MA3A6 Algebraic Number Theory

Samir Siksek

Contents

CHAPTER 1

Introduction

These are my notes for the 2018 Algebraic Number Theory module. They follow the lectures very closely. Thanks to Ben Windsor, Patricia Ricamara, Emily Olsen, Luke Kershaw, and others for sending corrections.

In addition to the notes you might find it helpful to consult these textbooks:

- Steward and Tall, *Algebraic Number Theory*. Newer editions have the title *Algebraic Number Theory and Fermat's Last Theorem* but old editions are more than adequate. This is the most basic book.
- Frazer Jarvis, *Algebraic Number Theory*. Very accessible and probably most useful.
- Pierre Samuel, *Algebraic Theory of Numbers*. This is a sophisticated introduction, particularly suited if you're happy with Commutative Algebra and Galois Theory.
- Frohlich and Taylor, *Algebraic Number Theory*. Too long and thorough. If you find yourself really into the subject you might want to dip into the chapter on fields of low degree.
- Peter Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*. Much more sophisticated and concise than the first two references, and covers lots of advanced topics that we won't touch. If Algeraic Number Theory was a 4th year module this would probably be the right textbook.

CHAPTER 2

Number Fields

1. Field Extensions and Algebraic Numbers

DEFINITION. Let K, L be fields. We say that L/K is a field extension if K is a subfield of L.

For example $\mathbb{C}/\mathbb{R}$ is a field extension, and so is $\mathbb{R}/\mathbb{Q}$.

DEFINITION. Let L/K be an extension and let $\alpha \in L$. We say that α is **algebraic over** K if there is a non-zero polynomial $g(X) \in K[X]$ such that $g(\alpha) = 0$ (that is α is the root of a non-zero polynomial with coefficients in K).

EXAMPLE 1. $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ as it is a root of $X^2+1 \in \mathbb{Q}[X]$. Also $\sqrt[4]{7}$ is algebraic over $\mathbb{Q}$ as it is a root of ...

LEMMA 2. *Let α be algebraic over K.*

(i) *Then there is a unique polynomial $\mu_{K,\alpha}(X) \in K[X]$ such that $\mu_{K,\alpha}(\alpha) = 0$ and $\mu_{K,\alpha}(X)$ is irreducible and monic. We call $\mu_{K,\alpha}(X)$ the **minimal polynomial of** α **over** K.*

(ii) *If $f \in K[X]$ satisfies $f(\alpha) = 0$ then $\mu_{K,\alpha} \mid f$.*

PROOF. Let $I = \{f \in K[X] \ : \ f(\alpha) = 0\}$. Check that $I \subseteq K[X]$ satisfies the following three properties

- $0 \in I$,
- if f, $g \in I$ then $f + g \in I$,
- if $f \in I$ and $g \in K[X]$ then $gf \in I$.

In other words, I is an ideal of $K[X]$. As $K[X]$ is a PID we have $I = m \cdot K[X]$ (a principal ideal). As α is algebraic we see that $I \neq 0$. So $m \neq 0$. We can scale m so that it's monic and we let this be $\mu_{K,\alpha}$. Note that (ii) holds: if $f(\alpha) = 0$ then $f \in I = \mu_{K,\alpha} \cdot K[X]$ so $\mu_{K,\alpha} \mid f$.

We have to show that $\mu_{K,\alpha}$ is irreducible. Suppose $\mu_{K,\alpha} = f \cdot g$ where $\deg(f)$ and $\deg(g)$ are smaller than $\deg(\mu_{K,\alpha})$. Then $f(\alpha)g(\alpha) = \mu_{K,\alpha}(\alpha) = 0$. Without loss of generality $f(\alpha) = 0$, so by (ii) $\mu_{K,\alpha} \mid f$. This contradicts $\deg(f) < \deg(\mu_{K,\alpha})$.

We leave it as an excercise to check the uniqueness of $\mu_{K,\alpha}$. □

EXAMPLE 3. We shall write μ_α instead of $\mu_{K,\alpha}$ if K is understood. But it is important to understand that the minimal polynomial depends on the field. Let

$$K = \mathbb{Q}(\sqrt{2}), \qquad L = \mathbb{Q}(\sqrt{2} + i).$$

Let $\alpha = \sqrt{2} + i$. Then

$$\mu_{L,\alpha} = X - \alpha$$

since $\alpha \in L$. Let's compute $\mu_{K,\alpha}$ next. Note that

$$(\alpha - \sqrt{2})^2 = -1$$

which we can rewrite as

$$\alpha^2 - 2\sqrt{2}\alpha + 3 = 0. \tag{1}$$

Thus α is a root of $X^2 - 2\sqrt{2}X + 3 \in K[X]$. This polynomial is irreducible over K. If not then its roots belong to K; these are $\alpha = \sqrt{2}+i$ and $\overline{\alpha} = \sqrt{2}-i$. But $K \subset \mathbb{R}$ which gives a contradiction. Hence $\mu_{K,\alpha} = X^2 - 2\sqrt{2}X + 3$. Next, from (1)

$$(\alpha^2 + 3)^2 = (2\sqrt{2}\alpha)^2 = 8\alpha^2$$

thus $\alpha^4 - 2\alpha^2 + 9 = 0$. In other words, α is a root of $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$. You can check that this is irreducible over $\mathbb{Q}$, so $\mu_{\mathbb{Q},\alpha} = X^4 - 2X^2 + 9$.

Definition. Let L/K be an extension and let $\alpha \in L$ be algebraic over K. We define the **degree of** α over K to be the degree of its minimal polynomial $\mu_\alpha \in K[X]$.

Example 4. $\sqrt{2}$ has degree 2 over $\mathbb{Q}$ but degree 1 over $\mathbb{R}$.

By Example 3, $\sqrt{2} + i$ has degree 4 over $\mathbb{Q}$, degree 2 over $\mathbb{Q}(\sqrt{2})$ and degree 1 over $\mathbb{Q}(\sqrt{2}, i)$.

Definition. $\alpha \in \mathbb{C}$ is called an **algebraic number** if α is algebraic over $\mathbb{Q}$. The **degree** of α is the degree of $\mu_{\mathbb{Q},\alpha} \in \mathbb{Q}[X]$.

Example 5. We will see later that the set of algebraic numbers is in fact a subfield of $\mathbb{C}$; that is if you add, subtract, multiply or divide algebraic numbers you get algebraic numbers. For now we content ourselves with Example 3: we know that $\sqrt{2}$, i are algebraic numbers and we found that $\sqrt{2} + i$ is a root of $X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ so it is also an algebraic number. Note that $\sqrt{2}$, i have degree 2 but $\sqrt{2} + i$ has degree 4.

2. Field Generation

Definition. Let L/K be a field extension and S a subset of L. We define the **extension of** K **generated by** S to be the intersection of all the subfields of L which contain both K and S; we denote this by $K(S)$. If $S = \{\alpha_1, \ldots, \alpha_n\}$ we simply write $K(\alpha_1, \ldots, \alpha_n)$ instead of $K(S)$.

Lemma 6. *$K(S)$ is a subfield of L. It is the smallest subfield of L containing both K and S.*

Proof. Think about it. Here smallest means contained in all the others. □

EXAMPLE 7. If K is a field and S is a subset of K then $K(S) = K$, because K contains K and S and it's the smallest field containing both.

EXAMPLE 8. $\mathbb{R}(i) = \mathbb{C}$.

EXAMPLE 9. Let $d \in \mathbb{Q}$ be a non-square (i.e. $\sqrt{d}$ is irrational). We show that

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}. \tag{2}$$

Let

$$K = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}.$$

First we need to show that K is field. The easiest way to do this is to show that K is a subfield of $\mathbb{C}$. We leave this as an exercise (but you will need 'rationalizing the denominator' trick to show that K is closed under taking inverses).

We see that K is a field, and that it contains $\mathbb{Q}$ and $\sqrt{d}$. Let L be another field that contains both $\mathbb{Q}$ and $\sqrt{d}$. If a, $b \in \mathbb{Q}$, then a, b, $\sqrt{d} \in L$ so $a + b\sqrt{d} \in L$. Hence $K \subseteq L$. Thus K is the smallest field that contains both $\mathbb{Q}$ and $\sqrt{d}$, showing that $K = \mathbb{Q}(\sqrt{d})$ as required.

We see that $\mathbb{Q}(\sqrt{d})$ is an extension of $\mathbb{Q}$.

EXAMPLE 10. **Warning:** You should not assume that $\mathbb{Q}(\sqrt[3]{d})$ is that same as $\{a + b\sqrt[3]{d} : a, b \in \mathbb{Q}\}$. The set $\{a + b\sqrt[3]{d} : a, b \in \mathbb{Q}\}$ is not a field (it's not closed under multiplication). We'll come to $\mathbb{Q}(\sqrt[3]{d})$ in due course.

3. Algebraic and Finite Extensions

DEFINITION. Let L/K be an extension. We say that L/K is **algebraic** if every $\alpha \in L$ is algebraic over K.

EXAMPLE 11. Let $d \in \mathbb{Q}$ be a non-square as before. The extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is algebraic as every $\alpha = a+b\sqrt{d}$ is the root of $(X-a)^2-b^2d \in \mathbb{Q}[X]$.

Observe that if L/K is a field extension then L is a vector space over K.

DEFINITION. We define the **degree** of L/K to be the dimension of L as a K-vector space and denote this by $[L : K]$. We say that L/K is **finite** if $[L : K] < \infty$.

EXAMPLE 12. $\mathbb{C}$ has basis 1, i over $\mathbb{R}$, so $[\mathbb{C} : \mathbb{R}] = 2$.

EXAMPLE 13. $\mathbb{Q}(\sqrt{d})$ has $\mathbb{Q}$-basis 1, $\sqrt{d}$. Therefore $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$; in particular $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is finite.

EXAMPLE 14. $\mathbb{R}/\mathbb{Q}$ is an infinite extension. One way to check this is to prove that any finite dimensional $\mathbb{Q}$-vector space is countable, so $\mathbb{R}$ must be infinite dimensional as a $\mathbb{Q}$-vector space.

THEOREM 15. *Let L/K be finite. Then L/K is algebraic.*

PROOF. Let $[L : K] = m < \infty$. Let $\alpha \in L$. Then $1, \alpha, \ldots, \alpha^m$ are $m+1$ elements in the K-vector space L, and so must be linearly dependent over K. I.e. there are $a_0, \ldots, a_m \in K$ not all zero such that

$$a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0.$$

Therefore α is a root of the non-zero polynomial $a_0+a_1X+\cdots+a_mX^m \in \mathbb{Q}[X]$. □

4. Simple Extensions

A **simple extension** $K(\alpha)/K$ is one obtained by adjoining one element α to the field K. If α is algebraic then it is every easy to compute the degree of $K(\alpha)/K$.

THEOREM 16. *Let L/K be an extension and let $\alpha \in L$ be algebraic over K with minimal polynomial $\mu_\alpha \in K[X]$. Let $n = \deg(\mu_\alpha)$. Then*

(i) *$K(\alpha) \cong K[X]/(\mu_\alpha)$. More explicitly, the map*

$$K[X]/(\mu_\alpha) \to K(\alpha), \qquad h(X) + (\mu_\alpha) \mapsto h(\alpha)$$

is a well-defined isomorphism.

(ii) *$K(\alpha)$ has K-basis $1, \alpha, \ldots, \alpha^{n-1}$. In particular, $[K(\alpha) : K] = \deg(\mu_\alpha)$.*

PROOF. Define

$$\phi \ : \ K[X] \to K(\alpha), \qquad \phi(f) = f(\alpha).$$

It is easy to check that this is a homomorphism of rings. Let I be the kernel of ϕ. Then $I = \{f \in K[X] \ : \ f(\alpha) = 0\}$. By the proof of Lemma 2 we recall that $I = (\mu_\alpha)$. We claim that the ideal I is maximal. Let's check that. If J is another ideal containing I then $J = (f(X))$ for some $f \in K[X]$ (since $K[X]$ is a PID). Thus $\mu_\alpha \in I \subseteq J$ so $f \mid \mu_\alpha$. Therefore $f = 1$ or $f = \mu_\alpha$. In the former case we have $J = K[X]$ and in the latter $J = I$, showing that I is indeed maximal. Hence $K[X]/I$ is a field. Now the First Isomorphism Theorem tells us that there is an isomorphism

$$\hat{\phi} \ : \ K[X]/I \to \mathrm{Im}(\phi).$$

Therefore $\mathrm{Im}(\phi)$ is a subfield of $K(\alpha)$. It contains α as $\phi(X) = \alpha$ and it contains K as for an $c \in K$ we have $\phi(c) = c$. But $K(\alpha)$ is the smallest field containing K and α so $K(\alpha) = \mathrm{Im}(\phi)$. This prove (i).

Let's prove (ii). If $\beta \in K(\alpha)$ then there $\beta \in \mathrm{Im}(\phi)$ and so there is some polynomial $f \in K[X]$ such that $\beta = f(\alpha)$. By the Euclidean algorithm we have

$$f = q\mu_\alpha + r, \qquad q, r \in K[X], \qquad \deg(r) < \deg(\mu_\alpha).$$

Thus $\beta = f(\alpha) = r(\alpha)$. As $\deg(r) < \deg(\mu_\alpha) = n$ we can write $r = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$. So

$$\beta = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

showing that $1, \ldots, \alpha^{n-1}$ spans $K(\alpha)$ as a K-vector space. Next we want to show that it is linearly idependent. Suppose there are $b_0, b_1, \ldots, b_{n-1} \in K$ such that

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

Then $g(\alpha) = 0$ where $g = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$. So $g \in I = (\mu_\alpha)$. Hence $\mu_\alpha \mid g$. As $\deg(g) \leq n - 1 < \deg(\mu_\alpha)$ we see that $g = 0$. So $b_0, \ldots, b_{n-1} = 0$ proving linear independence. This completes the proof. □

Example 17. Let $d \in \mathbb{Q}$ be a non-square. Then $\sqrt{d}$ has the minimal polynomial $\mu_{\sqrt{d}}(X) = X^2 - d$ over $\mathbb{Q}$. Theorem 16 now tells us that 1, $\sqrt{d}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{d})$. Thus

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Q}\}.$$

This is a much better way of obtaining this result than Example 9.

If $d \in \mathbb{Q}$ is a non-cube (i.e. $d \neq c^3$ for any $c \in \mathbb{Q}$) then $X^3 - d$ is irreducible, and is the minimal polynomial of $\sqrt[3]{d}$. Therefore

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

In fact, if α is an algebraic number of degree n, then its minimal polynomial over $\mathbb{Q}$ has degree n and so $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$, and so

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \ : \ a_i \in \mathbb{Q}\}.$$

5. Number Fields

Definition. A **number field** is a finite extension of $\mathbb{Q}$. The degree of a number field K is the degree $[K : \mathbb{Q}]$.

Example 18. $\mathbb{Q}$ is the only number field of degree 1 (why?). Thus $\mathbb{Q}$ is the simplest example of a number field.

If $d \in \mathbb{Q}$ and d is a non-square then $\mathbb{Q}(\sqrt{d})$ is a number field of degree 2. In fact we know thanks to Example 17 that if α is an algebraic number of degree n then $\mathbb{Q}(\alpha)$ is a number field of degree n. We will see later that if $\alpha_1, \ldots, \alpha_m$ are algebraic numbers then $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ is a number field. For this we will need the tower law.

Corollary 19. *Let K be a number field. Then every element of K is an algebraic number.*

Proof. By definition $K/\mathbb{Q}$ is finite, so by Theorem 15 every element is algebraic over $\mathbb{Q}$, in other words an algebraic number. □

6. The Tower Law

THEOREM 20. *Let $K \subseteq L \subseteq M$ be field extensions of finite degree (or we could write $M/L/K$). Let $\ell_1, \ell_2, \ldots, \ell_r$ be a basis for L/K and $m_1, \ldots, m_s$ be a basis for M/L. Then*

$$\{\ell_i m_j \ : \ i = 1, \ldots, r, \ j = 1, \ldots, s\} \tag{3}$$

is a basis for M/K. Moreover,

$$[M : K] = [M : L] \cdot [L : K]. \tag{4}$$

PROOF. Observe that

$$[L : K] = r < \infty \qquad [M : L] = s < \infty.$$

Suppose for the moment that (3) is a basis for M/K as claimed in the statement of the theorem. Then $[M : K] = rs = [M : L] \cdot [L : K]$ proving (4). Thus all we need to do is prove that (3) is indeed a basis for M/K.

Let us show first that (3) is linearly independent over K. Thus suppose $a_{ij} \in K$ such that

$$\sum_{j=1}^{s} \sum_{i=1}^{r} a_{ij} \ell_i m_j = 0.$$

We can rewrite this as

$$\sum_{j=1}^{s} (\sum_{i=1}^{r} a_{ij} \ell_i) m_j.$$

Let $b_j = \sum_{i=1}^{r} a_{ij} \ell_i$ for $j = 1, \ldots, s$. Since $a_{ij} \in K \subseteq L$ and $\ell_i \in L$ we see that $b_j \in L$. But

$$\sum_{j=1}^{s} b_j m_j = 0.$$

As $m_1, \ldots, m_s$ is a basis for M/L we have

$$b_1 = b_2 = \cdots = b_s = 0.$$

But

$$b_j = \sum_{i=1}^{r} a_{ij} \ell_i = 0, \qquad j = 1, \ldots, s.$$

As $\ell_1, \ldots, \ell_r$ is a basis for L/K and $a_{ij} \in K$ we have $a_{ij} = 0$ for $j = 1, \ldots, s$ and $i = 1, \ldots, r$. This proves that (3) is linearly independent.

Now we show (3) spans M as a vector space over K. Let $m \in M$. As $m_1, \ldots, m_s$ is a basis for M/L, we can write

$$m = b_1 m_1 + \cdots + b_s m_s$$

for some $b_1, \dots, b_s \in L$. Moreover, as $\ell_1, \dots, \ell_r$ is a basis for L/K we can express each of the bs as a linear combination of the ℓs with coefficients in K:

$$b_j = a_{1j}\ell_1 + \cdots + a_{rj}\ell_r, \qquad j = 1, \dots, s;$$

here $a_{ij} \in K$. Thus

$$m = \sum_{j=1}^{s} b_j m_j = \sum_{j=1}^{s} (a_{1j}\ell_1 + \cdots + a_{rj}\ell_r) m_j = \sum_{j=1}^{s}\sum_{i=1}^{r} a_{ij}\ell_i m_j \,.$$

We've shown that any $m \in M$ can be written as linear combination of $\ell_i m_j$ with coefficients in K. This completes the proof. □

7. Number Field Examples

Definition. A **quadratic field** is a number field of degree 2. A **cubic field** is a number field of degree 3. A **quartic field** ...

Lemma 21. *Let K be a quadratic field. Then $K = \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer, and $d \neq 0, 1$.*

Proof. As $[K : \mathbb{Q}] = 2$ we have $K \neq \mathbb{Q}$ and so there is some $\theta \in K \setminus \mathbb{Q}$. Now $1, \theta, \theta^2$ are linearly dependent over $\mathbb{Q}$ and so there are u, v, $w \in \mathbb{Q}$ not all zero such that

$$u + v\theta + w\theta^2 = 0.$$

If $w = 0$ then $\theta \in \mathbb{Q}$ giving a contradiction. Thus $w \neq 0$. Thus

$$\theta = \frac{-v \pm \sqrt{\Delta}}{2w}, \qquad \Delta = v^2 - 4uv.$$

Note that Δ is not a square in $\mathbb{Q}$, since θ does not belong to $\mathbb{Q}$. Rearranging we see that $\sqrt{\Delta} \in K$. Thus $[\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}] \neq 1$ and divides $[K : \mathbb{Q}] = 2$ by the tower law. Thus $[K : \mathbb{Q}(\sqrt{\Delta})] = 1$ and so $K = \mathbb{Q}(\sqrt{\Delta})$. Now write

$$\Delta = \frac{a}{b} = \frac{1}{b^2} \cdot ab$$

where a, b are coprime integers. Let $c = ab$ which will be an integer but a non-square. Then $K = \mathbb{Q}(\sqrt{c})$. Finally write $c = de^2$ where d is squarefree and $\neq 0, 1$. Then $K = \mathbb{Q}(\sqrt{d})$. □

Example 22. $\mathbb{Q}(\sqrt{-1/3}) = \mathbb{Q}(\sqrt{-12}) = \mathbb{Q}(\sqrt{-3})$.

Example 23. Recall that the cube roots unity are 1, ζ, ζ^2 where $\zeta = \exp(2\pi i/3)$ and their sum is zero. Thus ζ is a root of $X^2 + X + 1$ which is irreducible. In particular this is the minimal polynomial for ζ. Hence $\mathbb{Q}(\zeta)$ is a quadratic field. The proof of the lemma tells us how to write $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{d})$ where d is a squarefree integer $\neq 0, 1$. Specifically we find that the discriminant of $X^2 + X + 1$ is $\Delta = -3$. This is already a squarefree integer, so $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$.

DEFINITION. Let n be a positive integer and $\zeta_n = \exp(2\pi i/n)$. We call $\mathbb{Q}(\zeta_n)$ the **n-th cyclotomic field**. Note that $\mathbb{Q}(\zeta_n)$ is an example of a number field (why?).

EXERCISE 24. Show that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. For this you will have to revise the section on Eisenstein's criterion in your Algebra II notes.

EXAMPLE 25. We saw that every quadratic field has the form $\mathbb{Q}(\sqrt{d})$ thanks to the quadratic formula. It is **not true** that every cubic field has the form $\mathbb{Q}(\sqrt[3]{d})$. For example, let θ be a root of X^3+X+1 (which is irreducible over $\mathbb{Q}$). Then $\mathbb{Q}(\theta)$ is a cubic field. Can you show that $\mathbb{Q}(\theta) \neq \mathbb{Q}(\sqrt[3]{d})$ for any d? This question is a little hard right now but we'll come back to it later.

8. Extended Example $\mathbb{Q}(\sqrt{5}, \sqrt{6})$

We shall evaluate $[\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}]$. Write $L = \mathbb{Q}(\sqrt{5})$, $M = \mathbb{Q}(\sqrt{5}, \sqrt{6}) = L(\sqrt{6})$. By the tower law,

$$[M : \mathbb{Q}] = [L : \mathbb{Q}][M : L]\,.$$

The polynomial x^2-5 is monic, irreducible over $\mathbb{Q}$ and has $\sqrt{5}$ as a root. Therefore it is the minimal polynomial for $\sqrt{5}$ over $\mathbb{Q}$. By Theorem 16, we have 1, $\sqrt{5}$ is a $\mathbb{Q}$-basis for L over $\mathbb{Q}$. In particular, $[L : \mathbb{Q}] = 2$. We want to compute $[M : L]$. As $M = L(\sqrt{6})$, we need a minimal polynomial for $\sqrt{6}$ over L. Now $\sqrt{6}$ is a root of $x^2 - 6$. We want to know if $x^2 - 6$ is irreducible over $L = \mathbb{Q}(\sqrt{5})$. Suppose it isn't. Then, as it is quadratic, its roots must be contained in L. So $\sqrt{6} = a + b\sqrt{5}$ for some a, $b \in \mathbb{Q}$. Squaring both sides, and rearranging, we get

$$(a^2 + 5b^2 - 6) + 2ab\sqrt{5} = 0.$$

As 1, $\sqrt{5}$ are linearly independent over $\mathbb{Q}$,

$$a^2 + 5b^2 - 6 = 2ab = 0.$$

Thus either $a = 0$, $b = \sqrt{\frac{6}{5}}$ or $b = 0$, $a = \sqrt{6}$, in either case contradicting a, $b \in \mathbb{Q}$. Hence $\sqrt{6} \notin L$, and $x^2 - 6$ is irreducible over L. It follows that $x^2 - 6$ is the minimal polynomial for $\sqrt{6}$ over L. Hence $[M : L] = 2$ and so by the tower law, $[M : \mathbb{Q}] = 2 \times 2 = 4$.

We can also write a $\mathbb{Q}$-basis for $M = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ over $\mathbb{Q}$. By the above 1, $\sqrt{5}$ is a basis for L over $\mathbb{Q}$. Also, as $x^2 - 6$ is the minimal polynomial for $\sqrt{6}$ over L, we have (Theorem 16) that 1, $\sqrt{6}$ is a basis for $L(\sqrt{6}) = M$ over L. The tower law (Theorem 20) tells us

$$1,\ \sqrt{5},\ \sqrt{6},\ \sqrt{30}$$

is a basis for M over $\mathbb{Q}$. Note that M is a number field: that is M is a finite extension of $\mathbb{Q}$.

We'll go a little further with the example, and in fact show that $M = \mathbb{Q}(\sqrt{5}+\sqrt{6})$ (thus M is a **simple extension** of $\mathbb{Q}$). Let $\alpha = \sqrt{5}+\sqrt{6}$. Since $\alpha \in M$ it follows that $\mathbb{Q}(\alpha) \subseteq M$. To show $M = \mathbb{Q}(\alpha)$ it is enough to show that $\mathbb{Q}(\alpha) \supseteq M$. For this it is enough to show that $\sqrt{5} \in \mathbb{Q}(\alpha)$ and $\sqrt{6} \in \mathbb{Q}(\alpha)$. Note that

$$(\alpha - \sqrt{5})^2 = 6,$$

which gives

$$\alpha^2 + 5 - 2\sqrt{5}\alpha = 6. \tag{5}$$

Rearranging

$$\sqrt{5} = \frac{\alpha^2 - 1}{2} \in \mathbb{Q}(\alpha).$$

Similarly $\sqrt{6} \in \mathbb{Q}(\alpha)$ as required. Hence $M = \mathbb{Q}(\alpha)$.

Finally, we will write down a minimal polynomial μ_α for α over $\mathbb{Q}$. Since $M/\mathbb{Q}$ has degree 4, we know from (iii) that we are looking for a monic polynomial of degree 4. Rearranging (5) we have $\alpha^2 - 1 = 2\sqrt{5}\alpha$. Squaring both sides and rearranging, we see that α is the root of

$$f = x^4 - 22x^2 + 1.$$

Do we have to check if f is irreducible? Normally we do, but not here. Observe that $\mu_\alpha \mid f$ (as $f(\alpha) = 0$) and they both have degree 4. So $\mu_\alpha = f$.

9. Another Extended Example

Definition. Let $f \in \mathbb{Q}[x]$ and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\mathbb{C}$. Then $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is called the **splitting field** of f.

In this example we will compute the degree of the splitting field of $f = x^3 - 5$ over $\mathbb{Q}$. The splitting field of f over $\mathbb{Q}$ is the field we obtain by adjoining to $\mathbb{Q}$ all the roots of f. The three roots of f are

$$\theta_1 = \sqrt[3]{5}, \qquad \theta_2 = \zeta\sqrt[3]{5}, \qquad \theta_3 = \zeta^2\sqrt[3]{5},$$

where ζ is a primitive cube root of 1. The splitting field is therefore $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$.

Let

$$K = \mathbb{Q}(\theta_1), \qquad L = K(\theta_2) = \mathbb{Q}(\theta_1, \theta_2), \qquad M = L(\theta_3) = \mathbb{Q}(\theta_1, \theta_2, \theta_3).$$

By the tower law

$$[M : \mathbb{Q}] = [K : \mathbb{Q}][L : K][M : L].$$

As $x^3 - 5$ is irreducible over $\mathbb{Q}$, we have $[K : \mathbb{Q}] = 3$. To calculate $[L : K]$ we need to know the degree of the minimal polynomial of θ_2 over K. Note that θ_2 is a root of $f = x^3 - 5$. However, f is not the minimal polynomial of θ_2 over K. Indeed, as $\sqrt[3]{5} \in K$, we have

$$f = (x - \sqrt[3]{5}) \cdot g$$

where $g \in K[x]$ is monic and quadratic. Thus θ_2 is a root of g. Is g reducible over K? As g is quadratic, if it is reducible over K it would mean that $\theta_2 \in K$. However, $\theta_2 = \zeta\sqrt[3]{5} \notin \mathbb{R}$ and $K = \mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{R}$. Therefore $\theta_2 \notin K$, and so g is irreducible over K. It follows that g is the minimal polynomial of θ_2 over K. Hence $[L : K] = 2$.

Finally, we want $[M : L]$. Now, θ_3 is also a root of g. As g is quadratic and has one root in L (specifically θ_2) its other root must be in L. Thus $\theta_3 \in L$, and so $M = L(\theta_3) = L$, and hence $[M : L] = 1$. Hence $[M : \mathbb{Q}] = 3 \times 2 \times 1 = 6$. Note that M is a number field: that is M is a finite extension of $\mathbb{Q}$.

