MATH 242: Algebraic number theory

Matthew Morrow (mmorrow@math.uchicago.edu)

Contents

1 A review of some algebra

In this course all rings R are commutative with unity. Algebraic number theory historically began as a study of factorization, and so we begin by reviewing properties of factorization in general commutative rings. You are expected to be familiar with this material, which may be found in any standard algebra textbook, since it will gradually be needed in the course.

Definition 1.1. Let R be a ring (commutative with unity!).

(i) R is an *integral domain* if and only if whenever $a, b \in R$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.

(ii) We write $a|b$ to mean that a divides b, i.e. that there exists $c \in R$ such that $ac = b$.

(iii) An integral domain R is a *principal ideal domain (PID)* if and only if every ideal I of R is principal, i.e. $I = \langle a \rangle$ for some $a \in R$, where $\langle a \rangle = aR$ is the principal ideal generated by a; this notation will be used throughout.

(iv) An element u of R is called a *unit* if and only if it has a multiplicative inverse. $R^\times$ denotes the group of units.

An element p of R is called *irreducible* if and only if it is not a unit and whenever $p = ab$ for some $a, b \in R$ then a or b is a unit. Two elements $a, b \in R$ are called *associates* if and only if there is a unit $u \in R$ such that $a = bu$.

An integral domain R is a *unique factorization domain (UFD)* if and only if every non-unit of R is a finite product of irreducible elements and whenever two such products $p_1 \dots p_r$, $q_1 \dots q_s$ are equal, then $r = s$ and, up to reordering, p_i and q_i are associates.

(v) An integral domain R is a *Euclidean domain (ED)* if and only if there is a map

$$\nu : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

with the following two properties:

- For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$, where either $\nu(r) < \nu(b)$ or $r = 0$.
- For all non-zero $a, b \in R$, $\nu(a) \leq \nu(ab)$.

The map ν is then called a *Euclidean norm* on R.

(vi) R is a ED $\implies$ R is a PID $\implies$ R is a UFD.

Example 1.2. The following examples will frequently appear and should be familiar to you:

(i) The ring of integers $\mathbb{Z}$ is a ED, with Euclidean norm $\nu(n) = |n|$. Hence it is also a PID and a UFD.

(ii) If F is a field then the polynomial algebra $F[X]$ is a ED with Euclidean norm $\nu(f(X)) = \deg f(X) = d$, if $f(X) = a_0 + a_1 X + \dots + a_d X^d$ with $a_d \neq 0$. Hence it is also a PID and a UFD.

Next we review the rings $\mathbb{Z}/n\mathbb{Z}$, which also occur frequently in algebraic number theory:

Definition 1.3. Given $n \in \mathbb{Z}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is the quotient of $\mathbb{Z}$ by the principal ideal $n\mathbb{Z}$. Given $x, y \in \mathbb{Z}$, we say x is *congruent to y mod n*, and write $x \equiv y \bmod n$ if and only if $n|x - y$, which is equivalent to saying that $x + n\mathbb{Z} = y + n\mathbb{Z}$, or that x and y have the same class in $\mathbb{Z}/n\mathbb{Z}$. We may write "$x \bmod n$" to mean the class of x in $\mathbb{Z}/n\mathbb{Z}$, when it is not likely to cause confusion.

Note: I will never use the notation $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$.

If $x \in \mathbb{Z}$, then $x \bmod n$ is a unit in the ring $\mathbb{Z}/n\mathbb{Z}$ if and only if x is coprime to n. In particular, if $p \in \mathbb{N}$ is a prime number, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p - 1$: any element is equal to exactly one of $1, 2, \dots, p - 1 \bmod p$. The following results will be used:

Theorem 1.4. *Let $p \in \mathbb{N}$ be a prime number.*

(i) ("Fermat's little theorem") If $a \in \mathbb{Z}$ is coprime to p, then $a^{p-1} \equiv 1 \bmod p$.

(ii) $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group.

Proof. (i): [20.1, FRA]. (ii): [23.6, FRA]; more generally, any finite subgroup of the multiplicative group of a field is cyclic. □

Corollary 1.5. *Let $p \in \mathbb{N}$ be a prime number. Then there exists $g \in \mathbb{Z}$ with the following properties:*

(i) If $a \in \mathbb{Z}$ is coprime to p, then $a \equiv g^r \bmod p$ for some $r \geq 0$.

(ii) If $r \in \mathbb{Z}$ is such that $g^r \equiv 1 \bmod p$, then $p - 1 | r$.

Proof. Let $g \in \mathbb{Z}$ be such that $g \bmod p$ generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$; then (i) and (ii) are restatements of that fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p - 1$. □

The classical name for an integer g with the properties of the following corollary is a *primitive root modulo* p, but we will use this notation very little.

2 QUADRATIC RESIDUES AND QUADRATIC RECIPROCITY

In this section we study so-called quadratic residues modulo an odd prime number p, which is essentially an analysis of when the equation $X^2 \equiv a \bmod p$ has an integer solution, for a fixed value of $a \in \mathbb{Z}$. These results and ideas will frequently reappear during the course when we study explicit examples, while the key theorem, namely the Law of Quadratic Reciprocity, will play a key role in describing the arithmetic of quadratic number fields in section 9.1.

Definition 2.1. Let $p \geq 3$ be a prime number, and suppose that $a \in \mathbb{Z}$ is coprime to p. Then a is said to be a *quadratic residue modulo* p if and only if there exists $x \in \mathbb{Z}$ satisfying $x^2 \equiv a \bmod p$.

(Note: The condition that a is coprime to p is important; 0 is not a quadratic residue modulo p, even though $0^2 \equiv 0 \bmod p$.)

Example 2.2. Here are basic examples:

(i) 3 is a quadratic residue modulo 13, since $4^2 = 16 \equiv 3 \bmod 13$.

(ii) $0^2 \equiv 0 \bmod 3$, $1^2 \equiv 1 \bmod 3$, and $2^2 \equiv 1 \bmod 3$. So if x is an integer then $x^2 \equiv 0$ or $1 \bmod 3$. Therefore 2 is not a quadratic residue mod 3.

The following characterisation of quadratic residues is needed for later proofs:

Lemma 2.3. *Let $p \geq 3$ be a prime number and suppose that $a \in \mathbb{Z}$ is coprime to p. Then a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.*

Proof. $\Rightarrow$: Suppose first that a is a quadratic residue modulo p; then $a \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}$. Then x is also coprime to p, and so $x^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem. Therefore

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \bmod p.$$

$\Leftarrow$: Conversely, assume that $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. Let g be a primitive root modulo p (see the end of section 1); then $a \equiv g^r$ for some $r \geq 0$. Our assumption implies that

$$(g^r)^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

As $g \bmod p$ generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $p-1$, this implies that $p-1 | r\frac{p-1}{2}$. That is, $r/2$ is an integer, and so $a \equiv (g^{r/2})^2 \bmod p$; i.e. a is a quadratic residue modulo p. □

In order to develop a way of manipulating quadratic residues, and to clarify their properties, the following piece of notation is absolutely fundamental:

Definition 2.4. The *Legendre symbol*, for $p \geq 3$ a prime number and $a \in \mathbb{Z}$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a quadratic residue modulo } p, \\ 0 & \text{if } p | a. \end{cases}$$

Example 2.5. To clarify the definition we offer the following examples:

(i) 3 is a quadratic residue modulo 13, by the previous example, so $\left(\frac{3}{13}\right) = 1$.

(ii) 5 is not a quadratic residue modulo 7 (since $1^2 \equiv 6^2 \equiv 1$, $2^2 \equiv 5^2 \equiv 2$, $3^2 \equiv 4^2 \equiv 4 \bmod 7$), so $\left(\frac{5}{13}\right) = -1$.

(iii) $\left(\frac{-6}{3}\right) = 0$ since 3 divides -6.

The Legendre symbol is a convenient tool for discussing and manipulating quadratic residues; the following are some of its key properties:

Lemma 2.6. *Let $p \geq 3$ be a prime number and let $a, b \in \mathbb{Z}$. Then*

(i) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$ *("Euler's lemma");*

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) If $a \equiv b \bmod p$ *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. If p divides a or b then these identities are all trivial; so assume that p does not divide a or b.

(i) By Fermat's little theorem, $a^{p-1} \equiv 1 \bmod p$. So p divides

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1),$$

whence p divides $a^{\frac{p-1}{2}} - 1$ or $a^{\frac{p-1}{2}} + 1$, i.e. $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. But according to lemma 2.3, a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

(ii) Since $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$, part (i) implies that $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p$. As all these terms are ± 1, and since p is odd, it follows that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) This is quite clear: the definition of a quadratic residue only depends on $a \bmod p$.

□

From the proposition we obtain an important and useful corollary:

Proposition 2.7 (Legendre symbol of -1)**.** *Let $p \geq 3$ be a prime number. Then*

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

(ii) -1 *is a quadratic residue modulo p if and only if p is congruent to 1 modulo 4.*

Proof. For (i), apply part (i) of the previous proposition to $a = -1$, and then, as in the previous proposition, use the fact that a congruence mod p when both sides are either 1 or -1 is actually an equality. For (ii), note that if $p \equiv 1 \bmod 4$ then $(-1)^{\frac{p-1}{2}} = 1 \equiv 1$, whereas if $p \not\equiv 1 \bmod 4$ then $p \equiv 3 \bmod 4$ and so $(-1)^{\frac{p-1}{2}} = -1$. □

Here is an interesting application of the results so far:

Corollary 2.8. *There are infinitely many positive prime numbers which are congruent to 1 mod 4.*

Proof. Suppose not, and let $\{p_1, \ldots, p_n\}$ be the finite set of all positive prime numbers which are $\equiv 1 \bmod 4$. Put $M = (2p_1 \ldots p_n)^2 + 1$; then $M > 1$, so M is divisible by some positive prime number p. Since M is odd, $p \neq 2$.

Now observe that $-1 \equiv (2p_1 \ldots p_n)^2 \bmod p$, so $\left(\frac{-1}{p}\right) = 1$; the previous proposition therefore implies that $p \equiv 1 \bmod 4$. So $p = p_i$ for some i, whence $M \equiv 1 \bmod p$; this contradicts $p|M$. □

Remark 2.9. A deep result, beyond this course, is the following theorem of Dirichlet: if a, n are coprime integers, then there are infintely many prime numbers which are congruent to a modulo n. As we develop more tools during the course, we will see other special cases of this result.

The aim of this section is to prove the next two theorems (due to Gauss, Legendre, and Eisenstein), which allow us to easily calculate any Legendre symbol and therefore determine exactly when a is a quadratic residue modulo p. Their more theoretic importance will become clear in section 9.1.

The proofs will be postponed until the end of the section.

Theorem 2.10 (Legendre symbol of 2)**.** *$p \geq 3$ a prime number. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}.$$

Exercise 2.1 (Restatement of the Leg. sym. of 2 theorem)**.** Suppose that b is an odd integer; show that $b^2 - 1$ is divisible by 8, and that $\frac{b^2-1}{8}$ is even if $b \equiv \pm 1 \bmod 8$ and is odd if $b \equiv \pm 3 \bmod 8$.

Deduce that the Legendre symbol of 2 theorem can be rewritten as the statement that

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

This is sometimes a useful formulation.

Example 2.11. $61 \equiv -3 \bmod 8$ and so 2 is not a quadratic residue modulo 61; checking this any other way but by using the theorem would be extremely time consuming.

$73 \equiv 1 \bmod 8$ and so 2 is a quadratic residue mod 73; notice that we have proved this without actually finding any integer x satisfying $x^2 \equiv 2 \bmod 73$.

The following is the second main theorem. Despite its simple statement, it is an extraordinary result, telling us that if $p, q \geq 3$ are prime numbers then there is a mysterious relationship between the Legendre symbols $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$. A priori, there is absolutely no reason that these should be related: although both symbols encode the solubility of an equation, the first is really an equation in $\mathbb{Z}/p\mathbb{Z}$ and the second is in $\mathbb{Z}/q\mathbb{Z}$. These two equations should have nothing to do with one another!

Theorem 2.12 (Law of Quadratic Reciprocity)**.** *Let $p, q \geq 3$ be distinct primes. Then*

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

Exercise 2.2 (Restatement of the LQR)**.** Show that the Law of Quadratic Reciprocity can be restated in the follow way: If $p, q \geq 3$ are prime numbers (not necessarily distinct), then

$$\left(\frac{p}{q}\right) = \varepsilon \left(\frac{q}{p}\right), \quad \text{where } \varepsilon = \begin{cases} 1 & \text{if } p \text{ or } q \text{ is } \equiv 1 \bmod 4 \\ -1 & \text{if both } p \text{ and } q \text{ are } \equiv 3 \bmod 4 \end{cases}$$

It is almost always in this form that one uses the Law of Quadratic Reciprocity.

Example 2.13. We now demonstrate the power of the previous two theorems by effortlessly calculating some Legendre symbols:

(i)
$$\left(\frac{61}{89}\right) = \left(\frac{89}{61}\right) = \left(\frac{28}{61}\right) = \left(\frac{4}{61}\right)\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$$

(ii)
$$\left(\frac{33}{59}\right) = \left(\frac{3}{59}\right)\left(\frac{11}{59}\right) = -\left(\frac{59}{3}\right) \cdot -\left(\frac{59}{11}\right) = \left(\frac{-1}{3}\right)\left(\frac{4}{11}\right) = (-1)^{(3-1)/2} = -1$$

(iii)

$$\left(\frac{67}{89}\right) = \left(\frac{89}{67}\right) = \left(\frac{22}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{11}{67}\right) = -1 \cdot -\left(\frac{67}{11}\right) = \left(\frac{1}{11}\right) = 1$$

Before proving the two main theorems, we provide some sample applications to demonstrate their usefullness in questions of number theory; this week's homework includes modifications of all these results:

Proposition 2.14. *p an odd prime. Then -2 is a quadratic residue modulo p if and only if p is congruent to 1 or 3 modulo 8.*

Proof. We have

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

and

$$\frac{p-1}{2} + \frac{p^2-1}{8} = \frac{p^2+4p-5}{8} = \frac{(p-1)(p+5)}{8}.$$

One now checks that

$$p \equiv \begin{cases} 1 \\ 3 \\ -3 \\ -1 \end{cases} \mod 8 \Rightarrow \frac{(p-1)(p+5)}{8} \equiv \begin{cases} 0 \\ 0 \\ 1 \\ 1 \end{cases} \mod 2.$$

(e.g. $p \equiv -3 \bmod 8 \Rightarrow p = 8m-3 \Rightarrow \frac{(p-1)(p+5)}{8} = 8m+1 \equiv 1 \bmod 2$). Therefore

$$p \equiv \begin{cases} 1 \\ 3 \\ -3 \\ -1 \end{cases} \mod 8 \Rightarrow \left(\frac{-2}{p}\right) = \begin{cases} 1 \\ 1 \\ -1 \\ -1 \end{cases}.$$

□

Proposition 2.15. *There are infinitely many positive primes in $\mathbb{Z}$ which are congruent to -1 modulo 8.*

Proof. As usual, we prove this by contradiction, assuming that the set of all such primes is finite: $\{p_1, \ldots, p_m\}$. Let $M = 8(p_1 \ldots p_m)^2 - 1$, and let $M = q_1^{r_1} \ldots q_t^{r_t}$ be the prime factorization of M. If $q_i \equiv 1 \bmod 8$ for all i, then

$$M = q_1^{r_1} \ldots q_t^{r_t} \equiv 1^{r_1} \ldots 1^{r_t} \equiv 1 \bmod 8,$$

which is false. Therefore there is i such that $q_i \not\equiv 1 \bmod 8$.

Notice that q_i is odd since M is odd. Moreover, we have

$$(4p_1 \ldots p_m)^2 = 2(M+1) \equiv 2 \bmod q_i,$$

so 2 is a quadratic residue modulo q_i. The "Legendre symbol of 2" theorem now implies $q_i \equiv \pm 1 \bmod 8$, and so $q_i \equiv -1 \bmod 8$.

Therefore $q_i = p_j$ for some j, whence we get the usual contradiction: $q | p_1 \ldots p_m$ and $q | M$ implies $q | 2$. □

Proposition 2.16. *Let $p > 3$ be a Fermat prime (this means $p = 2^n + 1$ for some $n \geq 1$). Then 3 is a primitive root modulo p.*

Proof. Since the group $\mathbb{Z}/p\mathbb{Z}^\times$ has $p-1=2^n$ elements, any element g of the group which satisfies $g^{2^{n-1}} \neq 1$ is a generator. Therefore it is enough to prove that $3^{2^{n-1}} \not\equiv 1 \bmod p$.

But $2^{n-1} = (p-1)/2$ and $3^{(p-1)/2} = \left(\frac{3}{p}\right)$; therefore we must show that $\left(\frac{3}{p}\right) \neq 1$; i.e. that 3 is not a quadratic residue mod p.

Since $p \equiv 1 \bmod 4$, the Law of Quadratic Reciprocity implies $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$; since $2 \equiv -1 \bmod 3$, we see that $p \equiv (-1)^n + 1 \bmod 3$, which is 0 or 2 modulo 3. But p is prime, so not divisible by 3. Therefore $p \equiv 2 \bmod 3$; 2 is not a quadratic residue modulo 3, so now we know $\left(\frac{3}{p}\right) = -1$. Therefore $\left(\frac{3}{p}\right) = -1$, completing the proof. □

We now begin the proofs of the two main theorems: "Legendre symbol of 2" and "Law of Quadratic Reciprocity". Although Ireland and Rosen follows Gauss' methods, we will follow a proof due to Eisenstein (there are at least 233 different proofs in existence today[1]). The following technical lemma is essential:

Lemma 2.17 (Eisenstein's lemma)**.** *Let p be an odd prime, and $a \in \mathbb{Z}$ not divisible by p; then*

$$\left(\frac{a}{p}\right) = (-1)^s,$$

where

$$s = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ka}{p} \right\rfloor.$$

Proof. For any integer k, we will write $r(k)$ to denote the unique integer in the range $0, \ldots, p-1$ which is congruent to k modulo p; in other words, $r(k)$ is the remainder when k is divided by p. The proof is a little tricky so we will label the steps:

(1). Firstly, if $1 \leq l \leq p-1$ then $r((-1)^l l)$ is even and non-zero. Indeed, if l is even then $r((-1)^l l) = r(l) = l$ (which is even); if l is odd, then $r((-1)^l l) = r(-l) = p - l$ (which is even); and it is non-zero since $r((-1)^l l) \equiv (-1)^l l \not\equiv 0 \bmod p$.

(2). So, if $k \in \{1, 2, \ldots, (p-1)/2\}$ then $2ka$ is coprime to p and therefore $r(2ka) \in \{1, \ldots, p-1\}$; so paragraph (1), with $l = r(2ka)$, shows $r((-1)^{r(2ka)} r(2ka)) \in \{2, 4, \ldots, p-1\}$. Thus there is a well-defined map

$$R : \{1, \ldots, (p-1)/2\} \to \{2, 4, \ldots, p-1\}, \quad k \mapsto r((-1)^{r(2ka)} r(2ka)),$$

which we next prove is injective.

So suppose that $1 \leq k, k' \leq (p-1)/2$ and $R(k) = R(k')$; this implies

$$(-1)^{r(2ka)} r(2ka) \equiv (-1)^{r(2k'a)} r(2k'a) \bmod p.$$

Therefore $(-1)^{r(2ka)} 2ka \equiv (-1)^{r(2k'a)} 2k'a \bmod p$; since $2a$ is a unit modulo p, we may divide by it to deduce that $(-1)^{r(2ka)} k \equiv (-1)^{r(2k'a)} k' \bmod p$. So $k \equiv \varepsilon k' \bmod p$, where $\varepsilon = (-1)^{r(2k'a) - r(2ka)} \in \{0, 1\}$. But k, k' are both in the range $1 \leq k, k' \leq (p-1)/2$, so $k \equiv -k'$ is impossible, and $k \equiv k'$ happens if and only if $k = k'$. This proves that R is injective.

(3). Since the codomain and domain of R both have cardinality $(p-1)/2$, we see that R is actually a bijection: in other words, as k runs over the integers $1, 2, \ldots, (p-1)/2$, then $r((-1)^{r(2ka)} r(2ka))$ runs over the integers $2, 4, \ldots, (p-1)$. Therefore

$$\prod_{k=1}^{(p-1)/2} r((-1)^{r(2ka)} r(2ka)) = \prod_{l=1}^{(p-1)/2} 2l,$$

[1] http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

and so

$$\prod_{l=1}^{(p-1)/2} 2l \equiv \prod_{k=1}^{(p-1)/2} (-1)^{r(2ka)} r(2ka) \bmod p. \tag{\dagger}$$

(4). With identity (†) established, we may now complete the proof:

$$\begin{aligned} a^{(p-1)/2} \prod_{k=1}^{(p-1)/2} 2k &= \prod_{k=1}^{(p-1)/2} 2ka \\ &\equiv \prod_{k=1}^{(p-1)/2} r(2ka) \bmod p \\ &\equiv (-1)^{\sum_k r(2ka)} \prod_{k=1}^{(p-1)/2} (-1)^{r(2ka)} r(2ka) \bmod p \\ &\equiv (-1)^{\sum_k r(2ka)} \prod_{k=1}^{(p-1)/2} 2k \bmod p \end{aligned}$$

Since $\prod_{k=1}^{(p-1)/2} 2k$ is coprime to p, it follows that $a^{(p-1)/2} \equiv (-1)^{\sum_k r(2ka)} \bmod p$. But Euler's lemma says $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$, so $\left(\frac{a}{p}\right) \equiv (-1)^{\sum_k r(2ka)} \bmod p$. Since two powers of (-1) are congruent modulo p if and only if they are equal, we deduce $\left(\frac{a}{p}\right) = (-1)^{\sum_k r(2ka)}$. Finally, the definition of the floor function and r function mean that

$$2ka = \left\lfloor \frac{2ka}{p} \right\rfloor p + r(2ka),$$

which implies $\left\lfloor \frac{2ka}{p} \right\rfloor \equiv r(2ka) \bmod 2$. Therefore $\left(\frac{a}{p}\right) = (-1)^{\sum_k \left\lfloor \frac{2ka}{p} \right\rfloor}$, as required. □

Now we may prove the first of the main theorems:

Theorem 2.18 (Proof of "Legendre symbol of 2")**.** *p an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

Proof. If k is an integer in the range $1 \le k \le \lfloor p/4 \rfloor$ then $1 \le 4k \le p$, so actually $1 \le 4k < p$ (since p is prime) and so $0 \le 4k/p < 1$; therefore $\left\lfloor \frac{4k}{p} \right\rfloor = 0$. If instead k is the in the range $\lfloor p/4 \rfloor < k < (p-1)/2$ then a similar argument shows $\left\lfloor \frac{4k}{p} \right\rfloor = 1$. So $\left(\frac{2}{p}\right) = (-1)^s$ (by Eisenstein's lemma) where

$$s = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2k2}{p} \right\rfloor = \sum_{\text{s.t. } \lfloor p/4 \rfloor < k \le (p-1)/2} 1 = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor.$$

Therefore we must show that

$$\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor \text{ is } \begin{cases} \text{even} & p \equiv \pm 1 \bmod 8 \\ \text{odd} & p \equiv \pm 3 \bmod 8 \end{cases}$$

So, write $p = 8c + \varepsilon$ for some $c \in \mathbb{Z}$ and some $\varepsilon \in \{-3, -1, 1, 3\}$.

If $\varepsilon = \pm 1$ then

$$\begin{aligned}\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor &= \lfloor 4m \pm 1/2 \rfloor - \lfloor 2m \pm 1/4 \rfloor \\ &= \begin{cases} (4m-1) - (2m-1) & \varepsilon = -1 \\ 4m - 2m & \varepsilon = 1 \end{cases} \\ &= 2m \\ &\equiv 0 \bmod 2\end{aligned}$$

Secondly, if $\varepsilon = \pm 3$ then

$$\begin{aligned}\left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor &= \lfloor 4m \pm 3/2 \rfloor - \lfloor 2m \pm 3/4 \rfloor \\ &= \begin{cases} (4m-2) - (2m-1) & \varepsilon = -3 \\ (4m+1) - 2m & \varepsilon = 3 \end{cases} \\ &= \begin{cases} 2m - 3 & \varepsilon = -3 \\ 2m + 1 & \varepsilon = 3 \end{cases} \\ &\equiv 1 \bmod 2\end{aligned}$$

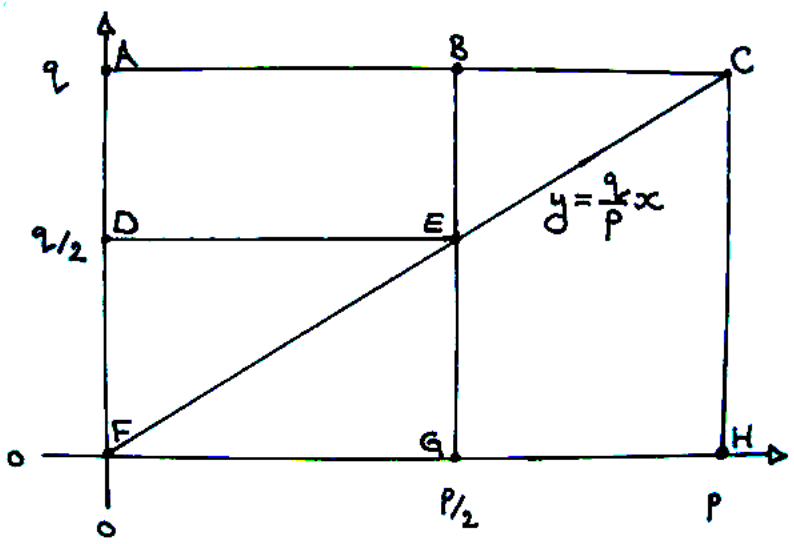
□

And now we prove the second main theorem:

Theorem 2.19 (Proof of the Law of Quadratic Reciprocity)**.** *Let p, q be distinct odd primes. Then*

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

Proof. We will study the following diagram in the (x, y)-plane:



Let Λ be the set of lattice points, i.e. points with integer coordinates, which are *strictly* inside the rectangle ACHF, i.e.

$$\Lambda = \{(x, y) \in \mathbb{Z}^2 : 0 < x < p,\ 0 < y < q\}.$$

We are going to count certain geometrically-defined subsets of Λ in different ways and compare the results.

Let $\Lambda(EFG) \subset \Lambda$ denote the set of lattice points strictly inside the triangle EFG, and $\Lambda(EFG)_e$ (resp. $\Lambda(EFG)_o$) those points with even (resp. odd) x-coordinate. Use the same style of notation for other triangles DEF, etc. and quadrilaterals $CEGH$, etc.

The map

$$R : \Lambda \to \Lambda, \quad (x, y) \mapsto (p - x, q - y)$$

is a bijection, geometrically given by rotation of 180° about the point $E = (p/2, q/2)$. Restricted to $\Lambda(EFG)_o$, it gives a bijection $R : \Lambda(EFG)_o \to \Lambda(BCE)_e$, and so

$$\#\Lambda(EFG)_o = \#\Lambda(BCE)_e. \tag{1}$$

Secondly,

$$\Lambda(BCE)_e \cup \Lambda(CEGH)_e = \Lambda(BCGH)_e = \{(x, y) \in \mathbb{Z}^2 : p/2 < x < p,\ x \text{ even},\ 0 < y < q\},$$

which has even cardinality $\lfloor (p + 2)/4 \rfloor \cdot (q - 1)$; therefore

$$\#\Lambda(BCE)_e \equiv \#\Lambda(CEGH)_e \bmod 2. \tag{2}$$

Next, for any fixed integer $m \geq 1$, the number of lattice points inside the triangle CFH with x-coordinate equalling m is $\lfloor mq/p \rfloor$, and so

$$\#\Lambda(CFH)_e = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2kq}{p} \right\rfloor. \tag{3}$$

Putting these identities together gives

$$\begin{aligned}
\#\Lambda(EFG) &= \#\Lambda(EFG)_o + \#\Lambda(EFG)_e \\
&= \#\Lambda(BCE)_e + \#\Lambda(EFG)_e && \text{(by (1))} \\
&\equiv \#\Lambda(CEGH)_e + \#\Lambda(EFG)_e \bmod 2 && \text{(by (2))} \\
&= \#\Lambda(CFH)_e \\
&= \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2kq}{p} \right\rfloor, && \text{(by (3))}
\end{aligned}$$

and so

$$(-1)^{\#\Lambda(EFG)} = (-1)^{\sum_{k=1}^{(p-1)/2} \lfloor \frac{2kq}{p} \rfloor} = \left(\frac{p}{q}\right).$$

Repeating the argument with p and q swapped implies

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

Finally,

$$\frac{p-1}{2}\frac{q-1}{2} = \#\Lambda(DEFG) = \#\Lambda(DEF) + \#\Lambda(EFG),$$

so

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\#\Lambda(DEFG)} = (-1)^{\#\Lambda(DEF)}(-1)^{\#\Lambda(EFG)} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right),$$

as required. □

This completes the proofs of the main theorems on quadratic residues and quadratic reciprocity.

3 Algebraic numbers and algebraic integers

Now we introduce the field of algebraic numbers and the ring of algebraic integers; these will be the main objects of study in this course. For the moment we study them one at a time, before introducing number fields in the next section.

Definition 3.1. An *algebraic number* is a complex number α for which there exist $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ $(n \geq 1)$ such that

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

An *algebraic integer* is a complex number α for which there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ $(n \geq 1)$ such that

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

The set of algebraic numbers is denoted $\mathbb{Q}^{\text{alg}}$, and the set of algebraic integers is denoted $\mathbb{Z}^{\text{alg}}$ (Ireland and Rosen use the notation Ω).

Example 3.2. Some remarks and examples:

(i) Any $\alpha \in \mathbb{Q}$ is an algebraic number (take $n = 1$, $a_0 = \alpha$), and every $\alpha \in \mathbb{Z}$ is an algebraic integer (again take $n = 1$, $a_0 = \alpha$).

(ii) Every algebraic integer is an algebraic number.

(iii) $\sqrt{-5}$ is an algebraic integer, since $\sqrt{-5}^2 + 5 = 0$.

