Abstract

Fix an integer $m > 2$ and let K be a number field containing the mth roots of unity with ring of integers R. Suppose that a is an element of K with $a = c/d$ for $c, d \in R$, and that $\mathfrak{b}$ is an ideal of R relatively prime to mR, cR, and dR. We define the mth power residue symbol $\left(\frac{a}{\mathfrak{b}}\right)$ and, using a method outlined by H. W. Lenstra, Jr., describe an algorithm for its computation. The algorithm has a running time that is polynomial in the input size when m is fixed but not when m is allowed to vary.

Acknowledgements

It is a pleasure to thank the many people who assisted me with this project.

First, of course, are members of the Reed College mathematics department. I learned an enormous amount about mathematics and the rest of life from my good friend Jerry Shurman. David Perkinson provided a humorous outlook and lots of encouragement at difficult times. And the entire department always made me feel welcome, especially in its collective effort to assist me in a return to school after several years away.

My family, the Buckleys, deserve special thanks as well. They have always been willing to allow me to proceed in my own direction at my own pace, even when my choices seemed less than wise to them. I would have been a much less happy mathematician without this freedom.

Among my many, many friends, I can name Trisha Pancio, Christina Holzer, Missy Rohs, Kristian Williams, Dan Handelman, Darcy Lyon, Jodi Benotovich, Sam Bean, and Hallie Hargrave as those who have done the most to assist me throughout my years at Reed and in Portland.

In a few lines at the end of his paper on the quadratic residue symbol, Hendrik Lenstra posed the problem of computing general mth power residue symbols and outlined a solution. I thank him for this inspiration as well as a very helpful conversation in which he found several errors and clarified many issues for me.

Finally, I must thank Joe Buhler, my thesis adviser. Work of any quality that may be found in this thesis must fall into one of two categories. Either it is my attempt to record one of Joe's many very patient explanations of his ideas, or else it is inspired by his piercingly clear lecture style and astonishing energy and creativity. I am grateful to have had the opportunity to work with him.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

ACKNOWLEDGEMENTS

This thesis was typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX, the TEX macro system of the American Mathematical Society. It was brought to you by the letter N and the number 8.

CONTENTS

CHAPTER I

BACKGROUND

In this chapter we present basic definitions and results for lattices and number fields. We often refer the reader to the literature for proofs of our statements.

1. Lattices

DEFINITION. If n is a positive integer, then a *lattice of rank* n is the set

$$\{\sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{Z}\}$$

where $x_1, \ldots, x_n$ form a basis of $\mathbb{R}^n$.

Note that there are many ways to define a lattice (see [4, p. 78] for some of them) but this simple one is all we will need. Observe that any lattice is isomorphic to $\mathbb{Z}^n$ and that any group G isomorphic to $\mathbb{Z}^n$ may be considered a lattice of rank n in a trivial way, since $\mathbb{Z}^n \subset \mathbb{R}^n$.

DEFINITION. A *basis* for a lattice L of rank n is an $\mathbb{R}$-linearly independent set in L which generates L additively.

Clearly any basis of a lattice of rank n has n elements.

The following lemma is an exercise in Marcus [13, p. 44].

LEMMA 1.1. *If L is a lattice of rank n and G is a subgroup contained in L, then G is a lattice of rank k where $k \leq n$.*

PROOF. We proceed by induction on n. The case $n = 1$ is obvious, so fix an integer $n > 1$ and assume that the lemma is proved for $n - 1$. Fix a lattice L of rank n and a subgroup G; identify L with $\mathbb{Z}^n$. Let $\pi : \mathbb{Z}^n \to \mathbb{Z}$ be the homomorphism defined by

$$\pi(a_1, \ldots, a_n) = a_1$$

for any integer n-tuple $(a_1, \ldots, a_n)$. Let $G' = G \cap \ker \pi$.

Clearly $\ker \pi$ is isomorphic to $\mathbb{Z}^{n-1}$ and thus by induction assumption the subgroup G' is a lattice of rank $\leq n-1$. If $\pi(G) = \{0\}$ then G is isomorphic to G' and we are done. If on the other hand $\pi(G) \neq \{0\}$, then $\pi(G) = t\mathbb{Z}$ for some $t \in \mathbb{Z}$, since all subgroups of $\mathbb{Z}$ are cyclic. Fix $h \in G$ such that $\pi(h) = t$. Then fix $g = (a_1, \ldots, a_n) \in G$. Clearly $a_1 = jt$ for some $j \in \mathbb{Z}$. It follows that $g' = g - jh \in G'$, so that $g = jh + g'$. Further, if $jh + g' = 0$ for some $j \in \mathbb{Z}$ and some $g' \in G'$, then $0 = \pi(jh + g') = jt$ so $j = 0$ and $g' = 0$. We have shown that G is isomorphic to $t\mathbb{Z} \oplus G'$ and this is obviously isomorphic to $\mathbb{Z}^n$. $\square$

Suppose that L and L' are lattices of rank n, X is a subgroup of L, and $L' \subset X \subset L$. Then an easy corollary of Lemma 1.1 is that X must be a lattice of rank n.

The Determinant and the LLL Algorithm. We have not yet made use of the fact that a lattice L of rank n is a subset of $\mathbb{R}^n$. In fact we shall usually ignore this inclusion and treat a lattice only as a free abelian group with n generators. However, we will sometimes want to use the fact that $L \subset \mathbb{R}^n$, for example to compute short vectors in a lattice, and we now explain how to do this.

For the whole subsection, we fix a lattice L of rank n. Let $v_1, \ldots, v_n$ be a basis of L. Let B be the matrix whose jth column is the real n-tuple v_j. The *determinant* $\det L$ of the lattice L is the absolute value of the determinant of the matrix B. The following proposition, which is an exercise in Marcus ([13, p. 146]), shows that $\det L$ is well-defined.

PROPOSITION 1.2. *The quantity* $\det L$ *does not depend on the choice of basis of* L.

PROOF. Suppose that $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ are two bases of L. Let B, resp. B', be the n by n real matrix whose jth column is v_j, resp. w_j. Clearly neither $\det B$ nor $\det B'$ is zero.

We may write $B = B'M$ for some n by n integer matrix M. Taking determinants of both sides we obtain $\det B = (\det B')(\det M)$, so $\det B$ is an integer multiple of $\det B'$. If we interchange the roles of the v_i and the w_i, we see that $\det B'$ is an integer multiple of B also, so that $\det B = \pm \det B'$. $\square$

If L' is a lattice of rank n containing L, then

$$\det L = (\det L')|L'/L|.$$

In particular, when $L' = \mathbb{Z}^n$, $\det L = |\mathbb{Z}^n/L|$. See [13, p. 135].

A *fundamental parallelotope* of L is a set of the form

$$\left\{ \sum_{i=1}^{n} a_i v_i \mid a_i \in \mathbb{R}, 0 \leq a_i < 1 \right\}$$

where $v_1, \ldots, v_n$ forms a basis of L. Of course the fundamental parallelotope depends on the basis chosen for L. If L' is a lattice of rank n containing L and P is a fundamental parallelotope of L, then $L' \cap P$ forms a set of coset representatives for L'/L.

As a subset of $\mathbb{R}^n$, the lattice L inherits a norm $\| \cdot \|$. We will want to find a vector x in L with $\|x\|$ small. This can be done using the LLL algorithm, named for its inventors A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. The LLL algorithm runs in polynomial time (see below for a definition) and finds $x \in L$ such that

$$\|x\| \leq \delta (\det L)^{1/n}$$

where δ is a positive real constant. (The algorithm actually finds an entire basis of L, each of whose elements have bounded absolute value.) The quantity δ depends on n but not on the lattice L. In fact, in the original LLL algorithm we can take

$$\delta = \left(\frac{1}{\alpha - 1/4} \right)^{(n-1)/4}$$

where α is a real-valued parameter with $1/4 < \alpha < 1$ (a larger choice of α gives a smaller basis but makes the algorithm slower). The value of δ has been subsequently improved in various ways but it remains exponential in n. See the original LLL paper [10]; also see [4, pp. 83–96] for an implementation of the algorithm and several improvements.

Hermite and Smith Normal Forms. For this entire subsection, let L be a lattice of rank n in $\mathbb{Z}^n$ and let $v_1, \ldots, v_n$ be a basis of L. Write the v_i as the columns of an n by n integer matrix B. Changing the basis of L corresponds to applying elementary column operations to B or, equivalently, multiplying B on the right by a unimodular matrix P. As is well known from linear algebra, we can find a basis of L such that the corresponding matrix is upper triangular.

In fact, we can do a little better, and find a canonical basis. There exists an n by n integer matrix $B' = (b'_{ij})$, called the *Hermite normal form of* B or *HNF of* B for short, which satisfies the following conditions.

(1) $B' = BP$ for some unimodular matrix P (or in other words, B' can be obtained from B by elementary column operations).
(2) B' is upper triangular.
(3) For $i = 1, 2, \ldots, n$, we have $b'_{ii} > 0$.
(4) For every $j > i$ we have $0 \leq b'_{ij} < b'_{ii}$.

The matrix B' is uniquely determined by B and therefore by L; its columns give a basis of L called the *HNF basis of* L.

In fact, the HNF is defined for any n by k matrix B. B' is again obtained from B by elementary column operations. If $k \geq n$, which is the only case we will be interested in, then the first $k - n$ columns of B' are 0 and the matrix formed by the last n columns of B' satisfies conditions (2)–(4) above. We can use this, for example, to find the HNF of a lattice generated by k vectors. See [4, pp. 66–74] for algorithms to compute the HNF.

We will also want to study the finite abelian group $G = \mathbb{Z}^n/L$ (every finite abelian group can be given in this form). Writing a basis of L in the columns of an n by n integer matrix B and performing both row and column operations on B, we obtain an n by n integer matrix $B' = (b'_{ij})$ called the *Smith normal form* or SNF of B such that

(1) B' is diagonal, that is $b'_{ij} = 0$ unless $i = j$, and
(2) we have $b'_{ii} \mid b'_{jj}$ whenever $j > i$.

The row operations correspond to a change of basis for $\mathbb{Z}^n$ and the column operations to a change of basis for L. Thus if L' is the lattice generated by the columns of B' then $\mathbb{Z}^n/L \cong \mathbb{Z}^n/L'$. See [4, pp. 74–78] for algorithms that compute the SNF.

2. Number Fields

In much of what we discuss in this section we follow Marcus [13]. See Cohen [4] for the properties of orders and Cassels [2] or Cassels and Fröhlich [3] for completions.

Definition. If $z \in \mathbb{C}$ and z is the root of a monic polynomial with coefficients in $\mathbb{Q}$, we say that z is an *algebraic number*. If z is the root of a monic polynomial with coefficients in $\mathbb{Z}$, we say that z is an *algebraic integer*.

The *conjugates* of an algebraic number are the roots of its minimal polynomial. Let z be an algebraic number with minimal polynomial f

and suppose that z is a repeated root of f. Write $f(X) = (X - z')g(X)$. Then z is also a root of $g(X)$ and $f'(X) = g(X) + (X - z')g'(X)$ so that $f'(z) = 0$. This is a contradiction since $\deg f' < \deg f$ and f is the minimal polynomial of z. We have shown that the minimal polynomial f cannot have repeated roots, and so z has exactly $\deg f$ conjugates.

DEFINITION. A field K is a *number field* if it has finite degree as a vector space over $\mathbb{Q}$.

Any number field K is isomorphic to $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$ (see [13, pp. 259–260]). The *degree* of the field K is its degree as a vector space over $\mathbb{Q}$, which is the same as the degree of the minimal polynomial of α. If n is the degree of K then there are exactly n embeddings of K in $\mathbb{C}$, each one mapping α to one of its conjugates. It is easy to see that any element of $\mathbb{Q}(\alpha)$ has a minimal polynomial of degree $\leq n$.

For the remainder of the chapter we fix a number field K of degree n.

Two important functions on K are the *trace* and the *norm*, denoted $\mathrm{Tr}^K(x)$ and $N^K(x)$ respectively. (When the field is clear from context we will simply write $\mathrm{Tr}(x)$ and $N(x)$.) Let K have degree n and let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of K in $\mathbb{C}$. For any $x \in K$, we set

$$\mathrm{Tr}^K(x) = \sum_{i=1}^{n} \sigma_i(x), \quad N^K(x) = \prod_{i=1}^{n} \sigma_i(x).$$

It is not hard to see that $\mathrm{Tr}^K(x + y) = \mathrm{Tr}^K(x) + \mathrm{Tr}^K(y)$ and $N^K(xy) = N^K(x)N^K(y)$ for any x and y in K. Also, if $r \in \mathbb{Q}$ and $x \in K$ then $\mathrm{Tr}^K(rx) = r\,\mathrm{Tr}(x)$ and $N^K(rx) = r^n N^K(x)$.

Fix $x \in K$ and let f be its minimal polynomial over $\mathbb{Q}$. Let k be the degree of f and let $\tau_1, \ldots, \tau_k$ be the k distinct embeddings of $\mathbb{Q}(x)$ in $\mathbb{C}$. Each τ lifts to exactly n/k embeddings of K in $\mathbb{C}$ (see [13, p. 259]) and so

$$\mathrm{Tr}^K(x) = \frac{n}{k} \sum_{i=1}^{n} \tau_i(x), \quad N^K(x) = \left(\prod_{i=1}^{n} \tau_i(x) \right)^{n/k}.$$

Observe that $n/k = [K : \mathbb{Q}(x)] \in \mathbb{Z}$. Writing

$$f(X) = a_0 + a_1 X + \cdots + a_{k-1} X^{k-1} + X^k$$

with the a_i in $\mathbb{Q}$ and observing that

$$\sum_{i=1}^{n} \tau_i(x) = -a_{k-1}, \quad \prod_{i=1}^{n} \tau_i(x) = \pm a_0,$$

we see that the trace and norm map K into $\mathbb{Q}$.

Note that our notions of trace and norm are often called the *absolute* trace and norm respectively, to distinguish them from the *relative* trace and norm $\mathrm{Tr}_K^{K'}(x)$ and $N_K^{K'}(x)$ which map an extension K' into K. We will not need the relative trace and norm.

A very important example of a number field is the *cyclotomic field* $\mathbb{Q}(\zeta)$. For any positive integer t, let $\phi(t)$ be the number of positive integers less than t and relatively prime to t (ϕ is called the *Euler phi function*). Then the degree of $\mathbb{Q}(\zeta)$ is $\phi(m)$; see [13, p. 15] for a proof of this.

Ring of Integers, Orders, and Ideals.

DEFINITION. The *ring of integers* R of K is the set of all elements of K which are algebraic integers over $\mathbb{Q}$.

For example, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$ (see [13, p. 35] for the proof). If α is an algebraic integer then the ring $\mathbb{Z}[\alpha]$ is an order in the number field $K = \mathbb{Q}(\alpha)$ (see below) but $\mathbb{Z}[\alpha]$ is not necessarily the full ring of integers.

We list several properties of R. Clearly $\mathbb{Z} \subset R$. As an additive group, R is isomorphic to $\mathbb{Z}^n$; a $\mathbb{Z}$-basis of R is called an *integral basis* of R. If $x \in K$ then there exists a $d \in \mathbb{Z}$ such that $dx \in R$. Thus K is the field of fractions of R. It is easy to see that the trace and norm map R into $\mathbb{Z}$.

If $\mathfrak{a}$ is an ideal of R generated over R by $a_1, \ldots, a_k$, we write $\mathfrak{a} = (a_1, \ldots, a_k)$ (there will be no confusion with the same notation for vectors since the a_i lie in R). If $a_1, \ldots, a_k$ generate $\mathfrak{a}$ over $\mathbb{Z}$ then we write $\mathfrak{a} = (a_1, \ldots, a_k)_{\mathbb{Z}}$.

Ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R may be added, intersected, or multiplied, the result in each case being another ideal of R. We have

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\},$$
$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

The product of two ideals is a subset of both. If $\mathfrak{a}$, $\mathfrak{b}$ are ideals of R with $\mathfrak{a} \subset \mathfrak{b}$, then there is an ideal $\mathfrak{c}$ of R such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.

A *prime ideal* $\mathfrak{p}$ in R is an ideal for which the quotient $R/\mathfrak{p}$ is an integral domain. The *norm* of an ideal $\mathfrak{b}$ in R, denoted $N(\mathfrak{b})$, is $|R/\mathfrak{b}|$. Note that if $x \in R$ then $N(xR) = |N^K(x)|$, and if $\mathfrak{b}$ and $\mathfrak{c}$ are ideals in R then $N(\mathfrak{b}\mathfrak{c}) = N(\mathfrak{b})N(\mathfrak{c})$ (see [13, p. 66]).

Every ideal in the ring of integers R can be written in a unique way as the product of prime ideals. See [13, p. 56] for a proof of this fact. The sum of two ideals of R is their greatest common divisor and their intersection is their least common multiple, where these have the obvious meanings.

DEFINITION. An *order* A in R is a subring of R whose additive group is isomorphic to $\mathbb{Z}^n$.

Just as for the full ring of integers R, we may define for an order A the set of prime ideals, the sum and product of two ideals, and the norm of an ideal.

An order A is not as well-behaved as R. Not only are there ideals which do not factor into primes, but it may be that $\mathfrak{a} \subset \mathfrak{b}$ without there being an ideal $\mathfrak{c}$ such that $\mathfrak{bc} = \mathfrak{a}$. We give an example of this.

Let t be a squarefree integer with $t \equiv 1 \bmod 8$, and let

$$K = \mathbb{Q}(\sqrt{t}), \quad R = \mathbb{Z}[(1+\sqrt{t})/2], \quad A = \mathbb{Z}[\sqrt{t}].$$

Then R is the ring of integers of K (see [13, p. 30]) and A is an order in K. Let

$$\mathfrak{P} = \left(2, \frac{1+\sqrt{t}}{2}\right) \quad \text{and} \quad \mathfrak{Q} = \left(2, \frac{1-\sqrt{t}}{2}\right).$$

The reader may verify (or look up in [13, pp. 74–75]) that $\mathfrak{P}$ and $\mathfrak{Q}$ are primes and that $\mathfrak{PQ} = 2R$.

Let $\mathfrak{p} = \mathfrak{P} \cap A$, $\mathfrak{q} = \mathfrak{Q} \cap A$. It is clear to see that $\mathfrak{p}$ and $\mathfrak{q}$ are both prime ideals of A containing $2A$. However, the reader may verify that

$$\mathfrak{p} = \left(2, 1+\sqrt{t}\right), \quad \mathfrak{q} = \left(2, 1-\sqrt{t}\right), \quad \mathfrak{pq} = \left(2+2\sqrt{t}, 2-2\sqrt{t}\right).$$

We can now see that $2 \notin \mathfrak{pq}$, so $\mathfrak{pq}$ is properly contained in $2A$. This means that $2A$ does not factor into prime ideals. Further, no other ideals contain $2A$ (the reader should verify this, remembering to check the case that some ideal $\mathfrak{c}$ contains $2A$ and is contained in $\mathfrak{p}$ or $\mathfrak{q}$). Thus there can be no ideal $\mathfrak{c}$ such that $\mathfrak{pc} = 2A$ although $2A \subset \mathfrak{c}$.

Let an order A be generated by $\omega_1, \ldots, \omega_n$ and let b be a nonzero element of A. It is easy to see that $b\omega_1, \ldots, b\omega_n$ cannot be linearly dependent and so bA is a lattice of rank n. Thus any nonzero ideal $\mathfrak{a}$ in A is a lattice of rank n since $\mathfrak{a}$ contains bA for any $b \in \mathfrak{a}$.

Extensions. Let K' be a number field containing K with ring of integers S. We say that K' is an *extension* of K. Fix a prime $\mathfrak{P}$ of S; then $\mathfrak{p} = \mathfrak{P} \cap K$ is a prime of R. We say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$. If K' is a Galois extension, each element of the Galois group $\mathrm{Gal}(K'/K)$ maps $\mathfrak{P}$ to another prime $\mathfrak{Q}$ of S which also lies over $\mathfrak{p}$.

Let $\mathcal{P}$ be the set of primes of S lying over $\mathfrak{p}$. This set is finite. Further,

$$\mathfrak{p} = \prod_{\mathfrak{Q} \in \mathcal{P}} \mathfrak{Q}^{e(\mathfrak{Q}|\mathfrak{p})}$$

where $e(\mathfrak{Q} \mid \mathfrak{p})$ is a positive integer called the *ramification index* of $\mathfrak{Q}$ over $\mathfrak{p}$. The product of primes on the right is called the *decomposition* of $\mathfrak{p}$ in the extension K'. If $e(\mathfrak{Q} \mid \mathfrak{p}) > 1$ then we say that $\mathfrak{Q}$ is *ramified*. If any of the primes in $\mathcal{P}$ is ramified then we say that $\mathfrak{p}$ *ramifies* in the extension K'.

