

ALGEBRAIC NUMBER THEORY AND QUADRATIC RECIPROCITY

HENRY COHN, JOSHUA GREENE, JONATHAN HANKE

1. INTRODUCTION

These notes are from a series of lectures given by Henry Cohn during MIT's Independent Activities Period in January, 1995. They were first revised by Henry Cohn and Jon Hanke at PROMYS 1995 and then Joshua Greene worked on further revision at PROMYS 1996. The main references are *A Classical Introduction to Modern Number Theory* by Ireland and Rosen and *Algebraic Theory of Numbers* by Weyl; the proofs of uniqueness of ideal factorizations and the finiteness of the class number are taken from Ireland and Rosen, and the proof of quadratic reciprocity is taken from Weyl. Several theorems from algebra are stated without proof. In all cases, proofs can be found in *Algebra* by M. Artin.

The goal of these notes is to develop the basic properties of rings of integers in algebraic number fields, and then to deduce the law of quadratic reciprocity in an especially clear and compelling way. We have tried to avoid using much algebra. (In particular, no Galois theory is required.) However, a few fundamental definitions are needed. One ought to know the definitions of rings (which we assume to be commutative and have multiplicative identities) and fields, and of vector spaces and dimension; the main non-obvious fact which we will assume is that the dimension of a finite-dimensional vector space is well-defined.

We will want to use the language of ideals, but we will not assume any prior familiarity with them. Suppose n is an integer, and consider the set (n) of multiples of n . This set has several useful properties: the sum of any two elements of (n) is in (n) , and if a is in (n) and b is any integer, then ab is in (n) . Any non-empty subset I of a ring R with these two properties ($a, b \in I$ implies $a + b \in I$ and $a \in I, b \in R$ implies $ab \in I$) is called an *ideal*. The intuition is that every ideal is the set of multiples of some element. For some rings, such as \mathbb{Z} , this claim is true, as we will prove below. For some rings, it is false, but we can imagine that the ideal is the set of multiples of some “ideal element” not contained in the actual ring (hence the name “ideal”).

Given any element $a \in R$, we define (a) to be the set of multiples of a . Clearly, (a) is an ideal, called the *principal ideal* generated by a . (Sometimes it is denoted by aR or Ra .) A ring in which every ideal is of this form (and which also is an integral domain, i.e., $ab = 0$ implies $a = 0$ or $b = 0$) is called a *principal ideal domain* (or PID).

More generally, we can look at ideals generated by several elements. We define

$$(a_1, a_2, \dots, a_n) = \{a_1b_1 + \dots + a_nb_n : b_1, \dots, b_n \in R\}.$$

This set is easily shown to be an ideal, and is in fact the smallest ideal of R containing a_1, \dots, a_n . As we will see in Theorem 2.2 (in the case $n = 2$), in \mathbb{Z} this ideal is generated by the greatest common divisor (gcd) of a_1, \dots, a_n .

The main use of ideals is that one can “mod out” by them. Given an ideal I , the quotient ring R/I is defined basically by identifying two elements of R iff they differ by an element of I . For example, if $n \in \mathbb{Z}$, the ring $\mathbb{Z}/(n)$ is the ring of integers modulo n . We assume some familiarity with this process, although perhaps not expressed in this language, so we will not pause to prove the basic properties of quotient rings. For the most part, they are evident from the definitions.

Date: July, 1996. Note that this is an unfinished draft, and should be treated as such, although it will likely never be finished.

2. IDEALS IN \mathbb{Z} AND UNIQUE FACTORIZATION

Lemma 2.1 (Division Algorithm in \mathbb{Z}). *For integers a and b with $b \neq 0$, there exist integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.*

We omit the proof (which is straightforward using induction or well ordering).

Theorem 2.2. *\mathbb{Z} is a principal ideal domain.*

Proof. Let $I \neq (0)$ be an ideal in \mathbb{Z} . It seems that I should be generated by its least positive element. Let g be that element, and let n be any element of I . Since we would like to show that n is a multiple of g , we divide n by g . By the division algorithm, there exist q and r such that $n = gq + r$ with $0 \leq r < g$. Since $r = n - gq$, $r \in I$. Because g is the smallest positive element of I and $0 \leq r < g$, $r = 0$ and therefore n is a multiple of g , as desired. \square

Proposition 2.3. *For $a, b \in \mathbb{Z}$, there exist $c, d \in \mathbb{Z}$ such that $ac + bd = \gcd(a, b)$.*

Proof. Consider the ideal (a, b) generated by a and b . Since \mathbb{Z} is a PID, $(a, b) = (g)$ for some g . Then g divides each of a and b . Since $g \in (a, b)$, there exist c and d such that $g = ac + bd$. Thus, any common divisor of a and b divides g . We see that $g = \gcd(a, b)$, and that g is a linear combination of a and b . \square

Using a variant of Euclid's algorithm (related to continued fractions), one can find efficiently the c and d which Proposition 2.3 says exist.

Definition 2.4. A *prime* is an integer p other than ± 1 whose only factors are ± 1 and $\pm p$. (In particular, we allow negative primes.)

Theorem 2.5. *If p is prime and p divides ab , then p divides a or p divides b .*

Proof. Suppose p does not divide a . Then since p is prime, p and a are relatively prime, i.e., their gcd is 1. By Proposition 2.3, there exist c and d such that $pc + ad = 1$. Multiplication by b yields $pcb + abd = b$. By assumption p divides ab and therefore abd , and clearly p divides pcb , so p divides b . \square

Theorem 2.6 (Unique Factorization in \mathbb{Z}). *Factorization of non-zero integers into primes is unique, up to rearrangement of the factors and change of their signs.*

Note that we consider 1 to have the empty prime factorization: it is the product of no primes.

Proof. We first need to establish the existence of prime factorizations. The proof is most easily organized by induction. The base case 2 is trivial because 2 is already prime. Now, say that n is a natural number and assume that all natural numbers less than n have a prime factorization. If n is prime already, then we are done. If n is composite, then there are two natural numbers a, b such that $ab = n$ and $a, b < n$. By induction $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_s$ for primes p_i, q_j . Then $p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s = n$ and this is a prime factorization.

The next step is to show that the prime factorization is unique. Suppose there were integers with several prime factorizations. Then there would be a non-zero integer n with several prime factorizations such that $|n|$ is as small as possible, say $n = p_1 \cdots p_s = q_1 \cdots q_t$. Then p_1 divides $q_1 \cdots q_t$ so by Theorem 2.5 (iterated) it divides some q_i , without loss of generality q_1 . Since p_1 and q_1 are prime, we must have $p_1 = \pm q_1$. Then $|n/p_1| < |n|$, but $n/p_1 = p_2 \cdots p_s = \pm q_2 \cdots q_t$ has two different prime factorizations. This is a contradiction, so prime factorizations are unique. \square

There are shorter proofs of unique factorization, but they are tricky and unrelated to algebraic number theory. This proof, however, generalizes nicely, as we will see in the next lecture.

Remark 2.7. There is a strong analogy in number theory between the ring \mathbb{Z} of integers and the ring $K[x]$ of polynomials over a field K . (The analogy is strongest when K is a finite field, but for these results any field will do.) Making only a few changes, we can carry over all of the results of this section to $K[x]$. The main change is that the right way to measure the size of a polynomial is by its degree. For reference, we restate the results of this section in terms of polynomials:

In the following statements, K is a field.

Lemma 2.8. For $f, g \in K[x]$ with $g \neq 0$, there exist $q, r \in K[x]$ such that $f = gq + r$ and $r = 0$ or $\deg r < \deg g$.

Theorem 2.9. $K[x]$ is a principal ideal domain.

Proposition 2.10. For $f, g \in K[x]$, there exist $h, k \in K[x]$ such that $fh + gk = \gcd(f, g)$.

Theorem 2.11. If f is irreducible and f divides gk , then f divides g or f divides k .

Theorem 2.12. Factorization of non-zero polynomials into irreducibles is unique, up to rearrangement of the factors and multiplication by units (here, units are just non-zero constants from K).

3. MODULAR ARITHMETIC

Theorem 3.1. If a is relatively prime to n , then there exists b such that $ab \equiv 1 \pmod{n}$.

Proof. Proposition 2.3 tells us that there exist b and c such that $ab + nc = 1$. Hence, $ab \equiv 1 \pmod{n}$. \square

Corollary 3.2. The group of units modulo m , $(\mathbb{Z}/m\mathbb{Z})^\times$, is $\{a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} : (a, m) = 1\}$.

Corollary 3.3. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Theorem 3.4 (Euler's Theorem). If a is relatively prime to n , then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ is the number of integers from 1 to n that are relatively prime to n .

Proof. By Theorem 3.1, a is invertible modulo n . Let $\{u_1, \dots, u_{\varphi(n)}\}$ be a system of integers representing the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$. It follows that, modulo n , the numbers $au_1, au_2, \dots, au_{\varphi(n)}$ are another system of representatives for $(\mathbb{Z}/n\mathbb{Z})^\times$. Multiplying these tells us that

$$u_1 \cdot u_2 \cdots u_{\varphi(n)} \equiv au_1 \cdot au_2 \cdots au_{\varphi(n)} \pmod{n}.$$

We can cancel the u_i to get $a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

Corollary 3.5 (Fermat's Little Theorem). If p is prime, then $a^p \equiv a \pmod{p}$.

Proof. For an integer a , there are only two possibilities: a is relatively prime to p or p divides a . In the former case Euler's Theorem tells us that $a^{\varphi(p)} \equiv 1 \pmod{p}$. Recall that $\varphi(p)$ is the number of positive integers less than p and relatively prime to p . Because p is prime, $\varphi(p) = p - 1$. Thus, $a^p \equiv a$.

If p divides a , then $a \equiv 0 \pmod{p}$ so $a^p \equiv a \pmod{p}$ trivially. \square

The logic that leads to Corollary 3.3 also proves the following result:

Corollary 3.6. If K is a field and $f \in K[x]$ is irreducible, then $K[x]/(f)$ is a field.

4. FIELD EXTENSIONS

This section and the next summarize the basic definitions and facts for field extensions. Some familiarity with field theory may be necessary to follow this, but we hope not too much.

Definition 4.1. Given fields K and L with $K \subset L$, we call L an *extension* of K . We often refer to the extension L/K . (Note that this does not indicate a quotient ring.) We can regard L as a vector space over K . The extension L/K is *finite* if L is a finite-dimensional K -vector space. The *degree* of L/K is the dimension of L as a K -vector space, and is denoted $[L : K]$.

Proposition 4.2 (Multiplicativity of Degrees). Given field extensions L/K and K/F , if two of the three degrees $[L : K]$, $[K : F]$, and $[L : F]$ are finite, then the third is, and

$$[L : F] = [L : K][K : F].$$

Sketch of Proof. If $\alpha_1, \dots, \alpha_n$ form a basis of L/K , and β_1, \dots, β_m form a basis of K/F , then one can check that $\alpha_i \beta_j$ ($i = 1, \dots, n$, $j = 1, \dots, m$) form a basis of L/F . \square

Definition 4.3. Given an extension L/K , an element $\alpha \in L$ is *algebraic* over K if it satisfies a non-zero polynomial equation with coefficients in K .

Proposition 4.4. If L/K is a finite extension, then every element of L is algebraic over K .

Proof. The infinitely many elements $1, \alpha, \alpha^2, \dots$ cannot be linearly independent. A linear dependence between them gives a polynomial equation, showing that α is algebraic. \square

Proposition 4.5. *Suppose L/K is a field extension. Each element α of L that is algebraic over K is the root of a unique irreducible polynomial over K (unique up to multiplication by non-zero constants, that is). If α is the root of an irreducible polynomial of degree n , then $K(\alpha)/K$ is finite, and has degree n .*

Proof. Consider the map $\pi : K[x] \rightarrow K[\alpha]$ that substitutes α for x in a polynomial. The kernel of this map is a principal ideal (since $K[x]$ is a PID), generated by a polynomial f , which is the polynomial of least degree which has α as a root. This polynomial is irreducible, since if it factored, then α would be a root of one of the factors. Further, f divides any polynomial which has α as a root because $\ker \pi = (f)$. Therefore, up to multiplication by a constant, it is the only irreducible polynomial to have α as a root.

Now suppose that $f(x)$ has degree n . The ring $K[\alpha]$ is isomorphic to $K[x]/(f(x))$ (the quotient of the polynomial ring $K[x]$ by the ideal generated by $f(x)$). In particular, $K[\alpha]$ has a basis $1, \alpha, \dots, \alpha^{n-1}$ consisting of n elements. Corollary 3.6 implies that $K[\alpha]$ is a field, from which it follows that $K(\alpha) = K[\alpha]$, and $K(\alpha)$ is a degree n extension of K . \square

Definition 4.6. If α is algebraic over K , then the unique monic irreducible polynomial satisfied by α is called the *minimal polynomial* of α over K .

Theorem 4.7. *Given any extension L/K , the set F of elements of L which are algebraic over K forms a field.*

Proof. Notice that for any $\alpha \in K$, α is the root of a polynomial $(x - \alpha) \in K[x]$. Therefore, α is algebraic over K , so $K \subset F$.

Suppose α and β are algebraic over K . Since $K(\alpha, \beta)$ is a finite extension of $K(\alpha)$, which is a finite extension of K , we see that $K(\alpha, \beta)$ is a finite extension of K , by Proposition 4.2. Hence, Proposition 4.4 implies that $\alpha + \beta$ and $\alpha\beta$ are algebraic. Thus, F is a ring. Since

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$$

implies

$$a_n + a_{n-1} \alpha^{-1} + \dots + a_1 \alpha^{-n+1} + a_0 \alpha^{-n} = 0,$$

we see that α^{-1} is algebraic if $\alpha \neq 0$ is. Hence, F is a field. \square

Proposition 4.8. *Let L/K be an extension of fields of characteristic 0. If $\alpha, \beta \in L$, then for all but finitely many choices of $c \in K$, $\alpha + c\beta$ generates $K(\alpha, \beta)$ over K , i.e. $K(\alpha, \beta) = K(\alpha + c\beta)$.*

The proof of this proposition can be found in Weyl's book or Artin's (see the references section).

Corollary 4.9. *Any finite extension L/K of fields of characteristic 0 is generated by a single element, i.e., there is some $\alpha \in L$ such that $L = K(\alpha)$.*

5. CONJUGATES AND SYMMETRY

Definition 5.1. A polynomial $f(x_1, \dots, x_n)$ of n variables is called *symmetric* if for each permutation σ of $\{1, \dots, n\}$,

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Definition 5.2. For $1 \leq i \leq n$, the *i -th elementary symmetric polynomial* $s_i(x_1, \dots, x_n)$ in the variables x_1, \dots, x_n is the sum of all products of i of the variables. For example,

$$s_1 = x_1 + \dots + x_n,$$

$$s_2 = \sum_{j < k} x_j x_k = x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + x_2 x_3 + x_2 x_4 + \dots + x_{n-1} x_n,$$

and

$$s_n = x_1 \cdots x_n.$$

Theorem 5.3 (Fundamental Theorem on Symmetric Polynomials). *Every symmetric polynomial is a polynomial in the elementary symmetric polynomials. In other words, if f is a symmetric polynomial of n variables, then there exists a polynomial g such that $f(x_1, \dots, x_n) = g(s_1, \dots, s_n)$. (This holds for polynomials with coefficients in any ring.)*

We omit the proof of this theorem. It can be found in Artin's book. Also, a solution is sketched in Exercise 7 below.