(iv) Let $\omega = \frac{-1+\sqrt{-3}}{2}$; then $\omega^2 + \omega + 1 = 0$, so ω is an algebraic integer (even though it looks like a 'fraction').

(v) If $n \geq 1$ then $\zeta := e^{2\pi i/n}$ is an algebraic integer, since $\zeta^n - 1 = 0$.

(vi) If α is an algebraic number and $r \in \mathbb{Q}$ then $r\alpha$ is an algebraic number. Moreover, it is possible to find a non-zero $r \in \mathbb{Z}$ such that $r\alpha$ is an algebraic integer; this is on the homework.

(vii) π and e are not algebraic numbers, though these are difficult theorems which we will not discuss in this course.

The following provides a useful abstract test for whether a complex number is an algebraic number/integer. We will use it many times in the course. Consider subsets $V \subseteq \mathbb{C}$ such that V is a vector space over $\mathbb{Q}$, i.e.

$$v, w \in V \Rightarrow v + w \in V$$
$$v \in V, r \in \mathbb{Q} \Rightarrow rv \in V.$$

For example, $V = \mathbb{Q}$, $V = \{r + s\sqrt{-5} : r, s \in \mathbb{Q}\}$. Note also that V even contains a finitely generated abelian group $M = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

Lemma 3.3. *Let $\alpha \in \mathbb{C}$. Then*

(i) α is an algebraic number if and only if there exists a non-zero finite dimensional vector space $V \subseteq \mathbb{C}$ over $\mathbb{Q}$ such that $\alpha V \subseteq V$.

(ii) α is an algebraic integer if and only if there exists a non-zero finitely generated group $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$.

Proof. (i). $\Rightarrow$: Assume α is an algebraic number. So there exist $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ such that

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

Let

$$V = \{r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} : r_0, \ldots, r_{n-1} \in \mathbb{Q}\},$$

and notice that V is a non-zero vector space over $\mathbb{Q}$ of dimension at most n. We claim that $\alpha V \subseteq V$. So let $v \in V$, and write $v = r_0 + r_0\alpha + \cdots + r_{n-1}\alpha^{n-1}$; then

$$\begin{aligned}
\alpha v &= r_0\alpha + r_1\alpha^2 + \cdots + r_{n-1}\alpha^n \\
&= r_0\alpha + r_1\alpha^2 + \cdots + r_{n-2}\alpha^{n-1} - r_{n-1}(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\
&= -a_0 + (r_0 - a_1)\alpha + (r_1 - a_2)\alpha^2 + \cdots + (r_{n-2} - a_{n-1})\alpha^{n-1} \\
&\in V.
\end{aligned}$$

$\Leftarrow$: Assume that there is a non-zero finite dimensional $\mathbb{Q}$ vector space $V \subseteq \mathbb{C}$ such that $\alpha V \subseteq V$. Let $v_1, \ldots, v_d \in V$ be a basis of V as $\mathbb{Q}$ vector space. For each i, $\alpha v_i \in V$, so we may write

$$\alpha v_i = \sum_{j=1}^{n} r_{i,j} v_j$$

for some $r_{i,1}, \ldots, r_{i,d} \in \mathbb{Q}$. In other words, the $\mathbb{Q}$-linear map

$$V \to V, \quad v \mapsto \alpha v$$

has matrix $R = (r_{i,j})_{1 \le i,j \le d}$ with respect to the basis $v_1, \ldots, v_d$. Now think of R as a matrix over $\mathbb{C}$; it satisfies

$$R \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{d} r_{1,j} v_1 \\ \vdots \\ \sum_{j=1}^{d} r_{d,j} v_d \end{pmatrix} = \alpha \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}.$$

So α is a complex eigenvalue of R and therefore $\det(\alpha I_{d\times d} - R) = 0$; expanding the determinant gives a monic polynomial of degree d with coefficients in $\mathbb{Q}$ of which α is a root. Therefore α is an algebraic number.

(ii). $\Rightarrow$: Imitate part (i), replacing V by the finitely generated abelian group

$$M = \{m_0 + m_1\alpha + \cdots + m_{n-1}\alpha^{n-1} : m_0, \ldots, m_{n-1} \in \mathbb{Z}\}.$$

$\Leftarrow$: Imitate part (ii); the matrix R will have coefficients in $\mathbb{Z}$ and so the polynomial obtained by expanding $\det(\alpha I_{d\times d} - A)$ will also have coefficients in $\mathbb{Z}$. □

We use the lemma to prove:

Proposition 3.4. *$\mathbb{Q}^{alg}$ is a subfield of $\mathbb{C}$. $\mathbb{Z}^{alg}$ is a subring of $\mathbb{C}$.*

Proof. Let α, β be algebraic numbers. According the previous lemma, there are non-zero finite dimensional vector spaces $V, W \subseteq \mathbb{C}$ over $\mathbb{Q}$ such that $\alpha V \subseteq V$ and $\beta W \subseteq W$. Let

$$VW := \{v_1w_1 + \cdots + v_tw_t : v_i \in V, w_i \in W\}$$

be the set of all finite sums of products vw for $v \in V$, $w \in W$. Observe the following:

(i) Let $v_1, \ldots, v_n$ span V and $w_1, \ldots, w_m$ span W. Then VW is spanned by $(v_iw_j)_{i,j}$; so VW is finite dimensional over $\mathbb{Q}$. Also, $VW \neq 0$.

(ii) If $v \in V$ and $w \in W$ then $\alpha vw = (\alpha v)w \in VW$ and $\beta vw = v(\beta w) \in VW$. Therefore, by linearity, if $z \in VW$ then $\alpha z, \beta z \in VW$.

So if $z \in VW$ we see that $\alpha z, \beta z \in VW$, so $(\alpha+\beta)z = \alpha z + \beta z \in VW$; also, since $\beta z \in VW$, we have $\alpha(\beta z) \in VW$, i.e. $(\alpha\beta)z \in VW$.

By the condition of the previous lemma, $\alpha+\beta$ and $\alpha\beta$ are algebraic numbers.

Secondly, if α, β are actually algebraic integers, then the previous lemma provides us with non-zero finitely generated abelian groups $M, N \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$, $\beta N \subseteq N$; we may then exactly repeat the argument above for algebraic numbers, replacing VW by

$$MN = \{v_1 w_1 + \cdots + v_t w_t : v_i \in M, w_i \in N\}.$$

This shows that α, β are also algebraic integers.

It remains only to check that if α is a non-zero algebraic number then so is α^{-1}. There exist $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ such that

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

Let $i \geq 0$ be the smallest index such that $a_i \neq 0$. Then

$$0 = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_i\alpha^i = \alpha^i(\alpha^{n-i} + a_{n-1}\alpha^{n-i-1} + \cdots + a_i)$$

and so $\alpha^{n-i} + a_{n-1}\alpha^{n-i-1} + \cdots + a_i = 0$. Multiply this by $\alpha^{i-n}a_i^{-1}$ to get

$$(\alpha^{-1})^{i-n} + a_{i+1}a_i^{-1}(\alpha^{-1})^{i-n-1} + \cdots + a_i^{-1} = 0;$$

therefore α^{-1} is an algebraic number. □

Exercise 3.1. Let $f(X)$ be a monic polynomial whose coefficients are algebraic integers. In this problem you will show that any complex root of $f(X)$ is also an algebraic integer.

(i) Prove that if $\alpha_0, \ldots, \alpha_{d-1}$ are algebraic integers, then there is a non-zero finitely generated abelian group $M \subseteq \mathbb{C}$ such that $\alpha_i M \subseteq M$ for $i = 0, \ldots, d-1$.

(ii) Let α be a complex root of $f(X)$. Show that there exists a non-zero finitely generated abelian group $N \subseteq \mathbb{C}$ such that $\alpha N \subseteq N$. Deduce that α is an algebraic integer.

(iii) Show that $\mathbb{Q}^{\text{alg}}$ is an *algebraically closed* field, i.e. every non-constant polynomial with coefficients in $\mathbb{Q}^{\text{alg}}$ has a root in $\mathbb{Q}^{\text{alg}}$. (Hint: you can either reprove analogues of the previous two results for algebraic numbers or, more quickly, use question (6) to reduce to the case of algebraic integers. You may quote the fact that $\mathbb{C}$ is an algebraically closed field.)

Example 3.5.

(i) Every element of $\mathbb{Z}[\sqrt{-5}]$ can be written as $a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$; since $\sqrt{-5}$ and $a, b \in \mathbb{Z}$ are all algebraic integers, we see that every element of $\mathbb{Z}[\sqrt{-5}]$ is an algebraic integer. For example, $\alpha := 2 - 3\sqrt{-5}$ is an algebraic number, and it is not hard to find an equation of which it is a root:

$$\begin{aligned}(2-3\sqrt{-5})^2 &= 4 - 12\sqrt{-5} - 45\\ &= -41 - 12\sqrt{-5}\\ &= 4(2-3\sqrt{-5}) - 49,\end{aligned}$$

so $\alpha^2 - 4\alpha + 49 = 0$.

(ii) $\sqrt{2}+\sqrt{3}$ is an algebraic integer since it is the sum of two algebraic integers. Let's find an integer polynomial it satisfies:

$$\begin{aligned}(\sqrt{2}+\sqrt{3})^4 &= 4 + 4\cdot 2\sqrt{2}\sqrt{3} + 6\cdot 6 + 4\sqrt{2}\cdot 3\sqrt{3} + 9\\ &= 49 + 20\sqrt{6}\\ &= 49 + 10(\sqrt{2}+\sqrt{3})^2 - 10\cdot 2 - 10\cdot 3\\ &= 10(\sqrt{2}+\sqrt{3})^2 - 1\end{aligned}$$

So $(\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1 = 0$.

Among all monic polynomials in $\mathbb{Q}[X]$ satisfied by an algebraic number, there is an optimal one, which you probably encountered in Algebra II:

Proposition 3.6. *Let $\alpha \in \mathbb{Q}^{alg}$ be non-zero. There there is a unique monic, irreducible polynomial $f(X) \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$. Moreover, if $g(X) \in \mathbb{Q}[X]$ is any polynomial satisfying $g(\alpha) = 0$ then $f(X)|g(X)$.*

Proof. This should be familiar from Alg II, but here is a proof.

Let

$$I = \{h(X) \in \mathbb{Q}[X] : h(\alpha) = 0\}.$$

If $h_1, h_2 \in I$ then $h_1 + h_2 \in I$, and if $h \in I$, $g \in \mathbb{Q}[X]$ then $gh \in I$; that is, I is an ideal of $\mathbb{Q}[X]$. Since α is an algebraic number, there exists a non-zero element of I, and since $\alpha \neq 0$, $I \neq \mathbb{Q}[X]$.

Therefore I is a non-zero, proper ideal of $\mathbb{Q}[X]$; as $\mathbb{Q}[X]$ is a principal ideal domain, there exists a non-constant polynomial $f \in I$ satisfying $I = \langle f \rangle$. Write $f = a_n X^n + \cdots + a_0$ with $a_n \neq 0$; then a_n is a unit in $\mathbb{Q}[X]$ and so $\langle a_n^{-1} f \rangle = \langle f \rangle = I$. Therefore, after replacing f by $a_n^{-1} f$, we may assume f is monic. Obviously $f(\alpha) = 0$, and if g is any polynomial satisfying $g(\alpha) = 0$ then $g \in I$, so f divides g.

For a contradiction, suppose that f is not irreducible. Then there exist monic polynomials $g, h \in \mathbb{Q}[X]$ such that $f = gh$ and such that $\deg g, \deg h < \deg f$. Thus $0 = f(\alpha) = g(\alpha)h(\alpha)$, so one of $g(\alpha)$, $h(\alpha)$ is zero, i.e. f divides g or h; but this is impossible since $\deg g, \deg h < \deg f$.

It remains to prove that f is unique. Suppose that F is also a monic irreducible polynomial $f(X)$ such $F(\alpha) = 0$. Then we have just seen that f divides F, i.e. $F = fg$ for some $g \in \mathbb{Q}[X]$. But F is irreducible, so this forces f or g to be a unit; f is not a constant polynomial, so it is not a unit. So g is a unit, i.e. constant polynomial; as F and f are both monic, this forces $g = 1$, i.e. $F = f$. □

Definition 3.7. If $\alpha \in \mathbb{Q}^{\text{alg}}$ then the unique monic, irreducible polynomial $f(X) \in \mathbb{Q}[X]$ satisfying $f(\alpha) = 0$ is called *the minimal polynomial* of α. The *degree* of α is defined to be the degree of its minimal polynomial.

If $\alpha \in \mathbb{Q}^{\text{alg}}$, write $\mathbb{Q}(\alpha) = \{h(\alpha) : h \in \mathbb{Q}[X]\}$; similarly, if $\alpha \in \mathbb{Z}^{\text{alg}}$, write $\mathbb{Z}(\alpha) = \{h(\alpha) : h \in \mathbb{Z}[X]\}$. These are obviously both subrings of $\mathbb{C}$: indeed, $\mathbb{Q}(\alpha)$ is the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and α, while $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and α.

Example 3.8. Every element of $\mathbb{Q}(\sqrt{-5})$ (resp. $\mathbb{Z}[\sqrt{-5}]$) can be written as $a + b\sqrt{-5}$ for some $a, b \in \mathbb{Q}$ (resp. $a, b \in \mathbb{Z}$). The following proposition demonstrates this is full generality.

Proposition 3.9. *Let $\alpha \in \mathbb{Q}^{alg}$, with minimal polynomial $f(X)$ and degree d. Then*

(i) As a vector space over $\mathbb{Q}$, $\mathbb{Q}(\alpha)$ has basis $1, \alpha, \ldots, \alpha^{d-1}$.

(ii) $\mathbb{Q}(\alpha)$ is a field.

Proof. (i). Let $\beta \in \mathbb{Q}(\alpha)$; we will show that β can be written as a sum, with rational coefficients, of $1, \alpha, \ldots, \alpha^{d-1}$. Well, $\beta = h(\alpha)$ for some $h \in \mathbb{Q}[X]$ and division of polynomials implies that there exist $q, r \in \mathbb{Q}[X]$ such that $h = qf + r$ and such that $\deg r < d$ (or perhaps $r = 0$). Thus

$$\beta = h(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$$

since $f(\alpha) = 0$. But $r(X) = a_0 + \cdots + a_{d-1}X^{d-1}$ for some $a_0, \ldots, a_{d-1} \in \mathbb{Q}$, and so $\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$, as required.

Secondly we must check that $1, \alpha, \ldots, \alpha^{d-1}$ are linearly independent over $\mathbb{Q}$. If we have a relation

$$b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1} = 0$$

for some $b_0, \ldots, b_{d-1} \in \mathbb{Q}$, and so $g(\alpha) = 0$, where $g(X) := b_0 + \cdots + b_{d-1}X^{d-1}$. Therefore $f(X)|g(X)$; but $\deg g < \deg f$, so this is possible only if $g = 0$, i.e. $b_0 = \cdots = b_{d-1} = 0$. This completes the proof of part (i).

(ii). Let $\beta \in \mathbb{Q}(\alpha)$ be non-zero; then $\beta = h(\alpha)$ for some $h \in \mathbb{Q}[X]$ which is not divisible by $f(X)$ (for else $h(\alpha) = 0$). Since f is irreducible, h is coprime to f and so the division algorithm implies that there exist $A, B \in \mathbb{Q}[X]$ such that $Af + Bh = 1$. Evaluating at α,

$$1 = A(\alpha)f(\alpha) + B(\alpha)h(\alpha) = B(\alpha)h(\alpha)$$

and so $h(\alpha)^{-1} = B(\alpha) \in \mathbb{Q}(\alpha)$. □

Example 3.10.

(i) The minimal polynomial of $\sqrt{-5}$ is X^2+5. Indeed, this polynomial is irreducible in $\mathbb{Q}[X]$ (why? Since it has degree two, if it were not irreducible then it would have a linear factor so it would have a root in $\mathbb{Q}$, which it doesn't), it is monic, and $\sqrt{-5}$ is clearly a root of it.

(ii) Let $\omega = \frac{-1+\sqrt{-3}}{2} (= e^{2\pi i/3})$. We saw in lecture 1 that $\omega^3 = 1$ (this is clear once you know that $\omega = e^{2\pi i/3}$). But X^3-1 is not the minimal polynomial of ω for the following reason: $X^3-1 = (X-1)(X^2+X+1)$, so $0 = (\omega-1)(\omega^2+\omega+1)$. Since $\omega - 1 \neq 0$, we deduce $\omega^2+\omega+1=0$, and in fact X^2+X+1 is the minimal polynomial of ω (why? As in the previous case, it is enough to observe that otherwise $\omega \in \mathbb{Q}$).

Typically it is enough to study minimal polynomials of algebraic integers, not arbitrary algebraic numbers. We must review some related results from Algebra II (Fraleigh §45):

If R is a UFD, recall that a polynomial $f(X) \in R[X]$ is called *primitive* when the gcd of its coefficients is equal to 1. Gauss' lemma states that the product of two primitive polynomials in $R[X]$ is again primitive. Moreover,

Lemma 3.11. *Let R be a UFD, with field of fractions F. Suppose that $f \in R[X]$ is a monic polynomial, and that $g, h \in F[X]$ are monic polynomials satisfying $f = gh$. Then g, h actually have coefficients in R.*

Proof. Write each coefficient of g as a fraction in lowest terms, and let $c \in R$ be the least common multiple of the denominators of all coefficients. Then cg has coefficients in R and is primitive. Similarly there is $d \in R$ such that dh is a primitive polynomial in $R[X]$.

By Gauss' lemma, $cg(X)dh(X) = cdf(X)$ must be primitive. But every coefficient of cdf is obviously divisible by cd; therefore cd is a unit, so each of c and d is a unit. Therefore $g = c^{-1}(cg)$, $h = d^{-1}(dh)$ have coefficients in R. □

We may now prove:

Proposition 3.12. *If $\alpha \in \mathbb{Z}^{alg}$ then its minimal polynomial (which by definition belongs to $\mathbb{Q}[X]$) actually belongs to $\mathbb{Z}[X]$.*

Proof. Let $f(X) \in \mathbb{Q}[X]$ be the irreducible polynomial of α. Since α is an algebraic integer, there is a monic polynomial $g(X) \in \mathbb{Z}[X]$ such that $g(\alpha) = 0$. By proposition 3.6, f divides g in $\mathbb{Q}[X]$; i.e. there exists $h(X) \in \mathbb{Q}[X]$ such that $fh = g$. By the previous lemma, $f, h \in \mathbb{Z}[X]$. □

Corollary 3.13. *Suppose that $\alpha \in \mathbb{Q}$ is an algebraic integer; then $\alpha \in \mathbb{Z}$.*

Proof. The minimal polynomial of α is $X - \alpha$, which has integer coefficients if and only if $\alpha \in \mathbb{Z}$. □

While we are studying irreducible polynomials with coefficients in $\mathbb{Z}$, now is a convenient time to recall the following test:

Theorem 3.14 (Eisenstein's criterion)**.** *Let $f(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ be a polynomial which satisfies, for some prime number p,*

$$p \not| a_n, \quad p | a_i \text{ for } i = 0, \ldots, n-1, \quad p^2 \not| a_0.$$

Then f is irreducible.

Proof. Should have been proved in Algebra II (Fraleigh 23.15). □

The most important application of Eisenstein's lemma is to the following example:

Example 3.15. Let $p \geq 3$ be prime. Then the minimal polynomial of the algebraic integer $\zeta = e^{2\pi i/p}$ is $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

The proof sometimes appears in algebra II, and always in algebra III, but here it is in case you haven't seen it:

Proof. Since ζ is a root of the polynomial

$$0 = \zeta^p - 1 = (\zeta - 1)\Phi_p(\zeta)$$

but $\zeta - 1 \neq 0$, we see that $\Phi_p(\zeta) = 0$. Also, the polynomial is monic, so it remains only to prove that it is irreducible in $\mathbb{Q}[X]$.

Write $\Psi_p(X) = \Phi_p(X+1)$; then it is enough to prove that Ψ_p is irreducible, for any factorization of Φ_p, e.g. $\Phi_p(X) = f(X)g(X)$, would result in a factorization of $\Psi_p(X)$: $\Psi_p(X) = f(X+1)g(X+1)$. Well,

$$X\Psi_p(X) = X\Phi_p(X+1) = (X+1)^p - 1 = X^p + \sum_{k=2}^{p-1} \binom{p}{k} X^k + pX + 1 - 1,$$

and so

$$\Psi_p(X) = X^{p-1} + \sum_{k=2}^{p-1} \binom{p}{k} X^{k-1} + p.$$

Next use the (easy-to-prove) fact that $p \mid \binom{p}{k}$ in $\mathbb{Z}$ whenever k is an integer in the range $1 \leq k \leq p-1$; this shows that $\Psi_p(X)$ satisfies Eisenstein's criterion, and so is irreducible. □

Finally in this section of the basics of algebraic numbers, we study conjugates:

Definition 3.16. Algebraic numbers α, β are said to be *conjugate* if and only if they have the same minimal polynomial. Thus *the conjugates* of fixed algebraic number α are the roots of the minimal polynomial of α.

Remark 3.17. (i) This is an equivalence relation on the set of algebraic numbers.

(ii) Two rational numbers are conjugate if and only if they are equal (as the minimal polynomial of $r \in \mathbb{Q}$ is $X - r$).

(iii) If α, β are conjugate and α is an algebraic integer then so is β (for proposition 3.12 implies that the minimal polynomial of α has integer coefficients, so β satisfies a monic polynomial with integer coefficients).

Lemma 3.18. *(i) Let $f \in \mathbb{Q}[X]$ be monic and irreducible of degree d. Then f has d distinct roots in $\mathbb{C}$.*

(ii) Let α be an algebraic number of degree d, with minimal polynomial $f(X)$. Then there exist exactly d (distinct) complex numbers $\alpha_1, \ldots, \alpha_d$ which are conjugate to α, and

$$f(X) = (X - \alpha_1) \ldots (X - \alpha_d).$$

Proof. (i) Since $\mathbb{C}$ is algebraically closed, $f(X)$ factors into linear terms over $\mathbb{C}$:

$$f(X) = (X - \alpha_1) \ldots (X - \alpha_d)$$

For a contradiction suppose that $\alpha_i = \alpha_j$ for some $i \neq j$; write $\alpha = \alpha_i$. Then $f(X) = (X - \alpha)^2 h(X)$ where $h(X) = \prod_{r \neq i,j} (X - \alpha_r)$, and so

$$f'(X) = 2(X - \alpha)h(X) + (X - \alpha)^2 h'(X),$$

whence $f'(\alpha) = 0$. But $f'(X)$ is a polynomial with rational coefficients and $f(X)$ is the minimal polynomial of α; therefore $f | f'$. As $\deg f' < \deg f$, this is only possible if $f' = 0$, which is absurd as it has top degree term dX^{d-1}.

(ii) As in (i) write $f(X) = (X - \alpha_1) \ldots (X - \alpha_d)$. If β is a conjugate of α then it is a root of $f(X)$ and therefore equals α_i for some i. Conversely, each α_i has minimal polynomial $f(X)$ and so is a conjugate of α. □

Example 3.19. (i) The conjugates of $\sqrt{5}$ are $\sqrt{5}$ and $\sqrt{-5}$.

It is tedious, though straightforward, to check that

$$f(X) := (X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X + \sqrt{2} + \sqrt{3})$$

has rational coefficients; indeed, it equals the polynomial $X^4 - 10X^2 + 1$ which we calculated in example 3.5. Here is a way to check that $f(X)$ is irreducible over $\mathbb{Q}$. If not then $f = gh$ with $g, h \in \mathbb{Q}[X]$ monic polynomials. Since f does not have any rational roots, g, h are quadratic, hence equal to

$$(X - \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})$$

or

$$(X - \sqrt{2} - \sqrt{3})(X + \sqrt{2} - \sqrt{3})$$

or

$$\vdots$$

It can be directly checked that none of these have coefficients in $\mathbb{Q}$. So f is irreducible.

Therefore f is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ and so the conjugates of $\sqrt{2} + \sqrt{3}$ are

$$\sqrt{2} + \sqrt{3},\ \sqrt{2} - \sqrt{3},\ -\sqrt{2} + \sqrt{3},\ -\sqrt{2} - \sqrt{3}.$$

Corollary 3.20. *α an algebraic number, with minimal polynomial $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ and conjugates $\alpha_1, \ldots, \alpha_d$. Then*

$$\alpha_1 \ldots \alpha_d = (-1)^d a_0$$

and

$$\alpha_1 + \cdots + \alpha_d = -a_{d-1}.$$

Proof. Immediate from the identity $f(X) = (X - \alpha_1) \cdots (X - \alpha_d)$. □

4 ALGEBRAIC NUMBER FIELDS

The following definition introduces the main object of study in the rest of the course. We begin by remarking that if F is a subfield of $\mathbb{C}$, then it automatically contains $0, \pm 1, \pm 2, \ldots$ and so contains $\mathbb{Q}$.

Definition 4.1. An *algebraic number field* is a subfield F of $\mathbb{C}$ which has finite dimension as a vector space over $\mathbb{Q}$. The *ring of integers* of F is $\mathfrak{D}_F = F \cap \mathbb{Z}^{\text{alg}}$, i.e., those elements of F which are algebraic integers.

Remark 4.2. We observe some elementary but important remarks and examples:

(i) Notice that $V = F$ is a finite dimensional $\mathbb{Q}$-vector space contained inside $\mathbb{C}$ such that $\alpha V \subseteq V$ for all $\alpha \in F$; according to the "standard test", lemma 3.3, this means that $\alpha \in \mathbb{Q}^{\text{alg}}$. So $F \subseteq \mathbb{Q}^{\text{alg}}$.

(ii) $\mathfrak{D}_F$ is a subring of $\mathbb{C}$ containing $\mathbb{Z}$. Rough philosophy: arithmetic properties of $\mathfrak{D}_F$ encodes arithmetic in $\mathbb{Z}$ which we could not otherwise see.

(iii) Consider the case $F = \mathbb{Q}$; then $\mathfrak{D}_{\mathbb{Q}} = \mathbb{Q} \cap \mathbb{Z}^{\text{alg}} = \mathbb{Z}$ by corollary 3.13.

Example 4.3. Let α be an algebraic number; then $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{C}$ of dimension $\deg \alpha$ over $\mathbb{Q}$ by proposition 3.9. Therefore $\mathbb{Q}(\alpha)$ is an algebraic number field. (In fact, the "Primitive element theorem", which is sometimes in Alg III, implies that if F is an algebraic number field then there exists an algebraic number α such that $F = \mathbb{Q}(\alpha)$. But we will not need to know this.)

Example 4.4. Very important example! Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free, and put $F = \mathbb{Q}(\sqrt{d})$. Let $\alpha \in \mathbb{Q}(\sqrt{d})$; you are proving on the current homework that α is an algebraic integer if and only if

(i) (Case: $d \equiv 2$ or $3 \bmod 4$) $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$.

(ii) (Case: $d \equiv 1 \bmod 4$) $\alpha = a + b\frac{-1+\sqrt{d}}{2}$ for some $a, b \in \mathbb{Z}$.

Therefore,

$$\mathfrak{D}_F = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \bmod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{d}}{2} \neq \mathbb{Z}[\sqrt{d}] & d \equiv 1 \bmod 4 \end{cases}$$

The case $d \equiv 1 \bmod 4$ demonstrates a very important principle: *if α is an algebraic integer then the ring of integers of the number field $\mathbb{Q}(\alpha)$ may be strictly bigger than $\mathbb{Z}[\alpha]$*. We will see that $\mathfrak{D}_F$ is a much more interesting ring to study.

Lemma 4.5. *If α is an algebraic number then there is a non-zero integer m such that $m\alpha$ is an algebraic integer. If F is a number field, then the field of fractions of $\mathfrak{D}_F$ is F.*

Proof. First claim on the homework. Second claim easily follows. □

So every number field F comes equipped with this special subring $\mathfrak{D}_F$ of which it is the field of fractions; we will see that $\mathfrak{D}_F$ is a very rich ring which can give us interesting results about ordinary integers themselves.

We now spend some time covering three examples in detail, focusing on factorisation properties in rings of integers. First recall the following results from Alg II:

Theorem 4.6 (Fraleigh §45, §46)**.** *Let R be an integral domain.*

(i) If R is a ED then it is a PID.

(ii) If R is a PID then it is a UFD.

A non-zero element $a \in R$ is called prime *if and only if the principal ideal $\langle a \rangle$ generated by it is a prime ideal. If a is prime then it is irreducible; the converse is true in UFDs.*

Exercise 4.1. Let N be a positive integer.

(i) Let d be a positive integer. Prove that there are only finitely many algebraic integers α of degree d such that all conjugates of α have complex absolute value $\leq N$.

(ii) Let F be a number field. Deduce that there are only finitely many $\alpha \in \mathfrak{D}_F$ such that all conjugates of α have complex absolute value $\leq N$.

4.1 First example: Gaussian integers

We are going to study three examples of number fields F and their rings of integers $\mathfrak{D}_F$; in each example we write $N(\alpha) = \alpha\overline{\alpha}$, for $\alpha \in F$. This is a special case of the so-called *norm map* $N_{F/\mathbb{Q}}$, which we will introduce in general after the examples.

Let $F = \mathbb{Q}(i)$ where $i = \sqrt{-1}$. Since $-1 \equiv 3 \bmod 4$, the previous example tell us that the ring of integers of F is

$$\mathfrak{D}_F = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i,$$

the subring of $\mathbb{C}$ which you have previously encountered under the name *Gaussian integers* [Fraleigh §47]. You also learnt that it is a Euclidean domain, with Euclidean norm

$$N(\alpha) = \alpha\overline{\alpha},$$

where $\overline{\ }$ denotes complex conjugation. In other words, $N(a + bi) = a^2 + b^2$. By the previous theorem, the ring of Gaussian integers is also a PID and a UFD.

