Algebraic Number Theory

Term 2, 2018–19

Martin Orr

1. Introduction

Gaussian integers.

The simplest example of what we will study in Algebraic Number Theory is the Gaussian integers

$$\{a + bi : a, b \in \mathbb{Z}\}.$$

If you did Introduction to Number Theory, you will have seen these before, but whether you have or not we will see them in this course as a special case of a much broader theory.

The key points about the Gaussian integers:

(1) We can describe the irreducible Gaussian integers in terms of the ordinary prime numbers (depending on whether a prime is 1 or 3 mod 4).
(2) Every Gaussian integer can be uniquely factorised as a product of irreducible Gaussian integers.

Gaussian integers are an example of algebraic integers i.e. numbers which are a root of a monic polynomial with integer coefficients. Algebraic Number Theory is about doing number theory with other algebraic integers, for example describing the primes in a ring of algebraic integers or deciding whether a ring of algebraic integers has unique factorisation.

Usually, a ring of algebraic integers does not have unique factorisation. We will define factorisation of ideals, instead of elements of the ring, and see that this restores the uniqueness of prime factorisations. We will also define the "class group" of an algebraic number ring, which measures how far it is away from having unique factorisation of elements.

Practical information about the course.

The course involves a lot of down-to-earth calculation with examples e.g. determining how a prime factorises in a number field or computing the class group of a number field. There is also a good deal of theory underpinning these calculations. Lectures will focus on the theory; example sheets and support classes on the examples.

Assignments – four pieces, best 3 of 4 will count (15% of module mark)
Deadlines: Friday 2pm in weeks 3, 6, 8, 10
Example sheets and lecture capture will be available on Moodle.
My email address: `martin.orr@warwick.ac.uk`
Office hours: Fri 2-3, Zeeman C2.11

Course outline.

(1) Number fields and embeddings
(2) Rings of integers
(3) Ideals and factorisation
(4) Class group
(5) Dirichlet's unit theorem

Related courses.

MA249 Algebra 2 – prerequisite. Rings, fields, ideals and factorisation of polynomials will be used throughout this course. We will also need quotient rings and the First Isomorphism Theorem for rings. Revise this!

MA257 Introduction to Number Theory – not strictly a prerequisite, but it will provide very helpful background.

MA3D5 Galois Theory – There is some overlap in the first 1–2 weeks, with various definitions and lemmas related to field extensions. We shall go through these again in this course.

Field extensions.

Our main object of study will be number fields. A number field is defined as a finite extension of the field $\mathbb{Q}$. Let's unpack this definition.

Definition. Let K and L be fields. If K is a subfield of L, we say that L/K is a **field extension** (often, we will just call it an **extension**).

e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}(i)$ but not $\mathbb{R}/\mathbb{Q}(i)$
where $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$.

Definition. Let L/K be a field extension and $\alpha \in L$. We say that α is **algebraic over** K if there exists a non-zero polynomial $f \in K[X]$ such that $f(\alpha) = 0$.

e.g. $i \in \mathbb{C}$, $\sqrt[4]{7} \in \mathbb{R}$ are algebraic over $\mathbb{Q}$
πi is algebraic over $\mathbb{R}$ but not algebraic over $\mathbb{Q}$

Lemma 1. *Let α be algebraic over K.*

*(i) There exists a unique monic polynomial $\mu_{K,\alpha}(X) \in K[X]$ of smallest degree such that $\mu_{K,\alpha}(\alpha) = 0$. (**monic** means that the leading coefficient is 1 – this forces the polynomial to be non-zero.)*
(ii) If $f \in K[X]$ satisfies $f(\alpha) = 0$, then $\mu_{K,\alpha}$ divides f.
(iii) $\mu_{K,\alpha}$ is irreducible.
(iv) If $f \in K[X]$ is monic and irreducible and $f(\alpha) = 0$, then $f = \mu_{K,\alpha}$.

Proof.

(i)+(ii) Let $I = \{f \in K[X] : f(\alpha) = 0\}$. One can check that this is an ideal in $K[X]$.

Recall from Algebra 2 that $K[X]$ is a PID (principal ideal domain) so $I = (\mu_{K,\alpha})$ for some $\mu_{K,\alpha} \in K[X]$.

Since α is algebraic over K, $I \neq \{0\}$ so $\mu_{K,\alpha} \neq 0$. Therefore we can multiply $\mu_{K,\alpha}$ by a scalar to ensure that it is monic.

Clearly $\mu_{K,\alpha}$ has the smallest degree of all polynomials in I, and it satisfies (ii) by the definition of a principal ideal.

(ii) implies that there is no other monic polynomial in I with the same degree as $\mu_{K,\alpha}$, i.e. it is unique.

(iii) Suppose $\mu_{K,\alpha} = fg$. Then $f(\alpha)g(\alpha) = 0$. Since L is a field, either $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, $f(\alpha) = 0$. By (ii), $\mu_{K,\alpha}$ divides f so g must be a constant. Thus $\mu_{K,\alpha}$ is irreducible.

(iv) Consequence of (ii). □

Definition. The polynomial $\mu_{K,\alpha}$ from Lemma 1 is called the **minimal polynomial** of α over K.

We will write μ_α instead of $\mu_{K,\alpha}$ if the base field K is clear from the context.

But! K matters for determining the minimal polynomial! e.g. $\alpha = i + \sqrt{2} \in \mathbb{C}$.

- Over $K = \mathbb{C}$: the minimal polynomial is $\mu_{\mathbb{C},\alpha}(X) = X - \alpha$.
- Over $K = \mathbb{R}$: $\alpha \notin \mathbb{R}$, so the minimal polynomial has degree > 1. A calculation shows that $\mu_{\mathbb{R},\alpha}(X) = X^2 - 2\sqrt{2}X + 3$.

Question. What is the minimal polynomial of $\alpha = i + \sqrt{2}$ over $\mathbb{Q}$?

2. Algebraic extensions

Example from last time.

- Over $K = \mathbb{R}$: We have
$$(\alpha - \sqrt{2})^2 = -1 \quad \text{so} \quad \alpha^2 - 2\sqrt{2}\alpha + 3 = 0.$$
$X^2 - 2\sqrt{2}X + 3 \in \mathbb{R}[X]$ is irreducible over $\mathbb{R}$ because it is a quadratic with no real roots. So $\mu_{\mathbb{R},\alpha}(X) = X^2 - 2\sqrt{2}X + 3$.
- Over $K = \mathbb{Q}$: α is algebraic over $\mathbb{Q}$ because
$$(\alpha^2 + 3)^2 = (2\sqrt{2}\alpha)^2 = 8\alpha^2 \quad \text{so} \quad \alpha^4 - 2\alpha^2 + 9 = 0.$$
One can check that $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$, so this is $\mu_{\mathbb{Q},\alpha}$. We will see a quicker proof later (avoiding checking irreducibility by hand).

Definition. Let $\alpha \in L$ be algebraic over K. The **degree of α over K** is the degree of the polynomial $\mu_{K,\alpha}$.

e.g. $i + \sqrt{2}$ has degree 1 over $\mathbb{C}$, 2 over $\mathbb{R}$, 4 over $\mathbb{Q}$.

Field generation.

Definition. Let L/K be a field extension and let S be a subset of L. The **extension of K generated by** S is the smallest subfield of L containing both K and S.

This means: the intersection of all subfields of L which contain both K and S. Check that this intersection is a field!

Written $K(S)$. If S is finite set $\{\alpha_1, \ldots, \alpha_n\}$, we write $K(\alpha_1, \ldots, \alpha_n)$ as an abbreviation for $K(\{\alpha_1, \ldots, \alpha_n\})$.

e.g. $\mathbb{C} = \mathbb{R}(i)$

If d is a non-square rational number, then
$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$
This is a field because
$$(a + b\sqrt{d})(c + e\sqrt{d}) = (ac + bed) + (ae + bc)\sqrt{d}$$
and
$$(a + b\sqrt{d})^{-1} = (a - b\sqrt{d})/(a^2 - db^2)$$
(the denominator is non-zero because d is not the square of a rational number).

But! $\mathbb{Q}(\sqrt[3]{d}) \neq \{a + b\sqrt[3]{d} : a, b \in \mathbb{Q}\}$ because this is not closed under multiplication. We will soon see how to write down a basis for $\mathbb{Q}(\sqrt[3]{d})$.

In general, $K(S)$ is the set of everything of the form $f(\alpha_1, \ldots, \alpha_r)/g(\beta_1, \ldots, \beta_s)$ where f, g are polynomials (in any number of variables) with coefficients in K, $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in S$ and $g(\beta_1, \ldots, \beta_s) \neq 0$.

Algebraic and finite extensions.

Definition. An extension L/K is **algebraic** if every $\alpha \in L$ is algebraic over K.

e.g. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is algebraic since $a + b\sqrt{d}$ is a root of $(X-a)^2 - b^2 d \in \mathbb{Q}[X]$.
$\mathbb{R}/\mathbb{Q}$ is not algebraic.

Definition. If L/K is a field extension, then L is a K-vector space. The **degree** of L/K, written $[L:K]$, is the dimension of L as a K-vector space.

Definition. L/K is a **finite extension** if its degree is finite.

e.g. $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}] = 2, \quad [\mathbb{C}:\mathbb{R}] = 2.$
$\mathbb{Q}(\pi)/\mathbb{Q}$ has infinite degree, even though it is generated by the finite set $\{\pi\}$, because $1, \pi, \pi^2, \ldots$ are $\mathbb{Q}$-linearly independent.

Lemma 2. *If L/K is a finite extension, then it is an algebraic extension.*

Proof. Let $m = [L:K] < \infty$. Let $\alpha \in L$. Then $1, \alpha, \ldots, \alpha^m$ are $m+1$ elements in a K-vector space of dimension m, so they are K-linearly dependent. In other words, there exist $\lambda_0, \ldots, \lambda_m \in K$, not all zero, such that

$$\lambda_0 + \lambda_1 \alpha + \cdots + \lambda_m \alpha^m = 0.$$

Thus α is the root of the polynomial $\lambda_0 + \lambda_1 X + \cdots + \lambda_m X^m \in K[X]$, so it is algebraic over K. □

The converse is false: the field of all algebraic numbers in $\mathbb{C}$ is an algebraic extension of $\mathbb{Q}$, but not a finite extension of $\mathbb{Q}$ (though we have not proved that this is a field yet).

Tower law.

Often we build field extensions by stacking one on top of another. The following theorem tells us how to calculate the degree of such an extension.

Theorem (Tower Law)**.** *Let M/L and L/K be two finite field extensions. Then M/K is also a finite extension, and*

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

Proof. Let $r = [L:K]$ and $s = [M:L]$. Let $\{\ell_1, \ldots, \ell_r\}$ be a K-basis for L and let $\{m_1, \ldots, m_s\}$ be an L-basis for M.

One can check that $\{l_i m_j : 1 \le i \le r, 1 \le j \le s\}$ is a K-basis for M. □

e.g. $M = \mathbb{Q}(\alpha)$ where $\alpha = i + \sqrt{2}, \quad L = \mathbb{Q}(\sqrt{2}), \quad K = \mathbb{Q}$
We saw that

$$\sqrt{2} = \frac{\alpha^2 + 3}{2\alpha}$$

so $L \subseteq M$.

Now $M = L(\alpha)$. To prove this: certainly L and α are both contained in M, so $L(\alpha) \subseteq M$. Furthermore, $L(\alpha)$ is a field which contains $\mathbb{Q}$ and α, so the definition of $\mathbb{Q}(\alpha)$ tells us that $L(\alpha) \supseteq \mathbb{Q}(\alpha) = M$. Thus $L(\alpha) = M$.

In fact, $L(\alpha) = L(i)$ because $i = \alpha - \sqrt{2}$ and $\sqrt{2} \in L$ (this is slightly simpler than the argument I gave in the lecture, using the quadratic formula). Note that $i \notin L$ because $L \subseteq \mathbb{R}$. We can show that $[L(i) : L] = 2$ for the same reason as $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Thus we get $[M : L] = 2$.

We also have $[L : K] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

So the Tower Law tells us that $[M : K] = 2 \times 2 = 4$.

The fact that $\mu_{\mathbb{Q},\alpha}$ has degree 4 is not a coincidence! We will see how to relate these facts (and thereby prove that $\mu_{\mathbb{Q},\alpha}$ has degree 4) in the next lecture.

3. Simple extensions and number fields

Simple extensions.

Definition. An extension L/K is **simple** if $L = K(\alpha)$ for a *single* element $\alpha \in L$.

Note that a simple extension need not be finite, e.g. $\mathbb{Q}(\pi)/\mathbb{Q}$. But if it is algebraic, then it is finite and we can describe the extension in terms of the minimal polynomial of α:

Theorem 3. *Let α be algebraic over K, with minimal polynomial $\mu_\alpha \in K[X]$. Let $n = \deg(\mu_\alpha)$. Then:*

(1) $K(\alpha)$ is isomorphic as a ring to $K[X]/(\mu_\alpha)$. More precisely, the following is a well defined isomorphism $K[X]/(\mu_\alpha) \to K(\alpha)$:

$$f(X) + (\mu_\alpha) \mapsto f(\alpha).$$

(2) $K(\alpha)$ has K-basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$.
$[K(\alpha) : K] = n$.

Proof. (1) Define $\phi\colon K[X] \to K(\alpha)$ by $\phi(f(X)) = f(\alpha)$.
One can check that this is a ring homomorphism.
From the proof of Lemma 1, we see that

$$\ker(\phi) = \{f \in K[X] : f(\alpha) = 0\} = (\mu_\alpha).$$

Hence by the first isomorphism theorem, ϕ induces an isomorphism $K[X]/(\mu_\alpha) \to \mathrm{im}(\phi)$. We just have to check that $\mathrm{im}(\phi) = K(\alpha)$.

Step 1. First we prove that $1, \alpha, \ldots, \alpha^{n-1}$ span $\mathrm{im}(\phi)$ as a K-vector space.
For any $\beta \in \mathrm{im}(\phi)$, we have $\beta = \phi(f)$ for some $f \in K[X]$. By the division algorithm for polynomials, we can write

$$f = q\mu_\alpha + r$$

where $q, r \in K[X]$ and $\deg(r) < \det(\mu_\alpha)$. Then

$$\beta = f(\alpha) = r(\alpha) = c_0 + c_1\alpha + \cdots + c_s\alpha^s$$

where $c_0, c_1, \ldots, c_s \in K$ and $s = \deg(r) < n$. Thus β is in the span of $1, \alpha, \ldots, \alpha^{n-1}$.

Step 2. We show that $\mathrm{im}(\phi)$ is a field. This is just one of many possible proofs.
We know that $\mathrm{im}(\phi)$ is a ring, so we just have to show that every $x \in \mathrm{im}(\phi) \setminus \{0\}$ has a multiplicative inverse in $\mathrm{im}(\phi)$.
Given $x \in \mathrm{im}(\phi) \setminus \{0\}$, define a K-linear map $m_x\colon \mathrm{im}(\phi) \to \mathrm{im}(\phi)$ by

$$m_x(y) = xy.$$

This is injective because $\mathrm{im}(\phi) \subseteq K(\alpha)$ which is a field.
Therefore by the rank-nullity theorem, m_x is surjective (this uses the fact that $\mathrm{im}(\phi)$, is finite-dimensional as a K-vector space, which follows from Step 1). Therefore there exists $y \in \mathrm{im}(\phi)$ such that $m_x(y) = 1$ i.e. $y = 1/x$.
Thus $\mathrm{im}(\phi)$ is a field.

Conclusion of (1). $\mathrm{im}(\phi)$ contains K and $\alpha = \phi(X)$, so by the definition of $K(\alpha)$, $K(\alpha) \subseteq \mathrm{im}(\phi)$. But also $\mathrm{im}(\phi) \subseteq K(\alpha)$. Thus $\mathrm{im}(\phi) = K(\alpha)$.

(2) We saw in Step 1 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $\mathrm{im}(\phi) = K(\alpha)$ as a K-vector space. We just have to show that $1, \alpha, \ldots, \alpha^{n-1}$ are K-linearly independ

Suppose we have $b_0, \ldots, b_{n-1} \in K$ such that

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

Then $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$ is a polynomial in $K[X]$ such that $g(\alpha) = 0$ and $\deg(g) \leq n-1 < \deg(\mu_\alpha)$ so the definition of minimal polynomial forces $g \equiv 0$ i.e. $b_0 = b_1 = \cdots = b_{n-1}$. □

e.g. We can immediately read off that $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{d})$ (as we saw already).

If $d \in \mathbb{Q}$ is not a cube, then $X^3 - d$ is irreducible so it is the minimal polynomial of $\sqrt[3]{d}$. So $[\mathbb{Q}(\sqrt[3]{d}) : \mathbb{Q}] = 3$ and

$$\mathbb{Q}(\sqrt[3]{d}) = \{a + b\sqrt[3]{d} + c\Big(\sqrt[3]{d}\Big)^2 : a, b, c \in \mathbb{Q}\}.$$

Returning to the example from the previous lecture: $\alpha = i + \sqrt{2}$, $M = \mathbb{Q}(\alpha)$. Using the Tower Law, we proved that $[M : \mathbb{Q}] = 4$. Therefore Theorem 3 tells us that $\deg(\mu_{\mathbb{Q},\alpha}) = 4$.

We also saw that α is a root of the polynomial $g(X) = X^4 - 2X^2 + 9$. Hence $\mu_{\mathbb{Q},\alpha} = g$ and g is irreducible over $\mathbb{Q}$ (by Lemma 1).

Theorem 3 tells us that a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ is given by

$$\{1, \alpha, \alpha^2, \alpha^3\} = \{1, \sqrt{2} + i, 1 + 2\sqrt{2}i, -\sqrt{2} + 5i\}.$$

We can get a different $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ from the proof of the Tower Law. Indeed, $\mathbb{Q}(\sqrt{2})$ has a $\mathbb{Q}$-basis $\{1, \sqrt{2}\}$ while $\mathbb{Q}(\alpha)$ has a $\mathbb{Q}(\sqrt{2})$-basis $\{1, i\}$ (follows from the argument with the quadratic formula). Thus the proof of the Tower Law gives us the following $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$:

$$\{1, \sqrt{2}, i, i\sqrt{2}\}.$$

Number fields.

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

Lemma 4. *Let K be a number field and let L/K be a finite extension. Then L is also a number field.*

Proof. This follows from the Tower Law. □

Definition. An **algebraic number** is an element of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$.

Lemma 5. *If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers, then $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is a number field.*

Proof. Let $K_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ for $1 \leq i \leq n$. We prove that K_i is a number field by induction on i.

The base case is that $K_0 = \mathbb{Q}$ is a number field.

For $i \geq 1$: Since α_i is an algebraic number, it has a minimal polynomial $\mu_{\mathbb{Q},\alpha_i}$. We have $\mu_{\mathbb{Q},\alpha_i}(X) \in \mathbb{Q}[X] \subseteq K_{i-1}[X]$, so α_i is algebraic over K_{i-1}. Hence by Theorem 3, $K_i = K_{i-1}(\alpha_i)$ is a finite extension of K_{i-1}. By induction, K_{i-1} is a number field, so Lemma 4 tells us that K_i is a number field. □

This gives us a way to construct lots of number fields, of which we have already seen several examples.

There is the following converse.

Lemma 6. *If K is a number field, then K is isomorphic to $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some algebraic numbers $\alpha_1, \ldots, \alpha_n$.*

It is easy to show that $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$ for some $\beta_1, \ldots, \beta_n$ which are algebraic elements of the extension $K/\mathbb{Q}$. But the definition of algebraic numbers requires them to be in $\mathbb{C}$. So the hard part of the theorem is showing that every number field K can be embedded in $\mathbb{C}$, even if it was constructed by some abstract method which had nothing to do with $\mathbb{C}$.

4. Number fields and algebraic numbers

Lemma 6. *If K is a number field, then K is isomorphic to $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for some algebraic numbers $\alpha_1, \ldots, \alpha_n$.*

In particular, every number field is isomorphic to a subfield of $\mathbb{C}$.

Proof. Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Q}$-basis for K. Then $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$. By Lemma 2, $\beta_1, \ldots, \beta_n$ are algebraic elements of the extension $K/\mathbb{Q}$.

Let $K_i = \mathbb{Q}(\beta_1, \ldots, \beta_i)$. We shall prove by induction that K_i is isomorphic to a field of the form $L_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic numbers (in particular, $L_i \subseteq \mathbb{C}$).

Base case: $K_0 = \mathbb{Q}$. There is nothing to prove.

For $i \geq 1$: We have $K_i = K_{i-1}(\beta_i)$. Because β_i is algebraic over $\mathbb{Q}$, it is also algebraic over K_{i-1} ($\mu_{\mathbb{Q},\alpha_i} \in \mathbb{Q}[X] \subseteq K_{i-1}[X]$). Let μ_i be the minimal polynomial of α_i over K_{i-1}.

By induction, there is an isomorphism $\sigma_{i-1} \colon K_{i-1} \to L_{i-1} = \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}) \subseteq \mathbb{C}$. Let $\nu_i \in L_{i-1}[X]$ be the polynomial obtained by applying σ_{i-1} to the coefficients of μ_i. Then we can think of ν_i as a polynomial over $\mathbb{C}$, and it is non-constant. By the Fundamental Theorem of Algebra, ν_i has a root $\alpha_i \in \mathbb{C}$. Since $\nu_i(\alpha_i) = 0$ and ν_i is monic and irreducible over L_{i-1}, ν_i is the minimal polynomial of α_i over L_{i-1}.

By Theorem 3 (twice), we have isomorphisms

$$K_i = K_{i-1}(\beta_i) \cong K_{i-1}[X]/(\mu_i) \cong L_{i-1}[X]/(\nu_i) \cong L_{i-1}(\alpha_i) = L(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i).$$

□

The field of algebraic numbers.

Lemma 7. *Let $\alpha, \beta \in \mathbb{C}$ be algebraic numbers. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β (if $\beta \neq 0$) are also algebraic numbers.*

Proof. $\mathbb{Q}(\alpha, \beta)$ is a number field by Lemma 5. Hence every element of $\mathbb{Q}(\alpha, \beta)$ is an algebraic number. But $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and α/β are all elements of $\mathbb{Q}(\alpha, \beta)$. □

This is quite incredible! In a simple example, we had to do some work before to show that $i + \sqrt{2}$ was algebraic (and more to find its minimal polynomial). For example, if α is a root of

$$X^{10000} + 5X^{73} + 2X^8 - 6X - 22$$

and β is a root of

$$X^{99999} + 777X^2 - 5$$

then there is a polynomial with rational coefficients which has $\alpha + \beta$ as a root. Finding this polynomial is a hard computation problem (can you guess what its degree might be?) but the theorem tells us that it exists.

Definition. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic number}\}$.

Corollary. $\overline{\mathbb{Q}}$ *is a field.*

Proof. Immediate corollary of Lemma 7. □

Question. Why is $\overline{\mathbb{Q}}$ not a number field?

Quadratic fields.

The simplest example of a number field is $\mathbb{Q}$. Indeed $\mathbb{Q}$ is the only number field of degree 1. (Why?)

The next simplest examples are quadratic fields. We will use these a lot in this course.

Definition. A **quadratic field** is a number field of degree 2.

We have already seen some examples: if $d \in \mathbb{Q}$ is not the square of a rational number, then $\mathbb{Q}(\sqrt{d})$ is a quadratic field. There is some redundancy here e.g.

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{18}) = \mathbb{Q}(\sqrt{1/2}) = \mathbb{Q}(\sqrt{9/8}) = \cdots$$

We can eliminate this by insisting that d is always a square-free integer.

Definition. $d \in \mathbb{Z}$ is **square-free** if it is not divisible by m^2 for any integer $m > 1$. (Note: 1 is square-free, 0 is not.)

In fact all quadratic fields have this form.

Proposition 8. *Let K be a quadratic field. Then $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 1$.*

Proof. Since $[K : \mathbb{Q}] = 2 > 1$, we can pick $\alpha \in K$ which is not in $\mathbb{Q}$. Then $\{1, \alpha, \alpha^2\}$ are linearly dependent over $\mathbb{Q}$ i.e. there exist $a, b, c \in \mathbb{Q}$ such that

$$a\alpha^2 + b\alpha + c = 0.$$

If $a = 0$ then $\alpha \in \mathbb{Q}$ giving a contradiction. Thus $a \neq 0$ and the quadratic formula gives

$$\alpha = \frac{-b \pm \sqrt{\Delta}}{2a}, \text{ where } \Delta = b^2 - 4ac \in \mathbb{Q}. \qquad (*)$$

Rearranging this, we see that $\sqrt{\Delta} = \pm(2a\alpha + b) \in K$.

Now write

$$\Delta = \frac{u}{v} = \frac{1}{v^2}uv$$

where $u, v \in \mathbb{Z}$. Then $uv \in \mathbb{Z}$ and $\sqrt{uv} = v\sqrt{\Delta} \in K$.

Finally we can write $uv = x^2y$ where x is an integer and u is a square-free integer (use the prime factorisation of uv). We get $\sqrt{y} = \frac{1}{x}\sqrt{uv} \in K$.

Note that $\sqrt{\Delta} \notin \mathbb{Q}$ (otherwise (*) would force $\alpha \in \mathbb{Q}$). Hence $\sqrt{y} \notin \mathbb{Q}$. So $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] = 2$.

By the Tower Law,

$$[K : \mathbb{Q}(\sqrt{y})] = [K : \mathbb{Q}]/[\mathbb{Q}(\sqrt{y}) : \mathbb{Q}] = 1$$

so $K = \mathbb{Q}(\sqrt{y})$. □

Furthermore, the square-free integer d such that $K = \mathbb{Q}(\sqrt{d})$ is unique – this is on example sheet 1.

Note that Proposition 8 does not generalise to higher-degree fields. For example a cubic field (i.e. a field of degree 3) does not have to have the form $\mathbb{Q}(\sqrt[3]{d})$. We will need some more theory before proving this.

5. Primitive element theorem, norm and trace

Cyclotomic fields.

Definition. Let n be a positive integer and let $\zeta_n = \exp(2\pi i/n)$. We call $\mathbb{Q}(\zeta_n)$ the **n-th cyclotomic field**.

Lemma 9. *If $n = p$ is prime, then the minimal polynomial of ζ_p is $X^{p-1} + X^{p-2} + \cdots + X + 1$ and hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.*

Proof. This is on the example sheet. You will need to use Eisenstein's criterion from Algebra 2.

(Note that there was a typo on the first version of the example sheet: it said $X^p + \cdots + 1$ where it should be $X^{p-1} + \cdots + 1$.) □

If n is not a prime, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ (the Euler φ-function). There is no general formula for the minimal polynomial of ζ_n when n is not prime, so this is harder to prove.

Primitive element theorem.

The primitive element theorem tells us that every extension of number fields is a simple extension. For example, we saw that $\mathbb{Q}(i, \sqrt{2})$ is a simple extension of $\mathbb{Q}$: it is equal to $\mathbb{Q}(i + \sqrt{2})$.

Lemma 10. *Let K be a number field contained in $\mathbb{C}$. Let $f \in K[X]$ be an irreducible polynomial over K of degree d. Then f has d distinct roots in $\mathbb{C}$.*

Proof. By the Fundamental Theorem of Algebra, we know that f has d roots in $\mathbb{C}$ counted with multiplicity. The problem is to show that f has no repeated roots.

Suppose for contradiction that $\alpha \in \mathbb{C}$ is a repeated root of f.

Let f' denote the derivative of f, and note that it also has coefficients in K. Since α is a repeated root of f, it is also a root of f'. Hence $X - \alpha$ is a common factor of f and f' in $\mathbb{C}[X]$. It follows that $\mathrm{HCF}(f, f')$ is a non-constant polynomial.

Now $\mathrm{HCF}(f, f')$ has coefficients in K (we can calculate it using Euclid's algorithm, and f, f' both have coefficients in K). But $\mathrm{HCF}(f, f')$ is a factor of f, it is non-constant, and

$$\deg(\mathrm{HCF}(f, f')) \leq \deg(f') = \deg(f) - 1.$$

This contradicts the hypothesis that f is irreducible over K. □

The name of the lemma is because it is related to the notion of "separable field extension" in Galois theory.

Note that Lemma 10 works only because number fields have characteristic zero – this is needed to ensure that $f' \neq 0$. (Over a field of characteristic p, the derivative of X^p is 0. Then the argument about the degree of the HCF would break down.) If you have done Galois theory, this is related to the idea of a separable extension (and the fact that every extension in characteristic zero is separable).

In order to prove the Primitive Element Theorem, we start with an extension generated by adjoining two elements. We can then build up other extensions by

induction on the number of elements we need to adjoin. The idea for $K(\alpha, \beta)$ is motivated by the example of $\mathbb{Q}(i + \sqrt{2})$: we try adjoining a linear combination of α and β. Just taking $\alpha + \beta$ does not always work so we have to be a little cleverer about which linear combination we choose.

Lemma. *Let L/K be an extension of number fields such that $K = L(\alpha, \beta)$. Then there is some $\gamma \in L$ such that $L = K(\gamma)$.*

Proof. Thanks to Lemma 6, we may assume that L (and hence also K) is a subfield of $\mathbb{C}$, allowing us to apply Lemma 10.

Let f, g be the minimal polynomials of α, β respectively over K. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f and let $\beta_1, \ldots, \beta_n$ be the roots of g in $\mathbb{C}$. We may label the roots so that $\alpha_1 = \alpha$ and $\beta_1 = \beta$.

For any i and any $j \neq 1$, the equation

$$\alpha + c\beta = \alpha_i + c\beta_j$$

has a unique solution $c = c_{ij} \in \mathbb{C}$ (this is just solving a linear equation for c). Since K is infinite, we can choose $c \in K$ different from all the c_{ij} (there are only finitely many c_{ij} because $1 \leq i \leq m$, $2 \leq j \leq n$). Thus

$$\alpha + c\beta \neq \alpha_i + c\beta_j \tag{$\dagger$}$$

for all i and for all $j \neq 1$.

Let $\gamma = \alpha + c\beta$. We shall show that $L = K(\gamma)$. It is enough to show that $\beta \in K(\gamma)$ because then $\alpha = \gamma - c\beta \in K(\gamma)$ (because $c \in K$).

