p$ in the sense of theorem 2.6 that is closed under multiplication. Generalize to non-archimedean completions of arbitrary number fields.

The next two exercises deal with the approximation of zeroes of a differentiable function f known as *Newton iteration*. If f is a differentiable function on $\mathbf{R}$ we define for arbitrary $x_0 \in \mathbf{R}$ the sequence of Newton iterates $\{x_n\}_{n=1}^{\infty} \subset \mathbf{R}$ by

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \qquad (n \geq 0).$$

This is well defined provided that $f'(x_n) \neq 0$ for each x_n. For K an arbitrary field and $f \in K[X]$ a polynomial the Newton iterates of $x_0 \in K$ are defined by the same formula, with f' the (formal) derivative of f.

8. *(Newton iteration in* $\mathbf{R}$*.)* Suppose that f is twice continuously differentiable on $\mathbf{R}$ and $x \in \mathbf{R}$ a zero of f for which $f'(x) \neq 0$.

a. Show that there is an open neighborhood of x in $\mathbf{R}$ such that $\lim_{n\to\infty} x_n = x$ for each initial value $x_0 \neq x$ in this neighborhood. Determine how large these neighborhoods can be taken for each of the zeroes of $f = X^3 - X$.
b. Show that there exists a constant $C = C(f) > 0$ and a neighborhood U of x such that the resulting sequence satisfies $|x_{n+1} - x| < C|x_n - x|^2$ for all starting values $x_0 \in U$. (This is called *quadratic convergence*.)

9. *(Hensel's lemma on polynomial zeroes.)* Suppose that K is complete with respect to a non-archimedean valuation ϕ. Let A be the valuation ring of K and $f \in A[X]$ a polynomial. Let $x_0 \in A$ be an element for which $\phi(f(x_0)) < \phi(f'(x_0))^2$. Show that the Newton iterates of x_0 converge to a zero $x \in A$ of f satisfying $\phi(x - x_0) \leq \phi(f(x_0)/f'(x_0))$. Show also that we have $\phi(x_n - x) \leq C^{2^n}\phi(f'(x_0))$ with $C = \phi(f(x_0)/f'(x_0)^2) < 1$ for all n.

10. Let p be a prime number and $n > 0$ an integer. Show that $\mathbf{Q}_p^*/\mathbf{Q}_p^{*n}$ is a finite group. Determine its order if p does not divide n. (For the general case see exercise 12.)

11. Show that $\mathbf{Q}_p$ has exactly 3 non-isomorphic quadratic extensions if p is odd. What is the corresponding statement for $p = 2$?

12. Let K be a field of characteristic zero that is complete with respect to a non-archimedean valuation ϕ. We define C as the open disk around the origin in K with radius 1 if $\phi|_{\mathbf{Q}}$ is trivial, and with radius $\phi(p)^{1/p-1}$ if $\phi|_{\mathbf{Q}}$ is p-adic. Show that the power series

$$\log(1+x) = -\sum_{k\geq 1} \frac{(-x)^k}{k} \qquad \text{and} \qquad \exp(x) = \sum_{k\geq 0} \frac{x^k}{k!}$$

define continuous group homomorphisms

$$\log : U_1 = 1 + \mathfrak{p} \to K \qquad \text{and} \qquad \exp : C \to K^*$$

such that $\log \circ \exp$ and $\exp \circ \log$ are the identity maps on C and $1 + C$. Show that log is injective on U_1 if $\phi|_{\mathbf{Q}}$ is trivial, and consists of the p-power roots of unity in K if $\phi|_{\mathbf{Q}}$ is p-adic.

13. Let p be a prime number and set $q = p$ if p is odd and $q = 4$ if $p = 2$. Show that the closure of the subgroup of $\mathbf{Z}_p^*$ generated by $1 + q$ equals $1 + q\mathbf{Z}_p$, and that the map $\mathbf{Z} \to \mathbf{Z}_p^*$ sending $x \to (1+q)^x$ can be extended to an isomorphism $\mathbf{Z}_p \xrightarrow{\sim} 1 + q\mathbf{Z}_p$ of topological groups that maps $p^n\mathbf{Z}_p$ onto $1 + qp^n\mathbf{Z}_p$ for $n \geq 1$. Use this to compute the order of $\mathbf{Q}_p^*/\mathbf{Q}_p^{*n}$ for arbitrary n.

14. Determine for each prime p (including ∞) the order of the group of roots of unity in $\mathbf{Q}_p$. Prove that $\mathbf{Q}_p$ and $\mathbf{Q}_{p'}$ are not isomorphic (as fields) when $p \neq p'$.

15. *(Product formula.)* For $\mathfrak{p}$ a finite prime of a number field K, we let the normalized $\mathfrak{p}$-adic valuation $\phi_{\mathfrak{p}}$ be the valuation satisfying $\phi_{\mathfrak{p}}[K^*] = \langle N_{K/\mathbf{Q}}(\mathfrak{p})\rangle$, i.e. the subgroup of $\mathbf{R}^*$ generated by the ideal norm of the corresponding prime ideal. For an infinite prime $\mathfrak{p}$ we set $\phi_{\mathfrak{p}}(x) = |N_{K_{\mathfrak{p}}/\mathbf{R}}(x)|$. Show that with this normalization, the formula $\prod_{\mathfrak{p}\ \text{prime}} \phi_{\mathfrak{p}}(x) = 1$ holds for all $x \in K^*$.

A *coefficient field* for a local ring A with maximal ideal $\mathfrak{p}$ is a subring $k \subset A$ for which the natural map $k \to A/\mathfrak{p}$ is an isomorphism. A field K with a non-archimedean valuation ϕ is said to have a coefficient field if its valuation ring has.

16. Let K be a field of positive characteristic that is complete with respect to a discrete valuation. Suppose that $\overline{K}$ is perfect. Show that K has a coefficient field.
[Hint: for $x \in \overline{K}$ there exists $x_n \in A$ such that $x_n^{p^n}$ has residue x. Show that the map $\overline{K} \to K$ sending x to $\lim x_n^{p^n}$ is well defined and yields the required field.]

17. Show that every complete non-archimedean field K with residue class field $\overline{K}$ of characteristic zero has a coefficient field.
[Hint: the valuation ring A contains a maximal subfield.]

18. Let K be a field that is complete with respect to a non-trivial discrete valuation, and suppose that the residue class field $\overline{K}$ is perfect and of the same characteristic as K. Show that K is isomorphic (as a topological field) to the field $\overline{K}((X))$ of Laurent series over $\overline{K}$. Deduce that a local field of characteristic $p > 0$ is of the form $F((X))$ with F finite.

19. Let F be a field and $P \in F[X]$ an irreducible separable polynomial with residue class field $E = F[X]/(P)$. Show that the completion of the function field $F(X)$ with respect to the valuation ϕ_P defined in 1.12 is topologically isomorphic to the field $E((Y))$ of Laurent series over E.

20. Let K be a field with a non-archimedean valuation φ. Denote the valuation ring and its maximal ideal by A and $\mathfrak{p}$.
    a. Let S be the set of those $x \in K$ for which $1+x$ has an nth root in K for infinitely many positive integers n. Prove: if K is complete with respect to φ then $\mathfrak{p} \subset S$, and if φ is discrete than $S \subset A$.
    b. Suppose that φ is non-trivial and that K is complete with respect to φ. Prove that any discrete valuation on K is equivalent to φ.
    c. For $i = 0$, 1, let K_i be a field that is complete with respect to a discrete valuation. Prove that any field homomorphism $K_0 \to K_1$ of which the image is not contained in the valuation ring of K_1 is continuous.
    d. Show that the fields $\mathbf{Q}_p$ for p prime or $p = \infty$ have no field automorphism except the identity.

3 Extending valuations

In this section, we will see how to extend a valuation ϕ on a field K to a finite extension L of K. If K is complete with respect to ϕ, the extension valuation is unique (Theorem 3.3), and the general case follows from this by considering L 'over the completion K_ϕ' in the tensor product $L \otimes_K K_\phi$ (Theorem 3.8). In the case where ϕ is non-archimedean, this yields a 'topological approach' to the factorization of ideals of Dedekind domains in extension rings that was treated in [ANT, §2 and 3].

If L/K is purely inseparable, the extension of valuations is automatic as we have $x^{[L:K]} \in K$ for every $x \in L$, and therefore an extension ψ of ϕ to L must be given by

$$\psi(x) = \phi(x^{[L:K]})^{1/[L:K]}.$$

It is easily seen that this is indeed a valuation on L.

▶ Vector spaces over complete fields

Let ϕ be a non-trivial valuation on K, and assume that ϕ satisfies the triangle inequality. A *vector norm* on a finite dimensional K-vector space V is a function $||.|| : V \to \mathbf{R}_{\geq 0}$ that is positive outside the origin $0 \in V$ and satisfies

$$||x + y|| \leq ||x|| + ||y|| \qquad \text{and} \qquad ||kx|| = \phi(k)||x||$$

for $x, y \in V$ and $k \in K$. It defines a metric topology on V under which the vector space operations of addition and scalar multiplication are continuous.

Two vector norms $||\cdot||_1$ and $||\cdot||_2$ on V are said to be equivalent if there are constants $C_1, C_2 \in \mathbf{R}_{>0}$ such that

$$C_1||x||_1 \leq ||x||_2 \leq C_2||x||_1$$

holds for all $x \in V$. In other words, they define the same topology on V.

For every basis $\{\omega_i\}_i$ of V over K, there is an associated vector norm on V defined by

$$||\sum_i k_i\omega_i||_0 = \max_i \phi(k_i).$$

If K is complete, this is up to equivalence the only one.

3.1. Lemma. *Let V be a finite dimensional vector space over a complete field K. Then all vector norms on V are equivalent, and V is complete with respect to these norms.*

Proof. Choose a basis $\{\omega_i\}_i$ for V over K, and let $||\cdot||_0$ be the associated vector norm. As K is complete with respect to ϕ, we see that V is complete with respect to this norm. Any norm $||\cdot||$ on V is continuous with respect the norm $||\cdot||_0$, as we have, with $n = \dim_K V$, inequalities

$$||\sum_i a_i\omega_i|| \leq n \max_i ||a_i\omega_i|| \leq n \max_i ||\omega_i|| \max_i \phi(a_i) = C_2||\sum_i a_i\omega_i||_0.$$

An inequality of the type $C_1||x||_0 \leq ||x||$ for such a norm can be derived by induction on $n = \dim_K V$. In the case that K is locally compact, which will usually be the case for us, there is an even shorter proof based on the observation that the unit ball $B = \{x \in V : ||x||_0 \leq 1\}$ and therefore the unit sphere $S = \{x \in V : ||x||_0 = 1\}$ are $||\cdot||_0$-compact in V. If $C_1 > 0$ denotes the minimum of the continuous function $||.||$ on S, we have $||x|| \geq C_1||x||_0$ on S and therefore on all of V, as every $x \in V$ can be written as $x = ks$ with $k \in K$ and $s \in S$. □

In the case where L is a finite field extension of the complete field K and ϕ satisfies the triangle inequality on K, every extension valuation ψ of ϕ to V also satisfies the triangle inequality, so it is a vector norm on V. By the preceding lemma, the topology on L induced by ψ does not depend on a choice of ψ. By Proposition 1.8, it follows that there can be at most one extension ψ of ϕ to L.

▶ Extending valuations: complete case

If L/K is separable and M a normal closure of L over K, the uniqueness of a hypothetical extension ψ of ϕ to M implies that we must have $\psi \circ \sigma = \psi$ for every $\sigma \in \mathrm{Gal}(M/K)$. If we apply this for $x \in L$ and σ ranging over the cosets of $\mathrm{Gal}(M/L)$ in $\mathrm{Gal}(M/K)$, we find $\psi(x)^{[L:K]} = \psi(N_{L/K}(x)) = \phi(N_{L/K}(x))$, so ψ is given on L by the formula

$$\psi(x) = \phi(N_{L/K}(x))^{1/[L:K]}. \tag{3.2}$$

we already encountered in the special case of Lemma 2.2. Note that this formula is also correct for purely inseparable extensions as in that case the norm raises to the power $[L : K]$. In the important special case that K is a local field, there is a simple topological argument that shows that 3.2 defines an extension valuation (exercise 2.3). This argument can be extended to the general case, but it is easier to use the fact that the complete archimedean case follows from Ostrowski's theorem 2.2 and treat the non-archimedean case separately.

3.3. Theorem. *Let K be complete with respect to a valuation ϕ and L a finite extension of K. Then ϕ has a unique extension to a valuation ψ on L. One has*

$$\psi(x) = \phi(N_{L/K}(x))^{1/[L:K]}$$

for $x \in L$, and L is complete with respect to ψ.

Proof. In the non-archimedean case the only non-trivial extension is $\mathbf{C}/\mathbf{R}$, and for this extension the theorem is obviously correct.

Assume now that ϕ is non-archimedean. As the function ψ is multiplicative on L and non-zero for $x \neq 0$, we only have to show that $\psi(x + y) \leq \max\{\psi(x), \psi(y)\}$ holds for $x, y \in L$. Dividing by $\max\{\psi(x), \psi(y)\}$ shows that this is equivalent to showing that we have $\psi(1 + x) \leq 1$ if $\psi(x) \leq 1$. As the norm $N_{L/K}(x)$ is the constant coefficient

of the characteristic polynomial of x, which is a power of the irreducible polynomial f_K^x of x, we have to show that we have $\phi(f_K^x(-1)) \leq 1$ if we know that $\phi(f_K^x(0)) \leq 1$. It therefore suffices to show that for each monic irreducible polynomial $f \in K[X]$, we have the remarkable implication

$$f(0) \in A_\phi \Rightarrow f \in A_\phi[X]. \tag{3.4}$$

This implication follows from Hensel's lemma 2.7: if f is not in $A_\phi[X]$, we can find $t \in K^*$ with $\phi(t) < 1$ such that tf is a primitive polynomial in $A_\phi[X]$. The highest and the lowest coefficient of tf are in the maximal ideal of A_ϕ, so $\overline{X}^k$ divides $\overline{tf}$ in $\overline{K}[X]$ for some $k \geq 1$, and if we take k to be maximal we have $k = \deg X^k < \deg f$. This contradicts the irreducibility of f, since Hensel's lemma implies that the factor $\overline{X}^k \in \overline{K}[X]$ lifts to a factor of degree k of tf (and therefore of f) in $K[X]$. □

As the valuation on a complete field K can uniquely be extended to every finite extension, it has a unique extension ψ to the algebraic closure K^{ac} of K. We have $\psi(x) = \phi(N_{K(x)/K}(x))^{1/[K(x):K]}$ for any $x \in K^{\mathrm{ac}}$.

We see from the implication 3.4 that the valuation ring $A_\psi \subset L$ consists exactly of the elements $x \in L$ that have irreducible polynomial $f_K^x \in A_\phi[X]$. We can phrase this as follows.

3.5. Corollary. *Suppose that the valuation ϕ in 3.3 is non-archimedean. Then the valuation ring of the extension valuation ψ is the integral closure of the valuation ring A_ϕ in the extension L.* □

▶ *e* AND *f*

If L/K is a finite field extension and ψ a valuation on L that extends a non-archimedean valuation ϕ on K, we define the *ramification index* $e(\psi/\phi)$ of ψ over ϕ as the group index

$$e(\psi/\phi) = [\psi[L^*] : \phi[K^*]]$$

and the *residue class degree* $f(\psi/\phi)$ of ψ over ϕ as the degree of the extension of residue fields

$$f(\psi/\phi) = [\overline{L} : \overline{K}].$$

Note that these quantities are multiplicative in towers of extensions.

If A is a Dedekind domain with field of fractions K and L a finite extension of K, we have defined [ANT, §3] quantities $e(\mathfrak{q}/\mathfrak{p})$ and $f(\mathfrak{q}/\mathfrak{p})$ carrying the same name for every extension $\mathfrak{q}$ of a prime $\mathfrak{p} \subset A$ to the integral closure B of A in L. This is of course no coincidence: if ψ is a $\mathfrak{q}$-adic valuation on L and ϕ its restriction to K then we have $e(\psi/\phi) = e(\mathfrak{q}/\mathfrak{p})$ because $\mathrm{ord}_\mathfrak{q}(x) = e(\mathfrak{q}/\mathfrak{p}) \cdot \mathrm{ord}_\mathfrak{p}(x)$ for all $x \in K^*$ and $f(\psi/\phi) = f(\mathfrak{q}/\mathfrak{p})$ because the residue class fields $\overline{L}$ and $\overline{K}$ of ψ and ϕ are simply the residue class fields of the primes $\mathfrak{q}$ and $\mathfrak{p}$. Led by the analogy, we say that a non-archimedean valuation ψ is *unramified* over ϕ if $e(\psi/\phi) = 1$ and the residue class field extension $\overline{L}/\overline{K}$ is separable. (In many situations, the field $\overline{K}$ will be perfect and the second condition is automatically satisfied.) Similarly, ψ is said to be *totally ramified* over ϕ if $e(\psi/\phi) = [L : K]$.

3.6. Theorem. *Let ϕ be a non-archimedean valuation on a field K and ψ an extension of ϕ to a finite extension L of K. Then $e(\psi/\phi)$ and $f(\psi/\phi)$ are finite and satisfy*

$$e(\psi/\phi)f(\psi/\phi) \leq [L:K].$$

Proof. Let $R \subset A_\psi$ be a set of elements whose residue classes in $\overline{L}$ are linearly independent over $\overline{K}$, and $S \subset L^*$ a set of elements whose ψ-images are in different cosets of $\phi[K^*]$ in $\psi[L^*]$. We are done if we can show that the elements $rs \in L$ with $r \in R$ and $s \in S$ are linearly independent over K, since in that case R and S are finite and satisfy $\#R{\cdot}\#S \leq [L:K]$. As R and S can have order $e(\psi/\phi)$ and $f(\psi/\phi)$, the theorem then follows immediately.

Suppose that we have a sum $\sum_{r,s} a_{r,s}rs = 0$ in which almost all $a_{r,s}$ equal zero. Then all non-zero elements $\alpha_s = \sum_r a_{r,s}r$ have valuation $\psi(\alpha_s) = \max_r \phi(a_{r,s}) \in \phi[K^*]$, as one can pick for such α_s a coefficient $a_{r,s}$ of maximal valuation and observe that $a_{r,s}^{-1}\alpha_s \in A_\psi$ is by definition of R in A_ψ^*. It follows that all non-zero terms $\alpha_s s$ have distinct valuation, so the ultra-metric inequality becomes an equality $0 = \psi(\sum_s \alpha_s s) = \max_s \psi(\alpha_s s)$ that shows that all terms in our sum are zero. □

Even when K is complete with respect to ϕ, the inequality in the previous theorem can be strict (exercise 7). However, in the important case that K is complete with respect to a *discrete* valuation, the theorem can be strengthened in the following way.

3.7. Theorem. *Let L be a finite extension of a field K that is complete with respect to a discrete valuation ϕ and ψ the extension of ϕ to L. Then we have an equality*

$$e(\psi/\phi)f(\psi/\phi) = [L:K].$$

Moreover, if π is a prime element for ψ and the residue classes of $r_1, r_2, \ldots, r_{f(\psi/\phi)} \in A_\psi$ form a basis for $\overline{L}$ over $\overline{K}$, then we have an integral basis

$$A_\psi = \bigoplus_{\substack{1\leq i\leq f(\psi/\phi)\\ 1\leq j\leq e(\psi/\phi)}} A_\phi \cdot r_i\pi^j.$$

Proof. As every integral basis for A_ψ over A_ϕ is also a basis for L as a vector space over K, the first statement is implied by the second.

For the second statement, we can apply theorem 2.6. More precisely, let $S_0 \subset A_\phi$ be a set of representatives of A_ϕ modulo its maximal ideal $\mathfrak{p}_\phi$ that contains 0. Choosing the elements r_i as in the theorem, we easily see that

$$S = \sum_{i=1}^{f(\psi/\phi)} S_0 \cdot r_i = \{ \sum_{i=1}^{f(\psi/\phi)} s_i r_i : \ s_i \in S_0 \text{ for all } i\}$$

is a set of representatives of A_ψ modulo its maximal ideal $\mathfrak{p}_\psi$ that contains 0. As $e(\psi/\phi)$ is finite and ϕ is discrete, ψ is again discrete. Let π_K and π_L be corresponding prime

elements, then we have $\psi(\pi_L)^{e(\psi/\phi)} = \phi(\pi_K)$ and any power $\mathfrak{p}_\psi^n$ is generated by an element of the form $\pi_L^j \pi_K^k$ with $0 \le j < e(\psi/\phi)$. Theorem 2.6 shows that any $x \in A_\psi$ has a unique representation

$$x = \sum_{\substack{1 \le i \le f(\psi/\phi) \\ 1 \le j \le e(\psi/\phi)}} \Big(\sum_{k=0}^{\infty} s_{ijk} \pi_K^k\Big) r_i \pi_L^j,$$

as was to be shown. □

If the extension L/K in 3.7 is either totally ramified or unramified, one deduces easily that we can find $\alpha \in A_\psi$ such that $A_\psi = A_\phi[\alpha]$. Such an element α is said to generate a *primitive integral basis*. If the residue class extension $\overline{L}/\overline{K}$ is separable, such an element α can always be found (exercise 13). Note that this is not in general the case for an extension $\mathcal{O}_K \subset \mathcal{O}_L$ of rings of integers, not even when $K = \mathbf{Q}$ (exercise 15).

▶ Extending valuations: general case

We continue with the general problem of extending a valuation ϕ on K to a finite extension L. As valuations extend uniquely in purely inseparable extensions, it is no essential restriction to assume L/K to be separable, and we will do so for convenience.

3.8. Theorem. *Let ϕ be a valuation on K, and L a finite separable field extension of K. Then there are only finitely many valuations ψ on L extending ϕ, and the canonical map*

$$K_\phi \otimes_K L \longrightarrow \prod_{\psi|\phi} L_\psi$$

is an isomorphism of K_ϕ-algebras.

Proof. Note first that that there are canonical K-homomorphisms of L and K_ϕ into every completion L_ψ at an extension ψ of ϕ, so that we have a map on the tensor product as stated.

As L/K is separable, we can find $\alpha \in L$ such that $L = K(\alpha)$. Let f be the irreducible polynomial of α over K. Then we have $L = K[X]/(f)$, and if $f = \prod_{i=1}^t g_i$ is the factorization of the separable polynomial f into (distinct) monic irreducibles in $K_\phi[X]$, we can apply the Chinese remainder theorem to write the tensor product

$$K_\phi \otimes_K L = K_\phi[X]/(f) \cong \prod_{i=1}^{t} K_\phi[X]/(g_i)$$

as a product of finite extensions of K_ϕ. If L_ψ is the completion of L with respect to a valuation ψ that extends ϕ, the image of the induced K-homomorphism $h_\psi : K_\phi \otimes_K L \to L_\psi$ is closed by 3.1 as it is of finite dimension over K_ϕ and dense as it contains L. It follows that h_ψ is surjective and factors as a projection of $K_\phi \otimes_K L$ on a component $K_\phi[X]/(g_i)$ followed by an isomorphism $K_\phi[X]/(g_i) \xrightarrow{\sim} L_\psi$.

Conversely, every component $K_\phi[X]/(g_i)$ of the tensor product is a finite extension of the complete field K_ϕ, so it comes by 3.3 with an extension valuation ψ of ϕ under which it is complete. The composition of the embedding $L \to K_\phi \otimes_K L$ with the projection $K_\phi \otimes_K L \to K_\phi[X]/(g_i)$ yields a K-homomorphism $L \to K_\phi[X]/(g_i)$ that maps α to the residue class of X, so ψ induces a valuation on L via this map. As the image of L in $K_\phi[X]/(g_i)$ is dense, we obtain an isomorphism of complete fields $L_\psi \xrightarrow{\sim} K_\phi[X]/(g_i)$ by 2.1. Thus, the extensions ψ of ϕ to L correspond bijectively to a factor g_i of f in $K_\phi[X]$ in the sense that there is an isomorphism $K_\phi[X]/(g_i) \cong L_\psi$. The theorem follows. □

3.9. Corollary. *Suppose that $L = K(\alpha)$ for some separable $\alpha \in L$ and f_K^α the irreducible polynomial of α over K. For each extension ψ of ϕ to L, let g_ψ be the irreducible polynomial of $\alpha \in L \subset L_\psi$ over K_ϕ. Then the map $\psi \mapsto g_\psi$ induces a bijection of finite sets*

$$\{\psi|\phi\} \leftrightarrow \{\textit{monic irreducible factors of } f \textit{ in } K_\phi[X]\}.$$

This shows that extending valuations is essentially the same thing as factoring polynomials over complete fields. Such factorizations can be found using Hensel's lemma from sufficiently accurate approximate factorizations. For discrete valuations ϕ, it is very often sufficient to factor the irreducible polynomial of a suitable element $\alpha \in L$ over the residue class field $\overline{K}$. When we phrase this in terms of the ideals in the valuation rings, we find that this observation is in fact nothing but a rewording of the Kummer-Dedekind theorem [ANT, theorem 3.1]. For the details we refer to exercise 10.

3.10. Example. Let $K = \mathbf{Q}(\alpha)$ be the extension of $\mathbf{Q}$ that is obtained by adjoining a root α of the irreducible polynomial $X^4 - 17$, and suppose we want to determine the extensions of the 2-adic valuation $\phi = |\cdot|_2$ on $\mathbf{Q}$ to K. We need to factor the polynomial $f = X^4 - 17$, which has a bad reduction over $\mathbf{F}_2$, over the field $\mathbf{Q}_2$. The approximate zero $3 \in \mathbf{Z}_2$ satisfies $|f(3)|_2 = |64|_2 < |f'(3)|_2^2 = |4|_2^2$, so the refined version of Hensel's lemma in exercise 2.9 shows that f has a zero $a \in \mathbf{Z}_2$ with $a \equiv 3 \bmod 16$. As $\mathbf{Z}_2$ does not contain the 4-th root of unity $i = \sqrt{-1}$, we conclude that f factors over $\mathbf{Q}_2$ as $X^4 - 17 = (X-a)(X+a)(X^2+a^2)$. This yields an isomorphism

$$\mathbf{Q}_2 \otimes_{\mathbf{Q}} \mathbf{Q}(\alpha) \xrightarrow{\sim} \mathbf{Q}_2 \times \mathbf{Q}_2 \times \mathbf{Q}_2(i)$$

of $\mathbf{Q}_2$-algebras that maps the element $x \otimes h(\alpha)$ to $(xh(a), xh(-a), xh(ia))$ for any $h \in \mathbf{Q}[X]$. We conclude that ϕ has two extensions ψ_1, ψ_2 to K with $e(\psi_1/\phi) = e(\psi_2/\phi) = 1$ and $f(\psi_1/\phi) = f(\psi_2/\phi) = 1$ and a single extension ψ_3 with $e(\psi_3/\phi) = 2$ and $f(\psi_3/\phi) = 1$. They are given by

$$\psi_1(h(\alpha)) = |h(a)|_2 \qquad \psi_2(h(\alpha)) = |h(-a)|_2 \qquad \psi_3(h(\alpha)) = |h(ia)|_2$$

for $h \in \mathbf{Q}[X]$, i.e. they are the composition of an embedding of K in $\mathbf{Q}_2$ or $\mathbf{Q}_2(i)$ with the unique 2-adic valuation on these complete fields. In terms of ideals, this means that

we have a factorization $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_2\mathfrak{r}_2^2$ of the rational prime 2. The ideals $\mathfrak{p}, \mathfrak{q}, \mathfrak{r} \subset \mathcal{O}_K$ are obtained by intersecting the ring $\mathcal{O}_K$, which becomes a subring of $\mathbf{Z}_2$ or $\mathbf{Z}_2[i]$ after an embedding, with the maximal ideal $2\mathbf{Z}_2$ or $(1+i)\mathbf{Z}_2[i]$. As 2 divides $[\mathcal{O}_K : \mathbf{Z}[x]]$ for every $x \in K$ (exercise 15), we cannot apply the Kummer-Dedekind theorem directly here.

Theorem 3.8 has another direct corollary that was already familiar to us [ANT, Theorem 3.4] from the theory of extensions of Dedekind rings. The separability assumption cannot be omitted here.

3.11. Corollary. *For L/K finite separable and ϕ a non-archimedean valuation on K, we have an inequality*

$$\sum_{\psi|\phi} e(\psi/\phi) f(\psi/\phi) \leq [L : K]$$

that is an equality when ϕ is discrete.

