VOORTGEZETTE GETALTHEORIE

P. Stevenhagen

Thomas Stieltjes Instituut
2002

Contents

1 Valuations

Valuation theory provides an approach to the arithmetic of number fields by methods reminiscent of those used in complex function theory. Here one employs the description of a meromorphic function as a function that can locally be expanded in a converging Laurent series. More precisely, one has a field $\mathcal{M}$ of meromorphic functions on $\mathbf{C}$ that is the field of fractions of the ring $\mathcal{O}$ of holomorphic functions on $\mathbf{C}$, and we can write any $f \in \mathcal{M}$ in a neighborhood of any point $\alpha \in \mathbf{C}$ in a unique way 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 meromorphic 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 $\mathcal{M}$. For instance, the rational function field $\mathbf{C}(X) \subset \mathcal{M}$ 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 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 $\mathcal{O}$, since every non-zero 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 $\mathcal{O}_K$ itself, and an element $x \in K^*$ is determined up to multiplication by an element in $\mathcal{O}^*$ 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 still have to specify which coefficients a_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. Such a notion is provided by the $\mathfrak{p}$-adic valuation on K, and this section is meant to introduce such valuations. In Theorem 2.6, we will see that this leads to a $\mathfrak{p}$-adic expansion of the elements 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 $x, y \in K$.*

The smallest constant C that can be taken in (3) is the *norm* of the valuation ϕ. It obviously cannot be smaller than 1. Note that if ϕ is a valuation on K of norm C, then $x \mapsto \phi(x)^r$ defines a valuation of norm C^r on K for each $r \in \mathbf{R}_{>0}$.

The two 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 these valuations equals 1. The value of the constant c in the definitions 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 (1.3) holds, a sum of small elements will never be large, so in this case the Archimedean postulate, which states that a non-zero quantity becomes arbitrarily large when repeatedly added to itself, does not hold. If ϕ is non-archimedean and $\phi(x_1) \neq \phi(x_2)$, the ultrametric inequality can be strengthened to the equality

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

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 $\phi(x_1 + x_2) = \phi(x_1)$. The identity $\phi(-1) = 1$ 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*

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

and this has amusing consequences for the geometry of the underlying space (exercise 7). A trivial example of a non-archimedean valuation that exists on any field K is the *trivial valuation* on K, which is identically 1 on K^*.

Exercise 1. Show that every valuation on a finite field is trivial.

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

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

Valuations of this form have norm 2 and satisfy the triangle inequality. In fact, there is the following simple relation between norm and triangle inequality. It implies that every valuation satisfies the triangle inequality when raised to a suitable power.

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, suppose that the valuation ϕ on K has norm $C \leq 2$. By induction, this yields $\phi(\sum_{i=1}^{2^m} x_i) \leq 2^m \max_i \phi(x_i)$. 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 $\phi(x+y) \leq \sqrt[n]{4(n+1)}(\phi(x)+\phi(y))$ 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 1.3 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. □

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 T_ϕ on K in which a basis of open neighborhoods of a point $x \in K$ is given by the collection of open balls

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

of radius ε around x. As all powers of ϕ induce the same topology, the topology T_ϕ is metrizable by 1.4.

Exercise 2. Show that T_ϕ 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 T_ϕ on K makes K into a *topological field*. As we will see, non-archimedean topological fields are topologically rather different from the archimedean topological fields such as $\mathbf{R}$ and $\mathbf{C}$.

Two valuations ϕ and ψ on a field K are said to be *equivalent* if they induce the same topology on K. For non-trivial valuations 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 T_ϕ is stronger than T_ψ;*
(4) *$\phi(x) < 1$ implies $\psi(x) < 1$ for all $x \in K$.*

Proof. The implications (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (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) $\Rightarrow$ (4).

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

An equivalence class of non-trivial valuations on K is known as a *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 following.

1.9. Ostrowski's theorem. *Every non-trivial valuation on the rational number field* $\mathbf{Q}$ *is either equal to 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 prime number p *or to a power*

$$\phi_\infty(x) = |x|^\alpha \qquad \textit{with} \;\; \alpha > 0$$

of the ordinary absolute value on $\mathbf{Q}$.

Proof. Let ϕ be a non-trivial non-archimedean valuation on $\mathbf{Q}$. Then it is bounded by 1 on $\mathbf{Z}$, and we easily check that $\mathfrak{p} = \{x \in \mathbf{Z} : \phi(x) < 1\}$ is 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 $k = \mathrm{ord}_p(x) \in \mathbf{Z}$, we find $\phi(x) = c^{\mathrm{ord}_p(x)}$ with $c = \phi(p) \in (0,1)$.

Suppose now that ϕ is an archimedean valuation on $\mathbf{Q}$. We may assume that it satisfies the triangle inequality, so that $\phi(k) \le |k|$ for $k \in \mathbf{Z}$. Given two integers $m, n > 1$, we can write all powers of n in base m 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 $s/t \le \log m/\log n$. The triangle inequality implies $\phi(m)^t \le (s+1)n \max\{1, \phi(n)^s\}$, so we can take t-th roots and let t tend to infinity to obtain the estimate

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

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 $\phi(m)^{1/\log m} \le \phi(n)^{1/\log n}$ 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 $\phi(n) = |n|^{\log a}$ for all $n \in \mathbf{Z}$. This implies $\phi(x) = |x|^\alpha$ for all $x \in \mathbf{Q}$, with $\alpha = \log a > 0$. □

Exercise 3. Show that the norm of a valuation ϕ on a field K equals $\max\{\phi(1), \phi(2)\}$.