If $\alpha_1, \ldots, \alpha_n$ form an integral basis of R, then we define the *discriminant* $\operatorname{disc} R$ by letting $\operatorname{disc} R = \det T$, where T is the n by n integer matrix whose entry in the ith row and jth column is $\mathrm{Tr}(\alpha_i \alpha_j)$. By a standard theorem ([13, p. 25]), $\operatorname{disc} R \neq 0$. Further, the primes in $\mathbb{Z}$ which divide $\operatorname{disc} R$ are precisely those which ramify in K ([13, p. 112]). The *different*, defined below, gives an even better characterization of the ramified primes. Note that the discriminant of $\mathbb{Z}[\zeta]$, the ring of integers of a cyclotomic field, divides m; hence the unramified primes are precisely those which do not divide m.

There is a natural embedding of $R/\mathfrak{p}$ in $S/\mathfrak{P}$: R is mapped into S by containment, reduction by $\mathfrak{P}$ gives a homomorphism from R into $S/\mathfrak{P}$, and clearly the kernel of this homomorphism is $R \cap \mathfrak{P} = \mathfrak{p}$. Since $R/\mathfrak{p}$ and $S/\mathfrak{P}$ are finite fields, we can let $f(\mathfrak{P} \mid \mathfrak{p})$ be the degree of the field extension. We call this integer $f(\mathfrak{P} \mid \mathfrak{p})$ the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$.

If K'' is an extension of K' with ring of integers T and $\mathfrak{U}$ is a prime of T lying over $\mathfrak{P}$, then it is not hard to see that

$$\begin{aligned} e(\mathfrak{U} \mid \mathfrak{p}) &= e(\mathfrak{U} \mid \mathfrak{P}) e(\mathfrak{P} \mid \mathfrak{p}) \text{ and} \\ f(\mathfrak{U} \mid \mathfrak{p}) &= f(\mathfrak{U} \mid \mathfrak{P}) f(\mathfrak{P} \mid \mathfrak{p}). \end{aligned}$$

The central result relating ramification index and inertial degree says that

$$\sum_{\mathfrak{Q} \in \mathcal{P}} e(\mathfrak{Q} \mid \mathfrak{p}) f(\mathfrak{Q} \mid \mathfrak{p}) = [K' : K].$$

See [13, pp. 65–69].

We define two subgroups of $\mathrm{Gal}(K'/K)$. Let

$$D(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

the *decomposition group*, and let

$$E(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma(\alpha) \equiv \alpha \mod \mathfrak{P} \text{ for all } \alpha \in S\},$$

the *inertia group*.

One can prove that $|E(\mathfrak{P} \mid \mathfrak{p})| = e(\mathfrak{P} \mid \mathfrak{p})$; see [13, pp. 100–101]. Further, we can construct a homomorphism from $D(\mathfrak{P} \mid \mathfrak{p})$ into $\mathrm{Gal}((S/\mathfrak{P})/(R/\mathfrak{p}))$. Restrict an element $\sigma \in D(\mathfrak{P} \mid \mathfrak{p})$ to S, then reduce mod $\mathfrak{P}$ to obtain a map σ' from S to $S/\mathfrak{P}$. It is clear to see that σ' has kernel $\mathfrak{P}$ and so we get an automorphism $\overline{\sigma}$ from $S/\mathfrak{P}$ to $S/\mathfrak{P}$. We can easily check that $\overline{\sigma}$ fixes $R/\mathfrak{P}$ and so the map $\sigma \mapsto \overline{\sigma}$ is the desired homomorphism of $D(\mathfrak{P} \mid \mathfrak{p})$ into $\mathrm{Gal}((S/\mathfrak{P})/(R/\mathfrak{p}))$. The kernel of this homomorphism is $E(\mathfrak{P} \mid \mathfrak{p})$. Since $|\mathrm{Gal}((S/\mathfrak{P})/(R/\mathfrak{p}))| = f(\mathfrak{P} \mid \mathfrak{p})$, we have $|D(\mathfrak{P} \mid \mathfrak{p})|/|E(\mathfrak{P} \mid \mathfrak{p})| = f(\mathfrak{P} \mid \mathfrak{p})$. Thus if $\mathfrak{p}$ is unramified so that $|E(\mathfrak{P} \mid \mathfrak{p})| = 1$, then $|D(\mathfrak{P} \mid \mathfrak{p})| = f(\mathfrak{P} \mid \mathfrak{p})$.

Completion. If $\mathfrak{b}$ is an ideal of R we define the *order of* $\mathfrak{b}$ *at* $\mathfrak{p}$, written $\mathrm{ord}_{\mathfrak{p}}\, \mathfrak{b}$, as follows: write

$$\mathfrak{b} = \mathfrak{p}^n \mathfrak{q}$$

where $\mathfrak{q}$ is relatively prime to $\mathfrak{p}$, and set $\mathrm{ord}_{\mathfrak{p}}\, \mathfrak{b} = n$.

An especially useful case is that where $\mathfrak{b} = xR$ for some $x \in R$, and here we write $\mathrm{ord}_{\mathfrak{p}}\, x$ for the order of xR at $\mathfrak{p}$. We may extend the definition to any $x \in K$ in an obvious way: if $x = a/b$ with $a, b \in R$ then

$$\mathrm{ord}_{\mathfrak{p}}\, x = \frac{\mathrm{ord}_{\mathfrak{p}}\, a}{\mathrm{ord}_{\mathfrak{p}}\, b}.$$

The following proposition is a generalization of the familiar Chinese Remainder Theorem and is often called the *weak approximation theorem*.

PROPOSITION 1.3. *Suppose that k is a positive integer, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ are prime ideals of R, $x_1, x_2, \ldots, x_k$ are elements of K, and $n_1, n_2, \ldots, n_k$ are integers. Then there exists an $x \in K$ such that*

$$\mathrm{ord}_{\mathfrak{p}_i}(x - x_i) \geq n_i$$

for $i = 1, 2, \ldots, k$, and $\mathrm{ord}_{\mathfrak{q}}\, x \geq 0$ for all primes $\mathfrak{q}$ not in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$.

See [14, p. 12] for the proof (note that there $v_{\mathfrak{p}}(x)$ is used for our $\operatorname{ord}_{\mathfrak{p}} x$).

For each prime $\mathfrak{p}$ of R lying over a prime p in $\mathbb{Q}$, we define a map $|\cdot|_{\mathfrak{p}}$ from K to $\mathbb{R}$ by setting

$$|x|_{\mathfrak{p}} = p^{-\operatorname{ord}_{\mathfrak{p}} x}$$

for every x in K. This is called the $\mathfrak{p}$-*adic valuation* on K. We have

$$\mathfrak{p} = \{x \in K \mid |x|_{\mathfrak{p}} < 1\}, \quad R = \{x \in K \mid |x|_{\mathfrak{p}} \leq 1\}.$$

(The reader will note that in fact we could take any valuation *equivalent* to $|\cdot|_{\mathfrak{p}}$, namely a valuation $|\cdot|$ for which $|x| = |x|_{\mathfrak{p}}^{\lambda}$ where λ is a positive real number. However the $\mathfrak{p}$-adic valuation suffices for our purposes. See [2] for more details.)

The reader will quickly see that $|\cdot|_{\mathfrak{p}}$ is a metric on K. It not only satisfies the triangle inequality but the *ultrametric property*

$$|x + y|_{\mathfrak{p}} \leq \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\}$$

for every x and y in K.

If K' is an extension of K with ring of integers S and $\mathfrak{P}$ is a prime of S lying over a prime $\mathfrak{p}$ of R, then it is easy to see that $|\cdot|_{\mathfrak{P}}$ extends $|\cdot|_{\mathfrak{p}}$ in the sense that $|x|_{\mathfrak{P}} = |x|_{\mathfrak{p}}$ for any $x \in K$.

Definition. The *completion of K at $\mathfrak{p}$* is the completion of K as a metric space with respect to $|\cdot|_{\mathfrak{p}}$.

Let K' be the completion of K at a prime $\mathfrak{p}$ and write $|\cdot|$ for both the valuation $|\cdot|_{\mathfrak{p}}$ and its extension to K'. Let

$$P = \{x \in K' \mid |x| < 1\}, \quad S = \{x \in K' \mid |x| \leq 1\}.$$

Then S is a ring, P is an ideal in S, and S/P is a finite field isomorphic to $R/\mathfrak{p}$. See [2, pp. 41–42].

The following result is known as *Hensel's Lemma*.

Proposition 1.4. *Let K' be the completion of K at a prime $\mathfrak{p}$ with S and P defined as above. Suppose that f is a polynomial with coefficients in the ring S and a_0 is an element of S such that*

$$|f(a_0)| < |f'(a_0)|^2.$$

Then there is an $a \in S$ such that $f(a) = 0$.

See [2, pp. 49–51] for the proof.

The Frobenius Automorphism. In defining the Frobenius automorphism we follow Marcus [13, pp. 108–110]. Suppose that K' is an extension of K with ring of integers S. Let p be a prime in $\mathbb{Q}$ that is not ramified in K', hence not ramified in K, and let $\mathfrak{p}$ be a prime of R lying over p, $\mathfrak{P}$ a prime of S lying over $\mathfrak{p}$. Let G be the Galois group of $S/\mathfrak{P}$ over $R/\mathfrak{p}$ and let $D = D(\mathfrak{P} \mid \mathfrak{p})$. It follows from our results above that D is isomorphic to G.

The finite fields $S/\mathfrak{P}$ and $R/\mathfrak{p}$ have characteristic p. Hence G is generated by the map which takes $x \in S/\mathfrak{P}$ to $x^{N(\mathfrak{p})}$ (see [13, p. 265]). Therefore we have a generator σ of D such that

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$$

for any $x \in S$. Certainly σ is the only element in $\mathrm{Gal}(K'/K)$ with this property. We call σ the *Frobenius automorphism corresponding to* $\mathfrak{P}$. Note that the order of σ is $|D| = f(\mathfrak{P}|\mathfrak{p})$.

If $\mathfrak{P}'$ is another prime lying over $\mathfrak{p}$ then for some $\phi \in \mathrm{Gal}(K'/K)$ we have $\phi(\mathfrak{P}) = \mathfrak{P}'$. The reader may easily check that the Frobenius automorphism corresponding to $\mathfrak{P}'$ is $\phi\sigma\phi^{-1}$. Thus in particular when K' is an abelian extension the Frobenius automorphism is determined by $\mathfrak{p}$, so we may extend the definition of the Frobenius automorphism to all unramified ideals $\mathfrak{b}$ in R as follows. Write

$$\mathfrak{b} = (\mathfrak{p}_1)^{e_1}(\mathfrak{p}_2)^{e_2} \cdots (\mathfrak{p}_r)^{e_r}$$

and let σ_i be the Frobenius automorphism of $\mathfrak{p}_i$. Then we declare that the *Frobenius automorphism of* $\mathfrak{b}$ *in* K'/K is

$$(\sigma_1)^{e_1}(\sigma_2)^{e_2} \cdots (\sigma_r)^{e_r}.$$

For an example, take $K = \mathbb{Q}(\zeta)$. The Galois group of $\mathbb{Q}(\zeta)$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$, with $n \in (\mathbb{Z}/m\mathbb{Z})^*$ corresponding to the mapping carrying ζ to ζ^n (see [13, p. 18]). Let p be a prime not dividing m, so that p is unramified, and let $\mathfrak{p}$ be a prime of $\mathbb{Z}[\zeta]$ lying over p. Let σ be the Frobenius automorphism corresponding to a prime $\mathfrak{p}$ and let n be the element of $(\mathbb{Z}/m\mathbb{Z})^*$ corresponding to σ. Then

$$\zeta^n = \sigma(\zeta) \equiv \zeta^p \mod \mathfrak{p}$$

and as we will prove below (Lemma 3.1), this means that $\zeta^p = \zeta^n$ so σ corresponds to p in $(\mathbb{Z}/m\mathbb{Z})^*$. A nice consequence is that $f(\mathfrak{p} \mid p)$ is the order of p mod m.

We will need one easy result on Frobenius automorphisms, which comes from [3, p. 166].

PROPOSITION 1.5. *Suppose that K' and K'' are both abelian Galois extensions of K with $K' \subset K''$ and that $\mathfrak{b}$ is an ideal in R unramified in K''. Let σ' be the Frobenius automorphism of $\mathfrak{b}$ in the extension K'/K, σ'' the Frobenius automorphism of $\mathfrak{b}$ in the extension K''/K, and $\theta : \mathrm{Gal}(K''/K) \to \mathrm{Gal}(K'/K)$ the restriction map. Then*

$$\sigma' = \theta(\sigma'').$$

PROOF. Clearly it suffices to prove the result for a prime $\mathfrak{p}$. Let $\mathfrak{P}'$ be any prime of K' lying over $\mathfrak{p}$ and let $\mathfrak{P}''$ be any prime of K'' lying over $\mathfrak{P}'$. Let S' be the ring of integers of K' and let S'' be the ring of integers of K''.

For any $x \in S''$,

$$\sigma''(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}''$$

by definition. When $x \in S'$, then

$$\sigma''(x) - x^{N(\mathfrak{p})} \in S',$$

and so since $\mathfrak{P}' = \mathfrak{P}'' \cap S'$,

$$\sigma''(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}'.$$

The proposition now follows by the uniqueness of the Frobenius automorphism. □

Fractional Ideals and the Different. This subsection is based closely on a series of exercises in Marcus [13, pp. 92–97].

DEFINITION. A subset $\mathfrak{A} \subset K$ is a *fractional ideal* if $\mathfrak{A} = x\mathfrak{a}$ where x is a nonzero element of K and $\mathfrak{a}$ is a nonzero ideal of R.

Clearly ideals of R are fractional ideals; we call these *integral ideals* when we need to distinguish them from fractional ideals. However in general by the word "ideal" we shall mean "ideal of an order A". Note that one can define "fractional ideals of an order A" but we shall not need this notion.

Let $\mathfrak{A}$ be a fractional ideal of R; clearly $R\mathfrak{A} \subset \mathfrak{A}$. Write $\mathfrak{A} = x\mathfrak{a}$ for some nonzero $x \in K$ and some nonzero ideal $\mathfrak{a}$ of R. Fix $y \in \mathfrak{A}$ and write $y = ax$ for some $a \in \mathfrak{a}$; then the map that takes y to a can be easily seen to be an isomorphism of additive groups mapping $\mathfrak{A}$ onto $\mathfrak{a}$. Since $\mathfrak{a}$ is isomorphic to $\mathbb{Z}^n$, so is $\mathfrak{A}$. Conversely, any subgroup G of K is a fractional ideal if

G is isomorphic to $\mathbb{Z}^n$ and $RG \subset G$. To see this, let G be generated by $g_1, \ldots, g_n$, write $g_i = x_i/y_i$ for algebraic integers x_i and y_i, set $x = \prod_{i=1}^n y_i$, and observe that xG is an integral ideal of R.

Fix two fractional ideals $\mathfrak{A}$ and $\mathfrak{B}$ and write $\mathfrak{A} = x\mathfrak{a}$, $\mathfrak{B} = y\mathfrak{b}$ for x and y nonzero in K and $\mathfrak{a}$ and $\mathfrak{b}$ nonzero ideals of R. We define the product $\mathfrak{AB}$ to be the fractional ideal $(xy)(\mathfrak{ab})$; clearly this is independent of our choice of x, y, $\mathfrak{a}$, and $\mathfrak{b}$.

The next proposition establishes that the fractional ideals form a group with the operation of multiplication and identity the integral ideal R.

PROPOSITION 1.6. *For every fractional ideal $\mathfrak{A}$ of R, there is a fractional ideal $\mathfrak{A}^{-1}$ of R such that $\mathfrak{A}\mathfrak{A}^{-1} = R$.*

PROOF. Fix a fractional ideal $\mathfrak{A}$ and let

$$\mathfrak{A}^{-1} = \{x \in K \mid x\mathfrak{A} \subset R\}.$$

Fix y nonzero in $\mathfrak{A}$ and let $\mathfrak{b} = y\mathfrak{A}^{-1}$. Then $\mathfrak{b}$ is clearly an ideal in R and $\mathfrak{A}^{-1} = (1/y)\mathfrak{b}$, so that $\mathfrak{A}^{-1}$ is a fractional ideal. Further, clearly $\mathfrak{A}\mathfrak{A}^{-1} \subset R$ so $\mathfrak{A}\mathfrak{A}^{-1}$ is an integral ideal.

Now we suppose that $\mathfrak{A}\mathfrak{A}^{-1} \neq R$ and derive a contradiction. By a lemma of Marcus [13, p. 57], there is an element $\gamma \in K$ with $\gamma \notin R$ and $\gamma\mathfrak{A}\mathfrak{A}^{-1} \subset R$. Clearly $\gamma\mathfrak{A}^{-1} \subset \mathfrak{A}^{-1}$. A well-known theorem (proved in [13, pp. 15–16]) says that if $\gamma A \subset A$ for any finitely generated additive group $A \subset \mathbb{C}$, then γ is an algebraic integer. Thus $\gamma \in R$; this contradiction establishes the proposition. □

With this result proved we are justified in calling $\mathfrak{A}^{-1}$ *the* inverse of $\mathfrak{A}$ since it is unique by group theory. Note that if $1 \in \mathfrak{A}$ then $\mathfrak{A}^{-1}$ is an integral ideal.

DEFINITION. The *codifferent* $\mathfrak{C}$ is the set

$$\{x \in K \mid \mathrm{Tr}(xR) \in \mathbb{Z}\}.$$

We show that the codifferent is a fractional ideal. Let $\omega_1, \ldots, \omega_n$ be an integral basis for R and let M be the n by n rational matrix whose entry in the ith row and jth column is $\mathrm{Tr}(\omega_i\omega_j)$. Let $d = \det M$; by definition $d = \mathrm{disc}\, R \neq 0$. For each $j = 1, 2, \ldots, n$, let m_j be the jth row of M.

Fix an element $y \in \mathfrak{C}$ and write

$$y = \sum_{i=1}^{n} a_i\omega_i$$

where the a_i lie in $\mathbb{Q}$. Let a be the rational n-tuple $(a_1, \ldots, a_n)$. Let

$$b = (\mathrm{Tr}(y\omega_1), \ldots, \mathrm{Tr}(y\omega_n)).$$

By definition b is an integer n-tuple. Further, it is easy to see that

$$b = (m_1 \cdot a, \ldots, m_n \cdot a) = Ma.$$

Thus $a = M^{-1}b$ and hence da is an integer n-tuple. This means that $dy \subset R$ and we have proven that $d\mathfrak{C} \subset R$. Since obviously $d\mathfrak{C}$ is a nonzero integral ideal of R, we have succeeded in proving that $\mathfrak{C}$ is a fractional ideal. The following definition therefore makes sense.

DEFINITION. The different $\mathfrak{d}$ is the inverse of the codifferent.

Clearly $1 \in \mathfrak{C}$ and so the different $\mathfrak{d}$ is an integral ideal.

The most interesting things about the different are that its norm is disc R and that its factors are exactly the ramified primes in K. For a proof of this see the exercises in [13, pp. 95–96]. We will see another use of the different in Chapter 5.

The Geometry of Numbers. We construct an embedding of a number field K in a real vector space, following closely the exposition of Lenstra in [12]. We have $K = \mathbb{Q}(\alpha)$ for some algebraic number α and we let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α. Let n be the degree of K over $\mathbb{Q}$, let r be the number of real roots of f, and let $2s$ be the number of complex roots of f; the complex roots come in conjugate pairs so s is an integer. Write the set of roots in the form

$$\{\gamma_1, \ldots, \gamma_r, \delta_1, \overline{\delta_1}, \ldots, \delta_s, \overline{\delta_s}\}$$

and embed the additive group of K in the real vector space $\mathbb{R}^r \oplus \mathbb{C}^s$ as follows: any $x \in K$ is equal to $g(\alpha)$ for some $g \in \mathbb{Q}[X]$ and we map x to

$$\psi(x) = (g(\gamma_1), \ldots, g(\gamma_r), g(\delta_1), \ldots, g(\delta_s)).$$

Identifying K with its image $\psi(K)$, we see that the norm map $N : K \to \mathbb{Q}$ can be extended to all of $\mathbb{R}^r \oplus \mathbb{C}^s$ as follows: let

$$N(x_1, \ldots, x_r, y_1, \ldots, y_s) = \left| \prod_{i=1}^{r} x_i \prod_{i=1}^{s} y_i \overline{y_i} \right|. \tag{2}$$

where the x_i are real and the y_i are complex. Notice that this is an extension only up to sign; that is, the norm we just defined on all of $\mathbb{R}^r \oplus \mathbb{C}^s$ is the absolute value of the usual norm defined earlier. However we will not need to worry about the sign.

Certainly $\psi(R)$ is a lattice in $\mathbb{R}^n$. Marcus ([13, p. 134]) proves that

$$\det \psi(R) = \frac{\sqrt{|\operatorname{disc} R|}}{2^s}.$$

We can thus compute the norm of an ideal $\mathfrak{a}$ in R by using the formula $\det \psi(\mathfrak{a}) = \det \psi(R) N(\mathfrak{a})$.

Kummer Theory. We will be interested in the mth roots of an element a in K. This we can handle with *Kummer theory*, which is the study of abelian extensions K' of K such that $x^m \in K$ for every $x \in K'$ (we say that K' has *exponent* m). We will need only one easy result.