10. Extensions of Number Fields

LEMMA 26. *Let L be a finite extension of a number field K. Then L is also a number field.*

PROOF. By the tower law $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] < \infty$. □

THEOREM 27. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers. Then $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is a number field. Coversely, any number field K can be written in the form $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where the α_i are algebraic numbers.*

PROOF. Recall that any element of a number field is an algebraic number. The converse part of the theorem is easy: if K is a number field and $\alpha_1, \ldots, \alpha_n$ is a basis then $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Suppose $\alpha_1, \ldots, \alpha_n$ are algebraic numbers and let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. We want to show that K is a number field. That is K is a finite extension of $\mathbb{Q}$. Let

$$K_0 = \mathbb{Q}, \quad K_1 = K_0(\alpha_1), \quad K_2 = K_1(\alpha_2), \ldots$$

Then $K_n = K$. By the tower law

$$[K : \mathbb{Q}] = [K_1 : K_0] \cdot [K_2 : K_1] \cdot \cdots \cdot [K_n : K_{n-1}].$$

So it is sufficient to show that $[K_{i+1} : K_i] < \infty$. But $K_{i+1} = K_i(\alpha_{i+1})$. So all we need, by Theorem 16, is to show that α_{i+1} is algebraic over K_i. But α_{i+1} is an algebraic number, so is that root of a non-zero polynomial $f \in \mathbb{Q}[X]$ and $\mathbb{Q} \subseteq K_i$ so $f \in K_i[X]$. Hence α_{i+1} is algebraic over K_i completing the proof. □

11. The field of algebraic numbers

THEOREM 28. *Let α, $\beta \in \mathbb{C}$ be algebraic numbers. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and α/β are algebraic numbers (where for the last one, we suppose $\beta \neq 0$).*

PROOF. Consider $\mathbb{Q}(\alpha, \beta)$. This is a number field by Theorem 27. Every element of a number field is an algebraic number by Corollary 19. But $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$ and α/β all belong to $\mathbb{Q}(\alpha, \beta)$, so they're algebraic numbers. □

EXAMPLE 29. You should take a moment to consider how incredible this theorem is. For example if α is a root of

$$X^{10^6} + 3X^9 + 5X^8 - 11X^4 + 72$$

and β is a root of

$$X^{99999} + 7777X - \frac{11111}{35353535}$$

then there is a monic polynomial with rational coefficients having $\alpha+\beta$ as a root. It might be an extremely hard computational problem to write down this polynomial (what would you guess its degree to be?) but the theorem tells us that it exists!

EXERCISE 30. Let α be a non-zero algebraic number with minimal polynomial

$$\mu_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in \mathbb{Q}[X].$$

Write down the minimal polynomial for $\beta = 1/\alpha$.

DEFINITION. We let

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

We call $\overline{\mathbb{Q}}$ the **field of algebraic numbers**.

THEOREM 31. *$\overline{\mathbb{Q}}$ is a field.*

PROOF. This immediate from Theorem 28. □

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

Note that $\overline{\mathbb{Q}}$ is countable, but $\mathbb{C}$ is uncountable. This is tells us that that there are lots of complex numbers that aren't algebraic. Such numbers are called **transcendental**. Examples of transcendental numbers are e and π, though this is not easy to prove.

12. Norms and Traces

Let K be a number field and $\alpha \in K$. We define

$$m_{K,\alpha} \ : \ K \to K, \qquad m_{K,\alpha}(\theta) = \alpha \cdot \theta.$$

We usually write m_α if the field K is understood. This m_α is not usually a homomorphism of fields (why?). But think of K as a $\mathbb{Q}$-vector space. Then m_α is a linear transformation. If $\alpha \neq 0$ then it is in fact injective and surjective, and therefore an isomorphism of K with itself as a $\mathbb{Q}$-vector. We define the **trace** of α as

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

and we define the **norm** of α as

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Det}(m_\alpha) \in \mathbb{Q}.$$

The following lemma tells us how to compute traces and norms in a quadratic field.

LEMMA 32. *Let d be a squarefree integer $\neq 0, 1$. Let $K = \mathbb{Q}(\sqrt{d})$. Let $a, b \in \mathbb{Q}$. Then*

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

PROOF. Let $\alpha = a + b\sqrt{d}$. We want to work out the trace and the determinant of the linear transformation m_α. Recall that the trace and determinant of a linear transformation are the trace and determinant of its matrix with respect to any basis. We choose the basis 1, $\sqrt{d}$ for K. Then

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

Thus the matrix of m_α with respect to this basis is

$$M_\alpha = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}. \tag{6}$$

It follows that $\mathrm{Trace}_{K/\mathbb{Q}}(\alpha) = \mathrm{Trace}(M_\alpha) = 2a$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Det}(M_\alpha) = a^2 - bd^2$ as required. □

PROPOSITION 33. *Let $\alpha, \beta \in K$. Then*

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

In other words, trace is additive and norm is multiplicative.

PROOF. Observe that $m_{\alpha+\beta} = m_\alpha + m_\beta$ and $m_{\alpha\beta} = m_\alpha m_\beta$. The proposition follows from the properties of traces and determinants of linear transformations. □

EXERCISE 34. Let $f = X^3 + 2X + 2$. Show that f is irreducible. Let θ be a root of f and let $K = \mathbb{Q}(\theta)$. Compute $\mathrm{Trace}_{K/\mathbb{Q}}(\theta^2)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\theta^2)$.

EXERCISE 35. Let $d \neq 0, 1$ be a cube-free integer. Compute the trace and norm of $a + b\sqrt[3]{d} + c\sqrt[3]{d}^2$ with $a, b, c \in \mathbb{Q}$.

13. Characteristic Polynomials

DEFINITION. Let K be a number field and $\alpha \in K$. We write $\chi_{K,\alpha} \in \mathbb{Q}[X]$ for the characteristic polynomial of $m_{K,\alpha}$. We call this the **characteristic polynomial** of α.

EXAMPLE 36. Recall that the characteristic polynomial of a linear transformation is the characteristic polynomial of its matrix with respect to any basis. Let's use this to work out the characteristic polynomial of $\alpha = a + b\sqrt{d}$ in $\mathbb{Q}(\sqrt{d})$ (where $a, b \in \mathbb{Q}$ as usual). We computed above the matrix M_α for m_α with respect to the basis 1, $\sqrt{d}$; this is given in (6). Thus the characteristic polynomial is

$$\chi_{K,\alpha} = \begin{vmatrix} X - a & -bd \\ -b & X - a \end{vmatrix} = (X - a)^2 - db^2 = X^2 - 2aX + (a^2 - db^2).$$

Note that $\chi_{K,\alpha}(\alpha) = 0$. Is this a coincidence? No, it turns out to be always true. Moreover it has the form $X^2 - \mathrm{Trace}(\alpha)X + \mathrm{Norm}(\alpha)$. Is this a coincidence?

THEOREM 37. *Let K be a number field and $\alpha \in K$.*

(i) $\deg(\chi_{K,\alpha}) = [K : \mathbb{Q}]$.

(ii) *Write*

$$\chi_{K,\alpha} = X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

Then

$$\mathrm{Trace}(\alpha) = -a_{n-1}, \qquad \mathrm{Norm}(\alpha) = (-1)^n a_0.$$

(iii) $\chi_{K,\alpha}(\alpha) = 0$.

PROOF. Let $n = [K : \mathbb{Q}]$. Recall that $\chi_{K,\alpha}$ is the characteristic polynomial of m_α and thus the characteristic polynomial of an $n \times n$ matrix. This gives (i).

For part (ii) we want $\mathrm{Trace}(m_\alpha) = -a_{n-1}$ and $\mathrm{Det}(m_\alpha) = (-1)^n a_0$. These are standard linear algebra facts, but let's go through them. By definition $\chi_{K,\alpha}(X) = \mathrm{Det}(XI_n - M_\alpha)$ where M_α is the matrix for m_α with respect to any basis. Now taking $X = 0$ we obtain $a_0 = \mathrm{Det}(-M_\alpha) = (-1)^n \mathrm{Det}(M_\alpha) = (-1)^n \mathrm{Norm}(\alpha)$. Moreover if $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of m_α, then

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = \chi_{K,\alpha}(X) = \prod_{i=1}^{n}(X - \lambda_i).$$

Comparing the coefficients of X^{n-1} we get

$$a_{n-1} = -\lambda_1 - \cdots - \lambda_n = -\mathrm{Trace}(m_\alpha) = -\mathrm{Trace}(\alpha).$$

For the final part we apply the Cayley–Hamilton Theorem. This tells us that $\chi_{K,\alpha}(m_\alpha) = 0$. Thus

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

Apply both sides to $1 \in K$ and recall that $m_\alpha(1) = \alpha \cdot 1 = \alpha$. So

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

This gives part (iii) of the theorem. □

LEMMA 38. *Let $K = \mathbb{Q}(\alpha)$ be a number field. Then $\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha}$.*

PROOF. This is easy. Both polynomials are monic of the same degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Moreover, as $\chi_{K,\alpha}(\alpha) = 0$ we know that $\mu_{\mathbb{Q},\alpha} \mid \chi_{K,\alpha}$. Therefore they must be equal. □

EXAMPLE 39. The lemma gives us an easy way of computing norms and traces of α when $K = \mathbb{Q}(\alpha)$. For example let α be a root of $X^3 - 2X - 2$, which you can check is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$. Then $\chi_{K,\alpha} = \mu_{\mathbb{Q},\alpha} = X^3 - 2X - 2$. From the coefficients,

$$\mathrm{Trace}_{K/\mathbb{Q}}(\alpha) = 0, \qquad \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = (-1)^3 \times -2 = 2.$$

LEMMA 40. *Let $K \subset L$ be number fields. Let $\alpha \in K$. Then*

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

In particular, if $K = \mathbb{Q}(\alpha)$ then

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

EXAMPLE 41. Before launching in the proof of Lemma 40 let try an example. Take $\alpha = a + b\sqrt{5}$ (with a, $b \in \mathbb{Q}$) inside $L = \mathbb{Q}(\sqrt{5}, \sqrt{6})$. Recall that a basis for $L/\mathbb{Q}$ is $1, \sqrt{5}, \sqrt{6}, \sqrt{5}\sqrt{6}$. Then

$$\begin{aligned}
\alpha \cdot 1 &= a \cdot 1 \ + b \cdot \sqrt{5} + 0 \cdot \sqrt{6} \ + 0 \cdot \sqrt{5}\sqrt{6} \\
\alpha \cdot \sqrt{5} &= 5b \cdot 1 + a \cdot \sqrt{5} + 0 \cdot \sqrt{6} \ + 0 \cdot \sqrt{5}\sqrt{6} \\
\alpha \cdot \sqrt{6} &= 0 \cdot 1 \ + 0 \cdot \sqrt{5} + a \cdot \sqrt{6} \ + b \cdot \sqrt{5}\sqrt{6} \\
\alpha \cdot \sqrt{5}\sqrt{6} &= 0 \cdot 1 \ + 0 \cdot \sqrt{5} + 5b \cdot \sqrt{6} + a \cdot \sqrt{5}\sqrt{6}
\end{aligned}$$

Thus the matrix for α with respect to this basis is

$$M' = \left(\begin{array}{cc|cc} a & 5b & 0 & 0 \\ b & a & 0 & 0 \\ \hline 0 & 0 & a & 5b \\ 0 & 0 & b & a \end{array}\right)$$

This has the form

$$M' = \begin{pmatrix} M & \mathbf{0} \\ \mathbf{0} & M \end{pmatrix}$$

where M is the matrix for $m_\alpha : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$ with respect to the basis 1, $\sqrt{5}$. Thus

$$\chi_{L,\alpha} = \mathrm{Det}(XI_4 - M') = \mathrm{Det}(I_2 - M)^2 = \chi_{K,\alpha}^2 = ((X-a)^2 - 5b^2)^2$$

where $K = \mathbb{Q}(\sqrt{5})$.

PROOF OF LEMMA 40. Let $\theta_1, \ldots, \theta_n$ be a basis for $K/\mathbb{Q}$ and let M_α be the matrix for $m_\alpha : K \to K$ with respect to this basis. Let $\phi_1, \phi_2, \ldots, \phi_m$ be a basis for L/K. By the tower law, a basis for $L/\mathbb{Q}$ is

$$\theta_1\phi_1, \theta_2\phi_1, \ldots, \theta_n\phi_1, \quad \theta_1\phi_2, \theta_2\phi_2, \ldots, \theta_n\phi_2, \ldots$$

The matrix for α with respect to this basis is

$$\begin{pmatrix} M_\alpha & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M_\alpha & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & & \ddots & & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & M_\alpha \end{pmatrix}$$

Thus

$$\chi_{L,\alpha}(X) = \det(XI_n - M_\alpha)^m = \chi_{K,\alpha}(X)^{[K:\mathbb{Q}]}.$$

□

EXAMPLE 42. Let $f = X^3 + X + 1$. Check that this is irreducible (easy!). Let θ be a root of f and let $K = \mathbb{Q}(\theta)$ so that $[K : \mathbb{Q}] = 3$ and $1, \theta, \theta^2$ is a basis for $K/\mathbb{Q}$. Let $\alpha = 1 + \theta + \theta^2$. We will determine the minimal polynomial for α over $\mathbb{Q}$. Note that

$$m_\alpha(1) = 1 + \theta + \theta^2$$
$$m_\alpha(\theta) = \theta + \theta^2 + \theta^3 = -1 + \theta^2$$
$$m_\alpha(\theta^2) = -\theta + \theta^3 = -1 - 2\theta.$$

Thus the matrix for m_α with respect to this basis is

$$M_\alpha = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 0 & -2 \\ 1 & 1 & 0 \end{pmatrix}.$$

Thus

$$\chi_\alpha(X) = \mathrm{Det}(XI_3 - M_\alpha) = X^3 - X^2 + 4X - 3.$$

By Lemma 40 this equals μ_α or μ_α^3 depeding on whether $[K : \mathbb{Q}(\alpha)]$ has degree 1 or 3. But we can see that χ_α is not a cube; for example the constant coefficient is not a cube. Therefore $\mu_\alpha = \chi_\alpha = X^3 - X^2 + 4X - 3$.

There are other ways of concluding the argument. For example if $\chi_\alpha = \mu_\alpha^3$ then μ_α must be linear and so $\alpha \in \mathbb{Q}$. In this case θ is a root of $X^2 + X + 1 - \alpha \in \mathbb{Q}[X]$ which contradicts the fact that the minimal polynomial of θ is cubic.

EXAMPLE 43. Theorem 37 tells us that we can read the trace and the norm from the characteristic polynomial. Here is an example.

Let p be an odd prime and let $\zeta = \exp(2\pi i/p)$. Let

$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \frac{X^p - 1}{X - 1}.$$

You know from Algebra II that Φ is irreducible (since $\Phi(X + 1)$ is Eisenstein). The roots of $\Phi(X)$ are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, so it is the minimal polynomial of all of them (note that these are conjugates). Let $K = \mathbb{Q}(\zeta)$ (this is the p-th cyclotomic field), which is the splitting field for $\Phi(X)$. Then $[K : \mathbb{Q}] = p - 1$. As the degree of the field is equal to the degree of the minimal polynomial of $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ we see that it is also the characteristic polynomial for all of them, and we may read off (from the coefficient of X^{p-2}):

$$\mathrm{Trace}_{K/\mathbb{Q}}(\zeta^i) = -1, \qquad i = 1, 2, \ldots, p - 1.$$

From the constant coefficient we get

$$\mathrm{Norm}_{K/\mathbb{Q}}(\zeta^i) = (-1)^{p-1} \cdot 1 = 1, \qquad i = 1, 2, \ldots, p - 1.$$

Let's compute $\mathrm{Norm}_{K/\mathbb{Q}}(\zeta^i - \zeta^j)$. If $i \equiv j \pmod{p}$ then $\zeta^i = \zeta^j$ and the desired norm is 0. Thus suppose $i \not\equiv j \pmod{p}$ and let $k = i - j$.

Then

$$\mathrm{Norm}_{K/\mathbb{Q}}(\zeta^i - \zeta^j) = \mathrm{Norm}(\zeta^j)\,\mathrm{Norm}(\zeta^k - 1) = \mathrm{Norm}(\zeta^k - 1).$$

Now ζ^k is one of the roots of $\Phi(X)$. Thus $\zeta^k - 1$ is one of the roots of

$$\Phi(X+1) = (X+1)^{p-1} + (X+1)^{p-2} + \cdots + 1 = X^p + \cdots + p.$$

We don't really care about the other coefficients, just that the polynomial is monic and that the constant coefficient is p. As this is irreducible and of degree $p-1$ it is the characteristic polynomial of $\zeta^k - 1$. From the constant coefficient we have

$$\mathrm{Norm}_{K/\mathbb{Q}}(\zeta^i - \zeta^j) = \mathrm{Norm}(\zeta^k - 1) = (-1)^{p-1}p = p.$$

Exercise 44. Let $K \subset L$ be number fields. Let $\alpha \in K$. Show that

$$\mathrm{Trace}_{L/\mathbb{Q}}(\alpha) = [L:K]\cdot\mathrm{Trace}_{K/\mathbb{Q}}(\alpha), \qquad \mathrm{Norm}_{L/\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)^{[L:K]}.$$

Hint: See the proof of Lemma 40.

CHAPTER 3

Embeddings of a Number Field

1. Homomorphisms of Fields

LEMMA 45. *Any homomorphism of fields $\sigma : K \to L$ must be injective.*

PROOF. Indeed, the kernel of σ is an ideal of K and as K is a field its ideals are 0 and K. But the kernel cannot be K since $\sigma(1) = 1$. So $\ker(\sigma) = 0$ and hence σ is injective. □

If $\sigma : K \to L$ is a homomorphism of fields then we write $\sigma : K \hookrightarrow L$. The hooked arrow is intended to allow us to think of K as homomorphically embedded inside L.

If $\sigma : K \hookrightarrow L$ is a homomorphism of fields and $f = a_n X^n + \cdots + a_0 \in K[X]$ then we write $\sigma(f) = \sigma(a_n)X^n + \cdots + \sigma(a_0) \in L[X]$. In other words we apply σ to the coefficients of f.

EXERCISE 46. With σ as above check that $\sigma : K[X] \to L[X]$ is an injective ring homomorphism. If $\sigma : K \hookrightarrow L$ is an isomorphism then $\sigma : K[X] \to L[X]$ is an isomorphism.

LEMMA 47. *Let $\sigma : K \to L$ be an isomorphism of number fields. Let $\alpha \in \mathbb{C}$ be a root of $f \in K[X]$ where f is irreducible over K. Let $\beta \in \mathbb{C}$ be a root of $\sigma(f)$. Then there is a unique isomorphism*

$$\tau : K(\alpha) \to L(\beta)$$

such that $\tau|_K = \sigma$ and $\tau(\alpha) = \beta$.

PROOF. Let's show uniqueness first. Recall that every element of $K(\alpha)$ can be written as a linear combination $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ where $a_i \in K$, and $n = \deg(f)$. Thus

$$\begin{aligned}\tau(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) &= \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_{n-1})\tau(\alpha)^{n-1} \\ &= \sigma(a_0) + \sigma(a_1)\tau(\alpha) + \cdots + \sigma(a_{n-1})\tau(\alpha)^{n-1}.\end{aligned}$$

Thus τ is determined by σ and $\tau(\alpha)$ and so if it exists must be unique.

Let's show the existence of τ. Write $I = (f)$. By Theorem 16 we have an isomorphism

$$\phi : K[X]/I \to K(\alpha), \qquad \phi(h + I) = h(\alpha).$$

Now σ induces an isomorphism $K[X] \to L[X]$ which we also denote by σ. As $f \in K[X]$ is irreducible so is $g = \sigma(f) \in L[X]$. Write $J = (g)$ for the principal ideal of $L[X]$ generated by g. We obtain an isomorphism

$$\hat{\sigma} : K[X]/I \to L[X]/J$$

which sends $h + I$ to $\sigma(h) + J$. Again by Theorem 16 we have an isomorphism

$$\psi : L[X]/J \to L(\beta), \qquad \psi(h + J) = h(\beta).$$

We take τ to be the composition of isomorphisms

$$K(\alpha) \xrightarrow{\phi^{-1}} K[X]/I \xrightarrow{\hat{\sigma}} L[X]/J \xrightarrow{\psi} L(\beta).$$

You can check by writing out the maps explicitly that $\tau|_K = \sigma$ and $\tau(\alpha) = \beta$. □

EXAMPLE 48. Let $\iota : \mathbb{Q} \to \mathbb{Q}$ be the identity. Let $d \neq 0, 1$ be a squarefree integer and let $f = X^2 - d$. Then $\iota(f) = f$. Let $\alpha = \sqrt{d}$ and $\beta = -\sqrt{d}$. Note that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{d})$. By Lemma 47, there is a unique homomorphism $\tau : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ satisfying $\tau|_{\mathbb{Q}} = \iota$ and $\tau(\alpha) = \beta$. Thus $\tau(a + b\sqrt{d}) = a - b\sqrt{d}$ with $a, b \in \mathbb{Q}$.

EXERCISE 49. Let $d \in \mathbb{Q}$ be a non-cube and let $\zeta = \exp(2\pi i/3)$. Show that the map

$$\tau : \mathbb{Q}(\sqrt[3]{d}) \to \mathbb{Q}(\zeta\sqrt[3]{d})$$

given by

$$\tau(a + b\sqrt[3]{d} + c\sqrt[3]{d}^2) = a + b\zeta\sqrt[3]{d} + c\zeta^2\sqrt[3]{d}^2$$

is an isomorphism of fields.

2. Embeddings into $\mathbb{C}$

DEFINITION. Let K be a number field. An **embedding** of K is a homomorphism $\sigma : K \hookrightarrow \mathbb{C}$.

Recall that any number field K contains $\mathbb{Q}$ as a subfield.

LEMMA 50. *Let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. Then $\sigma(a) = a$ for all $a \in \mathbb{Q}$.*

PROOF. Since $\sigma(0) = 0$ and $\sigma(1) = 1$ we have

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

for any natural number n. Moreover $\sigma(-n) = -\sigma(n) = -n$, so $\sigma(m) = m$ for all integers m. Finally $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$. □

EXAMPLE 51. Recall that $\mathbb{Q}$ is the most basic example of a number field. By the above lemma it has precisely one embedding which is $\sigma : \mathbb{Q} \hookrightarrow \mathbb{C}$, $\sigma(a) = a$.

We will see later that the number of distinct embeddings of a number field K is equal to its degree, but at least we can see that this is true for $\mathbb{Q}$.

EXAMPLE 52. Let d be a squarefree integer $\neq 0, 1$ and let $K = \mathbb{Q}(\sqrt{d})$ (which we now know as a quadratic field). Every element of K can be uniquely written as $a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. If $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding then

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

So σ is really determined once we know what $\sqrt{d}$ is. But $\sqrt{d}^2 = d \in \mathbb{Q}$ so $\sigma(\sqrt{d})^2 = \sigma(d) = d$. Hence $\sigma(\sqrt{d}) = \pm\sqrt{d}$. Thus we get two possible embeddings: $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{C}$ defined by

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}, \qquad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d} \qquad a, b \in \mathbb{Q}.$$

We say possible embeddings because we should really check that these are homomorphisms, which isn't hard.

LEMMA 53 (The separability lemma). *Let K be a number field and $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding of K. Let $f \in K[X]$ an irreducible polynomial of degree d. Then $\sigma(f)$ has d distinct roots in $\mathbb{C}$.*

PROOF. Let f' be the derivative of f which also belongs to $K[X]$. As f is irreducible and f' has smaller degree than f we see that $\gcd(f, f') = 1$. As $K[X]$ is Euclidean, there are polynomials h_1 and $h_2 \in K[X]$ such that

$$h_1(X)f(X) + h_2(X)f'(X) = 1. \tag{7}$$

Write $g = \sigma(f)$ and note that $g' = \sigma(f')$. Let $k_1 = \sigma(h_1)$ and $k_2 = \sigma(h_2)$. Applying σ to both sides of (7) gives

$$k_1(X)g(X) + k_2(X)g'(X) = 1. \tag{8}$$

If $\alpha \in \mathbb{C}$ is a root of $\sigma(f) = g$ of multiplicity at least 2 then

$$g(X) = (X - \alpha)^2 m(X), \qquad m(X) \in \mathbb{C}[X].$$

But then

$$g'(X) = (X - \alpha)^2 m'(X) + 2(X - \alpha)m(X)$$

so $g'(\alpha) = 0$. Substituting α in both sides of (8) gives $0 = 1$ which is a contradiction. □

3. The Primitive Element Theorem

THEOREM 54 (The Primitive Element Theorem). *Let L/K be an extension of number fields. Then $L = K(\gamma)$ for some $\gamma \in L$.*

Note that the theorem says that every extension of number fields is simple. We call γ a primitive element. To prove the primitive element theorem we first need the following lemma.

LEMMA 55. *Let $L = K(\alpha, \beta)$ be an extension of number fields. Then there is some $\gamma \in L$ such that $L = K(\gamma)$.*

PROOF. Let f, g be the minimal polynomials of α and β over $\mathbb{Q}$. We know that these have distinct roots in $\mathbb{C}$ by the Separability Theorem. Let $\alpha_1, \ldots, \alpha_m$ be the roots of f and let $\beta_1, \ldots, \beta_n$ be the roots of g. We may suppose $\alpha = \alpha_1$ and $\beta = \beta_1$. Note that the equation

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

has exactly one solution c if $j \neq 1$. As K is infinite, we may choose $c \in K$ such that

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

for all $j \neq 1$ and all i. We let $\gamma = \alpha + c\beta$. We will show that $L = K(\gamma)$ as required. For this it is enough to show that $\beta \in K(\gamma)$ as $\alpha = \gamma - c\beta$ and $c \in K$.

Let $M = K(\gamma)$ and consider $\mu_{M,\beta}$, the minimal polynomial of β over M. The polynomial $h = f(\gamma - cX)$ has coefficients in M and β is a root. Thus $\mu_{M,\beta} \mid h$. Moreover $\mu_{M,\beta} \mid g$ (as $g(\beta) = 0$). Let β' be a root of $\mu_{M,\beta}$ in $\mathbb{C}$. Then $\beta' = \beta_j$. Thus $h(\beta_j) = 0$ so $g(\gamma - c\beta_j) = 0$ so $\gamma - c\beta_j = \alpha_i$. Thus $\alpha_i + c\beta_j = \gamma = \alpha + c\beta$. By our choice of c we have $\beta' = \beta_j = \beta$. Therefore the only complex root of $\mu_{M,\beta}$ is β. Moreover, by the separability lemma it does not have multiple roots. Thus $\mu_{M,\beta} = X - \beta$. But $\mu_{M,\beta} \in M[X]$ so $\beta \in M = K(\gamma)$ as required. □

PROOF OF THE PRIMITIVE ELEMENT THEOREM. This is now an easy exercise using Lemma 55. □

EXERCISE 56. Let d_1, d_2 be distinct squarefree integers $\neq 0, 1$. Show that $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1} + \sqrt{d_2})$, by following the steps of the proof of Lemma 55.

4. Extending Embeddings

Let L/K be an extension of number fields and $\sigma : K \hookrightarrow \mathbb{C}$, $\tau : L \hookrightarrow \mathbb{C}$ be embeddings. We say that τ **extends** σ if $\tau|_K = \sigma$.

THEOREM 57. *Let K be a number field and $M = K(\alpha)$ where α is algebraic over K. Let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. 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 $\mathbb{C}$.*

(i) *Then there are precisely $n = [M : K]$ embeddings of $\tau_i : M \hookrightarrow \mathbb{C}$ $(i = 1, \ldots, n)$ extending σ.*
(ii) *These are specified by letting $\tau_i(\alpha) = \alpha_i$.*

PROOF. Let $L = \sigma(K)$. Then we can think of σ as an isomorphism $\sigma : K \to L$. Let μ_α be the minimal polynomial of α and $\alpha_1, \ldots, \alpha_n$ be the roots of $\sigma(\mu_\alpha)$. Here $n = \deg(\mu_\alpha) = [M : K]$ and the roots are distinct by the separability lemma. Lemma 47 now gives isomorphisms $\tau_i : M \to L(\alpha_i)$ such that $\tau_i|_K = \sigma$ and $\tau_i(\alpha) = \alpha_i$. Moreover as

$L(\alpha_i) \subset \mathbb{C}$ we can think of τ_i as an embedding $\tau_i : M \to \mathbb{C}$. These embeddings are distinct as the α_i are distinct.

To complete the proof we must show that there no more embeddings. Let

$$\mu_\alpha(X) = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_i \in K.$$

Let $\tau : M \hookrightarrow \mathbb{C}$ be an extension of σ. Now $\mu_\alpha(\alpha) = 0$ so

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

Apply τ to both sides, and recall that $\tau(a_i) = \sigma(a_i)$ since $a_i \in K$:

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

Thus $\tau(\alpha)$ is one of the roots of $\sigma(\mu_\alpha)$. In otherwords $\tau(\alpha)$ and these are $\alpha_1, \ldots, \alpha_n$. This completes the proof. □

EXAMPLE 58. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Compute the embeddings $K \hookrightarrow \mathbb{C}$.

Answer. Write $\theta = \sqrt[3]{2}$. Recall that

$$K = \{a + b\theta + c\theta^2 \ : \ a, b, c \in \mathbb{Q}\}.$$

If $\tau \ : \ K \hookrightarrow \mathbb{C}$ is an embedding then it extends the trivial embedding $\iota : \mathbb{Q} \hookrightarrow \mathbb{C}$ (here trivial means $\iota(a) = a$ for all $a \in \mathbb{Q}$). The minimal polynomial of θ is $X^3 - 2$. The complex roots of $\iota(X^3 - 2) = X^3 - 2$ are θ, $\zeta\theta$, $\zeta^2\theta$ where $\zeta = \exp(2\pi i/3)$. Thus the embeddings $\tau_i : K \hookrightarrow \mathbb{C}$ satisfy $\tau_1(\theta) = \theta$, $\tau_2(\theta) = \zeta\theta$ and $\tau_3(\theta) = \zeta^2\theta$. Thus

$$\tau_1(a + b\theta + c\theta^2) = a + b\theta + c\theta^2$$
$$\tau_2(a + b\theta + c\theta^2) = a + b\zeta\theta + c\zeta^2\theta^2$$
$$\tau_3(a + b\theta + c\theta^2) = a + b\zeta^2\theta + c\zeta\theta^2.$$

EXERCISE 59. Let $\sigma : \mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{C}$ be given by $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$. Explicitly write down the embeddings $\tau : \mathbb{Q}(\sqrt{5}, \sqrt{6}) \hookrightarrow \mathbb{C}$ that extend σ.