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

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

is a subring of K, the *valuation ring* of ϕ. We have $x \in A_\phi$ or $x^{-1} \in A_\phi$ for every $x \in K^*$. The valuation ring A_ϕ is a local ring with maximal ideal

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

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

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

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

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

Proof. If ϕ is a non-archimedean valuation on a number field K, then the ring of integers $\mathcal{O}$ is contained in the valuation ring A_ϕ. To see this, one observes that every $x \in \mathcal{O}$ 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, the ideal $\mathfrak{m}_\phi \cap \mathcal{O}$ is a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, and ϕ is identically 1 on $\mathcal{O}\backslash\mathfrak{p}$. The local ring $\mathcal{O}_\mathfrak{p}$ 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 $\mathfrak{p} \subset \mathcal{O}$. □

If $K = F(X)$ is the field of rational functions over a field F, the argument used in proving 1.10 yields the following.

1.11. 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 $c = \phi(X^{-1})$. □

If F is finite, then *all* valuations of $F(X)$ are trivial on F and 1.11 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 1.11 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 idèles. 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 valuations ϕ_P: it also corresponds to a finite prime of $F(X)$. Number fields are different from function fields in the sense that they have truely infinite primes, i.e., non-archimedean primes. We will see that these come from the valuations of the type given in (1.4), but as it requires extra arguments to show this, the complete description of the infinite primes of a number field will only be given in 2.4.

The proofs of 1.9, 1.10 and 1.11 show that non-archimedean valuations on K often come from discrete valuation rings $R \subset K$, and given their name it is of course no surprise that such rings provide valuations on their field of fractions. To make the terminology even more natural, 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 1.9 that $\phi[K^*]$ contains the dense subgroup $\phi[\mathbf{Q}^*] \subset \mathbf{R}_{>0}$. The following proposition shows that discrete valuation rings are indeed the valuation rings coming from non-trivial discrete valuations.

1.12. 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 4), 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 *local parameter* at the corresponding prime. Every choice of π leads to a splitting of the natural exact sequence $0 \to A^* \to K^* \xrightarrow{\nu} \mathbf{Z} \to 0$ induced by the normalized (exponential) valuation $\nu : K \to \mathbf{Z} \cap \{\infty\}$ on the discrete valuation ring A, i.e. to an isomorphism

$$K^* = \langle \pi \rangle \times A^*.$$

A fundamental system of neighborhoods of the zero element in K is given by the integral powers $\pi^k A$ of the maximal ideal of K. Analogously, the subgroups $1 + \pi^k A \subset K^*$ form a fundamental system of neighborhoods of the unit element in K^* 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

4. 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 $[h_1][h_2] = [h_1h_2]$ for $h_1, h_2 \in H$. For non-zero $x \in F[H]$ we set

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

   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?

5. 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.

6. 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.

7. Let K be a field and ϕ a non-archimedean valuation on K. Show that the metric space K (with distance function given by $d(x, y) = \phi(x - y)$) has the following properties.
   a. Every triangle in K is isosceles, i.e. given three points $x, y, z \in K$ there is one that has equal distances to the two others;
   b. Every point x in the open ball $U(x_0, \varepsilon)$ of radius ε around $x_0 \in K$ is a center, i.e. $U(x, \varepsilon) = U(x_0, \varepsilon)$ for such x.

8. *(Independence of inequivalent valuations.)* Let K be a field and $\phi_1, \phi_2, \ldots, \phi_n$ pairwise inequivalent valuations on K.
   a. Show that there exists a sequence $\{x_k\}_k$ in K that converges to 0 in the topology T_{ϕ_1} and to 1 in the topologies T_{ϕ_i} with $i \geq 2$.
   [Hint: use 1.8 to set $x_k = a^k/(1 + a^k)$ for suitable a.]
   b. Let K_i be the field K with topology T_{ϕ_i} and $\tau : K \to \prod_{i=1}^n K_i$ the diagonal embedding of K in $\prod_{i=1}^n K_i$. Show that the image of K is dense. (This result is known as the *weak approximation theorem.*)
   [Hint: Show that the closure of the diagonal $\tau[K]$ in $\prod_{i=1}^n K_i$ is a K-subspace containing the standard basis.]
   c. Is the result in b necessarily correct for an *infinite* set of valuations?

9. Let $\phi_1, \phi_2, \ldots, \phi_n$ be pairwise inequivalent non-archimedean valuations on a field K. Prove that for all $x_1, x_2, \ldots, x_n \in K^*$, there exists $x \in K^*$ such that $\phi_i(x) = \phi_i(x_i)$ for $i = 1, 2, \ldots, n$.

10. Does there exist a field K and a non-trivial valuation ϕ on K such that the implication

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

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

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

12. Let ϕ be a non-trivial discrete valuation on a field K, and denote by A and $\mathfrak{p}$ the valuation ring of ϕ and its maximal ideal. Let k be a positive integer, and set $U_r = 1 + \mathfrak{p}^r$ for $r \in \mathbf{Z}_{>0}$. Show that $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ is a 1-dimensional vector space over the residue class field k_ϕ, and that the map $x \mapsto x - 1$ induces a group isomorphism $U_k/U_{k+1} \xrightarrow{\sim} \mathfrak{p}^k/\mathfrak{p}^{k+1}$.

