VOORTGEZETTE GETALTHEORIE

P. Stevenhagen

Universiteit Leiden
2024

Disclaimer

These notes are being polished and extended as we go. Please email typos, inaccuracies and suggestions for improvement to psh@math.leidenuniv.nl.

Version: December 14, 2024

CONTENTS

Introduction

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

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

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

1 Valued fields

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

$$f(z) = \sum_{i \gg -\infty}^{\infty} a_i (z-\alpha)^i \tag{1.1}$$

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

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

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

$$x = \sum_{i \gg -\infty}^{\infty} a_i \pi^i \tag{1.2}$$

reminiscent of (1.1). It is not immediately clear which coefficients $a_i \in K$ should occur in such series, and for (1.2) to be meaningful we need a notion of convergence in K that will be provided by the $\mathfrak{p}$-adic valuation on K.

The resulting $\mathfrak{p}$-adic expansions are in many ways similar to the well-known decimal expansions of real numbers x as Laurent series

$$x = \sum_{i \gg -\infty}^{\infty} a_i \cdot 10^{-i}$$

'in 1/10' with digits $a_i \in \{0, 1, 2, \ldots, 9\}$, and they yield embeddings of K in its completions $K_\mathfrak{p}$ at $\mathfrak{p}$ that are much like the embedding of $\mathbf{Q}$ in $\mathbf{R}$. The concept of valuations that we are to introduce will actually put both kinds of embeddings on equal footing.

▶ Valuations

Valuations are *absolute values* on arbitrary fields K that define a metric topology on K.

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

Conditions (1) and (2) describe ϕ as the unique extension of a homomorphism $K^* \to \mathbf{R}_{>0}$ to a map on all of K, obtained by putting $\phi(0) = 0$. The subgroup $\phi[K^*] \subset \mathbf{R}$ is the *value group* of ϕ. Condition (3) expresses its 'continuity' with respect to addition. The smallest possible constant C in (3) is the *norm* $||\phi||$ of ϕ. If ϕ is a valuation and r a positive real number, the r-th power $\phi^r\colon x \mapsto \phi(x)^r$ of ϕ is a valuation of norm $||\phi^r|| = ||\phi||^r$.

The norm of a valuation ϕ cannot be smaller than 1, and by (2) it equals

$$||\phi|| = \sup_{x:\ \phi(x)\leq 1} \phi(1+x). \tag{1.4}$$

This supremum is actually a maximum and, as we will see, either equal to $\phi(1) = 1$ or to $\phi(2)$ (exercise 12).

1.5. Examples. A first example of a valuation that comes to mind is the ordinary absolute value on $\mathbf{C}$, or on a subfield of $\mathbf{C}$ such as $\mathbf{Q}$ or $\mathbf{R}$. It has norm equal to 2.

For a point $\alpha \in \mathbf{C}$, we have the valuation $\phi_\alpha\colon \mathcal{M} \to \mathbf{R}_{\geq 0}$ defined for $f \neq 0$ by

$$\phi_\alpha(f) = c^{\mathrm{ord}_\alpha(f)} \qquad \text{for some fixed } c \in (0,1). \tag{1.6}$$

On the polynomial ring $\mathbf{C}[X] \subset \mathcal{M}$, the function $\mathrm{ord}_\alpha(f)$ counts the number of factors $X - \alpha$ occurring in the factorization of f into irreducibles, which is unique up to multiplication by units in $\mathbf{C}[X]^* = \mathbf{C}^*$.

More generally, for an irreducible polynomial P in the polynomial ring $F[X]$ over an arbitrary field F, we have the number $\mathrm{ord}_P(f) \in \mathbf{Z}_{\geq 0}$ of factors P occurring in the factorization of a non-zero polynomial $f \in F[X]$, which is again unique up to multiplication by units, as $F[X]$ is a unique factorization domain. It leads to a valuation

$$\phi_P(x) = c^{\mathrm{ord}_P(x)} \qquad \text{for some fixed } c \in (0,1) \tag{1.7}$$

on the field of fractions $F(X)$ of F, the *rational function field* over F.

For a prime $\mathfrak{p}$ of a number field K, we have the valuation $\phi_\mathfrak{p} : K \to \mathbf{R}_{\geq 0}$ defined by

$$\phi_\mathfrak{p}(x) = c^{\mathrm{ord}_\mathfrak{p}(x)} \qquad \text{for some fixed } c \in (0,1). \tag{1.8}$$

We symbolically define $\mathrm{ord}(0) = +\infty$ in the three definitions above, and with this convention they also make sense for $f = 0$ and $x = 0$, with $c^{+\infty} = 0$ for $c \in (0,1)$. The precise value of

c in (1.6), (1.7) and (1.8) is not very relevant, and can be thought of as a normalization of ϕ_α, ϕ_P and $\phi_\mathfrak{p}$. From the obvious identities

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

we deduce that the norms of ϕ_α, ϕ_P and $\phi_\mathfrak{p}$ equal 1. ◊

A valuation ϕ of norm 1 satisfies the *ultrametric inequality*

$$\phi\left(\sum_{i=1}^n x_i\right) \leq \max_{i=1,2,\ldots,n} \phi(x_i) \tag{1.9}$$

and is called *non-archimedean*. For such ϕ, a sum of small elements is never large, and the Archimedean postulate, which states that a 'small but non-zero' quantity becomes arbitrarily large when repeatedly added to itself, does not hold. When quantities of unequal size are added under a non-archimedean valuation, the ultrametric inequality becomes an equality:

$$\phi(x_1) \neq \phi(x_2) \Rightarrow \phi(x_1+x_2) = \max\{\phi(x_1), \phi(x_2)\}. \tag{1.10}$$

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

$$\phi\left(\sum_{i=1}^n x_i\right) \leq \sum_{i=1}^n \phi(x_i), \tag{1.11}$$

and this has amusing consequences for the geometry of the underlying space (exercise 4). A trivial example of a non-archimedean valuation that exists on any field K is the *trivial valuation* on K, obtained by extending the trivial homomorphism $\phi\colon K^* \to \{1\}$.

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

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

$$\phi_\sigma(x) = |\sigma(x)|. \tag{1.12}$$

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

▶ Valuation topology

Although valuations are not required to satisfy the triangle inequality (1.11), they do so when raised to a suitable power. This is a consequence of the following proposition.

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

Proof. It is clear that a valuation satisfying the triangle inequality has norm at most 2. Conversely, if ϕ has norm at most 2, we can repeatedly apply condition (3) in definition 1.3 to obtain $\phi(\sum_{i=1}^{2^m} x_i) \le 2^m \max_i \phi(x_i)$. Taking some of the x_i in this inequality equal to 0, we see that a sum of n terms can be bounded by $\phi(\sum_{i=1}^{n} x_i) \le 2n \max_i \phi(x_i)$. In particular, we have $\phi(n \cdot 1) \le 2n$ for $n \in \mathbf{Z}_{\ge 1}$. We now use the multiplicativity of ϕ to obtain the estimate

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

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

An argument similar to that given in the preceding proof shows that it is possible to decide whether a valuation is archimedean by looking at its values on multiples of 1.

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

Proof. It is clear from the ultrametric inequality (1.9) that we have $\phi(\pm n \cdot 1) \le \phi(1) = 1$ if ϕ is non-archimedean, showing that ϕ is bounded on Z by 1.

For the converse, assume that ϕ is bounded by M on 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

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

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

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

Proof. In this case the subring Z is the finite field $\mathbf{F}_p$. □

If ϕ is bounded on Z, then it is bounded by 1. This also follows from the fact that $\phi[Z]$ is closed under multiplication. For ϕ unbounded on Z, we will prove in Theorem 1.18 that ϕ is a power of the ordinary absolute value on $Z = \mathbf{Z} \subset K$, so $\phi(1+1)$ already tells us whether ϕ is archimedean, and more (exercise 12).

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

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

of radius ε around x. As all powers of ϕ induce the same topology, the topology $\mathcal{T}_\phi$ is metrizable by Proposition 1.13.

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

Just as for the ordinary absolute value on $\mathbf{R}$ or $\mathbf{C}$, one shows for the valuation topology that the addition map $(x, y) \mapsto x+y$ and the multiplication map $(x, y) \mapsto xy$ are continuous maps from $K \times K$ to K, and that the inversion map $x \mapsto x^{-1}$ is continuous on K^*. These continuity properties can be summarized by stating that the valuation topology $\mathcal{T}_\phi$ on K makes K into a *topological field*. By the ultrametric property (1.9), a non-archimedean topological field K is topologically rather different from archimedean topological fields such as $\mathbf{R}$ and $\mathbf{C}$. For instance, given points $x, y, z \in K$ for which $x-y$ and $y-z$ have different valuation, the sum $x - z = (x - y) + (y - z)$ has the same valuation as either $x - y$ or $y - z$ by (1.10): every triangle in K is isosceles. In the same vein, it follows from the fact that every two points x, y in an open ball $U_\varepsilon(x_0)$ have distance

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

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

Exercise 4. Show that if two open balls in K are not disjoint, then one is contained in the other.

▶ Independence of valuations

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

1.16. 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) *$\mathcal{T}_\phi \supset \mathcal{T}_\psi$: the topology $\mathcal{T}_\phi$ is stronger than $\mathcal{T}_\psi$;*
(4) *$\phi(x) < 1$ implies $\psi(x) < 1$ for all $x \in K$.*

Proof. The implications (1) $\Rightarrow$ (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 $\mathcal{T}_\phi$, we also have (3) $\Rightarrow$ (4).

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

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

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 yx^{-n} would violate (4) for large n. Thus $\phi(x) < 1$, as desired.

For $x \in K^*$ arbitrary, define $\alpha, \beta \in \mathbf{R}$ by $\phi(x) = \phi(y)^\alpha$ and $\psi(x) = \psi(y)^\beta$. For $a, b \in \mathbf{Z}$ with $b > 0$, we then have

$$\alpha > \tfrac{a}{b} \Longleftrightarrow \phi(y)^\alpha = \phi(x) < \phi(y)^{a/b} \Longleftrightarrow \phi(x^b y^{-a}) < 1 \Longleftrightarrow \psi(x^b y^{-a}) < 1 \Longleftrightarrow \beta > \tfrac{a}{b}.$$

This implies $\alpha = \beta$, so $r = \log \phi(x)/\log \psi(x) = \log \phi(a)/\log \psi(a)$ does not depend on x, and we have $\phi = \psi^r$ as in (1). □

If ϕ and ψ are non-trivial valuations on K that are not equivalent, the proof of 1.16 shows that we can find $a \in K$ satisfying $\phi(a) < 1$ and $\psi(a) \geq 1$, and also $b \in K$ satisfying $\phi(b) \geq 1$ and $\psi(b) < 1$. The element $x = a/b$ then satisfies $\phi(x) < 1$ and $\psi(x) > 1$, and this means that for $n \to \infty$ the sequence $\{x_n\}_{n \geq 1}$ of elements

$$x_n = \frac{x^n}{1 + x^n}$$

converges to 0 in $\mathcal{T}_\phi$, but to 1 in T_ψ. This unrelated behavior under ϕ and ψ leads to an independence of non-equivalent valuations that can be phrased in the following way for a finite number of valuations.

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

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

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

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

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

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

▶ Prime divisors

An equivalence class of non-trivial valuations on K is known as a *place* or *prime divisor* of K, often shortened to *prime* of K. By Proposition 1.16, the prime divisor corresponding to a non-trivial valuation ϕ is the equivalence class $\{\phi^r : r > 0\}$. Depending on the type of valuations it contains, a prime divisor is said to be archimedean or non-archimedean. Archimedean prime divisors are also known as *infinite primes*, as opposed to the *finite primes* denoting the non-archimedean prime divisors.

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

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

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

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

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

Proof. Let ϕ be a non-archimedean valuation on $\mathbf{Q}$. Then ϕ is bounded by 1 on $\mathbf{Z}$, and $\mathfrak{p} = \{x \in \mathbf{Z} : \phi(x) < 1\}$ 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. We have $\phi(x) = 1$ for $x \in \mathbf{Z} \setminus p\mathbf{Z}$, so $\phi(u) = 1$ for all fractions $u = \frac{a}{b} \in \mathbf{Q}$ with $p \nmid ab$. Writing arbitrary $x \in \mathbf{Q}^*$ as $x = up^m$ with u as above and $m = \operatorname{ord}_p(x) \in \mathbf{Z}$, we find $\phi(x) = c^{\operatorname{ord}_p(x)}$ with $c = \phi(p) \in (0,1)$, so ϕ is equivalent to ϕ_p.

Suppose now that ϕ is an archimedean valuation on $\mathbf{Q}$. We may assume that it satisfies the triangle inequality, implying $\phi(m) \le |m|$ for $m \in \mathbf{Z}$. Given two integers $m, n > 1$, we can write all powers of m in base n as $m^t = \sum_{i=0}^{s} a_i n^i$ with $a_i \in \{0, 1, \dots, n-1\}$ and $a_s \neq 0$. As the number s of digits of m^t in base n satisfies $|s - \log(m^t)/\log n| \le 1$, we have $|s/t - \log m/\log n| \le \frac{1}{t}$. The triangle inequality implies $\phi(m)^t \le (s+1)n \max\{1, \phi(n)^s\}$, so if we take t-th roots and let t tend to infinity we 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 we have $\phi(n) = |n|^{\log a}$ for all $n \in \mathbf{Z}$. This implies $\phi(x) = |x|^{\log a}$ for all $x \in \mathbf{Q}$, showing ϕ to be equivalent to the ordinary absolute value ϕ_∞ on $\mathbf{Q}$. □

The normalization of the p-adic valuation ϕ_p in Theorem 1.18 is standard, and chosen in such a way that we have the *product formula*

$$\prod_{p \le \infty} \phi_p(x) = 1 \qquad \text{for} \quad x \in \mathbf{Q}^*. \tag{1.19}$$

Here the product is taken over all prime divisors of $\mathbf{Q}$, including the unique infinite prime. It shows that the approximation theorem 1.17 does not necessarily hold for an *infinite* collection of non-equivalent valuations.