4.2 SECOND EXAMPLE: $\mathbb{Z}[\omega]$ WHERE $\omega = e^{2\pi i/3}$

Several times we have encountered

$$\omega = \frac{-1+\sqrt{-3}}{2} = e^{2\pi i/3} \in \mathbb{C}$$

We are going to study the ring of integers of the number field $F = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. According to example 4.4, since $-3 \equiv 1 \bmod 4$, the ring of integers of F is

$$\mathfrak{D}_F = \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{-3}}{2} = \mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z}[\omega] \neq \mathbb{Z}[\sqrt{-3}].$$

You will prove in the homework that if we define $N(\alpha) = \alpha\overline{\alpha}$ for $\alpha \in F$, just as in the case of Gaussian integers, then N is a Euclidean norm on $\mathfrak{D}_F$. Therefore $\mathfrak{D}_F$ is a Euclidean domain, and hence a PID and UFD by the earlier theorem.

4.3 THIRD EXAMPLE: $\mathbb{Z}[\sqrt{-5}]$

In the previous two examples, we saw that $\mathfrak{D}_F$ was a Euclidean domain with the Euclidean norm given by $N(\alpha) = \alpha\overline{\alpha}$; this is *not what typically happens*, even for similar looking extensions.

Next we consider the example $F = \mathbb{Q}(\sqrt{-5})$. Since $-5 \equiv 3 \bmod 4$, the ring of integers of F is

$$\mathfrak{D}_F = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$$

Then $N(a+b\sqrt{-5}) = a^2 + 5b^2$; it is important to notice that if $\alpha \in \mathbb{Z}[\sqrt{-5}]$ then $N(\alpha) \in \mathbb{Z}_{\geq 0}$.

The next lemma analyses some elements of $\mathbb{Z}[\sqrt{-5}]$:

Lemma 4.7. *The only units in $\mathbb{Z}[\sqrt{-5}]$ are $-1, 1$. The elements $3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ are all irreducible.*

Proof. Firstly, $-1, 1$ are certainly units. Conversely, suppose $u = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is a unit; then there is $v \in \sqrt{-5}$ such that $uv = 1$ and so

$$1 = N(1) = N(uv) = N(u)N(v).$$

Since $N(u), N(v) \in \mathbb{Z}_{\geq 0}$, we deduce $N(u) = N(v) = 1$. Therefore $a^2 + 5b^2 = 1$, which is only possible if $b = 0$ and $a = -1, 1$; so $\alpha = -1, 1$, as required.

This argument also shows that $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is any element satisfying $N(\alpha) = 1$, then α is a unit.

Now we prove the claim that the given elements are irreducible (the argument is similar for each number):

(i) 3. Suppose 3 is not irreducible; then $3 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ such that neither α or β are units. Therefore $N(\alpha), N(\beta) > 1$, and

$$9 = N(3) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 3$. Let $\alpha = a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$; then

$$3 = N(\alpha) = a^2 + 5b^2,$$

which is clearly impossible. This contradication shows that 3 must be irreducible.

(ii) 7. Suppose 7 is not irreducible; then $7 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ such that neither α or β are units. Therefore $N(\alpha), N(\beta) > 1$, and

$$49 = N(7) = N(\alpha)N(\beta).$$

So $N(\alpha) = N(\beta) = 7$. Let $\alpha = a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$; then

$$7 = N(\alpha) = a^2 + 5b^2,$$

which is clearly impossible. This contradication shows that 7 must be irreducible.

(iii) $1+2\sqrt{-5}$. Suppose $1+2\sqrt{-5}$ is not irreducible; then $1+2\sqrt{-5}=\alpha\beta$ for some $\alpha,\beta\in\mathbb{Z}[\sqrt{-5}]$ such that neither α or β are units. Therefore $N(\alpha),N(\beta)>1$, and

$$21=N(1+2\sqrt{-5})=N(\alpha)N(\beta),$$

so $N(\alpha)=3$ or 7. But calculations (i) and (ii) showed that this is impossible. This contradication shows that $1+2\sqrt{-5}$ must be irreducible.

(iv) $1-2\sqrt{-5}$. Repeat the previous argument verbatim.

This completes the proof. □

Theorem 4.8. *$\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.*

Proof. We have

$$(1+2\sqrt{-5})(1-2\sqrt{-5})=1+4\cdot 5=21$$

and also

$$3\cdot 7=21.$$

We have therefore produced two decompositions of 21 into irreducibles, so to prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD it is enough to show that 3 is not an associate of $1+2\sqrt{-5}$ or of $1-2\sqrt{-5}$, i.e. that there is no unit u such that $3=u(1+2\sqrt{-5})$ or $3=u(1-2\sqrt{-5})$. As the only units are $-1,1$, this is clear. □

Corollary 4.9. *There is no Euclidean norm on $\mathbb{Z}[\sqrt{-5}]$.*

Proof. If there were a Euclidean norm on $\mathbb{Z}[\sqrt{-5}]$ then it would be a Euclidean domain, hence a PID and a UFD; but this contradicts the previous theorem. □

4.4 Introductory tools for studying number fields: Norm, Trace, Discriminant, and Integral bases

Here we first explain the notion of *norm, trace, and discriminant* for any finite field extension; we will then specialise to the case of number fields and introduce in addition the notion of an *integral basis*. These ideas, which use little more than some linear algebra, will be used throughout the rest of the course, both theoretically and in examples.

Recall from Algebra that an *extension of fields* L/F is simply a pair of fields $F\subseteq L$, where F is a subfield of L. The usual algebraic operations make L into a vector space over F, and one defines the *degree of* L/F, denoted $|L:F|$, to be $\dim_F L$. One says that L/F is a *finite field extension* of *finite extension of fields* if and only if this dimension is finite.

For example, if α is an algebraic number, then $\mathbb{Q}(\alpha)/\mathbb{Q}$ is an extension of fields of degree $|\mathbb{Q}(\alpha):\mathbb{Q}|=\deg\alpha$, by proposition 3.9, hence is a finite field extension.

Remark 4.10 (Tower Law)**.** If L/M and M/F are finite extension fields, and $\omega_1,\dots,\omega_r$ is a basis for L/M, then $L=M\omega_1\oplus\cdots\oplus M\omega_r$. Taking dimensions as F-vector spaces gives $\dim_F L=r\dim_F M$, i.e.

$$|L:F|=|L:M||M:F|.$$

This is called the *tower law*. For example, if F is a number field and $\alpha\in F$, then

$$|F:\mathbb{Q}|=|F:\mathbb{Q}(\alpha)||\mathbb{Q}(\alpha):\mathbb{Q}|.$$

As $|\mathbb{Q}(\alpha):\mathbb{Q}|=\deg\alpha$ we see in particular that $\deg\alpha$ divides $|F:\mathbb{Q}|$.

Here is an example of how this is useful: Just above we saw that $\alpha=\sqrt{2}+\sqrt{3}$ has minimal polynomial X^4-10X^2+1, but here is quicker proof:

Put $F = \mathbb{Q}(\alpha)$ and notice that F contains $\sqrt{2}$ and $\sqrt{3}$. For example, $\frac{\alpha^3 - 9\alpha}{-4} = \sqrt{2}$. Therefore $\mathbb{Q}(\sqrt{2}) \subseteq F$ and the tower law implies

$$|F : \mathbb{Q}| = |F : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = |F : \mathbb{Q}(\sqrt{2})|2.$$

It is easy to check that no element of $\mathbb{Q}(\sqrt{2})$ is a square root of 3, i.e. $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and so $|F : \mathbb{Q}(\sqrt{2})| > 1$. It follows that $|F : \mathbb{Q}|$ is an even number which is > 2. But since $|F : \mathbb{Q}| = \deg \alpha \leq 4$ (as α does satisfy a degree 4 monic polynomial), we deduce that $\deg \alpha = 4$; so α has minimal polynomial of degree 4, and this minimal polynomial divides, and therefore equals $X^4 - 10X^2 + 1$.

4.4.1 Norm and Trace

Definition 4.11. Let L/F be a finite extension of fields, and let $\alpha \in L$. The *norm* of α, denoted $N_{L/F}(\alpha)$ is defined to be the determinant of the following F-linear map of vector spaces:

$$L \to L, \quad \beta \mapsto \alpha\beta.$$

I.e., $N_{L/F}(\alpha) = \det \phi_\alpha \in F$.

Similarly, the *trace* of α, denote $\mathrm{Tr}_{L/F}(\alpha)$, is defined to the trace of ϕ_α; i.e., $\mathrm{Tr}_{L/F}(\alpha) = \mathrm{Tr}\, \phi_\alpha \in F$.

In other words, let $\beta_1, \ldots, \beta_n$ be a basis of L as an F-vector space, write $\alpha\beta_i = \sum_{j=1}^n c_{i,j}\beta_j$ with $c_{i,j} \in F$, and put $C = (c_{i,j})$; then

$$N_{L/F}(\alpha) = \det C, \qquad \mathrm{Tr}_{L/F}(\alpha) = \mathrm{Tr}\, C = \sum_{i=1}^n c_{i,i}.$$

Example 4.12. Here we compute norms and traces of typical elements in some extensions.

(i) $\mathbb{C}/\mathbb{R}$ has basis $1, i$. If $x + iy \in \mathbb{C}$, with $x, y \in \mathbb{R}$, then the matrix for multiplication by $x + iy$ with respect to this basis is $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ whence

$$N_{\mathbb{C}/\mathbb{R}}(x + iy) = x^2 + y^2, \qquad \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(x + iy) = 2x.$$

(ii) $\mathbb{Q}(i)/\mathbb{Q}$ has basis $1, i$, and exactly the same argument as in the previous example shows that

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy) = x^2 + y^2, \qquad \mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy) = 2x,$$

for $x, y \in \mathbb{Q}$.

(iii) $\mathbb{Q}(\omega)/\mathbb{Q}$, where $\omega^2 + \omega + 1 = 0$. This has basis $1, \omega$, and multiplication by $a + b\omega$ in this basis is given by the matrix

$$\begin{pmatrix} a & -b \\ b & a - b \end{pmatrix}.$$

So

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(a + b\omega) = a^2 + b^2 - ab, \qquad \mathrm{Tr}_{\mathbb{Q}(\omega)/\mathbb{Q}}(a + b\omega) = 2a - b.$$

The next two properties summarise the main theoretical properties of the Norm and Trace for a finite extension of fields L/F:

Proposition 4.13 (Main theoretic properties of the Norm)**.** *$N_{L/F} : L \to F$ has the following properties:*

(i) $N_{L/F}(\alpha_1\alpha_2) = N_{L/F}(\alpha_1)N_{L/F}(\alpha_2)$ *for* $\alpha_1, \alpha_2 \in L$.

(ii) $N_{L/F}(a) = a^{|L:F|}$ *if* $a \in F$.

(iii) $N_{L/F}(\alpha) = 0$ *if and only if* $\alpha = 0$.

(iv) If M *is an intermediate field between* L *and* F*, then* $N_{L/F} = N_{M/F} \circ N_{L/M}$.

Proof. For any $\alpha \in F$, let

$$\phi_\alpha : L \to L, \quad \beta \mapsto \alpha\beta$$

be the F-linear map 'multiplication by α', so that $N_{L/F}\alpha = \det \phi_\alpha$.

(i): For any $\beta \in F$,

$$\phi_{\alpha_1}(\phi_{\alpha_2}(\beta) = \alpha_1\alpha_2\beta = \phi_{\alpha_1\alpha_2}(\beta),$$

and so $\phi_{\alpha_1} \circ \phi_{\alpha_2} = \phi_{\alpha_1\alpha_2}$. Therefore

$$N_{L/F}(\alpha_1)N_{L/F}(\alpha_2) = \det \phi_{\alpha_1} \cdot \det \phi_{\alpha_2} = \det(\phi_{\alpha_1} \circ \phi_{\alpha_2}) = \det(\phi_{\alpha_1\alpha_2}) = N_{L/F}(\alpha_1\alpha_2).$$

(ii): If $a \in F$ then the matrix for ϕ_a, with respect to any basis $\alpha_1, \ldots, \alpha_n$, of L/F is the $n \times n$ diagonal matrix with a's all along the diagonal; this has determinant a^n.

(iii): If $\alpha = 0$ then $\phi_\alpha = 0$ so $N_{L/F}(\alpha) = \det \phi_\alpha = 0$; conversely, if $\alpha \neq 0$ then $1 = N_{L/F}(1) = N_{L/F}(\alpha\alpha^{-1}) = N_{L/F}(\alpha)N_{L/F}(\alpha^{-1})$, so $N_{L/F}(\alpha) \neq 0$.

(iv): We only sketch the proof in the special case that $\alpha \in M$. Let $\omega_1, \ldots, \omega_r$ be a basis for L/M; then (by the very definition of what a basis is), $L = M\omega_1 \oplus \cdots \oplus M\omega_r$. Since

$$\phi_\alpha(M\omega_i) = \alpha M\omega_i \subseteq M\omega_i,$$

for each i, we see that ϕ_α restricts to each F-vector space $M\omega_i$ and that

$$\phi_\alpha = \phi_\alpha|_{M\omega_1} \oplus \cdots \oplus \phi_\alpha|_{M\omega_n}.$$

By a 'block diagonal' argument, we see that

$$\det(\phi_\alpha) = \det(\phi_\alpha|_M)^r, \quad \text{i.e. } N_{L/M}(\alpha) = N_{M/F}(\alpha)^{|L:M|}.$$

Therefore

$$N_{L/M}(\alpha) = N_{M/F}(\alpha^{|F:M|}) = N_{M/F}(N_{L/M}(\alpha)).$$

□

Proposition 4.14 (Main theoretic properties of the Trace)**.** $\mathrm{Tr}_{L/F} : L \to F$ *has the following properties:*

(i) $\mathrm{Tr}_{L/F}(\alpha_1 + \alpha_2) = \mathrm{Tr}_{L/F}(\alpha_1) + \mathrm{Tr}_{L/F}(\alpha_2)$ *for* $\alpha_1, \alpha_2 \in L$.

(ii) $\mathrm{Tr}_{L/F}(a\alpha) = a\,\mathrm{Tr}_{L/F}(\alpha)$ *for* $a \in F$, $\alpha \in L$.

(iii) $\mathrm{Tr}_{L/F}(a) = |L : F|a$ *if* $a \in F$.

(iv) If M *is an intermediate field between* L *and* F*, then* $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{M/F} \circ \mathrm{Tr}_{L/M}$.

Proof. Copy the previous proof, replacing addition by multiplication. □

Remark 4.15 (Relation to Galois theory)**.** Readers who know Galois theory may find the following formulae (exercise!) useful, though we will not need them: If L/F is a finite Galois extension of fields and $\alpha \in L$, then

$$N_{L/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(\alpha), \qquad \mathrm{Tr}_{L/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(\alpha)$$

More generally, if L/F is not necessarily Galois, then these formulae remain true if we let σ run over all F-linear field embeddings of L into a fixed normal extension of F containing L, e.g. the normal closure of L/F.

In the special case of a number field, the norm and trace maps are compatible with the ring of integers:

Proposition 4.16. *F a number field, and $\alpha \in \mathfrak{O}_F$. Then $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha)$ and $N_{F/\mathbb{Q}}(\alpha)$ belong to $\mathbb{Z}$.*

Proof. Let $M = \mathbb{Q}(\alpha)$; then the previous two propositions imply that

$$N_{F/\mathbb{Q}}(\alpha) = N_{M/\mathbb{Q}}(\alpha)^{|F:M|}, \qquad \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = |F : M| \,\mathrm{Tr}_{M/\mathbb{Q}}(\alpha)$$

Therefore it remains only to show that $N_{M/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{M/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$; this is left to the homework. □

4.4.2 Discriminant

Using the trace maps we can construct an interesting invariant known as the discriminant:

Definition 4.17. L/F a finite extension of fields, and $\alpha_1, \ldots, \alpha_n \in L$ some elements. Then the associated *discriminant* is

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/F}(\alpha_i \alpha_j))$$

Example 4.18. Here is a computation of a discriminants:

Let $d \in \mathbb{Z} \setminus \{0, 1\}$ not be a cube, and set $F = \mathbb{Q}(d^{1/3})$. Then $\Delta(1, d^{1/3}, d^{2/3})$ is the determinant of the matrix

$$\begin{pmatrix} \mathrm{Tr}_{F/\mathbb{Q}} 1 & \mathrm{Tr}_{F/\mathbb{Q}} d^{1/3} & \mathrm{Tr}_{F/\mathbb{Q}} d^{2/3} \\ \mathrm{Tr}_{F/\mathbb{Q}} d^{1/3} & \mathrm{Tr}_{F/\mathbb{Q}} d^{2/3} & \mathrm{Tr}_{F/\mathbb{Q}} d \\ \mathrm{Tr}_{F/\mathbb{Q}} d^{2/3} & \mathrm{Tr}_{F/\mathbb{Q}} d & \mathrm{Tr}_{F/\mathbb{Q}} d^{4/3} \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{pmatrix}$$

So $\Delta(1, d^{1/3}, d^{2/3}) = -27d^2$.

The next two results are the main theoretic properties of the disciminant:

Proposition 4.19 (Discriminant detects bases)**.** *L/F a finite extension of fields, and $\alpha_1, \ldots, \alpha_n \in L$. If $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ then $\alpha_1, \ldots, \alpha_n$ are linearly independent over F. Conversely, if $\alpha_1, \ldots, \alpha_n$ form a basis for L/F, and F has characteristic zero, then $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Proof. Suppose that $\alpha_1, \ldots, \alpha_n$ are linearly dependent; so there are $a_1, \ldots, a_n \in F$, not all zero, such that $\sum_{i=1}^n a_i \alpha_i = 0$. Therefore, for any j,

$$0 = \mathrm{Tr}_{L/F}(\alpha_j \sum_{i=1}^n a_i \alpha_i) = \sum_{i=1}^n a_i \,\mathrm{Tr}(\alpha_i \alpha_j),$$

which can be rewritten as

$$(\mathrm{Tr}(\alpha_i \alpha_j)) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0,$$

where the column vector is non-zero. So $\det(\mathrm{Tr}(\alpha_i \alpha_j)) = 0$, as required.

Conversely, for a contradiction suppose that $\alpha_1, \ldots, \alpha_n$ are a basis for L/F and that $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. So the F-linear map $L \to L$ attached to the matrix $(\mathrm{Tr}(\alpha_i \alpha_j))$ has a kernel, i.e. there are $a_1, \ldots, a_n \in F$, not all zero, such that $\sum_{i=1}^n a_i \,\mathrm{Tr}(\alpha_i \alpha_j) = 0$. Set $\alpha := \sum_{i=1}^n a_i \alpha_i \in L$; this is non-zero since $\alpha_1, \ldots, \alpha_n$ form a basis and $a_1, \ldots, a_n$ are not all zero. However, if $\beta \in L$, then we may write $\beta = \sum_{j=1}^n b_j \alpha_j$ for some $b_1, \ldots, b_n \in F$, and we deduce that

$$\mathrm{Tr}_{L/F}(\beta\alpha) = \mathrm{Tr}_{L/F}(\sum_{j=1}^n b_j \alpha_j \alpha) = \sum_{j=1}^n b_j \,\mathrm{Tr}_{L/F}(\alpha \alpha_j) = \sum_{j=1}^n b_j \sum_{i=1}^n a_i \,\mathrm{Tr}_{L/F}(\alpha_i \alpha_j) = 0.$$

In particular, taking $\beta = \alpha^{-1}$, we have just shown that $n = \mathrm{Tr}_{L/F}(1) = 0$ *in the field F*, which contradicts the assumption that $\mathrm{char}\, F = 0$. □

Proposition 4.20 (Change of basis formula for discriminant)**.** *L/F a finite extension of fields, with bases $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_n$. Let C be the change of basis matrix from the β-basis to the α-basis, i.e. $C = (c_{i,j})$ where $\alpha_i = \sum_{j=1}^n c_{i,j}\beta_j$ with $c_{i,j} \in F$. Then*

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(C)^2 \Delta(\beta_1, \dots, \beta_n).$$

Proof. We have

$$\alpha_i \alpha_k = \sum_{j=1}^n \sum_{l=1}^n c_{i,j} c_{k,l} \beta_j \beta_l,$$

and taking traces gives

$$\mathrm{Tr}_{L/F}(\alpha_i \alpha_k) = \sum_{j=1}^n \sum_{l=1}^n c_{i,j} \, \mathrm{Tr}_{L/F}(\beta_j \beta_l) c_{k,l}.$$

In other words,

$$A = CBC^t,$$

where

$$A = (\mathrm{Tr}_{L/F}(\alpha_i \alpha_j)$$
$$B = (\mathrm{Tr}_{L/F}(\beta_i \beta_j))$$

Take determinants to get the desired result. □

4.4.3 Integral bases

Over the next few results we introduce the notion of an *integral basis* for a number field; this will be an important tool in proving all the main results in the next section.

Definition 4.21. Let F be a number field, I a non-zero ideal of $\mathfrak{D}_F$, and $\omega_1, \dots, \omega_n \in F$ a basis for $F/\mathbb{Q}$. Then $\omega_1, \dots, \omega_n$ is called an *I-integral basis* if and only if $I = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$.

In other words, if an element $\alpha \in F$ is expressed in the basis as $\alpha = \sum_{i=1}^n c_i \omega_i$, where $c_i \in \mathbb{Q}$, then

$$\alpha \in I \iff c_i \in \mathbb{Z} \text{ for all } i.$$

If $I = \mathfrak{D}_F$ (which is by far the most important case), simply say *integral basis* instead. So in this case, $\mathfrak{D}_F = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$; in other words, the isomorphism of $\mathbb{Q}$-vector spaces $\mathbb{Q}^n \xrightarrow{\sim} F$, $(c_i) \mapsto \sum_i c_i \omega_i$ restricts to an isomorphism of abelian groups $\mathbb{Z}^n \xrightarrow{\sim} \mathfrak{D}_F$.

Lemma 4.22. *F a number field.*

(i) If I is a non-zero ideal of $\mathfrak{D}_F$, then I contains a basis for $F/\mathbb{Q}$.

(ii) If $\omega_1, \dots, \omega_n \in \mathfrak{D}_F$ are a basis for $F/\mathbb{Q}$, then $\Delta(\omega_1, \dots, \omega_n)$ is a non-zero integer.

Proof. (i): Let $\alpha_1, \dots, \alpha_n \in F$ be a basis for $F/\mathbb{Q}$; by lemma 4.5 there is a non-zero integer m such that $m\alpha_i \in \mathfrak{D}_F$ for all i. Let $\beta \in I$ be non-zero. Then multiplication by $m\beta$ is an F-linear isomorphism $L \xrightarrow{\sim} L$, so $m\beta\alpha_1, \dots, m\beta\alpha_n$ is also a basis for $F/\mathbb{Q}$, and all terms belong to I.

(ii): By proposition 4.16, the matrix $(\mathrm{Tr}_{F/\mathbb{Q}}(\omega_i \omega_j))$ has entries in $\mathbb{Z}$, so its determinant $\Delta(\omega_1, \dots, \omega_n)$ is in $\mathbb{Z}$; it is non-zero by proposition 4.19. □

Proposition 4.23. *F a number field and I a non-zero ideal of $\mathfrak{D}_F$. Then an I-integral basis exists.*

Proof. Among all possible bases $\omega_1, \ldots, \omega_n$ of $F/\mathbb{Q}$ which are contained within I, pick one which minimises $|\Delta(\omega_1, \ldots, \omega_n)|$. This makes sense by the previous lemma!

Certainly $\mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_m \subseteq I$, so we must prove the converse. Let $\alpha \in I$ and write $\alpha = \sum_{i=1}^n a_i\omega_i$ for some $a_i \in \mathbb{Q}$; we must prove that $a_i \in \mathbb{Z}$ for all i.

If not, then by rearranging (for simplicity of notation), we may assume that $a_1 \notin \mathbb{Z}$. So $a_1 = \lfloor a_1 \rfloor + \theta$ for some $0 < \theta < 1$. Then

$$\omega_1' := \omega_1' - \lfloor a_1 \rfloor \omega_1 = \theta\omega_1 + a_2\alpha_2 + \cdots + a_n\omega_n,\ \omega_2' := \omega_2, \ldots,\ \omega_n' := \omega_n$$

is also a basis for $F/\mathbb{Q}$ belonging to I. The change of basis matrix $C = (c_{i,j})$ from the ω-basis to the ω'-basis (i.e. $\omega_i' = \sum_{j=1}^n c_{i,j}\omega_j$ with $c_{i,j} \in \mathbb{Q}$) is

$$C = \begin{pmatrix} \theta & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

which has determinant θ^2. According to proposition 4.20,

$$|\Delta(\omega_1', \ldots, \omega_n')| = \theta^2 |\Delta(\omega_1, \ldots, \omega_n)|,$$

contradicting the minimality assumption. □

Exercise 4.2. Let F be a number field, and let $\omega_1, \ldots, \omega_n \in \mathfrak{D}_F$ be an integral basis. The *absolute discriminant of* F is defined by

$$\Delta_F := \Delta(\omega_1, \ldots, \omega_n).$$

Using the change of basis formula for the discriminant, show that Δ_F does not depend on the chosen integral basis.

If $d \in \mathbb{Z} \setminus \{0, 1\}$ is a square-free integer and $F = \mathbb{Q}(\sqrt{d})$, show that

$$\Delta_F = \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod 4 \\ d & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

4.4.4 Applications of integral bases to number fields

In the next section we will use integral bases in almost all our proofs; here are two important applications already:

Definition 4.24. F a number field and I a non-zero ideal of $\mathfrak{D}_F$. The *norm of* I, denoted $N(I)$ is defined to be the size of $\mathfrak{D}_F/I$:

$$N(I) = \#\mathfrak{D}_F/I.$$

This definition makes sense because of the next lemma:

Proposition 4.25. *F a number field, and I a non-zero ideal of $\mathfrak{D}_F$. Then $\mathfrak{D}_F/I$ is a finite ring.*

Proof. Let $m \in I \cap \mathbb{Z}$ be non-zero (for example, let $\alpha \in I$ be non-zero, with minimal polynomial $f(X) = X^n + \cdots + a_0 \in \mathbb{Z}[X]$; then $a_0 = -a_1\alpha - \cdots - \alpha^n \in I \cap \mathbb{Z}$). Let $\omega_1, \ldots, \omega_n \in \mathfrak{D}_F$ be an integral basis for $F/\mathbb{Q}$.

For any $\alpha \in \mathfrak{D}_F/I$, write $\alpha = \sum_{i=1}^n c_i\omega_i$, with $c_i \in \mathbb{Z}$; then use Euclidean division to write $c_i = mq_i + r_i$ where $q_i \in \mathbb{Z}$ and $0 \leq r_i < q_i$. So now

$$\alpha = \sum_{i=1}^n (mq_i + r_i)\alpha_i = m(\sum_{i=1}^n q_i\alpha_i) + \sum_{i=1}^n r_i\alpha_i \equiv \sum_{i=1}^n r_i\alpha_i \bmod I.$$

Therefore any element of $\mathfrak{D}_F/I$ can be represented as $\sum_{i=1}^n r_i\alpha_i$, with $0 \leq r_i < m$; so $\mathfrak{D}_F/I$ is finite, with at most m^n elements.

(Quick proof: $\mathfrak{D}_F/\langle m\rangle \cong (\mathbb{Z}/m\mathbb{Z})^n$, and $\mathfrak{D}_F/I$ is a quotient of this ring since $m \in I$.) □

Our second applications of integral bases is to the cancellation of ideals:

Lemma 4.26 (Very useful!)**.** *F a number field, I a non-zero ideal of $\mathfrak{D}_F$ and $\alpha \in F$ such that $\alpha I \subseteq I$; then $\alpha \in \mathfrak{D}_F$.*

Proof. By the existence of an I-integral basis, I is a finitely-generated abelian group; since $\alpha I \subseteq I$, the standard test (lemma 3.3) implies α is an algebraic integer. So $\alpha \in F \cap \mathbb{Z}^{\text{alg}} = \mathfrak{D}_F$. □

Proposition 4.27. *F a number field, I, J non-zero ideals of $\mathfrak{D}_F$, and $\alpha \in \mathfrak{D}_F$ such that $\alpha I = JI$; then $J = \langle\alpha\rangle$.*

Proof. We first prove this in the case that $\alpha = 1$: so we assume $I = JI$ and we want to prove that $J = \mathfrak{D}_F$. Let $\omega_1, \ldots \omega_n \in I$ be an I-integral basis for $F/\mathbb{Q}$. Then $\omega_i \in I = JI$, so $\omega_i = \sum_{j=1}^n \beta_{i,j}\omega_j$ for some $\beta_{i,j} \in J$. Put $B = (\beta_{i,j})$; then

$$B\begin{pmatrix}\omega_1\\ \vdots \\ \omega_n\end{pmatrix} = \begin{pmatrix}\omega_1\\ \vdots \\ \omega_n\end{pmatrix}$$

and so $\det(\mathrm{Id} - B) = 0$. Expanding this determinant shows that 1 is a sum of products of terms from J, so $1 \in J$, i.e. $J = \mathfrak{D}_F$.

Now we prove the result for general α. Suppose $\beta \in J$; then

$$\frac{\beta}{\alpha}I \subseteq \frac{1}{\alpha}JI = \frac{1}{\alpha}\alpha I = I$$

and so the previous lemma implies that $\beta/\alpha \in \mathfrak{D}_F$. This is true for all $\beta \in J$, so $\alpha^{-1}J$ is a non-zero ideal of $\mathfrak{D}_F$. Moreover, $I = (\alpha^{-1}J)I$, so the special case $\alpha = 1$ implies that $\alpha^{-1}J = \mathfrak{D}_F$, i.e. $J = \langle\alpha\rangle$. □

The previous proposition will be significantly improved in theorem 5.11.

5 Main theoretic properties of $\mathfrak{D}_F$

We have seen that the ring of integers of a number field need not be a UFD. We will see later in the course that if it were always a UFD, then Fermat's last theorem would be easy to prove (and Kummer is famous of having presented this erroneous proof...). Attempts to fix this lack of UFDness led to two discoveries: firstly, the *ideals* of $\mathfrak{D}_F$ *do* satisfy a certain unique factorization property; secondly, the failure of the UFDness isn't arbitrarily bad – it can be measured by an abelian group which turns out to be finite. In this section we prove two main theorems about $\mathfrak{D}_F$ and establish some additional theoretic properties (which are needed to study examples):

(i) Subsection 1 introduces the class group and proves it is finite.

(ii) Subsection 2 explains the unique factorisation of ideals of $\mathfrak{D}_F$.

