Algebraic Number Theory

Vinesh Ramgi

July 12, 2019

Abstract

There's definitely mistakes in this but don't blame me if you fail (:

For an up to date version of this pdf, check my GitHub :)
https://github.com/vrvinny/algebraic_nt

Contents

1 Introduction/Review 4

1.1 Introduction 4

1.2 Definitions and Proofs 5

2 Materials from other courses on rings, ideals and fields 7

2.1 Quotient Rings 8

2.2 1st Isomorphism Theorem for Rings 9

2.3 Maximal Ideals 9

2.4 Field extensions 10

2.5 Finding Minimal Polynomials 11

2.6 Eisenstein's Criterion 11

2.7 Roots of Unity 12

2.8 Tower Law 13

2.9 Primitive Element Theorem 14

2.10 Conjugates and Complex Field Embeddings 14

2.11 Galois Separability Lemma 14

3 Rings of Algebraic Integers 16

3.1 The Standard Represenation 19

3.1.1 Properties of the Standard Representation 20

3.2 Norms and Traces 23

3.3 Properties of Norms and Traces 24

3.4 Integral Bases 24

3.5 Quadratic Fields 30

3.6 Cubic Fields 31

3.7 Cyclotomic Fields 34

4 Factorisation in Rings of Algebraic Integers 36

4.1 Prime ideals and Maximal ideals 39

4.2 Fractional Ideals and Unique Factorisation 41

4.3 Tricky Lemma 41

4.4 Norms of Ideals 45

4.5 Dedekind's Criterion 47

4.6 Ramified Primes 51

4.7 Quadratic Fields 52

4.8 Cyclotomic Fields 53

5 Class Groups 55

5.1 How to Calculate the Class Group 56

5.2 Ideal Descent Lemma 57

5.3 Calculating Class Groups 58

5.4 Using Class Groups in Diophantine Equations 63

5.5 Geometry of Numbers 64

5.5.1 Minkowski's Lemma 65

5.5.2 Minkowski Space 65

5.6 Messy Lemma 67

1 Introduction/Review

1.1 Introduction

This is the study of certain rings, numbers called algebraic integers, e.g.

- Quadratic rings $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$
- Cyclotomic rings $\mathbb{Z}[\zeta_n] \implies y = e^{2\pi\imath/n}$
- $\mathbb{Z}[z\sqrt{2}] = \{x + y^3\sqrt{2} + z^3\sqrt{z}^2\}\ x, y, z \in \mathbb{Z}$

Definition 1.1. *A Diophantine equation is an equation of the form $f(x_1, \ldots, x_n) = 0$ where f is a polynomial with coefficients in $\mathbb{Z}$*

We'll usually be interested in solution in integers (or maybe rational numbers), for example, Pell's equation- $x^2 - dy^2 = 1$, or $N(A) = n$ where $A = x + y\alpha$, $\alpha = \{\sqrt{d}, \frac{1+\sqrt{d}}{2}\}$.

In general Diophantine equations are hard, Matiyasevich's theorem shows Diophantine equations are as hard as any mathematical question. Inspite of this, there are some Diophantine eqations for which we have methods for solving, e.g. *What are the integer solutions of $x^3 = y^2 + y = y(y+1)$?*.

Since $y, y+1$ are both coprime and their product is a cube, both y and $y+1$ are a cube which implies $y = 0, -1$. So we have two solutions, $(0,0), (0,-1)$. To do this we used this lemma:

Lemma 1.2. *Descent Lemma*

Let R be a ring be a unique factorisation domain. Suppose $a, b, c \in R$ and $a^n = bc$. If b, c are coprime in R then $b = u^{rn}$, $c = vs^n$ where u, v are units in R.

Another example, $x^3 = y^2 + 1$:

Problem, $y^2 + 1$ doesn't factorise in $\mathbb{Z}$ but it does factorise in $\mathbb{Z}[i] \implies x^3 = (y+i)(y-i)$. We want to use the Descent lemma to solve the equation.

- $\mathbb{Z}[i]$ is a unique factorisation domain
- Are $y + i$ and $y - i$ coprime in $\mathbb{Z}[i]$?

Suppose $p \in \mathbb{Z}[i]$ is an irreducible common factor of $y+i$, $y-i$. If $p|y+i$ and $p|y-i \implies p|(y+i) - (y-i) \implies p|2i$. This means the norms also divide each other, $N(p)|N(2i) \implies N(p)|4$.

$N(p) \neq \pm 1$ because p isn't a unit, therefore, $2|N(p)|N(y+i) \implies N(y+i) = y^2 + 1 = x^3$, so $2|x^3$.

Since 2 is a prime, $2|x \implies x^3 \equiv 0 \pmod{8}$. This implies $y^2 + 1 \equiv 0 \pmod{8}$

y	$y^2 \mod 8$
0	0
± 1	1
± 2	4
± 3	1
4	0

Since the equation has no solutions, $y^2 + 1 \equiv 0 \ \ (8)$ has no solutions.
So $y+i, y-i$ are coprime in $\mathbb{Z}[i]$.
$\therefore y+1 = uA^3$ with $u \in \mathbb{Z}[i]^\times$, $A \in \mathbb{Z}[i]$ with $u = \pm 1$ or $\pm i$

So in fact

$$\begin{aligned} y+i &= (r+si)^3 \quad r,s \in \mathbb{Z} \\ &= r^3 + 3ir^2s - 3rs^2 - is^3 \\ &= r^3 - 3rs^2 + i(3r^2s - s^3) \end{aligned}$$

Organising the terms gives a new Diophantine equation:

$$1 = 3r^2s - s^3 \qquad\qquad y = r^3 - 3rs^2$$

We can solve the new equation:

$1 = (3r^2 - s^2)s \implies s = \pm 1$

If $s = 1 \implies 3r^2 - 1 = 1$ ↯
If $s = -1 \implies 3r^2 - 1 = -1 \implies r = 0 \quad$ so $(r,s) = (0,-1)$

This implies $x = 1, y = 0$ so $(1,0)$ is the only solution in integers.

This motivates the question: which rings are unique factorisation domains? More specifically which rings of algebraic integers are unique factorisation domains?

1.2 Definitions and Proofs

A ring is a set R with two operations + & ×. $(R,+)$ is an abelian group with identity element 0. × is commutative, associative and has identity 1. $x(y+z) = xy + xz \ \forall x,y,z \in R$

An element $x \in R$ is:

- a unit if $\exists\ x^{-1} \in R$ such that $xx^{-1} = 1$
- reducible if $x = yz$ where y, z not units
- irreducible otherwise

For examples, in $\mathbb{Z}$, units are ± 1, irreducible elements are $\pm p$ for prime numbers p.

Definition 1.3. *A ring R is an integral domain if $xy = 0 \implies x = 0$ or $y = 0$*

Lemma 1.4. *Cancellation property: If R is an integral domain, if $x \neq 0$ then $xy = xz \implies y = z$*

Proof.

$$\begin{aligned} xy = xz &\implies x(y-z) = 0 \text{ and since } x \neq 0 \\ &\implies y - z = 0 \\ &\implies y = z \end{aligned}$$

□

A ring R is a unique factorisation domain if:

- R is an integral domain
- If $x \in R$ and $x \neq 0$ then $x = Up_1 \dots p_r$ with $U \in R^\times$ and P_i irreducible

Suppose $p_1 \dots p_r = q_1 \dots q_s$ with p_i, q_i irreducible then $r = s$ and we can renumber so that $q_i = Up_i$ with $U \in R^\times$.

The 3^{rd} condition is equivalent to if $p \in R$ is irreducible and $p|ab$ then $p|a$ or $p|b$.

Lemma 1.5. *Descent Lemma: Let R be a UFD (Unique Factorisation Domain) and let $a, b, c \in R$ with $a^n = bc$ and b, c coprime. Then $b = ur^n$ and $c = vs^n$ with $u, v \in R^\times$*

Proof. If a is a unit then b and c are units, so the result is true.

If $a = 0$ then $b = 0$ or $c = 0$.

WLOG assume $b = 0 = 1 * 0^n$. But b and c are coprime $\implies$ c must be a unit (since it is a common factor of b and c.