Exercise 5. Show that Chinese remainder theorem for $\mathbf{Z}$ can be obtained as a special case of the approximation theorem.

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

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

is a subring of K, the *valuation ring* of ϕ. Every $x \in K^*$ satisfies $x \in A$ or $x^{-1} \in A$. In particular, A has field of fractions K. The valuation ring A is a local ring with unit group $A^* = \{x \in K : \ \phi(x) = 1\}$ and maximal ideal $\mathfrak{m} = \{x \in K : \ \phi(x) < 1\}$. The quotient $k = A/\mathfrak{m}$ is known as the *residue class field* of ϕ.

Exercise 6. Which possibilities are there for the pair $(\mathrm{char}\,(K), \mathrm{char}\,(k))$ of field characteristics?

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

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

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

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

Proof. Write $A \subset K$ for the valuation ring of ϕ, and $\mathfrak{m}$ for its maximal ideal. We have $\mathcal{O}_K \subset A$ as $x \in \mathcal{O}_K$ satisfies an equation $x^n = \sum_{i=0}^{n-1} a_i x^i$ of degree $n \geq 1$ with coefficients $a_i \in \mathbf{Z} \subset A$, and the inequalities

$$\phi(x^n) \leq \max_{i=1,2\cdots,n-1} \phi(a_i x^i) \leq \max_{i=1,2\cdots,n-1} \phi(x)^i$$

imply $\phi(x) \leq 1$. Just as in the case $K = \mathbf{Q}$, we obtain a prime ideal $\mathfrak{p} = \mathfrak{m} \cap \mathcal{O}_K$ in $\mathcal{O}_K$ that is non-zero for non-trivial ϕ, and we have $\phi(x) = 1$ for $x \in \mathcal{O}_K \setminus \mathfrak{p}$. The localization

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

of $\mathcal{O}_K$ at $\mathfrak{p}$ defined in [NR, §2] is a discrete valuation ring, and if we pick $\pi \in \mathcal{O}_K$ with $\mathrm{ord}_{\mathfrak{p}}(\pi) = 1$, then any $x \in K^*$ can be written as $x = u\pi^m$ with $u \in \mathcal{O}_{K,\mathfrak{p}^*}$ and $m = \mathrm{ord}_{\mathfrak{p}}(x)$. We find $\phi_{\mathfrak{p}}(x) = c^{\mathrm{ord}_{\mathfrak{p}}(x)}$ with $c = \phi(\pi) \in (0,1)$.

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

The proof of Theorem 1.20 shows that $\mathcal{O}_{K,\mathfrak{p}}$ is the valuation ring of $\phi_{\mathfrak{p}}$. It is the largest subring $A \supset \mathcal{O}_K$ of K to which the reduction map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ can be extended. The residue class field of the valuation $\phi_{\mathfrak{p}}$ is the residue class field $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ of the prime $\mathfrak{p}$.

For the rational function field $F(X)$ over a field F occurring in (1.7), the argument used in proving 1.20 yields the following.

1.21. Theorem. *Let ϕ be a non-trivial valuation on $F(X)$ that is trivial on F. Then ϕ is either a P-adic valuation ϕ_P given on K^* by*

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

for some monic irreducible polynomial $P \in F[X]$, or, with $\deg : K^* \to \mathbf{Z}$ the homomorphism extending the degree map on $F[X] \setminus \{0\}$, the degree valuation ϕ_∞ given by

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

Proof. As ϕ is trivial on F, it is non-archimedean by Proposition 1.14. Suppose first that we have $\phi(X) \le 1$. Then $F[X]$ is a subring of the valuation ring of ϕ, and $\mathfrak{p} = F[X] \cap \mathfrak{m}$ is a prime ideal of $F[X]$ that is non-zero as ϕ is non-trivial. We have $\mathfrak{p} = (P)$ for some non-constant monic irreducible polynomial $P \in F[X]$, and as before, the localization

$$F[X]_{(P)} = \left\{ \frac{a}{b} : \ a, b \in F[X], P \nmid b \right\}$$

of $F[X]$ at $\mathfrak{p}$ is a discrete valuation ring with uniformizer P. Writing $x \in F(X)^*$ as $x = uP^m$ with $u \in R_\mathfrak{p}^*$ and $m = \mathrm{ord}_P(x) \in \mathbf{Z}$, we find $\phi(x) = \phi(P)^k$ and $\phi = \phi_P$ with constant $c = \phi(P) \in (0,1)$.

Suppose now that we have $\phi(X) > 1$. Then we have $\phi(X^{-1}) < 1$, and the previous argument can be repeated with the ring $F[X^{-1}]$ in the role of $F[X]$. 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 $c = \phi(X^{-1})$. □

Exercise 7. What is the residue class field of the valuations ϕ_P and ϕ_∞ in Theorem 1.21?

If F is finite, then *all* valuations of $F(X)$ are trivial on F, and Theorem 1.21 classifies the valuations on $F(X)$.

▶ Discrete valuation rings

One cannot fail to notice the analogy between Theorems 1.18, 1.20 and 1.21. It reflects the similarity of the unique factorization domains $\mathbf{Z}$ and $F[X]$ and shows that, just as for the Dedekind domain $\mathcal{O}_K$, their non-zero prime ideals induce non-archimedean valuations on the field of fractions. In all cases, the localization at these primes is a discrete valuation ring: a principal ideal domain R with field of fractions $K \neq R$ that is local. With $\pi \in R$ a generator of the maximal ideal $\mathfrak{m} \subset R$, often called a *uniformizer* or *local parameter*, every $x \in K^*$ has a unique representation $x = u\pi^m$ with $u \in R^*$ and $m = \mathrm{ord}(x) \in \mathbf{Z}$.

A discrete valuation ring $R \subset K$ defines a prime divisor on K by the valuations that are given on K^* by $\phi(x) = c^{\mathrm{ord}(x)}$ for some $c \in (0,1)$. The terminology is consistent: the valuation ring of ϕ is equal to R, and the valuation ϕ is *discrete* in the sense that the value group $\phi[K^*]$ is a discrete subgroup of $\mathbf{R}_{>0}$ generated by $c = \phi(\pi)$.

1.22. Proposition. *Let ϕ be a non-trivial non-archimedean valuation on a field K and A its valuation ring. Then ϕ is discrete if and only if A is a discrete valuation ring.*

Proof. Suppose $\phi[K^*] \neq \{1\}$ is discrete in $\mathbf{R}_{>0}$. Then $\phi[K^*]$ is infinite cyclic (exercise 10), and we can find $\pi \in A$ such that $\phi[K^*]$ is generated by $\phi(\pi) < 1$. For $x \in K^*$ we have $\phi(x) = \phi(\pi)^m$ for a unique $m \in \mathbf{Z}$, so we can write $x = u\pi^m$ for some $u \in A^*$. It follows that A is a discrete valuation ring with maximal ideal πA.

Conversely, if A is a discrete valuation ring with uniformizer π, we can represent $x \in K^*$ as $x = u\pi^m$ with $u \in A^*$ and $m \in \mathbf{Z}$. Units in A have valuation 1, so $\phi(x) = \phi(\pi)^m$ and $\phi[K^*]$ is the discrete subgroup of $\mathbf{R}_{>0}$ generated by $\phi(\pi)$. □

An archimedean valuation ϕ on a field K is never discrete. For such ϕ it follows from Corollary 1.15 that we have $\mathbf{Q} \subset K$, from Proposition 1.14 that ϕ is non-trivial on $\mathbf{Q}$, and from Theorem 1.18 that $\phi[K^*]$ contains the dense subgroup $\phi[\mathbf{Q}^*] \subset \mathbf{R}_{>0}$.

For a discrete valuation ring $A \subset K$, the associated function $\nu\colon K \to \mathbf{Z} \cup \{\infty\}$ sending $x \in K^*$ to $\mathrm{ord}(x) \in \mathbf{Z}$ and $0 \in K$ to ∞ is the (normalized) *exponential valuation* of the prime divisor defined by A. The map ν is a formal extension to K of a homomorphism $K^* \to \mathbf{Z}$ that fits in a natural exact sequence

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

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

$$K^* = \langle \pi \rangle \times A^*. \tag{1.23}$$

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

1.24. Example. Let F be a field, and $A = F[[X]]$ be the ring of formal power series $x = \sum_{i=0}^{\infty} a_i X^i$ with coefficients $a_i \in F$. We have $x \in A^*$ if and only if the constant coefficient a_0 of x is non-zero, so A is a discrete valuation ring with maximal ideal $\mathfrak{m} = (X)$ and residue class field F. The field of fractions $K = F((X))$ of A is the field of formal Laurent series over F. The natural embedding $F[X] \subset F[[X]]$ of the polynomial ring $F[X]$ in A extends to an embedding $F(X) \to F((X)) = K$ of their fields of fractions.

The valuation $\phi_X : x \mapsto c^{\mathrm{ord}(x)}$ on K corresponding to A is an extension to K of the valuation ϕ_X on $F(X)$ defined in Theorem 1.21. Under the valuation topology on K, every formal power series is the limit of a sequence of polynomials, so $F(X)$ is a *dense* subfield of K. Note that the value groups of $\phi(X)$ on $F(X)$ and K are equal, and that the residue class field of ϕ_X is in both cases equal to F.

▶ Finite and infinite primes

The terminology of 'places' for the prime divisors of a field K comes from the geometric notion of points on curves. Theorem 1.21 describes the 'geometric' places of the rational function field $F(X)$, i.e., those places corresponding to valuations that are trivial on F.

If F is algebraically closed, the monic irreducibles in $F[X]$ are of the form $P = X - \alpha$ with $\alpha \in F$, and the primes $\phi_P = \phi_\alpha$ correspond directly to the 'points' of F as in (1.6). If F is not algebraically closed, 'points' may only be defined over extension fields, and an irreducible polynomial P accounts for $n = \deg(P)$ points defined over an extension field of degree P. The valuation ϕ_∞ does not correspond to an irreducible polynomial in $F[X]$, but one can view $-\deg(x)$ as the order of the zero of x at a '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. Here the points arise as the places of the function field of the curve.

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 terms of valuations, it comes down to considering all places of the function field.

For projective curves, the notion of being a point 'at infinity' is not canonical, and the degree valuation ϕ_∞ in Theorem 1.21, which corresponds to the discrete valuation ring $F[X^{-1}]_{(X^{-1})}$, is in no intrinsic way different from the valuation ϕ_X with valuation ring $F[X]_{(X)}$: it also corresponds to a finite prime of $F(X)$.

Number fields are different from function fields in the sense that they have 'intrinsically' infinite primes, i.e., non-archimedean primes. There are only finitely many of these infinite primes, and we will see in Corollary 2.5 that they come from embeddings of the number field K in $\mathbf{C}$ as in (1.12).

Despite the difference between finite and infinite primes that exists for number fields, there are good reasons to consider *all* primes of a number field, not just the finite ones. For many *product formulas* in number theory, of which (1.19) provides an easy example, it is necessary to include the infinite primes. Projective curves tend to have better properties than 'non-complete' affine curves, and the *Arakelov approach* to number fields is that inifinite primes have to be included in their treatment in order to fully exploit the existing analogies between number fields and function fields. We will get back to this in section *, which deals with the relation between 'global' and 'local' fields.

EXERCISES.

8. Let L/K be an algebraic extension and ψ a valuation on L. Show that ψ is trivial if and only if its restriction $\phi = \psi|_K$ to K is trivial.

9. An *exponential valuation* on a field K is a map $\nu\colon K \to \mathbf{R} \cup \{\infty\}$ satisfying

   (1) $\nu(x) = \infty$ if and only if $x = 0$;
   (2) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K^*$;
   (3) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for all $x, y \in K^*$.

   Show that exponential valuations correspond bijectively to non-archimedean valuations on K. What does it mean for exponential valuations to be 'non-trivial', 'discrete' or 'equivalent'?

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

11. Do there exist a field K and a non-trivial valuation ϕ on K for which we can strengthen the implication (1.10) to an equivalence

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

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

12. Show that the norm of a valuation ϕ on a field K is equal to $\phi(1) = 1$ if ϕ is non-archimedean, and to $\phi(2)$ if ϕ is archimedean.

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

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

15. Let A be an integral domain with field of fractions K, and $\phi : A \to \mathbf{R}_{\geq 0}$ a map satisfying the conditions in definition 1.3 for $x, y \in A$. Show that ϕ extends uniquely to a valuation on K.

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

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

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

17. Let ϕ be a non-trivial discrete valuation, A its valuation ring, and $k = A/\mathfrak{m}$ its residue class field. Write $U_k = 1 + \mathfrak{m}^k$ for $k \in \mathbf{Z}_{>0}$.

    a. Show that $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a 1-dimensional vector space over $k_\mathfrak{m}$;
    b. Show that the map $x \mapsto x - 1$ induces a group isomorphism $U_k/U_{k+1} \xrightarrow{\sim} \mathfrak{m}^k/\mathfrak{m}^{k+1}$.

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

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

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

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

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

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

analogous to the product formula for $K = \mathbf{Q}$, when ν ranges over all *suitably normalized* exponential valuations on K. (Informally: a rational function has 'as many' zeroes as it has poles if we take the 'point at infinity' into account.)

2 Complete fields

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

▶ Completions

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

2.1. Theorem. *Let ϕ be a valuation on K. Then there exists a field extension $K \subset K_\phi$ and an extension of ϕ to a valuation on K_ϕ such that K_ϕ is a complete valued field containing K as a dense subfield.*

For every extension field F of K that is complete with respect to a valuation extending ϕ, there exists a unique continuous K-homomorphism $K_\phi \to F$.

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

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

Note that this limit exists, as $\phi(a_i)$ is a Cauchy-sequence in $\mathbf{R}$.