(iii) Subsection 3 investigates the norm of an ideal, which will be a useful tool in the rest of the course.

Remark 5.1. Both the main theorems involve multiplying ideals together: In a commutative ring R, the product IJ of two ideals I, J is by definition the ideal generated by ab, for $a \in I$, $b \in J$; this product is associative, commutative, and the ideal R is the identity element; moreover, if $I = \langle a\rangle$ and $J = \langle b\rangle$ then $IJ = \langle ab\rangle$.).

Example 5.2. Let $F = \mathbb{Q}(\sqrt{-5})$, so that $\mathfrak{D}_F$ is not a UFD. Then

$$\langle 3, 1 + 2\sqrt{-5}\rangle\langle 3, 1 - 2\sqrt{-5}\rangle = \langle 3\rangle.$$

5.1 The class group, its finiteness, and cancellation of ideals

The absolutely most important object associated a number field F is an object known as its *class group*, denoted Cl_F. This is a finite abelian group whose elements are equivalence classes of non-zero ideals of $\mathfrak{D}_F$, and whose composition law is given by multiplication of these ideals. We will see later, in section 7, that the class group encodes some very subtle information about F which can be used to prove or disprove existence of Diophantine equations.

In this section we will define Cl_F as a set of equivalence classes of ideals, prove that it is finite (which is usually considered to be the first major theorem of algebraic number theory), and then use this finiteness to prove important results about the multiplication of ideals of $\mathfrak{D}_F$.

Definition 5.3. Let F be a number field. Non-zero ideals $I, J \subseteq \mathfrak{D}_F$ are called *principally equivalent*, written $I \sim J$, if and only if there are non-zero $\alpha, \beta \in \mathfrak{D}_F$ such that $\alpha I = \beta J$. This is an equivalence relation on the set of non-zero ideals (check this!), and the *class group* of F (or of $\mathfrak{D}_F$, depending on the preferred terminology) is defined to be the set of equivalence classes:

$$Cl_F := \{\text{non-zero ideals of } \mathfrak{D}_F\}/\text{principal equivalence}.$$

The equivalence class of a non-zero ideal $I \subseteq \mathfrak{D}_F$ is denoted $[I] \in Cl_F$.

The following lemma establishes the basic relation between principal equivalence and principal ideals, and shows that Cl_F is trivial precisely when $\mathfrak{D}_F$ is a PID:

Lemma 5.4. *Let F be a number field.*

(i) Let $I \subseteq \mathfrak{D}_F$ be a non-zero ideal; then I is principal if and only if it is principally equivalent to $\mathfrak{D}_F$. In other words, the equivalence class $[\mathfrak{D}_F]$ is the set of principal ideals.

(ii) $\#Cl_F = 1$ if and only if $\mathfrak{D}_F$ is a PID.

Proof. (i): The implication $\Rightarrow$ is easy, since a principal ideal $I = \langle \alpha \rangle$ is seen to be principally equivalent to $\mathfrak{D}_F$ via the equality $1I = \alpha \mathfrak{D}_F$. Conversely, suppose that $I \subseteq \mathfrak{D}_F$ is a non-zero ideal which is principally equivalent to $\mathfrak{D}_F$. Then $\alpha I = \beta \mathfrak{D}_F$ for some non-zero $\alpha, \beta \in \mathfrak{D}_F$; setting $\omega := \beta/\alpha \in F^\times$, we see that $\omega I = \beta I \subseteq I$ and so lemma 4.26 implies that $\omega \in \mathfrak{D}_F$. Since $I = \omega \mathfrak{D}_F$, this shows that I is principal.

(ii): Cl_F consists of a single equivalence class if and only if every non-zero ideal of $\mathfrak{D}_F$ belongs to the equivalence class $[\mathfrak{D}_F]$; but (i) implies that this is the same as all ideals being principal. □

Example 5.5. Here are some first examples of class groups:

(i) The class groups of $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are trivial, since we know that these rings of integers are PIDs.

(ii) If $F = \mathbb{Q}(\sqrt{-5})$ then we have seen that $\mathfrak{D}_F = \mathbb{Z}[\sqrt{-5}]$ is not a PID; so Cl_F consists of > 1 equivalence classes of ideals. In fact, we will see in section 7 that $\#Cl_F = 2$, which means (check this!) that any two non-principal ideals of $\mathfrak{D}_F$ are principally equivalent.

We now turn to the proof that Cl_F is a finite set, starting with a rather technical (and slightly tricky) lemma which analyses the extent to which $\alpha \mapsto |N_{F/\mathbb{Q}}(\alpha)|$ may not be a Euclidean norm on $\mathfrak{D}_F$; it should be compared with the manipulations used to prove that $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Euclidean domains.

Lemma 5.6. *Let F be a number field. There exists an integer $M \geq 1$ (depending only on F) with the following property: for any $\gamma \in F$ there exist $\omega \in \mathfrak{D}_F$ and an integer $t \in \{1, \ldots, M\}$ such that*

$$|N_{F/\mathbb{Q}}(t\gamma - \omega)| < 1.$$

Proof. Let $\omega_1, \ldots, \omega_n \in \mathfrak{D}_F$ be an integral basis for $F/\mathbb{Q}$. For each $r, j = 1, \ldots, n$, we may write

$$\omega_r \omega_j = \sum_{i=1}^{n} b_{r,i,j} \omega_i$$

for some $b_{r,i,j} \in \mathbb{Z}$. Put

$$C = \sum_{\sigma \in \mathrm{Sym}(n)} \prod_{i=1}^{n} \sum_{r=1}^{n} |b_{r,i,\sigma(i)}|,$$

pick an integer $m > \sqrt[n]{C}$ and put $M = m^n$. We will show that M has the desired property.

To do this we use a geometric argument: by expanding any element of F as a $\mathbb{Q}$-linear sum of $\omega_1, \ldots, \omega_n$, define a function

$$f : F \to [0,1]^n, \quad \sum_{i=1}^{n} a_i \omega_i \mapsto (\{a_1\}, \ldots, \{a_n\}),$$

where $\{a\} = a - \lfloor a \rfloor$ denotes the fractional part of any $a \in \mathbb{Q}$. Now fix $\gamma = \sum_{i=1}^{n} a_i \omega_i \in F$. If we split the cube $[0,1]^n$ into m^n subcubes of side length $1/m$, then at least two of the $m^n + 1$ elements

$$f(\gamma),\ f(2\gamma), \ldots, f((m^n+1)\gamma)$$

must lie in the same subcube; in other words, there are integers $1 \le h < h' \le m^n + 1$ such that

$$|\{h'a_r\} - \{ha_r\}| \le 1/m. \qquad (r = 1, \ldots, n)$$

So

$$(h' - h)\gamma = \sum_{r=1}^{n} (\lfloor h'a_r \rfloor - \lfloor ha_r \rfloor)\omega_i \ + \sum_{r=1}^{n} (\{h'a_r\} - \{ha_r\})\omega_i,$$

which can be rewritten as

$$t\gamma = \omega + \delta$$

where $1 \le t = h' - h \le m^n = M$, $\omega = \sum_{r=1}^{n} (\lfloor h'a_r \rfloor - \lfloor ha_r \rfloor)\omega_r \in \mathfrak{O}_F$, and $\delta = \sum_{r=1}^{n} \delta_r \omega_r$ where $\delta_r = (\{h'a_r\} - \{ha_r\})$. We claim that this value of t and ω have the desired property; to prove this we must show that $|N_{F/\mathbb{Q}}(\delta)| < 1$.

Since we must calculate the norm of δ, we first calculate the matrix D for "multiplication by δ" with respect to the basis $\omega_1, \ldots, \omega_n$: well, for $j = 1, \ldots, n$,

$$\delta\omega_j = \sum_{i=1}^{n} \left(\sum_{r=1}^{n} \delta_r b_{r,i,j} \right) \omega_j,$$

and so $D = (\sum_{r=1}^{n} a_r b_{r,i,j})_{i,j}$. Since $|\delta_r| \le 1/m$ for all r, we have $|D_{i,j}| \le \frac{1}{m} \sum_{r=1}^{n} |b_{r,i,j}|$ for all i, j, and so

$$\begin{aligned}
|N_{F/\mathbb{Q}}(\delta)| &= |\det D| \\
&= |\sum_{\sigma \in \mathrm{Sym}(n)} (-1)^{\mathrm{sign}\,\sigma} \prod_{i=1}^{n} D_{i,\sigma(i)}| \\
&\le \sum_{\sigma \in \mathrm{Sym}(n)} \prod_{i=1}^{n} |D_{i,\sigma(i)}| \\
&\le \sum_{\sigma \in \mathrm{Sym}(n)} \prod_{i=1}^{n} \left(\frac{1}{m} \sum_{r=1}^{n} |b_{r,i,\sigma(i)}| \right) \\
&= \frac{1}{m^n} C \\
&= \frac{1}{M} C \\
&< 1,
\end{aligned}$$

by choice of M. This completes the proof. □

Corollary 5.7. *Let F be a number field and let $M \geq 1$ satisfy the condition of the previous lemma. Then for any $\alpha, \beta \in \mathfrak{D}_F$, with $\beta \neq 0$, there exist $\omega, r \in \mathfrak{D}_F$ and an integer $t \in \{1, \ldots, M\}$ such that*

- $t\alpha = \omega\beta + r$, *and*
- $|N_{F/\mathbb{Q}}(r)| < |N_{F/\mathbb{Q}}(\beta)|$.

Proof. Apply the previous result with $\gamma = \alpha/\beta$ to obtain $\omega \in \mathfrak{D}_F$ and $t \in \{1, \ldots, M\}$; then set $r := t\alpha - \omega\beta$ and use multiplicativity of $N_{F/\mathbb{Q}}$. □

Exercise 5.1. Let F be a number field. Check the details of the previous proof. Then check that the following are equivalent:

(i) The function $\nu : \mathfrak{D}_F \to \mathbb{N},\ \alpha \mapsto |N_{F/\mathbb{Q}}(\alpha)|$ is a Euclidean norm on $\mathfrak{D}_F$.

(ii) For any $\gamma \in F$ there exists $\omega \in \mathfrak{D}_F$ such that $|N_{F/\mathbb{Q}}(\gamma - \omega)| < 1$.

(iii) $M = 1$ satisfies the property of the previous lemma and corollary.

Thus the magnitude of M in general measures the extend to which $|N_{F/\mathbb{Q}}|$ is *not* a Euclidean norm on $\mathfrak{D}_F$. Prove that condition (ii) is satisfied for $\mathbb{Q}(\sqrt{d})$ when $d = -1, -2, -3, -7$, and -11, and so deduce that the rings of integers of these fields are PIDs.

From the previous corollary we may prove the promised theorem that Cl_F is always finite:

Theorem 5.8. *Let F be a number field. Then Cl_F is a finite set; in other words, there are only finitely many equivalence classes of ideals up to principal equivalence.*

Proof. Let $M \geq 1$ be the integer of the previous lemma and corollary. Then $\mathfrak{D}_F/\langle M! \rangle$ is finite by proposition 4.25, so

$$S := \{\text{ideals of } \mathfrak{D}_F \text{ containing } M!\}$$

is a finite set (recall from algebra that ideals of $\mathfrak{D}_F/\langle M! \rangle$ are in one-to-one correspondence with elements of S). We will show that any non-zero ideal I of $\mathfrak{D}_F$ is principally equivalent to an ideal in S, whence Cl_F has at most $\#S$ elements.

For any non-zero $\beta \in I$, the value of $|N_{F/\mathbb{Q}}(\beta)|$ is a non-zero integer, so we may pick and fix a non-zero $\beta \in I$ which minimises this value. For any $\alpha \in I$ the previous corollary yields $\omega \in \mathfrak{D}_F$ and an integer $t \in \{1, \ldots, M\}$ such that $|N_{F/\mathbb{Q}}(t\alpha - \omega\beta)| < |N_{F/\mathbb{Q}}(\beta)|$. Since $t\alpha - \omega\beta \in I$, our minimality choice of β means that $t\alpha - \omega\beta$ must be zero. Therefore $\frac{t}{\beta}\alpha = \omega \in \mathfrak{D}_F$ and so $\frac{M!}{\beta}\alpha \in \mathfrak{D}_F$; this is true for all $\alpha \in I$, so we conclude

$$J := \frac{M!}{\beta} I \subseteq \mathfrak{D}_F.$$

Hence J is a non-zero ideal of $\mathfrak{D}_F$ which by construction satisfies $M!I = \beta J$. So I is principally equivalent to J. Moreover, $M! = \frac{M!}{\beta}\beta \in J$ since $\beta \in I$, so $J \in S$, as required. □

Definition 5.9. For a number field F, the size of the class group Cl_F is denoted

$$h_F = \#Cl_F$$

and is called the *class number* of F. It is an extremely important invariant of the number field. Rephrasing lemma 5.4, we see that $h_F = 1$ if and only if $\mathfrak{D}_F$ is a PID.

The finiteness of Cl_F has an extremely useful corollary for manipulating ideals:

Corollary 5.10. *Let F be a number field and let $I \subseteq \mathfrak{D}_F$ be a non-zero ideal. Then I^k is a principal ideal for some integer $k \in \{1, \ldots, h_F\}$.*

Proof. By the pigeon holeprinciple, at least two of the ideals $I, I^2, \ldots, I^{h_F+1}$ must be principally equivalent; that is, there are integers $1 \leq i < j \leq h_F + 1$ and non-zero $\alpha, \beta \in \mathfrak{D}_F$ such that $\alpha I^i = \beta I^j$. Then

$$\frac{\alpha}{\beta} I^i = \frac{\beta}{\beta} I^j = I^j \subseteq I^i$$

and so $\omega := \beta/\alpha$ is in $\mathfrak{D}_F$ by Lemma 4.26. Moreover, $\omega I^i = I^{j-i} I^i$, so proposition 4.27 implies that $I^{j-i} = \langle \omega \rangle$, which completes the proof. □

Exercise 5.2. Let F be a number field. Define a product operation on Cl_F by

$$[I][J] := [IJ].$$

Prove that this makes Cl_F into a finite, abelian group, with identity element $[\mathfrak{D}_F]$ (you must check associativity, commutativity, and existence of inverses); this is why Cl_F is known as the class *group*.

Exercise 5.3. Let F be a number field and $I \subseteq \mathfrak{D}_F$ a non-zero ideal. Using the previous exercise, prove the following:

(i) I^{h_F} is a principal ideal.

(ii) If I^k is a principal principal ideal for some integer $k \geq 1$ which is coprime to h_F, then I is already principal.

Back in proposition 4.27 we proved a result concerning the cancellation of ideals; here is a significant improvement:

Theorem 5.11. *Let F be a number field.*

(i) ("Cancellation of ideals") Let I, J, K be non-zero ideals of $\mathfrak{D}_F$. If $IJ = IK$ then $J = K$.

(ii) ("Containment equals division") Let I, J be non-zero ideals of $\mathfrak{D}_F$. Then $I \subseteq J$ if and only if there is a non-zero ideal $K \subseteq \mathfrak{D}_F$ such that $JK = I$.

Proof. (i): Assume $IJ = IK$. By corollary 5.10 there is $k \geq 1$ such that $I^k = \langle \alpha \rangle$ for some non-zero $\alpha \in \mathfrak{D}_F$. Certainly $I^{k-1}IJ = I^{k-1}IK$, whence $\alpha J = \alpha K$; now multiply both sides by α^{-1} to deduce $J = K$.

(ii): Implication $\Leftarrow$ is true in all rings since $JK \subseteq J$, so we only need to prove the $\Rightarrow$ direction. Suppose $I \subseteq J$. By corollary 5.10, there is $k \geq 1$ such that $J^k = \langle \alpha \rangle$ for some non-zero $\alpha \in \mathfrak{D}_F$. Then

$$J^{k-1} I \subseteq J^{k-1} J = \langle \alpha \rangle,$$

so $K := \frac{1}{\alpha} J^{k-1} I$ is a non-zero ideal of $\mathfrak{D}_F$. Moreover,

$$JK = \frac{1}{\alpha} J^k I = \frac{1}{\alpha} \alpha I = I,$$

as required. □

5.2 Dedekind domains and Unique factorisation of ideals

Although $\mathfrak{D}_F$ may not be a UFD, we will show in this section that the *ideals* of $\mathfrak{D}_F$ do satisfy unique factorisation into prime ideals:

Theorem 5.12 (Unique factorization of ideals)**.** *Let F be a number field and I a non-zero ideal of $\mathfrak{D}_F$. Then I may be written as a product of powers of prime ideals:*

$$I = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}, \qquad (\mathfrak{p}_i \text{ primes ideals of } \mathfrak{D}_F,\ e_i \geq 1)$$

and this expression is unique up to reindexing.

Remark 5.13. In fact, the previous theorem is true for any integral domain $\mathfrak{D}$ satisfying the following three properties:

(i) Every non-zero prime ideal of $\mathfrak{D}$ is a maximal ideal;

(ii) $\mathfrak{D}$ is Noetherian (i.e., any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ of $\mathfrak{D}$ is eventually stationary).

(iii) $\mathfrak{D}$ is *integrally closed*. This means that if an element α of the fraction field of $\mathfrak{D}$ is a root of a monic polynomial in $\mathfrak{D}[X]$ then $\alpha \in \mathfrak{D}$.

Rings with these three properties are called *Dedekind domains*; we will prove in the next lemma that the ring of integers of a number field is a Dedekind domain.

For example, any PID R is a Dedekind domain. The prime ideal = maximal ideal and Noetherian properties are standard results from algebra, while it easily follows from Gauss lemma and lemma 3.11 that UFDs, hence PIDs, are integrally closed.

Theorem 5.11 is true for any Dedekind domain, although our proof relied on finiteness of the class group. The proofs in this section use only properties (i)–(iii) and Theorem 5.11, hence they are "purely algebraic" and are true for any Dedekind domain. Moreover, principal equivalence and the class group may be defined in the same way for Dedekind domains, but it will no longer necessarily be true that it is finite.

However, we will continue to state our results only for rings of integers of number fields.

Exercise 5.4. Using the fact that a PID is a UFD, prove directly that the above Unique factorisation of ideals theorem is true for a PID.

Lemma 5.14. *If F is a number field then $\mathfrak{D}_F$ is a Dedekind domain.*

Proof. We begin by proving property (i), namely that every non-zero prime ideal of $\mathfrak{D}_F$ is a maximal. If $\mathfrak{p}$ is a non-zero prime ideal of $\mathfrak{D}_F$ then $R := \mathfrak{D}_F/\mathfrak{p}$ is a finite integral domain. We claim that this is enough to imply it is a field, whence $\mathfrak{p}$ is a maximal ideal. Well, if $r \in R$ is non-zero, then $R \to R$, $a \mapsto ra$ is an injective map; since the domain and codomain have the same finite size, it is a bijection, and so there is $a \in R$ such that $ra = 1$.

We secondly prove that $\mathfrak{D}_F$ is Noetherian, so suppose that $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending chain of ideals of $\mathfrak{D}_F$. If $I_i = 0$ for all $i \geq 1$ then the chain is already stationary and there is nothing to prove. Else I_i is a non-zero ideal for some i, whence $\mathfrak{D}_F/I_i$ is a finite ring and hence only has finitely many ideals. Therefore $\mathfrak{D}_F$ has only finitely many ideals containing I_i, so the chain $I_i \subseteq I_{i+1} \subseteq \cdots$ must clearly eventually be stationary.

Finally we prove that $\mathfrak{D}_F$ is integrally closed, so suppose that $\alpha \in F$ is the root of a monic polynomial $f(X) \in \mathfrak{D}_F[X]$. By exercise 3.1, $\alpha \in \mathbb{Z}^{\mathrm{alg}}$, so $\alpha \in \mathbb{Z}^{\mathrm{alg}} \cap F = \mathfrak{D}_F$ as required. □

Before beginning the proof of the theorem, let's see how "unique factorisation of ideals" compares with "unique factorisation of elements":

Example 5.15. Back in the first lecture we saw that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, because $3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ are non-associated irreducibles which satsify

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Here is how the 'ideal version of unique factorization' fixes the problem:

We have the following identities concerning products of ideals:

$$\begin{aligned}
\langle 3, 1 + 2\sqrt{-5}\rangle\langle 3, 1 - 2\sqrt{-5}\rangle &= \langle 3\rangle \\
\langle 7, 1 + 2\sqrt{-5}\rangle\langle 7, 1 - 2\sqrt{-5}\rangle &= \langle 7\rangle \\
\langle 3, 1 + 2\sqrt{-5}\rangle\langle 7, 1 + 2\sqrt{-5}\rangle &= \langle 1 + 2\sqrt{-5}\rangle \\
\langle 3, 1 - 2\sqrt{-5}\rangle\langle 7, 1 - 2\sqrt{-5}\rangle &= \langle 1 - 2\sqrt{-5}\rangle
\end{aligned}$$

(Prove two of these). Also need to know that all ideals on the left are prime! Let's just check $\mathfrak{q} = \langle 3, 1 + 2\sqrt{-5}\rangle$; all the others are the same argument. Firstly, it is impossible that $\langle 3, 1 + 2\sqrt{-5}\rangle$ is the whole ring, for that would imply (by one of the product identities above) that $\langle 3, 1 - 2\sqrt{-5}\rangle = \langle 3\rangle$, which is absurd because $1 - 2\sqrt{-5} \notin \langle 3\rangle$.

Now let $\alpha = a + b\sqrt{-5}$ be a typical element of $\mathbb{Z}[\sqrt{-5}]$. Then

$$a := \alpha - 3\sqrt{-5} + (1 + 2\sqrt{-5})b \in \mathbb{Z},$$

and $\alpha \equiv a \bmod \mathfrak{q}$. Consider the ring homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}[\sqrt{-5}]/\mathfrak{q};$$

we have just shown that f is surjective. Its kernel contains $3\mathbb{Z}$, which is a maximal ideal, so its kernel is equal to $3\mathbb{Z}$. By an isomorphism theorem for rings, we get

$$\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}[\sqrt{-5}]/\mathfrak{q};$$

this is a field, so $\mathfrak{q}$ is a prime ideal (even a maximal ideal) of $\mathbb{Z}[\sqrt{-5}]$.

Thus the identity $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ is really an identity concerning products of prime ideals:

$$\langle 21\rangle = \langle 3, 1 + 2\sqrt{-5}\rangle\langle 3, 1 - 2\sqrt{-5}\rangle\langle 7, 1 + 2\sqrt{-5}\rangle\langle 7, 1 - 2\sqrt{-5}\rangle$$

This is enough to prove part of the main theorem:

Theorem 5.16. *Every non-zero ideal of $\mathfrak{D}_F$ is a product of prime ideals.*

Proof. Let S be the set of all non-zero ideals of $\mathfrak{D}_F$ which *cannot* be written as a product of prime ideals. For a contradiction, suppose that S is not empty, and let $I_1 \in S$. Now pick $I_2 \in S$ strictly containing I_1 (if such an I_2 exists), then pick $I_3 \in S$ strictly containg I_2 (if such an I_3 exists), etc. This produces a strictly increasing chain of elements of S:

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

Since $\mathfrak{D}_F$ is Noetherian, this chain cannot go on forever, meaning that we eventually find an ideal $I \in S$ such that no other ideal in S properly contains I.

Now, $I \neq \mathfrak{D}_F$, since $\mathfrak{D}_F$ is the empty product of ideals, so I is a proper ideal of $\mathfrak{D}_F$. Recall that given a proper ideal of any commutative ring, there always exists a maximal ideal containing it. So there is a maximal ideal (= prime ideal since $\mathfrak{D}_F$ is a Dedkind domain) $\mathfrak{p} \subseteq \mathfrak{D}_F$ containing I. The previous proposition implies there exists a non-zero ideal J such that $I = \mathfrak{p}J$. Next, $I \subseteq J$, but $I \neq J$ (else cancellation of ideals would imply $\mathfrak{p} = \mathfrak{D}_F$), so the choice of I means that $J \notin S$.

But therefore J is a product of prime ideals, so $I = \mathfrak{p}J$ is also a product of prime ideals. □

All that remains is to prove uniqueness of the decomposition into prime ideals, for which the following tool is used:

Definition 5.17. Let I be a non-zero ideal of $\mathfrak{D}_F$, and $\mathfrak{p}$ a prime ideal. Let $\operatorname{ord}_{\mathfrak{p}} I$ be the unique integer $r \geq 0$ such that

$$I \subseteq \mathfrak{p}^r, \quad I \not\subseteq \mathfrak{p}^{r+1}.$$

We should check that the definition makes sense: If $\mathfrak{p}$ a non-zero prime ideal of $\mathfrak{D}_F$ then

$$\mathfrak{D}_F = \mathfrak{p}^0 \supset \mathfrak{p}^1 \supset \mathfrak{p}^2 \cdots$$

is a strictly descending chain of ideals of $\mathfrak{D}_F$ (for if $\mathfrak{p}^i = \mathfrak{p}^{i+1}$ then $\mathfrak{p} = \mathfrak{D}_F$ by the cancellation of ideals, which is absurd). Moreover, we claim that

$$\bigcap_{i=1}^{\infty} \mathfrak{p}^i = \{0\};$$

for if not, then $J := \bigcap_{i=1}^{\infty} \mathfrak{p}^i$ is a non-zero ideal of $\mathfrak{D}_F$ which is easily checked to satisfy $\mathfrak{p}J = \mathfrak{p}$, which would again imply $\mathfrak{p} = \mathfrak{D}_F$. Therefore the definition makes sense, and next we check the properties of $\operatorname{ord}_{\mathfrak{p}}$

Lemma 5.18. $\mathrm{ord}_{\mathfrak{p}}$ *has the following properties:*

(i) $\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{p} = 1$*;*

(ii) $\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{O}_F = 0$*;*

(iii) if $\mathfrak{q}$ *is a non-zero prime ideal of* $\mathfrak{O}_F$ *distinct from* $\mathfrak{p}$*, then* $\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{q} = 0$*;*

(iv) if I, J *are non-zero ideals of* $\mathfrak{O}_F$*, then* $\mathrm{ord}_{\mathfrak{p}}(IJ) = \mathrm{ord}_{\mathfrak{p}}\,I + \mathrm{ord}_{\mathfrak{p}}\,J$*.*

Proof. (i): Certainly $\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{p} \geq 1$, so we must only prove that $\mathfrak{p}^2 \not\subseteq \mathfrak{p}$; but if this happened then $\mathfrak{p}^2 = \mathfrak{p}$, whence $\mathfrak{p} = \mathfrak{O}_F$ by cancellation of ideals

(ii) is clear.

(iii): We must show that $\mathfrak{q} \not\subseteq \mathfrak{p}$. Since $\mathfrak{O}_F$ is a Dedekind domain, the prime ideal $\mathfrak{q}$ is also maximal, and so if $\mathfrak{q} \subseteq \mathfrak{p}$ then $\mathfrak{q} = \mathfrak{p}$, which we have assumed is not the case.

(iv): This is the most important part. Let $s = \mathrm{ord}_{\mathfrak{p}}\,I$, $t = \mathrm{ord}_{\mathfrak{p}}\,J$; thus $\mathfrak{p}^s \supseteq I$, so $\mathfrak{p}^s I' = I$ for some ideal I (by proposition **??**). Since $\mathfrak{p}^{s+1} \not\supseteq I$, we see that $\mathfrak{p} \not\supseteq I'$. Similarly, $\mathfrak{p}^t J' = J$ for some ideal J' not contained inside J.

Clearly $\mathfrak{p}^{s+t} \supseteq IJ = \mathfrak{p}^{s+t} I'J'$, so we must show that $\mathfrak{p}^{s+t+1} \not\supseteq \mathfrak{p}^{s+t} I'J'$. Well, if then $\mathfrak{p}^{s+t+1} \supseteq \mathfrak{p}^{s+t} I'J'$ then there is an ideal K such that $\mathfrak{p}^{s+t+1}K = \mathfrak{p}^{s+t} I'J'$, whence proposition **??** implies that $\mathfrak{p}K = I'J'$. So $I'J' \subseteq \mathfrak{p}$. But neither I' or J' is contained in $\mathfrak{p}$, so there exist $a \in I' \setminus \mathfrak{p}$, $b \in J' \setminus \mathfrak{p}$; since $\mathfrak{p}$ is prime, we see that $ab \notin \mathfrak{p}$, contadicting $I'J' \subseteq \mathfrak{p}$. □

Now we may prove the uniqueness of prime decomposition:

Theorem 5.19. *Let*

$$\mathfrak{p}_1^{r_1} \dots \mathfrak{p}_m^{r_m} = \mathfrak{q}_1^{s_1} \dots \mathfrak{q}_k^{s_k}$$

be two products of prime ideals, with $r_1, \dots, r_m, s_1, \dots, s_k \geq 1$*. Then* $n = m$ *and, after reordering,* $r_i = s_i$ *for all* i*.*

Proof. By reordering the product and inserting terms like $\mathfrak{p}^0 = \mathfrak{O}_F$, it is enough to prove that if we have two expressions

$$\mathfrak{p}_1^{r_1} \dots \mathfrak{p}_m^{r_m} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m},$$

with $r_1, \dots, r_m, s_1, \dots, s_m \geq 0$ then $r_i = s_i$ for all i. But this follows immediately from the previous lemma by applying $\mathrm{ord}_{\mathfrak{p}_i}$ to both sides. □

In other words,

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)},$$

where the product is taken over all non-zero prime ideals of $\mathfrak{O}_F$, and where $\mathrm{ord}_{\mathfrak{p}}(I) = 0$ for all but finitely many $\mathfrak{p}$.

5.3 Norms of ideals

Our final theory concerning rings of integers of number fields analyses norms of ideals. Recall from definition 4.24 that the *norm* of a non-zero ideal $I \subseteq \mathfrak{O}_F$ is defined to be the size of the quotient ring $\mathfrak{O}_F/I$:

$$N(I) := \#\mathfrak{O}_F/I$$

In this section we establish the following two fundamental properties of norms of ideals:

(N1) If $I = \langle \alpha \rangle$ is a principal ideal, then $N(I) = |N_{F/\mathbb{Q}}(\alpha)|$.

(N2) If $I, J \subseteq \mathfrak{O}_F$ are non-zero ideals, then $N(IJ) = N(I)N(J)$.

