B3.4 Algebraic Number Theory

Victor Flynn (flynn@maths.ox.ac.uk)

January 2021

These notes are modified from previous versions (due to Neil Dummigan, Alan Lauder and Roger Heath-Brown) and have been recently revised by me. They draw mainly upon "A Classical Introduction to Modern Number Theory", by Ireland and Rosen, and "Algebraic Number Theory", by Stewart and Tall. While I take full responsibility for their current contents, considerable thanks are clearly due to Neil, Alan and Roger.

I will be pleased to hear of any misprints or errors!
Email me at `flynn@maths.ox.ac.uk`.

Throughout these notes we use the abbreviation NE for "not examinable in this course".

Lectures will omit some of the non-examinable proofs, and some of the examples in Section 9. However these should prove helpful for examination revision.

Useful texts

Algebraic Number Theory and Fermat's Last Theorem, I. Stewart and D. Tall, Third Edition. We shall frequently cite this as "S&T".

Older editions under the name "Algebraic Number Theory" will also suffice.

Other useful but more advanced references:
A Classical Introduction to Modern Number Theory, (Chapter 12) K. Ireland and M. Rosen
Algebraic Number Theory, A. Frohlich and M.J. Taylor
A Course in Computational Algebraic Number Theory, H. Cohen.

1 Introduction

1.1 Motivation

Consider "Fermat's Last Theorem" which asserts that $x^n + y^n = z^n$ has no solution $x, y, z \in \mathbb{Z}$ (x, y, z all nonzero) if $n \in \mathbb{N}, n \geqslant 3$. It is sufficient to prove this for $n = 4$ and $n = p \geqslant 3$ prime [since any $n \geqslant 3$ is divisible by 4 or some prime $p \geqslant 3$; if $n = 4k$, then any solution to $x^n + y^n = z^n$ would give $(x^k)^4 + (y^k)^4 = (z^k)^4$; similarly if $n = pk$, then any solution to $x^n + y^n = z^n$ would give $(x^k)^p + (y^k)^p = (z^k)^p$].

Fermat himself proved the result for $n = 4$ after which it remained to prove it for $n = p \geqslant 3$ prime. Let $\zeta_p = \exp(2\pi i/p) \in \mathbb{C}$ and let $K := \mathbb{Q}(\zeta_p)$. Factoring the left hand side in $\mathbb{Z}[\zeta_p]$ we see that

$$(x + y)(x + \zeta_p y) \dots (x + \zeta_p^{p-1} y) = z^p.$$

Now in $\mathbb{Z}$ it is true that if $a_1 \dots a_p = b^p$ and the a_i have no common factors, then each a_i is an p-th power, by the unique factorisation property of $\mathbb{Z}$. To make progress on Fermat's Last Theorem it would be useful to know whether an analogous result holds true in $\mathbb{Z}[\zeta_p]$. More generally we might ask what sort of number theory can we do in a ring such as $\mathbb{Z}[\zeta_p]$? In particular do we still have an analogue of unique factorisation into primes?

These are the questions addressed in this course.

1.2 Background material

We need to know the statements (but not proof) of various pre-requisites for this course. Firstly we have, some results from "Polynomial Rings and Galois Theory".

Lemma 1.1 (Gauss's Lemma)**.** *Let $p(t) \in \mathbb{Z}[t]$ be irreducible in $\mathbb{Z}[t]$; then it is also irreducible in $\mathbb{Q}[t]$.*

Proof. NE. See S&T, page 18, Lemma 1.7. The broad strategy is to imagine $p(t)$ were reducible over $\mathbb{Q}$, with $p(t) = g(t)h(t)$ where $g(t), h(t) \in \mathbb{Q}[t]$, and then show there exists $\lambda \in \mathbb{Q}$, $\lambda \neq 0$, such that $\lambda g, \lambda^{-1} h \in \mathbb{Z}[t]$ (the existence of such λ is sometimes included in the statement of Gauss' Lemma). □

Theorem 1.2 (Eisenstein)**.** *Let $f(t) = a_0 + a_1 t + \dots + a_n t^n \in \mathbb{Z}[t]$. Suppose there exists a prime p such that p does not divide a_n, but p divides a_i for*

$i = 0, \ldots, n-1$, and p^2 does not divide a_0. Then, apart from constant factors, $f(t)$ is irreducible over $\mathbb{Z}$, and hence irreducible over $\mathbb{Q}$.

Such a polynomial is said to be Eisenstein with respect to the prime p. Note also: *irreducible over K* is just another way of saying: irreducible in $K[t]$.

Proof. NE. See S&T, page 19, Theorem 1.8. □

Definition 1.3. *A* number field *(or* algebraic number field*) is a finite extension K of $\mathbb{Q}$. The index $[K : \mathbb{Q}]$ is the* degree *of the number field.*

Theorem 1.4. *If K is a number field then $K = \mathbb{Q}(\theta)$ for some (algebraic) number $\theta \in K$.*

Proof. NE. See S&T, page 32, Theorem 2.2. □

Theorem 1.5. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms (embeddings)*

$$\sigma_i : K \to \mathbb{C} \ \ (i = 1, \ldots, n).$$

The elements $\sigma_i(\theta)$ are the distinct zeros in $\mathbb{C}$ of the minimal polynomial m_θ of θ over $\mathbb{Q}$.

If $\sigma_i(K) \subseteq \mathbb{R}$ then σ_i is called a real embedding, and otherwise it is called a complex embedding.

Recall that a monomorphism is a one-to-one map satisfying $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

Proof. NE. See S&T, page 38, Theorem 2.4. □

We now have some elementary results on free abelian groups. We shall express such groups with the operation written additively.

Definition 1.6. *A square matrix over $\mathbb{Z}$ is* unimodular *if it has determinant* ± 1.

Note that A is unimodular if and only if A^{-1} has coefficients in $\mathbb{Z}$.

Lemma 1.7. *Let G be a free abelian group of rank n with $\mathbb{Z}$-basis $\{x_1, \ldots, x_n\}$. Suppose (a_{ij}) is an $n \times n$ matrix with integer entries. Let*

$$y_i = \sum_j a_{ij} x_j \quad (1 \leqslant i \leqslant n).$$

Then the elements $\{y_1, \ldots, y_n\}$ form a $\mathbb{Z}$-basis for G if and only if (a_{ij}) is unimodular.

Proof. NE. See S&T, page 28, Lemma 1.15. □

Theorem 1.8. *Let G be a free abelian group of rank n, and H a subgroup. Then G/H is finite if and only if H has rank n. Moreover, if G and H have $\mathbb{Z}$-bases $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ with $y_i = \sum_j a_{ij} x_j$ we have*

$$\#G/H = |\det(a_{ij})|.$$

Proof. NE. See S&T, page 30, Theorem 1.17. □

2 Discriminants, Norms and Traces

Definition 2.1. *Let $K/\mathbb{Q}$ be an algebraic number field of degree n, and let $\alpha \in K$. Let $\sigma_i : K \to \mathbb{C}$ be the n embeddings, $i = 1, \ldots, n$. The $\sigma_i(\alpha)$ are called the (K-)*conjugates *of α. Define the* trace $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$ *and* norm $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\alpha) = N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$. *When $K = \mathbb{Q}(\alpha)$ these are called the* absolute *conjugates, trace and norm.*

For any $K = \mathbb{Q}(\beta)$, suppose that β has minimal polynomial $m_\beta(X)$. If $\beta_1, \ldots, \beta_n$ are the n roots of m_β in $\mathbb{C}$ then one can choose the embeddings so that $\sigma_i : \beta \mapsto \beta_i$.

We record the trivial properties:-

$$\mathrm{Norm}_{K/\mathbb{Q}}(\gamma\delta) = \mathrm{Norm}_{K/\mathbb{Q}}(\gamma)\mathrm{Norm}_{K/\mathbb{Q}}(\delta);$$

$$\mathrm{Norm}_{K/\mathbb{Q}}(\gamma) = 0 \quad \text{if and only if} \quad \gamma = 0;$$

$$\mathrm{Norm}_{K/\mathbb{Q}}(q) = q^n \quad \text{for} \quad q \in \mathbb{Q}.$$

If $K = \mathbb{Q}(\alpha)$ and $m_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$, then we have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -c_{n-1}$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = (-1)^n c_0$. In particular the norm and trace are in $\mathbb{Q}$.

More generally, for any $K = \mathbb{Q}(\beta)$, $\alpha \in K$, the norm and trace of α are symmetric functions of the conjugates $\sigma_i(\alpha)$, and are therefore in $\mathbb{Q}$.

Definition 2.2. *Let $w = \{w_1, \ldots, w_n\}$ be an n-tuple of elements of K, where $n = [K : \mathbb{Q}]$.*

- *The* determinant *is $\Delta(w) := \det(\sigma_i(w_j))$, i.e., the determinant of the $n \times n$ matrix whose (i, j)th entry is $\sigma_i(w_j)$.*
- *The* discriminant *of w is $\Delta(w)^2$. [sometimes also written as $\Delta^2(w)$.]*

Warning: S&T and some other books use Δ where we write Δ^2 (!).

Lemma 2.3. *We have $\Delta(w)^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(w_i w_j))$, and so $\Delta(w)^2 \in \mathbb{Q}$.*

Proof. Let $A = (\sigma_i(w_j))$. Then

$$\Delta(w)^2 = \det(A)^2 = \det(A^T A) = \det\left(\sum_k \sigma_k(w_i)\sigma_k(w_j)\right)$$

$$= \det\left(\sum_k \sigma_k(w_i w_j)\right) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(w_i w_j)).$$

□

Lemma 2.4. *If $v = \{v_1, \ldots, v_n\}$ is a basis for $K/\mathbb{Q}$ and $w = \{w_1, \ldots, w_n\} \subseteq K$, with $w_i = \sum_j c_{ij} v_j$ and $c_{ij} \in \mathbb{Q}$, then*

$$\Delta(w) = \det(C)\Delta(v) \text{ where } C = (c_{ij}).$$

Proof. Left as exercise. □

Lemma 2.5. *If $K = \mathbb{Q}(\alpha)$ and $v = \{1, \alpha, \ldots, \alpha^{n-1}\}$ then*

$$\Delta(v)^2 = \prod_{i<j} (\alpha_j - \alpha_i)^2.$$

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

Proof. We have

$$\Delta(v) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix}$$

(This is a so-called van der Monde determinant.) We can view this as a polynomial of degree $n(n-1)/2$ in $\alpha_1, \ldots, \alpha_n$. Since it vanishes when we set $\alpha_i = \alpha_j$ the polynomial is divisible by $\alpha_i - \alpha_j$ for all $i < j$. There are $n(n-1)/2$ of these factors. Hence, on checking that the coefficient of $\alpha_2\alpha_3^2 \ldots \alpha_n^{n-1}$ is $+1$ we deduce that

$$\Delta(w) = \prod_{i<j}(\alpha_j - \alpha_i).$$

□

Corollary 2.6. *$\Delta(w_1 \ldots, w_n) \neq 0$ if and only if $w_1 \ldots, w_n$ is a basis for $K/\mathbb{Q}$.*

Proof. Suppose $K = \mathbb{Q}(\alpha)$ and $v = \{1, \alpha, \ldots, \alpha^{n-1}\}$ are as in the previous lemma. Since the α_i are distinct, $\Delta(v) \neq 0$. By Lemma 2.4, $\Delta(w) \neq 0$ for any other basis w of $K/\mathbb{Q}$. If w is not a basis then $\det(C) = 0$ and so $\Delta(w) = 0$. □

3 The Ring of Integers

Definition 3.1. *We say that $\alpha \in K$ is an* algebraic integer *if and only if there exists a monic $g(x) \in \mathbb{Z}[x]$ such that $g(\alpha) = 0$. Define $\mathcal{O}_K$ as the set of all algebraic integers in K.*

We shall see that the set $\mathcal{O}_K$ will bear the same relation to K as $\mathbb{Z}$ does to $\mathbb{Q}$.

Note 3.2

1. Suppose $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial $m_\alpha(x)$ is in $\mathbb{Z}[x]$, by Gauss's lemma.

2. Suppose $\alpha \in K$ and $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$, $a_i \in \mathbb{Q}$. If $n \in \mathbb{Z}$ then
$$(n\alpha)^d + na_{d-1}(n\alpha)^{d-1} + \cdots + n^d a_0 = 0.$$
Choosing n to clear the denominators of all the a_i we can get $n\alpha \in \mathcal{O}_K$.

3. The minimal polynomial of $r \in \mathbb{Q}$ is $x - r$ which is in $\mathbb{Z}[x]$ if and only if $r \in \mathbb{Z}$. Hence if $K = \mathbb{Q}$ then $\mathcal{O}_K = \mathbb{Z}$. Generally, $\mathbb{Z} \subseteq \mathcal{O}_K$.

Example 3.3 Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$, $d \neq \pm 1$, with d squarefree (i.e. there is no prime p for which $p^2|d$). Then $[K : \mathbb{Q}] = 2$, and K has a $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$. If $a, b \in \mathbb{Q}$ then $\alpha = a + b\sqrt{d} \in K$. Since $\sigma_1(\alpha) = a + b\sqrt{d}$ and $\sigma_2(\alpha) = a - b\sqrt{d}$ we have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = a^2 - db^2$. Moreover $m_\alpha(x) = x^2 - 2ax + (a^2 - db^2)$ (if $b \neq 0$). Hence $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - db^2 \in \mathbb{Z}$.

Suppose $\alpha \in \mathcal{O}_K$. Then $(2a)^2 - d(2b)^2 \in \mathbb{Z}$, giving $d(2b)^2 \in \mathbb{Z}$. Writing $2b = u/v$ $(u, v \in \mathbb{Z})$ we have $du^2v^{-2} \in \mathbb{Z}$, so that $v^2|du^2$. Since d is squarefree this implies $v|u$, giving $2b \in \mathbb{Z}$. Write $2a = A$, $2b = B$, with $A, B \in \mathbb{Z}$. Then $a^2 - db^2 \in \mathbb{Z}$, so that $A^2 \equiv dB^2 \bmod 4$. Now observe that any square is congruent to 0 or 1 modulo 4.

- Case 1: Suppose $d \equiv 2$ or $3 \bmod 4$. Then we must have A, B even, and $a, b \in \mathbb{Z}$.
- Case 2: Suppose that $d \equiv 1 \bmod 4$. This implies that $A \equiv B \bmod 2$, so a, b are both in $\mathbb{Z}$ or both in $\mathbb{Z} + \frac{1}{2}$.

Of course we cannot have $d \equiv 0 \bmod 4$ since d is squarefree. We conclude that

$$\mathcal{O}_K = \begin{cases} \langle 1, \sqrt{d} \rangle = \{m + n\sqrt{d} : m, n \in \mathbb{Z}\}, & d \equiv 2, 3 \bmod 4, \\ \langle 1, \frac{1+\sqrt{d}}{2} \rangle = \{m + n\frac{1+\sqrt{d}}{2} : m, n \in \mathbb{Z}\}, & d \equiv 1 \bmod 4. \end{cases}$$

e.g. In $\mathbb{Q}(i)$ we have $\frac{1}{2} + \frac{2}{3}i \in K$ and $1 + 5i \in \mathcal{O}_K$. In $\mathbb{Q}(\sqrt{-3})$ we have $\frac{3}{5} - \sqrt{-3} \in K$, $-\frac{1}{2} + \frac{\sqrt{-3}}{2} \in \mathcal{O}_K$. (The latter has minimal polynomial $x^2 + x + 1$).

We now require a little about modules.

Definition 3.4. *Let R be an integral domain. An R-module M is an abelian group (which we shall write additively) with a map $R \times M \to M$, $(r, m) \mapsto rm$ such that*

$$(r_1 + r_2)m = r_1m + r_2m,\ (r_1r_2)m = r_1(r_2m)$$

$$r(m_1 + m_2) = rm_1 + rm_2,\ 1m = m$$

for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$.