Proof. Counting K_ϕ-dimensions for the tensor product in 3.8, we find that $[L : K] = \sum_{\psi|\phi} [L_\psi : K_\phi]$, and 3.6 and 3.7 imply that we have $[L_\psi : K_\phi] \geq e(\psi/\phi) f(\psi/\phi)$ with equality for discrete ϕ. □

In the archimedean case we put $f(\psi/\phi) = 1$ and $e(\psi/\phi) = [L_\psi : K_\phi]$, such that equality holds as for discrete ϕ. In line with this choice, we say that an extension $\psi|\phi$ of archimedean valuations (or primes) is *ramified* if ϕ is real and ψ is complex.

A final consequence of the basic theorem 3.8 is the following relation between global and local norms and traces.

3.12. Corollary. *For L/K finite separable and ϕ a valuation on K we have identities*

$$N_{L/K}(x) = \prod_{\psi|\phi} N_{L_\psi/K_\phi}(x) \qquad \text{and} \qquad \mathrm{Tr}_{L/K}(x) = \sum_{\psi|\phi} \mathrm{Tr}_{L_\psi/K_\phi}(x)$$

for every element $x \in L$.

Proof. The matrix M_x of multiplication by $x \in L$ is the same for the K-vector space L and the K_ϕ-vector space $K_\phi \otimes_K L$, and computing its trace or norm using the isomorphism in 3.8 gives the desired result. □

Exercises

1. Let K be a field. Show that there exists a non-trivial valuation on K if and only if K is *not* an algebraic extension of a finite field.
   [Hint: use exercise 1.15.]

2. Let K be complete with respect to a discrete valuation ϕ and ψ the extension of ϕ to an algebraic extension L of K. Show that $e(\psi/\phi)$ and $f(\psi/\phi)$ are finite if and only if the degree $[L : K]$ is finite.

3. Prove that a local field of characteristic 0 is a finite extension of $\mathbf{Q}_p$ for some p (possibly $p = \infty$).

4. Let L be a field that is complete with respect to a discrete valuation ψ, and let K be a subfield of L for which $K \subset L$ is finite and separable. Prove that K is complete with respect to the restriction of ψ to K.

5. Let K be a field, φ a non-archimedean valuation on K, and n a positive integer. Denote by S_h the set of those non-zero vectors $(x_1, x_2, \ldots, x_n) \in K^n$ with the property that h is the smallest of the subscripts i for which $\varphi(x_i) = \max\{\varphi(x_j) : 1 \leq j \leq n\}$.
   a. Prove that any sequence v_1, v_2, $\ldots$, v_n of vectors in K^n satisfying $v_i \in S_i$ for each i forms a basis for K^n over K.
   b. Prove that the two-dimensional Euclidean plane can be written as the union of three dense subsets with the property that no line in the plane intersects all three subsets.

6. Let L/K be an extension of number fields and ϕ a non-trivial archimedean valuation of K. Show that the image of the ring of integers $\mathcal{O}_L$ under the natural map $L \to K_\phi \otimes_K L = \prod_{\psi|\phi} L_\psi$ has closure $\prod_{\psi|\phi} A_\psi$.

7. Let K_0 be the field obtained by adjoining all 2-power roots of unity to $\mathbf{Q}_2$, and K the completion of K_0 with respect to the extension ϕ of the 2-adic valuation to K_0. Show that K has an automorphism σ of order 2 mapping each 2-power root of unity to its inverse, and that $E = K^{\langle\sigma\rangle} \subset K$ is a quadratic extension of complete fields with $e(\phi/\phi_E) = f(\phi/\phi_E) = 1$.

8. *(Kummer-Dedekind.)* Let L/K be an extension of number fields and $\alpha \in \mathcal{O}_L$ an element that generates L over K. Suppose that $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ that does not divide the index of $\mathcal{O}_K$-modules $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Prove: if f_K^α factors over $\overline{K} = \mathcal{O}_K/\mathfrak{p}$ as $\overline{f} = \prod_{i=1}^t \overline{g}_i^{e_i}$, then $\mathfrak{p}$ factors in $\mathcal{O}_L$ as $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^t \mathfrak{q}_i^{e_i}$, with $\mathfrak{q}_i \subset \mathcal{O}_L$ the prime ideal generated by $\mathfrak{p}$ and $g_i(\alpha)$ for some lift $g_i \in \mathcal{O}_K[X]$ of $\overline{g}_i$.
   [Hint: we have $f = \prod_{i=1}^t f_i \in K_\mathfrak{p}[X]$ by Hensel's lemma, and $L_{\mathfrak{q}_i} = K_\mathfrak{p}[X]/(f_i)$ has residue class field $\overline{K}[X]/(\overline{g}_i)$.]

9. Let K be complete with respect to a non-archimedean valuation ϕ and ψ the extension of ϕ to the algebraic closure Ω of K.
   a. *(Krasner's lemma.)* Let $\alpha \in \Omega$ be separable over K and suppose that $\beta \in \Omega$ satisfies $\psi(\alpha - \beta) < \psi(\alpha - \alpha')$ for every K-conjugate $\alpha' \neq \alpha$ of α. Show that α is contained in $K(\beta)$.
      [Hint: Show that α is fixed under every automorphism of $\Omega/K(\beta)$.]

b. Let $K(\alpha)/K$ be a Galois extension of degree n and $f \in K[X]$ the irreducible polynomial of α over K. Let $g \in K[X]$ be a polynomial of degree less than n. Show that there exists $\varepsilon > 0$ such that $K(\alpha)$ is the splitting field of $f + kg$ for all elements $k \in K$ with $\psi(k) < \varepsilon$.

10. Let p be a prime number and $F/\mathbf{Q}_p$ be a finite extension.
    a. Show that there exist a number field K and a prime $\mathfrak{p}|p$ in K such that $K_\mathfrak{p}$ is isomorphic to F.
    b. Let E/F be a finite Galois extension with group G. Show that we can choose number fields L and K that are dense in respectively E and F in such a way that L/K is also Galois with group G.

11. Let L be a finite extension of a field K that is complete with respect to a discrete prime divisor, and suppose that the residue class field extension $\overline{L}/\overline{K}$ is separable. Show that $A_L = A_K[\alpha]$ for some $\alpha \in A_L$.
    [Hint: If $\overline{L} = \overline{K}(\overline{x})$ there exists $x \in A_\psi$ with irreducible polynomial f such that $\overline{f}$ is the irreducible polynomial of $\overline{x}$ over $\overline{K}$. If π is a prime element of L, then $f(x+\pi)$ is also a prime element and $\alpha = x + \pi$ does what we want.]

12. Determine the structure of $\mathbf{Q}_p \otimes_\mathbf{Q} K$ for $K = \mathbf{Q}[X]/(X^4 - 17)$ and $p = 3, 5, 17, 149$ and ∞. What is the corresponding factorization of these rational primes in K?
    [Hint: $7^4 = 17 \bmod 149$.]

13. For $K = \mathbf{Q}(\alpha)$ with $\alpha^4 = 17$ we set $\beta = (\alpha^2+1)/2$. Show that there is no element $x \in \mathcal{O}_K$ for which the index $[\mathcal{O}_K : \mathbf{Z}[x]]$ is odd, and that $1, \alpha, \beta, (\alpha\beta+\beta)/2$ is a $\mathbf{Z}$-basis for $\mathcal{O}_K$. Compute a $\mathbf{Z}$-basis for each of the prime ideals lying over 2.

In the following three exercises K denotes a field with a non-archimedean valuation φ, and r is a positive real number.

14. For $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$, denote the largest and the smallest value of i for which $\varphi(a_i)r^i = \max_j \varphi(a_j)r^j$ by $l_r(f)$ and $s_r(f)$, respectively.
    a. Prove that l_r and s_r extend to group homomorphisms $K(X)^* \to \mathbf{Z}$.
    b. Suppose that K is algebraically closed, and let $f \in K[X]$, $f \neq 0$. Prove that the number of zeroes α of f in K with $\varphi(\alpha) = r$, counted with multiplicities, is equal to $l_r(f) - s_r(f)$.

15. Let $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$. The *Newton polygon* of f is defined to be the "lower convex hull" of the points $(i, -\log\varphi(a_i))$, with i ranging over all non-negative integers for which $a_i \neq 0$; more precisely, if $C \subset \mathbf{R} \times \mathbf{R}$ is the convex hull of the set of those points, then the Newton polygon equals $\{(x, y) \in C : \text{there is no } (x, y') \in C \text{ with } y' < y\}$. The Newton polygon is the union of finitely many line segments of different slopes.
    a. Draw, for each prime number p, the Newton polygon of $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5 \in \mathbf{Q}[X]$ with respect to the p-adic valuation of $\mathbf{Q}$.
    b. Prove: if $\log r$ occurs as the slope of one of the line segments that constitute the Newton polygon of f, then $l_r(f) - s_r(f)$ (as defined in the previous exercise) is equal to the length of the projection of that line segment on the x-axis, and otherwise $l_r(f) - s_r(f) = 0$.

    Remark. Combining b with part b of the preceding exercise one sees that the valuations of the zeroes of f (in some algebraic extension of K) can be read from the Newton polygon of f.

16. Let $f \in K[X]$, and suppose that $f(0) \neq 0$.
    a. Suppose that K is complete with respect to φ, and that f is irreducible. Prove that the Newton polygon of f is a single line segment.
    b. Suppose that the Newton polygon of f intersects the set $\mathbf{Z} \times (-\log \varphi(K^*))$ in exactly two points. Prove that f is irreducible.
    c. Prove that $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5$ is the product of two irreducible factors in each of $\mathbf{Q}_2[X]$ and $\mathbf{Q}_7[X]$, that it is irreducible in $\mathbf{Q}_3[X]$, and that it is the product of three linear factors in $\mathbf{Q}_5[X]$. How does it factor in $\mathbf{Q}[X]$?

4 Extensions of local fields

In this section, we study finite extensions of a field K that is complete with respect to a discrete prime divisor ϕ. For L a finite extension of K, we write ψ to denote the unique extension of ϕ to L. By 3.7, we have $[L:K] = e(\psi/\phi)f(\psi/\phi)$ for these extensions, so they are unramified when $\overline{L}/\overline{K}$ is separable of degree $[L:K]$ and totally ramified when $\overline{L} = \overline{K}$. We will often restrict to the case that the residue class field extension $\overline{L}/\overline{K}$ is *separable*. This is necessarily the case if $\overline{K}$ is perfect, so our assumption is satisfied for completions of number fields, for function fields of curves over a finite field and for function fields in any dimension over a field of characteristic zero.

▶ Unramified extensions

We first study the unramified extensions L/K, which are in a sense the simplest extensions. The main result is that these extensions can uniquely be 'lifted' from the residue class field extension $\overline{L}/\overline{K}$.

4.1. Proposition. *Let L be a finite extension of a field K that is complete with respect to a discrete valuation, and suppose that the residue class field extension $\overline{L}/\overline{K}$ is separable. Then there is a unique unramified subextension T/K of L/K such that $\overline{T} = \overline{L}$.*

Proof. As $\overline{L}/\overline{K}$ is finite separable we can write $\overline{L} = \overline{K}(\overline{x})$ for some separable $\overline{x} \in \overline{L}$. Let $f_{\overline{K}}^{\overline{x}}$ be the irreducible polynomial of $\overline{x}$, and let $f \in A_\phi[X]$ be a monic polynomial with reduction $\overline{f} = f_{\overline{K}}^{\overline{x}} \in \overline{K}[X]$. As $\overline{f}$ has a simple zero $\overline{x} \in \overline{L}$, there exists by Hensel's lemma 2.8 a unique element $x \in L$ with residue class $\overline{x} \in \overline{L}$ such that $f(x) = 0$. The polynomial f is irreducible in $K[X]$ as its reduction $\overline{f} \in \overline{K}[X]$ is, so it is the irreducible polynomial of x over K. For the subfield $T = K(x) \subset L$ we have $\overline{T} = \overline{K}(\overline{x}) = \overline{L}$ and therefore $[T:K] = \deg f = [\overline{T}:\overline{K}]$. This implies that T/K is unramified.

If E/K is any subextension of L/K with $\overline{E} = \overline{L}$, the irreducible polynomial f_K^x of x over K has a simple zero in the residue class field $\overline{E}$ that can be lifted to a zero $y \in E$ of f_K^x with $\overline{y} = \overline{x} \in \overline{L}$. But this implies $y = x$ as $x \in L$ is the unique zero of f with residue class $\overline{x} \in \overline{L}$. We obtain $T \subset E$, so if we require in addition that E be unramified over K the equality $[E:K] = [\overline{E}:\overline{K}] = [T:K]$ shows that $E = T$, i.e. T is unique. □

The field T in the proposition is the *inertia field* of the extension L/K. It is the largest subfield E of L for which the prime ideal $\mathfrak{p} \subset A_K$ remains inert, i.e. generates the prime ideal of the valuation ring in A_E. The construction of T as a primitive extension $K(x)$ for some element $x \in L$ for which the reduction $\overline{f} \in \overline{K}[X]$ of the irreducible polynomial f_K^x is separable shows that the inertia field of L/K is always separable over K. We will give a Galois theoretic construction of T in the next section.

The following theorem is a more precise version of 4.1 and expresses the fact that the construction of unramified extensions L/K from separable extensions $\overline{L}/\overline{K}$ is functorial and induces an *equivalence of categories*. We write F^{sep} for a separable closure of a field F.

4.2. Theorem. *Every unramified extension L/K is separable, and the assignment $L \mapsto \overline{L}$ establishes an inclusion preserving bijection between the set of finite unramified extensions $L \subset K^{\mathrm{sep}}$ of K and the set of finite separable extensions $\overline{L} \subset \overline{K}^{\mathrm{sep}}$ of $\overline{K}$. Moreover, for any two unramified extensions L_1 and L_2 of K the natural map*

$$\mathrm{Hom}_K(L_1, L_2) \xrightarrow{\sim} \mathrm{Hom}_{\overline{K}}(\overline{L}_1, \overline{L}_2)$$

is bijective.

Proof. If L/K is finite and unramified, we have $L = T$ in 4.1 and we observed already that T/K is separable. As an arbitrary unramified extension L/K is a union of finite unramified extensions, this implies that L/K is separable.

The proof of 4.1 shows that for every finite separable extension $\overline{K}(\overline{x})$ of $\overline{K}$, there is a *unique* finite unramified extension $L = K(x)$ of K inside K^{sep} with residue class field $\overline{K}(\overline{x})$. This establishes a bijection that clearly preserves inclusions.

If $\overline{\phi} : \overline{K}(\overline{x}) \to \overline{F}$ is a $\overline{K}$-homomorphism between finite separable extensions of $\overline{K}$, then $\overline{\phi}$ maps $\overline{x}$ to some zero $\overline{y}$ of $f^{\overline{x}}_{\overline{K}}$ in $\overline{F}$. If $f \in A[X]$ is a monic lift of $f^{\overline{x}}_{\overline{K}}$ and $x \in K^{\mathrm{sep}}$ its zero with reduction $\overline{x} \in \overline{K}^{\mathrm{sep}}$, then $\overline{y} \in \overline{F}$ can uniquely be lifted to a zero y in the unramified extension F/K corresponding to $\overline{F}$. We find that there is K-homomorphism $\phi : K(x) \to F$ satisfying $\phi(x) = y$, and that this is the unique element of $\mathrm{Hom}_K(K(x), F)$ inducing $\overline{\phi}$. □

We see from this theorem that a compositum of unramified extensions of K is again unramified, and that we can take the union of all unramified extensions inside K^{sep} to obtain the *maximal unramified extension* K^{unr} of K.

4.3. Corollary. *Let K be complete with respect to a discrete valuation and L/K a finite unramified extension. Then L/K is Galois if and only if $\overline{L}/\overline{K}$ is Galois, and if these extensions are Galois their Galois groups are isomorphic.*

Proof. We have $[\overline{L} : \overline{K}] = [L : K]$ because L/K is unramified and an isomorphism $\mathrm{Aut}_K(L) \xrightarrow{\sim} \mathrm{Aut}_{\overline{K}}(\overline{L})$ by taking $L_1 = L_2 = L$ in the previous theorem. □

Taking the projective limit with respect to all unramified extensions of K, we see that the maximal unramified extension K^{unr}/K is Galois with group $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(\overline{K}^{\mathrm{sep}}/\overline{K})$. In particular, one finds that $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \widehat{\mathbf{Z}}$ when $\overline{K}$ is finite. On a finite level, this can be formulated as follows.

4.4. Corollary. *Let K be a non-archimedean local field. Then there is for each $n \geq 1$ a unique unramified extension K_n/K of degree n inside K^{sep}. This extension is cyclic, and we have $K = K(\zeta)$ for a root of unity ζ of order coprime to* $\mathrm{char}\overline{K}$.

Proof. If $\overline{K}$ is finite of order $q = p^k$ with $p = \mathrm{char}\overline{K}$, the unique extension $\overline{K}_n$ of degree n of $\overline{K}$ is the field of order q^n. By the previous corollary, the corresponding unramified extension K_n of degree n of K is also unique and Galois with group isomorphic to $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \cong \mathbf{Z}/n\mathbf{Z}$. A generator $\overline{x}$ of the cyclic group $\mathbf{F}^*_{q^n}$ is a root of unity of order $m = q^n - 1$, so its

irreducible polynomial $f_{\overline{K}}^{\overline{x}}$ is a factor of the cyclotomic polynomial $(\Phi_m \bmod p) \in \overline{K}[X]$. As m is coprime to $p = \operatorname{char} K$, the polynomial Φ_m is separable over $\overline{K}$ and we can apply Hensel's lemma 2.7 to lift $f_{\overline{K}}^{\overline{x}}$ to a factor f of Φ_m in $K[X]$. As K_n is generated over K by a root of f, it follows that $K_n = K(\zeta_m)$ for an m-th root of unity $\zeta_m \in K_n$. □

We have shown that the identity $e \cdot f = [L : K]$ for an extension L of a field K that is complete with respect to a discrete prime divisor corresponds to a unique subextension $K \subset T \subset L$ such that T/K is unramified of degree f and L/T is totally ramified of degree e. We know how to generate the inertia field T over K, so we are left with the investigation of totally ramified extensions.

▶ Totally ramified extensions

A finite extension of non-archimedean valued fields is said to be *tamely ramified* if the residue class field extension is separable and the ramification index is not divisible by the characteristic of the residue class field. Note that every finite extension of K is tamely ramified when $\operatorname{char}\overline{K} = 0$, and that unramified extensions are always tame. For infinite algebraic extensions of K the ramification index can be infinite. In that case one says that the ramification is tame if this is the case for every finite subextension L/K.

Our first result applies to totally ramified extensions that are tamely ramified.

4.5. Theorem. *Let K be complete with respect to a discrete prime divisor and L/K a totally and tamely ramified extension of degree e. Then there exists a prime element π of K such that $L = K(\sqrt[e]{\pi})$.*

Proof. Let π_L and π_K be prime elements of L and K, respectively. Then π_L generates L as $K(\pi_L) \subset L$ has ramification index $e = [L : K]$, and we have $\pi_L^e = u\pi_K$ for some unit u in the valuation ring A_L of L. As L/K is totally ramified, we have $\overline{L} = \overline{K}$, so there exists $v \in A_K^*$ with $\overline{u} = \overline{v}$. The element $x = v\pi_K/\pi_L^e$ has residue class $\overline{x} = \overline{1} \in \overline{L}$, so we can apply Hensel's lemma (as in 2.8) to the polynomial $X^e - x$, which has a root $\overline{1} \in \overline{L}$ that is simple as the derivative $\overline{e}\overline{X}^{e-1}$ does not vanish outside $\overline{0}$. We find that there exists $y \in A_L^*$ such that $y^e = x$, so $L = K(y\pi_L) = K(\sqrt[e]{v\pi_K})$. □

4.6. Example. *The p-th cyclotomic extension $\mathbf{Q}_p(\zeta_p)$ is totally ramified of degree $p-1$ over $\mathbf{Q}_p$ and can be written as $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p(\sqrt[p-1]{-p})$.*

To see this, one considers the prime element $\pi_L = 1 - \zeta_p \in L = \mathbf{Q}_p(\zeta_p)$ and computes the residue class of $u^{-1} = p/(1-\zeta_p)^{p-1}$ in $\overline{L}$ as

$$\frac{p}{(1-\zeta_p)^{p-1}} = \prod_{i=1}^{p-1} \frac{1-\zeta_p^i}{1-\zeta_p} = \prod_{i=1}^{p-1} \sum_{j=0}^{i-1} \zeta_p^j \equiv (p-1)! = -1 \in \overline{L}$$

using the identity $\zeta_p = 1 \in \overline{L}$ and Wilson's theorem. Thus, one can take $v = -1$ in the preceding proof. □

One can deduce from 4.5 that every finite extension L of a field K that is complete with respect to a discrete prime divisor has a unique maximal subfield $V \subset L$ such that V/K is tamely ramified (exercise 4). This field obviously contains the inertia field T. The union of all tamely ramified extensions of K inside an algebraic closure yields an infinite separable extension $K^{\mathrm{tame}} \supset K$ containing K^{unr} that is known as the *maximal tamely ramified extension* of K, see exercise 5.

If L/K is a non-archimedean extension of valued fields that is not tamely ramified, then $\overline{L}/\overline{K}$ is inseparable or the ramification index e satisfies $\overline{e} = 0 \in \overline{K}$. Such extensions are said to be *wildly ramified*. The structure of these extensions is in general much more complicated than what we have seen so far. Even in the case that both L/K and $\overline{L}/\overline{K}$ are separable, there can be many non-isomorphic wildly ramified extensions of the same degree.

A general method to look at totally ramified extensions L/K proceeds by studying the irreducible polynomial of a prime element π_L. Such polynomials turn out to be Eisenstein polynomials in A_K, i.e. monic polynomials of the form $\sum_{i=0}^{n} a_i X^i$ with $a_0, a_1, \ldots, a_{n-1}$ in the maximal ideal $\mathfrak{p}_K \subset A_K$ and $a_0 \notin \mathfrak{p}_K^2$.

4.7. Lemma. *Let K be complete with respect to a discrete prime divisor and L/K a totally ramified extension of degree e. Then L equals $K(\pi_L)$ for every prime element π_L of L, and $f_K^{\pi_L}$ is an Eisenstein polynomial in $A_K[X]$. Conversely, every root of an Eisenstein polynomial in $A_K[X]$ generates a totally ramified extension of K.*

Proof. If L/K is totally ramified of degree e then $K(\pi_L)$ has ramification index $e = [L : K]$ over K, so its degree over K cannot be smaller then $[L : K]$ and we have $L = K(\pi_L)$. If ψ is the extension of the valuation on K to a normal closure M of L over K, then every root π of $f_K^{\pi_L}$ in M has valuation $\psi(\pi) = \psi(\pi_L) < 1$, so the same holds for all but the highest coefficient of $f_K^{\pi_L}$, which can be written as sums of products of roots. The constant coefficient $\pm N_{L/K}\pi_L$ of $f_K^{\pi_L}$ generates the maximal ideal in A_K as it has valuation $\psi(\pi_L)^e$, so $f_K^{\pi_L}$ is Eisenstein.

Conversely, every Eisenstein polynomial $f \in A_K[X]$ is irreducible, and a root π of f generates a totally ramified extension $K(\pi)$ of degree $e = \deg(f)$ of K by 3.3: the valuation $\psi(\pi)$ is the e-th root of the valuation of a prime element of K. □

► p-ADIC FIELDS OF GIVEN DEGREE

If K is a local field of characteristic zero, i.e. a finite extension of $\mathbf{Q}_p$, the preceding lemma can be used to show that the number of totally ramified extensions of K of given degree e is finite. This yields the following finiteness result.

4.8. Theorem. *Let p be a prime number and n an integer. Then there are only finitely many extensions $L/\mathbf{Q}_p$ of degree n inside a separable closure $\mathbf{Q}_p^{\mathrm{sep}}$ of $\mathbf{Q}_p$.*

Proof. As the inertia field of $L/\mathbf{Q}_p$ is uniquely determined inside $\mathbf{Q}_p^{\mathrm{sep}}$ by its degree (corollary 4.4), it suffices to show that a every subfield $K \subset \mathbf{Q}_p^{\mathrm{sep}}$ that is of finite degree

over $\mathbf{Q}_p$ only has finitely many totally ramified extensions L/K of given degree e inside $\mathbf{Q}_p^{\mathrm{sep}}$. By the lemma, such extensions are obtained by adjoining the root of a polynomial $f = X^e + \sum_{i=0}^{e-1} a_i X^i$ with 'coefficient vector'

$$v = (a_{e-1}, a_{e-2}, \ldots, a_1, a_0) \in C = \mathfrak{p}_K^{e-1} \times (\mathfrak{p}_K \setminus \mathfrak{p}_K^2).$$

to K. Conversely, every point $v \in C$ corresponds to a separable—here we use $e \neq 0 \in K$—polynomial $f \in A[X]$, each of whose e roots in K^{sep} generates a totally ramified extension of degree e of K. By Krasner's lemma (exercise 3.11), every point $w \in C$ that is sufficiently close to v gives rise to a polynomial $g \in A[X]$ that has the same splitting field as f. As C is compact, it follows that the Eisenstein polynomials of degree e in $A[X]$ have only finitely many different splitting fields in K^{sep}. It follows that there are only finitely many totally ramified extensions of degree e of K. □

► Different and discriminant

An important invariant to measure the ramification in an extension L/K is given by the different and the discriminant of the extension. We have already encountered these in the case of number fields, and the definitions are highly similar. In section 6, we will study the relation between local and global discriminants in more detail.

Let K be complete with respect to a discrete prime divisor. In order to avoid trivialities, we will assume that L is a finite *separable* extension of K. The *discriminant* $\Delta(L/K)$ of a finite extension L is defined as the A_K-ideal generated by the discriminant

$$\Delta(\omega_1, \omega_2, \ldots, \omega_n) = \det(\mathrm{Tr}_{L/K}(\omega_i \omega_j))_{i,j=1}^n$$

of an integral basis $\{\omega_1, \omega_2, \ldots, \omega_n\}$ of A_L over A_K. Such a basis exists by 3.7, and the value of the discriminant is defined up to the square of a unit in A_K. In particular, $\Delta(L/K) \subset A_K$ is well-defined, and it is non-zero because we assume L/K to be separable. The different $\mathfrak{D}(L/K)$ is the A_L-ideal with inverse

$$\mathfrak{D}(L/K)^{-1} = \{x \in L : \mathrm{Tr}_{L/K}(xA_L) \subset A_K\}.$$

Exactly as in the global case [ANT, Theorem 4.17], we have $N_{L/K}(\mathfrak{D}(L/K)) = \Delta(L/K)$, where $N_{L/K}$ denotes the ideal norm. Moreover, we have $\mathfrak{D}(M/K) = \mathfrak{D}(M/L)\mathfrak{D}(L/K)$ for a tower $K \subset L \subset M$ of finite extensions. If A_L has an A_K-basis consisting of powers of an element $\alpha \in A_L$, we know from [ANT, Proposition 4.6] that then $\Delta(L/K)$ is generated by the discriminant $\Delta(f)$ of $f = f_K^\alpha$. Moreover, the different is then equal to $\mathfrak{D}(L/K) = f'(\alpha) \cdot A_L$ [ANT, ex. 4.29]. We can use this to compute the *differential exponent* $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K))$ of a complete extension L/K. The result obtained is a refinement of [ANT, Theorem 4.17].

4.9. Theorem. *Let L be a finite separable extension of a field K that is complete with respect to a discrete prime divisor, and suppose that the residue class field extension $\overline{L}/\overline{K}$ is separable. Let e be the ramification index of L/K. Then*

$$\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = e - 1 + u$$

with $u = 0$ if L/K is tamely ramified and $u \geq 1$ if L/K is wildly ramified. We have $u \leq \mathrm{ord}_{\mathfrak{p}_L}(e)$ when $e \neq 0 \in K$.

Proof. If L/K is unramified, we can lift any basis of $\overline{L}/\overline{K}$ to obtain a basis of A_L over A_K by 3.7, and the discriminant of this basis is a unit as the separability of $\overline{L}/\overline{K}$ implies that its reduction in $\overline{K}$ is non-zero. It follows that $\Delta(L/K) = A_K$ and $\mathfrak{D}(L/K) = A_L$ for unramified extensions.

