CHAPTER 5

What is Class Field Theory?

In the introduction to *Number Theory 1*, we presented some of Fermat's results, such as "Every prime number congruent to 1 modulo 4 can be expressed in the form x^2+y^2, where x and y are integers" (Proposition 0.2). Such propositions are a prelude to class field theory. Class field theory is one of the summits of number theory, whose trail begins with Fermat's propositions mentioned above and Gauss's quadratic reciprocity law (see *Number Theory 1*, §2.2).

We give a full-scale account of class field theory in Chapter 8. In this chapter we give several examples which do not require much preparation and explain what class field theory is and how it works.

In §5.1 we present examples that illustrate phenomena where class field theory operates in the background. Please sit back and enjoy such mysterious phenomena! In §5.2 we explain the portions of class field theory concerning quadratic fields and cyclotomic fields. We give a proof of quadratic reciprocity law from the point of view of class field theory. The whole picture of class field theory is given in §5.3.

Some properties of algebraic number fields are part of the general theory of rings and fields, while others are specific to algebraic number fields. For example, the unique decomposition property into prime ideals of the ring of integers of an algebraic number field is a property that holds for any general Dedekind domain, while the quadratic reciprocity law for the ring of integers has no analogy in the general theory. Class field theory and the ζ functions, which are discussed in Chapter 7, apply only to algebraic number fields, but not to general fields. There lies the essence as well as the elegance of number theory.

5.1. Examples of class field theoretic phenomena

(a) Review. As we showed in the introduction (Chapter 0) to *Number Theory 1*, Fermat discovered the following phenomena:

For a prime number p different from 2, we have

$$\begin{aligned} p = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z} &\iff p \equiv 1 \mod 4, \\ p = x^2 + 2y^2 \text{ for some } x, y \in \mathbb{Z} &\iff p \equiv 1, 3 \mod 8, \\ p = x^2 - 2y^2 \text{ for some } x, y \in \mathbb{Z} &\iff p \equiv 1, 7 \mod 8. \end{aligned}$$

For a prime number p different from 3, we have

$$p = x^2 + 3y^2 \text{ for some } x, y \in \mathbb{Z} \iff p \equiv 1 \mod 3.$$

As we stated in §4.1 in *Number Theory 1*, these phenomena may be explained by "the way a prime number p *splits* (*decomposes* or *factors*) into a product of prime elements in the ring of integers of each of the quadratic fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ depends on p mod 4, p mod 8, p mod 8, and p mod 3, respectively," such as

$$\begin{aligned} 5 &= 2^2 + 1^2 = \big(2 + \sqrt{-1}\big)\big(2 - \sqrt{-1}\big), \\ 11 &= 3^2 + 2 \times 1^2 = \big(3 + \sqrt{-2}\big)\big(3 - \sqrt{-2}\big). \end{aligned}$$

From what we proved in §4.1, we obtain Table 5.1.

TABLE 5.1. Decomposition of a prime number p in $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$

	Decomposition type		
Field	$p = \alpha\beta$, α, β : prime, $(\alpha) \neq (\beta)$	p : prime	$p = \text{unit} \times \alpha^2$ α : prime
$\mathbb{Q}(\sqrt{-1})$	$p \equiv 1 \bmod 4$	$p \equiv 3 \bmod 4$	$p = 2$
$\mathbb{Q}(\sqrt{-2})$	$p \equiv 1, 3 \bmod 8$	$p \equiv 5, 7 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{2})$	$p \equiv 1, 7 \bmod 8$	$p \equiv 3, 5 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{-3})$	$p \equiv 1 \bmod 3$	$p \equiv 2 \bmod 3$	$p = 3$

The phenomena appearing in Table 5.1 are a part of class field theory as we see in this section. In this table mod 4, mod 8, and mod 3 appear. In class field theory there are a variety of fields that have different decomposition laws; for example, there are fields in which the decomposition of a prime number p is determined by p mod 7 or p mod 20 (see Tables 5.2–5.6). The quadratic reciprocity law (*Number Theory 1*, §2.1) is also a part of class field theory. In this section we see some examples of such class field theoretic phenomena.

(b) Decomposition of prime numbers in quadratic fields. How do prime numbers decompose in a general quadratic field? The quadratic fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$, which appeared in (a), have class number one, and thus their rings of integers are unique factorization domains. This means that a prime number is factored uniquely as a product of prime elements in each ring.

On the other hand, the fields $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-6})$ have class number two, and their rings of integers, $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-6}]$, do not necessarily allow decomposition of a prime number as a product of prime elements. As we stated in §4.2 in *Number Theory 1*, the ring of integers of an algebraic number field admit, in general, only a unique decomposition into prime ideals, not into prime elements. Table 5.2 shows, for a prime number p, how the ideal (p) decomposes into prime ideals in the ring of integers of various quadratic fields.

TABLE 5.2. Decomposition of a prime number in various quadratic fields

Field	Decomposition type		
	$(p) = \mathfrak{pq}$ $\mathfrak{p}, \mathfrak{q}$: prime ideals $\mathfrak{p} \neq \mathfrak{q}$	(p) : prime ideal	$(p) = \mathfrak{p}^2$ $\mathfrak{p}$: prime ideal
$\mathbb{Q}(\sqrt{3})$	$p \equiv 1, 11 \bmod 12$	$p \equiv 5, 7 \bmod 12$	$p = 2, 3$
$\mathbb{Q}(\sqrt{5})$	$p \equiv 1, 4 \bmod 5$	$p \equiv 2, 3 \bmod 5$	$p = 5$
$\mathbb{Q}(\sqrt{-5})$	$p \equiv 1, 3, 7, 9 \bmod 20$	$p \equiv 11, 13, 17, 19 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{6})$	$p \equiv 1, 5, 13, 19 \bmod 24$	$p \equiv 7, 11, 13, 17 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-6})$	$p \equiv 1, 5, 7, 11 \bmod 24$	$p \equiv 13, 17, 19, 23 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-15})$	$p \equiv 1, 2, 4, 8 \bmod 15$	$p \equiv 7, 11, 13, 14 \bmod 15$	$p = 3, 5$

Let us consider the field $\mathbb{Q}(\sqrt{-5})$ more closely. For example, 41, 3, 7 and 29 are prime numbers congruent to 1, 3, 7 and 9 mod 20, respectively. In $\mathbb{Z}[\sqrt{-5}]$ we have prime ideal decompositions

$$(41) = \big(6 + \sqrt{-5}\big)\big(6 - \sqrt{-5}\big), \quad (3) = \big(3, 1 + \sqrt{-5}\big)\big(3, 1 - \sqrt{-5}\big),$$
$$(7) = \big(7, 4 + \sqrt{-5}\big)\big(7, 4 - \sqrt{-5}\big), \quad (29) = \big(3 + 2\sqrt{-5}\big)\big(3 - 2\sqrt{-5}\big).$$

Furthermore, in the same ring, we have prime ideal decompositions

$$(2) = \big(2, 1 + \sqrt{-5}\big)^2, \quad (5) = \big(\sqrt{-5}\big)^2.$$

Next, we consider $\mathbb{Q}(\sqrt{-6})$. The numbers 73, 5, 7 and 11 are prime numbers which are congruent to 1, 5, 7 and 11 mod 24, respectively. In $\mathbb{Z}(\sqrt{-6})$ we have prime ideal decompositions

$$(73) = \big(7+2\sqrt{-6}\big)\big(7-2\sqrt{-6}\big), \quad (5) = \big(5, 2+\sqrt{-6}\big)\big(5, 2-\sqrt{-6}\big),$$
$$(7) = \big(1+\sqrt{-6}\big)\big(1-\sqrt{-6}\big), \quad (11) = \big(11, 4+\sqrt{-6}\big)\big(11, 4-\sqrt{-6}\big).$$

Furthermore, in $\mathbb{Z}[\sqrt{-6}]$, we have prime ideal decompositions

$$(2) = \big(2, \sqrt{-6}\big)^2, \quad (3) = \big(3, \sqrt{-6}\big)^2.$$

The phenomena in Table 5.2 is a premonition of Theorem 5.15.

The decompositions of prime numbers in quadratic fields are related to the following fact. Consider the quadratic field $\mathbb{Q}(\sqrt{-5})$. Let p be a prime number different from 2 and 5. Then the ideal (p) decomposes as a product of two distinct prime ideals if and only if there is an integer a such that $a^2 \equiv -5 \bmod p$, that is, p is a prime factor of an integer of the form a^2+5, $a \in \mathbb{Z}$ (by virtue of Lemma 5.19 later in this chapter). If there is an integer a such that $a^2 \equiv -5 \bmod p$, then

$$(p) = \big(p, a+\sqrt{-5}\big)\big(p, a-\sqrt{-5}\big)$$

is a prime ideal decomposition of (p) in $\mathbb{Z}[\sqrt{-5}]$. For example, $1^2 \equiv -5 \bmod 3$ implies the prime ideal decomposition

$$(3) = \big(3, 1+\sqrt{-5}\big)\big(3, 1-\sqrt{-5}\big).$$

The question whether or not a prime number divides the number expressed by a polynomial (such as a^2+5) (see subsection (f)) and the question whether or not a given prime number is of the form x^2+dy^2 (see subsection (g)) have no bearing on an algebraic number field at first sight, but as we saw, they are related to the way prime numbers are factored in algebraic number fields. Tables 5.1 and 5.2 show the mysterious laws (class field theory) in this regard.

QUESTION 1. Prove the following equalities for ideals:

$$(3) = \big(3, 1+\sqrt{-5}\big)\big(3, 1-\sqrt{-5}\big) \text{ in } \mathbb{Z}[\sqrt{-5}],$$
$$(5) = \big(5, 2+\sqrt{-6}\big)\big(5, 2-\sqrt{-6}\big) \text{ in } \mathbb{Z}[\sqrt{-6}].$$

(Hint: If ideals I and J are generated by $\alpha_i (1 \le i \le m)$ and $\beta_j (1 \le j \le n)$, respectively, then the ideal IJ is generated by $\alpha_i\beta_j (1 \le i \le m, 1 \le j \le n)$. Use this fact.)

QUESTION 2. Show that the ideals $\big(3, 1+\sqrt{-5}\big)$ in $\mathbb{Z}[\sqrt{-5}]$ and $\big(5, 2+\sqrt{-6}\big)$ in $\mathbb{Z}[\sqrt{-6}]$ are not principal ideals by using the fact that each of the equations $3 = x^2+5y^2$ and $5 = x^2+6y^2$ admits no integer solutions.

