CLASS FIELD THEORY

P. Stevenhagen

Explicit Algebraic Number Theory
Oberwolfach Seminar
November 2002

1. Class field theory: ideal groups

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

▶ Classical examples

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

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

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

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

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

$$(\mathcal{O}_K/6\mathcal{O}_K)^*/\operatorname{im}[\mathcal{O}_K^*] \xrightarrow{\sim} \operatorname{Gal}(K(\sqrt[3]{2})/K), \tag{1.1}$$

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

▶ Towards the main theorem

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

As we have phrased it, the statement is correct for our two examples, but it fails to hold for $K = \mathbf{Q}$. The reason is that the splitting primes in the cyclotomic field $\mathbf{Q}(\zeta_n)$ are the prime ideals $p\mathbf{Z}$ for which the *positive* generator is congruent to 1 modulo n. A sign change in the residue class modulo n changes the corresponding Artin symbol by a complex conjugation, so this peculiar detail is only relevant to abelian extensions $L/\mathbf{Q}$ that are complex, i.e. extensions in which the real prime is ramified. When we take this into account, we arrive at the following weak form of the main theorem of class field theory.

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

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

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

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

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

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

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

1.3. Artin's reciprocity law. *For every abelian extension of number fields L/K, there exists an $\mathcal{O}_K$-ideal $\mathfrak{f}$ divisible by all finite primes that ramify in L such that the Artin map*

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

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

▶ Cycles and ray classes

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

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

(i) *$n(\mathfrak{p})$ is a non-negative integer for all $\mathfrak{p}$ and $n(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$;*

(ii) *$n(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is real and $n(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex.*

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

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

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

(i) *$n = 0$;*

(ii) *$\mathfrak{p}$ is real, $n = 1$ and x is positive under the embedding $\mathfrak{p} : K^* \to \mathbf{R}^*$;*

(iii) *$\mathfrak{p}$ is finite, $n > 0$ and we have $x \in 1 + \mathfrak{p}^n \subset A_{\mathfrak{p}}$.*

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

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

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

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

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

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

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

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

of finite abelian groups.

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

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

1.7. Corollary. *If a cycle $\mathfrak{f}$ is divisible by $\mathfrak{g}$, the natural map $\mathit{Cl}_{\mathfrak{f}} \to \mathit{Cl}_{\mathfrak{g}}$ is surjective.*

Proof. The outer vertical arrows in the diagram

$$\begin{tikzcd}
0 \arrow[r] & (\mathcal{O}/\mathfrak{f})^*/\operatorname{im}[\mathcal{O}^*] \arrow[r] \arrow[d, "\text{can}"] & \mathit{Cl}_{\mathfrak{f}} \arrow[r] \arrow[d, "\text{can}"] & \mathit{Cl} \arrow[r] \arrow[d, "\text{id}"] & 0 \\
0 \arrow[r] & (\mathcal{O}/\mathfrak{g})^*/\operatorname{im}[\mathcal{O}^*] \arrow[r] & \mathit{Cl}_{\mathfrak{g}} \arrow[r] & \mathit{Cl} \arrow[r] & 0
\end{tikzcd}$$

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

▶ Ideal groups

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

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

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

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

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

$$\begin{tikzcd}
I(\mathfrak{g})/R(\mathfrak{g}) \arrow[r, "\phi_1"] \arrow[d, "\phi_2"] & I(\mathfrak{f}_1)/R(\mathfrak{f}_1) \arrow[d, "\chi_1"] \\
I(\mathfrak{f}_2)/R(\mathfrak{f}_2) \arrow[r, "\chi_2"] & I(\mathfrak{f})/R(\mathfrak{f})
\end{tikzcd}$$

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

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

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

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

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

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

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

▶ Main theorem

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

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

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

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

(1) *the primes dividing the conductor $\mathfrak{f}$ are the primes that ramify in L/K, and the primes whose square divides $\mathfrak{f}$ are the primes that are wildly ramified in L/K;*

(2) *for every multiple $\mathfrak{g}$ of the conductor $\mathfrak{f}$, the Artin map $\psi_{L/K} : I(\mathfrak{g}) \to \mathrm{Gal}(L/K)$ is a surjective homomorphism with kernel $B(\mathfrak{g})$.*

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

$$\psi_{L/K} : I(\mathfrak{g})/B(\mathfrak{g}) \xrightarrow{\sim} \mathrm{Gal}(L/K). \tag{1.10}$$

The splitting behavior of a prime of K in the extension L is determined by the ideal class of $\mathfrak{p}$ in the generalized ideal class group $I(\mathfrak{g})/B(\mathfrak{g})$. The field L is the unique field corresponding to this ideal group B and is known as the *class field* of B. This (highly non-trivial) existence of class fields for every given division of prime ideals into classes modulo a cycle accounts for the name *class field theory*.

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

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

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

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

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

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

$$\begin{tikzcd}
I(\mathfrak{g})/B_2(\mathfrak{g}) \arrow[r, "\sim"] \arrow[d, "\text{can}"] & \mathrm{Gal}(L_2/K) \arrow[d, "\text{res}"] \\
I(\mathfrak{g})/B_1(\mathfrak{g}) \arrow[r, "\sim"] & \mathrm{Gal}(L_1/K)
\end{tikzcd}$$

relating the Artin isomorphisms of L_1 and L_2 over K;

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

$$\begin{tikzcd}
I_E(\mathfrak{g})/N_{E/K}^{-1}B(\mathfrak{g}) \arrow[r, "\sim"] \arrow[d, "N_{E/K}"] & \mathrm{Gal}(LE/E) \arrow[d, "\text{res}"] \\
I(\mathfrak{g})/B(\mathfrak{g}) \arrow[r, "\sim"] & \mathrm{Gal}(L/K).
\end{tikzcd}$$

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

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

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

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

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

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

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

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

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

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

▶ Ray class fields

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

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

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

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

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

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

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

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

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

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

2. Class field theory: idèles

The formulation of class field theory as given in the preceding section is the classical formulation using ideal groups. From a computational point of view, these groups are often a convenient tool as they have a simple definition that makes them well-suited for most explicit computations. It is however somewhat annoying that every proof involving ideal groups starts by the choice of a common cycle modulo which everything is defined, and the end of the proof is the observation that the result obtained is independent of the choice of the common modulus.

In order to avoid the choice of moduli, say in the case of base field $\mathbf{Q}$, it is clear that one should not work with the groups $(\mathbf{Z}/n\mathbf{Z})^*$ for varying n, but pass to the projective limit

$$\widehat{\mathbf{Z}}^* = \lim_{\leftarrow n}(\mathbf{Z}/n\mathbf{Z})^* = \prod_p \mathbf{Z}_p^*$$

from the beginning and define the Artin map on $\widehat{\mathbf{Z}}^*$ rather than on an ideal group $I_{\mathbf{Q}}(n)$ for some large n. We see that for the rational field, this large group becomes a product of completions at all finite primes of the field.

▶ Subgroups of the idèle group

In the general case, one also needs the real completions in order to keep track of the sign conditions at the real primes. Chevalley observed that a very elegant theory results if one takes the product of the unit groups at *all* completions of the number field, i.e. the idèle group J of K, and writes all ray class groups as surjective images $J \twoheadrightarrow Cl_{\mathfrak{f}}$.