If T is the inertia field of L/K, we have $\mathfrak{D}(L/K) = \mathfrak{D}(L/T)$ since $\mathfrak{D}(T/K) = (1)$, so we can further assume that L/K is totally ramified of degree e. Let π be a prime element in L and $f = \sum_{i=0}^{e} a_i X^i \in A_K[X]$ its irreducible polynomial. Then $A_L = A_K[\pi]$ by 3.7 and we have

$$\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = \mathrm{ord}_{\mathfrak{p}_L}(f'(\pi)) = \mathrm{ord}_{\mathfrak{p}_L}(\sum_{i=1}^{e} i a_i \pi^{i-1}) = \min_i \{\mathrm{ord}_{\mathfrak{p}_L}(i a_i \pi^{i-1})\}.$$

The final equality follows from 1.3 and the fact that all terms in the sum have different order at $\mathfrak{p}_L$. The term with $i = e$ in the last sum has order $e - 1 + \mathrm{ord}_{\mathfrak{p}_L}(e)$ at $\mathfrak{p}_L$, and all other terms have order at least e because f is Eisenstein by 4.7. It follows that $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = e - 1$ if and only if $\mathrm{ord}_{\mathfrak{p}_L}(e) = 0$, i.e. if and only if L/K is tamely ramified. If L/K is wildly ramified we obtain $e \leq \mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) \leq e - 1 + \mathrm{ord}_{\mathfrak{p}_L}(e)$. The upper bound is finite only when $e \neq 0 \in K$. □

Theorem 4.8 does not hold for local fields of positive characteristic when $\mathrm{char}K$ divides n, see exercise 13. However, there is an elegant mass formula due to Serre [19, 1978] that is more precise than 4.8 and holds in any characteristic. The statement, which we will not prove in these notes, is that for $\mathcal{S}_n$ the set of totally ramified extensions of degree n of K inside a separable closure K^{sep}, there is an identity

$$\sum_{L \in \mathcal{S}_n} q^{n-1-d(L)} = n. \tag{4.10}$$

Here q denotes the cardinality of $\overline{K}$ and $d(L) = \mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K))$ is the differential exponent of L/K. If $\mathrm{char}K = 0$ we have a uniform upper bound $d(L) \leq e - 1 + \mathrm{ord}_{\mathfrak{p}_L}(e)$ for all L, so the number of terms in the sum must be finite. For n divisible by $p = \mathrm{char}K$, the set $\mathcal{S}_n$ is always infinite, but we see that the number of fields L with bounded differential exponent must be finite. This immediately implies a local counterpart to Hermite's theorem [ANT, 5.12], see exercise 14.

Exercises

1. Let K be a field with non-archimedean valuation ϕ and $f \in A_\phi[X]$ a polynomial that is separable over the residue class field $\overline{K}$. Show that every extension of ϕ to the splitting field of f is unramified over ϕ.

2. Let M be a valued field with subfields E and L, and suppose that L is finite over some field $K \subset L \cap E$. Show that EL/E is unramified if L/K is unramified.

3. *(Abhyankar's lemma)* Suppose that ϕ is a discrete valuation on a field K and let L and E be two extensions of K that are contained in some finite extension $M = LE$ of K. Let ψ be an extension of ϕ to M and ψ_L and ψ_E the restrictions of ψ to L and E. Suppose that ψ_L/ϕ is tamely ramified and that $e(\psi_L/\phi)$ divides $e(\psi_E/\phi)$. Prove that ψ is unramified over ψ_E.

4. Let K be complete with respect to a discrete prime divisor. Show that every tamely ramified extension of K is separable, and that a compositum of two tamely ramified extensions inside K^{sep} is again tamely ramified. Deduce that for every finite extension L/K there is a unique maximal subfield $V \subset L$ that is tamely ramified over K. If e_0 is the largest divisor of the ramification index of L/K that is coprime to $\mathrm{char}\overline{K}$, show that $V = T(\sqrt[e]{\pi})$ with T the inertia field of L/K and π a prime element of T. What can you say about $[L : V]$?

5. Let K be as in the previous exercise. Show that there exists a maximal tamely ramified extension K^{tame}/K inside K^{sep}. Show also that K^{tame} is Galois over K^{unr} and that we have

$$\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \begin{cases} \widehat{\mathbf{Z}} & \text{if } \mathrm{char}\overline{K} = 0; \\ \widehat{\mathbf{Z}}/\mathbf{Z}_p & \text{if } \mathrm{char}\overline{K} = p > 0. \end{cases}$$

6. Show that a compositum of two totally ramified extensions need not be totally ramified. Deduce that there is not in general a unique maximal totally ramified extension $K^{\mathrm{ram}} \subset K^{\mathrm{ac}}$ of a complete field K.

7. Let L/K and e_0 be as in exercise 4 and suppose that $\#\overline{K} = q < \infty$. Show that V/K is abelian if and only if e_0 divides $q - 1$.
[Hint: if V/K is abelian, there is a primitive e_0-th root of unity $\zeta_{e_0} = \tau(\sqrt[e]{\pi})/(\sqrt[e]{\pi})$ in T that is invariant under $\mathrm{Gal}(V/K)$.]

8. Show that the maximal tamely ramified abelian extension M of the field K in the previous exercise is cyclic of degree $q - 1$ over K^{unr}, and that $\mathrm{Gal}(M/K) \cong (\mathbf{Z}/(q-1)\mathbf{Z}) \times \widehat{\mathbf{Z}}$.

9. Show that $K = \cup_{n \geq 1} \mathbf{C}((X^{1/n}))$ is an algebraically closed field. Show also that K is not complete with respect to the extension valuation of $\mathbf{C}((X))$, and that the completion Ω of K consists of Laurent series $\sum_i a_i X^{n_i}$ with coefficients $a_i \in \mathbf{C}$ and exponents $n_i \in \mathbf{Q}$ that satisfy $\lim_i n_i = +\infty$. Is Ω algebraically closed?

10. Show that the algebraic closure of $\mathbf{Q}_p$ is not complete under the p-adic valuation, and let $\mathbf{C}_p$ be its completion. Show that $\mathbf{C}_p$ is algebraically closed. Compute the transcendence degree of $\mathbf{C}_p/\mathbf{Q}$, and deduce that $\mathbf{C}_p$ is isomorphic to the field of complex numbers (as a field, not as a topological field!).

11. Let L/K be an extension of local fields of degree n and residue class degree f. Show that we have $\mathrm{ord}_{\mathfrak{p}_K}(\Delta(L/K)) \geq n - f$ with equality if and only if L/K is tamely ramified.

12. Verify Serre's formula 4.10 for n coprime to $\mathrm{char}\overline{K}$.

13. For $K = \mathbf{F}_p((T))$ and $n \geq 1$, let K_n be the extension obtained by adjoining a root of the polynomial $f = X^p + T^n X + T$. Show that K_n is a totally ramified separable extension of degree p of the local field K, and that K_n and K_m are not isomorphic over K when $m \neq n$.

14. Deduce from Serre's formula that up to isomorphism, the number of extensions of a local field of given discriminant is finite.

5 Galois theory of valued fields

We have seen in the previous section that every finite extension L of a field K that is complete with respect to a discrete prime divisor gives rise to two subfields $T \subset V \subset L$ of L that are separable over K. In this section we will describe the Galois correspondence for such fields. We will assume in this section that both L/K and the residue class field extension $\overline{L}/\overline{K}$ are separable. There is always a maximal subfield $L_s \subset L$ for which these assumptions are satisfied, and in most cases that occur in practice one has $L_s = L$. After we have dealt with the case of complete extensions, we will pass to the global case and discuss the relation between local and global Galois groups.

▶ Inertia subgroup

Assume that K is complete with respect to a discrete prime divisor and that L/K is a finite Galois extension for which $\overline{L}/\overline{K}$ is separable.

5.1. Proposition. *The residue class field extension $\overline{L}/\overline{K}$ is Galois and the natural map $\rho : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\overline{L}/\overline{K})$ is surjective. The invariant field $L^{\ker \rho}$ is the inertia field of L/K.*

Proof. Every element $\sigma \in \mathrm{Gal}(L/K)$ induces an automorphism $\overline{\sigma} \in \mathrm{Aut}_{\overline{K}}(\overline{L})$, so we have a natural image $\overline{G}$ of $G = \mathrm{Gal}(L/K)$ in $\mathrm{Aut}_{\overline{K}}(\overline{L})$. We will prove that $\overline{L}/\overline{K}$ is Galois and that ρ is surjective by showing that $\overline{K}$ equals the invariant field $\overline{L}^{\overline{G}}$.

We clearly have $\overline{K} \subset \overline{L}^{\overline{G}}$, so let $\overline{x} \in \overline{L}^{\overline{G}}$ have representative $x \in A_L$. If $\overline{K}$ has characteristic zero, another representative is given by

$$\frac{1}{[L:K]} \sum_{\sigma \in G} \sigma(x) \in L^G = K$$

and we are done. For $\mathrm{char}\overline{K} = p > 0$ we let S be a p-Sylow subgroup of G and $\Gamma \subset G$ a system of left coset representatives of S in G. As every conjugate of x has image $\overline{x}$ in $\overline{L}$, the element

$$\frac{1}{[G:S]} \sum_{\sigma \in \Gamma} \sigma\Big(\prod_{\tau \in S} \tau(x)\Big) \in L^G = K$$

has image $\overline{x}^{\#S} \in \overline{K}$. As $\#S$ is a p-power and $\overline{L}/\overline{K}$ is separable, this implies $\overline{x} \in \overline{K}$, as was to be shown.

Let T be the invariant field $L^{\ker \rho}$. Then we have $[T : K] = [\overline{L} : \overline{K}]$. The natural map $\ker \rho = \mathrm{Gal}(L/T) \to \mathrm{Gal}(\overline{L}/\overline{T})$ is the zero map but, as we have just shown, it is also surjective. We therefore have $\overline{L} = \overline{T}$, and the equality $[T : K] = [\overline{T} : \overline{K}]$ shows that T/K is unramified. It follows from 4.1 that T is the inertia field of L/K. □

The kernel of the map in the proposition is the *inertia group* $I \subset \mathrm{Gal}(L/K)$ of the extension L/K. Its order is equal to the ramification index of L/K, so I is the trivial subgroup if and only if L/K is unramified. In that case 5.1 reduces to the statement in 4.3.

▶ Ramification groups

Let $\mathfrak{p}_L = \pi_L A_L$ be the maximal ideal in A_L. Then we define the *i-th ramification group* $G_i \subset G = \mathrm{Gal}(L/K)$ of L/K as

$$\begin{aligned} G_i &= \{\sigma \in G : \psi(x - \sigma(x)) < \psi(\pi_L^i) \text{ for all } x \in A_\psi\} \\ &= \ker[G \to \mathrm{Aut}(A_L/\mathfrak{p}_L^{i+1})]. \end{aligned}$$

The definition shows that all G_i are normal subgroups of G. As every $\sigma \neq \mathrm{id}_L$ is not in G_i for i sufficiently large, we have $G_i = \{1\}$ for large i. We formally have $G_{-1} = G$, and for $i = 0$ we find that $G_0 = I$ is the inertia group of ψ. The sequence

$$G = G_{-1} \supset I = G_0 \supset G_1 \supset G_2 \supset \dots$$

of subgroups corresponds to an sequence of fields $V_i = L^{G_i}$ that are known for $i \geq 1$ as the *ramification fields* of L/K. We will show in 5.4 that the first ramification field $V = V_1$ is the ramification field constructed in exercise 4.4.

5.2. Theorem. *Let π_L be a prime element of L and write $U_L^{(0)} = A_L^*$ and $U_L^{(i)} = 1 + \mathfrak{p}_L^i$ for $i \geq 1$. Then the map*

$$\begin{aligned} \chi_i : G_i &\longrightarrow U_L^{(i)}/U_L^{(i+1)} \\ \sigma &\longmapsto \sigma(\pi_L)/\pi_L \end{aligned}$$

is for each $i \geq 0$ a homomorphism with kernel G_{i+1} that does not depend on the choice of the prime element π_L.

Proof. Let us check first that χ_i does not depend on the choice of π_L. If $u \in A_L^*$ is a unit, then we have $\sigma(u)/u \in U_L^{(i+1)}$ for $\sigma \in G_i$ and consequently

$$\frac{\sigma(u\pi_L)}{u\pi_L} = \frac{\sigma(u)}{u} \cdot \frac{\sigma(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L} \in U_L^{(i)}/U_L^{(i+1)}.$$

For $\sigma, \tau \in G_i$ we conclude from this that we have

$$\chi_i(\sigma\tau) = \frac{(\sigma\tau)(\pi_L)}{\pi_L} = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \cdot \frac{\tau(\pi_L)}{\pi_L} = \chi_i(\sigma)\chi_i(\tau),$$

so χ_i is a homomorphism. In order to prove that $\ker \chi_i = G_{i+1}$, it suffices show that for $\sigma \in G_0$ an element of the inertia group and $i \geq 1$, we have

$$\sigma \in G_i \iff \sigma(\pi_L) - \pi_L \in \mathfrak{p}_L^{i+1} \iff \sigma(\pi_L)/\pi_L \in 1 + \mathfrak{p}_L^i.$$

For the last two conditions the equivalence is clear. The middle condition is obviously necessary to have $\sigma \in G_i$, and for its sufficiency we write $A_L = A_T[\pi_L]$ and remark that an element $x = \sum_k a_k \pi_L^k \in A_T[\pi_L]$ satisfies $\sigma(x) - x = \sum_k a_k(\sigma(\pi_L)^k - \pi_L^k) \in \mathfrak{p}_L^{i+1}$ since $\sigma(a_k) = a_k \in T$ for $\sigma \in G_0$ and $\sigma(\pi_L^k) - \pi_L^k$ is divisible by $\sigma(\pi_L) - \pi_L$ for all k. □

5.3. Corollary. *The group G_0/G_1 is cyclic of order coprime to* char$\overline{K}$. *If G is abelian, there is a canonical embedding $\chi_0 : G_0/G_1 \rightarrowtail \overline{K}^*$.*

Proof. The isomorphism $U_L^{(0)}/U_L^{(1)} = \overline{L}^*$ and 5.2 give us an injection $\chi_0 : G_0/G_1 \rightarrowtail \overline{L}^*$, so G_0/G_1 is a finite subgroup of the unit group of a field and therefore cyclic. Its order is coprime to char$K$ as there are no p-th roots of unity in a field of characteristic $p > 0$.

If G is abelian, we have $\sigma(\chi_0(\tau)) = (\sigma\tau)(\pi_L)/\sigma(\pi_L) = (\tau\sigma)(\pi_L)/\sigma(\pi_L) = \chi_0(\tau)$ for $\sigma \in G$ and $\tau \in G_0$, so the image of χ_0 is in $(\overline{L}^*)^G = \overline{K}^*$. □

5.4. Corollary. *The group G_1 is trivial for* char$\overline{K} = 0$ *and a p-group for* char$\overline{K} = p > 0$. *The first ramification field $V_1 = L^{G_1}$ is the largest subfield of L that is tamely ramified over K.*

Proof. For $i \geq 1$ we have an isomorphism $U_L^{(i)}/U_L^{(i+1)} \xrightarrow{\sim} \overline{L}$ that sends $1 + a\pi_l^i$ to $\overline{a}$. If char$\overline{K} = 0$ there are no elements of finite additive order in $\overline{L}$, so $G_i/G_{i+1} = 0$ for all $i \geq 1$ and therefore $G_1 = 0$. For char$\overline{K} = p > 0$ all non-zero elements of $\overline{L}$ have additive order p, so each quotient G_i/G_{i+1} is an elementary abelian p-group. It follows that G_1 is a p-group. In this case, the corresponding field $V = L^{G_1}$ is totally ramified of degree $\#(G_0/G_1)$ coprime to p over the inertia field T, whereas L/V is totally ramified of p-power degree. We conclude that V is the maximal tamely ramified subfield. For char$K = 0$ this is trivially true since $V = L$. □

Example. Consider for p prime the cyclotomic extension $L = \mathbf{Q}_p(\zeta_p)$ of $K = \mathbf{Q}_p$ occurring in example 4.6. This is a Galois extension with group $G = (\mathbf{Z}/p\mathbf{Z})^*$ if we identify t mod p with the automorphism $\sigma_t : \zeta_p \mapsto \zeta_p^t$. The extension is totally and tamely ramified, so we have $G_0 = G$ and $G_1 = 0$. Taking $\pi_L = 1 - \zeta_p$, we see that the homomorphism $\chi_0 : G_0 \to \overline{L} = \mathbf{F}_p$ maps σ_t to the residue class

$$\frac{\sigma_t(\pi_L)}{\pi_L} = \frac{1 - \zeta_p^t}{1 - \zeta_p} = 1 + \zeta_p + \zeta_p^2 + \ldots + \zeta_p^{t-1} \equiv t \in \overline{L},$$

so it is in this case an isomorphism.

More generally, we can consider $L = \mathbf{Q}_p(\zeta_{p^k})$ over $K = \mathbf{Q}_p$, which is abelian with group $G = (\mathbf{Z}/p^k\mathbf{Z})^*$. This is a totally ramified extension, so again $G_0 = G$. The argument above, when applied for the prime element $\pi_L = 1 - \zeta_{p^k}$, yields

$$G_i = \{\sigma_t : t \equiv 1 \bmod p^i\} = \langle 1 + p^i \rangle \subset (\mathbf{Z}/p^k\mathbf{Z})^*$$

for all $i \geq 1$. In particular, all injections $\chi_i : G_i/G_{i+1} \to U_L^{(i)}/U_L^{(i+1)} \cong \mathbf{F}_p$ are isomorphisms for this extension.

▶ Decomposition group

We now consider the case of an arbitrary finite field extension. If ϕ is any valuation on K and ψ an extension of ϕ to a finite Galois extension L of K, then the completion L_ψ

is the compositum of its subfields L and K_ϕ. Standard Galois theory tells us that L_ψ/K_ϕ is a finite Galois extension, and that $G_\psi = \mathrm{Gal}(L_\psi/K_\phi)$ is isomorphic to the subgroup of $\mathrm{Gal}(L/K)$ corresponding to the subfield $L \cap K_\phi$.

$$\begin{array}{ccc} & L_\psi \quad G_\psi & \\ L & & K_\phi \\ & L \cap K_\phi & \\ & K & \end{array}$$

By the uniqueness of the extension valuation in the complete extension L_ψ/K_ϕ, we have $\psi(\sigma(x)) = \psi(x)$ for $x \in L_\psi$ and $\sigma \in G_\psi$. If we view G_ψ as a subgroup of $\mathrm{Gal}(L/K)$, we can write

$$G_\psi = \{\sigma \in \mathrm{Gal}(L/K) : \psi(\sigma(x)) = \psi(x) \text{ for all } x \in L\}$$

since every element of the right hand side extends uniquely by continuity to an automorphism of L_ψ over K_ϕ. This subgroup is known as the *decomposition group* of ψ in L/K, and the corresponding invariant subfield L^{G_ψ} is the *decomposition field* of ψ in L/K.

We define a left action of $G = \mathrm{Gal}(L/K)$ on the finite set $X = \{\psi|\phi\}$ of extensions of ϕ to L by setting

$$(\sigma\psi)(x) = \psi(\sigma^{-1}(x)) \qquad \text{for } x \in L.$$

If ψ is non-archimedean with valuation ring A_ψ and maximal ideal $\mathfrak{q}_\psi$, the valuation $\sigma\psi$ has valuation ring $\sigma[A_\psi]$ and maximal ideal $\sigma[\mathfrak{q}_\psi]$. Thus, for a number field L the G-action on the finite primes of L is 'the same' as the natural G-action on the corresponding prime ideals in the ring of integers of L that was studied in [I, §8]. The theorem given there can be generalized in the following way.

5.5. Proposition. *Let L/K be a finite Galois extension with group G and X the set of extensions of a valuation ϕ on K to L. Then G acts transitively on X, and the stabilizer $G_\psi \subset G$ of $\psi \in X$ is the decomposition group of ψ in L/K. All decomposition groups G_ψ of $\psi \in X$ are conjugate in G.*

Proof. Suppose that there exist extensions $\psi_1, \psi_2 \in X$ that lie in different G-orbits. Then the orbits $G\psi_i = \{\sigma\psi_i : \sigma \in G\}$ are disjoint for $i = 1, 2$, so the approximation theorem implies that there exists $x \in L$ with $\psi(x) < 1$ for $\psi \in G\psi_1$ and $\psi(x) > 1$ for $\psi \in G\psi_2$. The product $\prod_{\sigma\in G}(\sigma\psi_i)(x) = \psi_i(N_{L/K}(x))$ is then smaller than 1 for $i = 1$ and greater than 1 for $i = 2$. This contradicts the fact that ψ_1 and ψ_2 coincide on $N_{L/K}(x) \in K$, so there cannot be two distinct G-orbits and G acts transitively on X.

We have already seen above that the decomposition group G_ψ is the stabilizer of ψ in G, and in view of the transitivity the general identity $G_{\sigma\psi} = \sigma G_\psi \sigma^{-1}$ for stabilizers shows that all decomposition groups of $\psi \in X$ are conjugate in G. □

5.6. Corollary. *For a normal extension L/K, the completions L_ψ for $\psi|\phi$ are all isomorphic over K_ϕ. In particular, the ramification indices $e = e(\psi/\phi)$ and the residue class degrees $f = f(\psi/\phi)$ do not depend on the choice of ψ, and one has $[L : K] = efg$ with g the number of different extensions of ϕ to L.*

Proof. If $\psi_2 = \sigma\psi_1$ for $\sigma \in \mathrm{Gal}(L/K)$, then σ induces an isomorphism $L_{\psi_1} \xrightarrow{\sim} L_{\psi_2}$ on the completions that is the identity on K_ϕ. The final formula follows from 3.10 and the convention for archimedean ϕ following it. □

If the extension L/K in 4.1 is *abelian*, all decomposition groups G_ψ for $\psi \in X$ coincide. In that case, we can speak of the decomposition group G_ϕ of ϕ in L/K.

5.7. Theorem. *Let L/K be a finite Galois extension and Z_ψ the decomposition field of a valuation ψ on L that is either archimedean or discrete and has restriction ϕ on K. Then Z_ψ/K is the largest subextension E/K of L/K for which*

$$e(\psi|_E/\phi) = f(\psi|_E/\phi) = 1.$$

Proof. By construction, Z_ψ is the largest subfield of L that is contained in K_ϕ, and a subfield $E \supset K$ of L is contained in K_ϕ if and only if its completion, which has degree $e(\psi|_E/\phi)f(\psi|_E/\phi)$ over K_ϕ by 3.10, is equal to K_ϕ. The theorem follows. □

▶ Galois theory for global fields

We will further suppose that L/K is a finite Galois extension with group G and ψ and ϕ correspond to discrete prime divisors $\mathfrak{q}$ and $\mathfrak{p}$ for which the residue class field extension $\overline{L}/\overline{K}$ is separable. In the case of an extension of number fields, one may think of $\mathfrak{q}$ and $\mathfrak{p}$ as ideals in the respective rings of integers. We see from 5.7 that the decomposition field $Z_\mathfrak{q}$ of $\mathfrak{q}$ in L/K is the largest subfield E for which $\mathfrak{q}_E = \mathfrak{q} \cap E$ satisfies $e(\mathfrak{q}_E/\mathfrak{p}) = f(\mathfrak{q}_E/\mathfrak{p}) = 1$. If L/K is in addition abelian, $Z_\mathfrak{q} = Z_\mathfrak{p}$ is the largest subextension in which the prime $\mathfrak{p}$ splits completely. This explains the name 'decomposition field'. Note that everything remains correct for infinite primes if we call an infinite prime $\mathfrak{p} : K \to \mathbf{C}$ 'totally split' in L if all its extensions $\mathfrak{q}$ to L have $[L_\mathfrak{q} : K_\mathfrak{p}] = e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p}) = 1$.

By definition of the decomposition field $Z_\mathfrak{q}$ of a prime $\mathfrak{q}$ in L/K, there is an identification of Galois groups

$$\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) \xrightarrow{\sim} G_\mathfrak{q} = \mathrm{Gal}(L/Z_\mathfrak{q})$$

that is obtained by restriction of the automorphisms of $L_\mathfrak{q}/K_\mathfrak{p}$ to L. We can apply our theory for complete Galois extensions to $L_\mathfrak{q}/K_\mathfrak{p}$, so the inertia and ramification fields of $L_\mathfrak{q}/K_\mathfrak{p}$ can be intersected with L to produce a sequence of fields

$$K \subset Z_\mathfrak{q} \subset T_\mathfrak{q} \subset V_\mathfrak{q} \subset L$$

corresponding to subgroups

$$G \supset G_\mathfrak{q} \supset I_\mathfrak{q} = G_{\mathfrak{q},0} \supset R_\mathfrak{q} = G_{\mathfrak{q},1} \supset \{1\}.$$

of G. Here $T_\mathfrak{q}$ is the inertia field of $\mathfrak{q}$ in L/K, it corresponds to the inertia group $I_\mathfrak{q} \cong \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})_0$ of $\mathfrak{q}$ in G. It is the largest subfield of L for which the restriction of $\mathfrak{q}$ is unramified over K. The (first) ramification field $V_\mathfrak{q}$ of $\mathfrak{q}$ in L/K corresponds to the (first) ramification group $R_\mathfrak{q} \cong \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})_1$ of $\mathfrak{q}$ in L/K. It is the largest subfield of L for which the restriction of $\mathfrak{q}$ is tamely ramified over K. The groups $I_\mathfrak{q}$ and $R_\mathfrak{q}$ are normal in $G_\mathfrak{q}$, but not necessarily in G. More precisely, one has

$$\sigma G_\mathfrak{q}\sigma^{-1} = G_{\sigma\mathfrak{q}} \qquad \sigma I_\mathfrak{q}\sigma^{-1} = I_{\sigma\mathfrak{q}} \qquad \sigma R_\mathfrak{q}\sigma^{-1} = R_{\sigma\mathfrak{q}}$$

for σ in G. In particular, we see that for *abelian* extensions, the decomposition, inertia and ramification group depend only on the prime of the base field K, not on the choice of the extension prime.

▶ Non-normal extensions

If L/K is a finite separable extension of discretely valued fields for which the residue class field extension is separable, we can obtain the decomposition, inertia and ramification fields of a prime $\mathfrak{q}$ in L/K by extending $\mathfrak{q}$ to a normal closure M of L over K and form the intersection of L with the decomposition, inertia and ramification fields of this extension in M/K. Conversely, knowledge of these fields in L/K can be helpful to determine the corresponding fields in M/K.

Example. The number field $K = \mathbf{Q}(\alpha)$ with $\alpha^4 = 17$ we considered after 3.9 is not normal over $\mathbf{Q}$. Its normal closure $M = K(i)$ is obtained by adjoining $i = \sqrt{-1}$ to K. This is a Galois extension of $\mathbf{Q}$ with group D_4, the dihedral group of 8 elements. We have seen that the prime 2 factors as $2\mathcal{O}_K = \mathfrak{p}\mathfrak{q}\mathfrak{r}^2$ in this field, so we have $Z_\mathfrak{p} = T_\mathfrak{p} = K$ and $Z_\mathfrak{r} = T_\mathfrak{r} = \mathbf{Q}(\sqrt{17})$. In the normal closure $M/\mathbf{Q}$, there are at least 3 primes over 2, and they are all ramified over $\mathbf{Q}$ by 5.6. The formula $efg = 8$ shows that there are 4 primes over 2 with $e = 2$ and $f = 1$. In particular, the primes $\mathfrak{p}$ and $\mathfrak{q}$ are ramified in the quadratic extension M/K and $\mathfrak{r}$ splits completely in M/K to yield a factorisation $2\mathcal{O}_M = \mathfrak{P}^2\mathfrak{Q}^2\mathfrak{R}_1^2\mathfrak{R}_2^2$. The decomposition fields of $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{Q}|\mathfrak{q}$ in $M/\mathbf{Q}$ are equal to K, whereas the primes $\mathfrak{R}_i|\mathfrak{r}$ have the conjugate field $\mathbf{Q}(i\alpha)$ as their decomposition field. Note that indeed $Z_\mathfrak{r} = Z_{\mathfrak{R}_i} \cap K$.

It is clear from what we said above that the splitting behaviour of a prime in a finite extension is determined by the decomposition and inertia groups of the primes that lie over it in a normal closure. Conversely, the knowledge of the splitting behaviour of a few primes can be used to determine the Galois group of the normal closure of an extension. More precisely, we have the following relation between the action of decomposition and inertia groups on the one hand and the factorization of a non-archimedean prime on the other hand. All residue class field extensions are supposed to be separable.