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

If $F \supset K$ is complete with respect to a valuation extending ϕ, the map $\mathfrak{R} \to F$ sending $(a_i)_{i=1}^\infty$ to $\lim_{i\to\infty} a_i \in F$ 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. □

2.2. Example. For the valuation $\phi = \phi_X$ on $K = F(X)$ in example 1.24, the completion K_ϕ is the field $F((X))$ of Laurent series, on which $\phi_X(f) = c^{\operatorname{ord}_X(f)}$ is the obvious extension valaution from $F(X)$ to $F((X))$. ◊

▶ Complete archimedean fields

The last statement in Theorem 2.1 implies that the completion K_ϕ is uniquely determined up to a unique topological K-isomorphism. It also implies that a complete archimedean field, which contains the prime field $\mathbf{Q}$ on which the valuation is non-trivial by Proposition 1.14 and equal to a power of the ordinary absolute value by Theorem 1.18, contains the field of real numbers $\mathbf{R}$ as a topological subfield. The following lemma allows us to focus on complete archimedean fields containing the field of complex numbers $\mathbf{C}$ as a topological subfield.

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

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

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

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

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

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

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

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

Lemma 2.3 does not assume that ϕ is archimedean, and the formula it gives to extend ϕ to a finite extension is a generality that we will encounter again in (3.3).

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

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

Proof. We already saw that a complete archimedean field K contains $\mathbf{R}$ as a topological subfield. By Lemma 2.3, the (possibly trivial) extension $L = K(i)$ is a complete archimedean field containing $\mathbf{C}$ as a topological subfield. It now suffices to show that L equals $\mathbf{C}$, as we then have $\mathbf{R} \subset K \subset L = \mathbf{C}$, leaving no further choice for K.

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

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

which yields, for all integers $n \geq 1$, an inequality

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

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

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

Proof. Theorems 2.1 and 2.4 show that we have an embedding $\sigma \colon K \to \mathbf{C}$ of topological fields, so the topology T_ϕ coincides with the topology of the valuation ϕ_σ from (1.12) that is induced by σ. By Proposition 1.16, this implies $\phi = \phi_\sigma^r$. □

If two embeddings $\sigma_1, \sigma_2 \colon K \to \mathbf{C}$ induce the same valuation on K, there is by 2.1 an induced topological isomorphism on the completions. As $\mathbf{R}$ has no non-trivial automorphisms and $\mathbf{C}$ has 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 to Theorem 1.20.

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

An infinite prime of a number field K is called *real* if it comes from a real embedding $K \to \mathbf{R}$, and *complex* if it comes from an embedding $K \to \mathbf{C}$ with non-real image. We see that, in contrast to the situation for non-archimedean primes in Theorem 1.20, a number field has only a finite number of archimedean prime divisors. More precisely, they correspond to the factors of the tensor product

$$K_{\mathbf{R}} = K \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{R}^r \times \mathbf{C}^s$$

from [NR, (5.3)], and we have $r + 2s = \dim_{\mathbf{R}} K_{\mathbf{R}} = [K : \mathbf{Q}]$ for the numbers r and s of real and complex primes of K. This is a special case, for ϕ_∞ and $\mathbf{Q} \subset K$, of a general theorem (Theorem 3.13) on extending valuations to finite extensions.

Under suitable normalizations, there is a product formula for *all* primes of a number field K (exercise 18). It reduces to (1.19) for $K = \mathbf{Q}$.

▶ Non-archimedean completions

For non-archimedean valued fields K, the residue class field k can be any field, and the value group $\phi[K^*]$ any subgroup of $\mathbf{R}_{>0}$ (cf. exercise 1.16). The same is true for complete archimedean fields, by the following lemma.

2.7. Lemma. *Let $\tilde{K}$ be the completion of a field K with respect to a non-archimedean valuation ϕ. Then we have an equality $\phi[\tilde{K}^*] = \phi[K^*]$ of value groups and a natural isomorphism $k \xrightarrow{\sim} \tilde{k}$ of residue class fields.*

Proof. For $x \in \tilde{K}^*$ we can find $a \in K^*$ with $\phi(a - x) < \phi(x)$, so the ultrametric inequality (1.9) gives $\phi(a) = \phi(a - x + x) = \phi(x)$, proving $\phi(x) \in \phi[K]$ and $\phi[K] = \phi[\tilde{K}]$.

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

Given the large variety of complete non-archimedean fields, no classification result of the simplicity of Theorem 2.4 exists for them. On the other hand, they all share 'analytic properties' that are in some ways easier than those of $\mathbf{R}$ and $\mathbf{C}$. By way of example, one can think of the characterization of converging sums $\sum_{k\geq 0} a_k$ in a complete non-archimedean field with valuation ϕ as those sums for which $\phi(a_k)$ tends to 0 for $k \to \infty$.

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

In non-archimedean fields, all open balls $U_\varepsilon = \{x \in K : \phi(x) < \varepsilon\}$ and closed balls $B_\varepsilon = \{x \in K : \phi(x) \leq \varepsilon\}$ are additive subgroups of K. For $\varepsilon = 1$ we obtain the valuation ring $A = B_1$ and its maximal ideal $\mathfrak{m} = U_1$. Open and closed balls are the same thing in case we are dealing with *discrete* valuations as in Proposition 1.22. Most non-archimedean valuations in number theory and geometry are of this nature, and give rise to totally disconnected topological fields.

Suppose ϕ is non-trivial and discrete on K. Then the value group $\phi[K^*]$ is an infinite cyclic group $\langle \phi(\pi) \rangle \subset \mathbf{R}_{>0}$ that is generated by the largest value $\phi(\pi) \in (0, 1)$ assumed by ϕ. A *uniformizer* $\pi \in K^*$ for the corresponding prime divisor $\mathfrak{p}$, on which ϕ assumes this largest value, is unique up to multiplication by units in the discrete valuation ring A. For a fixed choice of π, every $x \in K^*$ can uniquely be written as in (1.23) as

$$x = u \cdot \pi^{\mathrm{ord}_{\mathfrak{p}}(x)} \tag{2.8}$$

for a $\mathfrak{p}$-adic unit $u \in A^*$ and an integer $\mathrm{ord}_{\mathfrak{p}}(x) \in \mathbf{Z}$.

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

$$x = \sum_{i \geq \mathrm{ord}_{\mathfrak{p}}(x)} a_i \pi^i, \tag{2.9}$$

with a_i from some subset $S \subset A$ of $\mathfrak{p}$-*adic digits*. For S one can pick any set of representatives in A of the residue classes modulo the maximal ideal $\mathfrak{m} = \pi A$, where it is customary to pick $0 \in S$ for the representative of the class $\mathfrak{m}$ itself. In view of the application in Theorem 3.9, we include in the statement below a version in which the powers π^i are replaced by arbitrary elements π_i that generate the same ideal as π^i.

2.10. Theorem. *Let K be complete with respect to a non-trivial discrete valuation, with valuation ring A and $\mathfrak{m} = \pi A$ as above. Let $\pi_i \in K$ be a generator of $\mathfrak{m}^i$, for $i \geq 0$, and $S \subset A$ a set of representatives of $k = A/\mathfrak{m}$ containing 0. Then we have*

$$A = \left\{ \sum_{i=0}^{\infty} a_i \pi_i : \ a_i \in S \text{ for } i \geq 0 \right\},$$

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

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

Conversely, given $x \in A$, there exists $a_0 \in S$ with $x \equiv a_0 \bmod \mathfrak{m}$. We have $x = a_0 + \pi_1 x_1$ with $x_1 \in A$, and taking $a_1 \in S$ satisfying $x_1 \equiv a_1 \bmod \mathfrak{m}$ yields $x - a_0 - a_1 \pi_1 \in \pi_1 \mathfrak{m} = \mathfrak{m}^2$. 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_i for $i \geq 0$ such that we have $x \equiv \sum_{i=0}^{n} a_i \pi_i \bmod \mathfrak{m}^{n+1}$, and therefore $x = \sum_{i=0}^{\infty} a_i \pi_i$. We already know that the expansion is unique, proving the first statement.

For the second statement, we use (2.8) to reduce to the case $\mathrm{ord}_{\mathfrak{p}}(x) = 0$, and then apply the first statement with $\pi_i = \pi^i$. □

If the complete field K in Theorem 2.10 is obtained by completion of a subfield $K_0 \subset K$, the elements π_i and the coefficients a_i can be taken from K_0 by Lemma 2.7. This applies in particular to the completions of $\mathbf{Q}$ arising from the p-adic valuations in Theorem 1.18.

In the 'equal characteristic case' where K and k have the same characteristic, the natural map $A \to A/\mathfrak{m} = k$ often allows a section, i.e., there is a *coefficient field* $k \subset A$ that maps isomorphically to $A/\mathfrak{m}$ under reduction. When K has a coefficient field, one can take S in Theorem 2.10 equal to k, and then K is a topological field that is isomorphic to the field $k((X))$ of Laurent series over k. See exercises 19-22.

▶ *p*-ADIC NUMBERS

The p-adic number field $\mathbf{Q}_p$ is the field obtained by completing the rational number field $\mathbf{Q}$ under the p-adic valuation ϕ_p from Theorem 1.18. The valuation ring of $\mathbf{Q}_p$ is denoted by $\mathbf{Z}_p$, and its residue class field is the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} = \mathbf{Z}_p/p\mathbf{Z}_p$. Making the obvious choices $\pi_i = p^i$ and $S = \{0, 1, 2, \ldots, p-1\}$ for $K = \mathbf{Q}_p$ in Theorem 2.10, we see that p-adic numbers have a unique p-adic expansion

$$x = \sum_{i \gg -\infty}^{\infty} a_i p^i \qquad \text{with} \qquad a_i \in \{0, 1, 2, \ldots, p-1\},$$

where $i \gg -\infty$ indicates that there are only finitely many $i < 0$ with $a_i \neq 0$. These expansions are in many ways similar to the decimal expansions $x = \sum_{i \gg -\infty}^{\infty} a_i 10^{-i}$ with $a_i \in \{0, 1, 2, \ldots, 9\}$ that are commonly used in the archimedean completion $\mathbf{R}$ of $\mathbf{Q}$. 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, and computer algebra systems deal with them as efficiently as they do with real numbers, making explicit p-adic calculations very easy, and doable by hand in small examples.

An addition $\sum_i a_i p^i + \sum_i b_i p^i$ is performed as an addition of formal power series in p followed by a transport of 'carries', for i ranging from $-\infty$ to ∞, from coefficients $a_i + b_i$ not in S to the next higher coefficient. A carry at the i-th coefficient $a_i + b_i \notin S$ gives a new i-th coefficient $a_i + b_i - p \in S$ and replaces the $(i+1)$-st coefficient by $a_{i+1} + b_{i+1} + 1$. Similar remarks can be made for the multiplication of p-adic numbers, and for subtraction one transports 'carries' in the other direction. As an example for the addition, one can consider the representation

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

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 $\mathbf{Q}_p$.

Exercise 2. Find the p-adic expansion of $x = 100$ in $\mathbf{Q}_2$, $\mathbf{Q}_3$ and $\mathbf{Q}_5$, and that of its additive inverse.

For division in $\mathbf{Q}_p$, one can find the expansion of $a = x/y \in \mathbf{Q}_p$ by equating coefficients in a 'power series identity' $ay = x$ or perform 'long division' as for real numbers, solving $x - ay = 0$ for $x, y \in \mathbf{Z}_p^*$ by successively subtracting suitable multiples $a_i p^i y$ (with $a_i \in S$) of y from x that eliminate the lowest coefficient, leaving 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 10.

Exercise 3. Compute the p-adic expansion of $\frac{1}{100}$ in $\mathbf{Q}_2$, $\mathbf{Q}_3$ and $\mathbf{Q}_5$.

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 11).

▶ Local fields

If K is complete with respect to a non-trivial discrete valuation, the representation of elements of A by their expansions $\sum_{i\geq 0} a_i\pi_i$ from Theorem 2.10 establishes a bijection of A with a countable infinite product $\prod_{i\geq 0} S$ of 'digit sets' S that is actually an isomorphism of topological spaces if we give S the discrete topology: elements are close if their first N digits coincide for some large N. If the cardinality of S, which equals the cardinality of the residue class field $k = A/\mathfrak{m}$, is finite, then Tychonoff's theorem from topology implies that $\prod_{i\geq 0} S$, and therefore A and all open balls $\mathfrak{m}^n$ are compact, making the valuation topology on K into a *locally compact* topology.

A field K equipped with a non-trivial valuation is said to be a *local field* if the valuation topology on K is locally compact. Such fields admit a very 'concrete' description, and arise as completions of what we will call *global fields* in section 6.

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

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

Proof. If K is archimedean, its completion is topologically isomorphic to either $\mathbf{R}$ or $\mathbf{C}$ by Theorem 2.4. As a locally compact subfield of $\mathbf{R}$ contains a closed interval $[-\varepsilon, \varepsilon]$, and a locally compact subfield of $\mathbf{C}$ a closed disk $\{z : |z| \leq \varepsilon\}$, we deduce that K is equal to either $\mathbf{R}$ or $\mathbf{C}$.

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

Completions of a number field at its primes, either finite or infinite, are examples of local fields.

Exercise 4. Let F be a finite field. Show that every completion of the rational function field $F(X)$ at one of its primes is a local field.

Every local field K of positive characteristic is a field $K = k((X))$ of Laurent series over a

finite field k, with ϕ_X the corresponding valuation, and $k \subset K$ the coefficient field for this valuation (exercise 21). In exercise 3.5, we will see that a local field of characteristic 0 is the same thing as a finite extension of $\mathbf{Q}_p$, with $\mathbf{Q}_\infty = \mathbf{R}$ accounting for the archimedean case.

▶ Hensel's lemma

Over the field of real numbers $\mathbf{R}$, the completeness gives rise to various 'intermediate value theorems' stating that if a continuous function $f\colon \mathbf{R} \to \mathbf{R}$ that assumes both positive and negative values on an interval, it necessarily has a zero in the interval. This zero can be approximated by repeated bisection, but in case f is differentiable, *Newton iteration* (exercise 12) provides a much faster method.