Note that since

$$(y - x_1) \cdots (y - x_n) = y^n - s_1 y^{n-1} + \cdots + (-1)^n s_n,$$

the coefficients of the polynomial with roots x_1, \dots, x_n are plus or minus s_1, \dots, s_n . It is common to try to express some function of the roots of a polynomial in terms of its coefficients. We see now that if that function is a polynomial, then this can be done if (and obviously only if) the polynomial is symmetric.

For example, $x_1^2 + \cdots + x_n^2$ is symmetric, and

$$x_1^2 + \cdots + x_n^2 = s_1^2 - 2s_2.$$

The product

$$\prod_{j < k} (x_j - x_k)$$

is not symmetric, so it cannot be expressed in terms of elementary symmetric polynomials. However, its square

$$\prod_{j < k} (x_j - x_k)^2$$

is symmetric, and can therefore be expressed in terms of elementary symmetric polynomials. The expression is something of a mess, however. Incidentally, this is the discriminant of the polynomial

$$y^n - s_1 y^{n-1} + \cdots + (-1)^n s_n.$$

Proposition 5.4. *Let f be an irreducible polynomial over a field K of characteristic 0. In any extension of K , f has no multiple roots.*

Proof. Recall that a multiple root of f is the same as a common root of f and f' . Since f is irreducible and $\deg f' < \deg f$, they are relatively prime. (Note that this requires that the characteristic of f be 0. In characteristic p , we could have $f' = 0$. For example, the derivative of $x^p - a$ is $px^{p-1} = 0$. However, this cannot happen in characteristic 0. In characteristic 0, f' is not zero. Then since $\deg f' < \deg f$, f' is not divisible by f , and thus since f is irreducible, we must have $\gcd(f, f') = 1$.)

In particular, there exist g and k such that $fg + f'k = 1$. This implies that f and f' are relatively prime over any extension of K , and hence that f has no multiple roots in any extension of K . \square

Note the use of the derivative in the preceding proof. We used only purely formal properties of it, and can thus define it by the formula for differentiating a polynomial (so we needn't worry about limits if K is a weird field).

Definition 5.5. An *embedding* of a field K into a field L is a one-to-one homomorphism $K \hookrightarrow L$.

Let us consider the possible embeddings of \mathbb{Q} into another field. Say that K is a field, and $\sigma : \mathbb{Q} \hookrightarrow K$ is an embedding. Then $\sigma(1) \neq 0$ because σ is injective. Further, for any $a \in \mathbb{Q}^\times$,

$$\sigma(a) = \sigma(1 \cdot a) = \sigma(1)\sigma(a).$$

Cancelling $\sigma(a)$ from both sides (we are in a field here!), we obtain $\sigma(1) = 1$. This, and the fact that σ is additive, uniquely specifies σ on all of \mathbb{Z} . Given $r \in \mathbb{Q}$, we can write $r = m/n$ for appropriately chosen integers, m, n . We already know that $\sigma(m)$ and $\sigma(n)$ are specified, and $\sigma(r) = \sigma(m)(\sigma(n))^{-1}$. Therefore, σ is uniquely determined on all of \mathbb{Q} , so there can be at most one embedding of \mathbb{Q} into a given field. Also, if the characteristic of K is 0 then the map taking $1 \in \mathbb{Q}$ to $1 \in K$ does define an embedding.

In particular, \mathbb{Q} sits as a subset of \mathbb{C} and this argument shows that there is no other way to embed \mathbb{Q} in \mathbb{C} .

In the rest of this section, the results mention the field \mathbb{Q} explicitly. They can all be stated in more general forms, but for our purposes that won't be necessary.

Proposition 5.6. *An extension of \mathbb{Q} of degree n has exactly n embeddings into \mathbb{C} .*

Proof. By Corollary 4.9, the extension is $\mathbb{Q}(\alpha)$ for some α , and by Proposition 4.5, α is a root of an irreducible polynomial $f(x)$ of degree n . Suppose that the n roots of $f(x)$ in \mathbb{C} are $\alpha_1, \dots, \alpha_n$. These roots must all be distinct, by Proposition 5.4.

For $1 \leq i \leq n$, we can define a map $\sigma_i : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ that takes α to α_i . Note that σ_i has no choice about where to take \mathbb{Q} , so it is uniquely determined by the image of α . Also, note that there really is such a map. To see this, recall that $\mathbb{Q}(\alpha_i)$ is isomorphic to $\mathbb{Q}[x]/(f(x))$. To get σ_i , we just compose the isomorphism from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}[x]/(f(x))$ that takes α to x with the isomorphism from $\mathbb{Q}[x]/(f(x))$ to $\mathbb{Q}(\alpha_i)$ that takes x to α_i .

Now we have at least n embeddings from $\mathbb{Q}(\alpha)$ to \mathbb{C} . Say that τ is an embedding from $\mathbb{Q}(\alpha)$ to \mathbb{C} . Then $\tau(f(\alpha)) = \tau(0) = 0$. However, because τ fixes \mathbb{Q} and τ is a homomorphism, $\tau(f(\alpha)) = f(\tau(\alpha))$. The image of α under an embedding must, therefore, be a root of f . Thus, τ is one of the σ_i , so we have exactly n embeddings. \square

Definition 5.7. Suppose K/\mathbb{Q} is an extension of degree n , with embeddings $\sigma_1, \dots, \sigma_n$ into \mathbb{C} . Given $\alpha \in K$, the *conjugates* of α are $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$. The *trace* of α is

$$\text{tr}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$$

and the *norm* of α is

$$\text{nm}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

The conjugates, norm, and trace of α depend not only on α , but also on K . For example, in \mathbb{Q} , $\text{nm}(2) = 2$, but in $\mathbb{Q}(i)$ the two conjugates of 2 are 2 and 2, so $\text{nm}(2) = 4$. Because of this, we may sometimes denote the norm and trace by nm_K and tr_K .

Also, given any finite extension K/F , one can define relative norms and traces from K to F . However, we won't need to use them in these notes.

Proposition 5.8. *Given α in a finite extension K of \mathbb{Q} , $\text{nm}(\alpha)$ and $\text{tr}(\alpha)$ are in \mathbb{Q} . More generally, any symmetric polynomial in the conjugates of α is in \mathbb{Q} .*

Proof. By Corollary 4.9, we can suppose $K = \mathbb{Q}(\theta)$. Also, say that the degree of K over \mathbb{Q} is n , so $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ is a vector space basis for K over \mathbb{Q} . Then α can be written as a \mathbb{Q} -linear combination of these basis elements, and this is the same as writing α as a polynomial in θ with \mathbb{Q} coefficients. Let g be such a polynomial, so that $\alpha = g(\theta)$.

The conjugates of α are then given by $g(\sigma_i(\theta))$, where $\sigma_1, \dots, \sigma_n$ are the embeddings of K into \mathbb{C} . In other words, they are given by the same polynomial, with θ replaced by its conjugates. Any polynomial $p(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$ that is symmetric in the conjugates of α then becomes a polynomial $p(g(\sigma_1(\theta)), \dots, g(\sigma_n(\theta)))$, which is symmetric in the conjugates of θ . However, we know that θ is a root of a polynomial over \mathbb{Q} of degree n . Thus, the elementary symmetric polynomials in the conjugates of θ are rational, since they are plus or minus the coefficients of the irreducible polynomial of θ over \mathbb{Q} . By the Fundamental Theorem on Symmetric Polynomials, we see that p is also rational. \square

Proposition 5.9. *Suppose we have a finite extension K/\mathbb{Q} , and $\alpha, \beta \in K$. If the embeddings of K into \mathbb{C} are $\sigma_1, \dots, \sigma_n$, then the polynomials*

$$\prod_{i,j} (x - \sigma_i(\alpha) - \sigma_j(\beta))$$

and

$$\prod_{i,j} (x - \sigma_i(\alpha)\sigma_j(\beta))$$

have rational coefficients.

Proof. Pick one of the two polynomials and designate it as $F(x)$. Consider the coefficients of x in F . Each coefficient is symmetric separately in the conjugates of α and the conjugates of β . Focus on a_i , the

coefficient of x^l . This coefficient a_l , is a polynomial in the conjugates of β , with coefficients which are conjugates of α . That is a_l is some element of

$$h(X_1, \dots, X_n) \in \mathbb{Q}[\sigma_1(\alpha), \dots, \sigma_n(\alpha)][X_1, \dots, X_n]$$

evaluated at $(\sigma_1(\beta), \dots, \sigma_n(\beta))$. Then, because the coefficients of h are symmetric polynomials in the $\sigma_i(\alpha)$, these coefficients are actually rational. This means that $h(X_1, \dots, X_n)$ is really in $\mathbb{Q}[X_1, \dots, X_n]$. Thus, a_l is a rational polynomial in the conjugates of β , but it is also symmetric in the conjugates of β . Therefore, a_l is rational. Because a_l was an arbitrary coefficient, F is itself in $\mathbb{Q}[x]$. \square

Note that this gives polynomials over \mathbb{Q} satisfied by $\alpha + \beta$ and $\alpha\beta$, thus giving another, more concrete proof that they are algebraic. In general, this is how one gets a polynomial over \mathbb{Q} satisfied by an algebraic number. For example, consider a root α of

$$\sqrt{2}x^4 + \sqrt{3}x^3 - x^2 + \sqrt{6}.$$

Of course, α ought to be algebraic, but the equation we have here does not have rational coefficients. Instead, it has coefficients in the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. To get rational coefficients, we simply try to make everything symmetric in the conjugates of the coefficients. The field K has degree 4 over \mathbb{Q} . Its four embeddings into \mathbb{C} are the identity, the map sending $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to itself, the map sending $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$, and the map sending $\sqrt{2}$ to itself and $\sqrt{3}$ to $-\sqrt{3}$.

Now consider the product

$$(\sqrt{2}x^4 + \sqrt{3}x^3 - x^2 + \sqrt{6})(-\sqrt{2}x^4 + \sqrt{3}x^3 - x^2 - \sqrt{6})(-\sqrt{2}x^4 - \sqrt{3}x^3 - x^2 + \sqrt{6})(\sqrt{2}x^4 - \sqrt{3}x^3 - x^2 - \sqrt{6}).$$

This simplifies to

$$4x^{16} - 12x^{14} + 5x^{12} - 6x^{10} - 48x^9 - 23x^8 - 36x^6 - 12x^4 + 36.$$

Since α is a root of this polynomial over \mathbb{Q} , α is indeed algebraic over \mathbb{Q} . In general, the reasoning used in the proof of Proposition 5.9 shows that this always works.

6. PROBLEMS

Learning the material well requires more than just reading the notes. Besides reviewing what was done and possibly doing additional reading, working problems is very useful.

Each problem has a difficulty rating from 1 to 3. Problems rated 1 are meant to be relatively easy; everyone should work on them to see how well they understand the material from the preceding sections. Problems rated 2 should be doable. Problems rated 3 can be tricky or time consuming; one should work on them only if they look interesting.

- (1) 1. Imitating the proof of Theorem 2.5, use Proposition 2.3 to prove the following result: Given $a, b, c \in \mathbb{Z}$ such that a divides bc and $\gcd(a, b) = 1$, a divides c .
- (1.5) 2. Suppose p is prime. By Fermat's Little Theorem, the polynomial $x^{p-1} - 1$ has the roots $1, 2, \dots, p-1$ modulo p . How does it factor in $\mathbb{Z}/p\mathbb{Z}$? What can one conclude about $(p-1)!$ modulo p ? (The result is called Wilson's Theorem, although Wilson didn't prove it. Supposedly, he stated it as a conjecture, and then claimed that nobody could prove it because there was no good notation for dealing with primes. Gauss disproved Wilson's claim by proving his conjecture.)
- (1) 3. Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. What is the trace of $3 + 2\sqrt{2}$? What is its norm?
- (1.5) 4. Consider the extension $\mathbb{Q}(2^{1/3})/\mathbb{Q}$. What is the trace of $2 + 2^{1/3} - 2^{2/3}$? What is its norm?
- (1.5) 5. Find an element $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$. Find the irreducible polynomial satisfied by α .
- (2) 6. Prove that $2^{1/3} - 2^{1/5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- (2.5) 7. Prove the Fundamental Theorem on Symmetric Polynomials as follows. First, we define an ordering on the monomials in the variables x_1, \dots, x_n , so that we can talk about the leading term of a polynomial in several variables. For the ordering, we first order by degree, and then break ties using lexicographic (dictionary) ordering. For example, x_1^3 comes before x_2^2 because of their degrees, and $x_1^2x_2^2x_3$ comes before $x_1^2x_2x_3^2$ because although they have the same degrees and the exponents of x_1 are the same, the exponent of x_2 in $x_1^2x_2^2x_3$ is greater than that in $x_1^2x_2x_3^2$.

Now show that we can systematically express any symmetric polynomial in terms of elementary symmetric polynomials as follows. Suppose we have a symmetric polynomial p . Show that there is a unique product of elementary symmetric polynomials such that subtracting a multiple of it will cancel the leading term of p . Prove that doing this repeatedly eventually gives 0, thereby expressing p in terms of elementary symmetric polynomials.

For example, suppose $n = 3$, and we have the polynomial $p(x_1, x_2, x_3) = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$. The leading term of p is $x_1^4x_2^2$. From p , we subtract $s_1^2s_2^2$, since it has the same leading term. The remaining polynomial has leading term $-4x_1^4y_1z_1$, so we add to it $4s_1^3s_3$. Continuing in this way, we eventually find that

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2 = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 18s_1s_2s_3 - 27s_3^2.$$

(3) 8. Prove Proposition 4.8.

7. THE GAUSSIAN INTEGERS

Definition 7.1. The *Gaussian integers* are the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Note that the conjugate of a Gaussian integer α is just its complex conjugate, which we denote $\bar{\alpha}$. Then its norm is $\text{nm}(\alpha) = \alpha\bar{\alpha}$. This is the square of its absolute value, of course. It is a more convenient measure of size than the absolute value is. One reason is that it is always an integer, while its square root is not. Another, deeper reason has to do with quotients of $\mathbb{Z}[i]$. Given an element $a + bi$ of $\mathbb{Z}[i]$, we can form the quotient ring $\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$, just as we form $\mathbb{Z}/n\mathbb{Z}$ from \mathbb{Z} . One can show that

$$\left| \mathbb{Z}[i]/(a + bi)\mathbb{Z}[i] \right| = \text{nm}(a + bi),$$

i.e., $\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$ has $\text{nm}(a + bi)$ elements.

