Chapter 9
Ambiguous Ideal Classes and Quadratic Reciprocity

It is quite difficult to determine class numbers, even in the simplest case of quadratic number fields, for fields with large discriminant. It is, however, possible to make several rather precise statements concerning the parity of class numbers of quadratic number fields. The theory behind these statements is called genus theory and goes back to Gauss, who worked with quadratic forms rather than quadratic number fields. Genus theory may be generalized to cyclic extensions, and in fact the question we will answer is how the Galois group of an extension acts on the ideal classes. In this chapter we will only scratch the surface of genus theory by proving the ambiguous class number formula.

The essential idea behind the proof is to reduce the action of the Galois group on ideal classes to the action on ideals, then on principal ideals and finally on elements, where everything can be done explicitly. Once more we will be studying a difficult object, namely the class group, by studying homomorphisms into simpler structures.

9.1 Ambiguous Ideal Classes

Let A be a finite abelian group. Then A can be written as a direct sum of cyclic groups, say $A = A_1 \oplus \cdots \oplus A_n$. If A is a finite 2-group, i.e., a group whose order is a power of 2, then the 2-rank of A is the number n of cyclic components. Since it is easy to see that $A/A^2 \simeq A_1/A_1^2 \oplus \cdots \oplus A_n/A_n^2$, and since $A_j/A_j^2 \simeq \mathbb{Z}/2\mathbb{Z}$ for cyclic groups A_j, the 2-rank of A is n if and only if $\#A/A^2 = 2^n$.

The determination of the order of the quotient group $\mathrm{Cl}(k)/\mathrm{Cl}(k)^2$, i.e., of the 2-rank of the ideal class group, goes back to Gauss, who solved this problem in the language of binary quadratic forms. It is almost impossible to miss the central questions of this theory when studying the operation of the Galois group $G = \{1, \sigma\}$ of $k/\mathbb{Q}$ on the ideal class group.

F. Lemmermeyer, *Quadratic Number Fields*, Springer Undergraduate Mathematics Series, https://doi.org/10.1007/978-3-030-78652-6_9

For an ideal class $c = [\mathfrak{a}]$ we set $c^\sigma = [\mathfrak{a}^\sigma]$; of course we have to show that this action is well defined (see Exercise 9.1). Clearly an ideal class c and its conjugate c^σ always have the same order. Moreover, since $c \cdot c^\sigma = [\mathfrak{a}][\mathfrak{a}^\sigma] = [(N\mathfrak{a})] = (1)$ is the principal class, $c^\sigma = c^{-1}$ is always the inverse class of c.

We call an ideal class $c \in \mathrm{Cl}(k)$ ambiguous if $c^\sigma = c$. Similarly, an ideal $\mathfrak{a}$ is called ambiguous, if $\mathfrak{a}^\sigma = \mathfrak{a}$.

Lemma 9.1 *The nontrivial automorphism $\sigma : \sqrt{m} \to -\sqrt{m}$ of $k = \mathbb{Q}(\sqrt{m})$ acts as -1 on the class group $Cl(k)$. In particular, an ideal class c is ambiguous if and only if $c^2 = 1$.*

Proof We have already seen that $\mathfrak{a}^{1+\sigma} = \mathfrak{a}\mathfrak{a}' = (N\mathfrak{a})$ is principal, and that this implies that $c^\sigma = c^{-1}$.

If c is ambiguous, i.e., if $c = c^\sigma$, then $c^2 = c^{1+\sigma} = 1$. Conversely, if $c^2 = 1$, then $c^\sigma = c^{-1} = c$. □

If k is a number field with class number 2, then the nontrivial ideal class c is always ambiguous. For $k = \mathbb{Q}(\sqrt{-5})$, the nontrivial ideal class is generated by the prime ideal $(2, 1+\sqrt{-5})$; since this ideal is ambiguous because of $(2, 1+\sqrt{-5})^\sigma = (2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})$. The ideal class c is also generated by $(3, 1+\sqrt{-5})$, and here $(3, 1+\sqrt{-5})^\sigma = (3, 1-\sqrt{-5}) \neq (3, 1+\sqrt{-5})$. In $\mathbb{Q}(\sqrt{-5})$, each ideal class contains an ambiguous ideal (the principal class contains the ambiguous ideal (1)), as well as many non-ambiguous ideals.

For ideal class groups of order 4, the number of ambiguous classes determines the structure. If $\mathrm{Cl}(k) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is elementary abelian, then the number of ambiguous ideal classes is 4 since in this case, every ideal class is ambiguous. If $\mathrm{Cl}(k) \simeq \mathbb{Z}/4\mathbb{Z}$, on the other hand, then the two classes with order 4 are not ambiguous, whereas the class with order 2 and the principal class are ambiguous, Thus there are only 2 ambiguous ideal classes in this case.

If an ideal $\mathfrak{a}$ is ambiguous, then so is the ideal class $c = [\mathfrak{a}]$ it generates; the converse is not true in general: Since $k = \mathbb{Q}(\sqrt{34})$ has class number 2, the ideal class c of order 2 is ambiguous. This ideal class is not generated by an ambiguous ideal for the simple reason that all ambiguous ideals in k are principal. As we will see below, each ambiguous ideal is a product of ramified prime ideals and ideals generated by ordinary integers. But in k we have $(2, \sqrt{34}) = (6 + \sqrt{34})$ and $(17, \sqrt{34}) = (17 + 3\sqrt{34})$.