In complete non-archimedean fields K, there are no intermediate values as K has no linear ordering, and continuous functions on totally disconnected spaces are not particularly well-behaved. Still, in the case of polynomial functions $f\colon K \to K$, which come with formal derivatives, one can often apply Newton's method to refine approximate solutions to the equation $f(x) = 0$ to actual solutions in K, or to 'lift' approximate polynomial factors of f to actual factors in $K[X]$. Results of this nature all go under the name of *Hensel's lemma*. The version for 'simple' factors of f over the residue class field $k = A/\mathfrak{m}$ is the following.

2.12. 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 polynomial that factors over the residue class field $k = A/\mathfrak{m}$ as*

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

with $\overline{g}, \overline{h} \in k[X]$ non-zero and coprime. Then there exist $g, h \in A[X]$ with $\deg(g) = \deg(\overline{g})$ and reductions $\overline{g}, \overline{h} \in k[X]$ such that we have a factorization $f = g \cdot h \in A[X]$.

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, we set $n = \deg f$ and $s = \deg(\overline{g})$, and find $\pi \in \mathfrak{m}$ and polynomials g_0, h_0, a_0 and b_0 in $A[X]$ satisfying

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

This amounts to taking arbitrary lifts $g_0, h_0 \in A[X]$ of $\overline{g}, \overline{h} \in k[X]$ of the same degree, doing the same for polynomials $\overline{a}_0, \overline{b}_0 \in k[X]$ expressing the coprimality relation

$$\overline{a}_0 \overline{g} + \overline{b}_0 \overline{h} = 1 \in k[X],$$

and taking for $\pi \in \mathfrak{m}$ the largest of the finitely many coefficients that occur in the polynomials $f - g_0 h_0$ and $a_0 g_0 + b_0 h_0 - 1$ in $\mathfrak{m}[X]$. Note that there is no need to assume that the valuation is discrete.

We now construct polynomials 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

$$\begin{aligned} \deg(g_1) &= s & f &\equiv g_1 h_1 \bmod \pi^2 A[X] \\ \deg(h_1) &\leq n - s & a_1 g_1 + b_1 h_1 &\equiv 1 \bmod \pi^2 A[X]. \end{aligned} \tag{2.13}$$

Once we can do this, we can iterate the construction to obtain sequences of polynomials $g_i, h_i \in A[X]$ of degree $\deg(g_i) = s$ and $\deg(h_i) \leq n - s$ satisfying $f \equiv g_i h_i \bmod \pi^{2^i} A[X]$. The sequences g_i, h_i then converge *quadratically* in $A[X]$ as we have

$$\begin{aligned} g_{i+1} &\equiv g_i \bmod \pi^{2^i} A[X] \\ h_{i+1} &\equiv h_i \bmod \pi^{2^i} A[X]. \end{aligned}$$

The limits $g = \lim_{i\to\infty} g_i$ and $h = \lim_{i\to\infty} h_i$ yield the desired factorization $f = gh \in A[X]$.

To construct g_1 and h_1, we need polynomials $u, v \in A[X]$ of degree $\deg(u) < s$ and $\deg(v) \leq n - s$ such that $g_1 = g_0 + \pi u$ and $h_1 = h_0 + \pi v$ satisfy $f \equiv g_1 h_1 \bmod \pi^2 A[X]$. Writing $f = g_0 h_0 + \pi r_0$ with $r_0 \in A[X]$, this amounts to achieving the congruence

$$v g_0 + u h_0 \equiv r_0 \bmod \pi A[X]. \tag{2.14}$$

Multiplying our congruence $a_0 g_0 + b_0 h_0 \equiv 1 \bmod \pi A[X]$ by r_0 yields

$$a_0 r_0 g_0 + b_0 r_0 h_0 \equiv r_0 \bmod \pi A[X],$$

but $b_0 r_0$ is typically of degree $\geq s$. We therefore take for u the *remainder* of $b_0 r_0 \in A[X]$ upon division by the polynomial g_0 of degree s, which has its highest coefficient in A^*. This yields $u \in A[X]$ of degree $\deg(u) < s = \deg(g_0)$ satisfying $u \equiv b_0 r_0 \bmod g_0 A[X]$. We now have a congruence

$$u h_0 \equiv b_0 r_0 h_0 \equiv r_0 \bmod (\pi A[X] + g_0 A[X]),$$

so we can write $r_0 - u h_0 \equiv v g_0 \bmod \pi A[X]$ for some polynomial $v \in A[X]$ of degree at most $n - s$, as required in (2.14), to obtain the first congruence in (2.13).

Finally, 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 polynomials $a_1 = (1 - \pi t) a_0$ and $b_1 = (1 - \pi t) b_0$ in $A[X]$ to achieve the second congruence $a_1 g_1 + b_1 h_1 = (1 - \pi t)(1 + \pi t) \equiv 1 \bmod \pi^2 A[X]$ in (2.13). □

Exercise 5. For $f = 2X^2 + X + 2 \in \mathbf{Z}_2[X]$, we can take $\overline{g} = X$ and $\overline{h} = 1 \in \mathbf{F}_2[X]$. Find a few approximations $g_0, g_1, g_2, \ldots$ to the linear factor g of f.

For $\bar{g} = X - \overline{\alpha}$ a linear factor of $\bar{f}$, the hypothesis in Theorem 2.10 that $\bar{g}$ be coprime to $\overline{h} = \overline{f}/\overline{g}$ amounts to requiring that $\overline{\alpha}$ be a *simple* root of $\overline{f} \in k[X]$.

2.15. Corollary. *Let $f \in A[X]$ be a polynomial. Then every simple zero $\overline{\alpha} \in k = A/\mathfrak{m}$ of $\overline{f} \in k[X]$ can uniquely be lifted to a zero $\alpha \in A$ of f satisfying $(\alpha \bmod \mathfrak{m}) = \overline{\alpha}$.* □

Suppose $g_0 = X - \alpha_0 \in A[X]$ has reduction $X - \overline{\alpha} \in k[X]$ in the situation of corollary 2.15. Then we can write

$$f = (X - \alpha_0) h_0 + \pi \in A[X] \quad \text{with} \quad \pi = f(\alpha_0) \in \mathfrak{m},$$

and taking $r_0 = 1$ in the proof of Theorem 2.12, we obtain $g_1 = g_0 + \pi u$, with $u = b_0(\alpha) \in A^*$ some element that is the inverse (modulo πA, or simply in A) of

$$h_0(\alpha_0) = \left[\frac{f(X) - f(\alpha_0)}{X - \alpha_0}\right]_{X=\alpha_0} = f'(\alpha_0) \in A^*.$$

Iterating the process in which $g_0 = X - \alpha_0$ gets replaced by $g_1 = X - \alpha_1$, with

$$\alpha_1 = \alpha_0 - \frac{f(\alpha_0)}{f'(\alpha_0)}, \tag{2.16}$$

we obtain a classical root approximation method known as *Newton iteration*. It amounts to replacing α_0 by the zero α_1 of the linear approximation ('tangent line') to the function f in the point $(\alpha_0, f(\alpha_0))$. Non-archimedean Newton iteration converges not only for lifts of simple roots of $\overline{f} \in k[X]$, but also for 'sufficiently accurate' root approximations α_0, as follows.

2.17. Theorem. *Let K be complete under a non-archimedean valuation $|\,.\,|$. Suppose that $f \in A[X]$ is a polynomial, and $\alpha_0 \in A$ an element for which we have*

$$|f(\alpha_0)| < |f'(\alpha_0)|^2.$$

Then iteration of (2.16) yields a sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ in A converging to the unique zero $\alpha \in A$ of f satisfying

$$|\alpha - \alpha_0| \leq |f(\alpha_0)|/|f'(\alpha_0)|.$$

Proof. For $f \in A[X]$ of degree n there exist polynomials $f_i \in A[X]$ such that we have

$$f(X+Y) = \sum_{i=0}^{n} f_i(X) Y^i. \tag{2.18}$$

We have $f_0 = f$ and, by definition, $f_1 = f'$.

By assumption, the element $\pi_0 = f(\alpha_0)/f'(\alpha_0)^2$ is in the maximal ideal $\mathfrak{m} \subset A$, and so is $\delta_0 = -f(\alpha_0)/f'(\alpha_0)$, as we have $|\delta_0| < |f'(\alpha_0)| \leq 1$. Define $\alpha_1 = \alpha_0 + \delta_0$ as in (2.16). Putting $X = \alpha_0$ and $Y = \delta_0$ in (2.18) for our polynomial f, we find

$$f(\alpha_1) = f(\alpha_0) + \delta_0 f'(\alpha_0) + \textstyle\sum_{i=2}^{n} f_i(\alpha_0)\delta_0^i = \sum_{i=2}^{n} f_i(\alpha_0)\delta_0^i \in \delta_0^2 A.$$

For f', we obtain $f'(\alpha_1) \in f'(\alpha_0) + \delta_0 A$, so we have $|f'(\alpha_1)| = |f'(\alpha_0)| \neq 0$. From

$$|f(\alpha_1)| \leq |\delta_0^2| = |\pi_0| \cdot |f(\alpha_0)| < |f(\alpha_0)|$$

we see that in the next iteration step, $\pi_1 = f(\alpha_1)/f'(\alpha_1)^2$ and $\delta_1 = -f(\alpha_1)/f'(\alpha_1)$ satisfy

$$|\pi_1| \leq |\pi_0| \cdot |f(\alpha_0)| < |\pi_0| \qquad \text{and} \qquad |\delta_1| \leq |\pi_0| \cdot |\delta_0| < |\delta_0|.$$

It follows that the limit $\alpha = \lim_{i\to\infty} \alpha_i = \alpha_0 + \sum_{i=0}^{\infty} \delta_i$ is a zero of f satisfying $|f'(\alpha)| = |f'(\alpha_0)|$ and the inequality $|\alpha - \alpha_0| = |\sum_{i=0}^{\infty} \delta_i| \leq |\delta_0|$.

Suppose $\beta \neq \alpha$ is an other zero of f satisfying $|\beta - \alpha_0| \leq |\delta_0|$. Then $\delta = \beta - \alpha \neq 0$ satisfies $|\delta| = |(\beta - \alpha_0) - (\alpha - \alpha_0)| \leq |\delta_0|$ by the ultrametric inequality, and applying (2.18) with $X = \alpha$ and $Y = \delta$ we find

$$f(\beta) = 0 = 0 + \delta f'(\alpha) + \delta^2 a$$

for some $a \in A$. Dividing by δ we find $f'(\alpha) \in \delta A$, contradicting the estimate

$$|\delta| \leq |\delta_0| < |f'(\alpha_0)| = |f'(\alpha)|.$$

□

2.19. Example. For p an *odd* prime and $a \in \mathbf{Z}_p^*$, the polynomial $X^2 - \overline{a} \in \mathbf{F}_p[X]$ has two distinct roots in $\mathbf{F}_p$ if and only if $(a \bmod p) \in \mathbf{F}_p^*$ is a square. By corollary 2.15, this is equivalent to $a \in \mathbf{Z}_p^*$ being a square. We conclude that we have a natural isomorphism

$$\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^2 \xrightarrow{\sim} \mathbf{F}_p^*/(\mathbf{F}_p^*)^2 \cong \{\pm 1\},$$

and that the subgroup $(\mathbf{Z}_p^*)^2$ of squares in $\mathbf{Z}_p^*$ is of index 2.

For $p = 2$ and $a \in \mathbf{Z}_2^*$, the polynomial $X^2 - \overline{a} = X^2 + 1 = (X+1)^2 \in \mathbf{F}_2[X]$ has a double root, and Theorem 2.17 implies that $\alpha_0 = 1 \in \mathbf{Z}_2$ can be refined to an actual root of $X^2 - a$ in $\mathbf{Z}_2$ if we have $|1 - a|_2 < |2|^2$, i.e., for $a \in 1 + 8\mathbf{Z}_2$. As any element $1 + 2x \in \mathbf{Z}_2^*$ has square $1 + 4x(x+1) \in 1 + 8\mathbf{Z}_2$, we conclude that $(\mathbf{Z}_p^*)^2 = 1 + 8\mathbf{Z}_2$ is of index 4 in $\mathbf{Z}_2^*$.

Exercise 6. Compute a couple of p-adic digits of the square roots of $-1 \in \mathbf{Q}_5$ and $-7 \in \mathbf{Q}_2$.

2.20. Example. The polynomial $X^p - X = \prod_{i=0}^{p}(X - i) \in \mathbf{F}_p[X]$ splits into p distinct linear factors over the finite field $\mathbf{F}_p$, so by corollary 2.15 the polynomial $X^{p-1} - 1$ has $p - 1$ distinct roots in $\mathbf{Q}_p$. Every non-zero residue class $a \in \mathbf{F}_p^*$ lifts uniquely to a $(p-1)$-st root of unity $t_a \in \mathbf{Z}_p^*$, and the map $a \mapsto t_a$ provides a splitting of the natural exact sequence of groups

$$1 \to 1 + p\mathbf{Z}_p \longrightarrow \mathbf{Z}_p^* \longrightarrow \mathbf{F}_p^* \to 1.$$

With $t_0 = 0$, the set $S = \{t_a : a \in \mathbf{F}_p\}$ of *Teichmüller representatives* provides a multiplicatively closed set of digits that can be used for p-adic expansions in $\mathbf{Q}_p$.

Exercises.

7. Show that the ordinary absolute value on $\mathbf{C}$ does not extend to a valuation on the rational function field $\mathbf{C}(X)$.
8. 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 $X - \alpha$.
9. Show that $\mathbf{Q}_p$ is transcendental over $\mathbf{Q}$. What is its transcendence degree?
10. *(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.