5.8. Theorem. *Let L/K be a finite separable extension, M the normal closure of L over K and $\mathfrak{p}$ a discrete prime divisor on K. Set $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L) \subset G$, and*

let G act in the natural way on the set Ω of left cosets of H in G. Suppose we are given integers $e_i, f_i > 0$ for $i = 1, 2, \ldots, t$ such that $\sum_{i=1}^{t} e_i f_i = [L : K]$. Then the following two statements are equivalent.

(1) *the prime $\mathfrak{p}$ has t distinct extensions $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_t$ to L with ramification indices $e(\mathfrak{q}_i/\mathfrak{p}) = e_i$ and residue class field degrees $f(\mathfrak{q}_i/\mathfrak{p}) = f_i$;*

(2) *for every decomposition group $G_{\mathfrak{P}} \subset G$ of a prime $\mathfrak{P}$ above $\mathfrak{p}$ in M/K, there are t different $G_{\mathfrak{P}}$-orbits $\Omega_i \subset \Omega$ of length $\#\Omega_i = e_i f_i$. Under the action of the inertia group $I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$ on Ω_i, there are f_i orbits of length e_i each.*

Proof. Let $\mathfrak{P}$ be a prime over $\mathfrak{p}$ in M with restriction $\mathfrak{q}$ to L, and write $\Omega_{\mathfrak{P}}$ for the $G_{\mathfrak{P}}$-orbit of the coset $H \in \Omega$. The length of this orbit is $[G_{\mathfrak{P}} : G_{\mathfrak{P}} \cap H]$, and this is equal to the degree $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p})$ since we have a tower of complete extensions

$$M_{\mathfrak{P}} \supset L_{\mathfrak{q}} \supset K_{\mathfrak{p}}$$

in which $\mathrm{Gal}(M_{\mathfrak{P}}/K_{\mathfrak{p}}) = G_{\mathfrak{P}}$ contains a subgroup $H_{\mathfrak{P}} = H \cap G_{\mathfrak{P}}$ corresponding to $L_{\mathfrak{q}}$. An arbitrary $G_{\mathfrak{P}}$-orbit in Ω, say of the residue class gH, can be written as

$$G_{\mathfrak{P}} \cdot gH = g \cdot G_{g^{-1}\mathfrak{P}} H = g \cdot \Omega_{g^{-1}\mathfrak{P}},$$

so the length of such an orbit equals $e(\mathfrak{q}'/\mathfrak{p}) f(\mathfrak{q}'/\mathfrak{p})$ with $\mathfrak{q}'$ the restriction of $g^{-1}\mathfrak{P}$ to L. We do obtain a bijection between extensions of $\mathfrak{p}$ to L and $G_{\mathfrak{P}}$-orbits in Ω:

$$\begin{aligned} g_1^{-1}\mathfrak{P} \cap L = g_2^{-1}\mathfrak{P} \cap L &\iff \exists h \in H : h g_1^{-1}\mathfrak{P} = g_2^{-1}\mathfrak{P} \iff \exists h \in H : g_2 h g_1^{-1} \in G_{\mathfrak{P}} \\ &\iff \exists h \in H : G_{\mathfrak{P}} \cdot g_2 h = G_{\mathfrak{P}} \cdot g_1 \iff G_{\mathfrak{P}} \cdot g_2 H = G_{\mathfrak{P}} \cdot g_1 H. \end{aligned}$$

The inertia group $I_{\mathfrak{P}}$ of $\mathfrak{P}$ is a normal subgroup of $G_{\mathfrak{P}}$, so all $I_{\mathfrak{p}}$-orbits inside a single $G_{\mathfrak{P}}$-orbit have the same length. Inside the orbit $\Omega_{\mathfrak{P}}$ this length is equal to the group index $[I_{\mathfrak{P}} : I_{\mathfrak{P}} \cap H] = [I_{\mathfrak{P}} : I_{\mathfrak{P}} \cap H_{\mathfrak{P}}] = [I_{\mathfrak{P}} H_{\mathfrak{P}} : H_{\mathfrak{P}}]$. In the extension $M_{\mathfrak{P}}/K_{\mathfrak{p}}$, this corresponds to the subextension $L_{\mathfrak{q}}/T_{\mathfrak{q}}$, with $T_{\mathfrak{q}}$ the inertia field of $\mathfrak{q}$ in $L_{\mathfrak{q}}/K_{\mathfrak{p}}$. It follows that the length of the $I_{\mathfrak{P}}$-orbits in $\Omega_{\mathfrak{P}}$ is $[L_{\mathfrak{q}} : T_{\mathfrak{q}}] = e(\mathfrak{q}/\mathfrak{p})$ as asserted. The identity $I_{\mathfrak{P}} \cdot gH = g \cdot I_{g^{-1}\mathfrak{P}} H$ now shows that the length of the $I_{\mathfrak{P}}$-orbits in the $G_{\mathfrak{P}}$-orbit corresponding to a prime $\mathfrak{q}'$ of L equals $e(\mathfrak{q}'/\mathfrak{p})$. □

The preceding theorem remains correct for *infinite* primes $\mathfrak{p} : K \to \mathbf{C}$ of K if we choose appropriate conventions for these primes. For an extension $L_{\mathfrak{q}}/K_{\mathfrak{p}}$ of archimedean complete fields we defined $f(\mathfrak{q}/\mathfrak{p}) = 1$ and $e(\mathfrak{q}/\mathfrak{p}) = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$, so it makes sense to take the inertia group $I_{\mathfrak{q}}$ of an infinite prime in a Galois extension equal to the decomposition group. With this convention, the two assertions in (2) of theorem 5.8 coincide for infinite primes and the theorem holds unchanged.

▶ Frobenius automorphism, Artin symbol

If L/K is a Galois extension of local fields and $\mathfrak{q}$ a finite prime divisor of L extending $\mathfrak{p}$, we have by 5.1 a group isomorphism

$$G_\mathfrak{q}/I_\mathfrak{q} \xrightarrow{\sim} \mathrm{Gal}(F_\mathfrak{q}/F_\mathfrak{p})$$

between a factor group of $G_\mathfrak{q}$ and the Galois group of the residue class extension $\overline{L}/\overline{K} = F_\mathfrak{q}/F_\mathfrak{p}$ at $\mathfrak{q}|\mathfrak{p}$. As the residue class fields for primes of local fields are finite, the Galois group $\mathrm{Gal}(F_\mathfrak{q}/F_\mathfrak{p})$ is cyclic with a canonical generator, the Frobenius automorphism $\sigma_\mathfrak{q}$ that raises every element of $F_\mathfrak{q}$ to the power $\#F_\mathfrak{p}$. If $\mathfrak{q}|\mathfrak{p}$ is unramified, we have an inclusion $G_\mathfrak{q}/I_\mathfrak{q} = G_\mathfrak{q} \subset \mathrm{Gal}(L/K)$, so there exists a Frobenius element $\sigma_\mathfrak{q}$ at $\mathfrak{q}$ in $\mathrm{Gal}(L/K)$. This is is the *Frobenius symbol* $[\mathfrak{q}, L/K]$ of $\mathfrak{q}$ in the Galois group of L/K. It is a well defined element of the Galois group if $\mathfrak{q}$ is unramified over $\mathfrak{p} = \mathfrak{q} \cap K$. For ramified $\mathfrak{q}$ it can only be defined as a coset of $I_\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

If $\mathfrak{q}$ is infinite, there is no analogue of the Frobenius automorphism and we have set $G_\mathfrak{q} = I_\mathfrak{q}$. However, it is often convenient to take the Frobenius symbol for such primes to be equal to the generator of the decomposition group $G_\mathfrak{q}$. This is a group of order at most two, and the Frobenius at $\mathfrak{q}$ is only different from the unit element in $\mathrm{Gal}(L/K)$ when $\mathfrak{q}$ is complex and $\mathfrak{p} = \mathfrak{q}|_K$ is real. In this situation, $[\mathfrak{q}, L/K]$ is the complex conjugation on L induced by the embedding $\mathfrak{q} : K \to \mathbf{C}$.

It is immediate from the definition that the Frobenius symbol satisfies

$$[\sigma\mathfrak{q}, L/K] = \sigma[\mathfrak{q}, L/K]\sigma^{-1} \qquad \text{for } \sigma \in \mathrm{Gal}(L/K).$$

In particular, this shows that the Frobenius symbol of $\mathfrak{q}$ in an abelian extension L/K depends only on the restriction $\mathfrak{p} = \mathfrak{q} \cap K$. In that case the symbol is called the *Artin symbol* of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. It is denoted by $(\mathfrak{p}, L/K)$. It is of fundamental importance in describing abelian extensions of number fields. For a few formal properties of Frobenius and Artin symbols we refer to exercise 12.

Exercises

1. Show that every Galois extension of a local field is solvable.

2. Let L be a Galois extension of a non-archimedean local field K. Show that the valuation of the different $\mathfrak{D}(L/K)$ is given by the formula

$$\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = \textstyle\sum_{i=0}^{\infty}(\#G_i - 1).$$

   Deduce that $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = e - 1$ if and only if L/K is tamely ramified.
   [Hint: look at $f'(\pi_L)$ for $f = f_T^{\pi_L}$.]

3. Determine all ramification groups for the cyclotomic extension $\mathbf{Q}_p(\zeta_{p^k})/\mathbf{Q}_p$. Deduce that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}(\mathbf{Q}_p(\zeta_{p^k})/\mathbf{Q}_p)) = kp^k - (k+1)p^{k-1}$.

4. Determine the decomposition, inertia and ramification fields of the primes over 3, 5, 17 and 149 in the splitting field of $X^4 - 17$ over $\mathbf{Q}$. What are the decomposition fields of the infinite primes?

5. Let p be an odd prime number and $n = p^k m$ an integer with $p \nmid m$. Show that the decomposition, inertia and ramification groups and fields of p for the cyclotomic extension $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ with group $G = \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong (\mathbf{Z}/p^k\mathbf{Z})^* \times (\mathbf{Z}/m\mathbf{Z})^*$ are given by the following table.

$\mathbf{Q}(\zeta_n)$	$\leftrightarrow$	$\{1\}$	
$V_p = \mathbf{Q}(\zeta_p, \zeta_m)$	$\leftrightarrow$	$\langle (1+p) \bmod p^k \rangle$	$\times\{1\}$
$T_p = \mathbf{Q}(\zeta_m)$	$\leftrightarrow$	$(\mathbf{Z}/p^k\mathbf{Z})^*$	$\times\{1\}$
Z_p	$\leftrightarrow$	$(\mathbf{Z}/p^k\mathbf{Z})^*$	$\times\langle p \bmod m \rangle$
$\mathbf{Q}$	$\leftrightarrow$	$(\mathbf{Z}/p^k\mathbf{Z})^*$	$\times(\mathbf{Z}/m\mathbf{Z})^*$

   Deduce that the Artin symbol of p in $G/I_p \cong (\mathbf{Z}/m\mathbf{Z})^*$ is the residue class $p \bmod m$. What does the table look like for $p = 2$?

6. Determine the decomposition and inertia fields of all primes $p < 20$ in the cylotomic extension $\mathbf{Q}(\zeta_{20})/\mathbf{Q}$. Do all subfields occur as a decomposition field of some p?

7. Let $K = \mathbf{Q}(\sqrt{-5})$ and write $i = \sqrt{-1}$. Show that the extension $K \subset K(i)$ is unramified at all primes, and that there is an isomorphism

$$Cl_K \xrightarrow{\sim} \mathrm{Gal}(K(i)/K)$$

   that sends the class of a prime $\mathfrak{p} \subset \mathcal{O}_K$ in Cl_K to the Artin symbol of $\mathfrak{p}$ in $\mathrm{Gal}(K(i)/K)$.

8. Let K be a field that is complete with respect to a discrete valuation with a perfect residue class field. Let L/K be a finite Galois extension with Galois group G and ramification groups G_i. Let $H \subset G$ be a subgroup, and $E = L^H$ the corresponding subfield.
   a. Prove that the i-th ramification group of the extension L/E equals $G_i \cap H$ for every $i \geq 0$.
   b. Suppose that E is Galois over K, with Galois group Γ ($\cong G/H$). Prove that the images of G_0 and G_1 under the natural map $G \to \Gamma$ are the inertia group and the first ramification group of E/K, respectively. Show by an example that the corresponding statement for higher ramification groups is not in general true.

9. Let $L = \mathbf{Q}_5(\sqrt[4]{50})$, and let E be the maximal unramified subextension of $\mathbf{Q}_5 \subset L$. Exhibit a prime element π_E of the valuation ring of E such that $L = E(\sqrt{\pi_E})$. Can π_E be chosen to lie in $\mathbf{Q}_5$?

10. Let $f \in \mathbf{Z}[X]$ be a monic separable polynomial of degree n and G the Galois group of the splitting field Ω of f over $\mathbf{Q}$. View G as a subgroup of the symmetric group S_n via the action of G on the n roots of f in Ω. Let p be a prime number that does not divide the discriminant $\Delta(f)$ of f, and suppose that $f \bmod p$ factors in $\mathbf{F}_p[X]$ as a product of t irreducible factors of degree $n_1, n_2, \ldots, n_t$. Show that G contains a product of t disjoint cycles of length $n_1, n_2, \ldots, n_t$.
[This is a very effective criterion in computing G.]

11. Let K be a local field of characteristic $p > 0$ and L/K a finite separable extension. Show that $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) \not\equiv -1 \bmod p$.

12. Let $K \subset L \subset M$ be extensions of number fields and $\mathfrak{p}_M$ a prime of M with restrictions $\mathfrak{p}_L$ and $\mathfrak{p}_K$. If L/K and M/K are Galois and $\mathfrak{p}_M/\mathfrak{p}_K$ is unramified, show that the Frobenius symbols satisfy
$$[\mathfrak{p}_M, M/K]|_L = [\mathfrak{p}_L, L/K].$$
Similarly, for E/K any finite extension and $\mathfrak{p}_{EL}$ an extension of $\mathfrak{p}_L$ to EL, show that
$$[\mathfrak{p}_{EL}, EL/E]|_L = [\mathfrak{p}_L, L/K]^{f(\mathfrak{p}_E/\mathfrak{p}_K)}$$
for L/K Galois and $\mathfrak{p}_L/\mathfrak{p}_K$ unramified. Are there analogues for infinite primes? What are the resulting relations for the Artin symbols if M/K and L/K are assumed to be abelian?

In the next two exercises we let M/K be a Galois extension of number fields with group G and $L = M^H \subset M$ the invariant field of a subgroup H of G. We let $\mathfrak{r}$ be a prime of M with restrictions $\mathfrak{q}$ in L and $\mathfrak{p}$ in K.

13. Suppose that G is isomorphic to the symmetric group S_5 of order 120, that $G_\mathfrak{r}$ has order 6, and that $I_\mathfrak{r}$ has order 2.
    a. Prove that, if the identification of G with S_5 is suitably chosen, $G_\mathfrak{r}$ is generated by the permutation $(1\,2\,3)(4\,5)$ and $I_\mathfrak{r}$ by $(4\,5)$.
    b. Suppose that $[L : K] = 5$. How many extensions $\mathfrak{q}'$ does $\mathfrak{p}$ have to L, and what are the numbers $e(\mathfrak{q}'/\mathfrak{p})$ and $f(\mathfrak{q}'/\mathfrak{p})$?
    c. Suppose that $[L : K] = 15$. How many extensions $\mathfrak{q}'$ does $\mathfrak{p}$ have to L, and what are the numbers $e(\mathfrak{q}'/\mathfrak{p})$ and $f(\mathfrak{q}'/\mathfrak{p})$?

14. Suppose that G is isomorphic to the symmetric group S_4 of order 24, and that $\mathfrak{r}$ is the *only* prime of M extending $\mathfrak{p}$.
    a. Prove that $\mathfrak{p}$ is 2-adic, in the sense that the restriction of $\mathfrak{p}$ to $\mathbf{Q}$ is the 2-adic prime of $\mathbf{Q}$, and determine $G_\mathfrak{r}$ and $I_\mathfrak{r}$ as subgroups of S_4.
    b. Suppose that H is cyclic of order 4. Determine $e(\mathfrak{r}/\mathfrak{q})$, $f(\mathfrak{r}/\mathfrak{q})$, $e(\mathfrak{q}/\mathfrak{p})$, and $f(\mathfrak{q}/\mathfrak{p})$.

6 The Kronecker-Weber theorem

If K is a number field, the n-th *cyclotomic extension* $K \subset L = K(\zeta_n)$ obtained by adjoining the roots of $X^n - 1$ for some integer $n \geq 1$ to K is abelian, as $\sigma \in \mathrm{Gal}(L/K)$ is determined by the value $\sigma(\zeta_n) = \zeta_n^k$ it assumes on a primitive n-th root of unity ζ_n generating L over K. More precisely, we have an injective map

$$\mathrm{Gal}(K(\zeta_n)/K) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

sending an automorphism $\sigma_k : \zeta_n \mapsto \zeta_n^k$ to $(k \bmod n)$. For $K = \mathbf{Q}$ or, more generally, for K linearly disjoint from $\mathbf{Q}(\zeta_n)$, this map is an isomorphism as the n-th cyclotomic polynomial

$$\Phi_n = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^*} (X - \zeta_n^k) \in \mathbf{Z}[X]$$

is irreducible over $\mathbf{Q}$. The Kronecker-Weber theorem states that for $K = \mathbf{Q}$, cyclotomic extensions are the *only* source of abelian extensions.

6.1. Theorem. *Every finite abelian extension of the rational number field* $\mathbf{Q}$ *is contained in a cyclotomic extension.*

The theorem was stated by Kronecker in 1853, but his proof was incomplete. A second proof was given by Weber in 1886. In 1896 Hilbert used what is essentially the theory of section 5 to give the first complete proof.

▶ Global and local version

The Kronecker-Weber theorem accounts for the fact that *abelian number fields*, as the extensions in the theorem are called, are in many respects more manageable than arbitrary number fields. As Shafarevič (1951) observed, it can be derived from the *same* result for the local fields $\mathbf{Q}_p$, which is also of independent interest. Note that the local result is also correct for $\mathbf{Q}_\infty = \mathbf{R}$, albeit in a somewhat uninteresting way.

6.2. Theorem. *Every finite abelian extension of the p-adic number field* $\mathbf{Q}_p$ *is contained in a cyclotomic extension.*

Before we prove the local result, we will show first how it implies the global theorem.

Proof of (6.2 ⇒ 6.1). Let $L/\mathbf{Q}$ be an abelian extension. Then the completion $L_\mathfrak{p}$ of L at a prime $\mathfrak{p}|p$ is an abelian extension of $\mathbf{Q}_p$ that is determined up to $\mathbf{Q}_p$-isomorphism by the prime p. By 6.2, there exists an integer $n_p = p^{k_p} \cdot m_p$ with $p \nmid m_p$ such that $L_\mathfrak{p}$ is contained in $\mathbf{Q}_p(\zeta_{n_p})$. This implies that the ramification index $e(\mathfrak{p}/p)$ of p in $L/\mathbf{Q}$ does not exceed $[\mathbf{Q}_p(\zeta_{n_p}) : \mathbf{Q}_p(\zeta_{m_p})] = \phi(p^{k_p})$. We claim that L is a subfield of the n-th cyclotomic field $\mathbf{Q}(\zeta_n)$ for $n = \prod_{p|\Delta_L} p^{k_p}$. To see this, we look at the abelian extension $L(\zeta_n)/\mathbf{Q}$, which is ramified at exactly the same rational primes as $L/\mathbf{Q}$.

The ramification index of a prime $p|\Delta_L$ in $L(\zeta_n)$ is equal to $\phi(p^{k_p})$, as its completion at a prime over p is obtained by adjoining a p^{k_p}-th root of unity to an unramified extension of $\mathbf{Q}_p$. The subgroup I of the abelian group $G = \mathrm{Gal}(L(\zeta_n)/\mathbf{Q})$ that is generated by the inertia groups $I_p \subset G$ of the primes p dividing Δ_L has order at most $\prod_{p|\Delta_L} \#I_p = \prod_{p|\Delta_L} \phi(p^{k_p}) = \phi(n)$. By construction of I, every prime that ramifies in $L(\zeta_n)/\mathbf{Q}$ is unramified in $L(\zeta_n)^I/\mathbf{Q}$. It follows that $L(\zeta_n)^I/\mathbf{Q}$ is unramified at all finite primes, and by Minkowski's theorem [I, 9.11], we have $L(\zeta_n)^I = \mathbf{Q}$ and $I = G$. The inequality $[L(\zeta_n) : \mathbf{Q}] = \#I \leq \phi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}]$ now shows that we have $L \subset \mathbf{Q}(\zeta_n)$, as claimed. □

▶ Kummer theory

In the proof of theorem 6.2, we will use a general result from Galois theory to describe all abelian extensions L of a field K that satisfy $\mathrm{Gal}(L/K)^n = 1$ for some fixed integer $n > 1$ (i.e. the abelian extensions of *exponent* dividing n) in the case that K contains a primitive n-th root of unity.

6.3. Theorem. *Let $n \geq 1$ be an integer and K a field containing a primitive n-th root of unity ζ_n. Then there is a bijection*

$$\begin{array}{rcl} \{K \subset L \subset K^{\mathrm{ab}} : \mathrm{Gal}(L/K)^n = 1\} & \leftrightarrows & \{K^{*n} \subset W \subset K^*\} \\ L & \mapsto & L^{*n} \cap K^* \\ K(\sqrt[n]{W}) & \leftarrow & W \end{array}$$

between abelian extensions L of K of exponent dividing n and subgroups $W \subset K^*$ containing K^{*n}. If L corresponds to W, there is a perfect pairing

$$\begin{aligned} \mathrm{Gal}(L/K) \times W/K^{*n} &\longrightarrow \langle \zeta_n \rangle \\ (\sigma, w) &\longmapsto (\sigma, w)_{n,K} = \frac{\sigma(\sqrt[n]{w})}{\sqrt[n]{w}} \end{aligned}$$

that identifies $\mathrm{Gal}(L/K)$ *with* $\mathrm{Hom}(W/K^{*n}, \langle \zeta_n \rangle)$.

The *Kummer pairing* in 6.3 is canonical in the sense that for every automorphism τ of the algebraic closure of K, we have

$$(\sigma, w)^{\tau}_{L/K} = (\tau\sigma\tau^{-1}, \tau(w))_{n,\tau[K]}. \tag{6.4}$$

There is an analog of 6.3 known as *Artin-Schreier theory* when n equals the characteristic of K, see exercise 1.

▶ Proof of the theorem

We will now prove the local Kronecker-Weber theorem 6.2. We will assume $p \neq \infty$, as the only non-trivial extension of $\mathbf{Q}_\infty = \mathbf{R}$ is $\mathbf{C} = \mathbf{R}(\zeta_n)$, where we can take for n any integer exceeding 2.

For brevity, we call an extension of $\mathbf{Q}_p$ *cyclotomic* if it is contained in an extension $\mathbf{Q}_p(\zeta)$ obtained by adjoining a root of unity ζ.

As every finite abelian group is a product of cyclic groups of prime power order, every abelian extension L/K is a compositum of cyclic extensions L_i/K of prime power order. It is therefore sufficient to prove the theorem for cyclic extensions $L/\mathbf{Q}_p$ of order q^n with q prime. We distinguish three cases, and start with the easiest case.

6.5. A. Tame case. *A cyclic extension $L/\mathbf{Q}_p$ of order q^n with $q \neq p$ prime is cyclotomic.*

The extension $L/\mathbf{Q}_p$ is tamely ramified as the ramification e is a power of $q \neq p$. By 5.3 and 5.4, the inertia group of $L/\mathbf{Q}_p$ injects into $\mathbf{F}_p^*$, so its order e divides $p-1$. Applying Abhyankar's lemma (exercise 4.3) to $L/\mathbf{Q}_p$ and the extension $\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p$ from 4.6, we see that $L(\zeta_p)/\mathbf{Q}_p(\zeta_p)$ is an unramified extension. By 4.4, we have $L(\zeta_p) \subset \mathbf{Q}_p(\zeta_p, \zeta)$ for some root of unity ζ, so $L \subset \mathbf{Q}_p(\zeta_p, \zeta)$ is cyclotomic. This settles the tame case.

6.6. B. Wild case for $p \neq 2$. *A cyclic extension of $\mathbf{Q}_p$ of order p^n is cyclotomic when p is odd.*

If p is odd, there are two independent cyclic cyclotomic extensions of degree p^n for each $n \geq 1$: the unramified extension of degree p^n and the totally ramified subfield of degree p^n of $\mathbf{Q}_p(\zeta_{p^{n+1}})$. Let E be the compositum of these two extensions. We have to show that every cyclic extension $L/\mathbf{Q}_p$ of degree p^n is contained in E. If LE were strictly larger than E, the Galois group $G = \mathrm{Gal}(LE/\mathbf{Q}_p)$ would be an abelian group that is annihilated by p^n and has order exceeding p^{2n}. Then G/G^p would be an elementary abelian p-group on more than 2 generators, so there would be at least 3 linearly independent cyclic extensions of degree p of $\mathbf{Q}_p$. After adjoining a p-th root of unity ζ_p to them, they would still be linearly independent over $K = \mathbf{Q}_p(\zeta_p)$ as $[K : \mathbf{Q}_p] = p-1$ is coprime to p. This contradicts the following lemma, which describes explicitly the maximal abelian extension L of $\mathbf{Q}_p$ that is of exponent p over $\mathbf{Q}_p(\zeta_p)$ and shows that $[L : \mathbf{Q}_p(\zeta_p)] = p^2$.

6.7. Lemma. *The maximal abelian extension of exponent p of $K = \mathbf{Q}_p(\zeta_p)$ that is abelian over $\mathbf{Q}_p$ equals $K(\sqrt[p]{W})$ for the subgroup $W \subset K^*$ satisfying*

$$W/K^{*p} = \langle \zeta_p \rangle \times \langle 1 + \pi^p \rangle.$$

Here π denotes the prime element $1 - \zeta_p \in K$. The extension $K \subset K(\sqrt[p]{\zeta_p}) = K(\zeta_{p^2})$ is totally ramified and the extension $K \subset K(\sqrt[p]{1+\pi^p})$ is unramified.

Proof. *** □

We are left with the final case of 6.2 to be proved.

6.8. C. Wild case for $p = 2$. *A cyclic 2-power extension of $\mathbf{Q}_2$ is cyclotomic.*

In this case the proof we just gave for odd p has to be modified as the totally ramified cyclotomic extension $\mathbf{Q}_2(\zeta_{2^k})$ for $k > 2$ is not cyclic but a product of two cyclic groups of order 2 and 2^{k-2}. It is possible to adapt lemma 6.5 to this case (exercise 6), but there is also the following ad hoc argument.

We want to show again that every cyclic extension L of $\mathbf{Q}_2$ of degree 2^n is contained in the compositum E of $\mathbf{Q}_2(\zeta_{2^{n+2}})$ and the unramified extension of degree 2^n. For $n = 1$ this is done by direct inspection: the maximal abelian extension of exponent 2 of $\mathbf{Q}_2$ is the cyclotomic field $\mathbf{Q}_2(\sqrt{-1}, \sqrt{5}, \sqrt{2}) = \mathbf{Q}_2(\zeta_{24})$. It has Galois group $(\mathbf{Z}/2\mathbf{Z})^3$. For $n > 1$ we have to show that the Galois group $G = \mathrm{Gal}(LE/\mathbf{Q}_2)$ cannot be greater than $\mathrm{Gal}(E/\mathbf{Q}) = \mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^n\mathbf{Z})^2$. We know already by the case $n = 1$ that $G/G^2 \cong (\mathbf{Z}/2\mathbf{Z})^3$, so G can be generated by 3 elements. In order to conclude that we have $G \cong \mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^n\mathbf{Z})^2$, it suffices to show that G/G^4 cannot be isomorphic to $(\mathbf{Z}/4\mathbf{Z})^3$. If this were the case, every quadratic extension of $\mathbf{Q}_2$ would be contained in some cyclic extension $M/\mathbf{Q}_2$ of degree 4. This contradicts the following lemma, which is a simple application of Galois theory (cf. exercise 3), and concludes the proof of theorem 6.2. □

6.9. Lemma. *There is no cyclic quartic extension $M/\mathbf{Q}_2$ with $\sqrt{-1} \in M$.*

Proof. If M contains $i = \sqrt{-1}$, then there exists $\alpha \in \mathbf{Q}_2(i)$ such that $M = \mathbf{Q}_2(i, \sqrt{\alpha})$. Let σ be a generator of $\mathrm{Gal}(M/\mathbf{Q}_2)$. Then σ^2 generates the Galois group $\mathrm{Gal}(M/\mathbf{Q}_2(i))$, so we have $\sigma^2(\sqrt{\alpha}) = -\sqrt{\alpha}$. The element $\beta = \sigma(\sqrt{\alpha})/\sqrt{\alpha}$ now satisfies

$$\sigma\beta = \frac{\sigma^2(\sqrt{\alpha})}{\sigma(\sqrt{\alpha})} = -\frac{1}{\beta} \qquad \text{and} \qquad \sigma^2(\beta) = \beta,$$

so β is in $\mathbf{Q}_2(i)$ and has norm $N_{\mathbf{Q}_2(i)/\mathbf{Q}_2}(\beta) = \beta\sigma(\beta) = -1$. However, it is easy to see that $-1 \in \mathbf{Q}_2$ cannot be a norm from $\mathbf{Q}_2(i)$. If this were the case, there would be an element $x + iy \in \mathbf{Z}_2[i]$ such that $x^2 + y^2 = -1$, and this cannot happen since squares in $\mathbf{Z}_2$ are congruent to 0 or 1 modulo $4\mathbf{Z}_2$. □

If $L/\mathbf{Q}$ is abelian, the smallest integer n for which L is contained in the n-th cyclotomic field $\mathbf{Q}(\zeta_n)$ is known as the *conductor* of L.