PROPOSITION 1.7. *Suppose that K is a number field containing all mth roots of unity. If $a \in K$ and $x, x' \in \mathbb{C}$ with $x^m = a$ and $(x')^m = a$, then the extensions $K(x)/K$ and $K(x, x')/K$ are abelian Galois extensions.*

PROOF. Observe that the conjugates of x are exactly the complex numbers of the form $\zeta^k x$. Since every mth root of unity is in K we see that all the conjugates of x are in $K(x)$; it follows that $K(x)/K$ is Galois. We know that any element τ of the Galois group must map x to a conjugate of x, and so $\tau(x) = zx$ for some mth root of unity z. If we map τ to the associated z we obtain a mapping of $\operatorname{Gal}(K(x)/K)$ into μ_m, the group of mth roots of unity. This map is clearly a homomorphism since if τ' maps x to $z'x$ with z' another mth root of unity, then $\tau\tau'$ maps x to $zz'x$. Further, the map is injective since τ is completely determined by its action on x. It follows that $\operatorname{Gal}(K(x)/K)$ is abelian.

By similar reasoning we find that $K(x, x')$ contains all conjugates of x and x', and therefore is a Galois extension of K. Any element τ of the Galois group maps x to zx and x' to $z'x'$ with z and z' mth roots of unity; we associate τ with the element (z, z') in the group $\mu_m \oplus \mu_m$. We can rapidly verify that this is a homomorphism and an injective map, and therefore that $\operatorname{Gal}(K(x, x')/K)$ is abelian. □

3. Algorithms

An *algorithm* is a sequence of instructions which, if followed, provides an output and terminates in a finite time. Of course, this is not quite a

definition since we have not specified what an "instruction" is. However, we shall be content with this rather vague description. Algorithms are mathematical models of computer programs.

Encodings and Object Sizes. An algorithm takes certain objects as inputs and produces other objects as outputs. These may be orders, ideals, groups, field elements, and so on. We will only deal with a finite number of different types of objects; let T_1 be the set of all objects of one type, T_2 the set of all objects of another, and so on up to T_k. Let U be the union of the T_i. For simplicity, in this section we deal only with algorithms which take exactly one object as input and produce only one object as output. The reader will have no difficulty in extending our discussion to algorithms which, like many of the algorithms in the rest of this thesis, input or output multiple objects.

Abstractly it suffices to specify an object in ordinary mathematical language, but a real digital computer cannot operate with anything but positive integers of a finite size. Thus we must give *encodings of objects*, i.e. descriptions of objects which use only positive integers. In mathematical language we want an injective mapping e_i of T_i into $(\mathbb{Z}^+)^\infty$, where $(\mathbb{Z}^+)^\infty$ is the set of all vectors of positive integers with a finite number of entries. If W is an element of T_i then we say that $e(W)$ *encodes* W. In practice we will allow more structure on the encoding of W, for instance allowing it to be an integer matrix, but in principle all our encodings could be given as vectors of integers.

A simple example is the set of rational numbers. Every rational number q may be written $(-1)^t(a/b)$ where t is either 0 or 1, a and b are positive integers, and the fraction a/b is in lowest terms. Thus the encoding of q is (t, a, b). In Chapter 2 we will give encodings for all of the objects we will use.

We also want to measure the *size* of an object $W \in U$, which we denote $\text{size}(W)$. We let $\text{size}(0) = 1$ and, for any positive integer n, let

$$\text{size}(n) = \lfloor 1 + \log n \rfloor.$$

Let an object $W \in U$ be encoded by $(w_1, \ldots, w_n)$ where the w_i are integers. Then

$$\text{size}(W) = \sum_{i=1}^{n} \text{size}(w_i).$$

Note that the size of W is the number of bits required to write all the integers in the encoding of W in binary. (A *bit* is a binary digit, i.e. a 0

or a 1.) For example, the rational number 4/17 is encoded by the triple $(0, 4, 17)$, so

$$\text{size}(4/17) = 1 + \lfloor \log(1+4) \rfloor + \lfloor \log(1+17) \rfloor = 9.$$

Indeed, 4/17 can be encoded by the 9 bits $(0, 100, 10001)$.

The Order of a Function.

We would like to measure the asymptotic behavior of an algorithm, that is its behavior for large inputs. We can measure the asymptotic behavior of any function by using the so-called "big oh" notation.

DEFINITION. If f and g are functions mapping $\mathbb{Z}$ to $\mathbb{R}$ then f has *order* g if there is a positive integer N and a positive real number C such that for all integers $n > N$, $f(n) \leq Cg(n)$. We also write $f = O(g)$ to express the same thing (hence the name "big oh").

We will need an expanded version of this definition which takes into account our size function. First note that since the encoding function on each T_i is injective, clearly the set

$$\{u \in U \mid \text{size}(u) = s\}$$

is finite for any positive integer s.

DEFINITION. If V is a subset of U and f is a function mapping V to $\mathbb{R}$ then we define the function $\hat{f}$, which maps $\mathbb{Z}$ to $\mathbb{R}$, by

$$\hat{f}(s) = \max\{f(v) \mid v \in V,\ \text{size}(v) = s\}.$$

If g is another function mapping V to $\mathbb{R}$ then we say that f has *order* g, or write $f = O(g)$, if $\hat{f}$ has order $\hat{g}$ as defined above.

Note that trivially $\widehat{\text{size}}$ is just the identity mapping.

The following proposition usually makes it easy to find for a given f a simple function g (such as 1, x, α^x, and so forth) for which $f = O(g)$.

PROPOSITION 1.8. *Suppose that V is a subset of U and f_1, f_2, g_1, and g_2 are functions mapping V to $\mathbb{R}$ such that $f_1 = O(g_1)$, $f_2 = O(g_2)$. Let g be the function from V to $\mathbb{R}$ such that $g(v) = \max\{g_1(v), g_2(v)\}$ for every $v \in V$. Then*

(1) $f_1 + f_2 = O(g)$ *and*
(2) $f_1 \cdot f_2 = O(g_1 \cdot g_2)$.

The proof is easy and left to the reader. As an example of the use of Proposition 1.8, we suggest that the reader verify that when $V = \mathbb{Q}$ and f is a polynomial of degree d with rational coefficients then $f = O(X^d)$.

We can use the big oh notation to divide functions into a number of classes.

DEFINITION. If V is a subset of U and f and g are functions mapping V to $\mathbb{R}$ then

- f is *constant* in g if $f = O(g)$,
- f is *logarithmic* in g if $f = O(\log g)$,
- f is *linear* in g if $f = O(g)$,
- f is *polynomial* in g if $f = O(g^k)$ for some positive integer k, and
- f is *exponential* in g if $f = O(\alpha^g)$ for some positive real number $\alpha > 1$.

It is now clear how we will carry out our measurement of the asymptotic behavior of an algorithm. We will let $f(W)$ be some measure of the algorithm's behavior for a given input W and decide whether f is constant, logarithmic, etc. in size(W). Note that this necessarily gives a *worst-case analysis*, and that the algorithm's behavior on many inputs may be very different from its behavior on the worst-case input.

Running Time and Output Size. The two measures of an algorithm's behavior to which we will apply a big oh analysis will be the algorithm's *running time* and *output size.* We now define these.

The simplest possible algorithm is a *bit operation.* A bit operation takes as input one or two bits and gives as a result either one or two bits. For example, we may add two bits, perform a logical AND on two bits, or negate a bit.

Any algorithm performs a sequence of bit operations on its input. For a given input W we let $D(W)$ be the number of bit operations performed by the algorithm. The integer $D(W)$ is called the *running time* of the algorithm for the input D. The integer $\hat{D}(s)$ for any integer s is called the *worst-case running time* or just the running time.

For an example we examine an algorithm which adds 1 to a given positive integer. We use the grade school addition algorithm, which simply adds bits from right to left, carrying when necessary. For a fixed input size s, clearly the worst case for this algorithm is the input $2^s - 1$, in whose binary representation all bits are 1, and we can quickly see that this requires s bit additions. Thus $\hat{D}(s) = s$ for this algorithm.

If, for a given input W, an algorithm produces the output X, then we let the *output size* for W be the integer $E(W) = \text{size}(X)$. The integer $\hat{E}(s)$ for any positive integer s is called the *worst-case output size* or just the output size of the algorithm. Observe that $\hat{E}(s) = s + 1$ for our incrementing algorithm.

Actually carrying out the conversion from an English description of an algorithm to bit operations is tedious and never necessary for any but the most basic algorithms. Similarly, one almost never tries to calculate the actual output size for a given input. Instead one uses Proposition 1.8 and a small set of known results to apply a big oh analysis and classify the running time and output size as constant, linear, etc. in the size of the input. When we have made such a classification, we will say that we have a "polynomial-time algorithm", "an algorithm with linear output size", "an algorithm which runs in logarithmic time", and so forth.

We will use a large number of subroutines, that is algorithms which are used by other algorithms. In all cases that we deal with here, all subroutines called by an algorithm have polynomial running time and output size. To check that the algorithm itself runs in polynomial time, we can simply suppose that all subroutines return the right answer instantly and check whether the resulting running time is polynomial in the input size; if so, by Proposition 1.8 it easily follows that the original algorithm runs in polynomial time.

Polynomial-time algorithms for arithmetic in $\mathbb{Q}$ and linear algebra over both $\mathbb{Z}$ and $\mathbb{Q}$ are well-known; these algorithms can accept inputs of unlimited size. We will use them freely throughout the rest of this thesis.

For a more thorough discussion of algorithms, big oh, and various sorts of proofs, the reader should consult one of the many books on algorithms, such as Cormen et. al. [5].

CHAPTER II

ENCODINGS OF BASIC OBJECTS

Certain objects form the building blocks of our algorithm for the computation of the power residue symbol. In this chapter we present encodings for these objects and also sketch polynomial-time algorithms for basic operations on them. Detailed implementations of the algorithms, as well as proofs of termination, correctness, and polynomial running time, can be found in standard books on algorithms like Henri Cohen's [4].

1. Lattices

Most of the lattices on which we will operate will be considered as sublattices of a larger lattice, and we might as well assume that the larger lattice is $\mathbb{Z}^n$. Let L be a lattice of rank n which is contained in $\mathbb{Z}^n$ and let $v_1, \ldots, v_n$ be a basis of L, so that each v_i is an integer n-tuple. We write B for the matrix whose ith column is v_i. The lattice L is encoded by the Hermite normal form of B. (The HNF condition simply corresponds to a change of basis.)

When we want to apply the LLL algorithm, however, we will want to consider a lattice as nontrivially embedded in a real vector space. Let L be a lattice of rank n and let $v_1, \ldots, v_n$ be a basis of L. We encode L as the n by n real matrix whose jth column is the real n-tuple v_j. (Of course we cannot encode real numbers inside a digital computer, but in practice careful rational approximation suffices. See [4, p. 89] for a full discussion and references.)

Throughout the thesis, we will use the first encoding for our lattices except where we expressly invoke the second. In particular, the following operations use the first encoding. So, for the remainder of the section we fix lattices L and L' of rank n, each contained in $\mathbb{Z}^n$.

To find the lattice generated by a given set of vectors in $\mathbb{Z}^n$, we write all the given vectors as columns of a matrix B and apply the HNF algorithm

to B. The result is a matrix B' in HNF which encodes the desired lattice. (Of course the matrix B' may not be of full rank, in which case we do not have a lattice by our definition.) We can apply this process in particular to the sum $L + L'$, taking as the generating set the union of the generators of L and L'.

We can determine whether $L = L'$ simply by comparing the matrices encoding them. Since the HNF is unique, $L = L'$ only when these matrices are equal.

If indeed $L' \neq L$ but we know that $L \subset L'$, we can find an element a which is in L' but not in L. To do this, let $B = (b_{ij})$ be the n by n integer matrix encoding L and let $B' = (b'_{ij})$ be the n by n integer matrix encoding L'. Since both matrices are in HNF and are specifically upper triangular, it is easy to see that for each $j = 1, 2, \ldots, n$, we must have $b'_{jj} \mid b_{jj}$, and that if in fact $b'_{jj} = b_{jj}$ for each such j then $L = L'$. We can therefore take any j for which $b'_{jj} \neq b_{jj}$ and the jth column will encode the desired a.

To determine whether a given element $a \in \mathbb{Z}^n$ is in L, we apply linear algebra algorithms to determine whether a is in the image of the matrix B which encodes L. If a is found to lie in L, these algorithms also tell us how to find a as a $\mathbb{Z}$-linear combination of the generators of L.

We find $\det L$ by computing the determinant of the matrix encoding L. This simply means multiplying the diagonal elements since the matrix is in HNF.

Suppose that $v_1, \ldots, v_n$ is a basis of L and that P is the corresponding fundamental parallelotope. Given x in $\mathbb{Z}^n$, we can find $\ell \in L$ and $x' \in \mathbb{Z}^n \cap P$ with $x' = x - \ell$ as follows. Using linear algebra over $\mathbb{Q}$, write x as a $\mathbb{Q}$-linear combination of the v_i:

$$x = \sum_{i=1}^{n} r_i v_i.$$

Let $\ell = (\lfloor s_1 \rfloor, \ldots, \lfloor s_n \rfloor)$ and let $x' = x - \ell$.

2. Number fields

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n over $\mathbb{Q}$ and let $f \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Write

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1} + X^n$$

for some positive integer n and $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. We then encode K by the rational n-tuple $(a_0, \ldots, a_{n-1})$.

An element $x \in K$ has a unique minimal polynomial $g \in \mathbb{Q}[X]$ with degree $\leq n$. We write

$$g(X) = \sum_{i=0}^{n} b_i X^i$$

and encode x by the rational n-tuple $(b_0, \ldots, b_n)$.

For arithmetic operations, i.e. the sum, difference, product, and quotient of elements of K, we do polynomial operations using resultants. See [4, pp. 156–157] for implementations. The norm of an element is the constant coefficient of its minimal polynomial f (up to an easily computed sign) and the trace is the coefficient of $X^{\deg f - 1}$.

To find an element $x \in K$ as a quotient b/c with b, c in the ring of integers of K, let $f \in \mathbb{Q}[X]$ be the minimal polynomial of x and write

$$f(X) = \sum_{i=1}^{n} \frac{r_i}{s_i} X^i$$

where the r_i and s_i are integers. Let c be the least common multiple of the s_i and let

$$g(X) = \sum_{i=1}^{n} \frac{r_i c^{n-i}}{s_i} X^i.$$

Let $b = cx$. Clearly $g(b) = 0$ and the coefficients of g are integers, so b is an algebraic integer, and c is a rational integer, hence an algebraic integer. Thus we see that $x = b/c$ as desired.

3. Orders

Let K be a number field of degree n over $\mathbb{Q}$ and let A be an order in K. By definition, A is generated additively by some $\omega_1, \ldots, \omega_n$ in K. For each i and j with $1 \leq i < j \leq n$, we have integers $t_{ij1}, \ldots, t_{ijn}$ such that

$$\omega_i \omega_j = \sum_{k=1}^{n} t_{ijk} \omega_k.$$

We encode A by the ω_i together with the integers t_{ijk}.

If x is an element of A, we must have

$$x = \sum_{i=1}^{n} a_i \omega_i$$

for some integers i and so we encode x by the n-tuple $(a_1, \ldots, a_n)$.

Let x and y be elements of A and let $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ be the integer n-tuples encoding x and y respectively. The sum $x + y$ is just the sum of the n-tuples and similarly for the difference $x - y$. The reader can easily check that xy is the integer n-tuple whose kth component is

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_i b_j t_{ijk}.$$

For the quotient x/y, we let $X_1, \ldots, X_n$ be unknowns and set up a system of n integer linear equations, one for each $k = 1, \ldots, n$:

$$a_k = \sum_{i=1}^{n} \sum_{j=1}^{n} X_i b_j t_{ijk}.$$

The solution to this system encodes x/y. If there is no solution then y does not divide x in A.

Example: the ring of integers in a cyclotomic field. The case where $K = \mathbb{Q}(\zeta)$ and $A = \mathbb{Z}[\zeta]$ will come up repeatedly. We may take $1, \zeta, \ldots, \zeta^{\phi(m)-1}$ as a basis of $\mathbb{Z}[\zeta]$. Clearly $\zeta^i \zeta^j = \zeta^{i+j}$ so we may take the integers t_{ijk} to be 1 if $k = i + j \bmod \phi(m)$ and 0 otherwise.

Now for any $x \in \mathbb{Z}[\zeta]$, we may write

$$x = \sum_{i=0}^{\phi(m)-1} a_i \zeta^i,$$

where the a_i are integers, and the element x is encoded by the $\phi(m)$-tuple $(a_0, \ldots, a_{\phi(m)-1})$.

4. Integral Ideals

Let K be a number field, let A be an order in K, and let $\mathfrak{a}$ be an ideal in A. As we saw above, $\mathfrak{a}$ is a lattice of rank n contained in the lattice A, which has rank n. We therefore have a encoding of $\mathfrak{a}$ as a lattice L of rank n contained in $\mathbb{Z}^n$, where we have identified A and $\mathbb{Z}^n$.

Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in an order A. Then we can find the sum $\mathfrak{a} + \mathfrak{b}$ simply by summing the lattices L and L' which encode $\mathfrak{a}$ and $\mathfrak{b}$. If we know that $\mathfrak{b} \subset \mathfrak{a}$, then similarly we can test the condition $\mathfrak{a} = \mathfrak{b}$, and

find an element $a \in \mathfrak{a}$, $a \notin \mathfrak{b}$ when $\mathfrak{a} \neq \mathfrak{b}$, by using the corresponding lattice operations. For the product $\mathfrak{ab}$ of two general ideals $\mathfrak{a}$ and $\mathfrak{b}$, we compute the n^2 products of the form vv' where v is in the set of generators of L and v' is in the set of generators of L'; then the lattice generated by these n^2 vectors encodes $\mathfrak{ab}$.

5. Fractional ideals

Let K be a number field with ring of integers R. A fractional ideal $\mathfrak{A}$ of R is equal to $x\mathfrak{a}$ for some nonzero $x \in K$ and some nonzero integral ideal $\mathfrak{a}$ of R. We encode $\mathfrak{A}$ by the pair $(x, \mathfrak{a})$.

If $\mathfrak{A}$ and $\mathfrak{B}$ are fractional ideals encoded by $(x, \mathfrak{a})$ and $(y, \mathfrak{b})$ respectively, the the product $\mathfrak{AB}$ is encoded by $(xy, \mathfrak{ab})$.

6. Finite Abelian Groups

Let G be a finite abelian group, written additively. For some positive integer n and some lattice L of rank n in $\mathbb{Z}^n$, we have $G \cong \mathbb{Z}^n/L$. Let n and L be such that n is as small as possible. We encode G by the lattice L, given by some basis $v_1, \ldots, v_n$. Note that our choice of basis determines a fundamental parallelotope P, and that elements of $\mathbb{Z}^n \cap P$ with the operation of addition modulo L form a group isomorphic to G.

If G' is a subgroup of G, then there is a lattice L' in $\mathbb{Z}^n$ such that $L \subset L'$ and $G' \cong L'/L$. We encode G' by the lattice L' in $\mathbb{Z}^n$.

An element $g \in G$ is a coset $x + L$ where $x \in \mathbb{Z}^n$. There is a unique x' in the fundamental parallelotope P which is also in the coset $x + L$. We encode the element g by this x', which is an n-tuple of integers. Of course this means that our encoding of g is dependent upon the basis chosen for L, but if we should need to change the basis of L it is easy to use linear algebra to find the n-tuple corresponding to g with respect to the new basis.

Let γ be an endomorphism of G. There is a linear transformation τ of $\mathbb{Z}^n$ such that $\tau(L) \subset L$ and $\gamma(x + L) = \tau(x)$ for every $x \in \mathbb{Z}^n$. We encode γ by the matrix T of τ on the standard basis of $\mathbb{Z}^n$. T is an n by n integer matrix.

Notice that any n by n integer matrix T for which $TL \subset L$ gives a corresponding endomorphism γ of G by setting $\gamma(x + L) = Tx$.

Suppose that g and h are elements of G encoded by x and y and that γ, γ' are endomorphisms of G encoded by matrices T and T'. We find $g + h$ by computing $x + y$ and an element ℓ in L such that $x + y - \ell$ is in the fundamental parallelotope P; a similar process suffices to find $-g$ and γg. The composition $\gamma\gamma'$ is simply the matrix product TT'.

We may find the decomposition

$$G = \sum_{i=1}^{t} \mathbb{Z}/n_i\mathbb{Z}$$

of G into cyclic groups, where t is a positive integer and $n_i \mid n_{i+1}$ for each $i = 1, 2, \ldots, t-1$, by computing the SNF $B = (b_{ij})$ of the lattice L encoding G and setting $n_i = b_{ii}$.

If we are given G as a quotient $\mathbb{Z}^n/L$ with n not minimal and an endomorphism γ as a linear transformation of $\mathbb{Z}^n$, we can find the encoding of G and γ as follows. The lattice L is encoded as an n by n matrix in HNF. The condition that n is not minimal ensures that at least one diagonal entry is 1. If the entry in row i and column i is 1, strike out the ith row and ith column. The resulting matrix encodes a lattice L' of rank n' in $\mathbb{Z}^{n'}$ with $G = \mathbb{Z}^{n'}/L'$. Clearly n' is minimal, so L' encodes G. To find the encoding of γ, let $e_1, \ldots, e_n$ be the standard basis vectors of $\mathbb{Z}^n$ and compute γe_i for each i such that the ith row and ith column were not struck out. The result for each such i will be an element of the fundamental parallelotope of L and will therefore have zeroes in the jth entry whenever the jth row and jth column were struck out. Striking out these zeroes gives an element of $\mathbb{Z}^{n'}$, the image of one of the basis vectors of $\mathbb{Z}^{n'}$. It is now easy to write down the encoding of γ.