Example 3.5

1. Let R be a field and M a vector space over R. Then M is an R-module.
2. If $R = \mathbb{Z}$ and M is any additive abelian group then M is an R-module.

We say that M is finitely generated if there exist $m_1, \ldots, m_k \in M$ such that

$$M = \{r_1 m_1 + \cdots + m_k r_k : r_1, \ldots, r_k \in R\}.$$

Lemma 3.6. *$\alpha \in K$ is an algebraic integer if and only if there exists a nonzero finitely generated $\mathbb{Z}$-module $M \subseteq K$ such that $\alpha M \subseteq M$.*

Proof. Suppose $\alpha \in \mathcal{O}_K$, say $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$, with $a_i \in \mathbb{Z}$. Let $M = \mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\} \subseteq K$. Then $M = \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$ and $\alpha M \subseteq M$, since $\alpha(\alpha^{d-1}) = \alpha^d = -\sum_{i=0}^{d-1} a_i \alpha^i \in M$.

Conversely, suppose $M \subseteq K$ is a nonzero finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$. Take $w_1, \ldots, w_s$ to be a generating set for M. Let

$$\alpha w_i = \sum_j c_{ij} w_j,\ c_{ij} \in \mathbb{Z}.$$

Putting $C = (c_{ij})$ we see that

$$(\alpha I - C) \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

so that α satisfies $\det(xI - C) = 0$, a monic polynomial with integer coefficients. Hence $\alpha \in \mathcal{O}_K$. □

Theorem 3.7. *Let K be an algebraic number field. If $\alpha, \beta \in \mathcal{O}_K$ then $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$.*

Hence $\mathcal{O}_K$ is a ring, called the *ring of integers* of K.

Proof. Suppose $\alpha, \beta \in \mathcal{O}_K$. Let $M, N \subseteq K$ be finitely generated $\mathbb{Z}$-modules, generated respectively by $\{v_1, \ldots, v_d\}$ and $\{w_1, \ldots, w_e\}$, such that $\alpha M \subseteq M$ and $\beta N \subseteq N$. Consider

$$MN := \{\sum_{i=1}^{k} m_i n_i \ :\ m_i \in M, n_i \in N\}.$$

Then MN is finitely generatedy (by $\{v_i w_j : 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant e\}$) and in K. Moreover,

$$(\alpha+\beta)MN \subseteq (\alpha M)N + M(\beta N) \subseteq MN$$

$$(\alpha\beta)MN \subseteq (\alpha M)(\beta N) \subseteq MN.$$

It follows from Lemma 3.6 that $\alpha+\beta, \alpha\beta \in \mathcal{O}_K$. □

Corollary 3.8. *If $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. Assume that $\alpha \in \mathcal{O}_K$. Then all the $K/\mathbb{Q}$-conjugates $\alpha_1, \ldots, \alpha_n$ belong to $\mathcal{O}_L$ (where L is the splitting field of the polynomial $m_\alpha(x)(= m_{\alpha_i}(x))$). Thus $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \alpha_1 + \cdots + \alpha_n \in \mathcal{O}_L$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \alpha_1 \ldots \alpha_n \in \mathcal{O}_L$, by Theorem 3.7. However $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$, $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. □

Definition 3.9. *$\alpha \in \mathcal{O}_K$ is a* unit *if and only if $\alpha^{-1} \in \mathcal{O}_K$.*

Proposition 3.10. *$\alpha \in \mathcal{O}_K$ is a unit if and only if* $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Proof. Suppose α is a unit. Then

$$\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\mathrm{Norm}_{K/\mathbb{Q}}(\alpha^{-1}) = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = \mathrm{Norm}_{K/\mathbb{Q}}(1) = 1.$$

However $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha^{-1})$ are in $\mathbb{Z}$, so both are ± 1.

Conversely, suppose that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$. Let $\alpha_1, \ldots, \alpha_n$ be the $K/\mathbb{Q}$-conjugates, with $\alpha = \alpha_1$, say. Then $\alpha_1 \ldots \alpha_n = \pm 1$, so that $\alpha(\alpha_2 \ldots \alpha_n) = \pm 1$. Hence $\alpha^{-1} = \pm(\alpha_2 \ldots \alpha_n)$, which by Theorem 3.7 lies in $\mathcal{O}_L$. However we know that α^{-1} lies in K, and so $\alpha^{-1} \in \mathcal{O}_L \cap K = \mathcal{O}_K$. □

Definition 3.11. *We say that $w_1, \ldots, w_n \in \mathcal{O}_K$ is an* integral basis *for $\mathcal{O}_K$ if $\mathcal{O}_K = \{\sum_j c_j w_j : c_j \in \mathbb{Z}\}$.*

It can easily be shown that the above definition is equivalent to saying that $w_1, \ldots, w_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We shall show that every $\mathcal{O}_K$ has an integral basis. The set $\{w_1, \ldots, w_n\}$ is sometimes called an integral basis for $\mathcal{O}_K$, and sometimes just an integral basis for K.

Example 3.12 $K = \mathbb{Q}(\sqrt{d})$, d squarefree integer; $[K : \mathbb{Q}] = 2$; $\mathcal{O}_K$ has integral basis

$$\begin{cases} \{1, \sqrt{d}\}, & d \equiv 2, 3 \bmod 4, \\ \{1, \frac{1+\sqrt{d}}{2}\}, & d \equiv 1 \bmod 4. \end{cases}$$

Note 3.13 Let $v = \{v_1, \ldots, v_n\}$ and $w = \{w_1, \ldots, w_n\}$ be any two $\mathbb{Q}$-bases of K. Let $M = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$ and $N = \langle w_1, \ldots, w_n \rangle_{\mathbb{Z}}$, as $\mathbb{Z}$-submodules of K. Suppose $v, w \subseteq \mathcal{O}_K$, then $\Delta(v)^2, \Delta(w)^2 \in \mathbb{Z}$. (Recall that $\Delta(v)^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(v_i v_j))$.) Suppose $N \subseteq M$. Then there exist $c_{ij} \in \mathbb{Z}$ such that $w_i = \sum_{j=1}^{n} c_{ij} v_j$. Let $C = (c_{ij})$. Then by Theorem 1.8 we have

$$|\det(C)| = [M : N] = \#M/N = m, \text{ say},$$

as additive groups. So by Lemma 2.4 we have

$$\Delta(w)^2 = (\det(C))^2 \Delta(v)^2 = m^2 \Delta(v)^2.$$

If $M = N$ then $\det(C) = \pm 1$ by Lemma 1.7, and $\Delta(w)^2 = \Delta(v)^2$.

This allows us to make the following definition.

Definition 3.14. *Let M be any subset of $\mathcal{O}_K$ which has a $\mathbb{Z}$-basis. Define $\Delta(M)^2 := \Delta(w)^2$ for any $\mathbb{Z}$-basis w of M.*

Note that if $N \subseteq M$ then $\Delta(N)^2 = m^2 \Delta(M)^2$, and so in particular $\Delta(M)^2 | \Delta(N)^2$.

Theorem 3.15 (Integral Basis Theorem)**.** *The ring $\mathcal{O}_K$ has an integral basis (that is, a $\mathbb{Z}$-basis).*

Proof. Let $v = \{v_1, \ldots, v_n\}$ be any $\mathbb{Q}$-basis for K. Multiplying each v_i by a sufficiently large integer, we may suppose that $v \subseteq \mathcal{O}_K$. Let $M = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$. Then $\Delta(M)^2 \neq 0$ (and $\in \mathbb{Z}$) since $\{v_1, \ldots, v_n\}$ are $\mathbb{Q}$-linearly independent. Choose the basis v such that $|\Delta(M)^2|$ is minimal.

Claim: $M = \mathcal{O}_K$, so that $\{v_1, \ldots, v_n\}$ is an integral basis.

Proof of claim: Suppose there exists $\alpha \in \mathcal{O}_K$ such that $\alpha \notin M$. Certainly $\alpha = \sum_{j=1}^{n} c_j v_j$ with $c_j \in \mathbb{Q}$. Then for any j and any $m \in \mathbb{Z}$ we have $\alpha + m v_j \in \mathcal{O}_K$ but $\alpha + m v_j \notin M$. Hence by adding suitable $\mathbb{Z}$-multiples of the v_j to α we may assume that $|c_j| \leqslant 1/2$. Moreover, since $\alpha \notin M$ there exists j such that $c_j \neq 0$. Choose such a j.

Let w be a new $\mathbb{Q}$-basis for K obtained from v by replacing v_j by α. Then $w \subseteq \mathcal{O}_K$. The change of basis matrix

$$C = \begin{pmatrix} 1 & 0 & \dots & & 0 \\ 0 & 1 & \dots & & 0 \\ \vdots & & & \vdots & \\ c_1 & \dots & c_2 & \dots & c_n \\ \vdots & & & \vdots & \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

has determinant c_j. Hence

$$|\Delta(w)^2| = c_j^2 |\Delta(v)^2| < |\Delta(v)^2|,$$

by Note 3.13, contradicting the minimality of $|\Delta(v)^2|$. So such α does not exist, and $M = \mathcal{O}_K$. □

We can therefore define $\Delta(\mathcal{O}_K)^2$, as in Definition 3.14, to be $\Delta(w)^2$, where w is any integral basis of $\mathcal{O}_K$; we also define $\Delta(K)^2$ to be the same as $\Delta(\mathcal{O}_K)^2$.

The following proposition will be helpful for finding an integral basis for $\mathcal{O}_K$.

Proposition 3.16. *Let $w = \{w_1, \dots, w_n\}$ be any $\mathbb{Q}$-basis for K such that $w \subseteq \mathcal{O}_K$. Let $M = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$ and let $M \neq \mathcal{O}_K$. Then there exist p prime with $p^2 | \Delta(M)^2$ and $c_1, \dots, c_n \in \mathbb{Z}$, not all divisible by p, such that $\frac{1}{p}(c_1 w_1 + \dots + c_n w_n) \in \mathcal{O}_K$.*

Proof. Let $m = [\mathcal{O}_K : M] > 1$, so that $|\Delta(M)^2| = m^2 |\Delta(\mathcal{O}_K)^2|$. Since $m > 1$, there is a prime p dividing m, so that $p^2 | \Delta(M)^2$. Since $m = \#\mathcal{O}_K/M$ we conclude (by a theorem of Cauchy on finite groups) that $\mathcal{O}_K/M$ has an element of order p. Let $\alpha + M$ be such an element. Then $\alpha = \sum d_j w_j$ with $d_j \in \mathbb{Q}$. Moreover $p\alpha \in M$ so that all $pd_j \in \mathbb{Z}$. Hence $\alpha = \frac{1}{p} \sum_j c_j w_j$ with $c_j \in \mathbb{Z}$ not all being mutiples of p. □

We now describe how to go about finding an integral basis for $\mathcal{O}_K$, where $[K : \mathbb{Q}] = n$.

1. Let $w = \{w_1, \dots, w_n\}$ be any $\mathbb{Q}$-basis for K such that $w \subseteq \mathcal{O}_K$. Calculate $\Delta(w)^2$. Let $M = \langle w_1, \dots, w_n \rangle_{\mathbb{Z}}$. We know $M \subseteq \mathcal{O}_K$.

2. If $[\mathcal{O}_K : M] = m$, then $|\Delta(M)^2| = m^2|\Delta(\mathcal{O}_K)^2|$. If $\Delta(M)^2$ is squarefree then $m = 1$ and $\mathcal{O}_K = M$. Otherwise (and if $\mathcal{O}_K \neq M$), by Proposition 3.16, there exist p prime with $p^2|\Delta(M)^2$ and $c_1, \ldots, c_n \in \mathbb{Z}$, not all divisible by p, such that $\frac{1}{p}(c_1w_1 + \ldots + c_nw_n) \in \mathcal{O}_K$.

3. Hence if $\Delta(M)^2$ is not squarefree than for each prime p such that $p^2|\Delta(M)^2$, we look for $\alpha \in \mathcal{O}_K$ of the form $\alpha = \frac{1}{p}\sum_j c_jw_j$ with $c_j \in \mathbb{Z}$, not all divisible by p. Suppose that p does not divide c_j for $j = k$. Multiplying through by $r \in \mathbb{Z}$ such that $rc_k \equiv 1 \bmod p$, we may assume that $c_k \equiv 1 \bmod p$. Subtracting integer multiples of the w_i we may assume that $0 \leqslant c_i < p$ for all i, and so $c_k = 1$. Replacing w_k by our new α we get another basis, spanning a $\mathbb{Z}$-module M', say. The change of basis matrix is

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & \vdots & \\ c_1/p & \ldots & & \ldots & c_n/p \\ \vdots & & & \vdots & \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

and so $\Delta(M')^2 = \frac{1}{p^2}\Delta(M)^2$.

4. Repeat the whole process with M' instead of M. If α does not exist (there are only finitely many possibilities to check, since we only need to check each c_i in the range $0 \leqslant c_i < p$) then p cannot divide m. Eventually we reach a basis for which none of the available primes divide m, so that $m = 1$ and we have arrived at an integral basis.

Example 3.17 $K = \mathbb{Q}(\sqrt{d})$, d squarefree. Start with $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$. Then $\{1, \sqrt{d}\} \subseteq \mathcal{O}_K$ and

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

Since d is squarefree the only prime p such that $p^2|\Delta(\{1, \sqrt{d}\})^2$ is $p = 2$.

- Case 1: $d \equiv 1 \bmod 4$. We find $\frac{1}{2}(1+\sqrt{d}) \in \mathcal{O}_K$ (This element has minimal polynomial $x^2 - x + (1-d)/4 \in \mathbb{Z}[x]$). In this case we find

$$\Delta(\{1, \frac{1}{2}(1+\sqrt{d})\})^2 = \frac{1}{2^2}4d = d.$$

- Case 2: $d \not\equiv 1 \bmod 4$. Then $\frac{1}{2}(1+\sqrt{d}) \notin \mathcal{O}_K$ since $x^2 - x + \frac{1-d}{4} \notin \mathbb{Z}[x]$. The only other cases to check are $\frac{1}{2}, \frac{1}{2}\sqrt{d}$, which are not in $\mathcal{O}_K$. Since we did not find any "α", we conclude that 2 does not divide the index $m = [\mathcal{O}_K : \langle 1, \sqrt{d}\rangle_{\mathbb{Z}}]$. Hence $\{1, \sqrt{d}\}$ is an integral basis.

4 Cyclotomic fields

None of the proofs in this section are examinable!

Let $p > 2$ be a prime and $\zeta_p := e^{2\pi i/p}$, so that $\zeta_p^p = 1$. Let $K = \mathbb{Q}(\zeta_p)$, a *cyclotomic field*. Clearly $\zeta := \zeta_p$ satisfies

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

Lemma 4.1. *$f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Let $g(x) = f(x+1)$. It suffices to show $g(x)$ is irreducible. But

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

Since p divides all the coefficients apart from the first, but p^2 does not divide the final coefficient p, the polynomial $g(x)$ is irreducible over $\mathbb{Z}$ by Eisenstein's criterion and so over $\mathbb{Q}$ by Gauss' Lemma. □

Corollary 4.2. $[K : \mathbb{Q}] = p - 1$.

So a regular p-gon can be constructed with a ruler and compass only if $p - 1$ is a power of 2.

The roots of $x^{p-1} + x^{p-2} + \ldots x + 1$ are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. These are the conjugates of ζ, and so $f(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$.

Note 4.3

1. $\mathrm{Norm}_{K/\mathbb{Q}}(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i) = f(1) = p$
2. $\mathrm{Norm}_{K/\mathbb{Q}}(1-\zeta) = \mathrm{Norm}_{K/\mathbb{Q}}(\zeta-1)$ since $p-1$ is even. Thus $\zeta-1$ has minimal polynomial $g(x) = f(x+1)$.