The Kronecker-Weber theorem gives us a very explicit description of the maximal abelian extension $\mathbf{Q}^{\mathrm{ab}}$ of $\mathbf{Q}$. It is the field $\mathbf{Q}(\zeta_\infty)$ obtained by adjoining all roots of unity in an algebraic closure of $\mathbf{Q}$ to $\mathbf{Q}$. Its Galois group over $\mathbf{Q}$ is the profinite group

$$\mathrm{Gal}(\mathbf{Q}(\zeta_\infty)/\mathbf{Q}) = \lim_{\leftarrow n} \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) = \lim_{\leftarrow n} (\mathbf{Z}/n\mathbf{Z})^* = \widehat{\mathbf{Z}}^*$$

of units in the ring of profinite integers $\widehat{\mathbf{Z}}$.

Problems

1. *(Artin-Schreier theory.)* Let K be a field of chracteristic $p > 0$ with maximal abelian extension K^{ab}, and define the map $\wp : K^{\mathrm{ab}} \to K^{\mathrm{ab}}$ by $\wp(x) = x^p - x$. Prove the following theorem.

   Theorem. There is a bijection

   $$\{K \subset L \subset K^{\mathrm{ab}} : \mathrm{Gal}(L/K)^p = 1\} \quad \leftrightarrows \quad \{\wp[K] \subset W \subset K\}$$

   between abelian extensions L of K of exponent dividing p and subgroups $W \subset K$ containing $\wp[K]$ that sends an extension L to the subgroup $\wp[L] \cap K$ and a subgroup $W \subset K$ to the extension $L = K(\wp^{-1}W)$. If L corresponds to W, there is an isomorphism

   $$\mathrm{Gal}(L/K) \xrightarrow{\sim} (W/\wp[K])^\wedge = \mathrm{Hom}(W/\wp[K], \mathbf{F}_p)$$

   under which $\sigma \in \mathrm{Gal}(L/K)$ corresponds to the homomorphism $w \mapsto \sigma(\wp^{-1}(w)) - \wp^{-1}(w)$. In particular, one has an equality $[L : K] = [W : \wp[K]]$ in this case.

2. Show that an abelian extension $K/\mathbf{Q}$ is ramified at p if and only if p divides the conductor, and that it is wildly ramified at p if and only if p^2 divides the conductor.

3. Let K be a field of characteristic different from 2 and L/K a quadratic extension. Show that there exists an extension M/L such that M/K is cyclic of degree 4 if and only if $-1 \in N_{L/K}[L^*]$.

4. Show that the conductor of an abelian number field K divides the discriminant Δ_K, and that it is equal to $|\Delta_K|$ when K is quadratic.

5. Let $K \neq \mathbf{Q}$ be an abelian extension of $\mathbf{Q}$. Show that there are abelian extensions L/K that are not cyclotomic. Do you need the assumption that $K/\mathbf{Q}$ is abelian?

6. Show that for $K = \mathbf{Q}_2(\zeta_4)$, the subgroup $W \subset K^*$ consisting of elements $\alpha \in K^*$ for which the extension $K(\sqrt[4]{\alpha})$ is abelian over $\mathbf{Q}_2$ is equal to

   $$W/K^{*4} = \langle \zeta_4 \rangle \times \langle 1 + 4\zeta_4 \rangle,$$

   and that the extension $K \subset K(\sqrt[4]{\zeta_4}) = K(\zeta_{16})$ is totally ramified and the extension $K \subset K(\sqrt[4]{1 + 4\zeta_4})$ is unramified. How does case C of theorem 6.2 follow from this?
   [Hint: show that $\alpha \in W$ if and only if $N_{K/\mathbf{Q}_2}(\alpha) \in K^{*4} \cap \mathbf{Q}_2^* = \langle -4 \rangle \times (1 + 16\mathbf{Z}_2)$.]

7. *(Genus fields.)* ****

7 Local and global fields

We have already seen that it is possible to derive information on global fields from their completions at the various primes of the field. In this section, we will restrict to the case of number fields, even though most results hold for function fields as well. We show first that discriminants and differents of number fields can be conveniently computed from the discriminants and differents of the local extensions. Given our 'local definition' of the discriminant $\Delta(L/K)$ in [I, §7], this is of course not surprising. This definition used the fact that rings and modules are often easier to describe after localization at a prime. After passing to the completion of these localizations, we can use in addition the structure theorems for local fields of the previous sections. The reason why this is often possible lies in theorem 3.8, which tells us that for L/K a finite extension of number fields and $\mathfrak{p}$ a prime of K, we have an isomorphism

$$K_{\mathfrak{p}} \otimes_K L \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}. \tag{7.1}$$

In this section, we write $\mathcal{O}_{\mathfrak{p}}$ for the valuation ring of the $\mathfrak{p}$-adic valuation on a number field K, and $A_{\mathfrak{p}}$ for the valuation ring of the completion $K_{\mathfrak{p}}$. We have already seen that $\mathcal{O}_{\mathfrak{p}}$ is the localization of the ring of integers $\mathcal{O}$ of K at the prime $\mathfrak{p}$, and that $A_{\mathfrak{p}} = \lim_{\leftarrow n} \mathcal{O}/\mathfrak{p}^n$ is the completion of $\mathcal{O}_{\mathfrak{p}}$ in the valuation topology.

7.2. Theorem. *Let L/K be an extension of number fields with different $\mathfrak{D}(L/K) \subset \mathcal{O}_L$ and discriminant $\Delta(L/K) \subset \mathcal{O}_K$. Then we have*

$$\mathfrak{D}(L/K) \cdot A_{\mathfrak{q}} = \mathfrak{D}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$$

for every finite prime $\mathfrak{q}$ of L and

$$\Delta(L/K) \cdot A_{\mathfrak{p}} = \textstyle\prod_{\mathfrak{q}|\mathfrak{p}} \Delta(L_{\mathfrak{q}}/K_{\mathfrak{p}})$$

for every finite prime $\mathfrak{p}$ of K.

Proof. For every finite prime $\mathfrak{p}$ of K, the ring of integers $\mathcal{O}_L$ is a dense subring of $A = \prod_{\mathfrak{q}|\mathfrak{p}} A_{\mathfrak{q}} \subset \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}} = K_{\mathfrak{p}} \otimes L$ and the trace $\mathrm{Tr}_{L/K} : K_{\mathfrak{p}} \otimes L \to K_{\mathfrak{p}}$ is a continuous function. Using 3.11, we deduce that we have an implication

$$\mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K \Rightarrow \mathrm{Tr}_{L/K}(xA) = \textstyle\sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{Tr}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(xA_{\mathfrak{q}}) \subset A_{\mathfrak{p}}$$

for $x \in L$. This immediately implies an inclusion $\mathfrak{D}(L/K)^{-1} \subset \mathfrak{D}(L_{\mathfrak{q}}/K_{\mathfrak{p}})^{-1}$ for every extension $\mathfrak{q}|\mathfrak{p}$.

Conversely, for fixed $\mathfrak{q}|\mathfrak{p}$ and $x \in \mathfrak{D}(L_{\mathfrak{q}}/K_{\mathfrak{p}})^{-1}$ we can choose an element $y \in L$ such that y is close to x in $L_{\mathfrak{q}}$ and close to 0 in the other completions $L_{\mathfrak{q}'} \supset K_{\mathfrak{p}}$. Then we have again $\mathrm{Tr}_{L/K}(y\mathcal{O}_L) \subset \mathrm{Tr}_{L/K}(yA) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{Tr}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(yA_{\mathfrak{q}}) \subset A_{\mathfrak{p}}$ since the term for our selected extension $\mathfrak{q}$ is in $A_{\mathfrak{p}}$ as it is close to $\mathrm{Tr}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(xA_{\mathfrak{q}}) \subset A_{\mathfrak{p}}$ and the terms with $\mathfrak{q}' \neq \mathfrak{q}$

give a small contribution. It follows that y is contained in the inverse of the localized different $\mathfrak{D}(\mathcal{O}_{L,\mathfrak{q}}/\mathcal{O}_{\mathfrak{p}})^{-1} = \mathfrak{D}(L/K)^{-1}\mathcal{O}_{L,\mathfrak{q}}$, and this yields $xA_{\mathfrak{q}} = yA_{\mathfrak{q}} \subset \mathfrak{D}(L/K)^{-1}A_{\mathfrak{q}}$. This proves the other inclusion.

The identity for the discriminant follows by taking norms and using the product relation between local and global norms from 3.11. However, one can also give a direct proof in the following way. Let $\omega_1, \omega_2, \ldots, \omega_n$ be an $\mathcal{O}_{\mathfrak{p}}$-basis for the localization $\mathcal{O}_{L,\mathfrak{p}}$ of the ring of integers $\mathcal{O}_L$ at the prime $\mathfrak{p}$ of K. As this basis generates $A_{\mathfrak{q}}$ over $A_{\mathfrak{p}}$ in each completion $L_{\mathfrak{q}}$, we obtain an isomorphism of $A_{\mathfrak{p}}$-submodules

$$\textstyle\sum_{i=1}^{n} A_{\mathfrak{p}} \otimes \omega_i \xrightarrow{\sim} A = \prod_{\mathfrak{q}|\mathfrak{p}} A_{\mathfrak{q}}$$

induced by 7.1. The left hand side has discriminant $\Delta(L/K) \cdot A_{\mathfrak{p}}$ by definition of the global discriminant, the right hand side has discriminant $\prod_{\mathfrak{q}|\mathfrak{p}} \Delta(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ (cf. [I, 8.1]). □

By applying theorem 4.8 on local differents we obtain the following result.

7.3. Corollary. *Let L/K be an extension of number fields and $\mathfrak{q}$ a finite prime of L with restriction $\mathfrak{p}$ to K. Then we have*

$$\operatorname{ord}_{\mathfrak{q}}(\mathfrak{D}(L/K)) \geq e(\mathfrak{q}/\mathfrak{p}) - 1,$$

and equality holds if and only if $\mathfrak{q}$ is tamely ramified in L/K. □

The relations between a number field K and its various completions $K_{\mathfrak{p}}$ are sometimes referred to as *local-global* relations. In order for a statement to be true for K, it is often necessary for the statement to be true for the completions $K_{\mathfrak{p}}$ of K at all primes, both finite and infinite. For instance, a Diophantine equation of the form $f(x_1, x_2, \ldots, x_n) = 0$ with $f \in K[X_1, X_2, \ldots, X_n]$ can only have a solution in K^n if it has solutions in $K_{\mathfrak{p}}^n$ for all primes $\mathfrak{p}$ of K. It is not in general an easy matter to decide whether the converse is true. If it is, one says that the *Hasse principle* holds for f over K. We will encounter a classical example of this phenomenon in 11.12.

A convenient way to relate a number field K to its completions is given by the adèle ring $\mathbb{A}_K$ of K that was introduced by Chevalley around 1940. This ring is a large extension ring of K that is constructed from the completions $K_{\mathfrak{p}}$ of K at *all* prime divisors of K, both finite and infinite. We know that the finite primes of K correspond to the non-zero primes of the ring of integers $\mathcal{O}_K$, whereas the infinite primes come from embeddings of K into the complex numbers. We write $\mathfrak{p}$ to denote a prime of either kind, and take $A_{\mathfrak{p}} = K_{\mathfrak{p}}$ if $\mathfrak{p}$ is infinite. The *adèle ring* $\mathbb{A}_K$ of K is defined as

$$\mathbb{A}_K = \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}} = \{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}} : x_{\mathfrak{p}} \in A_{\mathfrak{p}} \text{ for almost all } \mathfrak{p}\}.$$

Informally, one can say that it is the subring of the full cartesian product of all completions consisting of vectors that are almost everywhere integral. It is an example of a 'restricted

direct product'. The topology on such a product is not the relative topology, but the topology generated by the open sets of the form

$$\prod_{\mathfrak{p}\in S} O_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} A_{\mathfrak{p}}$$

for some finite set of primes S and $O_{\mathfrak{p}}$ open in $K_{\mathfrak{p}}$. This topology makes $\mathbb{A}_K$ into a locally compact ring since all completions $K_{\mathfrak{p}}$ are locally compact and the rings $A_{\mathfrak{p}}$ are compact for all finite $\mathfrak{p}$. We have a canonical embedding $K \rightarrowtail \mathbb{A}_K$ along the diagonal since the vector $(x)_{\mathfrak{p}}$ for $x \in K$ is almost everywhere integral. We usually view this embedding as an inclusion and refer to the elements of K in $\mathbb{A}_K$ as *principal adèles*.

For $K = \mathbf{Q}$ we find

$$\mathbb{A}_{\mathbf{Q}} = \mathbf{R} \times \prod_p{}' \mathbf{Q}_p = \{(x_\infty, (x_p)_p) : x_p \in \mathbf{Z}_p \text{ for almost all } p\}.$$

The open subset $U = (-1/2, 1/2) \times \prod_p \mathbf{Z}_p$ of $\mathbb{A}_{\mathbf{Q}}$ satisfies $U \cap \mathbf{Q} = \{0\}$, since a rational number that is p-integral at all primes p is in $\mathbf{Z}$ and $\mathbf{Z} \cap (-1/2, 1/2) = \{0\}$. It follows that $\mathbf{Q}$ is a discrete subring of $\mathbb{A}_{\mathbf{Q}}$. Moreover, the closure $W = [-1/2, 1/2] \times \prod_p \mathbf{Z}_p$ of U is compact in $\mathbb{A}_{\mathbf{Q}}$ and it is not difficult to show (exercise 7) that $\mathbf{Q} + W = \mathbb{A}_{\mathbf{Q}}$, so that the natural map $W \to \mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ is continuous surjection. It follows that its image $\mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ is a *compact* additive group. Generalizing this proof or using the following theorem, one can prove analogous statements for arbitrary number fields K (exercise 9).

If L/K is a finite extension of number fields, we have a canonical embedding $\mathbb{A}_K \rightarrowtail \mathbb{A}_L$ that sends $(x_{\mathfrak{p}})_{\mathfrak{p}}$ to the element $(y_{\mathfrak{q}})_{\mathfrak{q}}$ that has $y_{\mathfrak{q}} = x_{\mathfrak{p}}$ when $\mathfrak{q}|\mathfrak{p}$.

7.4. Theorem. *There is an isomorphism of topological rings*

$$\mathbb{A}_K \otimes L \xrightarrow{\sim} \mathbb{A}_L$$

such that the induced maps $\mathbb{A}_K = \mathbb{A}_K \otimes 1 \rightarrowtail \mathbb{A}_L$ and $L = 1 \otimes L \rightarrowtail \mathbb{A}_L$ are the canonical embeddings.

Proof. Taking the product over all $\mathfrak{p}$ of the isomorphisms $K_{\mathfrak{p}} \otimes_K L \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$, we see that there is an isomorphism for the full cartesian product of all completions. In order to show that this isomorphism induces the required isomorphism for the adèle rings, we have to show that given a basis $\omega_1, \omega_2, \ldots, \omega_n$ of L/K, there is an induced isomorphism $\sum_{i=1}^n A_{\mathfrak{p}} \otimes \omega_i \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} A_{\mathfrak{q}}$ for almost all primes $\mathfrak{p}$ of L. This is clear: for almost all primes $\mathfrak{p}$ it is true that all ω_i are $\mathfrak{p}$-integral and that the discriminant $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ is in $A_{\mathfrak{p}}^*$, and for such $\mathfrak{p}$ our basis is an integral basis of the integral closure of $\mathcal{O}_{K,\mathfrak{p}}$ in L over $\mathcal{O}_{K,\mathfrak{p}}$. The other statements follow from the corresponding statements for $K_\phi = K_\phi \otimes 1$ and $L = 1 \otimes L$ in 7.1. □

7.5. Corollary. *The ring $\mathbb{A}_L$ is a free algebra of rank $[L:K]$ over $\mathbb{A}_K$, and the norm map $N_{L/K}:\mathbb{A}_L\to\mathbb{A}_K$ induces the field norm $N_{L/K}:L\to K$ on the subring $L\subset\mathbb{A}_L$.* □

The adèle ring of K is a locally compact additive group, so it comes with a translation invariant measure μ known as the *Haar measure* on $\mathbb{A}_K$. The measure μ is uniquely determined up to a multiplicative constant. and can be obtained as a product measure of the Haar measures $\mu_{\mathfrak{p}}$ on the completions $K_{\mathfrak{p}}$.

For infinite primes $\mathfrak{p}$ the completion $K_{\mathfrak{p}}$ is isomorphic to $\mathbf{R}$ or $\mathbf{C}$, and $\mu_{\mathfrak{p}}$ is the well known Lebesgue measure. For finite primes $\mathfrak{p}$ we can take for $\mu_{\mathfrak{p}}$ the unique translation invariant measure that satisfies

$$\mu_{\mathfrak{p}}(A_{\mathfrak{p}})=1 \qquad \text{and} \qquad \mu_{\mathfrak{p}}(\mathfrak{p}^n)=(N\mathfrak{p})^{-n} \quad \text{for} \quad n\in\mathbf{Z}.$$

Here $N\mathfrak{p}=N_{K/\mathbf{Q}}(\mathfrak{p})\in\mathbf{Z}_{>0}$ is the absolute norm of the prime $\mathfrak{p}$. We define the *normalized $\mathfrak{p}$-adic valuation* $|x|_{\mathfrak{p}}$ of an element $x\in K_{\mathfrak{p}}$ as the effect of the multiplication map $M_x: K_{\mathfrak{p}}\to K_{\mathfrak{p}}$ on the Haar measure $\mu_{\mathfrak{p}}$, i.e.

$$\mu_{\mathfrak{p}}(xV)=|x|_{\mathfrak{p}}\mu_{\mathfrak{p}}(V)$$

for every measurable subset $V\subset K_{\mathfrak{p}}$. If $\mathfrak{p}$ is finite, $|\cdot|_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation for which a prime element at $\mathfrak{p}$ has valuation $N(\mathfrak{p})^{-1}=(\#A_{\mathfrak{p}}/\mathfrak{p})^{-1}$. For a real prime $\mathfrak{p}$, the normalized absolute value is the ordinary absolute value on $K_{\mathfrak{p}}=\mathbf{R}$. However, for complex $\mathfrak{p}$ the normalized absolute value is the *square* of the ordinary absolute value.

7.6. Product formula. *For every non-zero element $x\in K^*$, we have*

$$\prod_{\mathfrak{p}}|x|_{\mathfrak{p}}=1.$$

Proof. With this normalization, we have $\prod_{\mathfrak{p}\text{ finite}}|x|_{\mathfrak{p}}=(\#(\mathcal{O}/x\mathcal{O}))^{-1}$ for every non-zero $x\in\mathcal{O}$ by the Chinese remainder theorem and the identity $|x|_{\mathfrak{p}}=(\#(\mathcal{O}_{\mathfrak{p}}/x\mathcal{O}_{\mathfrak{p}}))^{-1}$ for each finite prime $\mathfrak{p}$. On the other hand, the normalization for infinite primes yields $\prod_{\mathfrak{p}\text{ infinite}}|x|_{\mathfrak{p}}=\prod_{\sigma:K\to\mathbf{C}}|\sigma(x)|=|N_{K/\mathbf{Q}}(x)|=\#(\mathcal{O}/x\mathcal{O})$. The proves the theorem for integral non-zero x, the general result follows by multiplicativity. □

The unit group of the adèle ring $\mathbb{A}_K$ is the group

$$J_K=\prod_{\mathfrak{p}}{}'K_{\mathfrak{p}}^*=\{(x_{\mathfrak{p}})_{\mathfrak{p}}\in\prod_{\mathfrak{p}}K_{\mathfrak{p}}^* : x_{\mathfrak{p}}\in A_{\mathfrak{p}}^* \text{ for almost all } \mathfrak{p}\}$$

that is known as the *idèle group* of K. For the topology on this group we do not take the relative topology coming from the adèle ring, but the topology generated by open sets of the form

$$\prod_{\mathfrak{p}\in S}O_{\mathfrak{p}}\times\prod_{\mathfrak{p}\notin S}A_{\mathfrak{p}}^*$$

for S a finite set of primes and $O_{\mathfrak{p}}$ open in $K_{\mathfrak{p}}^*$. This topology is finer than the relative topology J inherits from $\mathbb{A}_K$, and it makes J_K into a locally compact group. Under the diagonal embedding, the unit group K^* of K becomes a subgroup of J_K consisting of the *principal idèles*. The product formula 7.6 implies that K^* is a discrete subgroup of J_K, so the factorgroup $C_K = J_K/K^*$ is again a locally compact group, the *idèle class group* of K. This is not a compact group, since the volume map

$$\begin{aligned} \tau : \quad J &\longrightarrow \mathbf{R}_{>0} \\ (x_{\mathfrak{p}})_{\mathfrak{p}} &\longrightarrow \prod_{\mathfrak{p}} |x_{\mathfrak{p}}|_{\mathfrak{p}} \end{aligned}$$

is a continuous surjective map that factors via C_K by the product formula. One can however show that the subgroup $C_K^1 = (\ker \tau)/K^*$ of C_K is a compact group—a fact that is closely related to the Dirichlet unit theorem and the finiteness of the class number, see exercises 16–18. The idèle class group will play a key role in the formulation of class field theory in section 9.

Problems

1. Let L/K be a normal extension of number fields of degree n and $\mathfrak{p}$ a finite prime of K with ramification index e in L/K. Show that $\mathrm{ord}_{\mathfrak{p}}(\Delta(L/K)) \geq (1 - e^{-1})n$, with equality if and only if $\mathfrak{p}$ is tamely ramified in L/K.

2. Let K be a number field of degree n with squarefree discriminant. Show that the normal closure M of K has group S_n over $\mathbf{Q}$.
[Hint: All inertia groups in $\mathrm{Gal}(M/\mathbf{Q})$ have order two, so $\mathrm{Gal}(M/\mathbf{Q})$ is a transitive subgroup of S_n that is generated by transpositions.]

3. It can be shown [Selmer, Math. Scand. **4**, 287–302, (1956)] that the polynomial $f_n = X^n - X - 1$ is irreducible over $\mathbf{Q}$ for all $n > 1$. Assuming this, prove that the splitting field of f_n has Galois group S_n over $\mathbf{Q}$.

4. Let D be a squarefree integer for which there exists a number field of degree n and discriminant D. Show that $\mathbf{Q}(\sqrt{D})$ has a normal extension N that is unramified at all finite primes and has Galois group $\mathrm{Gal}(N/\mathbf{Q}(\sqrt{D})) \cong A_n$, the alternating group on n elements.

5. Let K be a number field of contained in a normal extension N of $\mathbf{Q}$. Show that there exists an extension $E/\mathbf{Q}$ of such that $E \cap N = \mathbf{Q}$ and EL/E is unramified at all primes. Deduce that for every finite group G, there are infinitely many pairwise linearly disjoint number fields that have a Galois extension with group G that is unramified at all primes.
[Hint: write $K = \mathbf{Q}(\alpha)$ with $f = f_{\mathbf{Q}}^{\alpha} \in \mathbf{Z}[X]$ and choose a polynomial $g \in \mathbf{Z}[X]$ that is p-adically close to f at all p dividing Δ_K and Eisenstein at a prime $p \nmid \Delta_N$. Set $E = \mathbf{Q}[X]/(g)$.]

6. Let $\mathcal{O}$ be the ring of integers of a number field K, and define the profinite completion $\widehat{\mathcal{O}}$ of $\mathcal{O}$ as $\widehat{\mathcal{O}} = \lim_{\leftarrow n \geq 1} \mathcal{O}/n\mathcal{O}$. Show that $\widehat{\mathcal{O}}$ is isomorphic (as a topological ring) to the direct product $\prod_{\mathfrak{p}<\infty} A_{\mathfrak{p}}$ of all valuation rings of the finite completions $K_{\mathfrak{p}}$ of K.

7. Show that every element in $\mathbb{A}_{\mathbf{Q}}$ can uniquely be written as a sum of a rational number and an element in $[-1/2, 1/2) \times \prod_p \mathbf{Z}_p$. Deduce that there is an exact sequence

$$0 \longrightarrow \widehat{\mathbf{Z}} \longrightarrow \mathbb{A}_{\mathbf{Q}}/\mathbf{Q} \longrightarrow \mathbf{R}/\mathbf{Z} \longrightarrow 0$$

of topological groups and that $\mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ is a compact group of Haar measure 1 under the quotient Haar measure it inherits from $\mathbb{A}_{\mathbf{Q}}$. Show also that $\mathbb{A}_{\mathbf{Q}}/\mathbf{Q}$ is connected, and that it can be given a $\mathbf{Q}$-vector space structure.

An exact sequence $0 \to A \to B \to C \to 0$ of topological abelian groups with continuous group homomorphisms is said to *split* if there is an isomorphism $f\colon B \to A \times C$ of topological groups such that (i) the map $A \to B \to A \times C$ is the canonical inclusion $A \to A \times C$; and (ii) the map $B \to A \times C \to C$ is the given map $B \to C$.

8. Show that the sequence $0 \to \widehat{\mathbf{Z}} \to \mathbb{A}_{\mathbf{Q}}/\mathbf{Q} \to \mathbf{R}/\mathbf{Z} \longrightarrow 0$ does not split, even if in the definition given above the map f is only required to be an isomorphism of topological *spaces* satisfying (i) and (ii). Show also that the sequence does not split if in the definition given above the map f is only required to be a *group* isomorphism satisfying (i) and (ii).

9. Let K be a number field. Show that K is a discrete subring of $\mathbb{A}_K$, and that the quotient ring $\mathbb{A}_K/K$ is compact. Show that under the quotient measure coming from $\mathbb{A}_K$, one has $\mu(\mathbb{A}_K/K) = 2^{-s}|\Delta_K|^{1/2}$. Here s is the number of complex primes of K.

10. *(Strong approximation theorem)* Let K be a number field and $\mathfrak{p}_0$ a prime of K. Show that K is dense in $\prod_{\mathfrak{p} \neq \mathfrak{p}_0} K_{\mathfrak{p}}$ under the diagonal embedding.
[Hint: use the previous exercise to show that every subset of the form $\prod_{\mathfrak{p} \in S} O_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} A_{\mathfrak{p}} \subset \mathbb{A}_K$ with $\mathcal{O}_{\mathfrak{p}}$ an open neighborhood of $0 \in K_{\mathfrak{p}}$ and S a finite set of primes containing the infinite primes contains a non-zero element of K when $\prod_{\mathfrak{p} \in S} \mu_{\mathfrak{p}}(O_{\mathfrak{p}})$ is sufficiently large.]

11. Show that inversion is not a continuous operation on the idèle group J_K with respect to the relative topology of the adèle ring $\mathbb{A}_K \supset J_K$. Show also that the topology on J_K is the relative topology coming from the embedding $J_K \rightarrowtail \mathbb{A}_K \times \mathbb{A}_K$ that maps $x \in J_K$ to (x, x^{-1}).

12. Show that the topology on the adèle ring of K is induced by the metric d defined by

$$d((x_{\mathfrak{p}})_{\mathfrak{p}}, (y_{\mathfrak{p}})_{\mathfrak{p}}) = \sum_{\mathfrak{p}} 2^{-N(\mathfrak{p})} |x_{\mathfrak{p}} - y_{\mathfrak{p}}|_{\mathfrak{p}}.$$

Here $N(\mathfrak{p}) \in \mathbf{Z}_{>0}$ is the absolute norm of $\mathfrak{p}$ if $\mathfrak{p}$ is finite, and $N(\mathfrak{p}) = 1$ if $\mathfrak{p}$ is infinite. Can you find a metric that induces the topology on J_K?