(c) Ramification and decomposition. Class field theory studies not only quadratic fields, that is, quadratic extensions of the rational number field $\mathbb{Q}$, but also various extensions of algebraic number fields. We make some preparations here.

Let K be an algebraic number field and L a finite extension of K. This generalizes our previous case where $K = \mathbb{Q}$ and L is its quadratic extension. We consider an important question how a nonzero prime ideal of the ring of integers $\mathcal{O}_K$ (sometimes called a prime ideal of K for simplicity) decomposes in L. For this purpose, we introduce the terms: *ramified*, *unramified* and *totally decomposed* prime ideals of $\mathcal{O}_K$ in L.

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let $\mathcal{O}_L\mathfrak{p}$ (or $\mathfrak{p}\mathcal{O}_L$) be the ideal of $\mathcal{O}_L$ generated by $\mathfrak{p}$. Then we may express it in the form

$$\mathcal{O}_L\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}, \tag{5.1}$$

where $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ are distinct nonzero prime ideals of $\mathcal{O}_L$ and $e_i \geq 1$ for $1 \leq i \leq g$.

DEFINITION 5.1. If $e_1 = \cdots = e_g = 1$, we say that $\mathfrak{p}$ is *unramified* in L. Otherwise, that is, if $e_i \geq 2$ for some i, we say that $\mathfrak{p}$ is *ramified* in L.

For example, for $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-1})$, the only nonzero prime ideal of $\mathbb{Z}$ that is ramified in L is $2\mathbb{Z}$.

A quick proof of the fact $\sqrt{5} \notin \mathbb{Q}(\sqrt[3]{2}, \sqrt[6]{3}, \sqrt[4]{7})$ may illustrate how significant the notion of ramification is. Observe that $5\mathbb{Z}$ is ramified in a field L that contains $\sqrt{5}$. This is because the decomposition $\sqrt{5}\mathcal{O}_L = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_g^{n_g}$ in L would imply $5\mathcal{O}_L = \mathfrak{q}_1^{2n_1} \cdots \mathfrak{q}_g^{2n_g}$. But then this contradicts the fact that $5\mathbb{Z}$ is unramified in $\mathbb{Q}(\sqrt[3]{2}, \sqrt[6]{3}, \sqrt[4]{7})$, which follows from Proposition 5.2 below.

PROPOSITION 5.2. *Let K be an algebraic number field, and let $a_1, \ldots, a_n$ be elements of $\mathcal{O}_K$. For natural numbers $n_1, \ldots, n_m \geq 1$, let α_i be an n_ith root of a_i, and let $L = K(\alpha_1, \ldots, \alpha_m)$. If $\mathfrak{p}$ is a prime ideal of K such that $a_i \notin \mathfrak{p}$, $n_i \notin \mathfrak{p}$ $(1 \leq i \leq m)$, then $\mathfrak{p}$ is unramified in L.*

(For the example above, we have $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[6]{3}, \sqrt[4]{7})$ and $2, 3, 7, 4, 6 \notin \mathfrak{p} = 5\mathbb{Z}$.) For the proof of Proposition 5.2, see Example 6.40 in Chapter 6.

Next, we introduce the notion of totally decomposed prime ideals. In general, in the prime decomposition (5.1), it is known that

$$\sum_{i=1}^{g} e_i \leq [L : K], \tag{5.2}$$

where $[L : K]$ denotes the degree of the field extension. Hence, in particular, $g \leq [L : K]$. (Later in §6.3 we will prove a more precise formula in Proposition 6.22.)

DEFINITION 5.3. If $\mathcal{O}_L\mathfrak{p}$ decomposes into $[L : K]$ distinct nonzero prime ideals, or equivalently, if $g = [L : K]$, we say that $\mathfrak{p}$ is *totally decomposed* in L, or $\mathfrak{p}$ *splits completely* in L.

If $\mathfrak{p}$ is totally decomposed in L, then $\mathfrak{p}$ is unramified in L.

In the case where $K = \mathbb{Q}$, we say that a prime number p is ramified, unramified, or totally decomposed if the prime ideal $p\mathbb{Z}$ is ramified, unramified, or totally decomposed in L. Finding which prime ideals are totally decomposed is no less important than finding which prime ideals are ramified.

From Tables 5.1 and 5.2, we obtain Table 5.3. This table shows which prime numbers are totally decomposed or are ramified in quadratic fields.

Here is a list of what we can observe in Table 5.3.

(i) In any quadratic field, only a finite number of primes are ramified.

Generally, for any finite extension L of an algebraic number field K, there are only a finite number of nonzero prime ideals that are ramified in L. We will prove this fact in §6.3 (Corollary 6.33).

(ii) In $\mathbb{Q}(\sqrt{-1})$, the nature of decomposition is determined by $p \bmod 4 = 2^2$. Also in $\mathbb{Q}(\sqrt{-15})$, the nature of decomposition is determined by $p \bmod 15 = 3 \times 5$. For each quadratic field, the nature of decomposition is determined by $p \bmod N$, where N is a natural number that is a product of all the ramified prime numbers with some multiplicity.

As a matter of fact, this holds for every quadratic field (see §5.2, Theorem 5.15). Later, we will give its generalization in class field theory in Theorem 5.21(4) in §5.3.

(iii) The set $\{1, 2, 4, 8 \bmod 15\}$, appearing in the line of $\mathbb{Q}(\sqrt{-15})$, forms a subgroup of index 2 in the multiplicative group $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14 \bmod 15\}$.

TABLE 5.3

Field	totally decomposed prime numbers p	ramified prime numbers p
$\mathbb{Q}(\sqrt{-1})$	$p \equiv 1 \bmod 4$	$p = 2$
$\mathbb{Q}(\sqrt{2})$	$p \equiv 1, 7 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{-2})$	$p \equiv 1, 3 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{3})$	$p \equiv 1, 11 \bmod 12$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-3})$	$p \equiv 1 \bmod 3$	$p = 3$
$\mathbb{Q}(\sqrt{5})$	$p \equiv 1, 4 \bmod 5$	$p = 5$
$\mathbb{Q}(\sqrt{-5})$	$p \equiv 1, 3, 7, 9 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{6})$	$p \equiv 1, 5, 13, 19 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-6})$	$p \equiv 1, 5, 7, 11 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-15})$	$p \equiv 1, 2, 4, 8 \bmod 15$	$p = 3, 5$

By examining Table 5.3 carefully, we observe that the set of numbers mod N that describes the condition for which a prime number p is totally decomposed forms a subgroup of index 2 in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$. This assertion also holds for every quadratic field (see Theorem 5.15). If we extend the scope of our study beyond the quadratic fields, we realize that subgroups of index other than 2 also becomes significant, as we will state in Theorem 5.7. Indeed, for any N and $d \geq 1$, any subgroup of index d of $(\mathbb{Z}/N\mathbb{Z})^\times$ describes a condition for which primes are totally decomposed in a certain extension of $\mathbb{Q}$ of degree d. In the next subsection (d) we give an example.

(d) Decomposition of prime numbers in fields other than quadratic fields. So far, we have seen how prime numbers decompose in quadratic fields. Here, we consider the decomposition of prime numbers in fields other than quadratic fields. What we illustrate here will be formulated as Theorem 5.7 in §5.2.

Let us consider the quartic extension $\mathbb{Q}(\zeta_5)$ of $\mathbb{Q}$, where ζ_5 is a primitive fifth root of unity. Table 5.4 illustrates some known "class field theoretic phenomena" occurring in this field.

TABLE 5.4. Decomposition of p in $\mathbb{Q}(\zeta_5)$

p : prime number	Decomposition type
$p \equiv 1 \bmod 5$	(p) = product of 4 distinct prime ideals e.g., $(11) = (2+\zeta_5)(2+\zeta_5^2)(2+\zeta_5^3)(2+\zeta_5^4)$, $(31) = (2-\zeta_5)(2-\zeta_5^2)(2-\zeta_5^3)(2-\zeta_5^4)$
$p \equiv 4 \bmod 5$	(p) = product of 2 distinct prime ideals e.g., $(19) = \big(8+3\sqrt{5}\big)\big(8-3\sqrt{5}\big)$
$p \equiv 2, 3 \bmod 5$	(p) is a prime ideal
$p = 5$	$(5) = (1-\zeta_5)^4$, $(1-\zeta_5)$ is a prime ideal

From Table 5.4 we see that for a prime number p

$$p \equiv 1 \mod 5 \iff p \text{ is totally decomposed in } \mathbb{Q}(\zeta_5).$$

This shows that the set of prime numbers that are totally decomposed in $\mathbb{Q}(\zeta_5)$ is given by the subgroup $\{1 \bmod 5\}$ of index 4 of the group $(\mathbb{Z}/5\mathbb{Z})^\times$.

As we have already seen, the decomposition of a prime number p in the quadratic field $\mathbb{Q}(\sqrt{5})$ is determined by $p \bmod 5$. In fact, $\mathbb{Q}(\sqrt{5})$ is contained in $\mathbb{Q}(\zeta_5)$, since $\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$ is a square root of 5, as we will see from Proposition 5.18 in §5.2.

In $\mathbb{Q}(\zeta_5)$ and $\mathbb{Q}(\sqrt{5})$, $p \bmod 5$ determines the decomposition of the prime number p. Table 5.5 is a list of fields in which the decomposition of a prime number p is determined by $p \bmod 7$, and Theorem 5.10 shows that there is no other such field. Note that the group $(\mathbb{Z}/7\mathbb{Z})^\times$ has four subgroups

$$\{1 \bmod 7\},\ \{1, 6 \bmod 7\},\ \{1, 2, 4 \bmod 7\},\ \text{and } (\mathbb{Z}/7\mathbb{Z})^\times.$$

Note that $\mathbb{Q}(\sqrt{-7})$ is contained in $\mathbb{Q}(\zeta_7)$, because $\zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 + \zeta_7^6$ is a square root of -7. In §5.2 (d), we will discuss the inclusion relationship of quadratic fields and $\mathbb{Q}(\zeta_N)$, $N \geq 1$, such as $(\mathbb{Q}\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ and $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$.

Finally, Table 5.6 lists all the fields in which the decomposition of a prime number is determined by $p \bmod 20$.