   [this last statement uses: $f(x+1) = \mathrm{Norm}_{K/\mathbb{Q}}(x+1-\zeta) = \mathrm{Norm}_{K/\mathbb{Q}}(x-(\zeta-1))$ = minimal polynomial of $\zeta-1$.]

Lemma 4.4. *If* $w = \{1, \zeta, \ldots, \zeta^{p-2}\}$ *then* $\Delta(w)^2 = (-1)^{(p-1)/2}p^{p-2}$.

Proof. From Question 5 on Problem Sheet 1 we see that

$$\Delta(1, \zeta, \ldots, \zeta^{p-2})^2 = (-1)^{(p-1)(p-2)/2}\mathrm{Norm}_{K/\mathbb{Q}}(f'(\zeta)).$$

Here $K = \mathbb{Q}(\zeta)$ and

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Since p is odd the first factor reduces to $(-1)^{(p-1)/2}$. Now

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

and so

$$f'(\zeta) = \frac{-p\zeta^{p-1}}{1-\zeta}.$$

Hence from Note 4.3 above,

$$\mathrm{Norm}_{K/\mathbb{Q}}(f'(\zeta)) = \frac{\mathrm{Norm}_{K/\mathbb{Q}}(-p)\mathrm{Norm}_{K/\mathbb{Q}}(\zeta)^{p-1}}{\mathrm{Norm}_{K/\mathbb{Q}}(1-\zeta)} = \frac{(-p)^{p-1}1^{p-1}}{p} = p^{p-2}$$

as required. □

Theorem 4.5. *The set* $\{1, \zeta, \ldots, \zeta^{p-2}\}$ *is an integral basis for* $\mathcal{O}_K$.

Proof. Let $\theta = \zeta - 1$. Certainly we have $\mathbb{Z}[\theta] = \mathbb{Z}[\zeta]$. We shall show that $\{1, \theta, \ldots, \theta^{p-2}\}$ is an integral basis.

By Lemma 4.4 and Note 3.13 we see that

$$\Delta(\mathbb{Z}[\theta])^2 = \Delta(\mathbb{Z}[\zeta])^2 = (-1)^{(p-1)/2}p^{p-2}.$$

Hence p is the only prime whose square divides $\Delta(\mathbb{Z}[\theta])^2$. It follows that p is the only prime which may divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. If $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ then there exists $\alpha \in \mathcal{O}_K$ such that

$$\alpha = \frac{1}{p} \sum_{j=0}^{p-2} c_j \theta^j,$$

with $c_j \in \mathbb{Z}$ not all divisible by p. Let r be minimal such that p does not divide c_r. We may assume $c_j = 0$ for $j < r$ by subtracting integer multiples of the basis elements. Now $\alpha\theta^{p-2-r} \in \mathcal{O}_K$, since α and θ are in $\mathcal{O}_K$. Write

$$\theta^{p-2-r}\alpha = \frac{1}{p}(c_r\theta^{p-2} + c_{r+1}\theta^{p-1} + \cdots + c_{p-2}\theta^{2p-4-r}). \tag{4.1}$$

Then

$$\theta^{p-1} = -p\theta^{p-2} - \frac{p(p-1)}{2}\theta^{p-3} - \cdots - p$$

and so $p^{-1}\theta^{p-1} \in \mathcal{O}_K$. Hence by subtracting multiples of this from both sides of (4.1) we see that $p^{-1}c_r\theta^{p-2} \in \mathcal{O}_K$. However

$$\mathrm{Norm}_{K/\mathbb{Q}}\left(\frac{c_r}{p}\theta^{p-2}\right) = \left(\frac{c_r}{p}\right)^{p-1} p^{p-2} = \frac{c_r^{p-1}}{p},$$

since $\mathrm{Norm}_{K/\mathbb{Q}}(\theta) = p$ and $\mathrm{Norm}_{K/\mathbb{Q}}(c_r/p) = (c_r/p)^{p-1}$. This, finally, contradicts the fact that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_K$, since p does not divide c_r. □

5 Unique Factorisation Domains

5.1 Revision from Part A Algebra

Let R be an integral domain.

Definition 5.1.

1. *$\alpha \in R$ is a* unit *if and only if there exists $\beta \in R$ such that $\alpha\beta = 1$. The units in R form a group under multiplication; the* group of units.

2. *$\alpha, \beta \in R$ are* associates *if and only if there exists a unit $u \in R$ such that $\alpha = \beta u$.*

3. *A nonzero, non-unit element $\alpha \in R$ is* irreducible *if ($\alpha = \beta\gamma \Rightarrow \beta$ or γ is a unit). We write $\beta|\alpha$ if there exists $\gamma \in R$ such that $\alpha = \beta\gamma$.*

4. *A nonzero, non-unit element $\alpha \in R$ is* prime *if ($\alpha|\beta\gamma \Rightarrow \alpha|\beta$ or $\alpha|\gamma$).*

A prime element in R is irreducible (Problem Sheet 2).

Definition 5.2. *Let R be an integral domain. R is a* Euclidean domain *(ED) if and only if there exists a function (a Euclidean function) $d : R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ such that*

1. *For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.*

2. *For all nonzero $a, b \in R$, $d(a) \leqslant d(ab)$.*

Definition 5.3. *R is a* principal ideal domain *(PID) if and only if every ideal is principal (recall that I is an ideal if it is an additive subgroup of R and $\forall r \in R, a \in I$, $ra \in I$; furthermore I is principal if it is of the form $(\gamma) = \{r\gamma : r \in R\}$).*

Definition 5.4. *R is a* unique factorisation domain *(UFD) if and only if for all nonzero and non-unit $\alpha \in R$ there exist irreducible $\beta_1, \ldots, \beta_n \in R$ such that*

1. *$\alpha = \beta_1 \ldots \beta_n$*

2. *If $\alpha = \gamma_1 \ldots \gamma_m$ with irreducible γ_i, then $m = n$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that β_i and $\gamma_{\sigma(i)}$ are associates.*

In Part A algebra you proved:

$$R \text{ a ED} \Rightarrow R \text{ a PID} \Rightarrow R \text{ a UFD.}$$

In an integral domain R in which factorisation into irreducibles is possible then this factorisation is unique if and only if all *irreducible* elements are *prime* (Problem Sheet 2).

5.2 Some applications of unique factorisation

First, a useful lemma:

Lemma 5.5. *Let $\mathcal{O}_K$ be the ring of integers in a number field K, and $\alpha, \beta \in \mathcal{O}_K$. Then*

1. *α is a unit (in $\mathcal{O}_K$) if and only if $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.*
2. *If α and β are associates (in $\mathcal{O}_K$) then $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm \mathrm{Norm}_{K/\mathbb{Q}}(\beta)$.*
3. *If $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$ is a rational prime, i.e. a prime number in $\mathbb{Z}$, then α is irreducible in $\mathcal{O}_K$.*

Proof. 1. Proposition 3.10.

2. We have $\alpha = u\beta$ with u a unit, and so:
   $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K/\mathbb{Q}}(u)\mathrm{Norm}_{K/\mathbb{Q}}(\beta) = \pm \mathrm{Norm}_{K/\mathbb{Q}}(\beta)$, by part 1.
3. Let $\alpha = \gamma\delta$. Then $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = p = \mathrm{Norm}_{K/\mathbb{Q}}(\gamma)\mathrm{Norm}_{K/\mathbb{Q}}(\delta)$ for some prime $p \in \mathbb{Z}$. The result now follows from 1.

□

The converses of 2 and 3 are false (see later the proof of Proposition 5.8).

Application (1). Take $K = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}[i]$. This is a UFD (the "Gaussian Integers") — see Problem Sheet 2. We have $\mathrm{Norm}_{K/\mathbb{Q}}(a + bi) = a^2 + b^2$, so that the only units are $\pm 1, \pm i$, by Proposition 3.10.

Theorem 5.6 (Fermat/Euler)**.** *If p is a prime, and $p \equiv 1 \bmod 4$, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$, and this decomposition is unique. [here 'unique' means: up to $\pm$ and up to swapping a and b.]*

Proof. Assume $p \equiv 1 \bmod 4$. Then $\left(\frac{-1}{p}\right) = 1$, so there exists $r \in \mathbb{Z}$ such that $p | 1 + r^2$ (e.g. $r = g^{(p-1)/4} \bmod p$ where g is a primitive root modulo p). In $\mathbb{Z}[i]$, we have $p|(1 + ri)(1 - ri)$. If p is irreducible in the UFD $\mathbb{Z}[i]$, then $p|(1 + ri)$ or $p|(1 - ri)$, because any irreducible is prime. However p cannot divide $1 + ri$, for example, because $\frac{1}{p} + \frac{r}{p}i \notin \mathcal{O}_K$. Hence there exist $(a + bi), (c + di) \in \mathbb{Z}[i]$, neither units, such that $p = (a + bi)(c + di)$. Taking norms

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

Now $\mathbb{Z}$ is a UFD and neither $a+bi$ or $c+di$ has norm ± 1, giving $p = a^2+b^2 = (a+bi)(a-bi)$. This yields the existence part of the theorem.

If $a+bi = \alpha\beta$ in $\mathbb{Z}[i]$ then, taking norms, we find that

$$p = \text{Norm}(\alpha)\text{Norm}(\beta).$$

Thus α or β must be a unit. Hence $a+bi$ is irreducible in $\mathbb{Z}[i]$, and similarly for $a-bi$. Thus $p = (a+bi)(a-bi)$ is the unique factorisation of p into irreducibles.

If also $p = e^2+f^2 = (e+fi)(e-fi)$, then $e+fi$ is an associate of either $a+bi$ or $a-bi$, so that $e+fi$ is one of $a+bi, -(a+bi), i(a+bi), -i(a+bi)$, or $a-bi, -(a-bi), i(a-bi), -i(a-bi)$. It follows that $\{a^2, b^2\} = \{e^2, f^2\}$, which proves uniqueness. □

Application (2). Take $K = \mathbb{Q}(\sqrt{-2})$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. This is a UFD (Problem Sheet 2). We have $\text{Norm}_{K/\mathbb{Q}}(a+b\sqrt{-2}) = a^2+2b^2$, so that the only units are ± 1.

Theorem 5.7 (Fermat/Euler)**.** *The only integer solutions of* $y^2+2 = x^3$ *are* $x = 3, y = \pm 5$.

Proof. If y were even then x would be even, giving $8|y^2+2$, which is impossible since $4|y^2$. So y is odd.

We have $(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$. Suppose there is an irreducible element α which divides both $y+\sqrt{-2}$ and $y-\sqrt{-2}$. Then α divides the difference $2\sqrt{-2} = -(\sqrt{-2})^3$. However $\sqrt{-2}$ is irreducible since its norm is 2, which is prime in $\mathbb{Z}$. So we must have $\alpha = \pm\sqrt{-2}$. Now

$$\alpha | y+\sqrt{-2} \Rightarrow \sqrt{-2} | y \Rightarrow 2|y^2,$$

a contradiction, since y is odd. Hence $y+\sqrt{-2}$ and $y-\sqrt{-2}$ have no irreducible factor in common. Unique factorisation therefore implies that $y+\sqrt{-2}$ and $y-\sqrt{-2}$ are associates of cubes. Since the only units are ± 1, which are both cubes, we deduce that $y \pm \sqrt{-2}$ are both cubes.

We now have

$$y+\sqrt{-2} = (a+b\sqrt{-2})^3$$

$$= a^3 + 3a^2b\sqrt{-2} + 3ab^2(-2) + b^3(-2)\sqrt{-2} = (a^3-6ab^2) + (3a^2b-2b^3)\sqrt{-2},$$

and hence $b(3a^2-2b^2) = 1$. Thus $b = \pm 1$, $a = \pm 1$, and so

$$y = a^3 - 6ab^2 = a(a^2-6b^2) = \pm 5 \text{ and } x = 3.$$

□

More theorems of Fermat

1. If prime $p \equiv 1$ or $3 \bmod 8$ then $p = x^2 + 2y^2$ uniquely (Problem Sheet 2).

2. If prime $p \equiv 1 \bmod 3$ then $p = x^2 + 3y^2$.

Proposition 5.8. *For $K = \mathbb{Q}(\sqrt{-5})$ the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is not a UFD.*

Proof. We have the factorisation $6 = 2.3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$ in $\mathcal{O}_K$. We claim that the elements in $S = \{2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}\}$ are irreducible in $\mathcal{O}_K$. Now

$$\mathrm{Norm}_{K/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2$$

so the norms of the elements in S are $4, 9, 6, 6$, respectively. For $\alpha \in S$, if $\alpha = \beta\gamma$ with non-units $\beta, \gamma \in \mathcal{O}_K$, then $\mathrm{Norm}(\beta), \mathrm{Norm}(\gamma) = \pm 2, \pm 3$. However there are *no* elements in $\mathcal{O}_K$ with norm $\pm 2, \pm 3$, since $a^2 + 5b^2 = \pm 2, \pm 3$ has no solutions in integers a, b. This proves the claim.

By Lemma 5.5 Part 2, the elements $2, 3$ cannot be associates of $1 + \sqrt{-5}$, $1 - \sqrt{-5}$. So we have two distinct factorisations into irreducibles. □

6 Unique Factorisation of Ideals

To recover unique factorisation we will use ideals instead of elements. Recall that an ideal I of a commutative ring R is a non-empty subset for which $a \pm b \in I$ whenever $a, b \in I$, and for which $ra \in I$ whenever $r \in R$ and $a \in I$.

6.1 Statement of the Unique Factorisation Theorem

Definition 6.1. *Let R be an integral domain, and let I, J be ideals of R. Then $IJ := \left\{ \sum_{i=1}^{k} a_i b_i : a_i \in I, b_i \in J, k \geqslant 1 \right\}$.*

Observe that IJ consists of finite sums of arbitrary length k. We write

$$(a) := \{ra : r \in R\}$$

for the *principal ideal* generated by a.

Note 6.2 It is easy to check that:

1. IJ is an ideal of R,
2. If $I = (\alpha)$ and $J = (\beta)$, then $IJ = (\alpha\beta)$.
3. If $I = (\alpha)$ then $IJ = (\alpha)J = \{\alpha j : j \in J\}$.

Definition 6.3. *Let R be an integral domain. An ideal I of R is* prime *if it is proper and ($ab \in I \Rightarrow a \in I$ or $b \in I$). (recall: an ideal $I \lhd R$ is proper if $I \neq R$).*

Comment. We shall prove later (Theorem 6.26) that any nonzero proper ideal A of $\mathcal{O}_K$ can be written as a product of prime ideals $A = P_1 P_2 \dots P_r$ and this factorisation is unique up to the order of the factors.

Definition 6.4. *Let K, L be fields with $K \subseteq L$. Let I be an ideal of $\mathcal{O}_K$. Then $I \cdot \mathcal{O}_L$ is defined to be the ideal of $\mathcal{O}_L$ generated by products of the form $i\ell$, such that $i \in I, \ell \in \mathcal{O}_L$ (sometimes called the image of I in $\mathcal{O}_L$). Note that, for any ideals I, J of $\mathcal{O}_K$, any $n \in \mathbb{N}$ and any principal ideal $(a) = a\mathcal{O}_K$ of $\mathcal{O}_K$, $(IJ) \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)(J \cdot \mathcal{O}_L)$, $I^n \cdot \mathcal{O}_L = (I \cdot \mathcal{O}_L)^n$ and $(a) \cdot \mathcal{O}_L = a\mathcal{O}_L$, the principal ideal of $\mathcal{O}_L$ generated by the same element (Problem Sheet 3).*

6.2 Finiteness of the class number

Definition 6.5. *If I, J are nonzero ideals of $\mathcal{O}_K$, we write $I \sim J$ (and say that I is equivalent to J) if there exist $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$ such that $I(\alpha) = J(\beta)$.*

Lemma 6.6. *The relation $\sim$ is an equivalence relation on the set of nonzero ideals of $\mathcal{O}_K$.*

Proof. Problem Sheet 3. □

Definition 6.7. *Equivalence classes in $\mathcal{O}_K$ under $\sim$ are called* ideal classes. *Let C_K denote the set of ideal classes. The cardinality $h_K = |C_K|$ is the* class number *of K.*

We shall prove shortly that $h_K < \infty$.