We begin with (N1), whose proof is essentially some tricky linear algebra:

Proposition 5.20. *Let F be a number field and let $\alpha \in \mathfrak{D}_F$ be non-zero. Then*

$$N(\langle\alpha\rangle) = |N_{F/\mathbb{Q}}(\alpha)|.$$

Proof. We begin by recalling some linear algebra. If $P \in M_n(\mathbb{Z})$ is a matrix with non-zero determinant, then Gaussian elimination, the theory of Echelon forms, or the structure theory of finitely generated abelian groups implies that there exist elementary matrices $E_1, E_2 \in GL_n(\mathbb{Z})$ (i.e., matrices obtained by applying row and column operations to the identity matrix), and a diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_n) \in M_n(\mathbb{Z})$ such that $P = E_1 D E_2$. Then we have isomorphisms of abelian groups as follows:

$$\begin{aligned}
\mathbb{Z}^n/P\mathbb{Z}^n &= \mathbb{Z}^n/E_1 D E_n \mathbb{Z}^n \\
&= E_1\mathbb{Z}^n/E_1 D E_n \mathbb{Z}^n \\
&\cong \mathbb{Z}^n/D E_n \mathbb{Z}^n \\
&= \mathbb{Z}^n/D\mathbb{Z}^n \\
&\cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z},
\end{aligned}$$

and so $\#\mathbb{Z}^n/P\mathbb{Z}^n = d_1 \cdots d_n = \det D = |\det P|$, since $\det E_i = \pm 1$.

Now let $\omega_1, \ldots, \omega_n \in \mathfrak{D}_F$ be an integral basis for $F/\mathbb{Q}$ and let $P \in M_n(\mathbb{Z})$ be the matrix for "multiplication for α" with respect to this basis. Then, by definition of an integral basis, we have an isomorphism

$$\mathbb{Z}^n \xrightarrow{\sim} \mathfrak{D}_F, \quad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^{n} a_i \omega_i$$

and this takes $P\mathbb{Z}$ to $\alpha\mathfrak{D}_F = \langle\alpha\rangle$; therefore $\mathbb{Z}/P\mathbb{Z} \cong \mathfrak{D}_F/\langle\alpha\rangle$ as abelian groups. So,

$$|N_{F/\mathbb{Q}}(\alpha)| = |\det P| = \#\mathbb{Z}/P\mathbb{Z} = \#\mathfrak{D}_F/\langle\alpha\rangle = N(\langle\alpha\rangle). \qquad \square$$

Remark 5.21. In the special case that $\alpha = m \in \mathbb{Z}$, the proposition states that $N(\langle m\rangle) = |m|^n$, where $n = |F : \mathbb{Q}|$. We have already proved this directly in proposition 4.25.

To prove property (N2) of norms of ideals, we will check it first for powers of prime ideals, and then extend it to all ideals via a Chinese Remainder type argument; we begin with powers of prime ideals:

Lemma 5.22. *Let F be a number field and let $\mathfrak{p} \subseteq \mathfrak{D}_F$ be a prime ideal. Then*

$$N(\mathfrak{p}^e) = N(\mathfrak{p})^e$$

for all $e \geq 0$.

Proof. The claim is trivial when $e = 0, 1$, so assume that $e > 1$ and proceed by induction. A standard isomorphism theorem for rings implies that $I := \mathfrak{p}^{e-1}/\mathfrak{p}^e$ is an ideal of $R := \mathfrak{D}_F/\mathfrak{p}^e$, with quotient $R/I \cong \mathfrak{D}/\mathfrak{p}^e$. Counting elements, we see that

$$\frac{\#\mathfrak{D}_F/\mathfrak{p}^e}{\#\mathfrak{p}^{e-1}/\mathfrak{p}^e} = \#\mathfrak{D}/\mathfrak{p}^{e-1},$$

i.e., $N(\mathfrak{p}^e) = N(\mathfrak{p}^{e-1})\,\#\mathfrak{p}^{e-1}/\mathfrak{p}^e$. Therefore the proof by induction will be complete if we can show that $\#\mathfrak{p}^{e-1}/\mathfrak{p}^e = N(\mathfrak{p})$; in fact, we will prove the stronger statement that there is an isomorphism of abelian groups $\mathfrak{p}^{e-1}/\mathfrak{p}^e \cong \mathfrak{D}_F/\mathfrak{p}$.

Since $\mathfrak{p}^e \subset \mathfrak{p}^{e-1}$ is a strict inclusion (by uniqueness of prime factorization of ideals, or simply by cancellation of ideals), we may pick an element $\alpha \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$. From this element we define a group homomorphism

$$\phi : \mathfrak{D}_F \to \mathfrak{p}^{e-1}/\mathfrak{p}^e, \quad \beta \mapsto \alpha\beta \bmod \mathfrak{p}^e,$$

which we claim is surjective with kernel $\mathfrak{p}$.

Proof of surjectivity: Let $\mathfrak{q}$ be a prime ideal in the prime factorization of the ideal $\langle\alpha\rangle + \mathfrak{p}^e$; then $\mathfrak{p}^e \subseteq \langle\alpha\rangle + \mathfrak{p}^e \subseteq \mathfrak{q}$, whence $\mathfrak{p} \subseteq \mathfrak{q}$ and so $\mathfrak{p} = \mathfrak{q}$ (by the usual prime ideals = maximal ideal trick). So the only prime occuring in the prime factorization of $\langle\alpha\rangle + \mathfrak{p}^e$ is $\mathfrak{p}$ itself, and therefore $\langle\alpha\rangle + \mathfrak{p}^e = \mathfrak{p}^r$ for some $r \geq 0$. But $\mathfrak{p}^e \subset \langle\alpha\rangle + \mathfrak{p}^{e-1} \subseteq \mathfrak{p}^{e-1}$ and so $r = e - 1$; i.e., $\langle\alpha\rangle + \mathfrak{p}^e = \mathfrak{p}^{e-1}$. This means ϕ is surjective.

Proof that $\operatorname{Ker}\phi = \mathfrak{p}$: Let $\beta \in \mathfrak{D}_F$. Then $\phi(\beta) = 0$ if and only if $\alpha\beta \in \mathfrak{p}^e$, which is equivalent to $\operatorname{ord}_{\mathfrak{p}}\langle\alpha\beta\rangle \geq e$. But $\operatorname{ord}_{\mathfrak{p}}\langle\alpha\beta\rangle = e - 1 + \operatorname{ord}_{\mathfrak{p}}\langle\beta\rangle$, which is $\geq e$ if and only if $\operatorname{ord}_{\mathfrak{p}}\langle\beta\rangle \geq 1$; so

$$\operatorname{Ker}\phi = \{\beta \in \mathfrak{D}_F : \operatorname{ord}_{\mathfrak{p}}\langle\beta\rangle \geq 1\} = \mathfrak{p},$$

as required.

Therefore ϕ induces a group homomorphism $\mathfrak{D}_F/\mathfrak{p} \cong \mathfrak{p}^e/\mathfrak{p}^{e-1}$, as desired. □

Proposition 5.23. *Let F be a number field and let $I, J \subseteq \mathfrak{D}_F$ be non-zero ideals. Then $N(IJ) = N(I)N(J)$.*

Proof. We reduce the proof to powers of prime ideals using two intermediate results. First we recall the (Generalised) Chinese Remainder Theorem from algebra, which we do not prove:

> Let R be a commutative ring, let $I_1, \ldots, I_m$ be ideals of R such that $I_i + I_j = R$ whenever $i \neq j$, and set $I := I_1 \cdots I_m$. Then there is a natural isomorphism of rings
>
> $$R/I \xrightarrow{\sim} R/I_1 \oplus \cdots \oplus R/I_m.$$

Secondly we claim that this is valid for $\mathfrak{D}_F$ in the following sense: if $\mathfrak{p}, \mathfrak{q}$ are distinct non-zero prime ideals of $\mathfrak{D}_F$, and $r, s \geq 0$, then $\mathfrak{p}^r + \mathfrak{q}^s = \mathfrak{D}_F$. If r or s equals 0 then the claim is obvious, so assume $r, s \geq 1$. For a contradiction, assume $\mathfrak{p}^r + \mathfrak{q}^s$ is a proper ideal of $\mathfrak{D}_F$; then there exists a maximal ideal $\mathfrak{P} \subset \mathfrak{D}_F$ containing it. In particular, $\mathfrak{p}^r \subseteq \mathfrak{p}^r + \mathfrak{q}^s \subseteq \mathfrak{P}$, which implies $\mathfrak{p} \subseteq \mathfrak{P}$ (since $\mathfrak{P}$ is prime); but $\mathfrak{p}$ is a maximal ideal (since prime ideal = maximal ideal in $\mathfrak{D}_F$), so this forces $\mathfrak{p} = \mathfrak{P}$. But the same argument reveals that $\mathfrak{q} = \mathfrak{P}$, contradicting $\mathfrak{p} \neq \mathfrak{q}$. This completes the proof of the claim.

Now we are equipped to prove the proposition. We may write

$$I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}, \quad J = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$$

for some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \subset \mathfrak{D}_F$ and integers $r_1, \ldots, r_m, s_1, \ldots, s_m \geq 0$. Then $IJ = \mathfrak{p}_1^{r_1+s_1} \cdots \mathfrak{p}_m^{r_m+s_m}$ and so

$$\begin{aligned}
N(IJ) &= |\mathfrak{D}/IJ| \\
&= |\mathfrak{D}/\mathfrak{p}_1^{r_1+s_1}| \cdots |\mathfrak{D}/\mathfrak{p}_m^{r_m+s_m}| && \text{(by CRT)} \\
&= N(\mathfrak{p}_1)^{r_1+s_1} \ldots N(\mathfrak{p}_m)^{r_m+s_m} \\
&= N(\mathfrak{p}_1^{r_1}) \ldots N(\mathfrak{p}_m^{r_m}) \cdot N(\mathfrak{p}_1^{s_1}) \ldots N(\mathfrak{p}_m^{s_m}) \\
&= N(I)N(J). && \text{(by CRT again)}
\end{aligned}$$

□

Corollary 5.24. *Suppose that $\mathfrak{p}$ is a non-zero ideal of $\mathfrak{D}_F$ such that $N(\mathfrak{p})$ is a prime number; then $\mathfrak{p}$ is a prime ideal.*

Proof. Certainly $\mathfrak{p} \neq \mathfrak{D}_F$, so let $\mathfrak{q}$ be any prime ideal containing $\mathfrak{p}$. Then "containment equals division" implies $\mathfrak{p} = \mathfrak{q}I$ for some ideal I; so $N(\mathfrak{p}) = N(\mathfrak{q})N(I)$. But $N(\mathfrak{p})$ is prime and $N(\mathfrak{q}) \neq 1$; so $N(I) = 1$, whence $I = \mathfrak{D}_F$ and $\mathfrak{p} = \mathfrak{q}$. □

6 Explicitly constructing ideals in $\mathfrak{D}_F$ and generators of Cl_F

In the previous section we proved the main theoretic properties of rings of integers of number fields. To be able to apply this theory to a concrete number field F, we need to be able to calculate Cl_F; to do this we must describe the ideals of $\mathfrak{D}_F$, for which it is enough to describe the prime ideals (by factorisation of ideals). To do this, we begin by partitioning the prime ideals of $\mathfrak{D}_F$ according to which usual prime number they contain:

Definition 6.1. Let F be a number field and $p \in \mathbb{N}$ a prime number. Then a prime ideal $\mathfrak{p} \subset \mathfrak{D}_F$ is said to *sit over* p (or that p *sits under* $\mathfrak{p}$) if and only if $\mathfrak{p}$ occurs in the prime ideal factorisation of the principal ideal $\langle p \rangle \subset \mathfrak{D}_F$.

The following exercise offers alternative definitions, and the main properties, of this relationship; in particular, it shows that each prime ideal of $\mathfrak{D}_F$ sits over a *unique* prime number.

Exercise 6.1. Let F be number field, $p \in \mathbb{N}$ a prime number, and $\mathfrak{p} \subset \mathfrak{D}_F$ a prime ideal. Show that the following are equivalent:

(i) $\mathfrak{p}$ sits over p.

(ii) $p \in \mathfrak{p}$.

(iii) $N(\mathfrak{p})$ is a positive power of p.

Prove that for any fixed $\mathfrak{p}$, there is a unique p sitting under it. Then prove that if p is fixed, there are only finitely many $\mathfrak{p}$ sitting over it.

Therefore, to describe all prime ideals of $\mathfrak{D}_F$, it is necessary and sufficient to explicitly factor $\langle p \rangle$, for all prime numbers $p \in \mathbb{N}$. This will be achieved by theorem 6.3 in a moment, under the assumption that $\mathfrak{D}_F = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{D}_F$; this is true in all cases of interest to us, but can fail in general. We begin by explaining how to construct prime ideals sitting over p:

Lemma 6.2 (Constructing prime ideals of $\mathfrak{D}_F$)**.** *Let F be a number field such that $\mathfrak{D}_F = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{D}_F$, and let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α; let $p \in \mathbb{N}$ be a fixed prime number.*

Suppose that $g(X) \in \mathbb{F}_p[X]$ is a monic irreducible polynomial ($\neq 1$) which divides $\overline{f}(X) := f(X) \bmod p$. Let $\widetilde{g}(X) \in \mathbb{Z}[X]$ be any lift of $g(X)$ to $\mathbb{Z}[X]$, and put

$$\mathfrak{p}_g := \langle p, \widetilde{g}(\alpha) \rangle \subseteq \mathfrak{D}_F.$$

Then

(i) $\mathfrak{p}_g$ is a prime ideal of $\mathfrak{D}_F$ depending only on $g(X)$, not on the choice of lift $\widetilde{g}(X)$.

(ii) $N(\mathfrak{p}_g) = p^{\deg g}$.

(iii) If $g_1(X) \in \mathbb{F}_p[x]$ is a different monic irreducible polynomial dividing $\overline{f}(X)$, then $\mathfrak{p}_{g_1} \neq \mathfrak{p}_g$.

Proof. Firstly, any other lift of $g(X)$ to $\mathbb{Z}[X]$ has the form $g(X) + pA(X)$ for some $A(X) \in \mathbb{Z}[X]$; then it is clear that

$$\langle p, g(\alpha) \rangle = \langle p, g(\alpha) + pA(\alpha) \rangle,$$

so $\mathfrak{p}_g$ really does only depend on $g(X)$ and not on the chosen lift.

Next we prove that $\mathfrak{p}_g$ is prime and that $N(\mathfrak{p}_g) = p^{\deg g}$. We start with the ring homomorphism

$$\phi : \mathbb{Z}[X] \to \mathfrak{D}_F, \quad h(X) \mapsto h(\alpha),$$

which is surjective by our assumption that $\mathfrak{D}_F = \mathbb{Z}[\alpha]$. We claim that $\operatorname{Ker} \phi = \langle f(X) \rangle$. The inclusion $\supseteq$ is obvious, so suppose $h(X) \in \operatorname{Ker} \phi$: then $h(\alpha) = 0$ and so $h(X) = h_1(X) f(X)$ for some $h_1(X) \in \mathbb{Q}[X]$; but

Gauss' lemma implies that actually $h_1(X) \in \mathbb{Z}[X]$, and so $h(X) \in \langle f(X)\rangle$, proving the claim. Therefore ϕ induces an isomorphism

$$\overline{\phi} : \mathbb{Z}[X]/\langle f(X)\rangle \xrightarrow{\sim} \mathfrak{D}_F.$$

Furthermore, $\overline{\phi}(p) = p$ and $\overline{\phi}(\widetilde{g}(X)) = \widetilde{g}(\alpha)$, so there is another induced isomorphism

$$\mathbb{Z}[X]/\langle f(X), p, \widetilde{g}(X)\rangle \xrightarrow{\sim} \mathfrak{D}_F/\mathfrak{p}_g,$$

which we will use to prove (ii) and the rest of (i).

Since $g(X)$ divides $\overline{f}(X)$, we easily see that $f(X) \in \langle p, \widetilde{g}(X)\rangle$ and so $\langle f(X), p, \widetilde{g}(X)\rangle = \langle p, \widetilde{g}(X)\rangle$. Thus

$$\mathfrak{D}_F/\mathfrak{p}_g \cong \mathbb{Z}[X]/\langle p, \widetilde{g}(X)\rangle = \mathbb{F}_p[X]/\langle g(X)\rangle;$$

since $g(X)$ is an irreducible polynomial of degree $\deg g$, the right hand ring is indeed an integral domain with $p^{\deg g}$ elements (by Algebra). Hence $\mathfrak{p}_g$ is a prime ideal of $\mathfrak{D}_F$ with norm $p^{\deg g}$.

Finally, we prove (iii): suppose $g_1(X) \neq g(X)$ is a different monic irreducible polynomial in $\mathbb{F}_p[X]$. Then the Euclidean algorithm lets us write $G(X)g(X) + G_1(X)g_1(X) = 1$ for some $G, G_1 \in \mathbb{F}_p[X]$; lifting to $\mathbb{Z}[X]$, we may write $\widetilde{G}(X)\widetilde{g}(X) + \widetilde{G}_1(X)\widetilde{g}_1(X) = 1 + pE(X)$ for some $E(X) \in \mathbb{Z}[X]$. If $\mathfrak{p}_{g_1} = \mathfrak{p}_g$ then this ideal would contain

$$\widetilde{G}(\alpha)\widetilde{g}(\alpha) + \widetilde{G}_1(\alpha)\widetilde{g}_1(\alpha) - pE(\alpha) = 1,$$

whence $\mathfrak{p}_{g_1} = \mathfrak{p}_g = \mathfrak{D}_F$. But this contradicts $N(\mathfrak{p}_g) = p^{\deg g}$. □

The next theorem says that not only does the previous lemma give *all* the prime ideals of $\mathfrak{D}_F$ sitting over p, but it even offers the precise prime ideal factorisation of the ideal $\langle p\rangle$; the moral of the theorem is that factoring $\langle p\rangle$ is equivalent to factoring $f(X)$ mod p.

Theorem 6.3 (How to factor $\langle p\rangle$)**.** *Let F be a number field such that $\mathfrak{D}_F = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{D}_F$, and let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α; let $p \in \mathbb{N}$ be a fixed prime number.*

Let

$$\overline{f}(X) = f_1(X)^{e_1} \cdots f_r(X)^{e_r}$$

be the factorisation of $\overline{f}(X) := f(X)$ mod p into distinct monic irreducible polynomials $f_1(X), \ldots, f_r(X) \in \mathbb{F}_p[X]$, where $e_1, \ldots, e_r \geq 1$. Then the principal ideal $\langle p\rangle$ of $\mathfrak{D}_F$ has prime ideal factorization

$$\langle p\rangle = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i := \mathfrak{p}_{f_i}$ in the notation of the previous lemma.

Proof. According to the previous lemma, $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ is a product of powers of distinct prime ideals. Moreover, the inclusion

$$\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r} \subseteq \langle p\rangle$$

is quite clear: $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ is generated by terms all but one of which are obviously multiples of p, and the remaining generator is $\widetilde{f_1}(\alpha)^{e_1} \ldots \widetilde{f_r}(\alpha)^{e_r}$, which belongs to $f(\alpha) + \langle p\rangle = \langle p\rangle$.

To complete the proof it is now enough to show that $N(\langle p\rangle) = N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r})$, since this forces the above inclusion to be an equality. Well, $N(\langle p\rangle) = p^{|F:\mathbb{Q}|}$, while the norm of the right hand side, using proposition 5.23 is

$$\prod_{i=1}^{r} p^{e_i \deg f_i} = p^{\deg f}.$$

But $\deg f = |F : \mathbb{Q}|$, completing the proof. □

Corollary 6.4. *Let $F, \alpha, f(X)$ be as in the theorem, and let $p \in \mathbb{N}$ be a prime number. Then $\langle p\rangle$ is a prime ideal of $\mathfrak{D}_F$ if and only if $f(X)$ mod p is irreducible in $\mathbb{F}_p[X]$.*

Proof. Immediate from the theorem. □

Example 6.5. Let $F = \mathbb{Q}(\sqrt{-5})$. Since $\mathfrak{O}_F = \mathbb{Z}[\sqrt{-5}]$, the theorem may be applied with $\alpha = \sqrt{-5}$ and $f(X) = X^2 + 5$:

- $\boldsymbol{p = 2}$ **:** $X^2 + 5$ factors in $\mathbb{F}_2[X]$ as $X^2 + 5 = (X + 1)^2$, so the theorem implies that $\langle 2, 1 - \sqrt{-5}\rangle$ is the unique prime ideal of $\mathfrak{O}_F$ containing 2, that it has norm 2, and that the prime ideal factorisation of $\langle 2\rangle$ is $\langle 2\rangle = \langle 2, 1 - \sqrt{-5}\rangle^2$.
- $\boldsymbol{p = 3}$ **:** $X^2 + 5$ factors in $\mathbb{F}_3[X]$ as $X^5 + 5 = X^2 - 1 = (X - 1)(X + 1)$, so the theorem implies that $\langle 3, \sqrt{-5} - 1\rangle$ and $\langle 3, \sqrt{-5} + 1\rangle$ are the unique prime ideals of $\mathfrak{O}_F$ containing 3, that they are distinct and both have norm 3, and that the prime ideal factorisation of $\langle 3\rangle$ is $\langle 3\rangle = \langle 3, \sqrt{-5} + 1\rangle\langle 3, \sqrt{-5} - 1\rangle$.
- $\boldsymbol{p = 5}$ **:** $X^2 + 5$ factors in $\mathbb{F}_5[X]$ as $X^5 + 5 = X^2$, so the theorem implies that $\langle 5, \sqrt{-5}\rangle = \langle\sqrt{-5}\rangle$ is the unique prime ideal of $\mathfrak{O}_F$ containing 5, that it has norm 5, and that the prime ideal factorisation of $\langle 5\rangle$ is $\langle 5\rangle = \langle\sqrt{-5}\rangle^2$.
- $\boldsymbol{p = 7}$ **:** $X^2 + 5$ factors in $\mathbb{F}_7[X]$ as $X^2 + 5 = X^2 - 2 = (X - 3)(X + 3)$, so the theorem implies that $\langle 7, \sqrt{-5} - 3\rangle$ and $\langle 7, \sqrt{-5} + 3\rangle$ are the unique prime ideals of $\mathfrak{O}_F$ containing 7, that they are distinct and both have norm 7, and that the prime ideal factorisation of $\langle 7\rangle$ is $\langle 7\rangle = \langle 7, \sqrt{-5} + 3\rangle\langle 7, \sqrt{-5} - 3\rangle$.

  (Note that $\langle 7, 1 + 2\sqrt{-5}\rangle = \langle 7, \sqrt{-5} - 3\rangle$ and $\langle 7, 1 - 2\sqrt{-5}\rangle = \langle 7, \sqrt{-5} + 3\rangle$, so this agrees with an example we proved by hand.)
- $\boldsymbol{p = 11}$ **:** $X^2 + 5 = X^2 - 6$ in $\mathbb{Z}/11\mathbb{Z}[X]$, which is irreducible since 6 is not a quadratic residue mod 11. Therefore $\langle 11\rangle$ is a prime ideal of $\mathfrak{O}_F$ of norm 11^2.

Next we use this analysis to describe all ideals J of $\mathfrak{O}_F$ having norm ≤ 10. Well, if $N(J) \leq 10$, then the only possible primes dividing $N(J)$ are $2, 3, 5, 7$, so by exercise 6.2 below the only prime ideals occurring in the factorisation of J are prime ideals sitting over $2, 3, 5, 7$; i.e., J is a product of powers of the following ideals:

$$\mathfrak{p}_2 := \langle 2, 1-\sqrt{-5}\rangle,\ \mathfrak{p}_3 := \langle 3, \sqrt{-5}+1\rangle, \mathfrak{q}_3 := \langle 3, \sqrt{-5}-1\rangle,\ \mathfrak{p}_5 := \langle\sqrt{-5}\rangle,\ \mathfrak{p}_7 := \langle 7, 3+\sqrt{-5}\rangle, \mathfrak{q}_7 := \langle 7, 3-\sqrt{-5}\rangle$$

These ideals respectively have norms $2, 3, 3, 5, 7, 7$; since norms of ideals are multiplicative, we see that the following is an exhaustive list of all ideals J such that $N(J) \leq 10$, together with their norms:

$J =$	$\mathfrak{O}_F$	$\mathfrak{p}_2$	$\mathfrak{p}_2^2$	$\mathfrak{p}_2^3$	$\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_2\mathfrak{q}_3$	$\mathfrak{p}_2\mathfrak{p}_5$	$\mathfrak{p}_3$	$\mathfrak{p}_3^2$	$\mathfrak{q}_3$	$\mathfrak{q}_3^2$	$\mathfrak{p}_3\mathfrak{q}_3$	$\mathfrak{p}_7$	$\mathfrak{q}_7$
$N(J) =$	1	2	4	8	6	6	10	3	9	3	9	9	7	7

Notice that these ideals are all distinct, by unique factorisation of ideals.

Example 6.6. It is a fact that the ring of integers of $\mathbb{Q}[\sqrt[3]{5}]$ is $\mathbb{Z}[\sqrt[3]{5}]$; so we may apply the previous theorem with $\alpha = \sqrt[3]{5}$ and $f(X) = X^3 - 5$.

- $\boldsymbol{p = 2}$ **:** $X^3 - 5$ factors in $\mathbb{F}_2[X]$ as $X^3 - 5 = X^3 - 1 = (X - 1)(X^2 + X + 1)$ (notice that $X^2 + X + 1$ is irreducible mod 2 since it doesn't have a root mod 2), so the theorem implies that the prime ideal factorisation of $\langle 2\rangle$ is $\langle 2\rangle = \langle 2, \sqrt[3]{5} - 1\rangle\langle 2, \sqrt[3]{25} + \sqrt[3]{5} + 1\rangle$, and that these prime ideals on the right hand side have norm 2, 4 respectively.
- $\boldsymbol{p = 3}$ **:** $X^3 - 5$ factors in $\mathbb{F}_3[X]$ as $X^3 - 5 = X^3 - 2^3 = (X - 2)^3$, so the prime ideal factorisation of $\langle 3\rangle$ is $\langle 3\rangle = \langle 3, \sqrt[3]{5} - 2\rangle^3$.

Example 6.7. Suppose that $\mathfrak{O}_F = \mathbb{Z}[\alpha]$, where the minimal polynomial $f(X) \in \mathbb{Z}[X]$ satisfies Eisenstein's criterion for some prime number $p \in \mathbb{N}$. Then $f(X) \equiv X^n \bmod p$, so

$$\langle p\rangle = \mathfrak{p}^n$$

where $\mathfrak{p}$ is the prime ideal $\mathfrak{p} = \langle p, \alpha\rangle = \langle\alpha\rangle$, which has norm $N(\mathfrak{p}) = p$.

Example 6.5 shows, at least in principle, how we can exhaustively list all the ideals J of the ring of integers of a number field of norm $N(J)$ less than some fixed bound. But what is a reasonable bound if we wish to list all ideals up to principal equivalence, thus offering a representative of every element of the class group? This is offered by the next lemma.

We must first recall the constant C defined in lemma 5.6. If F is a number field and $\omega_1, \dots, \omega_n \in \mathfrak{D}_F$ is an integral basis, then let $(b_{r,i,j})_{i,j}$ be the matrix for multiplication by ω_r with respect to this basis, and set

$$C := \sum_{\sigma \in \mathrm{Sym}(n)} \prod_{i=1}^{n} \sum_{r=1}^{n} |b_{r,i,\sigma(i)}|$$

From now on C will be called the *Hurwitz constant* of F (don't forget that it depends on the choice of integral basis).

Proposition 6.8. *Let F be a number field; fix an integral basis $\omega_1, \dots, \omega_n \in \mathfrak{D}_F$ and let $C \in \mathbb{N}$ be the Hurwitz constant above. Then any non-zero ideal $I \subseteq \mathfrak{D}_F$ is principally equivalent to a non-zero ideal J such that $N(J) \leq C$. In other words,*

$$Cl_F = \{[J] : J \subseteq \mathfrak{D}_F \text{ a non-zero ideal s.t. } N(J) \leq C\}$$

Proof. Let I' be a non-zero ideal such that $I'I$ is principal (e.g. there exists $k \geq 1$ such that $I' = I^{k-1}$ works, by corollary 5.10). Now take $c \in \mathbb{N}$ large enough so that

$$(1 + c^{-1} N(I')^{-1/n})^n < 1 + \frac{1}{C}$$

and put $I'' = cI'$, which also has the property that $I''I$ is principal.

Put

$$S = \{\alpha = \sum_{i=1}^{n} c_i \omega_i : \ b_i \in \mathbb{N},\ 0 \leq b_i \leq N(I'')^{1/n}\} \subset \mathfrak{D}_F,$$

which has size $\#S = (\lfloor N(I'')^{1/n} \rfloor + 1)^n > N(I'')$. Since $\mathfrak{D}_F / I''$ has $N(I'')$ elements, the pigeonhole principle implies that there must be distinct $\alpha, \beta \in S$ such that $\alpha \equiv \beta \bmod I''$; put $\gamma := \alpha - \beta \neq 0$.

So $\langle \gamma \rangle \subseteq I''$ and therefore $\langle \gamma \rangle = I''J$ for some non-zero ideal $J \subseteq \mathfrak{D}_F$. Multiply both sides by I, noting that II'' is principal, to see that $J \sim I$. It remains to prove that $|N(J)| \leq C$.

Write $\gamma = \sum_{i=1}^{n} b_i \omega_i$ with $c_i \in \mathbb{Z}$; since $\alpha, \beta \in S$, we see that $|b_i| \leq N(I'')^{1/n} + 1$ for all i; therefore

$$|N_{F/\mathbb{Q}}(\gamma)| \leq C \max\{|c_1|, \dots, |c_n|\}^n \leq C(N(I'')^{1/n} + 1)^n,$$

where the first inequality follows just as it did for δ in the proof of lemma 5.6. Moreover, $|N_{F/\mathbb{Q}}(\gamma)| = N(I''J) = N(I'')N(J)$, so

$$\begin{aligned} |N(J)| &\leq CN(I'')^{-1}(N(I'')^{1/n} + 1)^n \\ &= C(1 + N(I'')^{-1/n})^n \\ &= C(1 + c^{-1}N(I'')^{-1/n})^n \\ &< C + 1. \end{aligned}$$

Thus $N(J) \leq C$, as required. □

Exercise 6.2. Let F be a number field and $I \subseteq \mathfrak{D}_F$ a non-zero ideal. Prove that if $\mathfrak{p}$ is a prime ideal occurring in the ideal factorisation of I, then $\mathfrak{p}$ sits over a prime number p which divides $N(I)$.