(e) Extension of algebraic number fields. So far, we have only dealt with algebraic extensions $K \subset L$ with $K = \mathbb{Q}$. We now

TABLE 5.5. All fields in which the decomposition of a prime number is determined by p mod 7

Field L	$[L:\mathbb{Q}]$	totally decomposed prime numbers p	ramified prime numbers p
$\mathbb{Q}(\zeta_7)$	6	$p \equiv 1 \bmod 7$	$p = 7$
$\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$	3	$p \equiv 1, 6 \bmod 7$	$p = 7$
$\mathbb{Q}(\sqrt{-7})$	2	$p \equiv 1, 2, 4 \bmod 7$	$p = 7$
$\mathbb{Q}$	1	all p	none

TABLE 5.6. All fields in which the decomposition of a prime number is determined by p mod 20

Field L	$[L:\mathbb{Q}]$	totally decomposed prime numbers p	ramified prime numbers p
$\mathbb{Q}(\zeta_{20})$	8	$p \equiv 1 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\zeta_5)$	4	$p \equiv 1 \bmod 5$	$p = 5$
$\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$	4	$p \equiv 1, 19 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{5}, \sqrt{-1})$	4	$p \equiv 1, 9 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{5})$	2	$p \equiv 1, 4 \bmod 5$	$p = 5$
$\mathbb{Q}(\sqrt{-5})$	2	$p \equiv 1, 3, 7, 9 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{-1})$	2	$p \equiv 1 \bmod 4$	$p = 2$
$\mathbb{Q}$	1	all p	none

take up an example where

$$K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}), \quad L = \mathbb{Q}(\zeta_3, \sqrt[3]{2}).$$

Table 5.7 shows class field theoretic phenomena for this extension. We see that phenomena occurring between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$ also occur between $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Note that instead of mod 5 for $\mathbb{Q}(\zeta_5)$ there appears mod $6\mathbb{Z}[\zeta_3]$. Also note that $(1 - 6\zeta_3)$ appearing in this list satisfies $43 = (1 - 6\,\zeta_3)(1 - 6\,\zeta_3^2)$, and is a prime factor of 43 in $\mathbb{Q}(\zeta_3)$.

TABLE 5.7. Decomposition of prime ideals $\mathfrak{p}$ of $\mathbb{Q}(\zeta_3)$ in $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$

$\mathfrak{p}$: prime ideal	Decomposition type
$\mathfrak{p} = (\alpha)$, $\alpha \equiv 1 \bmod 6\mathbb{Z}[\zeta_3]$	$\mathcal{O}_L\mathfrak{p} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ 3 distinct prime ideals in $\mathcal{O}_L$ e.g., $(1-6\zeta_3) = \prod_{a=1}^{3}\left(1+2\zeta_3+\sqrt[3]{4}\zeta_3^a\right)$
$\mathfrak{p} = (1-\zeta_3)$, (2)	$\mathcal{O}_L\mathfrak{p} = \mathfrak{q}^3$, $\mathfrak{q}$: a prime ideal of $\mathcal{O}_L$
other $\mathfrak{p}$	$\mathcal{O}_L\mathfrak{p}$ is a prime ideal of $\mathcal{O}_L$

Having gone over all the examples so far, we might expect that, for any extension L of an algebraic number field K, the phenomena as in the case where $K = \mathbb{Q}(\zeta_3)$ and $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ might occur, and that in the particular case where $K = \mathbb{Q}$, the decomposition of a prime number p in L can be determined by p mod N with a certain natural number N. Unfortunately, this is not really the case. For example, it is known that no matter what N we may use, which prime number p is totally decomposed in $\mathbb{Q}(\sqrt[3]{2})$ or $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ cannot be determined by p mod N (see §5.2, Theorem 5.10).

For example, take the two-step extension

$$K = \mathbb{Q} \subset \mathbb{Q}(\zeta_3) \subset L = \mathbb{Q}(\zeta_3, \sqrt[3]{2}).$$

For each step, the decomposition law for a prime number or a prime ideal is given in Tables 5.1 and 5.7, respectively. However, it does not mean that we can describe the law of decomposition for a prime number p in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ in terms of p mod N for some N. For instance, prime numbers 31 and 43 are totally decomposed as

$$(31) = (1+6\zeta_3)(1+\zeta_3^2), \quad (43) = (1-6\zeta_3)(1-\zeta_3^2)$$

in the ring of integers $\mathbb{Z}[\zeta_3]$ of $\mathbb{Q}(\zeta_3)$. Each of these factors is generated by elements congruent to 1 mod $6\mathbb{Z}[\zeta_3]$. Hence they are totally decomposed in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$, as we can see from Table 5.7. This means that 31 and 43 are totally decomposed in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. However, it is known that, no matter how we choose N, we cannot determine in terms of p mod N whether or not a prime number p is written in the

form

$$(p) = \mathfrak{p}\mathfrak{q}, \quad \mathfrak{p},\ \mathfrak{q} \text{ are distinct prime ideals in } \mathbb{Z}[\zeta_3]$$
$$\mathfrak{p} = (\alpha), \mathfrak{q} = (\beta), \alpha \equiv \beta \equiv 1 \bmod 6\mathbb{Z}[\zeta_3],$$

as in the case of $p = 31$, or 43.

Then, for which extensions L of an algebraic number field K do we have class field theoretic phenomena, as illustrated in Tables 5.1–5.7? The answer is: we do if and only if L is an abelian extension of K. An *abelian extension* is a Galois extension whose Galois group is abelian. For Galois theory, we refer the reader to Appendix B.1, B.2, or any standard book such as *Galois Theory* by E. Artin.

A quadratic field is an abelian extension of $\mathbb{Q}$ whose Galois group is the abelian group $\mathbb{Z}/2\mathbb{Z}$. We will show in §5.2 that other fields such as $\mathbb{Q}(\zeta_5)$ in Tables 5.1–5.6 are also abelian extensions. While $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is an abelian extension of $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ are not abelian extensions of $\mathbb{Q}$.

Class field theory is a theory for abelian extensions. The substance of class field theory is that in abelian extensions of algebraic number fields, phenomena of the type we have illustrated in Tables 5.1–5.7 occur, and that, conversely, if those phenomena occur in extensions of algebraic number fields, then they are abelian extensions, and finally that the abelian extensions of algebraic number fields are determined by those phenomena. For example, an algebraic number field in which the set of totally decomposed prime numbers coincides with the set of all prime numbers p satisfying $p \equiv 1 \bmod 4$ is nothing but $\mathbb{Q}(\sqrt{-1})$.

For nonabelian extensions of algebraic number fields, we are experiencing a rapid development of a theory, generalizing class field theory. A major breakthrough on the relationship between nonabelian extensions and automorphic forms (see *Number Theory 3*) achieved by Andrew Wiles led him to a proof of Fermat's Last Theorem and is a starting point of the recent development. Details of the proof by John Wiles will be discussed in *Fermat's Last Theorem* in the Iwanami Series in Modern Mathematics.

(f) Prime factors of polynomials. So far, we have seen class field theoretic phenomena about decompositions of prime numbers and prime ideals. In subsections (f) and (g), we look at somewhat different types of class field theoretic phenomena.

Given a polynomial $f(T)$ with integer coefficients, we show a "class field phenomenon" concerning the prime numbers that can be a prime factor of $f(n)$, $n \in \mathbb{Z}$.

For example, let $f(T) = T^2 + 6$. If we let $n = 0, 1, 2, 3, 4, \ldots$, then the values of $f(n)$ become

$$6 = 2 \times 3, \quad 7, \quad 10 = 2 \times 5, \quad 22 = 2 \times 11, \quad 15 = 3 \times 5,$$
$$42 = 2 \times 3 \times 7, \quad 55 = 5 \times 11, \quad 70 = 2 \times 5 \times 7, \quad 87 = 3 \times 29,$$
$$106 = 2 \times 53, \ldots$$

The prime numbers that appear here are 2, 3, and prime numbers congruent to $1, 5, 7 \bmod 24$. The reason is that for prime numbers p other than 2 and 3 we have

$$\begin{aligned} &p \text{ is a prime factor of a number of the form } n^2 + 6 \ (n \in \mathbb{Z}); \\ &\iff x^2 + 6 \equiv 0 \mod p \text{ has an integer solution;} \\ &\iff \left(\frac{-6}{p}\right) = 1 \iff p \equiv 1, 5, 7, 11 \mod 24. \end{aligned}$$

The last equivalence is due to the quadratic reciprocity law and its supplementary laws (see Theorem 2.2(b) in Chapter 2 of *Number Theory 1*).

In this way, given a quadratic polynomial $f(T)$ with integer coefficients, we can obtain a criterion of the following form for a prime number p:

$$\begin{aligned} &p \text{ is a prime factor of a number of the form } f(n) \ (n \in \mathbb{Z}) \\ &\iff p \equiv \cdots \mod N. \end{aligned}$$

What can we say in the case where $f(T)$ is a polynomial of degree greater than or equal to 3? The answer is shown in Table 5.8.

The information in Table 5.8 is closely related to the fact that a prime number p is totally decomposed in $\mathbb{Q}(\zeta_5)$ if and only if $p \equiv 1 \bmod 5$, and p is totally decomposed in $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ if and only if $p \equiv 6 \bmod 7$. Note that ζ_5 is a root of $x^4 + x^3 + x^2 + x + 1$, and $\zeta_7 + \zeta_7^{-1}$ is a root of $x^3 + x^2 - 2x - 1$. We also note that $\mathbb{Q}(\sqrt[3]{2})$ is not an abelian extension of $\mathbb{Q}$. See Example 6.42 for further details.