7. Finite $\mathbb{Z}[\zeta]$-Modules

Let M be a finite $\mathbb{Z}[\zeta]$-module, that is a finite abelian group written additively with an action of ζ. We encode M by its additive group together with the endomorphism γ of the additive group which takes $x \in M$ to ζx. Elements and endomorphisms of M are thus just encoded as the corresponding objects for the additive group of M.

Let Z be the n by n matrix encoding γ and let L be the lattice encoding the additive group of M. Note that Z satisfies two conditions: not only is ZL contained in L but also

$$1 + Z + Z^2 + \cdots + Z^{m-1} = 0$$

where 1 is the identity matrix and 0 is the zero matrix . If n is a positive integer and L is a lattice of rank n in $\mathbb{Z}^n$, then any n by n integer matrix Z for which these two conditions hold will give an action of ζ on the additive group $\mathbb{Z}^n/L$.

Let ϵ be an endomorphism of M and let E be the corresponding n by n integer matrix. Note that E satisfies two conditions: $EL \subset L$ and im $(EZ - ZE) \subset L$. Any n by n integer matrix satisfying these two conditions will give an endomorphism of M.

Addition and the operation of an endomorphism on M are performed just as in the case of a finite additive group. If x is an element of M then ζx is the group element γx. Thus to compute ax for any $a \in \mathbb{Z}[\zeta]$ we let $(a_0, \ldots, a_{\phi(m)-1})$ encode a and compute

$$ax = \sum_{i=0}^{\phi(m)-1} a_i \zeta^i x.$$

CHAPTER III

THE POWER RESIDUE SYMBOL

Throughout this chapter, K is an algebraic number field containing all mth roots of unity. We let R be the ring of integers of K.

The propositions and definitions of this chapter are based on Exercises 1 and 2 in [3, pp. 348 ff.]. In Section 1 we work out the first five parts of that exercise, and in Section 2 we use the definition of the extended power residue symbol found in part 10 of Exercise 2.

1. Definition and Properties

Recall that if a and p lie in $\mathbb{Z}$ then the *Legendre symbol* (a/p), also written $\left(\frac{a}{p}\right)$, is 0 if $p \mid a$, 1 if a is a quadratic residue mod p, and -1 if a is a quadratic nonresidue mod p. One can show that when $p \nmid a$ and $p \neq 2$ then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$

and that this is enough to define (a/p). It turns out to be useful to extend this symbol to the *Jacobi symbol*, whose "denominator" can be any integer. Thus if a and b are integers and b has the factorization

$$b = \prod_{i=1}^{k} p_i^{e_i}$$

for some primes p_i and positive integers e_i, then we define the Jacobi symbol (a/b) by

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Let ω be a cube root of unity, fix $a \in \mathbb{Z}[\omega]$ and a prime $\mathfrak{p}$ of $\mathbb{Z}[\omega]$ with $N(\mathfrak{p}) \neq 3$, and declare that the *cubic residue symbol* $(a/\mathfrak{p})_3$ is a cube root of unity satisfying

$$\left(\frac{a}{\mathfrak{p}}\right)_3 \equiv a^{(N(\mathfrak{p})-1)/3} \mod \mathfrak{p}.$$

One can prove that this property suffices to define $(a/\mathfrak{p})_3$ and also that $(a/\mathfrak{p})_3 = 1$ if and only if there exists an $x \in \mathbb{Z}[\omega]$ such that $x^3 \equiv a \mod \mathfrak{p}$. See [7] for a thorough discussion of the Legendre symbol, Jacobi symbol, and cubic residue symbol and elementary proofs of their properties.

It is natural to try to continue in this way, and to extend the notion of power residue symbol to general number fields. This is the goal of the present chapter.

First we need some notation. For any $a_1, \ldots, a_r \in K$, let $S(a_1, \ldots, a_r)$ be the set of all prime ideals $\mathfrak{p}$ in R for which either $\mathfrak{p} \mid mR$ or $|a_i|_\mathfrak{p} \neq 1$ for some $i \in \{1, \ldots, r\}$. Let $\mathcal{I}(a_1, \ldots, a_r)$ be the set of ideals in R which are relatively prime to every ideal in $S(a_1, \ldots, a_r)$.

Elements of $\mathcal{I}(a)$ are unramified in extensions of the form $K(x)/K$ with x any mth root of a. We prove this using the following lemma, in which we write μ_m for the group of mth roots of unity.

LEMMA 3.1. *If $\mathfrak{p}$ is a prime in R relatively prime to mR, let $\nu : \mu_m \to (R/\mathfrak{p})^*$ be defined by $\nu(z) = z + \mathfrak{p}$. Then ν is injective.*

PROOF. Clearly ν is a homomorphism. We have the polynomial identity

$$\sum_{i=0}^{m-1} X^i = \frac{X^m - 1}{X - 1} = \prod_{i=1}^{m-1} X - \zeta^i$$

and substituting $X = 1$ we have

$$m = \prod_{i=1}^{m-1} 1 - \zeta^i$$

Suppose that z is in the kernel of ν. Then $1 - z \in \mathfrak{p}$. If $z \neq 1$ we have just seen that $1 - z$ divides m so $m \in \mathfrak{p}$, a contradiction. It follows that $z = 1$ and ν is injective. $\square$

LEMMA 3.2. *If a is a nonzero element of K and x is an element of $\mathbb{C}$ with $x^m = a$ then every ideal in $\mathcal{I}(a)$ is unramified in $K(x)$.*

PROOF. We fix an ideal in $\mathcal{I}(a)$ and show that it must be unramified; clearly it suffices to consider a prime ideal $\mathfrak{p}$ in $\mathcal{I}(a)$.

We would also like to assume without loss of generality that $a \in R$. Our first step toward this goal is to find b and c in R such that $a = b/c$ and $|b|_\mathfrak{p} = |c|_\mathfrak{p} = 1$. Certainly we can find d and e in R such that $a = d/e$. Now write

$$dR = \mathfrak{p}^n \prod_{i=1}^{t} \mathfrak{q}_i^{s_i}$$

for some nonnegative integers n, t, and $s_1, \ldots, s_t$ and some prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ in R. Using Proposition 1.3, we find an element $b \in R$ with $\operatorname{ord}_\mathfrak{p} b = 0$ and $\operatorname{ord}_{\mathfrak{q}_i} b = s_i$ for each i. Then

$$bR = \mathfrak{d} \prod_{i=1}^{t} \mathfrak{q}_i^{s_i}$$

with $\mathfrak{d}$ an ideal of R relatively prime to $\mathfrak{p}$ and all the $\mathfrak{q}_i$. Now let $c = be/d$. Clearly $\operatorname{ord}_\mathfrak{p} e = n$ so $\operatorname{ord}_\mathfrak{p} c = 0$; it follows that c has nonnegative order at every prime so $c \in R$. We have thus found b and c in R with $|b|_\mathfrak{p} = |c|_\mathfrak{p} = 1$ and $b/c = a$.

Certainly $K(cx) = K(x)$ and

$$(cx)^m = c^m x^m = c^m a = bc^{m-1}.$$

By the result of the previous paragraph $\mathfrak{p} \in \mathcal{I}(bc^{m-1})$. It follows that by replacing a with bc^{m-1} and x with cx, we can assume that a lies in R without loss of generality.

Next we fix a prime ideal $\mathfrak{P}$ in $K(x)$ lying over $\mathfrak{p}$ and let $E = E(\mathfrak{P}|\mathfrak{p})$. Since $|E|$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, we need only show that E is trivial to complete our proof.

Let us therefore fix some element $\sigma \in E$. Clearly x is an algebraic integer so $\sigma(x) \equiv x \bmod \mathfrak{P}$. We know that σ maps x to one of its conjugates, which must be of the form ζx for some mth root of unity $\zeta \neq 1$. Therefore we have $\zeta x \equiv x \bmod \mathfrak{P}$ so

$$(1 - \zeta)x \in \mathfrak{P}.$$

Since $\mathfrak{P}$ is prime we must have either $x \in \mathfrak{P}$ or $1 - \zeta \in \mathfrak{P}$.

If $x \in \mathfrak{P}$ then $x(x^{m-1}) = a \in \mathfrak{P}$ so $a \in \mathfrak{P} \cap K = \mathfrak{p}$, but this is impossible since $|a|_{\mathfrak{p}} = 1$. If $1-\zeta \in \mathfrak{P}$ then $1-\zeta \in \mathfrak{p}$ (since $1-\zeta \in K$); now by Lemma 3.1 we have $\zeta = 1$ and we conclude that σ is the trivial automorphism. It follows that E is trivial, establishing the desired result. $\square$

DEFINITION. Suppose we are given a nonzero element $a \in K$ and an ideal $\mathfrak{b}$ in $\mathcal{I}(a)$. Choose $x \in \mathbb{C}$ such that $x^m = a$ and let σ be the Frobenius automorphism of the abelian extension $K(x)/K$ associated to the ideal $\mathfrak{b}$. Then the *power residue symbol* $(a/\mathfrak{b})$ is defined by

$$\left(\frac{a}{\mathfrak{b}}\right) = \frac{\sigma(x)}{x}.$$

We must check two things to verify that this definition is valid. First, we must show that $\mathfrak{b}$ is unramified in $K(x)/K$ so that the Frobenius automorphism is defined; this we did in Lemma 3.2. And second, we must show that $(a/\mathfrak{b})$ is independent of the choice of x. Observe that any $y \in \mathbb{C}$ for which $y^m = a$ satisfies $\zeta y = x$ for some mth root of unity ζ. Thus

$$\frac{\sigma(x)}{x} = \frac{\sigma(\zeta y)}{\zeta y} = \frac{\zeta\sigma(y)}{\zeta y} = \frac{\sigma(y)}{y}$$

establishing the result.

PROPOSITION 3.3. *The power residue symbol* $(a/\mathfrak{b})$ *is always an* m*th root of unity.*

PROOF. Fix a nonzero element a in K and an ideal $\mathfrak{b}$ in $\mathcal{I}(a)$. Choose $x \in \mathbb{C}$ with $x^m = a$ and let σ be the Frobenius automorphism of $\mathfrak{b}$. We have

$$\left(\frac{a}{\mathfrak{b}}\right)^m = \frac{\sigma(x)^m}{x^m} = \frac{\sigma(x^m)}{x^m} = \frac{\sigma(a)}{a} = 1. \quad \square$$

The power residue symbol is an extension of the Jacobi symbol and shares its characteristic properties, as we see in the following results.

PROPOSITION 3.4. *Fix nonzero elements* a, a' *in* K *and an ideal* $\mathfrak{b}$ *in* $\mathcal{I}(a, a')$. *Then*

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right).$$

PROOF. Choose $x, x' \in \mathbb{C}$ with $x^m = a$ and $(x')^m = a'$. Let σ, τ, μ, and η be the Frobenius automorphisms of $\mathfrak{b}$ in the extensions $K(x)/K$,

$K(x')/K$, $K(xx')/K$, and $K(x,x')/K$ respectively (this makes sense since all of these extensions are abelian by Proposition 1.7). By Proposition 1.5, $\sigma(x) = \eta(x)$, $\tau(x') = \eta(x')$, and $\mu(xx') = \eta(xx')$. Thus

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \frac{\mu(xx')}{xx'} = \frac{\eta(xx')}{xx'} = \frac{\eta(x)}{x}\frac{\eta(x')}{x'} = \frac{\sigma(x)}{x}\frac{\tau(x')}{x'} = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right). \quad \square$$

PROPOSITION 3.5. *Fix a nonzero element $a \in K$ and ideals $\mathfrak{b}$, $\mathfrak{b}'$ in $\mathcal{I}(a)$. Then*

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right).$$

PROOF. Fix $x \in \mathbb{C}$ with $x^m = a$. Let σ and τ be the Frobenius automorphisms of $\mathfrak{b}$ and $\mathfrak{b}'$ in $K(x)/K$. Then the Frobenius automorphism of $\mathfrak{b}\mathfrak{b}'$ is $\sigma\tau$ and

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \frac{\sigma(\tau(x))}{x} = \frac{\sigma\left(x\left(\frac{a}{\mathfrak{b}'}\right)\right)}{x} = \frac{\sigma(x)}{x}\left(\frac{a}{\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right). \quad \square$$

PROPOSITION 3.6. *If a is a nonzero element of K, $\mathfrak{p}$ is a prime ideal in $\mathcal{I}(a)$, and p is the rational prime lying under $\mathfrak{p}$, then m divides $(N(\mathfrak{p})-1)$ and*

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{N(\mathfrak{p})-1}{m}} \mod \mathfrak{p}.$$

PROOF. First we show that m divides $N(\mathfrak{p})-1$. In chapter 1 we showed that when K is the cyclotomic field $\mathbb{Q}(\zeta)$, $f(\mathfrak{p} \mid p)$ is the order of p mod m. Since by definition $N(\mathfrak{p}) = p^{f(\mathfrak{p}|p)}$ we see that m divides $N(\mathfrak{p}) - 1$ in this special case.

Turning to the general case we let $\mathfrak{p}'$ be the prime of $\mathbb{Z}[\zeta]$ lying above p and below $\mathfrak{p}$; then $N(\mathfrak{p}')^k = N(\mathfrak{p})$ for some integer k and since $N(\mathfrak{p}') \equiv 1$ mod m we see immediately that $N(\mathfrak{p}) \equiv 1 \bmod m$.

Now fix $x \in \mathbb{C}$ with $x^m = a$ and let $\mathfrak{P}$ be a prime of $K(x)$ lying over $\mathfrak{p}$. Since $|\cdot|_{\mathfrak{P}}$ extends $|\cdot|_{\mathfrak{p}}$,

$$1 = |a|_{\mathfrak{p}} = |x^m|_{\mathfrak{p}} = |x^m|_{\mathfrak{P}} = (|x|_{\mathfrak{P}})^m$$

and so $|x|_{\mathfrak{P}} = 1$. Let σ be the Frobenius automorphism in $\mathrm{Gal}(K(x)/K)$ associated to $\mathfrak{p}$. Note that by definition

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}. \tag{1}$$

Further,

$$a^{\frac{N(\mathfrak{p})-1}{m}} = (x^m)^{\frac{N(\mathfrak{p})-1}{m}} = x^{N(\mathfrak{p})-1} = \frac{x^{N(\mathfrak{p})}}{x}. \tag{2}$$

Combining (1) and (2) gives

$$a^{\frac{N(\mathfrak{p})-1}{m}} \equiv \frac{\sigma(x)}{x} \mod \mathfrak{P}$$

and $\sigma(x)/x$ is just $(a/\mathfrak{p})$. Since both a and $(a/\mathfrak{p})$ lie in K and $\mathfrak{p} = \mathfrak{P} \cap K$, we see that

$$a^{\frac{N(\mathfrak{p})-1}{m}} \equiv \left(\frac{a}{\mathfrak{p}}\right) \mod \mathfrak{p}. \quad \square$$

Note that the condition given in this proposition is clearly a defining property of the power residue symbol, by Lemma 3.1.

Note also that it is easy to use this result and one of the powering algorithms [4, pp. 8–12] to give a polynomial-time algorithm to compute $\left(\frac{a}{\mathfrak{p}}\right)$. However, this only works when the input ideal is known to be prime. If the input ideal is not prime then we can factor it and apply this algorithm, but unfortunately no polynomial-time algorithm is known for the factorization process, so this algorithm is not fast enough. We will find a way around this difficulty in the following two chapters.

PROPOSITION 3.7. *If a and a' are elements of R, $\mathfrak{b}$ is an ideal in $\mathcal{I}(a)$, and $a \equiv a' \mod \mathfrak{b}$, then $\mathfrak{b} \in \mathcal{I}(a')$ and*

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a'}{\mathfrak{b}}\right).$$

PROOF. Certainly we may assume without loss of generality that $\mathfrak{b}$ is a prime $\mathfrak{p}$. If $a' \in \mathfrak{p}$ then $a \in \mathfrak{p}$, a contradiction; hence $|a'|_{\mathfrak{p}} = 1$ so that $\mathfrak{p} \in \mathcal{I}(a')$.

Using $\equiv$ to mean equivalence mod $\mathfrak{p}$, we have

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{N(\mathfrak{p})-1}{m}} \equiv (a')^{\frac{N(\mathfrak{p})-1}{m}} \equiv \left(\frac{a'}{\mathfrak{p}}\right).$$

By Lemma 3.1, whenever two mth roots of unity are equivalent mod $\mathfrak{p}$ they must be equal. This gives the desired result. $\square$

PROPOSITION 3.8. *Suppose that a is a nonzero element of K and $\mathfrak{p}$ is a prime ideal in $\mathcal{I}(a)$. Let K' be the completion of K at $\mathfrak{p}$ and let $\overline{a}$ be the image of a in $R/\mathfrak{p}$. Then the following are equivalent:*

(1) $(a/\mathfrak{p}) = 1$.
(2) *There exists an x in $R/\mathfrak{p}$ such that $x^m = \overline{a}$.*
(3) *There exists a y in K' such that $y^m = a$.*

PROOF. (1) $\Rightarrow$ (2). The multiplicative group of any finite field is cyclic, so we may let v be a generator of $(R/\mathfrak{p})^*$. Write $v^j = \overline{a}$ for some integer j. By Proposition 3.6 we have

$$1 = (\overline{a})^{\frac{N(\mathfrak{p})-1}{m}} = (v^j)^{\frac{N(\mathfrak{p})-1}{m}} = v^{\frac{j|(R/\mathfrak{p})^*|}{m}}.$$

and so $|(R/\mathfrak{p})^*|$ divides $j|(R/\mathfrak{p})^*|/m$. It follows that m divides j and so we may let $x = v^{j/m}$; clearly $x^m = \overline{a}$ as desired.

(2) $\Rightarrow$ (3). Let $f(X) = X^m - a$. By (2) we have an $x \in R/\mathfrak{p}$ with $x^m = \overline{a}$; let $u \in R$ be any lift of x. Then

$$f(u) = u^m - a \in \mathfrak{p}$$

so $|f(u)|_\mathfrak{p} < 1$. Also,

$$|f'(u)|_\mathfrak{p} = |mu^{m-1}|_\mathfrak{p} = 1$$

since clearly $|u|_\mathfrak{p} = 1$, $|m|_\mathfrak{p} = 1$. The conditions of Hensel's Lemma (Proposition 1.4) are satisfied. Thus for some $y \in K'$, $f(y) = 0$ so $y^m = a$ as desired.

(3) $\Rightarrow$ (1). Write $|\cdot|$ for both the valuation $|\cdot|_\mathfrak{p}$ on K and its extension to K'. Then

$$1 = |a| = |y^m| = |y|^m$$

so $|y| = 1$. Let

$$P = \{x \in K' \mid |x| < 1\}, \quad S = \{x \in K' \mid |x| \leq 1\}.$$

Then as we stated in Chapter 1, Section 2, S is a ring, P is an ideal in S, and $R/\mathfrak{p}$ and S/P are isomorphic. Let $\overline{y}$ be the image of y in S/P. Then $\overline{y}^{|(R/\mathfrak{p})^*|} = 1$ whence $|y^{|(R/\mathfrak{p})^*|} - 1| < 1$. We now have

$$|a^{\frac{N(\mathfrak{p})-1}{m}} - 1| = |(y^m)^{\frac{N(\mathfrak{p})-1}{m}} - 1| = |y^{|(R/\mathfrak{p})^*|} - 1| < 1$$

and using Proposition 3.6 we see that $(a/\mathfrak{p}) - 1 \in \mathfrak{p}$. Lemma 3.1 tells us that $(a/\mathfrak{p}) = 1$ as desired. $\square$

2. An Extension of the Power Residue Symbol

Calculation of the mth power residue symbol $(a/\mathfrak{b})$ will require an extended version of the symbol. In this extended symbol the ideal $\mathfrak{b}$ need not be in $\mathcal{I}(a)$, but $\mathfrak{b}$ is required to be principal.

For any $a \in K$, we write $\mathcal{P}(a)$ for the set of all prime ideals in $\mathcal{I}(a)$.

DEFINITION. If a and b are any elements of K with b nonzero then the *extended power residue symbol* of a and b, written (a/b), is defined by

$$\left(\frac{a}{b}\right) = \prod_{\mathfrak{p} \in \mathcal{P}(a)} \left(\frac{a}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b}.$$

where the symbol on the right is the power residue symbol defined in the previous section.