11. Show that the Teichmüller representative t_a of $a \in \mathbf{F}_p$ equals $t_a = \lim_{i\to\infty} A^{p^i} \in \mathbf{Z}_p$, for A any integer with residue class a.

12. *(Newton iteration in* $\mathbf{R}$*.)* For a differentiable function $f\colon \mathbf{R} \to \mathbf{R}$ and a point $x_0 \in \mathbf{R}$, the sequence of Newton iterates $\{x_n\}_{n=1}^{\infty} \subset \mathbf{R}$ is defined as in (2.16) by

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

This is well defined if we have $f'(x_n) \neq 0$ for each x_n.

a. Suppose f is twice continuously differentiable on $\mathbf{R}$ and $x \in \mathbf{R}$ is a zero of f with $f'(x) \neq 0$. Show that there is an open neighborhood U of x in $\mathbf{R}$ such that x_n converges to x for each initial value $x_0 \in U$.

b. Does there exist a constant $C = C(f) > 0$ in (a) such that we have

$$|x_{n+1} - x| < C|x_n - x|^2$$

for all starting values $x_0 \in U$?

c. Take $f = X^3 - X \in \mathbf{R}[X]$. Determine how large U can be taken for each of the zeroes of f. Can you describe $\lim_{n\to\infty} x_n$ (if it exists) as a function of x_0?

13. 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) for $p \neq p'$.

14. Show that $\mathbf{Q}_p$ has only finitely many quadratic extensions (up to $\mathbf{Q}_p$-isomorphism), and determine their exact number.

15. 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.

16. 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.

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

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

define continuous group homomorphisms

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

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 $\phi\big|_{\mathbf{Q}}$ is trivial, and consists of the p-power roots of unity in K if $\phi\big|_{\mathbf{Q}}$ is p-adic.

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

19. Show that every complete non-archimedean field K with residue class field k of characteristic zero has a coefficient field.
[Hint: the valuation ring A contains a maximal subfield.]

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

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

22. Let F be a field and $P \in F[X]$ an irreducible separable polynomial with residue class field $E = F[X]/(P)$. Show that the completion of $F(X)$ with respect to the valuation ϕ_P defined in Theorem 1.21 is topologically isomorphic to the field $E((Y))$ of Laurent series over E.

23. Let K be a field with a non-archimedean valuation φ, Denote the valuation ring and its maximal ideal by A and $\mathfrak{m}$.

    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 $\mathfrak{m} \subset S$, and if φ is discrete than $S \subset A$.
    b. Suppose that φ is non-trivial and that K is complete with respect to φ. Prove that any discrete valuation on K is equivalent to φ.
    c. For $i = 0$, 1, let K_i be a field that is complete with respect to a discrete valuation. Prove that any field homomorphism $K_0 \to K_1$ of which the image is not contained in the valuation ring of K_1 is continuous.
    d. Show that the fields $\mathbf{Q}_p$ for p prime or $p = \infty$ have no field automorphism except the identity.

3 Extending valuations

If $K \subset L$ is a field extension, extending a valuation ϕ on K to a valuation ψ on L means finding a prime – in the sense of equivalence class of valuations – of L extending the prime of K corresponding to ϕ. In the case of archimedean ϕ, it follows from Corollary 2.5 that extending ϕ amounts to extending the embedding $K \to K_\phi \subset \mathbf{C}$ to an embedding $L \to \mathbf{C}$, with complex conjugate extensions giving rise to the same extension valuation.

For non-archimedean ϕ, the situation is similar in the case of *algebraic* extensions $K \subset L$: extending ϕ amounts to finding a K-embedding of L in an algebraic closure $\overline{K}_\phi$ of the completion K_ϕ of K, to which ϕ can uniquely be extended (Corollary 3.7), and two such K-embeddings $L \to K_\phi$ give rise to the same extension valuation if and only if they differ by an automorphism of $\overline{K}_\phi$ over K_ϕ. In view of Theorem 1.20, this provides a way (Theorem 3.13) to phrase the classical problem of extending primes in number field extensions that was treated in [NR, §2 and 3] as a problem of factoring polynomials over local fields.

In the case of purely transcendental extensions $K \subset L$, non-archimedean valuations extend in many ways, as we can extend ϕ on K to the rational function field $K(X)$ by picking $\phi(X) \in \mathbf{R}_{>0}$ arbitrarily (exercise 1.18). Using Zorn's lemma, one can obtain exotic valuations like p-adic valuations on $\mathbf{R}$ (exercise 7), but these are not of arithmetical relevance.

We will show first that ϕ extends uniquely to every finite extension $K \subset L$ in case K is complete with respect to ϕ. This is because such extensions provide a *vector norm* on the K-vector space L, and, in case K is complete, all vector norms on finite dimensional K-vector spaces are equivalent.

▶ Vector spaces over complete fields

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

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

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

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

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

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

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

$$||\sum_i k_i\omega_i|| = \max_i \phi(k_i) \tag{3.1}$$

under which convergence amounts to coordinate-wise convergence with respect to the basis. If K is complete, this is up to equivalence the only vector norm on V.

3.2. 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 define the associated vector norm $||\cdot||_1$ as in (3.1). Then V is complete with respect to this norm, as K is complete with respect to ϕ. Any other norm $||\cdot||_2$ on V is continuous with respect $||\cdot||_1$, as we have inequalities

$$||\sum_{i=1}^n a_i\omega_i||_2 \le \sum_{i=1}^n \phi(a_i)||\omega_i||_2 \le \max_i \phi(a_i)\cdot\sum_{i=1}^n ||\omega_i||_2 = C_2\cdot||\sum_{i=1}^n a_i\omega_i||_1$$

with $n = \dim_K V$ and $C_2 = \sum_{i=1}^n ||\omega_i||_2$. For the opposite inequality $C_1||x||_1 \le ||x||_2$, whose validity is unchanged if we replace x by kx for some $k \in K^*$, we need to show that $||\cdot||_2$ is bounded from below by some positive real constant C_1 on the unit sphere $S = \{x \in V : \ ||x||_1 = 1\}$ or, equivalently, on the union $Z = \bigcup_{i=1}^n V_i$ of the affine subspaces $V_i = \omega_i + \sum_{j\ne i} K\cdot\omega_j \subset V$.

For a local field K, this assertion is immediate as the unit ball $B = \{x \in V : \ ||x||_1 \le 1\}$ and therefore the unit sphere $S = \{x \in V : \ ||x||_1 = 1\}$ are $||\cdot||_1$-compact in V, such that the $||\cdot||_1$-continuous function $||\cdot||_2$ assumes a positive minimum C_1 on S.

For arbitrary complete K, we can argue by induction on $n = \dim_K V$, the case $n = 1$ being trivial. The induction hypothesis implies that in the topology induced by $||\cdot||_2$, every $(n-1)$-dimensional subspace $\sum_{j\ne i} K\cdot\omega_j \subset V$ is complete and therefore closed. The translates V_i and their union $Z = \bigcup_{i=1}^n V_i$ are therefore also $||\cdot||_2$-closed in V, and do not contain 0. This implies that there exists an open ball $\{x \in V : \ ||x||_2 < C_1\}$ around 0 that is disjoint from Z, and we obtain our lower bound. □

For a finite extension L of a field K that is complete under a valuation ϕ satisfying the triangle inequality, every extension valuation ψ of ϕ to L is a vector norm, as it also satisfies the triangle inequality. By Lemma 3.2, the topology on L induced by ψ does not depend on a choice of ψ, so Proposition 1.13 implies that *if* there exists an extension ψ of ϕ to L, it is necessarily unique.

▶ Extending valuations: complete case

Let K be complete with respect to ϕ, and $K \subset L$ a finite extension. Then every $x \in L$ has only finitely many K-conjugates inside a normal closure M of L over K, and they are of the form $\sigma(x)$ for some K-automorphism σ of M. If ψ is a valuation on M extending ϕ, we have $\psi\circ\sigma = \psi$ by the uniqueness of ψ. As the norm $N_{L/K}(x) \in K$ is a product of $[L:K]$ (not necessarily distinct) K-conjugates of x, we have $\psi(x)^{[L:K]} = \psi(N_{L/K}(x)) = \phi(N_{L/K}(x))$, so the extension ψ is necessarily given on L by the formula

$$\psi(x) = \phi(N_{L/K}(x))^{1/[L:K]} \tag{3.3}$$

that we already encountered in the special case of Lemma 2.3.

It is clear that (3.3) defines a function ψ satisfying the first two conditions of definition 1.3, but the validity of the third condition

$$\psi(x) \leq 1 \Rightarrow \psi(1+x) \leq C \tag{3.4}$$

for some $C \in \mathbf{R}_{>0}$, which shows that ψ is a valuation on L, is not immediate. In the important special case that K is a local field, one can use the continuity of $x \mapsto \psi(1+x)$ on the compact unit ball $\{x \in L : \ \psi(x) \leq 1\}$ to obtain the required constant C.

Exercise 1. Complete the details of this proof.

This argument can be extended to the general case [10], but it is easier to derive the archimedean case from Theorem 2.4, and treat the non-archimedean case separately.

3.5. Theorem. *Let K be complete with respect to ϕ and $K \subset L$ a finite extension. Then ϕ extends uniquely to a valuation ψ on L. It is given by*

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

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

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

For ϕ non-archimedean, we show that (3.4) is satisfied with $C = 1$. As the norm $N_{L/K}(x)$ is the constant coefficient of the characteristic polynomial of x, which is a power of the minimal polynomial f_K^x of x, this amounts to proving the implication

$$\phi(f_K^x(0)) \leq 1 \Longrightarrow \phi(f_K^x(-1)) \leq 1.$$

More generally, we claim that for $f \in K[X]$ monic irreducible, we have an equivalence

$$f(0) \in A \Longleftrightarrow f \in A[X], \tag{3.6}$$

where $A \subset K$ denotes the valuation ring of ϕ. Indeed, if f is not in $A[X]$, let $t \in K^*$ be a coefficient of f of maximal absolute value $\phi(t) > 1$. Then we have $t^{-1} \in \mathfrak{m}$ and $t^{-1}f \in A[X] \setminus \mathfrak{m}[X]$, with $\mathfrak{m}$ the maximal ideal of A. If we have $f(0) \in A$, then the highest and the lowest coefficient of $t^{-1}f$ are in $\mathfrak{m}$, so $\overline{X}^s$ divides $\overline{tf}$ in $k[X] = (A/\mathfrak{m})[X]$ for some $s \geq 1$. If we take s maximal, then $\overline{X}^s$ is a simple factor of $\overline{t^{-1}f}$ of degree $s < \deg f$. By Hensel's lemma, it lifts to a factor of degree s of $t^{-1}f$ (and therefore of f) in $K[X]$, contradicting the irreducibility of f. □

3.7. Corollary. *Let K be a complete non-archimedean field, and A_K its valuation ring. Then the valuation on K extends uniquely to an algebraic closure $\overline{K}$ of K, and its valuation ring $A_{\overline{K}} \subset \overline{K}$ is the integral closure of A_K in $\overline{K}$.*

Proof. By Theorem 3.5, the unique extension ψ of the valuation ϕ on K to $\overline{K}$ is given by

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

The equivalence (3.6), applied to f_K^x, shows that we have $\psi(x) \leq 1$ if and only if $f_K^x \in A[X]$, i.e., if and only if x is in the integral closure of A in $\overline{K}$. □

In the typical case where the extension $K \subset \overline{K}$ is of infinite degree, Lemma 3.2 does not apply, and $\overline{K}$ will not be complete with respect to the extension valuation. See **.

► Ramification index and residue class degree

Let $K \subset L$ be a field extension and ψ a valuation on L that extends a non-archimedean valuation ϕ on K. Then the *ramification index* $e(\psi/\phi)$ of ψ over ϕ is the group index

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

of the value group $\phi[K^*] = \psi[K^*]$ inside $\psi[L^*] \subset \mathbf{R}_{>0}$, and the *residue class degree* $f(\psi/\phi)$ of ψ over ϕ is the degree

$$f(\psi/\phi) = [\ell : k]$$

of the extension of residue class fields. Note that these quantities, when finite, are multiplicative in a tower $K \subset L \subset M$ of valued fields.

For $K \subset L$ an extension of number fields and $\mathfrak{q} \subset \mathcal{O}_L$ a prime lying above $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, we defined [NR, §3] the ramification index $e(\mathfrak{q}/\mathfrak{p}) = \mathrm{ord}_{\mathfrak{q}}(\mathfrak{p}\mathcal{O}_L)$ as the exponent to which $\mathfrak{q}$ occurs in the factorization of $\mathfrak{p}\mathcal{O}_L$. Define $\phi_{\mathfrak{q}}$ as in Theorem 1.20, with $\phi_{\mathfrak{p}} = \phi_{\mathfrak{q}}|_K$. As we have

$$\mathrm{ord}_{\mathfrak{q}}(x) = e(\mathfrak{q}/\mathfrak{p}) \cdot \mathrm{ord}_{\mathfrak{p}}(x) \quad \text{for} \quad x \in K^*,$$

$\phi_{\mathfrak{q}}[K^*] \subset \phi_{\mathfrak{q}}[L^*] \cong \mathbf{Z}$ is a subgroup of index $e(\phi_{\mathfrak{q}}/\phi_{\mathfrak{p}}) = e(\mathfrak{q}/\mathfrak{p})$. Moreover, as $k_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$ is the residue class field of $\phi_{\mathfrak{q}}$, the residue class field degree $f(\phi_{\mathfrak{q}}/\phi_{\mathfrak{p}})$ equals the residue class degree $f(\mathfrak{q}/\mathfrak{p}) = [k_{\mathfrak{q}} : k_{\mathfrak{p}}]$ for primes from [NR, §3].