Proposition 6.8. *We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a PID.*

Proof. ($\Leftarrow$): Suppose $\mathcal{O}_K$ is a PID. Then for any nonzero $I \subseteq \mathcal{O}_K$, there exists $\alpha \in \mathcal{O}_k$ such that $I = (\alpha)$. Then $I(1) = \mathcal{O}_K(\alpha)$, so $I \sim \mathcal{O}_K$.

($\Rightarrow$): Suppose $h_K = 1$. Then for all $I \lhd \mathcal{O}_K$ there exist $\alpha, \beta \in \mathcal{O}_K$ such that

$$I(\alpha) = \mathcal{O}_K(\beta). \tag{6.1}$$

Now the right hand side is just (β). Since $\beta \in (\beta)$ from Note 6.2 (3), we see that $\beta = i\alpha$ for some $i \in I$. Hence $\beta/\alpha \in I \subseteq \mathcal{O}_K$. We claim $I = (\beta/\alpha)$. Certainly $(\beta/\alpha) \subseteq I$. Also, $a \in I \implies a\alpha \in I(\alpha) = (\beta)$, so $a\alpha = r\beta$, for some $r \in \mathcal{O}_K$, giving: $a = r\beta/\alpha$, and so $a \in (\beta/\alpha)$; hence $I \subseteq (\beta/\alpha)$. □

Lemma 6.9. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $I \cap \mathbb{Z} \neq \{0\}$.*

Proof. Choose any nonzero $\alpha \in I$. Suppose that $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$ (all $a_i \in \mathbb{Z}$) with $a_0 \neq 0$. Then $a_0 = -\alpha(a_1 + \cdots + \alpha^{d-1}) \in I \cap \mathbb{Z}$. □

Lemma 6.10. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then $\mathcal{O}_K/I$ is a finite ring.*

Proof. Choose any nonzero $a \in I \cap \mathbb{Z}$. Then $\mathcal{O}_K \supseteq I \supseteq (a)$. The map from $\mathcal{O}_K/(a)$ to $\mathcal{O}_K/I$ which takes $\alpha + (a)$ to $\alpha + I$ is well-defined and onto. It therefore suffices to show that $\mathcal{O}_K/(a)$ is finite. Let $w = \{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then $\mathcal{O}_K/(a)$ is isomorphic as an additive group to $\oplus_{i=1}^n (\mathbb{Z}/(a))w_i \cong (\mathbb{Z}/(a))^n$, where $n := [K : \mathbb{Q}]$. So $\#\mathcal{O}_K/(a) = a^n < \infty$. □

Definition 6.11. *The* norm *of I is defined as $N(I) := \#\mathcal{O}_K/I$.*

Proposition 6.12. *Let $\sigma : K \to K$ be an automorphism. Then $I = (\alpha_1, \ldots, \alpha_n)$ and $I^\sigma = (\alpha_1^\sigma, \ldots, \alpha_n^\sigma)$ have the same norm. [So, for example, in $\mathcal{O}_{\mathbb{Q}(\sqrt{7})} = \mathbb{Z}[\sqrt{7}]$, $N\big((3, 1+\sqrt{7})\big) = N\big((3, 1-\sqrt{7})\big)$.]*

Proof. Problem Sheet 4. □

Proposition 6.13. *If $I = (\alpha)$ then $N(I) = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$.*

Proof. Let $w = \{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. Then $\alpha w := \{\alpha w_1, \ldots, \alpha w_n\}$ will be a $\mathbb{Z}$-basis for $I = (\alpha)$. Directly from the definition one sees that $\Delta(\alpha w) = \Big(\prod_{i=1}^n \sigma_i(\alpha)\Big)\Delta(w) = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha)\Delta(w)$. However I is an additive subgroup of $\mathcal{O}_K$ with index $N(I)$, by Definition 6.11. Thus if αw_i is expressed in terms of w as $\alpha w_i = \sum c_{ij} w_j$, with $c_{ij} \in \mathbb{Z}$, then we will have $N(I) = |\det(c_{ij})|$, by Theorem 1.8. On the other hand, we have $\Delta(\alpha w) = \det(c_{ij})\Delta(w)$, by Lemma 2.4. Hence $N(I) = |\Delta(\alpha w)/\Delta(w)| = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$. □

Lemma 6.14 (Hurwitz)**.** *Let K be a number field with $[K:\mathbb{Q}] = n$. Then there exists a positive integer M, depending only on the choice of integral basis for $\mathcal{O}_K$, such that for any $\gamma \in K$, there exist $w \in \mathcal{O}_K$ and $1 \leqslant t \leqslant M$, $t \in \mathbb{Z}$ with*

$$\left|\mathrm{Norm}_{K/\mathbb{Q}}(t\gamma - w)\right| < 1.$$

Remark. If one could take $M = 1$ then for any $\gamma \in K$ there would be a $w \in \mathcal{O}_K$ with $|\mathrm{Norm}_{K/\mathbb{Q}}(\gamma - w)| < 1$. This is equivalent to the Euclidean property for the norm function. That is to say, if one can take $M = 1$ then $\mathcal{O}_K$ is a Euclidean Domain with Euclidean function $d(\alpha) = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$.

In general one can regard Hurwitz's lemma as providing a statement weaker than the Euclidean property, but valid for any number field.

Proof. Let $\{w_1, \ldots, w_n\}$ be an integral basis for $\mathcal{O}_K$. For any $\gamma \in K$ we write $\gamma = \sum_{i=1}^n \gamma_i w_i$ with $\gamma_i \in \mathbb{Q}$. Let $\gamma_i = a_i + b_i$ with $a_i \in \mathbb{Z}$ and $0 \leqslant b_i < 1$. We define (for the duration of this proof only) $[\gamma] = \sum_{i=1}^n a_i w_i$ and $\{\gamma\} = \sum_{i=1}^n b_i w_i$. Hence we will have $\gamma = [\gamma] + \{\gamma\}$ and $[\gamma] \in \mathcal{O}_K$ for all $\gamma \in K$.

Let $w_i^{(1)}, \ldots, w_i^{(n)}$ be the $K/\mathbb{Q}$-conjugates of w_i, and set

$$C := \prod_{j=1}^n (\sum_{i=1}^n |w_i^{(j)}|).$$

Then if $\gamma = \sum_{i=1}^n \gamma_i w_i$ and $\mu := \max_{1 \leqslant i \leqslant n} |\gamma_i|$, we have

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\gamma)| = \left| \prod_{j=1}^n \left(\sum_{i=1}^n \gamma_i w_i^{(j)} \right) \right| \leqslant \prod_{j=1}^n \left(\sum_{i=1}^n \mu \left| w_i^{(j)} \right| \right) = C\mu^n. \tag{6.2}$$

Choose m to be the first integer after $C^{1/n}$ and let $M = m^n$, so that M depends only on our choice of $w_1 \ldots, w_n$. Define a linear map $\phi : K \to \mathbb{R}^n$ by

$$\phi \left(\sum_{i=1}^n \gamma_i w_i \right) = (\gamma_1, \ldots, \gamma_n). \tag{6.3}$$

Now $\phi(\{\gamma\})$ lies in the unit cube

$$B := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \,:\, 0 \leqslant x_i < 1\}.$$

Partition B into m^n subcubes of side $1/m$, and consider the points $\phi(\{k\gamma\})$, for $0 \leqslant k \leqslant m^n$. There are $m^n + 1$ such points and only m^n available

subcubes. Hence, by the "Pigeon-hole principle", there are two points lying in the same subcube. Suppose these correspond to $k = h$ and l, with $h > l$. Letting $t = h - l$, we have $1 \leqslant t \leqslant m^n = M$. It follows that $t\gamma = w + \delta$ where $w := [h\gamma] - [l\gamma] \in \mathcal{O}_K$ and $\delta := \{h\gamma\} - \{l\gamma\}$ with

$$\phi(\delta) \in [-1/m, 1/m]^n.$$

By (6.2) and (6.3), we now find that

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\delta)| \leqslant C(1/m)^n < 1,$$

since we took $m > C^{1/n}$. The lemma then follows, since $\delta = t\gamma - w$. □

Theorem 6.15. *The class number $h_K = \#C_K$ is finite.*

Proof. Let I be a nonzero ideal of $\mathcal{O}_K$. Choose $0 \neq \beta \in I$ such that $|\mathrm{Norm}(\beta)|$ is minimal, and let M be as in Hurwitz's lemma. Now consider an arbitrary $\alpha \in I$, and apply the lemma with $\gamma := \alpha/\beta$. Then there exists an integer t in the range $1 \leqslant t \leqslant M$ such that $|\mathrm{Norm}(t(\alpha/\beta) - w)| < 1$ with $w \in \mathcal{O}_K$. Thus $t\alpha - \beta w \in I$ and $|\mathrm{Norm}(t\alpha - \beta w)| < |\mathrm{Norm}(\beta)|$. This contradicts the minimality of $|\mathrm{Norm}(\beta)|$ unless $t\alpha - w\beta = 0$. We therefore deduce that $t\alpha \in (\beta)$. In general the integer t will be different for different values of α, but we can always deduce that $M!\alpha \in (\beta)$. Since α was arbitrary we conclude that

$$(M!)I \subseteq (\beta). \tag{6.4}$$

Let

$$J := \{1/\beta \times M! \times \alpha \,:\, \alpha \in I\}.$$

Then J is an ideal; the only non-trivial part is checking that $J \subseteq \mathcal{O}_K$, but this follows from (6.4). Moreover $(\beta)J = (M!)I$, so that $I \sim J$.

By taking $\alpha = \beta$ in the definition of J we see that $\mathcal{O}_K \supseteq J \supseteq (M!)$. By Lemma 6.10 we know that $\mathcal{O}_K/(M!)$ is finite, and so there are only finitely many possibilities for J. Hence I is equivalent to one of finitely many ideals. It follows that there are finitely many equivalence classes. □

6.3 Ideal classes form a group under multiplication

Lemma 6.16. *If $I, J \subseteq \mathcal{O}_K$ are ideals, with I nonzero, and $JI = I$ then $J = \mathcal{O}_K$.*

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis for I. Since $I = JI$ there exist $b_{ij} \in J$ such that $\alpha_i = \sum_{j=1}^{n} b_{ij}\alpha_j$. Hence $\det(b_{ij} - \delta_{ij}) = 0$, and expanding this determinant out, one sees that all terms lie in J, except the product of the 1's in the identity matrix. Hence $1 \in J$ and so $J = (1) = \mathcal{O}_K$. □

Lemma 6.17. *If I is a nonzero ideal of $\mathcal{O}_K$, and $w \in K$ with $wI \subseteq I$, then $w \in \mathcal{O}_K$.*

Proof. Take $M = I$ in Lemma 3.6. □

Lemma 6.18. *If I, J are nonzero ideals in $\mathcal{O}_K$, and $w \in \mathcal{O}_K$ is such that $(w)I = JI$, then $(w) = J$.*

Proof. Choose an arbitrary $\beta \in J$. Then $(w)I \supseteq (\beta)I$, so that $\{\beta/w\}I \subseteq I$. By Lemma 6.17 we therefore have $\beta/w \in \mathcal{O}_K$, and so $\beta \in (w)$. Since β was arbitrary we deduce that $J \subseteq (w)$, giving that $w^{-1}J$ is an ideal in $\mathcal{O}_K$. We then have $I = (w^{-1}J)I$ and so by Lemma 6.16, we obtain $w^{-1}J = \mathcal{O}_K$, so that $J = (w)$. □

Proposition 6.19. *For any nonzero ideal $I \subseteq \mathcal{O}_K$, there exists k such that $1 \leqslant k \leqslant h_K$ and I^k is principal.*

Proof. Among the $h_K + 1$ ideals $\{I^i : 1 \leqslant i \leqslant h_K + 1\}$ some two must be equivalent. Suppose that $I^i \sim I^j$ with $j > i$. Then $(\alpha)I^i = (\beta)I^j$ for some $\alpha, \beta \in \mathcal{O}_K$. Let $k = j - i$ and $J = I^k$. Then $(\alpha)I^i = (\beta)I^iJ \subseteq (\beta)I^i$, so that $\{\alpha/\beta\}I^i \subseteq I^i$. By Lemma 6.17 we have $\alpha/\beta \in \mathcal{O}_K$. Also $(\alpha/\beta)I^i = JI^i$ and so, by Lemma 6.18, $(\alpha/\beta) = J$. It follows that $J = I^k$ is principal. □

Proposition 6.20. *The ideal classes form a group C_K. It is called the* class group *of K and its order is the class number h_K.*

Proof. Given two ideal classes $[I], [J]$ we define the product $[I] \cdot [J] := [IJ]$. This is well-defined (easy). The element $[\mathcal{O}_K]$ acts as an identity, and associativity is easily verified. Thus it remains to show the existence of inverses. Let $[I]$ be the class of I, and $[\mathcal{O}_K] = [(1)]$ the identity. However, given $[I] \in C_K$, if I^k is principal, then $[I^{k-1}]$ is an inverse of $[I]$. □

6.4 Proof of the unique factorisation theorem

Lemma 6.21 (Cancellation Lemma)**.** *Let $A, B, C \subseteq \mathcal{O}_K$ be nonzero ideals with $AB = AC$. Then $B = C$.*

Proof. Let k be such that $A^k = (\alpha)$ is principal. Multiplying by A^{k-1}, we get $(\alpha)B = (\alpha)C$, and so $B = C$. □

Definition 6.22. *Let $A, B \subseteq \mathcal{O}_K$ be nonzero ideals. We write $B|A$ if there exists an ideal $C \subseteq \mathcal{O}_K$ such that $A = BC$.*

Proposition 6.23. *Let A, B be nonzero ideals in $\mathcal{O}_K$. Then $B \supseteq A$ if and only if there exists an ideal C such that $A = BC$, i.e., $B|A$.*

So to *contain* is to *divide*!

Proof. Let $k \geqslant 1$ be such that $B^k = (\beta)$ is principal. If $B \supseteq A$ then we have $B^{k-1}A \subseteq B^k = (\beta)$. Let $C := \{1/\beta\}B^{k-1}A$, so that $C \subseteq \mathcal{O}_K$ is an ideal. Then $BC = B\{1/\beta\}B^{k-1}A = A$. Hence $B|A$. Conversely, if $B|A$ then $A = BC'$, for some C'; furthermore $BC' \subseteq B$, since B is an ideal. Hence $B \supseteq A$. □

Lemma 6.24. *Let A, B be nonzero ideals, and P a prime ideal of $\mathcal{O}_K$ such that $P|AB$. Then either $P|A$ or $P|B$.*

Proof. Suppose that $P|AB$ and P does not divide A. We must show that $P|B$. Now $P \supseteq AB$ but $P \not\supseteq A$, so there exists $\alpha \in A$ with $\alpha \notin P$. For any $\beta \in B$ we will have $\alpha\beta \in P$, since $P \supseteq AB$. However P is a prime ideal, so if $\alpha\beta \in P$ one of α or β must belong to P. In our case we conclude that $\beta \in P$. Hence $P \supseteq B$, so that $P|B$ by Proposition 6.23. □

Note 6.25 In general, for any ring, every maximal ideal is prime. In the case of rings $\mathcal{O}_K$ the converse is true for nonzero ideals. To prove this, note that if P is a nonzero prime ideal of $\mathcal{O}_K$ then $\mathcal{O}_K/P$ is a *finite* integral domain. Any finite integral domain is a field, and hence $\mathcal{O}_K/P$ is a field. It then follows that P is maximal.

