Algebraic Number Theory

Christopher Birkbeck

September 24, 2021

Contents

Chapter 1

Number Fields

These notes have been heavily influenced by notes from several sources including: Richard Hill, David Loeffler, Keith Conrad, [Mar18],[Sam70] and others.

1.1 Recap on rings and fields

We begin by recalling some basic facts in commutative algebra. Specifically, some ring theory and field theory.

Remark. Throughout, we will not differentiate between $\subset$ and $\subseteq$. If such a distinction needs to be made we will state it or use $\subsetneq$.

Definition 1.1.1. A ring R is a set with two binary operations called addition $'+'$ and multiplication $'\cdot'$, such that:

1. R is an abelian group with respect to $+$. Note this means R contains a zero element denoted 0 and every $r \in R$ has an additive inverse $-r \in R$.

2. Multiplication is associative and distributive, i.e,

$$(xy)z = x(yz) \qquad x(y+z) = xy + xz \qquad (y+z)x = yx + zx$$

A ring is called commutative if $xy = yx$ and contains an identity element, denoted 1. Having a 1 is sometimes called being unital. Lastly, the subset of elements of R which have a multiplicative inverse are denoted $R^\times$.

Notation 1.1.2. Throughout this whole course, our rings will be assumed to be unital (i.e. have a 1) and unless otherwise stated, will be commutative.

Definition 1.1.3. We say a ring R is an integral domain, if whenever $xy = 0$ then either $x = 0$ or $y = 0$, for $x, y \in R$.

Definition 1.1.4. Let R, S be rings, then a ring homomorphism $\phi : R \to S$ is a map such that

$$\phi(x+y) = \phi(x) + \phi(y) \qquad \phi(xy) = \phi(x)\phi(y) \qquad \phi(1) = 1, \phi(0) = 0$$

A ring homomorphism is called an isomorphism if it is bijective.

Example 1.1.5. The map $\phi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $x \mapsto x \bmod p$ is a ring homomorphism.

Definition 1.1.6. Let $\phi : R \to S$ be a ring homomorphism. The kernel of ϕ is the set of all elements $r \in R$ such that $\phi(r) = 0$, this is denoted $\ker(\phi)$. The image of ϕ is the set $\{\phi(r) : r \in R\}$, this is denoted $\mathrm{Im}(\phi)$

Example 1.1.7.

1. The set of integers $\mathbb{Z}$ is a commutative ring.
2. The set $\mathbb{Z}[x]$ of polynomials with integer coefficients is a ring. In general, if R is a ring, then $R[x]$ is also a ring.

Definition 1.1.8. A field F is a commutative ring in which every non-zero element has an inverse. Equivalently, the set $F^\times := F \backslash \{0\}$.[a]

Example 1.1.9.

1. The rational numbers, $\mathbb{Q}$, are a field. As well as the Reals $\mathbb{R}$ and the complex numbers $\mathbb{C}$.
2. If p is a prime number, then $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ (the field of integers modulo p) is a field.

Non-example 1.1.10. The following are not fields: The integers $\mathbb{Z}$, the polynomial ring $\mathbb{Z}[x]$.

Definition 1.1.11. Let R be a ring, then an ideal $\mathfrak{a}$ is a subset of R which is an additive subgroup of R and such that for any $r \in R, a \in \mathfrak{a}$ we have $ra \in \mathfrak{a}$.

Example 1.1.12. Let R be a ring and $r \in R$, then we let

$$(r) = \{rx : x \in R\}.$$

This is an ideal in R and we call it the principal ideal generated by r. Similarly, if we take $r_1, \ldots, r_n$ then we can from the ideal $(r_1, \ldots, r_n) := \{\sum_i r_i x_i : x_i \in R\}$. Note that $(0) = 0$ and $(1) = R$.

Definition 1.1.13. If for every ideal $\mathfrak{a}$ in an integral domain R we can find $a \in R$ such that $\mathfrak{a} = (a)$ then we call R an Principal ideal domain, or PID for short.

[a] The symbol " := " means, "defined as".

Definition 1.1.14. Let R be an integral domain. We say an element $r \in R$ is irreducible if whenever $r = ab$ we must have exactly one of a, b being a unit.

Definition 1.1.15. An integral domain in which every element can be written uniquely as a product of irreducible elements is called a unique factorization domain, or UFD for short.

Definition 1.1.16. Let R be a ring and let $\mathfrak{a}$ be an ideal, then the quotient ring $R/\mathfrak{a}$ is the ring whose elements are of the form $r + \mathfrak{a}$ for $r \in R$, with addition and multiplication given by

$$(r_1 + \mathfrak{a}) + (r_2 + \mathfrak{a}) = r_1 + r_2 + \mathfrak{a} \qquad (r_1 + \mathfrak{a})(r_2 + \mathfrak{a}) = r_1 r_2 + \mathfrak{a}.$$

Exercise 1.1.17. Check that this ring structure is well-defined.

Proposition 1.1.18. *1. The kernel of a ring homomorphism is an ideal.*

2. The image of a ring homomorphism is a subring.

3. If ϕ is a ring homomorphism, then there is a ring isomorphism

$$R/\ker(\phi) \cong \mathrm{Im}(\phi).$$

Exercise 1.1.19. Prove Proposition 1.1.18.

Definition 1.1.20. Let R be a ring and $\mathfrak{p}, \mathfrak{m}$ an ideals with neither equal to (1).

1. The $\mathfrak{p}$ is called prime if whenever $xy \in \mathfrak{p}$ we have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
2. The ideal $\mathfrak{m}$ is called maximal if there does not exist an ideal $\mathfrak{a} \neq (1)$ such that $\mathfrak{m}$ is properly contained in $\mathfrak{a}$.

Example 1.1.21. Let p be a prime number, then $(p) \subset \mathbb{Z}$ is both a prime ideal as well as maximal.

Proposition 1.1.22. *1. Every maximal ideal is prime.*

2. Let R be a ring. Then $\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain. Similarly $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.

3. The only prime ideal in a field is (0).[b]

4. If ϕ is a non-zero ring homomorphism, then $\ker(\phi)$ is a proper ideal.

[b] When working with prime ideals later in the course, we will usually ignore the zero ideal.

5. *Every proper ideal (meaning one which isnt the whole ring) is contained in a maximal ideal.*

Definition 1.1.23. Let $\mathfrak{a}, \mathfrak{b}$ be ideals in a ring R. Then we let

1. $\mathfrak{ab}$ be the ideal generated by the product of elements of $\mathfrak{a}$ and $\mathfrak{b}$.
2. Similarly, $\mathfrak{a}+\mathfrak{b}$ denotes the ideal generated by sums of elements in $\mathfrak{a}, \mathfrak{b}$.
3. If $\mathfrak{a}+\mathfrak{b} = R = (1)$ we say $\mathfrak{a}, \mathfrak{b}$ are coprime.
4. If $\mathfrak{a}, \mathfrak{b}$ are ideals we write $\mathfrak{a} \mid \mathfrak{b}$ if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac}$.

1.2 Irreducible polynomials

How do we define more exotic fields? Well a good way is to take quotients of polynomial rings.

Definition 1.2.1. Let R be an integral domain. A non-zero polynomial $p(x)$ of degree at least 1 in $R[x]$ is said to be irreducible if whenever $p(x) = f(x)g(x)$ with $f(x), g(x) \in R[x]$ then one of $f(x)$ or $g(x)$ is in R. Note this is slightly different to Definition 1.1.14.

Example 1.2.2. The polynomial x^2+1 is irreducible in $\mathbb{Z}[x]$.

Non-example 1.2.3. The polynomial x^2-1 is not irreducible in $\mathbb{Z}[x]$ since it is $(x-1)(x+1)$ and neither is a unit.

Exercise 1.2.4. Let F be a field. Check that the only units in $F[x]$ are given by polynomials of degree 0, i.e., they are elements of F.

Exercise 1.2.5. True or False: If $p(x)$ is reducible in $F[x]$ then there exists $\alpha \in F$ such that $f(\alpha) = 0$ (i.e it has a root in F).

Now, here is a proposition whose content you should've seen in a previous course covering ring theory or commutative algebra

Proposition 1.2.6. *Let F be a field.*

1. *$F[x]$ is a Euclidean domain and thus a Principal Ideal Domain (PID).*
2. *In a PID, the ideal generated by a irreducible element is prime.*
3. *Every non-zero prime ideal in a PID is maximal.*
4. *Every PID is a UFD.*

Remark 1.2.7. Let me just remind you why $F[x]$ is a Euclidean domain. This is because if you have two polynomials $f(x), g(x)$ then we can do polynomial long division to write, $f(x) = q(x)g(x) + r(x)$ where $\deg(g) \leq \deg(f)$ and $\deg(r) < \deg(g)$ (this last bit having a strict inequality is what is important).

Ok great, so if we want to create fields then we just need to find some irreducible polynomials and then just need to quotient out by it. In other words:

Proposition 1.2.8. *Let F be a field, and $p(x)$ an irreducible polynomial in $F[x]$. Then*

$$F[x]/(p(x))$$

is a field.

Remark 1.2.9. (In case you've forgotten.) What does this field look like? well its elements can be thought of as $f(x)+a(x)p(x)$ where $f(x), a(x) \in F[x]$. Here $p(x)$ is the zero of this field, so $f(x)$ and $f + a(x)p(x)$ represent the same element in this field for any $a(x)$.

Ok, so how do we check if a polynomial is irreducible? Let look at the case we will most care about, which is $\mathbb{Q}[x]$. Now, we have the following Lemmas which you may have seen in the Galois theory course or algebra course, so we wont prove them:

Lemma 1.2.10 (Gauss's Lemma)**.** *A polynomial is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Here is a slightly different version for monic polynomials

Lemma 1.2.11 (Monic Gauss Lemma)**.** *Let $f \in \mathbb{Z}[x]$ be monic and assume that $f = gh$ with $g, h \in \mathbb{Q}[x]$ which are also monic. Then $g, h \in \mathbb{Z}[x]$.*

Remark 1.2.12. Convince yourself that both these lemmas deserve to be named similarly.

This reduces us to checking if a polynomial is irreducible over $\mathbb{Z}[x]$.

Proposition 1.2.13. *If $f(x)$ is a polynomial in $\mathbb{Z}[x]$, let $\bar{f}(x)$ denote its image in $\mathbb{F}_p[x]$. A polynomial $f(x)$ in $\mathbb{Z}[x]$ is irreducible, if we can find some prime number p such that $f(x)$ and $\bar{f}(x)$ have the same degree and $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$.*

Proof. This is the same as proving that, if $f(x)$ is reducible in $\mathbb{Z}[x]$ then it is also reducible in $\mathbb{F}_p[x]$, which is obvious. □

Lastly, we have:

Proposition 1.2.14 (Shönemann's Irreducibility Criterion)**.** *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $n > 0$. Assume that there is a prime p and an integer a such that*

$$f(x) = (x-a)^n + pg(x)$$

for $g(x) \in \mathbb{Z}[x]$. If $g(a) \not\equiv 0 \bmod p$ then $f(x)$ is irreducible modulo p^2 and in $\mathbb{Z}[x]$.

Proof. Assume for contradiction that

$$f(x) \equiv r(x)s(x) \bmod p^2,$$

where WLOG $r(x), s(x)$ are monic. Now, if we instead look at this modulo p, we have $(x-a)^n \equiv r(x)s(x) \bmod p$ and therefore, since we are in $\mathbb{F}_p[x]$ which is a UFD, we must have $r(x) \equiv (x-a)^i \bmod p$ and $s(x) \equiv (x-a)^j \bmod p$ with $i + j = n$ and $i, j > 0$. If we now evaluate at $x = a$ we see that

$$r(a) \equiv s(a) \equiv 0 \bmod p$$

as $i, j > 0$. But if we now go back to

$$f(x) \equiv r(x)s(x) \bmod p^2$$

we see that setting $x = a$ gives

$$pg(a) \equiv r(a)s(a) \equiv 0 \bmod p^2,$$

which contradicts $g(a) \not\equiv 0 \bmod p$.

Now, since we are irreducible modulo p^2 we are also irreducible in $\mathbb{Z}[x]$, since the same argument as in Proposition 1.2.13 applies. □

Corollary 1.2.15 (Eisenstein Criterion)**.** *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots, a_1 x + a_0$$

be a polynomial in $\mathbb{Z}[x]$ (with $n \geq 1$) and let p be a prime number. Suppose a_n is not divisible by p, $a_{n-1}, \ldots, a_0$ are all divisible by p and a_0 is not divisible by p^2. Then $f(x)$ is irreducible.

Proof. Since $a_n \not\equiv 0 \bmod p$, it is invertible. Now let b be any integer such that $b \equiv a_n^{-1} \bmod p$, then $bf(x) = x^n + pg(x)$ for some $g(x) \in \mathbb{Z}[x]$. Moreover, $g(0) \not\equiv 0 \bmod p$ since a_0 is not divisible by p^2. Therefore, we satisfy Shönemann's Irreducibility Criterion and therefore $bf(x)$ is irreducible and thus so is $f(x)$. □

Example 1.2.16. 1. The polynomial $3x^4 + 10x + 5$ is irreducible in $\mathbb{Z}[x]$ by Eisensteins criterion with $p = 5$.

2. Let p be a prime and let

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

Then this is irreducible. Lets prove this:

Note that we cant apply Eisenstein's criterion right away, but the trick is to consider

$$\Phi_p(x + 1) = x^{p-1} + px^{p-2} + \cdots + \binom{p}{2}x + p.$$

Now, by properties of binomial coefficients, we see that all coefficients other than the leading one are divisible by p and the last coefficient isn't divisible by p^2, so Eisensteins criterion applies.

Exercise 1.2.17. Prove that $f(x) \in \mathbb{Z}[x]$ is irreducible if and only if $f(x+a)$ is irreducible for any $a \in \mathbb{Z}$.

Example 1.2.18. Now we have more examples of fields:

1. Note that $x^2 - 2$ is irreducible in $\mathbb{Z}[x]$, so

$$\frac{\mathbb{Q}[x]}{(x^2 - 2)}$$

is a field.

2. $\mathbb{R}[x]/(x^2 + 1)$ is also a field as $x^2 + 1$ is irreducible over $\mathbb{R}$. This field is isomorphic to $\mathbb{C}$, but you need to be careful, its not *equal* to $\mathbb{C}$, only isomorphic to. We will talk about this more below.

3. Let $p(x) = x^2 + x + 1$ in $\mathbb{F}_2[x]$. Then $p(x)$ is irreducible in $\mathbb{F}_2[x]$ and thus

$$\mathbb{F}_2[x]/(x^2 + x + 1)$$

is also a field.

Exercise 1.2.19. Check that $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

Lastly, here is a fact about finite fields we will use several times later but we wont prove.

Proposition 1.2.20. *For each integer n and each prime number p, there is a unique finite field of size p^n. We denote it by $\mathbb{F}_{p^n}$. Conversely, every finite field has size p^n for some prime p and $n \in \mathbb{Z}_{>0}$.*

1.3 Field extensions

Definition 1.3.1 (Field extensions)**.** Let K be a field containing a field F. Then we call K a field extension of F (and F a subfield of K). This is denoted by K/F. The degree of a field extension K/F, denoted $[K : F]$ is the dimension of K as a vector space over F. A field extension is said to be finite if $[K : F]$ is finite, otherwise we say its infinite.

Proposition 1.3.2. *Let F be a field and $p(x)$ be an irreducible polynomial in $F[x]$ of degree n. Then $K := F[x]/(p(x))$ is a field extension of F and $[K : F] = n$.*

Proof. I claim that the image of $1, x, x^2, \ldots, x^{n-1}$ in K form a basis for K/F. To prove this, first note that, if $f(x) \in F[x]$ has degree less than n then its written in terms of this basis, so when we look at the image in K the same is true. So now assume that $\deg(f(x)) \geq n$ them we can do polynomial long division to write

$$f(x) = q(x)p(x) + r(x)$$

with $\deg(r(x)) < n$. So $f(x) \equiv r(x) \mod (p(x))$. So again we see that in K, $f(x)$ can be written in terms of this basis, so this basis spans K.

So we just need to prove that this basis is linearly independent. Let $\bar{x}^i$ denote the image of x^i in K. Then assume for contradiction, that $1, \bar{x}, \ldots, \bar{x}^{n-1}$ is not linearly independent. Then we can find $a_i \in F$ (not all zero) such that

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

this means

$$a_0 + a_1x + \cdots, +a_{n-1}x^{n-1} \equiv 0 \mod (p(x))$$

which means that $p(x)$ divides $a_0+a_1x+\cdots, +a_{n-1}x^{n-1}$ but this is impossible as $p(x)$ has degree n and $\deg(a_0 + a_1x + \cdots, +a_{n-1}x^{n-1}) < n$. □

Definition 1.3.3. Let K/F be a field extension and let $\alpha_1, \ldots, \alpha_n \in K$. Let $F(\alpha_1, \ldots, \alpha_n)$ denote the smallest subfield of K containing F and $\alpha_1, \ldots, \alpha_n$. We call it the field generated by $\alpha_1, \ldots, \alpha_n$.

A field generated by a single element is called a *simple extension*. In other words, $F(\alpha)$ is a simple extension of F. We call $\alpha \in K$ the primitive element for the extension.

Now, here is an important result:

Theorem 1.3.4. *Let F be a field and $p(x)$ an irreducible polynomial in $F[x]$. Moreover, let K/F be a field extension containing a root α of $p(x)$. Then there is an isomorphism*

$$F[x]/(p(x)) \cong F(\alpha)$$

given by sending $f(x)$ to $f(\alpha)$.[c]

Proof. Let me denote by ϕ' the map $F[x] \to F(\alpha)$ sending $f(x)$ to $f(\alpha)$. First note that $p(x)$ is in the kernel of ϕ', since $p(\alpha) = 0$ as α is taken to be a root of $p(x)$. Therefore, ϕ also induces a new map $F[x]/(p(x)) \to F(\alpha)$ which we call ϕ (we say that ϕ' "factors through" $F[x]/(p(x))$). Now we want to show ϕ is an isomorphism. First note that $\phi(x + (p(x))) = \alpha$ and if $a \in F$ then $\phi(a) = a$, so the image of ϕ has F and α in its image. Moreover, ϕ is a field homomorphism, so the image is again a field. This means that $F(\alpha)$ is in the image of ϕ (since by Definition 1.3.3, $F(\alpha)$ is defined to be the smallest such field). So we just need to check this map is injective.

Injectivity is easy, since if you recall, the kernel of any non-zero ring homomorphism to an integral domain is a prime ideal, and the only prime ideal in a field is the zero ideal. So since $F[x]/(p(x))$ is a field and our map is not the zero map, it must have kernel being the other prime ideal, which is (0) and thus is injective. □

Ok, so why is this so important. Well lets consider the first example in Example 1.2.18. Here we took $\mathbb{Q}[x]/(x^2 - 2)$, now the above result tells us that this field is ISOMORPHIC to $\mathbb{Q}(\sqrt{2})$ which you may remember as the field whose elements look like $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. But note that the theorem above doesn't say anything about which root of $x^2 - 2$ one should take. So we equally have

$$\mathbb{Q}(\sqrt{2}) \cong \frac{\mathbb{Q}[x]}{(x^2 - 2)} \cong \mathbb{Q}(-\sqrt{2}).$$

Remark 1.3.5. One slightly more philosophical observation, is that even to define $F(\alpha)$ in Definition 1.3.3 we needed to assume the existence of a field K containing a root of my polynomial $p(x)$, so by definition $F(\alpha)$ depends on K. So just for the moment let me highlight this dependence on K by writing $F(\alpha)$ as $F_K(\alpha)$.

Lets look at the example above. Here we have to assume that there is some field which contains $\sqrt{2}$. But how do we choose such a K? for example we could have K being $K_1 := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ or $K_2 := \mathbb{Q}(2^{1/4})$ or $\mathbb{C}$ or something else. In each case we get our own version $\mathbb{Q}(\sqrt{2})$ which we are for the moment denoting as $\mathbb{Q}_{K_1}(\sqrt{2}), \mathbb{Q}_{K_2}(\sqrt{2})$ and $\mathbb{Q}_{\mathbb{C}}(\sqrt{2})$. Now, one can ask, are all these versions the same? well in each case they are isomorphic to $\mathbb{Q}[x]/(x^2 - 2)$ but to construct the isomorphisms we had to make choices, particularly we had to pick a root. So all the versions are in fact isomorphic, but they aren't "equal", since to be equal we would require the existence of a canonical isomorphisms between them, i.e. choice free isomorphisms.

What's the point of all this? what I want to highlight is how defining $\mathbb{Q}(\sqrt{2})$ requires some choices, but defining $\mathbb{Q}[x]/(x^2 - 2)$ is choice free. In practice what we will do is just find some K in Definition 1.3.3 which works

[c] In other words, you evaluate a polynomial at α

in all cases. Meaning, we fix a K which contains the roots of all polynomials in $F[x]$. When $F = \mathbb{Q}$, then we will just take $K = \mathbb{C}$.

1.3.6 Algebraic extensions

Definition 1.3.7. Let K/F be a field extension and let $\alpha \in K$. Then we say α is algebraic over F if there exists a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise we say α is transcendental.

Example 1.3.8.
1. $\sqrt{2}$ is algebraic over $\mathbb{Q}$.
2. $\sqrt{-1}$ is algebraic over $\mathbb{R}$.

Exercise 1.3.9. Prove that if $\alpha \in K$ is algebraic over F, then it is also algebraic over any field extension of F.

Proposition 1.3.10. *Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x)$ in $F[x]$ which has α as a root. Moreover, $m_{\alpha,F}(x)$ divides any other polynomial in $F[x]$ with α as a root. This polynomial is called the minimal polynomial of α over F.*

Proof. Lets take $m_{\alpha,F}(x)$ to be a polynomial of minimal degree having α as a root. Moreover, since we are working over a field, we can multiply by some element in F to make sure its monic. This is our candidate for the minimal polynomial. We need to show its unique and irreducible.

If $m_{\alpha,F}(x)$ were reducible, then we would have

$$m_{\alpha,F}(x) = f(x)g(x),$$

so $f(\alpha)g(\alpha) = 0$. Therefore, since we are in a field, this means either $f(\alpha) = 0$ or $g(\alpha) = 0$. But $m_{\alpha,F}(x)$ has minimal degree, so one of f or g must have degree 0 (i.e. a constant.) thus $m_{\alpha,F}(x)$ is irreducible.

So we just need to check its unique. Note that if $f(x)$ is any polynomial with α as a root, then by polynomial long division we have

$$f(x) = q(x)m_{\alpha,F}(x) + r(x)$$

with $\deg(r(x)) < \deg(m_{\alpha,F}(x))$. But then evaluating this at α we would have $r(\alpha) = 0$, but which can't happen as it has smaller degree than $m_{\alpha,F}(x)$, so $r(x) = 0$. Therefore, $m_{\alpha,F}(x)$ divides any polynomial with α as a root. From this it follows that if we had two minimal polynomials $m_1(x), m_2(x)$ then $m_1(x)|m_2(x)$ and $m_2(x)|m_1(x)$ so $m_1(x) = am_2(x)$ for some $a \in F$, but now being monic comes to the rescue to say that $a = 1$, giving uniqueness and finishing the proof. □

Exercise 1.3.11. Let L/F be a field extension and let α be algebraic over F, then prove that $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Now, from Theorem 1.3.4, Proposition 1.3.2 and Proposition 1.3.10 we have the following:

Corollary 1.3.12. *Let K/F be a field extension and $\alpha \in K$ algebraic over F. Then*

$$F[x]/(m_{\alpha,F}(x)) \cong F(\alpha)$$

and moreover $[F(\alpha) : F] = \deg(m_{\alpha,F}(x))$.

Definition 1.3.13. Let K/F be a field extension. Then we say K is algebraic over F if every element of K is algebraic over F.

Example 1.3.14.

1. $\mathbb{Q}(\sqrt{2})$ is algebraic over $\mathbb{Q}$.
2. $\mathbb{C}$ is algebraic over $\mathbb{R}$.

Proposition 1.3.15. *Let K/F be a field extension. Then $\alpha \in K$ is algebriac over F if and only if there is a finite extension of F (inside K) containing α.*

Proof. If α is algebraic over F, then we know that $F(\alpha)$ is a field isomorphic to $F[x]/(m_{\alpha,K}(x))$. Moreover, $[F(\alpha) : F] = \deg(m_{\alpha,F}(x))$ by Corollary 1.3.12 and by definition of $F(\alpha)$ is is the the smallest such field, so $F(\alpha)$ is contained in K.

Conversely, if α is in a finite extension L/F of degree n. Then consider $1, \alpha, \alpha^2, \ldots, \alpha^n$. These $n+1$ elements must be linearly dependent over F, so there exist b_i such that

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$$

which proves that α is algebraic over F since its a root of $b_0 + b_1x + \cdots + b_nx^n$. □

Corollary 1.3.16. *If K/F is a finite extension, then is it algebraic.*

Exercise 1.3.17. Is the converse of this statement true? In other words, if K/F is an algebraic extension, then does it have to be finite?

Definition 1.3.18. We say a field extension K/F is finitely generated, if there are finitely many elements $\alpha_1, \ldots, \alpha_n$ such that $K = F(\alpha_1, \ldots, \alpha_n)$.

Now, here are a couple of facts you might remember from Galois theory

Proposition 1.3.19 (Tower Law)**.** *Let K/F be a field extension, α_i be elements of K which are algebraic over F and let $F_i = F(\alpha_1, \ldots, \alpha_i)$.*

1. *$F_n = F_{n-1}(\alpha_n)$ and in general $F_i = F_{i-1}(\alpha_i)$.*
2. *$[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F]$ (note $F_0 = F$)*

Proposition 1.3.19 and Corollary 1.3.16 gives us:

Theorem 1.3.20. *A field extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F.*

Corollary 1.3.21. *Let $\alpha, \beta \in K$ be non-zero and algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β, α^{-1}, β^{-1},etc are also algebraic over F.*

Proof. Note that $\alpha, \beta \in F(\alpha, \beta)$. But from Proposition 1.3.19 we have that $[F(\alpha, \beta) : F]$ is finite. So by Corollary 1.3.16 $F(\alpha, \beta)$ is algebraic over F, meaning all of its elements are algebraic over F, which gives the result. □

1.4 Algebraic numbers and number fields

Definition 1.4.1. An algebraic number is a complex number which is algebraic over $\mathbb{Q}$. Meaning, it is a root of a polynomial $f(x) \in \mathbb{Q}[x]$.

Notation 1.4.2. If α is an algebraic number, then it has a minimal polynomial which we denoted by $m_{\alpha,\mathbb{Q}}$ in Proposition 1.3.10. Since from now on we will be working over $\mathbb{Q}$, we will make the notational convention that $m_\alpha := m_{\alpha,\mathbb{Q}}$

Definition 1.4.3. If α is an algebraic number and $m_\alpha(x)$ is its minimal polynomial, then the set of roots of $m_\alpha(x)$ in $\mathbb{C}$ are called the *conjugates* of α.