For any a in K and b in R with b nonzero and $bR \in \mathcal{I}(a)$, we can verify immediately that $(a/b) = (a/bR)$, so our new symbol really does extend the previous one. Further, it is also obvious that for any a, b, and b' in K with b, b' nonzero,

$$\left(\frac{a}{b}\right)\left(\frac{a}{b'}\right) = \left(\frac{a}{bb'}\right).$$

However, the reader should take warning that the rule

$$\left(\frac{a}{b}\right)\left(\frac{a'}{b}\right) = \left(\frac{aa'}{b}\right) \tag{3}$$

for a, a' and b in K with b nonzero does *not* work in general. For example, suppose that

$$bR = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$$

where the $\mathfrak{p}_i$ are distinct primes in R, all relatively prime to mR, and the e_i are positive integers. Suppose further that a and b are relatively prime but that $\gcd(a'R, bR) = \mathfrak{p}_1$. Then $(aa'/b) = (a/b)(a'/b)(a/\mathfrak{p}_1)^{-1}$, as the reader may easily work out, and we see that (3) does not hold if $(a/\mathfrak{p}_1) \neq 1$.

We will need one other extension of our earlier results.

LEMMA 3.9. *If a, a', and b are elements of R such that b is nonzero and $a \equiv a' \bmod b$, then*

$$\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right).$$

PROOF. Let $\mathcal{B}$ be the set of primes dividing bR and fix $\mathfrak{p} \in \mathcal{P}(a) \cap \mathcal{B}$. Suppose that $\mathfrak{p} \mid a'R$; then $a' \in \mathfrak{p}$ and, since $\mathfrak{p} \mid bR$, $b \in \mathfrak{p}$. Since $a \equiv a' \bmod b$, there is some $c \in R$ such that $a = a' + cb$. The integer $a' + cb$ is in $\mathfrak{p}$ and so $\mathfrak{p} \mid aR$, which is a contradiction. Thus $\mathfrak{p} \nmid a'R$, so $\mathfrak{p} \in \mathcal{P}(a') \cap \mathcal{B}$. Interchanging a and a' gives a similar result, and so $\mathcal{P}(a) \cap \mathcal{B} = \mathcal{P}(a') \cap \mathcal{B}$. Further, it is clear that for any $\mathfrak{p} \in \mathcal{P}(a) \cap \mathcal{B}$, we have $a \equiv a' \bmod \mathfrak{p}$. Now

$$\left(\frac{a}{b}\right) = \prod_{\mathfrak{p} \in \mathcal{P}(a) \cap \mathcal{B}} \left(\frac{a}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b} = \prod_{\mathfrak{p} \in \mathcal{P}(a') \cap \mathcal{B}} \left(\frac{a'}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b} = \left(\frac{a}{b}\right). \quad \square$$

CHAPTER IV

REDUCTION TO THE CYCLOTOMIC CASE

In the article "Computing Jacobi symbols in algebraic number fields" [11], Hendrik W. Lenstra, Jr. gives in some detail a method for computing the quadratic power residue symbol. On the last page of the paper, Lenstra sketches a method for reducing the computation of an mth power residue symbol in a general number field K to the computation of several mth power residue symbols in the cyclotomic field $\mathbb{Q}(\zeta)$. In this chapter we fill in the details of Lenstra's method; in the next we will explain how to compute mth power residue symbols in $\mathbb{Q}(\zeta)$.

Lenstra's method uses a new object, which we will call the *signature* (ϵ, M) of a $\mathbb{Z}[\zeta]$-module M and an endomorphism ϵ of M. It turns out that if $M = R/\mathfrak{b}$ for a ring of integers R and an ideal $\mathfrak{b}$ of R, and if ϵ is multiplication by some $a \in R$, then

$$(\epsilon, M) = \left(\frac{a}{\mathfrak{b}}\right).$$

The multiplicative property

$$\left(\frac{c/d}{\mathfrak{b}}\right) = \left(\frac{c}{\mathfrak{b}}\right)\left(\frac{d}{\mathfrak{b}}\right)^{-1}$$

then makes it trivial to compute $(a/\mathfrak{b})$ for any $a \in K$ with $a = c/d$, c and d being elements of R.

The reader will notice, however, that when we turn to computations in the second half of the chapter, we assume only that M is $A/\mathfrak{b}$ for an order A in a number field with $\zeta \in A$ and an ideal $\mathfrak{b}$ in A. We do this because it is difficult in general to compute the full ring of integers of a number field K, but it is easy to generate orders in K (for example, if $K = \mathbb{Q}(\alpha)$ and α is an algebraic integer then $\mathbb{Z}[\alpha]$ is always an order). In many applications,

for example the number field sieve for factoring integers, one assumes that the order A is the full ring of integers R and computes merrily until some evidence appears that $A \neq R$; then one enlarges A and continues. Our algorithm fits nicely into this scheme. See [1] for a discussion of these issues.

We introduce the notation

$$\langle x_1, \ldots, x_k \rangle,$$

where $x_1, \ldots, x_k$ are elements of a $\mathbb{Z}[\zeta]$-module M, to mean the set

$$\left\{ \sum_{i=1}^{k} a_i x_i \mid a_i \in \mathbb{Z}[\zeta] \right\}.$$

One assumption will be made throughout the chapter: if R is a ring containing $\mathbb{Z}[\zeta]$ and $\mathfrak{b}$ is an ideal in R then we make $R/\mathfrak{b}$ into a $\mathbb{Z}[\zeta]$-module in a natural way. If $a \in \mathbb{Z}[\zeta]$ and $x \in R/\mathfrak{b}$, then we let $\overline{a}$ be the image of a in $R/\mathfrak{b}$ and let $ax = \overline{a}x$. We extend this notion to a direct sum of rings of the form $R/\mathfrak{b}$ in the obvious way, letting $a(x_1, \ldots, x_t) = (ax_1, \ldots, ax_t)$.

1. Definition and Properties of the Signature

DEFINITION. A finite $\mathbb{Z}[\zeta]$-module M is *admissible* if $\gcd(|M|, m) = 1$.

DEFINITION. If M is a finite admissible $\mathbb{Z}[\zeta]$-module, we say that $x, y \in M$ are *equivalent* whenever there exists some $k \in \{0, 1, 2, \ldots, m-1\}$ with $x = \zeta^k y$. We write $x \sim y$ for the statement "x and y are equivalent".

LEMMA 4.1. *If M is a finite admissible $\mathbb{Z}[\zeta]$-module, then $\sim$ is an equivalence relation on M. Each nonzero equivalence class has m elements; zero is the only element in its equivalence class. If M is finite, then $|M| \equiv 1 \mod m$.*

PROOF. The only nonobvious statement is that each nonzero equivalence class has m elements. To prove this, fix $x \in M$ with $x \neq 0$ and let k be the number of elements in the class containing x; we show that $k = m$.

Certainly $\zeta^k x = x$ and k is the smallest positive integer with this property. Since $\zeta^m x = x$, we see that $k \leq m$. Suppose, for a contradiction, that $k < m$. In the course of proving Lemma 3.1 we showed that $\zeta^k - 1$ divides m, so since $(\zeta^k - 1)x = 0$ we have $mx = 0$. Clearly $|M|x = 0$, and since $\gcd(|M|, m) = 1$ there exist a and b in $\mathbb{Z}$ with $a|M| + bm = 1$. It follows that $1x = 0$ which is the desired contradiction. □

If a map ϵ from a $\mathbb{Z}[\zeta]$-module to itself satisfies $\epsilon(\zeta x) = \zeta \epsilon(x)$ for every x in the module, we say that ϵ *commutes with* ζ.

LEMMA 4.2. *Suppose that M is an admissible $\mathbb{Z}[\zeta]$-module, C is the set of equivalence classes of M, and $\epsilon : M \to M$ is a map which commutes with ζ. Then ϵ acts faithfully on equivalence classes, inducing a map from C to C which we also call ϵ; if ϵ is bijective then so is the induced map.*

PROOF. Fix u and v in M with $u \sim v$ and write $u = \zeta^k v$ for some $k \in \{0, 1, 2, \dots, m-1\}$. Then $\epsilon(u) = \zeta^k \epsilon(v)$ so $\epsilon(u) \sim \epsilon(v)$; it follows that ϵ acts faithfully on equivalence classes.

Suppose that ϵ is bijective; we need only show that the induced map is injective. Fix classes U and V in C and let u and v be representatives of U and V. If $\epsilon(U) = \epsilon(V)$, then $\epsilon(u) \sim \epsilon(v)$ and so $\epsilon(u) = \zeta^k \epsilon(v) = \epsilon(\zeta^k v)$. Since ϵ is bijective, $u = \zeta^k v$ so $u \sim v$ whence $U = V$, establishing that the induced map is injective. □

DEFINITION. If M is a finite admissible $\mathbb{Z}[\zeta]$-module then a *representative set* for M is a subset of M containing exactly one representative of every nonzero equivalence class.

Fix a representative set S of a finite admissible $\mathbb{Z}[\zeta]$-module M. We define maps $\beta_S : M \to S$ and $\gamma_S : M \to \{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\}$ by setting $\beta_S(x)$ equal to the representative of the class containing x and declaring that

$$x = \gamma_S(x)\beta_S(x).$$

PROPOSITION 4.3. *Suppose that M is a finite admissible $\mathbb{Z}[\zeta]$-module, that both S and T are representative sets for M, and that $\epsilon : M \to M$ is a bijective map commuting with ζ. Then*

$$\prod_{s \in S} \gamma_S \epsilon(s) = \prod_{t \in T} \gamma_T \epsilon(t). \tag{1}$$

PROOF. We prove the proposition in the case where S and T differ by a single element; the full result follows since for general representative sets S and T, there exist representative sets $S_1 = S, S_2, S_3, \dots, S_r = T$ with S_i and S_{i+1} differing by a single element for each $i = 1, 2, \dots, r-1$.

Assume, then, that only on a single equivalence class E do S and T differ. Let s and t be the representatives of E in S and T respectively, and write $t = \zeta^k s$ for some $k \in \{0, 1, 2, \dots, m-1\}$.

Clearly we may cancel all representatives of equivalence classes other than E and $\epsilon^{-1}(E)$ in (1). When $E = \epsilon^{-1}(E)$, (1) becomes

$$\gamma_S \epsilon(s) = \gamma_T \epsilon(t)$$

and when $E \neq \epsilon^{-1}(E)$, (1) becomes

$$\gamma_S\epsilon(s)\gamma_S\epsilon(u) = \gamma_T\epsilon(t)\gamma_T\epsilon(u)$$

where u is the representative of $\epsilon^{-1}(E)$ (necessarily u is the representative in both S and T). We now prove these equations hold in their respective cases.

First suppose that $E = \epsilon(E)$. Then

$$\epsilon(t) = \gamma_T\epsilon(t)t = \gamma_T\epsilon(t)\zeta^k s$$

and

$$\epsilon(t) = \zeta^k\epsilon(s) = \zeta^k\gamma_S\epsilon(s)s.$$

Setting the right sides equal we see that $\gamma_S\epsilon(s) = \gamma_T\epsilon(t)$ as desired.

Next we suppose that $\epsilon(E) \neq E$. Let v be the representative of $\epsilon(E)$; necessarily $v \in S$ and $v \in T$. Observe that

$$\begin{aligned}
\epsilon(u) &= \gamma_T\epsilon(u)t = \gamma_T\epsilon(u)\zeta^k s,\\
\epsilon(u) &= \gamma_S\epsilon(u)s,\\
\epsilon(t) &= \gamma_T\epsilon(t)v, \text{ and}\\
\epsilon(t) &= \zeta^k\epsilon(s) = \zeta^k\gamma_S\epsilon(s)v.
\end{aligned}$$

From these we get

$$\begin{aligned}
\gamma_T\epsilon(u)\zeta^k &= \gamma_S\epsilon(u) \text{ and}\\
\gamma_T\epsilon(t) &= \zeta^k\gamma_S\epsilon(s).
\end{aligned}$$

and it follows that

$$\gamma_S\epsilon(s)\gamma_S\epsilon(u) = \gamma_T\epsilon(t)\gamma_T\epsilon(u)$$

as desired. □

DEFINITION. If M is a finite admissible $\mathbb{Z}[\zeta]$-module and $\epsilon : M \to M$ is a bijective map commuting with ζ, then the *signature of M and ϵ*, denoted (ϵ, M), is

$$\prod_{s\in S} \gamma_S\epsilon(s)$$

This definition is unambiguous since by Proposition 4.3 the choice of S does not affect the value of (ϵ, M). Since we shall henceforth choose only one representative set for each module we consider, we shall drop the subscript of the functions β_S and γ_S, letting the choice of representative set be clear from context.

PROPOSITION 4.4. *If M is a finite admissible $\mathbb{Z}[\zeta]$-module and $\epsilon : M \to M$ and $\epsilon' : M \to M$ are bijective maps commuting with ζ, then*

$$(\epsilon\epsilon', M) = (\epsilon, M)(\epsilon', M).$$

PROOF. Let S be a representative set for M. Then for any $s \in S$,

$$\begin{aligned}(\epsilon\epsilon')(s) &= \epsilon(\gamma\epsilon'(s)\beta\epsilon'(s)) \\ &= \gamma\epsilon'(s)\epsilon(\beta\epsilon'(s)) \\ &= \gamma\epsilon'(s)\gamma\epsilon(\beta\epsilon'(s))\beta\epsilon(\beta\epsilon'(s))\end{aligned}$$

so that

$$\gamma(\epsilon\epsilon')(s) = \gamma\epsilon'(s)\gamma\epsilon(\beta\epsilon'(s))$$

By Lemma 4.2, $\beta\epsilon'(s)$ runs through S as s runs through S, and so we see that

$$\prod_{s\in S} \gamma(\epsilon\epsilon')(s) = \prod_{s\in S} \gamma\epsilon(s) \prod_{s\in S} \gamma\epsilon'(s)$$

The proposition follows. □

PROPOSITION 4.5. *Suppose that M, M', and M'' are finite admissible $\mathbb{Z}[\zeta]$-modules such that the following diagram commutes and is exact:*

$$\begin{array}{ccccccccc} \{0\} & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{f} & M'' & \longrightarrow & \{0\} \\ & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\ \{0\} & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{f} & M'' & \longrightarrow & \{0\} \end{array} \tag{2}$$

Then if ϵ is bijective,

$$(\epsilon, M) = (\epsilon', M')(\epsilon'', M'').$$

It is clear to see from the diagram that ϵ' and ϵ'' are bijective whenever ϵ is, so the signatures (ϵ', M') and (ϵ'', M'') are defined.

PROOF. We may find a function $g : M'' \to M$ which commutes with ζ and for which $fg = 1$ as follows: set $g(0) = 0$ and, for each z in a representative set Z of M'', let $g(z)$ be any element of $f^{-1}(z)$; declaring

that g commutes with ζ now defines g. It follows that any element $x \in M$ has a unique representation in the form

$$x = i(r) + g(z)$$

with $r \in M'$, $g \in M''$.

Now let R and Z be representative sets for M' and M'' respectively and form the set

$$S = \{i(r) \mid r \in R\} \cup \{i(r) + g(z) \mid r \in M', z \in Z\}.$$

We claim that S is a representative set for M. First we show that if two elements of S are equivalent then they are equal. Fix s and s' in S and suppose that $s \sim s'$; write $s = \zeta^k s'$ for some $k \in \{0, 1, 2, \dots, m-1\}$. There are three possibilities:

(1) $s = i(r)$, $s' = i(r')$ for some $r, r' \in R$. Then $i(r) = i(\zeta^k r')$, so $r = \zeta^k r'$; it follows that $r = r'$ so $s = s'$.
(2) $s = i(r) + g(z)$, $s' = i(r')$ for some $r \in M'$, $r' \in R$, $z \in Z$. Then $i(r) + g(z) = i(\zeta^k r')$ so $z = 0$, an impossibility.
(3) $s = i(r) + g(z)$, $s' = i(r') + g(z')$ for some $r, r' \in M'$ and $z, z' \in Z$. Then $i(r) + g(z) = i(\zeta^k r') + g(\zeta^k z')$ so $z = \zeta^k z'$; it follows that $z = z'$ so $k = 0$ and $s = s'$.

We have thus established that the elements of S all lie in distinct equivalence classes. In addition,

$$|S| = \frac{|M'| - 1}{m} + |M'| \left(\frac{|M''| - 1}{m} \right) = \frac{|M'||M''| - 1}{m} = \frac{|M| - 1}{m}$$

and $\frac{|M|-1}{m}$ is the number of nonzero equivalence classes in M. Thus S has exactly one element in each nonzero equivalence class, so S is a representative set for M as claimed.

Next we define three new mappings of M to itself. Fix $x \in M$ and write $x = i(r) + g(z)$ with $r \in M'$, $z \in M''$; then let

$$\rho(x) = i(\epsilon'(r)) + g(z) \quad \text{and} \quad \sigma(x) = i(r) + g(\epsilon''(z)).$$

It is clear that ρ and σ are bijective and commute with ζ; thus we may let $\tau = \sigma^{-1}\rho^{-1}\epsilon$ and τ is also a bijective mapping which commutes with ζ. We now calculate (ρ, M), (σ, M), and (τ, M).

The signature (ρ, M). Fix $s \in S$ and write $s = i(r) + g(z)$, $\beta\rho(s) = i(r') + g(z')$ with $r, r' \in M'$, $z, z' \in Z \cup \{0\}$. If $z = 0$, then $r \in R$ and

$$\rho(s) = i(\epsilon'(r)) = i(\gamma\epsilon'(r)\beta\epsilon'(r)),$$
$$\rho(s) = i(\gamma\rho(s)r') + g(\gamma\rho(s)z').$$

It follows that $z' = 0$ and $\gamma\epsilon'(r)\beta\epsilon'(r) = \gamma\rho(s)r'$. Since $z' = 0$, we must have $r' \in R$; since $\beta\epsilon'(r) \in R$ also, we have $\beta\epsilon'(r) = r'$ and $\gamma\epsilon'(r) = \gamma\rho(s)$. If, on the other hand, $z \neq 0$, then $z \in Z$. We have

$$\rho(s) = i(\epsilon'(r)) + g(z),$$
$$\rho(s) = i(\gamma\rho(s)r') + g(\gamma\rho(s)z').$$

It follows that $z = \gamma\rho(s)z'$ and thus $z' \neq 0$. Hence $z' \in Z$, which means that $z = z'$ and $\gamma\rho(s) = 1$. We now see that

$$\prod_{s\in S} \gamma\rho(s) = \prod_{r\in R} \gamma\rho(i(r)) = \prod_{r\in R} \gamma\epsilon'(r)$$

and so $(\rho, M) = (\epsilon', M')$.

The signature (σ, M). Fix $s \in S$ and write $s = i(r) + g(z)$, $\beta\sigma(s) = i(r') + g(z')$ with $r, r' \in M'$ and $z, z' \in Z \cup \{0\}$. If $z = 0$, then $\sigma(s) = s$ so $\gamma\sigma(s) = 1$. If $z \neq 0$, then $z \in Z$ and

$$\sigma(s) = i(r) + g(\epsilon''(z)) = i(r) + g(\gamma\epsilon''(z)\beta\epsilon''(z)),$$
$$\sigma(s) = i(\gamma\sigma(s)r') + g(\gamma\sigma(s)z')$$

It follows that $\gamma\epsilon''(z)\beta\epsilon''(z) = \gamma\sigma(s)z'$. Since ϵ'' is bijective, we have $\beta\epsilon''(z) \neq 0$ so $z' \neq 0$ whence $z' \in Z$. This means that $\beta\epsilon''(z) = z'$ so $\gamma\sigma(s) = \gamma\epsilon''(z)$. Now

$$\prod_{s\in S} \gamma\sigma(s) = \prod_{r\in M'} \prod_{z\in Z} \gamma\sigma(i(r) + g(z)) = \prod_{r\in M'} \prod_{z\in Z} \gamma\epsilon''(z)$$
$$= \left(\prod_{z\in Z} \gamma\epsilon''(z)\right)^{|M'|} = \prod_{z\in Z} \gamma\epsilon''(z)$$

since $|M'| \equiv 1 \bmod m$ by Lemma 4.1. We see that $(\sigma, M) = (\epsilon'', M'')$.

The signature (τ, M). Fix $s \in S$ and write $s = i(r) + g(z)$, $\beta\tau(s) = i(r') + g(z')$ with $r, r' \in M'$, $z, z' \in Z \cup \{0\}$. If $z = 0$ then

$$\tau(s) = \tau(i(r)) = (\sigma^{-1}\rho^{-1})(\epsilon(i(r))) = (\sigma^{-1}\rho^{-1})(i(\epsilon'(r))) = i(r) = s$$

so $\gamma\tau(s) = 1$. If $z \neq 0$ then $z \in Z$. Observe that if $\beta\epsilon(s) = i(r'') + g(z'')$ with $r'' \in M'$, $z'' \in Z''$, then

$$f(\epsilon(s)) = \gamma\epsilon(s)z'',$$
$$\epsilon''(f(s)) = \epsilon''(z).$$

Since $f\epsilon = \epsilon'' f$, we see that $\gamma\epsilon(s)z'' = \epsilon''(z)$. It follows that

$$\epsilon(s) = i(\gamma\epsilon(s)r'') + g(\epsilon''(z)),$$

and of course this equation also holds, trivially, when $\beta\epsilon(s) = i(r'')$ for some $r'' \in R$. Thus

$$\tau(s) = (\sigma^{-1}\rho^{-1})(i(\gamma\epsilon(s)r'') + g(\epsilon''(z)) = i(\epsilon'^{-1}(\gamma\epsilon(s)r'')) + g(z),$$
$$\tau(s) = i(\gamma\tau(s)r') + g(\gamma\tau(s)z').$$

It follows that $z = \gamma\tau(s)z'$ so $z' \neq 0$ whence $z' \in Z$; we see that $z = z'$ so $\gamma\tau(s) = 1$. Thus $(\tau, M) = 1$.