This following key theorem is due to Dedekind — as is most of the theory of ideals in number fields.

Theorem 6.26. *(Unique Factorisation Theorem for ideals of $\mathcal{O}_K$). Let A be any nonzero proper ideal of $\mathcal{O}_K$. Then there exist prime ideals $P_1, \ldots, P_r$ such that $A = P_1 \ldots P_r$. The factorsiation is unique up to the order of the factors; that is, if $A = Q_1 \ldots Q_s$ is another prime ideal factorisation then $s = r$ and there exists a permutation σ such that $Q_i = P_{\sigma(i)}$, $1 \leqslant i \leqslant r$.*

Proof. Assume not every ideal A (nonzero and proper) has a prime factorisation. Let A be such an ideal with $N(A)$ minimal. There exists a maximal (hence prime) ideal P_1 containing A. So Proposition 6.23 shows that there is an ideal C with $A = P_1C$.

If $A = C$ then $P_1C = C$ and $P_1 = \mathcal{O}_K$, by Lemma 6.16. This is clearly impossible. Hence $A \subseteq C$, and by the definition of the norm (Definition 6.11) we have $N(A) = N(C)[C : A] > N(C)$. Hence, by our minimality assumption for A, one can factor C into prime ideals as $C = P_2 \dots P_r$ (or $C = \mathcal{O}_K$ and $A = P_1$). Therefore $A = P_1 \dots P_r$, a contradiction. Hence every nonzero proper ideal has a prime factorisation.

Suppose

$$A = P_1P_2 \dots P_r = Q_1Q_2 \dots Q_s.$$

Now $P_1|Q_1 \dots Q_s$. Let k be minimal such that $P_1|Q_1 \dots Q_k$. If $k = 1$ then $P_1|Q_1$. If $k > 1$ then $P_1|(Q_1 \dots Q_{k-1})Q_k$, but P_1 does not divide $Q_1 \dots Q_{k-1}$. Since P_1 is prime, we must have $P_1|Q_k$. We therefore have $P_1|Q_k$ (so $P_1 \supseteq Q_k$) in either case. Since Q_k is maximal this implies that $P_1 = Q_k$. Without loss of generality we take $k = 1$ and then, by the cancellation lemma 6.21, we have $P_2 \dots P_r = Q_2 \dots Q_s$. We may now repeat the process until every P_i has been shown to equal some Q_j. □

Note that the prime ideals which occur in the factorisation of A are those which contain A.

Note also that if $u \in \mathcal{O}_K$ is a unit, then $(u) = \mathcal{O}_K$ and so $(u)I = I$ for any ideal $I \subseteq R$; that is to say, ideals "absorb" units. Thus "unique factorisation of ideals" is simpler to describe than "unique factorisation of elements". If $\mathcal{O}_K$ is a PID then the theorem implies directly that it is a UFD. However, in general $\mathcal{O}_K$ will not be a PID, that is to say, not all ideals will be principal.

Note 6.27

At this point we explain how to multiply ideals in practice. It is a fact, which we will not prove here, that every ideal can be written with at most 2 generators. We shall write (α, β) for the ideal

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

Then the product

$$(\alpha, \beta)(\gamma, \delta) = \{\sum_1^n \mu_i\nu_i : \ \mu_i \in (\alpha, \beta), \ \nu_i \in (\gamma, \delta)\}$$

clearly contains the four elements $\alpha\gamma$, $\alpha\delta$, $\beta\gamma$, $\beta\delta$, giving

$$(\alpha\gamma,\ \alpha\delta,\ \beta\gamma,\ \beta\delta) \subseteq (\alpha,\beta)(\gamma,\delta).$$

Moreover any term $\mu_i\nu_i$ in the sum above is of the shape $(\alpha a+\beta b)(\gamma c+\delta d) \in (\alpha\gamma,\ \alpha\delta,\ \beta\gamma,\ \beta\delta)$, so that

$$(\alpha,\beta)(\gamma,\delta) = \{\sum_1^n \mu_i\nu_i :\ \mu_i \in (\alpha,\beta),\ \nu_i \in (\gamma,\delta)\} \subseteq (\alpha\gamma,\ \alpha\delta,\ \beta\gamma,\ \beta\delta).$$

Thus we must have

$$(\alpha,\beta)(\gamma,\delta) = (\alpha\gamma,\ \alpha\delta,\ \beta\gamma,\ \beta\delta).$$

To reduce the 4 generators on the right to at most 2 requires *ad hoc* methods (given only the technology from the present course). As an example consider

$$(11, 3+\sqrt{-13})(11, 3-\sqrt{-13}) = (121, 33-11\sqrt{-13}, 33+11\sqrt{-13}, 22).$$

All the generators belong to (11), and so

$$(121, 33-11\sqrt{-13}, 33+11\sqrt{-13}, 22) \subseteq (11).$$

On the other hand 11 is the highest common factor of 121 and 22, over $\mathbb{Z}$, so that one can solve $11 = 121m + 22n$ over $\mathbb{Z}$. It follows that

$$(11) \subseteq (121, 22) \subseteq (121, 33-11\sqrt{-13}, 33+11\sqrt{-13}, 22).$$

We can therefore conclude that

$$(121, 33-11\sqrt{-13}, 33+11\sqrt{-13}, 22) = (11)$$

and hence that

$$(11, 3+\sqrt{-13})(11, 3-\sqrt{-13}) = (11).$$

6.5 Multiplicativity of the Norm

Definition 6.28. *Let A, B be ideals. We define*

$$A + B := \{a + b \,:\, a \in A, b \in B\},$$

which is clearly an ideal. We say that A, B are coprime *if $A + B = \mathcal{O}_K$.*

This will occur if and only if there does not exist a maximal P such that $P \supseteq A$ and $P \supseteq B$. Thus, A and B are coprime if and only if they have no prime ideal factor in common.

Note also that, if A, B are coprime and $A|BC$ then $A|C$; furthermore, if A, B are coprime and $A|I, B|I$ then $AB|I$ (Problem Sheet 2).

Lemma 6.29. *If A and B are coprime then $AB = A \cap B$.*

Proof. Certainly $AB \subseteq A \cap B$, and so $A \cap B | AB$. On the other hand, since $A|A \cap B$ and $B|A \cap B$, it follows by coprimality and unique factorisation that $AB|A \cap B$. These two divisibility relations suffice for the proof. □

Lemma 6.30. *If nonzero A, B are coprime then $N(AB) = N(A)N(B)$.*

Proof. The Chinese Remainder Theorem gives

$$\mathcal{O}_K/(A \cap B) \cong \mathcal{O}_K/A \oplus \mathcal{O}_K/B$$

when $A + B = \mathcal{O}_K$, (that is to say, when they are coprime). By the previous lemma, $A \cap B = AB$. The lemma then follows on considering the cardinality of the two sides. □

Lemma 6.31. *If P is a nonzero prime ideal of $\mathcal{O}_K$ and $i \geqslant 0$ then $\#P^i/P^{i+1} = \#\mathcal{O}_K/P$.*

Proof. We have $P^{i+1} \subseteq P^i$, but by the Cancellation Lemma 6.21, we cannot have $P^i = P^{i+1}$. We may therefore choose $\pi \in P^i$ with $\pi \notin P^{i+1}$. Then $P^i \supseteq (\pi)$. Let $(\pi) = P^i B$ with B not divisible by P. Define a homomorphism of additive groups by

$$\begin{array}{rccc} \theta : & \mathcal{O}_K & \to & P^i/P^{i+1} \\ & \alpha & \mapsto & \overline{\alpha\pi}. \end{array}$$

(So one multiplies α by π and then reduces modulo P^{i+1}.) We now have

$$\theta(\alpha) = 0 \Leftrightarrow \alpha\pi \in P^{i+1} \Leftrightarrow (\alpha\pi) \subseteq P^{i+1} \Leftrightarrow (\alpha)P^i B \subseteq P^{i+1}$$

$$\Leftrightarrow P^{i+1}|(\alpha)P^iB \Leftrightarrow P|B(\alpha) \Leftrightarrow P|(\alpha).$$

Hence $\ker\theta = P$.

It now suffices to show that θ is surjective. However

$$(\pi) + P^{i+1} = P^iB + P^{i+1} = P^i$$

since $B + P = \mathcal{O}_K$. Thus, given any $\beta + P^{i+1} \in P^i/P^{i+1}$ (so that $\beta \in P^i$) there exist $\alpha \in \mathcal{O}_K$ and $\gamma \in P^{i+1}$ such that $\alpha\pi + \gamma = \beta$. We then have $\theta(\alpha) = \beta + P^{i+1}$, as required. Finally, the First Isomorphism Theorem for groups gives that:

$$\mathcal{O}_K/P \cong \mathcal{O}_K/\ker\theta \cong \mathrm{im}\theta = P^i/P^{i+1}.$$

Taking orders of both sides gives the required result. □

Corollary 6.32. *If P is a nonzero prime ideal and $e \geqslant 1$ then $N(P^e) = N(P)^e$.*

Proof. Considering $\mathcal{O}_K$ and P^i as additive groups we have

$$N(P^e) = \#\mathcal{O}_K/P^e = \#\mathcal{O}_K/P \cdot \#P/P^2 \cdot \cdots \cdot \#P^{e-1}/P^e$$

$$= (\#\mathcal{O}_K/P)^e = N(P)^e.$$

□

Corollary 6.33. *If $A = \prod_i P_i^{e_i}$, (P_i being distinct nonzero prime ideals), then we have $N(A) = \prod N(P_i)^{e_i}$.*

Proof. Use the corollary above and Lemma 6.30. □

From the Unique Factorisation Theorem 6.26 and this last corollary we deduce:

Proposition 6.34. *If A, B are nonzero ideals then $N(AB) = N(A)N(B)$.*

Note that if $N(I) = p$, a rational prime, then I is automatically prime. The converse is not true, but we shall soon see that every prime ideal P does have $N(P) = p^k$ for some rational prime p and integer k.

Example 6.35 What happens in $\mathbb{Z}[\sqrt{-5}]$? Recall that

$$6 = 2 \times 3 = [1 - \sqrt{-5}] \times [1 + \sqrt{-5}].$$

In terms of ideals we write this as

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

Let $P_1 = (2, 1 + \sqrt{-5})$, $P_2 = (2, 1 - \sqrt{-5})$, $Q_1 = (3, 1 + \sqrt{-5})$ and $Q_2 = (3, 1 - \sqrt{-5})$ where $(\alpha, \beta) := \{r\alpha + s\beta : r, s \in \mathcal{O}_K\}$. Now

$$(2) = (4, 6) \subseteq P_1P_2 \subseteq (2, 6) = (2)$$

giving $P_1P_2 = (2)$. We have $N((2)) = \text{Norm}(2) = 4$, and so $N(P_1)N(P_2) = 4$. Moreover an easy calculation shows that $a \equiv b \bmod 2$ whenever $a + b\sqrt{-5} \in P_i$, and so $P_i \neq \mathcal{O}_K$. We therefore deduce that $N(P_1) = N(P_2) = 2$. Similarly $(3) = (9, 6) \subseteq Q_1Q_2 \subseteq (3, 6) = (3)$, so that $Q_1Q_2 = (3)$, and $N(Q_1) = N(Q_2) = 3$. It follows that P_1, P_2, Q_1, Q_2 are all prime ideals. (In fact, $P_1 = P_2$, e.g. $1 - \sqrt{-5} = 2.1 - (1 + \sqrt{-5}).1 \in P_1$.)

We also have $P_1, Q_1 \supseteq (1+\sqrt{-5})$ and $P_2, Q_2 \supseteq (1-\sqrt{-5})$. Consideration of norms then shows that $(1 + \sqrt{-5}) = P_1Q_1$ and $(1 - \sqrt{-5}) = P_2Q_2$. Thus

$$(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ becomes } P_1P_2Q_1Q_2 = P_1Q_1P_2Q_2,$$

demonstrating that we have the same factorisation into ideals, even though the factorisations into irreducibles are different.

7 Decomposition into prime ideals

Let K be a number field of degree $[K : \mathbb{Q}] = n$. Let P be a nonzero prime ideal of $\mathcal{O}_K$. Then $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and so is of the form $p\mathbb{Z}$ for some rational prime p. We therefore have $P \supseteq p\mathcal{O}_K = (p)$. We say that P *lies above* the prime p.

Suppose that

$$(p) = P_1^{e_1} \dots P_r^{e_r}$$

where $P_1, \dots, P_r$ are distinct prime ideals in $\mathcal{O}_K$. Then $P_1, \dots, P_r$ are the prime ideals lying above the rational prime p. Taking norms we have

$$p^n = N(P_1)^{e_1} \dots N(P_r)^{e_r}$$

Hence, each $N(P_i) = p^{f_i}$ and $\sum_{i=1}^{r} e_i f_i = n$.

Note also that P must be one of the P_i and so $N(P)$ is a power of p.

Definition 7.1. *The integer e_i is called the* ramification index *of P_i. If $e_i > 1$ we say that P_i is* ramified. *If some $e_i > 1$ we say that p ramifies in K. The integer f_i is called the* degree *of P_i.*

Note that $p^{f_i} = \#\mathcal{O}_K/P_i$ and that $\mathcal{O}_K/P_i$ is isomorphic to the finite field with p^{f_i} elements.

Theorem 7.2 (Dedekind)**.** *Suppose that $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$ having minimal polynomial $m(x) \in \mathbb{Z}[x]$ of degree n. If p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and $\bar{m}(x) := m(x) \bmod p \in \mathbb{F}_p[x]$ factorises as*

$$\bar{m}(x) = \prod_{i=1}^{r} \bar{g}_i(x)^{e_i}$$

with $\bar{g}_i$ distinct and irreducible, then

1. *$P_i = (p, g_i(\alpha))$ is a prime ideal of $\mathcal{O}_K$ (here $g_i(x) \in \mathbb{Z}[x]$ is any polynomial such that $g_i(x) \equiv \bar{g}_i(x) \bmod p$).*
2. *The prime ideals P_i are distinct.*
3. *The degree of P_i is the degree of $\bar{g}_i$.*
4. *$(p) = \prod_{i=1}^{r} P_i^{e_i}$.*

Proof. Suppose that p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Consider the natural map $\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$. An element γ of the kernel must have the form $p\beta$ for $\beta \in \mathcal{O}_K$. Since p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ we must have $\beta \in \mathbb{Z}[\alpha]$. The kernel is thus precisely $p\mathbb{Z}[\alpha]$ and we get an injection $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \hookrightarrow \mathcal{O}_K/p\mathcal{O}_K$. Indeed this must be an isomorphism of rings since both sides have order p^n. Now consider the ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ taking $g(x)$ to $g(\alpha) + p\mathbb{Z}[\alpha]$. This has kernel

$$\{g(x) : \, g(x) = m(x)h(x) + pj(x)\} = (p, m(x)),$$

giving

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(p, m(x)).$$

Finally consider the homomorphism from $\mathbb{Z}[x]$ to $\mathbb{F}_p[x]/(\bar{m}(x))$, sending $g(x)$ to $\bar{g}(x) + (\bar{m}(x))$. The kernel of this map is

$$\{g(x) : \, \bar{m}(x) | \bar{g}(x)\} = \{g(x) : \, g(x) = m(x)h(x) + pj(x)\} = (p, m(x)).$$

Thus $\mathbb{Z}[x]/(p, m(x)) \cong \mathbb{F}_p[x]/(\bar{m}(x))$, and composing our various maps we obtain

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(p, m(x)) \cong \mathbb{F}_p[x]/(\bar{m}(x)).$$

We are looking for prime ideals P with $\mathcal{O}_K \supseteq P \supseteq p\mathcal{O}_K$. There is a $1-1$ correspondence between the prime ideals of $\mathcal{O}_K$ containing (p) and the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$, and between these latter prime ideals and the prime ideals of $\mathbb{F}_p[x]/(\bar{m}(x))$. However the prime ideals of $\mathbb{F}_p[x]/(\bar{m}(x))$ are generated by irreducible factors $\bar{g}_i(x)$ of $\bar{m}(x)$. Tracing back the effect of our various isomorphisms one sees that these correspond to $P_i = (p, g_i(\alpha))$ in $\mathcal{O}_K$. This proves parts 1 and 2 of the theorem. Moreover one sees, again by checking the effect of our three isomorphisms, that $N(P_i) = \#\mathbb{F}_p[x]/(\bar{g}_i(x))$, which proves part 3.