In other cases $a = p_1 \dots p_r$ with p_i irreducible. So

$$b = (\text{a unit}) * p_1^{s_1} \dots p_r^{s_r} \qquad\qquad s_i + t_i = n \forall i$$
$$c = (\text{a unit}) * p_1^{t_1} \dots p_r^{t_r}$$

But we're assuming b, c are coprime so:
$\implies$ each s_i is either 0 or n
$\implies$ b = (a unit) * (some n^{th} power) $\implies$ c = (a unit) * (some n^{th} power) □

Reminder about quadratic rings
Let $d \neq 1$ be a square free integer and $\mathbb{Z}[\alpha] = \{x + y\alpha : x, y \in \mathbb{Z}\}$

$$\alpha = \alpha_d = \begin{cases} \sqrt{d} & d \not\equiv 1 \ \ (4) \\ \dfrac{1+\sqrt{d}}{2} & d \equiv 1 \ \ (4) \end{cases}$$

If $A = x + y\sqrt{d}$ then $\bar{A} = x - y\sqrt{d}$ and $N(A) = A\bar{A} = x^2 - dy^2$.
Similarly $N(x + y\frac{1+\sqrt{d}}{2}) = x^2 + xy + \frac{1-d}{4}y^2$.

The ring $\mathbb{Z}[\alpha]$ is norm-Euclidean if for all $A, B \in \mathbb{Z}[\alpha]$ iwht $B \neq 0$, $\exists Q, R \in \mathbb{Z}[\alpha]$ such that $A = QB + R$ and $|N(R)| < |N(B)|$.

Proposition 1.6. *If $\mathbb{Z}[\alpha]$ is norm-Euclidean then $\mathbb{Z}[\alpha]$ is a UFD.*

Proof. (Sketch)
We'll show that if $p \in \mathbb{Z}[\alpha]$ is irreducible and $p|AB$ then $p|A$ or $p|B$.
If $p \not| A$ then $hcf(A, P) = 1 \implies 1 = HA + KP$ by the Euclidean algorithm.
$$B = \underbrace{HAB}_{\text{multiple of } p} + \underbrace{KPB}_{\text{multiple of } p} \implies p|B$$
□

Theorem 1.7. *Disappointing Theorem: $\mathbb{Z}[\alpha_d]$ is norm-Euclidean in the following cases $d = 2, 3, 5, 13, -1, -2, -3, -7, -11$. Conjecturally there are infinitely many real quadratic rings which are UFD.*

2 Materials from other courses on rings, ideals and fields

Mainly from Galois Theory, Commutative Algebra and Groups and Rings. In this course,

- All rings are commutative with 1
- A field is a ring with $1 \neq 0$
- If $x \neq 0$, x is a unit

Definition 2.1. *An ideal I in a ring R is a subset of R such that:*

- *$(I.+)$ is a subgroup of R*
- *$\forall x \in R,\ y \in I \implies xy \in I$*

Examples: If $x \in R$ then we define $(x) = \{xy : y \in R\}$. This set (x) is an ideal in R.

Definition 2.2. *Ideals of the form (x) are called principal ideals. (x) is the principle ideal generated by x.*
$(x_1, \dots, x_n) = \{x_1y_1 + \cdots + x_ny_n : y_i \in R\}$ this is also an ideal.

E.g. in $\mathbb{Z}$ $(4, 6) = (2)$ and in general $(n, m) = (hcf(n, m))$

Definition 2.3. *A principal ideal domain is an integral domain such that all ideals are principal. A Noetherian ring is a ring in which ideals are finitely generated.*

To show that $(x_1, \dots, x_n) \subseteq I$, it is equivalent to showing $x_1, \dots, x_n \in I$
E.g. in $\mathbb{Z}$ $(4, 6) = (2)$

Proof.

$$\begin{aligned} (4,6) &\subseteq 2 \\ 4 = 2 * 2 &\in (2) \\ 6 = 2 * 3 &\in (2) \end{aligned} \qquad\qquad \begin{aligned} (2) &\subseteq (4,6) \\ 2 = 2 * 4 + (-1) * 6 &\in (4,6) \end{aligned}$$

□

Definition 2.4. *A principal ideal domain is an integral domain in whicch every ideal is principal*

E.g. $\mathbb{Z}$ is a PID

Proof. Suppose $I \subseteq \mathbb{Z}$ is an ideal.

If $I = \{0\}$ then $I = (0)$.
If $I \neq \{0\}$ choose $x \in I$ with $|x|$ as small as possible with $x \neq 0$.

Claim $I = (x)$, $x \in I \implies x \subseteq I$.

Conversely, suppose $y \in I$ with $y = qx + r$ such that $|r| < |x|$. This means that $r = y - qx \in I \implies r = 0 \implies y = qx \in (x)$ which means $I \subseteq (x)$. □

E.g. If $\mathbb{Z}[\alpha]$ is a norm-Euclidean quadratic ring then $\mathbb{Z}[\alpha]$ is a PID.

Proof. Replace $|x|$ by $|N(A)$ for $A \in \mathbb{Z}[\alpha]$. □

E.g. If k is a field then $k[x]$ is a PID.

Proof. Replace $|x|$ by $deg(f)$ for $f \in k[x]$. □

2.1 Quotient Rings

Let I be an ideal in R, we'll say $x = y \in (I)$ if $x - y \in I$.

$R/I = \{\text{Congruency classes of elements of } R\}$

Lemma 2.5. *If $x \equiv x'\ (I)$ and $y \equiv y'\ (I)$ then $x + y \equiv x' + y'\ (I)$ and $xy = x'y'\ (I)$*

This means we can make R/I into a ring.

Proof. If $x - x' \in I$ and $y - y' \in I$ then:

$$(x + y) - (x' + y') = (x - x') + (y - y') \in I$$

$$\begin{aligned} xy - x'y' &= xy - xy' + xy' - x'y' \\ &= x(y - y') + (x - x')y \in I \end{aligned}$$

□

E.g. If $R = \mathbb{Z}$, $I = (n)$ and $x \equiv x'(I) \Leftrightarrow x \equiv x' \quad (n) \implies R/i = \mathbb{Z}/n$

E.g. If k is a field an $f \in k[x]$ with degree d and $I = (f)$, every element of $k[x]$ is congruent to a unique polynomial of degree $< d$. (The remainder after dividing by f).
$\therefore R/I = \{a_0 + a_1 + \cdots + a_{d-1}x^{d-1} : a_i \in k\}$

Definition 2.6. *Let R and S be rings. A ring homomorphism is a function $\phi : R \to S$ such that:*

- $\phi(x + y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x) + \phi(y)$

- $\phi(1_R) = 1_S$

$ker(\phi) = \{x \in R : \phi(x) = 0\}$ and $ker(\phi)$ is an ideal of R (trivial to prove)
$im(\phi) = \{\phi(x) : x \in R\}$ and $im(\phi)$ is a subring of S

2.2 1st Isomorphism Theorem for Rings

Let $\phi : R \to S$ be a ring homomorphism. Then there is an isomorphism:

$$R/ker(\phi) \cong im(\phi) \text{ by the mapping } (x \mod ker(\phi)) \to \phi(x)$$

2.3 Maximal Ideals

Definition 2.7. *Let R be a ring. An ideal $M \subseteq R$ is maximal if:*

- *$M \neq R$*
- *If $M \subseteq I \subseteq R$ with I an ideal then $I = M$ or R*

Proposition 2.8. *Suppose R is a PID, an ideal (x) is maximal if and only if x is irreducible.*

Proof. Algebra 4 □

Note that the difference between a field and a ring is that if $x \neq 0$ then $xx^{-1} = 1$ and $1 \neq 0$.

Proposition 2.9. *In any ring R, M is maximal if and only if R/M is a field*

Proof. ($\implies$) Assume M is maximal therefore $M \neq R$ and $1 \notin M$ and $1 \not\equiv 0 \pmod{M}$.
Assume $x \not\equiv 0 \pmod{M}$, let I be the ideal generated by M and x, then $I \supsetneq M$ which means $I = R$.