The ambiguous ideal classes form a group $\mathrm{Am}(k)$, in which the ideal classes generated by ambiguous ideals form a subgroup, namely the group $\mathrm{Am}_{\mathrm{st}}(k)$ of strongly ambiguous ideal classes. Our goal is determining the structure of the group $\mathrm{Am}(k)$.

This will allow us to deduce information about the elements of order 2 in the class group. In fact, since $c^\sigma = c^{-1}$ we have $c^{1-\sigma} = c^2$, and therefore the homomorphism $c \mapsto c^{1-\sigma}$ maps the class group $\mathrm{Cl}(k)$ of a quadratic number field k to the group $\mathrm{Cl}(k)^{1-\sigma} = \mathrm{Cl}(k)^2$ of ideal classes that are squares, and this homomorphism is onto. Its kernel consists of the ideal classes c with $c^{1-\sigma} = 1$, i.e., of the ambiguous

ideal classes. This implies that the order of the group $\mathrm{Am}(k)$ of ambiguous ideal classes is equal to the order of $\mathrm{Cl}(k)/\mathrm{Cl}(k)^2$:

Proposition 9.2 *Let k be a quadratic number field. Then*

$$\#Cl(k)/Cl(k)^2 = \#\,\mathrm{Am}(k),$$

and, in particular, the class number of k is odd if and only if the number of ambiguous ideal classes is 1.

Actually, since both groups are elementary abelian, equal cardinality implies isomorphism. The last claim follows from the observation that squaring is an isomorphism on a finite group if and only if it has odd order.

9.1.1 Exact Sequences

The calculations below are far easier to digest by using exact sequences. A short sequence of abelian groups A, B, C consists of group homomorphisms $\alpha : A \longrightarrow B$ and $\beta : B \longrightarrow C$, which are composed as follows:

$$1 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 1. \tag{9.1}$$

The map $1 \longrightarrow A$ (which is often denoted by $0 \longrightarrow A$ if A is written additively) sends the element of the trivial group $\{1\}$ to the neutral element of A. Similarly, $C \longrightarrow 1$ is the homomorphism sending each element of C to the element of the trivial group $\{1\}$.

A sequence of abelian groups is called exact if the kernel of each map in the sequence is equal to the image of the preceding map (if there is one). Thus the sequence (9.1) is exact if and only if the following conditions are satisfied:

- $\ker\alpha = \mathrm{im}\ (1 \longrightarrow A) = \{1\}$; in other word, α must be injective;
- $C = \ker(C \longrightarrow 1) = \mathrm{im}\ \beta$; in other words, β must be surjective;
- $\ker\beta = \mathrm{im}\ \alpha$.

Essentially, this short exact sequence contains the same information as the homomorphism theorem $C \simeq B/\mathrm{im}\ A$, but it has the advantage that all the maps occur explicitly in the diagram. Perhaps this advantage will only become clear by studying homological algebra more carefully. One goal of this chapter is showing that this is a useful thing to do for those who are interested in algebraic number theory.

The proof of Proposition 9.2 consisted in verifying the exactness of the sequence

$$1 \longrightarrow \mathrm{Am}(k) \longrightarrow \mathrm{Cl}(k) \xrightarrow{1-\sigma} \mathrm{Cl}(k)^2 \longrightarrow 1.$$

The definitions of principal ideals and the ideal class group $\mathrm{Cl}(k)$ of a number field k provide us with two exact sequences, namely

$$1 \longrightarrow E_k \longrightarrow k^\times \longrightarrow H_k \longrightarrow 1,$$
$$1 \longrightarrow H_k \longrightarrow I_k \longrightarrow \mathrm{Cl}(k) \longrightarrow 1,$$

where E_k is the unit group, H_k the group of (fractional) principal ideals $\neq (0)$, and I_k the group of all fractional ideals $\neq (0)$.

9.1.2 Ambiguous Ideal Classes

The group $\mathrm{Am}_{\mathrm{st}}(k)$ of strongly ambiguous ideal classes is, by definition, equal to $\mathrm{Am}_{\mathrm{st}}(k) = AH/H \simeq A/A \cap H$, where A denotes the group of nonzero ambiguous ideals and H the group of nonzero principal ideals. Clearly $A \cap H = H^G$ is the group of ambiguous principal ideals, and so we have $\mathrm{Am}_{\mathrm{st}}(k) \simeq A/H^G$. This observation gives us the exact sequence

$$1 \longrightarrow H^G \xrightarrow{\iota} A \longrightarrow \mathrm{Am}_{\mathrm{st}}(k) \longrightarrow 1.$$

The group P of all fractional ideals (a) with $a \in \mathbb{Q}^\times$ is a subgroup of both H^G and A; this allows us to modify the exact sequence slightly and turn it into

$$1 \longrightarrow H^G/P \xrightarrow{\iota} A/P \xrightarrow{\pi} \mathrm{Am}_{\mathrm{st}}(k) \longrightarrow 1. \tag{9.2}$$

Since $\mathrm{Am}(k)$ is elementary abelian, i.e., since $c^2 = 1$ for each ambiguous ideal class c, for determining the structure of $\mathrm{Am}(k)$ and $\mathrm{Am}_{\mathrm{st}}(k)$ it is sufficient to compute the orders of these groups. The exact sequence (9.2) is a first step in this direction. The next steps consist in the computation of the order of H^G/P and of A/P. Before we do so we present a simple but very effective tool.