Example 1.4.4.

1. $0, 47, \sqrt{2}, \sqrt{-1}, 3/4, \sqrt[10]{5}$ are all algebraic numbers
2. If d is a square-free integer, $\sqrt{d}$ is algebraic and its conjugate root is $-\sqrt{d}$.
3. $\alpha = \sqrt{2+\sqrt{2}}$ is an algebraic number. Lets prove it by finding its minimal polynomial:

$$\alpha = \sqrt{2+\sqrt{2}} \tag{1.1}$$
$$\alpha^2 - 2 = \sqrt{2} \tag{1.2}$$
$$(\alpha^2 - 2)^2 = 2 \tag{1.3}$$
$$\alpha^4 - 4\alpha^2 + 2 = 0 \tag{1.4}$$

So we see that α satisfies $x^4 - 4x^2 + 2$, which means its algebraic.

Is this the minimal polynomial? well lets check. By Eisensteins Criterion 1.2.15 with $p = 2$ we see that this is irreducible. Moreover its monic, so it must be the minimal polynomial.

Now, what are the conjugate roots of α? If you work backwards through the computation above you'll see that $\pm\sqrt{2 \pm \sqrt{2}}$ are all the roots of m_α and thus are the conjugates of α.

Non-example 1.4.5. $\pi = 3.1415\ldots$ is NOT an algebraic number (although this isn't easy to prove).

Definition 1.4.6. A *Number field* is a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$.

Example 1.4.7. Let d be a square-free integer then $\mathbb{Q}(\sqrt{d}) = \{a+b\sqrt{d} | a, b \in \mathbb{Q}\}$ is a number field of degree 2 over $\mathbb{Q}$.

Note that by Corollary 1.3.16 we see that every element of a number field is a algebraic number.

By the Fundamental Theorem of algebra, if we take any polynomial $f(x) \in \mathbb{Q}[x]$, then it has a root α in $\mathbb{C}$. Therefore $\mathbb{Q}(\alpha)$ is a number field. This gives us a great supply of number fields. Similarly, using Theorem 1.3.20 we can take any finite set $\{\alpha_1, \ldots, \alpha_n\}$ of algebraic numbers and then $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ will again be a number field.

Exercise 1.4.8. Let $\overline{\mathbb{Q}}$ denote the set of all algebraic numbers. Prove that $\overline{\mathbb{Q}}$ is actually a field. Is it a number field? explain your answer.

Exercise 1.4.9. Let α be an algebraic number with minimal polynomial $m_\alpha(x) = \sum_i a_i x^i$. Then using this, write down the minimal of $1/\alpha$.

1.5 Embeddings

Definition 1.5.1. Let K be a number field. Then an embedding of K is a non-zero ring homomorphism $\sigma : K \hookrightarrow \mathbb{C}$.

Remark 1.5.2. Note that since σ is a ring homomorphism, we must have that $\sigma(x) = x$ for all $x \in \mathbb{Q} \subset K$.

Exercise 1.5.3. Prove that an embedding is injective.

Now, since by definition our number fields are subfields of $\mathbb{C}$, then we have at least one embedding, which is just the identity embedding (i.e, send x to x), sometimes called the standard embedding. But there can be others.

Example 1.5.4. Let $K = \mathbb{Q}(\sqrt{2})$ then we have two embeddings:

$$\sigma_1 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C} \qquad \text{sending} \qquad a + b\sqrt{2} \mapsto a + b\sqrt{2} \tag{1.5}$$

$$\sigma_2 : \mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C} \qquad \text{sending} \qquad a + b\sqrt{2} \mapsto a + b(-\sqrt{2}) \tag{1.6}$$

Here σ_1 is just the identity embedding. Note that since the embedding has to keep rational numbers fixed, the a, b above stay the same, what the different embeddings change is where $\sqrt{2}$ maps to, but $\sqrt{2}$ cant just map to anything, we will see later that in fact it has to map to a conjugate root.

Lets take this as a given and now consider the embeddings of $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a degree 4 extension of $\mathbb{Q}$ and every element can be

written as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \mathbb{Q}$. Now, the embeddings are:

$$\nu_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \tag{1.7}$$
$$\nu_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \tag{1.8}$$
$$\nu_3 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \tag{1.9}$$
$$\nu_4 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \tag{1.10}$$

Notice that since $K \subset L$ (just take elements with $c = d = 0$), then it makes sense to restrict the embeddings of L to K. If you do this, then we see that ν_1, ν_3 both give the identity embedding $\sigma_1 : K \hookrightarrow \mathbb{C}$, while ν_2, ν_4 restrict to σ_2.

Definition 1.5.5. Let K/F be a finite extension of number fields and let $\sigma : F \hookrightarrow \mathbb{C}$ and $\nu : K \hookrightarrow \mathbb{C}$ be embeddings. Then we say ν extends σ if ν restricted to F agrees with σ. Symbolically, we say $\nu|_F = \sigma$.

Proposition 1.5.6. *Let K/F be an extension of number fields and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding such that $\sigma\,|_F = \mathrm{id}$ where* id *denotes the identity embedding. Then if $f(x) \in F[x]$ is an irreducible polynomial and α is one of its roots, then σ sends α to a conjugate of α.*

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then since σ fixes F, we see that since

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

it follows that

$$a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n = 0$$

and therefore, $\sigma(\alpha)$ also is a root of f, which gives the result. □

Lemma 1.5.7. *(Separability Lemma) Let K be a number field and let $f(x) \in K[x]$ be an irreducible polynomial of degree $n \geq 1$. Then $f(x)$ has n distinct roots.*

Moreover, if $\sigma : K \hookrightarrow \mathbb{C}$ is any embedding and $f^\sigma(x)$ denotes the polynomial obtained by applying σ to each coefficient, then f^σ also has n distinct roots.

Proof. By the fundamental theorem of algebra, $f(x)$ has n roots in $\mathbb{C}$, so we only need to show that there are no repeated roots. For this, consider the derivative $f'(x)$ of $f(x)$. f' is also in $K[x]$ and is non-zero. If $f(x)$ has a repeated root, then f and f' would share a common factor, call it h. So let g denote the greatest common divisor of f and f'. Then $\deg(g) \leq n - 1$ and divides f, but f is irreducible, so g must be a constant (i.e. $\deg(g) = 0$),

but then as $h|g$ this means h is also a constant and thus, f, f' do not share a common factor.

The same proof works using f^σ instead. So the result follows. □

Proposition 1.5.8. *For every embedding $\sigma : F \hookrightarrow \mathbb{C}$ there are $[K : F]$ embeddings of K that extend F.*

Proof. We will prove this by induction on $[K : F]$. If $K = F$ there is nothing to prove. So assume $K \neq F$ and let σ be an embedding of F. Now take $\alpha \in K \backslash F$ (i.e. in K but not F, which we can do since we are assuming $K \neq F$). Consider its minimal polynomial over F, denoted $m_{\alpha,F}$. Now let β be a root of the polynomial you get from applying σ to $m_{\alpha,F}$, which is $m^\sigma_{\alpha,F} = m_{\alpha,F^\sigma}$. Here F^σ denotes the image of F under σ, which is a number field isomorphic to F. Now, m_{α,F^σ} is again irreducible over F^σ since under an isomorphism an irreducible polynomial will stay irreducible.

Now, from Theorem 1.3.4 we have

$$F(\alpha) \cong F[x]/(m_{\alpha,F}) \cong F^\sigma[x]/(m^\sigma_{\alpha,F}) \cong F^\sigma[x]/(m_{\beta,F^\sigma}) \cong F^\sigma(\beta)$$

therefore there is an isomorphism $\sigma : F(\alpha) \cong F^\sigma(\beta)$ which sends α to β and restricts to σ on F. Doing this for each root of $m^\sigma_{\alpha,F}$ we see that there are $\deg(m_{\alpha,F}) = [F(\alpha) : F]$ extensions of σ to $F(\alpha)$. Now, use the inductive hypothesis. □

Definition 1.5.9. We say an embedding is real if its image is $\mathbb{R} \subset \mathbb{C}$. Otherwise we say the embedding is complex. Note that if σ is a complex embedding, then so is its complex conjugate $\overline{\sigma}$ (i.e. this is the embedding given by applying σ and then doing complex conjugation.) We call $\sigma, \overline{\sigma}$ a pair of complex conjugate embeddings.

Remark 1.5.10. Note that Proposition 1.5.8 applied to $K/\mathbb{Q}$ tells us that if r_1 is the number of real embedding and r_2 is the number of complex conjugate embeddings (i.e. there are $2r_2$ complex embeddings), then

$$[K : \mathbb{Q}] = r_1 + 2r_2.$$

Theorem 1.5.11 (Primitive element theorem)**.** *Let K/F be a finite extension of number fields. Then there exists $\alpha \in K$ such that $K \cong F(\alpha)$.*

Proof. We prove this by induction on $[K : F]$. If $K = F$ there is nothing to prove. So assume that $K \neq F$ and let $\alpha \in K \backslash F$. Then by our inductive hypothesis we have $K = F(\alpha, \beta)$ for some β. We claim that there are infinitely many c such that $K = F(\alpha + c\beta)$. To do this we will show that there can only be finitely many $c \in F$ such that $K \neq F(\alpha + c\beta)$. Assume this is the case, then lets think about how many conjugates $\alpha + c\beta$ has over F. If $K = F(\alpha + c\beta)$ then by Proposition 1.5.8 there would be $[K : F]$ conjugates

of $(\alpha + c\beta)$, but since we are assuming we aren't in this situation there must be fewer conjugates. In particular, we must have two distinct embeddings $\eta, \sigma : K \hookrightarrow \mathbb{C}$ which extend F and send $(\alpha + c\beta)$ to the same element. So

$$\eta(\alpha) + c\eta(\beta) = \sigma(\alpha) + c\sigma(\beta).$$

Now, note that $\sigma(\beta) \neq \eta(\beta)$ since otherwise, $\eta(\alpha) = \sigma(\alpha)$ and thus, since $K = F(\alpha, \beta)$ we'd have $\sigma = \eta$, which is a contradiction. Therefore

$$c = \frac{\eta(\alpha) - \sigma(\alpha)}{\sigma(\beta) - \eta(\beta)},$$

but by Proposition 1.5.6 there are only finitely many possibilities for $\eta(a)$, $\eta(\beta)$, $\sigma(\alpha)$, $\sigma(\beta)$.

If you use Galois theory then there is a much quicker proof: Since $[K : F]$ is finite, there are only finitely many intermediate fields. Now just pick $\alpha \in K$ which is not contained in any of there intermediate fields, then $F(\alpha)$ is an extension of F not contained in any proper subfield of K, so $K = F(\alpha)$. □

1.6 The standard representation

Definition 1.6.1. Let K be a number field and let $\alpha \in K$. Then we can associate to α a linear operator

$$A_\alpha : K \longrightarrow K \qquad x \mapsto \alpha x.$$

This can be written as a matrix over $\mathbb{Q}$ by picking a basis of K over $\mathbb{Q}$. The map $\alpha \to A_\alpha$ is called the *standard representation.*

Remark 1.6.2. If we had K/F an extension of number fields then by picking a basis of K/F we can write A_α as a matrix with coefficients in F.

Example 1.6.3. Let $K = \mathbb{Q}(\sqrt{5})$ and let $\alpha = 3 + 2\sqrt{5}$. We have a basis for $K/\mathbb{Q}$ given by $\{1, \sqrt{5}\}$. So $A_\alpha(1) = 3 + 2\sqrt{5}$ and

$$A_\alpha(\sqrt{5}) = (3 + 2\sqrt{5})(\sqrt{5}) = 10 + 3\sqrt{5}$$

therefore in this basis, we have

$$A_\alpha = \begin{pmatrix} 3 & 10 \\ 2 & 3 \end{pmatrix}$$

Proposition 1.6.4. *Let K be a number field and $\alpha \in K$.*

1 *The map $\alpha \to A_\alpha$ is injective.*

2 Let $\alpha, \beta \in K$ and $\lambda \in \mathbb{Q}$ then

$$A_{\alpha\beta} = A_\alpha A_\beta \qquad A_{\alpha+\beta} = A_\alpha + A_\beta \qquad A_{\lambda\alpha} = \lambda A_\alpha$$

3 If C_α is the characteristic polynomial of A_α then $C_\alpha(\alpha) = 0$.

Proof. For [1] we just need to note that $A_\alpha(1) = \alpha$, therefore $\alpha = \beta$ if and only if $A_\alpha = A_\beta$.

For [2], this is obvious from the definition of A_α as the multiplication by α map.

Lastly for [3] note that by Cayley–Hamilton that $C(A_\alpha) = 0$. Now, from [2] it follows that for any polynomial $f(x) \in \mathbb{Q}[x]$ we have $f(A_\alpha) = A_{f(\alpha)}$, so $A_{C_\alpha(\alpha)} = C_\alpha(A_\alpha) = 0$ but then by [1] we must have $C_\alpha(\alpha) = 0$.

□

Definition 1.6.5. For K a number field and $\alpha \in K$, then the characteristic polynomial of A_α is known as the *field polynomial* of α. We shall denote it by C_α, but note that it depends on the field we are working with. In particular, if we write a basis for K over $\mathbb{Q}$ or a basis for K over F (for F some subfield), then the field polynomial can be different in each case. Therefore, unless otherwise stated we will assume we mean a basis of $K/\mathbb{Q}$.

Proposition 1.6.6. *Let $K = \mathbb{Q}(\alpha)$ for some algebraic number α. Then $C_\alpha = m_\alpha$, in other words, the field polynomial of α agrees with the minimal polynomial.*

Proof. Note that C_α will be a monic polynomial of degree $[K : \mathbb{Q}]$ and has α as a root. But this means it is divisible by m_α. But the are both monic and have the same degree, therefore must be equal. □

Proposition 1.6.7. *Let K be a number field and $\beta \in K$. Then A_β is diagonalizable over $\mathbb{C}$ and*

$$C_\beta = \prod_i (x - \sigma_i(\beta)) \in \mathbb{C}[x]$$

Here the product is over all embeddings σ_i of K into $\mathbb{C}$.

Proof. By the Primitive Element Theorem 1.5.11 we can write $K \cong \mathbb{Q}(\alpha)$. Now, from Proposition 1.6.6, we know $C_\alpha = m_\alpha$ and by Proposition 1.5.6 we know that $m_\alpha = \prod_i (x - \sigma_i(\alpha))$, therefore, C_α has $n := [K : \mathbb{Q}]$ distinct roots (by Lemma 1.5.7), therefore A_α is diagonalisable over $\mathbb{C}$, with eigenvalues being the conjugates of α. So we can find a matrix P (over $\mathbb{C}$) such that

$$P^{-1} A_\alpha P = \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix}$$

Now, $\beta \in K$ we can find $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = \beta$ and therefore

$$P^{-1}A_\beta P = P^{-1}A_{f(\alpha)}P = P^{-1}f(A_\alpha)P = f(P^{-1}A_\alpha P) = \begin{pmatrix} f(\sigma_1(\alpha)) & & \\ & \ddots & \\ & & f(\sigma_n(\alpha)) \end{pmatrix}$$
$$= \begin{pmatrix} \sigma_1(\beta) & & \\ & \ddots & \\ & & \sigma_n(\beta) \end{pmatrix}$$

And since $P^{-1}A_\beta P$ and A_β have the same characteristic polynomial, we get the result. □

Corollary 1.6.8. *Let K be a number field and $\beta \in K$, then*

$$C_\beta(x) = m_\beta(x)^{[K:\mathbb{Q}(\beta)]} \in \mathbb{Q}[x]$$

Proof. By Proposition 1.6.7 we know all the roots of C_β are of the form $\sigma_i(\beta)$. Now, let v_i be the embedding of $\mathbb{Q}(\beta)$. Then from Proposition 1.5.8 we know that each v_i extends to $[K : \mathbb{Q}(\beta)]$ embeddings of K and by definition each of these embeddings keeps $v_i(\beta)$ the same. So for each $v_i(\beta)$ there are $[K : \mathbb{Q}(\beta)]$ embeddings σ_j such that $\sigma_j(\beta) = v_i(\beta)$. Now, since $m_\beta(x) = \prod_i (x - v_i(\beta))$ we see that

$$C_\beta = \left[\prod_i (x - v_i(\beta))\right]^{[K:\mathbb{Q}(\beta)]}$$

giving the result.

Note that $[K : \mathbb{Q}] = [K : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$ so the power is correct, since C_β has degree $[K : \mathbb{Q}]$ and m_β has degree $[\mathbb{Q}(\beta) : \mathbb{Q}]$. □

1.7 Norm and Trace

Let K/F be a field extension, we now look at ways of taking an element in K and obtaining elements in F.

Definition 1.7.1. Let $K/\mathbb{Q}$ be a number field and $\alpha \in K$. Then we define the norm of α by

$$N_{K/\mathbb{Q}}(\alpha) = \mathrm{Det}(A_\alpha) \in \mathbb{Q}$$

and the trace of α by

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Trace}(A_\alpha) \in \mathbb{Q}.$$

Here $\mathrm{Trace}(A_\alpha)$ is the sum of the diagonal entries of A_α.

Example 1.7.2. Let $K = \mathbb{Q}(\sqrt{5})$ and $\alpha = 3 + 2\sqrt{5}$, then $A_\alpha = \left(\begin{smallmatrix} 3 & 10 \\ 2 & 3 \end{smallmatrix}\right)$ and therefore $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 6$ and $N_{K/\mathbb{Q}}(\alpha) = -11$.

Proposition 1.7.3. *Let K be a number field of degree n over $\mathbb{Q}$ and $\alpha \in K$. Then*

$$C_\alpha(x) = x^n - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)x^{n-1} + \cdots + (-1)^n N_{K/\mathbb{Q}}(\alpha).$$

Proof. This is immediate from the definition of C_α as the characteristic polynomial of A_α.

Specifically, its a basic result in linear algebra, that says if M is a $n \times n$ matrix with characteristic polynomial $C(X)$ then

$$C(X) = X^n - \mathrm{Trace}(M)X^{n-1} + \cdots + (-1)^n \det(M)$$

where $\mathrm{Trace}(M)$ is the sum of the diagonal entries of M. □

Exercise 1.7.4. Let $K = \mathbb{Q}(\sqrt{d})$ with d square-free. Show that

$$\mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a \qquad N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2.$$

Proposition 1.7.5. *Let K be a number field and $\alpha, \beta \in K$. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta) \qquad N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta).$$

Proof. By definition we only need to consider the trace of $A_\alpha + A_\beta$ and the determinant of $A_\alpha A_\beta$. But we know from linear algebra that trace is additive and determinant is multiplicative, so the result follows. □

Proposition 1.7.6. *Let K be a number field, $\alpha \in K$ and let σ_i be the embeddings of K into $\mathbb{C}$. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_i \sigma_i(\alpha) \qquad N_{K/\mathbb{Q}}(\alpha) = \prod_i \sigma_i(\alpha)$$

Proof. First recall that the norm and trace of a matrix and invariant under conjugation. Therefore, the $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Trace}(A_\alpha) = \mathrm{Trace}(P^{-1}A_\alpha P)$ similarly for the norm. Now, by Proposition 1.6.7 we see that we can find P such that $P^{-1}A_\alpha P$ is diagonal with entries $\sigma_i(\alpha)$. From this the result follows. □

One of the important properties of the trace function is that it gives us a $\mathbb{Q}$-bilinear pairing on K, defined as follows:

Definition 1.7.7. Let K be a number field. We have a pairing

$$\langle , \rangle : K \times K \to \mathbb{Q}$$

given by

$$\langle \alpha, \beta \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta)$$

Proposition 1.7.8. *The trace pairing is a $\mathbb{Q}$-bilinear perfect pairing. In other words if $\alpha, \beta \in K$ and $\lambda \in \mathbb{Q}$ then*

$$\langle \lambda\alpha, \beta \rangle = \langle \alpha, \lambda\beta \rangle = \lambda \langle \alpha, \beta \rangle$$

and if $\alpha \in K$ is such that $\langle \alpha, \beta \rangle = 0$ for all $\beta \in K$, then $\alpha = 0$.

Proof. The fact that it is bilinear follows at once from the definition of $\mathrm{Tr}_{K/\mathbb{Q}}$. To check it is perfect, consider $\alpha \neq 0$. Then $\alpha^{-1} \in K$ and thus $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}]$ which is non-zero. □

Chapter 2

Algebraic integers

We will now move to studying some very important subrings of number fields, known as the rings of algebraic integers.

2.1 Rings of integers

Definition 2.1.1. Let K be a field extension of $\mathbb{Q}$ (not necessarily finite). An element α is called an algebraic integer if it is a root of a *monic* polynomial with coefficients in $\mathbb{Z}$.

Lemma 2.1.2. *If A is a matrix with integer coefficients, then its eigenvalues are algebraic integers.*

Proof. If the matrix is integral, its characteristic polynomial is monic with integer coefficients, and thus the eigenvalues are algebraic integers. □

Example 2.1.3.
1. $\sqrt{2}$ is an algebraic integer as it satisfies $x^2 - 2$.
2. Any integer $n \in \mathbb{Z}$ is an algebraic integer as they satisfy $x - n$.

Non-example 2.1.4. π,ϵ are not algebraic integers or even algebraic numbers.

Exercise 2.1.5. Let $K = \mathbb{Q}(\sqrt{5})$, is $\frac{1+\sqrt{5}}{2}$ an algebraic integer?

Notation 2.1.6. If K is a field extension of $\mathbb{Q}$ we denote the set of algebraic integers in K by $\mathcal{O}_K$. We will show later that this is in fact a ring.

Remark 2.1.7. Recall the we defined $\overline{\mathbb{Q}}$ to be the subfield of all algebraic numbers in $\mathbb{C}$. One can similarly define $\overline{\mathbb{Z}}$ to be the ring (we will see later why this is a ring) of all algebraic integers. From this, one then gets $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ for K a number field.

In general it can be hard to prove something isn't an algebraic integer, since you'd have to prove it satisfies no monic polynomial with inter coefficients. But we have the following result that helps in some cases:

Proposition 2.1.8. *Let $\alpha \in K$ be an algebraic number with minimal polynomial m_α. Then α is an algebraic integer if and only if m_α has integer coefficients (note that it will be monic by the definition of minimal polynomial).*

Proof. If α is an algebraic integer, then its an algebraic number, so I claim that m_α is monic with integer coefficient. We know α satisfies some some monic polynomial $f(x)$ with integer coefficients and therefore m_α divides $f(x)$. Now use the monic Gauss lemma 1.2.11 to get that m_α is in $\mathbb{Z}[x]$.

Conversely, if m_α is has integer coefficients, then α satisfies a monic polynomial with integer coefficients, thus is an algebriac integer. □

Corollary 2.1.9. *Let K be a number field and $\alpha \in K$. Then α is an algebraic integer if and only if C_α has integer coefficients.*

Proof. This follows from Corollary 1.6.8 and Proposition 2.1.8. □

Corollary 2.1.10. *Let K be a number fields and $\alpha \in K$. Then there exists a $n \in \mathbb{Z}\backslash\{0\}$ such that $n\alpha$ is an algebraic integer.*

Proof. Let A_α be the standard representation of α. Then this is a matrix with rational entries. So if we clear denominators by multiplying with a suitable integer n we get that $nA_\alpha = A_{n\alpha}$ is an matrix with integer entries and therefore $n\alpha$ is an algebraic integer by Lemma 2.1.2. □

Theorem 2.1.11 (Integers in quadratic fields)**.** *Let d be a square free integer and let $K = \mathbb{Q}(\sqrt{d})$ then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Proof. Let $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. If $b = 0$ then we are just asking which rational numbers are algebraic integers, which we have seen are only the integers. So assume $b \neq 0$. Then the minimal polynomial of α over $\mathbb{Q}$ is

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

Therefore, α is an algebraic integer if and only if $2a$ and $(a^2 - db^2)$ are integers.

Now, since $2a$ is an integer, we have $4a^2$ is an integer, and thus $d(2b)^2$ must be an integer. If $2b$ was not an integer, then a p^2 (for some prime p) would appear in the denominator of $(2b)^2$. This would force d to be divisible by p^2 contradicting the square-free assumption. Thus $2b \in \mathbb{Z}$.

So let $u = 2a, v = 2b$. Then we have $u^2 - dv^2 \equiv 0 \pmod 4$. Now, if v is even, then so is u in which case $a, b \in \mathbb{Z}$. So assume v is odd, we need to show this can only happen if $d \equiv 1 \mod 4$. Now, $v^2 \equiv 1 \pmod 4$, and u^2 is

either $0, 1 \pmod 4$. But note it can't be zero since d cant be $0 \pmod 4$ as its square-free, therefore $u^2 \equiv 1 \mod 4$ and hence $d \equiv 1 \mod 4$. $\square$

Exercise 2.1.12. Check that if d is square-free and congruent to 1 modulo 4 then $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \pmod 2\}$

Definition 2.1.13. Let $\alpha \in \mathbb{C}$. We let $\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[x]\}$, in other words its the smallest ring containing both $\mathbb{Z}$ and α.

If we think of $\mathbb{Z}[\alpha]$ simply as an additive group, then it is generated by $\{1, \alpha, \alpha^2, \dots\}$.

Definition 2.1.14. Let $\alpha \in \mathbb{C}$. We say $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group if there exits a finite set $\{b_1, \dots, b_n\}$ of elements $b_i \in \mathbb{Z}[\alpha]$ such that every element of $\mathbb{Z}[\alpha]$ may be written in the form

$$x_1 b_1 + \cdots + x_n b_n$$

with $x_i \in \mathbb{Z}$.

Theorem 2.1.15. *Let $\alpha \in \mathbb{C}$. The following are equivalent:*

(1) α is an algebraic integer.

(2) As an additive group, $\mathbb{Z}[\alpha]$ is finitely generated.

(3) α is an element of some subring of $\mathbb{C}$ having a finitely generated additive group.

(4) $\alpha A \subset A$ with $A \subset \mathbb{C}$ some finitely generated additive subgroup. Here αA is the set of elements of the form αx for $x \in A$.

Proof. (1) $\implies$ (2) : Since α is an algebraic integer, it is the root of the monic polynomial m_α of degree n, say, which has integer coefficients. In this case we claim that $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is generates $\mathbb{Z}[\alpha]$. For this we note that if $f(\alpha) \in \mathbb{Z}[\alpha]$, then by doing polynomial long division we have $f(x) = q(x)m_\alpha(x) + r(x)$ with $\deg(r) < n$. Now if evaluate at α we get $f(\alpha) = r(\alpha)$. But since $\deg(r) < n$ we see that $r(\alpha)$ is in the $\mathbb{Z}$ span of $\{1, \alpha, \cdots, \alpha^{n-1}\}$. Thus giving the claim.