Finally we have

$$\prod_{i=1}^{r} P_i^{e_i} = \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i} \subseteq \prod_{i=1}^{r} (p, g_i(\alpha)^{e_i}) \subseteq (p, \prod_{i=1}^{r} g_i(\alpha)^{e_i}) = (p).$$

However $p^{f_i} = N(P_i) = p^{\deg(g_i)}$ (by part 3), so that

$$N\left(\prod_{i=1}^{r} P_i^{e_i}\right) = p^{\sum_{i=1}^{r} e_i f_i} = p^{\sum_{i=1}^{r} e_i \deg(g_i)} = p^n.$$

On the other hand, $N((p)) = p^n$ and so $(p) = \prod_{i=1}^{r} P_i^{e_i}$. This proves part 4, the final assertion of the theorem. □

Corollary 7.3. *If p ramifies then $p|\Delta(\mathbb{Z}[\alpha])^2$.*

Proof. If $p|[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ then $p|\Delta(\mathbb{Z}[\alpha])^2$. So we may suppose that p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then the above theorem shows that if p ramifies, with a factor P^2, then $\bar{m}(x)$ has a multiple irreducible factor $\bar{g}(x)$ over $\mathbb{F}_p$, for which $g(\alpha) \in (p, g(\alpha)) = P$. We then have $m(x) = g(x)^2 h(x) + pk(x)$, say, so that

$$m'(x) = g(x)\{2g'(x)h(x) + g(x)h'(x)\} + pk'(x) = g(x)j(x) + pl(x),$$

say. Thus $m'(\alpha) = g(\alpha)j(\alpha) + p\beta$ with $\beta \in \mathcal{O}_K$. It follows that

$$\mathrm{Norm}_{K/\mathbb{Q}}(m'(\alpha)) = \prod_{\sigma} \sigma(m'(\alpha)) = \prod_{\sigma} \sigma(g(\alpha)j(\alpha)) + p\gamma$$

for some algebraic integer γ. We now have

$$\mathrm{Norm}_{K/\mathbb{Q}}(m'(\alpha)) = \mathrm{Norm}_{K/\mathbb{Q}}(g(\alpha))\mathrm{Norm}_{K/\mathbb{Q}}(j(\alpha)) + p\gamma,$$

so that in particular we see that $\gamma \in \mathbb{Z}$. However, since $P|(g(\alpha))$ we will have $N(P)|\mathrm{Norm}_{K/\mathbb{Q}}(g(\alpha))$ and hence $p|\mathrm{Norm}_{K/\mathbb{Q}}(g(\alpha))$. We therefore conclude that $p|\mathrm{Norm}_{K/\mathbb{Q}}(m'(\alpha))$. The result now follows, since $\Delta^2(\mathbb{Z}[\alpha]) = \pm\mathrm{Norm}_{K/\mathbb{Q}}(m'(\alpha))$, by Problem Sheet 1. □

Example 7.4 Let $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\Delta(\mathbb{Z}[\sqrt{-5}])^2 = 4(-5) = -20$. The possible ramified primes are 2 and 5. We have $m(x) = x^2 + 5$, and

$$x^2 + 5 \equiv x^2 + 1 \equiv (x+1)^2 \bmod 2$$

so that

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

Similarly, $x^2 + 5 \equiv x^2 \bmod 5$ so that

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

For all primes we have $\sum_{i=1}^{r} e_i f_i = 2$, so $r \leqslant 2$. Thus one of the following cases holds: $r = 1, e_1 = 2, f_1 = 1$ (ramified case), or $r = 1, e_1 = 1, f_1 = 2$ (we say p remains *inert*), or $r = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$ (we say p *splits*). We extend this language to general algebraic number fields, saying that p is *inert* if (p) is prime in $\mathcal{O}_K$, and that p *splits* otherwise.

We have already dealt with $p = 2, 5$ so consider $p \neq 2, 5$.

Case 1: $\left(\frac{-5}{p}\right) = -1$. Then $x^2 + 5$ is irreducible modulo p, and

$$(p) = P := (p, \sqrt{-5}^{\,2} + 5) = (p)$$

is inert.

Case 2: $\left(\frac{-5}{p}\right) = 1$. Then

$$x^2 + 5 \equiv (x - a)(x + a) \bmod p$$

where $a \not\equiv -a \bmod p$. In this case $(p) = P_1 P_2$ where $P_1 = (p, \sqrt{-5} - a)$ and $P_2 = (p, \sqrt{-5} + a)$. e.g. $x^2 + 5 \equiv x^2 - 1 \equiv (x-1)(x+1) \bmod 3$, so that $(3) = (3, \sqrt{-5} - 1)(3, \sqrt{-5} + 1)$. (Note that for case 2 we have $p \equiv 1, 3, 7, 9 \bmod 20$ by quadratic reciprocity.)

8 Minkowski: computation of the class group

8.1 Minkowski's convex body theorem

Let $\{v_1, \ldots, v_n\}$ be any basis for $\mathbb{R}^n$. Let $L = \{\sum_{i=1}^n a_i v_i \ : \ a_i \in \mathbb{Z}\}$ be the *lattice* generated by the v_i. It is an additive subgroup of $\mathbb{R}^n$. Let $D = \{\sum_{i=1}^n a_i v_i \ : \ a_i \in [0,1)\}$. We call D a *fundamental domain* for L. Every $v \in \mathbb{R}^n$ can be expressed uniquely as $v = u + w$ with $u \in L$ and $w \in D$.

If $v_i = \sum_{j=1}^n a_{ij} e_j$ where $\{e_1, \ldots, e_n\}$ is the "standard basis" for $\mathbb{R}^n$, then we define $\mathrm{Vol}(D) := |\det(a_{ij})|$; this is sometimes denoted $\mathrm{Vol}(L)$. We also have $\mathrm{Vol}(D)^2 = \det(v_i \cdot v_j)$, being the determinant of matrix $(a_{ij})(a_{ij})^t$. One can easily check that $\mathrm{Vol}(D)$ is independent of the choice of $\mathbb{Z}$-basis for the lattice L.

Lemma 8.1 (Blichfeldt)**.** *Let L be a lattice in $\mathbb{R}^n$, and let S be a bounded, measurable subset of $\mathbb{R}^n$ such that $\mathrm{Vol}(S) > \mathrm{Vol}(L)$. Then there exist $x, y \in S$ with $x \neq y$ and such that $x - y \in L$.*

Proof. (Non-examinable)

Let D be a fundamental domain for L. When $a \in L$ write $S(a) = (S-a) \cap D$. Then S is the disjoint union of the sets $S(a)+a$ as a runs over L. It follows that $\mathrm{Vol}(S) = \sum_{a \in L} \mathrm{Vol}(S(a))$. However $\mathrm{Vol}(S) > \mathrm{Vol}(D)$ and $S(a) \subseteq D$. Thus some $S(b)$ and $S(c)$ with $b \neq c$ must overlap. Let $v \in S(b) \cap S(c)$. Then $x = v + b \in S$ and $y = v + c \in S$, and $x - y = b - c \in L$. □

Definition 8.2. *We say $S \subseteq \mathbb{R}^n$ is* convex *if*

$$x, y \in S, \ 0 \leqslant \lambda \leqslant 1 \ \Rightarrow \ \lambda x + (1-\lambda) y \in S.$$

We say S is symmetric *(about the origin) if*

$$x \in S \Rightarrow -x \in S.$$

Theorem 8.3 (Minkowski's Convex Body Theorem)**.** *Let L be a lattice in $\mathbb{R}^n$. Let S be a bounded measurable subset of $\mathbb{R}^n$ which is convex and symmetric. If $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(L)$ then there exists $v \in L - \{0\}$ with $v \in S$.*

Proof. (Non-examinable)

We have $\mathrm{Vol}(\frac{1}{2}S) = 2^{-n}\mathrm{Vol}(S) > \mathrm{Vol}(L)$. Thus Blichfeldt's result tells us that there exist $x, y \in \frac{1}{2}S$ such that $x - y \in L - \{0\}$. Now $2x \in S$ and, by symmetry, $-2y \in S$. Using convexity we then find that $\frac{1}{2}(2x + (-2y)) \in S$, that is to say, $x - y \in S$. □

Note 8.4 If S is closed, and therefore compact, then it is enough to have $\mathrm{Vol}(S) \geqslant 2^n \mathrm{Vol}(L)$.

Example 8.5 We give another proof that if $p \equiv 1 \bmod 4$ then there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$.

We know that $\left(\frac{-1}{p}\right) = 1$, so there is an s such that $s^2 \equiv -1 \bmod p$. If $p = x^2 + y^2$ then $x^2 + y^2 \equiv 0 \bmod p$ and so $(x/y)^2 \equiv -1 \bmod p$. Hence $x \equiv \pm sy \bmod p$. We will search for a "small" integer solution to $x \equiv sy \bmod p$. Such points form a lattice L in $\mathbb{R}^2$. We have

$$x \equiv sy \bmod p \Leftrightarrow x = sy + pz, \text{ with } z \in \mathbb{Z} \Leftrightarrow (x, y) = y(s, 1) + z(p, 0).$$

Hence $\{(s, 1), (p, 0\}\}$ is a basis for L, and

$$\mathrm{Vol}(L) = \left| \det \begin{pmatrix} s & p \\ 1 & 0 \end{pmatrix} \right| = p.$$

Let C be the disc $x^2 + y^2 < 2p$, with radius $\sqrt{2p}$. The set C is clearly convex and symmetric about the origin, and

$$\mathrm{Vol}(C) = \pi(\sqrt{2p})^2 = 2\pi p > 2^2 p = 2^2 \mathrm{Vol}(L).$$

Hence by Minkowski's Theorem there exists a nonzero $v \in L$ such that $v \in C$. Suppose that $v = (x, y)$. Since $v \in L$ we have $x \equiv sy \bmod p$, and hence $x^2 + y^2 \equiv 0 \bmod p$. However $v \in C$ implies $x^2 + y^2 < 2p$, so that $x^2 + y^2 = 0$ or p. Finally, since $v \neq 0$ we must have $x^2 + y^2 = p$.

8.2 Minkowski's bound

Let $[K : \mathbb{Q}] := n = r + 2s$ where r is the number of real embeddings $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$, and s the number of pairs of complex embeddings $\sigma_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+1}, \ldots, \bar{\sigma}_{r+s} : K \to \mathbb{C}$

Definition 8.6. *Let* $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$ *be defined as* $\sigma(x) :=$

$$(\sigma_1(x), \ldots, \sigma_r(x), \Re(\sigma_{r+1}(x)), \Im(\sigma_{r+1}(x)), \ldots, \Re(\sigma_{r+s}(x)), \Im(\sigma_{r+s}(x))) .$$

Let $\mathcal{O}_K$ be the ring of integers of K, and let $\{v_1, \ldots, v_n\}$ be an integral basis for $\mathcal{O}_K$. Write A for the matrix whose ith row is $\sigma(v_i)$. By elementary column operations we find that

$$(-2i)^s \det(A) = \det(\sigma_j(v_i)) = \pm\sqrt{|\Delta^2|} \neq 0$$

where $\Delta^2 := \Delta^2(K)$. Thus $\det(A) \neq 0$, and $\sigma(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ of volume $\sqrt{|\Delta^2|}/2^s$.

If I is an ideal of $\mathcal{O}_K$, with basis $w = \{w_1, \ldots, w_n\}$ then $w_i = \sum_j c_{ij} v_j$ and

$$N(I) = [\mathcal{O}_K : I] = |\det(c_{ij})|$$

by Theorem 1.8. Moreover, $\Delta^2(w) = \det^2(c_{ij})\Delta^2(v)$ by Lemma 2.4, and so $\Delta^2(w) = N(I)^2\Delta^2(v)$. We can now replace the basis v in the previous calculation by w, to deduce that

$$\mathrm{Vol}(\sigma(I)) = \frac{\sqrt{|\Delta^2(w)|}}{2^s} = \frac{N(I)\sqrt{|\Delta^2(v)|}}{2^s} = \frac{N(I)\sqrt{|\Delta^2|}}{2^s}.$$

Lemma 8.7. *For $t > 0$ let*

$$R_t := \left\{ (x_1, \ldots, x_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \,:\, \sum_{i=1}^{r} |x_i| + 2\sum_{i=1}^{s} |z_i| \leqslant t \right\}.$$

Then

1. *R_t is a compact, symmetric, and convex subset of $\mathbb{R}^n$,*
2. *$\mathrm{Vol}(R_t) = 2^r t^n (\pi/2)^s / n!$*

Proof. Non-examinable. See Lang, *Algebraic Number Theory*, (Addison-Wesley, 1970), page 116. □

Theorem 8.8. *Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal. Then there exists a nonzero $\alpha \in I$ with*

$$|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leqslant c_K N(I)$$

where

$$c_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}$$

is Minkowski's constant *for K.*

Proof. Choose $t \in \mathbb{R}$ so that $\pi^s t^n / n! = 4^s \sqrt{|\Delta^2(K)|} N(I)$. Then

$$\mathrm{Vol}(R_t) = \frac{2^r t^n (\pi/2)^s}{n!} = \frac{2^n \sqrt{|\Delta^2(K)|} N(I)}{2^s} = 2^n \mathrm{Vol}(\sigma(I)).$$

By Minkowski's theorem (compact version), there exists a nonzero $\alpha \in I$ such that $\sigma(\alpha) \in R_t$. Hence

$$\sum_{i=1}^{r} |\sigma_i(\alpha)| + 2 \sum_{i=r+1}^{r+s} \sqrt{\Re(\sigma_i(\alpha))^2 + \Im(\sigma_i(\alpha))^2} \leqslant t.$$

This means that $\sum_{i=1}^{n} |\sigma_i(\alpha)| \leqslant t$ and so

$$\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \leqslant \frac{t}{n}.$$

By the inequality of the arithmetic and geometric means we have

$$\left(\prod_{i=1}^{n} |\sigma_i(\alpha)| \right)^{1/n} \leqslant \frac{1}{n} \left(\sum_{i=1}^{n} |\sigma_i(\alpha)| \right) \leqslant \frac{t}{n},$$

giving $|\mathrm{Norm}_{K/Q}(\alpha)| \leqslant \left(\frac{t}{n}\right)^n = c_K N(I)$. □

Theorem 8.9. *Any ideal class $c \in C_K$ contains an ideal J such that $N(J) \leqslant c_K$, that is to say*

$$N(J) \leqslant \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta^2(K)|}.$$

Proof. Let I be any ideal in the inverse class c^{-1}. We now know there exists a nonzero $\alpha \in I$ such that $|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leqslant c_K N(I)$. Since $(\alpha) \subseteq I$ we have $I|(\alpha)$, and so there exists an ideal J such that $IJ = (\alpha)$. The relations $I \in c^{-1}$ and $IJ = (\alpha)$ imply that $[J] = c$ and $J \in c$. Moreover $N(I)N(J) = N(IJ) = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| \leqslant c_K N(I)$, and so $N(J) \leqslant c_K$. □

Note 8.10 For a nonzero ideal $J \subseteq \mathcal{O}_K$ we have $N(J) = \#\mathcal{O}_K/J$ so that $N(J).x \in J$ for any $x \in \mathcal{O}_K$, by Lagrange's Theorem, regarding $\mathcal{O}_K/J$ as an additive group. Taking $x = 1$ shows that $N(J) \in J$. It follows that $J \supseteq (N(J))$, and hence that $J|(N(J))$.