$I = \{m + xy : m \in M, y \in R\} \implies 1 = m + xy$ and $1 \equiv xy \pmod{M}$

($\Longleftarrow$) Assume R/M is a field so $1 \not\equiv 0 \pmod{M}$.
$\therefore 1 \notin M$ so $M \neq R$.
Suppose $M \subsetneq I$, want to show $I = R$. Choose $x \in I, x \notin M$ so $x \not\equiv 0 \pmod{M}$
So $\exists y$ such that $xy =\equiv 1 \pmod{M}$ and by the definition of existence of x^{-1}, $1 \in I \implies I = R$ □

Corollary 2.10. *Let k be a field and $f \in k[x]$, then $k[x]/(f)$ is a field if f is irreducible over k*

Proof. f irreducible $\iff$ (f) is maximal $\iff$ $k[x]/(f)$ is a field.
(Polynomial ring is ideal) □

2.4 Field extensions

Definition 2.11. *If k and l are fields with $k \subseteq l$ then k is a subfield of l.*
l is called a field extension of k, e.g. $\mathbb{R} \subseteq \mathbb{C}$

When l is an extension of k, we can think of l as a vector space over k.

E.g. $\mathbb{C}$ has basis $\{1, i\}$ as a vector space over $\mathbb{R}$
The degree of the extension $[l : k]$ is the dimension of l as a vector space over k
E.g. $[\mathbb{C} : \mathbb{R}] = 2$
E.g. $\mathbb{Q}(i) = \{x + iy : x, y \in \mathbb{Q}\}$
This is an extension of $\mathbb{Q}$ with basis $\{1, i\} \implies [\mathbb{Q}(i) : \mathbb{Q}] = 2$

E.g. Let $f \in \mathbb{Q}[x]$ be irreducible $\implies \mathbb{Q}[x]/(f) = \{a_0 + a_1x + \ldots a_{d-1}x^{d-1}\}$ is a field.
This is an extension of $\mathbb{Q}$ and has degree $d = deg(f)$.
$\{1, x, \ldots, x^{d-1}\}$ is a basis, so $[\mathbb{Q}[x]/(f) : \mathbb{Q}] = d = deg(f)$.

Notation: Let l be an extension of k and let $\alpha \in l$, then:

Definition 2.12. *α is called "algebraic over k" if there exists a non-zero $f \in k[x]$ such that $f(\alpha) = 0$. Otherwise α is transcendental.*

E.g. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^2 - 2$

For any $\alpha \in l$ $k[\alpha] = \{g(\alpha) : g \in k[x]\}$, the ring generated by k and α.
$k(\alpha) = \{\dfrac{g(\alpha)}{h(\alpha)} : g, h \in k[x], h(\alpha) \neq 0\}$, the field generated by k and α.

Proposition 2.13. *Let α be algebraic over k. Then there is a unique monic polynomial $m(x) \in k[x]$ such that:*

- $m(\alpha) = 0$
- $f(\alpha) = 0 \iff m|f$

m is the only monic irreducible polynomial over k such that $m(\alpha) = 0$.

Definition 2.14. *This polynomial is called the minimal polynomial of α over k*

E.g. i is algebraic over $\mathbb{R}$ with minimal polynomial $x^2 + 1$
i is algebraic over $\mathbb{Q}$ with minimal polynomial $x^2 + 1$
i is algebraic over $\mathbb{C}$ with minimal polynomial $x - i$

Corollary 2.15. *Let α be algebraic over k, then $k[\alpha] = k(\alpha)$, i.e. $k[\alpha]$ is a field and there is an isomorphism*

$$k[x]/(m) \cong k(\alpha)$$
$$(g(x) \mod m) \mapsto g(\alpha)$$
$$a_0 + a_1x + \cdots + a_{d-1}x^{d-1} \mapsto a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$$

where m is the minimal polynomial and has degree d.

$\{1, \alpha, \ldots, \alpha^{d-1}\}$ forms a basis for $k(\alpha)$ and $[k(\alpha) : k] = d = deg(m)$

Proof. We have a homomorphism (surjective) $k[x] \to k[\alpha] \implies k[x]/(m) \cong k[\alpha]$ and $g \to g(\alpha)$. (Field because m is irreducible)

Kernel $= \{g : g(\alpha) = 0\} = (m)$, therefore $k[\alpha] = k(\alpha)$ the isomorphism takes $(g(x) \mod m)$ to $g(\alpha)$.

$\{1, x, \ldots, x^{d-1}\}$ is a basis for $k[x]/(m)$

So $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis for $k(\alpha)$ □

E.g. i is algebraic over $\mathbb{R}$ with minimal polynomial $x^2 + 1$
$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{R}(i) = \mathbb{C}$ with the map $a + bx \mapsto a + bi \; a, b \in \mathbb{R}$

Similarly $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$ with $a, b \in \mathbb{Q}$ with the map $a + bx \mapsto a + bi$

E.g. $\alpha = \sqrt[3]{2}$ This is a root of $x^3 - 2$ and so α is algebraic (over $\mathbb{Q}$).
$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\alpha)$ with the mapping $a + bx + cx^2 \mapsto a + b\alpha + c\alpha^2$.
The degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ with $\{1, \alpha, \alpha^2\}$ a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

2.5 Finding Minimal Polynomials

We need methods to check that a polynomial is irreducible over $\mathbb{Q}$.

Lemma 2.16. *Gauss Lemma: Suppose $f \in \mathbb{Z}[x]$ and $f = gh \;\; g, h \in \mathbb{Q}[x]$, then there exists $c \in Q^\times$ such that cg and c^{-1} are in $\mathbb{Z}[x]$.*

Lemma 2.17. *Monic Gauss Lemma: Let $f \in \mathbb{Z}[\alpha]$ be monic, if $f = gh \in \mathbb{Q}[x]$ both monic then $g, h \in \mathbb{Z}[x]$.*

Corollary 2.18. *If $f \in \mathbb{Z}[x]$ is monic the f is irreducible over $Q \iff$ irreducible over $\mathbb{Q}$*

Corollary 2.19. *Let $f \in \mathbb{Z}[x]$ be monic. Let $\bar{f}$ be the reduction of $f \mod n$, i.e. $\bar{f} \in (\mathbb{Z}/n)[x]$. If $\bar{f}$ is irreducible then f is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$. Note that n doesn't need to be prime*

2.6 Eisenstein's Criterion

Let $f \in \mathbb{Z}[x]$ and let p be prime. Let $f(x) = a_d x^d + \cdots + a_0$, if $p \not| a_d$ and $f(x) \equiv a_d x^d \;\; (p)$ and let $f(0) \not\equiv 0 \;\; (p^2)$ then f is irreducible over $\mathbb{Z}/p^2$ and over $\mathbb{Q}$.

E.g. $\alpha = 10^{\frac{1}{11}} \implies \alpha^{11} = 10$.
α is a root of $x^{11} - 10$
$x^{11} - 10$ is irreducible by Eisenstein's Criterion (either with $p = 2$ or $p = 5$)
So $m_\alpha(x) = x^{11} - 10$

E.g. $\alpha = 2^{\frac{2}{3}}$
$\alpha^3 = 4$

α is a root of $m(x) = x^3 - 4$

To show that m is the minimal polynomial, we must show that m is irreducible.

$m(x+1) = x^3 + 3x^2 + 3x - 3$

$m(x+1)$ is irreducible by Eisenstein's criterion with $p = 3 \implies m(x)$ is irreducible.

E.g. $\alpha = 3^{\frac{2}{3}}$

$\alpha^3 - 9 = 0$

α is a root of $m(x) = x^3 - 9$. Note that $deg(m) = [\mathbb{Q}[\alpha) : \mathbb{Q}]$. To show that m is the minimal polynomial it's sufficient to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 3$

$\alpha = 3\beta$ where $\beta = 3^{\frac{1}{3}} = \frac{1}{3}\alpha^2$ so $\beta \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$

β has minimal polynomial $x^3 - 3$ (by Eisenstein's criterion)

$\therefore [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$

$\therefore m(\alpha)$ has degree ≥ 3

$\therefore m_\alpha = x^3 - 9$

Alternatively suppose $x^3 - 9$ factorises over $\mathbb{Q}$. By the Monic Gauss lemma, $x^3 - 9 = (x - a)(x^2 + bx + c)$. By comparing coefficients, $ac = 9$, which means $a = \pm 1$ or ± 3 or ± 9 and $a^3 = 9$ because a is a root. ϟ

E.g. $\alpha = \sqrt{2} + \sqrt{3}$

$$\begin{aligned} \alpha^2 &= 2 + 2\sqrt{6} + 3 \\ &= 5 + 2\sqrt{6} \end{aligned} \qquad\qquad (\alpha^2 - 5) - 24 = 0$$

So α is a root of $m(x) = x^4 - 10x^2 + 1$

Suppose $m(x) = (x - a)(x^3 + bx +^2 +cx + d)$ with $a, b, c, d \in \mathbb{Z}$

a is a root of m and a is a factor of $m(0) = 1$ so $a = \pm 1$ which is a contradiction since $m(\pm 1) = -8 \neq 0$.