(g) $p = x^2 + 5y^2$, $p = x^2 + 6y^2$, etc. In relation to the question whether or not we can write a given prime number p in the form $x^2 + 5y^2$ or $x^2 + 6y^2$, we have some class field theoretic phenomena as follows:

TABLE 5.8. Prime factors of polynomials

polynomial $f(T)$	prime numbers p such that $f(x) \equiv 0 \bmod p$ has integer solutions
T^2+6	$p \equiv 1,5,7,11 \bmod 24$, or $p = 2,3$
$T^4+T^3+T^2+T+1$	$p \equiv 1 \bmod 5$, or $p = 5$
T^3+T^2-2T-1	$p \equiv 1,6 \bmod 7$, or $p = 7$
T^3-2	no criterion in the form $p \equiv \cdots \bmod \cdots$

For a prime number p different from 2 and 5,

$$p \text{ is of the form } p = x^2+5y^2, x, y \in \mathbb{Z} \iff p \equiv 1,9 \mod 20.$$

For a prime number p different from 2 and 3,

$$p \text{ is of the form } p = x^2+6y^2, x, y \in \mathbb{Z} \iff p \equiv 1,7 \mod 24.$$

Observe that the condition $p \equiv 1,9 \bmod 20$ in the first claim above is somewhat different from the condition $p \equiv 1,3,7,9 \bmod 20$ for totally decomposed primes p in $\mathbb{Q}(\sqrt{-5})$. Similarly, the condition in the second claim differs from $p \equiv 1,5,7,11 \bmod 24$ for totally decomposed primes p in $\mathbb{Q}(\sqrt{-6})$. (In the earlier discussions on $p = x^2+y^2$ and $p = x^2+2y^2$ and totally decomposed primes p in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$, there was no such discrepancy.) Fermat was aware of this difference (see Exercise 5.3 at the end of this chapter).

Furthermore, the question whether a prime number p can be written in the form x^2+26y^2, $x, y \in \mathbb{Z}$ cannot be decided by the information on $p \bmod N$, no matter what N we may choose. This phenomenon is also related to class field theory, which we will discuss in §5.3(b).

5.2. Cyclotomic fields and quadratic fields

The eighteen-year-old Gauss, as he woke up on the morning of March 30, 1796, discovered that a regular 17-gon can be constructed with ruler and compass (according to his diary). The construction was based on studying the field $\mathbb{Q}(\zeta_{17})$.

In the complex plane the N-th roots of unity appear when the unit circle is divided into N equal parts. Hence $\mathbb{Q}(\zeta_N)$ is called the

N-th *cyclotomic field*. Gauss studied cyclotomic fields as well as their relations to the arithmetic of quadratic fields. In this section we propose the point of view in which cyclotomic fields are placed as a central notion to understand the phenomena which are illustrated in §5.1 (a), (b) and (d), concerning quadratic fields, cyclotomic fields, and their subfields. We state the decomposition law for prime numbers in cyclotomic fields and their subfields (Theorem 5.7 in (b)). We prove it in this section, using a general theory on prime ideals that will be proved in Chapter 6. Based on the same idea, we also prove the quadratic reciprocity law in (f).

(a) The Galois group of a cyclotomic field. The field $\mathbb{Q}(\zeta_N)$ is a Galois extension of $\mathbb{Q}$. This is because all the conjugates of ζ_N are N-th roots of unity, and thus powers of ζ_N, which belong to $\mathbb{Q}(\zeta_N)$ (see Appendix B.2). We can define a group homomorphism

$$s_N : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$$

as follows. For each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, let r be an integer such that $\sigma(\zeta_N) = \zeta_N^r$, and define $s_N(\sigma) = r \bmod N$.

This homomorphism s_N is injective. Indeed, if $s_N(\sigma) = 1 \bmod N$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, then we have $\sigma(\zeta_N) = \zeta_N$. This implies that σ leaves all the elements of $\mathbb{Q}(\zeta_N)$ invariant, and thus $\sigma = 1$. It follows that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is isomorphic to a subgroup of the abelian group $(\mathbb{Z}/N\mathbb{Z})^\times$, and thus it is an abelian group. This shows that $\mathbb{Q}(\zeta_N)$ is an abelian extension of $\mathbb{Q}$.

Although Gauss did not discover Galois theory, he proved a fact that can be stated in the language of Galois theory as follows.

THEOREM 5.4. *The homomorphism s_N gives rise to an isomorphism between groups:*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^\times.$$

The proof will be given in (c).

Galois theory explains why a regular 17-gon can be constructed with compass and ruler as follows. A complex number α is constructible as a point in the complex plane with ruler and compass starting with the points 0 and 1 if and only if there exists a sequence of field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = \mathbb{Q}(\alpha)$$

such that K_i is a quadratic extension of K_{i-1} for each i, $1 \leq i \leq n$. (For the proof of this fact, the reader is referred to a book on commutative field theory or Galois theory.)

For example, the Ancient Greeks knew that a regular 5-gon is constructible; this is because the sequence $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$ satisfies the above condition, and thus ζ_5 is constructible. On the other hand, ζ_7 and 7-gon are not constructible. Indeed, if there is such a sequence of successive quadratic extensions for a complex number α, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K_n : K_0] = 2^n$, but $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ is not a power of 2. As for a regular 17-gon, we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q})$ with $(\mathbb{Z}/17\mathbb{Z})^\times$ by Theorem 5.4. By the fundamental theorem of Galois theory, corresponding to the sequence of subgroups of $(\mathbb{Z}/17\mathbb{Z})^\times$

$$(\mathbb{Z}/17\mathbb{Z})^\times \supset \{\pm 1, \pm 1, \pm 4, \pm 8\} \supset \{\pm 1, \pm 4\} \supset \{\pm 1\} \supset \{1\},$$

there is a sequence of field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 = \mathbb{Q}(\zeta_{17}).$$

Since the index of any two adjacent subgroups is 2, each K_i is a quadratic extension of K_{i-1}. Hence ζ_{17} is constructible, and so is a regular 17-gon.

QUESTION 3. Is angle 40° constructible with ruler and compass?

(b) Decomposition of a prime number in a subfield of the cyclotomic field. Galois theory gives a one-to-one correspondence

$$\text{subfields of } \mathbb{Q}(\zeta_N) \overset{1:1}{\longleftrightarrow} \text{subgroups of } \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}).$$

Using Theorem 5.4, we obtain a one-to-one correspondence

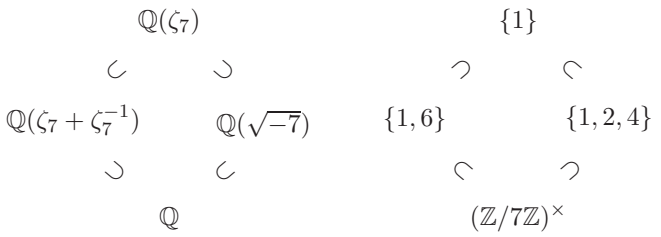
$$\text{subfields of } \mathbb{Q}(\zeta_N) \overset{1:1}{\longleftrightarrow} \text{subgroups of } (\mathbb{Z}/N\mathbb{Z})^\times.$$

EXAMPLE 5.5. For $N = 5$, the correspondence between subfields and subgroups is:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_5) & \longleftrightarrow & \{1\} \\ \cup & & \cap \\ \mathbb{Q}(\sqrt{5}) & \longleftrightarrow & \{1, 4\} \\ \cup & & \cap \\ \mathbb{Q} & \longleftrightarrow & (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}. \end{array}$$

Indeed, the only subgroups of $(\mathbb{Z}/5\mathbb{Z})^\times$ are the ones listed on the right side, and we know that $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}$ are subfields of $\mathbb{Q}(\zeta_5)$. Thus the correspondence must be as above.

EXAMPLE 5.6. Consider the case $N = 7$. If a subfield L of $\mathbb{Q}(\zeta_7)$ corresponds to a subgroup H of $(\mathbb{Z}/7\mathbb{Z})^\times$ through Galois theory, then the degree of the extension $[L : \mathbb{Q}]$ equals the index $[(\mathbb{Z}/7\mathbb{Z})^\times : H]$. Thus, considering the relation between the degree and the index, the correspondence must be as follows:



(Corresponding objects are placed at the corresponding positions.)

Comparing the diagrams in these examples with Tables 5.2–5.5, we realize that there are some matching coincidences. For example, while in Example 5.5 the group corresponding to $\mathbb{Q}(\sqrt{5})$ is $\{1, 4\} \subset (\mathbb{Z}/5\mathbb{Z})^\times$, the set of all totally decomposed prime numbers in $\mathbb{Q}(\sqrt{5})$ is $\{\, p \mid p \equiv 1, 4 \bmod 5 \,\}$ in Table 5.3.

This fact is generalized as follows.

THEOREM 5.7. *Let N be a natural number. Suppose that a subfield L of $\mathbb{Q}(\zeta_N)$ corresponds to a subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$ in the sense of Galois theory. Then, for any prime number p not dividing N, we have the following.*

1. *p is unramified in L.*
2. *p is totally decomposed in $L \iff p \bmod N \in H$.*
3. *More precisely, if f is the smallest natural number such that $p^f \bmod N \in H$, then, in $\mathcal{O}_L$, the ideal (p) is a product of $[L : \mathbb{Q}]/f$ distinct prime ideals.*

We will give a proof in (c).

COROLLARY 5.8. *Let N be a natural number and p a prime number not dividing N. Then, p is unramified in $\mathbb{Q}(\zeta_N)$, and*

$$p \text{ is totally decomposed in } \mathbb{Q}(\zeta_N) \iff p \equiv 1 \bmod N.$$

COROLLARY 5.9. *Let N and p be as in Corollary* 5.8. *Then, p is unramified in $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$, and*

$$p \text{ is totally decomposed in } \mathbb{Q}(\zeta_N) \iff p \equiv \pm 1 \bmod N.$$

(Note that we have $\mathbb{Q}(\zeta_N + \zeta_N^{-1}) = \mathbb{Q}(\cos(2\pi/N))$. This follows from the formula $\cos(2\pi/N) = (e^{2\pi i/N} + e^{-2\pi i/N})/2$.)

Corollaries 5.8 and 5.9 are obtained by letting $L = \mathbb{Q}(\zeta_N)$ and $L = \mathbb{Q}(\zeta_N + \zeta_N^{-1})$, respectively, in Theorem 5.7. We can see that the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponding to $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$ is equal to $\{\pm 1 \bmod N\} \subset (\mathbb{Z}/N\mathbb{Z})^\times$ as follows. Since the element $\zeta_N \mapsto \zeta_N^{-1}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ leaves $\zeta_N + \zeta_N^{-1}$ invariant, the subfield corresponding to $\{\pm 1 \bmod N\}$ contains $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$. On the other hand, since ζ_N is a root of the quadratic equation $x^2 - (\zeta_N + \zeta_N^{-1})x + 1 = 0$ over $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$, we have $[\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_N + \zeta_N^{-1})] \leq 2$. Thus, the only subfields of $\mathbb{Q}(\zeta_N)$ containing $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$ are $\mathbb{Q}(\zeta_N)$ and $\mathbb{Q}(\zeta_N + \zeta_N^{-1})$.