THEOREM 60. *A number field K has $[K : \mathbb{Q}]$ embeddings.*

PROOF. This follows from Theorem 57 and the Primitive Element Theorem. □

5. Real and Complex Embeddings; Signature

It is easy to check that if $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding then $\overline{\sigma}$ defined by

$$\overline{\sigma} : K \hookrightarrow \mathbb{C}, \qquad \overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$$

is also an embedding. Note that $\overline{\sigma} = \sigma$ if and only if $\sigma(K) \subset \mathbb{R}$ in which case we say σ is a **real embedding**. Otherwise if $\sigma(K) \not\subset \mathbb{R}$ we say that σ is a **complex** embedding; in this case $\overline{\sigma} \neq \sigma$. We usually talk of **pairs of complex embeddings**, since the complex embeddings come in conjugate pairs.

THEOREM 61. *Let K be a number field. Let $\sigma_1, \ldots, \sigma_r$ be its real embeddings. Let $\sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$ be its complex embeddings. Then $[K : \mathbb{Q}] = r + 2s$.*

PROOF. This follows from Theorem 60. □

We refer to the pair of non-negative integers (r, s) as the **signature** of K.

EXERCISE 62. Let $K = \mathbb{Q}(\alpha)$ be a number field and let μ_α be the minimal polynomial of α. Let (r, s) be the signature of K. Show that

(i) r is the number of real roots of μ_α.
(ii) s is the number of pairs of complex conjugate (non-real) roots of μ_α.
(iii) What is the signature of $\mathbb{Q}(\sqrt{d})$?
(iv) What is the signature of $\mathbb{Q}(\sqrt[3]{d})$?

EXAMPLE 63. Let $K = \mathbb{Q}(\sqrt{1+\sqrt{2}})$. We will determine the degree and signature of K. Write

$$\alpha = \sqrt{1+\sqrt{2}}.$$

Then

$$\alpha^2 - 1 = \sqrt{2}$$

so

$$(\alpha^2 - 1)^2 - 2 = 0.$$

Thus α is a root of

$$f = (X^2 - 1)^2 - 2 = X^4 - 2X^2 - 1.$$

You can check that is irreducible directly and so $[K : \mathbb{Q}] = 4$. We'll adopt a slightly less 'brute force' approach. We know that $[K : \mathbb{Q}] \leq 4$ since α is a root of f. We also know that $\mathbb{Q}(\sqrt{2}) \subseteq K$. Thus by the tower law $2 \mid [K : \mathbb{Q}]$ and so $[K : \mathbb{Q}] = 2$ or 4. If $[K : \mathbb{Q}] = 2$ then $[K : \mathbb{Q}(\sqrt{2})] = 1$ and so $K = \mathbb{Q}(\sqrt{2})$. In particular $\alpha \in \mathbb{Q}(\sqrt{2})$. Now $\alpha^2 = 1 + \sqrt{2}$. Taking norms we have

$$\mathrm{Norm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha)^2 = \mathrm{Norm}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1+\sqrt{2}) = -1$$

giving a contradiction. Thus $[K : \mathbb{Q}] = 4$ and so f is irreducible. In particular, it is the minimal polynomial of α. Let β be any root of f. Then

$$(\beta^2 - 1)^2 = 2$$

and so the four complex roots of f are

$$\alpha_1 = \sqrt{1+\sqrt{2}}, \quad \alpha_2 = -\sqrt{1+\sqrt{2}}, \quad \alpha_3 = \sqrt{1-\sqrt{2}}, \quad \alpha_4 = -\sqrt{1-\sqrt{2}}.$$

The four embeddings $\tau_i : K \hookrightarrow \mathbb{C}$ satisfy $\tau_i(\alpha) = \alpha_i$. As α_1, α_2 are real, we have that τ_1, τ_2 are real embeddings. Moreover α_3, α_4 are

non-real but complex conjugates, so τ_3, τ_4 are a single pair of complex embeddings. In particular, the signature of K is $(2, 1)$.

6. Conjugates

DEFINITION. Let $\alpha \in \overline{\mathbb{Q}}$. The **conjugates** of α are the roots of its minimal polynomial $\mu_{\mathbb{Q},\alpha}$ (i.e. the minimal polynomial of α over $\mathbb{Q}$) in $\mathbb{C}$.

By Theorem 57, the conjugates of α are $\sigma_i(\alpha)$ where the σ_i are the embeddings of $\mathbb{Q}(\alpha)$.

THEOREM 64. *Let K be a number field of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings $K \hookrightarrow \mathbb{C}$. Let $\alpha \in K$. Then the characteristic polynomial χ_α has the form*

$$\chi_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha)). \tag{9}$$

Moreover,

$$\mathrm{Trace}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

PROOF. By the Primitive Element Theorem we know that $K = \mathbb{Q}(\beta)$ for some $\beta \in K$. In this case we know that $\chi_\beta = \mu_{\mathbb{Q},\beta}$ by Lemma 38. Now by Theorem 57 the roots of $\mu_{\mathbb{Q},\beta}$ are $\sigma_1(\beta), \ldots, \sigma_n(\beta)$ (and these are distinct by the separability Lemma). Hence

$$\chi_\beta(X) = \mu_{\mathbb{Q},\beta}(X) = \prod_{i=1}^{n}(X - \sigma_i(\beta)).$$

By definition, $\chi_\beta(X)$ is the characteristic polynomial of m_β. Let M_β be the matrix for m_β with respect to the basis $1, \ldots, \beta^{n-1}$. As the roots of the characteristic polynomial (i.e. the eigenvalues) are distinct, M_β is diagonalizable. Thus there is a $n \times n$ invertible matrix T so that

$$T^{-1}M_\beta T = D, \qquad D = \mathrm{diag}(\sigma_1(\beta), \ldots, \sigma_n(\beta))$$

Here the notation means that D is the diagonal matrix with $\sigma_i(\beta)$ down the diagonal.

Now $\alpha \in K$ so we can write $\alpha = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$. It follows that

$$M_\alpha = c_0 I_n + c_1 M_\beta + \cdots + c_{n-1} M_\beta^{n-1}.$$

Observe that $D^j = (T^{-1}M_\beta T)^j = T^{-1}M_\beta^j T$. Thus

$$T^{-1}M_\alpha T = c_0 I_n + c_1 D + \cdots + c_{n-1} D^{n-1}.$$

This is diagonal matrix with the i-th diagonal entry being

$$c_0 + c_1\sigma_i(\beta) + c_2\sigma_i(\beta)^2 + \cdots + c_{n-1}\sigma_i(\beta)^{n-1} = \sigma_i(c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}) = \sigma_i(\alpha).$$

Thus χ_α, which is the characteristic polynomial of M_α is $\prod(X - \sigma_i(\alpha))$.

Finally we want to compute $\mathrm{Trace}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$. These are defined respectively as the trace and determinant of m_α, or equivalently the trace and determinant of any matrix for m_α. We found above the matrix M_α is diagonalizable with $\sigma_i(\alpha)$ down the diagonal. This proves the formulae for the trace and norm. □

EXAMPLE 65. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Let's compute the trace and norm of $\alpha = 1 + \sqrt[3]{2}$. One way of doing this is writing down a matrix for m_α. But we can also do this using the embeddings. We know that K has three embeddings that satisfy

$$\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}, \qquad \sigma_2(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \qquad \sigma_3(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2},$$

where $\zeta = \exp(2\pi i/3)$. Then

$$\begin{aligned}\mathrm{Trace}_{K/\mathbb{Q}}(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha)\\ &= (1 + \sqrt[3]{2}) + (1 + \zeta\sqrt[3]{2}) + (1 + \zeta^2\sqrt[3]{2})\\ &= 3\end{aligned}$$

since $1 + \zeta + \zeta^2 = 0$. Moreover, the norm is

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = (1 + \sqrt[3]{2})(1 + \zeta\sqrt[3]{2})(1 + \zeta^2\sqrt[3]{2}).$$

After expanding the brackets and simplifying we find that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = 3$.

EXAMPLE 66. Let $K = \mathbb{Q}(\sqrt{d})$ where as usual $d \neq 0, 1$ is squarefree. Let $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. We know the two embeddings of K satisfy

$$\sigma_1(\alpha) = a + b\sqrt{d}, \qquad \sigma_2(\alpha) = a - b\sqrt{d};$$

These are the conjugates of α. So the characteristic polynomial of α is

$$\chi_\alpha(X) = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d})) = X^2 - 2aX + (a^2 - b^2 d)$$

which clearly belongs to $\mathbb{Q}[X]$. If $b = 0$ then $\alpha = a \in \mathbb{Q}$ and $\chi_\alpha(X) = X^2 - 2aX + a^2 = (X - a)^2$ is the square of the minimal polynomial. If $b \neq 0$ then $\alpha \notin \mathbb{Q}$ and so χ_α is equal to the minimal polynomial.

7. Discriminants

Let K be a number field of degree n and let $\omega_1, \ldots, \omega_n$ be elements of K. We let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the embeddings of K into $\mathbb{C}$. Consider the matrix

$$\begin{vmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \cdots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \cdots & \sigma_n(\omega_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \cdots & \sigma_n(\omega_n) \end{vmatrix}. \tag{10}$$

Which we denote by the short-hand $(\sigma_j(\omega_i))$. We let $D(\omega_1, \ldots, \omega_n)$ be the determinant of this matrix, and we call this the **determinant of** $\omega_1, \ldots, \omega_n$. Note that the order of $\sigma_1, \ldots, \sigma_n$ is not uniquely determined

by K. If we permute the embeddings then we simply permute the columns of the matrix and so change $D(\omega_1, \ldots, \omega_n)$ by multiplying by ± 1 depending on the sign of the permutation. So it is perhaps better to square D. We let

$$\Delta(\omega_1, \ldots, \omega_n) = D(\omega_1, \ldots, \omega_n)^2$$

and we call this the **discriminant of** $\{\omega_1, \ldots, \omega_n\}$. We shall normally consider only discriminants of bases. The discriminant measures the 'size' of a basis is in a precise sense that we will see eventually.

EXAMPLE 67. Let d be a squarefree integer. Then 1, $\sqrt{d}$ is a basis for $\mathbb{Q}(\sqrt{d})$. Then

$$D(1, \sqrt{d}) = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix} = -2\sqrt{d},$$

and so

$$\Delta(1, \sqrt{d}) = 4d.$$

If instead we take the basis 1, $(1 + \sqrt{d})/2$ then

$$D\left(1,\ (1+\sqrt{d})/2\right) = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{vmatrix} = -\sqrt{d},$$

and so

$$\Delta\left(1,\ (1+\sqrt{d})/2\right) = d.$$

EXAMPLE 68. Let d be cubefree and $K = \mathbb{Q}(\sqrt[3]{d})$. The minimal polynomial of $\theta = \sqrt[3]{d}$ is $X^3 - d$ which has roots θ, $\zeta\theta$ and $\zeta^2\theta$ where $\zeta = \exp(2\pi i/3)$. Thus the embeddings of $\sigma_i : K \hookrightarrow \mathbb{C}$ satisfy

$$\sigma_1(\theta) = \theta, \qquad \sigma_2(\theta) = \zeta\theta, \qquad \sigma_3(\theta) = \zeta^2\theta.$$

It follows that the determinant of 1, θ, θ^2 is

$$\begin{aligned} D(1, \theta, \theta^2) &= \begin{vmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) \\ \sigma_1(\theta) & \sigma_2(\theta) & \sigma_3(\theta) \\ \sigma_1(\theta^2) & \sigma_2(\theta^2) & \sigma_3(\theta^2) \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & 1 \\ \theta & \zeta\theta & \zeta^2\theta \\ \theta^2 & \zeta^2\theta^2 & \zeta\theta^2 \end{vmatrix} \\ &= \theta \cdot \theta^2 \cdot \begin{vmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{vmatrix} \\ &= 3d \cdot (\zeta^2 - \zeta) = -3\sqrt{-3} \cdot d \end{aligned}$$

where we have used $\zeta = (-1 + \sqrt{-3})/2$, $\zeta^2 = (-1 - \sqrt{-3})/2$. Thus

$$\Delta(1, \sqrt[3]{d}, \sqrt[3]{d}^2) = -27d^2.$$

EXERCISE 69. **For the brave only. We'll see easier ways of doing this calculation.** Let p be an odd prime and $\zeta = \exp(2\pi i/3)$. Let $K = \mathbb{Q}(\zeta)$ and recall that $[K : \mathbb{Q}] = p - 1$. Compute $\Delta(1, \zeta, \ldots, \zeta^{p-2})$.

8. The Discriminant and Traces

THEOREM 70. *Let K be a number field of degree n and let $\omega_1, \ldots, \omega_n \in K$. Then*

$$\Delta(\omega_1, \ldots, \omega_n) = \mathrm{Det}(\mathrm{Trace}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j)).$$

In particular, $\Delta(\omega_1, \ldots, \omega_n) \in \mathbb{Q}$.

PROOF. Write T for the $n \times n$ matrix with (i, j)-th entry $\sigma_j(\omega_i)$. Then $D(\omega_1, \ldots, \omega_n) = \mathrm{Det}(T)$ and so

$$\Delta(\omega_1, \ldots, \omega_n) = \mathrm{Det}(T)^2 = \mathrm{Det}(T \cdot T^t)$$

where $T^t = (\sigma_i(\omega_j))$ is the transpose of T. Then (i, j)-th entry of $T \cdot T^t$ is

$$\sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i \cdot \omega_j) = \mathrm{Trace}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j)$$

as required. Here we have used Theorem 64.

For the last part recall that $\mathrm{Trace}_{K/\mathbb{Q}}$ maps elements of K to $\mathbb{Q}$. □

EXAMPLE 71. **Part I.** In Example 68 we computed $\Delta(1, \sqrt[3]{d}, \sqrt[3]{d}^2)$ directly from the definition. We can now do this again, and more easily, using Theorem 70. You'll find

$$\Delta(1, \sqrt[3]{d}, \sqrt[3]{d}^2) = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 3d \\ 0 & 3d & 0 \end{vmatrix} = -27d.$$

Part II. Let $f = X^3 + X^2 - 2X + 8$.

(i) Show that f is irreducible over $\mathbb{Q}$.

(ii) Let θ be a root of f and $K = \mathbb{Q}(\theta)$. Compute the discriminant

$$\Delta(1, \theta, \theta^2).$$

Answer:

(i). Suppose f is reducible in $\mathbb{Q}[X]$. As $f \in \mathbb{Z}[X]$ is monic we know by Gauss' Lemma, $f = GH$ where G, $H \in \mathbb{Z}[X]$ are monic of degree $< \deg(f) = 3$. So one of the two factors must have degree one. Thus without loss of generality $G = X - \alpha$ with $\alpha \in \mathbb{Z}$. Clearly $\alpha \mid 8$. Thus α must be one of ± 1, ± 2, ± 4, ± 8. We check these and find that none are roots. Thus f is irreducible.

(ii). We need to compute

$$\Delta(1, \theta, \theta^2) = \begin{vmatrix} \mathrm{Trace}(1) & \mathrm{Trace}(\theta) & \mathrm{Trace}(\theta^2) \\ \mathrm{Trace}(\theta) & \mathrm{Trace}(\theta^2) & \mathrm{Trace}(\theta^3) \\ \mathrm{Trace}(\theta^2) & \mathrm{Trace}(\theta^3) & \mathrm{Trace}(\theta^4). \end{vmatrix} \tag{11}$$

We know Trace(1) = 3 and from the minimal polynomial for f for θ (which is the same as the characteristic polynomial in this case)

$$\text{Trace}(\theta) = -1.$$

Note that

$$\theta^3 = -\theta^2 + 2\theta - 8, \qquad \theta^4 = -\theta^3 + 2\theta^2 - 8\theta.$$

As the traces are additive, we know how to compute Trace(θ^3) and Trace(θ^4) as soon as we've worked out Trace(θ^2).

It's most straightforward to write down the matrix M_θ for m_θ with respect to the basis $1, \theta, \theta^2$. This is

$$M_\theta = \begin{pmatrix} 0 & 0 & -8 \\ 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix}.$$

Thus

$$M_{\theta^2} = M_\theta^2 = \begin{pmatrix} 0 & -8 & -8 \\ 0 & 2 & -10 \\ 1 & -1 & 3 \end{pmatrix}.$$

Thus Trace(θ^2) = Trace(M_{θ^2}) = 5. Hence

$$\text{Trace}(\theta^3) = -5 - 2 - 24 = -31, \qquad \text{Trace}(\theta^4) = 31 + 10 + 8 = 49.$$

Substituting into (11) we get

$$\Delta(1, \theta, \theta^3) = -2012 = 2^2 \times 503.$$

EXERCISE 72. Suppose $f = X^3 + bX + c \in \mathbb{Q}[X]$ is irreducible and let θ be a root. Let $K = \mathbb{Q}(\theta)$. Show that

$$\Delta(1, \theta, \theta^2) = -4b^3 - 27c^2.$$

9. Discriminants and Bases

LEMMA 73. *If $\omega_1, \ldots, \omega_n$ are $\mathbb{Q}$-linearly dependent then*

$$D(\omega_1, \ldots, \omega_n) = \Delta(\omega_1, \ldots, \omega_n) = 0.$$

PROOF. Suppose $a_1\omega_1 + \cdots + a_n\omega_n = 0$ where $a_i \in \mathbb{Q}$ are not all 0. As the σ_j are $\mathbb{Q}$-linear, we have

$$0 = \sigma_j(a_1\omega_1 + \cdots + a_n\omega_n) = a_1\sigma_j(\omega_1) + \cdots + a_n\sigma_j(\omega_n).$$

If $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are the rows of (10) then $a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$. As the rows are linearly dependent the determinant is 0. □

In fact the converse if true, and so $\omega_1, \ldots, \omega_n$ is a basis for $K/\mathbb{Q}$ if and only if $\Delta(\omega_1, \ldots, \omega_n) \neq 0$. We prove this shortly.

LEMMA 74. *Let $c_{i,j} \in \mathbb{Q}$ and let*

$$\beta_i = \sum_{j=1}^{n} c_{i,j}\omega_j.$$

Then

$$D(\beta_1, \ldots, \beta_n) = \det(c_{i,j}) D(\omega_1, \ldots, \omega_n),$$

and

$$\Delta(\beta_1, \ldots, \beta_n) = \det(c_{i,j})^2 \cdot \Delta(\omega_1, \ldots, \omega_n).$$

PROOF. Recall that the embeddings σ_k are $\mathbb{Q}$-linear maps. Thus

$$\sigma_k(\beta_i) = \sum_{j=1}^{n} c_{i,j}\sigma_k(\omega_j).$$

Hence the matrix $(\sigma_k(\beta_i))$ is obtained by multiplying the matrix $(\sigma_k(\omega_j))$ by the matrix $(c_{i,j})$. The lemma follows by taking determinants. □

THEOREM 75. *Let K is a number field of degree n. Then*

(i) *Write $K = \mathbb{Q}(\alpha)$. The discriminant of the basis $1, \alpha, \ldots, \alpha^{n-1}$ is given by*

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

where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α.

(ii) *Let $\beta_1, \ldots, \beta_n \in K$. Then $\beta_1, \ldots, \beta_n$ is a $\mathbb{Q}$-basis if and only if $\Delta(\beta_1, \ldots, \beta_n) \neq 0$.*

PROOF. Recall that the conjugates of α are given by $\sigma_j(\alpha) = \alpha_j$. These are distinct as they are the roots of the minimal polynomial of α. Now $\sigma_j(\alpha^i) = \alpha_j^i$ and so

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha^n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \vdots & \alpha_n^{n-1} \end{vmatrix}.$$

This is a Vandermonde determinant and we know that

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j).$$

Squaring gives (i). Observe as the α_i are distinct (by the Separability Theorem), we have $\Delta(1, \alpha, \ldots, \alpha^{n-1}) \neq 0$.

Now let $\beta_1, \ldots, \beta_n \in K$. If $\beta_1, \ldots, \beta_n$ is not a basis then the discriminant is zero by Lemma 73. Suppose $\beta_1, \ldots, \beta_n$ is a basis. By the

Primitive Element Theorem we can write $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. As $1, \ldots, \alpha^{n-1}$ is also a basis (for $K/\mathbb{Q}$) there are $c_{i,j}$ such that

$$\beta_i = \sum_{j=1}^{n} c_{i,j}\alpha^{j-1},$$

where $\det(c_{i,j}) \neq 0$. By Lemma 74 we have

$$\Delta(\beta_1, \ldots, \beta_n) = \mathrm{Det}(c_{i,j})^2 \cdot \Delta(1, \ldots, \alpha^{n-1}).$$

Part (ii) follows from (i). □

Exercise 76. Let's do Exercise 69 but somewhat more easily. For this you need to revise Example 43. Recall that p is an odd prime and $\zeta = \exp(2\pi i/p)$. The conjugates of ζ are

$$\zeta_1 = \zeta, \quad \zeta_2 = \zeta^2, \quad \zeta_3 = \zeta^3, \ldots, \quad \zeta_{p-1} = \zeta^{p-1}.$$

(i) Show that

$$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = \prod_{1 \leq i < j \leq p-1} (\zeta_i - \zeta_j)^2 = (-1)^{(p-1)/2} \cdot \prod_{\substack{1 \leq i,j \leq p-1, \\ i \neq j}} (\zeta_i - \zeta_j).$$

(ii) Recall that the ζ_i all share the same minimal polynomial

$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \prod_{i=1}^{p-1}(X - \zeta_i).$$

With the help of the product rule show that

$$\Phi'(\zeta_i) = \prod_{\substack{1 \leq j \leq p-1, \\ j \neq i}} (\zeta_i - \zeta_j).$$

and thus

$$\prod_{i \neq j}(\zeta_i - \zeta_j) = \prod_{i=1}^{p-1} \Phi'(\zeta_i) = \mathrm{Norm}_{K/\mathbb{Q}}(\Phi'(\zeta))$$

(iii) By differentiating the identity

$$(X - 1)\Phi(X) = X^p - 1$$

show that $\Phi'(\zeta) = p\zeta^{p-1}/(\zeta - 1)$.

(iv) Deduce that

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

CHAPTER 4

Algebraic Integers

1. Definitions

Recall that $\overline{\mathbb{Q}}$ is the set of algebraic numbers. We call $\alpha \in \overline{\mathbb{Q}}$ an **algebraic integer** if is the root of a monic polynomial $f \in \mathbb{Z}[X]$. We write $\mathcal{O}$ for the set of algebraic integers.

If you're doing Commutative Algebra you'll recognize $\mathcal{O}$ as the integral closure of $\mathbb{Z}$ inside $\overline{\mathbb{Q}}$.

EXAMPLE 77. i is a root of the polynomial X^2+1 which is in $\mathbb{Z}[X]$ so i is an algebraic integer. A more subtle example is $(1+\sqrt{5})/2$ which is known as the golden ratio. This does not at first look integral, but it has minimal polynomial $X^2 - X - 1 \in \mathbb{Z}[X]$ and so is an algebraic integer.

What about $1/\sqrt{2}$? This has minimal polynomial $X^2 - 1/2 \notin \mathbb{Z}[X]$. However the definition does not immediately allow us to conclude that $1/\sqrt{2}$ is not an algebraic number, because we need to show that $f(1/\sqrt{2}) \neq 0$ for all monic $f \in \mathbb{Z}[X]$.

To answer the question in the above example we need some Algebra II revision.

LEMMA 78 (Gauss' Lemma). *Let $f \in \mathbb{Z}[X]$ be a monic polynomial. Let g, $h \in \mathbb{Q}[X]$ satisfy $f = gh$. Then there is a non-zero rational number λ such that $G = \lambda g$ and $H = \lambda^{-1}h$ are monic polynomials belonging to $\mathbb{Z}[X]$ and $f = GH$.*

PROOF. Write $f = gh$ where $h \in \mathbb{Q}[X]$. There are non-zero rationals λ, ε such that $G = \lambda g \in \mathbb{Z}[X]$, $H = \varepsilon h \in \mathbb{Z}[X]$. Then $(\lambda\varepsilon)f = GH \in \mathbb{Z}[X]$. Comparing the leading coefficients we see that $\lambda\varepsilon = n \in \mathbb{Z}$. By changing the sign of λ we may suppose $n \geq 1$. Choose λ, ε so that n is as small as possible. We claim that $n = 1$. Suppose otherwise and let $p \mid n$ be a prime. Now reduce the relation

$$nf(X) = G(X)H(X)$$

modulo p letting $\overline{G} \in \mathbb{F}_p[X]$, $\overline{H} \in \mathbb{F}_p[X]$ be the polynomials we obtain from reducing the coefficients of G, H modulo p. As $f(X) \in \mathbb{Z}[X]$ and $p \mid n$ we have

$$\overline{G}(X) \cdot \overline{H}(X) = 0.$$

But $\mathbb{F}_p[X]$ is an integral domain, so without loss of generality $\overline{G}(X) = 0$. Hence p divides all the coefficients of $G(X)$. In otherwords $(\lambda/p)g(X) \in$

$\mathbb{Z}[X]$. This contradicts the minimality of $n = \lambda\varepsilon$, proving our claim that $n = 1$. The theorem now follows as $\varepsilon = n/\lambda = \lambda^{-1}$. □

A consequence of the above is the following theorem which we also call Gauss' Lemma.

THEOREM 79 (Gauss' Lemma). *Let α be an algebraic number. Then α is an algebraic integer if and only if $\mu_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$.*

PROOF. The "if" part follows from the definition of algebraic integer. Let's prove the "only if" part. Suppose α is a root of a monic polynomial $f \in \mathbb{Z}[X]$. Now $\mu_{\mathbb{Q},\alpha} \mid f$ in $\mathbb{Q}[X]$. By Gauss's lemma there is a non-zero rational λ such that $\lambda \cdot \mu_{\mathbb{Q},\alpha}$ is monic and has coefficients in $\mathbb{Z}$. But $\mu_{\mathbb{Q},\alpha}$ is already monic. Hence $\lambda = 1$ completing the proof. □

EXAMPLE 80. We can now answer the question of whether $1/\sqrt{2}$ is an algebraic integer. This has minimal polynomial $X^2 - 1/2 \notin \mathbb{Z}[X]$ so $1/\sqrt{2}$ is an algebraic number but not an algebraic integer.

COROLLARY 81. *α is an algebraic integer if and only if all its conjugates are algebraic integers.*

PROOF. By definition, conjugates share the same minimal polynomial. □

COROLLARY 82. *Let K be a number field and let $\alpha \in K$. Then α is an algebraic integer if and only if one of the following is true*

(i) *α is a root of a monic polynomial $f \in \mathbb{Z}[X]$;*
(ii) *$\mu_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$;*
(iii) *the characterisitc polynomial of α belongs to $\mathbb{Z}[X]$.*

PROOF. (i) is the definition of algebraic integer. We know already that (i), (ii) are equivalent. Note that (iii) implies (i) since the characteristic polynomial is monic and α is a root of it. Moreover (ii) implies (iii) as the characteristic polynomial is a power of the minimal polynomial. □

DEFINITION. If K is a number field the we write

$$\mathcal{O}_K = K \cap \mathcal{O}.$$

We call $\mathcal{O}_K$ the **ring of integers** of K. Of course calling it that does not automatically make it into a ring; we still need to prove that it is a ring.

THEOREM 83. *$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

It is for this reason that we call $\mathbb{Z}$ the set of **rational integers**.

PROOF. If $\alpha \in \mathbb{Q}$ then the minimal polynomial of α is $X - \alpha$. This belongs to $\mathbb{Z}[X]$ if and only if $\alpha \in \mathbb{Z}$. Thus $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$ as required. □

We immediately see that $\mathbb{Z} \subseteq \mathcal{O}_K$ for any number field K.

It is natural to ask if every algebraic number is the ratio of two algebraic integers. In fact, more is true. Every algebraic number α can be write as β/m where β is an algebraic integer and m is a *rational integer*.

PROPOSITION 84. *Let K be a number field and let $\alpha \in K$. Then there is a rational integer $m \geq 1$ such that $m\alpha \in \mathcal{O}_K$.*

PROOF. Let

$$\mu_\alpha(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1} + X^n \in \mathbb{Q}[X].$$

Let m be the least common multiple of the denominators of the c_i. Note that

$$m^n \mu_\alpha(X/m) = m^n c_0 + m^{n-1}c_1 + \cdots + m c_{n-1}X^{n-1} + X^n$$

is both monic and coefficients in $\mathbb{Z}$. Moreover, $\beta = m\alpha$ is a root of this. Thus $\beta \in \mathcal{O}$. But also $\beta \in K$ as m, $\alpha \in K$ so $\beta \in \mathcal{O}_K$. □

2. Ring of Integers

We will prove in this section that $\mathcal{O}$ and $\mathcal{O}_K$ are rings. To make sure you understand this section start out by doing the following exercise.

EXERCISE 85. Consider the ring $R = \mathbb{Z}[1/2] = \{f(1/2) : f \in \mathbb{Z}[X]\}$. This is an additive abelian group (by just forgetting the multiplicative structure of R and concentrating on the additive structure). Show that R is *not* finitely generated as an additive abelian group. You might find the fundamental theorem of abelian groups helpful.

LEMMA 86. *Let f, $g \in \mathbb{Z}[X]$ and suppose that g is monic. Then there are unique q, r such that*

$$f = qg + r, \qquad q, r \in \mathbb{Z}[X], \qquad \deg(r) < \deg(g). \tag{12}$$

PROOF. You might be thinking "Of course I know this! It's Euclid!". However Euclid gives you q, $r \in \mathbb{Q}[X]$. The claim here is that the unique q, r that Euclid gives you actually belong to $\mathbb{Z}[X]$ provided f, $g \in \mathbb{Z}[X]$ and g is monic.