Suppose $R \subset L^*$ is a set of elements having residue classes in ℓ that are linearly independent over k, and $S \subset L^*$ a set of elements with valuations in $\psi[L^*]$ that lie in different cosets of $\phi[K^*]$. We claim that the elements $rs \in L$ with $r \in R$ and $s \in S$ are linearly independent over K. To see this, suppose we have a K-linear dependency

$$\sum_{(r,s)\in R\times S} a_{rs} rs = 0$$

with finitely many non-zero coefficients $a_{rs} \in K$. Fix $s \in S$, and suppose $\alpha_s = \sum_{r\in R} a_{rs} r$ has a non-zero coefficient a_{rs}. Pick $a_{rs} \in K^*$ with $\phi(a_{rs}) = \max_r \phi(a_{rs}) > 0$. Then $a_{rs}^{-1}\alpha_s$ has non-zero residue in ℓ by definition of R, and valuation $\psi(a_{rs}^{-1}\alpha_s) = 1$. We find $\alpha_s \neq 0$ and $\psi(\alpha_s) = \phi(a_{rs}) \in \phi[K^*]$, so all non-zero terms in the sum $\sum_{s\in S} \alpha_s s = 0$ have different valuation by definition of S. By (1.10) we conclude that all α_s equal 0, so no coefficient a_{rs} can be non-zero, as claimed. We obtain the following universal inequality.

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

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

Proof. We have $\#R \cdot \#S \leq [L : K]$ for integers $\#R \leq f(\psi/\phi)$ and $\#S \leq e(\psi/\phi)$. □

For K a complete non-archimedean field, the valuation extends uniquely to every finite extension $K \subset L$ by Theorem 3.5, and we write $e_{L/K}$ and $f_{L/K}$ for the associated ramification index and residue class degree, which are finite by Theorem 3.8. In the important case where K is complete with respect to a *discrete* valuation, the inequality $e_{L/K}f_{L/K} \leq [L : K]$ is an equality, and an explicit *integral basis* for the valuation ring A_L as a module over A_K.

3.9. Theorem. *For K complete with respect to a discrete valuation and $K \subset L$ a finite extension we have*

$$e_{L/K}f_{L/K} = [L : K].$$

Moreover, with $\pi_L \in A_L$ a uniformizer and residue classes of $r_1, r_2, \ldots, r_{f_{L/K}} \in L^*$ forming a k-basis for ℓ, we have

$$A_L = \bigoplus_{1 \leq i \leq f_{L/K},\ 0 \leq j < e_{L/K}} A_K \cdot r_i \pi_L^j.$$

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

The second statement is an application of Theorem 2.10. More precisely, write $e = e_{L/K}$ and $f = f_{L/K}$, and let $S_K \subset A_K$ be a set of representatives of A_K modulo its maximal ideal $\mathfrak{m}_K$ that contains 0. Then the set $S_L = \sum_{i=1}^{f} S_K \cdot r_i = \{\sum_{i=1}^{f} s_i r_i : \ s_i \in S_K \text{ for all } i\}$ is a set of representatives of A_L modulo its maximal ideal $\mathfrak{m}_L$ that contains 0.

With π_K and π_L uniformizers in A_K and A_L, we have $\mathfrak{m}_L^e = \pi_L^e A_L = \pi_K A_L$, so the powers of $\mathfrak{m}_L$ are generated by the elements of the form $\pi_L^j \pi_K^m$ with $m \in \mathbf{Z}_{\geq 0}$ and $0 \leq j < e$. By Theorem 2.10, every $x \in A_L$ has a unique representation

$$x = \sum_{1 \leq i \leq f,\ 0 \leq j < e} \Big(\sum_{m=0}^{\infty} s_{ijm} \pi_K^m\Big) r_i \pi_L^j,$$

proving the desired statement. □

In the case where $k \subset \ell$ is separable, we have $\ell = k(\overline{x})$, and we can take $r_i = x^{i-1}$ for an element $x \in A_L$ with residue class $\overline{x} \in \ell$. Then $A_L = A_K[x, \pi_L]$ is a free A_K-module with basis

$$\{x^i \pi_L^j : \ 0 \leq i < f_{L/K},\ 0 \leq j < e_{L/K}\}.$$

If $g \in A_K[X]$ is monic with reduction $f_k^{\overline{x}} \in k[X]$, we have $g(x) \in \mathfrak{m}_L$. If $g(x)$ generates $\mathfrak{m}_L$, we can take $\pi_L = g(x) \in A_K[x]$ to obtain $A_L = A_K[x]$. If not, we have $g(x) \in \mathfrak{m}_L^2$, but

$g'(x) \in A_L^*$, by the separability of $\overline{g} = f_k^{\overline{x}} \in k[X]$. Thus, after replacing x by $x + \pi_L$, which has the same reduction $\overline{x} \in \ell$, the element

$$g(x + \pi_L) \in g(x) + g'(x)\pi_L + \mathfrak{m}_L^2 = g'(x)\pi_L + \mathfrak{m}_L^2$$

is a uniformizer, and we see that $A_L = A_K[x + \pi_L]$ is *monogenic* as an A_K-algebra: it can be generated over A_K by a single element.

3.10. Theorem. *Let $K \subset L$ be a finite extension of complete discretely valued fields, and suppose the residue class field extension $k \subset \ell$ is separable. Then there exists $\alpha \in A_L$ such that we have $A_L = A_K[\alpha]$.* □

Note that, in contrast to Theorems 3.9 and 3.10, extensions $\mathcal{O}_K \subset \mathcal{O}_L$ of rings of integers in number fields do not in general have integral bases, and are not in general monogenic.

For non-discrete valuations, the inequality $e_{L/K} f_{L/K} \leq [L : K]$ in Theorem 3.8 can actually be strict.

3.11. Example. As the prime 2 is totally ramified in the cyclotomic extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_{2^n})$ of degree 2^{n-1} for all $n > 1$, the extension $\mathbf{Q}_2 \subset L_n = \mathbf{Q}_2(\zeta_{2^n})$ of complete fields has $e_{L_n/\mathbf{Q}_2} = 2^{n-1}$ and $f_{L_n/\mathbf{Q}_2} = 1$. The subextension $K_n = \mathbf{Q}_2(\zeta_{2^n} + \zeta_{2^n}^{-1}) \subset L_n$ is quadratic with $e_{L_n/K_n} = 2$, and we explicitly have

$$\mathrm{ord}_2[K_n^*] = 2^{2-n}\mathbf{Z} \overset{2}{\subset} \mathrm{ord}_2[L_n^*] = 2^{1-n}\mathbf{Z} \qquad \text{for } n > 1.$$

The field $L_\infty = \bigcup_{n>1} L_n = \mathbf{Q}_2(\zeta_{2^\infty})$ is an infinite algebraic extension of $\mathbf{Q}_2$ to which the 2-adic valuation, or, equivalently, the exponential valuation ord_2, extends uniquely, with value group

$$\mathrm{ord}_2[L_\infty^*] = \bigcup_{n>1} 2^{1-n}\,\mathbf{Z} = \mathbf{Z}[\tfrac{1}{2}] = \{\tfrac{a}{2^k} : a \in \mathbf{Z}, k \in \mathbf{Z}_{\geq 0}\} \tag{3.12}$$

and residue class field $\mathbf{F}_2$. By Lemma 2.7, the completion L of L_∞ is a complete non-archimedean field having the same residue class field and value group as L_∞. The $\mathbf{Q}_2$-automorphism $\sigma : \zeta \mapsto \zeta^{-1}$ of L_∞ sending every 2-power root of unity $\zeta \in L_\infty$ to its inverse extends to an automorphism of L of order 2, and its invariant field K is the completion of $K_\infty = \bigcup_{n>1} K_n$. As we have $\mathrm{ord}_2[L^*] = \mathrm{ord}_2[K^*] = \mathbf{Z}[\frac{1}{2}]$ the extension $K \subset L$ of complete fields has $e_{L/K} f_{L/K} = 1 < 2 = [L : K]$. It is 'caused' by the fact that a *non-discrete* value group like $\mathbf{Z}[\frac{1}{2}] \subset \mathbf{R}$, which is 2-*divisible* (i.e., every element in it is of the form $2x$ for some element x in the group) does not have a subgroup of index 2.

Exercise 2. Prove the various statements made in this example.

▶ Extending valuations: general case

We now treat the analogue of Theorem 3.5 in the case that K is not necessarily complete with respect to ϕ. As valuations extend uniquely in purely inseparable extensions (exercise 8), we

can and will restrict our attention to the case of finite separable extensions $K \subset L$. Such L can be given explicitly as $L = K[X]/(g)$ for some monic irreducible polynomial $g \in K[X]$. We now obtain an extension of ϕ to L for every irreducible factor that g has over the completion K_ϕ of K.

3.13. Theorem. *Let ϕ be a valuation on K, and $K \subset L$ a finite separable extension. Then we have a canonical isomorphism of K_ϕ-algebras*

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

Writing $L = K[X]/(g)$ with $g \in K[X]$ monic irreducible, the extension valuations $\psi|\phi$ on L correspond to the monic irreducible factors $g_i|g$ in $K_\phi[X]$, with

$$L = K[X]/(g) \longrightarrow K_\phi[X]/(g_i) = L_\psi$$

the completion of L induced by g_i.

Proof. A completion L_ψ at an extension valuation ψ comes with natural K-homomorphisms $L \to L_\psi$ and $K_\phi \to L_\psi$, so there is a canonical map $h_\psi \colon K_\phi \otimes_K L \to L_\psi$ for each such ψ. The image of h_ψ contains the dense subfield L, and as it has finite dimension over K_ϕ it is closed by Lemma 3.2. Thus L_ψ is a quotient of the K_ϕ-algebra $K_\phi \otimes_K L$.

Writing $L = K[X]/(g)$, we can factor the separable polynomial $g \in K[X]$ over K_ϕ into distinct monic irreducibles as $g = \prod_{i=1}^t g_i \in K_\phi[X]$. By the Chinese remainder theorem, the quotients L_ψ of the K_ϕ-algebra

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

are the fields $L_{\psi_i} = K_\phi[X]/(g_i)$, with $(X \bmod g) \in L = K[X]/(g) \subset L_\psi$ corresponding to $X \bmod g_i$. Every factor $K_\phi[X]/(g_i)$ comes with a unique valuation $\psi_i|\phi$ by Theorem 3.5. As an L-isomorphism $K_\phi[X]/(g_i) \to K_\phi[X]/(g_j)$ of K_ϕ-algebras, which maps $X \bmod g_i$ to $X \bmod g_j$, does not exist for $i \neq j$, it follows from Lemma 3.2 that the valuations ψ_i and ψ_j are inequivalent on L for $i \neq j$. □

For ϕ the archimedean absolute value on $\mathbf{Q}$, we have $K_\phi = \mathbf{R}$ in Theorem 3.13, and L is a number field. The $\mathbf{R}$-algebra $L_\mathbf{R} = L \otimes_\mathbf{Q} \mathbf{R}$ is the Euclidean space we used in [NR] in Minkowski's geometry of numbers. As we noticed already after Corollary 2.6, this is the product of the archimedean completions of L.

For ϕ the p-adic valuation on $\mathbf{Q}$, we recover a formula that we already proved for Dedekind domains in [NR, Theorem 3.4].

3.14. Corollary. *For $K \subset L$ finite separable and ϕ a non-archimedean valuation on K, there are finitely many extensions ψ of ϕ to L, we have an inequality*

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

If ϕ is discrete, we have equality.

Proof. The isomorphism in Theorem 3.13 shows that the K_ϕ-dimension of $K_\phi \otimes_K L$ equals $\sum_{\psi|\phi}[L_\psi : K_\phi] = [L : K]$. We have $e(\psi/\phi)f(\psi/\phi) \leq [L_\psi : K_\phi]$ by Theorem 3.8, with equality for discrete ϕ by Theorem 3.9. □

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 call an extension $\psi|\phi$ of archimedean valuations (or primes) *ramified* if ϕ is real and ψ is complex. This convention, although somewhat arbitrary, is the natural one in the context of class field theory.

Theorem 3.13 shows that extending a valuation ϕ from K to L amounts to factoring a generating polynomial $g \in K[X]$ for L over the completion K_ϕ. Such factorizations can be found using Hensel's lemma from sufficiently accurate approximate factorizations. If ϕ is non-archimedean and g is separable over the residue class field k, we recover the Kummer-Dedekind theorem [NR, Theorem 3.1] for primes not dividing the discriminant of g. For more details we refer to exercise 11.

3.15. 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. For this, we need to factor the polynomial $f = X^4 - 17$, which has inseparable 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 by Theorem 2.17 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 of $\mathbf{Q}_2$-algebras

$$\begin{aligned} \mathbf{Q}_2 \otimes_{\mathbf{Q}} \mathbf{Q}(\alpha) &\xrightarrow{\sim} \mathbf{Q}_2 \times \mathbf{Q}_2 \times \mathbf{Q}_2(i) \\ x \otimes h(\alpha) &\longmapsto (xh(a), xh(-a), xh(ia)). \end{aligned}$$

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 16), we cannot easily apply the Kummer-Dedekind theorem here. ◊

A final consequence of 3.13 is the following relation between global and local norms and traces.

3.16. Corollary. *For $K \subset L$ 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 Theorem 3.13 gives the desired result. □

Exercises.

3. Let K be a field. Show that there exists a non-trivial valuation on K if and only if K is *not* an algebraic extension of a finite field.
   [Hint: use exercise 1.13.]

4. 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.

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

6. 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.

7. 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.

8. 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 G acts 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.

9. Let L/K be an extension of number fields and ϕ a non-trivial non-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 $\prod_{\psi|\phi} A_\psi$.

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

11. *(Kummer-Dedekind.)* Let $K \subset L = K(\alpha)$ be an extension of number fields for which $\alpha \in \mathcal{O}_L$ integral, and $\mathfrak{p} \subset \mathcal{O}_K$ a prime that does not divide the index $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Prove: if the reduction modulo $\mathfrak{p}$ of $f = f_K^\alpha$ factors as $\overline{f} = \prod_{i=1}^t \overline{g}_i^{e_i} \in k_\mathfrak{p}[X]$, then $\mathfrak{p}$ factors in $\mathcal{O}_L$ as $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^t \mathfrak{q}_i^{e_i}$, with $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$ the prime in $\mathcal{O}_L$ 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 $\overline{K}[X]/(\overline{g}_i)$.]