We can therefore deduce that every class c contains an ideal J such that J has an element $m \in J \cap \mathbb{N}$ with $m \leqslant c_K$.

Corollary 8.11. *If $K \neq \mathbb{Q}$ then $|\Delta^2(K)| > 1$.*

Proof. Since $N(J) \geqslant 1$ for any ideal $J \subseteq \mathcal{O}_K$, we must have

$$1 \leqslant \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta^2(K)|} \leqslant \left(\frac{4}{\pi}\right)^n \frac{n!}{n^n}\sqrt{|\Delta^2(K)|}.$$

Let $b_n := \left(\frac{\pi}{4}\right)^n \frac{n^n}{n!}$. It will suffice to show that $b_n > 1$ for all $n \geqslant 2$. Now $b_2 = \pi^2/8 > 1$. Moreover

$$\frac{b_{n+1}}{b_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^n = \frac{\pi}{4}\left(1 + n\frac{1}{n} + \dots\right) \geqslant \frac{\pi}{2} > 1.$$

Hence $b_n > 1$ for all $n \geqslant 2$. □

9 Class group computations and Diophantine applications

Note 9.1 The class group is abelian. Let c be any ideal class. Then there exists $J \in c$ with $N(J) \leqslant c_K$. Write J as a product of prime ideals, $J = P_1 \dots P_s$, say. By the multiplicativity of the norm, $N(P_i) \leqslant c_K$ for each i. Moreover $c = [J] = [P_1 \dots P_s] = [P_1] \dots [P_s]$. Hence c is in the group generated by ideal classes of prime ideals of norm at most c_K. Thus the class group itself is generated by classes of prime ideals in $\mathcal{O}_K$ of norm at most c_K.

In order to find a suitable set of generators we observe that prime ideals of norm $\leqslant c_K$ are factors of ideals (p) where $p \in \mathbb{N}$ is prime and $p \leqslant c_K$. Using Dedekind's Theorem 7.2, we can factor all such primes p into prime ideals, to give a complete set of generators.

To determine the class group it remains to find any relations satisfied by the classes of these prime ideals. Some such relations can be found from the prime factorisations of the ideals (p), since these are principal, and others can be obtained by factoring principal ideals (α) generated by elements $\alpha \in \mathcal{O}_K$ of small norm.

To show that the set of relations found is complete one needs to show that appropriate combinations of the generators are not principal. In general this can be awkward, but for complex quadratic fields one can prove that an ideal I is non-principal by finding all elements $\alpha \in \mathcal{O}_K$ with $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = N(I)$, and checking whether or not $I = (\alpha)$. If K is complex quadratic there will only be finitely many possible α with $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = N(I)$ to check.

Example 9.2 Let $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We know from Proposition 5.8 that $\mathcal{O}_K$ is not a PID, so that $h_K > 1$. We have $n = 2, s = 1, r = 0$, and $\Delta^2(K) = -20$. Thus

$$c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3.$$

It follows that every ideal class contains an ideal of norm at most 2, and that C_K is generated by classes of prime ideals of norm at most 2. However $(2) = P_2^2$ where $P_2 = (2, 1 + \sqrt{-5})$ with $N(P_2) = 2$. Hence $[P_2]$ generates C_K. Moreover $P_2^2 = (2)$, giving $[P_2]^2 = [(2)] = [\mathcal{O}_K]$, which is the identity in C_K. Hence C_K is cyclic of order 2, and $h_K = 2$.

Example 9.3 Next consider $K = \mathbb{Q}(\sqrt{-6})$, for which $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, with $n = 2, r = 0, s = 1$ and $\Delta^2(K) = -24$. In this case

$$c_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{24} = \frac{4\sqrt{6}}{\pi} \approx 3.1.$$

The ideal class group C_K is generated by classes of prime ideals P such that $N(P) \leqslant c_K$, which means that $N(P) = 2$ or 3.

Now $x^2+6 \equiv x^2 \bmod 2$, and so $(2) = P_2^2$ where $P_2 := (2, \sqrt{-6})$. Similarly $x^2+6 \equiv x^2 \bmod 3$, so that $(3) = P_3^2$ with $P_3 := (3, \sqrt{-6})$. We have $N(P_2) = 2$ and $N(P_3) = 3$. (Indeed $e = 2, f = 1$ in both cases.) It follows that C_K is generated by $[P_2]$ and $[P_3]$, but we need to see if there are any relations satisfied by these classes.

If P_2 is principal then $P_2 = (x + y\sqrt{-6})$ with $x, y \in \mathbb{Z}$. Taking norms this gives $2 = |x^2 + 6y^2|$, which is impossible. Similarly P_3 is not principal, so that $[P_2], [P_3] \neq [\mathcal{O}_K]$ in C_K.

Since $P_2^2 = (2)$ we have $[P_2]^2 = [\mathcal{O}_K]$, and similarly $[P_3]^2 = [\mathcal{O}_K]$.

We next observe that $\sqrt{-6} = \sqrt{-6}.3 - 2.\sqrt{-6} \in P_2P_3$. We also have $\mathrm{Norm}_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, and we therefore deduce that $(\sqrt{-6}) = P_2P_3$. It follows that $[P_2][P_3] = [\mathcal{O}_K]$. Thus $[P_3] = [P_2]^{-1} = [P_2]$, and C_K must be cyclic of order 2, generated by $[P_2]$, and $h_K = 2$.

Example 9.4 *Find all integer solutions of the equation* $y^2 + 54 = x^3$.

Let $x, y \in \mathbb{Z}$ be a solution. If y is even then $x^3 \equiv 54 \equiv 2 \bmod 4$, which is impossible. If $3|y$ then $3|x$, and on setting $x = 3x_1, y = 3y_1$ we will have

$y_1^2 + 6 = 3x_1^3$. Hence $3|y_1$, and on writing $y_1 = 3y_2$ we obtain $3y_2^2 + 2 = x_1^3$. However $3y_2^2 + 2 \equiv 2$ or $5 \bmod 9$ while $x_1^3 \equiv 0, 1$ or $8 \bmod 9$. This contradiction shows that we must have y coprime to 3.

It follows that $\mathrm{hcf}(y, 6) = 1$, and hence that $\mathrm{hcf}(x, 6) = 1$.

We now use the ideal factorisation $(y + 3\sqrt{-6})(y - 3\sqrt{-6}) = (x)^3$. We proceed to show that the factors on the left are coprime. If a prime ideal P divides both factors then $6\sqrt{-6} = \{y + 3\sqrt{-6}\} - \{y - 3\sqrt{-6}\} \in P$, and so $P|(6\sqrt{-6}) = P_2^3 P_3^3$. (Recall that $(\sqrt{-6}) = P_2 P_3$.) Thus P can only be P_2 or P_3. However $P|(y + 3\sqrt{-6})$ implies $P|(x)^3$, and on taking norms we find that $N(P)|x^6$, which is impossible, since $\mathrm{hcf}(x, 6) = 1$.

It follows that $(y + 3\sqrt{-6})$ and $(y - 3\sqrt{-6})$ are coprime as ideals of $\mathcal{O}_K$. By unique factorisation of ideals we have

$$(y + 3\sqrt{-6}) = I^3$$

for some ideal I. Since I^3 is principal we have $[I]^3 = [\mathcal{O}_K]$, the identity in C_K. However we know from above that $h_K = 2$ (giving $[I]^2 = [\mathcal{O}_K]$ by Lagrange's Theorem), and so we must have $[I] = [\mathcal{O}_K]$. Thus I is principal, so that $I = (\alpha)$ for some $\alpha \in \mathcal{O}_K$.

It follows that $(y + 3\sqrt{-6}) = (\alpha)^3 = (\alpha^3)$, giving $y + 3\sqrt{-6} = u\alpha^3$ with u a unit. (Recall that if $(\alpha) = (\beta)$ then $\alpha = u\beta$ for some unit $u \in \mathcal{O}_K$.)

For $K = \mathbb{Q}(\sqrt{-6})$ the only units in $\mathcal{O}_K$ are $u = \pm 1$, and for both of these we have $u = u^3$. It follows that

$$y + 3\sqrt{-6} = \{u\alpha\}^3 = \{a + b\sqrt{-6}\}^3,$$

say. Equating the coefficient of $\sqrt{-6}$ on both sides gives $3 = b\{3a^2 - 6b^2\}$, and so $1 = b\{a^2 - 2b^2\}$. Hence $b = -1$ and $a^2 = 1$, giving $y = a^3 - 18b^2a = a\{a^2 - 18b^2\} = \pm 17$. With these y the only possible x is 7, so that the complete solution is $x = 7$, $y = \pm 17$.

Example 9.5 Let $K = \mathbb{Q}(\sqrt{-163})$, so that $\mathcal{O}_K = Z[\frac{1}{2}(1 + \sqrt{-163})]$ and

$$c_K = \frac{2}{\pi}\sqrt{163} \approx 8.13 < 9.$$

Thus the class group C_K is generated by the classes of prime ideals dividing $(2), (3), (5)$ and (7), so we proceed to factor $(2), (3), (5)$ and (7) in $\mathcal{O}_K$.

The minimal polynomial of $\frac{1}{2}\{1 + \sqrt{-163}\}$ is $x^2 - x + 41$. However we find that $x^2 - x + 41 \equiv x^2 + x + 1 \bmod 2$, which is irreducible. Thus (2) is inert, so that the only prime ideal above 2 is (2), which is principal.

For $p = 3, 5$ and 7 it is enough to consider the factorisation of the polynomial $x^2 + 163 \bmod p$, since p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\sqrt{-163}]] = 2$.

- $x^2 + 163 \equiv x^2 + 1 \bmod 3$, which is irreducible. Hence (3) is inert.
- $x^2 + 163 \equiv x^2 + 3 \bmod 5$, which is irreducible. Hence (5) is inert.
- $x^2 + 163 \equiv x^2 + 2 \bmod 7$, which is irreducible. Hence (7) is inert.

Thus the only relevant prime ideals are all principal; hence C_K is trivial and $h_K = 1$. It follows that $\mathcal{O}_K$ is a UFD. However, it is *not* a Euclidean domain. (For this non-examinable fact see S&T, Theorem 4.18)

Note: it is known that there are only finitely many imaginary quadratic fields K with $h_K = 1$ (the proof of this is hard!). On the other hand it is conjectured that $\mathcal{O}_K$ is a UFD for infinitely many *real* quadratic fields.

Proposition 9.6. *The fact that $h_K = 1$ for $K = \mathbb{Q}(\sqrt{-163})$ implies that $n^2 + n + 41$ is prime for $0 \leqslant n \leqslant 39$.*

Proof. Suppose $n^2 + n + 41$ is not prime for some $n < 40$. Now $n^2 + n + 41 < 41^2$, and so $n^2 + n + 41$ must have a prime factor $q < 41$.

Now

$$q | n^2 + n + 41 = \left\{ n + \frac{1}{2}\left(1 + \sqrt{-163}\right) \right\} \left\{ n + \frac{1}{2}\left(1 - \sqrt{-163}\right) \right\}.$$

However q clearly does not divide either factor in $\mathcal{O}_K$, and so q cannot be prime in $\mathcal{O}_K$. Since we are in a UFD, it follows that q cannot be irreducible. Thus $q = \alpha\beta$ where $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \mathrm{Norm}_{K/\mathbb{Q}}(\beta) = q$.

If

$$\alpha = x + y\frac{1 + \sqrt{-163}}{2}, \quad x, y \in \mathbb{Z},$$

then

$$q = \mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \left(x + \frac{y}{2}\right)^2 + 163\left(\frac{y}{2}\right)^2.$$

Since q is not a square we have $y \neq 0$, and we deduce that $q \geqslant 163/4 > 40$, which gives a contradiction. □

For similar reasons

- $n^2 + n + 17$ is prime for $0 \leqslant n \leqslant 15$ (consider $\mathbb{Q}(\sqrt{-67})$).
- $n^2 + n + 11$ is prime for $0 \leqslant n \leqslant 9$ (consider $\mathbb{Q}(\sqrt{-43})$).
- $n^2 + n + 5$ is prime for $0 \leqslant n \leqslant 3$ (consider $\mathbb{Q}(\sqrt{-19})$).
- $n^2 + n + 3$ is prime for $0 \leqslant n \leqslant 1$ (consider $\mathbb{Q}(\sqrt{-11})$).

Example 9.7 [Paper B9 2005] Find the structure of the ideal class group of $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-29})$.

Since $-29 \equiv 3 \bmod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$, and $\Delta^2(K) = -4 \times 29 = -116$. Moreover $n = 2$ and $s = 1$, so that

$$c_K = \left(\frac{2}{\pi}\right)\sqrt{116} \approx 6.9 < 7.$$

Thus C_K is generated by the classes of prime ideals dividing $(2), (3)$ and (5). We need to factor $(2), (3), (5)$ in $\mathcal{O}_K$, using Theorem 7.2.

- $x^2 + 29 \equiv (x+1)^2 \bmod 2$, so that $(2) = P_2^2$ where $P_2 := (2, \sqrt{-29} + 1)$ is a prime ideal of norm 2.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 3$, so that $(3) = P_3 P_3'$ where $P_3 := (3, \sqrt{-29} + 1)$ and $P_3' := (3, \sqrt{-29} - 1)$ are distinct prime ideals of norm 3.
- $x^2 + 29 \equiv x^2 - 1 \equiv (x+1)(x-1) \bmod 5$, so that $(5) = P_5 P_5'$ with $P_5 := (5, \sqrt{-29} + 1)$ and $P_5' := (5, \sqrt{-29} - 1)$ being distinct prime ideals of norm 5.

We have $[P_2]^2 = [P_3][P_3'] = [P_5][P_5'] = [\mathcal{O}_K]$. Hence C_K is generated by $[P_2], [P_3], [P_5]$.

We proceed to find the orders of these elements, and relations between them:

We have $\mathrm{Norm}_{K/\mathbb{Q}}(x + y\sqrt{-29}) = x^2 + 29y^2$, so there are no elements in $\mathcal{O}_K$ of norms $\pm 2, \pm 3, \pm 5$. Thus P_2, P_3, P_5 are not principal, and $[P_2]$ must have order 2.

The only element $\alpha \in \mathcal{O}_K$ of norm ± 9 is ± 3. Thus if $P_3^2 = (\alpha)$ we must have $P_3^2 = (3) = P_3 P_3'$. However this would imply $P_3 = P_3'$, giving a contradiction. Thus the order of $[P_3]$ is at least 3. Indeed it cannot have

order 3 since there are no solutions to $x^2 + 29y^2 = \pm 27$. We shall come back to $[P_3]$ later.

Turning to $[P_5]$, note that $3^2+29\times 2^2 = 125$, so that $N((3+2\sqrt{-29})) = 5^3$. Hence $(3 + 2\sqrt{-29})$ must be one of $P_5^3, P_5^2P_5', P_5P_5'^2$ or $P_5'^3$. However $2 + 2\sqrt{-29} \in P_5$, giving $3+2\sqrt{-29} \notin P_5$. Hence P_5 does not divide $(3+2\sqrt{-29})$. It follows that $(3 + 2\sqrt{-29}) = P_5'^3$, and, taking conjugates, we also have $(3-2\sqrt{-29}) = P_5^3$. Hence $[P_5]$ has order dividing 3. Since P_5 is not principal, it must have order exactly 3.