Fix monic $g \in \mathbb{Z}[X]$. We prove the existence of q, $r \in \mathbb{Z}[X]$ satisfying (12) by induction on the degree of f. If $\deg(f) < \deg(g)$ then $q = 0$ and $r = f$ so the claim is true. Now write $\deg(g) = n$ and suppose $\deg(f) \geq \deg(g)$ so we can write $\deg(f) = n + m$ where $m \geq 0$. Then f and g start with (recall g is monic)

$$f = a_{n+m}X^{n+m} + \cdots, \qquad g = X^n + \cdots,$$

where all the coefficients are in $\mathbb{Z}$. Let $f_1 = f - a_{n+m}X^m \cdot g$. Then $f_1 \in \mathbb{Z}[X]$ and $\deg(f_1) < \deg(f)$. By the inductive hypothesis

$$f_1 = q_1 g + r_1, \qquad q_1, r_1 \in \mathbb{Z}[X], \qquad \deg(r_1) < \deg(g).$$

Let $q = q_1 + a_{n+m}X^m$ and $r = r_1$. Then $q,\ r \in \mathbb{Z}[X]$ and satisfy (12). □

LEMMA 87. *Let α be an algebraic integer of degree d. Then for all $j \geq 0$ the power α^j can be written as $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{d-1}$.*

PROOF. Let $f = X^j$ and let $g = \mu_{\mathbb{Q},\alpha}(X)$. These belong to $\mathbb{Z}[X]$ and g is monic. Thus

$$X^j = q \cdot \mu_{\mathbb{Q},\alpha} + r, \qquad q, r \in \mathbb{Z}[X], \qquad \deg(r) < d$$

Thus $r = a_0 + a_1X + \cdots + a_{d-1}X^{d-1}$ with $a_i \in \mathbb{Z}$. Hence

$$\alpha^j = q(\alpha) \cdot \mu(\alpha) + r(\alpha) = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}.$$

□

If α is an algebraic number, we write

$$\mathbb{Z}[\alpha] = \{f(\alpha) \ : \ f \in \mathbb{Z}[X]\}.$$

If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers, we write

$$\mathbb{Z}[\alpha_1, \ldots, \alpha_n] = f(\alpha_1, \ldots, \alpha_n) \ : \ f \in \mathbb{Z}[X_1, \ldots, X_n]\}.$$

It is easy to see that this is a subring of $\mathbb{C}$.

LEMMA 88. *If $\alpha_1, \ldots, \alpha_n$ are algebraic integers then $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is finitely generated as an additive abelian group.*

PROOF. Every element of $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ can be written as an $\mathbb{Z}$-linear combination of expressions of the form $\alpha_1^{j_1} \cdots \alpha_n^{j_n}$. Let d_i be the degree of α_i. By Lemma 87 we know that $\alpha_i^{j_i}$ can be written as a $\mathbb{Z}$-linear combination of $1, \alpha_i, \ldots, \alpha_i^{d_i-1}$. Thus every element of $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ can be written as a $\mathbb{Z}$-linear combination of $\alpha_1^{j_1} \cdots \alpha_n^{j_n}$ with $j_i \leq d_i - 1$. This shows that $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is finitely generated as an additive abelian group. □

LEMMA 89 (Integral Stability Lemma). *Let H be a non-trivial finitely generated additive subgroup of $\mathbb{C}$. Let $\theta \in \mathbb{C}$ and suppose that $\theta H \subseteq H$. Then θ is an algebraic integer.*

PROOF. As H is finitely generated as an abelian group, there are $\omega_1, \ldots, \omega_n \in H$ that span H; i.e.

$$H = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n.$$

Now $\theta\omega_i \in \theta H \subseteq H$. Thus we may write

$$\theta\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j$$

where $a_{i,j} \in \mathbb{Z}$. Let A be the matrix $(a_{i,j})$. Let $\mathbf{w}$ be the column vector with entries $\omega_1, \ldots, \omega_n$. Then $A\mathbf{w} = \theta\mathbf{w}$. In otherwords θ is an eigenvalue of A and hence a root of $\chi_A(X) = \det(XI - A)$. However,

$\chi_A(X)$ is a monic polynomial with integer coefficients, and thus θ is an algebraic integer. □

THEOREM 90. *$\mathcal{O}$ is a ring.*

PROOF. We want to show that $\mathcal{O}$ is a subring of $\mathbb{C}$ (or a subring of $\overline{\mathbb{Q}}$). We know $0, 1 \in \mathcal{O}$. Thus it is enough to show that $\mathcal{O}$ is closed under addition, negation and multiplication. Let $\alpha, \beta \in \mathcal{O}$; i.e. α and β are algebraic integers. By Lemma 88 we know that the ring $\mathbb{Z}[\alpha, \beta]$ is finitely generated as an additive abelian group. Let γ be any of $\alpha + \beta$, $-\alpha$ and $\alpha - \beta$. As $\mathbb{Z}[\alpha, \beta]$ is a ring we have $\gamma\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{Z}[\alpha, \beta]$. Applying the Integral Stability Lemma shows that $\gamma \in \mathcal{O}$. □

We can now justify calling $\mathcal{O}_K$ the *ring* of integers of K.

COROLLARY 91. *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

PROOF. By definition $\mathcal{O}_K = \mathcal{O} \cap K$ so as the intersection of two subrings of $\mathbb{C}$ it is a subring. □

EXERCISE 92. Let K be a number field and $\alpha \in K$.

(i) Show that if $\alpha \in \mathcal{O}_K$ then $\mathrm{Trace}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ are in $\mathbb{Z}$.
(ii) If K is quadratic prove the converse of (i).
(iii) Give a counterexample to show that (i) does not hold for cubic polynomials.

EXAMPLE 93. Let's work out $\mathcal{O}_K$ for $K = \mathbb{Q}(i)$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha = a + bi$ where $a, b \in \mathbb{Q}$. Let $u, v \in \mathbb{Z}$ be the integer parts of a, b so that

$$a = u + \varepsilon, \qquad b = v + \eta, \qquad 0 \leq \varepsilon < 1, \qquad 0 \leq \eta < 1.$$

Then $\alpha = (u + vi) + (\varepsilon + \eta i)$. But as $\mathcal{O}_K$ is a ring containing $\mathbb{Z}$ and i we have $u + vi \in \mathcal{O}_K$. Hence $\varepsilon + \eta i \in \mathcal{O}_K$. Now $\mathrm{Trace}_{K/\mathbb{Q}}(\varepsilon + \eta i) = 2\varepsilon$. Thus $2\varepsilon \in \mathbb{Z}$. Hence $\varepsilon = 0$ or $1/2$. Also as $i \in \mathcal{O}_K$ we have $i(\varepsilon + \eta i) = -\eta + i\varepsilon \in \mathcal{O}_K$, so by taking traces we have $2\eta \in \mathbb{Z}$ and so $\eta = 0$ or $1/2$. Now we write down the characteristic polynomials for the four possibilities

$$\varepsilon + \eta i = 0, \quad 1/2, \quad i/2, \qquad (1 + i)/2.$$

We find that only 0 is an algebraic integer. Thus $\alpha = u + vi$ with $u, v \in \mathbb{Z}$. Hence

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

EXERCISE 94. Use the strategy of the above example to compute $\mathcal{O}_K$ for

(i) $K = \mathbb{Q}(\sqrt{5})$.
(ii) $K = \mathbb{Q}(\sqrt[3]{10})$.

(i) should be easy, but the answer might surprise you. (ii) is quite hard so don't waste too much time on it. It will be easier once we know more about rings of integers and their integral bases.

3. Integral Basis

We saw that if K is a number field then $\mathcal{O}_K$ is a ring. If we forget about the multiplicative structure of $\mathcal{O}_K$ and simply look at the additive structure then we will see that $\mathcal{O}_K$ is an additive abelian group. Let's write $\mathcal{O}_K^+$ for $\mathcal{O}_K$ viewed purely as an additive abelian group.

EXAMPLE 95. From Example 93 we see that every element of $\mathbb{Z}[i]^+$ can be written uniquely as $a \cdot 1 + b \cdot i$. Thus

$$\mathbb{Z}[i]^+ = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot i \cong \mathbb{Z}^2.$$

Note that the isomorphism $\mathbb{Z}[i]^+ \cong \mathbb{Z}^2$ is an isomorphism of abelian groups and not of rings. We call 1, i an integral basis for $\mathbb{Z}[i]$; that is a basis for $\mathcal{O}_K^+$ as an abelian group.

DEFINITION. An **integral basis** for a number field K is a set of elements $\xi_1, \ldots, \xi_n \in \mathcal{O}_K$ which are a $\mathbb{Z}$-basis for $\mathcal{O}_K$; that is every element of $\mathcal{O}_K$ can be written uniquely in the form $m_1\xi_1 + \cdots + m_n\xi_n$ with $m_i \in \mathbb{Z}$. In other words,

$$\mathcal{O}_K^+ = \mathbb{Z} \cdot \xi_1 \oplus \mathbb{Z} \cdot \xi_2 \oplus \cdots \oplus \mathbb{Z} \cdot \xi_n.$$

Just because we defined what an integral basis is, doesn't mean that it necessarily exists. We still have to do that. But for quadratic fields that isn't hard. We can even compute an integral basis which we do in the next section.

We need to do some Algebra I revision.

THEOREM 96 (The Fundamental Theorem of Finitely Generated Abelian Groups). *Let G be a finitely generated additive abelian group. Then there is an integer $r \geq 0$ (called the **rank**) and positive integers $d_1 \mid d_2 \mid d_3 \cdots \mid d_k$ such that*

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \mathbb{Z}/d_k\mathbb{Z}.$$

For now we will be interested only in **torsion-free** abelian group. An element $a \in G$ is torsion if it has finite order. We say G is **torsion-free** if the only element of finite order is 0.

EXAMPLE 97. $\mathbb{C}$ is an additive abelian group if we forget about the multiplicative structure. Let G be a subgroup of $\mathbb{C}$. If $a \in G$ has finite order, then $na = 0$ for some $n \geq 1$, and so $a = 0$ (as we are inside $\mathbb{C}$). Thus G is torsion-free.

Note that torsion-free means that G does not have any $\mathbb{Z}/d\mathbb{Z}$ inside it. As a corollary to the fundamental theorem we have.

COROLLARY 98. *Let G be a finitely generated torsion-free additive abelian group. Then there is an integer r called the rank such that $G \cong \mathbb{Z}^r$.*

LEMMA 99. *Let K be a number field. If $\mathcal{O}_K^+$ is finitely generated then it has an integral basis.*

PROOF. We know that $\mathcal{O}_K^+$ is torion-free (as it is a subgroup of $\mathbb{C}$). Suppose that it is finitely generated. Then $\mathcal{O}_K^+ \cong \mathbb{Z}^n$ for some n. Let $\phi : \mathcal{O}_K^+ \to \mathbb{Z}^n$ be an isomorphism, and let $\phi^{-1}(\mathbf{e}_i) = \omega_i$ where $\mathbf{e_1}, \ldots, \mathbf{e}_n$ are the standard basis vectors. Then

$$\mathcal{O}_K^+ = \mathbb{Z} \cdot \omega_1 \oplus \cdots \oplus \mathbb{Z} \cdot \omega_n.$$

□

LEMMA 100. *Let K be a number field of degree n. Let H be a finitely generated subgroup of $\mathcal{O}_K^+$ of rank m. Then $m \leq n$.*

PROOF. Let $\omega_1, \ldots, \omega_m$ be a $\mathbb{Z}$-basis for H and suppose $m > n$. Now K has dimension n as a $\mathbb{Q}$-vector space so $\omega_1, \ldots, \omega_m$ are linearly dependent over $\mathbb{Q}$. So there are $a_i \in \mathbb{Q}$, not all zero, such that

$$a_1\omega_1 + \cdots + a_n\omega_n = 0.$$

Multiplying by the lcm of the denominators of the a_i we may suppose $a_i \in \mathbb{Z}$ and not all 0. This contradicts the assumption that $\omega_1, \ldots, \omega_m$ is a $\mathbb{Z}$-basis for H. □

EXAMPLE 101. Let $K = \mathbb{Q}(i)$. Then $\mathcal{O}_K^+$ has rank 2. It has many subgroups of rank 1; for example $\mathbb{Z}$ or $\mathbb{Z} \cdot i$ or $\mathbb{Z} \cdot (1 + i)$. It also has many subgroups that are of rank 2 but are smaller than $\mathcal{O}_K^+$; for example

$$\mathbb{Z} \cdot 2 \oplus \mathbb{Z} \cdot i = \{2a + bi \ : \ a, b \in \mathbb{Z}\}.$$

Note that this subgroup has rank 2 and has index 2 in $\mathcal{O}_K^+$.

4. Integers of Quadratic Fields

LEMMA 102. *Let d be a squarefree integer. Let μ a non-zero rational number such that $\mu^2 d \in \mathbb{Z}$. Then $\mu \in \mathbb{Z}$.*

PROOF. Write $\mu = a/b$ where a, b are coprime integers and $b \geq 1$. Then $a^2 d/b^2 \in \mathbb{Z}$. As a, b are coprime, $b^2 \mid d$ and so $b = 1$ by the squarefreeness of d. □

LEMMA 103. *Let $d \neq 0, 1$ be a squarefree integer. The $(1 + \sqrt{d})/2$ is an algebraic integer if and only if $d \equiv 1 \pmod 4$.*

PROOF. The minimal polynomial for $(1 + \sqrt{d})/2$ is

$$(X - 1/2)^2 - d/4 = X^2 - X + \frac{1 - d}{4}.$$

This belongs to $\mathbb{Z}[X]$ if and only if $d \equiv 1 \pmod 4$. □

LEMMA 104. *Let d be squarefree, $\neq 0, 1$. Let $K = \mathbb{Q}(\sqrt{d})$.*

(i) *If $d \not\equiv 1 \pmod 4$ then $1, \sqrt{d}$ is an integral basis for $\mathcal{O}_K$. Therefore $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.*

(ii) *If $d \equiv 1 \pmod 4$ then $1, (1+\sqrt{d})/2$ is an integral basis for $\mathcal{O}_K$. Therefore $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$.*

PROOF. Note that $1, \sqrt{d} \in \mathcal{O}_K$. Thus $u + v\sqrt{d} \in \mathcal{O}_K$ for all $u, v \in \mathbb{Z}$. We need to discover if $\mathcal{O}_K$ contains algebraic integers not of this form.

Suppose $\alpha \in \mathcal{O}_K$. Then $\alpha \in K = \mathbb{Q}(\alpha)$ and so $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. The characteristic polynomial of α (which is a power of the minimal polynomial) is $X^2 - 2aX + (a^2 - bd^2)$. Thus $2a \in \mathbb{Z}$ and $a^2 - bd^2 \in \mathbb{Z}$. Moreover $(2b)^2 d = (2a)^2 - 4(a^2 - bd^2) \in \mathbb{Z}$. By Lemma 102 we have $2b \in \mathbb{Z}$. Thus

$$\alpha = (u + v\sqrt{d}) + \eta$$

where $u, v \in \mathbb{Z}$ and η is one of $0, 1/2, \sqrt{d}/2, (1+\sqrt{d})/2$. But clearly $u + v\sqrt{d} \in \mathcal{O}_K$ so $\eta \in \mathcal{O}_K$. Now $1/2$ and $\sqrt{d}/2 \notin \mathcal{O}_K$. If $d \not\equiv 1 \pmod 4$ the $(1+\sqrt{d})/2 \notin \mathcal{O}_K$ and so $\eta = 0$, and so $\alpha = u + v\sqrt{d}$ with $u, v \in \mathbb{Z}$. This gives (i).

Suppose $d \equiv 1 \pmod 4$. Then $(1+\sqrt{d})/2$ is an integer. Thus $\eta = 0$ or $(1+\sqrt{d})/2$. In the former case

$$\alpha = u + v\sqrt{d} = (u - v) + 2v\frac{(1+\sqrt{d})}{2}$$

and in the latter case

$$\alpha = u + v\sqrt{d} + \frac{(1+\sqrt{d})}{2} = (u - v) + (2v+1)\frac{(1+\sqrt{d})}{2}.$$

This completes the proof. □

Remark. If $d \not\equiv 1 \pmod 4$ then we know from the above that

$$\mathcal{O}_K = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Z}\}.$$

If $d \equiv 1 \pmod 4$, then the following is a very useful way of writing the integers:

$$\mathcal{O}_K = \{a + b\sqrt{d} \ : \ a, b \in \mathbb{Z}\} \cup \left\{\frac{r}{2} + \frac{s}{2} \cdot \sqrt{d} \ : \ r, s \in 2\mathbb{Z} + 1\right\}.$$

5. Bases and Discriminants

LEMMA 105. *Let K be a number field of degree n. Let H be a finitely generated subgroup of $\mathcal{O}_K^+$ of rank n. Suppose $\omega_1, \ldots, \omega_n$ and $\eta_1, \ldots, \eta_n$ are two bases for H. Then*

$$\Delta(\omega_1, \ldots, \omega_n) = \Delta(\eta_1, \ldots, \eta_n).$$

Thanks to the lemma we may write without ambiguity $\Delta(H) = \Delta(\omega_1, \ldots, \omega_n)$ where $\omega_1, \ldots, \omega_n$ is any basis for H.

PROOF. We know by Algebra I that

$$\omega_i = \sum_{j=1}^{n} c_{i,j}\eta_j$$

where $c_{i,j} \in \mathbb{Z}$ and the $n \times n$ matrix $(c_{i,j})$ is unimodular (meaning it has determinant ± 1). By Lemma 74 we have

$$\Delta(\omega_1, \ldots, \omega_n) = \mathrm{Det}((c_{i,j}))^2 \cdot \Delta(\eta_1, \ldots, \eta_n)$$

proving the result. □

LEMMA 106. *Let K be a number field of degree n. Let H be a finitely generated subgroup of $\mathcal{O}_K^+$ of rank n. Then $|\Delta(H)|$ is a positive integer (and in particular it is non-zero).*

PROOF. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for H. Recall that

$$\Delta(\omega_1, \ldots, \omega_n) = \mathrm{Det}(\mathrm{Trace}_{K/\mathbb{Q}}(\omega_i \cdot \omega_j)).$$

However $H \subset \mathcal{O}_K$ so the entries of the determinant are in $\mathbb{Z}$. It remains to show that $\Delta(H) \neq 0$. Suppose $\Delta(H) = 0$. Then, by Theorem 75, the elements $\omega_1, \ldots, \omega_n$ are not a $\mathbb{Q}$-basis for K and so they are linearly dependent over $\mathbb{Q}$: say $a_1\omega_1 + \cdots + a_n\omega_n = 0$ where $a_i \in \mathbb{Q}$ and not all zero. Multiplying by the lcm of the denominators of the a_i, we can suppose $a_i \in \mathbb{Z}$ and not all 0. This contradicts the fact that $\omega_1, \ldots, \omega_n$ is a $\mathbb{Z}$-basis for H. □

THEOREM 107. *Let K be a number field of degree n. Let G, H be finitely generated subgroups of $\mathcal{O}_K^+$ of rank n and suppose $H \subseteq G$. Then*

$$\Delta(H) = [G : H]^2 \cdot \Delta(G).$$

This is saying that the discriminant of a subgroup is bigger in absolute value than the discriminant of the group.

PROOF. We know by Algebra I that there is a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ for G such that

$$\eta_1 = d_1\omega_1,\ \eta_2 = d_2\omega_2, \ldots,\ \eta_n = d_n\omega_n$$

is a $\mathbb{Z}$-basis for H, with $d_1, \ldots, d_n$ being positive integers. Now the index $[G : H] = d_1 \cdot d_2 \cdots d_n$. The change of basis matrix for going from ω_i to the η_i is the diagonal matrix $\mathrm{diag}(d_1, \ldots, d_n)$. By Lemma 74

$$\begin{aligned}
\Delta(H) &= \Delta(\eta_1, \ldots, \eta_n) \\
&= \mathrm{Det}(\mathrm{diag}(d_1, \ldots, d_n))^2 \cdot \Delta(\omega_1, \ldots, \omega_n) \\
&= (d_1 d_2 \cdots d_n)^2 \cdot \Delta(G) \\
&= [G : H]^2 \cdot \Delta(G).
\end{aligned}$$

□

6. Existence of Integral Basis

THEOREM 108. *Let K be a number field of degree n. Then $\mathcal{O}_K$ has an integral basis of rank n. In other words there are algebraic integers $\omega_1, \ldots, \omega_n$ such that*

$$\mathcal{O}_K^+ = \mathbb{Z} \cdot \omega_1 \oplus \mathbb{Z} \cdot \omega_n \oplus \cdots \oplus \mathbb{Z} \cdot \omega_n.$$

PROOF. We need to show that $\mathcal{O}_K^+$ is finitely generated of rank n. First we show the existence of a subgroup of $\mathcal{O}_K^+$ that is finitely generated of rank n. This is easy. Start with any basis $\alpha_1, \ldots, \alpha_n$ for $K/\mathbb{Q}$. By Proposition 84 there are non-zero integers $m_1, \ldots, m_n$ such that $\beta_i = m_i \alpha_i$ are algebraic integers. Now just check that $\beta_1, \ldots, \beta_n$ is still a basis for $K/\mathbb{Q}$. Let $H = \mathbb{Z} \cdot \beta_1 \oplus \cdots \oplus \mathbb{Z} \cdot \beta_n$. We know by Lemma 106 that $|\Delta(H)|$ is a positive integer.

Now from among the finitely generated subgroups of rank n we choose one, let's call it H, such that $|\Delta(H)|$ is as small as possible. We will show that $\mathcal{O}_K^+ = H$. Let $\alpha \in \mathcal{O}_K^+$; we want to show that $\alpha \in H$. Let G be the subgroup of $\mathcal{O}_K^+$ generated by α and any basis for H. In particular G is finitely generated and H is a subgroup of G. As H has rank n, we see G must have rank $\geq n$. But by Lemma 100, the group G must have rank $\leq n$. Thus G has rank n. By Theorem 107 we know that

$$\Delta(H) = [G : H]^2 \cdot \Delta(G).$$

By the minimality of $|\Delta(H)|$ we have $[G : H] = 1$. Thus $G = H$ and so $\alpha \in H$. Hence $\mathcal{O}_K^+ = H$. The proof is complete as H is finitely generated of rank n. □

DEFINITION. We define the **discriminant of** K (also called the **discriminant of** $\mathcal{O}_K$) to be the discriminant of any integral basis for $\mathcal{O}_K$. It is denoted by Δ_K.

7. Algorithm for Computing an Integral Basis

LEMMA 109. *Let K be a number field of degree n. Let $\omega_1, \ldots, \omega_n \in \mathcal{O}_K$ be independent but not a $\mathbb{Z}$-basis. Then there is a prime p such that $p^2 \mid \Delta(\omega_1, \ldots, \omega_n)$ and rational integers $0 \leq u_i < p$, not all zero, such that*

$$\frac{u_1\omega_1 + \cdots + u_n\omega_n}{p} \in \mathcal{O}_K.$$

Moreover, if $\eta_1, \ldots, \eta_n$ is a basis for the subgroup spanned by $\omega_1, \ldots, \omega_n$ and $(u_1\omega_1 + \cdots + u_n\omega_n)/p$ then

$$\Delta(\eta_1, \ldots, \eta_n) = \frac{1}{p^2} \cdot \Delta(\omega_1, \ldots, \omega_n).$$

PROOF. Let H be the subgroup generated by the ω_i. Suppose $\mathcal{O}_K \neq H$ and let $m = [\mathcal{O}_K^+ : H] > 1$. Let $p \mid m$. We know $\Delta(H) = m^2 \cdot \Delta(\mathcal{O}_K^+)$ and so $p^2 \mid \Delta(H)$. Now consider the quotient $\mathcal{O}_K^+/H$. This is an abelian

group of order m. By the Fundamental Theorem of finitely generated abelian groups you can show it has an element of order p (you can also deduce this from Sylow's Theorems if you know what these are). Thus there is $\alpha \in \mathcal{O}_K$ such that $p(\alpha + H) = 0$ but $\alpha + H \neq 0$; i.e. $p\alpha \in H$ but $\alpha \notin H$. As $p\alpha \in H$ we may write

$$p\alpha = a_1\omega_1 + \cdots + a_n\omega_n$$

with $a_i \in \mathbb{Z}$. Now let $a_i = u_i + pb_i$ with u_i, $b_i \in \mathbb{Z}$ and $0 \leq u_i < p$. If all the u_i are zero then $\alpha = b_1\omega_1 + \cdots + b_n\omega_n \in H$ giving a contradiction. Thus not all u_i are zero. Let

$$\beta = \frac{u_1\omega_1 + \cdots + u_n\omega_n}{p}.$$

Then

$$\beta = \alpha - (b_1\omega_1 + \cdots + b_n\omega_n) \in \mathcal{O}_K$$

as required.

For the last step let G be the group generated by the ω_i and β. It is easy to show that H has index p in G so $\Delta(G) = \Delta(H)/p^2$. □

Example 110. Let θ be a root of $X^3 + X + 1$. We compute an integral basis for $K = \mathbb{Q}(\theta)$. We start with $1, \theta, \theta^2$ which is a basis for K and consists of elements of $\mathcal{O}_K$. By Exercise 72 this has discriminant

$$\Delta(1, \theta, \theta^2) = -4 - 27 = -31.$$

This is squarefree, so $1, \theta, \theta^2$ is an integral basis for $\mathcal{O}_K$.

Example 111. We continue Example 71. Recall that $f = X^3 + X^2 - 2X + 8$, that θ is a root of f and that $K = \mathbb{Q}(\theta)$. We would like to compute an integral basis and the discriminant of $\mathcal{O}_K$. We found that

$$\Delta(1, \theta, \theta^3) = -2012 = 2^2 \times 503.$$

If $1, \theta, \theta^3$ is not an integral basis, then the index of the subgroup generated by it in $\mathcal{O}_K^+$ can only be 2. Moreover, in this case there are integers $0 \leq u_i \leq 1$, not all zero, such that

$$\beta = \frac{u_0 + u_1\theta + u_2\theta^2}{2} \in \mathcal{O}_K.$$

This gives us seven possibilities to test. We can cut down the work a little. For example, taking traces we find

$$\frac{3u_0 - u_1 + 5u_2}{2} \in \mathbb{Z}.$$

This rules out $(u_0, u_1, u_2) = (1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 1)$. So we're left with three possibilities:

$$(u_0, u_1, u_2) = (1, 1, 0), \qquad (1, 0, 1), \qquad (0, 1, 1).$$

We can get a little further by trying norms. Note that

$$M_\beta = \frac{u_0}{2} \cdot I_3 + \frac{u_1}{2} \cdot M_\theta + \frac{u_2}{2} \cdot \mathrm{M}_{\theta^2}.$$

Thus

$$\mathrm{Norm}((1+\theta)/2)) = \begin{vmatrix} 1/2 & 0-4 & \\ 1/2 & 1/2 & 1 \\ 0 & 1/2 & 0 \end{vmatrix} = -5/4$$

thus $(u_0, u_1, u_2) \neq (1, 1, 0)$. Similarly

$$\mathrm{Norm}((1+\theta^2)/2) = \begin{vmatrix} 1/2 & -4 & 4 \\ 0 & 3/2 & -5 \\ 1/2 & -1/2 & 2 \end{vmatrix} = 29/4,$$

thus $(u_0, u_1, u_2) \neq (1, 0, 1)$. We're finally left with $\beta = (\theta + \theta^2)/2$. This has matrix

$$M_\beta = \begin{pmatrix} 0 & -4 & 0 \\ 1/2 & 1 & -4 \\ 1/2 & 0 & 1 \end{pmatrix}$$

and characteristic polynomial

$$\chi_{K,\beta}(X) = X^3 - 2X^2 + 3X - 10 \in \mathbb{Z}[X].$$

Thus $\beta \in \mathcal{O}_K$. Since $\theta^2 = 2\beta - \theta$, the subgroup generated by $1, \theta, \theta^2, \beta$ has basis $1, \theta, \beta$. This has discriminant $\Delta(1, \theta, \beta) = (1/4) \cdot \Delta(1, \theta, \theta^2) = -503$ which is squarefree (in fact prime). Thus $1, \theta, (\theta + \theta^2)/2$ is an integral basis, the $\Delta_K = -503$.

Remark. We showed in the above example that $\mathcal{O}_K \neq \mathbb{Z}[\theta]$. It can in fact be shown that $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_K$. We see that there is no analogue of the Primitive Element Theorem for rings of integers.

CHAPTER 5

Factorisation and Ideals

1. Revision: Units, Irreducibles and Primes

Let R be an integral domain (commutative ring with a 1 and without zero divisors). Recall that an element $a \in R$ is a **unit** if there is some $b \in R$ such that $ab = 1$. The set of units form a multiplicative group denoted by R^*.

Recall that an element $a \in R$ is called **irreducible** if it is non-zero, non-unit, and whenever we can write $a = bc$ with b, $c \in R$ then b is a unit or c is a unit. An element $a \in R$ is a **prime** if it is non-zero, non-unit, and whenever $a \mid bc$ with b, $c \in R$ then $a \mid b$ or $a \mid c$. We say that a, b are **associates** if $a = ub$ where u is a unit of R.

Exercise 112. Show that a prime is also an irreducible (you did this in Algebra II, and it's easy).

We say that R is **unique factorisation domain** (UFD) if every non-zero non-unit a can be written as a product $a = r_1 r_2 \cdots r_n$ where the r_i are irreducibles and if moreover $a = s_1 s_2 \cdots s_m$ where the s_j are irreducibles then $n = m$, and after permuting, r_i and s_i are associates. In a UFD, every irreducible is a prime.

