12. Quadratic Reciprocity in Number Fields

In [RL1, p. 273/274] we briefly mentioned how Eisenstein arrived at a hypothetical reciprocity law by assuming what later turned out to be an immediate consequence of the product formula for the Hilbert symbol, which in turn follows directly from Artin's reciprocity law. In this and the next chapter we will explain his beautiful idea in detail.

12.1 Quadratic Reciprocity in $\mathbb{Z}$

Eisenstein [22] realized that the reciprocity laws for quadratic and cubic residues can be formulated in a way that allows the immediate generalization to arbitrary powers and number fields: his observation was that the inversion factor $i(\alpha,\beta) = (\frac{\alpha}{\beta})(\frac{\beta}{\alpha})^{-1}$ for p-th power residue symbols in $\mathbb{Q}(\zeta_p)$ and odd primes p only depends on $\alpha, \beta \bmod (1-\zeta)^m$ for some integer m. In this section we show that Eisenstein's version for $p = 2$ over $\mathbb{Q}$ is equivalent to the quadratic reciprocity law; then we will prove its generalization for quadratic number fields. In the next chapter we will then show how to extract the reciprocity law for p-th power residues from the above conjecture.

For coprime odd integers $a, b \in \mathbb{Z}$, define a symbol $[a,b]$ with values in $\{0,1\}$ by $(\frac{a}{b})(\frac{b}{a}) = (-1)^{[a,b]}$. Let us make the following assumption:

Hypothesis (H). *There exists an integer $\sigma \in \mathbb{N}$ such that $[a,b] = [a',b']$ for all natural numbers $a, b, a', b' \in \mathbb{N}$ with $(a,b) = (a',b') = 1$, and $a \equiv a',\ b \equiv b' \bmod 2^\sigma$.*

We could also allow integers $a, b, a', b' \in \mathbb{Z}$, but then we would have to add the condition that $aa' > 0$ and $bb' > 0$. In that case, (H) may also be assumed to hold for $b = -1$; note that $(\frac{a}{-1}) = (\frac{a}{1}) = 1$, since by definition of the Jacobi symbol $(\frac{a}{1}) = \prod_{p|1}(\frac{a}{p})$, and this product is empty.

In order to better understand what Hypothesis (H) is all about we first derive the following result (which will not be used in the sequel):

Proposition 12.1. *If Hypothesis (H) holds, then*

$$\Big(\frac{a}{b}\Big) = \Big(\frac{a}{b + 2^\sigma a}\Big)$$

for all coprime numbers $a, b \in \mathbb{N}$.

In other words: Hypothesis (H) states that the Legendre symbol $(\frac{a}{\cdot})$, as a function of its denominator, has conductor dividing $2^\sigma a$. This is a weak form of the reciprocity law as given by Euler: compare [RL1,Thm. 2.28.iv)].

Proof. Observe that

$$\Big(\frac{a}{b}\Big)\Big(\frac{b}{a}\Big) = \Big(\frac{a}{b+2^\sigma a}\Big)\Big(\frac{b+2^\sigma a}{a}\Big) = \Big(\frac{a}{b+2^\sigma a}\Big)\Big(\frac{b}{a}\Big)$$

by Hypothesis (H) and reduction modulo a. □

Let us now sketch Eisenstein's idea for deriving the quadratic reciprocity law from (H). The basic ingredient is a special case of Hensel's Lemma, i.e., the observation that integers $a \equiv 1 \bmod 8$ are squares modulo 2^σ:

Lemma 12.2. *If $a \in \mathbb{Z}$ is an integer with $a \equiv 1 \bmod 8$, then for every $\sigma \in \mathbb{N}$ there is an integer μ_σ such that $a \equiv \mu_\sigma^2 \bmod 2^\sigma$.*

Proof. Assume that we know $a \equiv \mu_e^2 \bmod 2^e$ for some $e \geq 3$; then $a = \mu_e^2 + 2^e b$ for some integer b. But then $\mu_{e+1} = \mu_e + 2^{e-1}b$ will do it, since we have $a \equiv (\mu_e + 2^{e-1}b)^2 \bmod 2^{e+1}$ in light of $2^{2e-2} \equiv 0 \bmod 2^{e+1}$ for $e \geq 3$. □

This simple observation enables us to prove

Proposition 12.3. *If (H) holds for some integer σ, then it holds for $\sigma = 3$.*

Proof. Given an odd integer a, there is an integer $r \in \{1,3,5,7\}$ such that $a \equiv r \bmod 8$; this implies $a/r \equiv 1 \bmod 8$, so by Lemma 12.2, there is an integer m such that $a \equiv rm^2 \bmod 2^\sigma$. Similarly, we have $b \equiv s \bmod 8$ for some $s \in \{1,3,5,7\}$, and thus $b \equiv sn^2 \bmod 2^\sigma$ for some integer n. We have to show that if $(a,b) = (r,s) = 1$, then $[a,b] = [r,s]$. Since we may choose m and n in such a way that $(rm, sn) = 1$, hypothesis (H) then implies $[a,b] = [rm^2, sn^2] = [r,s]$. Thus the value of $[a,b]$ only depends on $a, b \bmod 8$. □

Corollary 12.4. *We have $[a,b] \equiv \frac{a-1}{2}\frac{b-1}{2} \bmod 2$.*

Proof. All we have to do is compute $[a,b]$ for all possible odd values of $a, b \bmod 8$. For example, if $a \equiv b \equiv 3 \bmod 8$, then $[a,b] = [3,11] = (\frac{3}{11})(\frac{11}{3}) = -1$, hence $[a,b] = 1$ in this case. Checking every case then gives the following table:

$[a,b]$	1	3	5	7
1	0	0	0	0
3	0	1	0	1
5	0	0	0	0
7	0	1	0	1

Thus $[a,b] \equiv \frac{a-1}{2}\frac{b-1}{2} \bmod 2$ as claimed. □

The preceding corollary immediately implies the following improvement of Prop. 12.3:

Corollary 12.5. *If (H) holds for some σ, then it holds for $\sigma = 2$.*

Deriving the quadratic reciprocity law (even for Jacobi symbols) from (H) was quite easy; the supplementary laws can be treated similarly. Adapting an idea of Eisenstein to the case of quadratic reciprocity, we now show that the supplementary laws follow from the general reciprocity law through a simple computation:

Corollary 12.6. *We have $(\frac{-1}{a}) = (-1)^{(a-1)/2}$ for $a \in \mathbb{N}$. For any $a, m \in \mathbb{N}$, the residue symbol $(\frac{a}{m})$ only depends on the residue class of $m \bmod 4a$; in particular, $(\frac{2}{a}) = (-1)^{(a^2-1)/8}$ for $a \in \mathbb{Z} \setminus \{0\}$.*

Proof. For the first claim we consider the equation $a - b = 4$; reducing it modulo a and b gives $(a/b) = (-b/a) = 1$, hence $(-1/a) = (a/b)(b/a) = (-1)^{(a-1)(b-1)/4} = (-1)^{(a-1)(a-5)/4} = (-1)^{(a-1)/2}$ by the quadratic reciprocity law and the fact that $\frac{a-1}{2} \equiv \frac{a-5}{2} \bmod 2$.

Now we are going to prove that (a/m) only depends on $m \bmod 4a$ (assuming that the denominator m remains positive); by induction, it suffices to show that $(a/m) = (a/n)$ for $m, n \in \mathbb{N}$ with $m - n = 4a$. Reducing this equation modulo m and n gives $(m/n) = (a/n)$ and $(-n/m) = (a/m)$; thus $(a/m)(a/n) = (m/n)(-n/m)$. But but for positive integers $m \equiv n \bmod 4$, the reciprocity law can be written in the form $(m/n) = (-n/m)$; thus the right hand side equals 1, and this implies the claim.

In particular, $(2/a)$ only depends on $a \bmod 8$, and then the formula $(\frac{2}{a}) = (-1)^{(a^2-1)/8}$ has only to be checked for $a = 1, 3, 5, 7$. □

We have shown that Hypothesis (H) implies the reciprocity law for positive odd integers a, b:

$$\Big(\frac{a}{b}\Big)\Big(\frac{b}{a}\Big) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}. \tag{12.1}$$

Now we show that this formula is still valid if one of the numbers, say b, is negative. In that case, (12.1) shows

$$\Big(\frac{a}{-b}\Big)\Big(\frac{-b}{a}\Big) = (-1)^{\frac{a-1}{2}\cdot\frac{-b-1}{2}}.$$

But $(\frac{a}{-b}) = (\frac{a}{b})$ and $(\frac{-b}{a}) = (-1)^{(a-1)/2}(\frac{b}{a})$, hence we find

$$\Big(\frac{a}{b}\Big)\Big(\frac{b}{a}\Big) = (-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{b+1}{2}} = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

A similar calculation shows that if a and b are both negative, then $(\frac{a}{b})(\frac{b}{a}) = -(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$. We can combine these formulas into a single formula valid for all odd integers as follows:

Theorem 12.7. *Let a and b be odd coprime integers. Then we have*

1. *The quadratic reciprocity law:*

$$\Big(\frac{a}{b}\Big)\Big(\frac{b}{a}\Big) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}+\frac{\operatorname{sgn}(a)-1}{2}\cdot\frac{\operatorname{sgn}(b)-1}{2}}.$$

2. *The supplementary laws:*

$$\Big(\frac{-1}{a}\Big) = (-1)^{\frac{a-1}{2}+\frac{\operatorname{sgn}(a)-1}{2}}, \quad \Big(\frac{2}{a}\Big) = (-1)^{\frac{a^2-1}{2}}.$$

In $\mathbb{Z}$, the correction factors involving the sgn-function are not really essential since for every nonzero $a \in \mathbb{Z}$ there is a unit $\varepsilon = \pm 1$ such that $\varepsilon a > 0$. In general number fields, this is not true in general, and the reciprocity law for totally positive elements is only a special case of the general law.