Since $\mathbb{Q}(\zeta_N)$ is an abelian extension, every subfield of $\mathbb{Q}(\zeta_N)$ is an abelian extension of $\mathbb{Q}$. Part (1) of the following theorem asserts the converse of this fact. Theorem 5.10 will be proved in §8.1(g).

THEOREM 5.10. *Let L be an algebraic number field.*

(1) (Kronecker's theorem) *The following are equivalent.*
   (i) *L is an abelian extension of $\mathbb{Q}$.*
   (ii) *There exists a natural number N such that $L \subset \mathbb{Q}(\zeta_N)$.*

(2) *Let N be a natural number. The following are equivalent.*
   (i) *$L \subset \mathbb{Q}(\zeta_N)$.*
   (ii) *Whether or not a prime number p is totally decomposed in L can be determined by $p \bmod N$.*

(3) *Let L be an abelian extension of L, and N the smallest natural number such that $L \subset \mathbb{Q}(\zeta_N)$. Then, for any prime number p*

$$p \text{ is ramified in } L \iff p \text{ divides } N.$$

(c) Proofs of Theorems 5.4 and 5.7. We prove Theorems 5.4 and 5.7 using some facts which will be proved in §6.3. Since we use the notion of Frobenius substitution, which is important but difficult to grasp, we recommend that the reader skip this subsection if it is too difficult.

From the general theory on the decomposition of prime ideals, which will be covered in §6.3, we know the following fact. Let K be an algebraic number field, L a finite abelian extension of K, and $\mathfrak{p}$

a prime ideal of K that is unramified in L. Then the Galois group $\mathrm{Gal}(L/K)$ contains an essential element called *Frobenius substitution*. This element, denoted by $\mathrm{Frob}_{\mathfrak{p},L}$ (or simply by $\mathrm{Frob}_{\mathfrak{p}}$), governs over the decomposition of $\mathfrak{p}$ in L: We might even claim that $\mathrm{Frob}_{\mathfrak{p}}$ has "the soul of $\mathfrak{p}$". It glimmers like a firefly in $\mathrm{Gal}(L/K)$ for each and every prime ideal. For the general theory on Frobenius substitution, see §6.3 (a). Here, we describe $\mathrm{Frob}_{p\mathbb{Z},L}$ (or simply $\mathrm{Frob}_{p,L}$) for $K = \mathbb{Q}$ and a prime number p unramified in L. $\mathrm{Frob}_{p,L}$ has the following characterization and properties. For the proof of Proposition 5.11, see §6.3 (a).

PROPOSITION 5.11. *Let L be a finite abelian extension of $\mathbb{Q}$ and p a prime number unramified in L.*

(1) *There is a unique element* $\mathrm{Frob}_{p,L} \in \mathrm{Gal}(L/\mathbb{Q})$ *such that*

$$\mathrm{Frob}_{p,L}(x) \equiv x^p \mod p\mathcal{O}_L$$

for all $x \in \mathcal{O}_L$.

(2) $\mathrm{Frob}_{p,L} = 1 \iff$ *p is totally decomposed in L.*
More precisely, if f is the order of $\mathrm{Frob}_{p,L}$*, then $p\mathcal{O}_L$ is a product of $[L:\mathbb{Q}]/f$ distinct prime ideals.*

(3) *If L' is a subfield of L, then the image of* $\mathrm{Frob}_{p,L}$ *by the natural surjection* $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(L'/\mathbb{Q})$ *coincides with* $\mathrm{Frob}_{p,L'}$.

For $L = \mathbb{Q}(\zeta_N)$ and for a prime number p not dividing N, $\mathrm{Frob}_{p,L}$ can be determined as follows.

PROPOSITION 5.12. *If p is a prime number not dividing N, then p is unramified in $\mathbb{Q}(\zeta_N)$, and $s_N : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ sends* $\mathrm{Frob}_{p,L}$ *to p mod N.*

We prove Theorems 5.4 and 5.7 assuming Proposition 5.12.

PROOF OF THEOREM 5.4. Since we already know that s_N is injective, we prove that it is surjective. Each element of $(\mathbb{Z}/N\mathbb{Z})^\times$ is of the form r mod N for some natural number r relatively prime to N. Factoring r into prime numbers, we see that $(\mathbb{Z}/N\mathbb{Z})^\times$ is generated by p mod N, where p does not divide N. Since $p \bmod N = s_N(\mathrm{Frob}_p)$ by Proposition 5.12, we see that s_N is surjective. □

PROOF OF THEOREM 5.7. Identify $\mathrm{Gal}(L/\mathbb{Q})$ with $(\mathbb{Z}/N\mathbb{Z})^\times/H$. By virtue of Propositions 5.11(3) and 5.12, $\mathrm{Frob}_{p,L} \in \mathrm{Gal}(L/\mathbb{Q})$

is equal to the image of $p \bmod N$ in $(\mathbb{Z}/N\mathbb{Z})^\times/H$. Hence, Theorem 5.7(2) follows from Proposition 5.11(2). □

Proof of Proposition 5.12. Let $L = \mathbb{Q}(\zeta_N)$. Since ζ_N is an N-th root of unity, a prime number p not dividing N is unramified in L by Proposition 5.2.

By Proposition 5.11(1), we have $\mathrm{Frob}_p(\zeta_N) \equiv \zeta_N^p \bmod p\mathcal{O}_L$. On the other hand, if r is a natural number satisfying $s_N(\mathrm{Frob}_p) = r \bmod N$, then we have $\mathrm{Frob}_p(\zeta_N) = \zeta_N^r$. Therefore, if we can show that $\zeta_N^a \equiv \zeta_N^b \bmod p\mathcal{O}_L$ implies $a \equiv b \bmod N$, then we can conclude that $s_N(\mathrm{Frob}_p) = p \bmod N$. For this purpose, it suffices to show that $\zeta_N^a \equiv 1 \bmod p\mathcal{O}_L$ implies $a \equiv 1 \bmod N$, or equivalently, $a \not\equiv 1 \bmod N$ implies $\zeta_N^a \not\equiv 1 \bmod p\mathcal{O}_L$. By differentiating both sides of the identity $T^N - 1 = \prod_{a=1}^{N}(T - \zeta_N^a)$ and letting $T = 1$, we obtain $N = \prod_{a=1}^{N-1}(1 - \zeta_N^a)$. Since $N \notin p\mathcal{O}_L$, we conclude $1 - \zeta_N^a \notin p\mathcal{O}_L$ for each a, $1 \le a \le N-1$. □

(d) Relations between cyclotomic fields and quadratic fields. Since any quadratic field is an abelian extension of $\mathbb{Q}$, Theorem 5.10(1) implies that it is contained in the cyclotomic field $\mathbb{Q}(\zeta_N)$ for some natural number N. Propositions 5.13 and 5.14 below give a concrete description of the way quadratic fields are contained in cyclotomic fields. As an application, from the decomposition law for prime numbers in cyclotomic fields (Theorem 5.7), we derive the decomposition law for quadratic fields (Theorem 5.15), which explain the phenomena shown in Tables 5.1–5.3.

A quadratic field can be written in the form $\mathbb{Q}(\sqrt{m})$, where m is a square free integer. We set

$$N = \begin{cases} |m| & \text{if } m \equiv 1 \mod 4, \\ 4|m| & \text{if } m \equiv 2, 3 \mod 4. \end{cases}$$

Proposition 5.13. *Let m and N as above. Then, we have*

$$\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\zeta_N).$$

Moreover, N is the smallest natural number for which we have such an inclusion.

For example:

(1) If $m = 5$, then $N = 5$ and $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$.
(2) If $m = -7$, then $N = 7$ and $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$.

(3) If $m = 7$, then $N = 28$ and $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\zeta_{28})$, but $\mathbb{Q}(\sqrt{7}) \not\subset \mathbb{Q}(\zeta_7)$.

In §4.3 of *Number Theory 1*, we defined the Dirichlet character for the quadratic field $\mathbb{Q}(\zeta_m)$

$$\chi_m : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\} \subset \mathbb{C}^\times$$

as follows: For an integer a relatively prime to N

$$\chi_m(a \bmod N) = \left(\prod_{\substack{l:\text{odd prime} \\ l|m}} \left(\frac{a}{l}\right) \right) \theta_m(a),$$

where $\theta_m(a)$ is defined as follows:

If $m \equiv 1 \bmod 4$, then $\theta_m(a) = 1$.

If $m \equiv 3 \bmod 4$, then

$$\theta_m(a) = \begin{cases} 1 & \text{if } a \equiv 1 \bmod 4 \\ -1 & \text{otherwise.} \end{cases}$$

If m is even, then

$$\theta_m(a) = \begin{cases} 1 & \text{if } a \equiv 1, \text{ or } 1-m \bmod 8 \\ -1 & \text{otherwise.} \end{cases}$$

PROPOSITION 5.14. *Let m, N, and χ_m be as above. Then the diagram*

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow[\cong]{s_N} & (\mathbb{Z}/N\mathbb{Z})^\times \\ \Big\downarrow \mathrm{res} & & \Big\downarrow \chi_m \\ \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) & \xrightarrow{\cong} & \{\pm 1\} \end{array}$$

*is commutative. Here, "*res*" is the restriction morphism which assigns an automorphism of $\mathbb{Q}(\zeta_N)$ to its restriction to $\mathbb{Q}(\sqrt{m})$.*

Although the original definition of χ_m is complicated, Proposition 5.14 gives an alternative definition of χ_m as a composite map:

$$(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\mathrm{res}} \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \cong \{\pm 1\} \subset \mathbb{C}^\times.$$

It follows from Proposition 5.14 that the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponding to the subfield $\mathbb{Q}(\sqrt{m})$ of $\mathbb{Q}(\zeta_N)$ coincides with the kernel of $\chi_m : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$. On the other hand, Theorem 5.7 describes the way prime numbers are decomposed in a subfield of $\mathbb{Q}(\zeta_N)$ in

terms of the corresponding subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. Hence, we obtain (2) of the following theorem.