9.1.3 Hilbert's Theorem 90

Hilbert's Theorem 90 (in Hilbert's report on algebraic numbers, his famous *Zahlbericht*, the theorems were numbered, and this one had the number 90) comes in two versions, one for elements and one for ideals.

Theorem 9.3 (Hilbert's Theorem 90 for Elements) *Let k be a quadratic number field and $\alpha \in k^\times$. Then $N\alpha = 1$ if and only if α has the form $\alpha = \beta^{1-\sigma}$. Here β is determined uniquely up to rational factors.*

Equivalent formulations of Hilbert's Theorem 90 are the following:

1. There is an exact sequence

$$1 \longrightarrow (k^\times)^{1-\sigma} \longrightarrow k^\times \xrightarrow{N} k^\times,$$

   where N denotes the norm map $N_{k/\mathbb{Q}} : k^\times \longrightarrow \mathbb{Q}^\times$.
2. The group $k^\times[N]/(k^\times)^{1-\sigma}$ is trivial. Here $k^\times[N]$ denotes the kernel of the norm map $N : k^\times \longrightarrow \mathbb{Q}^\times$.

Proof The proof of "$\Longleftarrow$" is trivial. Assume therefore that $N\alpha = 1$. If $\alpha = -1$, we set $\beta = \sqrt{m}$; if $\alpha \neq -1$, we set $\beta = \alpha^\sigma + 1$; then $\beta^{\sigma-1} = \frac{\alpha+1}{\alpha'+1} = \frac{\alpha(\alpha+1)}{\alpha\alpha'+\alpha} = \frac{\alpha(\alpha+1)}{1+\alpha} = \alpha$. □

The corresponding result for ideals is

Theorem 9.4 (Hilbert's Theorem 90 for Ideals) *If $\mathfrak{a}$ is a fractional ideal*[1] *in $\mathcal{O}_k$, then we have $N\mathfrak{a} = (1)$ if and only if $\mathfrak{a}$ has the form $\mathfrak{a} = \mathfrak{b}^{\sigma-1}$ for some (integral) ideal $\mathfrak{b}$.*

Proof As in the case of elements, the proof of "$\Longleftarrow$" is trivial. Assume therefore that $N\mathfrak{a} = 1$ (hence $\mathfrak{a} = \mathfrak{c}\mathfrak{d}^{-1}$ is the quotient of two integral ideals $\mathfrak{c}$ and $\mathfrak{d}$ with the same norm). By the uniqueness of prime ideal factorization we may assume that $\mathfrak{c}$ and $\mathfrak{d}$ are coprime. This immediately implies that $\mathfrak{c}$ and $\mathfrak{d}$ are not divisible by any inert prime ideals: If, for example, we had $(q) \mid \mathfrak{c}$, then q^2 would occur in the factorization of $N\mathfrak{d}$, hence $\mathfrak{d}$ would also be divisible by (q), and this contradicts our assumption that $\mathfrak{c}$ and $\mathfrak{d}$ are coprime. For the same reason, no ramified prime ideals can divide $\mathfrak{c}$. Thus $\mathfrak{c}$ and $\mathfrak{d}$ are products of split prime ideals. If $\mathfrak{c} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ is the prime ideal factorization of $\mathfrak{c}$, then we must have $N\mathfrak{c} = p_1^{e_1} \cdots p_r^{e_r} = N\mathfrak{d}$. Since $\mathfrak{c}$ and $\mathfrak{d}$ are coprime, none of the $\mathfrak{p}_j$ can divide $\mathfrak{d}$, hence the only possibility is that $\mathfrak{d} = \mathfrak{p}_1'^{e_1} \cdots \mathfrak{p}_r'^{e_r} = \mathfrak{c}'$. But then $\mathfrak{a} = \mathfrak{c}\mathfrak{d} = \mathfrak{d}'\mathfrak{d}^{-1} = \mathfrak{d}^{\sigma-1}$. □

9.2 The Ambiguous Class Number Formula

As a warm-up we construct a few exact sequences involving the following groups:

- $E = \mathcal{O}_k^\times$ is the unit group of $\mathcal{O}_k$;
- $E[N] = \{\varepsilon \in E : N_{k/\mathbb{Q}}(\varepsilon) = 1\}$ is the kernel of the norm map on the unit group, that is, the subgroup of units with norm $+1$;
- $E^{1-\sigma} = \{\varepsilon^{1-\sigma} : \varepsilon \in E\}$;
- $H^G = \{(\alpha) : (\alpha)^\sigma = (\alpha)\}$ is the group of ambiguous principal ideals;
- $P = \{(a) : a \in \mathbb{Q}^\times\}$ is the subgroup of A consisting of all nonzero ideals generated by rational numbers.

[1] For integral ideals, the statement is trivial since then $N\mathfrak{a} = (1)$ is equivalent to $\mathfrak{a} = (1)$.