Consider the polynomial $h(X) = f(\gamma - cX) \in K(\gamma)[X]$. Observe that $h(\beta) = f(\alpha) = 0$.

If β' is any root of h other than β, we have $f(\gamma - c\beta') = 0$ and so $\gamma - c\beta' = \alpha_i$ for some i. The fact that c does not satisfy any of the equations ($\dagger$) implies that $\beta' \neq \beta_j$ for any $j = 2, \ldots, n$.

Thus the only common root of g and h is β. Looking at the factorisations of g and h in $\mathbb{C}[X]$, we conclude that $\mathrm{HCF}(g, h) = (X - \beta)^r$ for some r.

Because g is a minimal polynomial, it is irreducible over K. Therefore by Lemma 10, g has no repeated roots in $\mathbb{C}$, so in fact we must have $\mathrm{HCF}(g, h) = X - \beta$.

Since g and h both have coefficients in $K(\gamma)$, so does $\mathrm{HCF}(g, h)$. Thus $\beta \in K(\gamma)$. □

Theorem 11 (Primitive Element Theorem)**.** *Let L/K be an extension of number fields. Then there is some $\gamma \in L$ such that $L = K(\gamma)$.*

Proof. Write $L = K(S)$ for some finite set S (this is always possible: for example, let S be a K-basis of L). Induct on the size of S, applying the previous lemma to reduce the size by 1 repeatedly. □

Norm and trace.

Let K be a number field. We define two functions $K \to \mathbb{Q}$ which can be helpful in transforming questions about elements of K into questions about rational numbers.

Recall that K is $\mathbb{Q}$-vector space and for any α we can define a $\mathbb{Q}$-linear map $m_{K,\alpha}\colon K \to K$ by $m_{K,\alpha}(\beta) = \alpha\beta$.

Definition. The **trace** of α is $\mathrm{Tr}(m_{K,\alpha})$ – written $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.

The **norm** of α is $\det(m_{K,\alpha})$ – written $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$.

The notation (subscript $K/\mathbb{Q}$) reminds us that $\mathrm{Tr}_{K/\mathbb{Q}}$ and $\mathrm{Nm}_{K/\mathbb{Q}}$ are functions $K \to \mathbb{Q}$.

Note that you could generalise this: instead of always having $\mathbb{Q}$ as the base field, you could define $\mathrm{Tr}_{L/K}$ and $\mathrm{Nm}_{L/K}$ for any extension of number fields L/K. These would be functions $L \to K$. The definition is essentially the same but we won't need this generalisation in the course.

e.g. Let $K = \mathbb{Q}(\sqrt{d})$. We want to work out the norm and trace of $\alpha = a + b\sqrt{d}$. To do this, we will write $m_{K,\alpha}\colon K \to K$ as a matrix with respect to the basis $\{1, \sqrt{d}\}$. We get

$$m_{K,\alpha}(1) = a \cdot 1 + b \cdot \sqrt{d}, \quad m_{K,\alpha}(\sqrt{d}) = bd \cdot 1 + a \cdot \sqrt{d}$$

so the matrix of $m_{K,\alpha}$ (with respect to this basis) is

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

Thus

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

6. Characteristic polynomial, embeddings

Lemma 12. *The trace is additive and the norm is multiplicative. In other words, for all α, β in K, we have*

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

Proof. Observe that $m_{K,\alpha+\beta} = m_{K,\alpha} + m_{K,\beta}$ and $m_{K,\alpha\beta} = m_{K,\alpha}m_{K,\beta}$. Thus the lemma follows from the properties of trace and determinant of linear maps. □

Characteristic polynomials.

Let V be a $\mathbb{Q}$-vector space and let $f\colon V \to V$ be a $\mathbb{Q}$-linear map. Recall that the **characteristic polynomial** of f is the polynomial

$$\chi_f(X) = \det(XI - f) \in \mathbb{Q}[X].$$

This polynomial is monic of degree $n = \dim(V)$. We can read off the determinant and trace of f from the coefficients of the characteristic polynomial: if $\chi_f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, then

$$\mathrm{Tr}(f) = -a_{n-1}, \quad \det(f) = (-1)^n a_0. \tag{*}$$

According to the Cayley–Hamilton theorem, $\chi_f(f) = 0$.

Consequently we can read off the norm and trace of $\alpha \in K$ from the characteristic polynomial of $m_{K,\alpha}$, which we denote $\chi_{K,\alpha}$.

Lemma 13. *Let $K = \mathbb{Q}(\alpha)$. Then the characteristic polynomial of $m_{K,\alpha}\colon K \to K$ is equal to the minimal polynomial of α over $\mathbb{Q}$.*

Proof. Let $\chi_{K,\alpha}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ denote the characteristic polynomial of $m_{K,\alpha}$. By the Cayley–Hamilton theorem, $\chi_{K,\alpha}(m_{K,\alpha}) = 0$. In other words,

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

(in the ring of $\mathbb{Q}$-linear maps $K \to K$). Applying both sides to $1 \in K$, and noting that $m_{K,\alpha}^i(1) = \alpha^i$, we get

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

or in other words $\chi_{K,\alpha}(\alpha) = 0$.

Furthermore $\chi_{K,\alpha} \in \mathbb{Q}[X]$, $\chi_{K,\alpha}$ is monic and $\deg(\chi_{K,\alpha}) = [K:\mathbb{Q}] = \deg(\mu_{\mathbb{Q},\alpha})$ (the latter holds because $K = \mathbb{Q}(\alpha)$). Hence by Lemma 1, $\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha}$. □

Note that the characteristic polynomial $\chi_{K,\alpha}$ depends on K as well as α. The following lemma tells us how.

Lemma 14. *Let L/K be an extension of number fields and let $\alpha \in K$. Let $\chi_{K,\alpha}$ and $\chi_{L,\alpha}$ be the characteristic polynomials of $m_{K,\alpha}\colon K \to K$ and $m_{L,\alpha}\colon L \to L$ respectively. Then*

$$\chi_{L,\alpha} = \chi_{K,\alpha}^{[L:K]}.$$

Proof. Let $\theta_1, \ldots, \theta_r$ be a $\mathbb{Q}$-basis for K and let $M_{K,\alpha}$ be the matrix of $m_{K,\alpha}$ with respect to this basis. Let $\phi_1, \ldots, \phi_s$ be a K-basis for L. By the Tower Law, a $\mathbb{Q}$-basis for L is given by

$$\theta_1\phi_1, \theta_2\phi_1, \ldots, \theta_r\phi_1,\ \theta_1\phi_2, \ldots, \theta_2\phi_r,\ \ldots,\ \theta_1\phi_s, \ldots, \theta_r\phi_s.$$

We can calculate that

$$m_{L,\alpha}(\theta_i\phi_j) = \alpha\theta_i\phi_j = m_{K,\alpha}(\theta_i) \cdot \phi_j.$$

Thus $m_{L,\alpha}(\theta_i\phi_j)$ lies in the $\mathbb{Q}$-space spanned by $\theta_1\phi_j, \ldots, \theta_r\phi_j$ (for fixed j), and the coefficients needed to express $m_{L,\alpha}(\theta_i\phi_j)$ as a combination of these basis vectors are the same as the coefficients needed to express $m_{K,\alpha}(\theta_i)$ as a combination of $\theta_1, \ldots, \theta_r$; in other words, they are entries of $M_{K,\alpha}$.

Consequently the matrix for $m_{L,\alpha}$ with respect to the basis $\{\theta_i\phi_j\}$ is block diagonal with blocks that are copies of $M_{K,\alpha}$:

$$M_{L,\alpha} = \begin{pmatrix} M_{K,\alpha} & 0 & \cdots & 0 \\ 0 & M_{K,\alpha} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & M_{K,\alpha} \end{pmatrix}$$

There is one block for each ϕ_j i.e. s blocks. This is consistent with the fact that $M_{K,\alpha}$ is an $s \times s$ matrix and $M_{L,\alpha}$ is an $rs \times rs$ matrix.

The characterstic polynomial of a block diagonal matrix is the product of the characteristic polynomials of the blocks (because the same thing holds for determinants). Thus

$$\chi_{L,\alpha}(X) = \chi_{K,\alpha}(X)^s. \qquad \square$$

Corollary 15. *Let L/K be an extension of number fields. If $\alpha \in K$, then*

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = [L : K]\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha),$$
$$\mathrm{Nm}_{L/\mathbb{Q}}(\alpha) = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)^{[L:K]}.$$

Proof. Let $r = [K : \mathbb{Q}]$ and $s = [L : K]$. Write

$$\chi_{K,\alpha}(x) = X^r + a_{r-1}X^{r-1} + \cdots + a_1X + a_0,$$
$$\chi_{L,\alpha}(x) = X^{rs} + b_{rs-1}X^{rs-1} + \cdots + b_1X + b_0.$$

By Lemma 14, we have $\chi_{L,\alpha} = \chi_{K,\alpha}^s$. Expanding this out and comparing coefficients, we see that

$$b_{rs-1} = sa_{r-1}, \quad b_0 = a_0^s.$$

The corollary now follows from (*). $\square$

By combining Lemmas 13 and 14, we can work out the characteristic polynomial of an arbitrary $\alpha \in K$ in terms of the minimal polynomial:

$$\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha}^{[K:\mathbb{Q}(\alpha)]}$$

It can be useful to apply this in reverse: by choosing a basis for K, we can work out the characteristic polynomial $\chi_{K,\alpha}$. This must be a power of an irreducible polynomial, which will be the minimal polynomial of α.

Embeddings of number fields.

Definition. Let K be a number field. An **embedding** of K is a field homomorphism $\sigma\colon K \to \mathbb{C}$.

Lemma 16. *Any homomorphism of fields $\sigma\colon K \to L$ is injective.*

Proof. The kernel of σ is an ideal in K. Since K is a field, its only ideals are 0 and K. But $\ker(\sigma) \neq K$ because $\sigma(1) = 1 \neq 0$. □

Lemma 17. *Let K be a number field and let $\sigma\colon K \to \mathbb{C}$ be an embedding. Then $\sigma(a) = a$ for all $a \in \mathbb{Q}$.*

Proof. By the definition of a ring homomorphism, $\sigma(1) = 1$ and $\sigma(0) = 0$. For any positive integer n, we have

$$\sigma(n) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = n.$$

Furthermore $\sigma(-n) = -\sigma(n) = n$.

Finally, any rational number can be written as m/n where $m, n \in \mathbb{Z}$, and $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$. □

7. Extending embeddings

Embeddings of quadratic fields.

We showed last time that any embedding of a number field must restrict to the identity on $\mathbb{Q}$. Hence, there is exactly one embedding $\sigma\colon \mathbb{Q} \to \mathbb{C}$, namely the inclusion.

What are the embeddings of a quadratic field $\mathbb{Q}(\sqrt{d})$? Thanks to Lemma 17, every embedding $\sigma\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ must satisfy

$$\sigma(a + b\sqrt{d}) = a + b\sigma(\sqrt{d}).$$

Hence the embedding is fully determined once we know $\sigma(\sqrt{d})$. This must satisfy

$$\sigma(\sqrt{d})^2 = d$$

so there are two choices: $\sigma(\sqrt{d}) = \sqrt{d}$ or $\sigma(\sqrt{d}) = -\sqrt{d}$. Thus we get two possible embeddings:

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}), \quad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

We should really check that both of these are field homomorphisms. This is not hard by calculation, or it follows from Proposition 18 which we are about to prove.

Extending embeddings of number fields.

Definition. Let L/K be an extension of number fields. Let $\sigma\colon K \to \mathbb{C}$ and $\tau\colon L \to \mathbb{C}$ be embeddings. We say that τ **extends** σ if $\tau_{|K} = \sigma$.

In order to state the next proposition about extensions of embeddings, we need to introduce a piece of notation: If $\sigma\colon K \to L$ is a field homomorphism, then it induces an injective ring homomorphism $K[X] \to L[X]$ which we also call σ, defined by

$$\sigma(a_0 + a_1X + \cdots + a_nX^n) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n.$$

Proposition 18. *Let L/K be an extension of number fields of degree n. Let $\sigma\colon K \to \mathbb{C}$ be an embedding.*

1. *There are exactly n embeddings $L \to \mathbb{C}$ which extend σ.*
2. *Suppose that $L = K(\alpha)$. Let μ_α be the minimal polynomial of α over K and let $\alpha_1, \ldots, \alpha_n$ be the roots of $\sigma(\mu_\alpha)$ in $\mathbb{C}$. Then for each $i = 1, \ldots, n$, there is a unique embedding $\tau_i\colon L \to \mathbb{C}$ extending σ such that $\tau_i(\alpha) = \alpha_i$.*

Proof. By the Primitive Element Theorem (Theorem 11), we can write $L = K(\alpha)$. Let μ_α be the minimal polynomial of α over K

By Theorem 3, $\deg(\mu_\alpha) = n$. Since μ_α is irreducible over K, by Lemma 10 tells us that $\sigma(\mu_\alpha)$ has n distinct roots in $\mathbb{C}$, which we call $\alpha_1, \ldots, \alpha_n$. Thus we can use (2) to prove (1).

To prove (2) we have to prove two things:

(i) For each $i = 1, \ldots, n$, there is an embedding $\tau_i\colon L \to \mathbb{C}$ extending σ such that $\tau_i(\alpha) = \alpha_i$.
(ii) For each $i = 1, \ldots, n$, there is only one such embedding.

To deduce (1), we have to prove:

(iii) There are no other embeddings $L \to \mathbb{C}$ extending σ, except those coming from (2).

Proof of (i). Same method as the proof of Lemma 6. We have $\sigma(\mu_\alpha) \in \sigma(K)[X]$, $\sigma(\mu_\alpha)$ is monic and $\sigma(K)$-irreducible and $\sigma(\mu_\alpha)(\alpha_i) = 0$. Hence $\sigma(\mu_\alpha)$ is the minimal polynomial of α_i over $\sigma(K)$. Therefore, using Theorem 3 twice, we have

$$L = K(\alpha) \cong K[X]/(\mu_\alpha) \cong \sigma(K)[X]/(\sigma(\mu_\alpha)) \cong \sigma(K)(\alpha_i) \subseteq \mathbb{C}. \qquad (*)$$

The resulting homomorphism $L \to \mathbb{C}$ extends σ (because the middle isomorphism in (*) is given by applying σ to the coefficients of the polynomials) and maps α to α_i (because the isomorphism from Theorem 3 maps α to X the first time, then X to α_i the second time), so this is the desired τ_i.

Proof of (ii). Let $\tau\colon L \to \mathbb{C}$ be an embedding extending σ. Thank to Theorem 3, we can write any $\beta \in L$ in the form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

for some $b_0, b_1, \ldots, b_{n-1} \in K$. Then

$$\tau(\beta) = \sigma(b_0) + \sigma(b_1)\tau(\alpha) + \cdots + \sigma(b_{n-1})\tau(\alpha)^{n-1}$$

Thus knowing $\tau(\alpha) = \alpha_i$ uniquely determines τ.

Proof of (iii). Let $\tau\colon L \to \mathbb{C}$ be an embedding extending σ. We have

$$\sigma(\mu_\alpha)(\tau(\alpha)) = \tau(\mu_\alpha)(\tau(\alpha)) = \tau(\mu_\alpha(\alpha)) = \tau(0) = 0.$$

Thus $\tau(\alpha)$ is a root of $\sigma(\mu_\alpha)$. In other words, it is one of $\alpha_1, \ldots, \alpha_n$. □

Corollary. *A number field L has exactly $[L : \mathbb{Q}]$ embeddings.*

Proof. By Lemma 17, every embedding $L \to \mathbb{C}$ extends the unique embedding $\mathbb{Q} \to \mathbb{C}$. So it suffices to apply Proposition 18 to the extension $L/\mathbb{Q}$. □

Real and complex embeddings.

Definition. Let $\sigma\colon K \to \mathbb{C}$ be an embedding of a number field. We say that σ is a **real embedding** if $\sigma(K) \subseteq \mathbb{R}$ and σ is a **complex embedding** if $\sigma(K) \not\subseteq \mathbb{R}$.

Note that complex embeddings come in conjugate pairs: if σ is an embedding of K, then

$$\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)}$$

is also an embedding of K (where the bar denotes complex conjugation). If σ is a complex embedding, then σ and $\bar{\sigma}$ are different. If σ is a real embedding, then $\sigma = \bar{\sigma}$.

Definition. The **signature** of K is (r, s) where r = number of real embeddings of K, s = number of *pairs of* complex embeddings of K.

e.g. Signature of a real quadratic field is $(2, 0)$
Signature of an imaginary quadratic field is $(0, 1)$

8. Conjugates, algebraic integers

Signature.

Let K be a number field with signature (r, s).

Counting up all the embeddings and applying the Corollary from the previous lecture, we see that $[K : \mathbb{Q}] = r + 2s$. (We have to multiply s by 2 because it counts pairs of embeddings.)

We often label the embeddings a $\sigma_1, \ldots, \sigma_r$ (the real embeddings), $\sigma_{r+1}, \ldots, \sigma_{r+s}$, $\overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$ (the complex embeddings).

Conjugates.

Definition. Let α be an algebraic number. The **conjugates** of α are the roots (in $\mathbb{C}$) of $\mu_{\mathbb{Q},\alpha}$, the minimal polynomial of α over $\mathbb{Q}$.

By Proposition 18, the conjugates of α are $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ where $\sigma_1, \ldots, \sigma_n$ are the embeddings of $\mathbb{Q}(\alpha)$.

We can express the norm and trace in terms of the conjugates of α.

Lemma 19. *Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings $K \to \mathbb{C}$. Then for any $\alpha \in K$,*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$
$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Proof. First suppose that $K = \mathbb{Q}(\alpha)$. Let $\mu_\alpha(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. By Lemma 13, $\mu_\alpha = \chi_{K,\alpha} =$ the characteristic polynomial of $m_{K,\alpha}$. The roots of $\chi_{K,\alpha}$ are the eigenvalues of $m_{K,\alpha}$.

Thus the eigenvalues of $m_{K,\alpha}$ are the conjugates of α, that is, $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Furthermore there are no repeats among the roots of μ_α by Lemma 10.

Since there are no repeated eigenvalues, the trace of $m_{K,\alpha}$ is the sum of its eigenvalues and the determinant of $m_{K,\alpha}$ is the product of its eigenvalues. Thus we get

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$
$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Now consider a field $K \neq \mathbb{Q}(\alpha)$. Let $s = [K : \mathbb{Q}(\alpha)]$ and $r = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thanks to Proposition 18, for each embedding of $\mathbb{Q}(\alpha)$, there are s embeddings of K extending it. Hence the values $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ consist of each of the conjugates $\tau_1(\alpha), \ldots, \tau_r(\alpha)$, repeated s times (where $\tau_1, \ldots, \tau_r$ are the embeddings of $\mathbb{Q}(\alpha)$). Thus

$$\sum_{i=1}^{n} \sigma_i(\alpha) = s \cdot \sum_{i=1}^{r} \tau_i(\alpha) = s \cdot \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$$

where the second equality holds because we have already proved the lemma for $\mathbb{Q}(\alpha)$, and the third by Corollary 15.

The same argument works for norm, considering products instead of sums. □

Algebraic integers

Definition of algebraic integers.

We have finished understanding number fields *as fields*. But fields are not the main thing we study in number theory - it is like we have been studying the rational numbers, while number theory is really about integers. In fields, we can't say interesting things about primes and factorisation because every non-zero element of a field divides every other element.

So we want to talk about a version of "integers" inside number fields, where we will have interesting properties relating to factorisation and primes. We have already seen one example: in $\mathbb{Q}(i)$, we have the Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

So maybe we could generalise this, and define the "integers" in $\mathbb{Q}(\alpha)$ to be

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\gamma + a_2\gamma^2 + \cdots : a_i \in \mathbb{Z}\}.$$

Unfortunately, this doesn't work: it depends on α, even when the field $\mathbb{Q}(\alpha)$ stays the same. For example, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8})$ but $\mathbb{Z}[\sqrt{2}] \neq \mathbb{Z}[\sqrt{8}]$ (and $\mathbb{Z}[\sqrt{\frac{1}{2}}]$ is worse!)

For quadratic fields, maybe $\sqrt{d}$ where d is a square-free integer provides natural choice of γ, but there is no analogue for higher-degree fields. (And $\mathbb{Z}[\sqrt{d}]$ turns out not to always be the correct choice for quadratic fields either, as we shall soon see.)

Definition. An algebraic number is an **algebraic integer** if its minimal polynomial (over $\mathbb{Q}$) has coefficients in $\mathbb{Z}$.

e.g. $\sqrt{d}$ (where $d \in \mathbb{Z}$) is an algebraic integer because it is a root of $X^2 - d$.

$\frac{1+\sqrt{-3}}{2} = \zeta_6$ is an algebraic integer because its minimal polynomial is $X^2 - X + 1$.

This one might be a little surprising, especially when you compare with $\frac{1+\sqrt{3}}{2}$ which is not an algebraic integer: the minimal polynomial of $\frac{1+\sqrt{3}}{2}$ is $X^2 - X - \frac{1}{2} \notin \mathbb{Z}[X]$.

Just as for algebraic numbers, which are defined as a root of any polynomial with coefficients in $\mathbb{Q}$, then shown to have a minimal polynomial, many books define an algebraic integer to be a root of emphany monic polynomial with integer coefficients. The following lemma shows that this is equivalent to the definition above.

Lemma 20. *An algebraic number is an algebraic integer if and only if it is a root of some monic polynomial with coefficients in* $\mathbb{Z}$.

The word *monic* is essential in this lemma: any algebraic number is the root of some polynomial with integer coefficients, because you can take a polynomial

with coefficients in $\mathbb{Q}$ and multiply by a lowest common denominator, but that might give you a leading coefficient which is greater than 1.

Before we prove this, we need to recall primitive polynomials and (a version of) Gauss's Lemma from Algebra 2.

Definition. Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. We say that f is **primitive** if $\mathrm{HCF}(a_0, a_1, \ldots, a_n) = 1$.

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

(The key property that makes Gauss's Lemma work is that $\mathbb{Z}$ is a unique factorisation domain.)

Proof of Lemma 20. If α is an algebraic integer, then its minimal polynomial gives an example of a monic integer polynomial which has α as a root.

The main thing we have to prove is the other direction. Let α be an algebraic number which is the root of some monic polynomial with integer coefficients.

Choose $f(X)$ to be a monic polynomial in $\mathbb{Z}[X]$ such that $f(\alpha) = 0$, *of smallest degree.*

Let $\mu_\alpha(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. By Lemma 1, μ_α divides f in $\mathbb{Q}[X]$. Hence $\deg(f) \geq \deg(\mu_\alpha)$.

Assume for contradiction that $\deg(f) > \deg(\mu_\alpha)$. Then the fact that μ_α divides f shows that f is reducible in $\mathbb{Q}[X]$. Since f is monic, it is primitive. Hence by Gauss's Lemma, f is reducible in $\mathbb{Z}[X]$, i.e.

$$f = f_1 f_2 \text{ where } f_1, f_2 \in \mathbb{Z}[X] \text{ and } \deg(f_1), \deg(f_2) < \deg(f).$$

The leading coefficient of f is the product of the leading coefficients of f_1 and f_2. Thus these are integers whose product is 1, so both f_1 and f_2 have leading coefficient ± 1. Changing the sign if necessary, we may ensure that f_1 and f_2 are both monic.

Since $f(\alpha) = 0$, either $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$. Thus either f_1 or f_2 gives us a monic polynomial in $\mathbb{Z}[X]$ with α as a root, contradicting the fact that f has the smallest degree.

Thus in fact $\deg(f) = \deg(\mu_\alpha)$. Since μ_α divides f and μ_α and f are both monic, this implies that $\mu_\alpha = f$ and so $\mu_\alpha \in \mathbb{Z}[X]$. □

9. Rings of integers

The algebraic integers form a ring.

Notation. We write $\overline{\mathbb{Z}} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic integer}\}$.

We want to prove that the algebraic integers form a ring. The method is similar to the proof that the algebraic numbers form a field, but harder. The key point there was that if $\alpha, \beta \in \overline{\mathbb{Q}}$ then $\alpha + \beta$ and $\alpha\beta$ are contained in a finite extension of $\mathbb{Q}$, and hence are algebraic numbers. In the same way, instead of considering the ring of algebraic integers all at once, we focus in on just two of them and show that if $\alpha, \beta \in \overline{\mathbb{Z}}$ then $\alpha + \beta$ and $\alpha\beta$ are contained in a ring which is finitely generated as an abelian group.

The next lemma is the hard part of proving that $\overline{\mathbb{Z}}$ is a ring. The idea of "finitely generated as an abelian group" is the analogue of "finite extension" for fields. In this lemma, it is important to distinguish between "generated as a ring" and "generated as an abelian group."

Lemma 21. *Let $\alpha \in \mathbb{C}$. Then α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group.*

Proof. First we assume that α is an algebraic integer. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be the minimal polynomial of α over $\mathbb{Q}$ and let $n = \deg(f)$.

We claim that $\mathbb{Z}[\alpha]$ is generated as an abelian group by $\{1, \alpha, \ldots, \alpha^{n-1}\}$. In fact, we shall show by induction on m that $\alpha^m \in \mathbb{Z}.1 + \mathbb{Z}.\alpha + \cdots + \mathbb{Z}.\alpha^{n-1}$.

Indeed, if $m < n$ this is trivial. If $m \geq n$, then since $f(\alpha) = 0$, we get

$$\alpha^m = \alpha^{m-n}\alpha^n = \alpha^{m-n}(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0).$$

(The fact that f is monic is crucial here!) Thus α^m is a $\mathbb{Z}$-linear combination of smaller powers of α, and hence by induction it is a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.

Since the powers of α generate $\mathbb{Z}[\alpha]$ as an abelian group by definition, we conclude that $1, \alpha, \ldots, \alpha^{n-1}$ generate $\mathbb{Z}[\alpha]$ as an abelian group.

Conversely, suppose that $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group, say by $\beta_1, \ldots, \beta_r$. We can write each of the β_i as

$$\beta_i = b_{i0} + \beta_{i1}\alpha + \cdots + \beta_{im_i}\alpha^{m_i}. \qquad (*)$$

Let n be the maximum power of α which appears in any of these expressions. Then we can write

$$\alpha^{n+1} = c_1\beta_1 + \cdots + c_r\beta_r$$

for some $c_1, \ldots, c_r \in \mathbb{Z}$. Substituting (*) into this equation, we get

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

for some $a_0, \ldots, a_n \in \mathbb{Z}$. Thus α is a root of the monic polynomial

$$X^{n+1} - a_nX^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0 \in \mathbb{Z}[X]$$

and so α is an algebraic integer. □

In order to prove that $\overline{\mathbb{Z}}$ is a ring, we will use both directions of Lemma 21.

Lemma 22. *$\overline{\mathbb{Z}}$ is a ring.*

Proof. Let $\alpha, \beta \in \overline{\mathbb{Z}}$. We have to show that $\alpha + \beta$ and $\alpha\beta \in \overline{\mathbb{Z}}$.

By Lemma 21, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated as abelian groups. Let $\theta_1, \ldots, \theta_r$ be generators $\mathbb{Z}[\alpha]$ and let $\phi_1, \ldots, \phi_s$ be generators $\mathbb{Z}[\beta]$ as abelian groups.

Write $\mathbb{Z}[\alpha, \beta]$ for the smallest ring containing α and β, that is,

$$\mathbb{Z}[\alpha, \beta] = \Big\{ \sum_{i,j=0}^{m} c_{ij} \alpha^i \beta^j : m \in \mathbb{N}, c_{ij} \in \mathbb{Z} \Big\}.$$

Each $\alpha^i \beta^j$ is a $\mathbb{Z}$-combination of θs multiplied by a $\mathbb{Z}$-combination of ϕs. Thus it is a $\mathbb{Z}$-combination of $\theta_k \phi_\ell$s. Hence $\{\theta_k \phi_\ell : 1 \le k \le r, 1 \le \ell \le s\}$ generates $\mathbb{Z}[\alpha, \beta]$ as an abelian group (this is like the Tower Law, except that we are talking only about generating sets, not necessarily about bases).

Thus $\mathbb{Z}[\alpha, \beta]$ is finitely generated as an abelian group. Every subgroup of a finitely generated abelian group is finitely generated, so in particular $\mathbb{Z}[\alpha + \beta]$ and $\mathbb{Z}[\alpha\beta]$ are finitely generated as abelian groups. Hence by the reverse direction of Lemma 21, $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

We have the following simple property of algebraic integers, which says that every algebraic number can be written as a "fraction" with an algebraic integer as the numerator and a rational (ordinary) integer as the denominator. Always having rational integers as denominators is convenient because it makes it easier to do things like find a common denominator for several fractions.

Lemma 23. *Let α be an algebraic number. Then there exists $m \in \mathbb{Z}$, $m \neq 0$, such that $m\alpha$ is an algebraic integer.*

Proof. Let the minimal polynomial of α be $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$, where $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. Let m be the lowest common multiple of the denominators of $a_0, \ldots, a_{n-1}$ (when we write them as fractions in lowest terms). Then

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

is a monic polynomial with coefficients in $\mathbb{Z}$. We have $g(m\alpha) = 0$, and so $m\alpha$ is an algebraic integer. □

Ring of integers of a number field.

Definition. If K is a number field, the **ring of integers** of K is $\overline{\mathbb{Z}} \cap K$, written $\mathcal{O}_K$.

Since $\overline{\mathbb{Z}}$ and K are both rings, so is their intersection $\mathcal{O}_K$.

e.g. The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, because the minimal polynomial of $a \in \mathbb{Q}$ is $X - a$.

In order to avoid confusion with algebraic integers, we sometimes call an element of $\mathbb{Z}$ a **rational integer**.

Lemma. *If $\alpha \in \mathcal{O}_K$, then $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ are rational integers.*

Proof. Let $\chi_{K,\alpha}$ be the characteristic polynomial of $m_{K,\alpha}$. By Lemmas 13 and 14, $\chi_{K,\alpha}$ is a power of $\mu_{\mathbb{Q},\alpha}$ so $\chi_{K,\alpha}$ has integer coefficients.