13. Let ϕ be a non-archimedean valuation on a field K. For every positive real constant c, we define the function $\psi_c : K[X] \to \mathbf{R}_{>0}$ on the polynomial ring over K by $\psi_c(\sum_i a_i X^i) = \max_i \phi(a_i)c^i$. Show that ψ_c gives rise to a valuation on the rational function field $K(X)$ that extends ϕ, and that the valuations ψ_{c_1} and ψ_{c_2} are not equivalent for ϕ non-trivial and $c_1 \neq c_2$. Which prime divisors are obtained when ϕ is trivial on K?

14. *(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?

15. *(Product formula.)* Show that the product $\prod_P \phi_P(x)$ over all prime divisors P of $\mathbf{Q}$ is well defined for $x \in \mathbf{Q}^*$, and that for a suitable choice of ϕ_P the value is equal to 1 for all $x \in \mathbf{Q}^*$.

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 $\sigma = \tau$ or $\sigma = \overline{\tau}$.

2 Completions

As is well known from analysis, the right setting to study functions defined over the rational number field $\mathbf{Q}$ is not the field $\mathbf{Q}$ 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.

A valued field K is said to be *complete* if every Cauchy sequence in K has a limit in K. Given a field K with valuation ϕ, we will construct the completion $K_\phi \supset K$ of K with respect to ϕ. The construction is similar to the construction of $\mathbf{R}$ from $\mathbf{Q}$. Note however that the general construction of K_ϕ uses the existence of the complete field $\mathbf{R}$ containing the values of ϕ.

2.1. Theorem. *Let ϕ be a valuation on a field K. Then there exists a field extension K_ϕ of K and an extension of ϕ to a valuation on K_ϕ such that K_ϕ is complete in the valuation topology and contains 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. The construction of K_ϕ from K is similar to Cantor's construction of the real numbers from $\mathbf{Q}$. One takes $\mathfrak{R}$ to be the ring of Cauchy sequences in K with componentwise addition and multiplication. The ideal

$$\mathfrak{m} = \{(a_i)_{i=1}^\infty \in \mathfrak{R} : \lim_{i\to\infty} \phi(a_i) = 0\}$$

consisting of all null-sequences in $\mathfrak{R}$ is a maximal ideal, and we set $K_\phi = \mathfrak{R}/\mathfrak{m}$.

For each sequence $(a_i)_{i=1}^\infty \in \mathfrak{R}$ the sequence $(\phi(a_i))_{i=1}^\infty$ is convergent in $\mathbf{R}$, so we can define $\overline{\phi} : K_\phi \to \mathbf{R}_{\geq 0}$ by setting

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

This is easily checked to be a valuation on K_ϕ, and, if we view K as the subfield of K_ϕ consisting of the residue classes of the constant sequences $(a)_{i=1}^\infty$ with $a \in K$, the valuation $\overline{\phi}$ extends ϕ. Note that K is dense in K_ϕ as every element $(a_i)_{i=1}^\infty \bmod \mathfrak{m}$ of K_ϕ is the limit of the sequence $(a_i)_{i=1}^\infty$ with elements 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. The sequence $x = (a_i)_{i=1}^\infty$ is then 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, then 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. □

The last statement in the theorem 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 a power of the ordinary absolute value, contains the real number field $\mathbf{R}$ as a topological subfield. In fact, complete archimedean fields cannot be much larger.

2.2. Theorem (Ostrowski). *Let K be a complete archimedean field and $\mathbf{R} \subset K$ the closure of the prime subfield $\mathbf{Q} \subset K$ in K. Then we have $K = \mathbf{R}$ or $K = \mathbf{R}(\sqrt{-1}) = \mathbf{C}$.*

Proof. We first show that the valuation ϕ on K can be extended to $K(\sqrt{-1})$, and that $K(\sqrt{-1})$ is complete under this valuation. This extension statement is clear when K contains $\sqrt{-1}$, so assume that $L = K(\sqrt{-1})$ is quadratic over K. We will assume that ϕ satisfies the triangle inequality, and define $\psi : L \to \mathbf{R}_{\geq 0}$ by the familiar formula

$$\psi(a + b\sqrt{-1}) = \sqrt{\phi(a^2 + b^2)}.$$

This is a multiplicative function, and it is non-zero outside 0 because $a^2 + b^2 = 0 \in K$ only occurs for $a = b = 0$. In order to show that ψ is a valuation on L, we have to show that $\psi(1 + x)$ remains bounded for $\psi(x) < 1$. This comes down to showing that $\phi(a)$ and $\phi(b)$ are bounded when $a, b \in K$ satisfy $\phi(a^2 + b^2) < 1$. Indeed, if one of them, say $\phi(a)$, is unbounded, the inequality $\phi(1 + (b/a)^2) < \phi(a)^{-2}$ shows that we can construct $x_n \in K$ satisfying $\phi(1 + x_n^2) < 4^{-n}$. We then have

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

by the triangle inequality, and upon changing the sign of x_{n+1} where necessary we obtain $\phi(x_{n+1} - x_n) < 2^{-n}$ for all $n \geq 1$. The limit x of the Cauchy sequence $(x_n)_n$ is an element of K by completeness and satisfies $x^2 + 1 = 0$, contrary to the assumption $\sqrt{-1} \notin K$.

We have now shown that $L = K(\sqrt{-1})$ is a complete archimedean field, and as it contains $\mathbf{R}(\sqrt{-1}) = \mathbf{C}$ as a subfield we can finish the proof by showing that L is in fact equal to $\mathbf{C}$.