12.2 Eisenstein's Version of Quadratic Reciprocity

In [RL1, Chapter 4] we have seen how Dirichlet reduced the quadratic reciprocity law in $\mathbb{Z}[i]$ to the one in $\mathbb{Z}$. The same method works for every quadratic number field $K = \mathbb{Q}(\sqrt{m}\,)$, as was shown by Dörrie [18] for quadratic number fields with class number 1, and by Welmin [136] in the general case.

Whereas Welmin stated the quadratic reciprocity law in quadratic number fields as a product formula for Hilbert symbols, our goal here is to provide explicit formulas that are as close to the classical formulation of the quadratic reciprocity law as possible.

Let us now explain the notions of primary and primitive elements. An element $\alpha \in \mathcal{O}_K$ coprime to 2 is called primary if $\alpha \equiv \xi^2 \bmod 4$ for some $\xi \in \mathcal{O}_K$ coprime to 2. From classical results on ramification in Kummer extensions (see [RL1, Thm. 4.12]) it is clear that α is primary if and only if $K(\sqrt{\alpha}\,)/K$ is unramified at the primes above 2. We call $\alpha \in \mathcal{O}_K$ primitive if it is not divisible by any rational prime number. Note that the set of primary elements is closed with respect to multiplication, whereas that of primitive elements is not.

Below we will also need the signature of elements of quadratic number fields K. Let sgn denote the usual sign function; then for $\alpha \in K^\times$ we let α' denote its conjugate, put

$$\operatorname{sign}(\alpha) = \begin{cases} (\operatorname{sgn}\,\alpha,\ \operatorname{sgn}\,\alpha') & \text{if } K \text{ is real,} \\ (+1,+1) & \text{if } K \text{ is complex,} \end{cases}$$

and call it the signature of $\alpha \in K^\times$. In particular, we have $\operatorname{sign}(\alpha) = (+1,+1)$ if and only if α is totally positive. We say that $\alpha \equiv \beta \bmod \infty$ for $\alpha, \beta \in K^\times$ if $\alpha\beta$ is totally positive, that is, if α and β have the same signature.

Before we state the quadratic reciprocity law in quadratic number fields, let us recall the relevant definition: for a prime ideal $\mathfrak{p}$ of odd norm and

some element $\alpha \in \mathcal{O}_K$ coprime to $\mathfrak{p}$, define the quadratic Legendre symbol $[\alpha/\mathfrak{p}] \in \{\pm 1\}$ by the congruence $[\frac{\alpha}{\mathfrak{p}}] \equiv \alpha^{(N\mathfrak{p}-1)/2} \bmod \mathfrak{p}$.

We will now present a version of Eisenstein's quadratic reciprocity law for quadratic number fields:

Theorem 12.8. *Eisenstein's quadratic reciprocity law holds for quadratic number fields $K = \mathbb{Q}(\sqrt{m})$: if $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ have odd norm, and if they satisfy $(\alpha, \beta) = (\gamma, \delta) = (1)$ and $\alpha \equiv \gamma, \beta \equiv \delta \bmod 4\infty$, then*

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] \;=\; \left[\frac{\gamma}{\delta}\right]\left[\frac{\delta}{\gamma}\right].$$

As a corollary we obtain

Corollary 12.9. *If α is primary and totally positive, then $[\frac{\alpha}{\beta}] = [\frac{\beta}{\alpha}]$.*

In fact, in this case we have $\alpha \equiv \xi^2 \bmod 4$ for some ξ coprime to β, and we may simply choose $\gamma = \xi^2$ in Theorem 12.8.

Our proof of Theorem 12.8 will go like this: we will introduce symbols $[\alpha]$ and $\{\alpha\}$ with values in $\{-1, +1\}$and then show

1. $\{\alpha\}$ only depends on the signature of α (Lemma 12.10);
2. $[\alpha]$ only depends on the residue class of α mod 4 (Lemma 12.12);
3. $[\frac{\alpha}{\beta}][\frac{\beta}{\alpha}] = [\alpha][\beta'][\alpha\beta']\{\alpha\}\{\beta'\}\{\alpha\beta'\}$ (Lemma 12.13).

Using this result, Theorem 12.8 follows easily: If $\alpha \equiv \gamma \bmod 4\infty$ and $\beta \equiv \delta \bmod 4\infty$, then $\{\alpha\} = \{\gamma\}$, $\{\beta'\} = \{\delta'\}$ and $\{\alpha\beta'\} = \{\gamma\delta'\}$ by 1), and similarly $[\alpha] = [\gamma]$, $[\beta'] = [\delta']$ and $[\alpha\beta'] = [\gamma\delta']$ by 2). Theorem 12.8 then follows from 3).

Before we start, let us recall the following congruence, which we will use repeatedly: for odd integers r, s we have

$$\frac{r-1}{2} + \frac{s-1}{2} \equiv \frac{rs-1}{2} \bmod 2. \tag{12.2}$$

Signatures and Residue Classes modulo 4

In the following, let $\alpha = a + b\omega$ denote an element in $\mathcal{O}_K$ with odd norm $A = N\alpha$. We will define two symbols $[\alpha]$ and $\{\alpha\}$ with values $\{-1, +1\}$ that only depend on the residue class of $\alpha \bmod 4$ and on the signature $\operatorname{sgn}(\alpha)$, respectively. We start with

$$\{\alpha\} = \begin{cases} (-1)^{\frac{\operatorname{sgn} A-1}{2}\cdot\frac{\operatorname{sgn} b-1}{2}} & \text{if } b \neq 0, \\ 1 & \text{if } b = 0. \end{cases}$$

Note that for complex quadratic fields K, we have $\{\alpha\} = 1$ for all $\alpha \in K^\times$. As an immediate consequence of the definition we obtain the useful observation

$$\{-\alpha\} = (-1)^{\frac{\operatorname{sgn} A-1}{2}}\{\alpha\}. \tag{12.3}$$

Since $\{f\alpha\} = \{\alpha\}$ for integers $f > 0$, this actually shows that

$$\{f\alpha\} = (-1)^{\frac{\operatorname{sgn} A-1}{2}\frac{\operatorname{sgn} f-1}{2}}\{\alpha\} \tag{12.4}$$

for all nonzero integers f.

Now we can prove:

Lemma 12.10. *The value* $\{\alpha\}$ *only depends on the signature* $\operatorname{sign}(\alpha)$.

Proof. This is trivial if $b = 0$, i.e., if $\alpha \in \mathbb{Z}$. Assume therefore that $b \neq 0$. Then the following table shows how $\{\alpha\}$ depends on the signature of α:

$\operatorname{sign}(\alpha)$	$\operatorname{sgn}(A)$	$\operatorname{sgn}(b)$	$\{\alpha\}$
$(+1,+1)$	$+1$	?	$+1$
$(+1,-1)$	-1	$+1$	$+1$
$(-1,+1)$	-1	-1	-1
$(-1,-1)$	$+1$	?	$+1$

(12.5)

If, for example, $\operatorname{sign}(\alpha) = (-1,+1)$, then $a + b\sqrt{m} < 0$ and $a - b\sqrt{m} > 0$ imply that $A = N\alpha = \alpha\alpha' < 0$ and $b < 0$, hence $\{\alpha\} = -1$. □

Next we define a symbol $[\,\cdot\,]$ for nonzero elements in $\mathcal{O}_K$ with odd norm. Observe that any such element can be written in the form $f\alpha$ for some positive odd integer f and a primitive $\alpha = a + b\omega \in \mathcal{O}_K$ with odd norm $A = N\alpha$. Then we put

$$[f\alpha] = \begin{cases} (-1)^{\frac{A-1}{2}\frac{f-1}{2}}\left(\frac{b}{A}\right)\{\alpha\} & \text{if } b \neq 0, \\ 1 & \text{if } b = 0. \end{cases} \tag{12.6}$$

Since $[\alpha] = (\frac{b}{A})\{\alpha\}$ for primitive $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ (just put $f = 1$ in (12.6)), the definition shows that the analog of (12.4) is

$$[f\alpha] = (-1)^{\frac{A-1}{2}\frac{f-1}{2}}[\alpha]. \tag{12.7}$$

Comparing the factors $[f\alpha]/[\alpha]$ and $\{f\alpha\}/\{\alpha\}$ with Theorem 12.7 we see that their product is the inversion factor of $(\frac{f}{A})(\frac{A}{f})$. It seems to me that there is more to (12.4) and (12.7) than meets the eye; in particular it would be nice if we had a more conceptual definition of these factors.