Now we claim

Proposition 9.5 *There is an exact sequence*

$$1 \longrightarrow E^{1-\sigma} \longrightarrow E[N] \xrightarrow{\lambda} H^G/P \longrightarrow 1.$$

Proof The map $E^{1-\sigma} \longrightarrow E[N]$ is the inclusion map: Each unit $\varepsilon^{1-\sigma}$ has norm 1 and thus is an element of $E[N]$. For constructing $\lambda : E[N] \longrightarrow H^G/P$ assume that $\varepsilon \in E[N]$, i.e., $N\varepsilon = 1$. By Hilbert's Theorem 90 there is an $\alpha \in k^\times$ such that $\varepsilon = \alpha^{1-\sigma}$; clearly $(\alpha) \in H^G$ since $(\alpha)^\sigma = (\alpha^\sigma) = (\varepsilon\alpha) = (\alpha)$. The map $\varepsilon \mapsto (\alpha)$ is not well defined, however, since with α each element αa for any $a \in \mathbb{Q}^\times$ has the property $(\alpha a)^{1-\sigma} = \varepsilon$. For this reason we set $\lambda(\varepsilon) = (\alpha)P$, and this map now is well defined. Clearly $\varepsilon \in \ker\lambda$ if and only if $\lambda(\varepsilon) = P$; this is equivalent to $(\alpha) = (a)$, i.e., to $\alpha = a\eta$ for some unit η. This implies $\varepsilon = \alpha^{1-\sigma} = \eta^{1-\sigma}$, which shows that $\ker\lambda = E^{1-\sigma}$.

The surjectivity of λ is clear: If (α) is ambiguous, then $(\alpha)^\sigma = (\alpha)$ and thus $\varepsilon\alpha^\sigma = \alpha$ for some unit ε, hence $\varepsilon = \alpha^{1-\sigma}$. □

The content of this proposition may also be expressed by the isomorphism

$$E[N]/E^{1-\sigma} \simeq H^G/P.$$

The quotient group $H^{-1}(G, E) = E[N]/E^{1-\sigma}$ is a cohomology group. We have come across such a group already in Hilbert's Theorem 90, which says that $H^{-1}(G, k^\times) = k^\times[N]/(k^\times)^{1-\sigma} = 1$. Hilbert's Theorem 90 for ideals claims accordingly that $H^{-1}(G, I_k) = I_k[N]/I_k^{1-\sigma} = 1$, where I_k denotes the group of nonzero fractional ideals in a quadratic number field. Such cohomology groups for cyclic Galois groups $G = \langle\sigma\rangle$ are all over the place in class field theory, the theory of abelian extensions of number fields.

Galois cohomology[2] gives the exact sequence in Proposition 9.5 in the other direction (Exercise 9.10).

The order of the group $E[N]/E^{1-\sigma}$ can be determined quickly. If $\Delta < 0$, then E consists only of roots of unity with norm 1. Thus $\varepsilon^\sigma = \varepsilon^{-1}$, hence $E^{1-\sigma} = E^2$ and

[2]Those who are familiar with the first principles of cohomology get the sequence for free: The trivial sequence

$$1 \longrightarrow E \longrightarrow k^\times \longrightarrow H \longrightarrow 1,$$

in which H denotes the group of nonzero fractional principal ideals, provides the long exact sequence

$$1 \longrightarrow E^G \longrightarrow (k^\times)^G \longrightarrow H^G \longrightarrow H^1(G, E) \longrightarrow H^1(G, k^\times),$$

from which the claim follows using Hilbert's Theorem 90 ($H^1(G, k^\times) = 1$), the periodicity $H^1(G, A) \simeq H^{-1}(G, A)$ for cyclic groups G, as well as $(k^\times)^G = \mathbb{Q}^\times$, $E^G = \{\pm 1\}$ and $\mathbb{Q}^\times/E^G \simeq P$.

$E[N]/E^{1-\sigma} = E/E^2 \simeq \mathbb{Z}/2\mathbb{Z}$. If $\Delta > 0$, then let ε denote the fundamental unit. If $N\varepsilon = +1$, then again $E[N] = E$ and $E^{1-\sigma} = E^2$, hence $E[N]/E^{1-\sigma} = E/E^2 = \langle -1, \varepsilon\rangle/\langle\varepsilon^2\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$. If $N\varepsilon = -1$, on the other hand, then $E[N] = \langle -1, \varepsilon^2\rangle$ and $E^{1-\sigma} = E^2 = \langle\varepsilon^2\rangle$, hence $E[N]/E^{1-\sigma} = E/E^2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Lemma 9.6 *Let k be a quadratic number field whose unit group E is generated by the fundamental unit ε (and -1). Then*

$$H^{-1}(G, E) = E[N]/E^{1-\sigma} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } d < 0, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } d > 0,\ N\varepsilon = -1, \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if } d > 0,\ N\varepsilon = +1. \end{cases}$$

It remains to determine the order of A/P. To this end we will use the following lemma.

Lemma 9.7 *An ideal $\mathfrak{a}$ is ambiguous if and only if $\mathfrak{a}$ is the product of ramified prime ideals and an ideal (a) with $a \in \mathbb{Q}^\times$. More exactly we have*

$$A/P \simeq (\mathbb{Z}/2\mathbb{Z})^t,$$

where t is the number of primes that ramify in $k/\mathbb{Q}$, in other words, the number of distinct prime factors of the discriminant of k.

Proof We may assume that $\mathfrak{a}$ is an integral ideal (otherwise we multiply it by a suitable rational integer). Among all decompositions $\mathfrak{a} = (a)\mathfrak{b}$ with an integral ideal $\mathfrak{b}$ we pick one in which $a \in \mathbb{N}$ is maximal.