THEOREM 5.15. *Let m and N be as above, and let p be a prime number.*

(1) *p is ramified in $\mathbb{Q}(\sqrt{m}) \iff p|N$.*
(2) *If p does not divide N, then in the ring of integers of $\mathbb{Q}(\sqrt{m})$*
$\chi_m(p) = 1 \iff (p)$ is a product of two distinct prime ideals,
$\chi_m(p) = -1 \iff (p)$ is a prime ideal.

The proof of (1) of Theorem 5.15 goes as follows. If p does not divide N, then p is unramified in $\mathbb{Q}(\zeta_N)$, hence in the subfield $\mathbb{Q}(\sqrt{m})$. Suppose p divides N. If p divides m, we can show that $(p) = \left(p, \sqrt{m}\right)^2$ in the ring of integers of $\mathbb{Q}(\sqrt{m})$ and thus p is ramified in $\mathbb{Q}(\sqrt{m})$. If p does not divide m, then we have $p = 2$ and $m \equiv 3 \bmod 4$. We can show that $(2) = \left(2, 1+\sqrt{m}\right)^2$ in the ring of integers of $\mathbb{Q}(\sqrt{m})$, which implies that 2 is ramified in $\mathbb{Q}(\sqrt{m})$.

The decomposition laws for prime numbers in quadratic fields described in Tables 5.1–5.3 can be obtained from Theorem 5.15. For example, if $m = -6$, we find easily from the definition that $\chi_m : (\mathbb{Z}/24\mathbb{Z})^\times \to \{\pm 1\}$ maps $1, 5, 7, 11 \bmod 24$ to 1, and $13, 17, 19, 23 \bmod 24$ to -1. Thus, the decomposition law for prime numbers in $\mathbb{Q}(\sqrt{-6})$ shown in Table 5.2 follows from Theorem 5.15.

QUESTION 4. From Theorem 5.15, derive the decomposition law for prime numbers in $\mathbb{Q}(\sqrt{-5})$ shown in Table 5.2.

(e) Proofs of the relations between cyclotomic fields and quadratic fields. In this subsection we prove Propositions 5.13 and 5.14 on the relations between cyclotomic fields and quadratic fields.

For a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ and a primitive N-th root ζ_N, we define the *Gauss sum* $G(\chi, \zeta_N)$ by

$$G(\chi, \zeta_N) = \sum_{a=1}^{N} \chi(a)\zeta_N^a.$$

(We set $\chi(a) = 0$ if a is not relatively prime to N.) A Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is said to be *primitive* if it cannot be factored as

$$(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$$

for any divisor d of N satisfying $1 \le d < N$ and any Dirichlet character $\chi' : (\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}^\times$.

PROPOSITION 5.16. *If $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is a primitive Dirichlet character, then we have*

$$\big|G(\chi, \zeta_N)\big| = \sqrt{N}.$$

PROOF. We prove that, for every integer n, we have

$$\bar{\chi}(n)G(\chi, \zeta_N) = G(\chi, \zeta_N^n), \tag{5.3}$$

where $\bar{\chi}$ is the complex conjugate of χ. If n and N are relatively prime, we obtain (5.3) by rewriting the right-hand side:

$$G(\chi, \zeta_N^n) = \sum_{a=1}^{N} \chi(a)\zeta_N^{an} = \bar{\chi}(n) \sum_{a=1}^{N} \chi(an)\zeta_N^{an}.$$

If n and N are not relatively prime, then ζ_N^n is a primitive d-th root of unity for some integer $d < N$. Let H be the kernel of the canonical map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times$. Since χ is primitive, we have $\chi(H) \neq \{1\}$. It follows that $\sum_{a\in H} \chi(a) = 0$, and thus $G(\chi, \zeta_N^n) = 0 =$ left-hand side. Taking the square of the absolute values of the both sides of (5.3), we obtain

$$|\bar{\chi}(n)|^2\big|G(\chi, \zeta_N)\big|^2 = G(\chi, \zeta_N^n)G(\bar{\chi}, \zeta_N^{-n}) = \sum_{a,b} \chi(a)\bar{\chi}(b)\zeta_N^{(a-b)n}.$$

If we add these for $n = 1, \dots, N$, then the terms for $a \neq b$ vanish, and we obtain

$$\varphi(N)\big|G(\chi, \zeta_N)\big|^2 = \sum_{a=1}^{N} |\chi(a)|^2 \cdot N = \varphi(N) \cdot N,$$

where $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$. Therefore, we obtain $|G(\chi, \zeta_N)| = \sqrt{N}$. □

PROPOSITION 5.17. *Let m, N be as in Proposition 5.13. Then,*

(1) *χ_m is primitive.*
(2) $\chi_m(-1) = \begin{cases} 1 & \text{if } m > 0, \\ -1 & \text{if } m < 0. \end{cases}$

PROOF. (1) follows from the definition of χ_m.
To prove (2), we see from the definition of θ_m

$$\theta_m(-1) = \begin{cases} 1 & \text{if } m \equiv 1 \bmod 4 \text{ or } m \equiv 2 \bmod 8, \\ -1 & \text{if } m \equiv 3 \bmod 4 \text{ or } m \equiv 6 \bmod 8. \end{cases}$$

Thus, we have

$$\theta_m(-1) = \begin{cases} \chi_{-1}(m) & \text{if } m \text{ is odd,} \\ \chi_{-1}\Big(\dfrac{m}{2}\Big) & \text{if } m \text{ is even.} \end{cases}$$

On the other hand, if $p_1, \dots, p_r$ are all the odd primes that divide m, we have

$$\Big(\frac{-1}{p_i}\Big) = (-1)^{\frac{p_i-1}{2}} = \chi_{-1}(p_i),$$

and thus,

$$\prod_{i=1}^{r}\Big(\frac{-1}{p_i}\Big) = \prod_{i=1}^{r}\chi_{-1}(p_i) = \chi_{-1}\Big(\prod_{i=1}^{r}p_i\Big) = \begin{cases} \chi_{-1}(|m|) & \text{for odd } m, \\ \chi_{-1}\Big(\dfrac{|m|}{2}\Big) & \text{for even } m. \end{cases}$$

Thus, we have

$$\chi_m(-1) = \Big(\prod_{i=1}^{r}\Big(\frac{-1}{p_i}\Big)\Big)\theta_m(-1) = \chi_{-1}\Big(\frac{m}{|m|}\Big) = \begin{cases} 1 & \text{for } m > 0, \\ -1 & \text{for } m < 0. \end{cases}$$

□

Proposition 5.18.

$$G(\chi_m, \zeta_N)^2 = \begin{cases} m & \textit{for } m \equiv 1 \bmod 4, \\ 4m & \textit{for } m \equiv 2, 3 \bmod 4. \end{cases}$$

Proof. By Proposition 5.16 and Proposition 5.17(1), we have

$$G(\chi_m, \zeta_N)G(\bar{\chi}_m, \zeta_N^{-1}) = N.$$

Since $\bar{\chi}_m = \chi_m$, it follows from (5.3) that the left-hand side is equal to $\chi_m(-1)G(\chi_m, \zeta_N)^2$. Now Proposition 5.17(2) implies Proposition 5.18. □

For example, letting $m = 5$, or -7 in Proposition 5.18, we have

$$(\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4)^2 = 5,$$

$$(\zeta_7 + \zeta_7^2 - \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6)^2 = -7,$$

the properties which we mentioned in §5.1(d).

It follows from Proposition 5.18 that $\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\zeta_N)$, which is the first assertion of Proposition 5.13. Proposition 5.14 can also be derived from Proposition 5.18 as follows. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, let

r be a natural number satisfying $s_N(\sigma) \equiv r \bmod N$. Then, it follows from Proposition 5.18 that

$$\frac{\sigma(\sqrt{m})}{\sqrt{m}} = \frac{\sigma(G(\chi_m, \zeta_N))}{G(\chi_m, \zeta_N)} = \frac{G(\chi_m, \zeta_N^r)}{G(\chi_m, \zeta_N)} = \bar{\chi}_m(r) = \chi_m(r).$$

(The third equality is due to (5.3).) This shows that the diagram in Proposition 5.14 is commutative.

(f) Proof of the quadratic reciprocity law à la class field theory. In this subsection we derive the quadratic reciprocity law from Theorem 5.15.

LEMMA 5.19. *Let L be a quadratic field and m a squarefree integer such that $L = \mathbb{Q}(\sqrt{m})$. If p is an odd prime number not dividing m, then in $\mathbb{Q}(\sqrt{m})$, we have*

$$\left(\frac{m}{p}\right) = 1 \iff (p) \text{ is a product of two distinct prime ideals,}$$
$$\left(\frac{m}{p}\right) = -1 \iff (p) \text{ is a prime ideal.}$$

PROOF. Commutative ring theory tells us that there is a one-to-one correspondence

$$\text{prime ideals of } \mathcal{O}_L \text{ containing } p \overset{1:1}{\longleftrightarrow} \text{prime ideals of } \mathcal{O}_L/p\mathcal{O}_L.$$

We study the residue ring $\mathcal{O}_L/p\mathcal{O}_L$ to find the decomposition of p in $\mathcal{O}_L$. Since $\mathcal{O}_L$ equals $\mathbb{Z}[\sqrt{m}]$ or $\mathbb{Z}\big[(1+\sqrt{m})/2\big]$ as we saw in *Number Theory 1*, §4.2 (a), the quotient group $\mathcal{O}_L/\mathbb{Z}[\sqrt{m}]$ is a group of order 1 or 2. This, together with the fact that p is odd, implies

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}].$$

Furthermore, since $\mathbb{Z}[\sqrt{m}] \cong \mathbb{Z}[x]/(x^2 - m)$, we have

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_p[x]/(x^2 - m).$$

We divide into two cases.

The case where $\left(\frac{m}{p}\right) = -1$. Since there is no square root of m in $\mathbb{F}_p$, $x^2 - m$ is irreducible over $\mathbb{F}_p$, and hence $\mathbb{F}_p[x]/(x^2 - m)$ is a field. Thus $\mathcal{O}_L/p\mathcal{O}_L$ is a field and $p\mathcal{O}_L$ is a prime ideal.