The following result will allow us to evaluate the symbols $[\alpha]$:

Lemma 12.11. *Let* $\alpha = a + b\omega$ *be an element with odd norm* A*, and assume that* $b = 2^r b'$ *for some odd integer* b'*. Then*

$$[\alpha] = (-1)^{\frac{A-1}{2}\frac{b'-1}{2}}\left(\frac{2}{A}\right)^r. \tag{12.8}$$

Proof. Write $\alpha = f\gamma$ for some positive integer f and some primitive $\gamma = c+d\omega$ with $N\gamma = C$. Then, using the general quadratic reciprocity law in $\mathbb{Z}$, we find

$$\begin{aligned}
[\alpha] &= (-1)^{\frac{C-1}{2}\frac{f-1}{2}}\left(\tfrac{d}{C}\right)\{\gamma\} \\
&= (-1)^{\frac{C-1}{2}\frac{f-1}{2}}\left(\tfrac{2}{C}\right)^r\left(\tfrac{d'}{C}\right)(-1)^{\frac{\operatorname{sgn} C-1}{2}\frac{\operatorname{sgn} d'-1}{2}} \\
&= (-1)^{\frac{C-1}{2}\left(\frac{f-1}{2}+\frac{\operatorname{sgn} d'-1}{2}\right)}\left(\tfrac{2}{C}\right)^r \\
&= (-1)^{\frac{A-1}{2}\frac{b'-1}{2}}\left(\tfrac{2}{A}\right)^r,
\end{aligned}$$

where we have used (12.2) and $A = f^2C \equiv C \bmod 8$. □

Now we claim (Skolem [122, Satz 1] proved this in the special case where $\alpha, \beta \in \mathcal{O}_K \setminus \mathbb{Z}$ are primitive):

Lemma 12.12. *The symbol $[\alpha]$ only depends on the residue class of α mod 4: if $\alpha \equiv \beta \bmod 4$ for $\alpha, \beta \in \mathcal{O}_K$ with odd norm, then $[\alpha] = [\beta]$.*

Proof. 1. If $\alpha, \beta \in \mathbb{Z}$, then $[\alpha] = 1 = [\beta]$.

2. Assume that $b \neq 0$ and $d = 0$. Since $\alpha \equiv \pm 1 \bmod 4$ in this case, we must have $r \geq 2$ in the notation of Lemma 12.11. This implies $A \equiv 1 \bmod 8$, hence $[\alpha] = 1$. Since we also have $[\beta] = 1$ by definition, the claim follows.

3. Finally assume that $bd \neq 0$. Write $\alpha = a + b\omega$ and $\beta = c + d\omega$ with odd norms $A = N\alpha$ and $B = N\beta$, and $b = 2^r b'$ and $d = 2^s d'$ for odd integers b', d'. From $\alpha \equiv \beta \bmod 4$ we immediately deduce that $r > 1 \iff s > 1$, and that $r = s$ if $r \leq 1$. Thus we have to consider the following cases:

1. $r, s \geq 2$. Then $A \equiv B \equiv 1 \bmod 8$, hence $[\alpha] = [\beta] = 1$.
2. $r = s = 0$. In this case $\alpha \equiv \beta \bmod 4$ implies $b \equiv d \bmod 4$ and $A \equiv B \bmod 4$, hence $[\alpha] = (-1)^{\frac{A-1}{2}\frac{b-1}{2}}(-1)^{\frac{B-1}{2}\frac{d-1}{2}} = [\beta]$.
3. $r = s = 1$. Here we distinguish some more cases:
   a) $m \equiv 2 \bmod 4$. Then $A \equiv B \equiv 1 \bmod 8$, hence $[\alpha] = [\beta] = 1$.
   b) $m \equiv 3 \bmod 4$. Now $A \equiv B \equiv 5 \bmod 8$, hence $[\alpha] = [\beta] = -1$.
   c) $m \equiv 1 \bmod 4$. Write $m = 4n + 1$; then $\omega + \omega' = 1$ and $\omega\omega' = -n$. Moreover, $A = a^2 + ab - nb^2 \equiv 1 + ab + 4n \bmod 8$ and $B \equiv 1 + cd + 4n \bmod 8$. In particular, $A \equiv B \equiv 3 \bmod 4$, hence $[\alpha] = (\frac{2}{A})(-1)^{(b'-1)/2}$ and $[\beta] = (\frac{2}{B})(-1)^{(d'-1)/2}$.
   Now $A - B \equiv b - d \bmod 8$ shows that $(\frac{2}{A})(\frac{2}{B}) = (-1)^{(b-d)/2} = (-1)^{b'-d'}$. The claim follows.

This completes the proof. □

Reduction to $\mathbb{Z}$

In the following, let m be a squarefree integer and $K = \mathbb{Q}(\sqrt{m}\,)$ a quadratic number field. Let $\{1, \omega\}$ denote the standard integral basis, that is, let $\omega = \sqrt{m}$ if $m \equiv 2, 3 \bmod 4$ and $\omega = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \bmod 4$.

We now want to compute the inversion factor $[\alpha/\beta][\beta/\alpha]$ for coprime primitive elements $\alpha, \beta \in \mathcal{O}_K$ with odd norm.

We start with a few preliminaries that should be familiar from [RL1, Chap. 5]. First we have the congruence

$$d\alpha = ad + bd\omega \equiv ad - bc \bmod \beta. \tag{12.9}$$

Next, $\alpha\beta' = (a + b\omega)(c + d\omega') = ac - ad - bdn - (ad - bc)\omega$, where $n = 0$ if $m \equiv 2, 3 \bmod 4$ and $n = \frac{m-1}{4}$ if $m \equiv 1 \bmod 4$. Thus if we write $\alpha\beta' = e + f\omega$, then (12.9) shows that $d\alpha \equiv -f \bmod \beta$.

We will also use the formulas $\left[\frac{\alpha}{a}\right] = \left(\frac{N\alpha}{a}\right)$ and $\left[\frac{a}{\alpha}\right] = \left(\frac{a}{N\alpha}\right)$ for coprime elements $\alpha \in \mathcal{O}_K$ and $a \in \mathbb{Z}$ with odd norm; here $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol in $\mathbb{Z}$.

The central result of this subsection is

Lemma 12.13. *Assume that $\alpha, \beta \in \mathcal{O}_K$ are coprime elements with odd norms. Then*

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = [\alpha][\beta'][\alpha\beta'\}\{\alpha\}\{\beta'\}\{\alpha\beta'\}. \tag{12.10}$$

Proof. Both sides are trivial if $\alpha, \beta \in \mathbb{Z}$. If $\alpha = a$ and $\beta = c + d\omega$ with $d \neq 0$, then the left hand side of (12.10) is

$$\left[\frac{a}{\beta}\right]\left[\frac{\beta}{a}\right] = \left(\frac{a}{B}\right)\left(\frac{B}{a}\right), \tag{12.11}$$

and, using (12.4) and (12.7), the right hand side can be transformed into

$$[a][\beta'][a\beta'\}\{a\}\{\beta'\}\{a\beta'\} = (-1)^{\frac{a-1}{2}\frac{B-1}{2}}(-1)^{\frac{\operatorname{sgn} a-1}{2}\frac{\operatorname{sgn} B-1}{2}}. \tag{12.12}$$

Now the quadratic reciprocity law 12.7 shows that the right hand sides of (12.11) and (12.12) agree, and the claim follows.

For the rest of the proof we therefore may assume that $bd \neq 0$.

Assume first that β is primitive, i.e., that $\gcd(d, \beta) = \gcd(c, d) = 1$); with $A = N\alpha$,$B = N\beta$ and $\alpha\beta' = e + f\omega$ we find

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{d}{\beta}\right]\left[\frac{d\alpha}{\beta}\right] = \left(\frac{d}{B}\right)\left(\frac{ad - bc}{B}\right) = \left(\frac{-df}{B}\right).$$

A similar calculation shows that

$$\left[\frac{\beta}{\alpha}\right] = \left(\frac{bf}{A}\right)$$

for primitive α, hence

$$\begin{aligned}\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] &= \left(\frac{-df}{B}\right)\left(\frac{bf}{A}\right) = \left(\frac{b}{A}\right)\left(\frac{-d}{B}\right)\left(\frac{f}{AB}\right)\\ &= [\alpha][\beta'][\alpha\beta']\{\alpha\}\{\beta'\}\{\alpha\beta'\}.\end{aligned}$$

This proves the claim for primitive $\alpha, \beta \in \mathcal{O}_K \setminus \mathbb{Z}$.