(2) $\implies$ (3) $\implies$ (4) : This is trivial.

It remains to prove (4) $\implies$ (1). Let $\{a_1, \dots, a_r\}$ be a basis of A. Then as each $\alpha a_i \in A$ we can again write it in terms of this basis, so we get a system of equations

$$\begin{aligned}
\alpha a_1 &= x_{1,1}a_1 + \cdots + x_{1,r}a_r \\
\alpha a_2 &= x_{2,1}a_1 + \cdots + x_{2,r}a_r \\
&\vdots \\
\alpha a_r &= x_{r,1}a_1 + \cdots + x_{r,r}a_r
\end{aligned}$$

with the $x_{i,j} \in \mathbb{Z}$. If we write this in matrix form by setting $X = x_{i,j}$, $a = (a_1, \ldots, a_r)$ then we have

$$Xa^T = \alpha a^T$$

(here $()^T$ denotes transpose). Therefore, α is an eigenvalue of X, which is a matrix with integer entries. Thus by Lemma 2.1.2 we must have that α is an algebraic integer.

□

Using this we can now prove that $\mathcal{O}_K$ is actually a ring.

Corollary 2.1.16. *Let α, β be algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Since α, β are algebraic integers, then by Theorem 2.1.15 (2) we have $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated (as additive groups). Moreover, the ring $\mathbb{Z}[\alpha, \beta]$ (take this to be defined as the smallest ring containing $\mathbb{Z}, \alpha, \beta$) is also finitely generated, since if $\{a_1, \ldots, a_n\}$ generate $\mathbb{Z}[\alpha]$ and $\{b_1, \ldots, b_m\}$ generates $\mathbb{Z}[\beta]$ then $\{a_i b_j\}_{i,j}$ generates $\mathbb{Z}[\alpha, \beta]$. Now, $\mathbb{Z}[\alpha, \beta]$ contains both $\alpha + \beta$ and $\alpha\beta$, then 2.1.15 (3) tells us that they must also be algebraic integers. □

Corollary 2.1.17. *If K is a number field, then $\mathcal{O}_K$ is a ring.*

Proof. This follows at once from the above, since if α, β are algebraic integers in K, then $\alpha + \beta \in K, \alpha\beta \in K$ and by the above, they are both algebraic integers. □

Exercise 2.1.18. Let K/F be an extension of number fields and assume that $\alpha \in K$ is a root of a monic polynomial with coefficients in $\mathcal{O}_F$. Prove that α is an algebraic integer.

Proposition 2.1.19. *If K is a number field and $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Z}$.*

Proof. By Corollary 2.1.9 we know C_α has integer coefficients and therefore by Proposition 1.7.3 we get the result.

□

Warning 2.1.20. Note that if α is an algebraic integer then A_α need not have integer entries. It possible that in different bases the matrix A_α does not have integer entries. What is true is that in any basis the norm and trace will always be integers as the corollary shows.

Warning 2.1.21. The converse is not true. For example $\frac{\sqrt{1+\sqrt{17}}}{2}$ has integer norm and trace, but it is not an algebraic integer.

Proposition 2.1.22. *Let α be an algebraic integer and $K = \mathbb{Q}(\alpha)$, then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$.*

Proof. Since α is an algebraic integer and by definition it is contained in K, we have $\alpha \in \mathcal{O}_K$, from which the result follows by Definition 2.1.13. □

Warning 2.1.23. If $K = \mathbb{Q}(\alpha)$ is a number field, then is it not always the case that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ as we can see from Theorem 2.1.11. You might ask if its possible to always find some algebraic integer α' such that $\mathcal{O}_K = \mathbb{Z}[\alpha']$ but this is also not true. There are rings of integers that are not generated by a single element. For example, if α is a root of $x^3 + x^2 - 2x - 8$, then one can show that if $K = \mathbb{Q}(\alpha)$ then $\mathcal{O}_K$ is never of the form $\mathbb{Z}[\alpha']$ for any algebraic integer α'.

So you may ask, why do we care about $\mathcal{O}_K$ instead of $\mathbb{Z}[\alpha]$? we'll it turns out $\mathcal{O}_K$ is a better invariant of K as we will see later.

Proposition 2.1.24. *Let K be a number field and let R be a subring of $\mathcal{O}_K$ which generates K as a field (i.e. $Frac(R) = K$). If R has unique factorization, then $R = \mathcal{O}_K$.*

Proof. We know that $R \subset \mathcal{O}_K$, we will show the opposite inclusion. Let $\alpha \in \mathcal{O}_K$. Then since K is the field of fractions of R we can find $\delta, \gamma \in R$ such that $\alpha = \frac{\gamma}{\delta}$, with δ, γ sharing no common factors other than a unit.

Now, since α is an algebraic integer, we can find some monic polynomial such that

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

If we now multiply through by δ^n we get

$$\gamma^n + a_{n-1}\gamma^{n-1}\delta + \cdots + a_0\delta^n = 0.$$

Since R is assumed to have unique factorization, we see that if ϖ is an irreducible factor of δ, then ϖ is an irreducible factor of γ^n and thus is a factor of γ. But we assumed that δ, γ shared no common factors other than units. So δ has no irreducible factors and is therefore a unit. So $\mathcal{O}_K \subset R$, giving the result. □

So, lets try to find a basis for $\mathcal{O}_K$.

Definition 2.1.25. Let K be a number field and let $\{b_1, \ldots, b_n\}$ be a basis for $K/\mathbb{Q}$. We call this an integral basis if $\mathcal{O}_K = \mathbb{Z}[b_1, \ldots, b_n] = \{x_1 b_1 + \cdots x_n b_n \mid x_i \in \mathbb{Z}\}$ as an additive group. In practice, the set $\{b_i\}$ will be some thing like $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ in which case, as rings, we have $\mathbb{Z}[\alpha] = \mathbb{Z}[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$

Ok, so we know what we are looking for, so how are we going to make such a basis. For this we will study the discriminant.

2.2 Discriminants

Definition 2.2.1. Let K be a number field and let $B = \{b_1, \ldots, b_n\}$ be a set of elements in K. The discriminant of B is defined as

$$\Delta(B) = \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(b_1 b_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(b_1 b_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(b_n b_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(b_n b_n) \end{pmatrix}.$$

If needed we will denote the matrix

$$\begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(b_1 b_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(b_1 b_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(b_n b_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(b_n b_n) \end{pmatrix}$$

by T_B.

Example 2.2.2. Let $K = \mathbb{Q}(\sqrt{d})$ with d square-free. Then lets take $B = \{1, \sqrt{d}\}$ which is our basis for K. Then we have

$$\Delta(B) = \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d}) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d}) & \mathrm{Tr}_{K/\mathbb{Q}}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

Proposition 2.2.3. *Let K be a number field and let $B = \{b_1, \ldots, b_n\}$ be a set of elements in K. Then $\Delta(B) \neq 0$ if and only if the elements in B are linearly independent.*

Proof. First recall from linear algebra, that if we have a finite dimensional vector space V with a non-degenerate bilinear form $\langle , \rangle$ on V, then $\{v_1, \ldots, v_n\}$ a basis of V if and only if

$$\det \begin{pmatrix} \langle v_1, v_1 \rangle & \cdots & \langle v_1, v_n \rangle \\ \vdots & & \vdots \\ \langle v_n, v_1 \rangle & \cdots & \langle v_n, v_n \rangle \end{pmatrix} \neq 0.$$

(This matrix appearing here is called the matrix associated to the pairing $\langle , \rangle$ with respect to our chosen basis).

Now, by Proposition 1.7.8 we know that the trace pairing is perfect, which in particular means it is non-degenerate. Moreover, $\Delta(B)$ is exactly the determinant of the matrix associated to the trace pairing. So, we see that B consists on linearly independent vectors if and only if $\Delta(B) \neq 0$. □

So this is a good way to check if a set of elements are a basis for $K/\mathbb{Q}$. Now, lets see how $\Delta(B)$ is related to $\Delta(B')$ for B, B' two different bases for $K/\mathbb{Q}$.

Proposition 2.2.4. *Let K be a number field and B, B' bases for $K/\mathbb{Q}$. If P denotes the change of basis matrix, then*

$$\Delta(B) = \det(P)^2 \Delta(B').$$

Proof. Let $T_B = (\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j))_{i,j}$ be the matrix associated to the trace pairing with respect to B. Then, it is a basic result in linear algebra that if you have the matrix associated to a bilinear pairing and change the basis, then the matrix gets conjugated by the change of basis matrix. This means that $T_B = P^t T_{B'} P$, (where $()^t$ denotes transpose). Now, taking determinants we get $\Delta(B) = \det(T_B) = \det(P^t T_{B'} P) = \det(P^t)\det(T_{B'})\det(P)$ which gives the result once you remember that $\det(P^t) = \det(P)$. □

Now, by the Primitive element theorem 1.5.11 we know that for a number field we can always find some α such that $K = \mathbb{Q}(\alpha)$ and in this case $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $K/\mathbb{Q}$ where $n = [K : \mathbb{Q}]$. But as we mentioned above, we cant do this for rings of integers. But, using the discriminant we can check if we have a basis for our ring of integers.

First note that:

Proposition 2.2.5. *Let K be a number field and $B = \{b_1, \ldots, b_n\}$ be elements in $\mathcal{O}_K$, then $\Delta(B) \in \mathbb{Z}$.*

Proof. If $b_i b_k$ is an algebraic integer, then $\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j) \in \mathbb{Z}$. Therefore the matrix T_B has integers coefficients, and therefore the determinant is a integer. □

Warning 2.2.6. Just because we take a basis consisting of algebraic integers, it doesn't mean that it is an integral basis. To find an integral basis we need to be a bit more careful.

Lemma 2.2.7. *Let K be a number field and $B = \{b_1, \ldots, b_n\}$ be a basis for $K/\mathbb{Q}$ consisting of algebraic integers. If B is not an integral basis then there exists an algebraic integer of the form*

$$\alpha = \frac{x_1 b_1 + \cdots + x_n b_n}{p}$$

where p is a prime and $x_i \in \{0, \dots, p-1\}$ with not all x_i zero. Moreover, if $x_i \neq 0$ and we let B' be the basis obtained by replacing b_i with α, then

$$\Delta(B') = \frac{x_i^2}{p^2}\Delta(B).$$

In particular $p^2 \mid \Delta(B)$.

Proof. If B is not an integral basis then we can find some element $\phi \in \mathcal{O}_K$ such that

$$\phi = y_1 b_1 + \dots y_n b_n$$

with not all the y_i in $\mathbb{Z}$. So, let N be the least common multiple of the denominators of the y_i (meaning $Ny_i \in \mathbb{Z}$ for all i). Now, let p be a prime factor of N. If we now consider $(N/p)\phi$ then all of the coefficients of b_i are in $\frac{1}{p}\mathbb{Z}$ (so they have denominator 1 or p.) and at least one of them has denominator p (since not all the y_i where in $\mathbb{Z}$). So by relabelling, wlog we can assume

$$\phi = y_1 b_1 + \dots y_n b_n$$

with $y_i \in \frac{1}{p}\mathbb{Z}$

Now look at

$$\psi := \lfloor y_1 \rfloor b_1 + \dots + \lfloor y_n \rfloor b_n$$

(here $\lfloor x \rfloor$ denotes the integer part of x). The both ψ and ϕ are algebraic integers (as the b_i are algebraic integers). Therefore, so is $\theta = \phi - \psi$. By construction, θ has coefficients of the for $\frac{x_i}{p} := y_i - \lfloor y_i \rfloor$ where $x_i \in \{0, \dots, p-1\}$ and not all the x_i are zero (since, again, not all the y_i were in $\mathbb{Z}$). This gives the first part of the lemma.

Now, assume $x_i \neq 0$, then let us replace $b_i \in B$ with θ to get a new basis B' which again consists of algebraic integers. Next, we note that the change of basis matrix from B to B' is

$$\begin{pmatrix} 1 & 0 & \cdots & \frac{x_1}{p} & \cdots & 0 \\ 0 & 1 & \cdots & \frac{x_2}{p} & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{x_n}{p} & \cdots & 1 \end{pmatrix}$$

(here the column of x_j/p's is in the i-th column).

This matrix has determinant $\frac{x_i}{p}$. Therefore, by Proposition 2.2.4 we see that $\Delta(B') = \frac{x_i^2}{p^2}\Delta(B)$. But both $\Delta(B), \Delta(B')$ are in $\mathbb{Z}$ by Proposition 2.2.5, therefore $p^2 \mid \Delta(B)$ giving the result. □

Corollary 2.2.8. *There exists a (finite) integral basis in K.*

Proof. The fact that it is finite follows from K being a finite extension of $\mathbb{Q}$. Let B be a basis consisting of algebraic integers, now by repeatedly applying

Lemma 2.2.7, we can obtain B such that $\mid \Delta(B) \mid$ is as small as possible. This must now be an integral basis, otherwise Lemma 2.2.7 would allow us to find a new basis B' with $|\Delta(B')| < |\Delta(B)|$ contradicting our choice of B. □

From this we also get:

Corollary 2.2.9. *If B is a basis consisting of integral elements and $\Delta(B)$ is square-free, then B is an integral basis.*

Proof. This follows at once from Lemma 2.2.7. □

Warning 2.2.10. Note that the converse is not true! For example if $K = \mathbb{Q}(\sqrt{-1})$ then $B = \{1, \sqrt{-1}\}$ is an integral basis, but $\Delta(B) = -4$ which is not square-free.

Remark 2.2.11. Note that this also gives us an algorithm for finding an integral basis as follows:

1. Pick B a basis consisting of algebraic integers and calculate $\Delta(B)$.
2. For each prime p such that $p^2 \mid \Delta(B)$ we can use Lemma 2.2.7 to get a new basis B' with smaller discriminant.
3. Now, repeat step one.

Example 2.2.12. Let $K = \mathbb{Q}(\sqrt{5})$ and take $B = \{1, \sqrt{5}\}$. Then we have $\Delta(B) = 2^2 \cdot 5$. So, if we apply Lemma 2.2.7 we get a new basis $B' = \{1, \frac{1+\sqrt{5}}{2}\}$ which has discriminant 5, which is square-free, and therefore is a basis of $\mathcal{O}_K$.

Proposition 2.2.13. *Let B, B' be two integral bases of a number field K. Then $\Delta(B) = \Delta(B')$.*

Proof. In this case the change of basis matrix from B to B' is an invertible matrix with integer coefficients, so its determinant is ± 1. Using Proposition 2.2.4, we see that a change of basis matrix won't alter the discriminant, since the factor of the determinant squared is what appears.

□

Definition 2.2.14. Let K be a number field, and let B be an integral basis. Then we define the discriminant of K as $\Delta(B)$. Note that by Proposition 2.2.13, this definition does not depend on the choice of integral basis. So we will sometimes denote it simply by $\Delta(\mathcal{O}_K)$.

2.2.15 Formulae for calculating discriminants

Let us now look at some alternative ways for calculating discriminants.

Proposition 2.2.16. *Let K be a number field with basis $B = \{b_1, \dots, b_n\}$ and let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Now let M be the matrix*

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_n) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \cdots & \sigma_n(b_n) \end{pmatrix}.$$

Then

$$\Delta(B) = \det(M)^2.$$

Proof. By Proposition 1.7.6 we know that $\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j) = \sum_k \sigma_k(b_i)\sigma_k(b_j)$ which is the same as the (i, j) entry of $M^t M$. Therefore

$$\det(T_B) = \det(M^t M) = \det(M)^2.$$

□

Now, by the Primitive element theorem 1.5.11, for any number field K we can find some α such that $K = \mathbb{Q}(\alpha)$ and thus $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $K/\mathbb{Q}$ where $n = [K : \mathbb{Q}]$. In this case the discriminant is given by:

Proposition 2.2.17. *Let K be a number field and $B = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for some $\alpha \in K$. Then*

$$\Delta(B) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

where σ_i are the embeddings of K into $\mathbb{C}$.

Proof. First we recall a classical linear algebra result relating to the Vandermonde matrix, which states that

$$\det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & & & \vdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{i<j} (x_i - x_j).$$

Combining this with Proposition 2.2.16 gives the result. □

Lastly, we have probably the more useful formula for computing the discriminant in this case, but before we state it we need the following lemma.

Lemma 2.2.18. *Let f be a monic irreducible polynomial over a number field K and let α be one of its roots in $\mathbb{C}$. Then*

$$f'(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta),$$

where the product is over the roots of f different from α.

Proof. We first write $f(x) = (x-\alpha)g(x)$ which we can do (over $\mathbb{C}$) as α is a root of f, where now $g(x) = \prod_{\beta \neq \alpha}(x-\beta)$. Differentiating we get

$$f'(x) = g(x) + (x-\alpha)g'(x).$$

If we now evaluate at α we get the result. □

Proposition 2.2.19. *Let $K = \mathbb{Q}(\alpha)$ be a number field with $n = [K : \mathbb{Q}]$ and let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then*

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m'_\alpha(\alpha))$$

where m'_α is the derivative of $m_\alpha(x)$ (which we recall denotes the minimal polynomial of α).

Proof. By Proposition 2.2.17 we have $\Delta(B) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ where $\alpha_k := \sigma_k(\alpha)$. Next, we note that the number of terms in this product is $1+2+\cdots+(n-1) = \frac{n(n-1)}{2}$. So if we write each term as $(\alpha_i - \alpha_j)^2 = -(\alpha_i - \alpha_j)(\alpha_j - \alpha_i)$ we get

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Now, by Lemma 2.2.18 and Proposition 1.7.6 we see that

$$N_{K/\mathbb{Q}}(m'_\alpha(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\alpha_i) = \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j),$$

which gives the result.

□

Example 2.2.20. Let α be a root of $m_\alpha(x) = x^8 - 2$ (which is irreducible by Eisensteins criterion 1.2.15). Therefore $\mathbb{Q}(\alpha)$ has degree 8 over $\mathbb{Q}$ and a basis is $B := \{1, \alpha, \ldots, \alpha^7\}$. From the above we then have

$$\begin{aligned}\Delta(B) = (-1)^{8\cdot 7/2} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(m'_\alpha(\alpha)) &= N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(8\alpha^7) \\ &= N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(8) N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^7) = 8^8 \cdot (-2)^7 = -2^{31}\end{aligned}$$

Here we use that $N_{K/\mathbb{Q}}(\alpha^7) = N_{K/\mathbb{Q}}(\alpha)^7$ and that $N_{K/\mathbb{Q}}(\alpha) = -2$.

Now, by Lemma 2.2.7, if we want to find an integral basis, we need to first pick a basis B of algebraic integers, and then check for which primes $p|\Delta(B)$ we have $p^2|\Delta(B)$. Its at these primes where we might need to modify our basis candidate B.

In order to make this simpler, here is a simple trick.

Lemma 2.2.21. *Let $K = \mathbb{Q}(\alpha)$ and α be an algebraic integer such that m_α satisfies Eisensteins Criterion 1.2.15 for a prime p. Then none of the elements*

$$\phi = \frac{1}{p}(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1})$$

is an algebraic integer, where $n = \deg(m_\alpha)$ and $x_i \in \{0, \ldots, p-1\}$.

Proof. We will only prove the case when m_α is Eisenstein, since the proof of the more general case is identical.

Suppose for contradiction that $\phi \in \mathcal{O}_K$ and let x_d be the first non-zero coefficient, so

$$\phi = \frac{1}{p}(x_d\alpha^d + x_{d+1}\alpha^{d+1} + \cdots + x_{n-1}\alpha^{n-1}) \in \mathcal{O}_K.$$

Now, rewrite this as $\phi = \frac{1}{p}(x_d\alpha^d + \alpha^{d+1}\beta)$ for some $\beta \in \mathcal{O}_K$. Next, multiply through by α^{n-1-d}, then we have

$$\frac{x_d\alpha^{n-1}}{p} + \frac{\alpha^n\beta}{p} \in \mathcal{O}_K.$$

Now, since m_α satisfies Eisenstein at p, we see that $\alpha^n = pf(\alpha)$ for some $f \in \mathbb{Z}[x]$ and therefore the above gives us that

$$\frac{x_d\alpha^{n-1}}{p} + \beta f(\alpha) \in \mathcal{O}_K.$$

and thus

$$\frac{x_d\alpha^{n-1}}{p} \in \mathcal{O}_K.$$

Lets now calculate the norm of this:

$$N_{K/\mathbb{Q}}\left(\frac{x_d\alpha^{n-1}}{p}\right) = \frac{x_d^n N_{K/\mathbb{Q}}(\alpha)^{n-1}}{p^n}.$$

By Eisenstein the constant coefficient of m_α is divisible by p but not p^2, so since the constant coefficient of m_α is $N_{K/\mathbb{Q}}(\alpha)$ we see that $N_{K/\mathbb{Q}}(\alpha) = pa$ where $p \nmid a$. Therefore we have

$$N_{K/\mathbb{Q}}\left(\frac{x_d\alpha^{n-1}}{p}\right) = \frac{x_d^n p^{n-1} a^{n-1}}{p^n} = \frac{x_d^n a^{n-1}}{p}.$$

But this cant be in $\mathbb{Z}$ since p doesn't divide x_d or a, and this gives us a contradiction since Proposition 2.1.19 says that the norm of an algebraic integer must be an integer. So ϕ couldn't have been an algebraic integer. □

How do we use this? well let me show you one use.

Example 2.2.22. Let α be a root of $x^8 - 2$. Then as we saw in Example 2.2.20 we know that $B = \{1, \alpha, \ldots, \alpha^7\}$ has discriminant -2^{31}. So the we only need to check at $p = 2$. But m_α satisfies Eisensteins criterion 1.2.15 with $p = 2$, therefore the Lemma 2.2.21 tells us that in fact this must be an integral basis, since dividing by 2 wont ever give us new algebraic integers.

2.2.23 Discriminants of trinomials

Lemma 2.2.24. *Let α be an algebraic number with minimal polynomial m_α and let $\beta \in \mathbb{Q}(\alpha)$ be such that $\alpha = \frac{a}{b\beta + c}$ with $a, b, c \in \mathbb{Q}$ and $b \neq 0$. Then* $\deg(m_\alpha) = \deg(m_\beta)$.

Proof. Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ (just do double inclusion). Then since $\deg(m_\beta) = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(m_\alpha)$ (by Cor. 1.3.12) we get the result.

□

Theorem 2.2.25. *Let $K = \mathbb{Q}(\alpha)$ a number field with $m_\alpha(x) = x^n + ax + b$. Then*

$$\Delta(\{1, \alpha, \ldots, \alpha^{n-1}\}) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

Proof. From Proposition 2.2.19 we have

$$\Delta(\{1, \alpha, \ldots, \alpha^{n-1}\} = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m'_\alpha(\alpha))).$$

Now, let $\beta = m'_\alpha(\alpha)$, then we have

$$\beta = n\alpha^{n-1} + a = -(n-1)a - nb\alpha^{-1}.$$

Since $\alpha^n + a\alpha + b = 0$ implies $n\alpha^{n-1} = -na - nb\alpha^{-1}$. Which gives

$$\alpha = \frac{-nb}{\beta + (n-1)a}.$$

Now, using Lemma 2.2.24 we see that $n = \deg(m_\alpha) = \deg(m_\beta)$. Moreover, if we take $m_\alpha(x) = x^n + ax + b$, evaluate at $\frac{-nb}{\beta+(n-1)a}$ and clear denominators, we get that

$$(\beta + (n-1)a)^n - na(\beta + (n-1)a)^{n-1} + (-n)^n b^{n-1} = 0.$$

Therefore β is a root of

$$(x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-n)^n b^{n-1}$$

which is a monic polynomial of degree $n = \deg(m_\beta)$, therefore this is the minimal polynomial of β.

Now, by Proposition 1.6.6 or Corollary 1.6.8 we have $C_\beta = m_\beta$. Therefore by Proposition 1.7.3 we see that $(-1)^n$ times the constant coefficient of m_β is $N_{K/\mathbb{Q}}(\beta)$. Therefore we get

$$N_{K/\mathbb{Q}}(\beta) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

which gives the result.

□

Corollary 2.2.26. *Let $K = \mathbb{Q}(\alpha)$ be a number field with $m_\alpha(x) = x^3+ax+b$. Then*

$$\Delta(\{1, \alpha, \alpha^2\}) = -27b^2 - 4a^3.$$

Let $K = \mathbb{Q}(\alpha)$ a number field with $[K : \mathbb{Q}] = 3$. Then $m_\alpha(x) = x^3 + ax^2 + bx + c$ for $a, b, c \in \mathbb{Q}$. If we replace α with $\alpha' := \alpha + a/3$ then $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ but this has the effect of removing the x^2 term in the minimal polynomial, so after relabelling if necessary, we have $K = \mathbb{Q}(\alpha)$ with $m_\alpha(x) = x^3 + ax + b$. Therefore Corollary 2.2.26 gives us a quick way to find the discriminant of a cubic field.

Example 2.2.27. Let α be a root of $x^3 + x + 1$, and let $K = \mathbb{Q}(\alpha)$. Then $\Delta(\{1, \alpha, \alpha^2\}) = -31$ which is square-free and therefore by Corollary 2.2.9 $\{1, \alpha, \alpha^2\}$ is an integral basis and therefore $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Exercise 2.2.28. Using Theorem 2.2.25 show what if $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, then

$$\Delta(\mathcal{O}_K) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

2.3 Cyclotomic fields

One of the more interesting number fields are the ones we get by adjoining a root of unity to $\mathbb{Q}$. In other words $\mathbb{Q}(\zeta_n)$ where ζ_n is a root of $x^n - 1$. From now on, when we write ζ_n we mean a primitive n-root of unity, meaning n is the smallest non-zero integer such that $\zeta_n^n = 1$.

Lets look at the case $n = p$ for p some prime number. Then from Example 1.2.16 we know that $x^p - 1$ is not irreducible, but

$$\Phi_p(x) = 1 + x + \cdots + x^{p-1}$$

is minimal. So $m_{\zeta_p} = \Phi_p$.

More generally, here is a Lemma we will use without proof.

Lemma 2.3.1. *For n any integer, Φ_n is an irreducible polynomial of degree $\varphi(n)$ (where φ is Euler's Totient function).*

Theorem 2.3.2. *Let ζ_p be a p-th root of unity for p an odd prime, let $\lambda_p = 1 - \zeta_p$ and $K = \mathbb{Q}(\zeta_p)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$ moreover*

$$\Delta(\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}) = \Delta(\{1, \lambda_p, \ldots, \lambda_p^{p-2}\}) = (-1)^{\frac{(p-1)}{2}} p^{p-2}$$

Proof. First note $[K : \mathbb{Q}] = p - 1$.