It turns out that $\mathbb{Z}[i]$ is in many ways analogous to \mathbb{Z} . For example, Gaussian integers factor uniquely into primes. It turns out that theorems about factorization in $\mathbb{Z}[i]$ have some surprising consequences, so in this section we will prove unique factorization in $\mathbb{Z}[i]$.

Of course, we have to be careful about what we mean by unique factorization. In \mathbb{Z} , the numbers ± 1 have a special role. Because they are units (i.e., have multiplicative inverses), they can occur arbitrarily in factorizations. In $\mathbb{Z}[i]$, the units are ± 1 and $\pm i$. Note that these are exactly the elements of norm 1.

In a factorization in $\mathbb{Z}[i]$, we do not want to distinguish between a number and that number multiplied by a unit, just as we do not distinguish between numbers and their negatives in a factorization in \mathbb{Z} . Two Gaussian integers are called *associates* of each other if each is a unit times the other. For example, 2 is an associate of $-2i$. In the same way, one can define units and associates in any ring.

We now can generalize the definition of prime. For reasons to be explained in Section 9, we use the term “irreducible” rather than “prime.” (In general, we call irreducibles primes when we are dealing with a ring in which factorizations are unique. Irreducible polynomials are an exception to this.)

Definition 7.2. An *irreducible* in a ring is an element which is not a unit, and whose only factors are units or associates.

Note that whether an element is irreducible depends on the ring in which you view it. For example, 2 is irreducible in \mathbb{Z} , but in $\mathbb{Z}[i]$ it factors as $2 = i(1 - i)^2$.

Now that we have a notion of irreducibles and units, we can say what it means for a ring to have unique factorization.

Definition 7.3. An integral domain R is called a *unique factorization domain* (UFD) if each non-zero element of R factors as a product of irreducibles and units, and the irreducible factors are unique up to rearrangement and multiplication by units.

We will show that $\mathbb{Z}[i]$ is a UFD. To do this, we will imitate the proof in \mathbb{Z} . We will prove an analogue of the division algorithm in $\mathbb{Z}[i]$, and deduce from that that $\mathbb{Z}[i]$ is a PID. Then essentially the same proof as in the case of \mathbb{Z} will show that $\mathbb{Z}[i]$ is a UFD.

In formulating the division algorithm in $\mathbb{Z}[i]$, we seem to run into a problem that $\mathbb{Z}[i]$ is not ordered, so we can't compare two Gaussian integers. However, this is not really a problem, since we can simply use the ordering on their norms.

Proposition 7.4 (Division Algorithm in $\mathbb{Z}[i]$). *For $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exist $\kappa, \rho \in \mathbb{Z}[i]$ such that $\alpha = \beta\kappa + \rho$ and $0 \leq \text{nm}(\rho) < \text{nm}(\beta)$.*

Before proving this, recall how we divide Gaussian integers in practice. Suppose we want to obtain a quotient and remainder from the division of $7 - 5i$ by $3 + 4i$. The main idea is to convert this into a problem of dividing integers. First, note that we have

$$\frac{7 - 5i}{3 + 4i} = \frac{(7 - 5i)(3 - 4i)}{(3 + 4i)(3 - 4i)} = \frac{1 - 43i}{25} = (1/25) + (-2 + 7/25)i.$$

We choose $-2i$ as the quotient because $-2i$ is close to $(1/25) + (-2 + 7/25)i$. In general, the quotient cannot be chosen uniquely. Then, we have

$$7 - 5i = (3 + 4i)(-2i) + (-1 + i),$$

and indeed $\text{nm}(-1 + i) = 2 < 25 = \text{nm}(3 + 4i)$ so we see that we have chosen the quotient well to obtain a remainder with smaller norm than that of the divisor.

Proof. As above, we divide $\alpha\bar{\beta}$ by $\text{nm}(\beta)$. Suppose $\alpha\bar{\beta} = x_1 + x_2i$, with $x_1, x_2 \in \mathbb{Z}$. Using division in \mathbb{Z} , we can divide each of x_1 and x_2 by $\text{nm}(\beta)$. We choose the quotient so that instead of getting the least positive remainder, we get the remainder with the smallest absolute value. Then we have

$$x_1 = \text{nm}(\beta)q_1 + r_1 \quad \text{and} \quad x_2 = \text{nm}(\beta)q_2 + r_2,$$

with $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $|r_1| \leq \text{nm}(\beta)/2$, and $|r_2| \leq \text{nm}(\beta)/2$. It follows that

$$\alpha\bar{\beta} = \text{nm}(\beta)(q_1 + q_2i) + (r_1 + r_2i) = \bar{\beta}\beta(q_1 + q_2i) + (r_1 + r_2i).$$

Every term in this equation is divisible by $\bar{\beta}$ except possibly for $r_1 + r_2i$, so it also must be divisible by $\bar{\beta}$. Write $r_1 + r_2i = \bar{\beta}\rho$ with ρ a Gaussian integer, and also write $\kappa = q_1 + q_2i$. Then $\alpha = \beta\kappa + \rho$ and

$$\text{nm}(\rho) = \frac{\text{nm}(r_1 + r_2i)}{\text{nm}(\bar{\beta})} = \frac{(r_1^2 + r_2^2)}{\text{nm}(\beta)} \leq \frac{(\text{nm}(\beta)^2/4 + \text{nm}(\beta)^2/4)}{\text{nm}(\beta)} = \frac{\text{nm}(\beta)}{2}.$$

□

Note that the proof shows that we can choose a quotient such that $\text{nm}(\rho) \leq \text{nm}(\beta)/2$, which is better than $\text{nm}(\rho) < \text{nm}(\beta)$. Also, note that the quotient and remainder are not necessarily unique. For example,

$$3 = (1 + i)(2 - i) - i \quad \text{and} \quad 3 = (1 + i)(1 - 2i) + i.$$

Now that we have the division algorithm, exactly the same proof as in the case of \mathbb{Z} shows that the Gaussian integers form a PID, and hence a UFD (see Proposition 2.3 to Theorem 2.6). As before, one needs to prove the existence of factorizations. In fact, one can prove that factorizations exist in any PID. One can also prove it directly in cases like $\mathbb{Z}[i]$. For example, suppose there were non-zero, non-unit Gaussian integers that didn't factor into irreducibles. Choose one with minimal norm, say z . It can't be irreducible itself, so z must factor non-trivially. Then its factors have smaller norm, so they factor into irreducibles, and combining those two factorizations gives one for z , which is a contradiction.

8. SUMS OF SQUARES AND SPLITTING OF PRIMES

Now that we know that Gaussian integers factor uniquely into primes, we can ask what their factorizations look like. In particular, one interesting and important question is how ordinary integers factor in $\mathbb{Z}[i]$. Of course, we only need to answer this for prime¹ integers, which we call “rational primes” to distinguish them from primes in $\mathbb{Z}[i]$. It turns out that this is connected to whether the prime is a sum of two squares.

Proposition 8.1. *If p is a rational prime, then p is a sum of two squares iff p is not prime in $\mathbb{Z}[i]$.*

For example, $5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i)$, but 3 is prime in $\mathbb{Z}[i]$.

¹In this section, “prime” means “positive prime.” When dealing with factorizations in various rings, it is more convenient not to try to normalize the primes, as one does in \mathbb{Z} by looking only at positive primes. However, when dealing with congruences, it is convenient to consider only positive primes, because -3 behaves like 3, which is a prime congruent to 3 modulo 4, even though $-3 \equiv 1 \pmod{4}$.

Proof. If $p = a^2 + b^2$, then $p = (a + bi)(a - bi)$, so p is not prime in $\mathbb{Z}[i]$. Conversely, suppose p factors as $\alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[i]$ and not units. Then taking norms gives $p^2 = \text{nm}(p) = \text{nm}(\alpha)\text{nm}(\beta)$. Since α and β are not units, $\text{nm}(\alpha)$ and $\text{nm}(\beta)$ are not 1, so they must each be p . Thus, p is the norm of a Gaussian integer. However, $\text{nm}(a + bi) = a^2 + b^2$, so that means p is the sum of two squares. \square

Proposition 8.2. *If p is a rational prime, then p is not prime in $\mathbb{Z}[i]$ iff there is a square root of -1 modulo p , i.e., iff there exists an integer h such that $h^2 \equiv -1 \pmod{p}$.*

Proof. If p is not prime in $\mathbb{Z}[i]$, then Proposition 8.1 implies that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Because p is a rational prime and $a, b \in \mathbb{Z}$, neither a nor b can be a multiple of p , so they are units modulo p . If we take $h \equiv a/b \pmod{p}$, then $h^2 \equiv a^2/b^2 \equiv -1 \pmod{p}$.

Now we prove the converse. Suppose $h^2 \equiv -1 \pmod{p}$. Then p divides $h^2 + 1$. In $\mathbb{Z}[i]$, $h^2 + 1$ factors as $(h + i)(h - i)$. Note that p does not divide $h + i$ (since it would have to divide the imaginary part), and p does not divide $h - i$. Since p divides the product $(h + i)(h - i)$ but neither factor, p must not be prime in $\mathbb{Z}[i]$. \square

Notice that this last conclusion of this proof depends on the fact that $\mathbb{Z}[i]$ has unique factorization.

So far, we have shown that p is the sum of two squares iff -1 is a square modulo p . Using the following lemma, we will be able to determine when -1 is a square modulo p :

Lemma 8.3 (Euler's Criterion). *If p is an odd, rational prime, and $a \not\equiv 0 \pmod{p}$, then a is a square modulo p iff $a^{(p-1)/2} \equiv 1 \pmod{p}$. If a is not a square modulo p , then $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Proof. If a is a square modulo p , then $a \equiv b^2 \pmod{p}$ for some b . Then $a^{(p-1)/2} \equiv b^{p-1} \equiv 1$ by Fermat's Little Theorem.

Note that there are $(p-1)/2$ non-zero squares modulo p (since there are $(p-1)/2$ pairs of non-zero square roots, which are plus or minus each other). The polynomial $x^{(p-1)/2} - 1$ can have only $(p-1)/2$ roots modulo p , since $\mathbb{Z}/p\mathbb{Z}$ is a field. Therefore, if a is not a square modulo p , then $a^{(p-1)/2} \not\equiv 1 \pmod{p}$.

Because $a^{p-1} \equiv 1 \pmod{p}$, $a^{(p-1)/2}$ is a square root of 1 modulo p . Since p is prime, if it is not 1, then it must be -1 , modulo p . \square

Corollary 8.4. *If p is an odd prime, then p is a sum of two squares iff $p \equiv 1 \pmod{4}$.*

At this point, it is easy to completely classify the primes in $\mathbb{Z}[i]$. First, note that Corollary 8.4 and Proposition 8.1 together imply that all rational primes $\equiv 3 \pmod{4}$ remain prime in $\mathbb{Z}[i]$. Rational primes p , which are $\equiv 1 \pmod{4}$ factor into $p = \pi\bar{\pi}$, but π is now prime in $\mathbb{Z}[i]$: if $\alpha\beta = \pi$, then $\text{nm}(\alpha\beta) = \text{nm}(\pi) = p$, but $\text{nm}(\alpha\beta) = \text{nm}(\alpha)\text{nm}(\beta)$, so this gives a factorization of p in \mathbb{Z} . One of $\text{nm}(\alpha), \text{nm}(\beta)$ must be 1, so $\alpha\beta$ is a trivial factorization of π . A similar argument reveals that $(1+i)$ is prime.

We will now show that, up to associates, these are the only primes in $\mathbb{Z}[i]$. Say that we start with $\pi \in \mathbb{Z}[i]$ a prime. Then we already know how to factor $\text{nm}(\pi)$ in \mathbb{Z} , so write

$$\pi\bar{\pi} = \text{nm}(\pi) = 2^r p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t$$

where the p_i are rational primes congruent to 1 $\pmod{4}$, and the q_j are rational primes congruent to 3 $\pmod{4}$. When we pass to $\mathbb{Z}[i]$ and factor further into primes, $2^r = i^r(1+i)^{2r}$, $p_i = \pi_i\bar{\pi}_i$ and the q_j remain prime.

Therefore,

$$\pi\bar{\pi} = i^r(1+i)^{2r} \pi_1\bar{\pi}_1 \cdots \pi_s\bar{\pi}_s q_1 q_2 \cdots q_t.$$

Because π is prime and factorization into primes is unique in $\mathbb{Z}[i]$, π must be an associate of one of the primes on the right hand side. Therefore, π was already on our list of Gaussian primes.

9. FAILURE OF UNIQUE FACTORIZATION

Ideally, every ring would have unique factorization. However, that is not the case, even for interesting rings. It turns out that $\mathbb{Z}[\sqrt{-2}]$ is a UFD. (One can conclude from this that an odd prime is of the form $x^2 + 2y^2$ iff -2 is a square modulo the prime.) However, $\mathbb{Z}[\sqrt{-3}]$ is not. In it, one has

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2.$$

Each factor has norm 4. Since there is nothing of norm 2, they are irreducible. However, the only units are ± 1 , so none of them are associates of each other. It follows that 4 has two different factorizations into irreducibles in $\mathbb{Z}[\sqrt{-3}]$.

Surprisingly, one can recover unique factorization by adding in additional elements. Suppose we don't just look at the ring $\mathbb{Z}[\sqrt{-3}]$ but also include the quotients $(1 \pm \sqrt{-3})/2$. These quotients are units, since their product is 1. With these new units, the factorization above ceases to be a problem. This suggests that the ring $\mathbb{Z}[\sqrt{-3}]$ isn't big enough to be really interesting. However, we would like a ring in $\mathbb{Q}(\sqrt{-3})$ which can help us understand this field in the same way that \mathbb{Z} helps us understand \mathbb{Q} . In the field $\mathbb{Q}(\sqrt{-3})$, the ring $\mathbb{Z}[\sqrt{-3}]$ is not the right ring to look at.

Definition 9.1. Let $\omega = (-1 + \sqrt{-3})/2$. The *Eisenstein integers* are the ring $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$.

We have to check that the set $\{a + b\omega : a, b \in \mathbb{Z}\}$ really is a ring. The non-obvious part is closure under multiplication. This is fine once we observe that $\omega^2 = -\omega - 1$. Note also that ω is a cube root of 1. This is one reason why the Eisenstein integers are important.

In fact, $\mathbb{Z}[\omega]$ is a UFD. One can prove this using methods like those we used with $\mathbb{Z}[i]$. (In other words, we prove a division algorithm, and then use this to show that the ring is a PID and hence a UFD.) This might lead one to expect that given any ring $\mathbb{Z}[\sqrt{n}]$, we can add in some additional elements to get unique factorization into primes, and that it can be proved by proving the division algorithm. However, this is not the case. It is true that adding enough extra elements does eventually bring us to a ring with unique factorization (e.g., the whole field $\mathbb{Q}(\sqrt{n})$), but this isn't what we want at all!