The other possible factorisation is $m(x) = (x^2 + ax + b)(x^2 + cx + d)$. Comparing coefficients:

$$\begin{aligned} 0 &= a + c \\ -10 &= b + d + ac \qquad\qquad c = -a \qquad\qquad a^2 = 10 \pm 2 = 8 \text{ or } 12 \text{ ϟ} \\ 0 &= ad + bc \\ 1 &= bd \qquad\qquad b = d = \pm 1 \end{aligned}$$

2.7 Roots of Unity

Let n be a positive integer. An n^th root of unity is a complex number ζ such that $\zeta^n = 1$. A primitive n^{th} root of unity is an n^{th} root of unity which is not a d^{th} root of unity for any $d < n$.

n^{th} root of unity: $e^{2\pi i \frac{a}{n}}$ for $a = 0, 1, \ldots, n-1$

Primitive n^{th} root of unity $e^{2\pi i \frac{a}{n}}$ for $a \in (\mathbb{Z}/n)^\times$.

There are $\phi(n)$ primitive n^{th} roots of unity.

The n^{th} cyclotomic polynomial is $\Phi_n(x) = \underbrace{\prod}_{\substack{\text{Primitive } n^{th} \\ \text{roots of unity}}} (x - \zeta)$

$deg(\Phi_n(x)) = \phi(n)$

Lemma 2.20. *For any n: $\prod_{d|n} \Phi_d(x) = x^n - 1$. We can use this to calculate Φ_n.*

E.g. If p prime then $\Phi_1(x)\Phi_p(x) = x^p - 1$.

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

Corollary 2.21. *$\Phi_n(x)$ has coefficient in $\mathbb{Z}$.*

Remark: If ζ is a primitive n^{th} root of unity then ζ is a root of Φ_n

Theorem 2.22. *Each Φ_n is irreducible over $\mathbb{Q}$. So Φ_n is the minimal polynomial of a primitive n^{th} root of unity.*

2.8 Tower Law

Theorem 2.23. *Suppose $k \subseteq l \subseteq m$ be fields. Then $[m : k] = [m : l] * [l : k]$*

Proof. Sketch: Let $\{b_1, \ldots, b_n\}$ be a basis for l as a vector space over k.
Let $\{c_1, \ldots, c_m\}$ be a basis for m over k.
Then $\{b_i, c_j\}$ s a basis for m over k. □

E.g. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $x^2 - 2$ is the minimal polynomial.

The minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is a factor of $x^2 - 3$ so degree is 1 or 2.
From the Tower theorem, we know $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = \cancel{2}$ or 4.

$\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\mathbb{Q} \underbrace{\subseteq}_{\substack{\text{deg 4 since} \\ \alpha \text{ has} \\ \text{minimal} \\ \text{polynomial} \\ x^4 - 10x^2 + 1}} \mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

By the Tower law $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is a multiple of 4.

$\therefore [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

$\therefore [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}] = 2$

$x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$

Also $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\alpha)] = 1$ i.e. $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\alpha)$

This is an example of:

2.9 Primitive Element Theorem

Theorem 2.24. *Suppose k is an extension of $\mathbb{Q}$ of finite degree then there exists $\alpha \in k$ such that $k = \mathbb{Q}(\alpha)$*

Proof. Sketch: k has only finitely many subfields. Choose an $\alpha \in k$ which is not in any of the proper subfields.

$\mathbb{Q}(\alpha)$ is not contained in a proper subfield of k but $\mathbb{Q}(\alpha)$ is a subfield of k, therefore $\mathbb{Q}(\alpha) = k$. □

2.10 Conjugates and Complex Field Embeddings

Let α, β be algebraic numbers. Then α and β are conjugates if $m_\alpha = m_\beta$. They have the same minimal polynomial over $\mathbb{Q}$.

E.g. $\alpha = i$, $\beta = -i$ both have minimal polynomial $x^2 + 1$.
E.g. $\zeta = e^{2\pi i \frac{1}{100}}$ This is a conjugate of ζ^3, both have minimal polynomial Φ_{100}.
E.g. $\sqrt{2} + \sqrt{3}$ has conjugates $\pm\sqrt{2} \pm \sqrt{3}$

2.11 Galois Separability Lemma

Lemma 2.25. *If α is algebraic over $\mathbb{Q}$ then $m_\alpha(x)$ has no repeated roots in $\mathbb{C}$, i.e. α has exactly d conjugates in $\mathbb{C}$ where $d = deg(m(x)) = [\mathbb{Q}(\alpha):\mathbb{Q}]$*

Proof. Suppose $(x-\beta)^2 \mid m_\alpha(x)$ where m_α is the minimal polynomial of β over $\mathbb{Q}$.

If $(x-\beta) \mid m_\alpha$ then $\alpha - \beta \mid m'_\alpha(x)$ but m'_α has smallest degree than m_a. ↯

□

Definition 2.26. *An algebraic number field is an extension $k \supseteq \mathbb{Q}$ with $[k:\mathbb{Q}]$*

By the primitive element theorem $k = \mathbb{Q}(\alpha)$ for some $\alpha \in k$ so $k \cong \mathbb{Q}[x]/(m)$ when m is the minimal polynomial of α and $deg(m) = [k:\mathbb{Q}]$. The polynomial has exactly d roots in $\mathbb{C}$ where $d = deg(m)$. Call these roots α_1, α_d. Each α_i has minimal polynomial m over $\mathbb{Q}$.

$\therefore \mathbb{Q}[x]/(m) \cong \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$

So for each conjugate α_i of α in $\mathbb{C}$, there is a field homomorphism:

$$\sigma_i : k \to \mathbb{C}$$
$$k \to \mathbb{Q}[x]/(m) \to \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}$$

$$a_0 + a_1\alpha + \cdots + a_{d-1} \to \quad a_0 + a_1 x_1 + \cdots + a_{d-1}x^{d-1} \to \quad a_0 + a_1\alpha_1 + \cdots + a_{d-1}\alpha_i^{d-1}$$

$$\sigma_i(a_0 + \cdots + a_{d-1}\alpha^{d-1}) = a_0 + \cdots + a_{d-1}\alpha_i^{d-1}$$

Proposition 2.27. *$\sigma_1, \ldots, \sigma_d$ are all the field homomorphisms from k to $\mathbb{C}$*

E.g. $k = \mathbb{Q}(\sqrt{2})$

The conjugates of $\sqrt{2}$ in $\mathbb{C}$ are ± 2. $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$

$$\sigma_1(x + y\sqrt{2}) = x + y\sqrt{2}$$
$$\sigma_2(x + y\sqrt{2}) = x - y\sqrt{2}$$

$k = \mathbb{Q}(\alpha)$, $m(x) = x^3 - 2$ and $\alpha_1 = 2^{\frac{1}{3}}$, $\alpha_2 = 2^{\frac{1}{3}} e^{\frac{2\pi i}{3}}$, $\alpha_3 = 2^{\frac{1}{3}} e^{\frac{4\pi i}{3}}$

3 Rings of Algebraic Integers

Definition 3.1. *Let k be a field extension of $\mathbb{Q}$. $\alpha \in k$ is an algebraic number if $f(\alpha) = 0$ for some $f \in \mathbb{Q}[x]$.*

α is an algebraic integer if $f(\alpha) = 0$ for some $f \in \mathbb{Z}[x]$.

E.g. $\sqrt{2}$ is an algebraic integer $f(x) = x^2 - 2$
E.g. $\alpha = \frac{1+\sqrt{5}}{2}$

$$\begin{aligned}\left(\alpha - \frac{1}{2}\right)^2 - \frac{5}{4} &= 0 \\ \alpha^2 - \alpha - 1 &= 0\end{aligned}$$

So $f(x) = x^2 - x - 1$

E.g. $\zeta = e^{\frac{2\pi i}{n}}$ then $f(x) = x^n - 1 \implies \zeta$ is an algebraic integer.