Now by Proposition 4.4,

$$(\epsilon, M) = (\rho\sigma\tau, M) = (\rho, M)(\sigma, M)(\tau, M) = (\epsilon', M')(\epsilon'', M''). \quad \square$$

2. The Signature and the Power Residue Symbol

We turn now to the relationship between the signature and the power residue symbol.

PROPOSITION 4.6. *Suppose that K is a number field containing all m-th roots of unity with ring of integers R. If a is a nonzero element of R, $\mathfrak{p}$ is a prime ideal of R in $\mathcal{I}(a)$, and $\epsilon : R/\mathfrak{p} \to R/\mathfrak{p}$ is defined by $\epsilon(x) = ax$ for every $x \in R/\mathfrak{p}$, then*

$$\left(\frac{a}{\mathfrak{p}}\right) = (\epsilon, R/\mathfrak{p})$$

Clearly ϵ is bijective and $R/\mathfrak{p}$ is admissible, so the signature $(\epsilon, R/\mathfrak{p})$ is defined.

PROOF. Let e be the image of ζ in $R/\mathfrak{p}$. Let $t = |(R/\mathfrak{p})^*| = N(\mathfrak{p}) - 1$. Observe that e has order m in $(R/\mathfrak{p})^*$, since if $e^k = 1$ for some $k \in \mathbb{Z}$ then $1 - \zeta^k \in \mathfrak{p}$ and by Lemma 3.1 we have $\zeta^k = 1$ whence $m \mid k$. It follows that for some generator b of $(R/\mathfrak{p})^*$, we have $e = b^{t/m}$; we prove the proposition first for $a = b$.

Let $S = \{1, b, b^2, \ldots, b^{(t/m)-1}\}$; one immediately verifies that S is a representative set for $R/\mathfrak{p}$. If $k \in \{0, 1, 2, \ldots, \frac{t}{m} - 2\}$ then $\epsilon(b^k) = b^{k+1} \in S$ so $\gamma\epsilon(b^k) = 1$. And $\epsilon(b^{(t/m)-1}) = b^{t/m} = e = \zeta \cdot 1$ so $\gamma\epsilon(b^{(t/m)-1}) = \zeta$. It follows that

$$(\epsilon, R/\mathfrak{p}) = \prod_{s \in S} \gamma\epsilon(s) = \zeta.$$

Now by Proposition 3.6, $(b/\mathfrak{p})$ is an mth root of unity equivalent to $b^{t/m} \bmod \mathfrak{p}$, and by Lemma 3.1 it is the only mth root of unity with this property. By construction, $\zeta \equiv b^{t/m} \bmod \mathfrak{p}$ and so $(b/\mathfrak{p}) = \zeta = (\epsilon, R/\mathfrak{p})$, establishing the proposition when $a = b$. Any nonzero a is a power of b, and so the full result follows by multiplicativity of both symbols. □

PROPOSITION 4.7. *Suppose K is a number field containing all mth roots of unity with ring of integers R. If a is a nonzero element in R, and $\mathfrak{b}$ is an ideal in $\mathcal{I}(a)$. Let $\epsilon : R/\mathfrak{b} \to R/\mathfrak{b}$ be multiplication by a; then*

$$\left(\frac{a}{\mathfrak{b}}\right) = (\epsilon, R/\mathfrak{b}).$$

PROOF. Let d be the number of prime factors dividing $\mathfrak{b}$, counting multiplicities; we proceed by induction on d. The base case $d = 1$ was proven in Proposition 4.6; we now assume the result for some d and prove it for $d + 1$. We may write $\mathfrak{b} = \mathfrak{p}\mathfrak{b}'$ where $\mathfrak{p}$ is prime. Let $x_1, \ldots, x_{N(\mathfrak{p})} \in R$ be a set of coset representatives for $R/\mathfrak{p}$ and let $i(x_j + \mathfrak{p}) = x_j + \mathfrak{b}$ for each $j = 1, 2, \ldots, N(\mathfrak{p})$. Also, let $f(x + \mathfrak{b}) = x + \mathfrak{b}'$. Let a' and a'' be the images of a in $R/\mathfrak{p}$ and $R/\mathfrak{b}'$ respectively and let $\epsilon' : R/\mathfrak{p} \to R/\mathfrak{p}$ and $\epsilon'' : R/\mathfrak{b}' \to R/\mathfrak{b}'$ be multiplication by a' and a'' respectively. Then the following diagram commutes and is exact:

$$\begin{array}{ccccccccc}
\{0\} & \longrightarrow & R/\mathfrak{p} & \xrightarrow{i} & R/\mathfrak{b} & \xrightarrow{f} & R/\mathfrak{b}' & \longrightarrow & \{0\} \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
\{0\} & \longrightarrow & R/\mathfrak{p} & \xrightarrow{i} & R/\mathfrak{b} & \xrightarrow{f} & R/\mathfrak{b}' & \longrightarrow & \{0\}
\end{array}$$

By Proposition 4.5 and the induction assumption,

$$(\epsilon, R/\mathfrak{b}) = (\epsilon', R/\mathfrak{p})(\epsilon, R/\mathfrak{b}') = \left(\frac{a'}{\mathfrak{p}}\right)\left(\frac{a''}{\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{p}}\right)\left(\frac{a}{\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right). \quad \square$$

LEMMA 4.8. *If R is the ring of integers of a number field K and $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in R, then there is an injective R-linear mapping $i : R/\mathfrak{a} \to R/\mathfrak{ab}$ whose image is $\{x + \mathfrak{ab} \mid x \in \mathfrak{b}\}$.*

PROOF. We may write $\mathfrak{ab} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$ and $\mathfrak{b} = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}$ with each $\mathfrak{p}_i$ prime, each $e_i > 0$, and each $d_i \geq 0$. For each $i = 1, \ldots, t$, choose $\beta_i \in R$ such that $\beta_i \in \mathfrak{p}_i^{d_i}$ and $\beta_i \notin \mathfrak{p}_i^{d_i+1}$. Using the Chinese Remainder Theorem we can find an $\alpha \in R$ such that

$$\alpha \equiv \beta_i \mod \mathfrak{p}_i^{d_i+1}$$

for each $i = 1, \ldots, t$. Clearly $\alpha \in \mathfrak{p}_i^{d_i}$ and $\alpha \notin \mathfrak{p}_i^{d_i+1}$ for each $i = 1, \ldots, t$. We conclude that $\alpha R = \mathfrak{bc}$ where $\mathfrak{c}$ is an ideal relatively prime to $\mathfrak{ab}$.

Now define a map $j : R \to R/\mathfrak{ab}$ by letting $j(x) = \alpha x + \mathfrak{ab}$ for each $x \in R$. Then j is R-linear and $\ker(j) = \mathfrak{a}$, since for any $x \in R$,

$$j(x) = 0 \Leftrightarrow \alpha x \in \mathfrak{ab} \Leftrightarrow \mathfrak{ab} \mid (\alpha R)(xR) \Leftrightarrow \mathfrak{ab} \mid \mathfrak{bc}(xR) \Leftrightarrow \mathfrak{a} \mid xR \Leftrightarrow x \in \mathfrak{a}.$$

Thus we may define an injective R-linear map $i : R/\mathfrak{a} \to R/\mathfrak{ab}$ as follows: for any $y \in R/\mathfrak{a}$, let x be any lift of y to R and set $i(y) = j(x)$. Further,

$$\begin{aligned} \mathrm{im}(i) = \mathrm{im}(j) &= \{x + \mathfrak{ab} \mid x \in \alpha R\} \\ &= \{x + x' + \mathfrak{ab} \mid x \in \alpha R, x' \in \mathfrak{ab}\} \\ &= \{x + \mathfrak{ab} \mid x \in \gcd(\alpha R, \mathfrak{ab})\} \\ &= \{x + \mathfrak{ab} \mid x \in \mathfrak{b}\}. \quad \square \end{aligned}$$

DEFINITION. Suppose that A is an order in R, $\mathfrak{b}$ is an ideal of A, and t is a positive integer. If $x = (x_1, \ldots, x_t) \in A^t$ then we write $x + \mathfrak{b}$ for the vector

$$(x_1 + \mathfrak{b}, \ldots, x_t + \mathfrak{b})$$

in $(A/\mathfrak{b})^t$. If ϵ is an endomorphism of $(A/\mathfrak{b})^t$, then a *matrix of* ϵ is a t by t matrix U with entries in A such that $U(x) + \mathfrak{b} = \epsilon(x + \mathfrak{b})$ for any $x \in A^t$.

LEMMA 4.9. *If R is the ring of integers of a number field K, $\mathfrak{b}$ is an ideal in R relatively prime to mR, t is a positive integer, $\epsilon : (R/\mathfrak{b})^t \to (R/\mathfrak{b})^t$ is a bijective R-linear mapping, and U is a matrix of ϵ, then $\mathfrak{b} \in \mathcal{I}(\det U)$.*

PROOF. Since $\det U \in R$ we need to show that $\mathfrak{b}$ is relatively prime to $(\det U)R$. Let $\overline{U}$ be the matrix obtained from U by reducing each entry mod $\mathfrak{b}$; clearly for any $(x_1, \dots, x_t) \in (R/\mathfrak{b})^t$ we have

$$\epsilon(x_1, \dots, x_t) = \overline{U}(x_1, \dots, x_t).$$

Since ϵ is bijective, $\overline{U}$ is invertible in R; this means that $\det U$ is invertible mod $\mathfrak{b}$ (see [8, p. 94]). It follows that

$$\gcd((\det U)R, \mathfrak{b}) = 1$$

so $\det U$ is relatively prime to $\mathfrak{b}$. □

PROPOSITION 4.10. *If $\mathfrak{b}$ is an ideal of $\mathbb{Z}[\zeta]$ relatively prime to $m\mathbb{Z}[\zeta]$, t is a positive integer, ϵ is a bijective $\mathbb{Z}[\zeta]$-linear mapping of $(\mathbb{Z}[\zeta]/\mathfrak{b})^t$ to itself, and $U = (u_{ij})$ is a matrix of ϵ, then $\mathfrak{b} \in \mathcal{I}(\det U)$ and*

$$(\epsilon, (\mathbb{Z}[\zeta]/\mathfrak{b})^t) = \left(\frac{\det U}{\mathfrak{b}}\right).$$

PROOF. The assertion that $\mathfrak{b} \in \mathcal{I}(\det U)$ is just Lemma 4.9. Turning to the given equation, we first prove that it holds in the case where $t = 1$. Here ϵ acts as multiplication by some element of R, say a. Let d be the number of prime factors of $\mathfrak{b}$, counting multiplicities; we proceed by induction on d. The base case $d = 1$ was proven in Proposition 4.6, with $K = \mathbb{Q}[\zeta]$; we now assume the proposition for some d and prove it for $d + 1$.

Let $\mathfrak{b}$ be an ideal with $d + 1$ prime factors. Write $\mathfrak{b} = \mathfrak{p}\mathfrak{c}$ where $\mathfrak{p}$ is prime. Lemma 4.8 gives us an injective $\mathbb{Z}[\zeta]$-linear mapping $i : \mathbb{Z}[\zeta]/\mathfrak{p} \to \mathbb{Z}[\zeta]/\mathfrak{b}$ with image $\{x + \mathfrak{b} \mid x \in \mathfrak{c}\}$. The surjective $\mathbb{Z}[\zeta]$-linear mapping $f : \mathbb{Z}[\zeta]/\mathfrak{b} \to \mathbb{Z}[\zeta]/\mathfrak{c}$ defined by $f(x + \mathfrak{b}) = x + \mathfrak{c}$ has kernel $\{x + \mathfrak{b} \mid x \in \mathfrak{c}\}$. Let a' and a'' be the image of a in $\mathbb{Z}[\zeta]/\mathfrak{p}$ and $\mathbb{Z}[\zeta]/\mathfrak{c}$ respectively, and let $\epsilon' : \mathbb{Z}[\zeta]/\mathfrak{p} \to \mathbb{Z}[\zeta]/\mathfrak{p}$ and $\epsilon'' : \mathbb{Z}[\zeta]/\mathfrak{c} \to \mathbb{Z}[\zeta]/\mathfrak{c}$ be multiplication by a' and a'' respectively. Then the following diagram commutes and is exact:

$$\begin{array}{ccccccccc}
\{0\} & \longrightarrow & \mathbb{Z}[\zeta]/\mathfrak{p} & \xrightarrow{i} & \mathbb{Z}[\zeta]/\mathfrak{b} & \xrightarrow{f} & \mathbb{Z}[\zeta]/\mathfrak{c} & \longrightarrow & \{0\} \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
\{0\} & \longrightarrow & \mathbb{Z}[\zeta]/\mathfrak{p} & \xrightarrow{i} & \mathbb{Z}[\zeta]/\mathfrak{b} & \xrightarrow{f} & \mathbb{Z}[\zeta]/\mathfrak{c} & \longrightarrow & \{0\}
\end{array}$$

By Proposition 4.5 and the induction assumption,

$$(\epsilon, \mathbb{Z}[\zeta]/\mathfrak{b}) = (\epsilon', \mathbb{Z}[\zeta]/\mathfrak{p})(\epsilon'', \mathbb{Z}[\zeta]/\mathfrak{c}) = \left(\frac{a'}{\mathfrak{p}}\right)\left(\frac{a''}{\mathfrak{c}}\right) = \left(\frac{a}{\mathfrak{p}}\right)\left(\frac{a}{\mathfrak{c}}\right) = \left(\frac{a}{\mathfrak{b}}\right).$$

This completes the induction and establishes the proposition when $t = 1$.

We now proceed by induction on t to give the full result. We have just proved the base case $t = 1$; we now assume the proposition for some t and prove it for $t + 1$. We suppose first that U is upper triangular. Let $i(x) = (x, 0, \dots, 0)$ for any $x \in \mathbb{Z}[\zeta]/\mathfrak{b}$ and let $f(x_1, x_2, \dots, x_{t+1}) = (x_2, x_3, \dots, x_{t+1})$ for any $(x_1, x_2, \dots, x_{t+1}) \in (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1}$. Let U' be the matrix obtained from U by deleting the first row and first column from U. Then let $\epsilon' : \mathbb{Z}[\zeta]/\mathfrak{b} \to \mathbb{Z}[\zeta]/\mathfrak{b}$ be multiplication by u_{11} and let $\epsilon'' : (\mathbb{Z}[\zeta]/\mathfrak{b})^t \to (\mathbb{Z}[\zeta]/\mathfrak{b})^t$ be multiplication by U'. Both are $\mathbb{Z}[\zeta]$-linear. Now the following diagram commutes and is exact:

$$\begin{array}{ccccccccc}
\{0\} & \longrightarrow & \mathbb{Z}[\zeta]/\mathfrak{b} & \xrightarrow{i} & (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1} & \xrightarrow{f} & (\mathbb{Z}[\zeta]/\mathfrak{b})^{t} & \longrightarrow & \{0\} \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
\{0\} & \longrightarrow & \mathbb{Z}[\zeta]/\mathfrak{b} & \xrightarrow{i} & (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1} & \xrightarrow{f} & (\mathbb{Z}[\zeta]/\mathfrak{b})^{t} & \longrightarrow & \{0\}
\end{array}$$

By Proposition 4.5 and the induction assumption,

$$(\epsilon, (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1}) = (\epsilon', \mathbb{Z}[\zeta]/\mathfrak{b})(\epsilon'', (\mathbb{Z}[\zeta]/\mathfrak{b})^t) = \left(\frac{u_{11}}{\mathfrak{b}}\right)\left(\frac{\det U'}{\mathfrak{b}}\right) = \left(\frac{\det U}{\mathfrak{b}}\right).$$

This completes the induction and establishes the proposition when U is upper triangular. An exactly similar proof establishes the same result when U is lower triangular.

Turning finally to a general ϵ, we recall that U is the product of matrices $U_1, U_2, \dots, U_r$ with each U_i either upper or lower triangular. For each $i = 1, \dots, r$, we let $\epsilon_i : (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1} \to (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1}$ be multiplication by U_i. We then use Proposition 4.4 to obtain

$$(\epsilon, (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1}) = \prod_{i=1}^{r} (\epsilon_i, (\mathbb{Z}[\zeta]/\mathfrak{b})^{t+1}) = \prod_{i=1}^{r} \left(\frac{\det U_i}{\mathfrak{b}}\right) = \left(\frac{\det U}{\mathfrak{b}}\right). \quad \square$$

3. Computation of the Signature: Subroutines

To simplify the presentation of the algorithm for the computation of the signature, we present first a number of subroutines to be used in the algorithm itself. In each case we leave to the reader the (easy) proofs that the algorithm terminates, that it produces correct output, and that both the running time and the output size are polynomial in the input size.

ALGORITHM 4.11. Given a number field K, an order A in K containing ζ, an ideal $\mathfrak{a}$ in A, and an element $a \in A$, this algorithm finds $A/\mathfrak{a}$ as a $\mathbb{Z}[\zeta]$-module and the encoding of the endomorphism ϵ of $A/\mathfrak{a}$ which maps $x \in A/\mathfrak{a}$ to ax.

Step 1 Write L for the lattice encoding $\mathfrak{a}$ and let G be the group $\mathbb{Z}^n/L$. For each generator $\omega_1, \ldots, \omega_n$ of A, compute $\zeta\omega_i$, which is an element of A and therefore is encoded by an element of $\mathbb{Z}^n$. Let τ be the endomorphism of $\mathbb{Z}^n$ which maps the ith standard basis vector to $\zeta\omega_i$ and let γ be the corresponding endomorphism of G.

Step 2 For each i, compute $a\omega_i$, which is an element of A and is therefore encoded by an element of $\mathbb{Z}^n$. Let ν be the endomorphism of $\mathbb{Z}^n$ which maps the ith standard basis vector to $a\omega_i$ and let η be the corresponding endomorphism of G. Output G with the action of γ as the encoding of $A/\mathfrak{a}$, output η as the encoding of ϵ, and terminate.

Note that it may happen that the lattice L is encoded by a matrix with 1's found on the diagonal, so that we need to strike out certain rows and columns and adjust γ and ν as we described in Chapter 1.

For the next two algorithms, we note that if G is an abelian group with subgroup G' and γ is an endomorphism of G such that $\gamma(G') = G'$, then there exist endomorphisms γ', γ'' of G' and G/G'' respectively such that $\gamma'(x) = \gamma(x)$ for all $x \in G'$ and $\gamma''(x + G') = \gamma(x)$ for every $x \in G$. We say that γ *splits on* G' *into* γ' *and* γ''. The same result and definition apply if G and G' are replaced by a $\mathbb{Z}[\zeta]$-module M and submodule M' throughout.

ALGORITHM 4.12. Given a finite abelian group G, a subgroup G' of G, and an endomorphism γ of G such that $\gamma(G') = G'$, this algorithm finds G/G' and endomorphisms γ', γ'' of G' and G'' such that γ splits on G' into γ' and γ''.

Step 1 There is a positive integer n and a lattice L' of rank n in $\mathbb{Z}^n$ such that $L \subset L'$ and $G' \cong L'/L$. Output L' as the encoding of G/G' (so that $G/G' \cong \mathbb{Z}^n/L'$).

Step 2 Let T be the n by n integer matrix encoding γ; then $TL \subset L$. Let $v_1, \ldots, v_n$ generate L' and compute Tv_i for each i. Since $\gamma(G') = G'$, each Tv_i is in L', so we may find integers b_{ij} such that

$$Tv_i = \sum_{j=1}^{n} b_{ij} v_j.$$

Let B be the n by n integer matrix (b_{ij}); we output B as the encoding of the endomorphism γ', output T as the encoding of the endomorphism γ'', and terminate.

ALGORITHM 4.13. Given a $\mathbb{Z}[\zeta]$-module M, a submodule M', and an endomorphism ϵ of M such that $\epsilon(M') = M'$, this algorithm finds M/M' and endomorphisms ϵ', ϵ'' of M' and M/M' respectively such that ϵ splits on M into ϵ' and ϵ''.

Method We write G and G' for the additive groups of M and M' respectively, apply Algorithm 4.12 to G, G', and Z, where Z is the action of ζ on G, and then apply Algorithm 4.12 again to G, G', and ϵ. We leave the details to the reader.

DEFINITION. If r, s and n are positive integers and B is an r by s integer matrix, then the *kernel of B mod n* is the set of all integer s-tuples w such that $Bw \in n\mathbb{Z}^r$.

ALGORITHM 4.14. Given an r by s integer matrix B, this algorithm either finds a nontrivial divisor of n or else a positive integer t and an s by t integer matrix C such that the columns of C form a basis for the kernel of B mod n.