As the idèle group J contains a subgroup

$$K_{\mathfrak{p}}^* = K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}'\neq\mathfrak{p}} \{1\} \subset J \tag{2.1}$$

for each prime $\mathfrak{p}$, we obtain a *local Artin map* for each completion $K_{\mathfrak{p}}$ of K. This point of view enables us to describe the relation between the global abelian extension L/K and the local extensions $L_{\mathfrak{q}}/K_{\mathfrak{p}}$, thus giving rise to a *local class field theory*. Moreover, it yields in a natural way a direct description of the power of a prime $\mathfrak{p}$ dividing the conductor of an extension L/K that strengthens the qualitative description of 1.9(1).

In order to describe the open subgroups of the idèle group J of K, we look at the open subgroups of the completions $K_{\mathfrak{p}}^*$ first. If $\mathfrak{p}$ is a finite prime, a basis of open neighborhoods of the unit element $1 \in K_{\mathfrak{p}}^*$ consists of the subgroups $U_{\mathfrak{p}}^{(n)} \subset K_{\mathfrak{p}}^*$ defined by

$$U_{\mathfrak{p}}^{(n)} = \begin{cases} U_{\mathfrak{p}} = A_{\mathfrak{p}}^* & \text{if } n = 0; \\ 1 + \mathfrak{p}^n & \text{if } n \in \mathbf{Z}_{>0}. \end{cases}$$

If $\mathfrak{p}$ is real, we have $K_{\mathfrak{p}} \cong \mathbf{R}$. Every open subgroup of the multiplicative group $\mathbf{R}^*$ contains the group $\mathbf{R}_{>0}$ of positive real numbers as $\mathbf{R}_{>0}$ is generated by any open neighborhood of $1 \in \mathbf{R}^*$. The open subgroups of $K_{\mathfrak{p}}^*$ are therefore

$$U_{\mathfrak{p}}^{(0)} = K_{\mathfrak{p}}^* \qquad \text{and} \qquad U_{\mathfrak{p}}^{(1)} = K_{\mathfrak{p},>0}.$$

Finally, if $\mathfrak{p}$ is complex, the only open subgroup of $K_\mathfrak{p}^*$ is the trivial subgroup $U_\mathfrak{p}^{(0)} = K_\mathfrak{p}^*$, which is generated by every open neighborhood of $1 \in K_\mathfrak{p}^* \cong \mathbf{C}^*$. With this notation, we have for each cycle $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ of K a subgroup

$$W_\mathfrak{f} = \textstyle\prod_\mathfrak{p} U_\mathfrak{p}^{n(\mathfrak{p})} \subset J. \tag{2.2}$$

2.3. Proposition. *A subgroup of the idèle group J of K is open if and only if it contains $W_\mathfrak{f}$ for some cycle $\mathfrak{f}$ of K.*

Proof. As almost all exponents $n(\mathfrak{p})$ in (2.2) are equal to zero, the definition of the idèle topology shows that $W_\mathfrak{f}$ is an open subgroup of J. Conversely, if $H \subset J$ is an open subgroup of J, we must have $W_\mathfrak{f} \subset H$ for some $\mathfrak{f}$ as every open neighborhood of $1 \in J$ generates some $W_\mathfrak{f}$. □

► Ray classes as idèle classes

It follows from 2.2 that a subgroup of the *idèle class group* $C = J/K^*$ is open if and only if it contains the homomorphic image $D_\mathfrak{f}$ of some subgroup $W_\mathfrak{f} \subset J$. We have a canonical isomorphism $J/K^*W_\mathfrak{f} \xrightarrow{\sim} C/D_\mathfrak{f}$ for the quotients of the basic open subgroups $D_\mathfrak{f} \subset C$.

2.4. Theorem. *For every cycle $\mathfrak{f}$ of K there are isomorphisms*

$$J/K^*W_\mathfrak{f} \xrightarrow{\sim} C/D_\mathfrak{f} \xrightarrow{\sim} Cl_\mathfrak{f} = I(\mathfrak{f})/R(\mathfrak{f})$$

such that the class of a prime element $\pi_\mathfrak{p}$ at a finite prime $\mathfrak{p} \nmid \mathfrak{f}$ in $J/K^*W_\mathfrak{f}$ or $C/D_\mathfrak{f}$ corresponds to $\mathfrak{p} \bmod R(\mathfrak{f})$ in $Cl_\mathfrak{f}$.

Proof. Write $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$, and define a map

$$\begin{aligned} \phi : \qquad J &\longrightarrow Cl_\mathfrak{f} = I(\mathfrak{f})/R(\mathfrak{f}) \\ (x_\mathfrak{p})_\mathfrak{p} &\longrightarrow \prod_{\mathfrak{p}\text{ finite}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x^{-1}x_\mathfrak{p})} \bmod R(\mathfrak{f}), \end{aligned}$$

where $x \in K^*$ is an element that satisfies $x^{-1}x_\mathfrak{p} \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for all primes $\mathfrak{p}$ dividing $\mathfrak{f}$. Such an element exists by the approximation theorem, and it is uniquely determined up to multiplication by an element $y \in K^*$ satisfying $y \equiv 1 \bmod^* \mathfrak{f}$. By definition of $R(\mathfrak{f})$, the map ϕ is a well defined homomorphism. Its surjectivity is clear as a prime element $\pi_\mathfrak{p} \in J$ at a finite prime $\mathfrak{p}\nmid\mathfrak{f}$ is mapped to $\mathfrak{p} \bmod R(\mathfrak{f})$. It remains to show that $\ker\phi = K^*W_\mathfrak{f}$.

Suppose we have $(x_\mathfrak{p})_\mathfrak{p} \in \ker\phi$. Then there exists $x \in K^*$ as above and $y \in K^*$ such that $y \equiv 1 \bmod^* \mathfrak{f}$ and

$$\prod_{\mathfrak{p}\text{ finite}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x^{-1}x_\mathfrak{p})} = \prod_{\mathfrak{p}\text{ finite}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(y)}.$$

This implies that $x_\mathfrak{p}(xy)^{-1}$ is a unit at all finite $\mathfrak{p}$ outside $\mathfrak{f}$ and satisfies $x_\mathfrak{p}(xy)^{-1} \equiv 1 \bmod^* \mathfrak{p}^{n(\mathfrak{p})}$ for $\mathfrak{p}|\mathfrak{f}$, so we have $(x_\mathfrak{p})_\mathfrak{p} \in xyW_\mathfrak{f}$. This proves the inclusion $\ker\phi \subset K^*W_\mathfrak{f}$. The other inclusion is obvious from the definition of ϕ. □

2.5. Corollary. *Every open subgroup of C is of finite index.*

Proof. Any open subgroup contains a subgroup $D_{\mathfrak{f}}$, which is of finite index in C by the finiteness of the ray class group $Cl_{\mathfrak{f}}$. □

If B is an ideal group and $\mathfrak{g}$ a modulus for B, we define the open subgroup $D_B \subset C$ corresponding to B as the kernel

$$D_B = \ker[C \longrightarrow I(\mathfrak{g})/B(\mathfrak{g})]$$

of the natural map induced by 2.3. We have a canonical isomorphism $C/D_B \xrightarrow{\sim} I(\mathfrak{g})/B(\mathfrak{g})$ that maps the class of a prime element $\pi_{\mathfrak{p}}$ at a finite prime $\mathfrak{p} \nmid \mathfrak{g}$ to $(\mathfrak{p} \bmod B(\mathfrak{g}))$, and it follows from the definition of equivalence of ideal groups that D_B depends on B, but not on the choice of the modulus $\mathfrak{g}$.