Finally we note that $30 = \{1 + \sqrt{-29}\}\{1 - \sqrt{-29}\}$. Thus

$$(2)(3)(5) = (1 + \sqrt{-29})(1 - \sqrt{-29}).$$

Now $(2)(3)(5) = P_2^2P_3P_3'P_5P_5'$. So, in order to have the correct norm, we see that $(1 \pm \sqrt{-29})$ must be one of $P_2P_3P_5, P_2P_3'P_5, P_2P_3P_5'$ or $P_2P_3'P_5'$. It follows that at least one of these products is principal, and so one or other (and hence both) of $[P_3]$ and $[P_3'] = [P_3]^{-1}$ is in the group generated by $[P_2]$ and $[P_5]$.

We conclude that C_K is an abelian group generated by an element of order 2 and an element of order 3. Thus it is cyclic of order 6. (In fact $\text{Norm}(2 \pm 5\sqrt{-29}) = 729 = 3^6$, and by the argument above we find that $(2 + 5\sqrt{-29}) = P_3^6$ and $(2 - 5\sqrt{-29}) = P_3'^6$.)

Example 9.8 [Paper B9 2005] Let $K = \mathbb{Q}(\sqrt{-37})$. Given that $h_K = 2$, prove there are no integral solutions of the equation $y^2 = x^3 - 37$.

Suppose that $x, y \in \mathbb{Z}$ are such that $y^2 + 37 = x^3$. Then as ideals we have

$$(y + \sqrt{-37})(y - \sqrt{-37}) = (x)^3.$$

We claim that $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ are coprime ideals. For suppose that a prime ideal P divides both. Then $y \pm \sqrt{-37} \in P$, so that the difference $2\sqrt{-37} \in P$. Hence $P|(2\sqrt{-37})$, and since P is prime we conclude that $P|(2)$ or $P|(\sqrt{-37})$.

Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{-37}]$, we may factor $(p) = (2)$ and $(p) = (37)$ in $\mathcal{O}_K$ by using the decomposition of $X^2 + 37$ modulo p. We have $X^2 + 37 \equiv (X + 1)^2 \bmod 2$, giving $(2) = P_2^2$, where $P_2 := (2, 1 + \sqrt{-37})$ is a prime ideal of norm 2. Similarly $X^2 + 37 \equiv X^2 \bmod 37$ and hence $(37) = (37, \sqrt{-37})^2 = P_{37}^2$, where $P_{37} := (\sqrt{-37})$ is prime of norm 37.

It follows that if P is a common factor of $(y + \sqrt{-37})$ and $(y - \sqrt{-37})$ then $P = P_2$ or P_{37}. In either case, since $P|(y + \sqrt{-37})$, we have $P|(x)^3$ and

taking norms we get $2|x^6$ or $37|x^6$ respectively. Hence either $2|x$ or $37|x$, as appropriate.

Suppose firstly that $P = P_{37}$. Then $37|x$, and since $x^3 = y^2 + 37$ we must also have $37|y$. Thus 37^2 divides $x^3 - y^2 = 37$, which is impossible. Alternatively if $P = P_2$, so that $2|x$, we will have $8|x^3$. The equation $y^2+37 = x^3$ then implies that $y^2 + 1 \equiv 0 \bmod 4$, which is impossible.

Thus $(y+\sqrt{-37})$ and $(y-\sqrt{-37})$ are coprime ideals as claimed. However their product is $(x)^3$, which is a cube. Hence by unique factorisation of ideals, each of the two factors is a cube. In particular,

$$(y + \sqrt{-37}) = I^3$$

for some ideal I. Since I^3 is principal, the order of $[I]$ in C_K divides 3. However $h_K = 2$, so I must be principal. Thus

$$(y + \sqrt{-37}) = (a + b\sqrt{-37})^3$$

for some $a, b \in \mathbb{Z}$. Hence $y + \sqrt{-37} = u(a + b\sqrt{-37})^3$ for some unit $u \in \mathcal{O}_K$. However the only units are $u = \pm 1$, which satisfy $u = u^3$. Hence, on replacing a, b by $-a, -b$ if $u = -1$, we may assume that $u = 1$. Expanding and comparing coefficients we obtain

$$y = a\{a^2 - 111b^2\},\ 1 = b\{3a^2 - 37b^2\}.$$

The second equation implies that $b = \pm 1$ and $3a^2 - 37 = \pm 1$. Hence $3a^2 = 38$ or 36, both of which are impossible.

Hence there are no solutions in integers.

10 The equation $x^3 + y^3 = z^3$

In this section we will establish "Fermat's Last Theorem" for cubes, that $x^3 + y^3 = z^3$ has no nontrivial (x, y, z all nonzero) solutions in $\mathbb{Z}$.

We shall work in $K = \mathbb{Q}(\sqrt{-3})$. It is convenient to write

$$\omega = (-1 + \sqrt{-3})/2,$$

so that $\mathcal{O}_K = \mathbb{Z}[\omega]$. We begin by collecting together some basic facts.

Lemma 10.1. *Let $K = \mathbb{Q}(\sqrt{-3})$ and $\omega = (-1 + \sqrt{-3})/2$.*

(i) *We have $\omega^3 = 1$. Moreover the set of units of $\mathcal{O}_K$ is $\{\pm 1, \pm\omega, \pm\omega^2\}$.*

(ii) *The ring $\mathcal{O}_K$ is a UFD.*

(iii) *The element $\lambda := \sqrt{-3}$ is prime, with norm 3. Moreover we have $\lambda = \omega(1-\omega) = (-\omega^2)(1-\omega^2)$.*

Proof. (i) To find the unit group we note that

$$\mathrm{Norm}_{K/\mathbb{Q}}(a+b\omega) = a^2 - ab + b^2, \quad a, b \in \mathbb{Z}.$$

Thus if $\mathrm{Norm}_{K/\mathbb{Q}}(a+b\omega) = 1$ then $(2a-b)^2 + 3b^2 = 4$, giving solutions $(a,b) = \pm(1,0), \pm(0,1)$ and $\pm(1,1)$, which produce the six units specified in the lemma.

(ii) See Problem sheet 2.

(iii) Trivial.

□

Lemma 10.2. *If $\alpha \in \mathbb{Z}[\omega]$ and λ does not divide α, then $\alpha^3 \equiv \pm 1 \bmod \lambda^4$.*

We may use congruences in $\mathbb{Z}[\omega]$ in precisely the same way as we are used to in $\mathbb{Z}$. In particular $\alpha \equiv \beta \bmod \gamma$ means that $\gamma | \alpha - \beta$.

Proof. Since $N((\lambda)) = 3$ the quotient $\mathbb{Z}[\omega]/(\lambda)$ has 3 elements, which are clearly $0+(\lambda), 1+(\lambda)$ and $-1+(\lambda)$, since these are distinct. It follows that $\alpha + (\lambda) = \pm 1 + (\lambda)$, so that we may write $\alpha = \pm 1 + \lambda\mu$ for some $\mu \in \mathbb{Z}[\omega]$. We now have

$$\alpha^3 = \pm 1 + 3\mu\lambda \pm 3\mu^2\lambda^2 + \mu^3\lambda^3 = \pm 1 - \mu\lambda^3 \mp \mu^2\lambda^4 + \mu^3\lambda^3,$$

so that $\alpha^3 \equiv \pm 1 + (\mu^3 - \mu)\lambda^3 \bmod \lambda^4$.

However the coset $\mu + (\lambda)$ must be one of $0+(\lambda), 1+(\lambda)$ or $-1+(\lambda)$, so that $\mu \equiv 0$ or $\pm 1 \bmod \lambda$. It follows that $\mu^3 \equiv \mu \bmod \lambda$ whichever of these 3 cases holds. This yields $\lambda | \mu^3 - \mu$ and so $\alpha^3 \equiv \pm 1 \bmod \lambda^4$ as required. □

To prove the non-existence of nontrivial solutions in $\mathbb{Z}$ to $x^3 + y^3 = z^3$, it is sufficient to prove there are none in $\mathbb{Z}[\omega]$; if there were a non-trivial solution in $\mathbb{Z}[\omega]$, we could remove any common factor from x, y and z; indeed any two of the variables would then have to be coprime (since any common factor of two of x, y, z would also divide the remaining variable). We shall first show that at least one variable must be divisible by λ and then that we cannot have any variable divisible by λ, to obtain a contradiction.

Lemma 10.3. *If $\alpha^3 + \beta^3 = \gamma^3$ with $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, then λ divides at least one of α, β or γ.*

Proof. If λ divides none of α, β, γ then Lemma 10.2 yields

$$0 = \alpha^3 + \beta^3 - \gamma^3 \equiv (\pm 1) + (\pm 1) - (\pm 1) \equiv \pm 3 \text{ or } \pm 1 \bmod \lambda^4.$$

However $\lambda^4 = (-3)^2 = 9$ which does not divide ± 3 or ± 1. □

We shall now, over the next few lemmas, show that cannot have precisely one variable divisible by λ.

Lemma 10.4. *Let*

$$\alpha^3 + \beta^3 = \mu \lambda^{3n} \gamma^3$$

with $n \in \mathbb{N}$, with μ a unit of $\mathbb{Z}[\omega]$ and $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ with α, β coprime and γ not divisible by λ. Then $n \geqslant 2$.

Proof. If either of α or β is a multiple of λ then the equation shows that both are, since $n \geqslant 1$. However this is impossible, as α and β are assumed to be coprime. Thus neither of them is divisible by λ. Now Lemma 10.2 yields

$$\mu \lambda^{3n} \gamma^3 = \alpha^3 + \beta^3 \equiv (\pm 1) + (\pm 1) \equiv \pm 2 \text{ or } 0 \bmod \lambda^4,$$

so that $n \neq 1$. □

Lemma 10.5. *Under the conditions of the previous lemma each of the elements $\alpha + \beta$, $\alpha + \omega\beta$ and $\alpha + \omega^2\beta$ is divisible by λ. Moreover the quotients*

$$\frac{\alpha + \beta}{\lambda}, \ \frac{\alpha + \omega\beta}{\lambda}, \ \frac{\alpha + \omega^2\beta}{\lambda}$$

are coprime in pairs.

Proof. We have

$$\lambda | \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta),$$

so that λ must divide at least one of these factors. However λ is an associate of $1 - \omega$ and $1 - \omega^2$ by Lemma 10.1. Hence

$$\alpha + \beta \equiv \alpha + \omega\beta \equiv \alpha + \omega^2\beta \bmod \lambda.$$

It follows that all three factors are divisible by λ.

Moreover if δ divides both $\alpha+\beta$ and $\alpha+\omega\beta$ then it divides

$$(\alpha+\omega\beta)-(\alpha+\beta)=(\omega-1)\beta$$

and also

$$(\alpha+\omega\beta)-\omega(\alpha+\beta)=(1-\omega)\alpha.$$

Hence $\delta|\omega-1$, since α and β are coprime. Similarly if δ divides both $\alpha+\beta$ and $\alpha+\omega^2\beta$ then $\delta|\omega^2-1$, while if δ divides both $\alpha+\omega\beta$ and $\alpha+\omega^2\beta$ then $\delta|\omega^2-\omega$. It follows in all three cases that $\delta|\lambda$, since $\omega-1, \omega^2-1$ and $\omega^2-\omega$ are each associates of λ. The second assertion of the lemma then follows. □

Theorem 10.6. *The equation*

$$\alpha^3+\beta^3=\mu\lambda^{3n}\gamma^3$$

with $n\in\mathbb{N}$ and μ a unit of $\mathbb{Z}[\omega]$ has no solutions $\alpha,\beta,\gamma\in\mathbb{Z}[\omega]$ with α,β coprime and γ not divisible by λ.

Proof. We assume we have an admissible solution to

$$\alpha^3+\beta^3=\mu\lambda^{3n}\gamma^3,$$

with the minimal possible value of n. Then

$$\mu\lambda^{3n}\gamma^3=(\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta)$$

and the previous two lemmas allow us to write

$$\mu\lambda^{3(n-1)}\gamma^3=\left\{\frac{\alpha+\beta}{\lambda}\right\}\left\{\frac{\alpha+\omega\beta}{\lambda}\right\}\left\{\frac{\alpha+\omega^2\beta}{\lambda}\right\}$$

with coprime factors on the right, belonging to $\mathbb{Z}[\omega]$. Since the factors are coprime there is one factor, $(\alpha+\omega^j\beta)/\lambda$ say, which is divisible by $\lambda^{3(n-1)}$. Write $\nu=\omega^j\beta$; then:

$$\mu\gamma^3=\left\{\frac{\alpha+\nu}{\lambda^{3n-2}}\right\}\left\{\frac{\alpha+\omega\nu}{\lambda}\right\}\left\{\frac{\alpha+\omega^2\nu}{\lambda}\right\}$$

with coprime factors on the right.

We now use the fact that $\mathbb{Z}[\omega]$ is a UFD. We have three coprime factors whose product is a unit times a cube, and we deduce that each factor must be a unit times a cube, say

$$\frac{\alpha+\nu}{\lambda^{3n-2}} = \mu_1\gamma_1^3, \quad \frac{\omega\{\alpha+\omega\nu\}}{\lambda} = \mu_2\gamma_2^3, \quad \frac{\omega^2\{\alpha+\omega^2\nu\}}{\lambda} = \mu_3\gamma_3^3,$$

with $\gamma = \gamma_1\gamma_2\gamma_3$ (and where μ_2, μ_3 have absorbed the extra factors ω, ω^2, respectively). We now observe that

$$\begin{aligned}\mu_1\lambda^{3(n-1)}\gamma_1^3 + \mu_2\gamma_2^3 + \mu_3\gamma_3^3 & \\ &= \lambda^{-1}\{(\alpha+\nu) + (\omega\alpha+\omega^2\nu) + (\omega^2\alpha+\omega\nu)\} \\ &= 0,\end{aligned}$$

since $1+\omega+\omega^2 = 0$. We therefore obtain an equation

$$\gamma_2^3 + \mu'\gamma_3^3 = \mu''\lambda^{3(n-1)}\gamma_1^3$$

for appropriate units μ' and μ''. Moreover γ_2 and γ_3 are coprime, since $(\alpha+\omega\nu)/\lambda$ and $(\alpha+\omega^2\nu)/\lambda$ were coprime; and λ does not divide γ_1 since it did not divide γ.

After Lemma 10.4 we know that $n \geqslant 2$, so that $n-1 \geqslant 1$ and

$$\gamma_2^3 + \mu'\gamma_3^3 \equiv 0 \bmod \lambda^3.$$

From Lemma 10.2 we deduce that $\mu' \equiv \pm 1 \bmod \lambda^3$. However λ^3 does not divide any of $\omega \pm 1$ or $\omega^2 \pm 1$ since these are either units or associates of λ. Thus only $\mu' = \pm 1$ is possible. Hence, finally, we obtain an equation of the form

$$\gamma_2^3 + (\mu'\gamma_3)^3 = \mu''\lambda^{3(n-1)}\gamma_1^3,$$

contradicting the supposed minimality of n. This concludes the proof of the theorem. □

We are now in a position to prove our desired result.

Theorem 10.7. *The equation $x^3 + y^3 = z^3$ has no nontrivial (x, y, z all nonzero) solutions in $\mathbb{Z}$.*

Proof. Any such solution must also give a solution in $\mathbb{Z}[\omega]$. Remove any common factor from x, y, z, which means they must be coprime in pairs (since any common factor of two of x, y, z would also divide the remaining variable). By Lemma 10.3, at least one of x, y, z must be a multiple of λ, and indeed only one, since the variables are coprime in pairs. We extract the largest possible power of λ from this variable, λ^n say, and use $\mu = 1$ (and replace some of x, y, z with $-x, -y, -z$, as needed) to put the equation into the form described in Theorem 10.6, which we have shown to have no solution. □