Some rings, such as $\mathbb{Z}[\sqrt{-5}]$, are even worse than $\mathbb{Z}[\sqrt{-3}]$. In $\mathbb{Z}[\sqrt{-5}]$, examples such as

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

show that factorization into irreducibles is not unique. One might hope to enlarge the ring to something like $\mathbb{Z}[(1 + \sqrt{-5})/2]$. However, that leads into awful complications. Unlike $\mathbb{Z}[i]$, there's no reasonable basis. For example, $\mathbb{Z}[i]$ has the basis $1, i$. This is called an integral basis, because every element of $\mathbb{Z}[i]$ can be expressed as a linear combination of 1 and i with integer coefficients. However, $\mathbb{Z}[(1 + \sqrt{-5})/2]$ has no integral basis. One could try $1, (1 + \sqrt{-5})/2$, but this fails because $((1 + \sqrt{-5})/2)^2 = -3/2 + (1 + \sqrt{-5})/2$, and $-3/2$ is not an integer.

In fact, we will see later that no matter how one extends $\mathbb{Z}[\sqrt{-5}]$ (within $\mathbb{Q}(\sqrt{-5})$), it no longer has an integral basis. Because of this, extending the ring by adding additional elements is not a reasonable way to proceed.

Even when the ring is a UFD, one can't necessarily prove it by first proving a division algorithm. For example, in $\mathbb{Q}(\sqrt{-19})$, the appropriate ring to look at is $\mathbb{Z}[(1 + \sqrt{-19})/2]$. This ring is a UFD, but it has no division algorithm. If one tries to imitate the proof of the division algorithm in $\mathbb{Z}[i]$, one finds that the remainder doesn't end up being small enough. In fact, one can prove that there can be no division algorithm, even though factorization is unique.

These examples show that the question of whether factorizations are unique can be quite subtle. It might seem that dealing with fields such as $\mathbb{Q}(2^{1/3})$ would be hopelessly difficult. However, we will see that there is a beautiful way to salvage unique factorization when it fails, and prove it when it doesn't fail. Instead of factoring numbers, we will factor ideals. In certain rings, even when the elements themselves don't factor uniquely, the ideals will. Non-principal ideals will provide additional factors to make everything work out.

10. PROBLEMS

- (2) 1. Prove the division algorithm in $\mathbb{Z}[\sqrt{-2}]$, and conclude that it is a UFD.
- (2) 2. Prove that an odd prime p can be written as $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ iff -2 is a square modulo p .
- (1) 3. Let p be an odd prime. Show that if p can be written in the form $x^2 + 5y^2$ with $x, y \in \mathbb{Z}$, then -5 is a square modulo p . Show that the converse is false.
- (2.5) 4. Investigate the arithmetic of $\mathbb{Z}[\sqrt{-5}]$. To what extent, and how, do the results we proved for $\mathbb{Z}[i]$ break down?
- (1.5) 5. Show that $\mathbb{Z}[(1 + \sqrt{-5})/2]$ contains $1/2^n$ for each n , and conclude that it has no integral basis.
- (3.5) 6. Does $\mathbb{Z}[2^{1/3}]$ have a division algorithm?

11. QUADRATIC RECIPROCITY

We have seen that an odd prime p is a sum of two squares iff -1 is a square modulo p , and is of the form $x^2 + 2y^2$ iff -2 is a square modulo p . Examples such as these, as well as other considerations, make it very interesting to know when an integer n is a square modulo p . It is easy to show that the product of two numbers is a square iff either both are squares, or neither are. Because of this, we see that it is enough to know which primes reduce to squares modulo p . That is taken care of by the famous Law of Quadratic Reciprocity:

Theorem 11.1 (Law of Quadratic Reciprocity). *Let p and q be distinct, positive, odd primes. If either is 1 modulo 4, then p is a square modulo q iff q is a square modulo p . If both are 3 modulo 4, then p is a square modulo q iff q is not a square modulo p . Furthermore, 2 is a square modulo p iff $p \equiv \pm 1 \pmod{8}$ and -1 is a square modulo p iff $p \equiv 1 \pmod{4}$.*

We will prove this theorem later in the course. It is one of the most amazing theorems in mathematics: who could imagine that whether p is a square modulo q has anything to do with whether q is a square modulo p ?

As an application of Quadratic Reciprocity, consider the question of when 3 is a square modulo p . We see that if $p \equiv 1 \pmod{4}$, then 3 is a square modulo p iff p is a square modulo 3, i.e., iff $p \equiv 1 \pmod{3}$. For $p \equiv 3 \pmod{4}$, $p \neq 3$, we see that 3 is a square modulo p iff p is not a square modulo 3, i.e., iff $p \equiv 2 \pmod{3}$. Combining these, we see that for primes $p > 3$, 3 is a square modulo p iff $p \equiv \pm 1 \pmod{12}$.

12. ALGEBRAIC INTEGERS

Definition 12.1. A *number field* is a finite extension of \mathbb{Q} .

We normally consider number fields to be embedded in \mathbb{C} . (Sometimes this is mildly inconvenient. However, it is often convenient. For example, then one embedding of it into \mathbb{C} is the identity map, so each element is one of its own conjugates.)

Given a number field K , we would like to have a ring $\mathcal{O}_K \subset K$ that stands in the same relation to K as \mathbb{Z} does to \mathbb{Q} . We call \mathcal{O}_K the *ring of integers* in K . (This is the reason for the term “rational integers” for ordinary integers.) If $K = \mathbb{Q}(i)$, then \mathcal{O}_K should be $\mathbb{Z}[i]$. However, we have seen that things can be more complicated. If $K = \mathbb{Q}(\sqrt{-3})$, then \mathcal{O}_K should be $\mathbb{Z}[\omega]$, where ω is a complex cube root of 1.

There are several properties which \mathcal{O}_K should have. First, K should be the field of fractions of \mathcal{O}_K . In other words, every element of K should be the ratio of two elements of \mathcal{O}_K .

Second, \mathcal{O}_K should have an integral basis, which is defined as follows:

Definition 12.2. An *integral basis* for a ring R consists of elements $\omega_1, \dots, \omega_n \in R$ such that each $\alpha \in R$ can be written uniquely in the form $\alpha = a_1\omega_1 + \dots + a_n\omega_n$, with $a_1, \dots, a_n \in \mathbb{Z}$.

It follows immediately that a ring has an integral basis iff its additive group is a free abelian group on finitely many generators.

Finally, \mathcal{O}_K should have unique factorization, if that is possible. (In many cases, such as $K = \mathbb{Q}(\sqrt{-5})$, it is not possible.)

To construct such a ring \mathcal{O}_K , we need the notion of an algebraic integer. Once we have defined algebraic integers, we will show that of all the rings contained in K , only the ring of algebraic integers can have all the properties we would like (i.e., the quotient field is K , there is an integral basis, and unique factorization holds). Of those three properties, the only one that ever fails is unique factorization.

Definition 12.3. A number is an *algebraic integer* if it is the root of a monic polynomial with coefficients in \mathbb{Z} .

For example, $(-1 + \sqrt{-3})/2$ is an algebraic integer, since it is a root of $x^2 + x + 1 = 0$. However, $(1 + \sqrt{-5})/2$ is not an algebraic integer. This will follow from Proposition 12.9, since the irreducible polynomial of $(1 + \sqrt{-5})/2$ is $x^2 - x + 3/2$.

Definition 12.4. Given a number field K , the *ring of integers* \mathcal{O}_K in K is defined to be the set of all algebraic integers in K .

Proposition 12.5. \mathcal{O}_K is a ring.

Proof. Suppose $\alpha, \beta \in \mathcal{O}_K$. Let $\alpha_1, \dots, \alpha_n$ be the roots of some monic polynomial over \mathbb{Z} satisfied by α , and let β_1, \dots, β_m be the roots of some monic polynomial over \mathbb{Z} satisfied by β . Then the polynomials

$$\prod_{i,j} (x - \alpha_i - \beta_j)$$

and

$$\prod_{i,j} (x - \alpha_i \beta_j)$$

are monic, and have integer coefficients. This follows by an argument identical to that given in the proof of Proposition 5.8.

Since these polynomials are monic polynomials over \mathbb{Z} with $\alpha + \beta$ and $\alpha\beta$ as roots, $\alpha + \beta$ and $\alpha\beta$ are both algebraic integers. \square

Proposition 12.6. *Suppose R is a subring of a number field K , and that R has an integral basis. Then $R \subset \mathcal{O}_K$.*

In fact, we can prove the same results with a weaker hypotheses. We do not really need to require that the integral basis be linearly independent. It is enough for it to span R .

Proposition 12.7. *Suppose R is a subring of a number field K , and that for some n , R contains elements $\omega_1, \dots, \omega_n$ such that for all $x \in R$, there exist $a_1, \dots, a_n \in \mathbb{Z}$ such that $x = a_1\omega_1 + \dots + a_n\omega_n$. Then $R \subset \mathcal{O}_K$.*

Proof. Let $x \in R$. For each i , there exist a_{1i}, \dots, a_{ni} such that $x\omega_i = a_{1i}\omega_1 + \dots + a_{ni}\omega_n$. Consider the following simultaneous equations in the variables y_1, \dots, y_n :

$$\begin{aligned} (a_{11} - x)y_1 + a_{21}y_2 + \dots + a_{n1}y_n &= 0 \\ a_{12}y_1 + (a_{22} - x)y_2 + \dots + a_{n2}y_n &= 0 \\ &\vdots \\ a_{1n}y_1 + a_{2n}y_2 + \dots + (a_{nn} - x)y_n &= 0 \end{aligned}$$

These equations have a non-zero solution, namely $y_i = \omega_i$. Hence, the determinant of the matrix of coefficients must be zero. Expanding this determinant out gives a monic polynomial with integer coefficients satisfied by x . \square

In fact, it isn't surprising that we can prove results like Proposition 12.7, because its hypotheses imply that R has an integral basis. To see this, we apply the following theorem:

Theorem 12.8. *Every torsion-free, finitely-generated abelian group is a free abelian group on finitely many generators. Every subgroup of a finitely generated free abelian group is a finitely generated free abelian group itself.*

A proof of this theorem can be found in Artin's book. One can sometimes use ad hoc arguments to avoid citing this theorem, but we won't bother.

Note that the hypotheses of Proposition 12.7 essentially say that the additive group of R is generated by finitely many elements $\omega_1, \dots, \omega_n$. The additive group is clearly torsion-free (since that just means it has no elements of finite order), so we see that it is a free abelian group on finitely many generators. Hence, R has an integral basis.

Proposition 12.9. *A algebraic number is an algebraic integer if and only if its minimal polynomial has integer coefficients.*

We have already found this theorem useful in showing that $\frac{1+\sqrt{-5}}{2}$ isn't an algebraic integer.

Proof. What we need to prove is that if α is an algebraic integer, then the minimal polynomial of α has integer coefficients. Consider the ring $\mathbb{Z}[\alpha]$.

Regardless of what α is, the additive group of this ring is generated by $1, \alpha, \alpha^2, \dots$. Suppose α satisfies a monic polynomial of degree n with integer coefficients. Let us write this polynomial as $x^n + q(x)$ where $q \in \mathbb{Z}[x]$ and has degree at most $n - 1$. Then for $k \geq n$, we can use the polynomial to write α^k as an

integer linear combination of lower powers of α . For example, $\alpha^n = -q(\alpha)$ and the general case follows by induction.

We see, then, that $1, \alpha, \dots, \alpha^{n-1}$ generate the additive group of $\mathbb{Z}[\alpha]$. Since it is finitely-generated, and is obviously torsion-free, it has an integral basis, say of m elements.

That integral basis is also a basis of $\mathbb{Q}(\alpha)/\mathbb{Q}$, so the degree of α must be the same as the size of the integral basis, (i.e., $m = n$). The proof of Proposition 12.7 shows that α satisfies a monic polynomial over \mathbb{Z} of degree n . Since this polynomial has the same degree as the minimal polynomial of α , they must be the same. Thus, the minimal polynomial of α has integer coefficients. \square

Proposition 12.10. *For a number field K , K is the field of fractions of \mathcal{O}_K . Moreover, given any $\alpha \in K$, there exists $d \in \mathbb{Z}$ such that $d\alpha \in \mathcal{O}_K$.*

Proof. Since $\alpha \in K$, α satisfies a polynomial equation

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0,$$

with $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$. Choose d to be divisible by the denominators of a_0, a_1, \dots, a_{n-1} . Then $d\alpha$ satisfies the equation

$$x^n + da_{n-1}x^{n-1} + \dots + d^{n-1}a_1x + d^n a_0 = 0,$$

which has integer coefficients. \square

Lemma 12.11. *If $\omega_1, \dots, \omega_n$ are a basis of K/\mathbb{Q} , and $\sigma_1, \dots, \sigma_n$ are the embeddings of K into \mathbb{C} , then square of the determinant of the matrix M with $M_{ij} = \sigma_i(\omega_j)$ is a non-zero rational number.*

Proof. One can change from any basis to any other via a matrix with rational entries. This changes $\det(M)^2$ by a factor of the square of the determinant of that change of basis matrix. Thus, we need only prove that $\det(M)^2 \in \mathbb{Q}$ for one basis, and it will follow for all the others.

Let $K = \mathbb{Q}(\theta)$ (again, this follows from Corollary 4.9). We choose the basis $1, \theta, \dots, \theta^{n-1}$. Then $\det(M)$ is a Vandermonde determinant, and $\det(M)^2$ is therefore the discriminant of the minimal polynomial of θ . As we saw in the section on symmetric polynomials, this is rational. Furthermore, by Proposition 5.4, all of the roots are distinct and the discriminant is non-zero. \square

Proposition 12.12. *For a number field K , \mathcal{O}_K has an integral basis.*

Proof. Let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into \mathbb{C} . Consider a basis $\omega_1, \dots, \omega_n$ of K/\mathbb{Q} such that each ω_i is an algebraic integer. (We can do this simply by taking any basis and multiplying each element of it by a suitable rational integer.) We will show that there is a $d \in \mathbb{Z}$ such that every element of \mathcal{O}_K is an integer linear combination of $\omega_1/d, \dots, \omega_n/d$. Then the additive group of \mathcal{O}_K is a subgroup of a free abelian group on $\omega_1/d, \dots, \omega_n/d$, and is hence finitely generated, so \mathcal{O}_K has an integral basis.

Suppose $\alpha \in \mathcal{O}_K$. We know that α can be expressed uniquely as $a_1\omega_1 + \dots + a_n\omega_n$ with $a_1, \dots, a_n \in \mathbb{Q}$. These a_1, \dots, a_n are determined by being the solutions of the following simultaneous linear equations:

$$\begin{aligned} a_1\sigma_1(\omega_1) + \dots + a_n\sigma_1(\omega_n) &= \sigma_1(\alpha) \\ &\vdots \\ a_1\sigma_n(\omega_1) + \dots + a_n\sigma_n(\omega_n) &= \sigma_n(\alpha) \end{aligned}$$

Note that the determinant of the coefficient matrix $(\sigma_i(\omega_j))$ is non-zero by Lemma 12.11. Thus, the a_i exist and are unique.