2.6. Proposition. *The correspondence $B \mapsto D_B$ is an inclusion preserving bijection between the set of ideal groups of K and the set of open subgroups of the idèle class group C. The conductor $\mathfrak{f}$ of an ideal group B is the smallest cycle satisfying $D_{\mathfrak{f}} \subset D_B$.*□

From the obvious equality $D_{\mathfrak{f}_1} \cdot D_{\mathfrak{f}_2} = D_{\gcd(\mathfrak{f}_1,\mathfrak{f}_2)}$, we obtain as a simple corollary of the formalism a statement that required a proof in 1.8.

2.7. Corollary. *If an ideal group can be defined modulo $\mathfrak{f}_1$ and $\mathfrak{f}_2$, it can be defined modulo* $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$. □

▶ The kernel of the Artin map

Combining the bijection between open subgroups of C and ideal groups in 2.6 with the main theorem 1.9, we see that every finite abelian extension L/K corresponds to an open subgroup D_L of C for which there is an Artin isomorphism

$$C/D_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

that maps the residue classes of the prime elements $\pi_{\mathfrak{p}} \bmod D_L$ for finite unramified $\mathfrak{p}$ to the Artin symbol $(\mathfrak{p}, L/K)$.

In order to describe the subgroup D_L of the idèle class group corresponding to L, we need to define the norm $N_{L/K} : C_L \to C_K$ on idèle class groups. We know (cf. A.2) that there is an adèle norm $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ that is the ordinary field norm $N_{L/K} : L \to K$ when restricted to L. It can be given explicitly as

$$N_{L/K}((x_{\mathfrak{q}})_{\mathfrak{q}}) = (\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(x_{\mathfrak{q}}))_{\mathfrak{p}}. \tag{2.8}$$

Here $\mathfrak{q}$ and $\mathfrak{p}$ range over the primes of L and K, respectively. The norm maps the unit group $J_L = \mathbb{A}_L^*$ into the unit group J_K and L^* into K^*, so we have an induced norm $N_{L/K} : C_L \to C_K$ on the idèle class groups.

We need to check that this norm corresponds to the norm on ideal class groups under the isomorphism 2.3. As in the previous section, we view a cycle $\mathfrak{f}$ of K as a cycle in a finite extension L when necessary, and use the obvious notation $W_{L,\mathfrak{f}} \subset J_L$ and $D_{L,\mathfrak{f}} \subset C_L$ for the corresponding subgroups in J_L and C_L. For a cycle $\mathfrak{f}$ of K we have $N_{L/K}[W_{L,\mathfrak{f}}] \subset W_{K,\mathfrak{f}}$ and $N_{L/K}[D_{L,\mathfrak{f}}] \subset D_{K,\mathfrak{f}}$.

2.9. Proposition. *Let L/K be a finite extension and $\mathfrak{f}$ a cycle of K. Then there is a commutative diagram*

$$\begin{tikzcd} C_L/D_{L,\mathfrak{f}} \arrow[r, "\sim"] \arrow[d, "N_{L/K}"] & I_L(\mathfrak{f})/R_L(\mathfrak{f}) \arrow[d, "N_{L/K}"] \\ C_K/D_{K,\mathfrak{f}} \arrow[r, "\sim"] & I_K(\mathfrak{f})/R_K(\mathfrak{f}) \end{tikzcd}$$

in which the horizontal isomorphisms are as in 2.3.

Proof. The commutativity of the diagram may be verified on prime elements $\pi_\mathfrak{q}$ at finite primes $\mathfrak{q}$ of L outside $\mathfrak{f}$, since these classes generate $C_L/D_{L,\mathfrak{f}}$. For such prime elements we have $N_{L/K}(\pi_\mathfrak{q}) = N_{L_\mathfrak{q}/K_\mathfrak{p}}(\pi_\mathfrak{q})$ by 2.8, and by the definition of extension valuations we have $N_{L_\mathfrak{q}/K_\mathfrak{p}}(\pi_\mathfrak{q}) \cdot A_\mathfrak{p} = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$. It follows that the diagam commutes. □

2.10. Proposition. *Let L be a finite extension of K. Then there exists a cycle $\mathfrak{f}$ of K such that $D_{K,\mathfrak{f}}$ is contained in $N_{L/K}C_L$ and all primes dividing $\mathfrak{f}$ are ramified in L/K. In particular, $N_{L/K}C_L$ is open in C_K.*

Proof. With $[L:K] = n$, we have $N_{L/K}J_L \supset U_\mathfrak{p}^n$ for all primes $\mathfrak{p}$. As $U_\mathfrak{p}^n$ contains an open neighborhood of $1 \in U_\mathfrak{p}$, one has $U_\mathfrak{p}^n \supset U_\mathfrak{p}^{(k)}$ for some $k \in \mathbf{Z}_{>0}$. If $\mathfrak{q}|\mathfrak{p}$ is unramified, the identity

$$N_{L_\mathfrak{q}/K_\mathfrak{p}}(x + y\pi_\mathfrak{p}^k) = N_{L_\mathfrak{q}/K_\mathfrak{p}}(x) + \mathrm{Tr}_{L_\mathfrak{q}/K_\mathfrak{p}}(y)\pi_\mathfrak{p}^k \bmod \mathfrak{p}^{k+1}A_\mathfrak{p}$$

for $x, y \in A_\mathfrak{q}$ and the surjectivity of the norm and trace map on the residue class field extension $k_\mathfrak{p} \subset k_\mathfrak{q}$ easily imply that we have $N_{L_\mathfrak{q}/K_\mathfrak{p}}[U_\mathfrak{q}] = U_\mathfrak{p}$. This proves our proposition, as it implies $N_{L/K}J_L \supset W_{K,\mathfrak{f}}$ for some $\mathfrak{f}$ divisible only by ramifying primes.

2.11. Theorem. *For any finite extension L/K there exists a cycle $\mathfrak{f}$ in K that is only divisible by ramifying primes and an isomorphism*

$$C_K/N_{L/K}C_L \xrightarrow{\sim} I(\mathfrak{f})/N_{L/K}I_L(\mathfrak{f}) \cdot R(\mathfrak{f})$$

that maps the class of $\pi_\mathfrak{p}$ to the class of $\mathfrak{p}$ for finite unramified $\mathfrak{p}$.

Proof. Take $\mathfrak{f}$ as in 2.10, then the isomorphism is obtained by taking cokernels in the diagram of 2.9. □

▶ Main theorem

We can now give the idèlic version of the main theorem of class field theory. Note that so far, none of the proofs in this section relied on the main theorem 1.9 or its corollaries.