Corollary 6.9. *Let F be a number field, and let C be the Hurwitz constant for some choice of integral basis. Then Cl_F is generated by the classes of prime ideals sitting over (positive) primes numbers which are $\leq C$.*

Proof. By the previous proposition, any element of the class group can be represented as $[J]$, where $N(J) \leq C$. Let $J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the prime ideal factorisation of J. Then $[J] = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_r]^{e_r}$ in Cl_F, and the previous exercise implies that each $\mathfrak{p}_i$ sits over a prime number which divides $N(J)$, hence is $\leq C$. □

Remark 6.10 (Minkowski's bound)**.** As we shall see, the Hurwitz constant C works well for computing class group of small number fields, but a much better result is called *Minkowski's bound*, which we will not prove in the course but which will be useful several times. It states that if F is a number field, then proposition 6.8, and hence corollary 6.9, remain true if C is replaced by the real number

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta_F|^{1/2},$$

where

- $n = |F : \mathbb{Q}|$.
- Δ_F is the absolute discriminant of F.
- r_2 is half the number of field embeddings of F into $\mathbb{C}$ which do *not* have image in $\mathbb{R}$ (i.e., if $F = \mathbb{Q}(\alpha)$ then r_2 is half the number of conjugates of α which are not in $\mathbb{R}$).

7 Calculations of class groups of quadratic extensions, and applications

Let $F = \mathbb{Q}(\sqrt{d})$ for a square-free integer $d \in \mathbb{Z} \setminus \{0, 1\}$. What do we know about the class group of F? In fact, all we have proved so far is that:

- If $d = -1, -2, -3, -7, -11$, then $|N_{F/\mathbb{Q}}|$ is a Euclidean norm on $\mathfrak{D}_F$ and so $h_F = 1$. See exercise 5.1.
- If $d = -5, -10, -14$ then $\mathfrak{D}_F$ if not a PID and so $h_F > 1$.

In this section we will improve the state of this list! As we do so, we will obtain applications to Diophantine equations.

However, to illustrate the difficulty of the problem, we mention the following results and conjectures:

- $|N_{F/\mathbb{Q}}|$ is a Euclidean norm on $\mathfrak{D}_F$ if and only if d is one of the following values:

  $$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

  We will prove most of the "if" direction in section 7.11.
- If $d = 69$ then $\mathfrak{D}_F$ is a Euclidean domain, but the Euclidean norm is *not* $|N_{F/\mathbb{Q}}|$.

  (See D. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscripta Math. 83 (1994), no. 3–4, 327–330.)
- $h_F \to \infty$ as $d \to -\infty$ ("Gauss conjecture", proved in 1934 by H. Heilbronn). In other words, for any fixed value of h, there are only finitely many square-free $d < 0$ for which $\mathbb{Q}(\sqrt{d})$ has class number h.

  For actual lists of values of d, given h in the range $1 \le h \le 100$, see M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. 73 (2004), no. 246, 907–938, which required seven months of computer run time on an ordinary desktop machine.
- Conversely, Gauss also conjectured that there are infinitely many square-free $d > 1$ for which $\mathfrak{D}_F$ is a PID; this conjecture remains wide open. In the 80s this prediction was made more precise via the so-called Cohen–Lenstra heuristics; for example, it is now believed that $\mathfrak{D}_F$ will be a PID for about 75.446% values of positive, square-free d.

Here is a table of the class numbers of quadratic number field when $|d| < 20$; we will prove almost all of these:

$d =$	-19	-17	-15	-14	-13	-11	-10	-7	-6	-5	-3	-2	-1	2	3	5	6	7	10	11	13	14	15	17	19
$h_F =$	1	4	2	4	2	1	2	1	2	2	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1

(The only cases where the structure of the class group is not obvious is $d = -14, -17$. If $d = -14$ then Cl_F is cyclic of order 4, generated by either of the prime ideals sitting over 3. If $d = -17$ I don't know yet...) To prove these and give applications we need to start by knowing the Hurwitz bound C for F:

Lemma 7.1. *Let $F = \mathbb{Q}(\sqrt{d})$ for a square-free integer $d \in \mathbb{Z} \setminus \{0, 1\}$. Then:*

- *If $d \equiv 2, 3$ mod 4 and we take $1, \sqrt{d}$ as integral basis, then $C = |d| + 1$.*
- *If $d \equiv 1$ mod 4 and we take $1, \frac{1+\sqrt{d}}{2}$ as integral basis, then $C = \left|\frac{d-1}{4}\right| + 2$.*

Proof. We only treat the case that $d \equiv 2, 3 \bmod 4$. The matrices for multiplication by 1 and multiplication by $\sqrt{d}$ are respectively given by

$$(b_{1,i,j}) := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (b_{2,i,j}) := \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}.$$

Recalling that $C = \sum_{\sigma \in \mathrm{Sym}(n)} \prod_{i=1}^{n} \sum_{r=1}^{n} |b_{r,i,\sigma(i)}|$, we make the following calculations:

- $\sigma = \mathrm{id}$, $i = 1$: Then $\sum_{r=1}^{n} |b_{r,i,\sigma(i)}| = |b_{1,1,1}| + |b_{2,1,1}| = 1 + 0 = 1$.
- $\sigma = \mathrm{id}$, $i = 2$: Then $\sum_{r=1}^{n} |b_{r,i,\sigma(i)}| = |b_{1,2,2}| + |b_{2,2,2}| = 1 + 0 = 1$.
- $\sigma =$ transpose, $i = 1$: Then $\sum_{r=1}^{n} |b_{r,i,\sigma(i)}| = |b_{1,1,2}| + |b_{2,1,2}| = 0 + |d| = |d|$.
- $\sigma =$ transpose, $i = 2$: Then $\sum_{r=1}^{n} |b_{r,i,\sigma(i)}| = |b_{1,2,1}| + |b_{2,2,1}| = 0 + 1 = 1$.

Therefore

$$C = 1 \cdot |d| + 1 \cdot 1 = |d| + 1,$$

as claimed. □

Remark 7.2. For comparative purposes, we also calculate Minkowski's bound from remark 6.10. Recall from exercise 4.2 that $\Delta_F = 4d$ if $d \equiv 2, 3 \bmod 4$ and $= 4$ if $d \equiv 1 \bmod 4$. Moreover, the field embedding number r_2 which appears in Minkowski's bound is given by $r_2 = 1$ if $d < 0$ and $= 0$ if $d > 0$. Therefore Minkowski's bound is

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta_F|^{1/2} = \frac{1}{2} \times \begin{Bmatrix} \frac{4}{\pi} & \text{if } d < 0 \\ 1 & \text{if } d > 0 \end{Bmatrix} \times \begin{Bmatrix} 2\sqrt{|d|} & \text{if } d \equiv 2, 3 \bmod 4 \\ \sqrt{|d|} & \text{if } d \equiv 1 \bmod 4 \end{Bmatrix}$$

For example, if d is negative and $\equiv 2$ or $3 \bmod 4$, then Minkowski's bound is $\frac{4}{\pi}\sqrt{|d|}$, which is (much) less, hence better, than Hurwitz's bound of $|d| + 1$. We will avoid using Minkowski's bound as much as possible, since we have not proved it, but will resort to it to compute the class group of $F(\sqrt{d})$ for certain $d \ll 0$.

7.1 $d = -5$

We may finally calculate our first example of a non-trivial class group:

Theorem 7.3. *Let $d = -5$ and $F = \mathbb{Q}(\sqrt{-5})$. Then Cl_F is a cyclic group of order 2, generated by the class of any non-principal ideal, such as $\langle 3, 1 + \sqrt{-5}\rangle$. Therefore, if I is a non-zero ideal of $\mathfrak{D}_F$, we deduce that:*

(i) I is either principal or principally equivalent to $\langle 3, 1 + \sqrt{-5}\rangle$.

(ii) I^2 is princpial

Any two non-principal ideals are principally equivalent.

Proof. The Hurwitz bound is $C = 6$, so corollary 6.9 tells us that the class group Cl_F is generated by the classes of prime ideals sitting over $2, 3$ and 5. By examples 6.5, we know that

$$\begin{aligned} \langle 2\rangle &= \mathfrak{p}_2^2, \text{ where } \mathfrak{p}_2 := \langle 2, 1 - \sqrt{-5}\rangle^2 \\ \langle 3\rangle &= \mathfrak{p}_3\mathfrak{q}_3, \text{ where } \mathfrak{p}_3 := \langle 3, 1 + \sqrt{-5}\rangle,\ \mathfrak{q}_3 := \langle 3, 1 - \sqrt{-5}\rangle \\ \langle 5\rangle &= \mathfrak{p}_5^2, \text{ where } \mathfrak{p}_5 := \langle \sqrt{-5}\rangle. \end{aligned}$$

So Cl_F is generated by $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3$ and $\mathfrak{p}_5$; the final of these is principal, so represents the trivial element in the class group and may be discarded. Also, $[\mathfrak{p}_3][\mathfrak{q}_3] = 1$ in Cl_F, so $[\mathfrak{p}_3] = [\mathfrak{q}_3]^{-1}$. Therefore Cl_F is generated by $\mathfrak{p}_2$ and $\mathfrak{p}_3$. But moreover $\mathfrak{p}_2 \sim \mathfrak{p}_3$, since

$$(1 - \sqrt{-5})\mathfrak{p}_3 = \langle 3 - 3\sqrt{-5}, 6\rangle = 3\mathfrak{p}_2;$$

hence Cl_F is cyclic, generated by $\mathfrak{p}_3$ (or by $\mathfrak{p}_2$, if you prefer).

Finally we claim that $\mathfrak{p}_3^2$ is principal, for which we point out a general principle:

If F is a number field, $I \subseteq \mathfrak{D}_F$ is a non-zero ideal, and $\alpha \in I$ satisfies $|N_{F/\mathbb{Q}}(\alpha)| = N(I)$, then $I = \langle \alpha \rangle$. (Proof: $|N_{F/\mathbb{Q}}(\alpha)| = N(\langle \alpha \rangle)$, so $\langle \alpha \rangle \subseteq I$ is an inclusion of ideals with the same norm, whence an equality.) So to prove that I is principal, you only need to find an element $\alpha \in I$ with $|N_{F/\mathbb{Q}}(\alpha)| = N(I)$.

Since $N(\mathfrak{p}_3)^2 = 9$, in order to prove $\mathfrak{p}_3^2$ is principal we must merely show that it contains an element α with $|N_{F/\mathbb{Q}}(\alpha)| = 9$. The only elements of $\mathfrak{D}_F$ with norm ± 9 are $\pm 2 \pm \sqrt{-5}$ and ± 3. Well,

$$\mathfrak{p}_3^2 = \langle 9, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5} \rangle,$$

which is easily checked to contain $2 - \sqrt{-5}$; hence $\mathfrak{p}_3^2 = \langle 2 - \sqrt{-5} \rangle$.

Since $\mathfrak{D}_F$ has no element of norm 3, the ideal $\mathfrak{p}_3$ is not principal; so this completes the proof that Cl_F is cyclic of order two generated by $[\mathfrak{p}_3]$.

If $I \subseteq \mathfrak{D}_F$ is a non-zero ideal, then either $[I] = 1$ in Cl_F, i.e. I is principal, or $[I] = [\mathfrak{p}_3]$, i.e. I is principally equivalent to $\mathfrak{p}_3$. In any case, $[I^2] = [I]^2 = 1$, so I^2 is principal. □

We have just computed our first example of a non-trivial class group, and so it is a good moment to ask "Why?". The following lemma, whose proof if very important since we will use it as an opportunity to point out several tools, demonstrates how the class group can be used. We will also show in the proof how, in the special case that $\mathfrak{D}_F$ is a UFD, the theory of ideals and the class group can be completely avoided. This accurately depicts the historical development of algebraic number theory: under the erroneous belief that $\mathfrak{D}_F$ was alway a UFD, it was seen to be a useful too for solving Diophantine equations, and when mathematicians realised their error, they studied ideals and introduced the class group to remedy the problem.

Lemma 7.4. *Let $d < 0$ be a negative square-free integer such that $d \equiv 2$ or $3 \bmod 4$, and suppose that there exist integers x, y satisfying $y^3 = x^2 - d$. Let $F = \mathbb{Q}(\sqrt{d})$. If h_F is not divisible by 3 then there exists $\alpha \in \mathfrak{D}_F$ such that*

$$x + \sqrt{d} = \alpha^3.$$

Hence there exists an integer $n \in \mathbb{Z}$ such that $x = n(n^2 + 3d)$ and $3n^2 = \pm 1 - d$.

Proof. We claim that y is odd and that x, y are coprime. Firstly, if y were even then $x^2 \equiv 2$ or $3 \bmod 4$, which is impossible. Secondly, if a prime number p were to divide both x and y, then $p^2 | x^2 - y^3 = d$, which contradicts d being square-free. So y is odd and x, y are coprime.

Let's now make the wild assumption that $\mathfrak{D}_F$ is actually a UFD (equivalently, a PID) and show how to easily finish the proof. In $\mathfrak{D}_F$ we may write $y^3 = (x + \sqrt{d})(x - \sqrt{d})$. We claim that $x + \sqrt{d}$ and $x - \sqrt{d}$ are coprime, which in a UFD means that the two elements have no common (non-unit) divisor. So, for a contradiction, suppose that we can write $x + \sqrt{d} = \alpha t$, $x - \sqrt{d} = \beta t$, where $\alpha, \beta, t \in \mathfrak{D}_F$, and t is not a unit. Notice that $2x = (a + b)t$ and $y = abt^2$, and take norms:

$$4x^2 = N_{F/\mathbb{Q}}(a + b) N_{F/\mathbb{Q}}(t), \qquad y^6 = N_{F/\mathbb{Q}}(ab) N_{F/\mathbb{Q}}(t)^2$$

Since t is not a unit, its norm is not ± 1. Since y is odd, the right equation shows that $N_{F/\mathbb{Q}}(t)$ is divisible by an odd prime number p, and then also $p | y$; but then the left equation shows that $p | x$, contradicting the coprimality of x and y. This contradiction shows that indeed $x + \sqrt{d}$ and $x - \sqrt{d}$ are coprime.

But if a product of two coprime elements in a UFD is a cube, then each element must be an associate of a cube: this is easily proved by looking at the unique factorisation of the two elements, and the reader should check if uncertain. Since $(x + \sqrt{d})(x - \sqrt{d}) = y^3$, we apply this to deduce that $x + \sqrt{d} = u\alpha^3$ for some $u, \alpha \in \mathfrak{D}_F$, with u a unit. But $\mathfrak{D}_F^\times = \{v \in \mathfrak{D}_F : N_{F/\mathbb{Q}}(v) = \pm 1\} = \{\pm 1\}$; if $u = -1$ replace α by $-\alpha$. We have written $x + \sqrt{d} = \alpha^3$, as desired.

Finally, writing $\alpha = n + m\sqrt{d}$ for some $n, m \in \mathbb{Z}$, we obtain

$$x + \sqrt{d} = \alpha^3 = n(n^2 + 3m^2 d) + m(3n^2 + m^2 d)\sqrt{d},$$

so we see that

$$m(3n^2 + m^2) = 1, \quad n(n^2 + 3m^2 d) = x.$$

Hence $m = \pm 1$, and so $-d = 3n^2 \pm 1$, $x = n(n^2 + 3d)$.

Now we drop the assumption that $\mathfrak{D}_F$ is a UFD, and show how to rescue the result under the much weaker assumption that $3 \nmid h_F$, using the theory of ideals and the class group which we have developed. Again, we may write $y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$ in $\mathfrak{D}_F$, and now we claim that the *ideals* $\langle x + \sqrt{-5}\rangle$ and $\langle x - \sqrt{-5}\rangle$ are coprime, i.e. that they are contained in no common proper ideal. If not, then there is a prime ideal $\mathfrak{p} \subseteq \mathfrak{D}_F$ such that $\mathfrak{p} \ni (x + \sqrt{-5}), (x - \sqrt{-5})$; so $\mathfrak{p}$ contains $2x$ and y. But y is odd, so if 2 is also in $\mathfrak{p}$ then $1 \in \mathfrak{p}$, which is impossible; therefore $2 \notin \mathfrak{p}$, so $x \in \mathfrak{p}$. Hence $x, y \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for whichever prime number p sits under $\mathfrak{p}$; this contradicts coprimality of x and y. This contradiction shows that indeed $\langle x + \sqrt{d}\rangle$ and $\langle x - \sqrt{d}\rangle$ are coprime ideals.

Under the wild assumption that $\mathfrak{D}_F$ was a UFD, we deduced that the elements $x + \sqrt{d}$ and $x - \sqrt{d}$ were cubes. Now we must work with ideals:

> If $\mathfrak{D}$ is a Dedekind domain, and $I_1, I_2 \subseteq \mathfrak{D}$ are coprime ideals such that $I_1 I_2 = J^k$ for some ideal J and $k > 0$, then there exist ideals J_1, J_2 such that $I_1 = J_1^k$ and $I_2 = J_2^k$. That is, if a product of coprime ideals is an k^{th} power, then each ideal is already a k^{th} power. (See the exercise after this lemma.)

Therefore we may write $\langle x + \sqrt{d}\rangle = I^3$ for some ideal $I \subseteq \mathfrak{D}_F$. The next observation is the fundamental application of the theory of the class group:

> Since $3 \nmid h_F$, the class group Cl_F contains no element of order 3. So, since I^3 is principal, I must already be principal!

Hence $I = \langle \alpha \rangle$ for some $\alpha \in \mathfrak{D}_F$, and so $\langle x + \sqrt{d}\rangle = \langle \alpha^3 \rangle$; this means $x + \sqrt{d} = u\alpha^3$ for some unit $u \in \mathfrak{D}_F$, and the final line of the proof is just as it was in the UFD case. □

Exercise 7.1. Carefully check the (relatively easy but important!) omitted claims in the previous proof:

(i) Show that if R is a UFD, and that $x, y \in R$ are coprime elements such that xy is a k^{th} power, then x and y are associates of k^{th} power.

(ii) Prove the first of the boxed claims in the previous proof.

(iii) Prove the following general version of the second boxed claim: if F is a number field and $I \subseteq \mathfrak{D}_F$ is a non-zero ideal such that I^k is principal for some integer k which is coprime to h_F, then I is already principal.

Theorem 7.5. *There are no integer solutions to $Y^3 = X^2 + 5$.*

Proof. Let $F = \mathbb{Q}(\sqrt{-5})$. For a contradiction, suppose that $x, y \in \mathbb{Z}$ satisfy $y^3 = x^2 + 5$. By the previous theorem, $h_F = 2$ is not divisible by 3, so the previous lemma plies that $3n^2 = 5 \pm 1$ for some integer n. But this is clearly impossible, so such x, y cannot not exist. □

Exercise 7.2. Check that this theorem could not have been proved using congruence arguments, by showing that $Y^3 = X^2 + 5$ has integer solutions mod n for any $n \in \mathbb{N}$.

7.2 $d = -6$

Let $F = \mathbb{Q}(\sqrt{-6})$. The Hurwitz bound is $C = 7$, so Cl_F is generated by the primes ideals sitting over $2, 3, 5, 7$.

$$\begin{aligned}
\langle 2\rangle &= \langle 2, \sqrt{-6}\rangle^2 \quad \text{since } X^2 + 6 \equiv X^2 \bmod 2\\
\langle 3\rangle &= \langle 3, \sqrt{-6}\rangle^2 \quad \text{since } X^2 + 6 \equiv X^2 \bmod 3\\
\langle 5\rangle &= \langle 5, 2 + \sqrt{-6}\rangle\langle 5, 2 - \sqrt{-6}\rangle \quad \text{since } X^2 + 6 \equiv (X + 2)(X - 2) \bmod 5\\
\langle 7\rangle &= \langle 7, 1 + \sqrt{-6}\rangle\langle 7, 1 - \sqrt{-6}\rangle \quad \text{since } X^2 + 6 \equiv (X + 1)(X - 1) \bmod 7
\end{aligned}$$

The prime ideals over 7 are principal, generated respectively by $1+\sqrt{-6}$ and $1-\sqrt{-6}$. Also, $\langle 2, \sqrt{-6}\rangle\langle 3, \sqrt{-6}\rangle = \langle\sqrt{-6}\rangle$, so the prime ideals over 2 and 3 are principally equivalent to one another. Finally, $\langle 2, \sqrt{-6}\rangle\langle 5, 2 + \sqrt{-6}\rangle$ contains $2 - \sqrt{-6}$, which has norm 10, and hence this element generates the product.

In conclusion, Cl_F is generated by $\langle 2, \sqrt{-6}\rangle$, which is non-principal by norm considerations. So Cl_F is cyclic of order 2.

Imitating theorem 7.5, one shows that $Y^3 = X^2 + 6$ has no integer solutions.

7.3 $d = -7$

Let $F = \mathbb{Q}(\sqrt{-7})$. The Hurwitz bound is $C = 4$, so we factor (using $\alpha = \frac{1+\sqrt{-7}}{2}$, $f(X) = X^2 - X + 2$)

$$\begin{aligned}
\langle 2\rangle &= \langle 2, \tfrac{1+\sqrt{-7}}{2}\rangle\langle 2, \tfrac{1-\sqrt{-7}}{2}\rangle\\
\langle 3\rangle &\text{ is prime since } f(X) = (X + 1)^2 - 2 \bmod 3
\end{aligned}$$

The prime ideals over 2 are principal, each generated by their second generator. Hence $h_F = 1$, i.e. $\mathfrak{D}_F$ is a PID. Indeed, this calculation was unnecessary since we already know it is a Euclidean domain.

Imitating theorem 7.5, one shows that $Y^3 = X^2 + 7$ has no integer solutions.

7.4 $d = -10$

Let $F = \mathbb{Q}(\sqrt{-10})$. The Hurwitz bound is $C = 11$, so we factor

$$\begin{aligned}
\langle 2\rangle &= \langle 2, \sqrt{-10}\rangle^2\\
\langle 3\rangle &\text{ is prime since 2 is not a quadratic residue mod 3}\\
\langle 5\rangle &= \langle 5, \sqrt{-10}\rangle^2\\
\langle 7\rangle &\text{ is prime since 3 is not a quadratic residue mod 3}\\
\langle 11\rangle &= \langle 11, 1 + \sqrt{-10}\rangle\langle 11, 1 - \sqrt{-10}\rangle
\end{aligned}$$

The prime ideals sitting over 11 are principal, each generated by their second generator. Hence Cl_F is generated by $\mathfrak{p}_2 = \langle 2, \sqrt{-10}\rangle$ and $\mathfrak{p}_5 = \langle 5, \sqrt{-10}\rangle$. But it is easy to see that $\mathfrak{p}_2\mathfrak{p}_5 = \langle\sqrt{-10}\rangle$, so Cl_F is generated by $[\mathfrak{p}_2]$, which has order 2.

Hence Cl_F is again a cyclic group of order 2, and the usual argument shows that $Y^3 = X^2 + 10$ has no integer solutions.

7.5 $d = -13$

Let $F = \mathbb{Q}(\sqrt{-13})$. The Hurwitz bound is $C = 14$, so we factor

$$\begin{aligned}
\langle 2\rangle &= \langle 2, 1+\sqrt{-13}\rangle^2 \\
\langle 3\rangle &\text{ is prime since 2 is not a quadratic residue mod 3} \\
\langle 5\rangle &\text{ is prime since 2 is not a quadratic residue mod 5} \\
\langle 7\rangle &= \langle 7, 1+\sqrt{-13}\rangle\langle 7, 1-\sqrt{-13}\rangle \\
\langle 11\rangle &= \langle 11, 3+\sqrt{-13}\rangle\langle 11, 3-\sqrt{-13}\rangle \\
\langle 13\rangle &= \langle \sqrt{-13}\rangle^2
\end{aligned}$$

Hence Cl_F is generated by $\mathfrak{p}_2 = \langle 2, 1+\sqrt{-13}\rangle$, $\mathfrak{p}_7 = \langle 7, 1+\sqrt{-13}\rangle$ and $\mathfrak{p}_{11} = \langle 11, 3+\sqrt{-13}\rangle$, and we must now check relations between these.

$\mathfrak{p}_2\mathfrak{p}_7$ contains both $7(1+\sqrt{-13})$ and $2(1+\sqrt{-13})$, hence contains $1+\sqrt{-13}$; since $N_{F/\mathbb{Q}}(1+\sqrt{-13}) = 14 = N(\mathfrak{p}_2\mathfrak{p}_7)$, we deduce that $\mathfrak{p}_2\mathfrak{p}_7 = \langle 1+\sqrt{-13}\rangle$ is principal.

Next we look at

$$\mathfrak{p}_2\mathfrak{p}_{11} = \langle 22, 6+2\sqrt{-13}, 11+11\sqrt{-13}, -1+4\sqrt{-13}\rangle,$$

which has norm 22. The only elements of $\mathfrak{D}_F$ with norm ± 22 are $\pm 3 \pm \sqrt{-13}$, and indeed $3+\sqrt{-13} = 22 + (11+11\sqrt{-13}) - 5(6+2\sqrt{-13}) \in \mathfrak{p}_2\mathfrak{p}_{11}$, so that $\mathfrak{p}_2\mathfrak{p}_{11} = \langle 3+\sqrt{-13}\rangle$.

This proves that Cl_F is cyclic, generated by $\mathfrak{p}_2$. But $\mathfrak{p}_2^2 = \langle 2\rangle$ is principal, and $\mathfrak{p}_2$ is not principal since $\mathfrak{D}_F$ contains no element of norm 2. Therefore Cl_F is cyclic of order 2 and $h_F = 2$.

Theorem 7.6. *The only integer solutions to the equation $Y^3 = X^2 + 13$ are $x = \pm 70$, $y = 17$.*

Proof. Suppose that $x, y \in \mathbb{Z}$ satisfy $y^3 = x^2 + 13$. Then lemma 7.4 implies (since we now know that $3 \nmid h_F$) that there exists $n \in \mathbb{Z}$ such that $x = n(n^2 - 39)$ and $3n^2 = 13 \pm 1$. This obviously forces $n = \pm 2$, whence $x = \pm 70$ and so $y = \sqrt[3]{70^2 + 13} = 17$. □

Notice that the theorem not only told us that $(\pm 70, 17)$ are the only solutions to the equation, but the proof actually *constructed* the solutions for us.

7.6 $d = -14$

Let $F = \mathbb{Q}(\sqrt{-14})$. The Hurwitz bound is $C = 15$, so we factor

$$\begin{aligned}
\langle 2\rangle &= \langle 2, \sqrt{-14}\rangle^2 \\
\langle 3\rangle &= \langle 3, 1+\sqrt{-14}\rangle\langle 3, 1-\sqrt{-14}\rangle \\
\langle 5\rangle &= \langle 5, 1+\sqrt{-14}\rangle\langle 5, 1-\sqrt{-14}\rangle \\
\langle 7\rangle &= \langle 7, \sqrt{-14}\rangle^2 \\
\langle 11\rangle &\text{ is prime since 8 is not a quadratic residue mod 11} \\
\langle 13\rangle &\text{ is prime since 12 is not a quadratic residue mod 13}
\end{aligned}$$

So Cl_F is generated by $\mathfrak{p}_2 = \langle 2, \sqrt{-14}\rangle$, $\mathfrak{p}_3 = \langle 3, 1+\sqrt{-14}\rangle$, $\mathfrak{p}_5 = \langle 5, 1+\sqrt{-14}\rangle$, and $\mathfrak{p}_7 = \langle 7, \sqrt{-14}\rangle$.

It is easy to see that $\mathfrak{p}_2\mathfrak{p}_7 = \langle \sqrt{-14}\rangle$. Moreover, $\mathfrak{p}_5\mathfrak{p}_3$ contains both $3(1+\sqrt{-14})$ and $5(\sqrt{-14})$, hence contains $1+\sqrt{-14}$; comparing norms we deduce $\mathfrak{p}_5\mathfrak{p}_3 = \langle 1+\sqrt{-14}\rangle$.

Exercise 7.3. Considering norms, show that $\mathfrak{p}_3, \mathfrak{p}_3^2$, and $\mathfrak{p}_3^3$ are not principal ideals. On the other hand, show that $\mathfrak{p}_3^2\mathfrak{p}_2$ is principal.

Theorem 7.7. *$F = \mathbb{Q}(\sqrt{-14})$. Then Cl_F is cyclic of order 4, generated by the class of $\mathfrak{p}_3$.*

Proof. The proceeding calculations show that Cl_F is generated by $[\mathfrak{p}_3]$, and that this generator has order ≥ 4. But the exercise also shows that $\mathfrak{p}_3^2\mathfrak{p}_2$ is principal; hence $\mathfrak{p}_3^4\mathfrak{p}_2^2 = \mathfrak{p}_3^4 2$ is principal, and so $[\mathfrak{p}_2]^4 = 1$. □

The usual argument now shows that $Y^3 = X^2 + 14$ has no integer solutions.

7.7 $d = -15$

$F = \mathbb{Q}(\sqrt{-15})$. Since $-15 \equiv 1 \bmod 4$, the Hurwitz bound is $|\frac{-15-1}{4}|+2 = 6$, so we factor (using $\alpha = \frac{1+\sqrt{-15}}{2}$, $f(X) = X^2 - X + 4$)

$$\langle 2\rangle = \langle 2, \alpha\rangle\langle 2, 1+\alpha\rangle$$
$$\langle 3\rangle = \langle 3, 1+\alpha\rangle^2$$
$$\langle 5\rangle = \langle 5, 2+\alpha\rangle^2$$

To finish: Cl_F will be cyclic of order 2.

7.8 $d = -17, -19$

These are going to be tough with Hurwitz's bound.