Let $\mathfrak{p}$ denote a prime ideal with $\mathfrak{p}^\sigma \neq \mathfrak{p}$; if $\mathfrak{p}$ divides $\mathfrak{b}$, then we must have $\mathfrak{p}^\sigma \mid \mathfrak{b}$. In fact by applying σ to $\mathfrak{p} \mid \mathfrak{a}$ we see that $\mathfrak{p}^\sigma \mid \mathfrak{b}^\sigma = \mathfrak{b}$. Thus $(p) \mid \mathfrak{b}$, where $(p) = \mathfrak{p}\mathfrak{p}^\sigma$, which contradicts the maximality of a. This shows that $\mathfrak{b}$ is not divisible by a split prime ideal.

For the same reason, $\mathfrak{b}$ is not divisible by any inert prime ideal (p). Thus $\mathfrak{b}$ is a product of ramified prime ideals. If $\mathfrak{p}$ is such a prime ideal, then $\mathfrak{p}^2 = (p)$, and the maximality of a implies that we can write $\mathfrak{a}$ uniquely in the form

$$\mathfrak{a} = (a)\prod \mathfrak{p}_j^{e_j},$$

where $\mathfrak{p}_j$ runs through the ramified prime ideals and where $e_j \in \{0, 1\}$. Now we set

$$\phi : A/P \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t : (a)\prod \mathfrak{p}_j^{e_j} \longmapsto (e_1, \ldots, e_t)$$

and show that ϕ is a group isomorphism, which is left as an exercise. □

If we collect everything, then the exact sequence (9.2) now implies

Corollary 9.8 *In the quadratic number field k with discriminant Δ and fundamental unit ε we have*

$$\#\,\mathrm{Am}_{\mathrm{st}}(k) = \begin{cases} 2^{t-1} & \text{if } \Delta < 0, \\ 2^{t-1} & \text{if } \Delta > 0,\ N\varepsilon = -1, \\ 2^{t-2} & \text{if } \Delta > 0,\ N\varepsilon = +1, \end{cases}$$

where t denotes the number of primes that ramify in k.

Thus it remains only to determine the difference between the group of ambiguous ideal classes $\mathrm{Am}(k)$ and that of strictly ambiguous ideal classes $\mathrm{Am}_{\mathrm{st}}(k)$:

Proposition 9.9 *There is an exact sequence*

$$1 \longrightarrow \mathrm{Am}_{\mathrm{st}}(k) \longrightarrow \mathrm{Am}(k) \xrightarrow{\mu} (E_{\mathbb{Q}} \cap Nk^{\times})/NE_k \longrightarrow 1.$$

In particular, $\mathrm{Am}(k) = \mathrm{Am}_{\mathrm{st}}(k)$ *except when* -1 *is the norm of an element, but not of a unit. In this case,* $\#\,\mathrm{Am}(k) = 2 \cdot \#\,\mathrm{Am}_{\mathrm{st}}(k)$.

Proof Let $c = [\mathfrak{a}]$ be ambiguous. Then $\mathfrak{a}^{\sigma} \sim \mathfrak{a}$, hence $\mathfrak{a}^{\sigma} = \alpha\mathfrak{a}$. Taking norms yields $(N\alpha) = (1)$, that is $N\alpha = \pm 1 \in E_{\mathbb{Q}} \cap Nk^{\times}$. We set $\mu(c) = N\alpha \cdot NE_k$ and claim that μ is well defined. In fact if we start from $c = [\mathfrak{b}]$, then $\mathfrak{b} = \gamma\mathfrak{a}$, and $\mathfrak{b}^{\sigma} = \gamma^{\sigma}\mathfrak{a}^{\sigma} = \gamma^{\sigma}\alpha\mathfrak{a} = \gamma^{\sigma-1}\alpha\mathfrak{b}$ shows that $N(\gamma^{\sigma-1}\alpha) \cdot NE_k = N\alpha \cdot NE_k$ since elements of the form $\gamma^{\sigma-1}$ have norm 1. Thus μ is well defined.

If $c \in \ker\mu$, then $N\alpha = N\eta$, d.h. $N(\alpha\eta) = 1$. According to Hilbert's Theorem 90, we have $\alpha\eta = \beta^{1-\sigma}$, and now $\mathfrak{a}^{\sigma} = \alpha\mathfrak{a}$ implies $(\beta\mathfrak{a})^{\sigma} = (\beta)\mathfrak{a}$. Thus $\mathfrak{b} = \beta\mathfrak{a}$ is an ambiguous ideal equivalent to $\mathfrak{a}$, and therefore $c = [\mathfrak{b}]$ is strongly ambiguous. Conversely, strongly ambiguous ideal classes are clearly contained in $\ker\mu$.