The case where $\left(\frac{m}{p}\right) = 1$. By taking $a \in \mathbb{Z}$ such that $a^2 - m \equiv 0 \bmod p$, we have $x^2 - m = (x-a)(x+a)$ in $\mathbb{F}_p[x]$. Hence $\mathbb{F}_p[x]/(x^2 - m)$ contains two prime ideals $(x-a)$ and $(x+a)$. Thus, $\mathcal{O}_L$ contains two prime ideals containing p. They are $(p, \sqrt{m} - a)$ and $(p, \sqrt{m} + a)$; call them $\mathfrak{p}$ and $\mathfrak{q}$. Since (p) is divisible by $\mathfrak{p}$, we have

$\mathfrak{pq} \supset (p)$. On the other hand, since $(x-a)(x+a)$ is 0 in $\mathbb{F}_p/(x^2-m)$, we get $\mathfrak{pq} \subset (p)$. This shows that $(p) = \mathfrak{pq}$. □

The quadratic reciprocity law can now be derived from Theorem 5.15 and Lemma 5.19 as follows. Let m and N be as in subsection (d). If p is an odd prime number that does not divide m, we know from Lemma 5.19 that

$$p \text{ is totally decomposed in } \mathbb{Q}(\sqrt{m}) \iff \left(\frac{m}{p}\right) = 1. \tag{5.4}$$

On the other hand, Theorem 5.15 says that

$$\begin{aligned} &p \text{ is totally decomposed in } \mathbb{Q}(\sqrt{m}) \\ &\iff p \bmod N \text{ belongs to the kernel of } \chi_m : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}. \end{aligned} \tag{5.5}$$

By putting (5.4) and (5.5) together we obtain

$$\left(\frac{m}{p}\right) = \chi_m(p). \tag{5.6}$$

Now we let m equal an odd prime number q different from p. By definition of χ_q we have

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

and hence the quadratic reciprocity law

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

Compare (5.4) and (5.5). The former, which says that the nature of decomposition for p in $\mathbb{Q}(\sqrt{m})$ can be determined by m mod p, will eventually be absorbed into Proposition 6.41 (2) in §6.3 (b) general Dedekind domains. The latter, which says that we can tell the decomposition of p by p mod N, is truly number-theoretic. The mystery of the quadratic reciprocity law as well as class field theory lies in this conversion of "m mod p" into "p mod N".

5.3. An outline of class field theory

Theorems 5.7 and 5.10 in §5.2 show what is happening in abelian extensions of $\mathbb{Q}$, that is, how a prime number p is decomposed in each abelian extension. Generalizing to the case of algebraic number field K, class field theory describes what is happening in abelian extensions of K, that is, how a prime ideal of K is decomposed in each abelian extension. We will outline class field theory in the subsection (a)

and show one of the tangible consequences of class field theory in the subsection (b).

(a) Outline of the class field theory. Let K be an algebraic number field. The content of class field theory can be summarized as follows.

> Corresponding to the extension $\mathbb{Q}(\zeta_N)$ over $\mathbb{Q}$, there is a certain extension $K(\mathfrak{a})$ over K for each nonzero ideal $\mathfrak{a}$ in the ring of integers $\mathcal{O}_K$. If $K = \mathbb{Q}$ and $\mathfrak{a} = (N)$, we have $K(\mathfrak{a}) = \mathbb{Q}(\zeta_N)$. Then, similar results to Theorems 5.7 and 5.10 hold for K and $K(\mathfrak{a})$ in replacing $\mathbb{Q}$ and $\mathbb{Q}(\zeta_N)$.

DEFINITION 5.20. An element $\alpha \neq 0$ in K is said to be totally positive if for every field homomorphism $K \to \mathbb{R}$ (that is, for every real place (see *Number Theory 1*, Definition 4.19)) the image of α is positive.

For example, the element $1+\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$ is not totally positive, because the homomorphism $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ such that $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ maps $1+\sqrt{2}$ into $1-\sqrt{2} < 0$.

The following theorem will be proved in §8.1.

THEOREM 5.21. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then*

(1) *There is a unique finite extension $K(\mathfrak{a})$ of K having the following property: if $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ not dividing $\mathfrak{a}$, then $\mathfrak{p}$ is unramified and we have the following equvalence.*

$\mathfrak{p}$ is totally decomposed in $K(\mathfrak{a})$	$\iff$ *There exists a totally positive element $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (\alpha), \alpha \equiv 1 \bmod \mathfrak{a}$.*

(2) *$K(\mathfrak{a})$ is an abelian extension of K, and every finite abelian extension of K is contained in $K(\mathfrak{a})$ for some $\mathfrak{a}$.*

(3) *If $\mathfrak{b}$ is a nonzero ideal of $\mathcal{O}_K$ with $\mathfrak{b} \subset \mathfrak{a}$, then*

$$K(\mathfrak{b}) \supset K(\mathfrak{a}).$$

(4) *If L is a finite abelian extension of K, then there exists a largest nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $L \subset K(\mathfrak{a})$. Moreover, $\mathfrak{a}$ has the following property: for any nonzero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$,*

$$\mathfrak{p} \text{ is ramified in } L \iff \mathfrak{p} \text{ divides } \mathfrak{a}.$$

EXAMPLE 5.22. For $K = \mathbb{Q}$, $\mathfrak{a} = (N)$ with N a natural number, we have $K(\mathfrak{a}) = \mathbb{Q}(\zeta_N)$, as we see from Theorems 5.7 and 5.21. Indeed, a nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}$ is generated by $\pm p$ with a prime number p. Now p is totally positive, whereas $-p$ is not. (Note that for elements of $\mathbb{Q}^\times$ "totally positive" simply means "positive".) Hence, to say "there exists a totally positive integer α such that $\mathfrak{p} = (\alpha)$, $\alpha \equiv 1 \bmod N$" is nothing but to say "$\mathfrak{p} = (p)$ with p a prime number such that $p \equiv 1 \bmod N$". Therefore, by Corollary 5.8 we see that $\mathbb{Q}(\zeta_N)$ has the property of $K(\mathfrak{a})$ stated in Theorem 5.21(1). By the uniqueness assertion in Theorem 5.21 we conclude that $\mathbb{Q}(\zeta_N) = K(\mathfrak{a})$.

EXAMPLE 5.23. Table 5.7 shows that for $\mathbb{Q}(\zeta_3)$ and $\mathfrak{a} = (6)$, we have $K(\mathfrak{a}) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. (Note that since K has no real place, every element of $K^\times$ is totally positive.)

EXAMPLE 5.24. Let $K = \mathbb{Q}(\sqrt{2})$. For the ideals $\mathfrak{a}_i = \left(\sqrt{2}^i\right)$ $(i \geq 0)$, we will prove the following in §8.1(g).

$$K(\mathfrak{a}_0) = K(\mathfrak{a}_1) = \mathbb{Q}(\sqrt{2}), \qquad K(\mathfrak{a}_2) = K(\mathfrak{a}_3) = \mathbb{Q}(\zeta_8),$$
$$K(\mathfrak{a}_4) = \mathbb{Q}\Big(\zeta_8, \sqrt{1+\sqrt{2}}\Big), \qquad K(\mathfrak{a}_5) = \mathbb{Q}\Big(\zeta_8, \sqrt{1+\sqrt{2}}, \sqrt[4]{2}\Big).$$

Consider the special case where $\mathfrak{a} = \mathcal{O}_K$. Theorem 5.21 states that every nonzero prime ideal in $\mathcal{O}_K$ is unramified in $K(\mathcal{O}_K)$. It is known that, among the extensions of $\mathbb{Q}$, $\mathbb{Q}$ is the only algebraic number field in which all prime numbers are unramified. However, it can be $K(\mathcal{O}_K) \neq K$ in general, as we see in the following examples.

EXAMPLE 5.25. If $K = \mathbb{Q}(\sqrt{-5})$, then $K(\mathcal{O}_K) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

EXAMPLE 5.26. If $K = \mathbb{Q}(\sqrt{-6})$, then $K(\mathcal{O}_K) = \mathbb{Q}(\sqrt{-6}, \zeta_3)$.

The assertions in Examples 5.25 and 5.26 will be proved in §8.1(g). Since $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-6})$ do not have any real places, every nonzero element is totally positive. Hence, by the assertions in Theorem 5.21 and Examples 5.25 and 5.26, we see that in the extension $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ of $\mathbb{Q}(\sqrt{-5})$ and in the extension $\mathbb{Q}(\sqrt{-6}, \zeta_3)$ of $\mathbb{Q}(\sqrt{-6})$, all principal prime ideals are totally decomposed, and all nonprincipal prime ideals do not decompose.

Note that, for $K = \mathbb{Q}(\sqrt{-5})$, we can prove that all nonzero prime ideals of $\mathcal{O}_K$ are unramified in $K(\sqrt{-1})$ in the following way. By Proposition 5.2, any prime ideal of $\mathcal{O}_K$ that does not contain 2 is

unramified in $K(\sqrt{-1})$. Since $K(\sqrt{-1}) = K(\sqrt{5}) \subset K(\zeta_5)$, it also follows from Proposition 5.2 that any nonzero prime ideal of $\mathcal{O}_K$ that does not contain 5 is unramified in $K(\sqrt{-1})$. Needless to say, there is no prime ideal that contains both 2 and 5.

QUESTION 5. For $K = \mathbb{Q}(\sqrt{-6})$, derive from Proposition 5.2 in a similar manner as above that all nonzero prime ideals of $\mathcal{O}_K$ are unramified in $K(\zeta_3)$.

Theorem 5.21 does not contain any description of the decomposition of prime ideals of K in a field L satisfying $K(\mathfrak{a}) \supset L \supset K$. If we include this description to refine Theorem 5.21, we come very close to showing the entire picture of class field theory, but we postpone it until Chapter 8.