We say that R is a **principal ideal domain** (PID) if every ideal of R is a principal ideal (i.e. generated by one element). In Algebra II you showed that a PID is also a UFD. The converse is not true in general, but we'll see that the converse is true for R the ring of integers of a number field.

Example 113. You know that $\mathbb{Z}$ (the ring of integers of $\mathbb{Q}$) is a UFD. If you did Introduction to Number Theory then you also know that $\mathbb{Z}[i]$ (the ring of itnegers of $\mathbb{Q}(i)$) is a UFD.

Here we consider $\mathbb{Z}[\sqrt{-5}]$ (the ring of integers of $\mathbb{Q}(\sqrt{-5})$). Note that

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

We have here two factorisations of 6. We claim that both are factorisations into irreducibles. Let's check for example that $1 + \sqrt{-5}$ is irreducible. Suppose $1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$ where a, b, c, d are integers. Taking norms we have

$$6 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Thus without loss of generality $a^2 + 5b^2 = 1$ and $c^2 + 5d^2 = 6$ or $a^2 + 5b^2 = 2$ and $c^2 + 5d^2 = 3$. It is clear that the second case forces $b = 0$ and $a^2 = 2$ which is impossible. It follows from the first case that $(a, b) = (\pm 1, 0)$ and so $a+b\sqrt{-5} = \pm 1$ is a unit. Thus $1+\sqrt{-5}$ is indeed irreducible. You can check that $1 - \sqrt{-5}$, 2, 3 are also irreducible.

We show that 2, $1 + \sqrt{-5}$ are not associates and 2, $1 - \sqrt{-5}$ are not associates. This is immediate because the ratios $(1 + \sqrt{-5})/2$ and $(1 - \sqrt{-5})/2$ do not belong to $\mathbb{Z}[\sqrt{-5}]$ (and hence certainly are not units in $\mathbb{Z}[\sqrt{-5}]$). This shows that $\mathbb{Z}[\sqrt{-5}]$ is *not* a UFD. It follows from this that $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

2. Revision: Ideals

We saw that unique factorization can fail for rings of integers of number fields. It turns out that we can recover unique factorization if we look at ideals instead of elements. What this means is that we will show that every ideal can be written as a product of powers of prime ideals in a unique way.

We shall mostly use gothic letters for ideals $\mathfrak{a}$, $\mathfrak{b}$, etc. Let R be a ring. Recall that an **ideal** $\mathfrak{a}$ of R is a subset $\mathfrak{a} \subseteq R$ satisfying

- $\mathfrak{a}$ is an abelian group under addition;
- $x\mathfrak{a} \subseteq \mathfrak{a}$ for $x \in R$.

If $\alpha \in R$ we define the **principal ideal** generated by α be

$$\alpha R = \{\alpha r \ : \ r \in R\}.$$

Another common notation for αR is $\langle \alpha \rangle$. Of course $\langle 1 \rangle = R$. When we think of R as an ideal it is usual to write it as $\langle 1 \rangle$. The **zero ideal** is just $\{0\}$; we usually write this as $\langle 0 \rangle$ or simply 0.

In more generality, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are non-zero elements R we define the ideal generated by $\alpha_1, \ldots, \alpha_n$ to be

$$\langle \alpha_1, \ldots, \alpha_n \rangle = \left\{ \sum_{i=1}^{n} \beta_i \alpha_i \ : \quad \beta_1, \ldots, \beta_n \in R \right\}.$$

If $\mathfrak{a}$, $\mathfrak{b}$ are ideals then so is

$$(\mathfrak{a}, \mathfrak{b}) = \{\alpha + \beta \ : \ \alpha \in \mathfrak{a}, \ \beta \in \mathfrak{b}\}.$$

We sometimes write $\mathfrak{a} + \mathfrak{b}$ for $(\mathfrak{a}, \mathfrak{b})$. We say that $\mathfrak{a}$, $\mathfrak{b}$ are **coprime** if $\mathfrak{a} + \mathfrak{b} = \langle 1 \rangle$.

We define the **ideal product** $\mathfrak{ab}$ to be the set of all finite sums $\sum_{i=1}^{r} \alpha_i \beta_i$ with $\alpha_i \in \mathfrak{a}$ and $\beta_i \in \mathfrak{b}$. It is an easy exercise to show that $\mathfrak{ab}$ is again an ideal.

Exercise 114. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals. Show that $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$ are ideals.

Lemma 115. *Let K be a number field. Every ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written in the form $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_n \rangle$ for some $\alpha_i \in \mathcal{O}_K$.*

PROOF. Write $\mathfrak{a}^+$ for $\mathfrak{a}$ considered as an abelian group. This is a subgroup of $\mathcal{O}_K^+$ which is finitely generated. Thus there exists $\alpha_1, \ldots, \alpha_n$ such that

$$\mathfrak{a}^+ = \mathbb{Z} \cdot \alpha_1 \oplus \cdots \oplus \mathbb{Z} \cdot \alpha_n.$$

Clearly

$$\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_n \rangle.$$

□

Lemma 115 tells us that every ideal is finitely generated. Rings with such a property are called Noetherian.

LEMMA 116. *If* $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_m \rangle$ *and* $\mathfrak{b} = \langle \beta_1, \ldots, \beta_n \rangle$ *then*

$$\mathfrak{a} + \mathfrak{b} = \langle \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \rangle,$$

and

$$\mathfrak{ab} = \langle \alpha_i \cdot \beta_j \ : \ i = 1, \ldots, m, \ j = 1, \ldots, n \rangle.$$

PROOF. This is clear from the definition of ideal addition and multiplication. □

EXAMPLE 117. Let $K = \mathbb{Q}(\sqrt{-5})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We saw in Example 113 that this is not a PID. Let's write down a non-principal ideal of $\mathcal{O}_K$. Let $\mathfrak{a} = \langle 2, 1 + \sqrt{-5} \rangle$. We want to show that it is non-principal. Suppose it is, say

$$\mathfrak{a} = \beta \cdot \mathcal{O}_K$$

for some $\beta \in \mathcal{O}_K$. Since $\beta \mid 2$ and $\beta \mid (1 + \sqrt{-5})$ we have $\mathrm{Norm}(\beta) \mid 4$ and $\mathrm{Norm}(\beta) \mid 6$ and so $\mathrm{Norm}(\beta) \mid 2$. Write $\beta = u + v\sqrt{-5}$ where u, v are integers. Thus $u^2 + 5v^2 = \pm 1$ or ± 2. It follows that $v = 0$ and $u = \pm 1$, so $1 = \pm\beta \in \mathfrak{a}$ (and so $\mathfrak{a} = \mathcal{O}_K$). However, any element of $\mathfrak{a}$ has the form

$$2(a + b\sqrt{-5}) + (c + d\sqrt{-5})(1 + \sqrt{-5}),$$

with a, b, c, $d \in \mathbb{Z}$. If this equals 1 then

$$2a + c - 5d = 1, \qquad 2b + c + d = 0.$$

But $2a + c - 5d \equiv 2b + c + d \pmod 2$, and so $1 \equiv 0 \pmod 2$ giving a contradiction! Therefore $\mathfrak{a}$ is non-principal.

From the recipes in Lemma 116

$$\mathfrak{a} + \mathfrak{a} = \mathfrak{a},$$

(which can be deduced from the definition of an ideal) and

$$\begin{aligned}
\mathfrak{a}^2 &= \langle 4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5} \rangle \qquad (\text{as } (1 + \sqrt{-5})^2 = -4 + 2\sqrt{-5}) \\
&= \langle 4, 2 + 2\sqrt{-5}, 2\sqrt{-5} \rangle \qquad (\text{adding first generator to the last}) \\
&= \langle 4, 2, 2\sqrt{-5} \rangle \qquad (\text{subtracting third generator from second}) \\
&= \langle 2 \rangle \qquad (\text{since 4 and } 2\sqrt{-5} \text{ are multiples of 2}).
\end{aligned}$$

Thus $\mathfrak{a}^2$ is a principal ideal, even though $\mathfrak{a}$ is non-principal.

Now let

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

You can check that this ideal is non-principal. Note that $\mathfrak{a} + \mathbf{b}$ contains both 2 and 3 so contains $3 - 2 = 1$. Thus $\mathfrak{a} + \mathbf{b} = \mathcal{O}_K$ (i.e. the ideals $\mathfrak{a}$, $\mathbf{b}$ are coprime). Also

$$\begin{aligned}
\mathfrak{a}\mathbf{b} &= \langle 6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5} \rangle \\
&= \langle 6, 1 + \sqrt{-5}, -4 + 2\sqrt{-5} \rangle \\
&= \langle 6, 1 + \sqrt{-5} \rangle \qquad \text{since } -4 + 2\sqrt{-5} = -6 + 4(1 + \sqrt{-5}) \\
&= \langle 1 + \sqrt{-5} \rangle \qquad (\text{since } (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6).
\end{aligned}$$

Thus again $\mathfrak{a}\mathbf{b}$ is principal even though both $\mathfrak{a}$ and $\mathbf{b}$ are non-principal.

3. The Noetherian Property

THEOREM 118. *Let R be a ring (commutative with 1). Then the following are equivalent.*

(i) *Every ideal of R is **finitely generated** (an ideal is finitely generated if it can be written as $\langle \alpha_1, \ldots, \alpha_n \rangle$ for some $\alpha_1, \ldots, \alpha_n \in R$).*

(ii) *R satisfies the **ascending chain property** for ideals: if $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ are ideals then there is some m such that $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$.*

(iii) *Every non-empty set of ideals S contains a maximal element (an element $\mathfrak{a} \in S$ is **maximal** if $\mathfrak{a}$ is not properly contained in any $\mathbf{b} \in S$).*

A ring satisfying any (and hence all) of properties (i)–(iii) is called **Noetherian**.

PROOF. **(i) implies (ii).** Write

$$\mathfrak{a} = \bigcup_{n=1}^{\infty} \mathfrak{a}_n.$$

It is easy to see that $\mathfrak{a}$ is an ideal. By (i) we have $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_n \rangle$. But each α_i is contained in some $\mathfrak{a}_{m_i}$. Let $m = \max(m_i)$. Then $\alpha_1, \ldots, \alpha_m \in \mathfrak{a}_m$. Hence $\mathfrak{a} = \mathfrak{a}_m$. It follows that $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \mathfrak{a}_{m+2} = \cdots$.

(ii) implies (iii). Suppose there is no maximal element. Let $\mathfrak{a}_1$ be any element of S. As it isn't maximal, there is some $\mathfrak{a}_2$ in S which properly cotains $\mathfrak{a}_1$. Repeat the process, to obtain an ascending chain

$$\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq \cdots$$

which is not stationary. This contradicts (ii).

(iii) implies (i). Let $\mathfrak{c}$ be an ideal. We want to show that $\mathfrak{c}$ is finitely generated. Let S be the set of finitely generated ideals contained in $\mathfrak{c}$. The set S is non-empty, since $\langle\gamma\rangle \in S$ for any $\gamma \in \mathfrak{c}$. By (iii), the set S has a maximal element $\mathfrak{a}$. As $\mathfrak{a}$ is finitely generated, $\mathfrak{a} = \langle\alpha_1, \ldots, \alpha_n\rangle$. We know $\mathfrak{a} \subseteq \mathfrak{c}$. We claim $\mathfrak{c} = \mathfrak{a}$ which would complete the proof. Let $\alpha \in \mathfrak{c}$. Then

$$\mathbf{b} = \langle\alpha_1 \ldots, \alpha_n, \alpha\rangle$$

is a finitely generated ideal contained in $\mathfrak{c}$ which contains $\mathfrak{a}$. By the maximality of $\mathfrak{a}$ we have $\mathbf{b} = \mathfrak{a}$. Thus $\alpha \in \mathfrak{a}$. Hence $\mathfrak{c} = \mathfrak{a}$, and so is finitely generated. □

THEOREM 119. *Rings of integers of number fields are Noetherian.*

PROOF. Any ideal of $\mathcal{O}_K$ is finitely generated by Lemma 115. The theorem follows from Theorem 118. □

4. Quotient Rings

Let $\mathfrak{a}$ be an ideal of the ring $\mathcal{O}_K$. A coset of $\mathfrak{a}$ is of the form

$$\alpha + \mathfrak{a} = \{\alpha + \alpha \ : \ \alpha \in \mathfrak{a}\}.$$

Recall that two cosets are equal $\alpha + \mathfrak{a} = \beta + \mathfrak{a}$ if and only if $\alpha - \beta = \mathfrak{a}$. We define the *quotient*

$$\mathcal{O}_K/\mathfrak{a} = \{x + \mathfrak{a} \ : \ x \in \mathfrak{a}\}.$$

A priori $\mathcal{O}_K/\mathfrak{a}$ is just the set of cosets of $\mathfrak{a}$, but we can make it into a ring by defining addition and multiplication as follows:

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}, \qquad (x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}.$$

It is an easy exercise to show that these operations are well-defined and that they do give a ring structure on $\mathcal{O}_K/\mathfrak{a}$.

We would like to prove that if $\mathfrak{a}$ is a non-zero ideal then $\mathcal{O}_K/\mathfrak{a}$ is finite. Before we can do this we need the following lemma.

LEMMA 120. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Let α be a non-zero element of $\mathfrak{a}$. Then* $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathfrak{a}$. *In particular $\mathfrak{a}$ contains a positive rational integer.*

PROOF. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K. Then $\mathrm{Norm}(\alpha) = \alpha_1\alpha_2 \cdots \alpha_n$ where $\alpha_i = \sigma_i(\alpha)$. Without loss of generality $\alpha_1 = \alpha$. Now the α_i are algebraic integers (they share the same minimal polynomial as α). Thus the product $\beta = \alpha_2 \cdots \alpha_n \in \mathcal{O}$. Moreover, $\beta = \mathrm{Norm}(\alpha)/\alpha$. But $\mathrm{Norm}(\alpha) \in \mathbb{Z} \subseteq \mathcal{O}_K$ and $\alpha \in \mathcal{O}_K$ so $\beta = \mathrm{Norm}(\alpha)/\alpha \in K$. Hence $\beta \in \mathcal{O} \cap K = \mathcal{O}_K$. It follows that $\mathrm{Norm}(\alpha) = \alpha\beta \in \mathfrak{a}$. As α is non-zero, $\mathrm{Norm}(\alpha)$ is a non-zero rational integer. So either $\mathrm{Norm}(\alpha)$ or $-\mathrm{Norm}(\alpha)$ is a positive rational integer in $\mathfrak{a}$. □

THEOREM 121. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite.*

PROOF. By Lemma 120 there is some positive rational integer $m \in \mathfrak{a}$. Thus $\mathcal{O}_K \supseteq \mathfrak{a} \supseteq m\mathcal{O}_K$. To show that the index $[\mathcal{O}_K : \mathfrak{a}]$ is finite it is enough to show that the index $[\mathcal{O}_K : m\mathcal{O}_K]$ is finite. But as an abelain group $\mathcal{O}_K \cong \mathbb{Z}^n$ (where $n = [K : \mathbb{Q}]$) and $m\mathcal{O}_K \cong m\mathbb{Z}^n$, so $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^n$ which is finite. □

5. Prime and Maximal Ideals

We need to revise some Algebra II.

DEFINITION. Let R be a ring (commutative with 1). We call a proper ideal $\mathfrak{p}$ **prime**, if for all α, $\beta \in R$ we have

$$\alpha\beta \in \mathfrak{p} \implies \alpha \in \mathfrak{p} \quad \text{or} \quad \beta \in \mathfrak{p}.$$

We call a proper ideal $\mathfrak{m}$ **maximal** if there isn't any ideal $\mathfrak{a}$ satisfying

$$\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R.$$

In words, a proper ideal is maximal if and only if it is not properly contained in some other proper ideal.

THEOREM 122. *Every proper ideal of $\mathcal{O}_K$ is contained in a maximal ideal.*

PROOF. Let $\mathfrak{a}$ be a proper ideal. Let S be the set of proper ideals containing $\mathfrak{a}$. This is non-empty as $\mathfrak{a} \in S$. By the Noetherian property of $\mathcal{O}_K$, the set S must contain a maximal element $\mathfrak{m}$. It is clear that $\mathfrak{m}$ is a maximal ideal. □

You will no doubt recall the following theorem from Algebra II and have no trouble in reconstructing its proof. Here we do the proof a little differently.

LEMMA 123. *Every finite integral domain is a field.*

PROOF. Let R be a finite integral domain and let a be a non-zero element in R. We would like to show that a is invertible. The sequence $a, a^2, a^3, \ldots$ must have repetition. Thus there are $n < m$ such that $a^m = a^n$. Thus $a^n(a^{m-n} - 1) = 0$. As $a \neq 0$ and R is an integral domain, $a^{m-n} = 1$. But $m - n \geq 1$, so a has an inverse in R, namely a^{m-n-1}. □

We shall need the following theorem, again from Algebra II.

THEOREM 124. *Let R be ring (commutative with 1). An ideal $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field. Maximal ideals are prime.*

PROOF. The definition of primality for an ideal $\mathfrak{p}$ can be reformulated as follows:

$$(\alpha + \mathfrak{p})(\beta + \mathfrak{p}) = 0 \implies \alpha + \mathfrak{p} = 0 \quad \text{or} \quad \beta + \mathfrak{p} = 0.$$

This is the same as saying that $\mathcal{O}_K/\mathfrak{p}$ is an integral domain.

Suppose $\mathfrak{m}$ is maximal. Let $a + \mathfrak{m} \neq 0$ (i.e. $a \notin \mathfrak{m}$). Then the ideal $a\mathcal{O}_K + \mathfrak{m}$ strictly contains $\mathfrak{m}$ and so by definition of maximality equals $\mathcal{O}_K$. In particular $1 \in a\mathcal{O}_K + \mathfrak{m}$ and so $1 = ab + m$ where $b \in \mathcal{O}_K$ and $m \in \mathfrak{m}$. But then $(a + \mathfrak{m})(b + \mathfrak{m}) = 1 - m + \mathfrak{m} = 1 + \mathfrak{m}$. Thus $\mathcal{O}/\mathfrak{m}$ is a field. Conversely, suppose $\mathcal{O}/\mathfrak{m}$ is a field. Let $\mathfrak{a}$ be a ideal properly containing $\mathfrak{m}$. Thus there is some element $a \in \mathfrak{a}$ with $a \notin \mathfrak{m}$. Hence $a + \mathfrak{m} \neq 0$ and is therefore invertible in the field $\mathcal{O}_K/\mathfrak{m}$. In particular there is some $b \in \mathcal{O}_K$ so that $(a+\mathfrak{m})(b+\mathfrak{m}) = 1+\mathfrak{m}$. So $1-ab \in \mathfrak{m} \subset \mathfrak{a}$. But $a \in \mathfrak{a}$ so $1 \in \mathfrak{a}$ so $\mathfrak{a} = \mathcal{O}_K$ proving maximality of $\mathfrak{m}$.

For the last part if $\mathfrak{m}$ is maximal, then $\mathcal{O}_K/\mathfrak{m}$ is a field and so an integral domain, therefore $\mathfrak{m}$ is prime. □

Exercise 125. Here is a direct way of showing the maximal ideals are prime. Suppose that $\mathfrak{m}$ is maximal and suppose that $\alpha\beta \in \mathfrak{m}$ but $\alpha \notin \mathfrak{m}$. Let $\mathfrak{m}' = (\alpha) + \mathfrak{m}$. Show that $\mathfrak{m}' = (1)$. Deduce that $\beta \in \mathfrak{m}$. Hence $\mathfrak{m}$ is prime.

Theorem 126 (Non-zero prime ideals are maximal). *Let K be a number field. An non-zero ideal of $\mathcal{O}_K$ is maximal if and only if it is prime.*

Proof. We know that maximal ideals are prime. If $\mathfrak{p}$ is a non-zero prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, which is finite by Theorem 121. Thus $\mathcal{O}_K/\mathfrak{p}$ is a field by Lemma 123, so $\mathfrak{p}$ is maximal. □

Exercise 127. The conclusion that a prime ideal is maximal is false for more general rings. Convince yourself that the ideal $X \cdot \mathbb{Q}[X, Y]$ in the ring $\mathbb{Q}[X, Y]$ is prime but not maximal.

6. Fractional Ideals

We aim to show that every non-zero ideals can be written as a product of prime ideals, and that any such factorisation is unique up to reordering. To achieve this we need to introduce the notion of a fractional ideal, which is merely a technical convenience.

Definition. A **fractional ideal** of $\mathcal{O}_K$ is a subset $\mathfrak{a} \subseteq K$ satisfying the following:

(i) $\mathfrak{a}$ is an abelian group under addition;
(ii) $x\mathfrak{a} \subseteq \mathfrak{a}$ for every $x \in \mathcal{O}_K$;
(iii) there exists some non-zero $y \in \mathcal{O}_K$ such that $y\mathfrak{a} \subseteq \mathcal{O}_K$.

Warning: A ideal of $\mathcal{O}_K$ is a fractional ideal of $\mathcal{O}_K$, but a fractional ideal of $\mathcal{O}_K$ need not be an ideal of $\mathcal{O}_K$. Indeed it is a subset of K but in general not of $\mathcal{O}_K$.

Exercise 128. Convince yourself that $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$ but not an ideal of $\mathbb{Z}$.

The following lemma is clear.

LEMMA 129. *Any ideal of $\mathcal{O}_K$ is also a fractional ideal. A fractional ideal of $\mathcal{O}_K$ is also an ideal of $\mathcal{O}_K$ if and only if it is contained in $\mathcal{O}_K$.*

LEMMA 130. *A subset $\mathfrak{a} \subseteq K$ is a fractional ideal of $\mathcal{O}_K$ if and only if $\mathfrak{a} = \frac{1}{\beta} \cdot \mathbf{b}$ where $\mathbf{b}$ is an ideal of $\mathcal{O}_K$ and β is a non-zero element of $\mathcal{O}_K$.*

PROOF. It is easy to see that if $\mathbf{b}$ is an ideal then $\frac{1}{\beta} \cdot \mathbf{b}$ is a fractional ideal. Conversely let $\mathfrak{a}$ be a fractional ideal. By (iii) in the definition, there is a non-zero β such that $\beta\mathfrak{a} \subseteq \mathcal{O}_K$. Let $\mathbf{b} = \beta\mathfrak{a}$. Now it's easy to check from (i) and (ii) that $\mathbf{b}$ is an ideal. □

We extend our earlier notation for ideals generated by elements. Given $\alpha_1, \ldots, \alpha_n \in K$ we write

$$\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle = \left\{ \sum_{i=1}^{n} \beta_i \alpha_i \ : \ \beta_1, \ldots, \beta_n \in \mathcal{O}_K \right\}.$$

We define multiplication for fractional ideals in the same way we defined it for ideals: $\mathfrak{a}\mathfrak{b}$ is the set of all finite sums $\sum_{i=1}^{r} \alpha_i \beta_i$ with $\alpha_i \in \mathfrak{a}$ and $\beta_i \in \mathfrak{b}$.

LEMMA 131. *The product of two fractional ideals is a fractional ideal.*

PROOF. This follows from Lemma 130 as the product of two ideals is an ideal. □

LEMMA 132. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$ and define*

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

Then

(a) *$\mathfrak{a}^{-1}$ is a fractional ideal of $\mathcal{O}_K$;*
(b) *$\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$;*
(c) *$\mathfrak{a}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$.*

It will turn out that $\mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_K = \langle 1 \rangle$ thus $\mathfrak{a}^{-1}$ is the inverse of $\mathfrak{a}$ in the group of fractional ideals. This will take us a while to prove.

PROOF. Let's show that $\mathfrak{a}^{-1}$ is a fractional ideal. Clearly $0 \in \mathfrak{a}^{-1}$. If β_1, $\beta_2 \in \mathfrak{a}^{-1}$ then

$$(\beta_1 + \beta_2)\mathfrak{a} \subseteq \beta_1\mathfrak{a} + \beta_2\mathfrak{a} \subseteq \mathcal{O}_K + \mathcal{O}_K = \mathcal{O}_K.$$

Thus $\beta_1 + \beta_2 \in \mathfrak{a}^{-1}$. Similarly $-\beta_1 \in \mathfrak{a}^{-1}$. Thus $\mathfrak{a}^{-1}$, considered additively, is a subgroup of K. Moreover, if $x \in \mathcal{O}_K$ and $\beta \in \mathfrak{a}^{-1}$ then

$$(x\beta)\mathfrak{a} = x(\beta\mathfrak{a}) \subseteq x\mathcal{O}_K \subseteq \mathcal{O}_K.$$

Hence $x\beta \in \mathfrak{a}^{-1}$ and so $x\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$. Thus $\mathfrak{a}^{-1}$ satisfies conditions (i) and (ii) in the definition of fractional ideal.

Finally let y be any non-zero element of $\mathfrak{a}$. Then $\beta y \in \mathcal{O}_K$ for all $\beta \in \mathfrak{a}^{-1}$. Thus $y\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$ so we satisfy condition (iii). Thus $\mathfrak{a}^{-1}$ is a fractional ideal of $\mathcal{O}_K$. This proves (a).

Part (b) is simply saying that $\beta\mathfrak{a} \subseteq \mathcal{O}_K$ for all $\beta \in \mathcal{O}_K$. But as $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ we have $\beta\mathfrak{a} \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$, proving (b).

By definition of $\mathfrak{a}^{-1}$, for any $\beta \in \mathfrak{a}^{-1}$ we have $\beta \cdot \mathfrak{a} \subseteq \mathcal{O}_K$. Thus

$$\mathfrak{a}^{-1}\mathfrak{a} = \sum_{\beta \in \mathfrak{a}^{-1}} \beta \cdot \mathfrak{a} \subseteq \mathcal{O}_K.$$

As the product of fractional ideals is a fractional ideal, we see that $\mathfrak{a}^{-1}\mathfrak{a}$ is a fractional ideal contained in $\mathcal{O}_K$, and thus an ideal of $\mathcal{O}_K$. This proves (c). □

Exercise 133. Check that $\langle\alpha\rangle^{-1} = \langle\alpha^{-1}\rangle$ for non-zero $\alpha \in \mathcal{O}_K$.

Exercise 134. Let $\mathfrak{a} \subseteq \mathbf{b}$ be non-zero ideals of $\mathcal{O}_K$. Check that $\mathbf{b}^{-1} \subseteq \mathfrak{a}^{-1}$.

7. To Contain is to Divide

We would like to define what it means for one ideal to be a divisor of another ideal. For principal ideals this perhaps clear; we want $\langle\alpha\rangle$ to divide $\langle\beta\rangle$ precisely when α divides β. The following exercise suggests how we can generalize this notion from principal ideals to arbitrary ideals.

Exercise 135. Let α, β be non-zero elements of $\mathcal{O}_K$. Show that $\alpha \mid \beta$ is equivalent to $\langle\alpha\rangle \supseteq \langle\beta\rangle$.

Definition. Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathcal{O}_K$. We say that $\mathfrak{a}$ **divides** $\mathfrak{b}$ and we write $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{a} \supseteq \mathfrak{b}$.

Before proceeding we need one more property of prime ideals.

Lemma 136. *Suppose that $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{p}$ are non-zero ideals such that $\mathfrak{p}$ is prime and $\mathfrak{p} \mid \mathfrak{ab}$. Then either $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.*

Perhaps you would like to prove this for yourself before looking at the proof.

Proof of Lemma 136. Proof suppose $\mathfrak{p} \mid \mathfrak{ab}$ but $\mathfrak{p} \nmid \mathfrak{a}$. This means $\mathfrak{p} \supseteq \mathfrak{ab}$ but $\mathfrak{p} \not\supseteq \mathfrak{a}$. In particular, there is some $a \in \mathfrak{a}$ such that $a \notin \mathfrak{p}$. Let $b \in \mathfrak{b}$. Then $ab \in \mathfrak{ab} \subseteq \mathfrak{p}$. As $\mathfrak{p}$ is prime and $a \notin \mathfrak{p}$ we have $b \in \mathfrak{p}$. Thus $\mathfrak{p} \supseteq \mathfrak{b}$, which means $\mathfrak{p} \mid \mathfrak{b}$. □

8. Unique Factorisation of Ideals

Lemma 137. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{a} \mid \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$.*

Proof. Note that $\mathfrak{a} \mid \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ means $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r \subseteq \mathfrak{a}$. Let S be the set of ideals not containing any product of non-zero prime ideals. The lemma is simply asserting that S is empty. We suppose S is non-empty. As $\mathcal{O}_K$ is Noetherian, S must have a maximal element $\mathfrak{a}$.