Proposition 3.2. *Suppose α is an algebraic number. Then α is an algebraic integer $\iff$ $m_\alpha \in \mathbb{Z}[x]$ (minimal polynomial).*

E.g. $\frac{1}{\sqrt{2}}$ is not an algebraic integer, it's minimal polynomial is $x^2 - \frac{1}{2}$

Proof. ($\Longleftarrow$) if $m_\alpha(x) \in \mathbb{Z}[x]$ then α is an algebraic integer $m_\alpha(\alpha) = 0$ and $m_\alpha \in \mathbb{Z}[x]$ is monic.
($\implies$) Assume α is an algebraic integer $f(\alpha) = 0$, $f \in \mathbb{Z}[x]$ monic.
$m_\alpha | f$ in $\mathbb{Q}(x)$ by definition of m_α, i.e. $f = m_\alpha^\times q$, $m_\alpha, q \in \mathbb{Q}[x]$ monic.
By the Monic Gauss lemma, m_α and $q \in \mathbb{Z}[x]$. □

Corollary 3.3. *The algebraic integers in $\mathbb{Q}$ are $\mathbb{Z}$*

Proof. Let $\alpha \in \mathbb{Q}$. $m_\alpha(x) = x - \alpha$. $m_\alpha \in \mathbb{Z}[x] \iff \alpha \in \mathbb{Z}$. □

Main aim of this chapter: Given an algebraic number field k, what are the algebraic integers in k?

Notation: $\mathcal{O}_k = \{$Algebraic integers in $k\}$.

E.g. $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ If $\alpha \in Q$ then $m_\alpha(x) = x - \alpha$

Proposition 3.4. *Let A be an $n * n$ matrix with entries in $\mathbb{Z}$. Then all eignevalues of A are algebraic integers.*

Proof. The eigenvalues are roots of $Ch_A(x) = \det(xI_n - A)$ □

Notation: $\mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[x]\}$ the ring generated by α

As a group $\mathbb{Z}[\alpha]$ is generated by $\{1, \alpha, \alpha^2, \dots\}$, i.e. $\mathbb{Z}[\alpha] = Span_{\mathbb{Z}}\{1, \alpha, \alpha^2 \dots\}$

Sometimes $\mathbb{Z}[\alpha]$ is finitely generated as an additive group, i.e. $\mathbb{Z}[\alpha] = Span_{\mathbb{Z}}\{b_1, \dots, b_r\}$.

E.g. $\mathbb{Z}[\sqrt{2}] = Span_{\mathbb{Z}}\{b_1, \dots, b_r\}$

Proposition 3.5. *$\mathbb{Z}[\alpha]$ is finitely generated as an additive group $\iff$ α is an additive integer.*

Proof. ($\implies$) Assume $\mathbb{Z}[\alpha] = Span_{\mathbb{Z}}\{b_1, \dots, b_r\}$ with $b_i \in \mathbb{Z}[\alpha]$

$$\alpha = a_{i1}b_1 + \dots + a_{1r}b_r \qquad \text{for some } a_{ij} \in \mathbb{Z}$$

$$\alpha b_1 = a_{11} + \dots a_{1r}b_r$$

$$\vdots \qquad \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = (a_{ij}) \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

$$\alpha b_r = ar_1 + \dots a_{rr}b_r$$

$$\alpha$$

So α is an eigenvalue of (a_{ij}) and α is an algebraic integer.

($\impliedby$) Assume α is an algebraic integer $f(\alpha) = 0$ for some monic $f \in \mathbb{Z}[x]$.
Let $d = deg(f)$, claim $\mathbb{Z}[\alpha] = Span_{\mathbb{Z}}\{1, \alpha, \dots, \alpha^{d-1}\}$.
Let R be a ring, $f, g \in R[x]$ such that $g = qf + r$ for $q, r \in R[x]$ with $deg(r) < d$

$$\mathbb{Z}[\alpha] = \{g(\alpha : g \in \mathbb{Z}[x]\}$$

$$g = qf = r, \quad deg(r) < d, \quad q, r \in \mathbb{Z}[x]$$

$$g(\alpha) = q(\alpha)f(\alpha) + r(\alpha)$$

$$g(\alpha) = r(\alpha) = a_0 + a_1\alpha + \dots + a_{d-1}\alpha^{d-1}$$

$$g(\alpha) \in Span_{\mathbb{Z}}\{1, \alpha, \dots, \alpha^{d-1}\}$$

□

Corollary 3.6. *Let $\alpha, \beta \in k$ be both algebraic integers, then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ are algebraic integers form a subring of k.*

Proof. Let $\mathbb{Z}[\alpha] = Span_{\mathbb{Z}}\{1, \alpha, \dots, \alpha^{d-1}\}$
$\mathbb{Z}[\beta] = Span_{\mathbb{Z}}\{1, \beta, \dots, \beta^{e-1}\}$

$$\alpha^i * \beta^j \in Span_{\mathbb{Z}}\{\alpha^i\beta^j : i < d, j < e\}$$

$$\therefore \mathbb{Z}[\alpha, \beta] = Span_{\mathbb{Z}}\{\alpha^i\beta^j : i < d, j < e\}$$

So $\mathbb{Z}[\alpha,\beta]$ is finitely generated.

Let $\gamma = \alpha+\beta$ or $\alpha-\beta$ or $\alpha\beta$ so $\gamma \in \mathbb{Z}[\alpha,\beta]$

$\mathbb{Z}[\gamma] \subseteq \mathbb{Z}[\alpha,\beta] \implies \mathbb{Z}[\gamma]$ is finitely generated as an additive group.

$\implies \gamma$ is an algebraic integer. □

E.g. Let $k = \mathbb{Q}(\sqrt{5}) = \{x+y\sqrt{5} : x,y \in \mathbb{Q}\}$. What is $\mathcal{O}_k$?

Let $A = x+y\sqrt{5}$, with $x,y\in\mathbb{Q}$, $y\neq 0$.
Assume $A \in \mathcal{O}_k$, $k=\mathbb{Q}(A)$ and $m_A(x)$ has degree 2.

$(A-x)^2 - 5y^2 = 0$

$A^2 - 2xA - 5y^2 + x^2 = 0$

So $m_A(x) = X^2 - 2xX + x^2 - 5y^2$

$$\begin{aligned} A\in\mathcal{O}_k &\iff m_A(x)\in\mathbb{Z}[x] \\ &\iff 2x\in\mathbb{Z},\ \text{and } x^2-5y^2\in\mathbb{Z}\end{aligned}$$

This means the denominator of x is at most 2.

$$x = \frac{r}{2} \quad r\in\mathbb{Z} \text{ since } x^2-5y^2\in\mathbb{Z}$$

$$y = \frac{s}{2} \quad s\in\mathbb{Z}$$

$$\begin{aligned}\frac{r^2-5s^2}{4}\in\mathbb{Z} \implies r^2-5s^2 &\equiv 0 \ \ (4) \\ r^2 &\equiv s^2 \ \ (2) \\ r &\equiv s \ \ (2) \\ r &= s+2t \ \ t\in\mathbb{Z}\end{aligned}$$

$$\begin{aligned} A &= \frac{r}{2} + \frac{s}{2}\sqrt{5} \\ &= \frac{s}{2} + t + \frac{s}{2}\sqrt{5} \\ &= t + s\left(\frac{1+\sqrt{5}}{2}\right)\end{aligned}$$

So every algebraic integer in k is actually in $\mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{5}}{2}$.
Conversely since $\alpha\in\mathcal{O}_k$ we know $\mathbb{Z}[\alpha]\subseteq\mathcal{O}_k$. $\mathcal{O}_k = \mathbb{Z}[\alpha] = \{t+s\alpha : t,s\in\mathbb{Z}\}$.

What is so special about the rings $\mathcal{O}_k$? Why not just study $\mathbb{Z}[\sqrt{5}]$ instead of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$?

Proposition 3.7. *Suppose $R \subseteq k$ is a UFD subring of k. If $A = \frac{\alpha}{\beta}$ is an algebraic integer in k with $\alpha, \beta \in R$ then $A \in R$.*

This implies $\mathbb{Z}[\sqrt{5}]$ is not a UFD (take $A = \frac{1+\sqrt{5}}{2}$).

Proof. Let $A = \frac{\alpha}{\beta}$ be an algebraic integer. Without loss of generality assume, $\alpha, \beta \in R$ are coprime.

To prove $A \in R$ we'll show that β is a unit.

Suppose $p|\beta$, $p \in R$ is irreducible.