$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ are coefficients of $\chi_{K,\alpha}$ (multiplied by ± 1) so they are in $\mathbb{Z}$. □

This can be a handy test for showing that a number is not an algebraic integer. The converse is false, except when K is a quadratic field (we will prove that the converse holds for a quadratic field next time).

10. Discriminant of a basis

Ring of integers of a quadratic field.

Proposition 24. *Let $d \neq 1$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$. Then*

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

(Note that $d \not\equiv 0 \bmod 4$ because it is square-free.)

Proof. Any element of $\mathbb{Q}(\sqrt{d})$ can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. If $\alpha \in \mathbb{Q}$ (i.e. $b = 0$), then we know already that α is an algebraic integer if and only if it is in $\mathbb{Z}$.

Otherwise, $K = \mathbb{Q}(\alpha)$ so the minimal polynomial of α over $\mathbb{Q}$ is the same as its characteristic polynomial, i.e.

$$X^2 - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \cdot X + \mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = X^2 - 2aX + (a^2 - db^2).$$

In passing, we see that α is an algebraic integer if and only if $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Z}$.

Hence if $a + b\sqrt{d}$ is an algebraic integer, then $2a \in \mathbb{Z}$. Also $a^2 - db^2 \in \mathbb{Z}$, from which we deduce that $4db^2 \in \mathbb{Z}$. Since d is square-free, this implies that $2b \in \mathbb{Z}$.

Thus every element of $\mathcal{O}_K$ must differ from an element of $\mathbb{Z}[\sqrt{d}]$ by one of $\left\{0, \frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\right\}$. The minimal polynomials of $\frac{1}{2}$ and $\frac{\sqrt{d}}{2}$ are $X - \frac{1}{2}$ and $X^2 - \frac{d}{4}$ respectively, so $\frac{1}{2}$ and $\frac{\sqrt{d}}{2}$ are never algebraic integers.

Finally, the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $X^2 - X + \frac{1-d}{4}$. So $\frac{1+\sqrt{d}}{2}$ is an algebraic integer if and only if $d \equiv 1 \bmod 4$.

Thus if $d \equiv 2$ or $3 \bmod 4$, $\alpha \in \mathcal{O}_K \Rightarrow \alpha \in \mathbb{Z}[\sqrt{d}]$. It is obvious that $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$, so in fact $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

If $d \equiv 1 \bmod 4$, then we have shown that

$$\alpha \in \mathcal{O}_K \Rightarrow \alpha = a + b\sqrt{d} + c\tfrac{1+\sqrt{d}}{2} \text{ with } a, b \in \mathbb{Z}, c \in \{0, 1\}.$$

To show that such an α is in $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, we need to show that $\sqrt{d} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. This is true because

$$\sqrt{d} = 2\left(\tfrac{1+\sqrt{d}}{2}\right) - 1.$$

Thus $\alpha \in \mathcal{O}_K \Rightarrow \alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Meanwhile, $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ and $\mathcal{O}_K$ is a ring so $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathcal{O}_K$, completing the proof. □

e.g. Since $-1 \equiv 3 \bmod 4$,$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ i.e. the Gaussian integers, but since $-3 \equiv 1 \bmod 4$, we have

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_3]$$

(where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity).

Discriminant of a basis.

It is not so easy to calculate the ring of integers by hand for number fields of degree greater than 2. The discriminant of a number field is a tool which we can use to calculate the ring of integers, and for other practical calculations such as the class group later in the course. It will also be important as a theoretical tool in some of the proofs.

The discriminant is a number which measures the size of the ring of integers of a number field (in a more refined sense than the degree). We begin by defining the discriminant of a *basis* of a number field, which varies depending on the basis we choose; we will subsequently pick a special kind of basis and use that to define the discriminant of the number field itself.

There are two equivalent formulae for the discriminant of a basis. Here is the first.

Definition. Let K be a number field with $n = [K : \mathbb{Q}]$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K and let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K.

The **discriminant** of $\{\alpha_1, \ldots, \alpha_n\}$ is defined to be

$$\Delta_K(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$$

(usually we will just write $\Delta(\alpha_1, \ldots, \alpha_n)$ with no K). In other words, $\Delta(\alpha_1, \ldots, \alpha_n)$ is the square of the determinant of the matrix with entries $\sigma_i(\alpha_j)$ i.e.

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}.$$

(Note that there are $[K : \mathbb{Q}]$ embeddings by the Corollary to Proposition 18, so this is indeed a square matrix and its determinant makes sense.)

Why is this a measure of "size"? This measures the "size" of the basis in the following sense: The volume of the parallelepiped in $\mathbb{R}^n$ with edges $v_1, \ldots, v_n$ is given by the determinant of the matrix which has $v_1, \ldots, v_n$ as columns (up to sign). So if we think of the basis element $\alpha_i \in K$ as being represented by the vector $(\sigma_1(\alpha_i), \sigma_2(\alpha_i), \ldots, \sigma_n(\alpha_i)) \in \mathbb{C}^n$, then $\Delta(\alpha_1, \ldots, \alpha_n)$ is the square of the volume of the parallelepiped formed from these vectors. Thus in some way it measures the "volume" of the basis.

Why do we need to square the determinant? Here are several reasons:

(1) If we swap two of the embeddings, or two of the α_i, then that swaps two of the rows or columns of the matrix, so it multiplies the determinant by ± 1. Thus squaring gives us something which is independent of the orderings.
(2) We have to square the determinant to match the second formula (which we are about to give)!
(3) $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$ but $\det(\sigma_i(\alpha_j))$ need not be in $\mathbb{Q}$. This is not obvious: the entries of the matrix are algebraic numbers so all we can immediately see is that $\Delta(\alpha_1, \ldots, \alpha_n)$ is an algebraic number. In order to prove that $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$, we shall use the second definition of discriminant below.

(If you did Galois theory, you might try to prove this directly from the first definition.)

Example: if $K = \mathbb{Q}$, we can calculate

$$\Delta(1, \sqrt{d}) = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

Due to Proposition 24, it might also be interesting to calculate the discriminant of the basis $\{1, \frac{1+\sqrt{d}}{2}\}$. We have

$$\Delta(1, \tfrac{1+\sqrt{d}}{2}) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = (-\sqrt{d})^2 = d.$$

Lemma 25. *Let K be a number field of degree n. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K. Then*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)).$$

(Note that the determinant is not squared this time!)

Proof. Let M be the matrix with entries $\sigma_i(\alpha_j)$. Then

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(M)^2 = \det(M^t)\det(M) = \det(M^t M)$$

The ij-th entry of $M^t M$ is

$$\sum_{k=1}^{n} M^t_{ik} M_{kj} = \sum_{k=1}^{n} M_{ki} M_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)$$

where the last equality is Lemma 19. □

One can check that calculating with Lemma 25 gives the same values when applied to the bases of a quadratic field which we considered previously:

$$\Delta(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d,$$

$$\Delta(1, \tfrac{1+\sqrt{d}}{2}) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\frac{1+\sqrt{d}}{2}) \\ \mathrm{Tr}(\frac{1+\sqrt{d}}{2}) & \mathrm{Tr}(\frac{1+d+2\sqrt{d}}{4}) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

11. More on discriminants

Last time, we proved that

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)).$$

Since $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$ is always in $\mathbb{Q}$, this immediately tells us that $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. Furthermore, if $\alpha_1, \ldots, \alpha_n$ are all in $\mathcal{O}_K$, then the traces $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$ are in $\mathbb{Z}$ and so $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

While we calculated the discriminant of a quadratic field using the first definition last time, if you want to calculate the discriminant of a specific field it is usually better to use the second formula. This is because the first formula involves calculating the determinant of a matrix whose entries are algebraic numbers, usually quite a hard calculation, while for the second formula you begin by calculating some traces and thereafter just have rational numbers to deal with. The first definition of discriminant will more often be useful in proofs, where you don't have to calculate a specific example.

Discriminants and change of basis.

We said that the discriminant depends on the choice of basis of K. When we change the basis, the discriminant gets multiplied by the square of the determinant of the change-of-basis matrix.

Lemma 26. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be $\mathbb{Q}$-bases for K. Let the change-of-basis matrix from $\{\beta_1, \ldots, \beta_n\}$ to $\{\alpha_1, \ldots, \alpha_n\}$ be (c_{ij}) i.e.*

$$\beta_j = \sum_{j=1}^{n} c_{ij}\alpha_i$$

with $c_{ij} \in \mathbb{Q}$. Then

$$\Delta(\beta_1, \ldots, \beta_n) = \det(c_{ij})^2\, \Delta(\alpha_1, \ldots, \alpha_n).$$

Proof. We can prove this using either formula for the discriminant. Let's use the first definition.

Let A and B be the matrices with entries $\sigma_i(\alpha_j)$ and $\sigma_i(\beta_j)$ respectively. Let C be the matrix with entries c_{ij}. Then

$$B_{ij} = \sigma_i(\beta_j) = \sigma_i\Big(\sum_{k=1}^{n} c_{kj}\alpha_k\Big) = \sum_{k=1}^{n} c_{kj}\sigma_i(\alpha_k) = \sum_{k=1}^{n} A_{ik}c_{kj}$$

(using the facts that σ_i is a field homomorphism, and that it restricts to the identity on $\mathbb{Q}$). Hence $B = AC$ as matrices and so

$$\Delta(\beta_1, \ldots, \beta_n) = \det(B)^2 = \Big(\det(A)\det(C)\Big)^2 = \det(C)^2\, \Delta(\alpha_1, \ldots, \alpha_n). \qquad \square$$

We can use this to prove an essential property of the discriminant.

Lemma 27. *For any $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of K, the discriminant $\Delta(\alpha_1, \ldots, \alpha_n)$ is non-zero.*

Proof. We will prove this first for a special choice of basis. By the Primitive Element Theorem, $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. By Theorem 3, there is a $\mathbb{Q}$-basis for K of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Now $\Delta(1, \alpha, \ldots, \alpha^{n-1})$ is the square of

$$\det \begin{pmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{n-1}) \\ 1 & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha^{n-1}) \end{pmatrix} = \det \begin{pmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^{n-1} \\ 1 & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^{n-1} \end{pmatrix}.$$

This is a special kind of matrix called a Vandermonde matrix and it is well-known that its determinant is

$$\prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

Thus

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

By Proposition 18, the $\sigma_i(\alpha)$ are pairwise distinct so this is non-zero.

Now consider an arbitrary $\mathbb{Q}$-basis $\beta_1, \ldots, \beta_n$ of K. By linear algebra, we can express this in terms of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ as

$$\beta_j = \sum_{i=1}^{n} c_{ij} \alpha^{i-1}$$

where the matrix (c_{ij}) has non-zero determinant. Hence by Lemma 26,

$$\Delta(\beta_1, \ldots, \beta_n) = \det(c_{ij})^2 \cdot \Delta(1, \alpha, \ldots, \alpha^{n-1}) \neq 0. \qquad \square$$

Note that we only defined the discriminant for a basis of K, but we could apply the same formulae to any set of n elements $\{\alpha_1, \ldots, \alpha_n\} \subseteq K$. (The proof that the two formulae give the same value still works.) In fact, $\{\alpha_1, \ldots, \alpha_n\}$ forms a basis of K if and only if $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

Integral bases.

Definition. Let K be a number field. An **integral basis** for K is a set of elements $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$ which form a $\mathbb{Z}$-basis for the abelian group $(\mathcal{O}_K, +)$. In other words, every element of $\mathcal{O}_K$ can be written uniquely in the form $x_1\alpha_1 + \cdots + x_m\alpha_m$ with $x_1, \ldots, x_m \in \mathbb{Z}$.

Lemma 28. *Let $\{\alpha_1, \ldots, \alpha_m\}$ be an integral basis for a number field K. Then $\{\alpha_1, \ldots, \alpha_m\}$ is a basis for K as a $\mathbb{Q}$-vector space. In particular, $m = [K : \mathbb{Q}]$.*

Proof. Lemma 23 tells us that $\{\alpha_1, \ldots, \alpha_n\}$ spans K as a $\mathbb{Q}$-vector space.

If $\{\alpha_1, \ldots, \alpha_n\}$ were $\mathbb{Q}$-linearly dependent, then we could multiply up by a common denominator to get a non-trivial $\mathbb{Z}$-linear relation between them, contradicting the fact that 0 can be written as a $\mathbb{Z}$-linear combination of the integral basis elements in only one way. $\square$

For example, Proposition 24 gives us an integral basis for $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer:

- $\{1, \sqrt{d}\}$ if $d \equiv 2, 3 \bmod 4$;
- $\{1, \frac{1+\sqrt{d}}{2}\}$ if $d \equiv 1 \bmod 4$.

Note that if $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for K and $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, this is *not enough* to establish that $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis. For example, if $d \equiv 1 \bmod 4$, then $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{d})$ consisting of algebraic integers but it is not an integral basis because $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ but not in $\mathbb{Z}.1 + \mathbb{Z}.\sqrt{d}$. (If we have a $\mathbb{Q}$-basis for K consisting of algebraic integers, then the "uniquely" part of the definition of integral basis is always satisfied. But, as here, the basis might fail to generate $\mathcal{O}_K$ over $\mathbb{Z}$.)

It is not obvious that an integral basis exists for every number field: we will prove this next lecture. It is worth pausing to reflect on why this is not obvious. The structure theory of finitely generated abelian groups tells us that every torsion-free finitely generated abelian group is isomorphic to $\mathbb{Z}^n$ for some n and hence possesses a $\mathbb{Z}$-basis. The group $(\mathcal{O}_K, +)$ is torsion-free (because number fields have characteristic 0). However it is not obvious that $(\mathcal{O}_K, +)$ is finitely generated – this is true, but we will only discover it as a corollary of the existence of an integral basis.

$\mathbb{Z}[\frac{1}{2}] \subseteq \mathbb{Q}$ is an example of a subring of a number field which is not finitely generated as an abelian group and so does not have an integral basis, demonstrating that we are really going to have to use some properties of algebraic integers to show that $(\mathcal{O}_K, +)$ is finitely generated.

One key property of algebraic integers was Lemma 21: if α is an algebraic integer, then $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group. However we can't apply this to $\mathcal{O}_K$ because $\mathcal{O}_K$ need not be of the form $\mathbb{Z}[\alpha]$ for any α (there is no analogue for the Primitive Element Theorem for rings of integers).

12. Discriminant and integral bases

CORRECTION. The proof of Lemma 29 in the original version of these notes (and maybe in the lectures) contained a mistake: I used the matrices P and Q the wrong way round. This should be fixed now.

Existence of an integral basis.

The following lemma refines Lemma 26 on discriminant and change-of-basis. The proof is largely a revision of Algebra 1.

Lemma 29. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be $\mathbb{Q}$-bases for K. Let $c_{ij} \in \mathbb{Q}$ be such that*

$$\beta_j = \sum_{i=1}^{n} c_{ij}\alpha_i.$$

Let $G = \mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n$ and $H = \mathbb{Z}.\beta_1 + \cdots + \mathbb{Z}.\beta_n$.

Suppose that $H \subseteq G$. (In other words, $\beta_1, \ldots, \beta_n \in G$.)

Then H has finite index in G and $[G : H] = |\det(c_{ij})|$. Consequently,

$$\Delta(\beta_1, \ldots, \beta_n) = [G : H]^2 \, \Delta(\alpha_1, \ldots, \alpha_n).$$

It is unfortunate that the notation $[G : H]$ for the index of a subgroup clashes with the notation $[L : K]$ for the degree of a field extension. Both are very standard notations. We will never want to talk about the index of a subgroup of a field (in characteristic zero, the index of one field as a subgroup of another is always infinite) so hopefully this will not cause confusion.

Proof. Since $\beta_1, \ldots, \beta_n \in G$, $c_{ij} \in \mathbb{Z}$ for all i, j.

By a result from Algebra I, we can write

$$C = PAQ$$

where P, Q are unimodular (i.e. integer matrices with determinant ± 1) and A is in Smith Normal Form (i.e. A is diagonal $A = \mathrm{diag}(d_1, \ldots, d_n)$ with d_i nonnegative integers and $d_i \mid d_{i+1}$ for all i – we don't care about the divisibility condition).

Let

$$\alpha'_j = \sum_{i=1}^{n} P_{ij}\alpha_i.$$

Since P is unimodular, P and P^{-1} both have integer entries so in fact $\{\alpha'_1, \ldots, \alpha'_n\}$ is another $\mathbb{Z}$-basis for G. Similarly, if we let

$$\beta'_j = \sum_{i=1}^{n} (Q^{-1})_{ij}\beta_i,$$

then $\{\beta'_1, \ldots, \beta'_n\}$ is a $\mathbb{Z}$-basis for H.

Now $\beta'_j = \sum_{i=1}^{n} A_{ij}\alpha'_i = d_j\alpha'_j$ so

$$G/H \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

We also have

$$|\det(C)| = |\det(PAQ)| = |\det(A)| = d_1 d_2 \cdots d_n$$

since $|\det(P)| = |\det(Q)| = 1$. Since $\det(C) \neq 0$, we deduce that $d_i \neq 0$ for all i.

Thus G/H is finite and

$$[G : H] = d_1 d_2 \cdots d_n = |\det(C)|.$$

The final formula, relating the discriminants, follows by Lemma 26. □

Theorem 30. *Every number field K possesses an integral basis.*

Proof. First note that there exists a $\mathbb{Q}$-basis of K consisting of algebraic integers. Indeed, if we take any $\mathbb{Q}$-basis of K, then by Lemma 23, we can multiply each of the basis elements by a non-zero rational integer to obtain something in $\mathcal{O}_K$.

Choose a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for K, consisting of elements of $\mathcal{O}_K$, such that $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is as small as possible. (Since $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is always a positive integer for $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, this minimum value is attained.)

We shall show that this set $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for K.

Suppose not. Since $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for K, $\alpha_1, \ldots, \alpha_n$ are certainly linearly independent over $\mathbb{Z}$. Hence the only way in which they can fail to be an integral basis is if they do not generate $(\mathcal{O}_K, +)$. Thus there is some $\beta \in \mathcal{O}_K$ such that $\beta \notin \mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n$. Let

$$H = \mathbb{Z}.\alpha_1 + \mathbb{Z}.\alpha_2 + \cdots + \mathbb{Z}.\alpha_n,$$
$$G = \mathbb{Z}.\beta + \mathbb{Z}.\alpha_1 + \mathbb{Z}.\alpha_2 + \cdots + \mathbb{Z}.\alpha_n.$$

G is a finitely generated abelian group, so by the structure theory of finitely generated abelian groups, it is isomorphic to $\mathbb{Z}^m$ for some m and hence has a $\mathbb{Z}$-basis $\beta_1, \ldots, \beta_m$.

Now $\beta_1, \ldots, \beta_m$ span K as a $\mathbb{Q}$-vector space because they generate $\alpha_1, \ldots, \alpha_n$, and they are linearly independent because they are a $\mathbb{Z}$-basis. Hence $\{\beta_1, \ldots, \beta_m\}$ is a $\mathbb{Q}$-basis for K and $m = n$. (This is the same argument as in the proof of Lemma 28.)

By Lemma 29, we have

$$\Delta(\alpha_1, \ldots, \alpha_n) = [G : H]^2 \Delta(\beta_1, \ldots, \beta_n).$$

Since $\beta \notin H$, $[G : H] > 1$ and so

$$|\Delta(\alpha_1, \ldots, \alpha_n)| > |\Delta(\beta_1, \ldots, \beta_n)|.$$

But $\{\beta_1, \ldots, \beta_n\}$ is a $\mathbb{Q}$-basis of K consisting of algebraic integers (because each β_i is a $\mathbb{Z}$-linear combination of $\beta, \alpha_1, \ldots, \alpha_n$). Hence this contradicts the fact that $|\Delta(\alpha_1, \ldots, \alpha_n)|$ is as small as possible. □

Discriminant of an integral basis.

An important observation is that all integral bases for a given number field have the same discriminant.

Lemma 31. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be integral bases for K. Then*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \Delta(\beta_1, \ldots, \beta_n).$$

Proof. From the definition of integral basis, we have

$$\mathcal{O}_K = \mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n = \mathbb{Z}.\beta_1 + \cdots + \mathbb{Z}.\beta_n.$$

Hence by Lemma 29,

$$\Delta(\beta_1, \ldots, \beta_n) = [\mathcal{O}_K : \mathcal{O}_K]^2 \, \Delta(\alpha_1, \ldots, \alpha_n).$$

We are done because $[\mathcal{O}_K : \mathcal{O}_K] = 1$. □

Consequently the following definition makes sense.

Definition. Let K be a number field. The **discriminant** of K, written Δ_K, is the discriminant of any integral basis of K.

The discriminant of K is always a non-zero integer.

e.g. according to calculations from lecture 10, the discriminant of $\mathbb{Q}(\sqrt{d})$ (for $d \neq 1$ a square-free integer) is as follows:

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \Delta(1, \sqrt{d}) = 4d \qquad \text{if } d \equiv 2, 3 \bmod 4,$$

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \Delta(1, \tfrac{1+\sqrt{d}}{2}) = d \qquad \text{if } d \equiv 1 \bmod 4.$$

We have the following easy sufficient criterion for recognising an integral basis.

Lemma 32. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K such that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. If $\Delta(\alpha_1, \ldots, \alpha_n)$ is square-free, then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis for K.*

Proof. Let $H = \mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n$. Let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis for K (which exists by Theorem 30). By Lemma 29,

$$\Delta(\alpha_1, \ldots, \alpha_n) = [\mathcal{O}_K : H]^2 \, \Delta(\beta_1, \ldots, \beta_n).$$

Here $[\mathcal{O}_K : H]^2$ is a square and $\Delta(\beta_1, \ldots, \beta_n)$ is an integer, while $\Delta(\alpha_1, \ldots, \alpha_n)$ is square-free, so $[\mathcal{O}_K : H] = 1$. Thus $H = \mathcal{O}_K$, and so $\alpha_1, \ldots, \alpha_n$ form an integral basis. □

This is only a one-way implication. For example, we saw that if d is square-free and congruent to 2 or 3 mod 4, then $\{1, \sqrt{d}\}$ is an integral basis for $\mathbb{Q}(\sqrt{d})$ but $\Delta(1, \sqrt{d}) = 4d$ is not square-free (because it is divisible by 4). Lemma 32 is only useful when Δ_K is itself square-free, which often doesn't hold.

Finding an integral basis.

Suppose we have a basis $\{\alpha_1, \ldots, \alpha_n\}$ for K consisting of algebraic integers but its discriminant is not square-free. We want to either find an element of $\mathcal{O}_K$ which is not in $\mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n$, thus showing that $\{\alpha_1, \ldots, \alpha_n\}$ is not an integral basis (but getting us closer to finding an integral basis) or else prove that no such element exists.

The following lemma, which we will prove next time, gives a finite list of elements of K such that it suffices to check whether each element of the list is in $\mathcal{O}_K$.

Lemma. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K such that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. If $\{\alpha_1, \ldots, \alpha_n\}$ is not an integral basis, then there exists a prime p and $u_1, \ldots, u_n \in \mathbb{Z}$ such that $p^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$, $0 \leq u_i < p$ for all i, the u_i are not all zero, and*

$$\frac{u_1\alpha_1 + \cdots + u_n\alpha_n}{p} \in \mathcal{O}_K.$$

13. Finding an integral basis

We can give an algorithm based on the proof of Theorem 30 which allows us to find an integral basis (and hence to calculate the discriminant and the ring of integers) of any number field. The key ingredient is the following lemma.

Lemma 33. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K such that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. If $\{\alpha_1, \ldots, \alpha_n\}$ is not an integral basis, then there exists a prime p and $u_1, \ldots, u_n \in \mathbb{Z}$ such that $p^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$, $0 \leq u_i < p$ for all i, the u_i are not all zero, and*

$$\frac{u_1\alpha_1 + \cdots + u_n\alpha_n}{p} \in \mathcal{O}_K.$$

Proof. Let $H = \mathbb{Z}.\alpha_1 + \cdots + \mathbb{Z}.\alpha_n$. Since $\{\alpha_1, \ldots, \alpha_n\}$ is not an integral basis, $H \neq \mathcal{O}_K$ so we can pick a prime p which divides $[\mathcal{O}_K : H]$. By Lemma 29, $\Delta(\alpha_1, \ldots, \alpha_n) = [\mathcal{O}_K : H]^2 \Delta_K$ and so $p^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$.

Now $\mathcal{O}_K/H$ is a finite abelian group and p divides $\#\mathcal{O}_K/H$. Cauchy's theorem states that $\mathcal{O}_K/H$ contains an element of order p. (Cauchy's theorem is a general theorem about finite groups; in the case of abelian groups, it can easily be deduced from the structure theory of finite abelian groups.) Thus we can choose $\beta \in \mathcal{O}_K$ such that $\beta + H$ has order p in $\mathcal{O}_K/H$.

Then $p\beta \in H$ so $p\beta = x_1\alpha_1 + \cdots + x_n\alpha_n$ for some $x_1, \ldots, x_n \in \mathbb{Z}$. Write $x_i = py_i + u_i$ where $y_i, u_i \in \mathbb{Z}$ and $0 \leq u_i < p$, and let

$$\beta' = \frac{u_1\alpha_1 + \cdots + u_n\alpha_n}{p}.$$

Then $\beta' - \beta = y_1\alpha_1 + \cdots + y_n\alpha_n \in H \subseteq \mathcal{O}_K$. Hence $\beta' \in \mathcal{O}_K$. Finally $\beta' + H = \beta + H$ has order p in $\mathcal{O}_K/H$, so $\beta' \notin H$. Thus $u_1, \ldots, u_n$ are not all zero. □

Algorithm to find an integral basis.

(1) Pick a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for K, such that $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$.
(2) Calculate $\Delta(\alpha_1, \ldots, \alpha_n)$.
(3) List all primes p such that $p^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$.
(4) For each p in the list, and each number of the form

$$\beta = \frac{u_1\alpha_1 + \cdots + u_n\alpha_n}{p}$$

with $0 \leq u_i < p$ not all zero, check whether β is an algebraic integer.
(5) If some β is an algebraic integer, then find a $\mathbb{Z}$-basis for the subgroup of $\mathcal{O}_K$ generated by $\alpha_1, \ldots, \alpha_n$ and β. You can do this as follows:
   (a) By reordering the basis elements, assume that $u_1 \neq 0$.
   (b) Let $x, y \in \mathbb{Z}$ be a solution to the equation $u_1x + py = 1$ (possible because u_i and p are coprime).
   (c) Let $\beta_1 = x\beta + y\alpha_1$.
   (d) Now $\{\beta_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ form a $\mathbb{Z}$-basis for the group generated by $\alpha_1, \ldots, \alpha_n$ and β.

   Go back to step 2 of the algorithm with this new basis. (Actually, you can skip step 2 because $\Delta(\beta_1, \alpha_2, \ldots, \alpha_n) = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)/p^2$ by Lemma 26.)

(6) If you did not find any β which was an algebraic integer, then you have found an integral basis (thanks to Lemma 33).

This algorithm is guaranteed to terminate because $|\Delta(\alpha_1, \ldots, \alpha_n)|$ gets smaller each time round.

Shortcut using Eisenstein's criterion.

Step 4 of the algorithm above can certainly be implemented on a computer, but it is a lot of work to carry it out by hand. There is a shortcut which is often useful, if K is generated by an element whose minimal polynomial satisfies Eisenstein's criterion, which we recall from Algebra 2.

Definition. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ be a monic polynomial in $\mathbb{Z}[X]$. We say that f satisfies **Eisenstein's criterion at a prime** p if $p \mid a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$.

Proposition 34. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial which satisfies Eisenstein's criterion at a prime p. Let $K = \mathbb{Q}(\alpha)$ where $f(\alpha) = 0$ and let $n = [K : \mathbb{Q}]$. Then:*

(i) p^{n-1} divides Δ_K.

(ii) $\frac{u_1\alpha_1 + \cdots + u_n\alpha_n}{p}$, for $u_i \in \mathbb{Z}$, $0 \leq u_i < p$ and u_i not all zero, is never an algebraic integer.

This proposition can be proved using the methods of this course but it is a bit long so we will skip the proof (for part (ii), we already have the tools to prove it; for part (i), the easiest proof uses the Dedekind–Kummer theorem which we will study later). You need to know the statement of the proposition and be able to use it to replace step 4 of the algorithm.

One example in which this shortcut is useful is cyclotomic fields. Let $\zeta = \exp(2\pi i/p)$ where p is an odd prime number and let $K = \mathbb{Q}(\zeta)$. According to example sheet 1 Q4, $\{1, \zeta, \ldots, \zeta^{p-1}\}$ is a $\mathbb{Q}$-basis for K and one can calculate

$$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{(p-1)/2}p^{p-2}.$$

(This calculation is on example sheet 2.) The only prime factor is p and so by Lemma 33, we only need to check whether

$$\beta = \frac{u_0 + u_1\zeta + \cdots + u_{p-2}\zeta^{p-2}}{p}$$

is an algebraic integer for $u_i \in \mathbb{Z}$, $0 \leq u_i < p$.

Let $\omega = \zeta - 1$. The minimal polynomial of ω satisfies Eisenstein's criterion at p, so we can apply Proposition 34 to the basis $\{1, \omega, \ldots, \omega^{p-2}\}$:

$$\frac{u_0 + u_1\omega + \cdots + u_{p-2}\omega^{p-2}}{p}$$

is never an algebraic integer unless $u_i \equiv 0 \bmod p$ for all i. Since

$$\mathbb{Z}.1 + \mathbb{Z}.\zeta + \cdots + \mathbb{Z}.\zeta^{p-2} = \mathbb{Z}.1 + \mathbb{Z}.\omega + \cdots + \mathbb{Z}.\omega^{p-2}$$

we can deduce that

$$\frac{u_0' + u_1'\omega + \cdots + u_{p-2}'\omega^{p-2}}{p}$$

is never an algebraic integer unless $u_i' \equiv 0 \bmod p$ for all i.

Hence by Lemma 33, $\{1, \zeta, \ldots, \zeta^{p-2}$ is an integral basis and $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Example sheet 2 Q7 takes you through a few steps which prove Proposition 34 for the cyclotomic case.

This ends the discussion about discriminants and integral bases. Next lecture we will look at factorisation and ideals, starting with some more Algebra 2 revision.