Now $\mathfrak{a}$ is not prime, otherwise we can take $\mathfrak{p}_1 = \mathfrak{a}$. Thus there are β, $\gamma \notin \mathfrak{a}$ such that $\beta\gamma \in \mathfrak{a}$. Let

$$\mathbf{b} = \mathfrak{a} + \langle\beta\rangle, \qquad \mathfrak{c} = \mathfrak{a} + \langle\gamma\rangle.$$

Then $\mathfrak{a} \subsetneq \mathbf{b}$, $\mathfrak{a} \subsetneq \mathfrak{c}$. By the maximality of $\mathfrak{a}$ in S, the ideals $\mathbf{b}$, $\mathfrak{c}$ do not belong to S. Thus there are prime ideals $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathbf{b}, \qquad \mathfrak{p}_{r+1} \cdots \mathfrak{p}_s \subseteq \mathfrak{c}.$$

But then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathbf{bc} \subseteq \mathfrak{a}^2 + \beta\mathfrak{a} + \gamma\mathfrak{a} + \langle\beta\gamma\rangle \subseteq \mathfrak{a},$$

giving a contradiction. □

LEMMA 138. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}^{-1}$ properly contains $\mathcal{O}_K$.*

PROOF. From the definition of $\mathfrak{p}^{-1}$ we see that $\mathfrak{p}^{-1}$ contains $\mathcal{O}_K$. We will suppose $\mathfrak{p}^{-1} = \mathcal{O}_K$ and obtain a contradiction. Let α be a non-zero element of $\mathfrak{p}$. Thus $\langle\alpha\rangle \subseteq \mathfrak{p}$ and so $\mathfrak{p} \mid \langle\alpha\rangle$. By Lemma 137, there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that

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

We may assume that r is minimal. Thus $\mathfrak{p} \mid \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$. By Lemma 136, we have $\mathfrak{p} \mid \mathfrak{p}_i$ for some i. Without loss of generality $\mathfrak{p} \mid \mathfrak{p}_1$, which means $\mathfrak{p} \supseteq \mathfrak{p}_1$. As prime ideals are maximal, we have $\mathfrak{p} = \mathfrak{p}_1$. Since $\langle\alpha\rangle \mid \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$ we have

$$\mathfrak{p} \cdot \mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r \subseteq \alpha \cdot \mathcal{O}_K.$$

Hence

$$\alpha^{-1}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r \cdot \mathfrak{p} \subseteq \mathcal{O}_K.$$

It follows that

$$\alpha^{-1}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}^{-1} = \mathcal{O}_K.$$

Hence

$$\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r \subseteq \alpha\mathcal{O}_K = \langle\alpha\rangle.$$

This contradicts the minimality of r. □

LEMMA 139. *Let $\mathfrak{a}$, $\mathfrak{p}$ be non-zero ideals with $\mathfrak{p}$ prime. Suppose $\mathfrak{a} \subseteq \mathfrak{p}$. Then $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ properly containing $\mathfrak{a}$.*

PROOF. Since $1 \in \mathfrak{p}^{-1}$ we see that $\mathfrak{p}^{-1}\mathfrak{a}$ contains $\mathfrak{a}$. Moreover, $\mathfrak{a} \subseteq \mathfrak{p}$ so $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$. Hence $\mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$. Thus $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ containing $\mathfrak{a}$.

Suppose $\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{a}$. Thus for all $\theta \in \mathfrak{p}^{-1}$ we have $\theta\mathfrak{a} \subseteq \mathfrak{a}$. By the Integral Stability Lemma (Lemma 89) we have $\theta \in \mathcal{O}_K$ for all $\theta \in \mathfrak{p}^{-1}$. So $\mathfrak{p}^{-1} = \mathcal{O}_K$. This contradicts Lemma 138. Hence $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ properly containing $\mathfrak{a}$. □

LEMMA 140. *If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$.*

PROOF. By Lemma 139, $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of $\mathcal{O}_K$ properly containing $\mathfrak{p}$. But $\mathfrak{p}$ is a maximal ideal. Thus $\mathfrak{p}^{-1}\mathfrak{p} = \langle 1 \rangle$. □

THEOREM 141 (Unique Factorization Theorem for Ideals). *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Then every non-zero ideal $\mathfrak{a}$ can be written as a product of of finitely non-zero prime ideals*

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i.$$

Moreover this factorization is unique up to re-ordering.

We note an important convention, which is that the ideal $\mathcal{O}_K = \langle 1 \rangle$ is regarded as the product of zero many prime ideals.

PROOF. **Existence.** Let S be the set of ideals that cannot be written as products of non-zero prime ideals. We want to show that S is empty. Suppose $S \neq \emptyset$. By the Noetherian property, S has a maximal element $\mathfrak{a}$. Now $\mathfrak{a} \neq \langle 1 \rangle$ (since this is the product of the empty set of prime ideals). Thus $\mathfrak{a}$ is proper and so contained in a maximal ideal $\mathfrak{p}$. Since $\mathfrak{a} \subseteq \mathfrak{p}$, Lemma 139 tells us that $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ properly containing $\mathfrak{a}$. As $\mathfrak{a}$ is maximal in S, $\mathfrak{p}^{-1}\mathfrak{a} \notin S$. Thus it can be written as a product of non-zero prime ideals

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

Multiplying both sides by $\mathfrak{p}$ (and using $\mathfrak{p}^{-1}\mathfrak{p} = \langle 1 \rangle$ from Lemma 140) we obtain a contradiction.

Uniqueness. Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are non-zero prime ideals of $\mathcal{O}_K$ satisfying

$$\prod_{i=1}^{m} \mathfrak{p}_i = \prod_{j=1}^{n} \mathfrak{q}_j \,. \tag{13}$$

We want to show that $n = m$ and that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are the same up to re-ordering. We do this by induction on $\min(m, n)$. Suppose first that $\min(m, n) = 0$. Without loss of generality suppose that $m = 0$. If $n = 0$ then there is nothing to prove. So suppose that $n > 0$. Hence we have

$$\langle 1 \rangle = \mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n.$$

But $\mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_n \subseteq \mathfrak{q}_i$ for $i = 1, \ldots, n$, so $\mathfrak{q}_i = \langle 1 \rangle$. As prime ideals are proper by definition, we have a contradiction. Hence if $\min(m, n) = 0$ then $m = n = 0$.

We now come to the inductive step. Suppose $\min(m, n) \geq 1$. Note that

$$\mathfrak{p}_m \supseteq \prod_{i=1}^{m} \mathfrak{p}_i = \prod_{j=1}^{n} \mathfrak{q}_j.$$

In otherwords, $\mathfrak{p}_m$ divides $\prod \mathfrak{q}_j$. By Lemma 136 we see that $\mathfrak{p}_m \mid \mathfrak{q}_j$ for some j. After re-labeling we can suppose that $\mathfrak{p}_m \mid \mathfrak{q}_n$ and so

$\mathfrak{p}_m \supseteq \mathfrak{q}_n$. Now we recall that prime ideals of $\mathcal{O}_K$ are maximal. Hence $\mathfrak{p}_m = \mathfrak{q}_n$. Now multiply both sides of (13) by $\mathfrak{p}_m^{-1}$. As $\mathfrak{p}_m^{-1}\mathfrak{p}_m = \langle 1 \rangle$ (by Lemma 140) we have

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_{m-1} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_{n-1}.$$

Now we can apply the inductive hypothesis to complete the proof of uniqueness. □

LEMMA 142. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be non-zero prime ideals and $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$. Then $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \cdots \mathfrak{p}_n^{-1}$. Moreover, $\mathfrak{a}^{-1}\mathfrak{a} = \langle 1 \rangle$.*

PROOF. Let $\mathbf{b} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \cdots \mathfrak{p}_n^{-1}$. From Lemma 140 we have $\mathbf{b}\mathfrak{a} = \langle 1 \rangle = \mathcal{O}_K$. Thus $\mathbf{b} \subseteq \mathfrak{a}^{-1}$ (by the definition of $\mathfrak{a}^{-1}$). However

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

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

THEOREM 143. *Let K be a number field. The set of non-zero fractional ideals form an abelian group under multiplication, with $\mathcal{O}_K = \langle 1 \rangle$ being the identity element.*

PROOF. It is clear that multiplication of fractional ideals is commutative and associative and that $\mathcal{O}_K = \langle 1 \rangle$ acts as an identity element. We must show that every that every non-zero fractional ideal has an inverse. By Lemma 130, any fractional ideal $\mathfrak{a}$ can be written in the form $\frac{1}{\beta}\mathbf{b}$ where $\beta \in \mathcal{O}_K$ and $\mathbf{b}$ is an ideal of $\mathcal{O}_K$. By the Unique Factorization Theorem and Lemma 142, we know that $\mathbf{b}^{-1}\mathbf{b} = 1$. Let $\mathfrak{c} = \beta \cdot \mathbf{b}^{-1}$. This is a fractional ideal and satisfies $\mathfrak{c}\mathfrak{a} = \mathcal{O}_K$. Thus $\mathfrak{a}$ has an inverse. □

9. To Contain is to Divide II

In Section 7 we defined $\mathfrak{a} \mid \mathbf{b}$ to mean $\mathfrak{a} \supseteq \mathbf{b}$. We are now able to rewrite this in a more natural way.

LEMMA 144. *Let $\mathfrak{a}$, $\mathbf{b}$ be non-zero ideals of $\mathcal{O}_K$. Suppose $\mathfrak{a} \supseteq \mathbf{b}$. Then there is an ideal $\mathfrak{c}$ of $\mathcal{O}_K$ such that $\mathbf{b} = \mathfrak{a}\mathfrak{c}$.*

PROOF. If $\mathfrak{a} \supseteq \mathbf{b}$ then $\mathcal{O}_K \supseteq \mathbf{b}\mathfrak{a}^{-1}$. Thus $\mathbf{b}\mathfrak{a}^{-1}$ is an ideal of $\mathcal{O}_K$ and we simply let $\mathfrak{c} = \mathbf{b}\mathfrak{a}^{-1}$. □

CHAPTER 6

Norms of Ideals

1. Definition of Ideal Norm

Recall that any non-zero ideal $\mathfrak{a}$ has finite index in $\mathcal{O}_K$ (Theorem 121).

DEFINITION. Suppose that $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$. We define the **norm** of the ideal $\mathfrak{a}$ by

$$\mathrm{Norm}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a} = [\mathcal{O}_K^+ : \mathfrak{a}^+].$$

Here $\mathfrak{a}^+$ is simply $\mathfrak{a}$ viewed as an additive group.

2. Multiplicativity of Ideal Norms

LEMMA 145. *Let $\mathfrak{a}$ be a non-zero ideal and $\mathfrak{p}$ a non-zero prime ideal. Then there is some $\alpha \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}$ such that*

$$\mathfrak{a} = \langle \alpha \rangle + \mathfrak{a}\mathfrak{p}.$$

PROOF. We know that $\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}$. Fix $\alpha \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}$. Let $\mathbf{b} = \langle \alpha \rangle + \mathfrak{a}\mathfrak{p}$. Thus we have inclusions

$$\mathfrak{a}\mathfrak{p} \subsetneq \mathbf{b} \subseteq \mathfrak{a}.$$

Multiplying by $\mathfrak{a}^{-1}$ we obtain inclusions

$$\mathfrak{p} \subsetneq \mathbf{b}\mathfrak{a}^{-1} \subseteq \mathcal{O}_K.$$

Thus $\mathbf{b}\mathfrak{a}^{-1}$ is an ideal of $\mathcal{O}_K$ strictly containing the maximal ideal $\mathfrak{p}$ and so $\mathbf{b}\mathfrak{a}^{-1} = \mathcal{O}_K$ so $\mathfrak{a} = \mathbf{b} = \langle \alpha \rangle + \mathfrak{a}\mathfrak{p}$. □

LEMMA 146. *Let $\mathfrak{a}$ be a non-zero ideal and $\mathfrak{p}$ be a non-zero prime ideal. Then*

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

PROOF. By Lemma 145 there is some $\alpha \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}$ such that $\mathfrak{a} = \langle \alpha \rangle + \mathfrak{a}\mathfrak{p}$. Define

$$\phi : \mathcal{O}_K \to \mathfrak{a}/\mathfrak{a}\mathfrak{p}, \qquad x \mapsto \alpha x + \mathfrak{a}\mathfrak{p}.$$

It is easy to see that ϕ is a homomorphism of abelian groups. We will show that

(i) ϕ is surjective.
(ii) $\ker(\phi) = \mathfrak{p}$.

Suppose (i), (ii) for now. By the First Isomorphism Theorem,

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

Thus

$$[\mathcal{O} : \mathfrak{p}] = \#\mathcal{O}_K/\mathfrak{p} = \#\mathfrak{a}/\mathfrak{a}\mathfrak{p} = [\mathfrak{a} : \mathfrak{a}\mathfrak{p}]$$

which is what we want. Now all we need is to show (i), (ii).

For (i), let $\beta \in \mathfrak{a}$. Since $\mathfrak{a} = \alpha\mathcal{O}_K + \mathfrak{a}\mathfrak{p}$ we can write $\beta = \alpha \cdot x + \gamma$ where $x \in \mathcal{O}_K$ and $\gamma \in \mathfrak{a}\mathfrak{p}$. Hence $\phi(x) = \alpha \cdot x + \mathfrak{a}\mathfrak{p} = \beta + \mathfrak{a}\mathfrak{p}$ so ϕ is surjective.

It is clear that $\mathfrak{p} \subseteq \ker(\phi)$. We will show that $\ker(\phi)$ is an ideal of $\mathcal{O}_K$ (the map ϕ is a homomorphism of abelian groups and not of rings, so we cannot immediately conclude that $\ker(\phi)$ is an ideal). Note

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

This is the intersection of a fractional ideal $\alpha^{-1}\mathfrak{a}\mathfrak{p}$ with $\mathcal{O}_K$ and hence is an ideal of $\mathcal{O}_K$. Since this contains $\mathfrak{p}$ and $\mathfrak{p}$ is maximal, we have $\ker(\phi) = \mathfrak{p}$ or $\ker(\phi) = \mathcal{O}_K$. To complete the proof we want to show the former, so suppose the latter. Hence

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

Thus

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

and so

$$\alpha\mathcal{O}_K \subseteq \mathfrak{a}\mathfrak{p}.$$

This contradicts $\alpha \notin \mathfrak{a}\mathfrak{p}$. □

THEOREM 147 (Multiplicativity of Ideal Norms). (i) *Let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *be non-zero prime ideals. Then*

$$\mathrm{Norm}(\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n) = \mathrm{Norm}(\mathfrak{p}_1)\,\mathrm{Norm}(\mathfrak{p}_2) \cdots \mathrm{Norm}(\mathfrak{p}_n).$$

(ii) *Let* $\mathfrak{a}$, $\mathbf{b}$ *be non-zero ideals. Then* $\mathrm{Norm}(\mathfrak{a}\mathbf{b}) = \mathrm{Norm}(\mathfrak{a})\,\mathrm{Norm}(\mathbf{b})$.

PROOF. We prove (i) by induction on n. If $n = 1$ then both sides are $\mathrm{Norm}(\mathfrak{p}_1)$. Suppose $n \geq 2$, and let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1}$. Then

$$\mathfrak{a}\mathfrak{p}_n \subseteq \mathfrak{a} \subseteq \mathcal{O}_K.$$

Thus

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

By Lemma 146 we know that $[\mathfrak{a} : \mathfrak{a}\mathfrak{p}_n] = [\mathcal{O}_K : \mathfrak{p}_n]$. Hence

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

By definition of ideal norm we can rewrite this as

$$\mathrm{Norm}(\mathfrak{a}\mathfrak{p}_n) = \mathrm{Norm}(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{p}_n).$$

Now we simply apply the inductive hypothesis to complete the proof of (i).

Part (ii) follows from (i) and the unique factorization theorem. □

3. Computing Norms

THEOREM 148. *Let K be a number field of degree n and $\mathfrak{a}$ a non-zero ideal of $\mathcal{O}_K$. Then $\mathfrak{a}^+$ is a subgroup of $\mathcal{O}_K^+$ of rank n. Moreover, if $\delta_1, \ldots, \delta_n$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$ and $\omega_1, \ldots, \omega_n$ is an integral basis for $\mathcal{O}_K$ then*

$$\mathrm{Norm}(\mathfrak{a}) = \left| \frac{D(\delta_1, \ldots, \delta_n)}{D(\omega_1, \ldots, \omega_n)} \right|.$$

PROOF. By Theorem 121, the index $[\mathcal{O}_K^+ : \mathfrak{a}^+]$ is finite. Thus $\mathfrak{a}^+$ must have the same rank as $\mathcal{O}_K^+$, which is n. By Theorem 107

$$\Delta(\mathfrak{a}^+) = [\mathcal{O}_K^+ : \mathfrak{a}^+]^2 \cdot \Delta(\mathcal{O}_K^+).$$

The theorem follows as

$$\Delta(\mathfrak{a}^+) = \Delta(\delta_1, \ldots, \delta_n) = D(\delta_1, \ldots, \delta_n)^2$$

and

$$\Delta(\mathcal{O}_K^+) = \Delta(\omega_1, \ldots, \omega_n) = D(\omega_1, \ldots, \omega_n)^2$$

and $[\mathcal{O}_K^+ : \mathfrak{a}^+] = \mathrm{Norm}(\mathfrak{a})$. □

The following theorem allow us to compute norms of principal ideals.

THEOREM 149. *Let $\beta \in \mathcal{O}_K$ be non-zero and $\mathfrak{b} = (\beta)$ be the principal ideal generated by β. Then*

$$\mathrm{Norm}(\mathfrak{b}) = |\mathrm{Norm}_{K/\mathbb{Q}}(\beta)|.$$

PROOF. Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$. As $\mathfrak{b} = (\beta) = \beta\mathcal{O}_K$ it is clear that $\beta\omega_1, \ldots, \beta\omega_n$ is a $\mathbb{Z}$-basis for $\mathfrak{b}^+$. Hence by Theorem 148 we have

$$\mathrm{Norm}(\mathfrak{b}) = \left| \frac{D(\beta\omega_1, \ldots, \beta\omega_n)}{D(\omega_1, \ldots, \omega_n)} \right|.$$

But

$$\begin{aligned}
D(\beta\omega_1, \ldots, \beta\omega_n) &= \begin{vmatrix} \sigma_1(\beta\omega_1) & \sigma_1(\beta\omega_2) & \ldots & \sigma_1(\beta\omega_n) \\ \sigma_2(\beta\omega_1) & \sigma_2(\beta\omega_2) & \ldots & \sigma_2(\beta\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta\omega_1) & \sigma_n(\beta\omega_2) & \ldots & \sigma_n(\beta\omega_n) \end{vmatrix} \\
&= \begin{vmatrix} \sigma_1(\beta)\sigma_1(\omega_1) & \sigma_1(\beta)\sigma_1(\omega_2) & \ldots & \sigma_1(\beta)\sigma_1(\omega_n) \\ \sigma_2(\beta)\sigma_2(\omega_1) & \sigma_2(\beta)\sigma_2(\omega_2) & \ldots & \sigma_2(\beta)\sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta)\sigma_n(\omega_1) & \sigma_n(\beta)\sigma_n(\omega_2) & \ldots & \sigma_n(\beta)\sigma_n(\omega_n) \end{vmatrix} \\
&= \sigma_1(\beta) \cdots \sigma_n(\beta) \cdot \begin{vmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \ldots & \sigma_n(\omega_n) \end{vmatrix} \\
&= \mathrm{Norm}_K(\beta) \cdot D(\omega_1, \ldots, \omega_n)
\end{aligned}$$

where we have used Theorem 64. Thus $\mathrm{Norm}(\mathfrak{b}) = |\mathrm{Norm}_{K/\mathbb{Q}}(\beta)|$. $\square$

EXAMPLE 150. Let's see an example of computing the norm of a non-principal ideal. Let $K = \mathbb{Q}(\sqrt{15})$. As 15 is squarefree and $15 \not\equiv 1 \pmod 4$, an integral basis for $\mathcal{O}_K$ is given by 1, $\sqrt{15}$. Let

$$\mathfrak{a} = \langle 7, 1+\sqrt{15}\rangle = 7\mathcal{O}_K + (1+\sqrt{15})\mathcal{O}_K.$$

Since, as an abelian group,

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{15},$$

we see that $\mathfrak{a}$ is spanned, as an abelian group, by 7, $7\sqrt{15}$, $1+\sqrt{15}$ and $\sqrt{15}\cdot(1+\sqrt{15}) = 15+\sqrt{15}$. We now switch to Algebra I notation. Write $x_1 = 1$ and $x_2 = \sqrt{15}$. Then $\mathcal{O}_K$ is the free abelian group with basis x_1, x_2 and $\mathfrak{a}$ the subgroup spanned by

$$7x_1,\ 7x_2,\ x_1+x_2,\ 15x_1+x_2.$$

Thus

$$\mathcal{O}_K/\mathfrak{a} \cong \langle x_1, x_2 \mid 7x_1,\ 7x_2,\ x_1+x_2,\ 15x_1+x_2\rangle.$$

To compute the quotient we need the Smith Normal Form of the matrix

$$\begin{pmatrix} 7 & 0 & 1 & 15 \\ 0 & 7 & 1 & 11 \end{pmatrix}.$$

This is (exercise)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \end{pmatrix}.$$

Thus

$$\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z}.$$

Hence $\mathrm{Norm}(\mathfrak{a}) = 7$. Now we prove that $\mathfrak{a}$ is not a principal ideal. Suppose it is. Then $\mathfrak{a} = \langle a+b\sqrt{15}\rangle$ where a, $b \in \mathbb{Z}$. Thus

$$7 = \mathrm{Norm}(\mathfrak{a}) = |\mathrm{Norm}(a+b\sqrt{15})| = |a^2 - 15b^2|.$$

Hence $a^2 - 15b^2 = \pm 7$. This means that $a^2 \equiv 2$ or $3 \pmod 5$. However, 2, 3 are non-squares modulo 5. Thus we have reached a contradiction. It follows that $\mathfrak{a}$ is non-principal.

Warning: The above procedure allows us to compute $\mathcal{O}_K/\mathfrak{a}$ *as an abelian group*. It doesn't necessarily tell us what $\mathcal{O}_K/\mathfrak{a}$ is as ring. In the above example we found that $\mathcal{O}_K/\mathfrak{a}$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$ as an abelian group. Any ring that is isomorphic to $\mathbb{Z}/7\mathbb{Z}$ as an abelian group is also isomorphic to $\mathbb{Z}/7\mathbb{Z}$ as a ring. Thus $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{F}_7$ as a ring.

However if we have an ideal $\mathfrak{a}$ (in some ring of integers $\mathcal{O}_K$) such that $\mathcal{O}_K/\mathfrak{a}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as an abelian group, then there are two possibilities for $\mathcal{O}_K/\mathfrak{a}$ as a ring. It could be isomorphic to the ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or to the ring (field in fact) $\mathbb{F}_4$.

EXERCISE 151. Let $f = X^3 + X^2 - 2X + 8$ and let θ be a root of f. Let $K = \mathbb{Q}(\theta)$. In Example 111 we showed that 1, θ, $(\theta^2 + \theta)/2$ is an integral basis for $\mathcal{O}_K$. Let

$$\mathfrak{a} = \langle 5, 1 + \theta \rangle.$$

Compute $\mathrm{Norm}(\mathfrak{a})$.

4. Is this ideal principal?

LEMMA 152. *Let $\mathfrak{a} \subseteq \mathbf{b}$ be non-zero ideals of $\mathcal{O}_K$. Then $\mathfrak{a} = \mathbf{b}$ if and only if* $\mathrm{Norm}(\mathfrak{a}) = \mathrm{Norm}(\mathbf{b})$.

PROOF. If $\mathfrak{a} = \mathbf{b}$ then clearly $\mathrm{Norm}(\mathfrak{a}) = \mathrm{Norm}(\mathbf{b})$. Suppose $\mathrm{Norm}(\mathfrak{a}) = \mathrm{Norm}(\mathbf{b})$. We have inclusions $\mathfrak{a} \subseteq \mathbf{b} \subseteq \mathcal{O}_K$. Thus

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

But $[\mathcal{O}_K : \mathfrak{a}] = \mathrm{Norm}(\mathfrak{a}) = \mathrm{Norm}(\mathbf{b}) = [\mathcal{O}_K : \mathbf{b}]$. Thus $[\mathbf{b} : \mathfrak{a}] = 1$. Hence $\mathfrak{a} = \mathbf{b}$. □

LEMMA 153. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{a}$. Then $\mathfrak{a} = \langle \alpha \rangle$ if and only if* $|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| = \mathrm{Norm}(\mathfrak{a})$.

PROOF. As $\alpha \in \mathfrak{a}$ we know that $\langle \alpha \rangle \subseteq \mathfrak{a}$. By Theorem 149 we have

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

The lemma now follows from Lemma 152.

EXAMPLE 154. Let $K = \mathbb{Q}(\sqrt{15})$. As 15 is squarefree and $\not\equiv 1 \pmod 4$ we know that a $\mathbb{Z}$-basis for $\mathcal{O}_K$ is 1, $\sqrt{15}$. Now consider the ideal $\mathfrak{a} = \langle 17, 7 + \sqrt{15} \rangle$. This has norm 17 (which you can check). Let's show that $\mathfrak{a}$ is non-principal, by contradiction. Suppose it is. Lemma 153 tells us that $17 = |\mathrm{Norm}(\alpha)|$ for some $\alpha \in \mathfrak{a}$. As $\alpha \in \mathcal{O}_K$ we may write $\alpha = x + y\sqrt{15}$ where x, $y \in \mathbb{Z}$. Thus

$$17 = |\mathrm{Norm}(\alpha)| = |x^2 - 15y^2|.$$

Hence

$$x^2 - 15y^2 = \pm 17.$$

We will get a contradiction by showing that this equation has no solutions in $\mathbb{Z}$. Reducing modulo 5 we have $x^2 \equiv \pm 2 \pmod 5$. But 2, 3 are non-squares modulo 5, so we have a contradiction.

□

CHAPTER 7

The Dedekind–Kummer Theorem

1. Motivation

LEMMA 155. *Let K be a number field and let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Let $a = \mathrm{Norm}(\mathfrak{a})$. Then $a \in \mathfrak{a}$.*

PROOF. Recall that, by definition, $a = \mathrm{Norm}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}$. By Lagrange's Theorem, $a \cdot (1 + \mathfrak{a}) = 0 + \mathfrak{a}$ in $\mathcal{O}_K/\mathfrak{a}$. Thus $a \in \mathfrak{a}$. □

This chapter is about practically factoring ideals as products of prime ideals. The motivation is provided by the above lemma. Write $a = \mathrm{Norm}(\mathfrak{a})$ we have a is a positive rational integer contained in $\mathfrak{a}$. Thus $a\mathcal{O}_K \subseteq \mathfrak{a}$, or in other words, $\mathfrak{a}$ divides $a\mathcal{O}_K$. Now at least we can factor a in $\mathbb{Z}$ as a product of rational primes $a = p_1 p_2 \dots p_r$. Thus $\mathfrak{a}$ divides $p_1\mathcal{O}_K \cdot p_2\mathcal{O}_K \cdots p_r\mathcal{O}_K$. So a first step to factoring, we want to factor $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$, for p a rational prime. The Dedekind–Kummer Theorem lets us write $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$. Thus we can factor $a\mathcal{O}_K$ as a product of prime ideals. Next we can try to workout which of these prime ideals are actually factors of $\mathfrak{a}$.

2. Theorem and Examples

THEOREM 156 (Dedekind–Kummer Theorem). *Let p be a rational prime. Let $K = \mathbb{Q}(\theta)$ be a number field where θ is an algebraic integer. Suppose $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let*

$$\mu_\theta(X) \equiv f_1(X)^{e_1} f_2(X)^{e_2} \cdots f_r(X)^{e_r} \pmod{p}$$

where the polynomials $f_i \in \mathbb{Z}[X]$ are monic, irreducible modulo p, and pairwise coprime modulo p. Let $\mathfrak{p}_i = \langle p, f_i(\theta)\rangle$. Then the $\mathfrak{p}_i$ are pairwise distinct prime ideals of $\mathcal{O}_K$ and

$$\langle p\rangle = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}.$$

Moreover, $\mathrm{Norm}(\mathfrak{p}_i) = p^{\deg(f_i)}$.

Let's do some examples of factoring ideals using the Dedekind–Kummer Theorem.

EXAMPLE 157. Let $K = \mathbb{Q}(\sqrt{-30})$. Then $1, \sqrt{-30}$ is an integral basis for $\mathcal{O}_K$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-30}]$. Since the index $[\mathcal{O}_K : \mathbb{Z}[\sqrt{-30}]] = 1$, we can factor $p\mathcal{O}_K$ for any prime p using the Dedekind–Kummer Theorem.

The minimal polynomial for $\sqrt{-30}$ is $\mu = X^2 + 30$. Let's factor $p\mathcal{O}_K$ for primes $p \leq 11$.

Note that

$$X^2 + 30 \equiv X^2 \pmod 2.$$

Thus $2\mathcal{O}_K = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = \langle 2, \sqrt{-30}\rangle$. Similarly $3\mathcal{O}_K = \mathfrak{p}_3^2$ where $\mathfrak{p}_3 = \langle 3, \sqrt{-30}\rangle$, and $5\mathcal{O}_K = \mathfrak{p}_5^2$ where $\mathfrak{p}_5 = \langle 5, \sqrt{-30}\rangle$.

Now

$$X^2 + 30 \equiv X^2 - 5 \pmod 7$$

is irreducible modulo 7 (all we have to do is check that $0, 1, \ldots, 6$ are not roots modulo 7, or we can use quadratic reciprocity which is quicker). Thus $7\mathcal{O}_K = \mathfrak{p}_7$ is a prime ideal.

Finally

$$X^2 + 30 \equiv (X + 5)(X + 6) \pmod{11}.$$

Hence $11\mathcal{O}_K = \mathfrak{p}_{11} \cdot \mathfrak{p}'_{11}$ where

$$\mathfrak{p}_{11} = \langle 11, \sqrt{-30} + 5\rangle, \qquad \mathfrak{p}'_{11} = \langle 11, \sqrt{-30} + 6\rangle.$$

You might wander whether the ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{11}$, $\mathfrak{p}'_{11}$ are principal or not. In fact $\mathfrak{p}_7 = 7\mathcal{O}_K$ so it is principal. Let's consider the others. We know that if an ideal $\mathfrak{a}$ is principal, say $\mathfrak{a} = \langle\alpha\rangle$ then $\mathrm{Norm}(\mathfrak{a}) = |\mathrm{Norm}(\alpha)|$. This often gives us an easy way of showing that an ideal is non-principal, or of searching for a generator if we suspect the ideal is principal. By the last part of the Dedekind–Kummer Theorem, $\mathrm{Norm}(\mathfrak{p}_2) = 2^{\deg(X)} = 2$. Now if $\mathfrak{p} = \langle\alpha\rangle$ then we can write $\alpha = x + y\sqrt{-30}$ (with x, y integers) and so $|\mathrm{Norm}(\alpha)| = x^2 + 30y^2$. Since $x^2 + 30y^2 = \pm 2$ has no solutions in integers we have a contradiction and so $\mathfrak{p}_2$ is non-principal. The same applies for $\mathfrak{p}_3$, $\mathfrak{p}_5$.