Suppose that there exists an element $\alpha \in L$ that is not contained in the subfield $\mathbf{C}$. The function $\mathbf{C} \to \mathbf{R}$ defined by $z \mapsto \psi(z - \alpha)$ is then 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 the inequality

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

for all integers $n \geq 1$. Letting n tend to infinity we conclude that $\psi(z - \alpha) = r$ whenever $\psi(z - z_0) < r$ holds. 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. □

2.3. Corollary. *Let ϕ be an archimedean valuation on a field K. Then there exists an embedding $\sigma : K \to \mathbf{C}$ such that $\phi(x) = |\sigma(x)|^\alpha$ for some $\alpha \in \mathbf{R}_{>0}$.*

Proof. The two preceding theorems show that we have an embedding $\sigma : K \rightarrowtail \mathbf{C}$ of topological fields, so the topology T_ϕ coincides with the topology of the valuation ϕ_σ induced by σ. By 1.8, this implies $\phi = \phi_\sigma^\alpha$. □

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 1.10.

2.4. Corollary. *The infinite prime divisors of a number field K correspond bijectively to the embeddings $\sigma : K \to \mathbf{C}$ when complex conjugate embeddings are identified.*

We see that in contrast to 1.10, a number field has only finitely many archimedean prime divisors. Under suitable normalizations, there is a product formula as for the rational number field (exercise 16).

As there is a wide variety of complete non-archimedean fields, there is no classification result for these fields that has the simplicity of 2.2. However, most of the complete fields one encounters in practice have additional properties as discreteness of the valuation or finiteness of the residue class field, and for such fields there are many strong results. A general structure result for fields that are complete with respect to a discrete valuation is found in exercise 19.

We begin with the basic fact that the value group $\phi[K]$ and the residue class field $\overline{K} = k_\phi$ of a non-archimedean valuation ϕ do not change under completion.

2.5. 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 gives $\phi(a) = \phi(a - x + x) = \phi(x)$. If $x \in K_\phi^*$ satisfies $\phi(x) \leq 1$ and $a \in K$ is chosen such $\phi(a - x) < 1$, then we have $\overline{a} = \overline{x} \in \overline{K_\phi}$. □

We are now ready to prove that every element in a discretely valued field can be expanded as a convergent power series in a 'local parameter' π. This is the theorem that was announced in the previous section. In view of the application of this theorem in 3.7, we prove a slightly more general version in which the powers π^k are replaced by arbitrary elements π_k that generate the same ideal as π^k.

2.6. Theorem. *Suppose that K is a field that is complete with respect to a discrete valuation, A the corresponding valuation ring and $\mathfrak{p}$ the maximal ideal of A. Let $\pi_k \in K$ be a generator of $\mathfrak{p}^k$ and $S \subset A$ a set of representatives of A modulo $\mathfrak{p}$ containing 0. Then every $x \in K$ can uniquely be written as a convergent series*

$$\sum_{k=-\infty}^{\infty} a_k \pi_k$$

with coefficients $a_k \in S$ that are equal to zero for k small. The valuation ring A consists of those $x \in K$ that have $a_k = 0$ for all $k < 0$.

Proof. If $(a_k)_{k \geq N}$ with $N \in \mathbf{Z}$ is any sequence in S, then the sum $\sum_{k \geq N} a_k \pi_k$ converges in K as its terms tend to 0 (cf. exercise 18). Moreover, its value x is in the closed subset $\mathfrak{p}^N \subset K$ as all partial sums are. By the same argument we have $x - a_N \pi_N \in \mathfrak{p}^{N+1}$, so the ultrametric inequality shows that $\phi(x) = \phi(\pi_N)$ when $a_N \neq 0$. In particular $\sum_{k \geq N} a_k \pi_k$ is integral if and only if $a_k = 0$ for all $k < 0$. We also obtain the uniqueness of our expansions, for the difference $\sum_{k=-\infty}^{\infty} a_k \pi_k - \sum_{k=-\infty}^{\infty} b_k \pi_k$ of two distinct expansions has non-zero valuation $\phi(\pi_N)$ with $N = \min\{k : a_k \neq b_k\}$.

It remains to be proved that every $x \in K$ has an expansion of the required form. Replacing x by $\pi^n x$ for some n if necessary, we may assume that x is integral. Let a_0 be the unique element in S for which $x \equiv a_0 \bmod \mathfrak{p}$. Then we have $x = a_0 + \pi_1 x_1$ with $x_1 \in A$, so 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 $x \equiv \sum_{k=0}^{n} a_k \pi_n \bmod \mathfrak{p}^{n+1}$, whence $x = \sum_{k=0}^{\infty} a_k \pi_n$. □

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 2.5. If π is a generator of $\mathfrak{p}$, we can take $\pi_k = \pi^k$ to obtain a power series in the local parameter π.

Before we study some examples of complete non-archimedean fields in more detail, we prove a fundamental result on the lifting of factorizations of polynomials over the residue class field to factorizations over the complete field. There are several versions of this result that all go under the same name.