Method We simply assume that n is prime so that $\mathbb{Z}/n\mathbb{Z}$ is a field and apply ordinary linear algebra over $\mathbb{Z}/n\mathbb{Z}$ to find the kernel of B. However, the Gaussian elimination we perform to do this involves finding inverses of elements of $\mathbb{Z}/n\mathbb{Z}$, which we can try to do using the powering algorithms (see [4, pp. 8–12]). However, it may happen that we find a zero-divisor d in this field, which is therefore a divisor of n. If this happens, we output d and terminate. If no zero-divisors are found throughout the kernel-finding process, the result is the desired matrix C, which we output and terminate.

When, as here, an algorithm returns a nontrivial factorization of n instead of what was expected, we call the result a "side exit". We will see that our power residue symbol algorithm will handle side exits gracefully.

The remainder of the subroutines take as input a finite $\mathbb{Z}[\zeta]$-module M such that the additive group of M is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^t$ for some positive integers n and t.

ALGORITHM 4.15. Given M as above and an element $x \in M$, this algorithm finds the annihilator of x or else returns a nontrivial factor d of n.

Method We have integer t-tuples $b_0, \ldots, b_{\phi(m)-1}$ such that b_j encodes $\zeta^j x$. Let B be the t by $\phi(m)$ integer matrix whose jth column is b_j. Apply Algorithm 4.14 to B. If the result is a nontrivial factor d of n, output d and terminate. Otherwise, the result is a $\phi(m)$ by $\phi(m)$ integer matrix C whose columns form a basis for the kernel of B mod n. Let L be the lattice generated by the columns of C, output L as the encoding of the ideal $\operatorname{Ann} x$, and terminate.

The claim that C has $\phi(m)$ columns may be proven by simply observing that the lattice spanned by the columns of C must be a basis of $\operatorname{Ann} x$ and $\operatorname{Ann} x$ is an ideal, hence is generated over $\mathbb{Z}$ by a $\mathbb{Z}$-linearly independent set with $\phi(m)$ elements.

ALGORITHM 4.16. Given M as above and an element $a \in \mathbb{Z}[\zeta]$, this algorithm determines whether $aM = 0$.

Step 1 Let L be the lattice of rank t in $\mathbb{Z}^n$ encoding the additive group of M; a basis of L is $ne_1, \ldots, ne_t$ where e_i is the ith standard basis vector of $\mathbb{Z}^t$.

Step 2 Compute ae_i for each $i = 1, 2, \ldots, t$, where each e_i is considered as an element of M. If all the products are zero, output "YES" and terminate, otherwise output "NO" and terminate.

For the rest of the algorithms in this section we assume not only that M has the form given above but that $\operatorname{Ann} M$ is known. For brevity's sake, we say that a set $\{x_1, \ldots, x_k\}$ in M is *linearly independent* mod $\operatorname{Ann} M$ when the following holds: if $\sum_{j=1}^{k} a_j x_j = 0$ for some $a_j \in \mathbb{Z}[\zeta]$, then all the a_j must be in $\operatorname{Ann} M$.

ALGORITHM 4.17. Given M as above and $x_1, \ldots, x_k$ in M such that the set $\{x_1, \ldots, x_{k-1}\}$ is linearly independent mod $\operatorname{Ann} M$, this algorithm either finds a nontrivial factor d of n or else determines whether the set $x_1, \ldots, x_k$ is linearly independent mod $\operatorname{Ann} M$ and, if not, finds a_k in $\mathbb{Z}[\zeta]$, $a \notin \operatorname{Ann} M$ such that for some $a_1, \ldots, a_{k-1}$ in $\mathbb{Z}[\zeta]$ we have $\sum_{j=1}^{k} a_j x_j = 0$.

Step 1 Compute each product of the form $\zeta^i x_j$ where i and j are integers

with $0 \le i \le \phi(m) - 1$ and $1 \le j \le k$. Let B be the t by $k\phi(m)$ integer matrix whose columns are these products expressed as t-tuples. Apply Algorithm 4.14 to B. If the result is a nontrivial factor d of n, return d and terminate. Otherwise, the result is a $k\phi(m)$ by $\phi(m)$ integer matrix C whose columns form a basis for the kernel of B mod n.

Step 2 Let C' be the $\phi(m)$ by $\phi(m)$ matrix consisting of the last $\phi(m)$ rows of C, let L be the lattice generated by the columns of C', and let J be the ideal of $\mathbb{Z}[\zeta]$ encoded by L. If $J = \operatorname{Ann} M$ then output "YES" and terminate. Otherwise, find $a_k \in J$ with $a_k \notin \operatorname{Ann} M$, output "NO" and a_k, and terminate.

As above, we know that C has $\phi(m)$ columns since the lattice L contains the ideal $\operatorname{Ann} M$.

ALGORITHM 4.18. Given M as above and elements $x_1, \ldots, x_k$ of M which are linearly independent mod $\operatorname{Ann} M$, this algorithm determines whether $M = \langle x_1, \ldots, x_k \rangle$. If $M \neq \langle x_1, \ldots, x_k \rangle$, the algorithm also finds $y \in M$ such that $y \notin \langle x_1, \ldots, x_k \rangle$.

Step 1 Compute the products $\zeta^i x_j$ where i and j are integers with $0 \le i \le \phi(m) - 1$ and $1 \le j \le k$, as well as ne_r where $r \in \{1, 2, \ldots, t\}$ and e_r is the rth standard basis vector of $\mathbb{Z}^t$. Write each of these as a t-tuple and let B be a t by $k\phi(m) + t$ matrix whose columns are the computed products of both forms.

Step 2 Determine whether B spans $\mathbb{Z}^t$; if so then output "EQUALITY" and terminate. Otherwise, find $x \in \mathbb{Z}^t$ such that $x \notin \operatorname{im} B$, output "NOT EQUAL" and x, and terminate.

For the following algorithm, we note that when $x_1, \ldots, x_k \in M$ are such that

(1) the set $\{x_1, \ldots, x_k\}$ is linearly independent mod $\operatorname{Ann} M$ and
(2) $M = \langle x_1, \ldots, x_k \rangle$,

then M is clearly isomorphic to $(\mathbb{Z}[\zeta]/\operatorname{Ann} M)^k$.

ALGORITHM 4.19. Given M as above, an endomorphism ϵ of M encoded in the usual way as an endomorphism of the additive group of M, and elements $x_1, \ldots, x_k$ of M satisfying (1) and (2) above, this algorithm finds a matrix of ϵ acting on $M \cong (\mathbb{Z}[\zeta]/\operatorname{Ann} M)^k$.

Step 1 Compute $\epsilon(x_j)$ and $\zeta^i x_j$ where i and j are integers with $0 \le i \le \phi(m) - 1$ and $1 \le j \le k$. These products are elements of M and are

therefore encoded as t-tuples of integers. Let B be the t by $k\phi(m)$ matrix whose columns are the products of the form $\zeta^i x_j$, arranged in the order

$$x_1, \zeta x_1, \dots, \zeta^{\phi(m)-1}x_1, x_2, \dots, \zeta^{\phi(m)-1}x_2, \dots, x_k, \dots, \zeta^{\phi(m)-1}x_k.$$

Step 2 For each $r = 1, 2, \dots, k$, the integer t-tuple $\epsilon(x_r)$ is in the image of B; find an integer $k\phi(m)$-tuple c_r such that $Bc_r = \epsilon(x_r)$. For pairs (i, j) with $i \in \{0, 1, 2, \dots, \phi(m) - 1\}$ and $j \in \{1, 2, \dots, k\}$, let c_{rij} be the $(i + \phi(m)j)$th component of c_r, so that

$$c = (c_{r11}, c_{r21}, \dots, c_{r\phi(m)1}, \dots, c_{r1k}, c_{r2k}, \dots, c_{r\phi(m)k}).$$

Also let $c_{rj} = (c_{r1j}, c_{r2j}, \dots, c_{r\phi(m)j})$ where $j \in \{0, 1, 2, \dots, k\}$. Let $C = (c_{rj})$, a k by k matrix with entries in $\mathbb{Z}[\zeta]$, output C, and terminate.

4. Computation of the Signature: Algorithm

We can now present the algorithm for the computation of the signature (ϵ, M).

ALGORITHM 4.20. Given a finite admissible $\mathbb{Z}[\zeta]$-module M and a bijective endomorphism ϵ of M, this algorithm finds (ϵ, M).

Step 1 Using the Smith Normal Form, compute the additive group of M in the form

$$M = \bigoplus_{j=1}^{t} (\mathbb{Z}/n_j\mathbb{Z})$$

for some integers $n_1, \dots, n_t$. If not all the n_j are equal, set d equal to the smallest of the n_j and go to step 7. Otherwise, let $n = n_1 = \cdots = n_t$ and let $\mathfrak{b} = n\mathbb{Z}[\zeta]$.

Step 2 Pick $x \in M$, $x \neq 0$. Apply Algorithm 4.15 to x. If the result is a nontrivial factor d of n, go to step 7. Otherwise the result is the ideal $\operatorname{Ann} x$.

Step 3 Determine whether $\operatorname{Ann} x$ is a proper divisor of $\mathfrak{b}$. If so, let a be an element of $\operatorname{Ann} x$ which is not in $\mathfrak{b}$ and proceed to step 4; if not, set $x_1 = x$, $k = 1$, and go to step 6.

Step 4 Use Algorithm 4.16 to determine whether $aM = 0$. If so, find $\mathfrak{c} = aR + \mathfrak{b} = \gcd(aR, \mathfrak{b})$, set $\mathfrak{b} = \mathfrak{c}$, and go to step 2. Otherwise, set $d = a$ and go to step 7.

Step 5 Apply Algorithm 4.17 to $x_1, \ldots, x_k$. If the result is a nontrivial factor d of n, go to step 7. Otherwise, we determine whether there exist $a_1, \ldots, a_k$ in $\mathbb{Z}[\zeta]$, not all in $\mathfrak{b}$, such that $\sum_{j=1}^{k} a_j x_j = 0$. If so, set $d = a_k$ and go to step 7; if not, proceed to step 6.

Step 6 Use Algorithm 4.18 to determine whether $M = \langle x_1, \ldots, x_k \rangle$. If so, go to step 8. If not, let x_{k+1} be any element of M not in $\langle x_1, \ldots, x_k \rangle$, set $k = k + 1$, and go to step 5.

Step 7 Use Algorithm 4.13 to find $M' = dM$ and $M'' = M/M'$, as well as encodings of the endomorphisms ϵ', ϵ'' of M' and M'' respectively such that ϵ splits on M' into ϵ' and ϵ''. Recursively find (ϵ', M') and (ϵ'', M''), output $(\epsilon', M')(\epsilon'', M'')$, and terminate.

Step 8 Use Algorithm 4.19 to find a matrix U with entries in $\mathbb{Z}[\zeta]$ such that U is a matrix of ϵ acting on $M \cong (\mathbb{Z}[\zeta]/\mathfrak{b})^k$, output the mth power residue symbol $(\det U/\mathfrak{b})$, and terminate.

Note that it is in step 8 that we use the mth power residue symbol in a cyclotomic field. We will explain how to calculate this in the next chapter.

We proceed to prove that the algorithm is correct, using two preparatory lemmas.

LEMMA 4.21. *The following facts hold:*

(1) $\mathfrak{b}M = 0$ *at all times after step 1 is completed.*
(2) *Each time* $\mathfrak{b}$ *is altered in step 4, the new ideal held in* $\mathfrak{b}$ *is a proper divisor of the previous one.*
(3) *When the loop in steps 2 to 4 terminates (without a side exit),* $\mathfrak{b} = \operatorname{Ann} M$.

PROOF. It is obvious that (1) is true immediately after step 1, when $\mathfrak{b} = n\mathbb{Z}[\zeta]$. $\mathfrak{b}$ is only changed in step 4, where it becomes $\gcd(a\mathbb{Z}[\zeta], \mathfrak{b})$; here a is an element of $\mathbb{Z}[\zeta]$ which is not in $\mathfrak{b}$ but for which $aM = 0$. Elements of $\gcd(a\mathbb{Z}[\zeta], \mathfrak{b}) = a\mathbb{Z}[\zeta] + \mathfrak{b}$ are of the form $ac + b$ for $b \in \mathfrak{b}$ and $c \in \mathbb{Z}[\zeta]$, and clearly $(ac+b)x = 0$ for any such b and c and for any $x \in M$. Thus (1) is proved. For (2), notice that if $\gcd(a\mathbb{Z}[\zeta], \mathfrak{b}) = \mathfrak{b}$ then $a \in \mathfrak{b}$. Finally, the loop in steps 2 to 4 terminates either in a side exit or in the jump from step 3 to step 6. This happens precisely when we have found an x such that $\gcd(\operatorname{Ann} x, \mathfrak{b}) = \mathfrak{b}$, or in other words $\operatorname{Ann} x \subset \mathfrak{b}$. Thus if $a \in \operatorname{Ann} M$ then $a \in \operatorname{Ann} x$ so $a \in \mathfrak{b}$; this together with (1) establishes (3). □

LEMMA 4.22. *In step 7,* $M' = dM$ *is a nontrivial submodule of* M.

PROOF. Step 7 can be reached from steps 1, 2, 4, or 5. If it is reached from steps 1, 2, or 4, or from the side exit in step 5, we claim that there are elements x and y in M such that $x \neq 0$, $dx = 0$ and $dy \neq 0$. This is obvious for step 4. For step 1, take x to be an element of M with additive order n_i and y to be an element of order n_j where $n_i \mid n_j$ (note that n_i and n_j cannot be 1 by the nature of our encoding of additive groups). In the case of the side exits in steps 2 and 5, take x to be an element of order d and y to be an element of order n. In each of these cases, $dy \neq 0$ so $dM \neq 0$. Also, since multiplication by d has a non-trivial kernel, $dM \neq M$. Thus in each case besides the second jump to step 7 in step 5, we have shown that M' is a nontrivial submodule of M.

To establish the result in the remaining case, observe that every time step 5 is entered, $k \geq 2$ and the set $\{x_1, \ldots, x_{k-1}\}$ is linearly independent mod $\mathfrak{b} = \operatorname{Ann} M$. When we jump to step 7 from step 5, we have found $a_1, \ldots, a_k$ in $\mathbb{Z}[\zeta]$, not all in $\mathfrak{b}$, such that $\sum_{j=1}^{k} a_j x_j = 0$. Clearly $d = a_k$ cannot be in $\mathfrak{b}$, since then we would have $\sum_{j=1}^{k-1} a_j x_j = 0$ and so all the a_j would be in $\mathfrak{b}$. Thus, since by Lemma 4.21 $\mathfrak{b}$ is the annihilator of M, $dM \neq 0$. Suppose now, for a contradiction, that $dM = M$, so that multiplication by d is a surjective endomorphism of M. Since M is finite, this map is injective also. Let $N = \langle x_1, \ldots, x_{k-1} \rangle$. Clearly $dN \subset N$, and multiplication by d is therefore an injective endomorphism of N. Again, since N is finite, this map is also surjective, and $dN = N$. We have $dx_k \in N$ and so $x_k \in N$ which is the desired contradiction. □

PROPOSITION 4.23. *Algorithm 4.20 terminates and correctly produces the signature (ϵ, M). Its running time is polynomial in the size of M.*

PROOF. For termination, we must show that the loops in steps 2 to 4 and steps 5 to 6 are finite and that the recursion terminates. Item (2) of Lemma 4.21 shows that the loop in steps 2 to 4 must end, since we cannot have an infinite sequence of ideals $\mathfrak{b}_1, \mathfrak{b}_2, \ldots$ such that $\mathfrak{b}_j$ is a nontrivial divisor of $\mathfrak{b}_{j+1}$. For the other loop, observe that on every entrance into step 6 the set $x_1, \ldots, x_k$ is linearly independent mod $\operatorname{Ann} M$. In particular all the x_j are distinct. Thus k is bounded by $|M|$ and, since k is incremented in each pass, the loop must end. Finally, by Lemma 4.22 the modules M' and M'' used in step 7 satisfy $1 \leq |M'| < |M|$ and $1 \leq |M''| < |M|$, and it follows that the recursion terminates, at worst, in the trivial case $|M| = 1$.

For correctness, we examine the two steps which produce output. In step 7, M' is not only a nontrivial submodule of M but also satisfies $\epsilon(M') = M'$. It quickly follows from Proposition 4.5 that $(\epsilon, M) = (\epsilon', M')(\epsilon'', M'')$ where

ϵ', ϵ'', M'' are as defined in step 7. In step 8 we need only appeal to Proposition 4.10 to see that $(\epsilon, M) = \left(\frac{\det U}{\mathfrak{b}}\right)$ as claimed. Thus the algorithm is correct.

Finally, we prove that the algorithm runs in polynomial time. M is encoded as an n by n integer matrix $B = (b_{ij})$ in HNF. Note that

$$\log |M| = \sum_{i=1}^{n} \log b_{ii} \leq \sum_{i=1}^{n} \operatorname{size} b_{ii} \leq \operatorname{size}(M).$$

We will therefore simply prove that the running time is polynomial in $\log |M|$; it follows immediately from this that the running time is polynomial in the size of M and therefore in the whole input size.

For a given M and ϵ, let $U(M, \epsilon)$ be the number of bit operations executed before either a recursion occurs in step 7 or the algorithm terminates in step 8. Let $U(s)$ be the maximum of $U(M, \epsilon)$ over all modules with $\log |M| = s$ and all endomorphisms ϵ of such a module. Clearly $U(s)$ is $O(s^k)$ for some positive integer k. It follows that for some positive real constant C, $U(s) \leq Cs^k$.

For a given M and ϵ, let $T(M, \epsilon)$ be the running time for the algorithm with input M and ϵ. If for this input the algorithm terminates with step 8, we have $T(M, \epsilon) = U(M, \epsilon)$, whereas if the algorithm terminates with step 7 and M is split into M' and M'',

$$T(M, \epsilon) = U(M, \epsilon) + T(M') + T(M'').$$

Let $T(s)$ be the maximum of $T(M, \epsilon)$ over all modules with $\log |M| = s$ and all endomorphisms ϵ. Since step 7 splits M into M' and M'' with $2 \leq |M'| \leq |M|/2$, $2 \leq |M''| \leq |M''|/2$, it is easy to see that

$$T(s) \leq \max\{Cs^k + T(s-t) + T(t) \mid 1 \leq t \leq s-1\}$$

for any $s > 0$ and that $T(0) \leq C$. We now prove by induction that

$$T(s) \leq Cs^{k+1}$$

which will establish that the running time is polynomial in the size of the input module.

The base case of our induction is $s = 0$ and is trivial. Now we suppose the result to be true for all $t < s$ and prove it for s. We have

$$T(s) \leq \max\{Cs^k + C(s-t)^{k+1} + Ct^{k+1} \mid 1 \leq t \leq s-1\}.$$

Clearly $C(s-t)^{k+1} + Ct^{k+1}$ reaches a maximum as a function of t when $t = 1$ or $t = s-1$. Thus it suffices to prove that

$$Cs^k + C(s-1)^{k+1} + C \leq Cs^k$$

or

$$s^k + (s-1)^{k+1} + 1 \leq s^{k+1}.$$

We have

$$\begin{aligned} s^{k+1} - (s-1)^{k+1} &= (s-(s-1))(s^k + s^{k-1}(s-1) + \cdots + (s-1)^k) \\ &\geq s^k + 1 \end{aligned}$$

establishing the result. □

The algorithm for the mth power residue symbol is now very simple. Given a nonzero element $a \in K$ and an ideal $\mathfrak{b}$ of R in $\mathcal{I}(a)$, we first write $a = c/d$ for some c and d in R. We use Algorithm 4.11 to find the encoding of $R/\mathfrak{b}$, ϵ_c, and ϵ_d where $\epsilon_c(x) = cx$, $\epsilon(x) = dx$. Then, using Algorithm 4.20, we compute the signatures $(\epsilon_c, R/\mathfrak{b})$ and $(\epsilon_d, R/\mathfrak{b})$. Now

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{c}{\mathfrak{b}}\right)\left(\frac{d}{\mathfrak{b}}\right)^{-1} = (\epsilon_c, R/\mathfrak{b})(\epsilon_d, R/\mathfrak{b})^{-1}.$$

Of course we have here assumed that R is given although in practice we do not usually know R. However, as we mentioned in the introduction to this chapter, for most applications it will suffice to compute a signature in an order A and assume that this is really the power residue symbol desired.

CHAPTER V

ALGORITHM FOR THE CYCLOTOMIC CASE

We now keep our promise of the last chapter to exhibit an algorithm for the calculation of the power residue symbol in $Q(\zeta)$, thus completing our algorithm for the general power residue symbol.

1. The Norm Residue Symbol

In this section and the next, K will be a number field containing the mth roots of unity and R will be the ring of integers in K.

The techniques of local class field theory can be used to define a very useful object called the *norm residue symbol*. It shares many of the properties of the power residue symbol and is closely related to it. We do not develop its theory fully since we are only interested in using an existing algorithm for its computation. We simply make assertions about the symbol and refer the reader to the relevant sections of [3] for definitions and proofs.

Class field theory introduces the notion of an *infinite prime*, whose valuation corresponds to an embedding of the field K in $\mathbb{R}$ or $\mathbb{C}$. Refer to [3, Chapter 2] for details. We will use the phrase "prime of K" to mean either an ordinary prime of R or an infinite prime.