14. Factorisation in integral domains

We need to recall several definitions relating to factorisation from Algebra 2.

Units.

Definition. Let R be a ring. An element $x \in R$ is a **unit** if there exists $y \in R$ such that $xy = 1$.

The set of units in R forms an abelian group under multiplication. We write $R^\times$ for this group. (That's a "times" symbol in the superscript, because it's a group under multiplication. Some people call this group R^*.)

Lemma 35. *Let $\mathcal{O}_K$ be the ring of integers of a number field. An element $x \in \mathcal{O}_K$ is a unit if and only if $\mathrm{Nm}_{K/\mathbb{Q}}(x) = \pm 1$.*

Proof. If x is a unit, then x, x^{-1} are both in $\mathcal{O}_K$ so $\mathrm{Nm}_{K/\mathbb{Q}}(x)$ and $\mathrm{Nm}_{K/\mathbb{Q}}(x^{-1})$ are both rational integers. Since

$$\mathrm{Nm}_{K/\mathbb{Q}}(x)\,\mathrm{Nm}_{K/\mathbb{Q}}(x^{-1}) = \mathrm{Nm}_{K/\mathbb{Q}}(xx^{-1}) = 1$$

we conclude that $\mathrm{Nm}_{K/\mathbb{Q}}(x) = \pm 1$.

Conversely, suppose that $x \in \mathcal{O}_K$ and $\mathrm{Nm}_{K/\mathbb{Q}}(x^{-1}) = \pm 1$. Assume that $K \subseteq \mathbb{C}$ (which we can do by Lemma 6). Label the embeddings of K as $\sigma_1, \ldots, \sigma_n$ such that σ_1 is the inclusion $K \to \mathbb{C}$. Let $y = \sigma_2(x)\sigma_3(x)\cdots\sigma_n(x)$. Then

$$xy = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x) = \mathrm{Nm}_{K/\mathbb{Q}}(x) = \pm 1$$

by Lemma 19. Thus $y = \pm 1/x \in K$.

Also each $\sigma_i(x)$ is an algebraic integer (they all have the same minimal polynomial as x) and so y is an algebraic integer. The $\sigma_i(x)$ are not necessarily in K, but we have shown that $y \in K$, so $y \in \mathcal{O}_K$. Thus $\pm y$ is an inverse of x in $\mathcal{O}_K$, so x is a unit in $\mathcal{O}_K$. □

Factorisation.

Let R be an integral domain.

Recall that "$x \mid y$" ("x **divides** y") means that there exists $z \in R$ such that $y = xz$.

Definition. Elements $x, y \in R$ are **associates** if there exists a unit $z \in R^\times$ such that $x = yz$.

An element $x \in R$ is:

- **irreducible** if it is non-zero, not a unit and whenever we can write $x = ab$ with $a, b \in R$, then either a is a unit or b is a unit;
- **prime** if it is non-zero, not a unit and whenever $x \mid ab$ with $a, b \in R$, either $x \mid a$ or $x \mid b$.

Definition. An integral domain R is a **unique factorisation domain (UFD)** if, for every non-zero non-unit $a \in R$:

(i) a can be written in the form $a = x_1 x_2 \cdots x_n$ for some irreducible elements $x_1, \ldots, x_n \in R$;

(ii) given another factorisation $a = y_1 y_2 \cdots y_m$ into irreducibles, we must have $m = n$ and after permuting $y_1, \ldots, y_m$, each y_i is an associate of the corresponding x_i.

The following facts were proved in Algebra 2.

Facts. *In any integral domain, every prime element is irreducible.*
In a UFD, every irreducible element is prime.
Every principal ideal domain (PID) is a UFD.

There are UFDs which are not PIDs, for example $\mathbb{Z}[X]$ ($\langle 2, X\rangle$ is a non-principal ideal). However we will prove later that if the *ring of integers of a number field* is a UFD, then it is a PID.

A classic example of an integral domain which is not a UFD is the ring of integers of $K = \mathbb{Q}(\sqrt{-5})$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have two factorisations of 6 in $\mathcal{O}_K$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

We can prove that $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible by considering their norms.

For example, $\mathrm{Nm}_{K/\mathbb{Q}}(1 + \sqrt{-5}) = 6$ so if $1 + \sqrt{-5} = ab$ with $a, b \in \mathcal{O}_K$, then either a, b have norms $\pm 1, \pm 6$ or $\pm 2, \pm 3$ (in some order). There are no elements of $\mathcal{O}_K$ of norm 2 (because the equation $x^2 + 5y^2 = 2$ has no solutions in rational integers), so the norms of a, b must be $\pm 1, \pm 6$. But by Lemma 35, if one of a, b has norm ± 1, then it is a unit in $\mathcal{O}_K$. This shows that $1 + \sqrt{-5}$ is irreducible.

To show that our two factorisations of 6 in $\mathcal{O}_K$ are truly different, observe that $\mathrm{Nm}_{K/\mathbb{Q}}(2) = 4$ is not equal to $\mathrm{Nm}_{K/\mathbb{Q}}(1 + \sqrt{-5}) = \mathrm{Nm}_{K/\mathbb{Q}}(1 - \sqrt{-5}) = 6$ so 2 is not an associate of either $1 + \sqrt{-5}$ or $1 - \sqrt{-5}$.

Thus $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Looking at the factorisation above, we see that $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

Since $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it cannot be a PID. An example of a non-principal ideal is $I = \langle 2, 1 + \sqrt{-5}\rangle$. Indeed, if $I = \langle a\rangle$ then a divides both 2 and $1 + \sqrt{-5}$. Since 2 and $1 + \sqrt{-5}$ are irreducible but not associates of each other, this forces a to be a unit and so $1 \in I$. However, one can check that every element of I has the form $x + y\sqrt{-5}$ with $x \equiv y \bmod 2$ so $1 + 0\sqrt{-5} \notin I$.

Product of ideals.

It will turn out that while not all rings of integers are UFDs, they always have unique factorisation of ideals. In order for this to make sense, we need to define the product of ideals.

Let R be a ring and let $\mathfrak{a}, \mathfrak{b}$ be ideals in R. The set $\{ab : a \in \mathfrak{a}, b \in \mathfrak{b}\}$ is not necessarily an ideal because it might not be closed under addition (to find an example of this, you will need both $\mathfrak{a}$ and $\mathfrak{b}$ to be non-principal). Instead we define

$$\mathfrak{ab} = \{a_1 b_1 + \cdots + a_m b_m : m \in \mathbb{N},\ a_1, \ldots, a_m \in \mathfrak{a},\ b_1, \ldots, b_m \in \mathfrak{b}\}.$$

This is an ideal in R.

If $\mathfrak{a} = \langle a_1, \ldots, a_r \rangle$ and $\mathfrak{b} = \langle b_1, \ldots, b_s \rangle$, then

$$\mathfrak{ab} = \langle a_i b_j : 1 \leq i \leq r,\, 1 \leq j \leq s \rangle.$$

e.g. We will calculate the square of the ideal $\langle 2, 1 + \sqrt{-5} \rangle$ in $\mathbb{Z}[\sqrt{-5}]$.

$$\begin{aligned} I = \langle 2, 1 + \sqrt{-5} \rangle^2 &= \langle 2 \cdot 2,\ 2(1 + \sqrt{-5}),\ (1 + \sqrt{-5})(1 + \sqrt{-5}) \rangle \\ &= \langle 4,\ 2 + 2\sqrt{-5},\ -4 + 2\sqrt{-5} \rangle. \end{aligned}$$

Now $(2 + 2\sqrt{-5}) + (-4 + 2\sqrt{-5}) = -2 \in I$ so $2 \in I$ and hence $\langle 2 \rangle \subseteq I$.
Meanwhile 2 divides all of 4, $2 + 2\sqrt{-5}$, $-4 + 2\sqrt{-5}$ so $I \subseteq \langle 2 \rangle$.
Thus $\langle 2, 1 + \sqrt{-5} \rangle^2 = \langle 2 \rangle$.

We see that the square of a non-principal ideal can be principal. Of course it doesn't always happen that a product of ideals is principal, but it usually does happen that after working out the products of all pairs of generators, you can reduce down to a smaller number of generators by taking some combinations.

15. Prime and maximal ideals

Prime and maximal ideals.

Yesterday we defined prime *elements* in an integral domain. Today we make the analogous definition for ideals. I don't think the following definitions were in Algebra 2. (You might have come across them in Commutative Algebra.)

Definition. Let R be a ring. An ideal $\mathfrak{a} \subseteq R$ is:

- **prime** if $\mathfrak{a} \neq R$ and for all $x, y \in R$ if $xy \in \mathfrak{a}$, then $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$;
- **maximal** if $\mathfrak{a} \neq R$ and there is no ideal $\mathfrak{b}$ satisfying $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$.

Observe that for $a \neq 0$, the principal ideal $\langle a \rangle$ is prime if and only if a is a prime element. (It's a historical quirk that the element 0 is defined not to be prime, but the ideal $\langle 0 \rangle$ can be prime – in fact $\langle 0 \rangle$ is prime if and only if R is an integral domain.)

These properties of ideals are closely related to properties of the quotient ring.

Lemma 36. *Let R be a ring and let $\mathfrak{a} \subseteq R$ be an ideal.*

(i) $\mathfrak{a}$ is a prime ideal if and only if $R/\mathfrak{a}$ is an integral domain.
(ii) $\mathfrak{a}$ is a maximal ideal if and only if $R/\mathfrak{a}$ is a field.

Proof. (This proof is pure algebra and non-examinable.)

(i) Consider $x + \mathfrak{a}$, $y + \mathfrak{a} \in R/\mathfrak{a}$. Then

$$(x + \mathfrak{a})(y + \mathfrak{a}) = 0 \text{ in } R/\mathfrak{a} \quad \Leftrightarrow \quad xy \in \mathfrak{a}$$

and hence the definition of $\mathfrak{a}$ being a prime ideal is equivalent to

$$(x + \mathfrak{a})(y + \mathfrak{a}) = 0 \quad \Rightarrow \quad x + \mathfrak{a} = 0 \text{ or } y + \mathfrak{a} = 0$$

i.e. the definition of $R/\mathfrak{a}$ being an integral domain.

(ii) The map $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ is a bijection from {ideals of R containing $\mathfrak{a}$} to {ideals of $R/\mathfrak{a}$}. Thus $\mathfrak{a}$ is a maximal ideal of R if and only if $R/\mathfrak{a}$ contains no ideals except $\{0\}$ and $R/\mathfrak{a}$ itself. A ring is a field if and only if its only proper ideal is $\{0\}$. □

Corollary. *In any ring R, every maximal ideal is prime.*

Proof. If $\mathfrak{a} \subseteq R$ is a maximal ideal, then $R/\mathfrak{a}$ is a field. Hence $R/\mathfrak{a}$ is an integral domain, so $\mathfrak{a}$ is a prime ideal. □

Whenever we form a product of ideals $\mathfrak{ab}$, we have $\mathfrak{ab} \subseteq \mathfrak{a}$ (because $\mathfrak{b} \subseteq R$. Thus multiplying ideals makes them smaller as sets, so the following definition is reasonable.

Definition. Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ be ideals. We say that $\mathfrak{a}$ **divides** $\mathfrak{b}$ (written $\mathfrak{a} \mid \mathfrak{b}$) if $\mathfrak{b} \subseteq \mathfrak{a}$.

As further justification for this definition, consider principal ideals. For any $\alpha, \beta \in R$, we have

$$\alpha \mid \beta \quad \Leftrightarrow \quad \langle \beta \rangle \subseteq \langle \alpha \rangle \quad \Leftrightarrow \quad \langle \alpha \rangle \mid \langle \beta \rangle.$$

We can use this to give an alternative (equivalent) definition of a prime ideal which looks much more like the definition of prime element.

Lemma 37. *Let R be any ring and let $\mathfrak{p}$ be a proper ideal in R. Then $\mathfrak{p}$ is a prime ideal if and only if, for all ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$, whenever $\mathfrak{p} \mid \mathfrak{ab}$, then $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.*

Proof. (Again this purely algebraic proof is non-examinable.)

Let $\mathfrak{p}$ be a prime ideal. Suppose for contradiction that $\mathfrak{p} \mid \mathfrak{ab}$ but $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid \mathfrak{b}$. Then $\mathfrak{a} \not\subseteq \mathfrak{p}$ so we can pick $x \in \mathfrak{a} \setminus \mathfrak{p}$. Similarly we can pick $y \in \mathfrak{b} \setminus \mathfrak{p}$. Then $xy \in \mathfrak{ab} \subseteq \mathfrak{p}$. So the definition of prime ideal tells us that $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, which contradicts how we chose x and y.

Conversely, suppose that $\mathfrak{p}$ satisfies the condition of the lemma and let $x, y \in R$ satisfy $xy \in \mathfrak{p}$. Then $\mathfrak{p} \mid \langle x \rangle \langle y \rangle$ so by the condition, $\mathfrak{p} \mid \langle x \rangle$ or $\mathfrak{p} \mid \langle y \rangle$. Thus $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ i.e. $\mathfrak{p}$ is prime. □

Ideals in the ring of integers of a number field.

Now we turn to properties which are special for the ring of integers of a number field.

Lemma 38. *Let K be a number field. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. If $x \in \mathfrak{a}$, then $\mathrm{Nm}_{K/\mathbb{Q}}(x) \in \mathfrak{a}$.*

Proof. This is similar to the proof that if $\mathrm{Nm}_{K/\mathbb{Q}}(x) = \pm 1$, then x is a unit. Assume that $K \subseteq \mathbb{C}$ and label the embeddings of K as $\sigma_1, \ldots, \sigma_n$, so that σ_1 is the inclusion $K \to \mathbb{C}$. Let $y = \sigma_2(x)\sigma_3(x) \cdots \sigma_n(x)$. Then

$$xy = \sigma_1(x)\sigma_2(x) \cdots \sigma_n(x) = \mathrm{Nm}_{K/\mathbb{Q}}(x).$$

Since $\mathrm{Nm}_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ and $x \in K$, we deduce that $y = \mathrm{Nm}_{K/\mathbb{Q}}(x)/x \in K$. Since $\sigma_2(x), \ldots, \sigma_n(x)$ are all algebraic integers, y is an algebraic integer. Hence $y \in \mathcal{O}_K$. Since $x \in \mathfrak{a}$ and $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$, we deduce that $xy \in \mathfrak{a}$. □

Consequence: if $\mathfrak{a}$ is a non-zero ideal in $\mathcal{O}_K$, then it contains a non-zero rational integer (pick any $x \in \mathfrak{a} \setminus \{0\}$ and then $\mathrm{Nm}_{K/\mathbb{Q}}(x)$ is a non-zero rational integer).

Lemma 39. *Let K be a number field. Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$. Then $\mathcal{O}_K/\mathfrak{a}$ is finite.*

Proof. Thanks to Lemma 38, $\mathfrak{a}$ contains a rational integer N. Then $\langle N \rangle \subseteq \mathfrak{a}$ and so $\mathcal{O}_K/\langle N \rangle$ surjects onto $\mathcal{O}_K/\mathfrak{a}$.

Because of the existence of an integral basis, $\mathcal{O}_K$ is isomorphic as an abelian group to $\mathbb{Z}^n$. Hence $\mathcal{O}_K/\langle N \rangle$ is isomorphic as an abelian group to $\mathbb{Z}/N\mathbb{Z}^n$ and this is finite. This implies that $\mathcal{O}_K/\mathfrak{a}$ is finite. □

Lemma 39 is a very special property of subrings of a number field – very few other integral domains have this property. (One example which does is $F[X]$ where F is a finite field. It turns out that you can do a lot of things very similar to Algebraic Number Theory in $F[X]$ or its finite extensions – called *function field arithmetic*.)

Definition. Let K be a number field and let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$. The **norm** of $\mathfrak{a}$, written $\mathrm{Nm}(\mathfrak{a})$, is defined to be $[\mathcal{O}_K : \mathfrak{a}]$ (meaning the index of $\mathfrak{a}$ as an abelian subgroup of $(\mathcal{O}_K, +)$).

This definition makes sense because of Lemma 39, and $\mathrm{Nm}(\mathfrak{a})$ is always a positive integer.

We have now defined the "norm of an element of K" and the "norm of an ideal in $\mathcal{O}_K$." The definitions look completely different, but they are compatible in the case of principal ideals, as the following lemma shows (except that the norm of an ideal is always positive, while the norm of an element may be positive or negative, so we need to take the absolute value).

Lemma 40. *Let K be a number field and let $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then*

$$\mathrm{Nm}(\langle\alpha\rangle) = |\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)|.$$

Proof. Choose an integral basis $\beta_1, \ldots, \beta_n$ for K. Let C be the matrix (with entries in $\mathbb{Q}$) representing "multiplication by α" with respect to this basis. Thus

$$\alpha\beta_j = \sum_{i=1}^{n} C_{ij}\alpha_i.$$

Then $\alpha\beta_1, \ldots, \alpha\beta_n$ form a $\mathbb{Z}$-basis for the ideal $\langle\alpha\rangle$ and C is the the change-of-basis matrix from $\{\alpha\beta_1, \ldots, \alpha\beta_n\}$ to $\{\beta_1, \ldots, \beta_n\}$. The argument from the proof of Lemma 29 shows that

$$[\mathcal{O}_K : \langle\alpha\rangle] = |\det(C)|.$$

Meanwhile the definition of norm of an element says that

$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \det(C). \qquad \square$$

Prime and maximal ideals in a number field.

(There is no Lemma 41 because I skipped it out in the numbering during the lecture.)

Lemma 42. *A finite integral domain is a field.*

Proof. (This proof is pure algebra, but it is fundamental to the properties of $\mathcal{O}_K$, so it is examinable.)

Let R be a finite integral domain and let $x \in R \setminus \{0\}$. The map $m_x \colon R \to R$ given by $m_x(y) = xy$ is injective because R is an integral domain. Since R is finite, this implies that m_x is a bijection $R \to R$. Thus there exists $y \in R$ such that $m_x(y) = 1$. In other words, y is a multiplicative inverse for x. $\square$

Corollary 43. *In the ring of integers of a number field, every non-zero prime ideal is maximal.*

Proof. Let $\mathfrak{a}$ be a non-zero prime ideal in $\mathcal{O}_K$. By Lemma 39, $\mathcal{O}_K/\mathfrak{a}$ is finite. Since $\mathfrak{a}$ is a prime ideal, $\mathcal{O}_K/\mathfrak{a}$ is an integral domain. Hence by Lemma 42, $\mathcal{O}_K/\mathfrak{a}$ is a field and so $\mathfrak{a}$ is a maximal ideal. $\square$

This property is not quite as special as Lemma 39. For example all rings $K[X]$ possess it where K is any field, but not the two-variable polynomial rings $K[X, Y]$. From the perspective of Algebraic Geometry, this corollary can be interpreted as saying that "$\mathcal{O}_K$ is a one-dimensional geometric object" (in a very abstract sense).

Lemma 44. *Every proper ideal in $\mathcal{O}_K$ is contained in a maximal ideal.*

Proof. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a proper ideal. Let S be the set of proper ideals of $\mathcal{O}_K$ which contain $\mathfrak{a}$. S is non-empty because $\mathfrak{a} \in S$. Since every non-zero ideal has a norm which is a positive integer, we can choose an element $\mathfrak{b} \in S$ of minimum norm.

We claim that $\mathfrak{b}$ is a maximal ideal. Indeed, if there is some ideal $\mathfrak{c}$ such that $\mathfrak{b} \subsetneq \mathfrak{c} \subsetneq \mathcal{O}_K$, then $\mathfrak{c}$ is a proper ideal and $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$ so $\mathfrak{c} \in S$. But because $\mathfrak{c} \subsetneq \mathfrak{b}$, $\mathrm{Nm}(\mathfrak{c}) < \mathrm{Nm}(\mathfrak{b})$, contradicting the fact that $\mathfrak{b}$ has minimal norm. □

This will be a proof strategy we will use several times: form a set of ideals, pick an ideal in the set of smallest norm, then prove that actually there must be an ideal of smaller norm in the set to get a contradiction. It is a bit of a cheat to use ideal norms in this strategy: really we are using the fact that $\mathcal{O}_K$ is a Noetherian ring (which you may have encountered in Rings and Modules, or maybe in Commutative Algebra) – but using ideal norms allows us to avoid introducing the concept of Noetherian rings.

16. Fractional ideals

Fractional ideals.

Our goal for the next two lectures will be to prove the unique factorisation of ideals in the ring of integers of a number field. One of the key tools, both in this proof and for the rest of the course, will be fractional ideals. Confusingly, a fractional ideal is not necessarily an ideal!

Definition. Let K be a number field. A **fractional ideal** of $\mathcal{O}_K$ is a subset $\mathfrak{a} \subseteq K$ satisfying the following conditions.

(a) if $x, y \in \mathfrak{a}$, then $x + y \in \mathfrak{a}$;
(b) $x\mathfrak{a} \subseteq \mathfrak{a}$ for every $x \in \mathcal{O}_K$;
(c) there exists some non-zero $x \in \mathcal{O}_K$ such that $x\mathfrak{a} \subseteq \mathcal{O}_K$.

Conditions (a) and (b) are the ordinary conditions from the definition of an ideal of $\mathcal{O}_K$. However, a fractional ideal doesn't have to be an ideal of $\mathcal{O}_K$ because it might not be contained in $\mathcal{O}_K$. (Also, it won't be an ideal of K because K is a field so its only ideals are 0 and K itself.) Condition (c) says that a fractional ideal is not too far away from being contained in $\mathcal{O}_K$ (for example, it implies that K itself is not a fractional ideal).

e.g. For $\mathbb{Z}$, $\langle \frac{1}{2} \rangle := \frac{1}{2}\mathbb{Z}$ is a fractional ideal which is not contained in $\mathbb{Z}$.

More generally, for any number field K and any $\alpha \in K$, we can form the principal fractional ideal $\langle \alpha \rangle := \alpha\mathcal{O}_K$. This will be an ideal of $\mathcal{O}_K$ if and only if $\alpha \in \mathcal{O}_K$.

The following is clear.

Lemma 45. *An ideal of $\mathcal{O}_K$ is a fractional ideal.*
A fractional ideal is an ideal of $\mathcal{O}_K$ if and only if it is contained in $\mathcal{O}_K$.

The following lemma justifies the idea that "fractional ideals are fractions of ideals."

Lemma 46. *A subset $\mathfrak{a} \subseteq K$ is a fractional ideal if and only if there exist an ideal $\mathfrak{b} \subseteq \mathcal{O}_K$ and an element $x \in \mathcal{O}_K$ such that $\mathfrak{a} = \frac{1}{x}\mathfrak{b}$.*

Proof. It is clear that, if $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$ and $x \in \mathcal{O}_K$, then $\frac{1}{x}\mathfrak{b}$ is a fractional ideal.

Conversely, if $\mathfrak{a}$ is a fractional ideal then condition (c) gives us $x \in \mathcal{O}_K$ such that $x\mathfrak{a} \subseteq \mathcal{O}_K$. Thanks to conditions (a) and (b), $\mathfrak{b} = x\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and we have $\mathfrak{a} = \frac{1}{x}\mathfrak{b}$. □

Thanks to Lemma 38, we can actually arrange that $x \in \mathbb{Z}$ in Lemma 46 (thus we get an "ideal version" of Lemma 23).

We can define the product of two fractional ideals in the same way as the product of two ideals: $\mathfrak{ab}$ is the set of all finite sums $a_1b_1 + \cdots + a_mb_m$ where $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$. The product of fractional ideals is a fractional ideal (you can prove this directly, or use Lemma 46).

One of the benefits of working with fractional ideals instead of ideals is that the non-zero fractional ideals form a group under this multiplication operation. We will not be able to prove this until after we have proved unique factorisation of ideals. For now, we define a fractional ideal which will ultimately turn out to be the inverse of $\mathfrak{a}$.

Definition. Let $\mathfrak{a}$ be a non-zero fractional ideal of $\mathcal{O}_K$. We define $\mathfrak{a}^{-1}$ to be

$$\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

The notation suggests that $\mathfrak{a}^{-1}$ should be an inverse to $\mathfrak{a}$, but that is not the definition! So we have to be careful not to use $\mathfrak{a}^{-1}$ as an inverse to $\mathfrak{a}$ until we have proved that it actually is an inverse.

e.g. if $\alpha \in K \setminus \{0\}$, then

$$\begin{aligned}\langle\alpha\rangle^{-1} = \{x \in K : x\langle\alpha\rangle \subseteq \mathcal{O}_K\} &= \{x \in K : x\alpha \in \mathcal{O}_K\} \\ &= \{x \in K : x \in \tfrac{1}{\alpha}\mathcal{O}_K\} = \left\langle \tfrac{1}{\alpha} \right\rangle.\end{aligned}$$

Lemma 47. *$\mathfrak{a}^{-1}$ is a fractional ideal of $\mathcal{O}_K$, and $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$.*

Proof. If $x \in \mathfrak{a}^{-1}$ and $y \in \mathfrak{a}$, then the definition of $\mathfrak{a}^{-1}$ shows that $xy \in \mathcal{O}_K$. Hence $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$.

To show that $\mathfrak{a}^{-1}$ is a fractional ideal: conditions (a) and (b) are clear. If we pick any $x \in \mathfrak{a} \setminus \{0\}$, then (from the previous paragraph) $x\mathfrak{a} \subseteq \mathcal{O}_K$ so condition (c) is satisfied. □

Factorisation of ideals.

We have seen that the ring of integers of a number field is not always a UFD. One of the central results of this module is that it does have unique factorisation *of ideals into prime ideals.*

Theorem 48. *Let $\mathcal{O}_K$ be the ring of integers of a number field and let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero proper ideal. Then:*

(i) there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$;

(ii) if we have another list of prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$, then $r = s$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are a permutation of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$.

Note that the uniqueness condition is simpler than for a UFD: because we are talking about ideals instead of elements, we don't need to mention associates (if x, y are associates, then they generate the same ideal).

This looks a bit like primary decomposition, which you might encounter in Commutative Algebra. However primary decomposition is much weaker, because it involves intersection of ideals rather than products and primary ideals rather than prime ideals. This allows primary decomposition to work in any Noetherian ring, while Theorem 48 is a special property of rings of integers of a number field.

The proof of Theorem 48 goes through a number of steps. Several of these steps will prove things which "obviously should be true" but each step depends on the previous ones, often in quite a subtle way, so we have to be careful to prove them in the right order.

Step 1. *Every non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ has the following property:*
(*) there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Proof. Suppose that the claim is false. So there exists at least one ideal which does *not* have property (*).

We use the same strategy as for the proof of Lemma 44: among the non-zero ideals of $\mathcal{O}_K$ which do not have property (*), choose $\mathfrak{a}$ so that its norm is as small as possible. The minimum norm is attained because the norms of ideals are positive integers.

Now $\mathfrak{a}$ is not a prime ideal, otherwise we could just take $r = 1$, $\mathfrak{p}_1 = \mathfrak{a}$. Also $\mathfrak{a} \neq \mathcal{O}_K$, or we could just pick $r = 1$, $\mathfrak{p}_1 =$ any non-zero prime ideal.. Hence (negating the definition of a prime ideal) we can pick $x, y \in \mathcal{O}_K$ such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$.

Let $\mathfrak{b} = \langle \mathfrak{a}, x \rangle$ and $\mathfrak{c} = \langle \mathfrak{a}, y \rangle$. Then

$$\mathfrak{b}\mathfrak{c} = \mathfrak{a}^2 + x\mathfrak{a} + y\mathfrak{a} + \langle xy \rangle \subseteq \mathfrak{a}.$$

Since $\mathfrak{a} \subseteq \mathfrak{b}$, we have a surjection $\mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{b}$. Since $x \notin \mathfrak{a}$, this surjection is not injective. Hence $\mathrm{Nm}(\mathfrak{b}) < \mathrm{Nm}(\mathfrak{a})$. Because $\mathrm{Nm}(\mathfrak{a})$ was minimal (among non-zero ideals which do not have property (*)), $\mathfrak{b}$ has property (*) i.e. there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{b}$.

Similarly $\mathrm{Nm}(\mathfrak{c}) < \mathrm{Nm}(\mathfrak{a})$ and so $\mathfrak{c}$ does not have property (*) i.e. there are prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{c}$.

But now

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}$$

contradicting the fact that $\mathfrak{a}$ does not have property (*). □

Aside: just as with Lemma 44, we could replace "pick an ideal of smallest norm ..." by the fact that $\mathcal{O}_K$ is Noetherian. Thus Step 1 works for any Noetherian ring. The subsequent steps in the proof of Theorem 48 will use more special properties of the ring of integers of a number field.

17. Proof of unique factorisation of ideals

We complete the proof of the unique factorisation of ideals in $\mathcal{O}_K$ (Theorem 48).

Step 2. *If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal, then $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1}$.*

Proof. Since $\mathfrak{p} \subseteq \mathcal{O}_K$, we have $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$. The hard part is to prove that $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

We want to apply Step 1 but applying it directly to $\mathfrak{p}$ is no use, because $\mathfrak{p}$ is already a prime ideal. Instead, pick a non-zero element $\alpha \in \mathfrak{p}$ and apply Step 1 to $\langle \alpha \rangle$. We get non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \langle \alpha \rangle.$$

Choose these prime ideals so that r is as small as possible.

Since $\langle \alpha \rangle \subseteq \mathfrak{p}$, this implies that

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}.$$

Since $\mathfrak{p}$ is a prime ideal, Lemma 37 tells us that $\mathfrak{p}$ contains one of the $\mathfrak{p}_i$. WLOG $\mathfrak{p}_1 \subseteq \mathfrak{p}$. By Corollary 43, $\mathfrak{p}_1$ is maximal ideal of $\mathcal{O}_K$ and so $\mathfrak{p}_1 = \mathfrak{p}$.

Since we chose $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ so that r is as small as possible,

$$\mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_r \not\subseteq \langle \alpha \rangle.$$

Therefore we can choose $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ which is not in $\langle \alpha \rangle$. But $\beta \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r \subseteq \langle \alpha \rangle$. Therefore $\alpha^{-1}\beta\mathfrak{p} \subseteq \mathcal{O}_K$ i.e. $\alpha^{-1}\beta \in \mathfrak{p}^{-1}$. But since $\beta \notin \langle \alpha \rangle$, $\beta\alpha^{-1} \notin \mathcal{O}_K$. □

Aside: in Step 2, we used Corollary 43, so this no longer applies in an arbitrary Noetherian ring.