7.9 $d = -23$

$F = \mathbb{Q}(\sqrt{-23})$. The Hurwitz bound is $C = |\frac{-23-1}{4}| + 2 = 8$, so Cl_F is generated by the classes of prime ideals which sit over $2, 3, 5, 7$. Let $\alpha = \frac{1+\sqrt{-23}}{2}$, which has norm $N_{F/\mathbb{Q}}(\alpha) = 6$ and minimal polynomial $f(X) = X^2 - X + 6$. We factor:

p	$X^2 - X + 6 \bmod p$	$\langle p\rangle =$
2	$X(X-1)$	$\langle 2, \alpha\rangle\langle 2, 1-\alpha\rangle$
3	$X(X-1)$	$\langle 3, \alpha\rangle\langle 3, 1-\alpha\rangle$
5	$(X+2)^2 - 3$ is irred.	$\langle 5\rangle$
7	$(X+3)^2 - 3$ is irred.	$\langle 7\rangle$

Therefore Cl_F is generated by the classes of $\mathfrak{p}_2 = \langle 2, \alpha\rangle$ and $\mathfrak{p}_3 = \langle 3, \alpha\rangle$. But $\mathfrak{p}_2\mathfrak{p}_3$ contains α, which has norm $30 = N(\mathfrak{p}_2\mathfrak{p}_3)$; so $\mathfrak{p}_2\mathfrak{p}_3 = \langle\alpha\rangle$ and $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$. Hence Cl_F is cyclic, generated by $[\mathfrak{p}_2]$, whose order we must now compute.

Given integers n, m, we have $N_{F/\mathbb{Q}}(n+m\alpha) = (n+\frac{m}{2})^2 + 23\frac{m^2}{4} = n^2 + nm + 6m^2$, which is ≥ 6 if $m \geq 1$ and is $= n^2$ if $m = 0$. So there is no element in $\mathfrak{O}_F$ of norm ± 2, and the only element with norm ± 4 is 2 itself, which does not generate $\mathfrak{p}_2^2$ (otherwise $\mathfrak{p}_2 = \langle\alpha, 2-\alpha\rangle$, which is not true). Hence $\mathfrak{p}_2$ and $\mathfrak{p}_2^2$ are not principal. However,

$$\mathfrak{p}_2^3 = \langle 8, 4\alpha, 2\alpha^2 = -12 + 2\alpha, \alpha^3 = -6 - 5\alpha\rangle,$$

which contains $2 - \alpha$. Since $N_{F/\mathbb{Q}}(2-\alpha) = 8 = N(\mathfrak{p}_2^3)$, we deduce $\mathfrak{p}_2^3 = \langle 2-\alpha\rangle$.

Theorem 7.8. *The class group of $F = \mathbb{Q}(\sqrt{-23})$ is cyclic of order 3, generated by $[\mathfrak{p}_2]$.*

7.10 $d = -30$

$F = \mathbb{Q}(\sqrt{-30})$. The Hurwitz bound if $C = 31$, so Cl_F is generated by the prime ideas sitting over $2, 3, 5, \ldots, 31$, which is far too many to check by hand quickly! Instead we use Minkowski's bound, which we know from remark 7.2 is $\frac{4}{\pi}\sqrt{30} \approx 6.79$ in this case; hence Cl_F is actually generated by the prime ideals sitting over $2, 3, 5$.

p	$X^2 + 30 \bmod p$	$\langle p\rangle =$
2	X^2	$\langle 2, \sqrt{-30}\rangle^2$
3	X^2	$\langle 3, \sqrt{-30}\rangle^2$
5	X^2	$\langle 5, \sqrt{-30}\rangle^2$

In the obvious notation, we now know that Cl_F is generated by the classes of $\mathfrak{p}_2, \mathfrak{p}_3$, and $\mathfrak{p}_5$, which have norm $2, 3, 5$ respectively. Since $\mathfrak{O}_F$ has no elements of norm $\pm 2, \pm 3$, or ± 5, we see that $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$ are each non-trivial elements of order 2 in Cl_F.

Moreover, $\mathfrak{p}_2\mathfrak{p}_3$ contains both $\sqrt{-30} = 3\sqrt{-30} - 2\sqrt{-30}$ and 6, so $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ contains $\sqrt{-30} = 6\sqrt{-30} - 5\sqrt{-30}$; since $N_{F/\mathbb{Q}}(\sqrt{-30}) = 30 = N(\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5)$, we deduce $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 = \langle\sqrt{-30}\rangle$. Therefore

$$[\mathfrak{p}_5] = [\mathfrak{p}_5]^{-1} = [\mathfrak{p}_2][\mathfrak{p}_3],$$

so we now know Cl_F is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, which are non-trivial and have order 2.

We claim that $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$, or equivalently that $\mathfrak{p}_2\mathfrak{p}_3$ is not principal; but $\mathfrak{D}_F$ contains no element of order 6, proving the claim.

Theorem 7.9. *The class group of $F = \mathbb{Q}(\sqrt{-30})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with generators $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$*

Proof. We have proved that Cl_F is generated by two distinct elements, each having order 2. □

The usual argument shows that $Y^3 = X^2 + 30$ has no integer solutions.

7.11 $d = 2, 3, 5, 6, 7, 11, 13, 17, 21, 29, 33, 37, 41$

Reference: A. Oppenheim, *Quadratic fields with and without Euclid's algorithm*, Math. Ann. 109 (1934), no. 1, pp. 349–352.

Lemma 7.10. *Let $d = 2, 3, 6,$ or 7, and fix rational numbers $1 \leq a, b \leq \frac{1}{2}$. Consider the following inequalities, for varying integers x, y:*

$$P(x,y): \quad (x-a)^2 \geq 1 + d(y-b)^2$$
$$N(x,y): \quad d(y-b)^2 \geq 1 + (x-a)^2$$

Then $P(x,y)$ and $N(x,y)$ are simultaneously false for some pair of integers x, y.

Proof. $P(0,0)$ is clearly false, so if $N(0,0)$ is also false then we are done; so henceforth assume $N(0,0)$ is true, i.e. $db^2 \geq 1 + a^2$.

It now easily follows that $P(1,0)$ is false (for else $(1-a)^2 \geq 1 + db^2 \geq 2 + a^2 \geq 2$, which is absurd); so if $N(1,0)$ is also false then we are done; so henceforth assume $N(1,0)$ is true, i.e. $db^2 \geq 1 + (1-a)^2$.

Next, if $P(-1,0)$ were true, then

$$(1+a)^2 \geq 1 + db^2 \geq 2 + (1-a)^2, \tag{$\dagger$}$$

whence $4a \geq 2$ and so $a = \frac{1}{2}$; this would force the left and right sides of ($\dagger$) to both be $\frac{9}{4}$, whence $1 + db^2 = \frac{9}{4}$ and so $b^2 = \frac{5}{4d}$, which is easily seen to be absurd. Hence $P(-1,0)$ is *not* true. But since $1 \leq d < 8$ and $0 \leq b \leq \frac{1}{2}$, we have

$$db^2 < 2 \leq 1 + (1+a)^2,$$

i.e. $N(-1,0)$ is false. Therefore both $P(-1,0)$ and $N(-1,0)$ are false.

In conclusion, there exists a pair $(x,y) = (0,0), (1,0)$, or $(-1,0)$ for which $P(x,y)$ and $N(x,y)$ are simultaneously false. □

Theorem 7.11. *Let d be any of $2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41$, and put $F = \mathbb{Q}(\sqrt{d})$. Then $|N_{F/\mathbb{Q}}|$ is a Euclidean norm on $\mathfrak{D}_F$.*

Proof. According to exercise 5.1, we must prove that if $\gamma \in F$ then there exists $\omega \in \mathfrak{D}_F$ such that $|N_{F/\mathbb{Q}}(\alpha - \omega)| < 1$. We will only give the full proof in the cases that $d \not\equiv 1 \bmod 4$, i.e. $d = 2, 3, 6,$ or 7.

Let $\gamma = p + q\sqrt{d}$ for any $p, q \in \mathbb{Q}$; let $m, n \in \mathbb{Z}$ be the integers which are closest to p, q respectively, so that $a := |p - m|$ and $b := |q - n|$ are $\leq \frac{1}{2}$. By the previous lemma there are integers x, y such that

$$-1 + d(y - |q-n|)^2 < (x - |p-m|)^2 < 1 + d(y - |q-n|)^2$$

Set

$$y' = \begin{cases} x - m & \text{if } p \geq m \\ m - x & \text{if } p \leq m \end{cases} \qquad x' = \begin{cases} y - n & \text{if } q \geq n \\ n - y & \text{if } q \leq n \end{cases}$$

Then

$$-1 + d(y' - q)^2 < (x' - p)^2 < 1 + d(y' - q)^2,$$

i.e., $-1 < N_{F/\mathbb{Q}}(\gamma - \omega) < 1$, as desired. This completes the proof for those values of d which are $\not\equiv 1 \bmod 4$.

If $d \equiv 1 \bmod 4$ then replace the inequalities of the previous lemma by

$$P(x,y): \quad (x + \tfrac{1}{2}y - a)^2 \geq 1 + d(y - b)^2$$
$$N(x,y): \quad d(y - b)^2 \geq 1 + (x + \tfrac{1}{2}y - a)^2$$

Repeating the previous lemma and argument verbatim works whenever $1 \leq \frac{d}{4} < 8$, i.e. $d = 5, 13, 17, 21, 29$. To extend the proof to $d = 33, 37, 41$, one must continue the argument of the previous lemma to pairs (x, y) with $|x|, |y| \leq 2$. □

Remark 7.12. The previous theorem remains true for $d = 19, 57$, and 73, but these are much harder to prove. An even deeper theorem is that this is then the complete list of positive values of square-free $d > 1$ for which $|N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}|$ is a Euclidean norm on the ring of integers of $\mathbb{Q}(\sqrt{d})$. For a survey see §4.2 of

> Lemmermeyer, F., *The Euclidean algorithm in algebraic number fields*, 2004,
> `http://www.fen.bilkent.edu.tr/~franz/publ/survey.pdf`

8 Cyclotomic extensions and Fermat's Last Theorem

Our main source of examples so far has been the quadratic number fields. In this section we investigate the number field $F = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_m = e^{2\pi i/n}$ is a primitive n^{th} root of unity. In fact, we will restrict attention to the easiest case, namely n being a prime number, and describe both the ring of integers $\mathfrak{O}_F$ and its group of units. We will then apply our results to prove Fermat's Last Theorem in the so-called "weak, regular" case.

8.1 $\mathbb{Q}(\zeta)$ and its ring of integers.

Let $p \geq 3$ be a fixed prime number and set $\zeta = e^{2\pi i/p}$ and $F = \mathbb{Q}(\zeta)$.

Then ζ is an algebraic integer with minimal polynomial

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1,$$

by proposition 3.15. So $|F : \mathbb{Q}| = p - 1$ and $\mathbb{Z}[\zeta]$ is a subring of $\mathfrak{O}_F$. Our first goal is to prove that $\mathfrak{O}_F = \mathbb{Z}[\zeta]$; it requires some preliminary results:

Lemma 8.1. *Suppose that r, s are integers, neither divisible by p. Then*

$$\frac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^\times.$$

Proof. We may write $r \equiv st \bmod p$ for some $t \in \mathbb{Z}$. Then

$$\frac{\zeta^r - 1}{\zeta^s - 1} = \frac{\zeta^{st} - 1}{\zeta^s - 1} = 1 + \zeta^s + \zeta^{2s} + \cdots + \zeta^{(t-1)s} \in \mathbb{Z}[\zeta].$$

The same argument, after swapping r and s shows that $\frac{\zeta^s - 1}{\zeta^r - 1}$ is also in $\mathbb{Z}[\zeta]$, which completes the proof. □

Lemma 8.2. *There is a unit $u \in \mathbb{Z}[\zeta]^\times$ such that $p = u(1 - \zeta)^{p-1}$.*

Proof. We have

$$X^{p-1} + \cdots + X + 1 = \Phi_p(X) = \prod_{i=1}^{p-1}(X - \zeta^i),$$

and we evaluate at 1 to get $p = \prod_{i=1}^{p-1}(1-\zeta^i)$. But the previous lemma implies that $u_i := \frac{1-\zeta^i}{1-\zeta}$ is a unit of $\mathbb{Z}[\zeta]$, and so $u = u_1 \dots u_{p-1}$ has the desired property:

$$p = \prod_{i=1}^{p-1} u_i(1-\zeta) = u(1-\zeta)^{p-1}.$$

□

It is common to use the notation $\pi = 1 - \zeta$, and we will do so in the proof of the next result. For the moment notice just two things: $1, \pi, \dots, \pi^{p-2}$ are a basis for $F/\mathbb{Q}$, and $\mathbb{Z}[\pi] = \mathbb{Z}[\zeta]$.

Theorem 8.3. *As above, let $p \geq 3$ be a prime number, $\zeta := e^{2\pi i/p}$, and $F := \mathbb{Q}(\zeta)$. Then $\mathfrak{D}_F = \mathbb{Z}[\zeta]$.*

Proof. The inclusion $\supseteq$ has already been noted, so we suppose that $\alpha \in \mathfrak{D}_F$ and we will prove $\alpha \in \mathbb{Z}[\zeta]$. The proof proceeds by two steps, firstly using $\mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$, then $\mathfrak{D}_F$.

Since $1, \zeta, \dots, \zeta^{p-2}$ is a basis for $F/\mathbb{Q}$, we may write

$$\alpha = c_0 + c_1\zeta + \cdots + c_{p-2}\zeta^{p-2}$$

for some $c_0, \dots, c_{p-2} \in \mathbb{Q}$ (which we don't yet know are in $\mathbb{Z}$). For i an integer not divisible by p, the algebraic integer ζ^i generates F and has minimal polynomial $\Phi_p(X)$, whence

$$\mathrm{Tr}_{F/\mathbb{Q}}(\zeta^i) = -1$$

by the standard formula for the trace of an element in terms of its minimal polynomial. Therefore, for $0 \leq r \leq p-2$,

$$\begin{aligned}\mathrm{Tr}_{F/\mathbb{Q}}(\alpha\zeta^{-r}) &= \mathrm{Tr}_{F/\mathbb{Q}}(c_0\zeta^{-r} + \cdots + c_{r-1}\zeta^{-1} + c_r + c_{r+1}\zeta + \cdots + c_{p-2}\zeta^{p-2-r}) \\ &= -c_0 - \cdots - c_{r-1} + (p-1)c_r - c_{r-1} - \cdots - c_{p-2},\end{aligned}$$

which is in $\mathbb{Z}$ since $\alpha\zeta^{-r} \in \mathfrak{D}_F$. The same argument show that

$$\mathrm{Tr}_{F/\mathbb{Q}}(\alpha\zeta) = -c_0 - \cdots - c_{p-2}$$

is also in $\mathbb{Z}$. Comparing these we see that $pc_r \in \mathbb{Z}$ for $r = 0, \dots, p-2$, and so $p\alpha \in \mathbb{Z}[\zeta]$. Since $\mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$, we may therefore write

$$p\alpha = b_0 + b_1\pi + \cdots + b_{p-2}\pi^{p-2}$$

for some $b_0, \dots, b_{p-2} \in \mathbb{Z}$.

The next step of the proof takes place in $\mathfrak{D}_F$. To complete the proof it is enough to show that $b_0, \dots, b_{p-2}$ are divisible by p:

(i) The previous lemma implies $p \in \langle\pi\rangle$ and so $b_0 = p\alpha - (b_1\pi + \cdots + b_{p-1}\pi^{p-2}) \in \langle\pi\rangle \cap \mathbb{Z} = p\mathbb{Z}$.

(ii) Proceeding by induction, suppose $b_0, \dots, b_{s-1}$ can be written as $pb'_0, \dots, pb'_{s-1}$ for some $b'_0, \dots, b'_{s-1} \in \mathbb{Z}$. We now have

$$b_s\pi^s = p\alpha - p(b'_0 + \cdots + b'_{s-1}\pi^{s-1}) - (b_{s+1}\pi^{s+1} + \cdots + b_{p-2}\pi^{p-2}).$$

But $p \in \langle\pi\rangle^{p-1}$ (by the previous lemma) and $\alpha \in \mathfrak{D}_F$ (by assumption), so every term on the right of this expression belongs to $\langle\pi\rangle^{s+1}$, and therefore

$$b_s\pi^s \in \langle\pi\rangle^{s+1}.$$

So $b_s \in \langle\pi\rangle$, whence $b_s \in \langle\pi\rangle \cap \mathbb{Z} = p\mathbb{Z}$ completing the proof of our claim.

□

We now know that $F = \mathbb{Q}(\zeta)$ has ring of integers $\mathfrak{D}_F = \mathbb{Z}[\zeta]$, so an integral basis is $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$.

Example 8.4. Since

$$\mathrm{Tr}_{F/\mathbb{Q}}(\zeta^i) = \begin{cases} p-1 & p|i \\ -1 & p \nmid i, \end{cases}$$

we deduce that

$$\Delta_F = \Delta(1, \zeta, \ldots, \zeta^{p-2}) = \begin{pmatrix} p-1 & -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & -1 & -1 \\ -1 & -1 & \cdots & -1 & -1 & p-1 \\ -1 & \cdots & -1 & -1 & p-1 & -1 \\ \vdots & & \ddots & \ddots & & \vdots \\ -1 & -1 & -1 & p-1 & \cdots & -1 \\ -1 & -1 & p-1 & \cdots & -1 & -1 \end{pmatrix}$$

(i.e. -1s everywhere except for at the top left and along a diagonal strip). Some rather tedious combinatorics allows one to evaluate this as $\Delta_F = (-1)^{(p-1)/2} p^{p-2}$.

Our next goal is to describe some of the units in $\mathfrak{D}_F$. The proofs of the following lemma requires the use of some mild Galois theory. Notice that $\mathfrak{D}_F$ is closed under complex conjugation $x \mapsto \overline{x}$.

Lemma 8.5.

(i) Let $\alpha \in \mathbb{Z}^{alg}$ be an algebraic integer with the following property: all the conjugates of α have complex absolute value 1. Then α is a root of unity.

(ii) If $u \in \mathfrak{D}_F^\times$ then $u/\overline{u}$ is a root of unity.

Proof. For (i), set

$$S = \{\beta \in \mathbb{Z}[\alpha] : \text{ all conjugates of } \beta \text{ have complex absolute value } \leq 1\},$$

which is finte by exercise 4.1. We will show that $\alpha^r \in S$ for all $r \geq 0$, which obviously forces $\alpha^r = \alpha^s$ for some $s > r \geq 1$; but then $\alpha^{s-r} = 1$, which will complete the proof of the first claim.

Well, if β is a conjugate of α^r then there is a field embedding $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ such that $\sigma(\alpha^r) = \beta$. Then $\sigma(\alpha)$ is a conjugate of α, hence has complex absolute value 1; so $\beta = \sigma(\alpha)^r$ also has complex absolute value 1. So all conjugates of α have complex absolute value 1, and therefore $\alpha \in S$, as desired.

For (ii), since $F/\mathbb{Q}$ is a Galois extension, the conjugates of $\alpha := u/\overline{u} \in \mathfrak{D}_F$ are precisely

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(F/\mathbb{Q})\}.$$

The Galois group $\mathrm{Gal}(F/\mathbb{Q})$ not only contains complex conjugation, but it is an abelian group (isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$); this means that $\sigma(\overline{u}) = \overline{\sigma(u)}$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. So each conjugate of $u/\overline{u}$ has the form

$$\sigma(u/\overline{u}) = \sigma(u)/\overline{\sigma(u)}$$

for some $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$: this number obviously has complex absolute value 1. The first part of the lemma now implies that $u/\overline{u}$ is a root of unity. □

Proposition 8.6. *Let $u \in \mathfrak{D}_F^\times$. There there exist $v \in \mathfrak{D}_F^\times$, such that $\overline{v} = v$, and $r \in \mathbb{Z}$ such that*

$$u = \zeta^r v.$$

Proof. By the previous lemma $u/\overline{u}$ is a root of unity contained in $\mathfrak{D}_F$, hence equal to $\pm\zeta^s$ for some $s \in \mathbb{Z}$ (by Homework).

For a contradiction, suppose that $u/\overline{u} = -\zeta^s$ for some $s \in \mathbb{Z}$. Since we now know $\mathfrak{D}_F = \mathbb{Z}[\zeta]$, we may write $u = a_0 + \cdots + a_{p-2}\zeta^{p-2}$ for some $a_0, \ldots, a_{p-2} \in \mathbb{Z}$, and so

$$u \equiv a_0 + \cdots + a_{p-2} \bmod \langle 1 - \zeta \rangle$$

Similarly,

$$\overline{u} = a_0 + a_1\zeta^{-1} \cdots + a_{p-2}\zeta^{-(p-2)} \equiv a_0 + \cdots + a_{p-2} \equiv u = -\zeta^s\overline{u} \equiv -\overline{u} \bmod \langle 1 - \zeta \rangle.$$

Therefore $2\overline{u} \in \langle 1-\zeta \rangle$, which is a prime ideal by lemma 8.2; since $2 \notin \langle 1-\zeta \rangle \cap \mathbb{Z} = p\mathbb{Z}$, we deduce $\overline{u} \in \langle 1-\zeta \rangle$. But $\overline{u}$ is a unit, so this is impossible.

So it must be the case that $u/\overline{u} = \zeta^s$ for some $r \in \mathbb{Z}$. Let $r \in \mathbb{Z}$ satisfy $2r \equiv s \bmod p$, and put $v = \zeta^{-r}u$. Then

$$\zeta^r v = \zeta^r\zeta^{-r}u = u$$

and

$$\overline{v} = \zeta^r\overline{u} = \zeta^r\zeta^{-s}u = \zeta^r\zeta^{-2r}u = \zeta^{-r}u = v,$$

as desired. □

8.2 Fermat's Last Theorem

In this section we will prove a special case of Fermat's Last Theorem; we must begin with the following definition:

Definition 8.7. A prime number $p \geq 3$ is said to be *regular* if and only if the class number of $\mathbb{Q}(\zeta_p)$ is not divisible by p, where $\zeta_p = e^{2\pi i/p}$.

Remark 8.8. The following primes are known to be regular:

$$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41,$$

while $37, 59, 67, 101, 103, 131, 149$ are not.

C. Siegel conjectured in 1964 that $e^{-\frac{1}{2}}$ of all primes should be regular ($\approx 61\%$), but it remains unknown even whether there are infinitely many regular primes. On the other hand, it is know that there are infinitely many irregular (i.e., not regular) primes.

The arithmetic of the cyclotomic fields $\mathbb{Q}(\zeta_p)$ is closely connected to the Bernoulli numbers; these are the sequence of rational numbers $B_0, B_1, \ldots$ defined by the generating function expression

$$\frac{X}{\exp X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k,$$

where $\exp X = \sum_{k=0}^{\infty} \frac{X^k}{k!}$ is the formal exponential. In particular, Kummer showed that a prime p is regular if and only if it does not divide the denominator of $B_2, B_4, \ldots, B_{p-3}$. Since the Bernoulli numbers can be easily calculated, either directly from the definition we have given or from various closed form expressions, this gives a straightforward way of checking whether any given prime number is regular (but does not offer much information on their theoretic properties!).

We may now state our special case of FLT:

Theorem 8.9 (Fermat's Last Theorem: weak, regular case. Due to E. Kummer)**.** *Assume that p is a regular prime and that x, y, z are integers, none of which are divisible by p (this is sometimes called the "weakness" hypothesis). Then*

$$x^p + y^p \neq z^p.$$

Outline of proof and historical remarks. To prove the theorem we will work in the number field $F = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ for some fixed prime number $p \geq 5$ (it is easy to prove the theorem when $p = 3$, using mod 9 congruences).

Using very similar arguments to lemma 7.4, which in particular require regularity of p and our theory of the class group, we will show that if x, y, z are integers which contradict the statement of the theorem, then (possibly after slightly modifying x, y, z – see lemma 8.11) we can write

$$x + \zeta y = u\alpha^p \tag{$\dagger$}$$

for some $u \in \mathfrak{D}_F^\times$, $\alpha \in \mathfrak{D}_F$. This is the key step, from which it will be easy to complete the proof.

As in lemma 7.4, if we were to simply erroneously assume that the ring $\mathbb{Z}[\zeta]$ were a UFD, then we would be able to prove ($\dagger$) very quickly (without any mention of rings of integers, ideals, or the class group). This was the famous incorrect proof of FLT presented by G. Lamé in 1847 which apocryphally led E. Kummer to develop a theory of "ideal numbers" which later become ideals and the class group. □

Having finished the outline, we now turn to proving the theorem properly. We first need some small lemmas:

Lemma 8.10. *Let $p \geq 5$ and $F = \mathbb{Q}(\zeta)$ be as above.*

(i) Suppose that $a_0, \ldots, a_{p-1}$ are integers, at least one of which is zero. Suppose that m is an integer such that

$$a_0 + \cdots + a_{p-1}\zeta^{p-1} \in \langle m \rangle \ (= m\mathfrak{D}_F).$$

Then $a_i \in m\mathbb{Z}$ for $i = 0, \ldots, p-1$.

(ii) Let $\alpha \in \mathfrak{D}_F$; then there exists $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \bmod \langle p \rangle$.

Proof. (i). Suppose $a_r = 0$ for some $0 \leq r \leq p-1$. Multiply through by ζ^{p-1-r} to reduce to the case $a_{p-1} = 0$, which then easily follows from the fact that $1, \zeta, \ldots, \zeta^{p-2}$ was shown to be an integral basis for F.

(ii). Since $\mathfrak{D}_F = \mathbb{Z}[\zeta]$ we may write $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ for some $a_0, \ldots, a_{p-2} \in \mathbb{Z}$. In any ring R, one has $(x+y)^p \equiv x^p + y^p \bmod pR$. Applying this repeatedly we get

$$\begin{aligned}\alpha^p &\equiv a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{p(p-2)} \bmod \langle p \rangle \\ &= a_0^p + a_1^p + \cdots a_{p-2}^p,\end{aligned}$$

so that $a := a_0^p + a_1^p + \cdots a_{p-2}^p$ works. □

Lemma 8.11. *Suppose that theorem 8.9 is false. Then there are integers x, y, z such that*

$$x^p + y^p = z^p,$$

$$p \text{ does not divide any of } x, y, z,$$

and

$$x \not\equiv y \bmod p,$$

$$x, y \text{ are coprime.}$$

In other words, we can modify our (non-existent) solution to also satisfy the second two conditions.

Proof. Suppose that x, y, z are integers such that $x^p + y^p = z^p$ and p does not divide any of x, y, z. We claim it is impossible that

$$x \equiv y \equiv -z \bmod p.$$

For, if not, then $-2z^p \equiv z^p \bmod p$, whence $3z \equiv 3z^p \equiv p \bmod 0$; but $p \nmid 3$ and $p \nmid z$, so this is impossible.

Therefore at least one of the triples

$$x, y, z, \qquad x, -z, -y$$

satisfies the first three desired properties. Divide through by the gcd to ensure that the fourth condition also holds. □

Lemma 8.12. *Suppose that x, y, z satisfy the conditions of the previous lemma. If i, j are integers such that $i \not\equiv j \bmod p$ then the ideals*

$$\langle x + \zeta^i y\rangle,\ \langle x + \zeta^j y\rangle$$

of $\mathfrak{D}_F$ are coprime.

Proof. For a contradiction, suppose that there is a prime ideal $\mathfrak{p}$ of $\mathfrak{D}_F$ containing both $x+\zeta^i y$ and $x+\zeta^j y$. After swapping i and j we may suppose that $i > j$. Then

$$\mathfrak{p} \ni \zeta^i y - \zeta^j y = \zeta^i(1-\zeta^{i-j})y = \zeta^i \frac{1-\zeta^{i-j}}{1-\zeta}(1-\zeta)y$$

and so $(1-\zeta)y \in \mathfrak{p}$ (the other terms are units, by lemma 8.2). Therefore either $1-\zeta \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Similarly,

$$\mathfrak{p} \ni (x+\zeta^i y) - \zeta^{i-j}(x+\zeta^j y) = \frac{1-\zeta^{i-j}}{1-\zeta}(1-\zeta)x$$

and so either $1-\zeta \in \mathfrak{p}$ or $x \in \mathfrak{p}$.

We claim that $1-\zeta \in \mathfrak{p}$. Otherwise we deduce that $x, y \in \mathfrak{p}$, whence $x, y \in \mathfrak{p} \cap \mathbb{Z}$, contradicting coprimality of x and y. So, $1-\zeta \in \mathfrak{p}$, whence $\mathfrak{p} = \langle 1-\zeta\rangle$ since $\langle 1-\zeta\rangle$ is a prime ideal by lemma 8.2 (recall that prime ideals are maximal ideals). Therefore

$$x + y = x + \zeta^i y + (1-\zeta^i)y \in \mathfrak{p},$$

and so $x + y \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Finally,

$$z^p = x^p + y^p \equiv (x+y)^p \equiv 0 \bmod p,$$

so we see that $p|z$, which is the required contradiction. □

Now we can finish the proof of theorem 8.9:

Proof of FLT's in the weak, regular case. For a contradiction suppose that theorem 8.9 is false. Then we have shown that there are integers x, y, z satisfying the conditions of lemma 8.11, and the previous lemma tells us that the ideals

$$\langle x+y\rangle,\ \langle x+\zeta y\rangle,\ \cdots,\ \langle x+\zeta^{p-1}y\rangle$$

are pairwise coprime.

But $\prod_{i=0}^{p-1}(x+\zeta^i y) = x^p + y^p = z^p$, so the product of these coprime ideals is a p^{th}-power:

$$\prod_{i=0}^{p-1}\langle x+\zeta^i y\rangle = \langle z\rangle^p.$$

By exercise 7.1(ii), each ideal is already a p^{th}-power: $\langle x+\zeta^i y\rangle = I_i^p$ for some non-zero ideal $I_i \subseteq \mathfrak{D}_F$.

We only care about $i = 1$: since I_1^p is principal, our assumption that p is regular, i.e. that $p \nmid h_F$, implies that I_1 is already principal by exercise 7.1(iii); so $I_1 = \langle\alpha\rangle$ for some $\alpha \in \mathfrak{D}_F$. Therefore

$$x + \zeta y = u\alpha^p$$

for some $u \in \mathfrak{D}_F^\times$: as explained in the outline to the proof, this is the key step.