2.12. Main theorem. *Let K be a number field, Σ_K the set of finite abelian extensions of K contained in some fixed algebraic closure and $\mathcal{D}$ the set of open subgroups of the idèle class group C of K. Then there exists an inclusion reversing bijection*

$$\Sigma_K \leftrightarrows \mathcal{D}$$

such that for an extension L/K corresponding to the subgroup D of C the following holds:

(1) $D = N_{L/K}C_L$;

(2) *there is a global Artin isomorphism $\psi_{L/K} : C/D \xrightarrow{\sim} \mathrm{Gal}(L/K)$ such that the image of a completion $K_{\mathfrak{p}}^*$ in C is mapped onto the decomposition group $G_{\mathfrak{p}}$ of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$. It induces a local Artin isomorphism*

$$\psi_{\mathfrak{p}} : K_{\mathfrak{p}}^*/N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}L_{\mathfrak{q}}^* \xrightarrow{\sim} G_{\mathfrak{p}} = \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}) \subset \mathrm{Gal}(L/K)$$

for the local extension at $\mathfrak{p}$. If $\mathfrak{p}$ is finite, this local isomorphism maps the local unit group $U_{\mathfrak{p}}$ onto the inertia group $I_{\mathfrak{p}} \subset G_{\mathfrak{p}}$ and the class of a prime element $\pi_{\mathfrak{p}}$ at $\mathfrak{p}$ to the coset of the Frobenius automorphism in $G_{\mathfrak{p}}$.

The idèlic main theorem 2.12 is similar in content to 1.9, but it has several advantages over the older formulation. First of all, it does without the choice of defining moduli, thus avoiding the cumbersome transitions between equivalent groups. Secondly, it yields a description of the contribution of a prime $\mathfrak{p}$ that shows the local nature of this contribution. The statement in (2) is not a simple corollary of the identity $D = N_{L/K}C_L$ since it requires the non-trivial identity

$$K_{\mathfrak{p}}^* \cap (K^* N_{L/K} J_L) = N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} L_{\mathfrak{q}}^* \tag{2.13}$$

for the intersection of the subgroup $K_{\mathfrak{p}}^* \subset C$ with the kernel $N_{L/K}C_L$ of the global Artin map. From (2), we obtain a description of the conductor that can be used to actually compute it.

2.14. Corollary. *Let $\mathfrak{f}_{L/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ be the conductor of the abelian extension L/K. If $\mathfrak{q}$ is a prime of L that extends $\mathfrak{p}$, then $n(\mathfrak{p})$ is the smallest non-negative integer n for which the inclusion*

$$U_{\mathfrak{p}}^{(n)} \subset N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}} U_{\mathfrak{q}}$$

is satisfied. □

As a supplement to 2.12, there are again the functorial diagrams occurring in 1.11. Both the statements and their derivation from the main theorem have an immediate translation in terms of the idèle class group, and we leave them to the reader.

► Local class field theory

The local Artin isomorphism, which occurs as a 'corollary' of the idèlic version of global class field theory, leads to a class field theory for local number fields that is interesting in its own right. This local theory can also be developed independently from the global theory, and one may argue that this in certain ways more natural. Our order of presentation however follows the history of the subject.

As we have formulated global class field theory for number fields only, and not for function fields of dimension 1 over finite fields (i.e. extensions of a finite field of transcendence degree 1), we obtain a local class field theory for local fields in characteristic 0 only. The theory in characteristic p is highly similar, even though some of the proofs have to be modified for extensions of degree divisible by the characteristic.

2.15. Proposition. *Let F be a finite extension of $\mathbf{Q}_p$ for some prime number p and E/F a finite abelian extension with group G. Then there is a canonical isomorphism*

$$\psi_{E/F}:\ F^*/N_{E/F}E^* \xrightarrow{\sim} G$$

that maps the unit group of the ring of integers of F onto the inertia group $I_{E/F}$ and a prime element onto the Frobenius residue class mod $I_{E/F}$.

Proof. We can choose number fields K and L that are dense in F and E, respectively, in such a way that L is G-invariant and $L^G = K$. This means that there are primes $\mathfrak{q}$ in L and $\mathfrak{p}$ in K such that $F = K_\mathfrak{p}$ and $E = L_\mathfrak{q}$, and $G_\mathfrak{p} = G$. The global Artin map for L/K now induces a local Artin isomorphism $\psi_{E/F}$ with the stated properties.

In order to prove the canonicity of $\psi_{E/F}$, we have to show that it does not depend on the choice of the G-invariant subfield $L \subset E$. Thus, let L' be another number field that is dense in E and stable under G. Replacing L' by LL' if necessary, we may assume that L is contained in L'. Then $K' = (L')^G$ contains K, and we have $F = K_\mathfrak{p} = K'_\mathfrak{r}$ for a prime $\mathfrak{r}|\mathfrak{p}$. The commutative diagram

$$\begin{tikzcd}
K'_\mathfrak{r} \arrow[r] \arrow[d, "\mathrm{id}"] & C_{K'}/N_{LK'/K'}C_{LK'} \arrow[r, "\sim"] \arrow[d, "N_{K'/K}"] & \mathrm{Gal}(LK'/K') \arrow[d, "\mathrm{res}"] \\
K_\mathfrak{p} \arrow[r] & C_K/N_{L/K}C_L \arrow[r, "\sim"] & \mathrm{Gal}(L/K);
\end{tikzcd}$$

derived from 1.11 (4) shows that L'/K' and L/K induce the same Artin isomorphism for the extension E/F. □

The description of the local Artin isomorphism given by the preceding proposition is somewhat indirect as the map is induced by the Artin isomorphism of a 'dense global extension'. Only in the case of an unramified extension E/F the situation is very transparent, as in that case both $F^*/N_{E/F}E^*$ and $\mathrm{Gal}(E/F)$ have canonical generators, and they correspond under the Artin isomorphism. Only relatively recently, in 1985, Neukirch realized that that the local Artin map in the general case is *completely determined* by this fact and the functorial properties of the Artin symbol. We do not give the argument here.

2.16. Main theorem for local number fields. *Let F be a local number field, Σ_F the set of finite abelian extensions of F contained in some fixed algebraic closure and $\mathcal{H}$ the set of open subgroups of finite index of F^*. Then there exists an inclusion reversing bijection*

$$\Sigma_F \leftrightarrows \mathcal{H}$$

such that for an extension E/F corresponding to the subgroup H of F^* the following holds:
(1) *$H = N_{E/F}E^*$;*
(2) *there is an Artin isomorphism $\psi_{E/F} : F^*/H \xrightarrow{\sim} \mathrm{Gal}(E/F)$ such that, for non-archimedean F, the unit group U of the valuation ring of F is mapped onto the inertia group $I_{E/F}$ and a prime element is mapped into the Frobenius coset modulo $I_{E/F}$.*

Note that $N_{E/F}E^* \subset F^*$ in 2.16 is indeed an open subgroup of finite index, as it contains F^{*n} for $n = [E : F]$. We leave it to the reader to formulate the local functorial diagrams, which are analogous to those in 1.11.

The extension corresponding to an open subgroup H of finite index in F^* is called the *class field* of H. In the global case we have class fields corresponding to open subgroups of the idèle class group.