In order to prove the surjectivity of μ we have to show that $-1NE_k$ lies in the image of μ if -1 is the norm of an element from k. Assume therefore that $N\alpha = -1$ for $\alpha = x + y\sqrt{m}$. Then $x^2 - my^2 = -1$, hence -1 is a quadratic residue modulo each odd prime divisor p of m. We know from elementary number theory (or from the arithmetic of Gaussian integers) that this holds if and only if $m = a^2 + b^2$ is a sum of two squares; here we may assume that a is odd. Now we verify that $\mathfrak{a} = (a, b + \sqrt{m})$ generates an ambiguous ideal class $c = [\mathfrak{a}]$, and that $\mu(c) = -1$. In fact we have

$$\begin{aligned} \mathfrak{a}^2 &= (a^2, ab + a\sqrt{m}, b^2 + 2b\sqrt{m} + m) \\ &= (a^2, ab + a\sqrt{m}, 2b^2 + 2b\sqrt{m}) \\ &= (a^2, a(b + \sqrt{m}), 2b(b + \sqrt{m})) = (a^2, b + \sqrt{m}) = (b + \sqrt{m}) \end{aligned}$$

because of $\gcd(a^2, 2b) = 1$ and $(b+\sqrt{m})(b-\sqrt{m}) = b^2 - m = -a^2$. Thus $\mathfrak{a}^2 = (b+\sqrt{m})$ and $\mathfrak{a}\mathfrak{a}^\sigma = N\mathfrak{a} = (a)$, and therefore $\mathfrak{a}^{1-\sigma} = \mathfrak{a}^2/\mathfrak{a}^{1+\sigma} = \frac{1}{a}(b+\sqrt{m})$. This yields $\mu(c) = N(\frac{b+\sqrt{m}}{a}) = \frac{b^2-m}{a^2} = -1$ as claimed. □

The group $(E_{\mathbb{Q}} \cap Nk^\times)/NE_k$ is small, because even $E_{\mathbb{Q}} = \{\pm 1\}$ has only two elements. In fact we have $(E_{\mathbb{Q}} \cap Nk^\times)/NE_k = 1$ unless -1 is the norm of an element from k or if $N\varepsilon = -1$, and $(E_{\mathbb{Q}} \cap Nk^\times)/NE_k \simeq \mathbb{Z}/2\mathbb{Z}$ if -1 is the norm of an element, but not the norm of a unit. As we just have seen, -1 is the norm of an element if and only if $\Delta = \square + \square$ is the sum of two squares. Thus we have

Theorem 9.10 (Ambiguous Class Number Formula) *In quadratic number fields k with discriminant Δ and fundamental unit ε we have*

$$\#\operatorname{Am}(k) = \begin{cases} 2^{t-2}, & \text{if } \Delta > 0,\ N\varepsilon = +1,\ \Delta \neq \square + \square, \\ 2^{t-1}, & \text{otherwise.} \end{cases}$$

where t denotes the number of primes ramified in k.

Examples

Δ	t	$N\varepsilon$	$\square + \square$	$\#\operatorname{Am}_{\mathrm{st}}(k)$	$\#\operatorname{Am}(k)$
8	1	-1	$1^2 + 1^2$	1	1
10	2	-1	$1^2 + 3^2$	2	2
12	2	$+1$	no	1	1
30	3	$+1$	no	2	2
34	2	$+1$	$3^2 + 5^2$	1	2
-30	3	$-$	no	4	4

As an additional consequence of the ambiguous class number formula we claim:

Corollary 9.11 *The class number of the quadratic number field with discriminant Δ is odd if and only if we are in one of the following cases; there p denotes prime numbers $\equiv 1 \bmod 4$ and q, q' prime numbers $\equiv 3 \bmod 4$:*

(1) Δ is a prime discriminant, i.e., $\Delta = -4, \pm 8, p, -q$;
(2) Δ is a product of two negative prime discriminants: $\Delta = 4q$, $\Delta = 8q$ or $\Delta = qq'$.

Proof The class number of k is even if and only if $\#\operatorname{Am}(k) \neq 1$, thus if the number of ambiguous ideal classes is even. The other claims follow directly from the ambiguous class number formula. □

9.3 The Quadratic Reciprocity Law

The quadratic reciprocity law is a corollary of Corollary 9.11. We begin by proving the two supplementary laws.

Theorem 9.12 (First Supplementary Law) *For all odd prime numbers p, the following assertions are equivalent:*

(1) $(\frac{-1}{p}) = +1$, *i.e., the congruence* $x^2 \equiv -1 \bmod p$ *is solvable.*
(2) $p = a^2 + 4b^2$ *is sum of two squares.*
(3) We have $p \equiv 1 \bmod 4$.

The equivalence of (1) and (3) may also be expressed by the equation

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Proof (1) $\Longrightarrow$ (2): If $(-1/p) = 1$, then p splits in $k = \mathbb{Q}(i)$. Multiplying through by i we may assume that the coefficient of i is even. Thus $p = (a + 2bi)(a - 2bi)$, and taking the norm yields $p = a^2 + 4b^2$.

(2) $\Longrightarrow$ (3): Since p and a are odd, $p = a^2 + 4b^2$ implies $p \equiv 1 \bmod 4$.

(3) $\Longrightarrow$ (1): If $p \equiv 1 \bmod 4$, then $(\frac{-1}{p}) = (-1)^{(p-1)/2} = 1$ according to Euler's Criterion. □

Similarly we can prove

Theorem 9.13 (Second Supplementary Law) *For all odd prime numbers p, the following assertions are equivalent:*

(1) $(\frac{2}{p}) = +1$, *i.e., the congruence* $x^2 \equiv 2 \bmod p$ *is solvable.*
(2) We have $p = e^2 - 2f^2$ *for integers* $e, f \in \mathbb{Z}$.
(3) We have $p \equiv \pm 1 \bmod 8$.