2.7. 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 to polynomials $g, h \in A[X]$ as we have congruences $g_k \equiv g_{k-1} \bmod \pi^{2^k} A[X]$ and $h_k \equiv g_{k-1} \bmod \pi^{2^k} A[X]$, and this 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 of f modulo $\pi^2 A[X]$. Writing $f = g_0 h_0 + \pi r_0$ for some $r_0 \in A[X]$, we see that we have to achieve a congruence relation

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

We have by assumption $a_0 g_0 + b_0 h_0 \equiv 1 \bmod \pi A[X]$, and we take $u \in A[X]$ to be the polynomial of degree smaller than $s = \deg(g_0)$ that satisfies $u \equiv b_0 r_0 \bmod g_0 A[X]$. 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.

2.8. Corollary. *Let $f \in A[X]$ be a polynomial. Then every simple zero of $\overline{f} = f \bmod \mathfrak{p}[X]$ 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.

Most of the non-archimedean complete fields we will encounter in the sequel are complete with respect to a discrete prime divisor. All completions with respect to the valuations on the function field $F(X)$ mentioned in theorem 1.9 are of this kind, see exercise 21. Another basic example is provided by the completions with respect to the p-adic valuations on $\mathbf{Q}$ in theorem 1.10 or, more generally, the $\mathfrak{p}$-adic valuations on an arbitrary number field K in theorem 1.10.

The completions of $\mathbf{Q}$ under the p-adic valuations from 1.9 are the p-adic number fields $\mathbf{Q}_p$. 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 choice $\pi_k = p^k$ and $S = \{0, 1, 2, \ldots, p-1\}$ in theorem 2.6 for $K = \mathbf{Q}_p$, 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 p-adic 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. A detailed description of the procedure is found in [5]. 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. We finally observe that 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).

Let A be a discrete valuation ring with maximal ideal $\mathfrak{p} = \pi A$ and $x \in A$ an element. Then theorem 2.6 implies that the element x is completely determined by the sequence of residues $x_n = (x \bmod \mathfrak{p}^n) \in A/\mathfrak{p}^n$ for $n \geq 1$. We therefore have an injective ring homomorphism $A \rightarrowtail \prod_{n \geq 1} A/\mathfrak{p}^n$ that sends x to $(x_n)_n$. It is obviously not surjective, since every element $(x_n)_n$ in the image satisfies the following property: for any two integers $i \geq j \geq 1$ the natural map $f_{i,j} : A/\mathfrak{p}^i \to A/\mathfrak{p}^j$ maps x_i to x_j. It is easy to see that the subset of elements of $\prod_{n \geq 1} A/\mathfrak{p}^n$ satisfying this property is actually a *subring* of $\prod_{n \geq 1} A/\mathfrak{p}^n$. It is known as the *projective limit* $\lim_{\leftarrow n} A/\mathfrak{p}^n$ of the rings $A/\mathfrak{p}^n$ with respect to the system of homomorphisms $\{f_{i,j}\}_{i \geq j}$. If we know that A is complete in the valuation topology, theorem 2.6 tells us that A is isomorphic to the projective limit. In general, we can view the projective limit $\lim_{\leftarrow n} A/\mathfrak{p}^n$ as the completion of the discrete valuation ring A with respect to the $\mathfrak{p}$-adic valuation.

The construction of the projective limit above is a special case of a categorical construction. Take any collection of sets X_i labelled by indices i from an index set I, and assume that I is *partially ordered* and *directed*. This means that there is a binary relation $\geq$ on I such that
(1) $i \geq i$ for all $i \in I$;
(2) $i \geq j$ and $j \geq k$ imply $i \geq k$;
(3) $i \geq j$ and $j \geq i$ imply $i = j$;
(4) for all $i, j \in I$ there exists $k \in I$ such that $k \geq i$ and $k \geq j$.
We suppose that we have a map $f_{ij} : X_i \to X_j$ whenever $i \geq j$, and that $f_{jk} \circ f_{ij} = f_{ik}$ whenever $i \geq j \geq k$. The projective limit of the X_i with respect to maps f_{ij} is defined as

$$X = \lim_{\leftarrow i \in I} X_i = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i : f_{ij}(x_i) = x_j \text{ whenever } i \geq j\}.$$

If all X_i are groups (rings, modules) and the f_{ij} homomorphisms, then the projective limit X is again a group (ring, module). If all X_i carry a topology, then $\prod_{i \in I} X_i$ has a product topology and we give X the relative topology.

A case of special importance arises when all X_i are finite groups and the f_{ij} homomorphisms. If we give all X_i the discrete topology and X the relative topology, then a basis for the topology on X is given by the open sets of the form

$$X \cap (\prod_{i \in I_0} \{x_i\} \times \prod_{i \notin I_0} X_i)$$

with $I_0 \subset I$ finite. These sets are also closed, so X is *totally disconnected*. As the group operations $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous maps, X is a topological group. It is called a *profinite group*. Being a closed subgroup of the product group $\prod_{i \in I} X_i$, which is compact by Tychonov's theorem, any profinite group is *compact*.

If G is any group, we can take for I the collection of normal subgroups N of finite index in G, ordered by inclusion: $N \geq N' \iff N \subset N'$. Taking for X_N the quotient group G/N and for $f_{NN'}$ the canonical homomorphism, we obtain the *profinite completion* $\widehat{G}$ of G. For $G = \mathbf{Z}$, the profinite completion is the *ring of profinite numbers*

$$\widehat{\mathbf{Z}} = \lim_{\leftarrow n > 0} \mathbf{Z}/n\mathbf{Z}.$$

Here the set of integers $n > 0$ is ordered by divisibility. As all finite groups $\mathbf{Z}/n\mathbf{Z}$ are in fact rings, this is an example of a *profinite ring* (definition left to the reader). Natural examples of profinite groups occur in infinite Galois theory, where the Galois group of an infinite algebraic extension L/K is defined as a projective limit $\mathrm{Gal}(L/K) = \lim_{\leftarrow} \mathrm{Gal}(L_i/K)$ of the Galois groups of the finite normal subextensions L_i/K of L/K with respect to the natural restriction maps.