13. Show that the norm on the idèle groups is compatible with the ideal norm in the sense that if we define the map $\phi_K : J_K \to I_K$ to the group of fractional $\mathcal{O}_K$-ideals I_K by $\phi : (x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}\ \text{finite}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})}$ and set $U_K = \prod A_{\mathfrak{p}}^* \subset J_K$ for every number field K, then there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & J_L & \longrightarrow & I_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & J_K & \longrightarrow & I_K & \longrightarrow & 0 \end{array}$$

for every finite extension of number fields L/K.

14. Show that there is a natural map $\widehat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^* \to C_{\mathbf{Q}}^1$ that is an isomorphism of topological groups. Conclude that $C_{\mathbf{Q}}^1$ is compact.

15. Show that the exact sequence $0 \to C_K^1 \to C_K \xrightarrow{\tau} \mathbf{R}_{>0} \to 0$ is split, and that every open subgroup of the idèle class group C_K of K has finite index in C_K.

16. Let $U_K \subset J_K$ be as in exercise 13 and write U_K^1 for $U_K \cap J_K^1$. Show that $U_K^1/\mathcal{O}_K^*$ is compact and that there is an exact sequence of topological groups

$$0 \longrightarrow U_K^1/\mathcal{O}_K^* \longrightarrow C_K^1 \longrightarrow Cl_K \longrightarrow 0.$$

Deduce that C_K^1 is a compact group for every number field K.
[Hint: let S be the set of infinite primes of K and define $L : U_K \to \mathbf{R}^S$ by $L : (x_\mathfrak{p})_\mathfrak{p} \mapsto (\log|x_\mathfrak{p}|)_{\mathfrak{p}\in S}$. Then $\ker L$ is compact and the Dirichlet unit theorem asserts that $L[\mathcal{O}^*]$ is a lattice of maximal rank in the hyperplane $H = L[U_K^1]$.]

17. Show that the map $\phi_K : J_K \to I_K$ in 7.11 is continuous when I_K is given the discrete topology, and that it induces a continuous surjection $C_K^1 \to Cl_K$. Deduce that Cl_K is finite if C_K^1 is compact.

18. *(S-unit theorem.)* Let S be a finite set of primes of a number field K including the infinite primes. The group K_S of *S-units* of K consists of the elements $x \in K^*$ that satisfy $|x|_\mathfrak{p} = 1$ for all $\mathfrak{p} \notin S$. Use the compactness of C_K^1 to show that there is an isomorphism

$$K_S \cong Z_K \times \mathbf{Z}^{\#S-1},$$

where Z_K is the subgroup of roots of unity in K^*.
[Hint: Set $J_S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} A_\mathfrak{p}^*$ and define $J_S \to \mathbf{R}^S$ by $(x_\mathfrak{p})_\mathfrak{p} \mapsto (\log|x_\mathfrak{p}|_\mathfrak{p})_{\mathfrak{p}\in S}$. Then $J_S^1 = J^1 \cap J_S$ is mapped to a hyperplane $H \subset \mathbf{R}^S$ and $K_S = K \cap J_S$ is cocompact in H if $J_S^1/K_S \subset C_K^1$ is compact.]

19. Let L/K be a Galois extension of number fields with group G. Show that G acts naturally on the adèle ring $\mathbb{A}_L$, and that there is an isomorphism

$$\mathbb{A}_K \xrightarrow{\sim} \mathbb{A}_L^G = \{x \in \mathbb{A}_L : \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Prove that the $N_{L/K}(x) = \prod_{\sigma\in G} \sigma(x)$.

20. Let k be a finite field, and let $K = k(t)$, where t is transcendental over k. We write $\mathcal{O} = k[t]$, and we let $\hat{\mathcal{O}}$ be the projective limit of the rings $\mathcal{O}/f\mathcal{O}$, with f ranging over $\mathcal{O} - \{0\}$. Let V_K and $J_K = V_K^*$ be the adele ring and the idele group of K. We denote by $k[[u]]$ the ring of power series in one variable u over k.
    a. Prove: $V_K/K \cong uk[[u]] \times \hat{\mathcal{O}}$ as topological groups.
    b. Prove: $J_K/K^* \cong \mathbf{Z} \times (1 + uk[[u]]) \times \hat{\mathcal{O}}^*$ as topological groups; here $1 + uk[[u]]$ denotes the kernel of the map $k[[u]]^* \to k^*$ that maps a power series to its constant term.

8 Class field theory: ideal groups

The Kronecker-Weber theorem shows that the splitting behavior of primes p in an abelian extension L of $\mathbf{Q}$ is very simple: it only depends on the residue class of p modulo the conductor n of L. This observation has a long history going back to Fermat and Euler.

▶ Classical examples

A prime number p is a sum $p = x^2 + y^2 = (x + iy)(x - iy)$ of two squares if and only if it does not remain prime in the ring of Gaussian integers $\mathbf{Z}[i]$. This is the ring of integers of the cyclotomic field $\mathbf{Q}(\zeta_4)$, and Fermat already knew p is a sum of 2 squares if and only if it is not congruent to 3 mod 4.

Euler studied similar problems, such as the determination of the rational primes that occur in the factorization of numbers of the form $x^2 - ay^2$ with $a \in \mathbf{Z}$ fixed and $x, y \in \mathbf{Z}$ ranging over pairs of coprime integers. This comes down to the determination of the primes for which the Legendre symbol $\left(\frac{a}{p}\right)$ has a given value, and the numerical observation of Euler was that this value only depends on $p \bmod 4|a|$. This statement is essentially equivalent to the quadratic reciprocity law. In modern terminology, we would say that the abelian extension $\mathbf{Q}(\sqrt{a})$ of $\mathbf{Q}$ is contained in the cyclotomic field $\mathbf{Q}(\zeta_{4|a|})$, so the splitting behavior of a prime p in $\mathbf{Q}(\sqrt{a})$ (i.e. the value of the Legendre symbol $\left(\frac{a}{p}\right)$) is determined by the splitting behavior of p in $\mathbf{Q}(\zeta_{4|a|})$, i.e. by the residue class of $p \bmod 4|a|$.

The question whether a prime p is *represented* by the quadratic form $X^2 - aY^2$, i.e., $p = x^2 - ay^2$ for certain $x, y \in \mathbf{Z}$, is already more complicated, since this requires that there is a *principal* prime ideal in $\mathbf{Z}[\sqrt{a}]$ of norm p. In Fermat's example $a = -1$, the resulting ring $\mathbf{Z}[i]$ is a principal ideal domain, but as soon as this is no longer the case, the situation is much more difficult. When we take $a = -5$, we are dealing with the ring $\mathbf{Z}[\sqrt{-5}]$ that has a class group of order 2, and the rational primes that are the norm of a principal ideal $x + y\sqrt{-5}$ are exactly the primes that split completely in the quadratic extension $\mathbf{Q}(\sqrt{-5}, i)$ of $\mathbf{Q}(\sqrt{-5})$. As this extension field is contained in the cyclotomic extension $\mathbf{Q}(\zeta_{20})$, the solvability of $p = x^2 + 5y^2$ is equivalent to p being equal to 5 or congruent to 1 or 9 modulo 20, a result conjectured by Euler in 1744.

For other values of a, the situation is even more complicated. For instance, for $a = -27$ Euler conjectured around 1750 that p is of the form $p = x^2 + 27y^2$ if and only if $p \equiv 1 \bmod 3$ and 2 is a cube modulo p. This is a special case of a more general question suggested by the quadratic reciprocity law: do there exist reciprocity laws for powers higher than 2? In order for this question to be interesting for general $n > 2$, one restricts to primes $p \equiv 1 \bmod n$, for which the n-th powers in $\mathbf{F}_p^* = (\mathbf{Z}/p\mathbf{Z})^*$ have index n in the full group, and asks which conditions on the prime p ensure that some fixed integer a is an n-th power modulo p. This means that we are looking for a characterization of the rational primes $p \equiv 1 \bmod n$ that split completely in the field $\mathbf{Q}(\sqrt[n]{a})$ or, equivalently, the rational primes p that split completely in the normal extension $M = \mathbf{Q}(\zeta_n, \sqrt[n]{a})$. For $n > 2$, this is not an abelian extension of $\mathbf{Q}$ for most a, and we will see that this implies that the splitting behavior of a rational prime p in $M/\mathbf{Q}$ is *not* determined by a congruence condition on p. In fact,

finding a 'reciprocity law' governing the splitting of primes in non-abelian extensions is a problem that is still very much open today.

Going back to Euler's conjecture for the special case where $n = 3$ and $a = 2$, we see that the rational primes p that split completely in $\mathbf{Q}(\zeta_3, \sqrt[3]{2})$ should be the primes of the form $p = x^2 + 27y^2$. This is not a congruence condition on p, but it states that a prime $\mathfrak{p}$ in $K = \mathbf{Q}(\zeta_3)$ of prime norm $p \neq 3$ splits completely in the abelian extension $K(\sqrt[3]{2})/K$ if and only if it is generated by an element $\pi = x + 3y\sqrt{-3} = (x + 3y) + 6y\zeta_3$. As x and y do not have the same parity, this means that the prime $\mathfrak{p}|p$ can be generated by an element $\pi \in \mathcal{O}_K = \mathbf{Z}[\zeta_3]$ that is congruent to 1 mod $6\mathcal{O}_K$. Generators are determined up to multiplication by elements in $\mathcal{O}_K^* = \langle\zeta_6\rangle$, so we see that proving Euler's conjecture on the cubic character of 2 comes down to showing that a prime $\mathfrak{p}$ of K splits completely in $K(\sqrt[3]{2})/K$ if and only if $\mathfrak{p}$ is a principal ideal whose generator is trivial in $(\mathcal{O}_K/6\mathcal{O}_K)^*/\langle\zeta_6\rangle$. This is a cyclic group of order 3, so we have an abstract isomorphism

$$(\mathcal{O}_K/6\mathcal{O}_K)^*/\operatorname{im}[\mathcal{O}_K^*] \xrightarrow{\sim} \operatorname{Gal}(K(\sqrt[3]{2})/K), \tag{8.1}$$

and primes $\mathfrak{p}$ whose class is the unit element should split completely. As Artin realized in 1925, this suggests strongly that the isomorphism above maps the class of prime $\mathfrak{p}$ to its *Artin symbol*, just like the familiar isomorphism $(\mathbf{Z}/n\mathbf{Z})^* \to \operatorname{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ for abelian extensions of $\mathbf{Q}$ maps (p mod n) to its Artin symbol. Note that the ramifying primes 2 and $(1 - \zeta_3)|3$ in $K(\sqrt[3]{2})/K$ are exactly the primes dividing the 'conductor' $6\mathcal{O}_K$. The tamely ramified prime 2 divides the conductor once, and the wildly ramified prime $(1-\zeta_3)$ divides it twice, a phenomenon that is well known for conductors over $\mathbf{Q}$

▶ Towards the main theorem

The two extensions $K \subset K(i)$ for $K = \mathbf{Q}(\sqrt{-5})$ and $K(\sqrt[3]{2})/K$ for $K = \mathbf{Q}(\zeta_3)$ have in common that they are abelian extensions, and that the primes of K that split completely in it are the primes that are principal and satisfy a congruence condition modulo certain powers of the ramified primes. In the first case, there are *no* ramified primes and the only condition is that $\mathfrak{p}$ be principal. In the second case all primes are principal, but only those satisfying a congruence modulo 6 split completely. A far reaching generalization that one might hope to be true would be the following: *for every abelian extension L/K of number fields, there exists an $\mathcal{O}_K$-ideal $\mathfrak{f}$ such that all principal primes generated by an element $\pi \equiv 1$ mod $\mathfrak{f}$ split completely in L/K.* As divisors of this 'conductor ideal' $\mathfrak{f}$ one expects to find the primes that ramify in L/K, and one can hope that, just as for $K = \mathbf{Q}$, the smallest possible $\mathfrak{f}$ is divisible exactly by the ramifying primes, and the primes occurring with exponent > 1 are the wildly ramifying primes.

As we have phrased it, the statement is correct for our two examples, but it fails to hold for $K = \mathbf{Q}$. The reason is that the splitting primes in the cyclotomic field $\mathbf{Q}(\zeta_n)$ are the prime ideals $p\mathbf{Z}$ for which the *positive* generator is congruent to 1 modulo n. A sign change in the residue class modulo n changes the corresponding Artin symbol by a

complex conjugation, so this peculiar detail is only relevant to abelian extensions $L/\mathbf{Q}$ that are complex, i.e. extensions in which the real prime is ramified. When we take this into account, we arrive at the following weak form of the main theorem of class field theory.

8.2. Main theorem (weak form). *For every abelian extension of number fields L/K there exists an $\mathcal{O}_K$-ideal $\mathfrak{f}$ such that all primes of K that are principal with totally positive generator $\pi \equiv 1 \bmod \mathfrak{f}$ split completely in L/K.*

The smallest ideal $\mathfrak{f}$ one can take in 1.2 is the *conductor ideal* $\mathfrak{f}_{L/K}$ of the extension. As we will see, it is exactly divisible by the finite primes of K that ramify in L. The wildly ramifying primes occur with higher exponent than 1.

For imaginary quadratic fields K, Theorem 1.2 was proved during the 19-th century by Jacobi, Dedekind, Kronecker, Weber and others. Such K have no real primes, and the reason that their abelian extensions are relatively accessible stems from the fact that they can be obtained by adjoining the values of complex analytic functions that occur when one tries to invert certain elliptic integrals. This is somewhat reminiscent of the situation for $\mathbf{Q}$, where the abelian extensions are obtained by adjoining values of the exponential function $e^{2\pi iz}$ at rational values of z.

For arbitrary number fields K, work of Hilbert, Furtwängler and Takagi in the period 1895–1919 culminated in a proof of a result somewhat stronger than 1.2. In particular, Takagi proved that given K and $\mathfrak{f}$, there exists a *maximal* abelian extension $H_{\mathfrak{f}}/K$ with conductor ideal $\mathfrak{f}$; he also gave an explicit description of the corresponding Galois group $\mathrm{Gal}(H_{\mathfrak{f}}/K)$.

For $K = \mathbf{Q}$, we know that the maximal abelian extension of conductor n is the n-th cyclotomic field $\mathbf{Q}(\zeta_n)$, and that the isomorphism $(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ sends the residue class of a prime p to its Artin symbol. In our two examples this was also the case. For $K = \mathbf{Q}(\sqrt{-5})$ we had an isomorphism $Cl_K \xrightarrow{\sim} \mathrm{Gal}(K(i)/K)$ mapping the class of a prime $\mathfrak{p}$ to its Artin symbol as the principal primes were exactly the primes that split completely in $K(i)$. For $K = \mathbf{Q}(\zeta_3)$ we can determine the Artin symbol in $K(\sqrt[3]{2})$ for every prime not dividing 6, and writing $I_K(6)$ for the group of fractional $\mathcal{O}_K$-ideals relatively prime to 6 we have the *Artin map*

$$\psi_{K(\sqrt[3]{2})/K} : I_K(6) \to \mathrm{Gal}(K(\sqrt[3]{2})/K)$$

that maps a prime $\mathfrak{p} \nmid 6$ to the Artin symbol $(\mathfrak{p}, L/K)$. Euler's conjecture is that the primes in the kernel are the primes generated by an element congruent to 1 mod $6\mathcal{O}_K$ and Artin's generalization is that the kernel of $\psi_{K(\sqrt[3]{2})/K}$ consists of *all* fractional ideals generated by an element congruent to $1 \in (\mathcal{O}_K/6\mathcal{O}_K)^*$, so that the Artin map induces the abstract isomorphism 1.1. In its full generality, this is the following important extension of 1.2 that Artin conjectured in 1925 and proved 2 years later, using a clever reduction to the case of cyclotomic extensions due to Čebotarev.

8.3. Artin's reciprocity law. *For every abelian extension of number fields L/K, there*

exists an $\mathcal{O}_K$-ideal $\mathfrak{f}$ divisible by all finite primes that ramify in L such that the Artin map

$$\begin{aligned} \psi_{L/K} : I_K(\mathfrak{f}) &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{p} &\longmapsto (\mathfrak{p}, L/K) \end{aligned}$$

is surjective and its kernel contains all principal ideals generated by an element $x \in \mathcal{O}_K$ that is congruent to $1 \bmod \mathfrak{f}$ *and positive at the real primes $\mathfrak{p} : K \to \mathbf{R}$ that ramify in L/K.*

▶ Cycles and ray classes

Artin's reciprocity law is a very strong statement that implies a large number of relations between the Artin symbols at different primes. It suggests that it is convenient to include the ramified real primes in the conductor $\mathfrak{f}$ of the extension, and to declare an element $x \in \mathcal{O}_K$ congruent to 1 mod $\mathfrak{f}$ if it is congruent to 1 modulo the ideal part and positive at the real primes in $\mathfrak{f}$. The corresponding notion is provided by the cycles of a number field.

8.4. Definition. *A cycle or divisor of a number field K is a formal product $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ with $\mathfrak{p}$ ranging over all primes of K such that*

(i) *$n(\mathfrak{p})$ is a non-negative integer for all $\mathfrak{p}$ and $n(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$;*
(ii) *$n(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is real and $n(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex.*

For any cycle $\mathfrak{f}$, the finite part $\mathfrak{f}_0 = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{n(\mathfrak{p})}$ of a cycle is simply an integral ideal of the ring of integers $\mathcal{O}_K$ of K, while its infinite part $\mathfrak{f}_\infty = \prod_{\mathfrak{p} \text{ infinite}} \mathfrak{p}^{n(\mathfrak{p})}$ is a collection of real primes of K. As for ideals, we refer to the exponents $n(\mathfrak{p})$ as $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f})$ and write $\mathfrak{p}|\mathfrak{f}$ if $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) > 0$. Divisibility of cycles is defined in the obvious way, so we write $\mathfrak{f}_1|\mathfrak{f}_2$ if $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_1) \le \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_2)$ for all $\mathfrak{p}$. Similarly, the greatest common divisor $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ is the cycle with order $\min(\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_1), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_2))$ at $\mathfrak{p}$.

Congruences modulo cycles have to be defined in such a way that the quotient of two integral elements $x_1, x_2 \equiv 1 \bmod \mathfrak{f}$ is again congruent to 1 mod $\mathfrak{f}$, which is not the case for the usual additive congruences.

8.5. Definition. *Let $\mathfrak{p}$ be a prime of K and $n \in \mathbf{Z}_{\ge 0}$ an integer. Then an element $x \in K^*$ is multiplicatively congruent to* 1 *modulo $\mathfrak{p}^n$, notation $x \equiv 1 \bmod^* \mathfrak{p}^n$, if one of the following conditions is satisfied.*

(i) *$n = 0$;*
(ii) *$\mathfrak{p}$ is real, $n = 1$ and x is positive under the embedding $\mathfrak{p} : K^* \to \mathbf{R}^*$;*
(iii) *$\mathfrak{p}$ is finite, $n > 0$ and we have $x \in 1 + \mathfrak{p}^n \subset A_{\mathfrak{p}}$.*

For a cycle $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ we write $x \equiv 1 \bmod^* \mathfrak{f}$ if $x \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for all $\mathfrak{p}$.

Let $I(\mathfrak{f})$ be the group of fractional $\mathcal{O}$-ideals $\mathfrak{a}$ that have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0$ for every finite prime $\mathfrak{p}$ dividing the cycle $\mathfrak{f}$. The principal ideals $x\mathcal{O}$ generated by elements $x \equiv 1 \bmod^* \mathfrak{f}$ form a subgroup $R(\mathfrak{f}) \subset I(\mathfrak{f})$ that is sometimes called the *ray* modulo $\mathfrak{f}$. The terminology stems from the fact that we may identify the ray $R(\infty)$ in $\mathbf{Q}$ with the positive rational half-line,

a 'ray' from the origin. The factor group $Cl_{\mathfrak{f}} = I(\mathfrak{f})/R(\mathfrak{f})$ is the *ray class group modulo* $\mathfrak{f}$. The ray class groups will appear as the basic abelian Galois groups over K.

Example. For $K = \mathbf{Q}$ there is a single real prime $\mathfrak{p} = \infty$, so every cycle of $\mathbf{Q}$ is of the form $\mathfrak{f} = (n)$ or $\mathfrak{f} = (n) \cdot \infty$ for some positive integer n. The corresponding ray class groups are $Cl_{(n)} = (\mathbf{Z}/n\mathbf{Z})^*/\langle -1 \bmod n \rangle$ and $Cl_{(n)\cdot\infty} = (\mathbf{Z}/n\mathbf{Z})^*$.

In order to describe the structure of general ray class groups, we define the group $(\mathcal{O}/\mathfrak{f})^*$ for a cycle $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ by

$$(\mathcal{O}/\mathfrak{f})^* = (\mathcal{O}/\mathfrak{f}_0)^* \times \prod_{\mathfrak{p}|\mathfrak{f}_\infty} \langle -1 \rangle.$$

Every $x \in K^*$ contained in the subgroup $K(\mathfrak{f}) \subset K^*$ of elements that are units at all finite primes in $\mathfrak{f}$ has a residue class in $(\mathcal{O}/\mathfrak{f})^*$ consisting of its residue class in $(\mathcal{O}/\mathfrak{f}_0)^*$ at the finite component and the sign of $\mathfrak{p}(x)$ at the component of a real prime $\mathfrak{p} : K \to \mathbf{R}$ dividing $\mathfrak{f}_\infty$.

8.6. Proposition. *The ray class group modulo* $\mathfrak{f}$ *is finite and fits in an exact sequence*

$$0 \longrightarrow (\mathcal{O}/\mathfrak{f})^*/\operatorname{im}[\mathcal{O}^*] \longrightarrow Cl_{\mathfrak{f}} \longrightarrow Cl \longrightarrow 0$$

of finite abelian groups.

Proof. Let $P(\mathfrak{f})$ denote the group of principal ideals generated by elements $x \in K(\mathfrak{f})$. Then we have an exact sequence $0 \to P(\mathfrak{f})/R(\mathfrak{f}) \to I(\mathfrak{f})/R(\mathfrak{f}) \to I(\mathfrak{f})/P(\mathfrak{f}) \to 0$ in which the middle term is by definition the ray class group modulo $\mathfrak{f}$. The final term is the ordinary class group, since every ideal class in Cl contains an ideal from $I(\mathfrak{f})$ by the approximation theorem.

The group $P(\mathfrak{f}) = K(\mathfrak{f})/\mathcal{O}^*$ admits a canonical surjection to $(\mathcal{O}/\mathfrak{f})^*/\operatorname{im}[\mathcal{O}^*]$, and the kernel consists by definition of the ray $R(\mathfrak{f})$ modulo $\mathfrak{f}$. This yields the required exact sequence, and the finiteness of $Cl_{\mathfrak{f}}$ follows from the finiteness of the outer terms. □

8.7. Corollary. *If a cycle* $\mathfrak{f}$ *is divisible by* $\mathfrak{g}$*, the natural map* $Cl_{\mathfrak{f}} \to Cl_{\mathfrak{g}}$ *is surjective.*

Proof. The outer vertical arrows in the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathcal{O}/\mathfrak{f})^*/\operatorname{im}[\mathcal{O}^*] & \longrightarrow & Cl_{\mathfrak{f}} & \longrightarrow & Cl & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{id}} & & \\
0 & \longrightarrow & (\mathcal{O}/\mathfrak{g})^*/\operatorname{im}[\mathcal{O}^*] & \longrightarrow & Cl_{\mathfrak{g}} & \longrightarrow & Cl & \longrightarrow & 0
\end{array}$$

are obviously surjective, so the same is true for the middle arrow. □

▶ Ideal groups

We want to characterize the abelian extensions L/K in terms of the kernel of the Artin map $\psi_{L/K} : I(\mathfrak{f}) \to \mathrm{Gal}(L/K)$ in 1.3. The problem is that this kernel depends on the chosen cycle $\mathfrak{f}$. If $\mathfrak{f}$ satisfies the requirements of 1.3, then so does any multiple of $\mathfrak{f}$. The same situation occurs if we want to specify an abelian number field $L \subset \mathbf{Q}(\zeta_n)$ by the subgroup $B_n \subset (\mathbf{Z}/n\mathbf{Z})^*$ to which it corresponds. If we replace n by a multiple m, we obtain another subgroup $B_m \subset (\mathbf{Z}/m\mathbf{Z})^*$ corresponding to L that is 'equivalent' to B_n in the sense that the natural map $(\mathbf{Z}/m\mathbf{Z})^* \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$ induces an isomorphism $(\mathbf{Z}/m\mathbf{Z})^*/B_m \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^*/B_n$.

An *ideal group defined modulo* $\mathfrak{f}$ is a group $B(\mathfrak{f})$ satisfying $R(\mathfrak{f}) \subset B(\mathfrak{f}) \subset I(\mathfrak{f})$. If $\mathfrak{f}'$ is another cycle and $B(\mathfrak{f}')$ an ideal group defined modulo $\mathfrak{f}'$, we say that $B(\mathfrak{f})$ and $B(\mathfrak{f}')$ are equivalent if for every common multiple $\mathfrak{g}$ of $\mathfrak{f}$ and $\mathfrak{f}'$, the inverse images of $B(\mathfrak{f})$ and $B(\mathfrak{f}')$ under the natural maps $I(\mathfrak{g}) \to I(\mathfrak{f})$ and $I(\mathfrak{g}) \to I(\mathfrak{f}')$ coincide. If this is the case, it follows from 1.7 that we have an isomorphism $I(\mathfrak{f})/B(\mathfrak{f}) \cong I(\mathfrak{f}')/B(\mathfrak{f}')$ of finite abelian groups. The notion of equivalence does not depend on the choice of a common multiple, and we obtain an equivalence relation on the set of ideal groups. The equivalence classes are simply referred to as *ideal groups*. If an ideal group B has a representative defined modulo $\mathfrak{f}$, we denote it by $B(\mathfrak{f})$ and say that B can be defined modulo $\mathfrak{f}$ or has modulus $\mathfrak{f}$.

Before we formulate the main theorem in its final form, we still need to show that the set of moduli of an ideal group consists of the multiples of some unique minimal modulus, the *conductor* of the ideal group. Over $\mathbf{Q}$, this reflects the fact that an abelian number field L can be embedded in $\mathbf{Q}(\zeta_m)$ if and only if m is divisible by the conductor of L. The general statement for ideal groups follows from the following lemma.

8.8. Lemma. *An ideal group that can be defined modulo* $\mathfrak{f}_1$ *and* $\mathfrak{f}_2$ *can be defined modulo* $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$.

Proof. Write $\mathfrak{f} = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ and $\mathfrak{g} = \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$ and $H_i = B(\mathfrak{f}_i)/R(\mathfrak{f}_i)$. By 1.7, all arrows in the commutative diagram

$$\begin{array}{ccc} I(\mathfrak{g})/R(\mathfrak{g}) & \xrightarrow{\phi_1} & I(\mathfrak{f}_1)/R(\mathfrak{f}_1) \\ \big\downarrow{\scriptstyle \phi_2} & & \big\downarrow{\scriptstyle \chi_1} \\ I(\mathfrak{f}_2)/R(\mathfrak{f}_2) & \xrightarrow{\chi_2} & I(\mathfrak{f})/R(\mathfrak{f}) \end{array}$$

are surjective. We can define $G = \phi_1^{-1}[H_1] = \phi_2^{-1}[H_2]$ by assumption, and we have to show that there exists a subgroup $H \subset I(\mathfrak{f})/R(\mathfrak{f})$ with inverse image G in $I(\mathfrak{g})/R(\mathfrak{g})$. The obvious candidate is $H = \chi_1[H_1] = \chi_2[H_2]$. We have $\chi_i\phi_i[G] = H$, so in order to prove that $G = (\chi_i\phi_i)^{-1}[H]$ we need to show $\ker(\chi_i\phi_i) \subset G$.