Finally assume that $\alpha = f\gamma$ and $\beta = g\delta$ for odd positive integers f, g and primitive $\gamma, \delta \in \mathcal{O}_K \setminus \mathbb{Z}$. Using the fact that $[\frac{f}{g}] = 1$ for odd integers f, g, and putting $C = N\gamma$ and $D = N\delta$ we get

$$\begin{aligned}\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] &= \left[\frac{f}{\beta}\right]\left[\frac{\beta}{f}\right]\left[\frac{g}{\alpha}\right]\left[\frac{\alpha}{g}\right]\left[\frac{\gamma}{\delta}\right]\left[\frac{\delta}{\gamma}\right]\\ &= \left(\frac{f}{B}\right)\left(\frac{B}{f}\right)\left(\frac{g}{A}\right)\left(\frac{A}{g}\right)\left[\frac{\gamma}{\delta}\right]\left[\frac{\delta}{\gamma}\right],\end{aligned}$$

and since the claim holds for primitive elements, we deduce

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = \left(\frac{f}{D}\right)\left(\frac{D}{f}\right)\left(\frac{g}{C}\right)\left(\frac{C}{g}\right)[\gamma][\delta'][\gamma\delta']\{\gamma\}\{\delta'\}\{\gamma\delta'\}. \tag{12.13}$$

On the other hand we know that

$$\begin{aligned}[\alpha][\beta'][\alpha\beta'] &= [f\gamma][g\delta'][fg\gamma\delta']\\ &= [\gamma][\delta'][\gamma\delta'](-1)^{\frac{f-1}{2}\frac{C-1}{2}}(-1)^{\frac{g-1}{2}\frac{D-1}{2}}(-1)^{\frac{fg-1}{2}\frac{CD-1}{2}}.\end{aligned}$$

Using (12.2) as well as the fact that f and g are positive we find

$$\begin{aligned}&(-1)^{\frac{f-1}{2}\frac{C-1}{2}}(-1)^{\frac{g-1}{2}\frac{D-1}{2}}(-1)^{\frac{fg-1}{2}\frac{CD-1}{2}}\\ &\quad= (-1)^{\frac{f-1}{2}\frac{C-1}{2}}(-1)^{\frac{g-1}{2}\frac{D-1}{2}}(-1)^{(\frac{f-1}{2}+\frac{g-1}{2})(\frac{C-1}{2}+\frac{D-1}{2})}\\ &\quad= (-1)^{\frac{f-1}{2}\frac{D-1}{2}+\frac{g-1}{2}\frac{C-1}{2}}\\ &\quad= \left(\frac{f}{D}\right)\left(\frac{D}{f}\right)\left(\frac{g}{C}\right)\left(\frac{C}{g}\right),\end{aligned}$$

hence

$$[\alpha][\beta'][\alpha\beta'] = \left(\frac{f}{D}\right)\left(\frac{D}{f}\right)\left(\frac{g}{C}\right)\left(\frac{C}{g}\right)[\gamma][\delta'][\gamma\delta']. \tag{12.14}$$

Since $f, g > 0$ we conclude that $\{\alpha\} = \{\gamma\}$, $\{\beta'\} = \{\delta'\}$ and $\{\alpha\beta'\} = \{\gamma\delta'\}$. Combining this with (12.13) and (12.14) we find

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = [\alpha][\beta'][\alpha\beta']\{\alpha\}\{\beta'\}\{\alpha\beta'\}.$$

This completes the proof. □

12.3 The Weak Quadratic Reciprocity Law

We will now derive various explicit versions of quadratic reciprocity in quadratic number fields. The following formulation gives a weak form of the reciprocity law that has several advantages: it is very similar to the quadratic reciprocity law in $\mathbb{Z}$, and it is easy to guess the correct generalization to arbitrary number fields. A special case was obtained by Hecke [44, 45], but the general form is due to Hasse [41]:

Theorem 12.14. *Let $\alpha, \beta \equiv 1 \bmod 2$ be coprime elements in the maximal order $\mathcal{O}_K$ of a quadratic number field $K = \mathbb{Q}(\sqrt{m})$. Then we have*

1. *The quadratic reciprocity law*

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] \;=\; (-1)^{S+T}, \tag{12.15}$$

   where $S = \frac{\operatorname{sgn}\alpha-1}{2}\frac{\operatorname{sgn}\beta-1}{2} + \frac{\operatorname{sgn}\alpha'-1}{2}\frac{\operatorname{sgn}\beta'-1}{2}$ and $T = \operatorname{Tr}\left(\frac{\alpha-1}{2}\frac{\beta-1}{2}\right)$.

2. *The first supplementary law*

$$\left[\frac{-1}{\alpha}\right] \;=\; (-1)^{U+Tr\,\frac{\alpha-1}{2}}, \tag{12.16}$$

   where $U = \frac{\operatorname{sgn}\alpha-1}{2} + \frac{\operatorname{sgn}\alpha'-1}{2}$.

3. *The second supplementary law*

$$\left[\frac{2}{\alpha}\right] = (-1)^{Tr\,\frac{\alpha^2-1}{8}}. \tag{12.17}$$

Note that this is not the most general quadratic reciprocity law in quadratic number fields: first, in the cases $m \equiv 2, 3 \bmod 4$ the condition $\alpha, \beta \equiv 1 \bmod 2$ is too restrictive since we also would like to know how to invert symbols involving elements congruent to $1+\sqrt{m} \bmod 2$ (if $m \equiv 2 \bmod 4$) or to $\sqrt{m} \bmod 2$ (if $m \equiv 3 \bmod 4$). Second, the supplementary laws should allow us to compute $[\varepsilon/\alpha]$ for the fundamental units of real quadratic fields, as well as $[\alpha/\beta]$ for elements α with even norm.

Corollary 12.15. *If $m \equiv 2, 3 \bmod 4$, then $[\frac{\alpha}{\beta}][\frac{\beta}{\alpha}] = 1$ for all $\alpha \equiv \beta \equiv 1 \bmod 2$ such that α or β is totally positive.*

In fact, the condition $\alpha \equiv \beta \equiv 1 \bmod 2$ guarantees that $T = 0$, and if one of these numbers is totally positive then $S = 0$. Note that this corollary contains e.g. the quadratic reciprocity law in $\mathbb{Z}[i]$ (see [RL1, Sect. 5.1]) as a special case.

For proving the actual reciprocity law in Theorem 12.14 we need to compute the product $\{\alpha\}\{\beta'\}\{\alpha\beta'\}$:

Lemma 12.16. *For nonzero $\alpha, \beta \in K^\times$ we have*

$$\{\alpha\}\{\beta'\}\{\alpha\beta'\} = (-1)^S, \tag{12.18}$$

where

$$S = \frac{\operatorname{sgn}\,\alpha - 1}{2}\frac{\operatorname{sgn}\,\beta - 1}{2} + \frac{\operatorname{sgn}\,\alpha' - 1}{2}\frac{\operatorname{sgn}\,\beta' - 1}{2}.$$

Proof. There are three cases to consider:

1. For $\alpha, \beta \in \mathbb{Z}$, both sides of (12.18) are equal to 1.

2. For $\alpha = a + b\omega$ with $b \neq 0$ and $\beta = c \in \mathbb{Z}$, (12.3) shows that

$$\{\alpha\}\{\beta'\}\{\alpha\beta'\} = (-1)^{\frac{\operatorname{sgn} c - 1}{2}\frac{\operatorname{sgn} A - 1}{2}}.$$

On the other hand we have

$$\begin{aligned} S &= \frac{\operatorname{sgn}\,\alpha - 1}{2}\frac{\operatorname{sgn}\,c - 1}{2} + \frac{\operatorname{sgn}\,\alpha' - 1}{2}\frac{\operatorname{sgn}\,c - 1}{2} \\ &= \frac{\operatorname{sgn}\,c - 1}{2}\Big(\frac{\operatorname{sgn}\,\alpha - 1}{2} + \frac{\operatorname{sgn}\,\alpha' - 1}{2}\Big) \\ &= \frac{\operatorname{sgn}\,c - 1}{2}\frac{\operatorname{sgn}\,A - 1}{2}. \end{aligned}$$

Thus in this case (12.18) also holds.

3. Finally assume that $\alpha = a + b\omega$ and $\beta = c + d\omega$ with $bd \neq 0$. Using table (12.5) we compute both $\{\alpha\}\{\beta'\}\{\alpha\beta'\}$ and $(-1)^S$ as functions of the signatures of α (left column) and β (top row), and find that they agree:

	$(+1,+1)$	$(+1,-1)$	$(-1,+1)$	$(-1,-1)$
$(+1,+1)$	$+1$	$+1$	$+1$	$+1$
$(+1,-1)$	$+1$	-1	$+1$	-1
$(-1,+1)$	$+1$	$+1$	-1	-1
$(-1,-1)$	$+1$	-1	-1	$+1$

This proves the claim. □

Now we can give the

Proof of Theorem 12.14. We know that $[\frac{\alpha}{\beta}][\frac{\beta}{\alpha}] = [\alpha][\beta'][\alpha\beta'][\alpha]\{\beta'\}\{\alpha\beta'\}$, and that $\{\alpha\}\{\beta'\}\{\alpha\beta'\} = (-1)^S$. Thus it remains to show that $[\alpha][\beta'][\alpha\beta'] = (-1)^T$ whenever $\alpha \equiv \beta \equiv 1 \bmod 2$. Since both sides are functions of the residue classes of $\alpha, \beta \bmod 4$, this is a simple (and, for once, quite short) calculation.