Since $\zeta_p = 1 - \lambda_p$ we at once get $\mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$ (just do double inclusion). Next, let $\alpha_i = \sigma_i(\zeta_p)$ denote the conjugates of ζ_p, which is the same as the image of ζ_p under one of the embeddings $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$. Now by Proposition 2.2.17 we have

$$\begin{aligned}\Delta(\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}) = \prod_{i<j} (\alpha_i - \alpha_j)^2 &= \prod_{i<j} ((1 - \alpha_i) - (1 - \alpha_j))^2 \\ &= \Delta(\{1, \lambda_p, \ldots, \lambda_p^{p-2}\})\end{aligned}$$

Now, by Proposition 2.2.19, we have

$$\Delta(\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p))$$

Since p is odd $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Next, we see that

$$\Phi_p'(x) = \frac{px^{p-1}(x-1) - (x^p - 1)}{(x-1)^2}$$

therefore

$$\Phi_p'(\zeta_p) = -\frac{p\zeta_p^{p-1}}{\lambda_p}.$$

Lastly, note that $N_{K/\mathbb{Q}}(\zeta_p) = 1$, since this is the constant term in its minimal polynomial. Similarly, from the computation in Example 1.2.16, we see $N_{K/\mathbb{Q}}(\lambda_p) = p$. Putting this all together, we get

$$N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)) = \frac{N_{K/\mathbb{Q}}(p) N_{K\mathbb{Q}}(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(-\lambda_p)} = (-1)^{p-1} p^{p-2} = p^{p-2}$$

So the last thing we need to prove is that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. From the calculation we just did, the only prime dividing the discriminant is p, therefore Lemma 2.2.7 tells us the only prime we need to check is p. But from Lemma 2.2.21 we know that dividing by p wont give us any new integral elements, so this must be an integral basis which give the result.

□

Exercise 2.3.3. 1. Let p be a prime, k a positive integer and ζ_{p^k} be a p^k-th root of unity and let $\lambda_{p^k} = 1 - \zeta_{p^k}$. Show that

$$\mathbb{Z}[\zeta_{p^k}] = \mathbb{Z}[\lambda_{p^k}]$$

and

$$\Delta(\{1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\varphi(p^k)}\}) = \Delta(\{1, \lambda_{p^k}, \ldots, \lambda_{p^k}^{\varphi(p^k)}\}).$$

Here φ is the usual Euler totient function.

2. Show that $\Delta(\{1, \zeta_{p^k}, \ldots, \zeta_{p^k}^{\varphi(p^k)}\})$ divides $p^{k\varphi(p^k)}$.

3. Let p be a prime and $n = p^k$. Let $S = \{1 \leq x \leq n \mid p \nmid x\}$ (i.e the set of elements less than n which are not divisible by p). Show that

$$\prod_{r \in S}(1 - \zeta_{p^k}^r) = p$$

and from this deduce that $\lambda_{p^k}^{\varphi(p^k)}$ divides p in $\mathbb{Z}[\zeta_{p^k}]$. [Hint: Consider the polynomial

$$f(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$$

]

4. Using the above prove that if $K = \mathbb{Q}(\zeta_{p^k})$ then $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^k}] = \mathbb{Z}[\lambda_{p^k}]$.

If one works harder, one can show (but we wont prove this):

Theorem 2.3.4. *Let n be a positive integer and ζ_n a root of unity. If $K = \mathbb{Q}(\zeta_n)$ then*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n].$$

Exercise 2.3.5. Let n be a positive integer and let ζ_n be an n-th root of unity. Show that if k is coprime to n then

$$1 + \zeta_n + \cdots + \zeta_n^{k-1}$$

is a unity in $\mathbb{Z}[\zeta_n]$.

[Hint:Check that its inverse is $\frac{1-\zeta_n}{1-\zeta_n^k}$]

Exercise 2.3.6. Let p be a prime and $n = p^k$. Show that

$$p = u(1 - \zeta_n)^{\varphi(n)}$$

where $u \in \mathbb{Z}[\zeta_n]^\times$ (i.e. u is a unit).

Chapter 3

Factorization in rings of integers

We now move on to the study of primes and prime ideals in rings of integers.

3.1 Units

One of the things we would like to know is what are the units in $\mathcal{O}_K$ for K some number field.

Proposition 3.1.1. *Let K be a number field and let $\mathcal{O}_K^\times$ denote the group of units, then*

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$$

Proof. If α is a unit the $\alpha^{-1} \in \mathcal{O}_K$ and therefore $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\alpha)^{-1} = N_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = N_{K/\mathbb{Q}}(1) = 1$. So $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}^\times$ and is therefore ± 1.

Now, assume $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ and let σ_i be the embeddings of K into $\mathbb{C}$ with σ_1 the identity embedding. Then

$$\alpha \prod_{i=2}^{n} \sigma_i(\alpha) = \pm 1$$

which means $\alpha^{-1} = \pm \prod_{i=2}^{n} \sigma_i(\alpha)$ but each $\sigma_i(\alpha)$ is again an algebraic integer so $\alpha^{-1} \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$ (see Remark 2.1.7).

□

Example 3.1.2. Let us look at $K = \mathbb{Q}(\sqrt{2})$. In this case we have already seen that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Now, is $1 + \sqrt{2}$ a unit? Well

$$N_{K/\mathbb{Q}}(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = -1$$

So yes it is.

Next we have a theorem which we will use but not prove.

Theorem 3.1.3 (Dirichlet's Unit theorem)**.** *Let K be a number field and let*

$$\mu_K = \{x \in K^\times \mid x^n = 1 \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

This is the set of roots of unity in K. Let r_1 denote the number of real embeddings of K and r_2 the number of complex conjugate pairs of embeddings. Then

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}$$

Corollary 3.1.4. *If $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{Z}_{>0}$ a square-free integer, then $\mathcal{O}_K^\times$ is μ_K.*

Proof. In this case $r_1 = 0$ and $r_2 = 1$ therefore Theorem 3.1.3 gives the result. □

Exercise 3.1.5. Show that if $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ a square-free integer, then

$$\mu_K = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & \text{if } d = -1 \\ \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\} & \text{if } d = -3 \\ \{\pm 1\} & \text{otherwise} \end{cases}$$

where $\zeta = e^{2\pi/6} = \frac{1+\sqrt{-3}}{2}$.

Corollary 3.1.6. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a positive square-free integer. Then*

$$\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}.$$

In this case there is a unique unit in $u \in \mathcal{O}_K^\times$ which generates $\mathcal{O}_K^\times/\{\pm 1\}$ and under the standard embedding we have $u \geq 1$. This unit u is called the fundamental unit.

Proof. Note that in this case $\mu_K = \{\pm 1\}$. So the structure of the group of units follows from Theorem 3.1.3. Now, $\mathcal{O}_K^\times/\{\pm 1\} \cong \mathbb{Z}$ so take any unit v mapping to a generator of $\mathcal{O}_K^\times/\{\pm 1\}$. Then one of $\{\pm v, \pm v^{-1}\}$ is in the set $(1, \infty)$. So let u be this unit. □

Proposition 3.1.7. *Let K be a number field and let $\alpha \in \mathcal{O}_K$. If $N_{K/\mathbb{Q}}(\alpha) = \pm p$ for p a prime number, then α is an irreducible element of $\mathcal{O}_K$.*

Proof. Let $\alpha = \beta\gamma$ we want to show that one of β, γ is a unit. Now taking norms we have

$$N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\gamma) = \pm p.$$

Therefore as p is prime we must have $N_{K/\mathbb{Q}}(\beta) = \pm 1$ or $N_{K/\mathbb{Q}}(\gamma) = \pm 1$. In either case we get the result. □

Remark 3.1.8. The converse is false. For example in $\mathbb{Z}[\sqrt{-1}]$ the element 3 is irreducible and has norm 9.

Proposition 3.1.9. *Let K be a number field and $\alpha \in \mathcal{O}_K$ be non-zero and not a unit. Then α can be written as a product of irreducible elements.*

Proof. We prove this by induction on $|N_{K/\mathbb{Q}}(\alpha)|$. If $N_{K/\mathbb{Q}}(\alpha) = 2$ then α is irreducible so we are done. Now assume it is true for all β with $|N_{K/\mathbb{Q}}(\beta)| < |N_{K/\mathbb{Q}}(\alpha)$. If α is irreducible then we are done, otherwise $\alpha = \beta\gamma$ with $|N_{K/\mathbb{Q}}(\beta)|, |N_{K/\mathbb{Q}}(\gamma)| < |N_{K/\mathbb{Q}}(\alpha)|$. Therefore both β and γ can be factored into irreducibles and thus so can α. □

Definition 3.1.10. We say a ring has unique factorization if whenever

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

for p_i, q_i irreducible elements, then $n = m$ and after possibly reordering we can find units u_i such that $p_i = u_i q_i$ for all i.

Example 3.1.11. The $\mathbb{Z}$ has unique factorization as does $\mathbb{Z}[\sqrt{-2}]$.

But this is not usually the case, for example $\mathbb{Z}[\sqrt{-10}]$ doesn't have unique factorization as $10 = 2 \cdot 5 = -\sqrt{-10}\sqrt{-10}$ all of which are irreducible as can be seen by taking norms: Note that $N_{K/\mathbb{Q}}(2) = 4, N_{K/\mathbb{Q}}(5) = 25, N_{K/\mathbb{Q}}(\sqrt{-10}) = 10$. Now, every element in $K = \mathbb{Q}(\sqrt{-10})$ has norm of the form $x^2 + 10y^2$ and this can never be $\pm 2, \pm 5$, so there can't be any irreducible elements dividing $2, 5, \sqrt{-10}$ therefore they are irreducible.

In order to fix this, we will later decompose things into prime ideals and work with this, but before this we need to understand ideals better.

3.2 Ideals in rings of integers

Let me recall some definition you may have seen in other courses.

Definition 3.2.1. Let R be a commutative ring. Then R is called *Noetherian* any of the following equivalent conditions holds:

1. Every ideal is finitely generated.
2. Every increasing chain of ideals $I_1 \subset I_2 \subset \dots$ is eventually constant.
3. Every non-empty set S of ideals contains a (not necessarily unique) maximal member.

Exercise 3.2.2. Check that these definitions are all equivalent.

Proposition 3.2.3. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is a Noetherian ring.*

Proof. We saw in Corollary 2.2.8 that $\mathcal{O}_K$ is finitely generated as an additive group. Now, any ideal $\mathfrak{a} \subset \mathcal{O}_K$ is an additive subgroup of the *abelian* group $\mathcal{O}_K$ and therefore is also finitely generated.[a] So $\mathcal{O}_K$ is Noetherian. □

Proposition 3.2.4. *Let K be a number field and $\mathfrak{a}$ a non-zero ideal in $\mathcal{O}_K$. Then $\mathfrak{a}$ contains some positive integer and moreover the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof. Let $\alpha \in \mathfrak{a}\backslash 0$ and $N = N_{K/\mathbb{Q}}(\alpha)$. Since $\alpha \neq 0$, then $N \neq 0$. Now, by Proposition 1.7.6 we see that $N = \alpha\beta$ where β is a product of conjugates of α so it is in $\overline{\mathbb{Z}}$. Moreover, $\beta \in \mathcal{O}_K$ since $\beta = N/\alpha \in K$ (recall $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$). But since $\mathfrak{a}$ is an ideal $N = \alpha\beta \in \mathfrak{a}$.

Now, lets use this to prove the quotient is finite. First note that since $N \in \mathfrak{a}$ then $(N) \subset \mathfrak{a}$ therefore $|\mathcal{O}_K/\mathfrak{a}| \leq |\mathcal{O}_K/(N)|$. Secondly, since $\mathcal{O}_K$ is finitely generated as an abelian group, by picking an integral basis we get an isomorphism (of additive abelian groups) $\mathcal{O}_K \cong \mathbb{Z}^n$ where $n = [K : \mathbb{Q}]$. Therefore $\mathcal{O}_K/(N) \cong (\mathbb{Z}/N\mathbb{Z})^n$ which is finite. Therefore so is $\mathcal{O}_K/\mathfrak{a}$. □

Lemma 3.2.5. *A finite integral domain is a field.*

Proof. Let R be a finite, non-trivial integral domain. Let $r \in R\backslash 0$. We need to show that r has an inverse. Here is the trick: consider the sequence $r, r^2, r^3, \ldots$. Since R is finite at some point we must have $r^n = r^m$ for some $m < n$. Then $r^m(r^{n-m} - 1) = 0$, but this is where being an integral domain comes in, since this means either $r^m = 0$ or $r^{n-m} - 1 = 0$. Since $r \neq 0$ and R is an integral domain $r^m \neq 0$. Therefore $r^{n-m} = 1$. This means $r^{-1} = r^{n-m-1}$ and therefore r has an inverse. □

Corollary 3.2.6. *Let K be a number field. Then every non-zero prime ideal in $\mathcal{O}_K$ is maximal.*

Proof. By Proposition 1.1.22 we know that if $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal then $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Now, by Proposition 3.2.4 $\mathcal{O}_K/\mathfrak{p}$ is finite. But by Lemma 3.2.5 this is then a field. Now, using Proposition 1.1.22 again, $\mathfrak{p}$ is maximal. □

Definition 3.2.7. Let R, A be rings with $A \subset R$ a subring and $x \in R$. We say x is integral over A if there exist $a_i \in A$ such that

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

for some n.

Let A' be the set of all elements of R that are integral over A. Then similarly to how we prove Corollary 2.1.16, A' is a ring which we call the integral closure of A in R.

[a] Be warned, its not true in general that a subgroup of a finitely generated group G is finitely generated. You really need G to be abelian for this to work.

Moreover, if R is an integral domain and we let

$$\mathrm{Frac}(R) := \{a/b | a, b \in R, b \neq 0\}$$

be its fields of fractions (this can alternatively be defined as smallest field containing R), then we say R is integrally closed, if it is integrally closed in its field of fractions.

3.3 Dedekind domains

Next we will study properties of rings of integers. It turns out they are of a very special type, called Dedekind domains.

Definition 3.3.1. A Dedekind domain is an integral domain R such that:

1. R is Noetherian.
2. Every non-zero prime ideal is maximal.
3. R is integrally closed.

Theorem 3.3.2. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. By Proposition 3.2.3 we get (1) and by Corollary 3.2.6 we get (2).

So we only need to prove $\mathcal{O}_K$ is integrally closed.

Let $\gamma = \alpha/\beta \in K$ satisfy a monic polynomial with coefficients in $\mathcal{O}_K$, then I claim that it is in fact an algebraic integer and therefore it is in $K \cap \overline{\mathbb{Z}} = \mathcal{O}_K$. (Note $\mathrm{Frac}(\mathcal{O}_K) = K$.)

The claim is Exercise 2.1.18.

□

Dedekind domains are great. Lets look at some of their properties.

Lemma 3.3.3. *Let R be a Dedekind domain. Then every ideal contains a product of prime ideals.*

Proof. Assume for contradiction this is not the case. Let S denote the set of all ideals that do not contain a product of prime ideals. Then, since R is Noetherian, by Definition 3.2.1(3), S must contain a maximal element $\mathfrak{m}$ (not to be confused with maximal ideal, here maximal means with respect to the property of not containing a product of prime ideals). Now $\mathfrak{m}$ cannot be prime (otherwise $\mathfrak{m} \subseteq \mathfrak{m}$ gives a contradiction). Therefore we can find $r, s \in R \backslash \mathfrak{m}$ such that $rs \in \mathfrak{m}$. Now the ideals $(r) + \mathfrak{m}$ and $(s) + \mathfrak{m}$ are both larger then $\mathfrak{m}$ so must contain a product of prime ideals, but then so does their product $((r) + \mathfrak{m})((s) + \mathfrak{m})$. This product is contained in $\mathfrak{m}$ (since $rs \in \mathfrak{m}$) so we have a contradiction. □

Lemma 3.3.4. *Let R be a Dedekind domain with field of fractions K and $\mathfrak{a}$ a proper ideal . Then there is an element $x \in K \backslash R$ such that $x\mathfrak{a} \subset R$.*

Proof. Let $a \in \mathfrak{a}$ be any non-zero element. By Lemma 3.3.3 the ideal (a) contains a product of prime ideals. So lets take prime ideals $\mathfrak{p}_i$ such that $\prod_{i=1}^{m} \mathfrak{p}_i \subset (a)$ with m as small as possible. Now, since every proper ideal is contained in a maximal ideal $\mathfrak{p}$ (see Proposition 1.1.22), which is also a prime ideal (as maximal ideals are always prime). Therefore $\mathfrak{a} \subset \mathfrak{p}$, so $\prod_i \mathfrak{p}_i \subset \mathfrak{p}$.

Now $\mathfrak{p}$ must contain some $\mathfrak{p}_i$ since if not, we can take $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}$ then $\mathfrak{p}$ contains $\prod_i a_i$ but none of the a_i which contradicts $\mathfrak{p}$ being a prime ideal. So after possibly relabelling we have $\mathfrak{p}_1 \subset \mathfrak{p}$. But by Definition 3.3.1, in a Dedekind domain all prime ideals are maximal, so $\mathfrak{p} = \mathfrak{p}_1$.

Since m was taken as small as possible, (a) can't contain any smaller product of prime ideals, so we can find $b \in (\prod_{i=2}^{m} \mathfrak{p}_i) \backslash (a)$.

We claim that taking $x = \frac{b}{a}$ gives the result: First note $x \in K \backslash R$ since otherwise $\frac{b}{a} = c \in R$ therefore $b = ac \in (a)$ which contradicts our choice of b. Moreover, we claim that $x\mathfrak{a} \subset R$. To see this note that since $b\mathfrak{p} \subset \prod_i \mathfrak{p}_i \subset (a)$ we have $x\mathfrak{p} \subset R$ and therefore since $\mathfrak{a} \subset \mathfrak{p}$ we have $x\mathfrak{a} \subset x\mathfrak{p} \subset R$.

□

Theorem 3.3.5. *Let R be a Dedekind domain and $\mathfrak{a}$ an ideal in R. Then there is an ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal.*

Proof. Let $\alpha \in \mathfrak{a} \backslash 0$ and let

$$\mathfrak{b} = \{\beta \in R \mid \beta\mathfrak{a} \in (\alpha)\}.$$

This is again an ideal and it is non-zero since $\alpha \neq 0$. By definition we have

$$\mathfrak{ab} \subset (\alpha) \tag{\dagger}$$

so we need to show equality.

For this consider the set $\mathfrak{c} = \frac{1}{\alpha}\mathfrak{ab}$. This is a subset of R by (†) and is in fact an ideal. Now, if $\mathfrak{c} = R$ then $\mathfrak{ab} = (\alpha)$ and we are done. So assume for contradiction that $\mathfrak{c}$ is a proper ideal. Then by Lemma 3.3.4 we can find $x \in K \backslash R$ with K the fraction field of R and $x\mathfrak{c} \subset R$.

Next, we note that $\mathfrak{c}$ contains $\mathfrak{b}$ since $\alpha \in \mathfrak{a}$, therefore $x\mathfrak{b} \subset x\mathfrak{c} \subset R$. Moreover, since $x\mathfrak{c} = \frac{x}{\alpha}\mathfrak{ba} \subset R$ we have $x\mathfrak{ba} \subset (\alpha)$. Now, if we look back at the definition of $\mathfrak{b}$ we see that since $x\mathfrak{b} \subset R$ we have $x\mathfrak{b} \subset \mathfrak{b}$.

If we let $\beta_1, \ldots, \beta_n$ be a generating set for $\mathfrak{b}$, we can use $x\mathfrak{b} \subset \mathfrak{b}$ to think of multiplication by x on $\mathfrak{b}$ as a matrix A_x defined by

$$x(\beta_1, \ldots, \beta_n)^t = A_x(\beta_1, \ldots, \beta_n)^t.$$

A_x is a $n \times n$ matrix over R which has x as an eigenvalue. This means, x satisfies a monic polynomial with coefficients in R. But R is integrally closed,

so $x \in R$ which gives a contradiction as we took $x \in K \backslash R$. This completes the proof. □

Exercise 3.3.6. Show that if $\mathfrak{a}$ is an ideal in an integral domain R and $(\alpha)\mathfrak{a}$ is principal for $\alpha \in R \backslash 0$, then $\mathfrak{a}$ is principal.

Definition 3.3.7. Let R be a Dedekind domain and K its field of fractions. A *fractional ideal* is a subset $\mathfrak{a} \subset K$ such that

1. $\mathfrak{a}$ is an abelian group under addition.
2. $x\mathfrak{a} \subset \mathfrak{a}$ for every $x \in R$.
3. There exists some $x \in R$ such that $x\mathfrak{a} \subset R$.

Example 3.3.8. Let $q \in \mathbb{Q}$, then

$$(q) = \{nq \mid n \in \mathbb{Z}\}$$

is a fractional ideal. More generally, if R is an Dedekind domain K its field of fractions and $\alpha \subset K$. Then for any ideal $\mathfrak{a} \in R$, $\frac{1}{\alpha}\mathfrak{a}$ is a fractional ideal.

Warning 3.3.9. If $\mathfrak{a}$ is a fractional ideal and $x, y \in \mathfrak{a}$ then it is not necessarily true that $xy \in \mathfrak{a}$.

Definition 3.3.10. Let R be a Dedekind ring and K its field of fractions. For each $x \in K$ we call the fractional ideal

$$(x) = \{xy \mid y \in R\}$$

a *principal fractional ideal.*

Proposition 3.3.11. *Let R be a Dedekind domain and K its field of fractions. Then the set J_K of non-zero fractional ideals forms a group under multiplication with $(1) = R$ being the identity.*

Proof. As we had before, if $\mathfrak{a}, \mathfrak{b}$ are fractional ideals, then $\mathfrak{ab}$ is defined as the fractional ideal generated by products of elements in $\mathfrak{a}$ and $\mathfrak{b}$. This is clearly associative, so we only need to check the existence of inverses.

If $\mathfrak{a}$ is a proper ideal of R, then by Theorem 3.3.5 we can find an ideal $\mathfrak{b}$ such that $\mathfrak{ab} = (\alpha)$ for some α. Then setting $\mathfrak{a}^{-1} = \frac{1}{\alpha}\mathfrak{b}$ gives an inverse to $\mathfrak{a}$. If $\mathfrak{a}$ is a fractional ideal, then we can find some $x \in R$ such that $x\mathfrak{a} \subset R$ is an ideal (not just a fractional ideal), call it $\mathfrak{c}$, then $\mathfrak{a}^{-1} = x\mathfrak{c}^{-1}$ is the inverse. □

Remark 3.3.12. It follows, that if $\mathfrak{a}$ is a fractional ideal in R, then

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subset R\}$$

where K is the field of fractions of R.

Corollary 3.3.13. *If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are non-zero ideals in a Dedekind domain and $\mathfrak{ab} = \mathfrak{ac}$ then $\mathfrak{b} = \mathfrak{c}$.*

Proof. Multiplying on the left by $\mathfrak{a}^{-1}$ gives the result. □

Corollary 3.3.14. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals in a Dedekind domain. Then $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$.*

Proof. If $\mathfrak{a} \mid \mathfrak{b}$ then by definition we have $\mathfrak{b} = \mathfrak{ca}$, which means $\mathfrak{b} \subset \mathfrak{a}$. Conversely, assume that $\mathfrak{b} \subset \mathfrak{a}$. Then by Theorem 3.3.5 we can find an ideal $\mathfrak{m}$ such that $\mathfrak{am} = (\alpha)$. Now, $\mathfrak{mb} \subset \mathfrak{am} = (\alpha)$ therefore $\mathfrak{c} = \frac{1}{\alpha}\mathfrak{mb}$ is again in R and moreover it is an ideal (since, for example it is the product of two fractional ideals). The result follows from then noting that $\mathfrak{ac} = \mathfrak{b}$. □

We can now use this as a fix to our problem of not being able to factor uniquely.

Theorem 3.3.15. *Let R be a Dedekind domain, then every ideal $\mathfrak{a}$ can be written uniquely as a product of prime ideals, i.e,*

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n,$$

with $\mathfrak{p}_i$ prime ideals (not necessarily distinct).

Proof. Lets begin by showing that every ideal can be written as a product of prime ideal. Assume for contradiction that this is not the case. Then the set of proper ideals which are not a product of prime ideals, must have a maximal element by Definition 3.2.1 (3). Let $\mathfrak{b}$ be this maximal element. Then $\mathfrak{b}$ must be contained in some maximal ideal $\mathfrak{p}$ of R (which we recall is also prime). Then by Corollary 3.3.14 we have $\mathfrak{b} = \mathfrak{pc}$.

This implies $\mathfrak{b} \subset \mathfrak{c}$ and this must be a strict containment as otherwise if $\mathfrak{c} = \mathfrak{b}$ then $\mathfrak{b} = \mathfrak{bp}$ which by Corollary 3.3.13 would mean $\mathfrak{p} = R$, which cannot happen as $\mathfrak{p}$ is a proper ideal.

Now, since $\mathfrak{c}$ is larger than $\mathfrak{b}$ we must have $\mathfrak{c}$ being a product of prime ideals. So then $\mathfrak{pc} = \mathfrak{b}$ is also a product of prime ideals contradicting our assumption.

Lets now prove that the representation as a product of prime ideals is unique. Suppose we have

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_m$$

with $\mathfrak{p}_i, \mathfrak{q}_i$ not necessarily distinct prime ideals. Then $\mathfrak{q}_1 \dots \mathfrak{q}_m \subset \mathfrak{p}_1$, which means $\mathfrak{p}_1$ contains some $\mathfrak{q}_i$ (see the proof of Lemma 3.3.4 to see why this is true). By relabelling the $\mathfrak{q}_i$ we can assume $\mathfrak{q}_1 \subset \mathfrak{p}_1$. But since all prime ideals in a Dedekind ring are maximal we must have $\mathfrak{q}_1 = \mathfrak{p}_1$. So we can cancel this from each side of the equality to get

$$\mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_2 \dots \mathfrak{q}_m.$$

Continuing like this we get $n = m$ and after relabelling $\mathfrak{p}_i = \mathfrak{q}_i$, which completes the proof.

□

Notation 3.3.16. Since ideal multiplication commutes, we usually write the factorization of a an ideal as

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_1}\dots\mathfrak{p}_r^{e_r}$$

with $\mathfrak{p}_i$ distinct prime ideals.

Corollary 3.3.17. *Let K be a number field. Then every ideal in $\mathcal{O}_K$ can factored uniquely into a product of prime ideals.*

Proof. We know $\mathcal{O}_K$ is a Dedekind domain, so the result follows. □

Definition 3.3.18. Let R be a Dedekind domain and let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then we define the greatest common divisor gcd and least common multiple lcm as follows: Let $\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i}$ and $\mathfrak{b} = \prod_i \mathfrak{p}_i^{m_i}$ then

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\min(n_i, m_i)} \qquad \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod_i \mathfrak{p}_i^{\max(n_i, m_i)}.$$

Here the $\mathfrak{p}_i$ are all different.