The equivalence of (1) and (3) can also be expressed by the equation

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof (1) $\Longrightarrow$ (2): If $(\frac{2}{p}) = +1$, then p splits in $\mathbb{Q}(\sqrt{2})$, and we have $\pm p = x^2 - 2y^2$; multiplying $x + y\sqrt{2}$, if necessary, by the unit $1 + \sqrt{2}$ we can make sure that $p = e^2 - 2y^2$.

(2) $\Longrightarrow$ (3): Reduction modulo 8 yields $p \equiv \pm 1 \bmod 8$ in all cases.

(3) $\Longrightarrow$ (1): Let h denote the class number of $k = \mathbb{Q}(\sqrt{p})$, which is odd by Corollary 9.11. If $p \equiv \pm 1 \bmod 8$, then 2 splits in $k/\mathbb{Q}$, hence $2\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$ for prime ideals $\mathfrak{p}, \mathfrak{p}'$. Since $\mathfrak{p}^h = \frac{1}{2}(x + y\sqrt{p})$ is a principal ideal, taking the norm yields $x^2 - py^2 = \pm 4 \cdot 2^h$. Reduction modulo p shows that $\pm 2^h$ and thus ± 2 is a quadratic residue modulo p; the claim now follows from the first supplementary law. □

The quadratic reciprocity law for odd prime numbers is the content of the following theorem.

Theorem 9.14 (Quadratic Reciprocity Law) *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof We first discuss the case where one of the primes, say p, is congruent to 1 mod 4. We will show that in this case we have $\left(\frac{p}{q}\right) = +1 \iff \left(\frac{q}{p}\right) = +1$.

Since $\left(\frac{p}{q}\right) = +1$, the prime q splits in $k = \mathbb{Q}(\sqrt{p})$. Thus $q\mathcal{O}_k = \mathfrak{q}\mathfrak{q}'$ and $\mathfrak{q}^h = \frac{1}{2}(x + y\sqrt{p})$ is a principal ideal, where h is the class number of k, which is odd by Corollary 9.11. Taking the norm yields $\pm 4q^h = x^2 - py^2$. This in turn provides us with the congruence $\pm 4q^h \equiv x^2 \bmod p$, and then $\left(\frac{-1}{p}\right) = +1$ implies $\left(\frac{q}{p}\right) = +1$ as claimed.

If $\left(\frac{q}{p}\right) = +1$, on the other hand, then we use the number field $k = \mathbb{Q}(\sqrt{q})$, which also has odd class number h. Again the fact that p splits in $\mathcal{O}_k$ yields the equation $\pm 4p^h = x^2 - qy^2$ and thus $\left(\frac{\pm p}{q}\right) = +1$. Since either $q \equiv 1 \bmod 4$ and $(\frac{-1}{q}) = +1$ or $q \equiv 3 \bmod 4$ and the sign is necessarily positive (Exercise 9.15), we obtain $\left(\frac{p}{q}\right) = +1$.

Finally assume that $p \equiv q \equiv 3 \bmod 4$. Consider the field $k = \mathbb{Q}(\sqrt{pq})$. According to Corollary 9.11, the class number h of k is odd. Thus the prime ideal $\mathfrak{p} = (p, \sqrt{pq})$ above p must be principal: In fact we have $\mathfrak{p}^2 \sim (1)$ and $\mathfrak{p}^h \sim 1$, and since $h = 2j+1$ we get $\mathfrak{p} = \mathfrak{p}^{h-2j} \sim (1)$. Assume therefore that $\mathfrak{p} = \frac{1}{2}(x+y\sqrt{pq})$. Then $\pm 4p = x^2 - pqy^2$, hence $x = pz$ and $\pm 4 = pz^2 - qy^2$. If the positive sign holds, then reduction modulo q and p shows that $(\frac{p}{q}) = +1$ and $(\frac{q}{p}) = -1$. If the negative sign holds, then we find accordingly that $(\frac{p}{q}) = -1$ and $(\frac{q}{p}) = +1$. This completes the proof. □

9.3.1 Summary

In this chapter we have proved the ambiguous class number formula for quadratic number fields, and derived the quadratic reciprocity as a corollary.

9.4 Exercises

9.1. Show that the operation $[\mathfrak{a}]^\sigma = [\mathfrak{a}^\sigma]$ on the ideal class group of a quadratic number field is well defined, i.e., that $[\mathfrak{a}] = [\mathfrak{b}]$ implies $[\mathfrak{a}^\sigma] = [\mathfrak{b}^\sigma]$.

9.2. Show that the ideal class of order 2 in $\mathbb{Q}(\sqrt{10})$ contains the ideals $(2, \sqrt{10})$, $(3, 1 + \sqrt{10})$ and $(5, 1 + \sqrt{10})$. Which of these ideals are ambiguous?

9.3. Let $p \equiv 5 \bmod 8$ be prime. Show that the ideal class $\mathbb{Q}(\sqrt{2p})$ generated by the ambiguous ideal $(2, \sqrt{2p})$ has order 2.

9.4. Let $p \equiv 1 \bmod 8$ be prime. Show that the ambiguous ideal $(2, \sqrt{2p})$ is principal in $k = \mathbb{Q}(\sqrt{2p})$ if and only if the norm of the fundamental unit in k is $+1$.
In this case write $2p = a^2 + b^2$ with $a > b > 0$ and show that the ideal $\mathfrak{a} = (a, b + \sqrt{m})$ generates an ambiguous ideal class of order 2.