In fact, if $m \equiv 2, 3 \bmod 4$, then $\operatorname{Tr}\alpha \equiv 0 \bmod 2$ for any $\alpha \in \mathcal{O}_K$, and if $m \equiv 1 \bmod 4$, than $\operatorname{Tr}\alpha \equiv 0 \bmod 2$ whenever $\alpha \equiv 1 \bmod 2$. Thus we only have to show that $[\alpha][\beta'][\alpha\beta'] = 1$ for all $\alpha \equiv \beta \equiv 1 \bmod 2$.

This is trivial if $m \equiv 2 \bmod 4$, since $[\alpha] = 1$ whenever $2 \mid b$ according to Lemma 12.12.

If m is odd and $\alpha \equiv \pm 1 \bmod 4$, then $[\alpha] = 1$ and $[\alpha\beta'] = [\beta']$, and the claim follows. If $\alpha, \beta \equiv \pm 1 + 2\sqrt{m} \bmod 4$, then $[\alpha] = (\frac{2}{A})$, $[\beta'] = (\frac{2}{B})$ and $[\alpha\beta'] = 1$ since $\alpha\beta' \equiv \pm 1 \bmod 4$. The claim now follows.

It remains to prove the two supplementary laws.

Proof of the First Supplementary Law. We have $[\frac{-1}{\alpha}] = [\frac{-1}{\alpha'}] = [-1][\alpha][-\alpha]\{-1\}\{\alpha\}\{-\alpha\}$. Clearly $[-1] = \{-1\} = 1$, and then (12.3) and (12.7) show that $[\frac{-1}{\alpha}] = (-1)^{\frac{A-1}{2}}(-1)^{\frac{\operatorname{sgn} A-1}{2}}$. But Lemma 12.2 shows that

$$\frac{A-1}{2} \equiv \frac{\alpha-1}{2} + \frac{\alpha'-1}{2} \bmod 2,$$
$$\frac{\operatorname{sgn} A-1}{2} \equiv \frac{\operatorname{sgn} \alpha-1}{2} + \frac{\operatorname{sgn} \alpha'-1}{2} \bmod 2,$$

and from these relations the claim follows.

Proof of the Second Supplementary Law. The second supplementary law will be proved using the fact that $[\frac{2}{\alpha}] = (\frac{2}{A})$; the first supplementary law also can be proved along these lines.

Note first that $[\frac{2}{\alpha}] = (\frac{2}{N\alpha})$. Writing $\alpha = a + b\sqrt{m}$ we get $\operatorname{Tr} \frac{\alpha^2-1}{8} = \frac{a^2+mb^2-1}{4}$. Now we distinguish several cases.

1. $m \equiv 2 \bmod 4$. If b is even, then $N\alpha = a^2 + mb^2 \equiv 1 \bmod 8$ and therefore $[\frac{2}{\alpha}] = 1$; if b is odd, then $N\alpha \equiv \pm 3 \bmod 8$ and $[\frac{2}{\alpha}] = -1$. This shows that $[\frac{2}{\alpha}] = (-1)^{b/2}$ for $\alpha = a + b\sqrt{m}$.
   On the other hand a simple calculation shows $\operatorname{Tr} \frac{\alpha^2-1}{8} = \frac{a^2+mb^2-1}{4} \equiv \frac{b}{2} \bmod 2$. Thus the formula (12.17) holds as soon as $N\alpha$ is odd.
2. $m \equiv 3 \bmod 4$. Since $\alpha = a + b\sqrt{m} \equiv 1 \bmod 2$ we have $2 \mid b$, hence $N\alpha \equiv 1 + b^2 \bmod 8$ and therefore $[\frac{2}{\alpha}] = (-1)^{b/2}$. Again we find $\operatorname{Tr} \frac{\alpha^2-1}{8} = \frac{a^2+mb^2-1}{4} \equiv \frac{b}{2} \bmod 2$. Thus (12.17) holds whenever $\alpha \equiv 1 \bmod 2$.
3. $m \equiv 1 \bmod 4$. Write $\alpha = a + b\sqrt{m} \equiv 1 \bmod 2$. Then a or b is even.
   If b is even, then as above we find $[\frac{2}{\alpha}] = (-1)^{b/2}$ and $\operatorname{Tr} \frac{\alpha^2-1}{8} \equiv \frac{b}{2} \bmod 2$.
   If b is odd, then $[\frac{2}{\alpha}] = (\frac{2}{a^2+m}) = (-1)^{\frac{m-1}{4}+\frac{a}{2}}$, and on the other hand $\operatorname{Tr} \frac{\alpha^2-1}{8} \equiv \frac{m-1}{4} + \frac{a}{2} \bmod 2$.

The proof of (12.17) is now complete. □

12.4 The Strong Quadratic Reciprocity Law

The complete quadratic reciprocity law (except for the supplementary laws) is given by the following

Theorem 12.17. *For any $\alpha \in \mathcal{O}_K$ with odd norm define elements $t_\alpha, t'_\alpha \in \mathbb{Z}/2\mathbb{Z}$ by*

$$\alpha \equiv \begin{cases} \sqrt{m}^{t_\alpha}(1+2\sqrt{m}\,)^{t'_\alpha}\xi^2 \bmod 4 & \text{if } m \equiv 1 \bmod 2, \\ (1+\sqrt{m}\,)^{t_\alpha}(-1)^{t'_\alpha}\xi^2 \bmod 4 & \text{if } m \equiv 0 \bmod 2 \end{cases}$$

for some $\xi \in \mathcal{O}_K$. Then the quadratic reciprocity law for coprime elements of odd norm is given by

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] \;=\; (-1)^{S+T}, \tag{12.19}$$

where S is as in Theorem 12.14 and

$$T \equiv \begin{cases} t_\alpha t'_\beta + t'_\alpha t_\beta + t_\alpha t_\beta \bmod 2 & \text{if } m \equiv 1, 2 \bmod 4, \\ t_\alpha t'_\beta + t'_\alpha t_\beta \bmod 2 & \text{if } m \equiv 3 \bmod 4. \end{cases}$$

The first supplementary law has the form

$$\left[\frac{-1}{\alpha}\right] \;=\; \begin{cases} (-1)^{U+t_\alpha} & \text{if } m \equiv 1, 2 \bmod 4, \\ (-1)^{U} & \text{if } m \equiv 3 \bmod 4, \end{cases}$$

where U is as in Theorem 12.14.

This result (which is modeled after the quadratic reciprocity law in $\mathbb{Z}[i]$ given by Hilbert [51]) clearly implies Theorem 12.8: the condition $\alpha \equiv \gamma \bmod 4$ shows that $t_\alpha = t_\gamma$ and $t'_\alpha = t'_\gamma$, and the fact that $\alpha \equiv \gamma \bmod \infty$ shows that S does not change when α is replaced by γ.

Since we know that $\{\alpha\}\{\beta'\}\{\alpha\beta'\} = (-1)^S$, we only have to show that $[\alpha][\beta'][\alpha\beta'] = (-1)^T$. For slightly simplifying the calculations we introduce the group $M = (\mathcal{O}_K/4\mathcal{O}_K)^\times$. We will see below that the symbol $[\alpha]$ only depends on the coset αM^2. Note that $M/M^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ for every quadratic number field (see Exercise 12.4).

The proof of the reciprocity law in $\mathbb{Q}(\sqrt{m}\,)$ is split up into three cases according to the residue class of m mod 4. In every case, we compute the symbols $[\alpha]$, t_α and t'_α in terms of the cosets αM^2 and then verify (12.19).

***m* ≡ 3 mod 4.** Write $\alpha = a + b\sqrt{m}$ and $A = a^2 - mb^2$. We have to show that $[\alpha][\beta'][\alpha\beta'] = (-1)^T$. To this end, we observe that squares of elements with odd norm are congruent to ± 1 mod 4 in this case; thus the symbols t_α, t'_α are defined by

$$\alpha \equiv \pm\sqrt{m}^{t_\alpha}(1+2\sqrt{m}\,)^{t'_\alpha} \bmod 4. \tag{12.20}$$

We now show that t_α, t'_α and $[\alpha]$, are functions on M/M^2 by computing their values on the residue classes modulo 4:

αM^2	$\alpha \bmod 4$	t_α	t'_α	$[\alpha]$
1	± 1	0	0	$+1$
$1+2\sqrt{m}$	$\pm 1+2\sqrt{m}$	0	1	$+1$
$\sqrt{m}$	$\pm\sqrt{m}$	1	0	$(\frac{2}{1-m})$
$2+\sqrt{m}$	$2\pm\sqrt{m}$	1	1	$-(\frac{2}{1-m})$

In fact, observe that we always have $A \equiv 1 \bmod 4$, hence $[\alpha] = (\frac{2}{A})^r$, where $b = 2^r b'$.