From $\ker \phi_i = (R(\mathfrak{f}_i) \cap I(\mathfrak{g}))/R(\mathfrak{g}) \subset G$ we have $[(R(\mathfrak{f}_1) \cap I(\mathfrak{g})) \cdot (R(\mathfrak{f}_2) \cap I(\mathfrak{g}))]/R(\mathfrak{g}) \subset G$. We claim the equality

$$(R(\mathfrak{f}_1) \cap I(\mathfrak{g})) \cdot (R(\mathfrak{f}_2) \cap I(\mathfrak{g})) = (R(\mathfrak{f}_1)R(\mathfrak{f}_2)) \cap I(\mathfrak{g}).$$

The inclusion $\supset$ is the nontrivial one, so let $x_i\mathcal{O} \in R(\mathfrak{f}_i)$ for $i = 1, 2$ be given such that $x_1x_2\mathcal{O} \in I(\mathfrak{g})$ holds. If $\mathfrak{p}$ is finite and divides $\mathfrak{g}$, say $\mathfrak{p}|\mathfrak{f}_1$, it follows from $\operatorname{ord}_\mathfrak{p}(x_1x_2) = 0$ and $x_1 \equiv 1 \bmod^* \mathfrak{f}_1$ that $\operatorname{ord}_\mathfrak{p}(x_2) = 0$. Thus $x_1\mathcal{O}$ and $x_2\mathcal{O}$ are in $I(\mathfrak{g})$, which establishes our claim.

As we have $\ker(\chi_i\phi_i) = (R(\mathfrak{f}) \cap I(\mathfrak{g}))/R(\mathfrak{g})$, the proof may be concluded by showing $R(\mathfrak{f})$ to be equal to $R(\mathfrak{f}_1)R(\mathfrak{f}_2)$. The inclusion $R(\mathfrak{f}) \supset R(\mathfrak{f}_1)R(\mathfrak{f}_2)$ is immediate from $R(\mathfrak{f}) \supset R(\mathfrak{f}_i)$ for both i. For $x \equiv 1 \bmod^* \mathfrak{f}$ the congruences $y \equiv x \bmod^* \mathfrak{f}_1$ and $y \equiv 1 \bmod^* \mathfrak{f}_2$ are compatible, so they are satisfied for some $y \in K^*$ by the approximation theorem. Now the representation $x\mathcal{O} = xy^{-1} \cdot y\mathcal{O}$ shows that we have $x\mathcal{O} \in R(\mathfrak{f}_1)R(\mathfrak{f}_2)$, thereby proving the other inclusion. □

The preceding proof is characteristic for many proofs using ideal groups in the sense that the approximation theorem plays an essential role. In the idèlic formulation given in the next section the existence of a conductor will be a trivial consequence of the formalism.

If B_1 and B_2 are ideal groups of K and $\mathfrak{f}$ is a common modulus, we define their product and intersection by $(B_1B_2)(\mathfrak{f}) = B_1(\mathfrak{f})B_2(\mathfrak{f})$ and $(B_1 \cap B_2)(\mathfrak{f}) = B_1(\mathfrak{f}) \cap B_2(\mathfrak{f})$. We write $B_1 \subset B_2$ if $B_1(\mathfrak{f}) \subset B_2(\mathfrak{f})$ holds. One easily checks that all this is independent of the choice of the common modulus $\mathfrak{f}$.

▶ Main theorem

We can now formulate the ideal group version of the main theorem of class field theory.

8.9. Main theorem. *Let K be a number field, Σ_K the set of finite abelian extensions of K contained in some fixed algebraic closure and $\mathcal{B}$ the set of ideal groups of K. Then there exists an inclusion reversing bijection*

$$\Sigma_K \;\leftrightarrows\; \mathcal{B}$$

such that for an extension L/K corresponding to an ideal group B with conductor $\mathfrak{f}$ the following holds:

(1) *the primes dividing the conductor $\mathfrak{f}$ are the primes that ramify in L/K, and the primes whose square divides $\mathfrak{f}$ are the primes that are wildly ramified in L/K;*
(2) *for every multiple $\mathfrak{g}$ of the conductor $\mathfrak{f}$, the Artin map $\psi_{L/K} : I(\mathfrak{g}) \to \operatorname{Gal}(L/K)$ is a surjective homomorphism with kernel $B(\mathfrak{g})$.*

The ideal group B corresponding to an abelian extension L of K determines the Galois group $\operatorname{Gal}(L/K)$ as for every modulus $\mathfrak{g}$ of B, the Artin map for L/K induces an *Artin isomorphism*

$$\psi_{L/K} : I(\mathfrak{g})/B(\mathfrak{g}) \xrightarrow{\sim} \operatorname{Gal}(L/K). \tag{8.10}$$

The splitting behavior of a prime of K in the extension L is determined by the ideal class of $\mathfrak{p}$ in the generalized ideal class group $I(\mathfrak{g})/B(\mathfrak{g})$. The field L is the unique field

corresponding to this ideal group B and is known as the *class field* of B. This (highly non-trivial) existence of class fields for every given division of prime ideals into classes modulo a cycle accounts for the name *class field theory*.

It is possible to give an explicit description of the ideal group corresponding to an abelian extension L/K in terms of L. In fact, this description follows completely from functorial properties of the Artin map. We will list all these properties in a single theorem and derive them from 1.9. We need the action of the norm on ideal groups to formulate it.

If $\mathfrak{f}$ is a cycle in K and L/K a finite extension, we can view $\mathfrak{f}$ as a cycle in L by taking $\mathfrak{f}_0\mathcal{O}_L$ as its finite part and the product of the real extensions of the $\mathfrak{p}|\mathfrak{f}_\infty$ as the infinite part. In this situation, the ideal norm $N_{L/K} : I_L \to I_K$ can be restricted to yield a norm map $N_{L/K} : I_L(\mathfrak{f}) \to I_K(\mathfrak{f})$ that maps the ray $R_L(\mathfrak{f})$ in L into the ray $R_K(\mathfrak{f})$ in K. In particular, the inverse image of an ideal group $B(\mathfrak{f})$ in K under the norm yields an ideal group $N_{L/K}^{-1}B(\mathfrak{f})$ modulo $\mathfrak{f}$ in L. We denote its equivalence class by $N_{L/K}^{-1}B$.

8.11. Theorem. *Let K be a number field, and L, L_1 and L_2 finite abelian extensions of K inside an algebraic closure $\overline{K}$ with corresponding ideal groups B, B_1 and B_2. Then the following properties hold:*

(1) *we have $B(\mathfrak{g}) = N_{L/K}(I_L(\mathfrak{g})) \cdot R(\mathfrak{g})$ for every modulus of B;*

(2) *the ideal group $B_1 \cap B_2$ corresponds to the compositum L_1L_2, and the ideal group B_1B_2 corresponds to the intersection $L_1 \cap L_2$;*

(3) *if L_2 contains L_1 and $\mathfrak{g}$ is a modulus of B_2, then $\mathfrak{g}$ is a modulus of B_1 and there is a commutative diagram*

$$\begin{array}{ccc} I(\mathfrak{g})/B_2(\mathfrak{g}) & \xrightarrow{\sim} & \mathrm{Gal}(L_2/K) \\ \big\downarrow{\scriptstyle \mathrm{can}} & & \big\downarrow{\scriptstyle \mathrm{res}} \\ I(\mathfrak{g})/B_1(\mathfrak{g}) & \xrightarrow{\sim} & \mathrm{Gal}(L_1/K) \end{array}$$

relating the Artin isomorphisms of L_1 and L_2 over K;

(4) *if $E \subset \overline{K}$ is any finite extension of K, then $LE \supset E$ is a finite abelian extension corresponding to the ideal group $N_{E/K}^{-1}B$ of E. For every modulus $\mathfrak{g}$ of B there is a commutative diagram*

$$\begin{array}{ccc} I_E(\mathfrak{g})/N_{E/K}^{-1}B(\mathfrak{g}) & \xrightarrow{\sim} & \mathrm{Gal}(LE/E) \\ \big\downarrow{\scriptstyle N_{E/K}} & & \big\downarrow{\scriptstyle \mathrm{res}} \\ I(\mathfrak{g})/B(\mathfrak{g}) & \xrightarrow{\sim} & \mathrm{Gal}(L/K). \end{array}$$

Moreover, the ideal group B_0 corresponding to the abelian extension $L \cap E$ of K satisfies $B_0(\mathfrak{g}) = N_{E/K}(I_E(\mathfrak{g})) \cdot B(\mathfrak{g})$;

(5) *if $E \subset \overline{K}$ is any finite extension of K, then the ideal group B_E corresponding to the maximal subextension of E/K that is abelian over K satisfies $B_E(\mathfrak{g}) = N_{E/K}(I_E(\mathfrak{g})) \cdot R(\mathfrak{g})$ for each of its moduli $\mathfrak{g}$.*

Proof. Property (2) is a generality on inclusion reversing bijections that we leave to the reader.

For (3), we observe first that the diagram is commutative because of the property $(\mathfrak{p}, L_2/K)|_{L_1} = (\mathfrak{p}, L_1/K)$ of the Artin symbol of the primes $\mathfrak{p} \nmid \mathfrak{g}$ that generate $I(\mathfrak{g})$. In particular, if $R(\mathfrak{g})$ is in the kernel of the Artin map of the extension L_2/K, it is in the kernel of the Artin map of the extension L_1/K. This implies that $\mathfrak{g}$ is a modulus for B_1.

The commutativity of the diagram in (4) is proved in a similar way. If $\mathfrak{r}$ is a prime in E lying above a finite prime $\mathfrak{p} \nmid \mathfrak{g}$, it is unramified in LE/E and one has $(\mathfrak{r}, LE/E)|_L = (\mathfrak{p}, L/K)^{f(\mathfrak{r}/\mathfrak{p})} = (N_{E/K}\mathfrak{r}, L/K)$. This also shows that the ray $R_E(\mathfrak{g})$ is in the kernel of the Artin map $\psi_{LE/E} : I_E(\mathfrak{g}) \to \mathrm{Gal}(LE/E)$, since its norm image $N_{E/K}(R_E(\mathfrak{g})) \subset R(\mathfrak{g})$ is in the kernel of $\psi_{L/K}$. As the restriction map on the Galois groups is injective, we have $\ker(\psi_{LE/E}) = N_{E/K}^{-1}B(\mathfrak{g})$ as the ideal group corresponding to the extension LE of E.

Using Galois theory, we see that the cokernels of the vertical maps give an isomorphism

$$I(\mathfrak{g})/N_{E/K}(I_E(\mathfrak{g})) \cdot B(\mathfrak{g}) \xrightarrow{\sim} \mathrm{Gal}((L \cap E)/K,$$

and the restriction property $(\mathfrak{p}, L/K)|_{L\cap E} = (\mathfrak{p}, (L \cap E)/K)$ of the Artin symbol shows that this is the Artin isomorphism for the extension $L \cap E$ of K. It follows that $B_0(\mathfrak{g}) = N_{E/K}(I_E(\mathfrak{g})) \cdot B(\mathfrak{g})$ is the ideal group of $L \cap E$ over K.

In order to derive the basic statement (1) from this we take E/K abelian in the previous argument and $\mathfrak{g}$ a modulus of the corresponding ideal group B_E. Setting L equal to the class field of $R(\mathfrak{g})$, we have an inclusion $E \subset L$ from $B_E \supset R(\mathfrak{g})$ and from what we have just proved we find $B_E(\mathfrak{g}) = N_{E/K}(I_E(\mathfrak{g})) \cdot R(\mathfrak{g})$.

Finally, for property (5), we apply this argument once more with E/K finite, $\mathfrak{g}$ a modulus of the ideal group of the maximal subextension $E_0 \subset E$ that is abelian over K and L the class field of $R(\mathfrak{g})$. This yields $L \cap E = E_0$ and the property follows. □

► Ray class fields

The abelian extension $H_\mathfrak{f}$ of K corresponding to the ray $R(\mathfrak{f})$ modulo a cycle $\mathfrak{f}$ is known as the *ray class field modulo* $\mathfrak{f}$. They can be viewed as generalizations of the cyclotomic fields in the sense of Kronecker-Weber to arbitrary K. By the main theorem, they have the following properties.

8.12. Theorem. *Let K be a number field with maximal abelian extension K^{ab}, $\mathfrak{f}$ a cycle of K and $H_\mathfrak{f} \subset K^{\mathrm{ab}}$ the ray class field modulo $\mathfrak{f}$. Then $H_\mathfrak{f}$ is the maximal abelian extension of K inside K^{ab} in which all primes of the ray $R(\mathfrak{f})$ split completely. The extension $H_\mathfrak{f}/K$ is unramified outside $\mathfrak{f}$, and we have an Artin isomorphism*

$$Cl_\mathfrak{f} \xrightarrow{\sim} \mathrm{Gal}(H_\mathfrak{f}/K).$$

The field K^{ab} is the union of all ray class fields of K inside K^{ab}. □

Example. For $K = \mathbf{Q}$ the ray class fields can be given explicitly as

$$H_n = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) \qquad \text{and} \qquad H_{n\cdot\infty} = \mathbf{Q}(\zeta_n).$$

In order to prove this, one applies (4) of 1.11 with $E = \mathbf{Q}(\zeta_n)$ and $L = H_{n\cdot\infty}$. For every prime $\mathfrak{p}|p$ in $\mathbf{Q}(\zeta_n)$ that does not divide $n\cdot\infty$, the norm $N_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}\mathbf{Z}$ is in the ray $R(n\cdot\infty)$, so the left vertical arrow is the zero map. This implies that $LE = H_{n\cdot\infty}(\zeta_n)$ equals $E = \mathbf{Q}(\zeta_n)$, so $H_{n\cdot\infty}$ is contained in $\mathbf{Q}(\zeta_n)$. As we know the Galois group $\mathrm{Gal}(H_{n\cdot\infty}/\mathbf{Q}) \cong Cl_{n\cdot\infty} = (\mathbf{Z}/n\mathbf{Z})^*$ we have $H_{n\cdot\infty} = \mathbf{Q}(\zeta_n)$ as stated. The real field $H_n \subset H_{n\cdot\infty}$ is contained in the maximal real subfield $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ of the cyclotomic field, and it must be equal to it as we have already seen that its Galois group over $\mathbf{Q}$ is $Cl_n = (\mathbf{Z}/n\mathbf{Z})^*/\langle -1 \bmod n\rangle$.

A ray class field of special importance is the ray class field modulo the trivial cycle $\mathfrak{f} = 1$ of K. It is known as the *Hilbert class field* of K. As the ray class group modulo the trivial cycle is the ordinary class group Cl_K of K, we have an Artin isomorphism

$$\psi_{H/K} : Cl_K \xrightarrow{\sim} \mathrm{Gal}(H/K)$$

between the class group of K and the Galois group over K of the maximal abelian extension H of K that is unramified at all primes of K. Moreover, the primes that split completely in H/K are the principal prime ideals in the ring of integers of K. This is a rather surprising relation: it is not at all obvious that the size of a certain unramified extension of K should be related to the class group of K, which measures how much the ring of integers of K differs from a principal ideal ring. On the other hand, this relation is extremely useful as it enables us to study the class group of a number field K by constructing unramified abelian extensions of K. In this context, one also uses a slightly larger field known as the *strict* or *narrow* Hilbert class field. It is the maximal abelian extension of K that is unramified at all *finite* primes of K.

A problem that has not been answered in a satisfactory way for any number field $K \neq \mathbf{Q}$ apart from imaginary quadratic number fields is how to find explicit generators over K of the abelian extensions whose existence is guaranteed by the general theory. For small examples (exercises 10, 16, 23), a more or less sophisticated combination of ad hoc arguments often leads to the desired result.

Exercises

1. Let it be given that for every integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ depends only on the residue class $p \bmod 4|a|$, and that the residue classes of p and $-p$ have the same behaviour if a is positive. Deduce the quadratic reciprocity law from this.
   [Hint: for $p - q = 4a$ we obtain $\left(\frac{p-q}{q}\right) = \left(\frac{p-q}{p}\right)$.]

2. Show that every prime number of the form $p = x^2 + 5y^2$ is equal to 5 or congruent to 1 or 9 modulo 20.

3. Let $n > 2$ be an integer. Determine all integers a for which the extension $\mathbf{Q}(\zeta_n, \sqrt[n]{a})$ is an abelian extension of $\mathbf{Q}$.

4. Prove the main theorem 8.9 for $K = \mathbf{Q}$.
   [There is more to it than Kronecker-Weber...]

5. Let B_1 and B_2 be ideal groups of K with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$. Show that $B_1 \cap B_2$ has conductor $\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$ and that $B_1 B_2$ has conductor dividing $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$. Give an example in the second case where the conductor is a strict divisor of $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$.

6. The Euler Φ-function is defined for cycles $\mathfrak{f}$ of K by $\Phi(\mathfrak{f}) = \#(\mathcal{O}/\mathfrak{f})^*$.
   a. Show that ϕ is multiplicative, i.e. $\Phi(\mathfrak{fg}) = \Phi(\mathfrak{f})\Phi(\mathfrak{g})$ if $\gcd(\mathfrak{f}, \mathfrak{g}) = 1$.
   b. Let E be the unit group of $\mathcal{O}$ and $E_{\mathfrak{f}}$ the subgroup of units in E that are $1 \bmod^* \mathfrak{f}$. Show that the ray class group of conductor $\mathfrak{f}$ has order $h(\mathfrak{f}) = h_K \Phi(\mathfrak{f})[E : E_{\mathfrak{f}}]^{-1}$.

7. The *strict* or *narrow Hilbert class field* $H^+ = H^+(K)$ of a number field K is the maximal abelian extension of K in which all finite primes are unramified. Show that H^+ is a Galois extension of the Hilbert class field H of K, and that $\operatorname{Gal}(H^+/H)$ is an elementary abelian 2-group of order $2^r[\mathcal{O}^* : \mathcal{O}_+^*]^{-1}$. Here r is the number of real primes of K and $\mathcal{O}_+^*$ denotes the group of *totally positive units* in $\mathcal{O}$, i.e. those units that are positive under every real embedding of K.

8. Let H be the Hilbert class field of K and $\mathfrak{p}$ a finite prime of K. Prove that $\mathfrak{p}$ splits completely in H/K if and only if $\mathfrak{p}$ is principal. Show also that the the norm map $N_{H/K} : Cl_H \to Cl_K$ is the zero map.

9. Let $K_1, K_2 \subset \mathbf{Q}^{\mathrm{ac}}$ be number fields of class number 1. Prove that $K_1 \cap K_2$ has class number 1.

10. Show that $K = \mathbf{Q}(\sqrt{-15})$ has Hilbert class field $K(\sqrt{5})$.

11. Let K be a number field that is Galois over $\mathbf{Q}$ with group G. Show that the Hilbert class field H of K is normal over $\mathbf{Q}$, and that there is an exact sequence

$$0 \longrightarrow Cl_K \longrightarrow \operatorname{Gal}(H/\mathbf{Q}) \longrightarrow G \longrightarrow 0.$$

    Show also $\operatorname{Gal}(H/\mathbf{Q})$ can be written as a semi-direct product $\operatorname{Gal}(H/\mathbf{Q}) \cong Cl_K \rtimes G$ with respect to the natural action of G on Cl_K if G is cyclic of prime order.

12. Let K be an imaginary quadratic field and L/K an unramified abelian extension. Show that $L/\mathbf{Q}$ is Galois. Can you describe $\operatorname{Gal}(L/\mathbf{Q})$?

13. Let E/K be an extension of number fields of degree n. Show that the class number h_K divides nh_E. Show also that h_K divides h_E and that the norm map $N_{E/K} : Cl_E \to Cl_K$ is surjective if there is a prime that is totally ramified in E/K.

14. Show that the class number of the real cyclotomic field $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ divides the class number of $\mathbf{Q}(\zeta_n)$ for every $n > 1$, and that the class number of $\mathbf{Q}(\zeta_m)$ divides the class number of $\mathbf{Q}(\zeta_n)$ if m divides n.

15. *(Ring class fields.)* Let K be a number field with ring of integers $\mathcal{O}$ and $R \subset \mathcal{O}$ a subring for which the conductor $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}/R}$ (in the sense of [I, 5.8]) is non-zero. Show that there is a unique subfield $R_\mathfrak{f} \subset H_\mathfrak{f}$ of the ray class field modulo $\mathfrak{f}$ that contains the Hilbert class field of K and yields an isomorphism

$$\mathrm{Pic}(R) \xrightarrow{\sim} \mathrm{Gal}(R_\mathfrak{f}/K)$$

under which the residue class of an invertible prime ideal $\mathfrak{p} \subset R$ is mapped to the Artin symbol of $\mathfrak{p}\mathcal{O}$ in $R_\mathfrak{f}/K$. If K is imaginary quadratic, show that $R_\mathfrak{f}/\mathbf{Q}$ is Galois and that $\mathrm{Gal}(R_\mathfrak{f}/\mathbf{Q})$ is isomorphic to the semidirect product $\mathrm{Pic}(R) \rtimes \mathbf{Z}/2\mathbf{Z}$, where the action of the non-trivial element of $\mathbf{Z}/2\mathbf{Z}$ on $\mathrm{Pic}(R)$ is the inversion $[\mathfrak{a}] \mapsto [\mathfrak{a}]^{-1}$.

16. Let K be a cubic number field of squarefree discriminant D. Show that the extension $K(\sqrt{D})/\mathbf{Q}(\sqrt{D})$ is cyclic of degree 3 and totally unramified. Conclude that the class number of $\mathbf{Q}(\sqrt{D})$ is divisible by 3. As an example, show that $K = \mathbf{Q}(\sqrt{-31})$ has Hilbert class field $K(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$.

17. Let $k \geq 1$ be an odd integer and α a root of the polynomial $X^3 + 4kX - k$. Show that $\mathbf{Q}(\alpha)$ is a cubic field with even class number.

18. For p be a prime number we let $m(p)$ be the number of distinct zeroes of $X^3 - X - 1$ in the finite field $\mathbf{F}_p$. Prove the following:
    $m = 0$ if and only if $\left(\frac{p}{23}\right) = 1$ and p cannot be written as $p = a^2 + 23b^2$ with $a, b \in \mathbf{Z}$;
    $m = 1$ if and only if $\left(\frac{p}{23}\right) = -1$;
    $m = 2$ if and only if $p = 23$;
    $m = 3$ if and only if p can be written as $p = a^2 + 23b^2$ with $a, b \in \mathbf{Z}$.

19. Suppose L/K is cyclic of prime power order p^k and p does not divide h_K. Prove that there is a prime that is totally ramified in L/K.

20. The *Hilbert class field tower* of K is the sequence of fields $K = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_i \subset \ldots$ in which H_{i+1} is the Hilbert class field of H_i for each $i \geq 0$. The Hilbert class field tower is said to be *finite* if $H_{i+1} = H_i$ for i sufficiently large. Prove that all fields H_i are normal extensions of K with root discriminant $|\Delta_{H_i}|^{1/[H_i:\mathbf{Q}]} = |\Delta_K|^{1/[K:\mathbf{Q}]}$, and that the Hilbert class field tower of K is finite if and only if there is a finite extension of K with class number 1.
    [It has been shown by Golod and Shafarevich in 1964 that there exist infinite class field towers. This implies that the asymptotic lower bound $|\Delta_K|^{1/[K:\mathbf{Q}]} > 5.803...$ for $[K : \mathbf{Q}]$ tending to infinity [I, §9] cannot be replaced by any lower bound that tends to infinity with $[K : \mathbf{Q}]$.]

21. Let $\mathcal{O}$ be the ring of integers of $K = \mathbf{Q}(\sqrt{5})$.
    a. Prove $\mathcal{O}$ is a principal ideal domain with unit group $\mathcal{O}^* = \langle -1, (1+\sqrt{5})/2 \rangle$.
    b. Let p be a prime number. Prove that there exists a field L satisfying

$$[L : \mathbf{Q}] = 4, \qquad \sqrt{5} \in L, \qquad |\Delta_{L/\mathbf{Q}}| = 25p$$

    if and only if $p \not\equiv 2,\ 3 \bmod 5$. Prove also that if such a field exists, it is uniquely determined by p, up to isomorphism. We denote this field by $L_{(p)}$.
    c. Prove that among all fields $L_{(p)}$, the only one that is Galois over $\mathbf{Q}$ is the field $L_{(5)}$. Can you embed $L_{(5)}$ in a cyclotomic extension of $\mathbf{Q}$?

22. *(Continuation.)* A number field is called *totally real* if it has no complex primes, *totally complex* if it has no real primes, and *mixed* if it is neither totally real nor totally complex. The *Fibonacci sequence* $(F_n)_{n=0}^{\infty}$ is inductively defined by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$. Let p be a prime number with $p \equiv 1$ or $4 \bmod 5$.
    a. Prove that $L_{(p)}$ is mixed if and only if $p \equiv 3 \bmod 4$.
    b. Suppose that $p \equiv 1 \bmod 8$. Prove that $L_{(p)}$ is totally real if p divides $F_{(p-1)/4}$, and totally complex otherwise.
    c. Suppose that $p \equiv 5 \bmod 8$. Prove that $L_{(p)}$ is totally complex if p divides $F_{(p-1)/4}$, and totally real otherwise.
    d. Let p be a prime number with $p \equiv 11$ or $19 \bmod 20$. Prove that the field $L_{(p)}$ has exactly one prime lying over 5 if $p \equiv 11 \bmod 20$, and exactly two primes lying over 5 if $p \equiv 19 \bmod 20$.

23. Show that the Hilbert class field H of $\mathbf{Q}(\sqrt{-17})$ is a dihedral extension of $\mathbf{Q}$ of degree 8. Find generators for H.
    [Hint: Show that H contains $i = \sqrt{-1}$ and that $H/\mathbf{Q}(i)$ is a V_4-extension.]

24. *(Artin)* Show that the real quadratic field $\mathbf{Q}(\sqrt{19 \cdot 151})$ has class number 1, and that it has a Galois extension of degree 60 that is unramified at all finite primes.
    [Hint: the polynomial $X^5 - X - 1$ has discriminant $19 \cdot 151$, so you can use exercise 7.4.]

25. Show that the splitting field of the polynomial $X^4 - X - 1$ is unramified over $\mathbf{Q}(\sqrt{-283})$. Deduce that the class number of $\mathbf{Q}(\sqrt{-283})$ is divisible by 3. [You may verify that it is equal to 3. Can you describe the Hilbert class field of $\mathbf{Q}(\sqrt{-283})$?]

26. Show that for every number field K, there is a canonical isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \lim_{\leftarrow} Cl_{\mathfrak{f}}$ between the Galois group of the maximal abelian extension of K and the projective limit of the ray class groups $Cl_{\mathfrak{f}}$ of K with respect to the natural maps $Cl_{\mathfrak{g}} \to Cl_{\mathfrak{f}}$ if $\mathfrak{f}$ divides $\mathfrak{g}$. Show that the direct product $\prod_{\mathfrak{p}} A_{\mathfrak{p}}^*$ of the unit groups of the completions $A_{\mathfrak{p}}$ of $\mathcal{O}$ at the finite primes $\mathfrak{p}$ admits a natural map to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Can you describe the cokernel? Is this map injective? Deduce that every number field $K \neq \mathbf{Q}$ has abelian extensions that are not cyclotomic.

9 Class field theory: idèles

The formulation of class field theory as given in the preceding section is the classical formulation using ideal groups. From a computational point of view, these groups are often a convenient tool as they have a simple definition that makes them well-suited for most explicit computations. It is however somewhat annoying that every proof involving ideal groups starts by the choice of a common cycle modulo which everything is defined, and the end of the proof is the observation that the result obtained is independent of the choice of the common modulus.

In order to avoid the choice of moduli, say in the case of base field $\mathbf{Q}$, it is clear that one should not work with the groups $(\mathbf{Z}/n\mathbf{Z})^*$ for varying n, but pass to the projective limit

$$\widehat{\mathbf{Z}}^* = \varprojlim_n (\mathbf{Z}/n\mathbf{Z})^* = \prod_p \mathbf{Z}_p^*$$

from the beginning and define the Artin map on $\widehat{\mathbf{Z}}^*$ rather than on an ideal group $I_{\mathbf{Q}}(n)$ for some large n. We see that for the rational field, this large group becomes a product of completions at all finite primes of the field.

► Subgroups of the idèle group

In the general case, one also needs the real completions in order to keep track of the sign conditions at the real primes. Chevalley observed that a very elegant theory results if one takes the product of the unit groups at *all* completions of the number field, i.e. the idèle group J of K, and writes all ray class groups as surjective images $J \twoheadrightarrow Cl_{\mathfrak{f}}$.

As the idèle group J contains a subgroup

$$K_{\mathfrak{p}}^* = K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}' \neq \mathfrak{p}} \{1\} \subset J \tag{9.1}$$

for each prime $\mathfrak{p}$, we obtain a *local Artin map* for each completion $K_{\mathfrak{p}}$ of K. This point of view enables us to describe the relation between the global abelian extension L/K and the local extensions $L_{\mathfrak{q}}/K_{\mathfrak{p}}$, thus giving rise to a *local class field theory*. Moreover, it yields in a natural way a direct description of the power of a prime $\mathfrak{p}$ dividing the conductor of an extension L/K that strengthens the qualitative description of 1.9(1).