Proposition 3.3.19. *If R is a Dedekind domain and $\mathfrak{a}, \mathfrak{b}$ are ideals. Then*

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$$

and

$$\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$$

Proof. Corollary 3.3.14 tells us that division turns into containment for ideals, so the greatest common divisor of $\mathfrak{a}, \mathfrak{b}$ is the smallest ideal containing both $\mathfrak{a}, \mathfrak{b}$ which by definition is $\mathfrak{a} + \mathfrak{b}$.

Similarly, the least common multiple is the largest ideal contained in both of them, which by definition is $\mathfrak{a} \cap \mathfrak{b}$. □

Exercise 3.3.20. Show that $\gcd(\mathfrak{a}, \mathfrak{b}) \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$.

Theorem 3.3.21 (Chinese remainder theorem)**.** *Let R be a commutative ring and let $\mathfrak{a}, \mathfrak{b}$ be coprime ideals (i.e., $\mathfrak{a} + \mathfrak{b} = (1)$) then*

$$R/\mathfrak{a}\mathfrak{b} \cong R/\mathfrak{a} \times R/\mathfrak{b}$$

Proof. Consider the ring homomorphism

$$\phi : R \to R/\mathfrak{a} \times R/\mathfrak{b}$$

given by $\phi(x) = (x \pmod{\mathfrak{a}}, x \pmod{\mathfrak{b}})$. Then the kernel is given by $\mathfrak{a} \cap \mathfrak{b}$.

Now, since $\mathfrak{a} + \mathfrak{b} = (1)$ then

$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a}) + (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{b}) \subset \mathfrak{ab}.$$

Moreover, its easy to see $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, therefore $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. So we have an injective ring homomorphism

$$\phi' : R/\mathfrak{ab} = R/(\mathfrak{a} \cap \mathfrak{b}) \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}.$$

It remains to check it is surjective. Write $1 = a + b$ for $a \in \mathfrak{a}, b \in \mathfrak{b}$, then for any $(r, s) \in R^2$ the element $x = as + br \in R$ is such that $x \equiv r \pmod{\mathfrak{a}}$ and $x \equiv s \pmod{\mathfrak{b}}$ which gives us subjectivity. □

Remark 3.3.22. By induction one can extend this to the case where we have several pairwise coprime ideals.

Theorem 3.3.23. *Let R be a Dedekind domain and let $\mathfrak{a}$ be an ideal. Then for any $\alpha \in \mathfrak{a}$ with α non-zero we can find $\beta \in \mathfrak{a}$ such that $\mathfrak{a} = (\alpha, \beta)$.*

Proof. We will find a β such that $\mathfrak{a} = \gcd((\alpha), (\beta)) = (\alpha) + (\beta) = (\alpha, \beta)$.

Let

$$\mathfrak{a} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$$

with $\mathfrak{p}_i$ distinct prime ideals. Then since $(\alpha) \subset \mathfrak{a}$ we have $(\alpha) \subset \mathfrak{p}_i^{n_i}$ for all i, in other words α is divisible by the $\mathfrak{p}_i^{n_i}$. Now, let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be any other prime ideals dividing (α) (if any exist). So we have

$$(\alpha) = \prod_i \mathfrak{p}_i^{n_i} \times \prod_j \mathfrak{q}_j.$$

We construct β as follows. Take $\beta_i \in \mathfrak{p}_i^{n_i} \backslash \mathfrak{p}_i^{n_i+1}$ and then use the Chinese remainder theorem 3.3.21 to find $\beta \in R$ such that $\beta \equiv \beta_i \pmod{\mathfrak{p}_i^{n_i+1}}$ for $i \in \{1, \ldots, r\}$ and $\beta \equiv 1 \pmod{\mathfrak{q}_j}$ for $j \in \{1, \ldots, s\}$. Note that we can do this, and the $\mathfrak{p}_i, \mathfrak{q}_j$ are all pairwise distinct so $\mathfrak{q}_j + \mathfrak{p}_i^{n_i} = (1)$ (as $\mathfrak{q}_j$ is maximal) for all i, j and moreover, $\mathfrak{p}_i^{n_i} + \mathfrak{p}_j^{n_j} = \gcd(\mathfrak{p}_i^{n_i}, \mathfrak{p}_j^{n_j})$ which by Definition 3.3.18 is just (1).

So now, Definition 3.3.18 gives us $\gcd((\alpha), (\beta)) = \prod_i \mathfrak{p}_i^{n_i} = \mathfrak{a}$ and therefore $\beta \in \mathfrak{a}$ which finishes the proof.

□

Theorem 3.3.24. *A Dedekind domain is a UFD if and only if it is a PID.*

Proof. If R is a Dedekind domain that is a PID, then by Proposition 1.2.6 it is a UFD.

Now, let R be a UFD and assume for contradiction it is not a PID. Then by Theorem 3.3.15 there must exist at least one non-principal prime

ideal, call it $\mathfrak{p}$. Now, let S be the set of ideals $\mathfrak{a}$ such that $\mathfrak{ap}$ is principal. By Theorem 3.3.5 S is non-empty, so we can do the usual trick and find a maximal element, $\mathfrak{m}$. Let $\mathfrak{mp} = (\alpha)$, we claim α must be irreducible. Assuming this for the moment, if we take $a \in \mathfrak{p} \backslash (\alpha)$ and $b \in \mathfrak{m} \backslash (\alpha)$ (which we can do in the first case as $\mathfrak{p}$ is not principal and in the second by Exercise 3.3.6) then $ab \in (\alpha)$ but $\alpha \mid ab$ but $\alpha \nmid a$ and $\alpha \nmid b$ which cannot happen in a UFD.

So it remains to prove the claim that α is irreducible. For this we note that if $\alpha = \beta\gamma$ then one of (β) or (γ) would be of the form $\mathfrak{pb}$ for some $\mathfrak{b}$ dividing $\mathfrak{m}$, but $\mathfrak{m}$ is maximal so $\mathfrak{b} = \mathfrak{m}$ and therefore one of β, γ is a unit. $\square$

3.4 Norms of ideals

Definition 3.4.1. Let K be a number field and $\mathfrak{a} \subset \mathcal{O}_K$ an ideal. We define the norm of $\mathfrak{a}$ to be

$$N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|.$$

Why does this deserve to be called norm? Well lets justify this.

Proposition 3.4.2. *Let K be a number field and let $\mathfrak{a}, \mathfrak{b}$ be ideals in $\mathcal{O}_K$, then*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Proof. By factoring each of $\mathfrak{a}, \mathfrak{b}$ into prime ideals, it suffices to prove that $N(\mathfrak{pb}) = N(\mathfrak{p})N(\mathfrak{b})$ where $\mathfrak{p}$ is a prime ideal and $\mathfrak{b}$ is any proper ideal.

Now, by group theory $\mathfrak{b}/\mathfrak{pb}$ is a subgroup of $\mathcal{O}_K/\mathfrak{pb}$ and the quotient is $\mathcal{O}_K/\mathfrak{b}$. This means

$$|\mathcal{O}_K/\mathfrak{pb}| = |\mathcal{O}_K/\mathfrak{b}||\mathfrak{b}/\mathfrak{pb}|.$$

So we need to show $|\mathfrak{b}/\mathfrak{pb}| = |\mathcal{O}_K/\mathfrak{p}|$.

Since $\mathfrak{p} \neq \mathcal{O}_K$ and (fractional) ideals form a group we have $\mathfrak{pb} \neq \mathfrak{b}$ (otherwise we could multiply through by $\mathfrak{b}^{-1}$ giving a contradiction), so let $x \in \mathfrak{b} \backslash \mathfrak{bp}$. Let us consider the map

$$\mathcal{O}_K \longrightarrow \mathfrak{b}/\mathfrak{pb}$$

given by $a \mapsto ax + \mathfrak{pb}$. The kernel of this map contains $\mathfrak{p}$ and the map is non-zero by our choice of x, so the kernel is an ideal containing $\mathfrak{p}$. But $\mathfrak{p}$ is maximal, so the kernel must be $\mathfrak{p}$. Therefore we have an injective map

$$\mathcal{O}_K/\mathfrak{p} \longrightarrow \mathfrak{b}/\mathfrak{pb}.$$

Now, to see that this map is also surjective we just note that by unique factorization, there cannot be any ideals strictly between $\mathfrak{b}$ and $\mathfrak{pb}$. Since otherwise, we would have $\mathfrak{bp} \subset \mathfrak{c} \subset \mathfrak{b}$ which means $\mathfrak{b} \mid \mathfrak{c}$ and $\mathfrak{b} \mid \mathfrak{bp}$ so by uniqueness of factorization we would have either $\mathfrak{c} = \mathfrak{b}$ or $\mathfrak{c} = \mathfrak{pb}$.

Therefore $\mathfrak{b} = (x) + \mathfrak{p}\mathfrak{b}$ giving surjectivity.

□

Lemma 3.4.3. *Let K be a number field and $\mathfrak{a} \subset \mathfrak{b} \subset \mathcal{O}_K$ non-zero ideals. Then $\mathfrak{a} = \mathfrak{b}$ if and only if $N(\mathfrak{a}) = N(\mathfrak{b})$*

Proof. Clearly, if $\mathfrak{a} = \mathfrak{b}$ they have the same norm. So lets check the other direction.

First note that since $\mathfrak{a} \subset \mathfrak{b} \subset \mathcal{O}_K$, the tower law (which works for groups) gives us that $[\mathcal{O}_K : \mathfrak{a}] = [\mathcal{O}_K : \mathfrak{b}][\mathfrak{b} : \mathfrak{a}]$. But $[\mathcal{O}_K : \mathfrak{a}] = N(\mathfrak{a}) = N(\mathfrak{b}) = [\mathcal{O}_K : \mathfrak{b}]$ therefore $[\mathfrak{b} : \mathfrak{a}] = 1$ giving the result.

□

Proposition 3.4.4. *Let K be a number field and $\mathfrak{a} \subset \mathcal{O}_K$ an ideal. If $N(\mathfrak{a})$ is a prime, then $\mathfrak{a}$ is a prime ideal. Conversely, if $\mathfrak{p}$ is a prime ideal, then $N(\mathfrak{p}) = p^f$ for some prime number p and $f \in \mathbb{Z}_{>0}$.*

Proof. If $\mathfrak{a}$ is not prime then $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ with $\mathfrak{p}$ a prime ideal and $\mathfrak{b} \neq (1)$. Then by Proposition 3.4.2 we have

$$N(\mathfrak{a}) = N(\mathfrak{p})N(\mathfrak{b})$$

which means $N(\mathfrak{a})$ could not have been prime, which is a contradiction.

For the converse we note that since $\mathfrak{p}$ is prime it is therefore maximal. Therefore $\mathcal{O}_K/\mathfrak{p}$ is a field, which we know is finite. Moreover, we know every finite field has size p^f for some prime p and natural number f, which gives the result. □

Proposition 3.4.5. *Let K be a number field. Let $\alpha \in \mathcal{O}_K \backslash 0$ and let (α) denote the ideal generated by α. Then*

$$|N_{K/\mathbb{Q}}(\alpha)| = |\mathcal{O}_K/(\alpha)|.$$

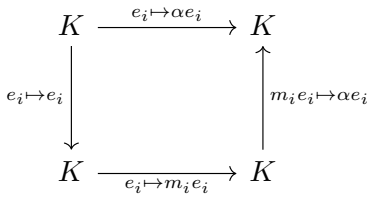
Proof. Let $e_1, \ldots, e_n$ be an integral basis of $\mathcal{O}_K$, then clearly $\alpha e_1, \ldots, \alpha e_n$ is an integral basis of (α). On the other hand, since $(\alpha) \subset \mathcal{O}_K \cong \mathbb{Z}^n$ we can make sure to choose the e_i such that there exist $m_i \in \mathbb{Z}$ such that $m_1 e_1, \ldots, m_n e_n$ is an integral basis of (α). Alternatively, this follows from the structure theorem for finitely generated abelian groups. Then

$$\mathcal{O}_K/(\alpha) \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

and therefore $N((\alpha)) = \prod_i |m_i|$.

Next we need to relate this number to $N_{K/\mathbb{Q}}(\alpha)$ in some way. For this, let us compare the three bases for K over $\mathbb{Q}$ that we have written down: $\{e_1, \ldots, \epsilon_n\}$, $\{m_1 e_1, \ldots, m_n e_n\}$ and $\{\alpha e_1, \ldots, \alpha e_n\}$.

Now, lets see look at the diagram summarising the associated change of basis matrices.



The top arrow corresponds to the action of A_α. The arrow on the left corresponds to the identity matrix I. The arrow along the bottom corresponds to a change of basis matrix with is diagonal which diagonal entries m_i, lets call it D. Lastly, whatever the matrix corresponding to the arrow going upwards on the right is, it represents a change of basis matrix between two integral bases for (α), therefore similarly to what we have seen before, it must correspond to an invertible matrix with integer coefficients, which we will denote by N. Note that this also means, $\det(N) = \pm 1$.

Now, from the diagram it is clear that going along the top of the diagram is the same as first going down, then right and then up. This means this is a commutative diagram and therefore we have $A_\alpha = NDI$ therefore

$$N_{K/\mathbb{Q}}(\alpha) = \det(A_\alpha) = \det(N)\det(D)\det(I) = \pm\det(D) = \prod_i m_i.$$

Taking absolute values now gives the result. □

Example 3.4.6. Let p be a odd prime, ζ_p a p-th root of unity and $\lambda_p = 1-\zeta_p$. Let $K = \mathbb{Q}(\zeta_p)$. Then from the proof of Theorem 2.3.2 we know $N_{K/\mathbb{Q}}(\lambda_p) = p$ and therefore $N((\lambda_p)) = p$ which by the above means, (λ_p) must be a prime ideal.

Corollary 3.4.7. *Let K be a number field, $\mathfrak{a} \subset \mathcal{O}_K$ an ideal and $\alpha \in \mathfrak{a}$. Then $\mathfrak{a} = (\alpha)$ if and only if $|N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{a})$.*

Proof. Since $\alpha \in \mathfrak{a}$ we have $(\alpha) \subset \mathfrak{a}$. Then by Lemma 3.4.3 and Proposition 3.4.5 gives the result. □

Lemma 3.4.8. *Let K be a number field and $\mathfrak{a} \subset \mathcal{O}_K$ a non-zero ideal. Let $a = N(\mathfrak{a})$. Then $a \in \mathfrak{a}$.*

Proof. Recall that by Lagrange's Theorem, every element in $\mathcal{O}_K/\mathfrak{a}$ has order at most a. Therefore, if we look at the element $1 + \mathfrak{a} \in \mathcal{O}_K/\mathfrak{a}$ we have $a \cdot (1 + \mathfrak{a}) = 0 + \mathfrak{a}$ therefore $a \in \mathfrak{a}$. □

Remark 3.4.9. We've seen something similar in the proof of Proposition 3.2.4.

Corollary 3.4.10. *Let K be a number field. Then there are only finitely many ideals with a given norm.*

Proof. If $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$ then by Lemma 3.4.8 we have $a \in \mathfrak{a}$ which means $\mathfrak{a} \mid (a)$. But by uniqueness of factorization, a only has finitely many factors, which gives the result. □

3.5 Splitting of prime ideals

We now want to understand how prime ideals change as we go up in field extensions, by which we mean the following: In $\mathbb{Z}$ we know that the prime ideals are all principal and generated by prime numbers, i.e, they are of the form (p) for p a prime. Now, what happens when we extend our number field? Well if we now go from $(\mathbb{Q}, \mathbb{Z})$ to $(\mathbb{Q}(\sqrt{-5}), \mathbb{Z}[\sqrt{-5}])$ then lets look at what happens to our prime ideals. In $\mathbb{Z}[\sqrt{-5}]$, the ideal (2) is no longer prime, since we will see that

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

where now $(2, 1 + \sqrt{-5})$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. (You actually have enough to check this. You can compute its norm and see that it has norm 2)

Similarly, if we look at the ideal (3) in $\mathbb{Z}[\sqrt{-5}]$, we find that

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

where again each idea on the right is now prime.

Definition 3.5.1. Let K/F be a finite extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. If $\mathfrak{P}$ is a non-zero prime ideal in $\mathcal{O}_K$ and $\mathfrak{p}$ is a non-zero prime ideal in $\mathcal{O}_F$ then we say $\mathfrak{P}$ lies over $\mathfrak{p}$ (or equivalently $\mathfrak{p}$ lies under $\mathfrak{P}$), if $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$. Here $\mathfrak{p}\mathcal{O}_K$ denotes the ideal generated by $\mathfrak{p}$ in $\mathcal{O}_K$.

Proposition 3.5.2. *Let K/F be a finite extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. If $\mathfrak{P}$ is a non-zero prime ideal in K and $\mathfrak{p}$ is a non-zero prime ideal in F then the following conditions are equivalent:*

(1) $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$

(2) $\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_K$

(3) $\mathfrak{P} \supset \mathfrak{p}$

(4) $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$

(5) $\mathfrak{P} \cap F = \mathfrak{p}$.

Proof. Corollary 3.3.14 gives that (1) and (2) are equivalent. Since $\mathfrak{P}$ is an ideal, if it contains $\mathfrak{p}$ it contains $\mathfrak{p}\mathcal{O}_K$, therefore (2) and (3) are equivalent. Since $\mathfrak{P} \subset \mathcal{O}_K$ it follows that (4) and (5) are equivalent.

So it remains to prove (3) and (4) are equivalent. It obvious that (4) $\implies$ (3) so we just need the reverse. Note that $\mathfrak{P} \cap \mathcal{O}_F$ contains $\mathfrak{p}$ and is moreover an ideal in $\mathcal{O}_F$. But now, since every prime ideal in a Dedekind domain is maximal, $\mathfrak{p}$ is also maximal and therefore we must have $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$ or $\mathfrak{P} \cap \mathcal{O}_F = \mathcal{O}_F$. But if $\mathfrak{P} \cap \mathcal{O}_F = \mathcal{O}_F$ then $1 \in \mathfrak{P}$ meaning $\mathfrak{P} = \mathcal{O}_K$ which contradicts it being a prime ideal. □

Example 3.5.3. If we take $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{3})$ then $(2, 1 + \sqrt{3})$ lies above (2). To see this we just note that $(2, 1 + \sqrt{3}) \cap \mathbb{Z} = (2)$.

Theorem 3.5.4. *Let K/F be a finite extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Then every non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ lies over a unique non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$.*

Conversely, every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ lies under at least one non-zero prime ideal $\mathfrak{P} \subset \mathcal{O}_K$.

Proof. For the first part, we claim that $\mathfrak{P} \cap \mathcal{O}_F$ is a prime ideal in $\mathcal{O}_F$ (this is enough as from Proposition 3.5.2 (4) will give us uniqueness). For this, we first note that since $1 \notin \mathfrak{P}$, then $\mathfrak{P} \cap \mathcal{O}_F$ wont be the whole ring. Moreover, by the proof of Proposition 3.2.4 we see that $\mathfrak{P}$ contains $N_{K/F}(a) \in \mathbb{Z}$ for all $a \in \mathfrak{P}$. Since the norm of a non-zero element is non-zero, and $\mathfrak{P}$ is non-zero, we get that $\mathfrak{P} \cap \mathbb{Z}$ is non-zero and therefore so is $\mathfrak{P} \cap \mathcal{O}_F$. So $\mathfrak{P} \cap \mathcal{O}_F$ is a proper ideal, so we just need to prove it is prime. So if $r, s \in \mathcal{O}_F$ with $rs \in \mathfrak{P} \cap \mathcal{O}_F$ then $rs \in \mathfrak{P}$, therefore either $r \in \mathfrak{P}$ or $s \in \mathfrak{P}$ since $\mathfrak{P}$ is prime. From this the first part follows.

For the second part, it suffices to look check that $\mathfrak{p}\mathcal{O}_K \neq \mathcal{O}_K$, since in this case, it will be divisible by some prime ideal, and by definition this prime ideal would lie over $\mathfrak{p}$. So we are reduced to checking $1 \notin \mathfrak{p}\mathcal{O}_K$. By Lemma 3.3.4 we can find $x \in F \backslash \mathcal{O}_F$ such that $x\mathfrak{p} \subset \mathcal{O}_F$. Then $x\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_F\mathcal{O}_K = \mathcal{O}_K$. If $1 \in \mathfrak{p}\mathcal{O}_K$ then $x \in \mathcal{O}_K$, but then x is in $\mathcal{O}_K \cap F = \mathcal{O}_F$ and this an algebraic integer, contradicting the fact that $x \in F \backslash \mathcal{O}_F$.

□

Definition 3.5.5. Let K/F be a finite extension of number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$ and let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_F$. Then

$$\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

We call the e_i the *ramification indices* and if needed we will denote them by $e_{\mathfrak{P}_i|\mathfrak{p}}$.

Now, let $\mathfrak{P}$ lie over $\mathfrak{p}$. Recall that $k_{\mathfrak{P}} := \mathcal{O}_K/\mathfrak{P}$ and $k_{\mathfrak{p}} := \mathcal{O}_F/\mathfrak{p}$ are both finite fields, since $\mathfrak{P}, \mathfrak{p}$ are both maximal ideals and by Proposition 3.2.4 we know the quotient ring is always finite. These are called the *residual fields* attached to $\mathfrak{P}$ and $\mathfrak{p}$ respectively. Moreover, $k_{\mathfrak{p}}$ is naturally a subfield of

$k_{\mathfrak{P}}$ (convince yourself of this). Therefore, $k_{\mathfrak{P}}$ is a finite extension of $k_{\mathfrak{p}}$ and $[k_{\mathfrak{P}} : k_{\mathfrak{p}}]$ is called the *inertial degree* or *residue degree* of $\mathfrak{P}$ over $\mathfrak{p}$, which will be denoted $f_{\mathfrak{P}|\mathfrak{p}}$.

Proposition 3.5.6. *Let $F \subset K \subset L$ be number fields and $p \subset \mathfrak{p} \subset \mathfrak{P}$ be prime ideals in $\mathcal{O}_F \subset \mathcal{O}_K \subset \mathcal{O}_L$. Then*

$$e_{\mathfrak{P}|p} = e_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{p}|p}$$

and

$$f_{\mathfrak{P}|p} = f_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{p}|p}$$

Proof. For the f's this follows easily from the Tower Law 1.3.19. For the e's the result is clear. □

Theorem 3.5.7. *Let K be a number field with $[K : \mathbb{Q}] = n$ and p a prime number. If $\mathfrak{p}_i$ are the prime ideals in $\mathcal{O}_K$ dividing $p\mathcal{O}_K$, then*

$$\sum_i e_{\mathfrak{p}_i|p} f_{\mathfrak{p}_i|p} = n$$

with notation as in Definition 3.5.5.

Proof. Let $e_i := e_{\mathfrak{p}_i|p}$ and $f_i := f_{\mathfrak{p}_i|p}$. By definition we have

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}.$$

Now, lets take norms on both sides: By Proposition 3.4.5 we have $N(p\mathcal{O}_K) = |N_{K/\mathbb{Q}}(p)| = p^n$.

So we have

$$p^n = \prod_i N(\mathfrak{p}_i)^{e_i}.$$

So it remains to show that $N(\mathfrak{p}_i) = p^{f_i}$. For this we note that $\mathcal{O}_K/\mathfrak{p}_i$ is a finite extension of $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} =: k_p$ of degree $[k_{\mathfrak{p}_i}/k_p] = f_i$. Therefore $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_p^{f_i}$ (as a vector space) from which it follows that $N(\mathfrak{p}_i) = p^{f_i}$. □

Note that we have only defined this for primes $\mathfrak{p}$ lying above a rational prime $p \in \mathbb{Z}$. But these things make sense in more generality for primes $\mathfrak{P}$ lying above a prime ideal $\mathfrak{p}$ in $\mathcal{O}_F$ for K/F a finite extension of number fields.

In this case one can again prove that

$$\sum_i e_{\mathfrak{P}_i|\mathfrak{p}} f_{\mathfrak{P}_i|\mathfrak{p}} = [K : F] \tag{3.1}$$

but the proof is a bit more involved. But if we assume the following proposition (which I wont prove)

Proposition 3.5.8. *Let K, F be a number fields with $[K : F] = n$. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_F$ and let $\mathfrak{A} = \mathfrak{a}\mathcal{O}_K$, then*

$$N(\mathfrak{A}) = N(\mathfrak{a})^n$$

Then 3.1 is easy to prove from this.

Exercise 3.5.9. Using Proposition 3.5.8 prove 3.1.

Theorem 3.5.10 (Dedekind–Kummer)**.** *Let K/F be an extension of number fields and $\alpha \in \mathcal{O}_K$ a primitive element so that $K \cong F(\alpha)$.*

Let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal and p the prime number such that $(p) = \mathfrak{p} \cap \mathbb{Z}$. Assume that p does not divide the index[b]

$$[\mathcal{O}_K : \mathcal{O}_F[\alpha]].$$

Let $m_{\alpha,F}$ be the minimal polynomial of α over F and let

$$\overline{m}_{\alpha,F} \in (\mathcal{O}_F/\mathfrak{p})[x]$$

be its reduction modulo $\mathfrak{p}$. Now, write $\overline{m}_{\alpha,F}$ as a product of powers of irreducible polynomials (i.e factorize it)

$$\overline{m}_{\alpha,F}(x) = \overline{m}_1(x)^{e_1} \dots \overline{m}_r(x)^{e_r}.$$

Next, let $m_i \in \mathcal{O}_F[x]$ be a polynomial whose reduction modulo $\mathfrak{p}$ is $\overline{m}_i$ and let

$$\mathfrak{P}_i = (\mathfrak{p}, m_i(\alpha)) = \mathfrak{p}\mathcal{O}_K + (m_i(\alpha)).$$

Then:

1. *The ideals $\mathfrak{P}_i$ are independent of choice of m_i. (This is by construction)*
2. *The $\mathfrak{P}_i$ are distinct prime ideals and they are precisely the prime ideals of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Therefore*

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

3. *$f_{\mathfrak{P}_i|\mathfrak{p}} = \deg(\overline{m}_i)$ and $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$*

Proof. The result will follow from the following three claims:

A Let $f_i = \deg(\overline{m}_i)$. For each i, either $\mathfrak{P}_i = \mathcal{O}_K$ or $\mathcal{O}_K/\mathfrak{P}_i$ is a field of size $|\mathcal{O}_F/\mathfrak{p}|^{f_i}$.

B $\mathfrak{P}_i + \mathfrak{P}_j = \mathcal{O}_K$ whenever $i \neq j$.