Thus $(-1)^T$, where $T \equiv t_\alpha t'_\beta + t'_\alpha t_\beta \bmod 2$, is a function of the cosets of α modulo M^2. A little calculation shows that $[\alpha][\beta'][\alpha\beta'] = (-1)^T$, the values being given by the following table:

	1	-1	$\sqrt{m}$	$2+\sqrt{m}$
1	$+1$	$+1$	$+1$	$+1$
-1	$+1$	$+1$	-1	-1
$\sqrt{m}$	$+1$	-1	$+1$	-1
$2+\sqrt{m}$	$+1$	-1	-1	$+1$

The first supplementary law $[\frac{-1}{\alpha}] = 1$ is a trivial consequence of these calculations.

Remark. The first supplementary law may be sharpened. The fact that $[\frac{-1}{\alpha}] = 1$ allows us to define the quartic symbol $[-1/\alpha]_4 = (-1)^{(|N\alpha|-1)/4}$. For totally positive α, the following result is easily verified:

Proposition 12.18. *For totally positve $\alpha \in \mathbb{Z}[\sqrt{m}\,]$ with $m \equiv 3 \bmod 4$ we have*

$$\Big[\frac{-1}{\alpha}\Big]_4 = (-1)^T \quad \textit{for} \quad T = \begin{cases} t_\alpha + t'_\alpha & \textit{if } m \equiv 3 \bmod 8, \\ t'_\alpha & \textit{if } m \equiv 7 \bmod 8. \end{cases}$$

$\boldsymbol{m \equiv 2 \bmod 4.}$ Write $\alpha = a + b\sqrt{m}$, put $A = a^2 - mb^2$ and $b = 2^r b'$ for some odd integer b'. Then $[\alpha] = (-1)^{\frac{A-1}{2}\frac{b'-1}{2}}(\frac{2}{A})^r$. The values of $[\alpha]$, as well as the symbols t_α and t'_α defined by

$$\alpha \equiv (1+\sqrt{m}\,)^{t_\alpha}(-1)^{t'_\alpha}\xi^2 \bmod 4 \tag{12.21}$$

again only depend on the cosets αM^2, as the following table shows:

αM^2	$\alpha \bmod 4$	t_α	t'_α	$[\alpha]$
1	$1, 3+2\sqrt{m}$	0	0	$+1$
-1	$-1, 1+2\sqrt{m}$	0	1	$+1$
$1+\sqrt{m}$	$\pm 1+\sqrt{m}$	1	0	$(\frac{2}{1-m})$
$1-\sqrt{m}$	$\pm 1-\sqrt{m}$	1	1	$-(\frac{2}{1-m})$

Using these tablse we compute the products $[\alpha][\beta'][\alpha\beta']$ as well as $(-1)^T$ for $T = t_\alpha t'_\beta + t'_\alpha t_\beta + t_\alpha t_\beta$. We find that both expressions agree; their values are given in the following table:

	1	-1	$1+\sqrt{m}$	$1-\sqrt{m}$
1	$+1$	$+1$	$+1$	$+1$
-1	$+1$	$+1$	-1	-1
$1+\sqrt{m}$	$+1$	-1	-1	$+1$
$1-\sqrt{m}$	$+1$	-1	$+1$	-1

Remark. If $\alpha \equiv 1 \bmod 2$ and $\beta \equiv 1 \bmod (2, \sqrt{m}\,)$, then

$$T \equiv \mathrm{Tr}\left(\frac{\alpha-1}{2\sqrt{m}}\frac{\beta-1}{2}\right) \bmod 2.$$

I have not been able to find a similar (and simple) formula covering all cases $\alpha, \beta \equiv 1 \bmod (2, \sqrt{m}\,)$.

***m* ≡ 1 mod 4.** Write $m = 4n+1$; the cosets αM^2 with odd $A = N\alpha$ contain the following residue classes modulo 4:

αM^2	$2 \mid n$	$2 \nmid n$
1	1	$1,\ n+\omega$
-1	-1	$-1, -n-\omega$
$\sqrt{m}$	$-1+2\omega$	$-1+2\omega, n-\omega$
$-\sqrt{m}$	$1+2\omega$	$1+2\omega, -n+\omega$

The difference is explained by the fact that there is only one coprime residue class modulo 2 if 2 splits (if $m \equiv 1 \bmod 8$, that is, if $2 \mid n$), but three of them if 2 is inert.

Again it is easily checked that t_α, t'_α and $[\alpha]$ only depend on the cosets αM^2:

αM^2	1	-1	$\sqrt{m}$	$-\sqrt{m}$
t_α	0	0	1	1
t'_α	0	1	0	1
$[\alpha]$	1	1	$(\frac{2}{m})$	$-(\frac{2}{m})$

Computing the values of $[\alpha][\beta'][\alpha\beta']$ and $(-1)^T$ gives the following table:

	1	-1	$\sqrt{m}$	$-\sqrt{m}$
1	$+1$	$+1$	$+1$	$+1$
-1	$+1$	$+1$	-1	-1
$\sqrt{m}$	$+1$	-1	-1	$+1$
$-\sqrt{m}$	$+1$	-1	$+1$	-1

This proves the reciprocity law for $m \equiv 1 \bmod 4$. Plugging in $\beta = -1$ gives the first supplementary law $[\frac{-1}{\alpha}] = (-1)^{t_\alpha}$.

12.5 Applications

Let us now see how to apply the explicit formulas in concrete situations.

Scholz's Reciprocity Law

Let $p, q \equiv 1 \bmod 4$ be primes; consider the fields $K = \mathbb{Q}(\sqrt{p})$ and $K' = \mathbb{Q}(\sqrt{q})$, and let ε_p, ε_q and h, h' denote their fundamental units and their class numbers, respectively.

If we assume that $(p/q) = +1$, then $(q) = \mathfrak{q}\mathfrak{q}'$ splits in K and $(p) = \mathfrak{p}\mathfrak{p}'$ splits in K'. We know that $\mathfrak{q}^h$ is principal, and that $\mathfrak{q}^{3h}$ is generated by an element $\alpha \in \mathbb{Z}[\sqrt{p}\,]$. Similarly, $\mathfrak{p}^{3h'} = (\beta)$ for some $\beta \in \mathbb{Z}[\sqrt{q}\,]$.

We want to evaluate the quadratic symbol $(\varepsilon_p/q) = [\varepsilon_p/\mathfrak{q}]$. Since raising this symbol to the power $3h$ does not change its value, we have $(\varepsilon_p/q) = [\varepsilon_p/\beta]$. Finally, replacing ε_p by its cube if necessary allows us to write $\varepsilon_p = t + u\sqrt{p}$ for integers t, u, where clearly t is even.

Write $\beta = c + d\sqrt{p}$. Then d is even, and and we can choose β totally positive. Then since $[\beta/\varepsilon_p] = 1$ the quadratic reciprocity law tells us that

$$\left[\frac{\varepsilon_p}{\beta}\right] = (-1)^T, \quad \text{where } T = \operatorname{Tr} \frac{\varepsilon_p - 1}{2}\frac{\beta - 1}{2}.$$

A simple calculation gives $T = \frac{(t-1)(c-1)+du p}{2} \equiv \frac{c-1}{2} \bmod 2$, hence we get

$$\left[\frac{\varepsilon_p}{\beta}\right] = \left(\frac{-1}{c}\right).$$

Now consider the equation

$$c^2 - pd^2 = q^{3h}. \tag{12.22}$$

Reducing this equation modulo c and applying the quadratic reciprocity law gives $(\frac{-1}{c}) = (\frac{pq}{c}) = (\frac{c}{pq})$. Reducing (12.22) modulo p gives $(\frac{c}{p}) = (\frac{q}{p})_4$, and reducing (12.22) modulo q shows that $(\frac{c}{q}) = (\frac{-1}{q})_4(\frac{p}{q})_4(\frac{d}{q})$. Writing $d = 2^j e$ for some odd integer e we get $(\frac{d}{q}) = (\frac{2}{q})^j(\frac{q}{e}) = (\frac{2}{q})^j$. Now $j = 1$ if and only if $q \equiv 5 \bmod 8$, and this implies $(\frac{2}{q})^j = (\frac{-1}{q})_4$. Collecting everything we find

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4,$$

and this immediately implies Scholz's Reciprocity Law.