The next step is a bit of a break from all these calculations with ideals – it is more of a fact about algebraic integers than about ideals (and it definitely only applies to rings of the form $\mathcal{O}_K$).

CORRECTION. In the original version of these notes (and probably in the lectures), the proof of Step 3 said that $Bv = \beta v$ when it should be $B^T v = \beta v$. Since B and B^T have the same eigenvalues, this does not matter. It is now fixed.

Step 3. *If $\mathfrak{a} \subseteq \mathcal{O}_K$ is a non-zero ideal and $\beta \in K$ is such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$, then $\beta \in \mathcal{O}_K$.*

Proof. Assume that K is a subfield of $\mathbb{C}$, by Lemma 6.

Since $\mathfrak{a}$ is a subgroup of $\mathcal{O}_K$, it is a finitely generated torsion-free abelian group. Hence it has a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_m\}$. Since $\beta\mathfrak{a} \subseteq \mathfrak{a}$, the matrix B of β with respect to this basis has coefficients in $\mathbb{Z}$ i.e.

$$\beta\alpha_j = \sum_{i=1}^{m} B_{ij}\alpha_i$$

where $B_{ij} \in \mathbb{Z}$.

Let $\underline{v}$ be the column vector $(\alpha_1, \ldots, \alpha_m)^t \in \mathbb{C}^m$. Then

$$B^T \underline{v} = \beta \underline{v}$$

and so β is an eigenvalue of B^T. Thus β is a root of the characteristic polynomial of B^T, which is a monic polynomial with integer coefficients. So β is an algebraic integer. □

Now we can put the previous steps together. The next step looks like a small strengthening of Step 2, but it is actually a big step forward because it uses Step 3 as well.

Step 4. *If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal and $\mathfrak{a} \subseteq \mathcal{O}_K$ is a non-zero ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$, then $\mathfrak{a} \subsetneq \mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$.*

Proof. Since $1 \in \mathfrak{p}^{-1}$, it is clear that $\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a}$. Since $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ and so $\mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$.

The key point is proving that $\mathfrak{a} \neq \mathfrak{p}^{-1}\mathfrak{a}$. Assume for contradiction that $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$. Then for every $\beta \in \mathfrak{p}^{-1}$, we have $\beta\mathfrak{p} \subseteq \mathfrak{p}$. Hence by Step 3, $\beta \in \mathcal{O}_K$.

Thus $\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$, contradicting Step 2. □

Now it is quite easy to prove that "$\mathfrak{p}^{-1}$" means what we expect, at least for prime ideals (the general case will come tomorrow).

Step 5. *If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a non-zero prime ideal, then $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.*

Proof. We know that $\mathfrak{p}\mathfrak{p}^{-1}$ is a fractional ideal contained in $\mathcal{O}_K$, so $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal of $\mathcal{O}_K$. By Step 4, we have $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1}$. Since $\mathfrak{p}$ is a maximal ideal, this implies that $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. □

At last we can prove existence and uniqueness of factorisation of ideals.

Step 6 (Existence of factorisation into prime ideals)**.** *For any non-zero proper ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$.*

Proof. This strengthens Step 1 because $\mathfrak{a}$ is equal to the product, rather than containing it. The proof strategy will be the same as for Step 1, but making use of all the steps we have proved since then.

Assume for contradiction that there exists some non-zero proper ideal of $\mathcal{O}_K$ which is not a product of prime ideals. Choose such an ideal $\mathfrak{a}$ so that $\mathrm{Nm}(\mathfrak{a})$ is as small as possible.

By Lemma 44, $\mathfrak{a} \subseteq \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$.

By Step 4, $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ which strictly contains $\mathfrak{a}$. Hence $\mathrm{Nm}(\mathfrak{p}^{-1}\mathfrak{a}) < \mathrm{Nm}(\mathfrak{a})$. Assume that $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathcal{O}_K$ (we'll return to the case $\mathfrak{p}^{-1}\mathfrak{a} = \mathcal{O}_K$ later). Then because $\mathrm{Nm}(\mathfrak{a})$ was as small as possible, $\mathfrak{p}^{-1}\mathfrak{a}$ is equal to a product of prime ideals i.e.

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

for some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Multiplying on both sides by $\mathfrak{p}$ and using Step 5, we get

$$\mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{a} = \mathcal{O}_K\mathfrak{a} = \mathfrak{a}.$$

This contradicts our assumption that $\mathfrak{a}$ was not a product of prime ideals.

We still have to deal with the case $\mathfrak{p}^{-1}\mathfrak{a} = \mathcal{O}_K$. We do the same thing: multiply on both sides by $\mathfrak{p}$ and use Step 5 to get

$$\mathfrak{p} = \mathfrak{p}\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{a} = \mathcal{O}_K\mathfrak{a} = \mathfrak{a}$$

so $\mathfrak{a}$ is a product of prime ideals (of the single ideal $\mathfrak{p}$). □

Step 7 (Uniqueness of factorisation into prime ideals)**.** *Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal and suppose that*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals. Then $r = s$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ form a permutation of $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$.

Proof. We proceed by induction on r.

If $r = 0$, then $\mathfrak{a} = \mathcal{O}_K$ and $s = 0$ so there is nothing to prove. (If you are not comfortable thinking of $\mathcal{O}_K$ as being the product of "the empty list of prime ideals," you can interpret this as meaning that the proof for $r = 1$ is the same as the proof for $r > 1$.)

If $r \geq 1$, since $\mathfrak{p}_1 \mid \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_r$ and the $\mathfrak{q}_i$ are prime ideals, by Lemma 37, we must have $\mathfrak{p}_1 \mid \mathfrak{q}_j$ for some j. WLOG $\mathfrak{p}_1 \mid \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is a maximal ideal, this implies that $\mathfrak{p}_1 = \mathfrak{q}_1$. Hence using Step 5 twice,

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{q}_1^{-1}\mathfrak{a} = \mathfrak{q}_1^{-1}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

By induction, we conclude that $r-1 = s-1$ and that $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are a permutation of $\mathfrak{q}_2, \ldots, \mathfrak{q}_s$. □

This completes the proof of Theorem 48.

Aside (non-examinable, for people with an interest in commutative algebra or algebraic geometry):

Looking back over the proof of Theorem 48, the properties of $\mathcal{O}_K$ which we used were:

(1) $\mathcal{O}_K$ is Noetherian (in Steps 1 and 6);
(2) every non-zero prime ideal is maximal (in Step 2);
(3) if $\alpha \in K$ is a root of a monic polynomial in $\mathcal{O}_K[X]$, then $\alpha \in \mathcal{O}_K$ (this is called "integral closedness" and is the property which makes Step 3 work).

An integral domain with these properties is called a **Dedekind domain** and Theorem 48 works in any Dedekind domain. Besides $\mathcal{O}_K$, the other important example are rings of the form $K[X]$ where K is any field, and "finite extensions of $K[X]$" which have a geometrical interpretation as "the ring of functions on a smooth curve."

18. Properties of ideals of number fields

Group of fractional ideals.

We promised to prove that fractional ideals form a group. This is an easy consequence of the unique factorisation of ideals.

First we extend Step 5 from prime ideals to all ideals.

Lemma 49. *Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal. Then $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.*

Proof. We can write $\mathfrak{a}$ as a product of prime ideals: $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$.

Let $\mathfrak{b} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\cdots\mathfrak{p}_r^{-1}$. By applying Step 5 repeatedly, we see that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$. Hence by the definition of $\mathfrak{a}^{-1}$, we have $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$.

Using the facts that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$ (just proved) and $\mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$ (Lemma 47), we have

$$\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathcal{O}_K = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} \subseteq \mathcal{O}_K\mathfrak{b} = \mathfrak{b}.$$

Thus $\mathfrak{b} = \mathfrak{a}^{-1}$. □

Proposition 50. *Let K be a number field. The set of non-zero fractional ideals of $\mathcal{O}_K$ forms an abelian group under the operation of multiplication, with $\langle 1\rangle = \mathcal{O}_K$ being the identity element. The inverse of $\mathfrak{a}$ is $\mathfrak{a}^{-1}$.*

Proof. Associativity and commutativity and the fact that $\mathcal{O}_K$ is the identity element are obvious. Inverses is basically Lemma 49, but we have to check that it works for fractional ideals as well as ideals in $\mathcal{O}_K$.

Let $\mathfrak{a}$ be a non-zero fractional ideal. By Lemma 46, we can write $\mathfrak{a} = \frac{1}{x}\mathfrak{b}$ for some $x \in \mathcal{O}_K$ and an ideal $\mathfrak{b} \subseteq \mathcal{O}_K$. We can see from the definition of $\mathfrak{a}^{-1}$ that $\mathfrak{a}^{-1} = x\mathfrak{b}^{-1}$. Then by Lemma 49,

$$\mathfrak{a}\mathfrak{a}^{-1} = x^{-1}\mathfrak{b}\, x\mathfrak{b}^{-1} = x^{-1}x\,\mathfrak{b}\mathfrak{b}^{-1} = 1\cdot\mathcal{O}_K = \mathcal{O}_K.$$ □

Recall that we defined $\mathfrak{a} \mid \mathfrak{b}$ to mean $\mathfrak{b} \subseteq \mathfrak{a}$. This looks rather different from the definition of divisibility of elements $a \mid b$ which says "there exists c such that $b = ac$." We can now verify that our definition of $\mathfrak{a} \mid \mathfrak{b}$ is actually equivalent to an "ideal version" of the definition for elements.

Lemma 51. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathcal{O}_K$ such that $\mathfrak{b} \subseteq \mathfrak{a}$ (i.e. $\mathfrak{a} \mid \mathfrak{b}$). Then there exists an ideal $\mathfrak{c} \subseteq \mathcal{O}_K$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

Proof. Let $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$. Since $\mathfrak{b} \subseteq \mathfrak{a}$, we have $\mathfrak{c} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$. Thus $\mathfrak{c}$ is an ideal of $\mathcal{O}_K$ (not just a fractional ideal). By Lemma 49,

$$\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_K\mathfrak{b} = \mathfrak{b}.$$ □

Ideal norms are multiplicative.

Now we prove a much harder, but fundamental, fact about the norms of ideals: when we multiply ideals, the ideals multiply. The analogous statement for *elements* of a number field was immediate from the definition. But for ideals, we will have to use unique factorisation – and even then it is non-trivial.

We begin with the case of multiplying by a prime ideal.

Lemma 52. *Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. Then*

$$[\mathfrak{a} : \mathfrak{ap}] = [\mathcal{O}_K : \mathfrak{p}].$$

Proof. Since $\mathfrak{p} \neq \mathcal{O}_K$ and the fractional ideals form a group, $\mathfrak{a} \neq \mathfrak{ap}$. Hence we can choose $\alpha \in \mathfrak{a} \setminus \mathfrak{ap}$.

Let $\mathfrak{b} = \langle \alpha, \mathfrak{ap} \rangle$. Then $\mathfrak{b}$ is an ideal and $\mathfrak{ap} \subsetneq \mathfrak{b} \subseteq \mathfrak{a}$. Multiplying by $\mathfrak{a}^{-1}$, we get $\mathfrak{p} \subsetneq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K$. Now $\mathfrak{p}$ is a maximal ideal (Corollary 43), so this implies that $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_K$ i.e. $\mathfrak{a} = \mathfrak{b}$.

Define a group homomorphism (of the additive groups) $\phi\colon \mathcal{O}_K \to \mathfrak{a}/\mathfrak{ap}$ by

$$\phi(x) = x\alpha + \mathfrak{ap}.$$

We want to apply the First Isomorphism Theorem to ϕ, in order to obtain an isomorphism $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$.

Claim: ϕ is surjective. Indeed, if $y + \mathfrak{ap} \in \mathfrak{a}/\mathfrak{ap}$, then we have

$$y \in \mathfrak{a} = \mathfrak{b} = \langle \alpha, \mathfrak{ap} \rangle$$

so we can write $y = x\alpha + z$ where $x \in \mathcal{O}_K$ and $z \in \mathfrak{ap}$. Then $y + \mathfrak{ap} = \phi(x)$, so ϕ is surjective.

Claim: $\ker(\phi) = \mathfrak{p}$. Indeed,

$$\ker(\phi) = \{x \in \mathcal{O}_K : x\alpha \in \mathfrak{ap}\} = \mathcal{O}_K \cap \alpha^{-1}\mathfrak{ap}.$$

Now $\alpha^{-1}\mathfrak{ap}$ is a fractional ideal, so $\mathcal{O}_K \cap \alpha^{-1}\mathfrak{ap}$ is an ideal in $\mathcal{O}_K$. (Note: it was not obvious that $\ker(\phi)$ was an ideal, because ϕ is only a group homomorphism and not a ring homomorphism.)

Since $\alpha \in \mathfrak{a}$, $\mathfrak{p} \subseteq \ker(\phi)$. Since $\alpha \notin \mathfrak{ap}$, $\phi(1) = \alpha + \mathfrak{ap} \neq 0 + \mathfrak{ap}$ and so $\ker(\phi) \neq \mathcal{O}_K$. Thus $\ker(\phi)$ is an ideal and $\mathfrak{p} \subseteq \ker(\phi) \subsetneq \mathcal{O}_K$. Since $\mathfrak{p}$ is a maximal ideal, we must have $\ker(\phi) = \mathfrak{p}$.

Using both Claims, the First Isomorphism Theorem for groups tells us that

$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$$

as additive groups, and so $[\mathcal{O}_K : \mathfrak{p}] = [\mathfrak{a} : \mathfrak{ap}]$. □

Lemma 53. *Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal and let $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ be its factorisation into prime ideals. Then*

$$\mathrm{Nm}(\mathfrak{a}) = \mathrm{Nm}(\mathfrak{p}_1)\,\mathrm{Nm}(\mathfrak{p}_2) \cdots \mathrm{Nm}(\mathfrak{q}_r).$$

Proof. By induction on r. The case $r = 1$ is trivial.

When $r > 1$, let $\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{r-1}$. Then

$$\mathrm{Nm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = [\mathcal{O}_K : \mathfrak{b}][\mathfrak{b} : \mathfrak{a}]$$

(this follows from the Third Isomorphism Theorem for groups). By Lemma 52, we have

$$[\mathfrak{b} : \mathfrak{a}] = [\mathfrak{b} : \mathfrak{bp}] = [\mathcal{O}_K : \mathfrak{p}].$$

Thus

$$\mathrm{Nm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{b}][\mathcal{O}_K : \mathfrak{p}] = \mathrm{Nm}(\mathfrak{b})\,\mathrm{Nm}(\mathfrak{p})$$

and we conclude by induction. □

Corollary 54. *Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ be non-zero ideals. Then*

$$\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{b}).$$

Proof. Apply Lemma 53 to each of $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{ab}$. □

Easy facts about norms of ideals.

We prove a few basic facts which don't even require unique factorisation of ideals.

We have already used this first lemma (whenever we said "pick an ideal $\mathfrak{a}$ of smallest norm, construct $\mathfrak{b} \subsetneq \mathfrak{a}$, then $\mathrm{Nm}(\mathfrak{a}) < \mathrm{Nm}(\mathfrak{b})$), so really we should have proved it earlier! Since the proof doesn't use factorisation of ideals, this doesn't lead to a circular argument. It is pretty easy, but we include the proof for completeness.

Lemma 55. *Let $\mathfrak{a}, \mathfrak{b}$ be non-zero ideals in $\mathcal{O}_K$. If $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathrm{Nm}(\mathfrak{a}) = \mathrm{Nm}(\mathfrak{b})$, then $\mathfrak{a} = \mathfrak{b}$.*

Proof. Since $\mathfrak{a} \subseteq \mathfrak{b}$, we have

$$\mathrm{Nm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = [\mathcal{O}_K : \mathfrak{b}][\mathfrak{b} : \mathfrak{a}] = \mathrm{Nm}(\mathfrak{b})[\mathfrak{b} : \mathfrak{a}].$$

Hence if $\mathrm{Nm}(\mathfrak{a}) = \mathrm{Nm}(\mathfrak{b})$, then $[\mathfrak{b} : \mathfrak{a}] = 1$ or in other words $\mathfrak{a} = \mathfrak{b}$. □

One reason for explicitly stating Lemma 55 is the following consequence:
If $\alpha \in \mathfrak{a}$ and $|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| = \mathrm{Nm}(\mathfrak{a})$, then $\mathfrak{a} = \langle \alpha \rangle$.
This will be valuable later for as a method of proving that an ideal is principal: you just have to find an element of the ideal which has the correct norm.

This next lemma might remind you of Lemma 38 but it is not the same: Lemma 38 tells us that the norm of any *element* of $\mathfrak{a}$ is in $\mathfrak{a}$; now we prove that the norm of *the ideal itself* is in $\mathfrak{a}$.

Lemma 56. *Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a non-zero ideal. Then $\mathrm{Nm}(\mathfrak{a}) \in \mathfrak{a}$.*

Proof. Since $\mathrm{Nm}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$, Lagrange's theorem for the additive group $\mathcal{O}_K/\mathfrak{a}$ tells us that $\mathrm{Nm}(\mathfrak{a}) \cdot (1 + \mathfrak{a}) = 0$ in $\mathcal{O}_K/\mathfrak{a}$. In other words $\mathrm{Nm}(\mathfrak{a}) \in \mathfrak{a}$. □

19. Dedekind–Kummer theorem

Prime ideals of a number field.

We have shown that ideals in $\mathcal{O}_K$ have unique factorisation into prime ideals. Now we want to describe the prime ideals in $\mathcal{O}_K$.

Definition. We shall use the phrase **rational prime** to mean a prime in $\mathbb{Z}$ (just the usual meaning of prime number) – similar to how we sometimes say "rational integers" to avoid confusion with algebraic integers. The purpose of this is to avoid any possible confusion with "prime ideals in $\mathcal{O}_K$" (or even "prime elements in $\mathcal{O}_K$"). Sorry if it causes more confusion!

Proposition 57. *Let K be a number field. Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Then $\mathrm{Nm}(\mathfrak{p}) = p^n$ for some rational prime p and some positive integer n. Furthermore, $\mathfrak{p} \mid \langle p \rangle$ and $\mathfrak{p} \nmid \langle q \rangle$ for any rational prime $q \neq p$.*

Proof. By Corollary 43, $\mathfrak{p}$ is a maximal ideal so $\mathcal{O}_K/\mathfrak{p}$ is a field. Furthermore $\mathcal{O}_K/\mathfrak{p}$ is finite by Lemma 39. By a result from Algebra 2, the order of any finite field is a prime power. So

$$\mathrm{Nm}(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p} = p^n$$

for some p and n.

By Lemma 56, we deduce that $p^n \in \mathfrak{p}$. If $n > 1$, we write $p^n = p \cdot p^{n-1}$ and use the definition of prime ideal to deduce that either $p \in \mathfrak{a}$ or $p^{n-1} \in \mathfrak{p}$. If $p^{n-1} \in \mathfrak{p}$, then we can repeat the process; eventually we conclude that $p \in \mathfrak{p}$ or in other words $\mathfrak{p} \mid \langle p \rangle$.

Finally we want to show that there is no other rational prime $q \neq p$ such that $\mathfrak{p} \mid \langle q \rangle$. Assume for contradiction that such a prime exists. Then $q \in \mathfrak{p}$. By Euclid's algorithm, we can find $x, y \in \mathbb{Z}$ such that $xp + yq = 1$. Since $p, q \in \mathfrak{p}$, we deduce that $1 \in \mathfrak{p}$ and so $\mathfrak{p} = \mathcal{O}_K$. But this contradicts the fact that $\mathfrak{p}$ is a prime ideal. □

Dedekind–Kummer theorem: statement.

By Proposition 57, each non-zero prime ideal of $\mathcal{O}_K$ divides exactly one rational prime. Thus in order to determine the prime ideals of $\mathcal{O}_K$, we just have to determine the prime ideals which divide each rational prime. Because $\langle p \rangle$ has a unique factorisation into prime ideals of $\mathcal{O}_K$, there are finitely many prime ideals dividing p.

The Dedekind–Kummer theorem tells us how to find these ideals. The statement of the theorem may look rather long, but it gives a very clear recipe which we can apply in practice.

Notation. If p is a rational prime, we write $\mathbb{F}_p$ for "the field with p elements" i.e. $\mathbb{Z}/p\mathbb{Z}$. We use this notation to emphasise that it is a field (of course $\mathbb{Z}/p\mathbb{Z}$ is only a field when p is prime).

Theorem 58 (Dedekind–Kummer)**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field where α is an algebraic integer. Let p be a rational prime which does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.*

Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α, and let $\bar{f}(X) \in \mathbb{F}_p[X]$ denote the reduction of f modulo p. Let the factorisation of $\bar{f}$ into monic irreducible polynomials be

$$\bar{f} = \bar{f}_1^{e_1} \bar{f}_2^{e_2} \cdots \bar{f}_r^{e_r}$$

where $\bar{f}_1(X), \ldots, \bar{f}_r(X) \in \mathbb{F}_p[X]$ are pairwise distinct.

For each i, choose a polynomial $f_i(X) \in \mathbb{Z}[X]$ such that $\bar{f}_i = f_i$ modulo p.

Let $\mathfrak{p}_i$ denote the ideal $\langle p, f_i(\alpha)\rangle$ in $\mathcal{O}_K$.

Then:

(i) the $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_K$;
(ii) the $\mathfrak{p}_i$ are the only prime ideals in $\mathcal{O}_K$ dividing $\langle p\rangle$;
(iii) $\mathrm{Nm}(\mathfrak{p}_i) = p^{\deg(\bar{f}_i)}$;
(iv) $\langle p\rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

Most of the words of this theorem are just carefully defining notation for the factorisation of f mod p.

There is one condition which it is important not to forget: $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. We want to apply the Dedekind–Kummer theorem with $\mathcal{O}_K = \mathbb{Z}[\alpha]$ whenever possible, because then $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ and so the condition $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is satisfied for every prime p.

However, it is not always possible to choose α such that $\mathcal{O}_K = Z[\alpha]$ and then we have to exclude the finitely many primes which divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ when using the Dedekind–Kummer theorem.

Example of the Dedekind–Kummer theorem.

$K = \mathbb{Q}(\sqrt{-10})$

Since $-10 \equiv 2 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$. so we can apply Dedekind–Kummer with $\alpha = \sqrt{-10}$ for every rational prime p. The minimal polynomial of $\sqrt{-10}$ is $f(X) = X^2 + 10$.

- $p = 2$: $f(X) \equiv X^2 \bmod 2$.
  In the notation of Theorem 58, we have $r = 1$, $f_1(X) = X$, $e_1 = 2$.
  So the only prime ideal of $\mathcal{O}_K$ dividing $\langle 2\rangle$ is $\mathfrak{p}_1 = \langle 2, f_1(\alpha)\rangle = \langle 2, \sqrt{-10}\rangle$.
  By (iii), $\mathrm{Nm}(\langle 2, \sqrt{-10}\rangle) = 2^{\deg(X)} = 2^1 = 2$.
  By (iv), $\langle 2\rangle = \langle 2, \sqrt{-10}\rangle^2$.
- $p = 3$: $f(X) \equiv X^2 - 2 \bmod 3$. This is irreducible (because it is quadratic, it suffices to check that it has no roots; it has no roots because 2 is not a quadratic residue mod 3).
  Thus in the notation of Theorem 58, we have $r = 1$, $f_1(X) = X^2 - 2$, $e_1 = 1$.
  Hence the only prime ideal of $\mathcal{O}_K$ dividing $\langle 3\rangle$ is $\langle 3, \alpha^2 - 2\rangle = \langle 3, -12\rangle = \langle 3\rangle$.
  In fact, we could have deduced this without any calculations using (iv):

since $r = e_1 = 1$, (iv) tells us that $\langle p \rangle = \mathfrak{p}_1^{e_1} = \mathfrak{p}_1$.
This gives us a general conclusion (valid for any p and K):

If $\bar{f}(X)$ is irreducible in $\mathbb{F}_p[X]$, then $\langle p \rangle$ is a prime ideal of $\mathcal{O}_K$.

- $p = 5$: $\langle 5 \rangle = \langle 5, \sqrt{-10} \rangle^2$ (similar to $p = 2$).
- $p = 7$: $f(X) \equiv X^2 - 4 \equiv (X + 2)(X - 2) \mod 7$.
  In the notation of Theorem 58, we have $r = 2$, $f_1(X) = X - 2$, $f_2(X) = X + 2$, $e_1 = e_2 = 1$.
  Since $f(X)$ has two distinct irreducible factors, there are two prime ideals of $\mathcal{O}_K$ which divide $\langle 7 \rangle$, namely

  $$\langle 7, f_1(\alpha) \rangle = \langle 7, 2 + \sqrt{-10} \rangle \text{ and } \langle 7, f_2(\alpha) \rangle = \langle 7, -2 + \sqrt{-10} \rangle.$$

  By (iv),

  $$\langle 7 \rangle = \langle 7, 2 + \sqrt{-10} \rangle \langle 7, -2 + \sqrt{-10} \rangle.$$

  (You can check this product by hand!)

20. Proof of Dedekind–Kummer theorem

Another example of Dedekind–Kummer.

$K = \mathbb{Q}(\sqrt{-7})$

Since $-7 \equiv 1 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-7}}{2}$. The minimal polynomial of α is $f(X) = X^2 - X + 2$.

For $p = 2$, we have $f(X) \equiv X^2 - X \equiv X(X-1) \bmod 2$.

Thus $\langle 2 \rangle = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p} = \langle 2, \alpha \rangle = \langle 2, \frac{1+\sqrt{-7}}{2} \rangle$ and $\mathfrak{q} = \langle 2, \alpha - 1 \rangle = \langle 2, \frac{-1+\sqrt{-7}}{2} \rangle$.

In fact, $\mathrm{Nm}(\mathfrak{p}) = 2^{\deg(X)} = 2$ while $\mathrm{Nm}_{K/\mathbb{Q}}(\frac{1+\sqrt{-7}}{2}) = (\frac{1}{2})^2 + 7(\frac{1}{2})^2 = 2$ so

$$\mathfrak{p} = \Big\langle \frac{1+\sqrt{-7}}{2} \Big\rangle.$$

Similarly, $\mathfrak{q} = \langle \frac{-1+\sqrt{-7}}{2} \rangle$.

The Dedekind–Kummer theorem tells us that the ideals $\mathfrak{p}$ and $\mathfrak{q}$ are distinct. We could also see this directly because if $\mathfrak{p} = \mathfrak{q}$, then this ideal would contain $\alpha - (\alpha - 1) = 1$, contradicting the fact that it must be a proper ideal of $\mathcal{O}_K$.

We would have got the wrong answer if we tried to use $\alpha = \sqrt{-7}$ instead of $\frac{1+\sqrt{-7}}{2}$! The Dedekind–Kummer theorem is not valid for $p = 2$ and $\alpha = \sqrt{-7}$, because

$$[\mathcal{O}_K : \mathbb{Z}[\sqrt{-7}]] = 2,$$

so this is not a contradiction. Rather it is a warning that the condition $p \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt{-7}]]$ is important (and that making sure you use the correct ring of integers for a quadratic field is also important).

Indeed, the minimal polynomial of $\sqrt{-7}$ is $X^2 + 7 \equiv (X+1)^2 \bmod 2$, so if we (incorrectly) used Dedekind–Kummer for $\sqrt{-7}$ we would conclude that $\langle 2 \rangle$ is the square of a prime ideal, but we saw that in fact $\mathfrak{p}$ and $\mathfrak{q}$ are *distinct* prime ideals.

Note that, if $p \neq 2$, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt{17}]]$ so we can apply Dedekind–Kummer either for $\alpha = \frac{1+\sqrt{-7}}{2}$ or for $\alpha = \sqrt{-7}$ and both will give the right answer.

Proof of Dedekind–Kummer theorem.

This proof may look a bit intimidating because of its repeated use of the isomorphism theorems for rings and the heavy notation for elements in several different rings, but it is actually shorter and simpler than the proof of unique factorisation of ideals.

We recall the notation from the statement of Theorem 58:

Notation. *Let $K = \mathbb{Q}(\alpha)$ be a number field where α is an algebraic integer. Let p be a rational prime which does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.*

Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α, and let $\bar{f}(X) \in \mathbb{F}_p[X]$ denote the reduction of f modulo p. Let the factorisation of $\bar{f}$ into monic irreducible polynomials be

$$\bar{f} = \bar{f}_1^{e_1} \bar{f}_2^{e_2} \cdots \bar{f}_r^{e_r}$$

where $\bar{f}_1, \ldots, \bar{f}_r$ are pairwise distinct monic irreducible polynomials in $\mathbb{F}_p[X]$. For each i, let $f_i(X) \in \mathbb{Z}[X]$ be a polynomial in $\mathbb{Z}[X]$ such that $\bar{f}_i = f_i$ modulo p.

Let $\mathfrak{p}_i$ denote the ideal $\langle p, f_i(\alpha) \rangle_{\mathcal{O}_K}$.

Because we will need to work with ideals in several different rings, the notation $\langle\alpha\rangle$ might get confusing – it means the ideal generated by α, but in which ring? To avoid this confusion, we will often include the ring as a subscript: we will write $\langle\alpha\rangle_R$ to mean "the ideal of the ring R generated by α."

For simplicity, we shall assume that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ – in practice, this is usually the situation in which we shall want to use the Dedekind–Kummer theorem. (Without this assumption, it is not much harder – there is just an extra step showing that $\mathcal{O}_K/\langle p\rangle_{\mathcal{O}_K} \cong \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}$, which is where the hypothesis $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ gets used.)

The goal of the first few steps is to obtain a ring isomorphism

$$\mathbb{F}_p[X]/\langle\bar{f}\rangle_{\mathbb{F}_p[X]} \cong \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}.$$

We do this by constructing two homomorphisms from $\mathbb{Z}[X]$ to the two sides of this desired isomorphism, which both have the same kernel, and then applying the First Isomorphism Theorem.

Let $I = \langle p, f(X)\rangle_{\mathbb{Z}[X]}$.