$A \in \mathcal{O}_k$ so $A^d + \alpha_{d-1}A^{d-1} + \ldots a_0 = 0 \quad a_i \in \mathbb{Z}$

$$\frac{\alpha^d}{\beta^d} + a_{d-1}\frac{\alpha^{d-1}}{\beta^{d-1}} + \cdots + a_0 = 0$$

Multiply by β^d:

$$\alpha^d + \underbrace{a_{d-1}\alpha^{d-1}\beta + \cdots + a_0\beta^d}_{\text{multiples of } p} = 0$$

So $p|\alpha^d$ and $p|\alpha$ since R is a UFD and p is irreducible.

p is a common factor of α and β. $\lightning \beta$ has no irreducible factors so β is a unit.

□

3.1 The Standard Represenation

Definition 3.8. *The map $\beta \mapsto A_\beta$ is called the standard representation.*

Let $k/\mathbb{Q}$ be an algebraic number field.

$d = [k : \mathbb{Q}]$ for some $\alpha \in k$

$k = \mathbb{Q}(\alpha)$

$m = m_\alpha$ minimal polynomial of α

$\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ the (distinct) complex roots of m_α, i.e. conjugates of α in $\mathbb{C}$.

For each α_i we have a field embedding:

$$\begin{aligned}
&\sigma_i : k \longrightarrow \mathbb{C} \\
&\sigma_i(a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}) = a_0 + a_1\alpha_i + \cdots + a_{d-1}\alpha_i^{d-1} \\
&\sigma_i(f(\alpha)) = f(a_i) \quad f \in \mathbb{Q}[x]
\end{aligned}$$

For an element $\beta \in k$, let A_β be the linear map $k \to k$, $A_\beta(x) = \beta x$. After choosing a basis for $k/\mathbb{Q}$, A_β is a d×d matrix of rational numbers.

E.g. $k = \mathbb{Q}(\sqrt{2})$, $\beta = 3 + 2\sqrt{2}$

We find the matrix of A_β with respect to the basis $\{1, \sqrt{2}\}$.

$$A_\beta(1) = (3 + 2\sqrt{2}) * 1 = 3 \cdot 1 + 2\sqrt{2}$$
$$A_\beta(\sqrt{2}) = (3 + 2\sqrt{2}) * 1 = 4 \cdot 1 + 3\sqrt{2} \qquad A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

Remark : We can recover β from A_β by $\beta = A_\beta(1)$ and the map $\beta \mapsto A_\beta$ is injective.

3.1.1 Properties of the Standard Representation

- $A_{\beta+\gamma} = A_\beta + A_\gamma \quad (\gamma, \beta \in k \;\; x \in \mathbb{Q})$
- $A_{\beta\gamma} = A_\beta \cdot A_\gamma$
- $A_{x\beta} = xA_\beta$

Proof.

$$\begin{aligned} A_{\beta\gamma}(t) &= \beta\gamma t \\ &= A_\beta(\gamma t) \\ &= A_\beta(A_\gamma(t)) \qquad \text{so } A_{\beta\gamma} = A_\beta \circ A_\gamma \end{aligned}$$

Other proofs are similar. □

Corollary 3.9. *If $g \in \mathbb{Q}[x] \quad A_{g(\beta)} = g(A_\beta)$. The polynomial = the linear map*

Proof. Let $g(x) = a_0 + a_1 x + \cdots + a_n x^n \quad a_i \in \mathbb{Q}$. Then:

$$\begin{aligned} A_{g(\beta)} &= A_{a_0 + a_1\beta + \cdots + a_n\beta^n} \\ &= A_{a_0} + A_{a_1\beta} + \cdots + A_{a_n\beta^n} \\ &= a_0 A_1 + a_1 A_\beta + \cdots + a_n A_{B^n} \\ &= a_0 A_1 + a_1 A_\beta + 1_2 (A_\beta)^2 + \cdots + a_n (A_\beta)^n \\ &= g(A_\beta) \end{aligned}$$

□

Definition 3.10. *Let $\beta \in k$ be the field polynomial $F_\beta(x)$ is $F_\beta(x) = \det(xI - A_\beta)$ i.e. the characteristic polynomial of β.*

F_β is the monic polynomial of degree d in $\mathbb{Q}[x]$.

Lemma 3.11. *If $k = \mathbb{Q}(\alpha)$ then $F_\alpha(x) = m_\alpha(x)$.*

Proof. By the Cayley-Hamilton ($Ch_A(A) = 0$): $F_\alpha(A_\alpha) = A_{F_\alpha(\alpha)} = \underline{0}$. So $F_\alpha(\alpha) = 0$ and F_α is a multiple of m_α. Since it has degree d and is monic, $F_\alpha = m_\alpha$. □

Theorem 3.12. *For any $\beta \in k$, the matrix A_β is diagonalisable over $\mathbb{C}$ with diagonal entries $\sigma_1(\beta), \dots, \sigma_d(\beta)$ and $F_\beta(x) = \big(x - \sigma_1(\beta)\big) \dots \big(x - \sigma_d)\big)$*

Proof. First prove in the case $\beta = \alpha$, $k = \mathbb{Q}(\alpha)$).

The eigenvalues of A_α are the roots of $F_\alpha = m_\alpha$ (by the lemma)

These are $\alpha_1, \dots, \alpha_d$. By the Galois Separability lemma, we have d eigenvalues.

$\therefore A_\alpha$ is diagonalisable over $\mathbb{C}$ and $P^{-1}A_\alpha P = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_d \end{pmatrix}$

Now check for any $\beta \in k \quad \beta = g(\alpha)$ for some $g \in \mathbb{Q}[x]$

$$\begin{aligned} A_\beta = A_g(\alpha) &= g(A_\alpha)a \\ &= g\left(P \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_d \end{pmatrix} P^{-1}\right) \\ &= Pg\left(\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_d \end{pmatrix}\right)P^{-1} \\ &= P\begin{pmatrix} g(\alpha_1) & & \\ & \ddots & \\ & & g(\alpha_d) \end{pmatrix}P^{-1} \\ &= P\begin{pmatrix} \sigma_1(\beta) & & \\ & \ddots & \\ & & \sigma_d(\beta) \end{pmatrix}P^{-1} \end{aligned}$$

□

E.g. $k = \mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} : x, y \in \mathbb{Q}\} \quad d = 2.$

Use the basis $\{1, \sqrt{2}\}$

$$A_{\sqrt{2}}(1) = \sqrt{2} \cdot 1 = 0 \cdot 1 + 1 \cdot \sqrt{2}$$

$$A_{\sqrt{2}}(\sqrt{2}) = 2 \cdot 1 + 0 \cdot \sqrt{2} \qquad A_{\sqrt{2}} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Let $P = \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & 1 \end{pmatrix}$ and $P^{-1}A_{\sqrt{2}}P = \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$

Let $\beta = x + y\sqrt{2} \quad A_\beta = xI_2 + y \quad A_{\sqrt{2}} \begin{pmatrix} x & 2y \\ y & x \end{pmatrix}$

$$P^{-1}A_\beta P = \begin{pmatrix} x+y\sqrt{2} & 0 \\ 0 & x-y\sqrt{2} \end{pmatrix} = \begin{pmatrix} \sigma_1(\beta) & \\ & \sigma_2(\beta) \end{pmatrix}$$
$$F_\beta(x) = \big(x-\sigma_1(\beta)\big)\big(x-\sigma_2(\beta)\big)$$

Corollary 3.13. *For any $\beta \in k$, $[k : \mathbb{Q}(\beta)]$*

Proof. Suppose $p(x)$ is a monic irreducible factor of F_β in $\mathbb{Q}[x]$. Want to show $p = m_\beta$.

The roots of F_β are $\sigma_1(\beta), \dots, \sigma_d(\beta)$. These are the conjugates of β, i.e. the roots of m_β.

Therefore the roots of p have minimal polynomial m_β.