Let d be the square of the determinant of the coefficient matrix of these equations. We use Cramer's Rule to solve the simultaneous equations. This gives the solutions a_i as the ratio of two determinants. If we multiply numerator and denominator by the denominator, then the denominator becomes d , and the numerator is the product of two determinants.

Because d is the square of the determinant of a matrix of algebraic integers, d is an algebraic integer. By Lemma 12.11, $d \in \mathbb{Q}$. Therefore, d is an integer (by Proposition 12.9). For essentially the same reason that d is an algebraic integer, the numerators of the fractions giving a_i are also algebraic integers. Because a_i and d are rational, the numerators must be rational as well, so they are also ordinary integers.

Therefore, we have proved that each a_i is an integer divided by a fixed integer d . Therefore, every element of \mathcal{O}_K is an integer linear combination of $\omega_1/d, \dots, \omega_n/d$. As we saw above, this implies that \mathcal{O}_K has an integral basis. \square

Note that the proof of Proposition 12.12 lets us find an integral basis for \mathcal{O}_K (and thereby find \mathcal{O}_K itself) with only a finite amount of computation. There are ways to do the computation slightly more efficiently, but we won't go into that here.

Proposition 12.13. *Suppose K is a number field, and R is a subring of K such that K is the field of fractions of R . If R has unique factorization, then $\mathcal{O}_K \subset R$.*

Proof. Let $\alpha \in \mathcal{O}_K$. Since K is the field of fractions of R , $\alpha = p/q$ for some $p, q \in R$. Since R has unique factorization, we choose p and q to be relatively prime.

Because α is an algebraic integer, it satisfies a monic polynomial equation

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

with $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$. Therefore,

$$p^n + a_{n-1}p^{n-1}q + \dots + a_1pq^{n-1} + a_0q^n = 0.$$

It follows that q divides p^n . Now we use the fact that R has unique factorization. Since q is relatively prime to p , it is relatively prime to p^n . The only way it can divide p^n is if q is a unit. Then since $\alpha = p/q$ and q is a unit, we have $\alpha \in R$. Thus, $\mathcal{O}_K \subset R$. \square

Therefore, the only subring of a number field K that can possibly have our three properties is \mathcal{O}_K . It always has the first two, but usually it is not a UFD. When we discuss ideal factorization, we will deal with that problem.

We now show that in the case of quadratic number fields, the ring of integers is what we expect.

Proposition 12.14. *Let d be a square-free integer. Then the ring of integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ unless $d \equiv 1 \pmod{4}$, in which case it is $\mathbb{Z}[(1 + \sqrt{d})/2]$.*

Proof. Because d is square-free, $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}$. The only algebraic integers in \mathbb{Q} are the integers, so we find the rest of the integers in $\mathbb{Q}(\sqrt{d})$ if we restrict our attention to an arbitrary element $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, with $a, b \in \mathbb{Q}$ and $b \neq 0$. It is a root of the irreducible polynomial

$$x^2 - 2ax + (a^2 - db^2).$$

Thus, it is an algebraic integer iff $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$.

From this, we see that $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, so $d(2b)^2 \in \mathbb{Z}$. Since d is square-free, we then have $(2b)^2 \in \mathbb{Z}$, which implies $2b \in \mathbb{Z}$. Now let $a = a'/2$ and $b = b'/2$. We must have $a', b' \in \mathbb{Z}$. The number α is an algebraic integer iff $(a')^2 - d(b')^2$ is divisible by 4. When $d \not\equiv 1 \pmod{4}$, this is true iff a' and b' are even. When $d \equiv 1 \pmod{4}$, it is true iff a' and b' have the same parity. This is equivalent what we were trying to prove. \square

Note that $\mathbb{Z}[(1 + \sqrt{d})/2]$ is the same as $\mathbb{Z}[(\pm 1 \pm \sqrt{d})/2]$.

13. DETERMINING THE RING OF INTEGERS

Let K be a number field, and \mathcal{O}_K its ring of integers. As we have seen, \mathcal{O}_K can sometimes be larger than one might guess. For example, if $K = \mathbb{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{-3})/2]$, rather than $\mathbb{Z}[\sqrt{-3}]$. In this section, we will develop an algorithm for determining \mathcal{O}_K , and apply it to certain cyclotomic fields.

Suppose $\omega_1, \dots, \omega_n$ is a basis K/\mathbb{Q} , and $\sigma_1, \dots, \sigma_n$ are the embeddings of K into \mathbb{C} . Let M be the matrix whose i, j entry is $\sigma_i(\omega_j)$. Then the rational number $d = \det(M)^2$ is called the discriminant of the basis. Recall that in proving Proposition 12.12 we proved the following:

Proposition 13.1. *Suppose K is a number field, and $\omega_1, \dots, \omega_n$ is a basis of K/\mathbb{Q} such that each ω_i is an algebraic integer. Let d be the discriminant of the basis. Then every element of \mathcal{O}_K can be expressed in the form $(a_1\omega_1 + \dots + a_n\omega_n)/d$ with $a_1, \dots, a_n \in \mathbb{Z}$.*

Given a basis of K/\mathbb{Q} consisting of integers, we can therefore find all the algebraic integers with only a finite amount of computation. We simply need to find all the algebraic integers of the form $(a_1\omega_1 + \dots + a_n\omega_n)/d$ with $0 \leq a_i < d$.

For an example, consider the field $K = \mathbb{Q}(\zeta)$ with ζ a primitive p -th root of unity, for p an odd prime. We will show that $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

First, we show that the polynomial $x^{p-1} + x^{p-2} + \dots + x + 1$ (which has ζ as a root) is irreducible.

Proposition 13.2 (Eisenstein's Criterion). *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n such that $f(x) \equiv x^n \pmod{p}$ (i.e., the leading term is 1 modulo p and the other coefficients are 0 modulo p), and such that the constant term of $f(x)$ is not divisible by p^2 . Then $f(x)$ is irreducible.*

Proof. Suppose $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ non-constant. We have $x^n \equiv g(x)h(x) \pmod{p}$, so for some i and $c \not\equiv 0 \pmod{p}$, we have $g(x) \equiv cx^i \pmod{p}$ and $h(x) \equiv c^{-1}x^{n-i} \pmod{p}$. Since $g(x)$ and $h(x)$ are not constant, we cannot have $i = 0$ or $i = n$. Therefore, the constant terms of $g(x)$ and $h(x)$ are divisible by p . It follows that the constant term of $f(x) = g(x)h(x)$ is divisible by p^2 . This contradicts our hypotheses, so $f(x)$ must be irreducible. \square

If we set $x = y + 1$, then $x^{p-1} + \dots + x + 1 = ((y + 1)^p - 1)/y$. Now,

$$\frac{(y + 1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{k+1}y^k \dots + \binom{p}{p-1},$$

which satisfies the hypotheses of Eisenstein's Criterion. Since the change of variables doesn't affect irreducibility, we see that $x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible. Therefore $[K : \mathbb{Q}] = p - 1$, and the numbers $1, \zeta, \dots, \zeta^{p-2}$ form a basis for K/\mathbb{Q} . Note that this basis consists of algebraic integers. We will show that it is in fact an integral basis for \mathcal{O}_K .

Lemma 13.3. *Suppose a and b are not divisible by p . Then $(1 + \zeta^a)/(1 + \zeta^b)$ is a unit in \mathcal{O}_K .*

Proof. There exists a c such that $a \equiv bc \pmod{p}$. Then

$$\frac{1 + \zeta^a}{1 + \zeta^b} = \frac{1 + \zeta^{bc}}{1 + \zeta^b} = 1 + \zeta^b + \zeta^{2b} + \dots + \zeta^{b(c-1)} \in \mathcal{O}_K.$$

For the same reason, its reciprocal is also in \mathcal{O}_K , so it is a unit in \mathcal{O}_K . \square

Let $\lambda = 1 - \zeta$. Since

$$x^{p-1} + x^{p-2} + \dots + x + 1 = \prod_{i=1}^{p-1} (x - \zeta^i),$$

we have $p = \prod_{i=1}^{p-1} (1 - \zeta^i)$. Applying Lemma 13.3, we see that p differs from λ^{p-1} by a unit factor.

Proposition 13.4. *The discriminant of the basis $1, \zeta, \dots, \zeta^{p-2}$ is $\pm p^{p-2}$.*

Proof. The discriminant d is given by the square of a Vandermonde determinant. That is, given the matrix

$$M = \begin{pmatrix} 1 & \zeta & \zeta^2 & \dots & \zeta^{p-1} \\ 1 & (\zeta^2) & (\zeta^2)^2 & \dots & (\zeta^2)^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \dots \\ 1 & (\zeta^{p-1}) & (\zeta^{p-1})^2 & \dots & (\zeta^{p-1})^{p-1} \end{pmatrix},$$

then $d = (\det(M))^2$. We have

$$d = \left(\prod_{i>j} (\zeta^i - \zeta^j) \right)^2.$$

In this product, we get a lot of units times $(p-1)(p-2)$ factors of λ . Therefore, d is a unit times p^{p-2} , since λ^{p-1} is a unit times p . Since $d \in \mathbb{Q}$ and $p^{p-2} \in \mathbb{Q}$, the unit factor must be in \mathbb{Q} . Since it is rational and an algebraic integer, it must be an integer. The only units in \mathbb{Z} are ± 1 , so $d = \pm p^{p-2}$. \square

(In fact, $d = (-1)^{p-1} p^{p-2}$. We will need that fact in later, but for now we will ignore the sign.)

Proposition 13.5. $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Proof. Suppose that $\mathcal{O}_K \neq \mathbb{Z}[\zeta]$. From Proposition 13.1, we see that there exist $a_0, \dots, a_{p-2} \in \mathbb{Z}$, not all divisible by p , such that $(a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2})/p \in \mathcal{O}_K$. (This is true since p is the only prime factor of the discriminant. If there were any other algebraic integers, multiplying by a power of p would produce one of this form.)

We now change from the basis $1, \zeta, \dots, \zeta^{p-2}$ to $1, \lambda, \dots, \lambda^{p-2}$. Then it is not hard to check that there are integers b_0, \dots, b_{p-2} , not all divisible by p , such that

$$a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2} = b_0 + b_1\lambda + \dots + b_{p-2}\lambda^{p-2}.$$

We will show that each b_i must be divisible by p , which will be a contradiction.

We begin with b_0 . In \mathcal{O}_K , p divides $b_0 + b_1\lambda + \dots + b_{p-2}\lambda^{p-2}$. Since λ divides p , we see that λ divides b_0 . If b_0 is not divisible by p , then there exist $a_1, a_2 \in \mathbb{Z}$ such that $b_0a_1 + pa_2 = 1$. Then since λ is a common factor of b_0 and p , we must have that λ divides 1. However, since p is a unit times λ^{p-1} , that would imply that p is a unit, which is a contradiction. Therefore, b_0 must be divisible by p .

Now we see that λ^{p-2} divides $b_1 + b_2\lambda + \dots + b_{p-2}\lambda^{p-3}$. From this, we can deduce as above that λ divides b_1 , and then that p divides b_1 . Continuing in this way, we see that p divides each b_i , which means that $(b_0 + b_1\lambda + \dots + b_{p-2}\lambda^{p-2})/p \in \mathbb{Z}[\zeta]$, and therefore we must have $\mathcal{O}_K = \mathbb{Z}[\zeta]$. \square

14. IDEAL FACTORS

We have seen that in some rings of integers, such as $\mathbb{Z}[\sqrt{-5}]$, factorization is not unique. We could try to enlarge the ring to make it unique, but if we do so while staying within the field $\mathbb{Q}(\sqrt{-5})$, we find that the enlarged ring never has an integral basis.

Instead, we introduce “ideal factors.” These new factors will not actually be elements of a ring, but they will restore unique factorization. They will correspond to ideals in the ring of integers.

To see how this will restore unique factorization, consider the two factorizations

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}]$. Define the ideals

$$\mathfrak{p} = (2, 1 + \sqrt{-5}),$$

$$\mathfrak{q} = (3, 1 + \sqrt{-5}),$$

and

$$\mathfrak{r} = (3, 1 - \sqrt{-5}).$$

The notation is meant to suggest that \mathfrak{p} is the gcd of 2 and $1 + \sqrt{-5}$. Of course, in the ring $\mathbb{Z}[\sqrt{-5}]$, 2 and $1 + \sqrt{-5}$ have no common factors. However, if we are going to reconcile the two factorizations of 6, then there should be such an element \mathfrak{p} .

The basic idea is this: 2 and $1 + \sqrt{-5}$ do not generate the unit ideal $(1) = \mathbb{Z}[\sqrt{-5}]$. If they did, then there would be two algebraic integers $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ such that $2\alpha + (1 + \sqrt{-5})\beta = 1$. Multiply both sides by $1 - \sqrt{-5}$ to obtain $2\alpha(1 - \sqrt{-5}) + 2(3\beta) = 1 - \sqrt{-5}$. This says that 2 divides $1 - \sqrt{-5}$. but we know that it doesn't. Because 2 and $1 + \sqrt{-5}$ do not generate the unit ideal, they ought to have some common factor. However, they do not have any non-trivial common factor in $\mathbb{Z}[\sqrt{-5}]$.

The ideal \mathfrak{p} is not a principal ideal (since if it were, it would be generated by a common factor of 2 and $1 + \sqrt{-5}$ and would therefore be the unit ideal). However, like all ideals, it behaves like the set of multiples of some number. We will think of \mathfrak{p} as defining an “ideal factor,” which doesn't correspond to any element of $\mathbb{Z}[\sqrt{-5}]$.

Recall the following definitions:

Definition 14.1. Let R be a ring, and I and J ideals in R . The *product* IJ is the ideal generated by all products ij with $i \in I$ and $j \in J$. A *prime ideal* P is an ideal other than R such that if $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$. A *maximal ideal* is an ideal $M \subset R$ such that $M \neq R$, but R is the only ideal properly containing M .

There are two useful facts which we should mention now, but whose proof we delay to a later section. First, any ideal different from the ring itself is contained in a maximal ideal. Second, maximal ideals are always prime.

From time to time, we might write “ideal” when we mean “non-zero ideal.” This is especially likely to happen when we are talking about prime ideals.

The following lemma is often useful. We omit the proof, since it is easy and probably well known.

Lemma 14.2. *An ideal $P \neq R$ in an arbitrary ring R is prime iff for all ideals A and B , $AB \subset P$ implies $A \subset P$ or $B \subset P$. Also, P is prime (or $P = R$) iff R/P is an integral domain.*

We will now show that \mathfrak{p} , \mathfrak{q} , and \mathfrak{r} are prime ideals. Note that the principal ideal generated by a number α is prime iff α is prime, so we think of this as saying that the “ideal elements” generating \mathfrak{p} , \mathfrak{q} , and \mathfrak{r} are prime.