Appendix: adèles and idèles

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

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

Informally, one can say that it is the subring of the full cartesian product of all completions consisting of vectors that are almost everywhere integral. It is an example of a 'restricted direct product'. The topology on such a product is not the relative topology, but the topology generated by the open sets of the form

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

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

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

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

The open subset $U = (-1/2, 1/2) \times \prod_p \mathbf{Z}_p$ of $\mathbb{A}_\mathbf{Q}$ satisfies $U \cap \mathbf{Q} = \{0\}$, since a rational number that is p-integral at all primes p is in $\mathbf{Z}$, and we have $\mathbf{Z} \cap (-1/2, 1/2) = \{0\}$. It follows that $\mathbf{Q}$ is a discrete subring of $\mathbb{A}_\mathbf{Q}$. The closure $W = [-1/2, 1/2] \times \prod_p \mathbf{Z}_p$ of U is compact in $\mathbb{A}_\mathbf{Q}$ and satisfies $\mathbf{Q} + W = \mathbb{A}_\mathbf{Q}$. As the natural map $W \to \mathbb{A}_\mathbf{Q}/\mathbf{Q}$ is a continuous surjection. it follows that its image $\mathbb{A}_\mathbf{Q}/\mathbf{Q}$ is a *compact* additive group. Analogous statements hold for arbitrary number fields K. They can be proved by generalizing the proof for $\mathbf{Q}$, or by using the following theorem.

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

A.1. Theorem. *There is an isomorphism of topological rings*

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

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

Proof. For each prime $\mathfrak{p}$ of K, we have a local isomorphism

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

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

A.2. Corollary. *The ring* $\mathbb{A}_L$ *is a free algebra of rank* $[L : K]$ *over* $\mathbb{A}_K$*, and the norm map* $N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ *induces the field norm* $N_{L/K} : L \to K$ *on the subring* $L \subset \mathbb{A}_L$*.* □

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

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

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

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

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

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

A.3. Product formula. *For every non-zero element* $x \in K^*$*, we have*

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

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

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

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

that is known as the *idèle group* of K. For the topology on this group we do not take the relative topology coming from the adèle ring, for which inversion $x \mapsto x^{-1}$ is not continuous, but the topology generated by open sets of the form

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

with S a finite set of primes and $O_{\mathfrak{p}}$ open in $K_{\mathfrak{p}}^*$. This topology is finer than the relative topology J inherits from $\mathbb{A}_K$, and it makes J_K into a locally compact group.

Under the diagonal embedding, the unit group K^* of K becomes a subgroup of J_K consisting of the *principal idèles*. By the product formula, K^* is a discrete subgroup of J_K, so the factor group $C_K = J_K/K^*$ is again a locally compact group, the *idèle class group* of K. It is not a compact group, since the volume map

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

is a continuous surjective map that factors via C_K by the product formula. It is true that the subgroup $C_K^1 = (\ker \tau)/K^*$ of C_K is a compact group. This follows from the Dirichlet unit theorem and the finiteness of the class number of K. See René Schoof's lecture on Arakelov class groups.

3. Kummer theory and class field theory

The following is a theorem from Galois theory.

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

$$\{K \subset L \subset K^{\mathrm{ab}} : \mathrm{Gal}(L/K)^n = 1\} \quad \leftrightarrows \quad \{K^{*n} \subset W \subset K^*\}$$

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

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} (W/K^{*n})^{\wedge} = \mathrm{Hom}(W/K^{*n}, \langle\zeta_n\rangle).$$

In particular, one has an equality $[L:K] = [W:K^{*n}]$ in this case.

If K is a number field and $L = K(\sqrt[n]{W})$ a Kummer extension of exponent n, the ramification of L/K can be bounded in terms of W and n.

3.2. Proposition. *Let $L = K(\sqrt[n]{W})$ be a Kummer extension of the number field K, and suppose that the elements $x_1, x_2, \ldots, x_k \in \mathcal{O}_K$ generate W over K^{*n}. Then a prime $\mathfrak{p}$ of L satisfies:*

(1) *$\mathfrak{p}$ is totally split in L/K if and only if W is contained in $K_{\mathfrak{p}}^n$;*
(2) *if $\mathfrak{p}$ is ramified in L/K, then $\mathfrak{p}$ divides $n \cdot \infty$ or one of the x_i.*

Proof. The prime $\mathfrak{p}$ splits completely in the abelian extension L/K if and only if $K_{\mathfrak{p}}(\sqrt[n]{W})$ equals $K_{\mathfrak{p}}$, so we have (1). If $\mathfrak{p}$ does not divide $n \cdot \infty$ or one of the x_i, then the polynomials $X^n - x_i$ are separable over the residue class field at $\mathfrak{p}$ and their zeroes generate unramified extensions of $K_{\mathfrak{p}}$. □

If F is a local field, we have a description of the Galois group $\mathrm{Gal}(E/F)$ of the maximal extension E of exponent n of F by class field theory: $F^*/F^{*n} \xrightarrow{\sim} \mathrm{Gal}(E/F)$ under the local Artin map. If F contains a primitive n-th root of unity, Kummer theory tells us that we have $E = F(\sqrt[n]{F^*})$, and that $\mathrm{Gal}(E/F)$ is the *dual* of F^*/F^{*n}. This yields a pairing of F^*/F^{*n} with itself.

3.3. Corollary. *Let F be a local number field containing a primitive n-th root of unity. Then F^*/F^{*n} is its own dual under the pairing*

$$\begin{array}{ccc} F^*/F^{*n} \times F^*/F^{*n} & \longrightarrow & \langle\zeta_n\rangle \\ (\alpha,\beta) & \longmapsto & \dfrac{\sigma_\alpha(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}. \end{array}$$

Here σ_α denotes the Artin symbol of α in the extension $F(\sqrt[n]{F^*})/F$. □

The basic properties of this *n-th power norm residue symbol* are the following.

3.4. Theorem. *Let F be a local number field containing a primitive n-th root of unity and $(\cdot\,,\,\cdot) : F^* \times F^* \to \langle\zeta_n\rangle$ the n-th norm residue symbol. Then the following statements hold for $\alpha, \beta \in F^*$.*

(1) $(\alpha, \beta) = 1$ *if and only if α is a norm from $F(\sqrt[n]{\beta})$;*

(2) $(\alpha, \beta) = 1$ *if F is non-archimedean and α, β and n are in U_F;*

(3) $(\alpha, -\alpha) = 1$ *for $\alpha \in F^*$ and $(\alpha, 1-\alpha) = 1$ for $\alpha \in F \setminus \{0, 1\}$;*

(4) $(\alpha, \beta) = (\beta, \alpha)^{-1}$.

Proof. Property (1) follows from the fact that α is in the kernel of the Artin map $F^* \to \mathrm{Gal}(F(\sqrt[n]{\beta})/F)$ if and only if it is in the norm image of $F(\sqrt[n]{\beta})^*$. If F is non-archimedean and β and n are in U_F, then $F(\sqrt[n]{\beta})/F$ is unramified by 11.5 and every $\alpha \in U_F$ is a norm from $F(\sqrt[n]{\beta})^*$. This yields (2).