$m_\beta | p$ so $p = m_\beta$ and since F_β and m_β are both monic, $F_\beta = m_\beta^r$ for some $r \in \mathbb{Z}$. Also m_β has degree $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

So by the Tower law, $r = [k : \mathbb{Q}(\beta)]$. □

Corollary 3.14. $\beta \in \mathcal{O}_k \iff F_\beta(x) \in \mathbb{Z}[x]$

Proof. ($\implies$)

Suppose $\beta \in \mathcal{O}_k$, $m_\beta \in \mathbb{Z}[x]$ but F_β is a power of $m_\beta \implies F_\beta \in \mathbb{Z}[x]$

($\impliedby$) Assume $F_\beta \in \mathbb{Z}[x]$ $\quad F_\beta(\beta) = m_\beta(\beta)^{[k:\mathbb{Q}(\beta)]} = 0^Y = 0$ for some y. Therefore $\beta \in \mathcal{O}_k$. □

E.g. $k = \mathbb{Q}(i) \quad \beta = \frac{3}{2} + \frac{5}{7}i$

$$\begin{aligned} F_\beta(x) &= \big(x-\sigma_1(\beta)\big)\big(x-\sigma_2(\beta)\big) \\ &= \left(x - \frac{3}{2} - \frac{5}{7}i\right)\left(x - \frac{3}{2} + \frac{5}{7}i\right) \\ &= \left(x - \frac{3}{2}\right)^2 + \frac{25}{49} \notin \mathbb{Z}[x] \qquad \text{so } \beta \notin \mathcal{O}_k \end{aligned}$$

Corollary 3.15. *Let $b \in k$ then $n \in \mathbb{Z}$ $(n > 0)$ such that $n\beta \in \mathcal{O}_k$.*

Proof. Choose n so that $nA_\beta = A_{n\beta}$ has entries in $\mathbb{Z}$. Then $F_{n\beta} \in \mathbb{Z}[x]$ and so by the previous corollary $n\beta \in \mathcal{O}_k$. □

E.g. $k = \mathbb{Q}(\alpha)$, $\alpha = 10^{\frac{1}{3}}$, $\quad \alpha \in \mathcal{O}_k$ so $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_k$.

$\mathbb{Z}[\alpha] = \{x + y\alpha + z\alpha^2 \ : x, y, z \in \mathbb{Z}\}$

Let $\beta = \frac{1+\alpha+\alpha^2}{3}$ then $A_\beta = \frac{1}{3}\begin{pmatrix} 1 & 10 & 10 \\ 1 & 1 & 10 \\ 1 & 1 & 1 \end{pmatrix}$ Is β an algebraic integer?

$F_\beta(x) = \det(xI_3 - A_\beta)$

First calculate the standard representation:

$$\begin{aligned}A_\alpha(1) &= \alpha = 0\cdot 1 + 1\cdot\alpha + 0\cdot\alpha^2\\ A_\alpha(\alpha) &= \alpha^2 = 0\cdot 1 + 0\cdot\alpha + 1\cdot\alpha^2\\ A_\alpha(\alpha^2) &= 10 = 10\cdot 1 + 0\cdot\alpha + 0\cdot\alpha^2\end{aligned}$$

$$A_\alpha = \begin{pmatrix} 0 & 0 & 10\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} \; A_\alpha^2 = \begin{pmatrix} 0 & 0 & 10\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}^2 = \begin{pmatrix} 0 & 10 & 0\\ 0 & 0 & 10\\ 1 & 0 & 0\end{pmatrix}$$

$$A_\beta = \tfrac{1}{3}\left(I_3 + \begin{pmatrix} 0 & 0 & 10\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} + \begin{pmatrix} 0 & 10 & 0\\ 0 & 0 & 10\\ 1 & 0 & 0\end{pmatrix} \right) = \tfrac{1}{3}\begin{pmatrix} 1 & 10 & 10\\ 1 & 1 & 10\\ 1 & 1 & 1\end{pmatrix}$$

$$\begin{aligned}F_\beta &= \det(xI_3 - A_\beta)\\ &= \det\left(\frac{1}{3}\begin{pmatrix} 3x-1 & -10 & -10\\ -1 & 3x-1 & -10\\ -1 & -1 & 3x-1\end{pmatrix}\right)\\ &= \frac{1}{27}\Big(\big((3x-1)^3 - 100 - 10\big) - \big(3(10(3x-1))\big)\Big)\\ &= \frac{1}{27}\big(27x^3 - 27x^2 - 81x - 81\big)\end{aligned}$$

$F_\beta(x) = x^3 - x^2 - 3x - 3 \in \mathbb{Z}[x] \quad \beta \in \mathcal{O}_k$

$\mathbb{Z}[\alpha]]$ is not a UFD.

3.2 Norms and Traces

Definition 3.16. *For an element $\beta \in k$ we define $N(\beta) = \det(A_\beta)$ to be the norm of β and $Tr(\beta) = Tr(A_\beta)$ to be the trace of β.*

Note that $N(\beta)$ and $Tr(\beta) \in \mathbb{Q}$.

E.g. $Tr(\begin{pmatrix} 3 & 7 & 3\\ 4 & 7 & 6\\ 1 & 2 & 3\end{pmatrix} = 3 + 7 + 3$

Proposition 3.17. $N(\beta) = \sigma_1(\beta) \times \cdots \times \sigma_d(\beta)$
$Tr(\beta) = \sigma_1(\beta) + \cdots + \sigma_d(\beta)$

Proof. $A_\beta \sim \begin{pmatrix} \sigma_1(\beta) & & 0\\ & \ddots & \\ 0 & & \sigma_d(\beta)\end{pmatrix}$ □

3.3 Properties of Norms and Traces

- $N(\beta\gamma) = N(\beta)N(\gamma)$ for $\beta, \gamma \in k$
- $N(x\beta) = x^d N(\beta)$ for $x \in \mathbb{Q}$
- $Tr(\beta + \gamma) = Tr(\beta) + Tr(\gamma)$
- $Tr(x\beta) = xTr(\beta)$

Proof. $N(\beta\gamma) = \det(A_{\beta\gamma}) = \det(A_\beta A_\gamma) = N(\beta)N(\gamma)$ □

Proposition 3.18. $F_\beta(x) = x^d - Tr(\beta)x^{d-1} + \cdots + (-1)^d N(\beta)$

Proof.

$$\begin{aligned} F_\beta(x) &= \big(x - \sigma_1(\beta)\big) \times \cdots \times \big(x - \sigma_d(x)\big) \\ &= x^d - \big(\sigma_1(\beta) + \cdots + \sigma_d(\beta)\big)x^{d-1} + \cdots + (-1)^d\big(\sigma_1(\beta) \times \cdots \times \sigma_d(\beta)\big) \\ &= x^d - Tr(\beta)x^{d-1} + \cdots + (-1^d)N(\beta) \end{aligned}$$

□

E.g. $\alpha = 10^{\frac{1}{3}}$, $\beta = \frac{1+\alpha+\alpha^2}{3}$

$N(\beta) = 3$, $Tr(\beta) = 1$ and $F_\beta(\alpha) = x^3 - x^2 - 3x - 3$

Corollary 3.19. *If $\beta \in \mathcal{O}_k$ then $N(\beta), Tr(\beta) \in \mathbb{Z}$.*

Proof. $F_\beta \in \mathbb{Z}[x]$ □

E.g. $k = \mathbb{Q}(i)$, $\beta = \frac{1+i}{2}$

$N(\beta) = \frac{1+i}{2} * \frac{1-i}{2} = \frac{1+1}{4} = \frac{1}{2} \notin \mathbb{Z}$

$\beta \in \mathcal{O}_k$

3.4 Integral Bases

E.g. $\alpha = 10^{\frac{1}{3}}$, $k = \mathbb{Q}(\alpha)$ $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_k$

We also found another element $\beta \in \mathcal{O}_k$, $\beta = \frac{1+\alpha+\alpha^2}{3}$ for $\mathbb{Z}[\alpha, \beta] \in \mathcal{O}_k$.

Is this all of $\mathcal{O}_k$ or are there more?

Eventually this process will end with the whole of $\mathcal{O}_k$ which will be proved later.

Definition 3.20. *Suppose $\mathcal{B} = \{b_1, \dots, b_n\}$ is a basis for k as a vector space over $\mathbb{Q}$. We call β an integral basis if:*

$$\mathcal{O}_k = Span_{\mathbb{Z}}(\beta = \{x_1 b_1 + \cdots + x_d b_d : x_i \in \mathbb{Z}\})$$

Theorem 3.21. *There exists an integral basis in k and a method for finding it.*

Proof. (Sketch)
Start with any basis $\{b_1, \dots, b_d\}$.