Singular Numbers

Let K be a number field. An element $\omega \in K^\times$ is called *singular* if $(\omega) = \mathfrak{c}^2$ is the square of some (fractional) ideal. The set of singular numbers in K modulo squares form a group called the Selmer group:

$$\operatorname{Sel}(K) = \{\omega \in K^\times : (\omega) = \mathfrak{c}^2\}/F^{\times 2}.$$

Lemma 12.19. *Let $\mathfrak{m}$ be an ideal in $\mathcal{O}_K$. Then every class $\omega K^{\times 2} \in \mathrm{Sel}(K)$ can be represented by some ω coprime to $\mathfrak{m}$.*

Proof. Write $(\omega) = \mathfrak{c}^2$ and find an ideal $\mathfrak{b}$ coprime to $\mathfrak{m}$ in the ideal class of $\mathfrak{c}$. Then $\gamma\mathfrak{c} = \mathfrak{b}$ for some $\gamma \in K^\times$, and now $\beta = \omega\gamma^2$ represents the same element in $\mathrm{Sel}(K)$ as ω, and we have $(\beta) = \mathfrak{b}^2$. □

As a corollary we observe

Corollary 12.20. *For singular numbers ω, the quadratic residue symbol $[\frac{\omega}{\alpha}]$ is defined for all $\alpha \in K^\times$ coprime to 2.*

In fact, by Lemma 12.19 there is some $\gamma \in K^\times$ such that $\omega\gamma^2 = \beta$ with β coprime to 2α. Now put $[\frac{\omega}{\alpha}] = [\frac{\beta}{\alpha}]$. It is easily checked that this is well defined.

Let us now introduce the following subgroups of the Selmer group:

$$\begin{aligned}
\mathrm{Sel}^+(K) &= \{\alpha \in K^\times : (\alpha) = \mathfrak{a}^2,\ \alpha \gg 0\}/K^{\times 2},\\
\mathrm{Sel}_4(K) &= \{\alpha \in K^\times : (\alpha) = \mathfrak{a}^2,\ \alpha \equiv \xi^2 \bmod 4\}/K^{\times 2},\\
\mathrm{Sel}_4^+(K) &= \{\alpha \in K^\times : (\alpha) = \mathfrak{a}^2,\ \alpha \equiv \xi^2 \bmod 4,\ \alpha \gg 0\}/K^{\times 2}.
\end{aligned}$$

These subgroups will play a central role in later chapters; here we will only deal with the last group. Note that $\alpha K^{\times 2} \in \mathrm{Sel}_4^+(K)$ if and only if the quadratic extension $K(\sqrt{\alpha})/K$ is unramified everywhere. We now derive another surprising characterization of elements in $\mathrm{Sel}_4^+(F)$, bringing out a connection with quadratic reciprocity:

Theorem 12.21. *Let K be a quadratic number field. Then the following assertions are equivalent:*

1. $\omega K^{\times 2} \in \mathrm{Sel}_4^+(K)$;
2. $[\frac{\omega}{\alpha}] = 1$ *for all* α *coprime to* 2ω

Proof. (1) $\Longrightarrow$ (2): Since $\omega \equiv \xi^2 \bmod 4$ is totally positive, we have $[\frac{\omega}{\alpha}] = [\frac{\alpha}{\omega}]$ by the quadratic reciprocity law. Since ω is singular, we find $[\frac{\alpha}{\omega}] = [\frac{\alpha}{\mathfrak{c}}]^2 = +1$.

(2) $\Longrightarrow$ (1): We first claim that (ω) is an ideal square. Assume not; then we will show that $[\frac{\omega}{\beta}] = -1$ for infinitely many ideals (β).

In fact, write $(\omega) = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ and assume that a_r is odd. Pick a set of prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ different from the $\mathfrak{p}_i$ and with odd norm, and let ν denote a quadratic nonresidue modulo $\mathfrak{p}_r$. Then use the generalized Chinese Remainder Theorem (i.e., the approximation theorem) to find a totally positive element $\beta \in \mathcal{O}_K$ with

$$\begin{aligned}
\beta &\equiv 1 \bmod \mathfrak{q}_1 \cdots \mathfrak{q}_s,\\
\beta &\equiv 1 \bmod 4,\\
\beta &\equiv 1 \bmod \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1},\\
\beta &\equiv \nu \bmod \mathfrak{p}_r.
\end{aligned}$$

Then $[\frac{\beta}{\omega}] = \prod [\frac{\beta}{\mathfrak{p}_i}]^{a_i} = [\frac{\beta}{\mathfrak{p}_r}] = -1$; on the other hand, the reciprocity law for primary elements implies that $[\frac{\omega}{\beta}] = [\frac{\beta}{\omega}] = -1$.

Now use Cor. 12.20 to make ω coprime to 2. Then we claim that $\omega \equiv \xi^2 \bmod 4$. If not, then an inspection of the tables giving the inversion factors shows that there is some residue class $\tau \bmod 4$ such that for all totally positive $\beta \in \mathcal{O}_K$ coprime to 2α and with $\beta \equiv \tau \bmod 4$ we have $[\frac{\omega}{\beta}] = -[\frac{\beta}{\omega}]$. Now choose such a β with $\beta \equiv 1 \bmod \omega$. Then $[\frac{\omega}{\beta}] = -[\frac{\beta}{\omega}] = -1$.

Finally we show that ω is totally positive. If not, then there is some signature σ such that for every $\beta \equiv 1 \bmod 4$ and $\operatorname{sign}(\beta) = \sigma$ we have $[\frac{\omega}{\beta}] = -[\frac{\beta}{\omega}]$. Choosing such a β with the additional property $\beta \equiv 1 \bmod \omega$ then leads to a contradiction as above. □

Notes

The first mathematician who came up with a quadratic reciprocity law in a number field different from $\mathbb{Q}$ was Gauss: he discovered and proved the quadratic reciprocity law in $\mathbb{Z}[i]$ (see [RL1, Section 5.1]); a simpler proof was later given by Dirichlet. Next came Eisenstein's quadratic (actually sextic) reciprocity law in $\mathbb{Z}[\zeta_3]$ ([RL1, Section 7.3]). As we have seen in [RL1, Sections 6.5, 9.4], Goldscheider [37] proved the quadratic (as well as quartic and octic) reciprocity law in $\mathbb{Z}[\zeta_8]$. In 1892, Bonaventura [13] derived the quadratic reciprocity law in $\mathbb{Z}[\sqrt{-2}\,]$. In his 1898 dissertation, Dörrie [18] used Dirichlet's technique to derive the quadratic reciprocity law in quadratic fields with class number 1, and in 1902 Rückle [111] and K.S. Hilbert [57] studied the product formula for quadratic Hilbert symbols in algebraic number fields, in particular in $\mathbb{Z}[\zeta_{2^n}]$. Welmin [136] finally used Dirichlet's method to derive the quadratic reciprocity law in arbitrary quadratic number fields from the one in rational integers. The possibility of such a proof was realized independently by Hecke [43, footnote 2, p. 28], who derived the quadratic reciprocity law in real quadratic number fields using generalized Gauss sums. Hecke also proved the following version of the second supplementary law:

Theorem 12.22. *Let k be a real quadratic number field, let $\mathfrak{l}_1$ and $\mathfrak{l}_2$ be prime ideals above 2, and let $\lambda \in \mathcal{O}_k$ be an algebraic integer with $(\lambda) = \mathfrak{l}_1^{a_1}\mathfrak{l}_2^{a_2}$ (put $a_2 = 0$ if there is only one prime ideal above 2 in k). Assume that*

$$\lambda \equiv \xi^2 \bmod \begin{cases} 4 & \text{if } a_1 \equiv a_2 \equiv 0 \bmod 2, \\ 4\mathfrak{l}_1 & \text{if } a_1 \equiv 1,\ a_2 \equiv 0 \bmod 2, \\ 4\mathfrak{l}_2 & \text{if } a_1 \equiv 0,\ a_2 \equiv 1 \bmod 2, \\ 4\mathfrak{l}_1\mathfrak{l}_2 & \text{if } a_1 \equiv\ a_2 \equiv 1 \bmod 2. \end{cases}$$

Then

$$\Big(\frac{\lambda}{\alpha}\Big) = (-1)^S, \qquad S = \frac{\operatorname{sgn}\,\alpha - 1}{2}\frac{\operatorname{sgn}\,\lambda - 1}{2} + \frac{\operatorname{sgn}\,\alpha' - 1}{2}\frac{\operatorname{sgn}\,\lambda' - 1}{2}.$$

Our discussion of quadratic reciprocity in quadratic number fields is loosely based on Skolem's approach in [122]; Skolem rediscovered and then simplified Welmin's results, and was able to see how to generalize Dirichlet's technique to arbitrary number fields; in practice, however, this method will be far too technical for deriving explicit quadratic reciprocity laws in number fields of degree > 2.

Eisenstein's way of formulating the quadratic reciprocity law (see Hypothesis (H) on p. 1, and Theorem 12.8) goes back to [23], where the case of odd primes ℓ is discussed. Eisenstein does not deal with quadratic reciprocity there, but he was aware of its exceptional status; [21, p. 619], he writes:

> dieses bildet übrigens hier einen Ausnahmefall, da der Unterschied zwischen pos. und neg. Zahlen nicht durch Congruenzen dargestellt werden kann.[1]

This problem was later overcome by Hilbert and Furtwängler, who invented infinite primes in order to simplify statements in class field theory; Hasse then introduced congruences modulo infinite primes and was thus able to express the "difference between positive and negative numbers" by such congruences.

E.F. Stueben also has studied quadratic reciprocity in quadratic fields, but his publication [126] was not available to me.