For (3), it suffices to observe that every element of the from $x^n - \beta$ with $x \in F$ is a norm from $F(\sqrt[n]{\beta})$ and substitute the special values $x = 0$ and $x = 1$. In particular, we have the relation $(\alpha\beta, -\alpha\beta) = 1$ that yields $(\alpha, -\alpha)(\alpha, \beta)(\beta, \alpha)(\beta, -\beta) = (\alpha, \beta)(\beta, \alpha) = 1$ upon expansion. □

If a number field K contains a primitive n-th root of unity, the same is true for all completions $F = K_\mathfrak{p}$ of K, and we have a local n-th power norm residue pairing

$$(\cdot\,,\,\cdot)_{n,\mathfrak{p}} : \qquad K_\mathfrak{p}^* \times K_\mathfrak{p}^* \longrightarrow \langle\zeta_n\rangle$$

as in 3.3 for each prime $\mathfrak{p}$. If α and β are in K^*, the symbol $(\alpha, \beta)_{n,\mathfrak{p}}$ equals 1 for almost all $\mathfrak{p}$ by property (2). The factorization of the Artin map $\psi_{L/K} : J_K \to \mathrm{Gal}(L/K)$ for abelian extensions of K via the idèle class group has the following global consequence for the local norm residue symbols.

3.5. Product formula. *Suppose that K contains a primitive n-th root of unity and α and β are in K^*. Then the product $\prod_\mathfrak{p} (\alpha, \beta)_{n,\mathfrak{p}}$ over all local n-th power norm residue symbols equals* 1.

Proof. The restriction of the global Artin map $\psi : J_K \to \mathrm{Gal}(K(\sqrt[n]{\beta})/K)$ to $K_\mathfrak{p}^*$ yields the local Artin map $\psi_\mathfrak{p} : K_\mathfrak{p}^* \to \mathrm{Gal}(K_\mathfrak{p}(\sqrt[n]{\beta})/K_\mathfrak{p})$, so we have a commutative diagram

$$\begin{tikzcd}
\prod'_\mathfrak{p} K_\mathfrak{p}^* \arrow[r, "\oplus\psi_\mathfrak{p}"] \arrow[d, "\wr"] & \bigoplus_\mathfrak{p} \mathrm{Gal}(K_\mathfrak{p}(\sqrt[n]{\beta})/K_\mathfrak{p}) \arrow[d] & (\sigma_\mathfrak{p})_\mathfrak{p} \arrow[d] \\
J_K \arrow[r, "\psi"] & \mathrm{Gal}(K(\sqrt[n]{\beta})/K) & \prod_\mathfrak{p} \sigma_\mathfrak{p}.
\end{tikzcd}$$

As $\alpha \in K^*$ is in the kernel of the global Artin map ψ, we obtain the product relation $\prod_\mathfrak{p} (\alpha, K_\mathfrak{p}(\sqrt[n]{\beta})/K_\mathfrak{p}) = \mathrm{id}_{K(\sqrt[n]{\beta})}$ for the local Artin symbols. The product formula follows by looking at their action on $\sqrt[n]{\beta}$. □

We will use the norm residue symbol to discuss the so-called *higher reciprocity laws*. These generalize the famous quadratic reciprocity law, which states that the Legendre symbol $\left(\frac{p}{q}\right)$ of two distinct odd rational primes p and q satisfies the 'symmetry property'

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

This is a rather surprising result, since the Legendre symbol $\left(\frac{a}{p}\right) \in \{\pm 1\}$ of an integer $a \in \mathbf{Z}$ modulo a prime $p \nmid a$ is defined by the congruence $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ that is in no obvious way symmetric in the arguments a and p. The restriction to primes in the quadratic reciprocity law is not at all essential, since we can multiply quadratic characters as in 7.* and define the Jacobi symbol $\left(\frac{a}{b}\right)$ of two coprime odd integers a and b by the equation $\left(\frac{a}{b}\right) = \prod_p \left(\frac{a}{p}\right)^{\mathrm{ord}_p(b)}$. With this convention, one can formulate the quadratic reciprocity law following Jacobi.

3.6. Quadratic reciprocity law. *Let a and b be coprime odd integers, and write* $\mathrm{sgn}(x) \in \{\pm 1\}$ *for the sign of a non-zero real number x. Then we have a reciprocity*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{(a-1)(b-1)}{4} + \frac{(\mathrm{sgn}(a)-1)(\mathrm{sgn}(b)-1)}{4}}.$$

Note that the right hand side consists of two factors that are equal to 1 exactly when a and b are sufficiently close to 1 in the completions $\mathbf{Q}_2$ and $\mathbf{Q}_\infty = \mathbf{R}$. This phenomenon will be explained by the general power reciprocity law 3.13.

Apart from the reciprocity law, there are the so-called *supplementary laws*

$$(3.7) \qquad \left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} \qquad \text{and} \qquad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$$

for b an odd integer that enable us to compute any Jacobi symbol $\left(\frac{a}{b}\right)$ without factoring the integer b into primes.

For an n-th power reciprocity law for arbitrary $n \geq 2$, we need a character of order n on the unit group of residue class field $\mathbf{F}_p{}^*$ that has its image in the group $\langle \zeta_n \rangle$ of n-th roots of unity. Such a map can only be defined in a canonical way for all primes if the base field contains a primitive n-th root of unity. Thus, we let K be a number field containing a primitive n-th root of unity ζ_n. If $\mathfrak{p}$ is a finite prime of K that does not divide n and $\alpha \in K^*$ is a $\mathfrak{p}$-adic unit, we define the *n-th power residue symbol* $\left(\frac{\alpha}{\mathfrak{p}}\right)_n \in \langle \zeta_n \rangle$ by the congruence

$$(3.8) \qquad \left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(\mathbf{N}\mathfrak{p}-1)/n} \bmod \mathfrak{p}.$$

Note that this is well defined as all n-th roots of unity are distinct modulo $\mathfrak{p}$ and $\alpha^{(\mathbf{N}\mathfrak{p}-1)/n}$ is an n-th root of unity in the residue class field $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. The name of the symbol is explained by the fact that the kernel $k_\mathfrak{p}^{*n}$ of the character $\left(\frac{\cdot}{\mathfrak{p}}\right)_n : k_\mathfrak{p}^* \to \langle \zeta_n \rangle$ consists of the residue classes in $k_\mathfrak{p}^*$ that are n-th powers.

The n-th power residue symbol of $\alpha \in K^*$ modulo an arbitrary fractional ideal $\mathfrak{b}$ of K is defined by

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p} \notin S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{\mathrm{ord}_\mathfrak{p}(\mathfrak{b})}.$$

Here $S(\alpha) = S_n(\alpha)$ stands for the set of primes of K that either divide $n \cdot \infty$ or occur in the factorization of (α). Note that we do not require $\mathfrak{b}$ to be in the group $I(\alpha) = I_n(\alpha)$

of fractionals ideals coprime to n and α, but simply set $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$ for $\mathfrak{p} \in I(\alpha)$. With this definition, the n-th power symbol $\left(\frac{\alpha}{\mathfrak{b}}\right)_n$ is unrestrictedly multiplicative in $\mathfrak{b}$ for fixed α, and the identity $\left(\frac{\alpha}{\mathfrak{b}}\right)_n\left(\frac{\alpha'}{\mathfrak{b}}\right)_n = \left(\frac{\alpha\alpha'}{\mathfrak{b}}\right)_n$ holds whenever α and α' are units at the primes occurring in the factorization of $\mathfrak{b}$. The power residue symbol for arbitrary $\alpha, \beta \in K^*$ is defined as

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\alpha}{(\beta)}\right)_n = \prod_{\mathfrak{p}\in S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}}\right)_n. \tag{3.9}$$

We have already seen in the introductory part of section 1 that the power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ for a prime $\mathfrak{p}$ outside $S(\alpha)$ equals 1 exactly when $\mathfrak{p}$ splits completely in the extension $K(\sqrt[n]{\alpha})/K$, i.e. when the Artin symbol $(\mathfrak{p}, K(\sqrt[n]{\alpha})/K)$ is the identity. The precise relation is the following.