12. 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 minimal 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 $\psi(k) < \varepsilon$.

13. Let p be a rational prime (possibly $p = \infty$) and $\mathbf{Q}_p \subset F$ a finite extension.

    a. Show that there exist a number field K and a prime $\mathfrak{p}$ of K extending p such that the completion $K_\mathfrak{p}$ 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.

14. 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 minimal polynomial f such that $\overline{f}$ is the minimal 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.]

15. 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: $7^4 = 17 \bmod 149$.]

16. 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.

17. 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, equals $l_r(f) - s_r(f)$.

18. 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.

19. 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 complete fields

We let $K \subset L$ be a finite extension of a field K that is complete with respect to a non-archimedean valuation. Then L is complete under the extension valuation, and by Theorems 3.8 and 3.9 we have $e_{L/K} \cdot f_{L/K} \leq [L : K]$, with equality if the valuation is discrete.

If the residue class field extension $k \subset \ell$ of degree $f_{L/K}$ is *separable*, we can *canonically* 'lift' it (proposition 4.5) to obtain an intermediate extension

$$K \subset T = T_{L/K} \subset L$$

such that $K \subset T$ is *unramified* of degree $f_{L/K} = [\ell : k]$, with residue class field ℓ. This lifting property is a direct corollary of Hensel's lemma, and it gives rise to a canonical extension by a rigidity property (Corollary 4.4) of separable extensions $K \subset K(\alpha)$ of complete fields that follows from *Krasner's lemma* 4.1. Roughly speaking, it says that such extensions are unchanged under 'small perturbations' of the irreducible polynomial of α.

In the case of local fields, k is finite and the extension $k \subset \ell$ is cyclic with group generated by the Frobenius automorphism $x \mapsto x^{\#k}$. It follows that unramified extensions of local fields are always cyclic, with Galois group generated by a 'Frobenius automorphism' (corollary 4.8) that will play an essential role in class field theory.

The extension $T \subset L$ is not so easily described. We restrict to the case of discrete valuations, where it is totally ramified of degree $e = e_{L/K}$. In the *tame* case where e is not divisible by the characteristic $\mathrm{char}\,(k)$, we can write $L = T(\sqrt[e]{\pi_T})$ for some uniformizer π_T of T (Theorem 4.9). If $p = \mathrm{char}\,(k)$ does divide e, we can write $e = p^n \cdot e_0$ with $n = \mathrm{ord}_p(e)$ and obtain a further canonical intermediate extension L_1 in the tower

$$K \subset T \subset L_1 = T(\sqrt[e_0]{\pi_T}) \subset L$$

such that $T \subset L_1$ is totally and tamely ramified of degree e_0, and $L_1 \subset L$ totally and wildly ramified of degree p^n.

We always have $L = T(\pi_L)$ with $f_T^{\pi_L} \in A_T[X]$ an Eisenstein polynomial of degree e (Theorem 4.11), and this can be used to count the number of totally ramified extensions of a local field.

▶ Krasner's lemma

In the unique case $\mathbf{R} \subset \mathbf{C}$ of a non-trivial extension of archimedean complete fields, it is clear that if we 'move' a generator $\alpha \in \mathbf{C}$ of the extension over a distance at most $\frac{1}{2}|\alpha - \bar{\alpha}|$ inside $\mathbf{C}$, then the extension $\mathbf{R} \subset \mathbf{R}(\alpha) = \mathbf{C}$ is unchanged.

For non-archimedean complete fields K, there is a similar statement that is even slightly stronger because of the ultrametric inequality. To ease notation, we denote by $|\cdot|$ the unique extension of the valuation on K to the algebraic closure $\overline{K}$ from Corollary 3.7.

4.1. Krasner's lemma. *Let K be a non-archimedean complete field, and $\alpha \in \overline{K}$ an element that is separable over K. Suppose $\beta \in \overline{K}$ satisfies $|\beta - \alpha| < |\alpha - \alpha'|$ for every K-conjugate $\alpha' \neq \alpha$ of α. Then $K(\alpha)$ is contained in $K(\beta)$.*

Proof. The extension $K(\beta) \subset K(\beta, \alpha)$ is separable, and for every automorphism σ of $\overline{K}$ over $K(\beta)$, the ultrametric inequality (1.9) yields

$$|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \sigma(\beta) + \beta - \alpha| \leq \max\{|\sigma(\alpha) - \sigma(\beta)|, |\beta - \alpha|\} = |\beta - \alpha|,$$

as we have $\sigma(\beta) = \beta$ by assumption and $|\sigma(\alpha) - \sigma(\beta)| = |\alpha - \beta|$ by the uniqueness of the valuation on $\overline{K}$. For $\sigma(\alpha) = \alpha' \neq \alpha$ this contradicts our assumption, so σ fixes α, proving that we have $\alpha \in K(\beta)$, as claimed. □

In the case where β in the preceding lemma is known to be in $K(\alpha)$, we have $K(\alpha) = K(\beta)$, showing that 'slightly moving' α inside $K(\alpha)$ does not change the extension. In terms of the coefficients of the monic irreducible polynomial $f_K^\alpha \in K[X]$ of α, we can phrase this in terms of a 'neighborhood' of f_K^α. In order to do so, we define the norm $||\cdot|| : K[X] \to \mathbf{R}_{\geq 0}$ by $||\sum_k a_k X^k|| = \max_k |a_k|$ and, for $f \in K[X]$ a *monic* polynomial and $\varepsilon \in \mathbf{R}_{>0}$, we set

$$U(f, \varepsilon) = \{g \in K[X] \text{ monic} : \deg(f) = \deg(g) \text{ and } ||f - g|| < \varepsilon\}. \tag{4.2}$$

4.3. Theorem. *Let K be a non-archimedean complete field, and $f \in K[X]$ a monic separable polynomial that factors as $f = \prod_{i=1}^n (X - \alpha_i)$ over $\overline{K}$. Then there exists $\varepsilon \in \mathbf{R}_{>0}$ such that every polynomial $g \in U(f, \varepsilon) \subset K[X]$ factors as $g = \prod_{i=1}^n (X - \beta_i)$ and $K(\alpha_i) = K(\beta_i) \subset \overline{K}$ for $i = 1, 2 \ldots, n$.*

Proof. As f is separable, we have $\delta = \min_{i \neq j} |\alpha_i - \alpha_j| > 0$. For $g \in U(f, \varepsilon)$, the values $g(\alpha_i)$ and $g'(\alpha_i)$ will be arbitrarily close to $f(\alpha_i) = 0$ and $f'(\alpha_i) \neq 0$ if we take $\varepsilon \in \mathbf{R}_{>0}$ sufficiently small. Thus, we can choose $0 < \varepsilon < 1$ such that for $i = 1, 2, \ldots, n$, every $g \in U(f, \varepsilon)$ satisfies

$$|g(\alpha_i)|/|g'(\alpha_i)| < \min\{\delta, |g'(\alpha_i)|\}.$$

By Theorem 2.17, applied to the polynomial $g \in K(\alpha_i)[X]$ for the approximate root α_i of g satisfying $|g(\alpha_i)| < |g'(\alpha_i)|^2$, we see that for $i = 1, 2, \ldots, n$, the polynomial g has a unique zero $\beta_i \in K(\alpha_i)$ satisfying $|\beta_i - \alpha_i| < |g(\alpha_i)|/|g'(\alpha_i)| < \delta$. As the β_i are distinct by the ultrametric inequality and the definition of δ, we have $g = \prod_{i=1}^n (X - \beta_i)$. By Krasner's lemma 4.1, we have $K(\alpha_i) \subset K(\beta_i)$, hence $K(\alpha_i) = K(\beta_i)$. □

4.4. Corollary. *Let $K \subset L = K(\alpha)$ be a separable extension of complete fields defined by $f = f_K^\alpha \in K[X]$. Then all polynomials $g \in K[X]$ in a sufficiently small open neighborhood $U(f, \varepsilon)$ of f as in 4.2 are irreducible and define the same extension $K \subset L$.* □

▶ Unramified extensions

A finite extension $K \subset L$ of a complete non-archimedean field K is said to be *unramified* if the residue class field extension $k \subset \ell$ is separable of degree $f_{L/K} = [L : K]$. Such extensions have ramification index $e_{L/K} = 1$ in view of Theorem 3.8. For an extension $K \subset L$ of local fields, k is finite and the valuation discrete, so the extension is unramified if and only if it has $e_{L/K} = 1$.

Unramified extensions of complete fields arise as the *canonical lift* of their residue class field extension.

4.5. Proposition. *Let K be complete, $K \subset L$ a finite extension, and suppose that the residue class field extension $k \subset \ell$ is separable. Then there is a unique unramified subextension $K \subset U(\ell)$ of $K \subset L$ with residue class field extension $k \subset \ell$.*

Proof. As $k \subset \ell$ is finite separable, we can write $\ell = k(\overline{x})$, with irreducible polynomial $\overline{f} = f_k^{\overline{x}}$ separable in $k[X]$. As $\overline{x} \in \ell$ is a simple zero of $\overline{f}$, Corollary 2.15 tells us that *any* monic polynomial $f \in A_K[X]$ with reduction $\overline{f} \in k[X]$ has a unique root $x_f \in L$ with reduction $\overline{x} \in \ell$. Such f are irreducible in $K[X]$ as the reduction $\overline{f} \in k[X]$ is, so f is the irreducible polynomial of x_f over K. As $K \subset K(x_f)$ is a subextension of $K \subset L$ of degree $\deg f = [\ell : k]$ with separable residue class field extension $k \subset k(\overline{x}) = \ell$, it is unramified.

As *any* subextension $K \subset E$ of $K \subset L$ with residue class field ℓ contains the roots $x_f \in L$ for all lifts f of $\overline{f}$ by Corollary 2.15, the field $U(\ell) = K(x_f)$ depends on ℓ but not on the choice of the lift f, making $K \subset U(\ell)$ the unique unramified subextension of $K \subset L$ of degree $[\ell : k]$. □

We call $T = U(\ell)$ the *inertia field* (German: *Trägheitskörper*) of the extension $K \subset L$. As we have $e_{T/K} = 1$, the maximal ideal $\mathfrak{m}_K \subset A_K$ remains *inert* in $K \subset T$, i.e., it generates the maximal ideal of the valuation ring in A_T.

The construction of T as a primitive extension $K(x)$ in the proof of proposition 4.5 depends more on ℓ than on L. When performed for an arbitrary finite separable extension of $k \subset \ell$, it yields a finite unramified extension $K \subset U(\ell)$ inside a separable closure K^{sep} of K giving rise to that residue class field extension. Taking the union of all these finite unramified extensions of K inside K^{sep}, we obtain the *maximal unramified extension*

$$K \subset K^{\mathrm{unr}} \subset K^{\mathrm{sep}}.$$

We may describe the functoriality of its construction in categorical terms, viewing the intermediate fields of $K \subset K^{\mathrm{unr}}$ as the objects of a category $\mathbf{T}_{K^{\mathrm{unr}}/K}$ and their natural inclusions as the morphisms, and similarly for the category $\mathbf{T}_{k^{\mathrm{sep}}/k}$ of separable extensions of k inside a seprarable closure k^{sep}.

4.6. Theorem. *Let K be complete with residue class field k, and K^{unr} a maximal unramified extension of K. Then the residue class field functor $L \mapsto \ell$ on $\mathbf{T}_{K^{\mathrm{unr}}/K}$ maps K^{unr} to a separable closure k^{sep} of k, and induces an equivalence of categories*

$$\mathbf{T}_{K^{\mathrm{unr}}/K} \xrightarrow{\sim} \mathbf{T}_{k^{\mathrm{sep}}/k}.$$

Proof. The lift $U : \ell \mapsto U(\ell)$ in the proof of proposition 4.5 provides the required inverse functor. □

4.7. Corollary. *Let K be complete and L/K a finite unramified extension. Then L/K is Galois if and only if ℓ/k is Galois, and if these extensions are Galois their Galois groups are isomorphic.* □

We conclude that the maximal unramified extension K^{unr} is Galois over K with group $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(k^{\mathrm{sep}}/k)$. In particular, one finds that $\mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \widehat{\mathbf{Z}}$ when k is finite. On a finite level, this can be formulated as follows.

4.8. 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* $\mathrm{char}\, k$.

Proof. If k is finite of order $q = p^k$ with $p = \mathrm{char}\, k$, the unique extension k_n of degree n of 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 $f_k^{\overline{x}}$ is a factor of the cyclotomic polynomial $(\Phi_m \bmod p) \in k[X]$. As m is coprime to $p = \mathrm{char}\ K$, the polynomial Φ_m is separable over k and we can apply Hensel's lemma 2.12 to lift $f_k^{\overline{x}}$ 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.

▶ Tamely 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 $\mathrm{char}\, k = 0$, 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.

4.9. 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 $\ell = k$, so there exists $v \in A_K^*$ with $\overline{u} = \overline{v}$. The element $x = v\pi_K/\pi_L^e$ has residue class $\overline{x} = \overline{1} \in \ell$, so we can apply Hensel's lemma (as in 2.9) to the polynomial $X^e - x$, which has a root $\overline{1} \in \ell$ 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 $L = K(y\pi_L) = K(\sqrt[e]{v\pi_K})$. □

4.10. 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 $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p(\sqrt[p-1]{-p})$.*

Proof. 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 ℓ as

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

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

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 6). 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 7.

If $K \subset L$ is a finite extension of non-archimedean valued fields that is not tamely ramified, then either $k \subset \ell$ is inseparable or the ramification index e satisfies $\overline{e} = 0 \in k$. 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 where both $K \subset L$ and $k \subset \ell$ are separable, there can be many non-isomorphic wildly ramified extensions of the same degree (exercise 15)

▶ Totally ramified extensions

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 $a_0 \notin \mathfrak{p}_K^2$.