Step 1. *There is a ring homomorphism $\psi_1 \colon \mathbb{Z}[X] \to \mathbb{F}_p[X]/\langle\bar{f}\rangle_{\mathbb{F}_p[x]}$ which has kernel I and such that $\psi_1(X) = X + \langle\bar{f}\rangle_{\mathbb{F}_p[X]}$.*

Proof. Define $\psi_1(g) = \bar{g} + \langle\bar{f}\rangle_{\mathbb{F}_p[X]}$ (where $\bar{g} \in \mathbb{F}_p[X]$ means "the reduction of g mod p.") Clearly $\psi_1(X)$ is what we want, and we can calculate

$$\begin{aligned}
g \in \ker(\psi_1) &\Leftrightarrow \bar{g} \in \langle\bar{f}\rangle_{\mathbb{F}_p[X]} \\
&\Leftrightarrow \bar{g} = \bar{h}\bar{f} \text{ for some } \bar{h}(X) \in \mathbb{F}_p[X] \\
&\Leftrightarrow g \equiv hf \bmod p \text{ for some } h(X) \in \mathbb{Z}[X] \\
&\Leftrightarrow g = hf + pr \text{ for some } h(X), r(X) \in \mathbb{Z}[X] \\
&\Leftrightarrow g \in \langle p, f(X)\rangle_{\mathbb{Z}[X]} = I. \qquad \square
\end{aligned}$$

Step 2. *There is a ring homomorphism $\psi_2 \colon \mathbb{Z}[X] \to \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}$ which has kernel I and such that $\psi_2(X) = \alpha + \langle p\rangle_{\mathbb{Z}[\alpha]}$.*

Proof. Define $\psi_2(g) = g(\alpha) + \langle p\rangle_{\mathbb{Z}[\alpha]}$. Clearly $\psi_2(X)$ is what we want. The calculation of the kernel is similar to Step 1, except with the roles of p and $f(X)$ swapped.

$$\begin{aligned}
g \in \ker(\psi_2) &\Leftrightarrow g(\alpha) \in \langle p\rangle_{\mathbb{Z}[\alpha]} \\
&\Leftrightarrow g(\alpha) = ph(\alpha) \text{ for some } h(X) \in \mathbb{Z}[X] \\
&\Leftrightarrow (g - ph)(\alpha) = 0 \text{ for some } h(X) \in \mathbb{Z}[X] \\
&\Leftrightarrow g - ph \in \langle f(X)\rangle_{\mathbb{Q}[X]} \text{ for some } h(X) \in \mathbb{Z}[X] \text{ (defn of minimal poly)} \\
&\Leftrightarrow g - ph \in \langle f(X)\rangle_{\mathbb{Z}[X]} \text{ for some } h(X) \in \mathbb{Z}[X] \text{ (Gauss's lemma)} \\
&\Leftrightarrow g \in \langle p, f(X)\rangle_{\mathbb{Z}[X]} = I. \qquad \square
\end{aligned}$$

Step 3. *There is a ring isomorphism*

$$\phi\colon \mathbb{F}_p[X]/\langle \bar{f}(X)\rangle_{\mathbb{F}_p[X]} \to \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}$$

such that $\phi(X + \langle \bar{f}\rangle_{\mathbb{F}_p[X]}) = \alpha + \langle p\rangle_{\mathbb{Z}[\alpha]}$.

Proof. The homomorphisms ψ_1, ψ_2 from Steps 1 and 2 are both surjective (because in each case the image of X generates the codomain as a ring). So by the First Isomorphism Theorem, we get isomorphisms

$$\phi_1\colon \mathbb{Z}[X]/I \to \mathbb{F}_p[X]/\langle \bar{f}\rangle_{\mathbb{F}_p[x]},$$
$$\phi_2\colon \mathbb{Z}[X]/I \to \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}.$$

Now $\phi = \phi_2 \circ \phi_1^{-1}$ is the desired isomorphism.

The claim about $\phi(X + \langle \bar{f}_{\mathbb{F}_p[X]}\rangle)$ follows from what we know about $\psi_1(X)$ and $\psi_2(X)$. □

Step 4. *The* $\mathfrak{p}_i$ *are distinct prime ideals of* $\mathcal{O}_K$*, and they are the only prime ideals of* $\mathcal{O}_K$ *dividing* $\langle p\rangle$.

Proof. By the Third Isomorphism Theorem for rings (twice) and using the isomorphism ϕ, we get bijections between the sets of ideals

$$\begin{aligned}\{\text{ideals in } \mathbb{F}_p[X] \text{ containing } \langle \bar{f}\rangle_{\mathbb{F}_p[X]}\} &\leftrightarrow \{\text{ideals in } \mathbb{F}_p[X]/\langle \bar{f}\rangle_{\mathbb{F}_p[X]}\}\\ &\leftrightarrow \{\text{ideals in } \mathbb{Z}[\alpha]/\langle p\rangle_{\mathbb{Z}[\alpha]}\}\\ &\leftrightarrow \{\text{ideals in } \mathcal{O}_K/\langle p\rangle_{\mathcal{O}_K}\}\\ &\leftrightarrow \{\text{ideals in } \mathcal{O}_K \text{ containing } \langle p\rangle_{\mathcal{O}_K}\}.\end{aligned}$$

(In the middle, we used our assumption that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.)

Using Lemma 36 and the third isomorphism theorem, we see that if R is a ring and $\mathfrak{a}, \mathfrak{b}$ are ideals such that $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathfrak{b}$ is a prime ideal of R if and only if $\mathfrak{b}/\mathfrak{a}$ is a prime ideal of $R/\mathfrak{a}$. Hence the bijections above match prime ideals with prime ideals, and we get a bijection

$$\{\text{prime ideals in } \mathbb{F}_p[X] \text{ containing } \langle \bar{f}\rangle\} \leftrightarrow \{\text{prime ideals in } \mathcal{O}_K \text{ containing } \langle p\rangle\}.$$

The right hand side is what we are interested in; we can describe the left hand side by factorising $\bar{f}$ in $\mathbb{F}_p[X]$.

Since $\mathbb{F}_p[X]$ is the polynomial ring over a field, it is a PID. Hence its prime ideals are simply the ideals of the form $\langle \bar{g}\rangle_{\mathbb{F}_p[X]}$ where $\bar{g}(X) \in \mathbb{F}_p[X]$ is (monic and) irreducible. In particular,

$$\begin{aligned}&\{\text{prime ideals in } \mathbb{F}_p[X] \text{ containing } \langle \bar{f}\rangle_{\mathbb{F}_p[X]}\}\\ &\qquad = \{\langle \bar{f}_i\rangle : \bar{f}_i(X) \in \mathbb{F}_p[X] \text{ is an irreducible factor of } \bar{f}\}.\end{aligned}$$

Because $\phi(X + \langle \bar{f}\rangle_{\mathbb{F}_p[X]}) = \alpha + \langle p\rangle_{\mathcal{O}_K}$, the sequence of bijections above map the ideal $\langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}$ to $\left\langle f_i(\alpha) + \langle p\rangle_{\mathcal{O}_K}\right\rangle_{\mathcal{O}_K/\langle p\rangle_{\mathcal{O}_K}}$, and thence to $\langle p, f_i(\alpha)\rangle_{\mathcal{O}_K} = \mathfrak{p}_i$. □

21. The class group and end of proof of Dedekind–Kummer

End of proof of Dedekind–Kummer theorem.

Step 5. $\mathrm{Nm}(\mathfrak{p}_i) = p^{\deg(\bar{f}_i)}$.

Proof. Since $\langle p\rangle_{\mathcal{O}_K} \subseteq \mathfrak{p}_i$ and $\langle \bar{f}\rangle_{\mathbb{F}_p[X]} \subseteq \langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}$, we can use the Third Isomorphism Theorem for rings (twice) and the isomorphism ϕ to obtain

$$\frac{\mathcal{O}_K}{\mathfrak{p}_i} \cong \frac{\mathcal{O}_K/\langle p\rangle_{\mathcal{O}_K}}{\mathfrak{p}_i/\langle p\rangle_{\mathcal{O}_K}} \cong \frac{\mathbb{F}_p[X]/\langle \bar{f}\rangle_{\mathbb{F}_p[X]}}{\langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}/\langle \bar{f}\rangle_{\mathbb{F}_p[X]}} \cong \frac{\mathbb{F}_p[X]}{\langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}}.$$

Hence

$$\mathrm{Nm}(\mathfrak{p}_i) = [\mathcal{O}_K : \mathfrak{p}_i] = [\mathbb{F}_p[X] : \langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}].$$

The quotient $\mathbb{F}_p[X]/\langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}$ is an $\mathbb{F}_p$-vector space with basis $1, X, \ldots, X^{\deg(\bar{f}_i)-1}$ (see Theorem 3). Thus it is a $\mathbb{F}_p$-vector space of dimension $\deg(\bar{f}_i)$, so

$$[\mathbb{F}_p[X] : \langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}] = p^{\deg(\bar{f}_i)}. \qquad \square$$

Step 6. $\langle p\rangle = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ *in* $\mathcal{O}_K$.

Proof. Since $\bar{f}_1(X)^{e_1}\cdots\bar{f}_r(X)^{e_r} = \bar{f}(X)$, the product of ideals $\prod_{i=1}^r \langle \bar{f}_i\rangle_{\mathbb{F}_p[X]}^{e_i}$ maps to the zero ideal in the quotient $\mathbb{F}_p[X]/\langle \bar{f}\rangle_{\mathbb{F}_p[X]}$. Applying ϕ from Step 3, we deduce that $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ maps to the zero ideal in $\mathcal{O}_K/\langle p\rangle_{\mathcal{O}_K}$. Thus $\prod_{i=1}^r \mathfrak{p}_i^{e_i} \subseteq \langle p\rangle_{\mathcal{O}_K}$.

We compare norms. By Lemma 40 and Corollary 15,

$$\mathrm{Nm}(\langle p\rangle_{\mathcal{O}_K}) = |\mathrm{Nm}_{K/\mathbb{Q}}(p)| = p^{[K:\mathbb{Q}]}.$$

Meanwhile by Lemma 53 and Step 5,

$$\mathrm{Nm}(\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}) = \prod_{i=1}^r \mathrm{Nm}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^r p^{e_i\deg(\bar{f}_i)}.$$

Finally because $\bar{f}(X) = \prod \bar{f}_i(X)^{e_i}$, we have

$$\sum_{i=1}^r e_i \deg(\bar{f}_i) = \deg(\bar{f}) = \deg(f) = [K:\mathbb{Q}]$$

(the equality $\deg(\bar{f}) = \deg(f)$ is because f is monic, so its highest-degree term does not vanish mod p). Thus $p^{[K:\mathbb{Q}]} = \prod_{i=1}^r p^{e_i\deg(\bar{f}_i)}$ and so

$$\mathrm{Nm}(\langle p\rangle_{\mathbb{F}_p[X]}) = \mathrm{Nm}(\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}).$$

Since we showed that $\prod \mathfrak{p}_i^{e_i} \subseteq \langle p\rangle_{\mathcal{O}_K}$, we are done by Lemma 55. $\square$

The class group.

The class group of a number field K is a finite abelian group which measures "how badly unique factorisation fails in $\mathcal{O}_K$."

Definition. Let K be a number field. Write:

- I_K = the group of non-zero fractional ideals of K (under multiplication);
- P_K = the group of non-zero principal fractional ideals of K (under multiplication).

The **class group** of K is the quotient group $\mathrm{Cl}(K) = I_K/P_K$.

The elements of $\mathrm{Cl}(K)$ are called **ideal classes**. If $\mathfrak{a}$ is a non-zero fractional ideal of K, we write $[\mathfrak{a}]$ for its class in $\mathrm{Cl}(K)$.

Observe that $[\mathfrak{a}] = [\mathfrak{b}]$ if and only if $\mathfrak{a} = \gamma\mathfrak{b}$ for some $\gamma \in K$.

We showed that I_K was a group in Proposition 50. P_K is a subgroup of I_K because $\langle\alpha\rangle\langle\beta\rangle = \langle\alpha\beta\rangle$ and $\langle\alpha\rangle\langle\alpha^{-1}\rangle = \mathcal{O}_K$. The group I_K is abelian because multiplication is commutative, and hence every subgroup of I_K is a normal subgroup. Therefore the quotient I_K/P_K is a group (indeed, an abelian group).

Observe that

$$\mathrm{Cl}(K) = \{1\} \quad \Leftrightarrow \quad P_K = I_K \quad \Leftrightarrow \quad \mathcal{O}_K \text{ is a PID.}$$

We said that $\mathrm{Cl}(K)$ is finite but this is far from obvious. Notice that I_K and P_K are both infinite groups – indeed, they are non-finitely generated groups (by unique factorisation of ideals, the set of all non-zero prime ideals forms a minimal generating set for I_K). Hence it is not at all obvious that their quotient is finite. The finiteness of the class group is one of the deepest theorems of the course.

Minkowski's theorem.

In order to prove the finiteness of the class group, we will use Minkowski's theorem. Minkowski's theorem is also useful for calculating the class group of a particular number field, because it gives us a way to find ideals which represent every class in $\mathrm{Cl}(K)$.

Definition. Let K be a number field of signature (r, s) and degree $n = r + 2s$. Let Δ_K be the discriminant of K. The **Minkowski bound** of K is

$$B_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_K|}.$$

Theorem 59 (Minkowski's theorem on ideal classes)**.** *Every ideal class in* $\mathrm{Cl}(K)$ *has a representative* $\mathfrak{a}$ *which is an ideal of* $\mathcal{O}_K$ *(not just a fractional ideal) and satisfies* $\mathrm{Nm}(\mathfrak{a}) \leq B_K$.

e.g. As an example, we will use Minkowski's theorem to prove that $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ is a PID, where $K = \mathbb{Q}(\sqrt{6})$. The degree is 2, the signature is $(2, 0)$ and $\Delta_K = 4 \times 6 = 24$ so the Minkowski bound is

$$B_K = \left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2}\sqrt{24} = \frac{1}{2}\sqrt{24} = \sqrt{6} < 3.$$

So by Theorem 59, every ideal class in $\mathrm{Cl}(K)$ has a representative of norm 1 or 2.

The only ideal of norm 1 is $\mathcal{O}_K$ itself.

An ideal of norm 2 must be a prime ideal dividing $\langle 2 \rangle$ (by Proposition 57). We use Dedekind–Kummer to factorise $\langle 2 \rangle$. $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ and the minimal polynomial of $\sqrt{6}$ is $X^2 - 6 \equiv X^2 \bmod 2$. So $\langle 2 \rangle = \mathfrak{p}^2$ where $\mathfrak{p} = \langle 2, \sqrt{6} \rangle$. Thus $\mathfrak{p}$ is the unique ideal of norm 2 in $\mathcal{O}_K$.

Is $\mathfrak{p}$ principal? We look for an element $x + y\sqrt{6} \in \mathcal{O}_K$ with

$$\mathrm{Nm}_{K/\mathbb{Q}}(x + y\sqrt{6}) = x^2 - 6y^2 = \pm 2.$$

$x = 2, y = 1$ gives a solution to this equation, and we can see that $2 + \sqrt{6} \in \mathfrak{p}$. Thus $\mathfrak{p} = \langle 2 + \sqrt{6} \rangle$ is principal.

We have shown that all ideals of norm < 3 in $\mathcal{O}_K$ are principal. By Theorem 59, this implies that the only ideal class in $\mathrm{Cl}(K)$ is the trivial class. In other words, $\mathbb{Z}[\sqrt{6}]$ is a PID.

22. Computing the class group

UFDs and PIDs.

The following lemma justifies the slogan that $\mathrm{Cl}(K)$ measures how badly $\mathcal{O}_K$ fails to be a UFD.

Lemma 60. *Let K be a number field. Then $\mathrm{Cl}(K) = \{1\}$ if and only if $\mathcal{O}_K$ is a UFD.*

Proof. From the definition of $\mathrm{Cl}(K)$, we saw immediately that

$$\mathrm{Cl}(K) = \{1\} \quad \Leftrightarrow \quad \mathcal{O}_K \text{ is a PID.}$$

Every PID is a UFD. So what we have to prove is: if $\mathcal{O}_K$ is a UFD, then it is a PID.

Since every proper ideal of $\mathcal{O}_K$ is a product of prime ideals, it suffices to prove that every prime ideal of $\mathcal{O}_K$ is principal.

Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ and let $\alpha \in \mathfrak{p} \setminus \{0\}$. Write

$$\alpha = \pi_1 \pi_2 \cdots \pi_r.$$

where $\pi_1, \ldots, \pi_r \in \mathcal{O}_K$ are irreducible elements.

In a UFD, irreducible elements are prime. In any integral domain, the ideal generated by a prime element is a prime ideal. Hence the ideals $\langle \pi_i \rangle$ are prime ideals of $\mathcal{O}_K$.

In $\mathcal{O}_K$, every non-zero prime ideal is maximal. So $\langle \pi_i \rangle$ are maximal ideals.

We have

$$\mathfrak{p} \mid \langle \alpha \rangle = \langle \pi_1 \rangle \cdots \langle \pi_r \rangle.$$

By the definition of prime ideal, we deduce that $\mathfrak{p} \mid \langle \pi_i \rangle$ for some i. In other words $\langle \pi_i \rangle \subseteq \mathfrak{p}$. Since $\langle \pi_i \rangle$ is maximal, we conclude that $\mathfrak{p} = \langle \pi_i \rangle$. □

Computing the class group.

Generalising our example for $\mathbb{Q}(\sqrt{6})$, we can use Minkowski's Theorem (Theorem 59), together with the Dedekind–Kummer Theorem (Theorem 58), to compute some more class groups.

Theorem 59 tells us that we only need to look at ideals of norm $\leq B_K$ in order to hit every class in $\mathrm{Cl}(K)$. In fact, we only need to look at *prime* ideals of norm $\leq B_K$: these don't necessarily hit every ideal class, but they do generate $\mathrm{Cl}(K)$. For convenience, we state this as a lemma.

Lemma 61. *Let K be a number field. The group $\mathrm{Cl}(K)$ is generated by the classes of prime ideals in $\mathcal{O}_K$ of norm $\leq B_K$. Furthermore, any such prime ideal divides $\langle p_i \rangle$ for some rational prime $p_i \leq B_K$.*

Proof. By Theorem 59, every class in $\mathrm{Cl}(K)$ has a representative $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $\mathrm{Nm}(\mathfrak{a}) \leq B_K$. We can write $\mathfrak{a}$ as a product of prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Because ideal norms are multiplicative, $\mathrm{Nm}(\mathfrak{p}_i) \leq B_K$ for each i.

By Proposition 57, $\mathfrak{p}_i \mid \langle p_i \rangle$ for some rational prime p_i, and $\mathrm{Nm}(\mathfrak{p}_i) = p_i^{n_i}$ for some $n_i \in \mathbb{N}$. Hence $p_i \leq \mathrm{Nm}(\mathfrak{p}_i) \leq B_K$. □

Thus we have the following strategy for finding $\mathrm{Cl}(K)$:

(1) Calculate the Minkowski bound B_K.
(2) For each rational prime $p \leq B_K$, use Dedekind–Kummer to factorise $\langle p \rangle$ into prime ideals of $\mathcal{O}_K$. (When we do this, some of the prime ideals we obtain may have norm $> B_K$. We can throw these away.)
(3) Check whether each of the prime ideals we have found is principal.
(4) For any non-principal ideals, look for relations between their ideal classes, and eventually prove that we have found all the relations. This is an *ad hoc* process – if we only found a single non-principal prime ideal, then it is just a matter of finding the smallest power of that ideal which becomes principal. If there are multiple non-principal prime ideals of norm $\leq B_K$, then this may require more tricks.

Class group examples.

$K = \mathbb{Q}(\sqrt{-10})$

Since $-10 \equiv 2 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-10}]$ and $\Delta_K = -40$. The signature is $(0, 1)$. Thus the Minkowski bound is

$$B_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{|-40|} = \frac{2}{\pi}\sqrt{40} < \frac{2}{3} \times 7 < 5.$$

Thus by Lemma 61, $\mathrm{Cl}(K)$ is generated by prime ideals dividing $\langle 2 \rangle$ or $\langle 3 \rangle$.

We work out these prime ideals using the Dedekind–Kummer theorem with $\alpha = \sqrt{-10}$, $f(X) = X^2 + 10$:

- $p = 2$: $f(X) \equiv X^2 \bmod 2$ so $\langle 2 \rangle = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = \langle 2, \sqrt{-10} \rangle$.
- $p = 3$: $f(X) \equiv X^2 - 2 \bmod 3$ which is irreducible since 2 is not a quadratic residue mod 3, so $\langle 3 \rangle$ is a prime ideal of $\mathcal{O}_K$.

We can discard $\langle 3 \rangle$ because it has norm $9 > B_K$. Thus $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$.

By Theorem 58(iii), $\mathrm{Nm}(\mathfrak{p}_2) = 2^{\deg(X)} = 2$. Thus to test whether $\mathfrak{p}_2$ is principal, we look for elements of $\mathcal{O}_K$ of norm ± 2. The equation $\mathrm{Nm}(x + y\sqrt{-10}) = x^2 + 10y^2 = \pm 2$ has no solutions in $\mathbb{Z}$, so $\mathcal{O}_K$ contains no elements of norm ± 2. Hence $\mathfrak{p}_2$ is not principal.

On the other hand, from the Dedekind–Kummer calculation above, $\mathfrak{p}_2^2 = \langle 2 \rangle$ is principal. So $[\mathfrak{p}_2] \neq [1]$ in $\mathrm{Cl}(K)$ but $[\mathfrak{p}_2]^2 = [\langle 2 \rangle] = [1]$. Thus $[\mathfrak{p}_2]$ has order 2, so $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

$K = \mathbb{Q}(\sqrt{-14})$

Since $-14 \equiv 2 \bmod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ and $\Delta_K = -56$. The signature is $(0, 1)$. Thus the Minkowski bound is

$$B_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{|-56|} = \frac{2}{\pi}\sqrt{56} < \frac{2}{3} \times 8 = \frac{16}{3}.$$

This is only just over 5, and the inequality is quite weak because 56 is a long way from $8^2 = 64$. So it seems likely that $B_K < 5$. It would be a shame to make extra work for ourselves by having to factorise $\langle 5 \rangle$, so we get out the calculator and find

$$B_K \approx 4.76 < 5.$$

(You could also prove this by hand, by noting that $56 < 56.25 = 7.5^2$.)

Thus by Lemma 61, $\mathrm{Cl}(K)$ is generated by prime ideals dividing $\langle 2 \rangle$ or $\langle 3 \rangle$.

Using the Dedekind–Kummer theorem with $\alpha = \sqrt{-14}$, $f(X) = X^2 + 14$:

- $p = 2$: $f(X) \equiv X^2 \bmod 2$ so $\langle 2 \rangle = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = \langle 2, \sqrt{-14} \rangle$.
- $p = 3$: $f(X) \equiv (X-1)(X+1) \bmod 3$ so $\langle 3 \rangle = \mathfrak{p}_3\mathfrak{q}_3$ where $\mathfrak{p}_3 = \langle 3, -1 + \sqrt{-14} \rangle$ and $\mathfrak{q}_3 = \langle 3, 1 + \sqrt{-14} \rangle$.

Now $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{q}_3]$. Since $\mathfrak{p}_2^2 = \langle 2 \rangle$ and $\mathfrak{p}_3\mathfrak{q}_3 = \langle 3 \rangle$ are principal, we have

$$[\mathfrak{p}_2]^2 = [1], \quad [\mathfrak{p}_3][\mathfrak{q}_3] = [1].$$

The latter implies that

$$[\mathfrak{q}_3] = [\mathfrak{p}_3]^{-1}$$

so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. We still have to figure out if there is any relation between $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

We know that $[\mathfrak{p}_2]^2 = [\langle 2 \rangle] = [1]$ and $[\mathfrak{p}_3][\mathfrak{q}_3] = [\langle 3 \rangle] = [1]$ so $[\mathfrak{q}_3] = [\mathfrak{p}_3]^{-1}$. But we still have to figure out if there is any relation between $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$.

One way to do this is to try looking for principal ideals whose norm is a product of small powers of 2 and 3. You find that $\mathcal{O}_K$ contains an element of norm 18:

$$\mathrm{Nm}(2 + \sqrt{-14}) = 4 + 14 = 18.$$

(How did we find this? Maybe just by luck/intelligent guesswork. If I set this as a question on an exam, there would be some sort of hint like: "Find an element of $\mathcal{O}_K$ of norm 18.")

Let's factorise the ideal $\langle 2 + \sqrt{-14} \rangle$. Since its norm is a product of powers of 2 and 3,

$$\langle 2 + \sqrt{-14} \rangle = \mathfrak{p}_2^a \mathfrak{p}_3^b \mathfrak{q}_3^c.$$

Comparing norms, and since $\mathrm{Nm}(2 + \sqrt{-14}) = 2 \times 3^2$, we get $a = 1$ and $b + c = 2$. We can't have $b = c = 1$ because then $\mathfrak{p}_3\mathfrak{q}_3 = \langle 3 \rangle$ divides $\langle 2 + \sqrt{-14} \rangle$, but $3 \nmid 2 + \sqrt{-14}$. Finally $2 + \sqrt{-14} \in \langle 3, -1 + \sqrt{-14} \rangle = \mathfrak{p}_3$. Thus

$$\langle 2 + \sqrt{-14} \rangle = \mathfrak{p}_2\mathfrak{p}_3^2.$$

In $\mathrm{Cl}(K)$, this tells us that

$$[\mathfrak{p}_2][\mathfrak{p}_3]^2 = [1].$$

Since $[\mathfrak{p}_2] = [\mathfrak{p}_2]^{-1}$, we deduce that

$$[\mathfrak{p}_2] = [\mathfrak{p}_3]^2$$

and so $[\mathfrak{p}_3]$ generates $\mathrm{Cl}(K)$, with $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = [1]$. Thus $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$.

23. Minkowski's theorem

Recall Minkowski's theorem on ideal classes.

Theorem (Theorem 59)**.** *Every ideal class in* $\mathrm{Cl}(K)$ *has a representative* $\mathfrak{a}$ *which is an ideal of* $\mathcal{O}_K$ *(not just a fractional ideal) and satisfies* $\mathrm{Nm}(\mathfrak{a}) \leq B_K$*, where*

$$B_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_K|}.$$

Today we will use Minkowski's theorem to prove the finiteness of the class group (easy) and start the proof of Minkowski's theorem (harder).

Finiteness of the class group.

Starting from Minkowski's theorem on ideal classes, it is easy to prove that the class group is finite. We just need a lemma about ideals.

Lemma 62. *For any positive integer* N*, there are only finitely many ideals in* $\mathcal{O}_K$ *of norm* N*.*

Proof. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal of norm N. By Lemma 56, $N \in \mathfrak{a}$ so $\langle N\rangle \subseteq \mathfrak{a}$. Hence by the Third Isomorphism Theorem, $\mathfrak{a}/\langle N\rangle$ is an ideal in $\mathcal{O}_K/\langle N\rangle$.

Thus $\mathfrak{a} \mapsto \mathfrak{a}/\langle N\rangle$ is an injective map

$$\{\text{ideals of } \mathcal{O}_K \text{ of norm } N\} \to \{\text{ideals of } \mathcal{O}_K/\langle N\rangle\}.$$

Since $\mathcal{O}_K/\langle N\rangle$ is a finite ring, it contains only finitely many ideals. □

Theorem 63. *Let* K *be a number field. Then* $\mathrm{Cl}(K)$ *is finite.*

Proof. Thanks to Lemma 62, $\mathcal{O}_K$ has finitely many ideals of norm $\leq B_K$. Thus we are done by Theorem 59. □

Definition. For any number field K, the **class number** of K is the size of $\mathrm{Cl}(K)$ (it is often denoted h_K).

Proof of Minkowski's theorem.

The proof of Minkowski's theorem on ideal classes (Theorem 59) relies on two other theorems of Minkowski:

Minkowski's theorem on ideal classes	
⇑	(easy, examinable)
Minkowski's theorem on ideals	
⇑	(harder, non-examinable)
Minkowski's theorem on lattices	

We will next prove that Minkowski's theorem on ideals implies the theorem on ideal classes – this proof, and the statement of Minkowski's theorem on ideals, are examinable material for this module.

We will then spend the rest of this lecture and all of tomorrow's lecture outlining the proof that Minkowski's theorem on lattices implies the theorem on ideals –

this is non-examinable. A (slightly simplified) version of Minkowski's theorem on lattices was in Introduction to Number Theory, so we will skip the proof of the lattice theorem altogether.

Theorem 64 (Minkowski's theorem on ideals)**.** *Let K be a number field. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a non-zero element α such that*

$$|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| \leq B_K \,\mathrm{Nm}(\mathfrak{a}).$$

Proof of Theorem 59. There is one subtle point to watch out for in this proof – we apply Theorem 64 to a representative of the *inverse* of the ideal class we are interested in!

Let C be an ideal class in $\mathrm{Cl}(K)$. Pick a fractional ideal $\mathfrak{b} \in I_K$ which represents the *inverse* class C^{-1}. Thanks to Lemma 46, we may assume that $\mathfrak{b}$ is an ideal in $\mathcal{O}_K$. By Theorem 64, we can find $\alpha \in \mathfrak{b} \setminus \{0\}$ such that $|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| \leq B_K \,\mathrm{Nm}(\mathfrak{b})$.

Let $\mathfrak{a} = \alpha\mathfrak{b}^{-1}$. Then $[\mathfrak{a}] = [\mathfrak{b}]^{-1} = C$, $\mathfrak{a} \subseteq \mathcal{O}_K$ because $\alpha \in \mathfrak{b}$ (by the definition of $\mathfrak{b}^{-1}$), and

$$\mathrm{Nm}(\mathfrak{a}) = |\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| \cdot \mathrm{Nm}(\mathfrak{b})^{-1} \leq B_K. \qquad \square$$

Lattices (non-examinable).

The proof of Minkowski's theorem on ideals (Theorem 64) is quite long. Surprisingly, it relies on geometry and analysis, even though we are proving a theorem which appears algebraic! That's how π appears in B_K. This method is called "geometry of numbers."