3.10. Proposition. *Let K be a number field containing a primitive n-th root of unity, $\alpha \in K^*$ a non-zero element and $\mathfrak{b}$ a fractional ideal in $I(\alpha)$. Then we have*

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \frac{\sigma_{\mathfrak{b}}(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}},$$

with $\sigma_{\mathfrak{b}}$ the Artin symbol of $\mathfrak{b}$ in $\mathrm{Gal}(K(\sqrt[n]{\alpha})/K)$.

Proof By 11.5, the extension $K(\sqrt[n]{\alpha})/K$ is unramified at all primes in $I(\alpha)$, so the right hand side is a well-defined root of unity. As both sides are multiplicative in $\mathfrak{b}$, we can assume that $\mathfrak{b} = \mathfrak{p}$ is a prime ideal in $I(\alpha)$. For this $\mathfrak{p}$ we have a congruence

$$\frac{\sigma_{\mathfrak{p}}(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \equiv (\sqrt[n]{\alpha})^{\mathbf{N}\mathfrak{p}-1} = \alpha^{(\mathbf{N}\mathfrak{p}-1)/n} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \bmod \mathfrak{p},$$

and this implies equality as n-th roots of unity that are congruent modulo $\mathfrak{p}$ are equal. □

3.11. Corollary. *Let $\mathfrak{f}$ be the conductor of $K(\sqrt[n]{\alpha})/K$ and $\mathfrak{p}_1, \mathfrak{p}_2$ primes in $I(\alpha)$ that are in the same class in $Cl_{\mathfrak{f}}$. Then the power residue symbols $\left(\frac{\alpha}{\mathfrak{p}_1}\right)_n$ and $\left(\frac{\alpha}{\mathfrak{p}_2}\right)_n$ are equal.* □

Example. Take $K = \mathbf{Q}$ and $a \in \mathbf{Z}$ an odd integer, then the conductor of $\mathbf{Q}(\sqrt{a})/\mathbf{Q}$ has finite part $|\Delta_{\mathbf{Q}(\sqrt{a})}|$ and is divisible by the infinite prime of $\mathbf{Q}$ exactly when a is negative. We readily obtain Euler's observation that $\left(\frac{a}{p}\right)$ is always determined by the residue class of p modulo $4|a|$. For $a \equiv 1 \bmod 4$ it only depends on $p \bmod |a|$, and for $a > 0$ the behavior of the residue classes $p \bmod 4a$ and $-p \bmod 4a$ is the same.

In the general case, we need local norm residue symbols to describe the quotient of the symbols $\left(\frac{\alpha}{\beta}\right)_n$ and $\left(\frac{\beta}{\alpha}\right)_n$. As our number field K contains a primitive n-th root of unity, we have a local n-th power norm residue pairings

$$(\,\cdot\,,\,\cdot\,)_{n,\mathfrak{p}}: \quad K_{\mathfrak{p}}^* \times K_{\mathfrak{p}}^* \longrightarrow \langle \zeta_n \rangle$$

for each prime $\mathfrak{p}$. They bear the following relation to the n-th power residue symbol.

3.12. Proposition. *Let K contain a primitive n-th root of unity. Then we have*

$$(\beta, \alpha)_{n,\mathfrak{p}} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{\mathrm{ord}_{\mathfrak{p}}(\beta)}$$

for $\alpha, \beta \in K^*$ and $\mathfrak{p}$ a prime of K outside the set $S(\alpha)$ of primes that divide $n \cdot \infty$ or occur in the factorization of (α). In particular, the n-th power residue symbol can be written as a product

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p} \in S(\alpha)} (\beta, \alpha)_{n,\mathfrak{p}}.$$

Proof. The local extension $K_{\mathfrak{p}}(\sqrt[n]{\alpha})/K_{\mathfrak{p}}$ is unramified at $\mathfrak{p} \notin S(\alpha)$, so we can write $\beta = u \cdot \pi_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(\beta)}$ and use 3.4 (2) to obtain $(\beta, \alpha)_{n,\mathfrak{p}} = (\pi_{\mathfrak{p}}, \alpha)_{n,\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(\beta)}$. By 3.10 and the definition of the local Artin map we have $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = (\pi_{\mathfrak{p}}, \alpha)_{n,\mathfrak{p}}$, which yields the first identity. In view of 3.9, the final statement follows immediately. □

The symmetry relation $(\alpha, \beta)_{n,\mathfrak{p}}(\beta, \alpha)_{n,\mathfrak{p}} = 1$ for the norm residue symbols and the product formula 3.5 now yield the main result of this chapter.

3.13. Power reciprocity law. *Let K contain a primitive n-th root of unity. Then we have*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} \in S(\alpha) \cap S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}.$$

for $\alpha, \beta \in K^*$. If α is a unit at primes outside n, this yields the supplementary law $\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p} | n \cdot \infty} (\alpha, \beta)_{n,\mathfrak{p}}$.

Proof. By the preceding proposition, we have

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} \notin S(\alpha)} (\beta, \alpha)_{n,\mathfrak{p}} \prod_{\mathfrak{p} \notin S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}^{-1}.$$

By the product formula, we can replace the second factor by $\prod_{\mathfrak{p} \in S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}$. All symbols in the first factor at primes outside $S(\alpha) \cup S(\beta)$ equal 1, and the remaining symbols at the primes $\mathfrak{p} \in S(\beta) \setminus S(\alpha)$ annihilate the corresponding symbol in $\prod_{\mathfrak{p} \in S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}$,so we are left with the product $\prod_{\mathfrak{p} \in S(\alpha) \cap S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}$. The final statement is a direct consequence of the definition 3.9. □

We see that the power reciprocity law expresses the quotient of the power residue symbols $\left(\frac{\alpha}{\beta}\right)_n$ and $\left(\frac{\beta}{\alpha}\right)_n$ in terms of norm residue symbols at a few primes. If α and β are coprime, these are just the primes dividing $n \cdot \infty$. Note that the hypothesis $\zeta_n \in K$ implies for $n > 2$ that the norm residue symbols at the archimedean primes are trivial.

For $n = 2$ and $K = \mathbf{Q}$, Jacobi's reciprocity law 3.6 expresses the fact that the quadratic norm residue symbols at $\mathbf{Q}_\infty = \mathbf{R}$ is given by

$$(a, b)_\infty = (-1)^{\frac{(\mathrm{sgn}(a)-1)(\mathrm{sgn}(b)-1)}{4}},$$

and the symbol at $\mathbf{Q}_2$ for a and b odd by

$$(a,b)_2 = (-1)^{(a-1)(b-1)/4}.$$

We leave the second identity as an exercise and do a more complicated example instead: the biquadratic reciprocity law for the ring of Gaussian integers $\mathbf{Z}[i]$. This reciprocity law was formulated by Gauss in 1830 and proved by Eisenstein in 1844.