[b] Note that here I am thinking of $\mathcal{O}_F[\alpha]$ as a subgroup of $\mathcal{O}_K$ and then $[\mathcal{O}_K : \mathcal{O}_F[\alpha]]$ denotes the size of the quotient group $\mathcal{O}_K/\mathcal{O}_F[\alpha]$.

C $\mathfrak{p}\mathcal{O}_K$ divides $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$.

From this we get the result as follows: By relabelling the $\mathfrak{P}_i$ we can assume that $\mathfrak{P}_1, \dots, \mathfrak{P}_s \neq \mathcal{O}_K$ and $\mathfrak{P}_{s+1}, \dots, \mathfrak{P}_r = \mathcal{O}_K$.

Now, from ((1)) it follows that $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ are all prime ideals (since quotienting out by them gives a field). Moreover, by construction they contain $\mathfrak{p}$, so lie above $\mathfrak{p}$ and $f_{\mathfrak{P}_i|\mathfrak{p}} = f_i$ (to see this just look at how the residue degrees are defined).

Next ((2)) tells us that $\mathfrak{P}_1, \dots, \mathfrak{P}_s$ are all distinct and ((3)) becomes

$$\mathfrak{p}\mathcal{O}_K \mid \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_s^{e_s}.$$

From this it follows that

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{d_1} \dots \mathfrak{P}_s^{d_s}$$

with $d_i \leq e_i$. Now, using 3.1 we have

$$[K : F] = \sum_{i=1}^{s} d_i f_i$$

but on the other hand

$$\deg(m_{\alpha,F}) = [K : F] = \sum_{i=1}^{r} e_i f_i.$$

So comparing these gives $r = s$, $d_i = e_i$ for all i.

So lets prove these three claims.

Proof of (1). Note that each $\overline{m}_i$ is an irreducible polynomial in $(\mathcal{O}_F/\mathfrak{p})[x]$. So if we let $E := \mathcal{O}_F/\mathfrak{p}$ (which is a field), then $M_i := E[x]/\overline{m}_i$ is again a field. We have a map

$$\mathcal{O}_F[x] \longrightarrow M_i$$

given by first reducing modulo $\mathfrak{p}$ and then modulo $\overline{m}_i$. This map is clearly surjective and the kernel is given by the ideal in $\mathcal{O}_F[x]$ generated by $\mathfrak{p}$ and m_i. So we have an isomorphism

$$\mathcal{O}_F[x]/(\mathfrak{p}, m_i) \xrightarrow{\sim} M_i.$$

Alongside this, note that we have a ring homomorphism

$$\phi : \mathcal{O}_F[x] \longrightarrow \mathcal{O}_K/\mathfrak{P}_i$$

given by evaluation at α (i.e $x \mapsto \alpha$) and reducing modulo $\mathfrak{P}_i$. By definition of $\mathfrak{P}_i$ its clear that $(\mathfrak{p}, m_i)$ is in the kernel. But from the above, we know $(\mathfrak{p}, m_i)$ is a maximal ideal, so $\ker(\phi)$ is either $(\mathfrak{p}, m_i)$ or $\mathcal{O}_F[x]$.

Next, we claim that ϕ is surjective. To show this we need to show that $\mathcal{O}_K = \mathcal{O}_F[\alpha] + \mathfrak{P}_i$. It turns out that in fact something stronger is true, which is that $\mathcal{O}_K = \mathcal{O}_F[\alpha] + (p)\mathcal{O}_K$ (note that $p\mathcal{O}_K \subset \mathfrak{P}_i$). To prove this, we need to make use of the one thing we know, which is that $p \nmid [\mathcal{O}_K : \mathcal{O}_F[\alpha]]$. How do we use this fact? notice that the index[c] of $\mathcal{O}_F[\alpha] + p\mathcal{O}_K$ in $\mathcal{O}_K$ must divide both of $[\mathcal{O}_K : \mathcal{O}_F[\alpha]]$ and $[\mathcal{O}_K : p\mathcal{O}_K]$. But $[\mathcal{O}_K : p\mathcal{O}_K]$ is some power of p and by assumption $p \nmid [\mathcal{O}_K : \mathcal{O}_F[\alpha]]$, so these indexes are coprime and therefore

$$[\mathcal{O}_K : (\mathcal{O}_F[\alpha] + p\mathcal{O}_K)] = 1 \implies \mathcal{O}_K = \mathcal{O}_F[\alpha] + p\mathcal{O}_K.$$

Therefore since $\ker(\phi)$ is either is either or $\mathcal{O}_F[x]$, it follows that either $\mathcal{O}_K/\mathfrak{P}_i \xrightarrow{\sim} M_i$ (which would be if the kernel is $(\mathfrak{p}, m_i)$) or $\mathfrak{P}_i = \mathcal{O}_K$ if the kernel is $\mathcal{O}_F[x]$.

□

Proof of (2). By construction the $\overline{m}_i$ are distinct irreducible polynomials in $E[x]$. Therefore for $i \neq j$ we can find $\overline{g}, \overline{h}$ such that $\overline{m}_i\overline{g} + \overline{m}_j\overline{h} = 1$ (in $E[x]$). This mean that we can find $g, h \in \mathcal{O}_F[x]$ such that $m_i g + m_j h \equiv 1 \pmod{\mathfrak{p}}$. If we now simply evaluate at $x = \alpha$ we see that

$$m_i(\alpha)g(\alpha) + m_j(\alpha)h(\alpha) \equiv 1 \mod \mathfrak{p}$$

and therefore

$$1 \in (\mathfrak{p}, m_i(\alpha), m_j(\alpha)) = \mathfrak{P}_i + \mathfrak{P}_j$$

□

Proof of (3). Since $\mathfrak{P}_i = (\mathfrak{p}, m_i(\alpha))$ it follows that $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ is contained in

$$(\mathfrak{p}, m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r}).$$

But this means (by Corollary 3.3.14) that $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ is divisible by $(\mathfrak{p}, m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r})$.

But note that

$$\overline{m}_1(\alpha)^{e_1} \dots \overline{m}_r(\alpha)^{e_r} = \overline{m}_\alpha(\alpha) = 0.$$

Therefore

$$m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r} \equiv 0 \mod \mathfrak{p}\mathcal{O}_K$$

thus $(\mathfrak{p}, m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r}) = \mathfrak{p}\mathcal{O}_K$ which gives the result.

□

□

[c] By index I mean the size the of the quotient.

This theorem is really useful for us. It will make it really easy to understand how prime ideals change as we extend our field. For clarity, lets just see what this theorem says when our bottom field (F) is simply $\mathbb{Q}$.

Corollary 3.5.11. *Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha \in \mathcal{O}_K$ be a primitive element so that $K \cong \mathbb{Q}(\alpha)$.*

Let p be a prime number not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and let

$$\overline{m}_\alpha(x) = \overline{m}_1(x)^{e_1} \dots \overline{m}_r(x)^{e_r}$$

be the reduction modulo p of the minimal polynomial m_α of α. Then in $\mathcal{O}_K$ the ideal (p) factorizes as

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i = (p, m_i(\alpha))$ and $f_{\mathfrak{p}_i|p} = \deg(\overline{m}_i)$ and $e_i = e_{\mathfrak{p}_i|p}$.

Definition 3.5.12. Let K be a number field and p a prime number. We say

1. p is *ramified* in K, if there exists a $\mathfrak{p}|p$ such that $e_{\mathfrak{p}|p} > 1$. Otherwise we say p is *unramified*.
2. p is *totally ramified* if there is a $\mathfrak{p}|p$ such that $e_{\mathfrak{p}|p} = [K : \mathbb{Q}]$.
3. p is *inert* if p is unramified and there exists a unique prime $\mathfrak{p}$ lying above p (which will have $f_{\mathfrak{p}|p} = [K : \mathbb{Q}]$).
4. p is *split* if it is unramified and for some $\mathfrak{p}|p$ we have $f_{\mathfrak{p}|p} = 1$. If it is unramified and for all $\mathfrak{p}|p$ we we have $f_{\mathfrak{p}|p} = 1$, we say p is *totally split*.

Example 3.5.13. Going back to $\mathbb{Z}[\sqrt{-5}]$, we saw that the ideal (2) is no longer prime, since we will see that

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

where now $(2, 1 + \sqrt{-5})$ is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. Therefore (2) is totally ramified in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, if we look at the ideal (3) in $\mathbb{Z}[\sqrt{-5}]$, we find that

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

where again each idea on the right is now prime. So (3) totally splits in $\mathbb{Z}[\sqrt{-5}]$.

Lastly, if we look at (11) we will see that this remains prime in $\mathbb{Z}[\sqrt{-5}]$ and is therefore inert.

Lets now do some examples:

Example 3.5.14. Let $K = \mathbb{Q}(\sqrt{6})$ (so here $\alpha = \sqrt{6}$). From Theorem 2.1.11 we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ and therefore $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ so Theorem 3.5.10 works for any prime number. Now, note that $m_\alpha = x^2 - 6$.

Lets use this to find how the ideal $2\mathcal{O}_K$ factorizes in $\mathbb{Z}[\sqrt{6}]$. From now on I will just denote $p\mathcal{O}_K$ by (p). First step is to reduce m_α modulo 2. Which gives $\overline{m}_\alpha(x) = x^2 = \overline{m}_1(x)^2$ (if you cant see why we only have one $\overline{m}_i$ on the right hand side, just look back at the theorem and note that the $\overline{m}_i$ are distinct by construction).

Next, we need to find some $m_1(x)$ whose reduction modulo (2) agrees with $\overline{m}_1(x)$. For this lets just be lazy and take $m_1(x) = x$ (this might be a good point to comeback to and try and convince yourself the the choice of $m_1(x)$ wont make a difference to then end result, i.e. see what happens if we take $m_1(x) = x + 2$). The theorem then says that

$$(2) = \mathfrak{p}_2^2 := (2, \sqrt{6})^2.$$

This means (2) ramifies in $\mathcal{O}_K$.

Ok lets do some more examples. To speed things up here is a table of values of $m_\alpha(x)$ for some small x which is useful for figuring out how m_α factorizes modulo p.

x	$m_\alpha(x) = x^2 - 6$
0	-6
± 1	-5
± 2	-2
± 3	3
± 4	10
± 5	19

From this table we see that:

$$\begin{aligned} m_\alpha(x) &= x^2 \pmod 3 \\ m_\alpha(x) &= (x-1)(x+1) \pmod 5 \\ m_\alpha(x) &= (x^2 - 6) \pmod 7 \\ m_\alpha(x) &= (x^2 - 6) \pmod{11} \end{aligned}$$

From this it follows that:

$$
\begin{aligned}
(3) &= \mathfrak{p}_3^2 := (3, \sqrt{6})^2 \\
(5) &= \mathfrak{p}_5\mathfrak{p}_5' := (5, \sqrt{6}-1)(5, \sqrt{6}+1) \\
(7) &= \mathfrak{p}_7 := (7) \\
(11) &= \mathfrak{p}_{11} := (11)
\end{aligned}
$$

So we see that (3) ramified in $\mathcal{O}_K$, (5) splits and (7), (11) are inert in $\mathcal{O}_K$.

BUT WAIT, THERE'S MORE (insert relevant meme): The theorem tells us the norm of the ideals $\mathfrak{p}$. Specifically, the theorem says that $f_{\mathfrak{p}|p} = \deg(\overline{m}_i)$ and by Theorem 3.5.7 we saw $N(\mathfrak{p}) = p^{f_{\mathfrak{p}|p}}$. So, in this case we get

$$
\begin{aligned}
N(\mathfrak{p}_2) &= 2 \\
N(\mathfrak{p}_3) &= 3 \\
N(\mathfrak{p}_5) &= 5^1 \text{ and } N(\mathfrak{p}_5') = 5^1 \\
N(\mathfrak{p}_7) &= 7^2 \\
N(\mathfrak{p}_{11}) &= 11^2
\end{aligned}
$$

We can also use this factorize other ideals in $\mathcal{O}_K$.

1. Say $\mathfrak{a}$ is an ideal, then we can first calculate $N(\mathfrak{a})$ (which if $\mathfrak{a}$ is principal we know how to do, but in general this might be hard) and factorize it.
2. For each prime number p appearing, we then factor (p) in $\mathcal{O}_K$ as we did above.
3. Note that Corollary 3.4.10 tells us that there are only finitely many prime ideals of norm p, we can find them all by looking at the factorization of (p).
4. Next we use Proposition 3.3.14, tells us that $\mathfrak{p}|\mathfrak{a}$ if and only if the generators of $\mathfrak{p}$ are in $\mathfrak{a}$.

Lets do this for $\mathfrak{a} = (12 + 7\sqrt{6})$. To find the norm of this ideal we use Proposition 3.4.5 this gives

$$
N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(12 + 7\sqrt{6})| = |12^2 - 6 \cdot 7^2| = 150 = 2 \cdot 3 \cdot 5^2
$$

From the above calculation we see that $\mathfrak{p}_2$ is the only prime ideal of norm 2 and $\mathfrak{p}_3$ is the only prime ideal of norm 3 and that we have two ideals of

norm 5. This immediately gives us that there are only 3 ideals of norm 150 and they are

$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2 \qquad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2 \qquad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5'$$

So we need to check with one of these is $\mathfrak{a}$. First we see that since $\mathfrak{p}_5\mathfrak{p}_5' = (5)$ and $12 + 7\sqrt{6}$ is not a multiple of 5, it follows it can't be the one with a $\mathfrak{p}_5\mathfrak{p}_5'$ term. Now, note that $12 + 7\sqrt{6} = 5 + 7(1 + \sqrt{6})$ therefore its contained in $\mathfrak{p}_5'$ and therefore

$$\mathfrak{a} = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2.$$

Example 3.5.15. Lets do a cubic. Let $K = \mathbb{Q}(\alpha)$ where α is a root of $m_\alpha(x) = x^3 + 10x + 1$. This is irreducible since it is irreducible in $\mathbb{F}_{13}$ (just check it doesnt have a root). By Corollary 2.2.26 we have that

$$\Delta(\{1, \alpha, \alpha^2\}) = -4027$$

which is a prime number, in particular it is square-free, so this is an integral basis by Corollary 2.2.9. So $\mathcal{O}_K = \mathbb{Z}[\alpha]$. So we can freely apply Theorem 3.5.10.

Lets see how some prime split in K:

We have

$$\overline{m}_\alpha(x) = (x + 1)(x^2 + x + 1) \mod 2,$$

therefore

$$(2) = \mathfrak{p}_2\mathfrak{p}_2' = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1).$$

Thus (2) is unramified, and the residue degrees are $f_{\mathfrak{p}_2|2} = 1$ and $f_{\mathfrak{p}_2'|2} = 2$.

Lets look at (29). Here we see that

$$\overline{m}_\alpha(x) = (x + 5)(x - 3)(x - 2) \mod 29$$

meaning

$$(29) = \mathfrak{p}_{29}\mathfrak{p}_{29}'\mathfrak{p}_{29}'' = (29, \alpha + 5)(29, \alpha - 3)(29, \alpha - 2).$$

Thus (29) is also unramified and in particular it is totally split. So the residue degrees are all 1.

Lastly, lets look at (4027). Here we see

$$\overline{m}_\alpha(x) = (x + 2215)^2(x + 3624) \mod 4027$$

therefore

$$(4027) = \mathfrak{p}_{4027}^2\mathfrak{p}_{4027}' = (4027, \alpha + 2215)^2(4027, \alpha + 3624).$$

Thus (4027) is ramified. $e_{\mathfrak{p}_{4027}|4027} = 2$, $e_{\mathfrak{p}_{4027}'|4027} = 1$ and the residue degrees are all 1.

Proposition 3.5.16. *Let K be a number field and $\alpha \in \mathcal{O}_K$ a primitive element with m_α Eisenstein at p. Then we have*

$$(p) = \mathfrak{p}^{[K:\mathbb{Q}]}$$

with $\mathfrak{p} = (p, \alpha)$.

Proof. If α is Eisenstein at p then $\frac{\mathcal{O}_K}{\mathbb{Z}[\alpha]}$ has no element of order p by Lemma 2.2.21 and therefore the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is coprime to p. So we can apply Theorem 3.5.10 which, since m_α is Eisenstein at p, gives $\overline{m}_\alpha(x) = x^{[K:\mathbb{Q}]}$, from which the result follows. □

Lets see what this tells us for quadratic extensions:

Note that if n is a square-free integer, then in $\mathbb{Q}(\sqrt{n})$ there are three possibilities for how primes decompose (this follows from Theorem 3.5.7). These being

$$(p) = \begin{cases} \mathfrak{p}^2, & f_{\mathfrak{p}|p} = 1 \\ \mathfrak{p}, & f_{\mathfrak{p}|p} = 2 \\ \mathfrak{p}\mathfrak{p}', & f_{\mathfrak{p}|p} = f_{\mathfrak{p}'|p} = 1 \end{cases} \tag{3.2}$$

Theorem 3.5.17. *Let n be a square-free integer, $K := \mathbb{Q}(\sqrt{n})$ and p a prime number.*

(1) If $p \mid n$ then $(p) = (p, \sqrt{n})^2$.

(2) If n is odd then

$$(2) = \begin{cases} (2, 1+\sqrt{n})^2, & \text{if } n \equiv 3 \pmod 4 \quad (3.3) \\ \left(2, \frac{1+\sqrt{n}}{2}\right)\left(2, \frac{1-\sqrt{n}}{2}\right) & \text{if } n \equiv 1 \pmod 8 \quad (3.4) \\ (2) & \text{if } n \equiv 5 \pmod 8 \quad (3.5) \end{cases}$$

(3) If p is odd and $p \nmid n$, then

$$(p) = \begin{cases} (p, a+\sqrt{n})(p, a-\sqrt{n}) & \text{if } n \equiv a^2 \pmod p \quad (3.6) \\ (p) & \text{if } \left(\frac{n}{p}\right) = -1 \end{cases}$$

Moreover, in (3.4) and (3.6) the ideals appearing are distinct.

Proof. We will defer the proof that the ideals in (3.4) and (3.6) are distinct to Corollary 3.6.12.

For (1), note that $(p, \sqrt{n})^2 = (p^2, p\sqrt{n}, n)$, which if $p \mid n$ is contained in (p). Conversely, $(p^2, p\sqrt{n}, n)$ contains the GCD of p^2 and n, which is p, so we get $(p) \subset (p, \sqrt{n})^2$, therefore we get the equality we are after.

We will split the rest of proof into two cases, which together give the result. The first is if $n \equiv 2, 3 \pmod 4$ and the second if $n \equiv 1 \pmod 4$.

From Theorem 2.1.11 we know that if $n \equiv 2, 3 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$. In this case Theorem 3.5.10 (using $\alpha = \sqrt{n}$ and $m_\alpha = x^2 - n$) gives (3) and (3.3) (which is the only one that applies in this case).

Now, we look at the case $n \equiv 1 \pmod 4$. In this case, Theorem 2.1.11 tells us that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$. Note that this means the index $[\mathcal{O}_K : \mathbb{Z}[\sqrt{n}]] = 2$ but p is odd, so it doesn't divide this index. So Theorem 3.5.10 gives (3).

So, we are left with (3.4) and (3.5) of (2). Here we cannot apply Theorem 3.5.10. So lets assume $n \equiv 1 \pmod 8$, then

$$\left(2, \frac{1+\sqrt{n}}{2}\right)\left(2, \frac{1-\sqrt{n}}{2}\right) = \left(4, 1-\sqrt{n}, 1+\sqrt{n}, \frac{1-n}{4}\right).$$

Now, since each of these generators is divisible by 2, we get that

$$\left(2, \frac{1+\sqrt{n}}{2}\right)\left(2, \frac{1-\sqrt{n}}{2}\right) \subset (2).$$

Conversely, $\left(4, 1-\sqrt{n}, 1+\sqrt{n}, \frac{1-n}{4}\right)$ contains the $\gcd(4, 1-\sqrt{n}) = 2$ which gives the reverse inclusion.

Finally, lets assume $n \equiv 5 \pmod 8$. In this case lets consider $\mathcal{O}_K/(2)$. By Theorem 3.5.7 its enough to show that $\mathcal{O}_K/(2)$ is a field not isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (since this means the residue degree is 2 and therefore, since we are in a quadratic field, it must be inert). To show they are not isomorphic, consider

$$m_\alpha(x) = x^2 - x + \frac{1-n}{4}.$$

By construction, this has a root in $\mathcal{O}_K$ and therefore has a root in $\mathcal{O}_K/(2)$ (just reduce your root modulo 2). On the other hand, since $n \equiv 5 \pmod 8$ we have $m_\alpha(x) = x^2 + x + 1 \pmod 2$ which by Exercise 1.2.19 we know is irreducible in $\mathbb{Z}/2\mathbb{Z}$ and therefore has no root in $\mathbb{Z}/2\mathbb{Z}$. So $\mathcal{O}_K/(2)$ is an extension of $\mathbb{F}_2$ by a root of $x^2 + x + 1$, so its a field, which also goes by the name $\mathbb{F}_4$.

□

Remark 3.5.18. Using this theorem together with the quadratic reciprocity law, which says

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

(with p, q primes) we can easily find how primes decompose in quadratic extensions.

3.6 Embeddings and prime ideals

Lets now look at how embeddings interact with prime ideals. We begin with a definition you may have seen in your Galois theory course.

Definition 3.6.1. Let K/F be an extension of number fields. We say K is *normal* over F every embedding $\sigma : K \to \mathbb{C}$ which fixes F has image again in K. In other words the embedding σ is an automorphism $\sigma : K \to K$ which fixes the elements of F.

In particular, if $K = F(\alpha)$ and K contains all of the conjugates of α, then K is normal.

Example 3.6.2. Let $K = \mathbb{Q}(\sqrt{2})$ and $F = \mathbb{Q}$. Then since each embedding that fixes $\mathbb{Q}$ sends $\sqrt{2}$ to one of $\pm\sqrt{2} \in K$, we see that K is normal.

Non-example 3.6.3. If $K = \mathbb{Q}(\sqrt[3]{2})$ then this is not normal, since one of the embeddings will send $\sqrt[3]{2}$ to $\zeta_3\sqrt[3]{2}$ (where ζ_3 is a non-trivial cube root of unity) which is a complex number and therefore not contained in K.

Proposition 3.6.4. *Let K/F be a finite extension of number fields. Then there is a finite extension L/K such that L/F is normal as is L/K.*

Proof. If $K = F(\alpha)$, then just set $L = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where α_i are the conjugates of α. □

Notation 3.6.5. If K/F is a normal extension, $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal and σ is an embedding of K fixing F (which in particular is an automorphism). Then we let $\sigma(\mathfrak{a})$ be the ideal in K generated by the images of the elements of $\mathfrak{a}$ under σ.

Furthermore, we let $\mathrm{Gal}(K/F)$ denote the set of embeddings of K which fix F. Since K/F is normal, this can be made into a group by using composition as our group operation, i.e. $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ we let $(\sigma_1\sigma_2)(x) = \sigma_1(\sigma_2(x))$. By Proposition 1.5.8 there are only $[K : F]$ such embeddings, so this group has size $[K : F]$ and is known as the Galois group.

Theorem 3.6.6. *Let K/F be a normal extension of number fields. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_F$ and $\mathfrak{P}, \mathfrak{P}'$ be two prime ideals of $\mathcal{O}_K$ above $\mathfrak{p}$. Then $\sigma(\mathfrak{P})$ is again a prime ideal lying over $\mathfrak{p}$, moreover there is some element $\sigma \in \mathrm{Gal}(K/F)$, such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Proof. Let $G := \mathrm{Gal}(K/F)$. Note that since $\mathfrak{P}$ is a prime ideal $\mathcal{O}_K/\mathfrak{P}$ is a integral domain. Now, apply σ to this quotient. Since $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ (as K/F is normal) we get

$$\mathcal{O}_K/\mathfrak{P} \cong \mathcal{O}_K/\sigma(\mathfrak{P})$$

and therefore $\sigma(\mathfrak{P})$ is again a prime ideal. Moreover, since $\mathfrak{P} \cap \mathcal{O}_F = \mathfrak{p}$ (this is what lying above means) and σ fixes F we see that $\sigma(\mathfrak{P}) \cap \mathcal{O}_F = \mathfrak{p}$.

Now, suppose that $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$ for all $\sigma \in G$. Then we can use the Chinese remainder theorem 3.3.21 to find some $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv 0 \mod \mathfrak{P}'$$

and

$$\alpha \equiv 1 \mod \sigma(\mathfrak{P})$$

for all $\sigma \in G$.

Now,

$$N_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \in \mathfrak{P}' \cap \mathcal{O}_F = \mathfrak{p}.$$

On the other hand $\alpha \notin \sigma(\mathfrak{P})$ by construction, and therefore $\sigma^{-1}(\alpha) \notin \mathfrak{P}$. But we have

$$N_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{\sigma^{-1} \in G} \sigma^{-1}(\alpha).$$

This gives us a contradiction, since we have just seen that the left hand side is in $\mathfrak{p}$. But the right hand is not contained in $\mathfrak{P}$ since $\sigma^{-1}(\alpha) \notin \mathfrak{P}$, but $\mathfrak{p} \subset \mathfrak{P}$.

□

Corollary 3.6.7. *Let K/F be a normal extension of number fields and let $\mathfrak{P}$ and $\mathfrak{P}'$ be two primes lying above the prime $\mathfrak{p}$. Then*

$$e_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{p}} \qquad f_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}'|\mathfrak{p}}$$

Proof. Lets start by factoring $\mathfrak{p}$ in $\mathcal{O}_K$. We have

$$\mathfrak{p}\mathcal{O}_K = \prod_i \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathfrak{p}}}.$$

Now, by Theorem 3.6.6, if we apply σ to this equation we get

$$\mathfrak{p}\mathcal{O}_K = \sigma(\mathfrak{p})\mathcal{O}_K = \prod_i \sigma(\mathfrak{P}_i)^{e_{\mathfrak{P}_i|\mathfrak{p}}}$$

but then by the fact that for any i, j we can find σ such that $\mathfrak{P}_i = \sigma(\mathfrak{P}_j)$ and uniqueness of factorization, we get that

$$e_{\mathfrak{P}_i|\mathfrak{p}} = e_{\mathfrak{P}_j|\mathfrak{p}}$$

which gives the first part of the result.

For the second part, we note that by the proof of Theorem 3.6.6 we have seen that

$$\mathcal{O}_K/\mathfrak{P} =: k_{\mathfrak{P}} \cong k_{\sigma(\mathfrak{P})} := \mathcal{O}_K/\sigma(\mathfrak{P})$$

from which the result follows. □

Corollary 3.6.8. *Let n be an integer and ζ_n an n-th root of unity. Let $K = \mathbb{Q}(\zeta_n)$ and p a prime number. Then*

$$(p) = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r)^e$$

where $\mathfrak{p}_i$ are the primes of $\mathcal{O}_K$ over p, which moreover all have the same inertial degree.