4.11. Theorem. *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 theorem 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.

4.12. 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 4.8), 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 theorem 4.11, 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 4.1), every point $w \in C$ that is sufficiently close to v gives rise to a polynomial $g \in A[X]$ that has the same splitting field as f. As C is compact, it follows that the Eisenstein polynomials of degree e in $A[X]$ have only finitely many different splitting fields in K^{sep}. It follows that there are only finitely many totally ramified extensions of degree e of K. □

▶ Different and discriminant

An important invariant to measure the ramification in an extension L/K is given by the different and the discriminant of the extension. We have already encountered these in the case of number fields, and the definitions are highly similar.

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 $\{\omega_1, \omega_2, \dots, \omega_n\}$ of A_L over A_K. Such a basis exists by 3.9, and the value of the discriminant is defined up to the square of a unit in A_K. In particular, $\Delta(L/K) \subset A_K$ is well-defined, and it is non-zero because we assume L/K to be separable. The different $\mathfrak{D}(L/K)$ is the A_L-ideal with inverse

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

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

4.13. 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 ℓ/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 ℓ/k to obtain a basis of A_L over A_K by 3.9, and the discriminant of this basis is a unit as the separability of ℓ/k implies that its reduction in 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 3.9 and we have

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

The final equality follows from 1.10 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 4.11. It follows that $\mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) = e-1$ if and only if $\mathrm{ord}_{\mathfrak{p}_L}(e) = 0$, i.e. if and only if L/K is tamely ramified. If L/K is wildly ramified we obtain $e \leq \mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K)) \leq e - 1 + \mathrm{ord}_{\mathfrak{p}_L}(e)$. The upper bound is finite only when $e \neq 0 \in K$. □

Lemma 4.11 does not hold for local fields of positive characteristic when $\mathrm{char}\, K$ divides n, see exercise 15. However, there is an elegant mass formula due to Serre [11, 1978] that is

more precise than 4.11 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

$$\sum_{L\in\mathcal{S}_n} q^{n-1-d(L)} = n. \tag{4.14}$$

Here q denotes the cardinality of k and $d(L) = \mathrm{ord}_{\mathfrak{p}_L}(\mathfrak{D}(L/K))$ is the differential exponent of L/K. If $\mathrm{char}\, K = 0$ we have a uniform upper bound $d(L) \leq e - 1 + \mathrm{ord}_{\mathfrak{p}_L}(e)$ for all L, so the number of terms in the sum must be finite. For n divisible by $p = \mathrm{char}\, K$, the set $\mathcal{S}_n$ is always infinite, but we see that the number of fields L with bounded differential exponent must be finite. This immediately implies a local counterpart to Hermite's theorem [ANT, 5.12], see exercise 16.

Exercises.

1. Let K be a complete non-archimedean field and $\overline{K}$ its algebraic closure. Show that the residue class field of $\overline{k}$ of $\overline{K}$ is an algebraic closure of k.
2. For K be a field and $n \geq 1$, we define the *coefficient map* $\Phi : K^n \to K^n$ by sending $(x_i)_{i=1}^n$ to the vector $(\sigma_i)_{i=1}^n$, defined by $\prod_{i=1}^n (X - x_i) = X^n + \sum_{i=1}^n (-1)^n \sigma_i X^{n-i}$. Show that ϕ is a polynomial map, and that the determinant of its Jacobian equals
$$\det(\partial\Phi_i/\partial X_j) = \prod_{i\neq j}(X_i - X_j).$$
3. 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 k. Show that every extension of ϕ to the splitting field of f is unramified over ϕ.
4. 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.
5. *(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.
6. 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 $\mathrm{char}\, k$, show that $V = T(\sqrt[e_0]{\pi})$ with T the inertia field of L/K and π a prime element of T. What can you say about $[L : V]$?
7. 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
$$\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \begin{cases} \widehat{\mathbf{Z}} & \text{if } \mathrm{char}\, k = 0; \\ \widehat{\mathbf{Z}}/\mathbf{Z}_p & \text{if } \mathrm{char}\, k = p > 0. \end{cases}$$

8. 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.

9. Let L/K and e_0 be as in exercise 6 and suppose that $\#k = q < \infty$. 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 $\mathrm{Gal}(V/K)$.]

10. 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 $\mathrm{Gal}(M/K) \cong (\mathbf{Z}/(q-1)\mathbf{Z}) \times \widehat{\mathbf{Z}}$.

11. 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?

12. 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!).

13. 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.

14. Verify Serre's formula 4.14 for n coprime to $\mathrm{char}\, k$.

15. 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 $m \neq n$.

16. 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 $K \subset L$ and the residue class field extension $k \subset \ell$ are separable. There is always a maximal subextension $K \subset L_s \subset L$ for which these assumptions are satisfied, and in most cases that occur in practice one has $L_s = L$. Having dealt with the case of complete extensions, we will pass to the global case and discuss the relation between local and global Galois groups.

▶ Inertia subgroup

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

5.1. Proposition. *The residue class field extension $k \subset \ell$ is Galois and the natural map $\rho : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$ 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 $\overline{\sigma} \in \mathrm{Aut}_k(\ell)$, so we have a natural image $\overline{G}$ of $G = \mathrm{Gal}(L/K)$ in $\mathrm{Aut}_k(\ell)$. We will prove that $k \subset \ell$ is Galois and that ρ is surjective by showing that k equals the invariant field $\ell^{\overline{G}}$.

We clearly have $k \subset \ell^{\overline{G}}$, so let $\overline{x} \in \ell^{\overline{G}}$ have representative $x \in A_L$. If 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 $\mathrm{char} k = p > 0$ 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 ℓ, the element

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

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

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

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

▶ Ramification groups

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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$k$*. If G is abelian, there is a canonical embedding $\chi_0 : G_0/G_1 \rightarrowtail k^*$.*

Proof. The isomorphism $U_L^{(0)}/U_L^{(1)} = \ell^*$ and 5.2 give us an injection $\chi_0 : G_0/G_1 \rightarrowtail \ell^*$, 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 $(\ell^*)^G = k^*$. □

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

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

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

so it is in this case an isomorphism.

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

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

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

▶ Decomposition group

We now consider the case of an arbitrary finite field extension. If ϕ is a 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, with $G_\psi = \mathrm{Gal}(L_\psi/K_\phi)$ isomorphic to the subgroup of $\mathrm{Gal}(L/K)$ corresponding to the subfield $L \cap K_\phi$.

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

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

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

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

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

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

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

5.6. 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. □

5.7. 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.

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

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

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

▶ Galois theory for global fields

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

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

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

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

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

corresponding to subgroups

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

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

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

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

► Non-normal extensions

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

5.9. 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.

5.10. Theorem. *Let L/K be a finite separable extension, M the normal closure of L over K and $\mathfrak{p}$ a discrete prime divisor on K. Set $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L) \subset G$, and let G act in the natural way on the set Ω of left cosets of H in G. Suppose we are given*

integers $e_i, f_i > 0$ for $i = 1, 2, \ldots, t$ such that $\sum_{i=1}^{t} e_i f_i = [L : K]$. Then the following two statements are equivalent.

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

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

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

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

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

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

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

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

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

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

▶ Frobenius automorphism, Artin symbol

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

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

between a factor group of $G_\mathfrak{q}$ and the Galois group of the residue class extension $\ell/k = F_\mathfrak{q}/F_\mathfrak{p}$ 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 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 13.

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.

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

7. 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?

8. 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

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

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

9. 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.

10. 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 $\mathbf{Q}_5$?

11. 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.]

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

13. 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.

14. 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 $f(\mathfrak{q}'/\mathfrak{p})$?

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

6 The Kronecker-Weber theorem

If K is any field and $n \in \mathbf{Z}_{\geq 1}$ an integer not divisible by $\mathrm{char}\,(K)$, the n-th *cyclotomic extension* K_n of K is the splitting field of the separable polynomial $X^n - 1 \in K[X]$ over K. We have $K_n = K(\zeta_n)$ for any primitive n-root of unity $\zeta_n \in K_n$, and $\sigma \in \mathrm{Gal}(K_n/K)$ is determined by the value $\sigma(\zeta_n) = \zeta_n^k$. More precisely, we have an injection of *abelian* groups

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

sending $\sigma_k : \zeta_n \mapsto \zeta_n^k$ to $(k \bmod n)$. For $K = \mathbf{Q}$ this is an isomorphism, by the irreducibility in $\mathbf{Z}[X]$ of the n-th cyclotomic polynomial

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

A finite abelian extension $K \subset L$ is said to be *cyclotomic* if it allows a K-embedding $L \subset K_n$ for some $n \in \mathbf{Z}_{\geq 1}$. Clearly, all cyclotomic extensions are abelian. For $K = \mathbf{Q}$, there are no other abelian extensions.

6.1. Kronecker-Weber theorem. *Every finite abelian extension $\mathbf{Q} \subset L$ is cyclotomic.*

The theorem was stated by Kronecker in 1853, but his proof was incomplete. A second proof was given by Weber in 1886. In 1896 Hilbert used what is essentially the theory of Section 5 to give the first complete proof. All proofs show that, after 'twisting' by suitable cyclotomic extensions, an abelian extension of $\mathbf{Q}$ becomes unramified over $\mathbf{Q}$ at *all* finite primes, and therefore of discriminant 1, and equal to $\mathbf{Q}$.

The smallest positive integer n for which an abelian extension $\mathbf{Q} \subset L$ can be embedded in $\mathbf{Q}(\zeta_n)$ is the *conductor* of L.

▶ Global and local version

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

6.2. Local Kronecker-Weber theorem. *Every finite abelian extension $\mathbf{Q}_p \subset L$ is cyclotomic.*

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

Proof that 6.2 implies 6.1. Let $\mathbf{Q} \subset L$ be finite abelian. Any completion $L_\mathfrak{p}$ of L at a prime $\mathfrak{p}|p$ is then abelian over $\mathbf{Q}_p$, and determined up to $\mathbf{Q}_p$-isomorphism by p and L. By assumption, there exists $n_p = p^{k_p} \cdot m_p$ 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 $L(\zeta_n)$, which is abelian over $\mathbf{Q}$ with group $G = \mathrm{Gal}(L(\zeta_n)/\mathbf{Q})$ and ramified over $\mathbf{Q}$ at exactly the same rational primes as L.

The ramification index of a prime $p|\Delta_L$ in $L(\zeta_n)$ equals $\phi(p^{k_p})$, as the completion of $L(\zeta_n)$ at a prime over p is obtained by adjoining a p^{k_p}-th root of unity to an unramified extension of $\mathbf{Q}_p$. As G is abelian, the subgroup $I \subset G$ generated by the inertia groups $I_p \subset G$ of the primes $p|\Delta_L$ 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, so by Minkowski's theorem [I, 9.11], we have $L(\zeta_n)^I = \mathbf{Q}$ and $I = G$. The inequality

$$[L(\zeta_n) : \mathbf{Q}] = \#G = \#I \leq \phi(n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}]$$

now shows that we have $L \subset L(\zeta_n) = \mathbf{Q}(\zeta_n)$, as claimed. □

► Kummer theory

Abelian extensions $K \subset L$ admit an explicit description as *radical extensions* in cases were the ground field K contains 'sufficiently many' roots of unity. More precisely, we can characterize all abelian extensions $K \subset L$ satisfying $\mathrm{Gal}(L/K)^n = 1$ for $n \in \mathbf{Z}_{>1}$ (i.e., the abelian extensions of *exponent* dividing n) in this way when K contains a primitive n-th root of unity.

6.3. Theorem. *Let K be a field containing a primitive n-th root of unity ζ_n, with $n \in \mathbf{Z}_{\geq 1}$. Then there is a bijection*

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

between abelian extensions $K \subset L$ of exponent dividing n inside an algebraic closure $\overline{K}$ and subgroups $W \subset K^*$ containing K^{*n}. If $K \subset L$ 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 $\mathrm{Hom}(W/K^{*n}, \langle \zeta_n \rangle)$, so we have

$$[L : K] = [W : K^{*n}]$$

in the case of finite extensions.

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

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

In the case $n = p = \mathrm{char}\,(K)$, when no p-th roots of unity exist in K, there is an analog of Theorem 6.3 known as *Artin-Schreier theory*, see exercise 1.

▶ Proof of Theorem 6.2

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

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 that any cyclic extension $\mathbf{Q}_p \subset L$ of degree q^n, with q prime, is cyclotomic. We distinguish three cases, and start with the easiest case.

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

Proof. The extension $L/\mathbf{Q}_p$ is tamely ramified as the ramification index 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 4.5) to $L/\mathbf{Q}_p$ and the extension $\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p$ from 4.10, we see that $\mathbf{Q}_p(\zeta_p) \subset L(\zeta_p)$ is an unramified extension. By 4.8, we have $L(\zeta_p) = \mathbf{Q}_p(\zeta_p, \zeta)$ for some root of unity ζ, so $L \subset \mathbf{Q}_p(\zeta_p, \zeta)$ is cyclotomic. This settles the tame case. □

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

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

6.6. 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 to be proved.

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

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

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

6.8. Lemma. *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 $\widehat{\mathbf{Z}}$.

Exercises.

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 that 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, show that 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 $w \mapsto \sigma(\wp^{-1}(w)) - \wp^{-1}(w)$.

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 quadratic number field. Show that K has an abelian extension that is not cyclotomic. *Is the same true for arbitrary number fields $K \neq \mathbf{Q}$?

4. 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 $-1 \in N_{L/K}[L^*]$.

5. 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.

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

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

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

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. H. W. Lenstra, Jr. and P. Stevenhagen, *Über das Fortsetzen von Bewertungen in vollständigen Körpern*, Archiv für Mathematik **53**, 547–552 (1989).
11. J.-P. Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*, C. R. Acad. Sci. Paris Série A **286**, no. 22, 1031–1036 (1978).

Index