What about $\mathfrak{p}_{11}$, $\mathfrak{p}'_{11}$? Again by the last part of the Dedekind–Kummer Theorem,

$$\mathrm{Norm}(\mathfrak{p}_{11}) = \mathrm{Norm}(\mathfrak{p}'_{11}) = 11.$$

But the equation $x^2 + 30y^2 = \pm 11$ has no solutions in integers. Therefore $\mathfrak{p}_{11}$, $\mathfrak{p}'_{11}$ are non-principal.

Example 158. Let $K = \mathbb{Q}(\sqrt{17})$. As $17 \equiv 1 \pmod 4$ we know that an integral basis is $1, \theta$ with $\theta = (1 + \sqrt{17})/2$. Thus $\mathcal{O}_K = \mathbb{Z}[\theta]$. The generator θ has minimal polynomial $\mu = X^2 - X - 4$. Let's factor $2\mathcal{O}_K$. Here

$$\mu \equiv X^2 - X = X(X - 1) \pmod 2.$$

Thus $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}'_2$ where $\mathfrak{p}_2 = \langle 2, \theta\rangle$ and $\mathfrak{p}'_2 = \langle 2, \theta - 1\rangle$. Note that these are distinct prime ideals; the Dedekind–Kummer Theorm already tells us that. But we can also check that by hand: if $\mathfrak{p}_2 = \mathfrak{p}'_2$ then θ, $\theta - 1 \in \mathfrak{p}_2$, so $1 \in \mathfrak{p}_2$, so $\mathfrak{p}_2 = \mathcal{O}_K$ giving us a contradiction (prime ideals are proper!). Thus $\mathfrak{p}_2 \neq \mathfrak{p}'_2$.

The assumption $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ in the Dedekind–Kummer Theorem is important. If we take $\phi = \sqrt{17}$ then $[\mathcal{O}_K : \mathbb{Z}[\phi]] = 2$. So factoring

$X^2 - 17$ (the minimal polynomial for ϕ) modulo 2 will not necessarily give us the correct factorization of $2\mathcal{O}_K$. Indeed, $X^2 - 17 \equiv (X-1)^2 \pmod 2$, suggesting that $2\mathcal{O}_K$ is the square of a prime ideal, which it is not. However, if p is an odd prime, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\phi]]$ and so we'll obtain the correct answer from factoring $X^2 - 17$ modulo p.

EXAMPLE 159. Let $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt[3]{6}$. You can check that 1, θ, θ^2 is an integral basis for $\mathcal{O}_K$ and thus $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let's factor $5\mathcal{O}_K$. The minimal polynomial for θ is $\mu = X^3 - 6$.

To factor $5\mathcal{O}_K$ note that

$$\mu \equiv X^3 - 1 = (X-1)(X^2 + X + 1) \pmod 5.$$

where the two factors are irreducible. Hence the ideals

$$\mathfrak{p} = \langle 5, \sqrt[3]{6} - 1\rangle, \qquad \mathfrak{q} = \langle 5, 1 + \sqrt[3]{6} + \sqrt[3]{6}^2\rangle$$

are prime, and they have norms $\mathrm{Norm}(\mathfrak{p}) = 5^{\deg(X-1)} = 5$ and $\mathrm{Norm}(\mathfrak{q}) = 5^{\deg(X^2+X+1)} = 25$. Moreover,

$$5\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{q}.$$

Let's show that $\mathfrak{p}$ and $\mathfrak{q}$ are principal. To do this for $\mathfrak{p}$ all we have to do is find an element in $\mathfrak{p}$ that has norm 5. However $\sqrt[3]{6} - 1$ is in $\mathfrak{p}$ and

$$\mathrm{Norm}(\sqrt[3]{6} - 1) = (\sqrt[3]{6} - 1)(\zeta\sqrt[3]{6} - 1)(\zeta^2\sqrt[3]{6} - 1) = 6 - 1 = 5,$$

where $\zeta = \exp(2\pi i/3)$. Thus $\mathfrak{p} = (\sqrt[3]{6} - 1)\mathcal{O}_K$ is principal. What about $\mathfrak{q}$? The easiest way to check that this is principal is to note that

$$5\mathcal{O}_K = (\sqrt[3]{6} - 1)\mathcal{O}_K \cdot \mathfrak{q}$$

thus

$$\mathfrak{q} = \left(5/(\sqrt[3]{6} - 1)\right) \cdot \mathcal{O}_K.$$

Now

$$5/(\sqrt[3]{6} - 1) = (\zeta\sqrt[3]{6} - 1)(\zeta^2\sqrt[3]{6} - 1) = \sqrt[3]{6}^2 + \sqrt[3]{6} + 1.$$

Thus

$$\mathfrak{q} = \langle \sqrt[3]{6}^2 + \sqrt[3]{6} + 1\rangle.$$

Next let's factor $2\mathcal{O}_K$ and $3\mathcal{O}_K$ and show that the factors are principal. Dedekind–Kummer tells us that

$$2\mathcal{O}_K = \mathfrak{r}^3, \qquad 3\mathcal{O}_K = \mathfrak{s}^3$$

where

$$\mathfrak{r} = \langle 2, \sqrt[3]{6}\rangle, \qquad \mathfrak{s} = \langle 3, \sqrt[3]{6}\rangle,$$

are prime ideals having norms 2, 3 respectively. Observe that $2 - \sqrt[3]{6} \in \mathfrak{r}$ and has norm

$$\mathrm{Norm}(2 - \sqrt[3]{6}) = (2 - \sqrt[3]{6})(2 - \zeta\sqrt[3]{6})(2 - \zeta^2\sqrt[3]{6}) = 8 - 6 = 2.$$

Thus

$$\mathfrak{r} = (2 - \sqrt[3]{6})\mathcal{O}_K.$$

Now to check that $\mathfrak{s}$ is principal we can use a trick. Note that

$$(\sqrt[3]{6}\mathcal{O}_K)^3 = 6\mathcal{O}_K = 2\mathcal{O}_K \cdot 3\mathcal{O}_K = \mathfrak{r}^3 \cdot \mathfrak{s}^3.$$

Hence (by unique factorization)

$$\sqrt[3]{6}\mathcal{O}_K = \mathfrak{rs}.$$

Thus

$$\mathfrak{s} = \left(\sqrt[3]{6}/(2 - \sqrt[3]{6})\right) \cdot \mathcal{O}_K = (3 + 2\sqrt[3]{6} + \sqrt[3]{6}^2) \cdot \mathcal{O}_K.$$

How did we do the division $\sqrt[3]{6}/(2 - \sqrt[3]{6})$? If you don't know how to do this see Homework Assignment 1, Question 11.

3. Proof of the Dedekind–Kummer Theorem

We follow the notation of the theorem.

LEMMA 160. *Let*

$$I = p\mathbb{Z}[X] + f_i\mathbb{Z}[X].$$

Then

$$\mathbb{Z}[X]/I \cong \mathbb{F}_p[X]/\langle \overline{f_i} \rangle,$$

where $\overline{f_i}$ denotes the image of f_i in $\mathbb{F}_p[X]$ (i.e. the polynomial you obtain by reducing the coefficents of f_i modulo p). In particular $\mathbb{Z}[X]/I$ is a field of size $p^{\deg(f_i)}$.

PROOF. Let

$$\phi : \mathbb{Z}[X] \to \mathbb{F}_p[X]/\langle \overline{f_i} \rangle, \qquad g \mapsto \overline{g} + \langle \overline{f_i} \rangle.$$

This is clearly a surjective ring homomorphism. More $g \in \ker(\phi)$ if and only if $\overline{f_i} \mid \overline{g}$, which is equivalent to $g = h_1 f_i + p h_2$ for h_1, $h_2 \in \mathbb{Z}[X]$. Thus $\ker(\phi) = I$. The isomorphism in the lemma follows from the First Isomorphism Theorem.

Now consider the quotient $\mathbb{F}_p[X]/\langle \overline{f_i} \rangle$. Since $\overline{f_i}$ is irreducible, this quotient is a field extension of $\mathbb{F}_p$ of degree $\deg(f_i)$ and hence has cardinality

$$\#\mathbb{F}_p[X]/\langle \overline{f_i} \rangle = p^{\deg(f_i)}.$$

□

LEMMA 161. *Let*

$$J = p\mathbb{Z}[\theta] + f_i(\theta)\mathbb{Z}[\theta].$$

Then

$$\mathbb{Z}[\theta]/J \cong \mathbb{F}_p[X]/\langle \overline{f_i} \rangle.$$

In particular $\mathbb{Z}[\theta]/J$ is a field of size $p^{\deg(f_i)}$.

PROOF. In view of Lemma 160, all we have to do is establish an isomorphism of rings $\mathbb{Z}[X]/I \cong \mathbb{Z}[\theta]/J$. Now let

$$\psi : \mathbb{Z}[X] \to \mathbb{Z}[\theta]/J, \qquad g \mapsto g(\theta) + J.$$

This is clearly a surjective ring homomorphism. All we need to do is show that the kernel is I. Observe $g \in \ker(\psi)$ iff $g(\theta) \in J$ iff $g(\theta) = ph_1(\theta) + h_2(\theta)f_i(\theta)$ for some h_1, $h_2 \in \mathbb{Z}[X]$. But this is equivalent to $g - ph_1 - h_2 f_i$ being a multiple of $\mu(X)$ (the minimal polynomial of θ. Hence

$$\ker(\psi) = p\mathbb{Z}[X] + f_i\mathbb{Z}[X] + \mu\mathbb{Z}[X].$$

Clearly $I \subseteq \ker(\psi)$. To show equality we need to show that $\mu \in I$. But $\overline{f_i}$ is a factor of $\overline{\mu}$. Thus $\mu = h_3 f_i + ph_4$ for some h_3, $h_4 \in \mathbb{Z}[X]$. Thus $\mu \in I$ and so $\ker(\psi) = I$ as required. □

LEMMA 162. *$\mathfrak{p}_i$ is a prime ideal and* $\mathrm{Norm}(\mathfrak{p}_i) = p^{\deg(f_i)}$.

PROOF. We will show that $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}[\theta]/J$. In view of Lemma 161 we know $\mathcal{O}_K/\mathfrak{p}_i$ is a field and so $\mathfrak{p}_i$ is prime; moreover $\mathrm{Norm}(\mathfrak{p}_i) = \#\mathcal{O}_K/\mathfrak{p}_i = \#\mathbb{Z}[\theta]/J = p^{\deg(f_i)}$.

Let

$$\xi : \mathbb{Z}[\theta]/J \to \mathcal{O}_K/\mathfrak{p}_i, \qquad g(\theta) + J \mapsto g(\theta) + \mathfrak{p}_i.$$

We need to show that ξ is well-defined. But this follows as $J \subseteq \mathfrak{p}_i$, and thus if $g_1(\theta) + J = g_2(\theta) + J$ then $g_1(\theta) - g_2(\theta) \in J \subseteq \mathfrak{p}_i$, and so $g_1(\theta) + \mathfrak{p}_i = g_2(\theta) + \mathfrak{p}_i$. Hence ξ is well-defined and clearly a homomorphism of rings. Next we show that ξ is surjective. This is the only place we use the hypothesis $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let $m = [\mathcal{O}_K : \mathbb{Z}[\theta]]$. Then there are a, $b \in \mathbb{Z}$ such that $am + bp = 1$. Let $\alpha \in \mathcal{O}_K$. Then

$$\alpha + J = (am + bp)\alpha + J = am\alpha + J$$

as $p \in J$. But $am\alpha = m(a\alpha) \in m\mathcal{O}_K \subseteq \mathbb{Z}[\theta]$. Thus $\alpha + J$ is in the image of ξ. Hence ξ is surjective. Finally as $\mathbb{Z}[\theta]/J$ is a field, ξ is injective. Thus ξ is an isomorphism. □

LEMMA 163. *The ideals $\mathfrak{p}_i$ are pairwise distinct.*

PROOF. Suppose $\mathfrak{p}_1 = \mathfrak{p}_2$. Then $\mathfrak{p}_1$ contains p, $f_1(\theta)$, $f_2(\theta)$. Now $\overline{f}_1$, $\overline{f}_2$ are coprime in $\mathbb{F}_p[X]$. Thus there polynomials g_1, $g_2 \in \mathbb{Z}[X]$ such that

$$\overline{g_1}(X)\overline{f}_1(X) + \overline{g_2}(X)\overline{f}_2(X) = \overline{1}.$$

Thus

$$g_1(X)f_1(X) + g_2(X)f_2(X) = 1 + ph(X)$$

where $h \in \mathbb{Z}[X]$. Thus

$$1 = g_1(\theta)f_1(\theta) + g_2(\theta)f_2(\theta) - ph(\theta) \in \mathfrak{p}_1.$$

But $\mathfrak{p}_1$ is a prime ideal and therefore proper, giving a contradiction. □

LEMMA 164. *Let g, $h \in \mathbb{Z}[X]$ be monic polynomials. Then*

$$\langle p, g(\theta)\rangle \cdot \langle p, h(\theta)\rangle \subseteq \langle p, g(\theta)h(\theta)\rangle.$$

PROOF. The ideal $\langle p, g(\theta)\rangle \cdot \langle p, h(\theta)\rangle$ is generated by p^2, $ph(\theta)$, $pg(\theta)$ and $g(\theta)h(\theta)$. But these are all contained in the ideal $\langle p, g(\theta)h(\theta)\rangle$. □

PROOF OF DEDEKIND–KUMMER. Let

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

By Lemma 164, we have

$$\mathfrak{a} = \prod_{i=1}^{r} \langle p, f_i(\theta)\rangle^{e_i} \subseteq \langle p, \prod f_i(\theta)^{e_i}\rangle.$$

However

$$\prod f_i(X)^{e_i} = \mu_\theta(X) + pg(X)$$

for some polynomial $g \in \mathbb{Z}[X]$. Substituting θ and recalling that $\mu_\theta(\theta) = 0$

$$\prod f_i(\theta)^{e_i} = pg(\theta).$$

Thus

$$\mathfrak{a} \subseteq \langle p\rangle.$$

However,

$$\mathrm{Norm}(\mathfrak{a}) = \prod_{i=1}^{r} \mathrm{Norm}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{r} p^{e_i \cdot \deg(f_i)} = p^{\sum_{i=1}^{r} e_i \cdot \deg(f_i)} = p^n$$

where $n = \deg(\mu_\theta) = [K : \mathbb{Q}]$. Moreover,

$$\mathrm{Norm}(\langle p\rangle) = |\mathrm{Norm}_{K/\mathbb{Q}}(p)| = p^n.$$

Since $\mathfrak{a}$ and $\langle p\rangle$ have the same norm and $\mathfrak{a} \subseteq \langle p\rangle$ we conclude that they're equal. □

CHAPTER 8

The Class Group

1. Ideal Classes

DEFINITION. Let K be a number field. We know that non-zero fractional ideals of $\mathcal{O}_K$ form an abelian group under multiplication which we denote by I_K. It is easy to see that the non-zero principal fractional ideals form a subgroup which we denote by P_K. The **class group** is defined as the quotient

$$\mathrm{Cl}(K) = I_K/P_K.$$

If $\mathfrak{a}$ is a non-zero fractional ideal, we denote its class in $\mathrm{Cl}(K)$ by $[\mathfrak{a}]$ (thus $[\mathfrak{a}]$ is simply the coset $\mathfrak{a}P_K$). Note that two ideals $\mathfrak{a}$, $\mathbf{b}$ have the same class if and only if the fractional ideal $\mathfrak{a}\mathbf{b}^{-1}$ is principal. This is equivalent to $\mathfrak{a} = \gamma\mathbf{b}$ for some $\gamma \in K$.

THEOREM 165. *$\mathcal{O}_K$ is a UFD if and only if $\mathrm{Cl}(K)$ is trivial.*

PROOF. If $\mathrm{Cl}(K)$ is trivial then every ideal is principal, and so $\mathcal{O}_K$ is a PID. Thus $\mathcal{O}_K$ is a UFD.

Conversely, suppose $\mathcal{O}_K$ is a UFD. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$ and let α be a non-zero element of $\mathfrak{a}$. As $\mathcal{O}_K$ is a UFD, there are irreducible elements $\pi_1, \ldots, \pi_r$ of $\mathcal{O}_K$ such that

$$\alpha = \pi_1\pi_2\cdots\pi_r.$$

Let $\mathfrak{p}_i = \langle\pi_i\rangle$. It follows that the ideals $\mathfrak{p}_i$ are prime ideals (exercise). Now

$$\mathfrak{a} \supseteq \langle\alpha\rangle = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r.$$

Thus $\mathfrak{a}$ divides $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$. Without loss of generality (by Lemma 144),

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$$

for some $s \leq r$. But the $\mathfrak{p}_i$ are principal so $\mathfrak{a}$ is principal. Thus $\mathcal{O}_K$ is a PID. It follows that $\mathrm{Cl}(K)$ is trivial. □

The above illustrates the fact that the class group measures the failure of unique factorization.

2. Minkowski's Theorem

THEOREM 166. *(Minkowski) Let K be a number field of degree n and signature (r, s). Let*

$$B_K = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\Delta_K|}.$$

Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a non-zero element α such that $|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leq B_K \cdot \mathrm{Norm}(\mathfrak{a})$.

Minkowski's Theorem is proved using the geometry of numbers. The constant B_K is called the **Minkowski Bound**.

To prove Minkowski's Theorem 166 you need another theorem of Minkowski! This one is from the Geometry of Numbers, and was proved in MA257.

THEOREM 167. *(Minkowski's Theorem for Lattices) Let S be a compact, convex, symmetric subset of $\mathbb{R}^n$. Let L be a lattice in $\mathbb{Z}^n$ of index m. Suppose*

$$2^n m \leq \mathrm{Volume}(S).$$

Then S contains a non-zero element of L.

PROOF OF THEOREM 166. The proof is not hard, but it's best to understand it in small dimension first, and then prove it full generality. So we'll only do the proof for imaginary quadratic fields and if you're interested you can look up the general proof.

Let K be an imaginary quadratic field. In particular K has degree $n = 2$, and signature $(r, s) = (0, 1)$. Thus $B_K = (2/\pi) \cdot \sqrt{|\Delta_K|}$.

We're given that $\mathfrak{a}$ is a non-zero ideal. Thus $\mathfrak{a}$ has a $\mathbb{Z}$-basis consisting of two algebraic integers which we'll call ω_1, ω_2. We want to show the existence of some non-zero $\alpha \in \mathfrak{a}$ such that

$$|\mathrm{Norm}(\alpha)| \leq \frac{2}{\pi} \cdot \sqrt{|\Delta_K|} \cdot \mathrm{Norm}(\mathfrak{a}). \tag{14}$$

Write $\alpha = x\omega_1 + y\omega_2$ with x, $y \in \mathbb{Z}$. To simplify things (remembering that we're in a complex quadratic field) write [1]

$$\omega_1 = a + bi, \qquad \omega_2 = c + di, \qquad a, b, c, d \in \mathbb{R}.$$

The field has the form $K = \mathbb{Q}(\sqrt{-D})$ where $D > 0$. It has two embeddings σ_1, σ_2 which respecively send $u + v\sqrt{-D}$ to $u + v\sqrt{-D}$ and $u - v\sqrt{-D}$ (for any u, $v \in \mathbb{Q}$). Note that the first is just the identity and the second is complex conjugation. Hence

$$\begin{aligned}
\mathrm{Norm}(\alpha) &= (x\omega_1 + y\omega_2)\overline{(x\omega_1 + y\omega_2)} \\
&= ((ax + cy) + i(bx + dy))((ax + cy) - i(bx + dy)) \\
&= (ax + cy)^2 + (bx + dy)^2.
\end{aligned}$$

[1] a, b, c, d don't have to be rationals. For example in $K = \mathbb{Q}(\sqrt{-2})$ with $\omega_1 = 1 + \sqrt{-2}$ we take $a = 1$, $b = \sqrt{2}$.

Hence we can rewrite (14) as

$$(ax+cy)^2+(bx+dy)^2 < \frac{2}{\pi}\cdot\sqrt{|\Delta_K|}\cdot \mathrm{Norm}(\mathfrak{a}). \tag{15}$$

Now recall that $\Delta(\mathfrak{a}) = \Delta(\mathcal{O}_K)\cdot[\mathcal{O}_K : \mathfrak{a}]^2$. But $\Delta(\mathcal{O}_K) = \Delta_K$ and $[\mathcal{O}_K : \mathfrak{a}] = \mathrm{Norm}(\mathfrak{a})$. Hence

$$\begin{aligned}\sqrt{|\Delta_K|}\cdot\mathrm{Norm}(\mathfrak{a}) &= \sqrt{|\Delta(\mathfrak{a})|}\\ &= |D(\mathfrak{a})|,\end{aligned}$$

where $D(\mathfrak{a})$ is the determinant

$$D(\mathfrak{a}) = D(\omega_1,\omega_2) = \begin{vmatrix}\omega_1 & \omega_2\\ \overline{\omega_1} & \overline{\omega_2}\end{vmatrix} = 2i(ad-bc).$$

Hence we may rewrite (15) as

$$(ax+cy)^2+(bx+dy)^2 < \frac{4}{\pi}\cdot|ad-bc|.$$

All we need to show is there are $x, y \in \mathbb{Z}$, not both zero, such that this inequality is satisfied. Let

$$S = \left\{\begin{pmatrix}x\\y\end{pmatrix}\in\mathbb{R}^2 \;:\; (ax+cy)^2+(bx+dy)^2 \le \frac{4}{\pi}\cdot|ad-bc|\right\}.$$

We will take $L = \mathbb{Z}^2$. Thus the index $m = [\mathbb{Z}^2 : L] = 1$. All we have to do is show that there is a non-zero vector in S belonging to $\mathbb{Z}^2 = L$. It is here that we need Minkowski's Theorem on lattices. All we have to do is show that S is convex, compact and has volume ≥ 4 (clearly S is symmetric). Define

$$T \;:\; \mathbb{R}^2\to\mathbb{R}^2, \qquad \begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}z\\w\end{pmatrix} = \begin{pmatrix}ax+cy\\bx+dy\end{pmatrix}.$$

Then T is a linear transformation. It has determinant $ad-bc$. We know that this is non-zero since $\Delta(\mathfrak{a}) = -4(ad-bc)^2$. Thus T is an invertible linear transformation (and in particular a homeomorphism). Moreover,

$$T(S) = \left\{\begin{pmatrix}z\\w\end{pmatrix}\in\mathbb{R}^2 \;:\; z^2+w^2 \le \frac{4}{\pi}\cdot|ad-bc|\right\}.$$

This is a closed circle and hence compact and convex. As T^{-1} is a linear map, it preserves line segments, so S is convex. Moreover, as it is a homeomorphism, S is compact. We merely have to check that $\mathrm{Volume}(S) \ge 4$. Note that

$$\iint_{T(S)} 1\,dzdw = \mathrm{Volume}(T(S)) = 4\cdot|ad-bc|.$$

The Jacobian of the transformation T is $ad-bc$. Thus

$$4\cdot|ad-bc| = \iint_{T(S)} 1\,dzdw = \iint_S |ad-bc|\,dxdy.$$

We deduce that

$$\text{Volume}(S) = \iint_S 1 dx dy = 4.$$

□

3. Finiteness of the Class Group

THEOREM 168. *Let K be a number field of degree n and signature (r, s).*

(I) $\text{Cl}(K)$ *is finite.*
(II) $\text{Cl}(K)$ *is generated by the set of classes*

$$\{[\mathfrak{p}] \ : \ \mathfrak{p} \text{ is a prime ideal, } \text{Norm}(\mathfrak{p}) \leq B_K\}. \tag{16}$$

We define the **class number of** K as $h_K = \#\,\text{Cl}(K)$. Part (I) of the theorem tells us that $h_K < \infty$.

Before proving Theorem 168 we need the following lemma.

LEMMA 169. *Let $B > 0$. The number of ideals of $\mathcal{O}_K$ of norm $\leq B$ is finite.*

PROOF. The norm of an ideal is a positive integer. Thus it is enough to show, for each integer A in the range $1 \leq A \leq B$, that the number of ideals $\mathfrak{a}$ of norm A is finite. Suppose $\text{Norm}(\mathfrak{a}) = A$. Then $A = \#\mathcal{O}_K/\mathfrak{a}$. By Lagrange $A \cdot (1 + \mathfrak{a}) = 0 + \mathfrak{a}$. Hence $A \in \mathfrak{a}$. Thus $\langle A \rangle \subseteq \mathfrak{a}$ we means $\mathfrak{a} \mid \langle A \rangle$. By unique factorisation and Lemma 144 there are only finitely many possibilities for $\mathfrak{a}$. □

PROOF OF THEOREM 168. Let $\mathbf{b}$ be a non-zero fractional ideal of $\mathcal{O}_K$. Then $\mathbf{b} = \frac{1}{\beta}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and $\beta \in \mathcal{O}_K$. Hence $[\mathbf{b}] = [\mathfrak{a}]$. By Minkowski's Theorem, there is a non-zero $\alpha \in \mathfrak{a}$ such that $|\text{Norm}(\alpha)| \leq B_K \cdot \text{Norm}(\mathfrak{a})$.

However $\langle \alpha \rangle \subseteq \mathfrak{a}$ thus $\mathfrak{a} \mid \langle \alpha \rangle$. Hence we can write $\langle \alpha \rangle = \mathfrak{a}\mathfrak{c}$ for some ideal $\mathfrak{c}$ of $\mathcal{O}_K$. Moreover, by the multiplicativity of norms

$$\text{Norm}(\mathfrak{c}) = \text{Norm}(\langle \alpha \rangle)/\,\text{Norm}(\mathfrak{a}) = |\text{Norm}(\alpha)|/\,\text{Norm}(\mathfrak{a}) \leq B_K.$$

Moreover $[\mathfrak{c}] \cdot [\mathfrak{a}] = [\langle 1 \rangle]$. Thus $[\mathbf{b}] = [\mathfrak{a}] = [\mathfrak{c}]^{-1}$. Hence

$$\text{Cl}(K) = \{[\mathfrak{c}]^{-1} \ : \ \mathfrak{c} \text{ is an ideal of } \mathcal{O}_K \text{ of norm} \leq B_K\}.$$

As there are only finitely many ideals of a given norm, this proves (I).

Now, $\mathfrak{c} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ where the $\mathfrak{p}_i$ are prime ideals. Moreover $\text{Norm}(\mathfrak{p}_i) \mid \text{Norm}(\mathfrak{c})$, so $\text{Norm}(\mathfrak{p}_i) \leq B_K$ and

$$[\mathfrak{c}]^{-1} = [\mathfrak{p}_1]^{-1} \cdots [\mathfrak{p}_r]^{-1}.$$

Thus the set (16) generates $\text{Cl}(K)$. □

4. Examples of Computing Class Groups

LEMMA 170. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then there is a unique rational prime p such that $\mathfrak{p} \mid p\mathcal{O}_K$. Moreover,* $\mathrm{Norm}(\mathfrak{p}) = p^f$ *for some positive integer f.*

We call p the prime **below** $\mathfrak{p}$. We say that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ **above** p. We call f the **degree** of p.

PROOF. As $\mathfrak{p}$ is a maximal ideal, we know that $\mathcal{O}_K/\mathfrak{p}$ is a finite field, say $\mathbb{F}_q$. From Algebra II we know $q = p^f$ for some rational prime p and positive integer f. Hence $\mathrm{Norm}(\mathfrak{p}) = \#\mathbb{F}_q = q = p^f$.

Now we make use of the fact that $\mathrm{Norm}(\mathfrak{p}) \in \mathfrak{p}$ (Lemma 155). Thus $p^f \in \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal, $p \in \mathfrak{p}$. Thus $p\mathcal{O}_K \subseteq \mathfrak{p}$ and so $\mathfrak{p} \mid p\mathcal{O}_K$.

All that is left if the proof of uniqueness. Suppose p_1, p_2 are distinct rational primes such that $\mathfrak{p} \mid p_i\mathcal{O}_K$. Then p_1, $p_2 \in \mathfrak{p}$. By Euclid (or Bezout as some call it), there are a, $b \in \mathbb{Z}$ such that $ap_1 + bp_2 = 1$. Thus $1 \in \mathfrak{p}$ contradicting the fact that prime ideals are proper, and therefore proving uniqueness. □

Note: Because of this lemma, to compute the set of classes (16), we merely have to list the rational primes $p \leq B_K$, factor each $p\mathcal{O}_K$ (using Dedekind–Kummer), and keep only those prime ideal factors whose norm is at most B_K.

EXAMPLE 171. We compute the class group for $K = \mathbb{Q}(i)$. Then $\mathcal{O}_K = \mathbb{Z}[i]$, $\Delta_K = -4$, $n = 2$ and $(r, s) = (0, 1)$. Thus the Minkowski bound is $B_K = (2!/2^2) \cdot (4/\pi)^1 \cdot \sqrt{4} = 4/\pi < 2$. We need to factor $p\mathcal{O}_K$ for rational prime $p < 2$. There are no such primes. Thus $\mathrm{Cl}(K)$ is generated by the empty set of ideal classes, and so $\mathrm{Cl}(K) = \{1\}$ (thus $h_K = 1$). This tells us that $\mathcal{O}_K$ is a PID.