Just as the power residue symbol was defined in terms of the Frobenius automorphism, the norm residue symbol will be defined in terms of another map, the *local Artin map*. Fix nonzero $a \in K$ and a prime $\mathfrak{p}$ of K, fix $x \in \mathbb{C}$ such that $x^m = a$, and let $K' = K(x)$. Let $\mathfrak{P}$ be a prime of K' lying over $\mathfrak{p}$. Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and let $K'_\mathfrak{P}$ be the completion of K' at $\mathfrak{P}$. There is an obvious embedding of $K_\mathfrak{p}$ in $K'_\mathfrak{P}$. Let $G = \mathrm{Gal}(K'_\mathfrak{P}/K_\mathfrak{p})$ and note that G depends only on $\mathfrak{p}$ and not on $\mathfrak{P}$ (see [3, p. 174]). The local Artin map, denoted $\psi_\mathfrak{p}$, takes $(K'_\mathfrak{p})^*$ onto G. See [3, pp. 174–176] for the definition and properties of the local Artin map.

We can now define the norm residue symbol $(a,b)_{\mathfrak{p}}$ where b is any nonzero element of K, by writing

$$(a,b)_{\mathfrak{p}} = \frac{\psi_{\mathfrak{p}}(b)(x)}{x}.$$

One can prove that $(a,b)_{\mathfrak{p}}$ is an mth root of unity independent of the choice of x, that

$$(a,b)_{\mathfrak{p}}(a,b')_{\mathfrak{p}} = (a,bb')_{\mathfrak{p}}$$

and

$$(a,b)_{\mathfrak{p}}(a',b)_{\mathfrak{p}} = (aa',b)_{\mathfrak{p}}$$

for any nonzero a' and b' in K. Further, letting N denote the norm on the extension $K_{\mathfrak{p}}(x)/K_{\mathfrak{p}}$, we have $(a,b)_{\mathfrak{p}} = 1$ if and only if $b = N(y)$ for some $y \in K_{\mathfrak{p}}(x)/K_{\mathfrak{p}}$. Finally, we have $(a,b)_{\mathfrak{p}} = 1$ when $\mathfrak{p}$ is infinite (this is not quite true when $m = 2$, but we have fixed $m > 2$). All these results are stated as exercises with hints in [3, pp. 351–352].

Daberkow [6] has recently discovered an algorithm for the computation of the norm residue symbol in polynomial time. This is easy when $\mathfrak{p} \in \mathcal{I}(a)$, since a simple formula exists:

$$(a,b)_{\mathfrak{p}} = \left(\frac{a}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}} b}. \tag{1}$$

See [3, p. 352] and recall from our discussion after Proposition 3.6 that we can compute the power residue symbol when the given ideal is prime. However, construction of an algorithm is nontrivial for the case $\mathfrak{p} \notin \mathcal{I}(a)$ (Daberkow's method uses K-theory).

Our purpose in defining the norm residue symbol is to use the formula (2) below, which generalizes of the quadratic reciprocity law proven in elementary number theory. It will allow us to compute the mth power residue symbol in a way exactly analogous to the usual method of computing Jacobi symbols. Let $\mathcal{Q}(a,b)$ be the set of all primes of K which divide m together with those which divide both a and b.

PROPOSITION 5.1. *For any nonzero a and b in K,*

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) \prod_{\mathfrak{q} \in \mathcal{Q}(a,b)} (a,b)_{\mathfrak{q}}. \tag{2}$$

See [3, p. 352]. Observe that the infinite primes lie in $\mathcal{Q}(a,b)$ but that we need not concern ourselves with them since they all give a norm residue symbol of 1.

2. Subroutines

In this section we describe subroutines which will be used in the polynomial-time algorithm for the power residue symbol in $\mathbb{Q}(\zeta)$. However, the following algorithms are valid over any number field K and so we state them in this generality. Thus we fix a number field K of degree n with ring of integers R. We assume that an integral basis $\omega_1, \ldots, \omega_n$ of R is known as well as the discriminant $\operatorname{disc} R$ (in our specific application to cyclotomic fields, both of these are easy to compute). As in the last chapter, we leave to the reader the (easy) proofs that these algorithms terminate, are correct, run in polynomial time, and produce output of polynomial size.

First we give an algorithm to compute the inverse of an ideal in R, assuming that the different $\mathfrak{d}$ of K is known. The different can be computed; see [4, p. 204], where the method amounts to applying Algorithm 5.2 to the codifferent. In the specific case of a cyclotomic field, which is all we are really interested in, one could with a little work find a formula for the different.

ALGORITHM 5.2. Given an ideal $\mathfrak{a}$ of R, this algorithm finds the inverse of $\mathfrak{a}$, that is the fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = R$.

Step 1 Let M be the n by n matrix encoding $\mathfrak{a}$. Compute $\operatorname{Tr}(\omega_k)$ for $k = 1, 2, \ldots, n$ and let T be the n by n integral matrix whose entry at row i, column j is $\operatorname{Tr}(\omega_i\omega_j)$.

Step 2 Compute $M' = M^t T^{-1}$. Note that M' is an n by n rational matrix. Let d be the least common multiple of all denominators appearing in M', so that dM' is an integer matrix. Let $\mathfrak{a}$ be the ideal of R encoded by dM', output $(1/d, \mathfrak{a})$ as the encoding of the desired fractional ideal, and terminate.

The proof of correctness for this algorithm is given in [4, p. 203].

Let r be the number of real embeddings of K and let s be half the number of complex embeddings. We now present two algorithms which use the embedding ψ of K in $\mathbb{R}^r \oplus \mathbb{C}^s$ described in Chapter 1, Section 2. Recall that the norm N (really, its absolute value) can be extended to all of $\mathbb{R}^r \oplus \mathbb{C}^s$ as follows: if v is an element of $\mathbb{R}^r \oplus \mathbb{C}^s$, write

$$v = (v_1, \ldots, v_r, w_1, \ldots, w_s)$$

where the v_i are real and the w_i are complex, and let

$$N(v) = \prod_{i=1}^{r} |v_r| \prod_{i=1}^{s} |w_i||\overline{w_i}| = \prod_{i=1}^{r} |v_r| \prod_{i=1}^{s} |w_i|^2.$$

Let

$$\theta = \det \psi(R) = \frac{\sqrt{|\operatorname{disc} R|}}{2^s}$$

so that for any ideal $\mathfrak{a}$ in R, $\det \mathfrak{a} = \theta N(\mathfrak{a})$. Finally, let δ be the constant used in our discussion of the LLL algorithm (Chapter 1, Section 1).

Given an ideal $\mathfrak{b}$, Algorithm 5.3 finds an ideal $\mathfrak{c}$ of bounded norm for which $\mathfrak{bc}$ is principal. We can therefore reduce the computation of the symbol $(a/\mathfrak{b})$ to the problem of computing two symbols (a/bR) and $(a/\mathfrak{c})$, where bR is principal and $N(\mathfrak{c})$ is less than the given bound.

ALGORITHM 5.3. Given an ideal $\mathfrak{b}$ in R, this algorithm finds $b \in \mathfrak{b}$ and an ideal $\mathfrak{c}$ in R such that $\mathfrak{bc} = bR$ and $N(\mathfrak{c}) \leq \delta^n \theta$.

Step 1 Let $a_1, \ldots, a_n$ generate $\mathfrak{b}$ over $\mathbb{Z}$ and let L be the lattice in $\mathbb{R}^r \oplus \mathbb{C}^s$ generated by $\psi(a_1), \ldots, \psi(a_n)$. Apply the LLL algorithm to this lattice. We obtain $b \in \mathfrak{b}$ such that

$$\|\psi(b)\| \leq \delta(\det L)^{1/n}.$$

Step 2 Using Algorithm 5.2, find the fractional ideal $\mathfrak{b}^{-1}$. Let $\mathfrak{c} = bR\mathfrak{b}^{-1}$, output $\mathfrak{c}$, and terminate.

Correctness of this algorithm can be proved as follows. Write $\psi(b)$ as a vector $(b_1, \ldots, b_r, c_1, \ldots, c_s)$ in the vector space $\mathbb{R}^r \oplus \mathbb{C}^s$. Then certainly $|b_i|$ and $|c_i|$ are each bounded by $\delta(\det L)^{1/n}$. It follows that

$$|N(b)| \leq \delta^n \det L.$$

By our results in Chapter 1, Section 1, $\det L = \theta N(\mathfrak{b})$. Now

$$\begin{aligned} N(\mathfrak{c}) &= \frac{N(bR)}{N(\mathfrak{b})} = \frac{|N(b)|}{N(\mathfrak{b})} \\ &\leq \frac{\delta^n \det L}{\theta^{-1} \det L} = \delta^n \theta \end{aligned}$$

as desired.

Algorithm 5.4 uses an idea of Hurwitz, mentioned in this context by Lenstra [12]. One would like a version of the Euclidean algorithm for R, which would give for any elements a and b of R an element $b' \in R$ such that $b = ca + b'$ for some $c \in R$ and $|N(b')| < |N(a)|$. Unfortunately this is not possible. However, if we allow multiplication by a rational integer j whose absolute value is bounded, then we can obtain b' satisfying the norm inequality such that $jb = ca + b'$. This algorithm computes b' and j. Observe that we get something better than the inequality $|N(b')| < |N(a)|$: in fact the norm is reduced by a factor of 2.

ALGORITHM 5.4. Given elements a and b of R, $a \neq 0$, this algorithm finds a nonzero integer j with $|j| \leq 4\delta^{n+1}\theta$ and an element $b' \in R$ such that $jb \equiv b' \bmod a$ and $|N(b')| \leq |N(a)|/2$.

Step 1 Compute $N(aR)$ and let

$$\lambda = \frac{N(aR)^{1/n}}{4\delta^{n+1}\theta}.$$

Step 2 Let $a_1, \ldots, a_n$ be a $\mathbb{Z}$-basis of aR. Let L be the lattice in $\mathbb{R}^{n+1}$ generated by

$$(\psi(a_1), 0), \ldots, (\psi(a_n), 0), (0, \ldots, 0, \lambda).$$

Apply the LLL algorithm to L. We get $w = (w_1, \ldots, w_{n+1})$ in $\mathbb{Z}^{n+1}$ such that

$$\|\psi(w_1, \ldots, w_{n+1}), \lambda w_{n+1})\| \leq \delta(\det L)^{1/(n+1)}.$$

Let b' be the element of R encoded by $(w_1, \ldots, w_n)$ and let $j = w_{n+1}/\lambda$. Output b' and j and terminate.

We prove this algorithm is correct as follows. By an argument exactly similar to that following Algorithm 5.3, we obtain

$$|N(b')| \leq \delta^n (\det L)^{n/(n+1)}.$$

It is clear that $\det L = \lambda \det \psi(aR) = \lambda\theta N(aR)$. So

$$\begin{aligned} |N(b')| &\leq \delta^n (\lambda\theta N(aR))^{n/(n+1)} \\ &= \frac{\delta^n (\theta N(aR))^{n/(n+1)} N(aR)^{1/(n+1)}}{4^{n/(n+1)} \delta^n \theta^{n/(n+1)}} \\ &= \frac{N(aR)}{4^{n/(n+1)}} \leq |N(a)|/2. \end{aligned}$$

Further, by similar reasoning

$$|j\lambda| \leq \delta(\lambda\theta N(aR))^{1/n+1},$$

so

$$\begin{aligned}|j| &\le \delta\lambda^{-n/(n+1)}(\theta N(aR))^{1/n+1} \\ &= \delta(\theta N(aR))^{1/n+1}\left(\frac{N(aR)^{1/n}}{4\delta^{n+1}\theta}\right)^{-n/(n+1)} \\ &= \delta\theta^{1/n+1}(4\delta^{n+1}\theta)^{n/(n+1)} \\ &= 4^{n/(n+1)}\delta^{n+1}\theta \le 4\delta^{n+1}\theta.\end{aligned}$$

Finally, if $j = 0$ then $b' = ax$ for some $x \in R$. Thus $|N(b')| = |N(ax)| = |N(a)||N(x)| \ge |N(a)|$ since $x \in R$. However, we have just proved that $|N(b')| < |N(a)|$. This contradiction establishes that $j \neq 0$. We have now shown that Algorithm 5.4 is correct.

3. Precomputations

Our algorithm requires us to perform some precomputations which depend only on the size of m. We describe these precomputations in this section. For ease of notation we write $R = \mathbb{Z}[\zeta]$.

Since m is fixed for us, we do not care about the speed of these precomputations. We will feel free, then, to assume that any rational integer may be factored into primes, although the best algorithms to do this do not run in polynomial time. The reader may consult [4, Chapter 10] for a selection of factoring algorithms. By factoring norms, it is easy to find the decomposition of a given rational prime or to factor an ideal into prime ideals (see [4, pp. 314–316 and Chapter 6] for implementations). In a similar way we can also find all ideals, or all prime ideals, of norm less than some bound.

We now list the objects which we precompute.

- The factorization of m and mR.
- The degree of $\mathbb{Q}(\zeta)$ (namely $\phi(m)$) and the discriminant of $\mathbb{Z}[\zeta]$. There is a formula for each (see [7, p. 20] and [13, p. 44]).
- The quantity θ defined above. Since all the embeddings of K in $\mathbb{C}$ are complex, we have

$$\theta = 2^{-\phi(m)/2}\sqrt{|\operatorname{disc} R|}.$$

- The set $\mathcal{P}$ of all prime ideals of norm less than $4\delta^{\phi(m)+1}\theta$.

We will need to make one more type of precomputation. Let

$$\mathcal{B} = \{\text{ideals } \mathfrak{b} \text{ in } R \mid N(\mathfrak{b}) \le \delta^{\phi(m)}\theta\}$$

and

$$\mathcal{C} = \{jR \mid j \in \mathbb{Z}, 0 < j \leq 4\delta^{\phi(m)+1}\theta\}.$$

To make use of Algorithms 5.3 and 5.4 we will want to compute power residue symbols of the form $(a/\mathfrak{b})$ with $\mathfrak{b} \in \mathcal{B}$ and of the form (a/jR) with $jR \in \mathcal{C}$. We do this by precomputing tables of power residue symbols.

The precomputation of the tables goes as follows. It is easy to use the set $\mathcal{P}$ to construct the set $\mathcal{B}$, and the set $\mathcal{C}$ is trivial to construct. Then for each $\mathfrak{b} \in \mathcal{B}$ we let $\{b_1, \ldots, b_k\} \subset R$ be a set of coset representatives for $R/\mathfrak{b}$, compute $(b_i/\mathfrak{b})$ for each $i = 1, 2, \ldots, k$ (first factoring $\mathfrak{b}$ and then using the obvious but non-polynomial-time algorithm described after Proposition 3.6), and let the first table consist of all symbols of this form. For the second table, we do precisely the same thing for all elements $jR \in \mathcal{C}$. These two tables clearly permit us to find, in polynomial time, $(a/\mathfrak{b})$ or (a/jR) for any $a \in R$ and $\mathfrak{b} \in \mathcal{B}$ or $jR \in \mathcal{C}$.

4. Algorithm and Analysis

We now present a polynomial-time algorithm that computes the power residue symbol in $\mathbb{Q}(\zeta)$. The algorithm is in two parts, the first being a reduction to an (extended) symbol of the form (a/b) and the second being a recursive algorithm to compute (a/b). As in the last section, we let $R = \mathbb{Z}[\zeta]$.

ALGORITHM 5.5. Given an element $a \in R$ and an ideal $\mathfrak{b}$ in R such that $\mathfrak{b} \in \mathcal{I}(a)$, this algorithm finds $(a/\mathfrak{b})$.

Step 1 Apply Algorithm 5.3 to find an element $b \in \mathfrak{b}$ and an ideal $\mathfrak{c}$ of norm less than $\delta^{\phi(m)}\theta$ such that $\mathfrak{b}\mathfrak{c} = bR$. Compute $(a/\mathfrak{c})$.

Step 2 Find a' such that $a' \equiv a \mod b$ and a' is in the fundamental parallelotope of the lattice bR.

Step 3 Use Algorithm 5.6 to find (a'/b), output

$$\left(\frac{a'}{b}\right)\left(\frac{a}{\mathfrak{c}}\right)^{-1},$$

and terminate.

ALGORITHM 5.6. Given elements a and b in R with b nonzero, this algorithm finds (a/b).

Step 1 If $a = 0$ then output 1 and terminate.

Step 2 Use Algorithm 5.4 to find a nonzero $j \in \mathbb{Z}$ and $b' \in R$ such that $|j| \leq 4\delta^{\phi(m)+1}\theta$, $jb \equiv b' \bmod a$ and $|N(b')| \leq |N(a)|/2$. Compute (a/j).

Step 3 For all primes $\mathfrak{p}$ in the set $\mathcal{P}$, determine whether both a and b are in $\mathfrak{p}$. Let $\mathcal{Q}(a,b)$ be the set of all such primes together with all those that divide mR.

Step 4 Use Daberkow's algorithm and the formula (1) to find the product

$$\prod_{\mathfrak{q} \in \mathcal{Q}(a,b)} (a,b)_{\mathfrak{q}}.$$

Step 5 Recursively calculate (b'/a), output

$$\left(\frac{a}{j}\right)^{-1} \left(\frac{b'}{a}\right) \prod_{\mathfrak{q} \in \mathcal{Q}(a,b)} (a,b')_{\mathfrak{q}},$$

and terminate.

The condition $|N(b')| < |N(a)|/2$ means that the recursion must eventually terminate. For correctness, we need only verify that step 3 of Algorithm 5.6 produces $\mathcal{Q}(a,b)$ as we defined it in Section 1; then the algorithm is correct by the formulas

$$(a/\mathfrak{b})(a/\mathfrak{c}) = (a/b), \quad (a/jb) = (a/j)(a/b),$$

and (2). To check step 3, observe first that when Algorithm 5.5 calls Algorithm 5.6, the only primes which can divide both aR and bR are those which divide $\mathfrak{c}$, and these primes must necessarily lie in $\mathcal{P}$. Further, at each recursive call we have $b' = jb - ca$ and so in order to divide both aR and $b'R$ a prime must either divide both aR and bR or both aR and jR. Each such prime must lie in $\mathcal{P}$. We see that it suffices to examine only the primes in $\mathcal{P}$ to determine the primes dividing both aR and bR, so step 3 is obviously correct.

Note that we obtain from the last paragraph an easy check of the correctness of our input. That is, in the final step we have $a = 0$ and it is easy to see that only primes in $\mathcal{P}$ can divide bR. We thus test, for each $\mathfrak{p} \in \mathcal{P}$, whether b lies in $\mathfrak{p}$, and compute the product of all such primes. If this product is not equal to bR, we conclude that our initial input was in error and $\mathfrak{b}$ could not have been in $\mathcal{I}(a)$.

We now show that the algorithm runs in polynomial time. Clearly steps 1 and 2 of Algorithm 5.5 run in a time polynomial in the input size, so we need only check that the running time of Algorithm 5.6 is polynomial in the size of the input to Algorithm 5.5.

Observe that by reasoning similar to that in Chapter 4,

$$\log N(\mathfrak{b}) \leq \text{size}(\mathfrak{b}).$$

Further, clearly

$$\log |N(b)| \leq \log N(\mathfrak{b}) + \log N(\mathfrak{c}) \leq \text{size}(\mathfrak{b}) + C$$

where $C = \log \delta^{\phi(m)}\theta$.

Let t be the maximum number of bit operations used in steps 1–4 of Algorithm 5.6 for inputs a'' and b'' with $|N(a'')| \leq |N(b)|$, $|N(b'')| \leq |N(b)|$. Let k be the total number of recursions that occur during the running of Algorithm 5.6 for the inputs a' and b; observe that $k \leq \log |N(a')|$ and that the running time of Algorithm 5.6 for the inputs a' and b is less than kt. We have

$$kt \leq \log |N(a')|t \leq \log |N(b)|t \leq (\text{size}(\mathfrak{b}) + C)t.$$

The quantity t depends on $\mathfrak{b}$ and it is clear that it is polynomial in the size of $\mathfrak{b}$. We can now quickly see that the running time of the algorithm is polynomial in the size of $\mathfrak{b}$, hence polynomial in the whole input size.

Bibliography

1. Johannes A. Buchmann and Hendrik W. Lenstra, Jr., *Approximating rings of integers in number fields*, Journal de Théorie des Nombres de Bordeaux **6** (1994), 221–260.
2. J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.
3. J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Thompson Book Co., 1967.
4. Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.
5. Thomas H. Cormen, Charles E. Leierson, and Ronald L. Rivet, *Introduction to Algorithms*, The MIT Press, 1990.
6. Mario Daberkow, *On computations in Kummer extensions*, Journal of Symbolic Computation (to appear).
7. Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1990.
8. Nathan Jacobson, *Basic Algebra I*, W. H. Freeman, 1980.
9. Serge Lang, *Algebraic Number Theory*, Addison-Wesley, 1970.
10. A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.
11. Hendrik W. Lenstra, Jr., *Computing Jacobi symbols in algebraic number fields*, Nieuw Arch. Wisk. **13** (1995), 421–426.
12. _____, *Euclidean number fields II*, Math. Intelligencer **2** (1979/80), 73–77.
13. Daniel A. Marcus, *Number Fields*, Springer-Verlag, 1977.
14. Jean P. Serre, *Local Fields*, Springer-Verlag, 1979.