In order to describe the open subgroups of the idèle group J of K, we look at the open subgroups of the completions $K_{\mathfrak{p}}^*$ first. If $\mathfrak{p}$ is a finite prime, a basis of open neighborhoods of the unit element $1 \in K_{\mathfrak{p}}^*$ consists of the subgroups $U_{\mathfrak{p}}^{(n)} \subset K_{\mathfrak{p}}^*$ defined by

$$U_{\mathfrak{p}}^{(n)} = \begin{cases} U_{\mathfrak{p}} = A_{\mathfrak{p}}^* & \text{if } n = 0; \\ 1 + \mathfrak{p}^n & \text{if } n \in \mathbf{Z}_{>0}. \end{cases}$$

If $\mathfrak{p}$ is real, we have $K_{\mathfrak{p}} \cong \mathbf{R}$. Every open subgroup of the multiplicative group $\mathbf{R}^*$ contains the group $\mathbf{R}_{>0}$ of positive real numbers as $\mathbf{R}_{>0}$ is generated by any open neighborhood of $1 \in \mathbf{R}^*$. The open subgroups of $K_{\mathfrak{p}}^*$ are therefore

$$U_{\mathfrak{p}}^{(0)} = K_{\mathfrak{p}}^* \qquad \text{and} \qquad U_{\mathfrak{p}}^{(1)} = K_{\mathfrak{p},>0}.$$

Finally, if $\mathfrak{p}$ is complex, the only open subgroup of $K_\mathfrak{p}^*$ is the trivial subgroup $U_\mathfrak{p}^{(0)} = K_\mathfrak{p}^*$, which is generated by every open neighborhood of $1 \in K_\mathfrak{p}^* \cong \mathbf{C}^*$. With this notation, we have for each cycle $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ of K a subgroup

$$W_\mathfrak{f} = \prod_\mathfrak{p} U_\mathfrak{p}^{n(\mathfrak{p})} \subset J. \tag{9.2}$$

9.3. Proposition. *A subgroup of the idèle group J of K is open if and only if it contains $W_\mathfrak{f}$ for some cycle $\mathfrak{f}$ of K.*

Proof. As almost all exponents $n(\mathfrak{p})$ in (2.2) are equal to zero, the definition of the idèle topology shows that $W_\mathfrak{f}$ is an open subgroup of J. Conversely, if $H \subset J$ is an open subgroup of J, we must have $W_\mathfrak{f} \subset H$ for some $\mathfrak{f}$ as every open neighborhood of $1 \in J$ generates some $W_\mathfrak{f}$. □

► Ray classes as idèle classes

It follows from 2.2 that a subgroup of the *idèle class group* $C = J/K^*$ is open if and only if it contains the homomorphic image $D_\mathfrak{f}$ of some subgroup $W_\mathfrak{f} \subset J$. We have a canonical isomorphism $J/K^*W_\mathfrak{f} \xrightarrow{\sim} C/D_\mathfrak{f}$ for the quotients of the basic open subgroups $D_\mathfrak{f} \subset C$.

9.4. Theorem. *For every cycle $\mathfrak{f}$ of K there are isomorphisms*

$$J/K^*W_\mathfrak{f} \xrightarrow{\sim} C/D_\mathfrak{f} \xrightarrow{\sim} Cl_\mathfrak{f} = I(\mathfrak{f})/R(\mathfrak{f})$$

such that the class of a prime element $\pi_\mathfrak{p}$ at a finite prime $\mathfrak{p} \nmid \mathfrak{f}$ in $J/K^*W_\mathfrak{f}$ or $C/D_\mathfrak{f}$ corresponds to $\mathfrak{p}$ mod $R(\mathfrak{f})$ in $Cl_\mathfrak{f}$.

Proof. Write $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$, and define a map

$$\begin{aligned} \phi: \qquad J &\longrightarrow Cl_\mathfrak{f} = I(\mathfrak{f})/R(\mathfrak{f}) \\ (x_\mathfrak{p})_\mathfrak{p} &\longrightarrow \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(x^{-1}x_\mathfrak{p})} \bmod R(\mathfrak{f}), \end{aligned}$$

where $x \in K^*$ is an element that satisfies $x^{-1}x_\mathfrak{p} \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for all primes $\mathfrak{p}$ dividing $\mathfrak{f}$. Such an element exists by the approximation theorem, and it is uniquely determined up to multiplication by an element $y \in K^*$ satisfying $y \equiv 1 \bmod^* \mathfrak{f}$. By definition of $R(\mathfrak{f})$, the map ϕ is a well defined homomorphism. Its surjectivity is clear as a prime element $\pi_\mathfrak{p} \in J$ at a finite prime $\mathfrak{p} \nmid \mathfrak{f}$ is mapped to $\mathfrak{p}$ mod $R(\mathfrak{f})$. It remains to show that $\ker \phi = K^*W_\mathfrak{f}$.

Suppose we have $(x_\mathfrak{p})_\mathfrak{p} \in \ker \phi$. Then there exists $x \in K^*$ as above and $y \in K^*$ such that $y \equiv 1 \bmod^* \mathfrak{f}$ and

$$\prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(x^{-1}x_\mathfrak{p})} = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\operatorname{ord}_\mathfrak{p}(y)}.$$

This implies that $x_\mathfrak{p}(xy)^{-1}$ is a unit at all finite $\mathfrak{p}$ outside $\mathfrak{f}$ and satisfies $x_\mathfrak{p}(xy)^{-1} \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for $\mathfrak{p} | \mathfrak{f}$, so we have $(x_\mathfrak{p})_\mathfrak{p} \in xyW_\mathfrak{f}$. This proves the inclusion $\ker \phi \subset K^*W_\mathfrak{f}$. The other inclusion is obvious from the definition of ϕ. □

9.5. Corollary. *Every open subgroup of C is of finite index.*

Proof. Any open subgroup contains a subgroup $D_{\mathfrak{f}}$, which is of finite index in C by the finiteness of the ray class group $Cl_{\mathfrak{f}}$. □

If B is an ideal group and $\mathfrak{g}$ a modulus for B, we define the open subgroup $D_B \subset C$ corresponding to B as the kernel

$$D_B = \ker[C \longrightarrow I(\mathfrak{g})/B(\mathfrak{g})]$$

of the natural map induced by 2.3. We have a canonical isomorphism $C/D_B \xrightarrow{\sim} I(\mathfrak{g})/B(\mathfrak{g})$ that maps the class of a prime element $\pi_{\mathfrak{p}}$ at a finite prime $\mathfrak{p} \nmid \mathfrak{g}$ to $(\mathfrak{p} \bmod B(\mathfrak{g})$, and it follows from the definition of equivalence of ideal groups that D_B depends on B, but not on the choice of the modulus $\mathfrak{g}$.

9.6. Proposition. *The correspondence $B \mapsto D_B$ is an inclusion preserving bijection between the set of ideal groups of K and the set of open subgroups of the idèle class group C. The conductor $\mathfrak{f}$ of an ideal group B is the smallest cycle satisfying $D_{\mathfrak{f}} \subset D_B$.* □

From the obvious equality $D_{\mathfrak{f}_1} \cdot D_{\mathfrak{f}_2} = D_{\gcd(\mathfrak{f}_1,\mathfrak{f}_2)}$, we obtain as a simple corollary of the formalism a statement that required a proof in 1.8.

9.7. Corollary. *If an ideal group can be defined modulo $\mathfrak{f}_1$ and $\mathfrak{f}_2$, it can be defined modulo* $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$. □

▶ The kernel of the Artin map

Combining the bijection between open subgroups of C and ideal groups in 2.6 with the main theorem 1.9, we see that every finite abelian extension L/K corresponds to an open subgroup D_L of C for which there is an Artin isomorphism

$$C/D_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

that maps the residue classes of the prime elements $\pi_{\mathfrak{p}}$ mod D_L for finite unramified $\mathfrak{p}$ to the Artin symbol $(\mathfrak{p}, L/K)$.

In order to describe the subgroup D_L of the idèle class group corresponding to L, we need to define the norm $N_{L/K} : C_L \to C_K$ on idèle class groups. We know (cf. A.2) that there is an adèle norm $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ that is the ordinary field norm $N_{L/K} : L \to K$ when restricted to L. It can be given explicitly as

$$N_{L/K}((x_{\mathfrak{q}})_{\mathfrak{q}}) = (\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x_{\mathfrak{q}}))_{\mathfrak{p}}. \tag{9.8}$$

Here $\mathfrak{q}$ and $\mathfrak{p}$ range over the primes of L and K, respectively. The norm maps the unit group $J_L = \mathbb{A}_L^*$ into the unit group J_K and L^* into K^*, so we have an induced norm $N_{L/K} : C_L \to C_K$ on the idèle class groups.

We need to check that this norm corresponds to the norm on ideal class groups under the isomorphism 2.3. As in the previous section, we view a cycle $\mathfrak{f}$ of K as a cycle in a finite extension L when necessary, and use the obvious notation $W_{L,\mathfrak{f}} \subset J_L$ and $D_{L,\mathfrak{f}} \subset C_L$ for the corresponding subgroups in J_L and C_L. For a cycle $\mathfrak{f}$ of K we have $N_{L/K}[W_{L,\mathfrak{f}}] \subset W_{K,\mathfrak{f}}$ and $N_{L/K}[D_{L,\mathfrak{f}}] \subset D_{K,\mathfrak{f}}$.

9.9. Proposition. *Let L/K be a finite extension and $\mathfrak{f}$ a cycle of K. Then there is a commutative diagram*

$$\begin{array}{ccc} C_L/D_{L,\mathfrak{f}} & \xrightarrow{\sim} & I_L(\mathfrak{f})/R_L(\mathfrak{f}) \\ \big\downarrow{\scriptstyle N_{L/K}} & & \big\downarrow{\scriptstyle N_{L/K}} \\ C_K/D_{K,\mathfrak{f}} & \xrightarrow{\sim} & I_K(\mathfrak{f})/R_K(\mathfrak{f}) \end{array}$$

in which the horizontal isomorphisms are as in 2.3.

Proof. The commutativity of the diagram may be verified on prime elements $\pi_{\mathfrak{q}}$ at finite primes $\mathfrak{q}$ of L outside $\mathfrak{f}$, since these classes generate $C_L/D_{L,\mathfrak{f}}$. For such prime elements we have $N_{L/K}(\pi_{\mathfrak{q}}) = N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(\pi_{\mathfrak{q}})$ by 2.8, and by the definition of extension valuations we have $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(\pi_{\mathfrak{q}}) \cdot A_{\mathfrak{p}} = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$. It follows that the diagam commutes. □

9.10. Proposition. *Let L be a finite extension of K. Then there exists a cycle $\mathfrak{f}$ of K such that $D_{K,\mathfrak{f}}$ is contained in $N_{L/K}C_L$ and all primes dividing $\mathfrak{f}$ are ramified in L/K. In particular, $N_{L/K}C_L$ is open in C_K.*

Proof. With $[L : K] = n$, we have $N_{L/K}J_L \supset U_{\mathfrak{p}}^n$ for all primes $\mathfrak{p}$. As $U_{\mathfrak{p}}^n$ contains an open neighborhood of $1 \in U_{\mathfrak{p}}$, one has $U_{\mathfrak{p}}^n \supset U_{\mathfrak{p}}^{(k)}$ for some $k \in \mathbf{Z}_{>0}$. If $\mathfrak{q}|\mathfrak{p}$ is unramified, the identity

$$N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x + y\pi_{\mathfrak{p}}^k) = N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x) + \mathrm{Tr}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(y)\pi_{\mathfrak{p}}^k \bmod \mathfrak{p}^{k+1}A_{\mathfrak{p}}$$

for $x, y \in A_{\mathfrak{q}}$ and the surjectivity of the norm and trace map on the residue class field extension $k_{\mathfrak{p}} \subset k_{\mathfrak{q}}$ easily imply that we have $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[U_{\mathfrak{q}}] = U_{\mathfrak{p}}$. This proves our proposition, as it implies $N_{L/K}J_L \supset W_{K,\mathfrak{f}}$ for some $\mathfrak{f}$ divisible only by ramifying primes.

9.11. Theorem. *For any finite extension L/K there exists a cycle $\mathfrak{f}$ in K that is only divisible by ramifying primes and an isomorphism*

$$C_K/N_{L/K}C_L \xrightarrow{\sim} I(\mathfrak{f})/N_{L/K}I_L(\mathfrak{f}) \cdot R(\mathfrak{f})$$

that maps the class of $\pi_{\mathfrak{p}}$ to the class of $\mathfrak{p}$ for finite unramified $\mathfrak{p}$.

Proof. Take $\mathfrak{f}$ as in 2.10, then the isomorphism is obtained by taking cokernels in the diagram of 2.9. □

▶ Main theorem

We can now give the idèlic version of the main theorem of class field theory. Note that so far, none of the proofs in this section relied on the main theorem 1.9 or its corollaries.

9.12. Main theorem. *Let K be a number field, Σ_K the set of finite abelian extensions of K contained in some fixed algebraic closure and $\mathcal{D}$ the set of open subgroups of the idèle class group C of K. Then there exists an inclusion reversing bijection*

$$\Sigma_K \;\leftrightarrows\; \mathcal{D}$$

such that for an extension L/K corresponding to the subgroup D of C the following holds:

(1) *$D = N_{L/K}C_L$;*

(2) *there is a global Artin isomorphism $\psi_{L/K} : C/D \xrightarrow{\sim} \mathrm{Gal}(L/K)$ such that the image of a completion $K_\mathfrak{p}^*$ in C is mapped onto the decomposition group $G_\mathfrak{p}$ of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. It induces a local Artin isomorphism*

$$\psi_\mathfrak{p} : K_\mathfrak{p}^*/N_{L_\mathfrak{q}/K_\mathfrak{p}}L_\mathfrak{q}^* \xrightarrow{\sim} G_\mathfrak{p} = \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}) \subset \mathrm{Gal}(L/K)$$

for the local extension at $\mathfrak{p}$. If $\mathfrak{p}$ is finite, this local isomorphism maps the local unit group $U_\mathfrak{p}$ onto the inertia group $I_\mathfrak{p} \subset G_\mathfrak{p}$ and the class of a prime element $\pi_\mathfrak{p}$ at $\mathfrak{p}$ to the coset of the Frobenius automorphism in $G_\mathfrak{p}$.

The idèlic main theorem 2.12 is similar in content to 1.9, but it has several advantages over the older formulation. First of all, it does without the choice of defining moduli, thus avoiding the cumbersome transitions between equivalent groups. Secondly, it yields a description of the contribution of a prime $\mathfrak{p}$ that shows the local nature of this contribution. The statement in (2) is not a simple corollary of the identity $D = N_{L/K}C_L$ since it requires the non-trivial identity

$$K_\mathfrak{p}^* \cap (K^* N_{L/K} J_L) = N_{L_\mathfrak{q}/K_\mathfrak{p}} L_\mathfrak{q}^* \tag{9.13}$$

for the intersection of the subgroup $K_\mathfrak{p}^* \subset C$ with the kernel $N_{L/K}C_L$ of the global Artin map. From (2), we obtain a description of the conductor that can be used to actually compute it.

9.14. Corollary. *Let $\mathfrak{f}_{L/K} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ be the conductor of the abelian extension L/K. If $\mathfrak{q}$ is a prime of L that extends $\mathfrak{p}$, then $n(\mathfrak{p})$ is the smallest non-negative integer n for which the inclusion*

$$U_\mathfrak{p}^{(n)} \subset N_{L_\mathfrak{q}/K_\mathfrak{p}} U_\mathfrak{q}$$

is satisfied. □

As a supplement to 2.12, there are again the functorial diagrams occurring in 1.11. Both the statements and their derivation from the main theorem have an immediate translation in terms of the idèle class group, and we leave them to the reader.

▶ Local class field theory

The local Artin isomorphism, which occurs as a 'corollary' of the idèlic version of global class field theory, leads to a class field theory for local number fields that is interesting in its own right. This local theory can also be developed independently from the global theory, and one may argue that this in certain ways more natural. Our order of presentation however follows the history of the subject.

As we have formulated global class field theory for number fields only, and not for function fields of dimension 1 over finite fields (i.e. extensions of a finite field of transcendence degree 1), we obtain a local class field theory for local fields in characteristic 0 only. The theory in characteristic p is highly similar, even though some of the proofs have to be modified for extensions of degree divisible by the characteristic.

9.15. Proposition. *Let F be a finite extension of $\mathbf{Q}_p$ for some prime number p and E/F a finite abelian extension with group G. Then there is a canonical isomorphism*

$$\psi_{E/F}:\ F^*/N_{E/F}E^* \xrightarrow{\sim} G$$

that maps the unit group of the ring of integers of F onto the inertia group $I_{E/F}$ and a prime element onto the Frobenius residue class mod $I_{E/F}$.

Proof. We can choose number fields K and L that are dense in F and E, respectively, in such a way that L is G-invariant and $L^G = K$. This means that there are primes $\mathfrak{q}$ in L and $\mathfrak{p}$ in K such that $F = K_\mathfrak{p}$ and $E = L_\mathfrak{q}$, and $G_\mathfrak{p} = G$. The global Artin map for L/K now induces a local Artin isomorphism $\psi_{E/F}$ with the stated properties.

In order to prove the canonicity of $\psi_{E/F}$, we have to show that it does not depend on the choice of the G-invariant subfield $L \subset E$. Thus, let L' be another number field that is dense in E and stable under G. Replacing L' by LL' if necessary, we may assume that L is contained in L'. Then $K' = (L')^G$ contains K, and we have $F = K_\mathfrak{p} = K'_\mathfrak{r}$ for a prime $\mathfrak{r}|\mathfrak{p}$. The commutative diagram

$$\begin{array}{ccccc} K'_\mathfrak{r} & \longrightarrow & C_{K'}/N_{LK'/K'}C_{LK'} & \xrightarrow{\sim} & \mathrm{Gal}(LK'/K') \\ \big\downarrow{\scriptstyle \mathrm{id}} & & \big\downarrow{\scriptstyle N_{K'/K}} & & \big\downarrow{\scriptstyle \mathrm{res}} \\ K_\mathfrak{p} & \longrightarrow & C_K/N_{L/K}C_L & \xrightarrow{\sim} & \mathrm{Gal}(L/K); \end{array}$$

derived from 1.11 (4) shows that L'/K' and L/K induce the same Artin isomorphism for the extension E/F. □

The description of the local Artin isomorphism given by the preceding proposition is somewhat indirect as the map is induced by the Artin isomorphism of a 'dense global extension'. Only in the case of an unramified extension E/F the situation is very transparent, as in that case both $F^*/N_{E/F}E^*$ and $\mathrm{Gal}(E/F)$ have canonical generators, and they correspond under the Artin isomorphism. Only relatively recently, in 1985, Neukirch realized that that the local Artin map in the general case is *completely determined* by this fact and the functorial properties of the Artin symbol. We do not give the argument here.

9.16. Main theorem for local number fields. *Let F be a local number field, Σ_F the set of finite abelian extensions of F contained in some fixed algebraic closure and $\mathcal{H}$ the set of open subgroups of finite index of F^*. Then there exists an inclusion reversing bijection*

$$\Sigma_F \ \leftrightarrows \ \mathcal{H}$$

such that for an extension E/F corresponding to the subgroup H of F^* the following holds:
(1) *$H = N_{E/F}E^*$;*
(2) *there is an Artin isomorphism $\psi_{E/F} : F^*/H \xrightarrow{\sim} \mathrm{Gal}(E/F)$ such that, for non-archimedean F, the unit group U of the valuation ring of F is mapped onto the inertia group $I_{E/F}$ and a prime element is mapped into the Frobenius coset modulo $I_{E/F}$.*

Note that $N_{E/F}E^* \subset F^*$ in 2.16 is indeed an open subgroup of finite index, as it contains ${F^*}^n$ for $n = [E : F]$. We leave it to the reader to formulate the local functorial diagrams, which are analogous to those in 1.11.

The extension corresponding to an open subgroup H of finite index in F^* is called the *class field* of H. In the global case we have class fields corresponding to open subgroups of the idèle class group.

The global theorem 2.13 implies the existence of the Artin isomorphism in (2). The injectivity of the map $E \mapsto N_{E/F}E^*$ follows then easily, as an abelian extension F' with $N_{F'/F}{F'}^* = N_{E/F}E^*$ gives a vertical zero map in (4) that implies $E \subset F'$, whence $E = F'$ by symmetry. The surjectivity however is not obvious, and we will prove a *local existence theorem* in section 12 to show that every open subgroup $H \subset F^*$ has a class field. Apart from this independent statement, the local main theorem can be seen as a corollary of the global theorem. It is also possible, and to some extent more natural, to use the local case in order to prove the more complicated global theorem. For such an approach we refer to [7] or [9].

The next three sections will be devoted to the proof of the main theorem of class field theory. Section 10 introduces cyclic group cohomology in order to prove the norm-index inequality $[C_K : N_{L/K}C_L] \geq [L : K]$ for cyclic extensions L of a number field K. Section 11 proves the reverse inequality $[C_K : N_{L/K}C_L] \leq [L : K]$, which holds for arbitrary finite extensions L/K, by an explicit construction of idèle norms in suitable extensions. Section 12 combines the inequalities into a proof of Artin's reciprocity law and finishes all proofs by establishing the existence theorems in has a class field.

Exercises

1. Let $\mathfrak{p}$ be a prime of K and C the idèle class group of K. Show that the natural map $K_{\mathfrak{p}}^* \to C$ maps $K_{\mathfrak{p}}^*$ isomorphically to a closed subgroup of C. Is the analogous statement for the natural map $K_{\mathfrak{p}} \times K_{\mathfrak{p}'} \to C$ correct?

2. Let F be a non-archimedean local field and E/F a finite extension.
   a. Show that the norm map and the trace map for the residue class field extension $\overline{E}/\overline{F}$ are surjective.
   b. Suppose that E/F is unramified. Show that
   $$N_{E/F}[U_E^{(i)}] = U_F^{(i)} \qquad \text{for } i \geq 0.$$

3. Let L/K be a finite abelian extension of number fields and $x \in K^*$ an element that is contained in the local norm image $N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}[L_{\mathfrak{q}}]^* \subset K_{\mathfrak{p}}^*$ at all primes $\mathfrak{p} \neq \mathfrak{p}_0$ of K. Show that x is also a local norm at $\mathfrak{p}_0$.
   [Hint: use 9.14.]

4. Let L/K be a finite abelian extension of number fields with conductor $\mathfrak{f}_{L/K}$, and $\mathfrak{p}|p$ a finite prime of K. Denote by m the exponent to which $\mathfrak{p}$ appears in $\mathfrak{f}_{L/K}$, and let $e = e(\mathfrak{p}/p)$ be the ramification index of $\mathfrak{p}$ over the rational prime p. We write U_i for $U_{\mathfrak{p}}^{(i)}$ in this exercise. Prove the following assertions.
   a. If i, j are positive integers with $j \not\equiv 0 \bmod p$, then the map $U_i \to U_i$ sending every x to x^j is an isomorphism.
   b. For $i > e/(p-1)$ there is an isomorphism $U_i \to U_{i+e}$ sending every x to x^p.
   c. If j is a positive integer, then $(K_{\mathfrak{p}}^*)^j$ is an *open* subgroup of $K_{\mathfrak{p}}^*$, and it contains $U_{e'+ke}$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in j.
   d. If $K_{\mathfrak{p}} \subset E$ is a finite extension, then $N_{E/K_{\mathfrak{p}}}[E^*]$ is an open subgroup of $K_{\mathfrak{p}}^*$, and it contains $U_{e'+ke}$, with e' as in (c) and k the number of factors p in $[E : K_{\mathfrak{p}}]$.
   e. One has $m \leq e' + ke$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in $[L : K]$.
   f. More precisely, one has $m \leq e' + ke$, with e' as before, but with k now equal to the number of factors p in the exponent of the inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

5. Let $K = \mathbf{Q}(\sqrt{-3})$ and $L = K(\sqrt[3]{2})$. We write ζ_3 for the cube root of unity $(-1+\sqrt{-3})/2$ in K, and μ_3 for the subgroup of K^* generated by ζ_3. The unique primes of K lying over 2 and 3 are denoted by 2 and $\mathfrak{t}$, respectively.
   a. Prove that $K \subset L$ is cyclic of degree 3, and that the map $\epsilon\colon \mathrm{Gal}(L/K) \to \mu_3$ sending σ to $\sigma(\sqrt[3]{2})/\sqrt[3]{2}$ is a group isomorphism.
   b. Show that the conductor $\mathfrak{f}_{L/K}$ divides $2\mathfrak{t}^4$.
   c. Let $\mathfrak{p}$ be a finite prime of K not dividing $2\mathfrak{t}$, and let $\mathbf{N}\mathfrak{p}$ be the cardinality of its residue class field. Prove that $\epsilon((\mathfrak{p}, L/K))$ is the unique element of μ_3 that is congruent to $2^{(\mathbf{N}\mathfrak{p}-1)/3}$ modulo $\mathfrak{p}$.
   d. Show that L is the ray class field of K with modulus 6 $(= 2 \cdot \mathfrak{t}^2)$.

6. *(Euler's conjecture.)* Let $p \neq 3$ be a prime number. Show that 2 has a unique cube root in $\mathbf{F}_p$ if $p \equiv 2 \bmod 3$, and that we have

$$2 \text{ is a cube in } \mathbf{F}_p \Longleftrightarrow p = x^2 + 27y^2 \text{ with } x, y \in \mathbf{Z}$$

for primes $p \equiv 1 \bmod 3$.

7. Let a be an integer that is not a square. Show that a prime $p \nmid 2a$ can be written as $p = x^2 - ay^2$ if and only if p splits completely in the ring class field $R \supset \mathbf{Q}(\sqrt{a})$ corresponding to the order $\mathbf{Z}[\sqrt{a}]$.

8. Prove the following criterion, discovered by Euler, on the biquadratic character of 2 modulo a prime number $p \equiv 1 \bmod 4$:

$$2 \text{ is a fourth power in } \mathbf{F}_p \Longleftrightarrow p = x^2 + 64y^2 \text{ with } x, y \in \mathbf{Z}.$$

9. Derive the local Kronecker-Weber theorem 7.2 from the local main theorem 9.17.

10. Prove the local main theorem 9.17 for archimedean F. For non-archimedean F, show that the theorem holds for unramified extensions, i.e. show that there is an inclusion reversing bijection between unramified extensions E/F and subgroups of F^* containing U_F given by $E \mapsto N_{E/F}[E^*]$.

11. Let K be a local field and H a subgroup of K^*.
    a. Suppose the K is archimedean. Show that $[K^* : H]$ is finite if and only if H is open.
    b.
    b. Suppose that K is non-archimedean and $\mathrm{char}K = 0$. Show that $[K^* : H]$ is finite if and only if H is open and not contained in the unit group U_K of the valuation ring.
    c. Suppose that $\mathrm{char}K = p > 0$. Show that there exists a subgroup $H \subset K^*$ that is of finite index but not open.

12. Let K be an extension of $\mathbf{Q}_p$ with residue class field $\overline{K}$ of order q and L/K a totally ramified extension of degree coprime to $pq - p$. Show that the largest subextension M of L/K for which M/K is abelian is K itself, and that $N_{L/K}L^* = K^*$. Can you prove this without class field theory?

13. Let M be the splitting field of $X^4 - 17$ over $\mathbf{Q}_p$. Determine the subgroup $N_{M/\mathbf{Q}_p}M^* \subset \mathbf{Q}_p^*$ for $p = 2$, 3, 5, 17 and 149.

14. Let L/K be a *tamely* ramified abelian extension of local number fields. Prove directly (i.e. without using 9.17) that the order of the group $K^*/N_{L/K}L^*$ equals the degree $[L : K]$.

15. Show that the Artin isomorphisms $\psi_{E/F}$ in 9.17 for $E \subset F^{\mathrm{ab}}$ induce an injective homomorphism $\psi_F : F^* \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ of topological groups that fits in an exact diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_F & \longrightarrow & F^* & \xrightarrow{\mathrm{ord}} & \mathbf{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \psi_F} & & \downarrow{\scriptstyle \mathrm{can}} & & \\
0 & \longrightarrow & \mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{unr}}) & \longrightarrow & \mathrm{Gal}(F^{\mathrm{ab}}/F) & \longrightarrow & \mathrm{Gal}(F^{\mathrm{unr}}/F) & \longrightarrow & 0
\end{array}$$

Deduce that the image of ψ_F is dense.