Proof. This follows from Corollary 3.6.7 by noting that K is a normal extension. □

Next we have a theorem that tells us about which primes will ramify in an extension.

Theorem 3.6.9. *Let p be a prime number and K a number field. If p is ramified in $\mathcal{O}_K$ then $p \mid \Delta(\mathcal{O}_K)$.*

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ over p such that $e_{\mathfrak{p}|p} > 1$. Then we can write $(p) = \mathfrak{p}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal divisible by all prime ideals in $\mathcal{O}_K$ which are above p.

Now, let $\alpha_1, \ldots, \alpha_n$ be a integral basis for $\mathcal{O}_K$. Since $\mathfrak{a}$ properly contains (p) we can find some $\alpha \in \mathfrak{a}\backslash(p)$. Then writing

$$\alpha = \alpha_1 m_1 + \cdots + \alpha_n m_n$$

with $m_i \in \mathbb{Z}$ we see that since $\alpha \notin (p)$, one of the m_i must not be divisible by p. So after relabelling, we can assume $p \nmid m_1$. Now, similar to Proposition 2.2.4 we have that

$$\Delta(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2\Delta(\alpha_1, \ldots, \alpha_n) = m_1^2\Delta(\mathcal{O}_K).$$

Since $p \nmid m_1$ its enough to show that $p \mid \Delta(\alpha, \alpha_2, \ldots, \alpha_n)$.

Now, let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K into $\mathbb{C}$. Let L be a finite extension of K such that $L/\mathbb{Q}$ is normal (which we can do by Proposition 3.6.4). Let $G := \mathrm{Gal}(L/\mathbb{Q})$. Then the elements of G are just the embeddings of L extending the embeddings of K (if you dont remember what this means go to Definition 1.5.5)

Since α is contained in $\mathfrak{a}$, its contained in every prime ideal in $\mathcal{O}_K$ over p. It follows that α is also in every prime ideal $\mathfrak{P}$ in $\mathcal{O}_L$ containing p, since each such prime contains p and $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ is again a prime ideal which contains p, hence $\mathfrak{p}$ lies over p and therefore contains α. Fix $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ over p. Then we claim that for any $\sigma \in G$, $\sigma(\alpha) \in \mathfrak{P}$. To see this note that $\sigma^{-1}(\mathfrak{P})$ is again a prime ideal in $\mathcal{O}_L$ over p and thus contains α. In particular, $\sigma_i(\alpha) \in \mathfrak{P}$ for all i. Therefore, by Proposition 2.2.16 $\Delta(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{P}$. But since the discriminant is an integer, we have $\Delta(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ and therefore p divides the discriminant. □

Corollary 3.6.10. *Let K be a number field with $K = \mathbb{Q}(\alpha)$ for α a primitive element and let $f \in \mathbb{Z}[x]$ be any monic polynomial such that $f(\alpha) = 0$. If p is a prime number such that $p \nmid N_{K/\mathbb{Q}}(f'(\alpha))$ then p is unramified.*

Proof. Since every monic polynomial with α as a root is divisible by m_α (see Proposition 1.3.10), its enough to check this for m_α. But then Proposition 2.2.19 gives the result. □

Corollary 3.6.11. *There are only finitely many primes of $\mathbb{Z}$ which ramify in a number field K.*

Corollary 3.6.12. *In (3.4) and (3.6) of Theorem 3.5.17 the ideals appearing are distinct.*

Proof. Using Exercise 2.2.28 and Theorem 3.6.9 we see that since in each case the prime does not divide the discriminant, the prime cannot be ramified and therefore the ideals are distinct. □

Going back to the cyclotomic example, one can determine the ramification and the inertial degree completely in this case.

Theorem 3.6.13 (Decomposition theorem for cyclotomic fields)**.** *Let n be a positive integer and ζ_n an n-th root of unity. Let $K = \mathbb{Q}(\zeta_n)$ and p a prime number. Write $n = p^k m$ with $p \nmid m$ and set $e = \varphi(p^k)$ (where φ is Euler's Totient function). Lastly, let f be the (multiplicative) order of p modulo m.*

Then

$$(p) = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r)^e$$

(so $e = e_{\mathfrak{p}_i|p}$) and moreover $f = f_{\mathfrak{p}_i|p}$.

Proof. We start by letting $\alpha = \zeta^m$ and $\beta = \zeta^{p^k}$. So α is a p^k-th root of unity and β is a m-th root of unity. We will prove the theorem by seeing how (p) factorizes in $\mathbb{Q}(\alpha)$ and in $\mathbb{Q}(\beta)$ and then combining the result.

Lemma 3.6.14. *With the above notation. In $\mathbb{Q}(\alpha)$ we have*

$$(p) = (1 - \alpha)^{\varphi(p^k)}$$

with $(1 - \alpha)$ a prime ideal.

Proof. First note that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(p^k)$ since this is the degree of the p^k cyclotomic polynomial (See Lemma 2.3.1).

Next, from Exercise 2.3.6 we have $p = u(1 - \alpha)^{\varphi(p^k)}$, this tells us that (as ideals in $\mathbb{Z}[\alpha]$)

$$(p) = (1 - \alpha)^{\varphi(p^k)}.$$

Theorem 3.5.7 then gives the result.

□

Lemma 3.6.15. *In $\mathbb{Q}(\beta)$, p is unramified and for each $\mathfrak{p}$ over p, we have $f_{\mathfrak{p}|p} = f$.*

Proof. Using Corollary 3.6.10 with $f(x) = x^m - 1$, we need to check if p divides

$$m^{[\mathbb{Q}(\beta):\mathbb{Q}]} N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta^{m-1}).$$

But $p \nmid m$ and β is a unit, so its norm is $\{\pm 1\}$ therefore p is unramified.

So in $\mathbb{Z}[\beta]$ we have

$$(p) = \mathfrak{p}_1 \dots \mathfrak{p}_s.$$

Moreover, since $\mathbb{Q}(\beta)/\mathbb{Q}$ is normal we know that $f_{\mathfrak{p}_i|p} = f_{\mathfrak{p}_j|p}$. So let $\mathfrak{p} := \mathfrak{p}_1$. Its enough to check that $f_{\mathfrak{p}|p} = f$ (where f is as above- the multiplicative order of p modulo m).

Let $\mathbb{F}_{\mathfrak{p}} := \mathbb{Z}[\beta]/\mathfrak{p}$. First, recall that $f_{\mathfrak{p}|p} = [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]$. So $f_{\mathfrak{p}|p} = h$ for some h. We want to show that $h = f$. We will do this in two steps, by first showing $h \geq f$ and then $h \leq f$.

($h \geq f$): Let $\overline{\beta}$ denote the image of β in $\mathbb{F}_{\mathfrak{p}}$. We will first show that $\overline{\beta}$ has order m in $\mathbb{F}_{\mathfrak{p}}$. Assume for contradiction this is not the case, then $\overline{\beta}^{m/l} \equiv 1 \pmod{\mathfrak{p}}$ (i.e. $\mathfrak{p} \mid (\beta^{m/l} - 1)$) for some prime factor l of m. Now, $\beta^{m/l}$ is an l-th root of unity. Then, by Exercise 2.3.6 we see that $\beta^{m/l} - 1$ divides l and l is a factor of m. Thus $\mathfrak{p} \mid m$. This gives a contradiction as $\mathfrak{p} \mid p$ and $\gcd(m, p) = 1$.

So $\overline{\beta}$ has order m in $\mathbb{F}_{\mathfrak{p}}$. By Lagrange's theorem this means $m \mid N(\mathfrak{p}) - 1$ and note that since $\mathfrak{p}$ is a prime ideal over p, we have $N(\mathfrak{p}) = p^h$. Thus $p^h \equiv 1 \pmod{m}$. But the order of p modulo m is f, so we have $h \geq f$.

($h \leq f$): Since $p^f \equiv 1 \pmod{m}$ it follows that $\beta^{p^f} = \beta$. Now, note that

$$(x + y)^{p^f} \equiv x^{p^f} + y^{p^f} \mod p\mathbb{Z}[\beta].$$

This means that for all $\gamma \in \mathbb{Z}[\beta]$ we have

$$\gamma^{p^f} \equiv \gamma \mod p\mathbb{Z}[\beta]$$

(also using FLT). Now since $(p) \subset \mathfrak{p}$ we see that

$$\gamma^{p^f} \equiv \gamma \pmod{\mathfrak{p}}.$$

Therefore every non-zero element of $\mathbb{F}_{\mathfrak{p}}$ is a root of $x^{p^f} - x$. Now, since we are in a field, any polynomial of degree d has at most d roots. This polynomial has p^h roots (as this is the size of $\mathbb{F}_{\mathfrak{p}}$) therefore $p^h \leq p^f \implies h \leq f$. This gives the result.

□

Lets now put these two lemmas together and finish proving the theorem.

Lemma 3.6.14 and Theorem 3.5.7 tells us that

$$e_{(1-\alpha)|p} \cdot f_{(1-\alpha)|p} = e \cdot 1 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \varphi(p^k)$$

Similarly, Lemma 3.6.15 gives

$$s \cdot e_{\mathfrak{p}|p} \cdot f_{\mathfrak{p}|p} = s \cdot 1 \cdot f = [\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(m)$$

Now, if $\mathfrak{P}_i$ denote the prime ideals of $\mathbb{Z}[\zeta_n]$ over p, then we know that

$$\sum_i e_{\mathfrak{P}_i|p} f_{\mathfrak{P}_i|p} = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi(p^k)\varphi(m)$$

Lastly, using Proposition 3.5.6 together with

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$$

gives

$$s \cdot e \cdot f = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

from which the result follows.

□

This theorem is sometimes called the cyclotomic reciprocity law, since it allows us to quickly find out how primes factor in cyclotomic fields, just like quadratic reciprocity is used for quadratic fields. For general number fields, we know of no such simple description.

Example 3.6.16. Lets use this theorem to see how primes factorize in $\mathbb{Q}(\zeta_5)$.

$p \mod 5$	Order of $p \mod m$	Factorization of (p)	Norms
0	-	$(p) = \mathfrak{p}^4$	$N(\mathfrak{p}) = p$
1	1	$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$N(\mathfrak{p}_i) = p$
2	4	(p)	$N((p)) = p^4$
3	4	(p)	$N((p)) = p^4$
4	2	$(p) = \mathfrak{p}_1\mathfrak{p}_2$	$N(\mathfrak{p}_i) = p^2$

We can use this to say things about how primes factor in extensions of $\mathbb{Q}(\zeta_5)$. For example, in $\mathbb{Q}(\zeta_{55})$ we see that

$$(11) = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^{10}$$

with $f_{\mathfrak{p}_i|p} = 1$.

Exercise 3.6.17. Describe the factorization of the following ideals into prime ideals in $\mathbb{Q}(\zeta_{55})$:

$$(13) \qquad (14) \qquad (5)$$

Exercise 3.6.18. Let ζ_7 be a 7-th root of unity and $K = \mathbb{Q}(\zeta_7)$. Complete the following table describing the decomposition of ideals (p) (with p a prime number) in $\mathcal{O}_K$.

$p \mod 7$	Order of $p \mod m$	Factorization of (p)	Norms
0			
1			
2			
3			
4			
5			
6			

Chapter 4

The ideal class group

Recall that in a number field K, a principal fractional ideal is a fractional ideal of the form $(x) = \{xy | y \in \mathcal{O}_K\}$ for $x \in K$. For example, principal ideals are principal fractional ideals. Note that furthermore, if (x) and (y) are two principal fractional ideals, then $(x)(y) = (xy)$ is also a fractional ideal and moreover, $(x)(x^{-1}) = \mathcal{O}_K$. Thus the set of principal fractional ideals forms a subgroup of J_K (the group of fractional ideal as defined in Proposition 3.3.11). Let P_K denote the subgroup of principal fractional ideals.

Definition 4.0.1. The *class group* of K is defined to be quotient group

$$\mathrm{Cl}_K = \frac{J_K}{P_K}.$$

Its elements are called ideal classes. If $\mathfrak{a}$ is a fractional ideal, we let $[\mathfrak{a}]$ denote its class in Cl_K. We let h_K denote the size of Cl_K (which we will see below is finite), this is called the *class number* of K.

Remark. Note that in the class group, the identity element is given by the class of principal fractional ideals, which we denote by $[1]$ or $[(1)]$.

Furthermore, note that if $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals then

$$[\mathfrak{a}] = [\mathfrak{b}]$$

means that there is some principal fractional ideal (α) such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. So as a SET $[\mathfrak{a}] = \{(x)\mathfrak{a} \mid x \in K\}$.

Note that, $\mathcal{O}_K$ is a PID if and only if Cl_K is trivial. Moreover, since a Dedekind domain is a PID if and only if its a UFD, this means that $\mathcal{O}_K$ is a UFD if and only if Cl_K is trivial. So Cl_K can be thought of measuring how far $\mathcal{O}_K$ is from being a UFD.

Theorem 4.0.2. *Let K be a number field. Then Cl_K is finite.*

To prove this theorem we will make use of the following result, which we will prove later.

Theorem 4.0.3. *Let K be a number field with r_1 real embeddings and r_2 conjugate pairs of complex embeddings. Let $[K:\mathbb{Q}] = n$ and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then there is an element $a \in \mathfrak{a}$ such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta(\mathcal{O}_K)|^{1/2} N(\mathfrak{a})$$

Definition 4.0.4. The quantity $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\Delta(\mathcal{O}_K)|^{1/2}$ is known as the Minkowski bound and we will denote it by M_K.

Now, we have:

Proposition 4.0.5. *Let K be a number field and let C be an ideal class in Cl_K. Then C contains an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that*

$$N(\mathfrak{a}) \leq M_K.$$

Proof. Consider the class C^{-1}. This has a representative which is an ideal $\mathfrak{b}$ of $\mathcal{O}_K$. By Theorem 4.0.3 there is an $x \in \mathfrak{b}$ such that $|N_{K/\mathbb{Q}}(x)| \leq M_K N(\mathfrak{b})$.

Set $\mathfrak{a} = \mathfrak{b}^{-1}(x)$. Then this is in the same class as C since its a multiple of $\mathfrak{b}^{-1}$ by a principal ideal (x). Moreover, since $x \in \mathfrak{b}$ it follows that $\mathfrak{b}^{-1}(x) \subset \mathcal{O}_K$ (recall that $\mathfrak{b}^{-1} = \{y \in K | y\mathfrak{b} \subset \mathcal{O}_K\}$), so $\mathfrak{a}$ is a proper ideal. Now by construction

$$N(\mathfrak{a}) = \frac{|N_{K/\mathbb{Q}}(x)|}{N(\mathfrak{b})} \leq M_K$$

which gives the result. □

Proof of Theorem 4.0.2. By Proposition 4.0.5 each ideal class C in Cl_K must contain an ideal of norm at most M_K. Now Corollary 3.4.10 implies there are only finitely many such ideals. So there are only finitely many ideal classes. □

4.1 Computing class groups

The proof of Theorem 4.0.3 will require some work, so lets first convince ourselves that this theorem is worth all the work. In particular, lets see how we can use it to compute some class groups

Example 4.1.1. Let $i = \sqrt{-1}$. Lets look at $K = \mathbb{Q}(i)$. Using Proposition 2.2.19 we see that $\Delta(\mathcal{O}_K) = -4$. Moreover, K has no real embeddings, so $r_1 = 0$ and $r_2 = 1$. Putting this together we get

$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{4} = \frac{4}{\pi} \approxeq 1.273.$$

Theorem 4.0.3 tells us that each ideal class contains an ideal of norm ≤ 1. But the only ideal of norm 1 is the trivial ideal. So Cl_K is trivial. If follows that $\mathcal{O}_K = \mathbb{Z}[i]$ is a PID.

Exercise 4.1.2. Show that if $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ then $\mathbb{Q}(\sqrt{d})$ has trivial class group and is thus a PID.

Example 4.1.3. Let $K = \mathbb{Q}(\sqrt{-5})$. From Theorem 2.1.11 we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Here again we have $r_1 = 0$, $r_2 = 1$ and $\Delta(\mathcal{O}_K) = -20$. Therefore

$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} = \sqrt{80\pi} < 3$$

This means every class contains an ideal of norm 1 or 2. We know the trivial ideal has norm 1, so lets look at what ideal has norm 2. As we saw in the proof of Corollary 3.4.10, its enough to look at what prime ideals divide 2. By Theorem 3.5.17 we have

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

and therefore $\mathfrak{p}_2 := (2, 1 + \sqrt{-5})$ is the unique ideal of norm 2.

So, this means the class group Cl_K has either 1 or 2 elements, depending of whether or not these two ideals are in the same class, i.e., if $[1] = [\mathfrak{p}_2]$. In other words, is $\mathfrak{p}_2$ a principal ideal (since principal ideals are the things which [1] consists of). If it where principal, then Proposition 3.4.5 would mean that there is some element in $\mathcal{O}_K$ of norm ± 2. Now

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

and its easy to see that this is never equal to ± 2. So $\mathfrak{p}_2$ is not principal and therefore

$$\mathrm{Cl}_K = \{[1], [\mathfrak{p}_2]\}$$

so Cl_K is cyclic of order 2.

Example 4.1.4. Let $K = \mathbb{Q}(\sqrt{-31})$. In this case by Theorem 2.1.11 we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-31}}{2}$, $n = [K : \mathbb{Q}] = 2$ and $r_1 = 0, r_2 = 1$. Lastly, Exercise 2.2.28 gives $\Delta(\mathcal{O}_K) = -31$. This means $M_K = \frac{2}{\pi}\sqrt{31} < 4$.

So we need to find the ideals of norm less than 4. Using Theorem 3.5.17 gives

$$(2) = \mathfrak{p}_2\mathfrak{p}_2' := (2, \frac{1 + \sqrt{-31}}{2})(2, \frac{1 - \sqrt{-31}}{2})$$

with $\mathfrak{p}_2 \neq \mathfrak{p}_2'$, both of which have norm 2. Moreover, we see that (3) is inert in K, so has norm 9.

So the ideals of norm < 4 are $(1), \mathfrak{p}_2, \mathfrak{p}_2'$. We know $\mathfrak{p}_2 \neq \mathfrak{p}_2'$, but this does NOT mean we have $[\mathfrak{p}_2] \neq [\mathfrak{p}_2']$. We need to see whether or not this is the case. We know that $\mathfrak{p}_2\mathfrak{p}_2' = (2)$ which means we have $[\mathfrak{p}_2][\mathfrak{p}_2'] = [(2)] = [1]$

so we have $[\mathfrak{p}_2] = [\mathfrak{p}_2']^{-1}$. Therefore if we had $[\mathfrak{p}_2] = [\mathfrak{p}_2']$ this would mean that $[\mathfrak{p}_2]^2 = [1]$ which means that $\mathfrak{p}_2$ would have to be principal. Can this happen? Assume this is the case, then we have $\mathfrak{p}_2^2 = (\beta)$ for some $\beta \in \mathcal{O}_K$ (its in $\mathcal{O}_K$ and not K since $\mathfrak{p}_2$ is a ideal in $\mathcal{O}_K$ not a fractional ideal). Now, we know that $N(\mathfrak{p}_2) = 2$ (this follows from Corollary 3.5.11). This would mean β has norm 4. Note that the norm of an arbitrary element in $\mathcal{O}_K$ is

$$N_{K/\mathbb{Q}}(x + y\alpha) = x^2 + xy + 8y^2 \qquad x, y \in \mathbb{Z}.$$

Therefore we need to check if this can be equal to 4. Clearly this can happen, and moreover it can only happen if $x = \pm 2$ and $y = 0$. This would mean that we have $\beta = 2$ and therefore

$$\mathfrak{p}_2^2 = (2)$$

but we know that

$$(2) = \mathfrak{p}_2\mathfrak{p}_2'$$

therefore, by uniqueness of factorization and the fact that $\mathfrak{p}_2 \neq \mathfrak{p}_2'$ we see that $\mathfrak{p}_2^2$ cant be principal and therefore $[\mathfrak{p}_2] \neq [\mathfrak{p}_2']$.

It remains to check if $[\mathfrak{p}_2] = [1]$ or $[\mathfrak{p}_2'] = [1]$. Similar to what we did above, we now need to see if there is some element of norm ± 2.

So the question is, can we find x, y which make $x^2 + xy + 8y^2$ this equal to 2. The first thing to note is that $N_{K/\mathbb{Q}}(x + y\alpha) \geq 7y^2$, (to see this, note that $x^2 + xy + y^2 \geq 0$) so we are going to need $y = 0$. This means we would need $x^2 = 2$ which cant happen, therefore $[\mathfrak{p}_2] \neq [1] \neq [\mathfrak{p}_2']$. Thus we have

$$\mathrm{Cl}_K = \{[1], [\mathfrak{p}_2], [\mathfrak{p}_2']\}$$

so its cyclic of order 3. From this we can deduce that $[\mathfrak{p}_2^2] = [\mathfrak{p}_2']$ and $[\mathfrak{p}_2^3] = [1]$ (i.e. $\mathfrak{p}_2^3$ is principal). Lets finish off by writing down the multiplication table for the group:

	$[1]$	$[\mathfrak{p}_2]$	$[\mathfrak{p}_2^2]$
$[1]$	$[1]$	$[\mathfrak{p}_2]$	$[\mathfrak{p}_2^2]$
$[\mathfrak{p}_2]$	$[\mathfrak{p}_2]$	$[\mathfrak{p}_2^2]$	$[1]$
$[\mathfrak{p}_2^2]$	$[\mathfrak{p}_2^2]$	$[1]$	$[\mathfrak{p}_2]$

Example 4.1.5. Lets look at $K = \mathbb{Q}(\sqrt[3]{7})$ and let $\alpha = \sqrt[3]{7}$. The minimal polynomial is clearly $x^3 - 7$ which has discriminant $-1323 = -3^3 \cdot 7^2$. Next, lets check that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$. For this we need to check if any of

$$\frac{x_2\alpha^2 + x_1\alpha + x_0}{3} \qquad \text{or} \qquad \frac{y_2\alpha^2 + y_1\alpha + y_0}{7}$$

can be algebraic integers for $0 \leq x_i \leq 2$, $0 \leq y_i \leq 6$. Since the minimal polynomial is clearly Eisenstein at 7 we know from Lemma 2.2.21 that we

only need to worry about 3. Here is a trick: note that

$$(x+7)^3 - 7$$

is Eisenstein at 3 and at 7 so if β is one of its roots, then $\mathbb{Z}[\beta] = \mathcal{O}_{K'}$ where $K' = \mathbb{Q}(\beta)$, but $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$. Therefore $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$.

Knowing this means we can freely use Theorem 3.5.10. Now, lets calculate the Minkowski bound. In this case $n = 3$, $\Delta(\mathcal{O}_K) = -1323$, and $r_1 = r_2 = 1$. Putting this together we get

$$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{1323} = \frac{56\sqrt{3}}{3\pi} \approxeq 10.3$$

So we need to find all ideals of norm at most 10. So lets factor the ideals given by $2, 3, 5, 7$ using Theorem 3.5.10.

- $x^3 - 7 \equiv (x-1)(x^2+x+1) \mod 2$
- $x^3 - 7 \equiv (x-1)^3 \mod 3$
- $x^3 - 7 \equiv (x-3)(x^2+3x-1) \mod 5$
- $x^3 - 7 \equiv x^3 \mod 7$

From this we deduce

- $(2) = \mathfrak{p}_2\mathfrak{p}_2' = (2, \alpha - 1)(2, \alpha^2 + \alpha + 1)$
- $(3) = \mathfrak{p}_3^3 = (3, \alpha - 1)^3$
- $(5) = \mathfrak{p}_5\mathfrak{p}_5' = (5, \alpha - 3)(5, \alpha^2 + 3\alpha - 1)$
- $(7) = \mathfrak{p}_7^3 = (7, \alpha)^3 = (\alpha)^3$

By Theorem 3.5.7 we know that $N(\mathfrak{p}_i) = p^{f_{\mathfrak{p}_i|p}}$ so if we calculate the residue degrees, we will know the norms of these ideals. But again Theorem 3.5.10 tells us that this is exactly the degrees of the polynomials appearing on the right hand side of each factorization modulo p. So combining this we have:

- $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_2') = 4$
- $N(\mathfrak{p}_3) = 3$
- $N(\mathfrak{p}_5) = 5$ and $N(\mathfrak{p}_5') = 25$
- $N(\mathfrak{p}_7) = 7$

So by combining these ideals we can construct any ideal of norm at most 10. The next question is are these ideals distinct in Cl_K? Lets see if any of them are principal:

Clearly, $(7) = (\alpha)^3$ is principal so this gives the trivial class in the class group. Note that since $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ we have $[\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2']$.

So lets look at the other ideals.

Note that

$$N_{K/\mathbb{Q}}(x + y\alpha + z\alpha^2) = x^3 + 7y^3 + 49z^3 - 21xyz.$$

So, do we have elements of norm $2, 3$ or 5? We'll from the above we see that the norm of an element must be a cube modulo 7. But the only cubes modulo 7 are ± 1. So there are no elements of norm $2, 3, 5$. So these ideals are not principal. So Cl_K is generated by $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5$.

The next question is, do these ideals give distinct classes in Cl_K? First note that $\mathfrak{p}_3^3 = (3)$ therefore $[\mathfrak{p}_3]$ has order 3 in Cl_K (since we already know its not trivial). Note that $N_{K/\mathbb{Q}}(2 + \sqrt[3]{7}) = 15$ and $N_{K/\mathbb{Q}}(-1 + \sqrt[3]{7}) = 6$.

Therefore, since we only have one prime ideal of norm $2, 3$ and 5 we must have

$$(2 + \sqrt[3]{7}) = \mathfrak{p}_3\mathfrak{p}_5 \qquad (-1 + \sqrt[3]{7}) = \mathfrak{p}_3\mathfrak{p}_2$$

thus $[\mathfrak{p}_5][\mathfrak{p}_3] = [1]$ and $[\mathfrak{p}_2][\mathfrak{p}_3] = [1]$ giving $[\mathfrak{p}_5] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2]$. Thus Cl_K is generated by $[\mathfrak{p}_3]$ and is therefore cyclic of order 3. The multiplication table is then

	$[1]$	$[\mathfrak{p}_3]$	$[\mathfrak{p}_3^2]$
$[1]$	$[1]$	$[\mathfrak{p}_3]$	$[\mathfrak{p}_3^2]$
$[\mathfrak{p}_3]$	$[\mathfrak{p}_3]$	$[\mathfrak{p}_3^2]$	$[1]$
$[\mathfrak{p}_3^2]$	$[\mathfrak{p}_3^2]$	$[1]$	$[\mathfrak{p}_3]$

Roughly, the steps for computing a class group of a number field K are as as follows:

Algoritheorem 4.1.6.