To see this, we look at the quotients $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}$, $\mathbb{Z}[\sqrt{-5}]/\mathfrak{q}$, and $\mathbb{Z}[\sqrt{-5}]/\mathfrak{r}$. These are all very similar, so we will deal only with the first. For it, we have

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} = \left(\frac{\mathbb{Z}[\sqrt{-5}]}{(1 + \sqrt{-5})} \right) / (2) = \mathbb{Z}/(2),$$

which is a field (and therefore an integral domain). We can check in the same way that \mathfrak{q} and \mathfrak{r} are prime.

Now we will show that how these factors reconcile the two factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$. In general, when dealing with ideal factorizations, instead of looking at actual elements α of the ring of integers, we will look at the principal ideals (α) . To start off with, we will show that the principal ideal (2) factors as \mathfrak{p}^2 .

We have $\mathfrak{p}^2 = (2^2, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5})$. Since $2 = (2 + 2\sqrt{-5}) - (4 + (-4 + 2\sqrt{-5}))$, it follows that $2 \in \mathfrak{p}^2$, and we have $\mathfrak{p}^2 \subset (2)$, so $(2) = \mathfrak{p}^2$. In the same way, we can show that $(3) = \mathfrak{q}\mathfrak{r}$, $(1 + \sqrt{-5}) = \mathfrak{p}\mathfrak{q}$, and $(1 - \sqrt{-5}) = \mathfrak{p}\mathfrak{r}$. Thus, both factorizations of 6 can be refined to $\mathfrak{p}^2\mathfrak{q}\mathfrak{r}$. Of course, this doesn’t prove that 6 has only one factorization into prime ideals, but at least it looks encouraging.

15. UNIQUENESS

We will now prove unique factorization for ideals in rings of integers (except for one proposition which we will put off until section 16). We begin with the following very important result:

Proposition 15.1. *Let K be a number field, and let \mathcal{O}_K denote the ring of integers of K . Every non-zero ideal of \mathcal{O}_K divides a non-zero principal ideal.*

We will prove this in section 16. Part of the importance of this result is that it says that there are no unnecessary ideal factors. At first, this might seem obvious. However, it is false in most rings. For example, consider the ring $\mathbb{Z}[x]$, which is a UFD but not a PID. One non-principal ideal in $\mathbb{Z}[x]$ is $(2, x)$. This ideal does not divide any non-zero principal ideal. To see this, suppose that I is an ideal, and $(2, x)I$ is principal, say $(2, x)I = (f(x))$. For all $g(x) \in I$, we must have $f(x)|2g(x)$ and $f(x)|xg(x)$, so $f(x)|g(x)$, and hence $I \subset (f(x))$. We can then conclude that $(2, x)(f(x)) = (f(x))$, and therefore that $(2, x) = (1)$. However, $1 \notin (2, x)$, so this is impossible. Note that this last step depends on a cancellation law. In a general ring with arbitrary ideals $AC = BC$, we cannot cancel, but it isn’t hard to show that cancellation always holds when C is principal.

So we see that Proposition 15.1 isn’t completely obvious. It will be the key to almost all of our results in this section.

We begin with the following two results:

Proposition 15.2 (Cancellation Law). *Suppose A , B , and C are ideals of \mathcal{O}_K , with $C \neq 0$. If $AC = BC$, then $A = C$.*

Proof. Let C' be an ideal such that CC' is principal, say $CC' = (\alpha)$, with $\alpha \neq 0$. Then

$$(\alpha)A = (\alpha)B,$$

from which it follows easily (as noted above) that $A = B$. \square

Proposition 15.3 (“To Contain is to Divide”). *Suppose A and B are non-zero ideals of \mathcal{O}_K . Then A divides B iff A contains B .*

Proof. Clearly, if A divides B , then A contains B . Suppose $B \subset A$. Let A' be an ideal such that $AA' = (\alpha)$ with $\alpha \neq 0$. Then $BA' \subset (\alpha)$. Let $C = (BA')/\alpha$, (i.e., the set of all β such that $\alpha\beta \in BA'$). Then C is an ideal of \mathcal{O}_K . Also, because $BA' \subset (\alpha)$, it is easy to check that $C(\alpha) = BA'$. In other words, $CAA' = BA'$. By cancellation, we have $AC = B$, so A divides B . \square

Now we prove that all ideals in \mathcal{O}_K factor into primes. (This is not as obvious as it was in rings such as \mathbb{Z} , although it is not hard to prove.) First, we need the following lemma:

Lemma 15.4. *Let R be a ring, and I an ideal of R . Then ideals J_1 of R that contain I are in one-to-one correspondence with the ideals J_2 of R/I via $J_1 = \varphi^{-1}(J_2)$, where $\varphi : R \rightarrow R/I$ is the canonical map.*

Proof. The substance of this lemma is to check that φ^{-1} carries ideals of R/I to ideals of R containing I and that φ takes ideals of R containing I to ideals in R/I . We will leave the details here to the reader. After the two maps are shown to be well-defined, it follows immediately that the two maps are inverses and, thus, that each is bijective. \square

Because a field is the same as a ring without any proper ideals (every non-zero element has a reciprocal iff every non-zero principal ideal is the unit ideal), we deduce the following corollary:

Corollary 15.5. *An ideal I in a ring R is maximal iff R/I is a field.*

Note that because every field is an integral domain, it follows that every maximal ideal is prime.

Lemma 15.6. *Let I be a non-zero ideal of \mathcal{O}_K . Then $I \cap \mathbb{Z} \neq (0)$.*

Proof. Let $\alpha \in I$ and $\alpha \neq 0$. Since α is an algebraic integer, it satisfies a polynomial equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

with $a_i \in \mathbb{Z}$. We can take $a_0 \neq 0$. Because $a_0 \in (\alpha) \subset I$, we have $I \cap \mathbb{Z} \neq (0)$. \square

Proposition 15.7. *Let I be a non-zero ideal of \mathcal{O}_K . Then \mathcal{O}_K/I is finite.*

Proof. Let $a > 0$ be in $\mathbb{Z} \cap I$. Since $(a) \subset I$, $\mathcal{O}_K/(a)$ maps surjectively onto \mathcal{O}_K/I . If $\omega_1, \dots, \omega_n$ form an integral basis for \mathcal{O}_K , then we see that every element of $\mathcal{O}_K/(a)$ can be represented by a unique element

$$a_1\omega_1 + \cdots + a_n\omega_n$$

with $0 \leq a_i < a$ for each i . Therefore, $\mathcal{O}_K/(a)$ has a^n elements, and \mathcal{O}_K/I has at most a^n elements, and is therefore finite. \square

Proposition 15.8. *Every non-zero ideal of \mathcal{O}_K factors into prime ideals.*

Proof. Let I be an ideal of \mathcal{O}_K . Combining Lemmas 15.4 and 15.7 shows that only finitely many ideals of \mathcal{O}_K contain I . Therefore, I has only finitely many factors.

Now let P_1 be a maximal ideal containing I . Then P_1 divides I , and $I = P_1I_1$ for some ideal I_1 . We can continue in this way. Since I has only finitely many factors, this process must eventually halt. This gives a factorization of I into prime ideals (since maximal ideals are prime). \square

Lemma 15.9. *Every finite integral domain is a field.*

Proof. Suppose $x \neq 0$ is an element of a finite integral domain. Since there are infinitely many powers of x , we must have $x^i = x^j$ for some $i > j$. Because we are working in an integral domain, that implies that $x^{(i-j)} = 1$. Therefore, x is invertible. Since every non-zero element of the integral domain is invertible, it is a field. \square

Proposition 15.10. *Every non-zero prime ideal of \mathcal{O}_K is maximal.*

Proof. Suppose P is a non-zero prime ideal of \mathcal{O}_K . Then \mathcal{O}_K/P is finite, by Proposition 15.7. Since P is prime, \mathcal{O}_K/P is an integral domain. Therefore, it is a field, so P is maximal (by Corollary 15.5). \square

From this, we see that the only divisibility relations among non-zero prime ideals are merely equality. That is, if A, B are non-zero primes and A divides B , then A must contain B . But B is maximal and $A \neq \mathcal{O}_K$, so $A = B$.

Theorem 15.11. *Let K be a number field, and \mathcal{O}_K its ring of integers. In \mathcal{O}_K , factorization of ideals into prime ideals is unique.*

Proof. We have seen that every ideal factors into prime ideals. Suppose we had two different prime factorizations

$$(15.1) \quad P_1 P_2 \cdots P_r = Q_1 Q_2 \cdots Q_s.$$

For any ideals A and B and prime ideal P , if $AB \subset P$ then $A \subset P$ or $B \subset P$ by Proposition 14.2. It follows that if P divides a product, then it divides one factor. Since P_1 divides the right side of (15.1), P_1 divides Q_i for some i . Then P_1 contains Q_i . Since Q_i is maximal, we must have $P_1 = Q_i$. Now we can cancel these factors from both sides. Continuing in this way, we see that prime factorizations of ideals are unique. \square

16. THE IDEAL CLASS GROUP

We will now complete the proof that ideals factor uniquely into prime ideals, and at the same time prove that something called the ideal class group is finite. Let K be a number field, and \mathcal{O}_K its ring of integers.

Definition 16.1. Two ideals A and B of \mathcal{O}_K are called *equivalent* if there exist non-zero $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A = (\beta)B$. We then write $A \sim B$. The set of equivalence classes of non-zero ideals is called the *ideal class group* of K . Its order h is called the *class number* of K .

We will prove that the set of ideal classes forms a group under the operation induced by multiplication of ideals, and that the class number is always finite. Note that the class of a non-zero principal ideal will be the identity element in the ideal class group. To show that the ideal class group really is a group, we just need to prove the following proposition, whose proof was omitted in section 15:

Proposition 16.2. *Every non-zero ideal of \mathcal{O}_K divides a non-zero principal ideal.*

If A, B are ideals such that AB is principal, then the class of B is the inverse of the class of A in the ideal class group of K . Therefore, Proposition 16.2 says that every ideal class has an inverse.

We will deduce Proposition 16.2 from the fact that the ideal class group is finite. Along the way, we will need to use a special case of the Cancellation Law. Because we used Proposition 16.2 to prove the general form of the cancellation law, we need to give another proof for the special case. (There are other ways to prove Proposition 16.2. However, the following approach is nice because it proves at the same time that the class number is finite, which is an important result.)

Proposition 16.3. *Suppose $\alpha \in K$, and multiplication by α maps a finitely-generated subgroup of the additive group of K to itself. Then $\alpha \in \mathcal{O}_K$.*

The proof of this statement is essentially the same as the proof of Proposition 12.7. Note that the subgroup is free (since it is torsion free), and therefore has a basis. If we multiply each basis element by α and express the result in terms of the basis, then we get simultaneous linear equations satisfied by the basis elements (whose coefficients are integers minus α on the diagonal and integers elsewhere). The determinant of the coefficients must be 0, and this gives a monic polynomial over \mathbb{Z} satisfied by α .

Note that ideals are subgroups of \mathcal{O}_K , and therefore finitely-generated subgroups of K . We will usually apply Proposition 16.3 to ideals.

Lemma 16.4. *If A and B are ideals such that $A = AB$, and $A \neq (0)$, then $B = \mathcal{O}_K$.*

Proof. Let $\alpha_1, \dots, \alpha_n$ be an integral basis for A . Since $A = AB$, there exist elements $b_{ij} \in B$ such that for each i , $\alpha_i = \sum_j b_{ij} \alpha_j$. This gives us a set of simultaneous linear equations satisfied by the α_i . The determinant of the matrix of coefficients must be 0. That is the determinant of the matrix whose i, j entry is $b_{ij} - \delta_{ij}$. Expanding this determinant gives 1 plus many products of elements of B . Since the total is 0, we see that 1 must be in B , so $B = \mathcal{O}_K$. \square

Proposition 16.5 (Weak Cancellation Law). *Let A and B be ideals of \mathcal{O}_K , and $\omega \in \mathcal{O}_K$. If $A \neq 0$ and $A(\omega) = AB$, then $(\omega) = B$.*

Proof. Let $\beta \in B$. Then β/ω maps A into itself, so by Proposition 16.3, $\beta/\omega \in \mathcal{O}_K$. Therefore, $B \subset (\omega)$. It follows that B/ω is an ideal of \mathcal{O}_K . We have $A(B/\omega) = A$. By Lemma 16.4, $B/\omega = \mathcal{O}_K$, so $B = (\omega)$, as desired. \square

Proposition 16.6. *There exists an $M > 0$ (depending only on K) such that given $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$, there exists an integer t with $1 \leq t \leq M$ and an algebraic integer $\omega \in \mathcal{O}_K$ such that $|\text{nm}(t\alpha - \omega\beta)| < |\text{nm}(\beta)|$.*

We will prove the following equivalent form. There exists $M > 0$ such that for all $\alpha \in K$, there exists an integer t such that $1 \leq t \leq M$ and an algebraic integer $\omega \in \mathcal{O}_K$ such that $|\text{nm}(t\alpha - \omega)| < 1$.

To see that Proposition 16.6 is implied by the latter statement, apply the last paragraph to $\alpha' = \alpha/\beta$. Then the conclusion implies that there is an integer t and an algebraic integer $\omega \in \mathcal{O}_K$ such that $1 \leq t \leq M$ and $|\text{nm}(t\alpha' - \omega)| < 1$. Multiply through by $|\text{nm}(\beta)|$ to obtain the conclusion of Proposition 16.6.

Proof. Let $\omega_1, \dots, \omega_n$ be an integral basis for \mathcal{O}_K . They then form a basis of K/\mathbb{Q} (since every element of K is an algebraic integer divided by a rational integer). Let $\gamma \in K$. Then there are $a_i \in \mathbb{Q}$ such that $\gamma = a_1\omega_1 + \dots + a_n\omega_n$.

If $\sigma_1, \dots, \sigma_n$ are the embeddings of K into \mathbb{C} , then

$$\text{nm}(\gamma) = \prod_j (a_1\sigma_j(\omega_1) + \dots + a_n\sigma_j(\omega_n)).$$

We therefore have

$$(16.1) \quad |\text{nm}(\gamma)| = \prod_j |a_1\sigma_j(\omega_1) + \dots + a_n\sigma_j(\omega_n)| \leq C(\max_i |a_i|)^n,$$

where $C = (n \max_{i,j} |\sigma_j(\omega_i)|)^n$. Let m be an integer greater than $n \max_{i,j} |\sigma_j(\omega_i)|$, and let $M = m^n$.