If A is a discrete valuation ring with residue class field $A/\mathfrak{p}$, we can form its completion

$$\widehat{A} = \lim_{\leftarrow n > 0} A/\mathfrak{p}^n$$

with the set of integers being totally ordered in the usual way. This is a ring containing A, and it follows from 2.6 that itis equal to A if and only if A is complete in the valuation topology. If $A/\mathfrak{p}$ is finite, the completion $\widehat{A}$ is a profinite ring and therefore compact. If we assume in addition that A is complete, the basic neigborhoods $\mathfrak{p}^n = \pi^n A$ of $0 \in A$ are isomorphic to $A = \widehat{A}$ as topological groups and therefore compact. The field of fractions K of A is then *locally compact* in the valuation topology coming from the $\mathfrak{p}$-adic valuation. In general, a field with a non-trivial valuation ϕ is said to be a *local field* if K is locally compact in the topology T_ϕ.

If K is a number field and $\mathfrak{p}$ a non-zero prime of its ring of integers $\mathcal{O}$, the local ring $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring [I, §4] with finite residue class field. In this case the completion $\widehat{\mathcal{O}_\mathfrak{p}}$ is the valuation ring of the completion $K_\mathfrak{p}$ of K with respect to the $\mathfrak{p}$-adic valuation. For example, the ring $\mathbf{Z}_p = \lim_{\leftarrow n} \mathbf{Z}/p^n\mathbf{Z}$ is the completion of the local ring $\mathbf{Z}_{(p)} \subset \mathbf{Q}$. We will often refer to non-archimedean completions of number fields as $\mathfrak{p}$-*adic fields*. It follows from results in the next section that they are exactly the finite extensions of the p-adic fields $\mathbf{Q}_p$.

All completions of number fields at non-trivial valuations are examples of local fields. Conversely, one can show that every local field F of characteristic zero is of this form. This is clear if F is archimedean, see exercise 19. For non-archimedean F, one can show that F is a finite extension of either $\mathbf{Q}_p$ or the field $\mathbf{F}((X))$ of Laurent series over a finite field $\mathbf{F}$.

Exercises

1. Let K be a field complete with respect to a non-archimedean valuation. Show that a sum $\sum_{n\geq 1} a_n$ of elements in K is convergent in K if and only if $\lim_{n\to\infty} a_n = 0$, and that the value of a convergent sum is the same for every ordering of the terms.

2. Let K be a local field and ϕ the valuation on K. Show that K is topologically isomorphic to $\mathbf{R}$ or $\mathbf{C}$ if ϕ is archimedean, and that for ϕ non-archimedean K is complete, ϕ is discrete and $\overline{K}$ is finite.

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. Apply 2.2 or 2.3 to 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 13.)

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. Show that there is an isomorphism of topological rings $\widehat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p$.

16. *(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.

17. 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.]

18. 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.]

19. 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.

20. Let F be a field and $f \in F[X]$ an irreducible separable polynomial with residue class field $E = F[X]/(f)$. Show that the completion of the function field $F(X)$ with respect to the valuation ϕ_f defined in 1.9 is topologically isomorphic to the field $E((Y))$ of Laurent series over E.

21. 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.

22. Let A be a local ring with residue class field k, and let $g, h \in A[X]$. Suppose that g is monic, and that the images of g and h in $k[X]$ are coprime. Prove that $gA[X] + hA[X] = A[X]$.

23. Let R be a complete discrete valuation ring with residue class field F. Show that there is an isomorphism of topological spaces $R \cong \prod_{i \geq 0} F$. Deduce that R is compact if and only if F is finite.

3 Extending valuations

In this section, we will see how a valuation ϕ on a field K can be extended to a finite algebraic extension L of K.

If L/K is purely inseparable, then the extension problem is trivial since we have $x^{[L:K]} \in K$ for every $x \in L$ and consequently 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.

We are left with the problem of extending ϕ to the maximal separable subextension L_s of L over K. The most interesting case will be the case in which ϕ is non-archimedean, as the extension theory will then give a topological approach to the factorization of ideals from Dedekind domains in extension rings as treated in [I, §4]. However, there is no need to restrict to this case, so we merely assume that ϕ satisfies the triangle inequality on K.

Recall that 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 $k \in K$. 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 $x \in V$. 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 V is a finite field extension of K, then every extension valuation ψ of ϕ to V is a vector norm.

We first treat the case that K is complete with respect to ϕ.

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 $n = \dim_K V$ (exercise *). 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 $s \in S$. □

It follows from 1.8 that there can be at most one extension of a valuation ϕ on a complete field K to a finite extension L of K. 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

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

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 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.* □

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 [I, §4 and §7] 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 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 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 $\overline{L}$ over 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 9). 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

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

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 $0 \le k < e(\psi/\phi)$. Theorem 2.6 shows that any $x \in A_\psi$ has a unique representation

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

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).

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 K be a field with valuation ϕ and L a finite separable 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 [I, theorem 4.1 and 7.1]. For the details we refer to exercise 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 [I, Theorem 4.2] from the theory of extensions of Dedekind rings. The separability assumption cannot be omitted here.