The explicit quadratic reciprocity laws given in this chapter do certainly not exhaust the subject, and there are lots of problems remaining to be solved. Consider e.g. a quadratic number field K, let $\mathfrak{2}$ denote a prime ideal above 2, and let $\mathfrak{a}$ and $\mathfrak{b}$ denote ideals of odd norm in the ideal class $[\mathfrak{2}]^{-1}$. Then $\mathfrak{2a} = (\alpha)$ and $\mathfrak{2b} = (\beta)$ for $\alpha, \beta \in \mathcal{O}_K$, and we may ask when $[\frac{\alpha}{\mathfrak{q}}][\frac{\beta}{\mathfrak{p}}]$ is independent of the choices of α and β, and what its value is.

Exercises

12.1 Assume that $(2/A)$ only depends on $A \bmod 2^\sigma$ for some integer σ, and show that this implies that that we can take $\sigma = 3$.

12.2 Let K/k be a quadratic extension. Show that the set of primitive elements does not form a monoid. Prove that if α and β are primitive and coprime, then so are $\alpha\beta'$ and $\alpha'\beta$.

12.3 Show that $\{\alpha\}\{\alpha'\} = \operatorname{sgn} A$.

12.4 Let K be an algebraic number field of degree n, let $\mathcal{O}$ denote the ring of integers in K, and put $M = (\mathcal{O}/4\mathcal{O})^\times$. Show that squaring induces an exact sequence

$$1 \longrightarrow M[2] \longrightarrow M \longrightarrow M^2 \longrightarrow 1,$$

where $M[2] = \alpha \in M : \alpha^2 = 1$. Next show that $\beta + 2\mathcal{O} \longmapsto 1 + 2\beta + 4\mathcal{O}$ defines an isomorphism $\mathcal{O}/2\mathcal{O} \longrightarrow M[2]$. Finally, use an integral basis to prove that $\mathcal{O}/2\mathcal{O} \simeq (\mathbb{Z}/2\mathbb{Z})^n$, and deduce that this implies $M/M^2 \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

[1] this forms an exception here, since the difference between pos[itive] and neg[ative] numbers cannot be represented by congruences.

12.5 Let $k = \mathbb{Q}(\sqrt{m}\,)$ be a quadratic number field, and assume that $\alpha \in \mathcal{O}_k$ satisfies $\alpha \equiv 1 \bmod 2$. Show that $\frac{N\alpha-1}{2} \equiv \operatorname{Tr} \frac{\alpha-1}{2} \bmod 2$.

12.6 (continued) Deduce from the preceding exercises that, for totally positive $\alpha \equiv 1 \bmod 2$, we have $[\frac{-1}{\alpha}] = (-1)^T$, where $T = \operatorname{Tr} \frac{\alpha-1}{2}$. Deduce that $[\frac{-1}{\alpha}]$ only depends on the residue class $\alpha \bmod 4$ (as long as α is totally positive).

12.7 Consider the quadratic number field $k = \mathbb{Q}(\sqrt{m}\,)$ with $m \equiv 2, 3 \bmod 4$, and let $\mathfrak{l}$ denote the prime ideal above 2 (thus $\mathfrak{l} = (2, \sqrt{m}\,)$ if $m \equiv 2 \bmod 4$, and $\mathfrak{l} = (2, 1 + \sqrt{m}\,)$ if $m \equiv 3 \bmod 4$). Show that $T = \operatorname{Tr}(\frac{\alpha-1}{2}\frac{\beta-1}{2}) \in \mathbb{Z}$ whenever $\alpha \equiv \beta \equiv 1 \bmod \mathfrak{l}$, and that the formula $(\alpha/\beta)(\beta/\alpha) = (-1)^T$ for the quadratic reciprocity law that we have proved for totally positive $\alpha \equiv \beta \equiv 1 \bmod 2$ does not hold in general under the weaker assumption $\alpha \equiv \beta \equiv 1 \bmod \mathfrak{l}$.

12.8 For $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}\,]$ with $\alpha \equiv 1 \bmod 2$, show that $[\sqrt{2}/\alpha] = (-2/a)$.
Hints: Use (12.15) to show that $[\frac{\sqrt{2}}{\alpha}] = [\frac{2\sqrt{2}}{\alpha}] = [\frac{\alpha+2\sqrt{2}}{\alpha}] = [\frac{\alpha}{\alpha+2\sqrt{2}}] = \frac{\sqrt{2}}{\alpha+2\sqrt{2}}]$. Now observe that $\alpha \equiv a \bmod 2\sqrt{2}$.

12.9 Prove the following version of the second supplementary law in $\mathbb{Z}[\sqrt{m}\,]$ for $m \equiv 3 \bmod 4$: Let $\lambda \in \mathbb{Z}[\sqrt{m}\,]$ be an element of norm 2^n; for $\alpha \in \mathbb{Z}[\sqrt{m}\,]$ with odd positive norm and $\alpha \equiv 1 \bmod 4$ we have

$$\left[\frac{\lambda}{\alpha}\right] = \begin{cases} +1 & \text{if } \alpha \equiv \xi^2 \bmod 4\mathfrak{l}, \\ -1 & \text{if } \alpha \not\equiv \xi^2 \bmod 4\mathfrak{l}, \end{cases}$$

where $\mathfrak{l} = (2, 1 + \sqrt{m}\,)$ is the prime ideal of norm 2.

Hints: write $\lambda = r + s\sqrt{m}$ and $\alpha = a + b\sqrt{m}$ with $r \equiv s \equiv a \equiv 1 \bmod 2$ and $4 \mid b$.

1. Show that $(\frac{b}{N\alpha}) = (\frac{2}{N\alpha})$.
2. Show that $[\frac{\lambda}{\alpha}] = (\frac{2}{N\alpha})(\frac{rb-sa}{N\alpha})$.
3. Use quadratic reciprocity in $\mathbb{Z}$ to show that $(\frac{rb-sa}{N\alpha}) = (\frac{2}{rb-sa})$.

12.10 Derive the quartic reciprocity law in $\mathbb{Z}[i]$ from Eisenstein's hypothesis (E) for prime powers.

12.11 Derive the second supplementary law for quartic residues from the quartic reciprocity law in $\mathbb{Z}[i]$.

12.12 Let k be a number field, let ∞ denote the product of all real places, and let $2\mathcal{O}_k = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_r^{e_r}$ be the prime ideal factorization of 2. Show that if an element $\alpha \in \mathcal{O}_k$ coprime to 2 is a square modulo $\mathfrak{l}_i^{2e_i+1}$, then it is a square modulo $\mathfrak{l}_i^r$ for all $r \geq 1$.

12.13 Let k be a number field, let ∞ denote the product of all real places, and let $2\mathcal{O}_k = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_r^{e_r}$ be the prime ideal factorization of 2. If Eisenstein's quadratic reciprocity law holds modulo $\mathfrak{m}\infty$ in k, where $\mathfrak{m}$ is a product of powers of prime ideals dividing (2), then it holds modulo $4\mathfrak{l}_1 \cdots \mathfrak{l}_r\infty$.

12.14 Let k be a number field with class number 1; show that if Eisenstein's quadratic reciprocity law holds in k, then it holds in any quadratic extension K of k.

12.15 Consider the ring $\mathcal{O}_K = \mathbb{Z}[\omega]$ of algebraic integers in the cubic number field $K = \mathbb{Q}(\omega)$, where $\omega^3 = 2$; its fundamental unit is $\varepsilon = \omega - 1$.

1. Compute $[\frac{\varepsilon}{\pi}]$ for the primes $\pi = 1 + \omega$ and $\pi = 1 + \omega^2$;
2. Assuming that Eisenstein's quadratic reciprocity law holds in K, show that $[\frac{\varepsilon}{\pi}]$ only depends on the residue class $\pi \bmod 4\mathcal{O}_K$ if $N\pi > 0$;

3. Show that any element in $\mathcal{O}_K$ with odd norm is associated to an element of the form $a + b\omega + c\omega^2$, where $a - 1 \equiv b \equiv 0 \bmod 4$ and $c \equiv 0 \bmod 2$.
4. Prove that $[\frac{\varepsilon}{\pi}] = (-1)^{c/2}$, where $\pi = a+b\omega+c\omega^2$ and $a-1 \equiv b \equiv 0 \bmod 4$, $c \equiv 0 \bmod 2$.

This result is due to Aigner [3].

12.16 Assume that in the cubic number field $K = \mathbb{Q}(\omega)$ with $\omega^3 = 2$ we have the reciprocity law

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = (-1)^{\mathrm{Tr}\,\frac{\alpha-1}{2}\,\frac{\beta-1}{2}}$$

for all (totally) positive $\alpha, \beta \in \mathbb{Z}[\omega]$. Show that this implies the result of the preceding exercise.

12.17 Prove the following analog of Theorem 12.21:
Let K be a quadratic number field. Then the following assertions are equivalent:

1. $\omega {K^\times}^2 \in \mathrm{Sel}_4(K)$;
2. $[\frac{\omega}{\alpha}] = 1$ for all totally positive α coprime to 2ω

12.18 (continued) Find an analog of Theorem 12.21 involving $\mathrm{Sel}^+(K)$ and prove it.