Consider the multiples $\alpha, 2\alpha, \dots, (M+1)\alpha$. By the pigeon-hole principle, two of these, say $i\alpha$ and $j\alpha$ with $i > j$, must have coordinates (when expressed in terms of the basis) such that the fractional parts of corresponding coordinates in $i\alpha$ and $j\alpha$ differ by at most $1/m$. Let $t = i - j$. Then $1 \leq t \leq M$, and there exists an algebraic integer ω such that $t\alpha - \omega$ has all coordinates from $-1/m$ to $1/m$. By (16.1), we have $|\text{nm}(t\alpha - \omega)| \leq C/M < 1$, as desired. \square

Note that Proposition 16.6 is similar to (but weaker than) the division algorithm. It is not strong enough to prove that every ideal is principal, but if used properly it is strong enough to prove that there are only finitely many ideal classes.

Lemma 16.7. *Let A be an ideal of \mathcal{O}_K , and $\beta \in \mathcal{O}_K$. If $A \subset (\beta)$, then there exists an ideal B such that $A = (\beta)B$.*

Of course, this is a special case of the proposition that to contain is to divide. However, we will give a proof of this that is independent of Proposition 16.2, so that we can use it to help in the proof of Proposition 16.2.

Proof. We assume $\beta \neq 0$. (Otherwise, the result is trivial.) Let $B = A/\beta$ (i.e., the set of all elements α/β with $\alpha \in A$). Since $A \subset (\beta)$, $B \subset \mathcal{O}_K$. Since A is an ideal, so is B . Now $B(\beta) = A$, as desired. \square

Theorem 16.8. *The class number h is finite.*

Proof. Let M be as in Proposition 16.6. We will show that every non-zero ideal is equivalent to an ideal that contains $M!$. Only finitely many ideals contain any given non-zero number (since only finitely many contain the principal ideal generated by it). This will prove that there are only finitely many ideal classes.

Let A be any non-zero ideal of \mathcal{O}_K . Choose $\beta \in A$ ($\beta \neq 0$) such that $|\text{nm}(\beta)|$ is minimal. (Since the norm of each non-zero element is a non-zero integer, this can be done.) By Proposition 16.6, for all $\alpha \in A$, there exists an integer t such that $1 \leq t \leq M$ and an algebraic integer ω such that $|\text{nm}(t\alpha - \beta\omega)| < |\text{nm}(\beta)|$. Since $t\alpha - \beta\omega \in A$, we have $t\alpha = \beta\omega$ (since $|\text{nm}(\beta)|$ is minimal). Therefore, $(M!)A \subset (\beta)$.

By Lemma 16.7, there exists an ideal B such that $(M!)A = (\beta)B$. Since $\beta \in A$, we have $(M!)\beta \in (\beta)B$, so B contains $M!$. Because $A \sim B$, we see that A is equivalent to an ideal containing $M!$. As noted above, this proves that there are only finitely many ideal classes. \square

Proposition 16.9. *Let A be any non-zero ideal of \mathcal{O}_K . Then for some k such that $1 \leq k \leq h$, A^k is principal.*

Proof. Since there are only finitely many ideal classes, two powers of A must be in the same ideal class. Suppose $A^i \sim A^j$ with $i > j$. We will show that A^{i-j} is principal.

There exist non-zero $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)A^i = (\beta)A^j$, so $(\alpha)A^j A^{i-j} = (\beta)A^j$. Multiplication of β/α maps A^j into itself, so by Proposition 16.3, $\beta/\alpha \in \mathcal{O}_K$. Let $\omega = \beta/\alpha$. Then $A^j A^{i-j} = A^j(\omega)$, so by the Weak Cancellation Law $A^{i-j} = (\omega)$, which is principal. \square

Proposition 16.2 follows immediately from this. That completes the proof that ideals factor uniquely into prime ideals.

17. FACTORIZATION OF RATIONAL PRIMES

Suppose we have a rational prime p . We have seen (in the section on the Gaussian integers) that how p factors in an extension of \mathbb{Q} can be of interest. In general, we make the following definitions.

Definition 17.1. Suppose $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are distinct prime ideals of \mathcal{O}_K . The ramification index of \mathfrak{P}_i is e_i . We say that p ramifies in K if some ramification index is greater than 1. The residue field of \mathfrak{P}_i is $\mathcal{O}_K/\mathfrak{P}_i$ (which is a field since non-zero prime ideals of \mathcal{O}_K are maximal). Since it is a finite field of characteristic p , it has order p^{f_i} for some f_i . We call f_i the residue field degree of \mathfrak{P}_i .

Every non-zero ideal of \mathcal{O}_K contains a non-zero rational integer, so every ideal divides a rational integer. Hence, every prime of \mathcal{O}_K divides a rational prime. If p and q are distinct rational primes, then $(p) + (q) = \mathbb{Z}$, and hence $(p)\mathcal{O}_K + (q)\mathcal{O}_K = \mathcal{O}_K$, so no prime of \mathcal{O}_K divides both p and q .

Suppose that $[K : \mathbb{Q}] = n$, and p is a rational prime, such that in K , $p = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ such that each \mathfrak{P}_i has degree f_i . We will prove that $\sum_i e_i f_i = n$. To do this, we will need to Chinese Remainder Theorem (which we will not prove here), and a lemma.

Proposition 17.2 (Chinese Remainder Theorem). *Let R be any ring, and A_1, \dots, A_n ideals of R such that for $i \neq j$, $A_i + A_j = R$. Then*

$$R/(A_1 \cdots A_n) \approx R/A_1 \oplus \cdots \oplus R/A_n.$$

Lemma 17.3. *Let \mathfrak{P}_1 and \mathfrak{P}_2 be distinct prime ideals of \mathcal{O}_K . For any positive integers m and n , $\mathfrak{P}_1^m + \mathfrak{P}_2^n = (1)$.*

Proof. Let $A = \mathfrak{P}_1^m + \mathfrak{P}_2^n$. Since A contains \mathfrak{P}_1^m , it divides \mathfrak{P}_1^m . Similarly, A divides \mathfrak{P}_2^n . By uniqueness of ideal factorization, A must be the unit ideal. \square

Lemma 17.4. *Suppose \mathfrak{P} is a prime in \mathcal{O}_K , and $\mathcal{O}_K/\mathfrak{P}$ has p^f elements. Then $\mathcal{O}_K/\mathfrak{P}^e$ has p^{ef} elements.*

Proof. We prove this by induction. First, note that $\mathfrak{P}^{e-1}/\mathfrak{P}^e$ has p^f elements. (This is not hard to check.) Now we use the fact that

$$\mathcal{O}_K/\mathfrak{P}^{e-1} = (\mathcal{O}_K/\mathfrak{P}^e)/(\mathfrak{P}^{e-1}/\mathfrak{P}^e).$$

This shows that if $\mathcal{O}_K/\mathfrak{P}^{e-1}$ has $p^{(e-1)f}$ elements, then $\mathcal{O}_K/\mathfrak{P}^e$ has p^{ef} elements. This completes the proof. \square

Proposition 17.5. *If e_i and f_i are the ramification indices and residue field degrees of the primes dividing a rational prime p in a degree n extension of \mathbb{Q} , then*

$$\sum_i e_i f_i = n.$$

Proof. Suppose $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, and \mathfrak{P}_i has degree f_i . Then $\mathcal{O}_K/(p)$ has order p^n , and by the Chinese Remainder Theorem (together with Lemma 17.4) also has order $p^{e_1 f_1 + \cdots + e_g f_g}$. (The Chinese Remainder Theorem applies because of Lemma 17.3.) Therefore, $n = e_1 f_1 + \cdots + e_g f_g$. \square

In general, we make the following definition:

Definition 17.6. The norm of an ideal A in \mathcal{O}_K is the order of \mathcal{O}_K/A .

One can show that if $A = (\alpha)$ with $\alpha \in \mathcal{O}_K$, then $\text{nm}(A) = |\text{nm}(\alpha)|$. Note that the methods used above prove the following result:

Proposition 17.7. For any ideals A and B , $\text{nm}(AB) = \text{nm}(A)\text{nm}(B)$.

18. FACTORIZATION OF RATIONAL PRIMES IN $\mathbb{Z}[\theta]$

We now look at how rational primes factor when the ring of integers is generated by a single element, i.e., there exists a $\theta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$. This is not usually the case. For example, in $\mathbb{Q}(175^{1/3})$, one can show that the ring of integers is $\mathbb{Z}[245^{1/3}, 175^{1/3}]$, and that it is not generated by a single element.

Suppose K is a number field, and $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let θ be a root of $f(x)$, with $f(x)$ a monic, irreducible polynomial over \mathbb{Z} .

Theorem 18.1. Let p be a rational prime. Suppose that $f_1(x), \dots, f_g(x)$ are polynomials over \mathbb{Z} such that modulo p , $f(x)$ factors as $f(x) \equiv f_1(x)^{e_1} \cdots f_g(x)^{e_g} \pmod{p}$, and when reduced modulo p , $f_1(x), \dots, f_g(x)$ are irreducible polynomials, such that none is a constant times any other.

For each i , let $\mathfrak{P}_i = (p, f_i(\theta))$. Then $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are distinct prime ideals, and

$$(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Proof. First, we prove that each \mathfrak{P}_i is prime. We have $\mathcal{O}_K/\mathfrak{P}_i = \mathbb{Z}[\theta]/\mathfrak{P}_i = (\mathbb{Z}/p\mathbb{Z})[\theta]/(f_i(\theta))$. Therefore, $\mathcal{O}_K/\mathfrak{P}_i = (\mathbb{Z}/p\mathbb{Z})[x]/(f_i(x), f_i(x))$. Since $f_i(x)$ is a factor of $f(x)$ modulo p , we have $\mathcal{O}_K/\mathfrak{P}_i = (\mathbb{Z}/p\mathbb{Z})[x]/(f_i(x))$. Since $f_i(x)$ is irreducible modulo p , this is a field, so \mathfrak{P}_i is a prime ideal.

Note that for $i \neq j$, we have $\mathfrak{P}_i \neq \mathfrak{P}_j$. This is true because the canonical map from \mathcal{O}_K to $\mathcal{O}_K/\mathfrak{P}_i$ takes θ to an element with minimal polynomial $f_i(x)$ over $\mathbb{Z}/p\mathbb{Z}$. Because modulo p , $f_i(x)$ is not a constant times $f_j(x)$, we cannot have $\mathfrak{P}_i = \mathfrak{P}_j$.

For any ideals A, B_1 , and B_2 , we have $(A + B_1)(A + B_2) \subset A + B_1B_2$. Since $\mathfrak{P}_i = (p) + (f_i(\theta))$, we have

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \subset (p) + (f_1(\theta)^{e_1} \cdots f_g(\theta)^{e_g}).$$

The product on the right vanishes modulo p , so we have $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \subset (p)$. Therefore, (p) divides $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$.

If we let f_i be the residue field degree of \mathfrak{P}_i , then the product $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ has norm $p^{e_1 f_1 + \cdots + e_g f_g}$. Since f_i is the degree of the reduction of $f_i(x)$ modulo p , and $f(x) \equiv f_1(x)^{e_1} \cdots f_g(x)^{e_g} \pmod{p}$, we see that $n = e_1 f_1 + \cdots + e_g f_g$, where n is the degree of $f(x)$. Because p has norm p^n , and (p) divides $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, we see that in the factorization of (p) , no \mathfrak{P}_i can occur with ramification index less than e_g . Therefore

$$(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

as desired. \square

19. GALOIS EXTENSIONS

Definition 19.1. An extension K/\mathbb{Q} of degree n is called a Galois extension if its n embeddings into \mathbb{C} all have the same image.

For example, $\mathbb{Q}(\sqrt{2})$ is a Galois extension of \mathbb{Q} . However, $\mathbb{Q}(2^{1/3})$ is not. One embedding takes $2^{1/3}$ to the real cube root of 2; this embeddings maps $\mathbb{Q}(2^{1/3})$ into \mathbb{R} . The other two embeddings do not.

If K/\mathbb{Q} is a Galois extension of degree n , then K has n automorphisms. We denote the group of automorphisms by $\text{Gal}(K/\mathbb{Q})$, and call it the Galois group. For $\sigma \in \text{Gal}(K/\mathbb{Q})$, we write α^σ for the value of σ at α .

If A is any ideal of \mathcal{O}_K and $\sigma \in \text{Gal}(K/\mathbb{Q})$, then A^σ is also an ideal of \mathcal{O}_K . If A is prime, then so is A^σ , since $\mathcal{O}_K/A^\sigma = \mathcal{O}_K^\sigma/A^\sigma \approx \mathcal{O}_K/A$.

Proposition 19.2. Let p be a rational prime, and K/\mathbb{Q} a Galois extension. Then $\text{Gal}(K/\mathbb{Q})$ acts transitively on the primes of \mathcal{O}_K dividing (p) . In other words, if \mathfrak{P}_1 and \mathfrak{P}_2 are primes dividing (p) , then there exists a $\sigma \in \text{Gal}(K/\mathbb{Q})$ such that $\mathfrak{P}_1^\sigma = \mathfrak{P}_2$.

Proof. Suppose there were a prime \mathfrak{P}_2 dividing (p) and not in $\{\mathfrak{P}_1^\sigma : \sigma \in \text{Gal}(K/\mathbb{Q})\}$. By the Chinese Remainder Theorem, we can find $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 0 \pmod{\mathfrak{P}_2}$ and $\alpha \equiv 1 \pmod{\mathfrak{P}_1^\sigma}$ for each $\sigma \in \text{Gal}(K/\mathbb{Q})$.

Now consider $\text{nm}(\alpha) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \alpha^\sigma$. We have $\text{nm}(\alpha) \in \mathbb{Z} \cap \mathfrak{P}_2 = (p)$. Therefore, $\text{nm}(\alpha) \in \mathfrak{P}_1$, so since \mathfrak{P}_1 is prime, $\alpha^\sigma \in \mathfrak{P}_1$ for some σ . Therefore, $\alpha \in \mathfrak{P}_1^{\sigma^{-1}}$. This contradicts the fact that $\alpha \equiv 1 \pmod{\mathfrak{P}_1^{\sigma^{-1}}}$. Therefore, there exists a $\sigma \in \text{Gal}(K/\mathbb{Q})$ such that $\mathfrak{P}_2 = \mathfrak{P}_1^\sigma$. \square

Corollary 19.3. *Let K/\mathbb{Q} be a Galois extension of degree n , and p a rational prime. Suppose $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ in \mathcal{O}_K . Then $e_1 = \cdots = e_g$, and $f_1 = \cdots = f_g$.*

20. CYCLOTOMIC EXTENSIONS

Let q be a rational prime. We will look at the extension $\mathbb{Q}(\zeta)$, where ζ is a primitive q -th root of unity. We have seen that the ring of integers in this field is $\mathbb{Z}[\zeta]$.