3.10. 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.

3.11. 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 14.]

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 $\varphi(x_i) = \max\{\varphi(x_j) : 1 \le j \le n\}$.
   a. Prove that any sequence v_1, v_2, …, 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 ϕ be a valuation on a field K and let Ω be an algebraic closure of the completion K_ϕ.
   a. Show that the valuation on K_ϕ has a unique extension ψ to Ω and that $\psi \circ \sigma = \psi$ for all $\sigma \in G = \mathrm{Aut}_{K_\phi}(\Omega)$.
   b. Let L/K be a finite extension. Show that Gacts naturally on the set $\mathrm{Hom}_K(L, \Omega)$, and that the G-orbits correspond bijectively to the extension valuations of ϕ on L. What is the length of the orbit corresponding to ψ?
   c. Suppose that ϕ is discrete and let L be as in b. Show that we have

$$\sum_{\psi|\phi} \frac{[L : K]_{\mathrm{ins}}}{[L_\psi : K_\phi]_{\mathrm{ins}}} e(\psi/\phi) f(\psi/\phi) = [L : K]$$

   with $[L : K]_{\mathrm{ins}}$ and $[L_\psi : K_\phi]_{\mathrm{ins}}$ the degrees of inseparability of the extensions L/K and L_ψ/K_ϕ.

7. Let ϕ be a valuation on a field K and L a finite extension of K. Show that the natural homomorphism $K_\phi \otimes_K L \to \prod_{\psi|\phi} L_\psi$ is surjective, and that the maximal ideals of $K_\phi \otimes_K L$ correspond bijectively to the extensions ψ of ϕ to L. Show also that the image of $L = 1 \otimes L$ is dense in $\prod_{\psi|\phi} L_\psi$.

8. 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 $\prod_{\psi|\phi} A_\psi$.

9. 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

$L = K(\sqrt{3})$ is a quadratic extension of K, and that the unique extension valuation ψ of ϕ to L satisfies $e(\psi/\phi) = f(\psi/\phi) = 1$.

10. *(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 $\overline{K}[X]/(\overline{g}_i)$.]

11. 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 $\psi(k) < \varepsilon$.

12. 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.

13. 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.]

14. 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: $7^4 = 17 \bmod 149$.]

15. 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.

16. 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 $l_r(f) - s_r(f)$.

17. 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.

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

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 $f_{\overline{K}}^{\overline{x}}$ in $\overline{F}$. If $f \in A[X]$ is a monic lift of $f_{\overline{K}}^{\overline{x}}$ 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 $p = \mathrm{char}K$, 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.

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 $\mathrm{char}\overline{K} = 0$, 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 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. □

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. □

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, we have $N_{L/K}(\mathfrak{D}(L/K)) = \Delta(L/K)$, where $N_{L/K}$ denotes the ideal norm defined in [I, §7]. 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 as in [I, 8.5]. If A_L has an A_K-basis consisting of powers of an element $\alpha \in A_L$, we know from [I, §7] that $\Delta(L/K)$ is generated by the discriminant $\Delta(f)$ of $f = f_K^\alpha$. Moreover, the different is then equal to $\mathfrak{D}(L/K) = f'(\alpha)\cdot A_L$ by [I, ex. 8.8]. We can use this to compute the *differential exponent* $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K))$ of a complete extension L/K.

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 1.4 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 $e \le \mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) \le e-1+\mathrm{ord}_{\mathfrak{p}_L}(e)$. 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 $d(L) \le e-1+\mathrm{ord}_{\mathfrak{p}_L}(e)$ 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 [I, 9.13], 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 $\zeta_{e_0} = \tau(\sqrt[e_0]{\pi})/(\sqrt[e_0]{\pi})$ 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.

Assume now 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

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

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.

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* $\mathrm{char}\overline{K} = 0$ *and a p-group for* $\mathrm{char}\overline{K} = p > 0$. *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 $\mathrm{char}\overline{K} = 0$ 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 $\mathrm{char}\overline{K} = p > 0$ 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 $\mathrm{char}K = 0$ 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 $t \bmod p$ 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

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

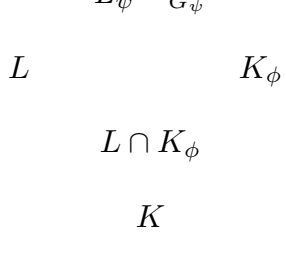
so it is in this case an isomorphism.

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.

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 $L \cap K_\phi$.



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. □

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.

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:

$$g_1^{-1}\mathfrak{P} \cap L = g_2^{-1}\mathfrak{P} \cap L \Longleftrightarrow \exists h \in H : hg_1^{-1}\mathfrak{P} = g_2^{-1}\mathfrak{P} \Longleftrightarrow \exists h \in H : g_2 h g_1^{-1} \in G_{\mathfrak{P}}$$
$$\Longleftrightarrow \exists h \in H : G_{\mathfrak{P}} \cdot g_2 h = G_{\mathfrak{P}} \cdot g_1 \Longleftrightarrow G_{\mathfrak{P}} \cdot g_2 H = G_{\mathfrak{P}} \cdot g_1 H.$$

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.

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 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

$$K_{\mathfrak{p}} \otimes_K L \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}. \tag{6.1}$$

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.

6.2. 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 6.1. 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.