First we need to define lattices in $\mathbb{R}^n$.

Definition. A **lattice** in $\mathbb{R}^n$ is a subgroup of $(\mathbb{R}^n, +)$ which is generated by a basis of $\mathbb{R}^n$.

e.g. $\mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$ because it is generated by the standard basis.

Every lattice in $\mathbb{R}^n$ is isomorphic to $\mathbb{Z}^n$ as a group, but it might be a different subgroup of $\mathbb{R}^n$.

Definition. Let $L \subseteq \mathbb{R}^n$ be a lattice, generated by the basis $\{\underline{v}_1, \ldots, \underline{v}_n\}$. The **covolume** of L is the volume of the parallelepiped

$$\{x_1\underline{v}_1 + \cdots + x_n\underline{v}_n : x_1, \ldots, x_n \in \mathbb{R}, 0 \leq x_1, \ldots, x_n \leq 1\}.$$

The prefix "co" is here because this is not the volume of the lattice itself (that's zero because it is a countable set of points!); rather it is the volume of the "spaces in between the lattice."

Note that any lattice has many bases, and the covolume is the same whichever basis we choose. To prove this, we will use another way of defining the covolume: if C is the matrix with $\underline{v}_1, \ldots, \underline{v}_n$ as columns, then

$$\mathrm{covol}(L) = |\det(C)|.$$

(This is just the formula for the volume of a parallelepiped.) If we have two bases which generate the same lattice L, then the change-of-basis matrix between them

has determinant ± 1, proving that the covolume of L is independent of the choice of basis.

Minkowski's theorem on lattices (non-examinable).

Suppose we have a lattice $L \subseteq \mathbb{R}^n$, and a compact set $S \subseteq \mathbb{R}^n$. If we make S big enough, can we guarantee that it contains an element of L? How big does it need to be?

This is a trick question: you can make S as big as you want without ever intersecting L by drawing a set which has holes round the lattice points! Even if you insist that S is no holes (is simply connected), you still draw a set S which wiggles in and out around the lattice points. We can rule this out by insisting that S is convex.

Definition. A subset $S \subseteq \mathbb{R}^n$ is **convex** if for all $x, y \in S$ and all $t \in \mathbb{R}$ with $0 \leq t \leq 1$, we have $tx + (1-t)y \in S$.

It turns out that this is not enough. We need one more condition on S.

Definition. A subset $S \subseteq \mathbb{R}^n$ is **symmetric** if for all $x \in S$, we have $-x \in S$.

Now it looks like we have gone too far: A convex symmetric set S automatically contains $\frac{1}{2}x + \frac{1}{2}(-x) = 0$ for any $x \in S$, so $S \cap L$ is always non-empty. We will ignore 0.

Thus the right question to ask is: if we make a convex symmetric set S large enough, can we guarantee that it contains an element of $L \setminus \{0\}$? How large we will need to make S obviously depends on how big the gaps between elements of L are, i.e. on $\operatorname{covol}(L)$.

The following theorem answers this question.

Theorem 65 (Minkowski's theorem on lattices)**.** *Let L be a lattice in $\mathbb{R}^n$. Let $S \subseteq \mathbb{R}^n$ be a compact, convex, symmetric set. If*

$$\operatorname{vol}(S) \geq 2^n \operatorname{covol}(L),$$

then S contains a non-zero element of L.

In Introduction to Number Theory, you proved Theorem 65 for lattices which are contained in $\mathbb{Z}^n$. One can reduce to that case by a linear transformation, so we will omit the proof of Theorem 65.

24. Proof of Minkowski's theorem

(All of this lecture is non-examinable.)

We are aiming to prove Minkowski's theorem on ideals:

Theorem (Theorem 64)**.** *Let K be a number field. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a non-zero element α such that*

$$|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| \leq B_K \,\mathrm{Nm}(\mathfrak{a}).$$

In order to prove Theorem 64, we need to pick a lattice L and a compact, convex, symmetric set S and calculate their volumes. Then we will be able to apply Theorem 65.

Canonical embedding of a number field.

In order to obtain lattices related to a number field, we need to put K inside a real vector space. K is isomorphic to $\mathbb{Q}^n$, so we can put it inside $\mathbb{R}^n$. We will do this in the following way, using the real and complex embeddings of K:

Definition. Let K be a number field of signature (r, s) and degree $n = r + 2s$. Label the real embeddings of K as $\sigma_1, \ldots, \sigma_r$ and the complex embeddings as $\sigma_{r+1}, \ldots, \sigma_{r+s}$, $\overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$. The **canonical embedding** of K is the map $\iota\colon K \to \mathbb{R}^n$ defined by

$$\iota(\alpha) = (\sigma_1(\alpha),\, \ldots,\, \sigma_r(\alpha),\, \mathrm{Re}\,\sigma_{r+1}(\alpha), \mathrm{Im}\,\sigma_{r+1}(\alpha),\, \ldots,\, \mathrm{Re}\,\sigma_{r+s}(\alpha), \mathrm{Im}\,\sigma_{r+s}(\alpha)).$$

(Note that we couldn't just use the embeddings of K directly i.e.

$$(\sigma_1(\alpha), \ldots, \sigma_r(\alpha),\, \sigma_{r+1}(\alpha), \overline{\sigma_{r+1}}(\alpha), \ldots, \sigma_{r+s}(\alpha), \overline{\sigma_{r+s}}(\alpha))$$

because this has values in $\mathbb{C}^n$, not $\mathbb{R}^n$.)

Lemma 66. *Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$. Then $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with covolume*

$$2^{-s}\sqrt{|\Delta_K|}.$$

Outline proof. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for K. Let $C \in \mathrm{M}_{n\times n}(\mathbb{R})$ be the matrix with columns $\iota(\alpha_1), \ldots, \iota(\alpha_n)$.

We will calculate $\det(C)$. We will see that $\det(C) \neq 0$, so $\iota(\alpha_1), \ldots, \iota(\alpha_n)$ form a basis of $\mathbb{R}^n$. Consequently the subgroup which they generate, namely $\iota(\mathcal{O}_K)$, is a lattice. Furthermore the covolume is given by $|\det(C)|$.

In order to calculate $\det(C)$, consider a different matrix $B \in \mathrm{M}_{n\times n}(\mathbb{C})$ with columns

$$\begin{pmatrix} \sigma_1(\alpha_i) \\ \vdots \\ \sigma_n(\alpha_i) \end{pmatrix}.$$

By the definition of discriminant, we have

$$\Delta_K = \det(B)^2.$$

To get from B to C, we multiply by a matrix of the form

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & \frac{1}{2} & \frac{1}{2} & & & \\ & & & -\frac{1}{2}i & \frac{1}{2}i & & & \\ & & & & & \ddots & & \\ & & & & & & \frac{1}{2} & \frac{1}{2} \\ & & & & & & -\frac{1}{2}i & \frac{1}{2}i \end{pmatrix}.$$

For each pair of complex embeddings, we have a block $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2}i & \frac{1}{2}i \end{pmatrix}$ because

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2}i & \frac{1}{2}i \end{pmatrix} \begin{pmatrix} z \\ \bar{z} \end{pmatrix} = \begin{pmatrix} \operatorname{Re} z \\ \operatorname{Im} z \end{pmatrix}.$$

The determinant of $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2}i & \frac{1}{2}i \end{pmatrix}$ is $\frac{1}{2}i$ so

$$\det(C) = (\tfrac{1}{2}i)^s \det(B).$$

Consequently

$$\operatorname{covol}(\iota(\mathcal{O}_K)) = |\det(C)| = 2^{-s}|\det(B)| = 2^{-s}\sqrt{|\Delta_K|}. \qquad \square$$

Since $\mathfrak{a}$ is a finite-index subgroup of $\mathcal{O}_K$, $\iota(\mathfrak{a})$ is also a lattice and to get its covolume we just multiply by the index i.e. $\operatorname{Nm}(\mathfrak{a})$:

$$\operatorname{covol}(\iota(\mathfrak{a})) = 2^{-s}\sqrt{|\Delta_K|}\operatorname{Nm}(\mathfrak{a}).$$

Proof of Minkowski's theorem on ideals.

Now $\iota(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$, and we have calculated its covolume. In order to apply Theorem 65, we need to choose a compact, convex, symmetric set S. If $\underline{x} \in S \cap \iota(\mathfrak{a})$, then the fact that $\underline{x} \in \iota(\mathfrak{a})$ tells us that $\underline{x} = \iota(\alpha)$ for some $\alpha \in \mathfrak{a}$. So we want the fact that $\underline{x} \in S$ to tell us that $\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)$ is bounded.

We extend $\operatorname{Nm}_{K/\mathbb{Q}}$ from a function on K to a continuous function on $\mathbb{R}^n$.

Define a function $N_{r,s}\colon \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ by

$$N_{r,s}(x_1, \dots, x_r, y_1, z_1, \dots, y_s, z_s) = |x_1| \cdots |x_r| \, (y_1^2 + z_1^2) \cdots (y_s^2 + z_s^2).$$

We have labelled the coordinates in this way in order to relate them to the canonical embedding of K: the x_is correspond to real embeddings of K, the y_is to the real part of complex embeddings, the z_is to the imaginary part of complex embeddings. This relation with the canonical embedding also explains why $N_{r,s}$ involves factors $y_i^2 + z_i^2$ which look like the norm of a complex number.

The significance of this function $N_{r,s}$ is that, for all $\alpha \in K$, we have

$$\begin{aligned} N_{r,s}(\iota(\alpha)) &= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)|\, |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2 \\ &= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)|\, |\sigma_{r+1}(\alpha)||\overline{\sigma_{r+1}}(\alpha)| \cdots |\sigma_{r+s}(\alpha)||\overline{\sigma_{r+s}}(\alpha)| \\ &= \prod_{i=1}^{n} |\sigma_i(\alpha)| = |\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)|. \end{aligned}$$

(The final step is Lemma 19).

Let

$$Y_{r,s}(T) = \{\underline{x} \in \mathbb{R}^n : N_{r,s}(\underline{x}) \leq T\}.$$

We have to show that $Y_{r,s}(B_K \,\mathrm{Nm}(\mathfrak{a}))$ contains a non-zero element of $\iota(\mathfrak{a})$.

Unfortunately we cannot deduce this directly from Theorem 65 because the set $Y_{r,s}(T)$ is usually neither compact nor convex. In the lecture I drew pictures:

- for an imaginary quadratic field, $n = 2$, $(r, s) = (0, 1)$,

  $$Y_{r,s}(T) = \{(y, z) \in \mathbb{R}^2 : y^2 + z^2 \leq T\}.$$

  Thus $Y_{r,s}(T)$ is a disc, which is compact and convex. (This is the easy case!)
- for a real quadratic field, $n = 2$, $(r, s) = (2, 0)$,

  $$Y_{r,s}(T) = \{(x_1, x_2) \in \mathbb{R}^2 : |x_1||x_2| \leq T\}.$$

  This set is bounded by hyperbolae – it is the set A in Figure 10.1 of Stewart and Tall, p. 175. It is neither compact nor convex.

We will choose a compact convex set inside $Y_{r,s}(T)$, and apply Theorem 65 to that. If we only want to prove the finiteness of the class group, we don't need to describe exactly which compact convex set we choose because we don't need an exact value for B_K, just that there exists some B_K – so we could just say that when we make T large enough, we know that $Y_{r,s}(T)$ will always contain a compact convex set which is large enough for Theorem 65 to apply.

On the other hand, in order to calculate class groups via Minkowski's theorem, we need a value for B_K. In order to get the best value we can, we choose the largest compact convex set we can inside $Y_{r,s}(T)$. In the real quadratic field case, this will be set B in Stewart and Tall, Figure 10.1.

To define this new set, we define a new function $\phi_{r,s} \colon \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ by

$$\phi_{r,s}(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = |x_1| + \cdots + |x_r| + 2\sqrt{y_1^2 + z_1^2} + \cdots + 2\sqrt{y_s^2 + z_s^2}.$$

By the AM-GM inequality, we have

$$N_{r,s}(\underline{x})^{1/n} \leq \tfrac{1}{n}\, T_{r,s}(\underline{x}).$$

Consequently, if we choose $\lambda = n(B_K \,\mathrm{Nm}(\mathfrak{a}))^{1/n}$, then the set

$$X_{r,s}(\lambda) = \{\underline{x} \in \mathbb{R}^n : T_{r,s}(\underline{x}) \leq \lambda\}$$

is contained in $Y_{r,s}(B_K \,\mathrm{Nm}(\mathfrak{a}))$.

The set $X_{r,s}(\lambda)$ is compact, convex and symmetric. All that remains is to compute its volume. It turns out that

$$\mathrm{vol}(X_{r,s}(\lambda)) = 2^r \Big(\frac{\pi}{2}\Big)^s \frac{1}{n!}\,\lambda^n.$$

We will skip the calculation (which is quite fiddly, especially to get the correct powers of 2) but broadly speaking: the 2^r comes from integrating the x_is, because a bound on $|x_i|$ allows both positive or negative values of x_i, the $(\pi/2)^s$ comes from the circles defined by $2\sqrt{y_i^2 + z_i^2}$, and the $1/n! \cdot \lambda^n$ comes from the fact that when we integrate a constant n times we get $1/n! \cdot t^n$.

Inserting our choice of λ into this formula, we get

$$\mathrm{vol}(X_{r,s}(\lambda)) = 2^r \Big(\frac{\pi}{2}\Big)^s \frac{n^n}{n!}\, B_K \,\mathrm{Nm}(\mathfrak{a}) = 2^{r+s}\sqrt{|\Delta_K|}\,\mathrm{Nm}(\mathfrak{a}) = 2^n \,\mathrm{covol}(\iota(\mathfrak{a})).$$

Hence by Theorem 65, $X_{r,s}(\lambda)$ contains a non-zero element $\underline{x} \in \iota(\mathfrak{a})$. Write $\underline{x} = \iota(\alpha)$ where $\alpha \in \mathfrak{a}$. Since $X_{r,s}(\lambda)$ is contained in (*), we have

$$|\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| = N_{r,s}(\underline{x}) \leq B_K \,\mathrm{Nm}(\mathfrak{a})$$

as required.

(End of non-examinable material)

25. Mordell equation

One of the purposes of all this theory of algebraic numbers is to solve Diophantine equations i.e. polynomial equations in ordinary integers. We will consider one example: the so-called **Mordell equation**

$$y^2 = x^3 + k$$

where $k \in \mathbb{Z}$.

Mordell proved that, for each k, this equation has only finitely many solutions with $x, y \in \mathbb{Z}$. We will not prove this, but we will look at a method which allows you to find the integer solutions for a given value of k.

e.g. Consider the equation

$$y^2 = x^3 - 13.$$

We rearrange this to get

$$x^3 = y^2 + 13.$$

In order to factorise the right hand side, we will work in the field $K = \mathbb{Q}(\sqrt{-13})$. We get

$$x^3 = (y + \sqrt{-13})(y - \sqrt{-13}). \tag{1}$$

If $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$ were a UFD, then we could say: $y + \sqrt{-13}$ and $y - \sqrt{-13}$ are coprime and their product is a cube, so $y + \sqrt{-13}$ and $y - \sqrt{-13}$ must themselves be cubes (at least up to multiplying by a unit).

Unfortunately, $\mathbb{Z}[\sqrt{-13}]$ is not a UFD. (We can use the Minkowski and Dedekind–Kummer theorems to show that $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$.) However, it does have unique factorisation of ideals, so we will try to follow a similar method using ideals instead. Calculating the class group will allow us to deduce that certain ideals are principal, and so turn equations of ideals back into equations of elements.

We will need the following lemma.

Lemma 67. *Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ be ideals which are coprime (have no common prime ideal factors). Suppose that*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}^n$$

for some ideal $\mathfrak{c} \subseteq \mathcal{O}_K$ and some $n \in \mathbb{N}$. Then there are ideals $\mathfrak{a}', \mathfrak{b}' \subseteq \mathcal{O}_K$ such that

$$\mathfrak{a} = (\mathfrak{a}')^n, \quad \mathfrak{b} = (\mathfrak{b}')^n.$$

Proof. This is an easy consequence of the unique factorisation of ideals (Theorem 48) – think about how you would prove the same result for rational integers. □

Equation (1) implies the following equation of principal ideals:

$$\langle x \rangle^3 = \langle y + \sqrt{-13} \rangle \langle y - \sqrt{-13} \rangle. \tag{2}$$

If we want to use Lemma 67 here, we have to show that the ideals $\langle y + \sqrt{-13} \rangle$ and $\langle y - \sqrt{-13} \rangle$ are coprime.

Suppose $\mathfrak{p}$ was a prime ideal which divides $\langle y + \sqrt{-13}\rangle$ and $\langle y - \sqrt{-13}\rangle$. Then

$$(y + \sqrt{-13}) - (y - \sqrt{-13}) = 2\sqrt{-13} \in \mathfrak{p}.$$

Hence $\mathrm{Nm}(\mathfrak{p})$ divides

$$\mathrm{Nm}_{K/\mathbb{Q}}(2\sqrt{-13}) = 4 \times 13 = 52.$$

Since $\mathrm{Nm}(\mathfrak{p})$ is a prime power (by Proposition 57), it must be either 13 or a power of 2.

If $\mathrm{Nm}(\mathfrak{p}) = 13$, then 13 divides $\mathrm{Nm}_{K/\mathbb{Q}}(y + \sqrt{-13}) = y^2 + 13$. Consequently $13 \mid y$. But then $x^3 = y^2 + 13$ will be divisible by 13 but not by 13^2, which is impossible for a cube. Thus $\mathrm{Nm}(\mathfrak{p}) \neq 13$.

If $\mathrm{Nm}(\mathfrak{p}) = 2$, then 2 divides $\mathrm{Nm}_{K/\mathbb{Q}}(y + \sqrt{-13}) = y^2 + 13$. Hence y is odd, so $y^2 \equiv 1 \bmod 8$. Consequently $x^3 = y^2 + 13 \equiv 6 \bmod 8$. This forces x to be even, but then $8 \mid x^3$ which gives a contradiction.

We deduce that there are no prime ideals of $\mathcal{O}_K$ which divide both $\langle y + \sqrt{-13}\rangle$ and $\langle y + \sqrt{-13}\rangle$.

Therefore we can apply Lemma 67 with $n = 3$. The equation (2) implies that there is an ideal $\mathfrak{a}$ such that

$$\langle y + \sqrt{-13}\rangle = \mathfrak{a}^3 \tag{3}$$

(and similarly for $\langle y - \sqrt{-13}\rangle$, but we won't need that).

Now we use the class group. Using the Minkowski bound and Dedekind–Kummer theorem, we can calculate $\mathrm{Cl}(\mathbb{Q}(\sqrt{-13})) = \mathbb{Z}/2\mathbb{Z}$. From equation (3), we get the following equation in the class group:

$$[\mathfrak{a}]^3 = [\langle y + \sqrt{-13}\rangle] = [1].$$

Since the class group has order 2, $[\mathfrak{a}]^2 = [1]$ so we deduce that $[\mathfrak{a}] = [1]$. In other words, $\mathfrak{a}$ is principal, so we have

$$\mathfrak{a} = \langle u + v\sqrt{-13}\rangle$$

for some $u, v \in \mathbb{Z}$.

Substituting this into (3), we get

$$\langle u + v\sqrt{-13}\rangle^3 = \langle y + \sqrt{-13}\rangle.$$

This implies that

$$(u + v\sqrt{-13})^3 = \alpha(y + \sqrt{-13})$$

where α is a unit in $\mathbb{Z}[\sqrt{-13}]$. The only units in $\mathbb{Z}[\sqrt{-13}]$ are ± 1 (because a unit must have norm ± 1, and the only integer solutions to $x^2 + 13y^2 = \pm 1$ are $(\pm 1, 0)$). So we get

$$(u + v\sqrt{-13})^3 = \pm(y + \sqrt{-13}).$$

Multiplying u and v by -1 if necessary, we may assume WLOG that

$$(u + v\sqrt{-13})^3 = y + \sqrt{-13}.$$

Expanding this out, we get

$$u^3 + 3u^2v\sqrt{-13} - 3 \times 13uv^2 - 13v^3\sqrt{-13} = y + \sqrt{-13}. \tag{4}$$

Because $\{1, \sqrt{-13}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{-13})$, we can group together the terms to get

$$u(u^2 - 39v^2) = y, \tag{5}$$

$$v(3u^2 - 13v^2) = 1. \tag{6}$$

From (6), we deduce that $v = \pm 1$ (since $u, v \in \mathbb{Z}$).
If $v = +1$, then $3u^2 - 13 = 1$ so $3u^2 = 14$ which has no integer solutions.
If $v = -1$, then $3u^2 - 13 = -1$ so $3u^2 = 12$ so $u = \pm 2$.
Substituting $(u, v) = (\pm 2, -1)$ into (5), we get

$$y = u(u^2 - 39v^2) = \pm 2 \times (4 - 39) = \pm 70.$$

We could find x by substituting this back into the original equation:

$$x^3 = y^2 + 13 = 4913.$$

Of course, we could calculate $\sqrt[3]{4913}$, but I don't know $\sqrt[3]{4913}$ off by heart!

With a little more manipulation of algebraic numbers, we can avoid calculations involving big numbers. In fact, our original equation (1) can be rewritten as

$$x^3 = \mathrm{Nm}_{K/\mathbb{Q}}(y + \sqrt{-13}).$$

Since norms are multiplicative, this becomes

$$x^3 = \mathrm{Nm}_{K/\mathbb{Q}}(u + v\sqrt{-13})^3.$$

Both sides of this equation are in $\mathbb{Z}$, where the only cube root of 1 is 1 itself. Thus we get

$$x = \mathrm{Nm}_{K/\mathbb{Q}}(u + v\sqrt{-13}) = u^2 + 13v^2 = 4 + 13 = 17.$$

Hence the only integer solutions to $y^2 = x^3 - 13$ are

$$x = 17, \quad y = \pm 70.$$

This equation has solutions which are rather large to find by manual brute force search. Of course a computer could have found them quickly, but it could not prove that they are the only solutions. This method allows us to do both – find the solutions and prove that there are no more – entirely by hand.

26. Dirichlet's Unit Theorem

Our final topic will be to understand the units in $\mathcal{O}_K$. We have seen that $x \in \mathcal{O}_K$ is a unit if and only if $\mathrm{Nm}_{K/\mathbb{Q}}(x) = \pm 1$.

Out of laziness I might say "unit of K" to mean "unit of $\mathcal{O}_K$" (the true units of K are not very interesting – just all the non-zero elements of K, because it is a field).

The following lemma shows that the property "α is a unit in $\mathcal{O}_K$" doesn't depend on which number field K we choose to look at (providing $\alpha \in K$ of course).

Lemma 68. *Let L/K be an extension of number fields and suppose that $\alpha \in K$. Then $\alpha \in \mathcal{O}_K^\times$ if and only if $\alpha \in \mathcal{O}_L^\times$.*

Proof. If $\alpha \in \mathcal{O}_K^\times$, then $\alpha \in \mathcal{O}_K \subseteq \mathcal{O}_L$ and $\alpha^{-1} \in \mathcal{O}_K \subseteq \mathcal{O}_L$ so $\alpha \in \mathcal{O}_L^\times$.

If $\alpha \in \mathcal{O}_L^\times$, then $\alpha, \alpha^{-1} \in \mathcal{O}_L$ so α, α^{-1} are both algebraic integers. We are given that $\alpha \in K$; since K is a field, this implies that $\alpha^{-1} \in K$ (note that $\alpha \neq 0$ because $\alpha \in \mathcal{O}_L^\times$). Thus α, α^{-1} are both algebraic integers contained in K i.e. they are both in $\mathcal{O}_K$. Hence $\alpha \in \mathcal{O}_K^\times$. □

Roots of unity.

Definition. Let K be a number field. We write

$$\mu_K = \{\zeta \in K : \zeta \text{ is a root of unity}\}.$$

Lemma 69. $\mu_K \subseteq \mathcal{O}_K^\times$.

Proof. Let $\zeta \in \mu_K$. Then ζ is a root of $X^n - 1$ for some n, so ζ is an algebraic integer. Since $\zeta \in K$, we deduce that $\zeta \in \mathcal{O}_K$.

We have $\zeta^{-1} = \zeta^{n-1} \in \mathcal{O}_K$ (because $\mathcal{O}_K$ is a ring) so ζ is a unit in $\mathcal{O}_K$. □

Indeed, roots of unity are elements of $\mathcal{O}_K^\times$ of finite order w.r.t. multiplication; conversely, any element of $\mathcal{O}_K^\times$ of finite order is a root of unity.

Lemma 70. *For any number field K, μ_K is a finite cyclic group under multiplication.*

Proof. It is clear that μ_K is closed under multiplication and under multiplicative inverses, and contains 1, so μ_K is a group under multiplication.

To prove that μ_K is finite: let ζ be a primitive n-th root of unity (i.e. $\zeta^n = 1$ but $\zeta^m \neq 1$ if $1 \leq m \leq n-1$). The minimal polynomial of ζ is the n-th cyclotomic polynomial $\Phi_n(X)$, which has degree $\phi(n)$ (Euler's totient function) – this was proved in Algebra 2. Hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$. Furthermore, $\phi(n) \geq \sqrt{n}$ for all $n \geq 3$ (you can prove this using the formula for $\phi(n)$ in terms of the prime factorisation of n).

So if $\zeta \in K$, we must have

$$[K : \mathbb{Q}] > [\mathbb{Q}(\zeta) : \mathbb{Q}] \geq \sqrt{n}.$$

Since K is a fixed number field, this means that there are only finitely many possible values of n. In other words, there are only finitely many possible values for the order n of a root of unity in K.

Furthermore for each n, there are only finitely many n-th roots of unity. Hence K contains only finitely many roots of unity.

To show that μ_K is cyclic, we use another result from Algebra 2: any finite subgroup of the multiplicative group of a field is cyclic. □

Lemma 71. *If K has at least one real embedding, then $\mu_K = \{\pm 1\}$.*

Proof. Let σ be a real embedding of K. For $\zeta \in \mu_K$, we have $\zeta^n = 1$ for some n. Then $\sigma(\zeta) \in \mathbb{R}$ and $\sigma(\zeta)^n = 1$, which implies that $\sigma(\zeta) = \pm 1$.

But of course $\sigma(1) = 1$ and $\sigma(-1) = -1$. Since σ is injective, we must have $\zeta = \pm 1$. □

On the other hand, if all the embeddings of K are complex, then there is no shortcut to finding μ_K.

For imaginary quadratic fields, we can easily work out all the units.

Lemma 72. *Let d be a square-free positive integer and let $K = \mathbb{Q}(\sqrt{-d})$. Then $\mathcal{O}_K^\times = \mu_K$. More precisely,*

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } d = 1 \\ \{\pm 1, \pm\zeta, \pm\zeta^2\} & \text{if } d = 3, \text{ where } \zeta = \exp(2\pi i/3) = \frac{-1+\sqrt{-3}}{2} \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

Proof. If $d \equiv 1$ or $2 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$. So any $\alpha \in \mathcal{O}_K^\times$ can be written as $x + y\sqrt{-d}$, with $x, y \in \mathbb{Z}$ and

$$\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = x^2 + dy^2 = \pm 1.$$

Now $x^2 + dy^2$ is always positive, so there are no solutions to $x^2 + dy^2 = -1$. To get a solution to $x^2 + dy^2 = 1$, we must have $x^2 = 1, dy^2 = 0$ (giving $x = \pm 1$, $y = 0$ – this corresponds to the units ± 1, which exist in every field) or else $x^2 = 0, dy^2 = 1$ (this is only possible if $d = 1$, in which case $x = 0$, $y = \pm 1$ so $\alpha = \pm i$).

If $d \equiv 3 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. So any $\alpha \in \mathcal{O}_K^\times$ can be written as $\frac{x+y\sqrt{-d}}{2}$, with $x, y \in \mathbb{Z}$. Since $\mathrm{Nm}_{K/\mathbb{Q}} = (x^2 + dy^2)/4$, we get

$$x^2 + dy^2 = \pm 4.$$

This implies that $x^2 \leq 4$ so we get three cases:

- $x = 0$. Then $dy^2 = 4$. This forces $d = 1$, 2 or 4 but none of these are $\equiv 3 \bmod 4$.
- $x = \pm 1$. Then $dy^2 = 3$. So we must have $d = 3$, $y = \pm 1$. Thus we get the units $\frac{\pm 1 \pm \sqrt{-3}}{2} = \pm\zeta, \pm\zeta^2$.
- $x = \pm 4$. Then $dy^2 = 0$ so $y = 0$. This gives the units ± 1, in any field. □

Thus for imaginary quadratic fields, we see that $\mathcal{O}_K^\times$ is finite.

For real quadratic fields, Lemma 71 tells us that $\mu_K = \{\pm 1\}$. But we shall show that $\mathcal{O}_K^\times$ is always infinite. For now, observe that this is true for $K = \mathbb{Q}(\sqrt{2})$

because $1+\sqrt{2} \in \mathcal{O}_K$ and $\mathrm{Nm}_{K/\mathbb{Q}}(1+\sqrt{2}) = -1$, so $1+\sqrt{2} \in \mathcal{O}_K^\times$. But $1+\sqrt{2}$ is not a root of unity (it is real and not in ± 1) so the set $\{(1+\sqrt{2})^n : n \in \mathbb{Z}\}$ is an infinite set of units in $\mathbb{Z}[\sqrt{2}]$.

Dirichlet's Unit Theorem.

Dirichlet's Unit Theorem gives us a description of $\mathcal{O}_K^\times$ as a group under multiplication. We have seen that the torsion elements are the roots of unity μ_K, which form a finite cyclic group. The theorem tells us that the group $\mathcal{O}_K^\times$ is the product of μ_K with a finitely generated abelian group, and furthermore it tells us the rank of that finitely generated abelian group in terms of the signature of K.

Theorem 73. *Let K be a number field of signature (r,s). Let μ_K denote the set of roots of unity in K. Then $\mathcal{O}_K^\times$ is isomorphic to $\mu_K \times \mathbb{Z}^{r+s-1}$ as an abelian group (with the operation of multiplication).*

e.g. $K = \mathbb{Q}$: the signature is $(1,0)$ so $r+s-1 = 0$. Thus $\mathcal{O}_K^\times = \mu_K = \{\pm 1\}$, which matches what we know about $\mathbb{Z}^\times$.