Let us call an element $\alpha \in \mathbf{Z}[i]$ *primary* if it is congruent to 1 mod $(1+i)^3$. The isomorphism $\langle i\rangle \xrightarrow{\sim} (\mathbf{Z}[i]/(1+i)^3\mathbf{Z}[i])^*$ shows that every element of $\mathbf{Z}[i]$ coprime to $1+i$ is primary after multiplication by a suitable power of i.

3.14. Biquadratic reciprocity law. *Suppose that $\alpha,\beta \in \mathbf{Z}[i]$ are primary and coprime. Then we have*

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = (-1)^{(N\alpha-1)(N\beta-1)/16},$$

where $N : \mathbf{Z}[i] \to \mathbf{Z}$ denotes the norm.

Proof. By the general power reciprocity law, we have $\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = (\alpha,\beta)_{4,(1+i)}$, so we have to compute part of the biquadratic norm pairing $F^* \times F^* \to \langle i\rangle$ on the local field $F = \mathbf{Q}_2(i)$.

Let $A = \mathbf{Z}_2[i]$ be the ring of integers of F and U the unit group of A. By definition, the primary elements of $\mathbf{Z}[i]$ are those elements that lie in $U^{(3)}$, and it is easy to see that $\alpha \in U^{(3)}$ has norm $N(\alpha) \in 1+8\mathbf{Z}$ if and only if it is in $U^{(4)}$. As $U^{(3)}/U^{(4)}$ has order 2, the theorem states that the norm pairing for F^* induces the unique non-degenerate bilinear map

$$U^{(3)}/U^{(4)} \times U^{(3)}/U^{(4)} \longrightarrow \langle -1\rangle.$$

In order to check that $U^{(3)}$ and $U^{(4)}$ annihilate each other, it suffices by the exercise following 3.15 to show the equality $U^4 = U^{(7)} = 1 + (1+i)^7 A$. From the identity $U = \langle i\rangle \times U^{(3)}$ one easily derives the inclusion $U^4 \subset U^{(7)}$, and equality follows as we have $[U : U^4] = 2^6 = [U : U^{(7)}]$ (exercise!). We finally need to show the identity $(\alpha,\alpha)_4 = -1$ for a generator α of $U^{(3)}/U^{(4)}$. Indeed, we have $(\alpha,\alpha)_4 = (-1,\alpha)_4 = (-1)^{(N(\alpha)-1)/4} = -1$ as required. □

With a little extra work, one can compute the full biquadratic norm pairing on $F = \mathbf{Q}_2(i)$. This is necessary if one wants to have the biquadratic supplementary laws as well. Denote by $\pi = 1 - i$ a prime element and by $\eta_k = 1 - (1-i)^k$ a generator of $U^{(k)}/U^{(k+1)}$, then we have

$$\begin{aligned} F^*/F^{*4} = \langle\pi\rangle \times U/U^4 &= \langle\pi\rangle \times \langle\eta_1\rangle \times \langle\eta_3\rangle \times \langle\eta_4\rangle \\ &= \langle 1-i\rangle \times \langle i\rangle \times \langle 3+2i\rangle \times \langle 5\rangle. \end{aligned}$$

We can compute the biquadratic symbol on these generators by elementary arguments. By the anti-symmetry of the symbol, we only need to compute the symbols (π,π), (π,η_k) and (η_k,η_l) with $k,l \in \{1,3,4\}$ and $k \le l$. This can be done *using* the reciprocity law, by computing explicit power residue symbols, but often there are shorter arguments.

We have $(1-i, 1-i) = (1-i, -1) = (1-i, i)^2 = 1$ and also $(1-i, \eta_k) = 1$ for $k = 1, 3$ since $(1-i, \eta_k)^k = (1-\eta_k, \eta_k) = 1$. Further $(i, 1-i) = 1$ and $(i, i) = 1$ since $(i, i)^3 = (i, -i) = 1$. For $k = 3, 4$ we have $(i, \eta_k) = \left(\frac{i}{\eta_k}\right)_4$ and we can use the definition of the power residue symbol. This also applies to $(1-i, \eta_4)$. The result is the following.

$(\cdot,\cdot)_4$	π	η_1	η_3	η_4
π	1	1	1	i
η_1	1	1	$-i$	-1
η_3	1	i	-1	1
η_4	$-i$	-1	1	1

In a similar way one can derive a cubic reciprocity law for the ring $\mathbf{Z}[\zeta_3]$. As in the case of the biquadratic reciprocity law, the first proof was given by Eisenstein in 1844. Every element $\alpha \in \mathbf{Z}[\zeta_3]$ coprime to $(3) = (1-\zeta_3)^2$ can be multiplied by a cube root of unity to satisfy the congruence $\alpha \equiv \pm 1 \bmod (1-\zeta_3)^2$. Let us call such an element 3-primary.

3.15. Cubic reciprocity law. *Suppose that $\alpha, \beta \in \mathbf{Z}[\zeta_3]$ are 3-primary and coprime. Then we have*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

Proof. Let U be the unit group of the ring of integers of $F = \mathbf{Q}_3(\zeta_3)$. By assumption, we have $\pm\alpha, \pm\beta \in U^{(2)}$, and since -1 is a cube we have to show that the cubic norm residue symbol on F^* induces the trivial pairing on $U^{(2)} \times U^{(2)}$. This follows from the exercise below and the identity $U^{(4)} = U^3$. □

Exercise. Show that under the n-th power norm residue pairing on a non-archimedean local number field F, the unit groups $U_F^{(i)}$ and $U_F^{(j)}$ annihilate each other when $U_F^{(i+j)}$ is contained in U_F^n.
[Hint: Use the relation $(\frac{1+a}{1-ab}, 1-\frac{1+a}{1-ab}) = 1$.]

The original 19-th century proofs of the cubic and biquadratic reciprocity laws made use of Jacobi sums, see [Ireland-Rosen]. For higher exponents these methods fail, and only after class field theory had been developed the first general reciprocity laws were proved by Artin and Hasse in the period 1930-1940. There is no loss of generality in assuming that the exponent is a prime power p^k, and in that case the power reciprocity law reduces everything to the explicit computation of the p^k-th power norm residue symbols in local fields $F \supset \mathbf{Q}_p(\zeta_{p^k})$.

A basic case is the p-power reciprocity in $\mathbf{Q}(\zeta_p)$ for a prime $p > 2$. In that case the reciprocity law for elements $\alpha, \beta \in \mathbf{Q}(\zeta_p)^*$ that are relatively prime has the simple form

$$\left(\frac{\alpha}{\beta}\right)_p \left(\frac{\beta}{\alpha}\right)_p^{-1} = (\alpha, \beta)_F, \tag{3.16}$$

where $(\alpha, \beta)_F$ is the p-th power norm residue symbol in $F = \mathbf{Q}_p(\zeta_p)$.