Proposition 20.1. *$\mathbb{Q}(\zeta)$ is a Galois extension of \mathbb{Q} , whose Galois group is isomorphic to the multiplicative group modulo q .*

Proof. Each embedding of $\mathbb{Q}(\zeta)$ into \mathbb{C} takes ζ to ζ^i for some $i \neq 0$, since it must take ζ to a root of $x^{q-1} + x^{q-2} + \cdots + x + 1$. Therefore, all of the embeddings have the same image, so $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois.

Let σ_i denote the automorphism taking ζ to ζ^i . Then $\sigma_i \circ \sigma_j = \sigma_k$ where $k \equiv ij \pmod{q}$. Thus, the map taking σ_i to i is an isomorphism from $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to the multiplicative group of $\mathbb{Z}/q\mathbb{Z}$. \square

Proposition 20.2. *Any finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Let G be such a subgroup, and suppose G has order n . In any field, the equation $x^d = 1$ has at most d roots. Therefore, there are at most d elements in G of order dividing d . Let $f(d)$ denote the number of elements of order d . Then $f(d) \leq \varphi(d)$, since there are $\varphi(d)$ elements of order d in a cyclic group of order d . (Any element of order d generates such a cyclic group, and since at most d elements have orders dividing d there can be only one such cyclic group. In fact, we have seen that either $f(d) = 0$ or $f(d) = \varphi(d)$.)

Since every element of G has order dividing n , we have

$$n = \sum_{d|n} f(d).$$

We also have

$$n = \sum_{d|n} \varphi(d).$$

To prove it, consider the fractions $1/n, 2/n, \dots, n/n$. When reduced to lowest terms, exactly $\varphi(d)$ have denominator d , for each $d|n$, and there are n fractions total.

Since for each d , $f(d) \leq \varphi(d)$, we must have $f(d) = \varphi(d)$ for all d . Therefore, there are $\varphi(n-1)$ element of order n , and $\varphi(n-1) > 0$, so G is cyclic. \square

Corollary 20.3. *$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic of order $q-1$.*

Proposition 20.4. *Suppose F is a finite field containing $\mathbb{Z}/p\mathbb{Z}$, and generated by a single element z . Then F has order p^f where f is the smallest positive integer such that $z^{p^f} = z$.*

Proof. Note that raising to the p -th power is an automorphism σ of F , called the Frobenius automorphism. Iterating it shows, for each i , that raising to the p^i -th power (i.e., σ^i) is also an automorphism.

If $z^{p^f} = z$, then since $F = (\mathbb{Z}/p\mathbb{Z})[z]$, the automorphism σ^f is trivial. Therefore, every element of F satisfies the equation $x^{p^f} = x$. Since this equation has at most p^f roots, $|F| \leq p^f$.

Suppose the minimal polynomial for z has degree n . Then F has p^n elements (since it has a basis of size n), and F has at most n automorphisms (since each automorphism is determined by where it sends z , and must send z to a root of its minimal polynomial). If f is the least positive integer such that σ^f is trivial, then F has f automorphisms, namely, $1, \sigma, \dots, \sigma^{f-1}$. Therefore, $n \geq f$, and $|F| \geq p^f$.

Thus, $|F| = p^f$. \square

Proposition 20.5. *Let $p \neq q$ be a rational prime, and let f be the order of p modulo q . Then in $\mathbb{Z}[\zeta]$, (p) is the product of $(q-1)/f$ distinct primes, each with residue field degree f .*

Proof. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, all the primes dividing (p) have the same ramification indices and residue field degrees. We see that the ramification indices are all 1, since when we factor $x^{q-1} + \cdots + x + 1$ modulo p , we get no repeated factors. (To see this, note that it is $(x^q - 1)/(x - 1)$, and $x^q - 1$ has no repeated factors modulo p since it is relatively prime to its derivative.)

Now we just need to check what the residue field degree is. Suppose \mathfrak{P} is a prime dividing (p) . We have $\mathbb{Z}[\zeta]/\mathfrak{P} = (\mathbb{Z}/p\mathbb{Z})[\bar{\zeta}]$, where $\bar{\zeta}$ is the image of ζ . The residue field degree is the least f such that $\zeta^{p^f} \equiv \zeta \pmod{\mathfrak{P}}$.

If $p^f \equiv 1 \pmod{q}$, then $\zeta^{p^f} - \zeta = 0 \in \mathfrak{P}$. If $p^f \not\equiv 1 \pmod{q}$, then $\zeta^{p^f} - \zeta$ is an associate of $1 - \zeta$. Since $(1 - \zeta)$ divides (q) , and q and p are coprime, we see that $\zeta^{p^f} - \zeta \notin \mathfrak{P}$. Therefore, the order f of p modulo q is equal to the residue field degree of the primes dividing (p) . \square

Proposition 20.6. *Let $q^* = (-1)^{(q-1)/2}q$. Then $\mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta)$. If σ generates $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, then σ restricts to conjugation on $\mathbb{Q}(\sqrt{q^*})$. Any element of $\mathbb{Q}(\zeta)$ that is mapped to itself by σ^2 is in $\mathbb{Q}(\sqrt{q^*})$.*

Proof. We start with

$$q = \prod_{i=1}^{q-1} (1 - \zeta^i).$$

We have $(1 - \zeta^i)(1 - \zeta^{q-i}) = (1 - \zeta^i)(1 - \zeta^{-i}) = -\zeta^{-i}(1 - \zeta^i)^2$. Therefore,

$$q = (-1)^{(q-1)/2} \zeta^j \prod_{i=1}^{(q-1)/2} (1 - \zeta^i)^2$$

for some j (which we could easily compute, but won't). We can solve the congruence $2k \equiv j \pmod{p}$. Then

$$q^* = \left(\zeta^k \prod_{i=1}^{(q-1)/2} (1 - \zeta^i) \right)^2.$$

We thus see that $\mathbb{Q}(\sqrt{q^*}) \subset \mathbb{Q}(\zeta)$.

The field $\mathbb{Q}(\sqrt{q^*})$ has only two automorphisms, so to show that σ restricts to conjugation, we just need to show that it takes $\sqrt{q^*}$ to $-\sqrt{q^*}$. The most natural way to show this is to point out that if it didn't, there would be $q-1$ automorphisms of $\mathbb{Q}(\zeta)$ fixing $\mathbb{Q}(\sqrt{q^*})$, and since $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{q^*})] = (q-1)/2 < q-1$, this is impossible. However, we haven't really done much with automorphisms fixing a subfield, so we'll give a more elementary proof. A direct way to see the result here is to notice that if $(\sqrt{q^*})^\sigma = \sqrt{q^*}$, then $\text{tr}(\sqrt{q^*}) = (q-1)\sqrt{q^*} \notin \mathbb{Z}$. Thus, we see that σ restricts to conjugation.

Now consider the elements of $\mathbb{Q}(\zeta)$ mapped to themselves by σ^2 . The elements $\zeta^\sigma, \dots, \zeta^{\sigma^{q-1}}$ form a basis of $\mathbb{Q}(\zeta)/\mathbb{Q}$. From this, we see that the elements fixed by σ^2 form a vector space of dimension 2. Since the elements of $\mathbb{Q}(\sqrt{q^*})$ are fixed by σ^2 , they are the only ones. \square

21. QUADRATIC RECIPROCITY

Definition 21.1. Let p be a rational prime. We define the Legendre symbol as follows:

$$\left(\frac{a}{p} \right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if there exists } b \not\equiv 0 \text{ such that } a \equiv b^2 \pmod{p}, \\ -1 & \text{otherwise.} \end{cases}$$

Let p and q be distinct odd primes, and let $q^* = (-1)^{(q-1)/2}q$. As in the last section, let ζ be a q -th root of unity. Suppose that σ generates $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

We can reformulate Quadratic Reciprocity as follows:

Theorem 21.2 (Quadratic Reciprocity).

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

Proposition 21.3. *In $\mathbb{Q}(\sqrt{q^*})$, p splits as a product of two primes if*

$$\left(\frac{q^*}{p}\right) = 1$$

and remains prime if

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

Proof. Since the ring of integers is generated by a single element, we simply have to look at how its minimal polynomial factors modulo p . We take the generator to be $(1 + \sqrt{q^*})/2$ (since $q^* \equiv 1 \pmod{4}$), which has minimal polynomial $x^2 - x + (1 - q^*)/4$. This immediately gives the desired result, since the polynomial's discriminant is q^* , since it splits into two factors iff q^* is a square modulo p . \square

Recall the following lemma:

Lemma 21.4 (Euler's Criterion).

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

Proposition 21.5. *The prime p is the product of an even number of prime factors in $\mathbb{Q}(\zeta)$ iff it splits as the product of two prime factors in $\mathbb{Q}(\sqrt{q^*})$.*

Proof. Suppose $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ in $\mathbb{Q}(\sqrt{q^*})$. The ideals \mathfrak{p}_1 and \mathfrak{p}_2 give ideals $\mathfrak{q}_1 = \mathfrak{p}_1 \mathbb{Z}[\zeta]$ and $\mathfrak{q}_2 = \mathfrak{p}_2 \mathbb{Z}[\zeta]$ of $\mathbb{Z}[\zeta]$. Since \mathfrak{p}_1 and \mathfrak{p}_2 are mapped to each other by conjugation, we must have $\mathfrak{q}_1^\sigma = \mathfrak{q}_2$ and $\mathfrak{q}_2^\sigma = \mathfrak{q}_1$. We see therefore that in $\mathbb{Z}[\zeta]$, \mathfrak{q}_1 and \mathfrak{q}_2 must factor into the same number of primes. Thus, (p) factors into an even number of primes in $\mathbb{Z}[\zeta]$.

Now suppose $(p) = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_g$ in $\mathbb{Q}(\zeta)$, and g is even. By Propositions 20.5 and 19.2, the primes $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are distinct, and $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on them. Because g is even, they form two orbits under the action of σ^2 (where σ generates $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$). Define

$$\mathfrak{p}_1 = \mathfrak{P}_1^{1+\sigma^2+\sigma^4+\cdots+\sigma^{g-3}} = \mathfrak{P}_1^\sigma \mathfrak{P}_1^{\sigma^2} \mathfrak{P}_1^{\sigma^4} \cdots \mathfrak{P}_1^{\sigma^{g-3}}$$

and

$$\mathfrak{p}_2 = \mathfrak{P}_1^{\sigma+\sigma^3+\sigma^5+\cdots+\sigma^{g-2}}.$$

These are two coprime ideals of $\mathbb{Z}[\zeta]$. Their intersections with $\mathbb{Q}(\sqrt{q^*})$ divide (p) (since they contain (p)), so if we can show that the intersections are coprime, then (p) must split in $\mathbb{Q}(\sqrt{q^*})$. (Neither intersection can be the unit ideal, since neither ideal contains 1.)

Because \mathfrak{p}_1 and \mathfrak{p}_2 are coprime, there exist $\alpha \in \mathfrak{p}_1$ and $\beta \in \mathfrak{p}_2$ such that $\alpha + \beta = 1$. We would like α and β to be in $\mathbb{Q}(\sqrt{q^*})$. They might not be at first, but we will fix things so they are invariant under σ^2 . We start with

$$1 = \prod_{i=0}^{(q-3)/2} (\alpha^{\sigma^{2i}} + \beta^{\sigma^{2i}}).$$

Expanding this out gives

$$1 = \alpha^{1+\sigma^2+\sigma^4+\cdots+\sigma^{q-3}} + \beta^{\sigma+\sigma^3+\sigma^5+\cdots+\sigma^{q-2}} + \gamma,$$

where γ is in both \mathfrak{p}_1 and \mathfrak{p}_2 . All of the terms here but γ are fixed by σ^2 , so γ is also. Thus, each term is in $\mathbb{Q}(\sqrt{q^*})$. We see then that 1 is the sum of elements of $\mathfrak{p}_1 \cap \mathbb{Q}(\sqrt{q^*})$ and $\mathfrak{p}_2 \cap \mathbb{Q}(\sqrt{q^*})$, so these intersections are relatively prime. Since they divide (p) in $\mathbb{Q}(\sqrt{q^*})$, it follows that (p) must split, as desired. \square

Lemma 21.6. *The prime p is the product of an even number of primes on $\mathbb{Q}(\zeta)$ iff $p^{(q-1)/2} \equiv 1 \pmod{q}$*

Proof. We know that p is the product of $(q-1)/f$ factors, where f is the order of p modulo q . This is even iff f divides $(q-1)/2$, i.e., iff $p^{(q-1)/2} \equiv 1 \pmod{p}$. \square

Finally, we prove Quadratic Reciprocity:

Proof. The prime p splits in $\mathbb{Q}(\sqrt{q^*})$ iff

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

Also, it splits iff p is the product of an even number of primes in $\mathbb{Q}(\zeta)$. This is true iff

$$p^{(q-1)/2} \equiv 1 \pmod{q},$$

which is true iff

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

Therefore,

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

This proves Quadratic Reciprocity. □

(One can give a similar, but somewhat easier, proof that

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

iff $p \equiv \pm 1 \pmod{8}$.)

22. REFERENCES

This list is not intended to be at all complete, or to point out the best books available. It's just meant to provide a list of references for looking up the topics that come up in these notes.

Algebra, M. Artin. This book contains more than enough algebra for our purposes. Chapters 13 and 14 are good references for field theory and Galois theory, and Chapter 11 contains a discussion of ideal factorization in quadratic number fields. Chapter 10 provides an introduction to rings.

Local Fields, J.W.S. Cassels. This beautiful book is quite readable and includes many wonderful examples and applications. It is on local fields, which don't appear in these notes, but it also includes a good discussion of the material on number fields which are our focus.

Algebraic Number Theory, J.W.S. Cassels and A. Fröhlich. This book is hard to read and fairly sophisticated, but proves pretty much everything we need and lots more (in much greater generality).

Algebraic Number Theory, A. Fröhlich and M.J. Taylor. This book is a good introduction to algebraic number theory in general. It includes lots of computations of interesting explicit examples. (This is useful since algebraic number theory is a subject in which it is possible to learn general theorems without ever learning how to do non-trivial computations. We try to be fairly concrete in these notes, but aren't be able to go into as much detail as this book.)

Lectures on the Theory of Algebraic Numbers, E. Hecke. Like Weyl's book, this book is quite old-fashioned. The methods and style aren't the most modern, but the writing is very clear. Also, the book assumes practically no background knowledge.

A Classical Introduction to Modern Number Theory, K. Ireland and M. Rosen. This book doesn't focus on the same topics as us, but it is very elegant and readable. The proof we give of the finiteness of the class number and uniqueness of ideal factorization is given in Chapter 12 of this book, but few other books.

An Invitation to Arithmetic Geometry, D. Lorenzini. This book focuses on the analogy between algebraic curves and number fields. It covers most of the topics we cover, in slightly greater generality, as well as others.

Algebraic Theory of Numbers, H. Weyl. This is an old-fashioned book. Some of the material, especially Chapter II, is not done the way it would be today (although it's not wrong). However, the book is still very nice. Chapter I is quite relevant to these notes. In 32 pages, it gives a good account of field theory and Galois theory.