9.5. Show that if k is a quadratic number field with class number 2, then $\mathrm{Am}(k) = \mathrm{Cl}(k)$.

9.6. Show that if k is a quadratic number field with odd class number, then $\mathrm{Am}(k) = 1$.

9.7. Show: If A and B are subgroups of an abelian group, then $AB/B \simeq A/A \cap B$.
Hint: Show that $A \cap B$ is the kernel of the natural map $A \longrightarrow AB/B$.

9.8. Show that the inclusion $\iota : H^G/P \longrightarrow A/P$ in (9.2) is injective and that the map $\pi : A/P \longrightarrow \mathrm{Am}_{\mathrm{st}}(k)$ defined by $\pi(\mathfrak{a}P) = [\mathfrak{a}]$ is well defined and surjective. Also show that $\ker \pi = \mathrm{im}\ \iota$.

9.9. (O. Taussky) Solve the Pythagorean equation $x^2 + y^2 = z^2$ using Hilbert's Theorem 90. Hint: $\alpha = \frac{x+yi}{z} \in \mathbb{Q}(i)$ satisfies the equation $N\alpha = 1$. Write $\alpha = \frac{m+ni}{m-ni}$ and rationalize the denominator.
Generalize this exercise to all equations of the form $x^2 - my^2 = z^2$ for squarefree values $m \in \mathbb{Z} \setminus \{0, 1\}$.

9.10. Show that there is an exact sequence

$$1 \longrightarrow P \longrightarrow H^G \longrightarrow E[N]/E^{1-\sigma} \longrightarrow 1,$$

where H denotes the group of nonzero principal ideals.

9.11. Let $m = a^2 + b^2$ be a sum of two squares. Then the ideals $(a, b + \sqrt{m})$ do not necessarily lie in the same ideal class for each choice of a and b. Verify this for $m = 10 = 1^2 + 3^2 = 3^2 + 1^2$.
For the distribution of these ideals over the ideal classes see [82] and [9].

9.12. Let p be a ramified prime in $k = \mathbb{Q}(\sqrt{m})$, where $m \neq \pm p$, and assume that the prime ideal $\mathfrak{p}$ above p is principal, say $\mathfrak{p} = (\pi)$. Show that $\varepsilon = \frac{1}{p}\pi^2$ is a unit in $\mathcal{O}_k$, and that neither ε nor $-\varepsilon$ is a square. Generalize this to products of ramified prime ideals. Use this to compute the fundamental unit of $\mathbb{Q}(\sqrt{30})$.

9.13. Let $p \equiv 1 \bmod 4$ be a prime number. Show that $\left(\frac{q}{p}\right) = +1$ implies $\left(\frac{p}{q}\right) = +1$.
Hint: Use $k = \mathbb{Q}(\sqrt{q^*})$ for $q^* = (\frac{-1}{q})q$ instead of $\mathbb{Q}(\sqrt{q})$.

9.14. Show that the solvability of the Pell equation implies that the norm of the fundamental unit ε_p of $\mathbb{Q}(\sqrt{p})$ for primes p is equal to $N\varepsilon_p = -(\frac{-1}{p})$. Show also that $N\varepsilon_{pq} = -1$ if $p \equiv q \equiv 1 \bmod 4$ are primes with $(\frac{p}{q}) = -1$.

9.15. Let $\pm 4p^h = x^2 - qy^2$ for prime numbers $p \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$. Show that x and y are both even, and that the plus sign must hold.

9.16. Let $k = \mathbb{Q}(\sqrt{m})$ be a quadratic number field with fundamental unit ε_m. Show: If $N\varepsilon_m = +1$, then there is an ambiguous principal ideal $\mathfrak{a} = (\alpha)$ with $\mathfrak{a} \neq (1), (\sqrt{m})$.
Hint: By Hilbert's Theorem 90 we have $\varepsilon = \alpha'/\alpha$.

9.17. Show that the norm of the fundamental unit ε of $\mathbb{Q}(\sqrt{p})$ is negative if $p \equiv 1 \bmod 4$ is prime.
Hint: Use the preceding exercise.

9.18. The idea behind Kummer's ideal numbers was the construction of ring homomorphisms $\mathcal{O}_k \longrightarrow \mathbb{F}_q$ of the ring of integers of number fields into finite fields. Restrict these homomorphisms to the multiplicative group, that is, consider the group homomorphism $\psi : \mathcal{O}_k^\times \longrightarrow \mathbb{F}_q^\times$. Find examples of real quadratic number fields and primes q for which this homomorphism is trivial, or where it is surjective.

9.19. Let p be a prime number such that $(\frac{10}{p}) = +1$. Then there exist two possibilities:

1. $(\frac{2}{p}) = (\frac{5}{p}) = +1$; in this case $p = x^2 - 10y^2$.
2. $(\frac{2}{p}) = (\frac{5}{p}) = -1$; in this case $\pm 2p = X^2 + 10y^2$ and, using $X = 2x$, $\pm p = 2x^2 - 5y^2$.

Show that this implies that each element $x + y\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ can be written uniquely as a product of a unit and irreducible elements of the form $a + b\sqrt{10}$ or $c\sqrt{2} + d\sqrt{5}$.

9.20. Let $q \equiv 3 \bmod 8$ be a prime number. Show that the class number of $\mathbb{Q}(\sqrt{2q})$ is odd and deduce that the equation $2x^2 - qy^2 = -1$ is solvable. Deduce that $(\frac{2}{q}) = -1$.