1. Find the ring of integers $\mathcal{O}_K$ and the discriminant $\Delta(\mathcal{O}_K)$ (as defined in Definition 2.2.14). As we have seen in the problem sheet, in many cases (but not all) we can calculate the discriminant using Theorem 2.2.25.

2. Find how many real r_1 and complex conjugate r_2 embeddings our number field K has. To do this, you need to write down the embeddings (all $[K : \mathbb{Q}]$ of them) and see how many of them are real or complex. How do you do this quickly? If $K = \mathbb{Q}(\alpha)$ then look at the conjugates of α. With this r_1 will be the number of conjugates of α that are real numbers and r_2 will be half the number conjugates that are complex.

3. Compute the Minkowski bound

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta(\mathcal{O}_K)|^{1/2}$$

where $n = [K : \mathbb{Q}]$.

4. Find all ideals of norm $\leq \lfloor M_K \rfloor$. To do this, look at all the primes p less than $\lfloor M_K \rfloor$ and factor the ideal (p) in $\mathcal{O}_K$ using Corollary 3.5.11, or if we are in a quadratic field, use Theorem 3.5.17 which makes things really quick.

5. After doing this you will have a list of prime ideals $\mathfrak{p}_i$ all with norm $\leq \lfloor M_K \rfloor$. The next step is to see if any of them are trivial in the class group. This means, we need to check if $[\mathfrak{p}_i] = [1]$, in other words is $\mathfrak{p}_i$ principal?[a] How does one do this? Well if $\mathfrak{p}_i$ was principal, it would be generated by an element β such that $|N_{K/\mathbb{Q}}(\beta)| = N((\beta)) = N(\mathfrak{p}_i)$. Now check if this gives a contradiction by looking at the possibilities for the norm of β.

6. After this we now have a possibly smaller list of prime ideals, all of which we know are not principal. The next question is to check if they are distinct from one another. In other words, if $[\mathfrak{p}] = [\mathfrak{q}]$. In general this might be difficult, but in the examples above, we have seen some tricks how to do this.

7. Once this is all done, we have our final set of generators, and by this point we know the size of the group and it should be easy to write down the multiplication table for the class group.

[a] Warning: Just because Corollary 3.5.11 says $\mathfrak{p}_i = (p, \textit{something})$ doesn't mean this ideal can't be principal.

Chapter 5

Solving Diophantine equations

Now, one of the big problems we have is that in general $\mathcal{O}_K$ isn't a unique factorization domain, but in the cases when it is, we can use this to solve Diophantine equations. For example, consider

$$x^3 = y^2 + 2.$$

Lets try and find its integer solutions, without using any of the machinery we have developed. This will serve as an example going forwards.

To do this, lets factorize this equation in the ring $\mathbb{Z}[\sqrt{-2}]$ which is a UFD. We then get

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Next, we see that the factors on the right hand side must be coprime: any common factor would be a factor of $2\sqrt{-2}$, meaning that x is even, so x^3 is divisible by 8. But $y^2 + 2$ is never a multiple of 4 so this cannot happen. So, up to a unit we have

$$y + \sqrt{-2} = \pm\beta^3,$$

since -1 is a cube, wlog we take the $+$ sign. If we let $\beta = u + v\sqrt{-2}$ then

$$y + \sqrt{-2} = u^3 + 3u^2v\sqrt{-2} - 6uv^2 - 2v^3\sqrt{-2}.$$

Now, lets equate coefficients, to get

$$y = u^3 - 6uv^2 \qquad 1 = 3u^2v - 2v^3.$$

This implies that $v|1$, so $v = \pm 1$, which in turn means

$$y = u^3 - 6u \qquad 1 = v(3u^2 - 2).$$

Again the second equation implies $u = \pm 1$ and $v = 1$, which we can use to

see that $y = \pm 5$. Therefore the solutions are $(x, y) = (3, 5)$ or $(3, -5)$.

In order to go further, lets recall the following results form the problem sheets:

Lemma 5.0.1. *Let K be a number field and $\alpha, \beta \in \mathcal{O}_K$. If $(\alpha) = (\beta)$ then there is $u \in \mathcal{O}_K^\times$ such that $\alpha = u\beta$.*

Lemma 5.0.2. *Let R be a Dedekind domain and $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideals such that*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}^3$$

and suppose $\mathfrak{a}, \mathfrak{b}$ are coprime. Then there exist ideals $\mathfrak{e}, \mathfrak{d}$ such that

$$\mathfrak{a} = \mathfrak{e}^3 \qquad \mathfrak{b} = \mathfrak{d}^3 \qquad \mathfrak{e}\mathfrak{d} = \mathfrak{c}$$

Using this we can prove the following:

Example 5.0.3. Lets find all the integral solutions to $x^3 = y^2 + 74$ assuming that $h_K = 10$ where $K = \mathbb{Q}(\sqrt{-74})$. The trick here is to factor this expression in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-74}]$, but before that, note the following:

Assume $x, y \in \mathbb{Z}$ are solutions. First thing to note is that y cannot be even, since this would mean x is even. But then $x^3 - y^2 \equiv 0 \pmod 4$ but $4 \nmid 74$. So x, y must be odd. Similarly, we see that x, y must be coprime, since if p divides both then p^2 divided $x^3 - y^2 = 74$ but 74 is square-free.

Now lets look at the ideals. We have

$$(x)^3 = (y - \sqrt{-74})(y + \sqrt{-74})$$

as ideals. Now, are the two ideals on the right hand side coprime?

If $\mathfrak{p}$ divided them both, we would have

$$y - \sqrt{-74} \equiv 0 \mod \mathfrak{p} \qquad y + \sqrt{-74} \equiv 0 \mod \mathfrak{p}$$

and therefore $\mathfrak{p}$ divides their sum, so $\mathfrak{p}|(2y)$. Looking at the other side of the equation, we see that $\mathfrak{p}|(x)$. We know x is odd, so $\mathfrak{p}$ cannot divide (2) (if it did, then we would have $(x) = \mathfrak{p}_2\mathfrak{a}$ where $\mathfrak{a}$ is some ideal and $\mathfrak{p}_2^2 = (2)$ (as can be seen from Theorem 3.5.11), but this means $N(\mathfrak{p}_2) = 2$ which would mean $N((x)) = |N_{K/\mathbb{Q}}(x)| = x^2$ is even, which can't happen as x is odd). So we have $\mathfrak{p} \mid (y)$ and $\mathfrak{p}|(x)$ but we know x, y are coprime (as integers, which means their ideals are also coprime). Therefore we cannot have a $\mathfrak{p}$ dividing both factors on the right, so they are coprime.

Now, using Lemma 5.0.2 we must have $(y - \sqrt{-74}) = \mathfrak{a}^3$ and $(y + \sqrt{-74}) = \mathfrak{b}^3$ with $\mathfrak{a}\mathfrak{b} = (x)$. Note this means $[\mathfrak{a}^3] = [1] = [\mathfrak{b}^3]$. But note the class group has size 10 so we cant have ideal classes of order 3. Therefore $\mathfrak{a}, \mathfrak{b}$ are principal. So let $\mathfrak{a} = (a + b\sqrt{-74})$.

Then we have

$$(y - \sqrt{-74}) = (a + b\sqrt{-74})^3.$$

Using Lemma 5.0.1 and Exercise 3.1.5 we see that up to ± 1 we have

$$y - \sqrt{-74} = a^3 + 3a^2b\sqrt{-74} - 3 \cdot 74b^2a - b^3 74\sqrt{-74}.$$

Equating each side we have

$$y = a^3 - 3b^2a74 \qquad 3a^2b - b^3 74 = -1.$$

The second equation implies $b \mid -1$ and therefore $b = \pm 1$. This then gives $a = \pm 5$. Substituting, it then follows that $y = \pm 985$ and $x = 99$ are the only solutions.

Example 5.0.4. Lets do another example. Lets show that $x^3 = y^2 + 5$ has no integral solutions. We saw in Example 4.1.3 that the class group in this case has size 2.

Now, as we did before, lets start by assuming x, y are integer solutions to this equation. If x was even then $y^2 + 5 \equiv 0 \mod 4$ which would make -1 a square modulo 4 which can't happen, so x cannot be even. Similarly, x, y must be coprime since if p divided both of them, $p^2 | (x^3 - y^2)$ meaning $p^2 \mid 5$ which is a contradiction.

Ok, with this done, lets now factor this in $\mathcal{O}_K$ as ideals where $K = \mathbb{Q}(\sqrt{-5})$. We have

$$(x)^3 = (y - \sqrt{-5})(y + \sqrt{-5}).$$

Next, lets see if the terms on the right are coprime. If a prime ideal $\mathfrak{p}$ divided both of them, then $\mathfrak{p}$ would divide their sum $(2y)$ so $\mathfrak{p} \mid (2y)$. Looking at the left of the equation we see $\mathfrak{p}$ divides (x) and therefore as in the previous example, since x is odd, we cant have $\mathfrak{p}$ dividing (2). But then $\mathfrak{p} \mid (y)$ and $\mathfrak{p} \mid (x)$ but this also cant happen as x, y are coprime.

So, using Lemma 5.0.2 we see that we must have $\mathfrak{a}^3 = (y - \sqrt{-5})$ and $\mathfrak{b}^3 = (y + \sqrt{-5})$ for some ideals $\mathfrak{a}, \mathfrak{b}$. Now, if we think of what the class group having size 2 says, it means that in particular, we cannot have any non-principal ideals whose cube is principal, since this would give an element of order 3 in the class group. Therefore, both $\mathfrak{a}$ and $\mathfrak{b}$ must be themselves principal.

So lets just look as $\mathfrak{a} = a + b\sqrt{-5}$. We must have

$$(a + b\sqrt{-5})^3 = (y - \sqrt{-5})$$

which means there is some unit $u \in \mathcal{O}_K^\times$ such that

$$u(a + b\sqrt{-5})^3 = y - \sqrt{-5}$$

now as elements, ot just ideals. Since $\mathcal{O}_K^\times = \{\pm 1\}$ as we saw in sheet 6, wlog we can assume

$$(a + b\sqrt{-5})^3 = y - \sqrt{-5}$$

(since -1 is a cube). If we expand out we get

$$a^3 + 3a^2b\sqrt{-5} - 15b^2a - b^3 5\sqrt{-5} = y - \sqrt{-5}.$$

Now, equating each side we have $y = a^3 - 15ab^2$ and $-1 = 3a^2b - 5b^3$. The second equation tells us $b \mid -1$ so $b = \pm 1$. If we now, substitute this back into the first equation we get $-1 = 3a^2 - 5$ which has no solution for $a \in \mathbb{Z}$. So $x^3 = y^2 + 5$ has no integer solutions.

Exercise 5.0.5. Find all integer solutions to $x^3 = y^2 + 13$. (You will need to fist compute a class group for this)

Chapter 6

Geometry of numbers

NON-EXAMINABLE CHAPTER

In this chapter we will develop the machinery necessary for proving Theorem 4.0.3.

Definition 6.0.1. A lattice $\Lambda \subset \mathbb{R}^n$ is a subgroup (under addition) generated by n linearly independent vectors.

Remark 6.0.2. If Λ is a lattice in $\mathbb{R}^n$ then

$$\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$$

where e_i are linearly independent vectors over $\mathbb{R}$, i.e. there does not exist $r_i \in \mathbb{R}$ such that $\sum_i r_i e_i = 0$. So its not enough that the e_i be independent over $\mathbb{Q}$, so $(1, 0)$ and $(\pi, 0)$ do not generate a lattice in $\mathbb{R}^2$.

Definition 6.0.3. If $\Lambda \subset \mathbb{R}^n$ is a lattice generated by e_i then

$$P(\Lambda) = \{x \in \mathbb{R}^n \mid x = \sum_i r_i e_i, 0 \leq r_i < 1\}$$

is called the *fundamental domain* of Λ.

Note that if we $\lambda \in \Lambda$ and let $P(\Lambda) + \lambda = \{x + \lambda \mid x \in P(\Lambda)\}$ then

$$\mathbb{R}^n = \bigcup_{\lambda \in \Lambda} P(\Lambda) + \lambda.$$

Lemma 6.0.4. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then the volume of $P(\Lambda)$ does not depend on the choice of basis of Λ. Moreover, if $\{e_i\}$ is the basis, then*

$$\mathrm{Vol}(P(\Lambda)) = |\det(e_1, e_2, \ldots, e_n)|$$

(here the right hand side is the determinant of the matrix whose columns are given by the e_i).

Proof. The second statement is just linear algebra, so we will only prove the first. Let f_i denote a second basis of Λ and let $M(e_i), M(f_i)$ denote the matrices whose columns are given by e_i and f_i respectively. Then

$$M(e_i) = M(f_i)A$$

where A is a $n \times n$ matrix with entries in $\mathbb{Z}$. Similarly ,

$$M(f_i) = M(e_i)B.$$

Therefore,

$$M(e_i) = M(e_i)BA$$

Now, since $M(e_i), M(f_i)$ are non-degenerate we have $BA = I$ and therefore $\det(A) = \pm 1$. □

Lemma 6.0.5. *Let $S \subset \mathbb{R}^n$ be a measurable set (i.e. $\mathrm{Vol}(S) = |\int \cdots \int_S dx_1 \cdots dx_n|$ exists) and Λ is a lattice. Then if $\mathrm{Vol}(S) > \mathrm{Vol}(P(\Lambda))$ then there exist $x, y \in S$ with $x \neq y$ such that $x - y \in \Lambda$.*

Furthermore, if S is compact, then the same conclusion holds if $\mathrm{Vol}(S) \geq \mathrm{Vol}(P(\Lambda))$.

Proof. We begin by writing

$$\mathbb{R}^n = \bigcup_{\lambda \in \Lambda} (P(\Lambda) + \lambda) \qquad \text{(as a disjoint union)}$$

therefore

$$S = \mathbb{R}^n \cap S = \bigcup_{\lambda \in \Lambda} (P(\Lambda) + \lambda) \cap S \qquad \text{(as a disjoint union).}$$

From this it follows that

$$\mathrm{Vol}(S) = \sum_{\lambda \in \Lambda} \mathrm{Vol}\left((P(\Lambda) + \lambda) \cap S\right) = \sum_{\lambda \in \Lambda} \mathrm{Vol}\left((P(\Lambda)) \cap (S - \lambda)\right).$$

Now, if $P(\Lambda) \cap (S - \lambda)$ are all disjoint, then the sum their volume is $< \mathrm{Vol}(P(\Lambda))$ contradicting our assumption that $\mathrm{Vol}(S) > \mathrm{Vol}(P(\Lambda))$. Therefore two of these sets meet, say $P(\Lambda) \cap (S - \lambda)$ and $P(\Lambda) \cap (S - \mu)$ (with $\lambda \neq \mu$) and therefore we have some $x - \lambda = y - \mu$ giving $x - y = \lambda - \mu \in \Lambda$.

For the second part, if S is now compact with $\mathrm{Vol}(S) \geq \mathrm{Vol}(P(\Lambda))$. Then let $S' = (1 + \epsilon)S$ such that $\mathrm{Vol}(S') > \mathrm{Vol}(P(\Lambda))$. Then by the above, we can find $x, y \in S'$ such that $x - y \in \Lambda$. Let Λ_ϵ denote the set of such x, y.

Note that if $\epsilon' \leq \epsilon$ then $\Lambda_{\epsilon'} \subset \Lambda_\epsilon$. Therefore $\cap_{\epsilon > 0} \Lambda_\epsilon \neq \emptyset$. So let $\lambda \in \cap_{\epsilon > 0} \Lambda_\epsilon$. We claim that $\lambda = x - y$ for some $x, y \in S$. Take $\epsilon = 1/n$ and write $\lambda = x_n - y_n$ with $x_n, y_n \in (1 + 1/n)S$ (which we can do by the first part). Since $x_n, y_n \in 2S$ for all n and $2S$ is compact. So (x_n, y_n) form a

sequence in a compact set, so there is a subsequence that converges to a point (x, y). Since $x_n, y_n \in (1 + 1/n)S$ we have $x \in \bigcap(1 + 1/n)S = S$ and similarly $y \in S$. Since $\lambda = x_n - y_n$ for all n we see that in the limit $\lambda = x - y$ which then gives the result.

□

Definition 6.0.6. A subset $S \subset \mathbb{R}^n$ is called:

1. Convex if whenever $x, y \in S$ then the line segment joining x and y is also contained in S.

2. Centrally symmetric if whenever $x \in S$ then $-x \in S$.

Lemma 6.0.7 (Minkowski's convex body lemma)**.** *Let S be a compact, convex and centrally symmetric subset of $\mathbb{R}^n$ and Λ a lattice. If*

$$\mathrm{Vol}(S) \geq 2^n \,\mathrm{Vol}(P(\Lambda))$$

then S contains a point of Λ.

Proof. Consider the set

$$\frac{1}{2}S = \{\frac{1}{2}x \mid x \in S\}.$$

Then $\mathrm{Vol}(\frac{1}{2}S) \geq \mathrm{Vol}(P(\Lambda))$. So by Lemma 6.0.5 there exist $x, y \in \frac{1}{2}S$ such that $x - y \in \Lambda$. We claim that $x - y \in S$.

Note that $2x, 2y \in S$. Now, since S is centrally symmetric, we have $-2y \in S$. Furthermore, since S is convex,

$$\frac{1}{2}(2x - 2y) \in S.$$

Thus $x - y \in S$. □

Let now apply this to number theory. Let K be a number field with $[K : \mathbb{Q}] = n$. Then we have n embeddings of $K \hookrightarrow \mathbb{C}$ and in fact if we let r_1 be the number of real embeddings and r_2 the number of complex conjugate embeddings then we have:

Definition 6.0.8. Let K be a number field with r_1 real embeddings and r_2 complex conjugate pairs of embeddings, then the canonical embedding is

$$\Theta : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n$$

given by

$$\begin{aligned} x \mapsto &(\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \\ &\mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x)), \Im\sigma_{r_1+1}(x) \end{aligned}$$

where the first r_1 of the σ_i are the real embeddings then rest are the complex ones and $\Re, \Im$ denote real and imaginary parts.

Example 6.0.9. 1. Let $K = \mathbb{Q}(\sqrt{-d})$ with d a square-free positive integer. Then the embedding is given by sending $x + y\sqrt{-d}$ to

$$(x, y\sqrt{-d}) \in \mathbb{R}^2.$$

2. If $K = \mathbb{Q}(\sqrt{d})$ with d a square-free positive integer. Then the embedding is given by sending $x + y\sqrt{d}$ to

$$(x + y\sqrt{d}, x - y\sqrt{d}) \in \mathbb{R}^2.$$

Proposition 6.0.10. *Let K be a number field with $[K : \mathbb{Q}] = n$ and $\Theta : K \to \mathbb{R}^n$ is canonical embedding. Then $\Theta(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ and if $P = P(\Theta(\mathcal{O}_K))$ then*

$$\mathrm{Vol}(P) = 2^{-r_2}\sqrt{|\Delta(\mathcal{O}_K)|}$$

where r_2 is the number of complex conjugate pairs of embeddings.

Furthermore, if $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal, then $\Lambda_\mathfrak{a} := \Theta(\mathfrak{a})$ is a sublattice of $\Theta(\mathcal{O}_K)$. Moreover,

$$\mathrm{Vol}(P(\Lambda_\mathfrak{a})) = 2^{-r_2}\sqrt{|\Delta(\mathcal{O}_K)|}N(\mathfrak{a})$$

Proof. Let $\{e_i\}$ be an integral basis of $\mathcal{O}_K$. Then

$$\Theta(\mathcal{O}_K) = \left\{ \sum_i \lambda_i \Theta(e_i) \mid \lambda_i \in \mathbb{Z} \right\}.$$

We want to compute

$$|\det(M(\Theta))| := |\det(\Theta(e_1), \ldots, \Theta(e_n))|.$$

By definition

$$\Theta(e_i) = (\sigma_1(e_i), \ldots, \sigma_{r_1}(e_i), \Re\sigma_{r_1+1}(e_i), \Im\sigma_{r_1+1}(e_i), \ldots, \Re\sigma_{r_1+r_2}(e_i)), \Im\sigma_{r_1+1}(e_i))^T.$$

Now, note that

$$\Re\sigma_{r_1+1}(e_i) = \frac{1}{2}(\sigma_{r_1+1}(e_i) + \overline{\sigma}_{r_1+1}(e_i)) \qquad \Im\sigma_{r_1+1}(e_i) = \frac{1}{2\sqrt{-1}}(\sigma_{r_1+1}(e_i) - \overline{\sigma}_{r_1+1}(e_i)).$$

Using this we have

$$|\det(M(\Theta))| = \left(\frac{1}{2}\right)^{2r_2} \left| \det \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(e_1) & \cdots & \sigma_{r_1}(e_n) \\ (\sigma_{r_1+1}(e_1) + \overline{\sigma}_{r_1+1}(e_1)) & \cdots & (\sigma_{r_1+1}(e_n) + \overline{\sigma}_{r_1+1}(e_n)) \\ (\sigma_{r_1+1}(e_1) - \overline{\sigma}_{r_1+1}(e_1)) & \cdots & (\sigma_{r_1+1}(e_n) - \overline{\sigma}_{r_1+1}(e_n)) \\ \vdots & & \vdots \end{pmatrix} \right|$$

Doing simple row operations we can transform this into

$$\left(\frac{1}{2}\right)^{2r_2} \left| \det \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(e_1) & \cdots & \sigma_{r_1}(e_n) \\ (\sigma_{r_1+1}(e_1) + \overline{\sigma}_{r_1+1}(e_1)) & \cdots & (\sigma_{r_1+1}(e_n) + \overline{\sigma}_{r_1+1}(e_n)) \\ 2\sigma_{r_1+1}(e_1) & \cdots & 2\sigma_{r_1+1}(e_n) \\ \vdots & & \vdots \end{pmatrix} \right|$$

and then to

$$\left(\frac{1}{2}\right)^{r_2} \left| \det \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_1(e_n) \\ \vdots & & \vdots \\ \sigma_{r_1}(e_1) & \cdots & \sigma_{r_1}(e_n) \\ \overline{\sigma}_{r_1+1}(e_1) & \cdots & \overline{\sigma}_{r_1+1}(e_n)) \\ \sigma_{r_1+1}(e_1) & \cdots & \sigma_{r_1+1}(e_n) \\ \vdots & & \vdots \end{pmatrix} \right|$$

Notice the power of $1/2$ has changed. But now, if we look back at Proposition 2.2.16 we see that this is simply

$$2^{-r_2}\sqrt{|\Delta(\mathcal{O}_K)|}.$$

Lets now look at the sublattice $\Lambda_{\mathfrak{a}}$. Note that as additive abelian groups we have $\mathcal{O}_K \cong \mathbb{Z}^n$ and $\mathfrak{a}$ is a subgroup of index $N(\mathfrak{a})$. Since Θ is injective we have $\Lambda_{\mathfrak{a}}$ is a subgroup of $\Theta(\mathcal{O}_K)$ of index $N(\mathfrak{a})$. From this it follows that

$$P(\Lambda_{\mathfrak{a}}) = N(\mathfrak{a})P(\Theta(\mathcal{O}_K))$$

(compare this with the proof of Proposition 3.4.5) from which the result follows. □

Lemma 6.0.11. *Let $S_t \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ be a subset given by points*

$(y_i, z_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ *such that*

$$\sum_i |y_i| + \sum_j |z_j| \leq t.$$

Then S is compact, convex and centrally symmetric and moreover

$$\mathrm{Vol}(S) = \frac{2^{r_1} t^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}.$$

Proof. S is closed and bounded and therefore is compact. S is also clearly symmetric. For $\lambda \in (0,1)$ we have

$$\begin{aligned}\sum_i |\lambda y_i + (1-\lambda) y_i'| + 2\sum_j |\lambda z_i + (1-\lambda) z_i'| &\leq \sum_i |\lambda y_i| + |(1-\lambda) y_i'| + 2\sum_j |\lambda z_i| + |(1-\lambda) z_i'| \\ &= \lambda \sum_i |y_i| + (1-\lambda) \sum_j |z_i| + \lambda \sum_i |y_i'| + (1-\lambda) \sum_j |z_i'| \\ &\leq \lambda + (1-\lambda) = 1\end{aligned}$$

From this it follows that S is also convex.

Note that if $r_1 = 1$ and r_2 then $S = [-t, t]$ which has volume (in this case length) 2. Similarly, if $r_1 = 0$ and $r_2 = 1$ then S is just a ball in $\mathbb{C}$ of radius $\frac{1}{2}$ so has volume (in this case area) $\frac{\pi t^2}{4}$. We will prove the formula for the volume by induction on (r_1, r_2).

Assume we know the formula for (r_1, r_2). Lets look at the $(r_1 + 1, r_2)$ case. Here the set is given by points such that

$$\sum_{i=1}^{r_1+1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq 1$$

which can be rewritten as

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq t - |y|$$

where $y = y_{r_1+1}$. This set has volume

$$\int_0^1 \frac{2^{r_1} t^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} (t-|y|)^n dy = \frac{2^{r_1} t^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} \int_0^1 (t-y)^n dy = \frac{2^{r_1+1} t^{n+1}}{n+1!} \left(\frac{\pi}{4}\right)^{r_2}.$$

A slightly more involved, yet still elementary proof gives the $(r_1, r_2 + 1)$ and thus the result. □

Finally, with this we can finally prove Theorem 4.0.3

Theorem. *Let K be a number field with r_1 real embeddings and r_2 conjugate*

pairs of complex embeddings. Let $[K:\mathbb{Q}] = n$ *and let* $\mathfrak{a}$ *be an ideal of* $\mathcal{O}_K$*. Then there is an element* $a \in \mathfrak{a}$ *such that*

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}|\Delta(\mathcal{O}_K)|^{1/2}N(\mathfrak{a})$$

Proof. Let S_t be as in Lemma 6.0.11 and pick t such that

$$\mathrm{Vol}(S_t) = 2^n \,\mathrm{Vol}(P(\Lambda_{\mathfrak{a}}))$$

i.e. such that

$$t^n = 2^{n-r_1}\pi^{-r_2}n!\sqrt{|\Delta(\mathcal{O}_k)|}N(\mathfrak{a}) \tag{1}$$

Then by Lemma 6.0.7 there is an $a \in \mathfrak{a}$ such that $\Theta(a) \in S_t$. Then we have

$$|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r_1}|\sigma_i(a)| \prod_{j=r_1+1}^{r_1+r_2}|\sigma_j(a)|^2$$

(here we use Proposition 1.7.6). Now, using the arithmetic-geometric mean inequality

$$\sqrt[n]{z_1 \dots z_n} \leq \frac{1}{n}\sum_i z_i$$

for z_i positive real numbers, we have

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(a)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(a)|\right)^n \leq \frac{t^n}{n!}$$

by definition of S_t. Using (1) then gives the result.

□

Bibliography

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.