(b) $p = x^2 + 5y^2, p = x^2 + 6y^2, \ldots$ and class field theory. The content of class field theory stated in the subsection (a) may sound rather abstract. However, Theorem 5.21 can lead to Proposition 5.27, which produces concrete results on prime numbers that can be written in the form $x^2 + 5y^2$ or $x^2 + 6y^2$, where $x, y \in \mathbb{Z}$. Let K be a quadratic field, σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ the norm map $\alpha \mapsto \alpha\sigma(\alpha)$. (For the norm, see Appendix B3.) For example, we have for $x, y \in \mathbb{Q}$

$$N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}\big(x + y\sqrt{-5}\big) = \big(x + y\sqrt{-5}\big)\big(x - y\sqrt{-5}\big) = x^2 + 5y^2,$$

$$N_{\mathbb{Q}(\sqrt{-6})/\mathbb{Q}}\big(x + y\sqrt{-6}\big) = \big(x + y\sqrt{-6}\big)\big(x - y\sqrt{-6}\big) = x^2 + 6y^2.$$

PROPOSITION 5.27. *Let K be a quadratic field, and p a prime number that is unramified in K. Then, the following three conditions are equivalent.*

- (i) *There exists an element $\alpha \in \mathcal{O}_K$ such that $p = N_{K/\mathbb{Q}}(\alpha)$.*
- (ii) *p is totally decomposed in the field $K(\mathcal{O}_K)$.*
- (iii) *$(p) = \mathfrak{pq}$ in $\mathcal{O}_K$, where $\mathfrak{p}$ and $\mathfrak{q}$ are distinct prime ideals in $\mathcal{O}_k$ generated by totally positive elements in $\mathcal{O}_K$.*

PROOF. The equivalence of (ii) and (iii) follows from the property of the extension field $K(\mathcal{O}_K)$ of K stated in Theorem 5.21.

We show that (i) implies (iii). Let $p = N_{K/\mathbb{Q}}(\alpha)$, $\alpha \in \mathcal{O}_K$. If K is an imaginary quadratic field, then α is totally positive. If K is a real quadratic field, then K has two real places. Let $\iota : K \to \mathbb{R}$ be one of the two. Then, the other is $\iota \circ \sigma : K \to \mathbb{R}$. If $\iota(\alpha) > 0$, then $p = \alpha\sigma(\alpha)$ implies $\iota \circ \sigma(\alpha) > 0$, and hence α is totally positive. If $\iota(\alpha) < 0$, then by a similar argument we see that $-\alpha$ is totally

positive and $p = N_{K/\mathbb{Q}}(-\alpha)$. Thus, in any case, there is a totally positive α such that $p = \alpha\sigma(\alpha)$. Since (p) is a product of at most two distinct prime ideals, it follows that (α) and $(\sigma(\alpha))$ are distinct prime ideals of $\mathcal{O}_K$. This proves (iii).

Finally, we show that (iii) implies (i). We have $\mathfrak{p} = (\alpha)$, where α is a totally positive element in $\mathcal{O}_K$. We show that $p = N_{K/\mathbb{Q}}(\alpha)$. If we set $p = \alpha\beta, \beta \in \mathcal{O}_K$, then we have $p^2 = \alpha\sigma(\alpha) \cdot \beta\sigma(\beta)$. We know that both $\alpha\sigma(\alpha)$ and $\beta\sigma(\beta)$ are integers, and that neither of them equals ± 1. Hence $\alpha\sigma(\alpha) = \pm p$. Since α is totally positive, we conclude that $\alpha\sigma(\alpha) = p$. □

EXAMPLE 5.28. Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathfrak{a} = \mathcal{O}_K$. By Proposition 5.27 we see that for prime numbers $p \neq 2, 5$ we have

There exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 5y^2$

$\iff$ p is totally decomposed in $K(\alpha)$

$\iff$ p is a product of two distinct principal prime ideals in K.

From Example 5.25 we have $K(\mathfrak{a}) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. This field is contained in $\mathbb{Q}(\zeta_{20})$, and it corresponds to the subgroup of $(\mathbb{Z}/20\mathbb{Z})^\times$ given by

$$\begin{aligned}&\mathrm{Ker}\big((\mathbb{Z}/20\mathbb{Z})^\times \xrightarrow{\chi_{-5}} \{\pm 1\}\big) \cap \mathrm{Ker}\big((\mathbb{Z}/20\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\chi_{-1}} \{\pm 1\}\big)\\ &\quad = \{1, 3, 7, 9 \bmod 20\} \cap \{1, 9, 13, 17 \bmod 20\} = \{1, 9 \bmod 20\}.\end{aligned}$$

It follows from Theorem 5.7 that

$$p \text{ is totally decomposed in } \mathbb{Q}(\sqrt{-5}, \sqrt{-1}) \iff p \equiv 1, 9 \bmod 20.$$

We thus conclude that

$$\text{There exist } x, y \in \mathbb{Z} \text{ such that } p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20.$$

Recall that prime numbers p such that $p \equiv 1, 3, 7, 9 \bmod 20$ are totally decomposed in $\mathbb{Q}(\sqrt{-5})$ (see Table 5.2). Among these prime numbers, (p) becomes a product of principal prime ideals in $\mathbb{Z}(\sqrt{-5})$ for p with $p \equiv 1, 9 \bmod 20$, For p with $p \equiv 3, 7 \bmod 20$, (p) is a product of nonprincipal prime ideals. (See the decompositions of (41), (3), (7), and (29) in $\mathbb{Z}[\sqrt{-5}]$ shown in §5.1 (b).)

EXAMPLE 5.29. By a similar argument we can show that for $p \neq 2, 3$

$$\text{There exist } x, y \in \mathbb{Z} \text{ such that } p = x^2 + 6y^2 \iff p \equiv 1, 7 \bmod 24.$$

To show this, let $K = \mathbb{Q}(\sqrt{-6}), \mathfrak{a} = \mathcal{O}_K$ in Proposition 5.27. Then, it follows from Example 5.26 and the fact that, as a subfield of $\mathbb{Q}(\zeta_{24})$, $\mathbb{Q}(\sqrt{-6}, \zeta_3)$ corresponds to the subgroup $\{1, 7 \bmod 24\}$ of $(\mathbb{Z}/24\mathbb{Z})^\times$. Also, we see that prime numbers $p \equiv 1, 5, 7, 11 \bmod 24$ are totally decomposed in $\mathbb{Q}(\sqrt{-6})$ (see Table 5.2). Among those, (p) is a product of principal prime ideals of $\mathbb{Z}[\sqrt{-6}]$ for $p \equiv 1, 7 \bmod 24$, and is a product of nonprincipal prime ideals for $p \equiv 5, 11 \bmod 24$. (See the decomposition of (73), (5), (7), and (22) in $\mathbb{Z}[\sqrt{-6}]$.)

The following Proposition 5.30, which is a slight generalization of Proposition 5.27, can be derived from Theorem 5.21, just as we did for Proposition 5.27.

PROPOSITION 5.30. *Let K be a quadratic field, σ a generator of $\mathrm{Gal}(K/\mathbb{Q})$, and $\mathfrak{a}$ a nonzero ideal of $\mathcal{O}_K$ such that $\sigma(\mathfrak{a}) = \mathfrak{a}$. Then, the following two statements are equivalent.*

(i) *There exits a totally positive $\alpha \in \mathcal{O}_K$ such that $p = N_{K/\mathbb{Q}}(\alpha)$ and $\alpha \equiv 1 \bmod \mathfrak{a}$.*
(ii) *p is totally decomposed in the field $K(\mathfrak{a})$.*

EXAMPLE 5.31. For a prime number $p \neq 2$, we have

$$\text{There exist } x, y \in \mathbb{Z} \text{ such that } p = x^2 - 8y^2 \iff p \equiv 1 \bmod 8.$$

This can be seen by taking $K = \mathbb{Q}(\sqrt{2})$ and $\mathfrak{a} = (2)$ in Proposition 5.30 as follows. Since $x^2 - 8y^2 = x^2 - 2(2y)^2$, we see that

$$\begin{aligned}
&\text{There exist } x, y \in \mathbb{Z} \text{ such that } p = x^2 - 8y^2 \\
&\iff \text{There exist an odd } x \text{ and an even } y \text{ such that } p = x^2 - 2y^2 \\
&\iff \text{There exists } \alpha \in \mathbb{Z}[\sqrt{2}] = \mathcal{O}_K \text{ such that } p = N_{K/\mathbb{Q}}(\alpha) \\
&\qquad \text{and } \alpha \equiv 1 \bmod 2\mathbb{Z}[\sqrt{2}].
\end{aligned}$$

We may assume α to be totally positive by replacing it with $-\alpha$ if necessary. Hence, by Proposition 5.30, we see that

$$\iff p \text{ is totally decomposed in } K(\mathfrak{a}).$$

As we saw in Example 5.24, we have $K(\mathfrak{a}) = \mathbb{Q}(\zeta_8)$. It then follows from Corollary 5.8 that

$$\iff p \equiv 1 \bmod 8.$$

EXAMPLE 5.32. Let $K = (\sqrt{-26})$ and $\mathfrak{a} = \mathcal{O}_K$. In this case it is known that $K(\mathfrak{a})$ is not an abelian extension of $\mathbb{Q}$. By Proposition 5.27, we have for primes $p \neq 2, 13$,

$$\text{There exist } x, y \in \mathbb{Z} \text{ such that } p = x^2 + 26y^2$$
$$\iff p \text{ is totally decomposed in } K(\mathfrak{a}).$$

However, in view of Theorem 5.10, we cannot rephrase this statement in the form

$$\iff p \equiv \cdots \bmod N$$

no matter which natural number N we may take.

Summary

5.1. Questions such as whether or not a prime number p can be written in the form $x^2 + 6y^2$, or whether or not p is a prime factor of a number of the form x^2+6, are related to the way p decomposes in an algebraic number field.

5.2. The way a prime number p decomposes in a subfield of the cyclotomic field $\mathbb{Q}(\zeta_N)$ is determined by $p \bmod N$.

5.3. Every quadratic field is a subfield of a certain cyclotomic field. Hence, the way a prime number decomposes in a quadratic field is determined by $p \bmod N$ for some N. The quadratic reciprocity law may be interpreted as a statement of this fact.

5.4. For the decomposition of a prime ideal of an algebraic number field K in its abelian extension, there is a similar law (class field theory).

Exercises

5.1. List all subfields of $\mathbb{Q}(\zeta_8)$. For each subfield, which prime numbers are totally decomposed?

5.2. Same question for the field $\mathbb{Q}(\zeta_{15})$.

5.3. Fermat said, "A prime number p such that $p \equiv 3, 7 \bmod 20$ cannot be written in the form x^2+5y^2, but it seems that the product of two such prime numbers can be written in the form x^2+5y^2 with some $x, y \in \mathbb{Z}$. It seems very likely, but I cannot prove it." Study this question.

5.4. Let p be a prime number and N a natural number.

(1) Using the fact that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ (see Appendix B.4), show that $p \equiv 1 \bmod N$ if and only if $\mathbb{F}_p$ has a primitive N-th root of unity.

(2) From the case where $N = 4$ in (1), show that for an odd prime number p we have

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