By proposition 8.6 we may write $u = \zeta^r v$ for some $r \in \mathbb{Z}$ and some unit $v \in \mathfrak{D}_F^\times$ such that $\overline{v} = v$. By lemma 8.10(ii) there is $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \bmod \langle p\rangle$. So

$$x + \zeta y = \zeta^r v\alpha^p \equiv \zeta^r v a \bmod \langle p\rangle$$

Similarly, taking complex conjugates,

$$x + \zeta^{-1} y = \zeta^{-r}\overline{v\alpha}^p \equiv \zeta^{-r} v a \bmod \langle p\rangle,$$

and so $\zeta^{-r}(x+\zeta y) \equiv \zeta^r(x+\zeta^{-1}y) \bmod \langle p\rangle$. In other words,

$$x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y \in \langle p\rangle \qquad (\dagger)$$

Finally, we will analyse several cases to get a contradiction from (†):

(i) Case: $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are all distinct. Then lemma 8.10(i) implies that $x, y \in p\mathbb{Z}$, contradicting our original assumption that $p \nmid x$ and $p \nmid y$.

(ii) Case: $1 = \zeta^2 r$. Then (†) implies that $\zeta y - \zeta^{-1}y \in \langle p\rangle$, whence lemma 8.10(i) implies (using $\zeta^{-1} = \zeta^{p-1}$) that $y \in p\mathbb{Z}$, contradicting our original assumption that $p \nmid y$.

(iii) Case: $1 = \zeta^{2r-1}$. Then (†) implies that $(x-y)-(x-y)\zeta \in \langle p\rangle$, whence lemma 8.10(i) implies $x-y \in p\mathbb{Z}$, contradicting our original assumption that $x \not\equiv y \bmod p$.

(iv) Case: $\zeta = \zeta^{2r-1}$. Then (†) implies that $x-\zeta^2 x \in \langle p\rangle$, whence lemma 8.10(i) implies $x \in p\mathbb{Z}$, contradicting our original assumption that $p \nmid x$.

These cases are the only possibilities, since $1 \neq \zeta$ and $\zeta^{2r} \neq \zeta^{2r-1}$, so the proof is complete. □

9 RAMIFICATION THEORY

If F is a number field and $p \in \mathbb{Z}$ is a prime number then in section 6 we have already studied the factorisation of the principal ideal $\langle p\rangle$ in $\mathfrak{O}_F$ (especially in the case in which $\mathfrak{O}_F = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{O}_F$). The name given to the study of such factorisations is *ramification*. Whereas we previously studied this from a hands-on perspective of computing factorisations, now we will examine it theoretically.

Definition 9.1. Let $\mathfrak{p} \subset \mathfrak{O}_F$ be a prime ideal, and let p be the prime number sitting under it. Recalling that $N(\mathfrak{p})$ is a power of p, we define the *inertia degree*, $f_\mathfrak{p} \geq 1$, of $\mathfrak{p}$ by the formula

$$N(\mathfrak{p}) = p^{f_\mathfrak{p}}.$$

Meanwhile, the *ramification degree*, $e_\mathfrak{p} \geq 1$ is the exponent of $\mathfrak{p}$ in the prime ideal factorisation of $\langle p\rangle$ (or equivalently, $e_\mathfrak{p} := \operatorname{ord}_\mathfrak{p} p$).

Definition 9.2. This definition is a little long, but explains all the notation used for how the prime factorisation of $\langle p\rangle$ may look.

Let F be a number field of degree n over $\mathbb{Q}$. Let $p \in \mathbb{Z}$ be a prime number, let $\langle p\rangle$ be the principal ideal of $\mathfrak{O}_F$ generated by p, and let

$$\langle p\rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

$(e_1, \dots, e_m \geq 1)$ be its prime factorization in $\mathfrak{O}_F$. Then e_i is called the *ramification degree* of p at $\mathfrak{p}_i$. Then,

> p is said *to be ramified in* F, or *to ramify in* F if and only if $e_i > 1$ for some i (in other words, if and only if there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{O}_F$ such that $\mathfrak{p}^2 \ni p$)

and otherwise

> p is said to be *unramified* in F when $e_i = 1$ for all i.

When p is unramified there are two extreme possibilities (notice that these conditions really do imply that p is unramified):

> p is said to be *inert* in F when $\langle p\rangle$ is a prime ideal of $\mathfrak{O}_F$.
>
> p is said to *split completely* when $e_1 = \dots = e_m = 1$ and $f_{\mathfrak{p}_1} = \dots = f_{\mathfrak{p}_m} = 1$ (by the previous theorem, p splits completely if and only if $\langle p\rangle$ is a product of n distinct prime ideals).

Remark 9.3. Suppose that $F = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{D}_F$, and let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α. Then our hands-on factorisation result implies that the prime ideal factorisation of $\langle p \rangle$ in $\mathfrak{D}_F$ is described exactly by the factorisation of $f(X)$ mod p into irreducibles. Thus the study of how prime numbers ramify in F is exactly the study of how the fixed polynomial factors mod p, as we vary p.

Exercise 9.1. Let F be a number field and suppose that there is $\alpha \in \mathfrak{D}_F$ such that $\mathfrak{D}_F = \mathbb{Z}[\alpha]$; let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α. Let $\ell \in \mathbb{Z}$ be a prime number.

Suppose that there is a polynomial $g(X) \in \mathbb{Z}[X]$ with the following two properties:

(i) $f(X)$ divides $g(X)$;

(ii) $g(X)$ mod ℓ and $g'(X)$ mod ℓ are coprime in $\mathbb{F}_\ell[X]$.

Show that ℓ is unramified in F.

Exercise 9.2. Let $p \in \mathbb{Z}$ be an odd prime number, $\zeta = e^{2\pi i/p}$, and $F = \mathbb{Q}(\zeta)$. In this exercise you will prove that the only roots of unity in F have the form $\pm\zeta^n$ for some $n \in \mathbb{Z}$. (We will need this to prove a special case of Fermat's Last Theorem.)

For a contradiction, suppose that F contains a root of unity which cannot be written in the form $\pm\zeta^n$ for some $n \in \mathbb{Z}$; show that F contains one of the the following:

(i) $e^{2\pi i/\ell}$ for some prime number $\ell \in \mathbb{Z}$ not equal to p; or

(ii) $e^{2\pi i/p^2}$; or

(iii) $\sqrt{-1}$.

In each case, arrive at a contradiction by following the hints:

(i) Show that the prime ideal factorization of $\langle \ell \rangle$ has the form

$$\langle \ell \rangle = \mathfrak{l}^{(\ell-1)e_1} \dots \mathfrak{l}^{(\ell-1)e_r},$$

for some prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_r$ of $\mathfrak{D}_F$ and some integers $e_1, \dots, e_r \geq 1$. Apply the previous question to get a contradiction.

(ii) Put $\mathfrak{p} = \langle 1 - \zeta \rangle$; show that $e^{2\pi i/p^2} \equiv 1 \bmod \mathfrak{p}$ and then show $1 - \zeta \in \mathfrak{p}^2$. Derive a contradiction.

(iii) Use a similar argument as in (a): show that the prime ideal factorization of $\langle 2 \rangle$ has the form

$$\langle 2 \rangle = \mathfrak{q}_1^{2e_1} \dots \mathfrak{q}_r^{2e_r}$$

for some prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ of $\mathfrak{D}_F$ and some integers $e_1, \dots, e_r \geq 1$; then apply the previous question to get a contradiction.

Proposition 9.4. *Let F be a number field of degree n over $\mathbb{Q}$, and assume that $F/\mathbb{Q}$ is Galois (If you don't know what this means, this is the only case we need: $F/\mathbb{Q}$ will be Galois if $F = \mathbb{Q}(\alpha)$ for some $\alpha \in F$ such that all the conjugates of α also belong to F). Let $p \in \mathbb{Z}$ be a prime number, let $\langle p \rangle$ be the principal ideal of $\mathfrak{D}_F$ generated by p, and let*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$$

($e_1, \dots, e_m \geq 1$) be its prime factorization in $\mathfrak{D}_F$. Then

$$e_1 = \dots = e_m$$

and

$$f_{\mathfrak{p}_1} = \dots = f_{\mathfrak{p}_m}.$$

Sketch of proof. For any $i = 1, \dots, r$ and $\sigma \in Gal(F/\mathbb{Q})$, the set $\sigma(\mathfrak{p}_i) := \{\sigma(x) : x \in \mathfrak{p}_i\}$ is a prime ideal containing $\sigma(p) = p$, hence $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$ for some other j. In other words, $Gal(F/\mathbb{Q})$ acts on $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$.

The key point is to prove that this action is transitive. So fix indices i, j and suppose for a contradiction that $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$ for all $\sigma \in Gal(F/\mathbb{Q})$. Then $\mathfrak{p}_j \not\subseteq \sigma(\mathfrak{p}_i)$, so the prime avoidance lemma implies that $\mathfrak{p}_j \not\subseteq \bigcup_{\sigma \in Gal(F/\mathbb{Q})} \sigma(\mathfrak{p}_i)$. So there exists an element $\alpha \in \mathfrak{p}_j$ such that $\sigma(\alpha) \notin \mathfrak{p}_i$ for any σ (here we have replaced σ by σ^{-1}, since we are running over *all* $\sigma \in Gal(F/\mathbb{Q})$). Then

$$N_{F/\mathbb{Q}}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \alpha \prod_{\sigma \neq \mathrm{id}} \sigma(\alpha) \in \mathfrak{p}_j \cap \mathbb{Z} = p\mathbb{Z} \subseteq \mathfrak{p}_i,$$

implying that at least one of the terms in the product is in $\mathfrak{p}_i$, which is the desired contradiction.

So, we now know that for any $i, j = 1, \dots, m$ we can find σ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Then

$$e_i = \mathrm{ord}_{\mathfrak{p}_i} \langle p \rangle = \mathrm{ord}_{\sigma(\mathfrak{p}_i)} \sigma(\langle p \rangle) = \mathrm{ord}_{\mathfrak{p}_j} \langle p \rangle = e_j.$$

Also, σ induces an isomorphism

$$\mathfrak{D}_F/\mathfrak{p}_i \cong \mathfrak{D}_F/\mathfrak{p}_j,$$

whence $f_{\mathfrak{p}_i} = f_{\mathfrak{p}_j}$. □

9.1 Ramification in quadratic extensions and quadratic reciprocity

We have factored many prime numbers in particular quadratic extensions; now we return to the subject from a theoretic point of view and relate it to quadratic reciprocity.

For this whole section fix a quadratic extension $F = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z} \setminus \{0, 1\}$ is a square-free integer as usual. Recall that the absolute discriminant of F is

$$\Delta_F = \begin{cases} 4d & d \equiv 2, 3 \bmod 4 \\ d & d \equiv 1 \bmod 4 \end{cases}$$

If $p \in \mathbb{Z}$ is a prime number, then $\langle p \rangle \subset \mathfrak{D}_F$ factors into a product of at most two prime ideals; therefore it must factor in exactly one of the following ways:

(i) $\langle p \rangle$ is a prime ideal of $\mathfrak{D}_F$ (i.e. p is unramified and inert).

(ii) $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ for some non-zero, distinct, prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathfrak{D}_F$ (i.e. p is unramified and splits completely).

(iii) $\langle p \rangle = \mathfrak{p}^2$ for some non-zero prime ideal $\mathfrak{p} \subseteq \mathfrak{D}_F$ (i.e. p ramifies).

The aim of this section is to prove the following theorem:

Theorem 9.5. *Let $F = \mathbb{Q}(\sqrt{d})$ be as above. Then The way that $\langle p \rangle$ factors depends only on the value of $p \bmod \Delta_F$. In other words, if $p, p' \in \mathbb{Z}$ are prime numbers and $p \equiv p' \bmod \Delta_F$, then p is inert/completely split/ramified in F if and only if the same is true of p'.*

In particular, a prime number ramifies in F if and only if it divides Δ_F.

The proof will crucially depend on all the main theorems about quadratic residues: the descriptions of $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and the Law of Quadratic reciprocity itself.

The theorem will be proved in several steps. We begin by showing that a Legendre symbol determines the ramification, a result we have essentially already used when factoring $\langle p \rangle$ in particular quadratic number fields.

Lemma 9.6. *Let $F = \mathbb{Q}(\sqrt{d})$ be as above, and p an odd prime number. Then*

(i) p is inert in $F \iff \left(\frac{d}{p}\right) = -1$.

(ii) p splits completely in $F \iff \left(\frac{d}{p}\right) = 1$.

(iii) p ramifies in $F \iff \left(\frac{d}{p}\right) = 0$ (which happens $\iff p \mid \Delta_F$).

Proof. To avoid separately considering the cases $d \equiv 2, 3 \bmod 4$ and $d \equiv 1 \bmod 4$, put

$$\alpha := \frac{\Delta_F + \sqrt{\Delta_F}}{2} = \begin{cases} 2d + \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4 \\ \frac{d-1}{2} + \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4 \end{cases}$$

Then $\mathfrak{D}_F = \mathbb{Z}[\alpha]$ and α has minimal polynomial $f(X) = X^2 - \Delta_F X + \frac{\Delta_F(\Delta_F - 1)}{4} \in \mathbb{Z}[X]$.

Let $s = \frac{p+1}{2}$ so that $2s \equiv 1 \bmod p$. Then

$$f(X) \equiv (X - s\Delta_F)^2 - s^2\Delta_F \bmod p,$$

so the correspondence between the factorisation of $\langle p \rangle$ and that of $f(X) \bmod p$ immediately gives:

(i) p is inert in $F \iff \overline{f}(X)$ is irreducible $\iff s^2\Delta_F$ is not a square in $\mathbb{Z}/p\mathbb{Z} \iff \left(\frac{s^2\Delta_F}{p}\right) = -1$.

(ii) p splits completely in $F \iff \overline{f}(X)$ is a product of two distinct irreducible polynomials $\iff s^2\Delta_F$ is a non-zero square in $\mathbb{Z}/p\mathbb{Z} \iff \left(\frac{s^2\Delta}{p}\right) = 1$.

(iii) p ramifies in $F \iff \overline{f}(X)$ is the square of an irreducible polynomial $\iff s^2\Delta_F$ is zero in $\mathbb{Z}/p\mathbb{Z} \iff \left(\frac{s^2\Delta_F}{p}\right) = 0$.

To complete the proof notice that $\left(\frac{s^2\Delta_F}{p}\right) = \left(\frac{d}{p}\right)$, regardless of whether $\Delta_F = 4d$ or d. □

Next we give an analogue of the previous result for $p = 2$:

Lemma 9.7. *Let $F = \mathbb{Q}(\sqrt{d})$ be as above. Then*

(i) 2 is inert in $F \iff d \equiv 5 \bmod 8$.

(ii) 2 splits completely in $F \iff d \equiv 1 \bmod 8$.

(iii) 2 ramifies in $F \iff d \equiv 2$ or $3 \bmod 4$ (which happens $\iff 2 \mid \Delta_F$).

Proof. Since the left and right sides constitute all possibilities, it is enough to prove $\Longleftarrow$ in each case.

(i): Then $d \equiv 1 \bmod 4$, so $\mathfrak{D}_F = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{d}}{2}$, with minimal polynomial $f(X) = X^2 - X - \frac{d-1}{4}$. Then $f(X) \equiv X^2 - X - 1 \bmod 2$, which is well-known to be irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$ (since it doesn't have a root) so $\langle 2 \rangle$ is a prime ideal in $\mathfrak{D}_F$; i.e. 2 is inert in F.

(ii): Again $d \equiv 1 \bmod 4$ and $\mathfrak{D}_F = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{d}}{2}$, with minimal polynomial $f(X) = X^2 - X - \frac{d-1}{4}$. But now $f(X) \equiv X(X-1) \bmod 2$, so $\langle 2 \rangle = \langle 2, \alpha \rangle \langle 2, \alpha - 1 \rangle$ is a product of distinct prime ideals in $\mathfrak{D}_F$; i.e. 2 splits completely in F.

(iii): In this case $\mathfrak{D}_F = \mathbb{Z}[\sqrt{d}]$ and we put $f(X) = X^2 - d$. Then

$$f(X) = \begin{cases} X^2 + 1 = (X+1)^2 & d \equiv 3 \bmod 4 \\ X^2 & d \equiv 2 \bmod 4 \end{cases}$$

so $\langle 2 \rangle$ is a square of a prime ideal in $\mathfrak{D}_F$; i.e. 2 ramifies in F. □

Notice that parts (iii) of the previous two lemmas already prove the claim in the main theorem that a prime ramifies if and only if it divides the Δ_F. Now we may prove the rest of the main theorem:

Proof of theorem 9.5. We first obtain a formula for a certain Legendre symbol. The prime factorisation of d has the form

$$d = 2^\varepsilon q_1 \cdots q_m$$

where $\varepsilon = 0$ or 1, and $q_1, \ldots, q_m$ are distinct odd prime numbers, which are allowed to be negative to accommodate for the fact that d may be negative. (Being careful, notice that if $d = -2$ then it cannot be expressed in this form, but the reader will have no difficulty introducing an extra piece of notation to fix this problem.) So, for any odd prime number $p \in \mathbb{Z}$,

$$\begin{aligned}\left(\frac{d}{p}\right) &= \left(\frac{2}{p}\right)^\varepsilon \left(\frac{q_1}{p}\right) \ldots \left(\frac{q_m}{p}\right) \\ &= \left(\frac{2}{p}\right)^\varepsilon \left(\frac{p}{q_1}\right) \ldots \left(\frac{p}{q_m}\right) (-1)^{\frac{p-1}{2}\left(\frac{q_1-1}{2}+\cdots+\frac{q_m-1}{2}\right)} \\ &= \left(\frac{2}{p}\right)^\varepsilon \left(\frac{p}{q_1}\right) \ldots \left(\frac{p}{q_m}\right) (-1)^{\frac{p-1}{2}r} \qquad (\dagger)\end{aligned}$$

by quadratic reciprocity, where r is the number of the primes among $q_1, \ldots, q_m$ which are $\equiv 3 \bmod 4$.

Now let $p, p' \in \mathbb{Z}$ be prime numbers which are congruent modulo Δ_F; we will prove that p, p' ramify in the same way in $\mathfrak{D}_F$, thereby completing the proof of the theorem. We will separately consider two cases: either p, p' are both odd, or p is odd and p' is even (there is nothing to prove if both p and p' are even!!).

Suppose first that both p and p' are odd. Then lemma 9.6 tells us that the ramification-type of p, p' is determined by $\left(\frac{d}{p}\right)$, $\left(\frac{d}{p'}\right)$, so we must prove $\left(\frac{d}{p}\right) = \left(\frac{d}{p'}\right)$. Using formula (†) and the fact that $p \equiv p' \bmod q_i$ for all i, it remains only to prove that

$$\left(\frac{2}{p}\right)^\varepsilon (-1)^{\frac{p-1}{2}r} = \left(\frac{2}{p'}\right)^\varepsilon (-1)^{\frac{p'-1}{2}r}. \qquad (\ddagger)$$

Well, if $d \equiv 3 \bmod 4$ then $\varepsilon = 0$ and $4|\Delta_F$ so that $\frac{p-1}{2} \equiv \frac{p'-1}{2} \bmod 2$, proving (‡) in this case. Next, if $d \equiv 2 \bmod 4$ then $\varepsilon = 1$ and $8|\Delta_F$, so $p \equiv p' \bmod 8$, whence $\left(\frac{2}{p}\right) = \left(\frac{2}{p'}\right)$ by the Legendre symbol of 2 theorem, and still $\frac{p-1}{2} \equiv \frac{p'-1}{2} \bmod 2$ since $p \equiv p' \bmod 4$; again (‡) follows. Finally, if $d \equiv 1 \bmod 4$ then $\varepsilon = 0$ and r must be even, whence both sides of (‡) are 1 (moreover, this shows that if $d \equiv 1 \bmod 4$ and p is an odd prime, then $\left(\frac{d}{p}\right) = \left(\frac{p}{q_1}\right) \ldots \left(\frac{p}{q_m}\right)$; we will need this in a moment). This completes the proof when both p and p' are odd.

The remaining case is to assume that p is odd and that $p' = \pm 2$. This forces $d \equiv 1 \bmod 4$, for otherwise $4|\Delta_F$, implying that $p \equiv \pm 2 \bmod 4$, which is absurd. So $d \equiv 1 \bmod 4$, and we just noticed that this implies

$$\left(\frac{d}{p}\right) = \left(\frac{p}{q_1}\right) \ldots \left(\frac{p}{q_m}\right)$$

But moreover $p \equiv \pm 2 \bmod q_i$ for all i, so the Legendre symbol of 2 theorem and the identity $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ now give

$$\left(\frac{d}{p}\right) = (\pm 1)^{\frac{q_1-1}{2}+\cdots+\frac{q_m-1}{2}} (-1)^{\frac{q_1^2-1}{8}+\cdots+\frac{q_m^2-1}{8}}$$

The exponent of the ± 1 is congruent mod 2 to r, which is even since $d \equiv 1 \bmod 4$, so this factor is $= 1$. Next, the exponent of the -1 is congruent mod 2 to $\frac{d^2-1}{8}$ (this follows inductively from the simple identity that $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \bmod 2$ whenever a, b are odd integers). In conclusion,

$$\left(\frac{d}{p}\right) = (-1)^{\frac{d^2-1}{8}} = \begin{cases} 1 & d \equiv 1 \bmod 8 \\ -1 & d \equiv 5 \bmod 8 \end{cases}$$

Finally, looking at the previous two lemmas, we see that if $d \equiv 1 \bmod 8$ then both p and 2 completely split, while if $d \equiv 5 \bmod 8$ then both p and 2 are inert.

This completes the proof of the main theorem. □

Remark 9.8. The previous theorem is probably the most important consequence of quadratic reciprocity: the way $\langle p \rangle$ factors in $\mathfrak{D}_F$ depends only on a certain congruence class of p. We will see similar results for other number fields; the most general abstract result of this type is an important consequence of so-called "class field theory", which is the next step in algebraic number theory.

9.2 RAMIFICATION IN CYCLOTOMIC EXTENSIONS

In this section we will prove an analogue for cyclotomic extensions of theorem 9.5: the way in which a prime number ramifies is still determined by a congruence condition. If $\zeta = e^{2\pi i/m}$ is a primitive m^{th} root of unity for some integer m, then it is a fact that

$$\mathfrak{D}_F = \mathbb{Z}[\zeta].$$

We have proved this when m is a prime number and it was HW exercise ????? if m is a prime power; the case of general m can be deduced from the prime power case (non-trivially).

Theorem 9.9 ("Cyclotomic reciprocity law" – a slightly misleading name!)**.** *Let $m \geq 1$ be an integer and let $F = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/m}$ is a primitive m^{th} root of unity. Let $p \in \mathbb{Z}$ be a prime number. Then*

(i) p ramifies in F if and only if p divides m.

(ii) Suppose p doesn't divide m. Let $s \geq 1$ be the smallest integer such that $p^s \equiv 1 \bmod m$; in other words, s is the order of p mod m in the unit group $(\mathbb{Z}/m\mathbb{Z})^\times$. Then the prime ideal factorisation of $\langle p \rangle$ has the form

$$\langle p \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct primes ideals with norm p^s, and $r = |F : \mathbb{Q}|/s$.

In particular, the factorisation type of p depends only on p mod m.

Proof. If p is a prime number dividing m, then $\zeta_p = \zeta^{m/p}$ is a primitive p^{th} root of unity; so F contains $\mathbb{Q}(\zeta_p)$. Since p ramifies in $\mathbb{Q}(\zeta_p)$, it ramifies in F.

Conversely, suppose that p is a prime number not dividing m. The minimal polynomial of ζ, which is commonly denoted $\Phi_m(X)$, divides $X^m - 1$. Since $X^m - 1$ and its formal derivative mX^{m-1} are coprime in $\mathbb{F}_p[X]$, the prime number p is unramified in F by exercise 9.1. We have proved (i).

Continuing to suppose that p is a prime number not dividing m, let $s \geq 1$ be as in (ii) and let $\mathfrak{p} \subset \mathfrak{D}_F$ be any prime ideal sitting over p. To complete the proof we must show $N(\mathfrak{p}) = p^s$ (the description of r comes from taking norms of both sides).

Let $\mathfrak{f}$ be the inertia degree of $\mathfrak{p}$; i.e., $N(\mathfrak{p}) = p^{\mathfrak{f}}$. Put $K = \mathfrak{D}_F/\mathfrak{p}$, which is a finite field with $p^{\mathfrak{f}}$ elements. Let $z \in K$ denote the element ζ mod $\mathfrak{p}$.

Noting first that $z^m = 1$ in k, we claim that the order of z in the group $K^\times$ is exactly m. For a contradiction, suppose not. Then $z^{m/\ell} = 1$ for some prime number ℓ dividing m, which means that $1 - \zeta^{m/\ell} \in \mathfrak{p}$. But $\zeta_\ell = \zeta^{m/\ell}$ is a primitive ℓ^{th} root of unity, so lemma 8.2 implies that $\ell = u(1 - \zeta_\ell)^{\ell-1}$ for some unit $u \in \mathbb{Z}[\zeta_\ell] \subseteq \mathfrak{D}_F$. Therefore $\ell \in \mathfrak{p}$. But ℓ and p are distinct primes, since only one of them divides m, and p is also in $\mathfrak{p}$, by choice of $\mathfrak{p}$; so this is a contradiction. This proves our claim that the order of z in the group $K^\times$ is exactly m.

Lagrange's theorem from group theory now tells us that m divides $\#K^\times = p^{\mathfrak{f}} - 1$, i.e. $p^{\mathfrak{f}} \equiv 1 \bmod m$; therefore $\mathfrak{f} \geq s$. The theory of finite fields now tells us that

$$M = \{x \in K : x^{p^s} = x\}$$

is a subfield of K such that $|K : M| = \mathfrak{f} - s$. Since m divides $p^s - 1$ (by the definition of s), we see that $z^{p^s-1} = 1$ and so $z^{p^s} = z$, i.e. $z \in M$. But $\mathfrak{D}_F = \mathbb{Z}[\zeta]$, so any element of $K = \mathfrak{D}_F/\mathfrak{p}$ is an integer linear combination of powers of z; but all these integer linear combinations lie in M, since $\zeta \in M$, so this proves that $K = M$. Therefore $\mathfrak{f} = s$, completing the proof □

10 A NEW PROOF OF QUADRATIC RECIPROCITY

Let $p \geq 3$ be a prime number, let $\zeta = e^{2\pi i/p}$ be a primitive p^{th} root of unity, and let $F = \mathbb{Q}(\zeta)$. In this section we are going to present a proof of the Law of Quadratic Reciprocity using the algebraic number theory of F. The key tools will be the following two points, together with some basic Galois theory:

- F contains $\sqrt{p^*}$, where $p^* = (-1)^{\frac{p-1}{2}}$.
- The Galois group of $F/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, via

$$(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(F/\mathbb{Q}), \quad a \mapsto \sigma_a,$$

  where σ_a is defined by the rule $\sigma_a(\zeta) = \zeta^a$. Although we have not proved this, many of you know it from Galois theory.

We need two provisional lemmas:

Lemma 10.1. *If a is an integer which is coprime to p, then*

$$\sigma_a(\sqrt{p^*}) = \left(\frac{a}{p}\right)\sqrt{p^*}.$$

Proof. Since the only conjugates of $\sqrt{p^*}$ are $\pm\sqrt{p^*}$, we see that $\sigma_a(\sqrt{p^*})$ is either $\sqrt{p^*}$ or $-\sqrt{p^*}$. Therefore it is enough to prove that

$$\sigma_a(\sqrt{p^*}) = \sqrt{p^*} \iff \left(\frac{a}{p}\right) = 1.$$

Well, $\sigma_a(\sqrt{p^*}) = \sqrt{p^*}$ if and only if σ_a fixes the subfield $M = \mathbb{Q}(\sqrt{p^*}) \subset F$, i.e. if and only if $\sigma_a \in \mathrm{Gal}(F/M) \subset \mathrm{Gal}(F/\mathbb{Q})$. Since $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic of order $p-1$, its index two subgroup $\mathrm{Gal}(F/M)$ is precisely the set $\{\sigma^2 : \sigma \in \mathrm{Gal}(F/\mathbb{Q})\}$. According to the isomorphism $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})$, this means that $\sigma_a(\sqrt{p^*}) = \sqrt{p^*}$ if and only if a is a square mod p, i.e. if and only if $\left(\frac{a}{p}\right) = 1$. □

Lemma 10.2. *If $q \geq 3$ is a prime number distinct from p, then*

$$\sigma_q(\alpha) \equiv \alpha^q \bmod \langle q \rangle$$

for all $\alpha \in \mathfrak{D}_F$.

Proof. Put $S = \{\alpha \in \mathfrak{D}_F : \sigma_q(\alpha) \equiv \alpha^q \bmod \langle q \rangle\}$. Then S is obviously closed under multiplication, and the standard identity $(\alpha+\beta)^q \equiv \alpha^q + \beta^q \bmod \langle q \rangle$ implies it is closed under addition. Clearly S contains 1 and ζ, so we now know that S is a subring of $\mathfrak{D}_F$ containing ζ. But $\mathfrak{D}_F = \mathbb{Z}[\zeta]$, so $S = \mathfrak{D}_F$, as desired. □

Now we may give the new proof of quadratic reciprocity. Let $q \geq 3$ be a prime number distinct from p. Combining the previous two lemmas gives us

$$\left(\frac{q}{p}\right)\sqrt{p^*} = \sigma_q(\sqrt{p^*}) \equiv \sqrt{p^*}^q \bmod \langle q \rangle$$

i.e., $\left(\frac{q}{p}\right) \equiv {p^*}^{\frac{q-1}{2}} \bmod \langle q \rangle$. So $\left(\frac{q}{p}\right) - {p^*}^{\frac{q-1}{2}} \in \langle q \rangle \cap \mathbb{Z} = q\mathbb{Z}$. Also, ${p^*}^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}}$, giving

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \bmod q$$

Finally, recall from Euler's lemma (lemma 2.6(i)) that $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \bmod q$, and that a mod q congruence when both sides are ± 1 is necessary an equality; hence

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

which is exactly the Law of Quadratic Reciprocity!