Now let's see an application of this. Let $p \equiv 1 \pmod 4$ be a prime. Quadratic reciprocity tells us that -1 is a quadratic residue modulo p. Hence the minimal polynomial $\mu = X^2 + 1$ for i factors as a product of two linear factors modulo p. By the Dedekind–Kummer Theorem, $\langle p \rangle = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$, $\mathfrak{p}'$ are prime ideals with $\mathrm{Norm}(\mathfrak{p}) = \mathrm{Norm}(\mathfrak{p}') = p$. But as $\mathcal{O}_K$ is a PID, we can write $\mathfrak{p} = \langle x + iy \rangle$ where x, $y \in \mathbb{Z}$. Therefore

$$p = \mathrm{Norm}(\mathfrak{p}) = |x^2 + y^2| = x^2 + y^2$$

and we recover the familiar fact from Introduction to Number Theorem: any prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

EXAMPLE 172. We compute the class group for $K = \mathbb{Q}(\sqrt{7})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$, $\Delta_K = 28$, $n = 2$ and $(r, s) = (2, 0)$. Thus the Minkowski bound is $B_K = (2!/2^2) \cdot (4/\pi)^0 \cdot \sqrt{28} = \sqrt{7} < 3$. The only rational prime $p \leq B_K$ is $p = 2$. We factor the ideal $\langle 2 \rangle$ using Dedekind–Kummer. We have

$$X^2 - 7 \equiv (X - 1)^2 \pmod 2.$$

Thus $\langle 2\rangle = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = \langle 2, \sqrt{7}-1\rangle$. The prime ideal $\mathfrak{p}_2$ has norm $2 \leq B_K$. Thus $\mathrm{Cl}(K)$ is generated by $\{[\mathfrak{p}]\}$. We note that $\mathfrak{p}$ contains the element $3+\sqrt{7} = 2\times 2 + (\sqrt{7}-1)$ of norm $9-7=2$. Thus $\mathfrak{p}_2 = \langle 3+\sqrt{7}\rangle$. So $[\mathfrak{p}_2] = 1$ (the trivial ideal class). Thus $\mathrm{Cl}(K) = \{1\}$ and so $h_K = 1$.

Example 173. We compute the class group of $K = \mathbb{Q}(\sqrt{-30})$. As -30 is squarefree, $\not\equiv 1 \pmod 4$ we know that 1, $\theta = \sqrt{-30}$ is an integral basis. In particular $\mathcal{O}_K = \mathbb{Z}[\theta]$ so $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$. Moreover θ has minimal polynomial $\mu = X^2 + 30$. Now $\Delta_K = -120$, $n = 2$, $(r,s) = (0,1)$. Thus

$$B_K = \frac{2!}{2^2}\cdot(4/\pi)^1 \cdot \sqrt{120} = 6.97\ldots.$$

Thus $\mathrm{Cl}(K)$ is generated by

$$\{[\mathfrak{p}] \ : \ \mathfrak{p} \text{ is a prime ideal, } \mathrm{Norm}(\mathfrak{p}) \leq B_K\}.$$

But $\mathrm{Norm}(\mathfrak{p}) = p^d$ for some rational prime p and some $d \geq 1$. Thus we need to factor the primes $p \leq B_K$, i.e. $p = 2,\ 3,\ 5$. However $\mu \equiv X^2 \pmod p$ for any of these 3 primes. By the Dedekind–Kummer Theorem the ideals

$$\mathfrak{p}_2 = \langle 2, \theta\rangle, \qquad \mathfrak{p}_3 = \langle 3, \theta\rangle, \qquad \mathfrak{p}_5 = \langle 5, \theta\rangle$$

are prime and $\langle p\rangle = \mathfrak{p}_p^2$ for $p = 2,\ 3,\ 5$. Thus these classes have order dividing 2 in $\mathrm{Cl}(K)$. Moreover $\mathrm{Norm}(\mathfrak{p}_2) = 2^{\deg(X)} = 2$. If $\mathfrak{p}_2$ is principal then $\mathfrak{p}_2 = \langle x + y\theta\rangle$ some integers x, y and then $|x^2 + 30y^2| = \mathrm{Norm}(\mathfrak{p}_2) = 2$ which is impossible. Thus $\mathfrak{p}_2$ is not principal. Likewise $\mathfrak{p}_3$, $\mathfrak{p}_5$ are not principal as the equations $|x^2 + 30y^2| = 3,\ 5$ have no solutions. Thus $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$ all have order 2. Also $\mathfrak{p}_2\mathfrak{p}_3$ is non-principal as it has norm 6, and the equation $|x^2 + 30y^2| = 6$ has no solutions. Thus $[\mathfrak{p}_2\mathfrak{p}_3] \neq 1$ and so $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$. Finally, $\theta^2 = -2\times 3\times 5$ and so $\langle\theta\rangle^2 = \mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_5^2$ so

$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 = \langle\theta\rangle.$$

Thus $[\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5] = 1$ so $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}[\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2][\mathfrak{p}_3]$.

Thus $\mathrm{Cl}(K) \cong C_2 \times C_2$. Hence $h_K = 4$.

Example 174. We will work out the class group for $K = \mathbb{Q}(\sqrt{-23})$, leaving some of the details to you. Note $\mathcal{O}_K = \mathbb{Z}[\theta]$ where $\theta = (1+\sqrt{-23})/2$ has minimal polynomial $X^2 - X + 6$. The Minkowski bound $B_K \approx 3.05$. Thus $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$ and $3\mathcal{O}_k = \mathfrak{p}_3\mathfrak{p}_3'$ where

$$\mathfrak{p}_2 = \langle 2, \theta\rangle, \quad \mathfrak{p}_2' = \langle 2, \theta - 1\rangle, \quad \mathfrak{p}_3 = \langle 3, \theta\rangle, \quad \mathfrak{p}_3' = \langle 3, \theta - 1\rangle.$$

Moreover, $\mathfrak{p}_2$, $\mathfrak{p}_2'$ both have norm 2 and $\mathfrak{p}_3$, $\mathfrak{p}_3'$ both have norm 3. We know that the class group is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_2']$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$.

Let's $\alpha \in \mathcal{O}_K$ and write $\alpha = x + y\theta$ with $x,\ y \in \mathbb{Z}$. Then

$$\mathrm{Norm}(\alpha) = \mathrm{Norm}((x + y/2) + y\sqrt{-23}/2) = (2x+y)^2/4 + 23y^2/4.$$

If $\mathfrak{p}_2 = \langle \alpha \rangle$ is principal then taking norms we have

$$(2x + y)^2 + 23y^2 = 8$$

which is impossible. Similarly $\mathfrak{p}_2'$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$ are not principal. Now let's check $\mathfrak{p}_2^2$. If $\mathfrak{p}_2^2 = \langle \alpha \rangle$ is principal then

$$(2x + y)^2 + 23y^2 = 16$$

which gives us $x = \pm 2$ and $y = 0$, so $\alpha = \pm 2$. But then $2\mathcal{O}_K = \mathfrak{p}_2^2$ which we know to be false as $\mathfrak{p}_2$, $\mathfrak{p}_2'$ are distinct prime ideals by Dedekind–Kummer. We persevere and check $\mathfrak{p}_2^3$. Here

$$\begin{aligned}
\mathfrak{p}_2^3 &= \langle 2, \theta \rangle \cdot \langle 4, 2\theta, \theta^2 \rangle \\
&= \langle 2, \theta \rangle \cdot \langle 4, 2\theta, \theta - 6 \rangle \\
&= \langle 2, \theta \rangle \cdot \langle 4, 2\theta, \theta + 2 \rangle \\
&= \langle 8, 4\theta, 2\theta + 4, 2\theta^2, \theta^2 + 2\theta \rangle \\
&= \langle 8, 4\theta, 2\theta + 4, 2\theta - 12, 3\theta - 6 \rangle \\
&= \langle 8, 4\theta, 2\theta + 4, 2\theta - 12, \theta + 6 \rangle \\
&= \langle 8, 4\theta, 2\theta + 4, 2\theta - 12, \theta - 2 \rangle \\
&= \langle 8, 8, 8, -8, \theta - 2 \rangle \\
&= \langle \theta - 2 \rangle
\end{aligned}$$

as $8/(\theta - 2) = -1 - \theta \in \mathcal{O}_K$. We see that $[\mathfrak{p}_2]$ is an element of order 3 in $\mathrm{Cl}(K)$. Moreover,

$$[\mathfrak{p}_2][\mathfrak{p}_2'] = [\langle 2 \rangle] = 1$$

so $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]^2$. In the same way $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}]$. All that remains is to relate $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. However,

$$\begin{aligned}
\mathfrak{p}_2\mathfrak{p}_3 &= \langle 6, 2\theta, 3\theta, \theta^2 \rangle \\
&= \langle 6, \theta \rangle \\
&= \langle \theta \rangle
\end{aligned}$$

as $6/\theta = 1 - \theta$. Thus $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1}$. Hence $\mathrm{Cl}(K)$ is cyclic of order 3 generated by $[\mathfrak{p}_2]$.

CHAPTER 9

Units

1. Revision

Let R be a ring. Recall that a **unit** in R is an element u such that $uv = 1$ for some other $v \in R$. The set of units is denoted by R^* and is a multiplicative group called the **unit group of** R. For example, if K is a field then $K^* = \{a \in K : a \neq 0\}$. But $\mathbb{Z}^* = \{1, -1\}$.

2. Units and Norms

Let K be a number field. We shall denote $\mathcal{O}_K^*$ by $U(K)$ and call it the **unit group of** K (even though it is really the unit group of $\mathcal{O}_K$).

PROPOSITION 175. *Let K be a number field. Then*

$$U(K) = \{\alpha \in \mathcal{O}_K \ : \ \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1\}.$$

PROOF. Let u be a unit in $\mathcal{O}_K$. By definition there is some $v \in \mathcal{O}_K$ such that $uv = 1$. By the multiplicativity of norms we get $\mathrm{Norm}_{K/\mathbb{Q}}(u) \cdot \mathrm{Norm}_{K/\mathbb{Q}}(v) = 1$. But the norm of an algebraic integer is a rational integer. Thus $\mathrm{Norm}_{K/\mathbb{Q}}(u) = \pm 1$.

Conversely, suppose $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α and recall that

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \alpha_2 \cdots \alpha_n.$$

Without loss of generality, $\alpha = \alpha_1$. Let

$$\beta = \alpha_2 \alpha_3 \cdots \alpha_n.$$

Note that the α_i do not necessarily belong to K, but $\beta = \pm 1/\alpha \in K$. Moreover, the α_i are algebraic integers (being conjugates of an algebraic integer α). Thus $\beta \in K \cap \mathcal{O} = \mathcal{O}_K$. Now $\alpha \cdot (\pm\beta) = 1$ showing that α is a unit. □

3. Units of Imaginary Quadratic Fields

THEOREM 176. *Let $K = \mathbb{Q}(\sqrt{-d})$ where d is squarefree and $d > 0$. Then*

(i) *If $K = \mathbb{Q}(i)$ then $U(K) = \{\pm 1, \pm i\}$.*
(ii) *If $K = \mathbb{Q}(\sqrt{-3})$ then $U(K) = \{\pm 1, \pm\zeta, \pm\zeta^2\}$ where $\zeta = (-1 + \sqrt{-3})/2 = \exp(2\pi i/3)$.*
(iii) *In all other cases $U(K) = \{1, -1\}$.*

PROOF. Suppose first that $-d \not\equiv 1 \pmod 4$. Then

$$\mathcal{O}_K = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \sqrt{-d}.$$

Let $\alpha \in \mathcal{O}_K$. Then $\alpha = a + b\sqrt{-d}$ where a, $b \in \mathbb{Z}$. This is a unit if and only if $\text{Norm}(\alpha) = \pm 1$ or equivalently $a^2 + d \cdot b^2 = 1$. If $d > 1$ then $b = 0$ and $a = \pm 1$, so $\alpha = \pm 1$. If $d = 1$, then $a^2 + b^2 = 1$ and the only solutions are $(a, b) = (\pm 1, 0)$, $(0, \pm 1)$. In this case $K = \mathbb{Q}(i)$ and the units are $a + bi = \pm 1$, $\pm i$.

Suppose now that $-d \equiv 1 \pmod 4$. Then every element of $\mathcal{O}_K$ can be written as $a + b\sqrt{-d}$ where a, b are both integers or a, b are both halves of odd integers. If $\alpha = a + b\sqrt{-d}$ is a unit, and a, b are both integers, then the argument above tells us that $\alpha = \pm 1$. We consider $a = r/2$, $b = s/2$ where r, s are odd integers. Then $r^2 + ds^2 = 4$. As s is odd, we have $s^2 \geq 1$ and so $4 \geq ds^2 \geq d$. But $d \equiv 3 \pmod 4$ and so $d = 3$. Thus $r^2 + 3s^2 = 4$. The only solutions in odd integers are $(r, s) = (\pm 1, \pm 1)$. In this case $K = \mathbb{Q}(\sqrt{-3})$ and $\alpha = (\pm 1 \pm \sqrt{-3})/2$. □

We'll see later that rings of integers of real quadratic fields have infinitely many units. For now you can check this for $\mathbb{Q}(\sqrt{2})$.

EXERCISE 177. Show that $1 + \sqrt{2}$ is a unit of $\mathbb{Z}[\sqrt{2}]$. Deduce that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

4. Units of Finite Order

Let K be a number field. We define

$$\eta(K) = \{\epsilon \in U(K) \ : \ \epsilon \text{ has finite multiplicative order}\}.$$

We call $\eta(K)$ the **torsion unit group** of K. For example, from the previous section we know that

$$\eta(\mathbb{Q}(i)) = U(\mathbb{Q}(i)) = \{1, i, -1, -i\}.$$

LEMMA 178. *$\eta(K)$ is a finite subgroup of $U(K)$.*

PROOF. Note $U(K)$ is an abelian group. Thus the set $\eta(K)$ is in fact the torsion subgroup of $U(K)$. We need to show that $U(K)$ is finite. Now if ζ in $U(K)$ has order m, then ζ is a primitive m-th root of unity. Let $\omega_1, \ldots, \omega_n$ be an integral basis for $\mathcal{O}_K$. Then

$$\zeta = a_1\omega_1 + \cdots + a_n\omega_n \tag{17}$$

where the $a_i \in \mathbb{Z}$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings $K \hookrightarrow \mathbb{C}$. Thus

$$\sigma_i(\zeta) = \sum_{j=1}^{n} a_j \sigma_i(\omega_j)$$

for $i = 1, \ldots, n$. Let $A = (\sigma_i(\omega_j))$. Then $\det(A)^2 = D(\omega_1, \ldots, \omega_n)^2 = \Delta(\omega_1, \ldots, \omega_n) \neq 0$ by Theorem 75. In particular, A is invertible. Let $A^{-1} = (b_{i,j})$. Then

$$a_j = \sum_{i=1}^{n} b_{i,j}\sigma_i(\zeta).$$

But $\sigma_i(\zeta)$ is a root of unity so $|\sigma_i(\zeta)| = 1$, so

$$|a_j| \leq C \cdot n$$

where $C = \max|b_{i,j}|$. As C and n are fixed, there are only finitely many possibilities for the integer coefficients a_j in (17). Thus there are only finitely many possibilities for ζ. This completes the proof. □

THEOREM 179. *Let K be a number field. Then $\eta(K) = \langle\zeta\rangle$ where ζ is a root of unity.*

Warning: Here the notation $\eta(K) = \langle\zeta\rangle$ means that ζ is a generator for the multiplicative group $\eta(K)$. It does **not** mean that $\eta(K)$ is a principal ideal! The set $\eta(K)$ is not an ideal at all.

PROOF OF THEOREM 179. We know that $\eta(K)$ is finite by Lemma 178. By the Fundamental Theorem of Abelian Groups,

$$\eta(K) \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}$$

where $d_1 \mid d_2 \mid \cdots \mid d_r$. Note that the order of $\eta(K)$ is $d = d_1 d_2 \cdots d_r$, but every $\alpha \in \eta(K)$ satisfies $\alpha^{d_r} = 1$. Thus all elements of $\eta(K)$ are roots of $X^{d_r} - 1$. But $X^{d_r} - 1$ has at most d_r roots. Hence

$$d_1 d_2 \cdots d_r = d = \#\eta(K) \leq d_r.$$

This can only happen is $d_1 = d_2 = \cdots = d_{r-1} = 1$ and $d = d_r = \#\eta(K)$. Thus $\eta(K) \cong C_d$ and its elements are in fact the roots of $X^d - 1$. Hence $\eta(K) = \langle\zeta\rangle$ where $\zeta = \exp(2\pi i/d)$. □

THEOREM 180. *Let K have at least one real embedding $\sigma : K \hookrightarrow \mathbb{R}$. Then $\eta(K) = \{1, -1\}$.*

PROOF. Let ζ be a cyclic generator of $\eta(K)$. Then $\zeta^d = 1$ and thus $\sigma(\zeta)^d = 1$. The only real roots of unity are ± 1. Thus $\sigma(\zeta)^2 = 1$ and so $\sigma(\zeta^2) = 1$. But σ is injective (it's an embedding!) and so $\zeta^2 = 1$ and hence $\zeta = \pm 1$. Thus $\eta(K) = \{1, -1\}$. □

5. Dirichlet's Unit Theorem

THEOREM 181 (Dirichlet's Unit Theorem). *Let K be a number field of signature (r, s) and write $t = r + s - 1$. Then $U(K)$ is a finitely generated group of rank $r + s - 1$. More precisely, there are units $\epsilon_1, \ldots, \epsilon_t$ such that every $\epsilon \in U(K)$ can be written uniquely as*

$$\epsilon = \omega \cdot \epsilon_1^{n_1}\epsilon_2^{n_2} \cdots \epsilon_t^{n_t}$$

where $\omega \in \eta(K)$ and $n_i \in \mathbb{Z}$.

EXAMPLE 182. In this example we shall show that the unit group for $K = \mathbb{Q}(\sqrt{2})$ is

$$U(K) = \{\pm(1+\sqrt{2})^m : m \in \mathbb{Z}\} \tag{18}$$

with the help of Dirichlet's Unit Theorem. Since $\sqrt{2}$ has minimal polynomial $X^2 - 2$ which has two real roots, we see that K has two real embeddings and no complex ones; in particular K has signature $(2, 0)$. Thus the rank of $U(K)$ is $t = 2 + 0 - 1 = 1$. Moreover, by Theorem 180 we know that $\eta(K) = \{1, -1\}$. Thus by Dirichlet's Unit Theorem there is some unit ϵ (called ϵ_1 in the theorem) such that every unit can be written uniquely as $\pm\epsilon^m$ for some $m \geq 1$. Thus

$$U(K) = \{\pm\epsilon^m \ : \ m \in \mathbb{Z}\}. \tag{19}$$

Replacing ϵ by ϵ^{-1} does not affect (19). Thus we may suppose that $|\epsilon| \geq 1$.

Now $1 + \sqrt{2} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ and has norm $1 - 2 = -1$ and so is a unit. Thus $1 + \sqrt{2} = \pm\epsilon^n$ for some $n \in \mathbb{Z}$. Moreover, as $1 + \sqrt{2} > 1$ and $|\epsilon| \geq 1$ we have $n \geq 1$. If $n = 1$ then (18) follows. Thus suppose $n \geq 2$. Write $\epsilon = a + b\sqrt{2}$ with a, $b \in \mathbb{Z}$. Thus

$$1 + \sqrt{2} = \pm(a + b\sqrt{2})^n.$$

To this we apply the embeddings σ_1, $\sigma_2 : K \hookrightarrow \mathbb{R}$ which are given by $\sigma_1(u + v\sqrt{2}) = u + v\sqrt{2}$ and $\sigma_2(u + v\sqrt{2}) = u - v\sqrt{2}$ for u, $v \in \mathbb{Q}$. We obtain,

$$1 + \sqrt{2} = \pm(a + b\sqrt{2})^n, \qquad 1 - \sqrt{2} = \pm(a - b\sqrt{2})^n.$$

Hence

$$|a + b\sqrt{2}| \leq |1 + \sqrt{2}|^{1/n}, \qquad |a - b\sqrt{2}| \leq |1 - \sqrt{2}|^{1/n}.$$

By the triangle inequality

$$|b| \leq \frac{1}{2\sqrt{2}} \left(|1 + \sqrt{2}|^{1/n} + |1 - \sqrt{2}|^{1/n} \right).$$

We shall need approximate values for $1 + \sqrt{2}$ and $1 - \sqrt{2}$. To 1 decimal place we have

$$|1 + \sqrt{2}| \approx 2.4\ldots, \qquad |1 - \sqrt{2}| \approx 0.4\ldots.$$

As $n \geq 2$ we know that

$$|1 + \sqrt{2}|^{1/n} \leq |1 + \sqrt{2}|^{1/2} \leq (2.5)^{1/2} \leq 1.6,$$

and

$$|1 - \sqrt{2}|^{1/n} < 1.$$

Thus

$$|b| \leq \frac{1.6 + 1}{2\sqrt{2}} < 1.$$

Therefore $b = 0$. But $a^2 - 2b^2 = \text{Norm}(\epsilon) = \pm 1$. This forces $\epsilon = a = \pm 1$, giving a contradiction. Thus $n = 1$ and so (18) holds.

The number field $\mathbb{Q}(\sqrt{2})$ is a real quadratic field. The units of real quadratic fields can be computed rather efficiently using continued fractions. However the continued fraction method is not useful for number fields of higher degree.

EXERCISE 183. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Show that $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ is an integral basis for $\mathcal{O}_K$. Show that

$$U(K) = \{\pm(\sqrt[3]{2} - 1)^n \ : \ n \in \mathbb{Z}\}.$$

You may need to use `WolframAlpha`, `MATLAB` or a similar package to compute approximations to the embeddings of some algebraic numbers.

CHAPTER 10

Some Diophantine Examples

LEMMA 184. *Let α, β be non-zero elements of $\mathcal{O}_K$ and suppose $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$. Then $\alpha = \varepsilon\beta$ for some $\varepsilon \in U(K)$.*

PROOF. As $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$ we have $\alpha = \beta\varepsilon$ and $\beta = \alpha\varepsilon'$ for some ε, $\varepsilon' \in \mathcal{O}_K$. But then $\varepsilon\varepsilon' = 1$ and so ε is a unit. □

LEMMA 185. *Let n be a positive integer. Let $\mathfrak{a}$, $\mathbf{b}$, $\mathfrak{c}$ be non-zero ideals satisfying $\mathfrak{a}\mathbf{b} = \mathfrak{c}^n$. Suppose $\mathfrak{a}$, $\mathbf{b}$ are coprime. Then there are ideals $\mathfrak{c}_1$, $\mathfrak{c}_2$ such that*

$$\mathfrak{a} = \mathfrak{c}_1^n, \qquad \mathbf{b} = \mathfrak{c}_2^n, \qquad \mathfrak{c}_1\mathfrak{c}_2 = \mathfrak{c}.$$

PROOF. As $\mathfrak{a}$, $\mathbf{b}$ are coprime, they have no common prime ideal divisor. Let

$$\mathfrak{c} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

where the $\mathfrak{p}_i$ are distinct primes. Then

$$\mathfrak{a}\mathbf{b} = \mathfrak{c}^n = \mathfrak{p}_1^{nr_1} \cdots \mathfrak{p}_k^{nr_k}.$$

Since $\mathfrak{a}$, $\mathbf{b}$ have no common prime divisor, we may rearrange the $\mathfrak{p}_i$ so that $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ divide $\mathfrak{a}$ but not $\mathbf{b}$, and $\mathfrak{p}_{\ell+1}, \ldots, \mathfrak{p}_k$ divide $\mathbf{b}$ but not $\mathfrak{a}$. Hence

$$\mathfrak{a} = \mathfrak{p}_1^{nr_1} \cdots \mathfrak{p}_\ell^{nr_\ell}, \qquad \mathbf{b} = \mathfrak{p}_{\ell+1}^{nr_{\ell+1}} \cdots \mathfrak{p}_k^{nr_k}.$$

Letting

$$\mathfrak{c}_1 = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_\ell^{r_\ell}, \qquad \mathfrak{c}_2 = \mathfrak{p}_{\ell+1}^{r_{\ell+1}} \cdots \mathfrak{p}_k^{r_k}$$

completes the proof. □

EXERCISE 186. Give a counterexample (with $K = \mathbb{Q}$) to show that Lemma 185 does not hold without the coprimality assumption.

EXAMPLE 187. Determine all solutions to the equation $x^2 + 2 = y^3$ with x, $y \in \mathbb{Z}$.

Answer: There is a standard strategy for solving such problems which involves factoring in quadratic fields. The field we need for this problem is $K = \mathbb{Q}(\sqrt{-2})$. Here $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$, and $\mathrm{Cl}(K) = \{1\}$ (check).

Suppose x, $y \in \mathbb{Z}$ and satisfy $x^2 + 2 = y^3$. If either x or y is even then both are even and 4 divides $y^3 - x^2 = 2$ giving a contradiction. Thus they're both odd.

Now

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3.$$

We shall show that the ideal $\mathfrak{a} = (x + \sqrt{-2})\mathcal{O}_K$ is the cube of an ideal. Let $\mathbf{b} = (x - \sqrt{-2})\mathcal{O}_K$ and $\mathfrak{c} = y\mathcal{O}_K$. Then $\mathfrak{a}\mathbf{b} = \mathfrak{c}^3$. Let's show by contradiction that $\mathfrak{a}$ and $\mathbf{b}$ are coprime. So suppose $\mathfrak{p}$ be a prime ideal dividing both $\mathfrak{a}$, $\mathbf{b}$. Then $\mathfrak{p}$ divides (i.e. contains) $(x + \sqrt{-2}) - (x - \sqrt{2}) = 2\sqrt{-2} = -(\sqrt{-2})^3$. Thus $\mathfrak{p}$ divides $\sqrt{-2}\mathcal{O}_K$. But $\sqrt{-2}\mathcal{O}_K$ is a prime ideal (you get this from factoring $2\mathcal{O}_K$ using Dedekind–Kummer). As non-zero prime ideals are maximal, we get $\mathfrak{p} = \sqrt{-2}\mathcal{O}_K$. However $\mathfrak{p} \mid y\mathcal{O}_K$ and so $\mathrm{Norm}(\mathfrak{p}) \mid y^2$ and so y is even giving a contradiction. Hence $\mathfrak{a}$, $\mathbf{b}$ are coprime.

By Lemma 185 we have $\mathfrak{a} = \mathfrak{c}_1^3$ for some ideal $\mathfrak{c}_1$. However, $\mathrm{Cl}(K) = \{1\}$ so $\mathfrak{c}_1$ is principal, and we may write $\mathfrak{c}_1 = (u + v\sqrt{-2})\mathcal{O}_K$ for some u, $v \in \mathbb{Z}$. Hence

$$(x + \sqrt{-2})\mathcal{O}_K = (u + v\sqrt{-2})^3\mathcal{O}_K.$$

By Lemma 184 we have

$$x + \sqrt{-2} = \varepsilon(u + v\sqrt{-2})^3$$

where $\varepsilon \in U(K) = \{\pm 1\}$. After possibly changing the signs of u, v we have

$$x + \sqrt{-2} = (u + v\sqrt{-2})^3 = (u^3 - 6uv^2) + (3u^2v - 2v^3)\sqrt{-2}.$$

Comparing coefficients of $\sqrt{-2}$ we have $v(3u^2 - 2v^2) = 1$. Hence $v = \pm 1$ and $3u^2 - 2v^2 = \pm 1$. The only solutions are $(u, v) = (\pm 1, 1)$. Hence $x = u^3 - 6uv^2 = \pm 5$. Since $x^2 + 2 = y^3$ we see that the only solutions are $(\pm 5, 3)$.

Example 188. Let p be an odd prime and suppose that -23 is a square modulo p. Show that either p or $2p$ can be written as $x^2 + xy + 6y^2$ for some integers x, y.

Answer: The key to this is to spot that $x^2 + xy + 6y^2$ is a norm. Indeed, completing the square, we have

$$x^2 + xy + 6y^2 = (x + y/2)^2 + 23y^2/4 = \mathrm{Norm}_{K/\mathbb{Q}}(x + y\theta)$$

where $\theta = (1 + \sqrt{-23})/2$ and $K = \mathbb{Q}(\sqrt{-23})$. As $-23 \equiv 1 \pmod 4$ we know that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Hence all we have to do is show that either p or $2p$ is the norm of some element of $\mathcal{O}_K$.

Note that $[\mathcal{O}_K : \mathbb{Z}[\sqrt{-23}]] = 2$, and so not divisible by p. Thus we may apply the Dedekind–Kummer Theorem to factor $p\mathcal{O}_K$ by factoring $X^2 + 23$ modulo p. We are given that -23 is a square modulo p. Thus $X^2 + 23$ is the product of two linear factors modulo p and hence $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$, $\mathfrak{p}'$ are both prime ideals of norm p. If $\mathfrak{p}$ is principal, say $\langle x + y\theta\rangle$ with x, $y \in \mathbb{Z}$, then $p = x^2 + xy + 6y^2$ as required. Suppose $\mathfrak{p}$ is not principal. We know from Example 174 that the class group is cyclic of order 3 with the two non-trivial classes being $[\mathfrak{p}_2]$ and $[\mathfrak{p}_2']$ where $\mathfrak{p}_2$, $\mathfrak{p}_2'$ are ideals of norm 2. Thus either $\mathfrak{p}_2\mathfrak{p}$ or $\mathfrak{p}_2'\mathfrak{p}$ is principal. Thus $2p = x^2 + xy + 6y^2$ for some x, $y \in \mathbb{Z}$.