6.3. 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 $\mathfrak{q}|\mathfrak{p}$.

6.4. 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 6.1. □

6.5. 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.

6.6. 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 6.6 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 $f = f^{\alpha}_{\mathbf{Q}} \in \mathbf{Z}[X]$ 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 $\widehat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^* \to C^1_\mathbf{Q}$ that is an isomorphism of topological groups. Conclude that $C^1_\mathbf{Q}$ is compact.

15. Show that the exact sequence $0 \to C^1_K \to C_K \xrightarrow{\tau} \mathbf{R}_{>0} \to 0$ 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^1_K for $U_K \cap J^1_K$. Show that $U^1_K/\mathcal{O}^*_K$ is compact and that there is an exact sequence of topological groups

$$0 \longrightarrow U^1_K/\mathcal{O}^*_K \longrightarrow C^1_K \longrightarrow Cl_K \longrightarrow 0.$$

Deduce that C^1_K 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 $H = L[U^1_K]$.]

17. Show that the map $\phi_K : J_K \to I_K$ in 6.11 is continuous when I_K is given the discrete topology, and that it induces a continuous surjection $C^1_K \to Cl_K$. Deduce that Cl_K is finite if C^1_K 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^1_K 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.

7 The Kronecker-Weber theorem

In this section, we will apply our knowledge of the local fields $\mathbf{Q}_p$ to prove a classification theorem for abelian extensions of the rational number field. The theorem was first stated by Kronecker in 1853, but his proof was incomplete. A second proof, as Kronecker's proof in terms of Lagrange resolvents, was given by Weber in 1886. Hilbert used what is essentially the theory of section 5 to give the first complete proof (1896). The theorem is a direct corollary of the class field theory presented in the next section, but we will follow the historical development and use the theorem as a motivation for general class field theory. Moreover, the techniques employed in the proof are interesting in their own right and provide nice illustrations of the general theory of local fields.

7.1. Kronecker-Weber theorem. *Every finite abelian extension of the rational number field* $\mathbf{Q}$ *is contained in a cyclotomic extension.*

This 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. We will follow an idea of Shafarevič (1951) to derive the Kronecker-Weber theorem from the corresponding result for the 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.

7.2. Local Kronecker-Weber 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 7.2 $\Rightarrow$ 7.1. Let $L/\mathbf{Q}$ be an abelian extension. 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 7.2, 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. □

In the proof of theorem 7.2, 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.

7.3. Kummer theory. *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 7.3 is canonical in the sense that for every automorphism τ of the algebraic closure of K, we have

$$(\sigma, w)_{L/K}^{\tau} = (\tau\sigma\tau^{-1}, \tau(w))_{n,\tau[K]}. \tag{7.4}$$

There is an analog of 7.3 known as *Artin-Schreier theory* when n equals the characteristic of K, see exercise 1.

Proof of 7.2. We will assume $p \neq \infty$. 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.

7.5. 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.

7.6. 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 $[L : \mathbf{Q}_p(\zeta_p)] = p^2$.

7.7. 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 7.2 to be proved.

7.8. 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 7.5 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 $\mathbf{Q}_2(\sqrt{-1}, \sqrt{5}, \sqrt{2}) = \mathbf{Q}_2(\zeta_{24})$, cf. exercise 28. 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 7.2. □

7.9. 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

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

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 7.2 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.)* ****

Literature

In addition to the texts mentioned in *Number Rings*, there are a few texts covering valuation theory and/or class field theory that are recommended.

1. F. Gouvêa, *p-adic Numbers*, Springer Universitext, 1993.
2. J. W. S. Cassels, *Local fields*, London Mathematical Society Student Text 3, Cambridge, 1986.
3. E. Weiss, *Algebraic number theory*, McGraw Hill, 1963. Chelsea reprint 1976.
   The first few chapters give a very clear account on valuation theory.
4. E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, 1967.
   Develops valuation theory both for number fields and function fields, thus stressing their similarity.
5. N. Koblitz, *p-adic numbers, p-adic analysis and zeta-functions*, Springer GTM 58, 1977.
   Careful introduction to p-adic numbers and functions, with several numerical examples.
6. J.P. Serre, *Corps locaux*, Hermann, 1962. English translation: *Local fields*, Springer GTM 67, 1979.
   The basic reference on local fields. No formal groups.
7. J.W.S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Academic Press, 1967.
   Proceedings of a 1967 instructional conference. Contains cohomological class field theory and accounts of then new developments on formal groups and class field towers.
8. E. Artin, J. Tate, *Class field theory*, Benjamin, 1967. Reprinted as Addison-Wesley 'advanced book classic', 1990.
   Notes of the 1951–52 Princeton seminar on class field theory that led to the cohomological set-up of class field theory. Still very useful.
9. J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.
   Contains class field theory in Neukirch's own axiomatic set up and an extensive chapter on zeta functions and L-series.

References

10. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.
11. G. Cornell, J. H. Silverman, *Arithmetic Geometry*, Springer, 1986.
12. Goss function fields
13. Hasse Abelsche Zahlk.
14. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84, 1982. Second edition, 1992?.

15. S. Lang, *Algebraic number theory,* Addison Wesley, 1970. Second edition by Springer (GTM 110, 1994)

16. H. W. Lenstra, Jr. and P. Stevenhagen, *Über das Fortsetzen von Bewertungen in vollständigen Körpern*, Archiv für Mathematik **53**, 547–552 (1989).

19. Serre Mass formula