Similarly for an imaginary quadratic field: the signature is $(0,1)$ so $r+s-1 = 0$. Thus $\mathcal{O}_K^\times = \mu_K$ is finite, agreeing with Lemma 72.

Meanwhile a real quadratic field has signature $(2,0)$ so $r+s-1 = 1$. Hence $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$ by Lemma 71. Thus $\mathcal{O}_K^\times$ is infinite, matching what we saw for $\mathbb{Q}(\sqrt{2})$.

27. Units of a real quadratic field

Fundamental units.

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. We saw yesterday that Dirichlet's Unit Theorem implies that

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

In other words, there is some $\varepsilon \in \mathcal{O}_K^\times$ such that

$$\mathcal{O}_K^\times = \{\pm \varepsilon^n : n \in \mathbb{Z}\},$$

and ε is not a root of unity.

There may be more than one possible choice of ε such that $\mathcal{O}_K^\times$ has this form: indeed, $-\varepsilon$, ε^{-1} or $-\varepsilon^{-1}$ will also work. In fact, these are the only possibilities. This could be considered obvious from the structure of the group $\{\pm 1\} \times \mathbb{Z}$, but let's prove it carefully.

Lemma 74. *Let K be a real quadratic field and suppose that*

$$\mathcal{O}_K^\times = \{\pm \varepsilon^n : n \in \mathbb{Z}\}.$$

Let $\eta \in \mathcal{O}_K^\times$ be such that we also have

$$\mathcal{O}_K^\times = \{\pm \eta^n : n \in \mathbb{Z}\}.$$

Then

$$\eta \in \{\pm \varepsilon, \pm \varepsilon^{-1}\}.$$

Proof. From the defining property of ε and since $\eta \in \mathcal{O}_K^\times$, we have

$$\eta = u\varepsilon^n$$

for some $n \in \mathbb{Z}$ and $u \in \{\pm 1\}$.

Similarly from the defining property of η and since $\varepsilon \in \mathcal{O}_K^\times$, we have

$$\varepsilon = v\eta^m$$

for some $m \in \mathbb{Z}$ and $v \in \{\pm 1\}$.

Now

$$\eta = uv^n \eta^{mn}$$

so

$$\eta^{mn-1} = uv^n = \pm 1.$$

Since η is not a root of unity, this implies that $mn - 1 = 0$ and so $m = n = 1$ or $m = n = -1$. □

We consider K as a subfield of $\mathbb{R}$ (via the embedding for which $\sqrt{d} > 0$).

Replacing ε by $-\varepsilon$ if necessary, we may assume that ε is positive. Then replacing ε by ε^{-1} if necessary, we may assume that $\varepsilon > 1$. We then have

$$-\varepsilon < -1, \quad -1 < -\varepsilon^{-1} < 0, \quad 0 < \varepsilon^{-1} < 1.$$

In conclusion we see that there is a *unique* $\varepsilon > 1$ such that

$$\mathcal{O}_K^\times = \{\pm \varepsilon^n : n \in \mathbb{Z}\}.$$

We call this ε the **fundamental unit** of K.

The following proposition tells us how to find the fundamental unit.

Proposition 75. *The fundamental unit is given by $x + y\sqrt{d}$ where (x, y) is the solution to*

$$x^2 - dy^2 = \pm 1$$

with the smallest *possible value of x, where*

- *x, y are positive integers if $d \equiv 2, 3 \bmod 4$,*
- *x, y are positive half-integers if $d \equiv 1 \bmod 4$.*

Proof. First let η be *any* unit of $\mathcal{O}_K$ greater than 1. Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \bmod 4$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$, we can write $\eta = u + v\sqrt{d}$ where u, v are integers or half-integers respectively. Since $\eta \in \mathcal{O}_K^\times$, we have

$$(u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2 = \mathrm{Nm}_{K/\mathbb{Q}}(\eta) = \pm 1.$$

Hence $u - v\sqrt{d} = \pm\eta^{-1}$.

We conclude that the four elements $\pm u \pm u\sqrt{d}$ are in fact $\pm\eta, \pm\eta^{-1}$ in some order. Since $\eta > 1$, it is the largest of these four elements, so u, v are both positive.

Let ε be the fundamental unit. Applying the above argument to ε, we can write

$$\varepsilon = x + y\sqrt{d}$$

where x, y are positive integers or half-integers as appropriate, satisfying $x^2 - dy^2 = \pm 1$.

If (u, v) is another solution of the equation with u, v positive integers (when $d \equiv 2, 3 \bmod 4$) or positive half-integers (when $d \equiv 1 \bmod 4$), then $\eta := u + v\sqrt{d}$ is in $\mathcal{O}_K^\times$. (To prove this, we first check that $u + v\sqrt{d} \in \mathcal{O}_K$; then the equation tells us that the norm is ± 1, so it is in $\mathcal{O}_K^\times$. If $d \equiv 2$ or $3 \bmod 4$, then $u, v \in \mathbb{Z}$ so certainly $u + v\sqrt{d} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. But if $d \equiv 1 \bmod 4$, then we are only given that $2u, 2v \in \mathbb{Z}$ and we have to check that $u + v\sqrt{d} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. In other words, we have to check that u and v are either both integers or both non-integers – we can rewrite this as $2u \equiv 2v \bmod 2$ (remember this is a non-trivial congruence because u, v might not be integers). This follows from the equation $(2u)^2 - d(2v)^2 = \pm 4$, since d is odd.) Consequently $\eta = \pm\varepsilon^n$ for some $n \in \mathbb{Z}$.

Furthermore since $u, v > 0$, η is the largest out of $\{\pm u \pm v\sqrt{d}\}$, and as above this set is equal to $\{\pm\eta, \pm\eta^{-1}\}$. Hence $\eta > \eta^{-1}$ so $\eta > 1$. Therefore

$$\eta = \varepsilon^n \text{ with } n > 1.$$

Hence $\eta \geq \varepsilon$. Thus ε is the smallest unit greater than 1.

It remains to show that "smallest $\varepsilon > 1$" is equivalent to "smallest $x > 0$."

If $\mathrm{Nm}(\varepsilon) = +1$, then also $\mathrm{Nm}(\eta) = +1$. We want to show that $x \leq u$. Assume for contradiction that $x > u$. Then

$$v^2 = \frac{u^2 - 1}{d} < \frac{x^2 - 1}{d} = y^2.$$

Since y, v are both positive, we get $y > v$. But now $x + y\sqrt{d} > u + v\sqrt{d}$, contradicting the fact that $\varepsilon \leq \eta$.

If $\mathrm{Nm}(\varepsilon) = -1$, then $\mathrm{Nm}(\eta)$ may be $+1$ or -1. Again assume for contradiction that $x > u$. We get

$$v^2 = \frac{u^2 \pm 1}{d} < \frac{x^2 + 1}{d} = y^2.$$

Thus again $y > v$ so $x + y\sqrt{d} > u + v\sqrt{d}$, contradicting the fact that $\varepsilon \leq \eta$.

At the end of the lecture, someone suggested another way of getting from "$\varepsilon \leq \eta$" to "$x \leq u$": write out the binomial expansion of

$$u + v\sqrt{d} = (x + y\sqrt{d})^n.$$

Since $1, \sqrt{d}$ are $\mathbb{Q}$-linearly independent, you get $u = x^n +$ positive terms. If $x \geq 1$, this immediately implies that $x \leq u$. If $x = \frac{1}{2}$, then you have to work a little harder but can still finish it off. □

e.g. $1 + \sqrt{2}$ is a unit of $\mathbb{Q}(\sqrt{2})$ which is bigger than 1. It has $x = 1$, which is certainly the smallest possible value for a positive integer! So $1 + \sqrt{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{2})$, proving that

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^n : n \in \mathbb{Z}\}.$$

e.g. We find the fundamental unit of $K = \mathbb{Q}(\sqrt{6})$.

Here $6 \equiv 2 \bmod 4$ so we look for solutions to $x^2 - 6y^2 = \pm 1$ with x, y positive integers.

If $x = 1$, then $6y^2 = 1 \pm 1 = 0$ or 2, leading to the solution $x = 1$, $y = 0$. But we are looking for y to be a positive integer, so this doesn't count. (We have just rediscovered that $1 \in \mathcal{O}_K^\times$, but it is a root of unity!)

If $x = 2, 3$ or 4, then there are no integer solutions for y.

If $x = 5$, then $6y^2 = 25 \pm 1 = 24$ or 26. This has a solution $y = 2$. Thus the fundamental unit of $\mathbb{Q}(\sqrt{6})$ is

$$5 + 2\sqrt{6}.$$

Consequently all the units of $\mathbb{Z}[\sqrt{6}]$ are given by

$$\mathcal{O}_K^\times = \{\pm(5 + 2\sqrt{6}^n : n \in \mathbb{Z}\}.$$

We have

$$\mathrm{Nm}_{K/\mathbb{Q}}(5 + 2\sqrt{6}) = 25 - 24 = +1.$$

Hence all units of $\mathbb{Q}(\sqrt{6})$ have norm $+1$.

We can translate the fact that $5 + 2\sqrt{6}$ is the fundamental unit into a statement about solutions of **Pell's equation**: the integer solutions of $x^2 - 6y^2 = 1$ are precisely

$$\{(x, y) : x + y\sqrt{6} = \pm(5 + 2\sqrt{6})^n, n \in \mathbb{Z}\}.$$

There are no units of norm -1, so the equation $x^2 - 6y^2 = -1$ has no solutions (we could also have proved this by working mod 3!).

On the other hand, if the fundamental unit turned out to have norm -1, then solutions of Pell's equation $x^2 - dy^2 = 1$ would be given by even powers of the fundamental unit, while solutions of $x^2 - dy^2 = -1$ would be given by odd powers of the fundamental unit.

28. Pell's equation

Pell's equation for $d \equiv 1 \bmod 4$.

We want to use the theory of units in quadratic fields to study solutions of the Diophantine equation

$$x^2 - dy^2 = 1,$$

where d is a positive square-free integer, known as **Pell's equation**.

We saw yesterday that, if $d \equiv 2$ or $3 \bmod 4$, and if the fundamental unit ε of $\mathbb{Q}(\sqrt{d})$ has norm $+1$, then all the integer solutions to Pell's equation are given by

$$\{(x, y) : x + y\sqrt{d} = \pm\varepsilon^n \text{ for some } n \in \mathbb{Z}\}.$$

Similarly, if the fundamental unit ε has norm -1, then all the integer solutions to Pell's equation are given by

$$\{(x, y) : x + y\sqrt{d} = \pm\varepsilon^{2n} \text{ for some } n \in \mathbb{Z}\},$$

In particular, if $d \equiv 2$ or $3 \bmod 4$, then Pell's equation always has infinitely many integer solutions.

If $d \equiv 1 \bmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and so ε might not be in $\mathbb{Z}[\sqrt{d}]$. This means we have to work a bit harder to guarantee that Pell's equation has a non-trivial integer solution.

We will prove this by doing "modular arithmetic in $\mathcal{O}_K$." More specifically, we will work modulo the ideal $\langle 2\rangle$ (a natural choice because of the denominator of $\frac{1+\sqrt{d}}{2}$). In order to do this, we need to understand the structure of the quotient ring $\mathcal{O}_K/\langle 2\rangle$, and we shall find this using a version of the Chinese Remainder Theorem.

Recall the abstract form of the Chinese Remainder Theorem from Algebra 2.

Theorem 76 (Chinese Remainder Theorem)**.** *Let $I_1, \ldots, I_n$ be a finite set of ideals in a ring R. Let $J = I_1 \cap \cdots \cap I_n$. Suppose that for every pair of ideals I_i, I_j, we have $I_i + I_j = R$. Then there is a ring isomorphism $R/J \to \prod_{i=1}^n R/I_i$.*

Corollary 77. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct non-zero prime ideals in the ring of integers of a number field $\mathcal{O}_K$. Let $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i$. Then there is a ring isomorphism $R/\mathfrak{a} \to \prod_{i=1}^n R/\mathfrak{p}_i$.*

Proof. Since $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct maximal ideals, they satisfy the condition $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$ for each pair i, j. Hence by Theorem 76, there is a ring isomorphism $\mathcal{O}_K/\mathfrak{b} \to \prod_{i=1}^n \mathcal{O}_K/\mathfrak{p}_i$, where $\mathfrak{b} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.

This is not quite what we want: we have to check that $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = \prod_{i=1}^n \mathfrak{p}_i$. First, it is clear that $\prod_{i=1}^n \mathfrak{p}_i \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ i.e. $\mathfrak{a} \subseteq \mathfrak{b}$. Hence there is a surjection $\mathcal{O}_K/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{b}$. Composing with the isomorphism from Theorem 76, we get a surjection

$$\phi\colon \mathcal{O}_K/\mathfrak{a} \to \prod_{i=1}^n \mathcal{O}_K/\mathfrak{p}_i.$$

Since ideal norms are multiplicative, we have

$$\#\mathcal{O}_K/\mathfrak{a} = \mathrm{Nm}(\mathfrak{a}) = \prod_{i=1}^{n} \mathrm{Nm}(\mathfrak{p}_i) = \#\Big(\prod \mathcal{O}_K/\mathfrak{p}_i\Big).$$

Thus ϕ is a surjection between finite sets of the same size, so it is a bijection. □

Lemma 78. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer with $d \equiv 1 \bmod 4$, $d \neq 0$ or 1. Then $\mathcal{O}_K/\langle 2\rangle$ is isomorphic (as a ring) to either $\mathbb{F}_2 \times \mathbb{F}_2$ or the field of order 4.*

Proof. Let $\alpha = \frac{1+\sqrt{d}}{2}$, so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The minimal polynomial of α is $f(X) = X^2 - X + \frac{1-d}{4}$.

If $d \equiv 1 \bmod 8$, then $f(X) \equiv X(X-1) \bmod 2$ and so by the Dedekind–Kummer theorem, $\langle 2\rangle = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p}$, $\mathfrak{q}$ are distinct prime ideals each of norm 2. By Corollary 77, there is a ring isomorphism $\mathcal{O}_K/\langle 2\rangle \to \mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{q}$. Since each of $\mathfrak{p}$ and $\mathfrak{q}$ is a maximal ideal, the quotient rings $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{q}$ are fields; since $\mathrm{Nm}(\mathfrak{p}) = \mathrm{Nm}(\mathfrak{q}) = 2$, they are both isomorphic to $\mathbb{F}_2$. Thus $\mathcal{O}_K/\langle 2\rangle \cong \mathbb{F}_2 \times \mathbb{F}_2$.

If $d \equiv 5 \bmod 8$, then $f(X) \equiv X^2 + X + 1 \bmod 2$, which is irreducible in $\mathbb{F}_2[X]$. Hence by the Dedekind–Kummer theorem, $\langle 2\rangle$ is a prime ideal in $\mathcal{O}_K$. Consequently it is a maximal ideal, so $\mathcal{O}_K/\langle 2\rangle$ is a field. We have $\mathrm{Nm}(\langle 2\rangle) = 4$, so $\mathcal{O}_K/\langle 2\rangle$ must be the field of order 4. □

We now use another result of modular arithmetic: a version of the Fermat–Euler theorem for $\mathcal{O}_K$.

Lemma 79. *Let K be a number field and let $\mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal. Let $f = \#(\mathcal{O}_K/\mathfrak{a})^\times$. For every $\beta \in \mathcal{O}_K^\times$, we have $\beta^f \in 1 + \mathfrak{a}$.*

Proof. If $\beta \in \mathcal{O}_K^\times$, then $\beta^{-1} \in \mathcal{O}_K$. So we have the following equation in $\mathcal{O}_K/\mathfrak{a}$:

$$(\beta + \mathfrak{a})(\beta^{-1} + \mathfrak{a}) = 1 + \mathfrak{a}.$$

Thus $\beta + \mathfrak{a} \in (\mathcal{O}_K/\mathfrak{a})^\times$.

By Lagrange's theorem in the multiplicative group $(\mathcal{O}_K/\mathfrak{a})^\times$, we get

$$\beta^f + \mathfrak{a} = (\beta + \mathfrak{a})^f = 1 + \mathfrak{a}$$

and so $\beta^f \in 1 + \mathfrak{a}$. □

Lemma 80. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer with $d \equiv 1 \bmod 4$, $d \neq 1$. For every $\alpha \in \mathcal{O}_K^\times$, we have $\alpha^3 \in \mathbb{Z}[\sqrt{d}]$.*

Proof. In order to apply Lemma 79, we need to calculate the size of $(\mathcal{O}_K/\mathfrak{a})^\times$.

If $\mathcal{O}_K/\langle 2\rangle \cong \mathbb{F}_2 \times \mathbb{F}_2$: the only unit in $\mathbb{F}_2 \times \mathbb{F}_2$ is $(1,1)$ so $(\mathcal{O}_K/\langle 2\rangle)^\times \cong (\mathbb{F}_2 \times \mathbb{F}_2)^\times$ is the trivial group.

If $\mathcal{O}_K/\langle 2\rangle$ is the field of order 4: every non-zero element of a field is invertible. Hence the field of order 4 contains $4-1 = 3$ invertible elements, i.e. $\#(\mathcal{O}_K/\langle 2\rangle)^\times = 3$.

Thus $\#(\mathcal{O}_K/\mathfrak{a})^\times = 1$ or 3. So Lemma 79 tells us that for any $\alpha \in \mathcal{O}_K^\times$, $\alpha^3 \in 1 + \langle 2\rangle$ i.e. $\alpha^3 = 1 + 2\beta$ for some $\beta \in \mathcal{O}_K$. Since $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, we have $2\beta \in \mathbb{Z}[\sqrt{d}]$ and so $1 + 2\beta \in \mathbb{Z}[\sqrt{d}]$. □

Now let ε be the fundamental unit of $\mathbb{Q}(\sqrt{d})$ where $d \equiv 1 \bmod 4$. If $\varepsilon \in \mathbb{Z}[\sqrt{d}]$, then we can get all the solutions of Pell's equation $x^2 - dy^2 = 1$ in the same way as before.

If $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$, then Lemma 80 tells us that $\varepsilon^3 \in \mathbb{Z}[\sqrt{d}]$, and also ε^{3n} for every $n \in \mathbb{Z}$. Thus Pell's equation still has infinitely many solutions: an infinite set of solutions is given by

$$\{(x, y) : x + y\sqrt{d} = \pm\varepsilon^{3n} \text{ for some } n \in \mathbb{Z}\} \text{ if } \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon) = +1,$$
$$\{(x, y) : x + y\sqrt{d} = \pm\varepsilon^{6n} \text{ for some } n \in \mathbb{Z}\} \text{ if } \mathrm{Nm}_{K/\mathbb{Q}}(\varepsilon) = -1.$$

(End of examinable material)

29. Proof of Dirichlet's Unit Theorem

(All of this lecture is non-examinable.)

Our goal today is to outline the proof of Dirichlet's unit theorem.

Lattices and discrete subgroups of $\mathbb{R}^n$.

First we need some more facts about lattices.

Lemma 81. *Let L be a subgroup of $(\mathbb{R}^n, +)$. Then L is a lattice if and only if both of the following conditions are satisfied:*

(i) L is discrete;
(ii) there exists a compact set C such that $L + C = \mathbb{R}^n$.

Lemma 82. *Let L be a subgroup of $(\mathbb{R}^n, +)$. Then L is discrete if and only if, for every bounded subset $B \subseteq \mathbb{R}^n$, the intersection $B \cap L$ is finite.*

(In the lecture, I said that Lemma 82 holds for every subset of $\mathbb{R}^n$. This is false – it only holds for subgroups.)

Corollary 83. *For any positive real number R, the set*

$$\{\alpha \in \mathcal{O}_K : |\sigma(\alpha)| \leq R \text{ for all embeddings } \sigma \text{ of } K\}$$

is finite.

Proof. We use the canonical embedding $\iota\colon K \to \mathbb{R}^n$ from lecture 24.

Since $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$, it is a discrete subgroup. The set

$$\{(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^n : |x_i| \leq R \text{ for } 1 \leq i \leq r, \sqrt{y_i^2 + z_i^2} \leq R \text{ for } 1 \leq i \leq s\}$$

is a bounded subset, so its intersection with $\iota(\mathcal{O}_K)$ is finite. □

The logarithm map.

The group $\mathcal{O}_K^\times$ has multiplication as its operation, but in order to use lattices we need additive groups. So we will use a logarithm map to map $\mathcal{O}_K^\times$ into an additive group.

We can only take the logarithm of non-zero numbers, so let

$$(\mathbb{R}^{r+2s})^* = \{(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) \in \mathbb{R}^{r+2s} : x_i \neq 0, (y_i, z_i) \neq (0, 0) \text{ for all } i\}.$$

Note that we can make $(\mathbb{R}^{r+2s})^*$ into a multiplicative group. Formally we define

$$\begin{aligned}(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) &\cdot (x_1', \ldots, x_r', y_1', z_1', \ldots, y_s', z_s') \\ &= (x_1x_1',\ \ldots,\ x_rx_r',\ y_1y_1' - z_1z_1',\ y_1z_1' + z_1y_1',\ \ldots,\ y_sy_s' - z_sz_s',\ z_sz_s' + z_sy_s').\end{aligned}$$

In other words: we just multiply together the x_is coordinate-wise. We treat each pair y_j, z_j as a complex number $y_j + iz_j$ and multiply these as complex numbers, then split back up into real and imaginary parts.

With this definition, ι restricts to a homomorphism of multiplicative groups $K^\times \to (\mathbb{R}^{r+2s})^*$. (Indeed, we have just defined a ring structure on $\mathbb{R}^{r+2s}$, isomorphic to $\mathbb{R}^r \times \mathbb{C}^s$, and ι is a ring homomorphism i.e. both additive and multiplicative.)

Recall that we defined $N_{r,s}\colon \mathbb{R}^{r+2s} \to \mathbb{R}$ by

$$N_{r,s}(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = |x_1| \cdots |x_r|(y_1^2 + z_1^2) \cdots (y_s^2 + z_s^2).$$

Observe that

$$(\mathbb{R}^{r+2s})^* = \{\underline{x} \in \mathbb{R}^{r+2s} : N_{r,s}(\underline{x}) \neq 0\}$$

and $N_{r,s}$ restricts to a homomorphism of multiplicative groups $(\mathbb{R}^{r+2s})^* \to \mathbb{R}^\times$.

Define $\ell\colon (\mathbb{R}^{r+2s})^* \to \mathbb{R}^{r+s}$ by

$$\ell(x_1, \ldots, x_r, y_1, z_1, \ldots, y_s, z_s) = (\log|x_1|, \ldots, \log|x_r|, \log(y_1^2 + z_1^2), \ldots, \log(y_s^2 + z_s^2)).$$

This is a homomorphism from a multiplicative group to an additive group.

Let $\lambda = \ell \circ \iota\colon K^\times \to \mathbb{R}^{r+s}$.

We will study the kernel and the image of λ restricted to $\mathcal{O}_K^\times$.

The kernel of the logarithm map.

The map $\lambda\colon \mathcal{O}_K^\times \to \mathbb{R}^{r+s}$ is not injective. Its kernel is

$$\{\alpha \in \mathcal{O}_K^\times : |\sigma(\alpha)| = 1 \text{ for all embeddings } \sigma \text{ of } K\}.$$

By Corollary 83, $\ker(\lambda)$ is finite. Since $\ker(\lambda)$ is a group, every element of it must be torsion i.e. every element of $\ker(\lambda)$ is a root of unity.

Conversely, if ζ is a root of unity, then every embedding of ζ satisfies $|\sigma(\zeta)| = 1$.

Thus $\ker(\lambda) = \mu_K$.

The image of the logarithm map.

We would like to show that $\lambda(\mathcal{O}_K^\times)$ is a lattice in $\mathbb{R}^{r+s}$ – but this cannot quite be true, because it is contained in a linear subspace of $\mathbb{R}^{r+s}$.

Indeed, observe that if $\underline{x} \in (\mathbb{R}^{r+2s})^*$ and $\ell(\underline{x}) = (u_1, \ldots, u_{r+s})$, then

$$u_1 + \cdots + u_{r+s} = \log N_{r,s}(\underline{x}).$$

If $\alpha \in \mathcal{O}_K^\times$, then $N_{r,s}(\iota(\alpha)) = |\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| = 1$ so if $\lambda(\alpha) = (u_1, \ldots, u_{r+s})$, we get

$$u_1 + \cdots + u_{r+s} = 0.$$

In other words, $\lambda(\mathcal{O}_K^\times)$ is contained in the linear subspace

$$H = \{(u_1, \ldots, u_{r+s}) \in \mathbb{R}^{r+s} : u_1 + \cdots + u_n = 0\}.$$

It will be useful to consider a "multiplicative" version of H. Let

$$S = \{\underline{x} \in \mathbb{R}^n : N_{r,s}(\underline{x}) = 1\}.$$

Then the fact that $\lambda(\mathcal{O}_K^\times) \subseteq H$ can be broken up as:

$$\iota(\mathcal{O}_K^\times) \subseteq S, \quad \ell(S) \subseteq H.$$

Now H is a $\mathbb{R}$-vector space of dimension $r + s - 1$. We will use Lemma 81 to show that $\lambda(\mathcal{O}_K^\times)$ is a lattice in H. The easier part is showing that it is discrete.

Lemma 84. *$\lambda(\mathcal{O}_K^\times)$ is a discrete subgroup of $(H, +)$.*

Proof. Let $B \subseteq H$ be a bounded subset. Then $B' = \ell^{-1}(B)$ is a bounded subset of $\mathbb{R}^{r+2s}$ (if all coordinates of elements of B are bounded by R, then all coordinates of $\ell^{-1}(B)$ are bounded by $\exp(R)$). Hence by Lemma 82, $B' \cap \iota(\mathcal{O}_K)$ is finite.

Applying ℓ, we deduce that $B' \cap \lambda(\mathcal{O}_K^\times)$ is finite and so we are done by the other direction of Lemma 82. □

Now we have to prove the second condition from Lemma 81. We shall deduce this from an analogous result for $\iota(\mathcal{O}_K^\times) \subseteq S \subseteq \mathbb{R}^n$.

Lemma 85. *There exists a compact set $C' \subseteq S$ such that $S = \iota(\mathcal{O}_K^\times).C'$ (in the multiplicative group structure on S; note that S is a subgroup of $(\mathbb{R}^{r+2s})^*$).*

Proof. Choose a compact, convex, symmetric set $X \subseteq \mathbb{R}^n$ of volume at least $2^n \operatorname{covol}(\iota(\mathcal{O}_K))$. (Unlike when we used Minkowski's theorem to study ideals, we don't care what compact set we use, only that it is large enough.)

Since X is compact, the continuous function $N_{r,s}$ is bounded on X i.e. we can pick N such that $N_{r,s}(\underline{x}) \leq N$ for all $\underline{x} \in X$.

We know that $\mathcal{O}_K$ contains only finitely many non-zero ideals of norm $\leq N$; hence it contains only finitely many non-zero principal ideals of norm $\leq N$. Pick $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_K$ such that $\langle\alpha_1\rangle, \ldots, \langle\alpha_m\rangle$ is the list of all non-zero principal ideals of $\mathcal{O}_K$ of norm $\leq N$. Now if β is any non-zero element of $\mathcal{O}_K$ of norm $\leq N$, $\langle\beta\rangle = \langle\alpha_i\rangle$ for some i and so $\beta = \varepsilon\alpha_i$ for some $\varepsilon \in \mathcal{O}_K^\times$.

Consider any $\gamma \in S$. Multiplication by γ gives a linear map $m_\gamma \colon \mathbb{R}^{r+2s} \to \mathbb{R}^{r+2s}$, and $\det(m_\gamma) = N_{r,s}(\gamma) = 1$. Hence

$$\operatorname{vol}(\gamma.X) = \operatorname{vol}(X) \geq 2^n \operatorname{covol}(\iota(\mathcal{O}_K)).$$

Hence by Minkowski's theorem on lattices, $\gamma.X \cap \iota(\mathcal{O}_K) \neq \{0\}$ i.e. we can choose $\beta \in \mathcal{O}_K \setminus \{0\}$ such that $\iota(\beta) \in \gamma.X$. Multiplying by γ does not change $N_{r,s}$, so

$$|\mathrm{Nm}_{K/\mathbb{Q}}(\beta)| = N_{r,s}(\iota(\beta)) \leq N.$$

Hence $\beta = \varepsilon\alpha_i$ for some i and some $\varepsilon \in \mathcal{O}_K^\times$ as above. Then

$$\gamma \in \beta^{-1}.X = \varepsilon^{-1}\alpha_i^{-1}X.$$

So if we let

$$C' = \bigcup_{i=1}^{m} \alpha_i^{-1}X \cap S,$$

we get $\gamma \in \mathcal{O}_K^\times.C'$. Furthermore C' is compact because $\alpha_i^{-1}.X$ is compact for each i, so the union of finitely many such sets is compact; and then we are intersecting with S which is closed in $\mathbb{R}^n$. □

Using the fact that $\ell \colon S \to H$ is surjective, we deduce that $\lambda(\mathcal{O}_K^\times) + C = H$ where $C' = \ell(C)$. Combining these lemmas establishes that $\ell(\iota(\mathcal{O}_K^\times))$ is a lattice in H, so it is isomorphic to $\mathbb{Z}^{\dim(H)} = \mathbb{Z}^{r+s-1}$.

So $\lambda_{|\mathcal{O}_K^\times} \colon \mathcal{O}_K^\times \to H$ has kernel μ_K and image isomorphic to $\mathbb{Z}^{r+s-1}$. It follows that $\mathcal{O}_K^\times$ is a finitely generated abelian group. By the structure theorem for finitely generated abelian groups, it is isomorphic to $A \times \mathbb{Z}^m$ where $A = (\mathcal{O}_K^\times)_{\mathrm{tors}}$ is a finite group and m is a nonnegative integer. We know that $(\mathcal{O}_K^\times)_{\mathrm{tors}} = \mu_K$, and then the fact that $\mathcal{O}_K^\times/\mu_K \cong \mathbb{Z}^{r+s-1}$ establishes that $m = r + s - 1$.