After multiplying b_i by integer, we can assume $b_i \in \mathcal{O}_k$, $Span_{\mathbb{Z}}\{b_i\} \subset \mathbb{Q}$

If $Span_{\mathbb{Z}}\{\mathcal{B}\} \neq \mathcal{O}_k$ then we can find an element $\mathcal{O} \in \mathcal{O}_k$ with $\mathcal{O} \notin Span_{\mathbb{Z}}\beta$.

Replace some b_i by $\mathcal{O}$ to get a new basis $\mathcal{C}$ and this new basis is "smaller" than $\mathcal{B}$ but we need to explain what smaller means. □

E.g. $\mathbb{Q}(i)$ $\quad \mathcal{B} = \{1, i\}$ is an integral basis because $\mathcal{O}_k = \mathbb{Z}[i]$.

If $\mathcal{B}$ is any basis then we define $\Delta(\mathcal{B}) = \det(Tr(b_i b_j)) \in \mathbb{Q}$. If $\mathcal{B} \subseteq \mathcal{O}_k$ then $\Delta\mathcal{B} \in \mathbb{Z}$.

The symmetric matrix $\big(Tr(b_i b_j)\big)$ is the matrix of a symmetric bilinear form $k \times k \to \mathbb{Q}$.

$(A, B) \mapsto Tr(AB) \qquad A, B \in k$

$Tr\big((A + xC)B\big) = Tr(AB + xCB) = Tr(AB) + xTr(CB) \qquad x \in \mathbb{Q}$

Corollary 3.22. $\Delta\mathcal{B} \neq 0$ *if $\mathcal{B}$ is any basis*

Proof. Suppose $\Delta\mathcal{B} = 0$, so 0 is an eigenvalue of the matrix of the bilinear form.
There exists $A \in k \quad (A \neq 0)$ such that $Tr(AB) = 0 \quad \forall B \in k$.
Let $B = \frac{1}{A}$, thus $Tr(1) = 0$ and $d = 0$ ↯. □

Corollary 3.23. *Suppose $\mathcal{B} = \{b_i\}$ $\mathcal{C} = \{c_i\}$ are two bases. Let $M = (m_{ij})$ be the transition matrix i.e. $c_i = \sum_j m_{ij} b_j$ then $\Delta\mathcal{C} = \big(\det(M))\big)^2 \Delta\mathcal{B}$.*

Proof. Recall from Algebra 3, $Tr(c_i c_j) = M^T Tr(b_i b_j) M$.

Take the determinant $\Delta\mathcal{C} = \det(M) \Delta\mathcal{B} \det(M)$.

□

Lemma 3.24. *Let $\mathcal{B} = \{b_1, \dots, b_d\}$ be a basis for $k/\mathbb{Q}$ with $\mathcal{B} \subset \mathcal{O}_k$.*
Assume $\mathcal{B}$ is not an integral basis. Then there is a prime number p with $p|\Delta\mathcal{B}$ and an element:

$$\theta = \frac{x_1 b_1 + \cdots + x_d b_d}{p} \qquad\qquad x_i \in \{0, \dots, p-1\} \textit{ not all 0}$$

such that θ is an algebraic integer.

If $x_i \neq 0$ then we can replace b_i by θ to get a new basis $\mathcal{C}$ and $\Delta(\mathcal{C}) = \left(\dfrac{x^i}{p}\right)^2 \Delta\mathcal{B}$

Theorem 3.25. *There is an integral basis in k*

Proof. Choose a basis $\mathcal{B} \subseteq \mathcal{O}_k$ with $|\Delta\mathcal{B}|$ as small as possible.

Claim $\mathcal{B}$ is an integral, suppose not. By the lemma there is a basis $\mathcal{C} \subseteq \mathcal{O}_k$ such that $\Delta\mathcal{C} = \left(\frac{x^i}{p}\right)^2 \Delta\mathcal{B}$ for $|x_i| < p$.

$|\Delta\mathcal{C}| < |\Delta\mathcal{B}|$ ↯

□

The lemma also give a method for finding an integral basis.

1. Start off with any basis for $k/\mathbb{Q}$
   For example if $k = \mathbb{Q}(\alpha)$ we can take $\{1, \alpha, \ldots, \alpha^{d-1}\}$
2. Multiplying the basis vectors by non-zero integers we can assume $\{b_1, \ldots, b_d\} \subseteq \mathcal{O}_k$
3. Calculate $\Delta\{b_1, \ldots, b_d\}$
   For each element $\theta = \dfrac{x_1 b_1 + \ldots, + x_d b_d}{p}$ where $x_i \in \{0, \ldots, p-1\}$ not all 0, p prime and $p|\Delta\mathcal{B}$
   - If θ is an algebraic integer then replace some b_i by θ to get a new basis and go back to 3).
   - If none of the θ are algebraic integers then $\mathcal{B}$ is an integral basis.

E.g. $k = \mathbb{Q}(\sqrt{5})$ Start with basis $\{1, \sqrt{5}\}$

$$\begin{aligned}\Delta\{1, \sqrt{5}\} &= \det\begin{pmatrix} Tr(1 * 1) & Tr(1 * \sqrt{5}) \\ Tr(\sqrt{5} * 1) & Tr(\sqrt{5}\sqrt{5}) \end{pmatrix} \\ &= \det\begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix} \\ &= 20 \\ &= 2^2 * 5\end{aligned}$$

The only prime whose square divides this is $p = 2$.

So $\theta = x + y\sqrt{5} \quad x, y \in \{0, 1\}$ not both 0.

The following combinations are possible, $\frac{1}{2}$, $\frac{\sqrt{5}}{2}$ and $\frac{1+\sqrt{5}}{2}$. Trivially $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_k$.

So the new basis $\mathcal{C} = \{1, \frac{1+\sqrt{5}}{2}\}$ and $\Delta(\mathcal{C}) = \frac{1}{2}^2 \Delta\mathcal{B} = 5$

There are no primes p such that $p^2|\mathcal{B}$. This means there are no more θ to check $\implies \mathcal{C}$ is an integral basis.

$\mathcal{O}_k = \{x + y\alpha : x, y \in \mathbb{Z}\} \quad \alpha = \frac{1+\sqrt{5}}{2}$.

$Tr(x + y\sqrt{5}) = 2x$

Proof. Lemma 3.2.4

Assume $\mathcal{B}$ is not an integral basis, then there exists an algebraic integer $\Phi = y_1 b_1 + \cdots + y_d b_d$ $y_i \in \mathbb{Q}$, y_i not all in $\mathbb{Z}$.

Let N be the lowest common denominator of $y_1, \ldots, y_d$. Replace Φ by $\frac{N}{p}\Phi$ where p is prime.

The denominators are the prime p factor of N.

Let $\Psi = \lfloor y_1 \rfloor b_1 + \cdots + \lfloor y_d \rfloor b_d \in \mathcal{O}_k$.

$\theta = \Phi - \Psi \in \mathcal{O}_k$

The coefficients of θ are in $[0, 1)$, not all 0 and with denominator p.

$$\theta = \frac{x_1 b_1 + \cdots + x_d b_d}{p} \qquad\qquad x_i \in \{0, \ldots, p-1\}$$

Suppose $x_i \neq 0$, let $\mathcal{C}$ be the new basis with b_i replaced by θ.
The new transition matrix is:

$$\begin{aligned} c_1 &= b_1 \\ c_2 &= b_2 \\ &\vdots \\ c_i &= \frac{x_i}{p} b_i + \cdots + \frac{x_d}{p} b_d \\ &\vdots \\ c_d &= b_d \end{aligned}$$

$$M = \begin{pmatrix} 1 & & & \frac{x_1}{p} & & \\ & 1 & & & & \\ & & \ddots & \vdots & & \\ & & & \frac{x_i}{p} & & \\ & & & \vdots & \ddots & \\ & & & \frac{x_d}{p} & & 1 \end{pmatrix} \text{(0s elsewhere)}$$

So $\Delta\mathcal{C} = \det(M)^2 \Delta\mathcal{B} = (\frac{x^i}{p})^2 \Delta\mathcal{B}$

$$p^2 \Delta\mathcal{C} = x_i^2 \Delta\mathcal{B} \qquad\qquad x_i \in \{1, \ldots, p-1\},\ x_i \text{ coprime to } p^2 \text{ and } p^2 | \Delta\mathcal{B}$$

□

We found an integral basis, 1, $\frac{1+\sqrt{5}}{2}$ in $\mathbb{Q}(\sqrt{5})$.

We'll see methods which will find an integral basis in $\mathbb{Q}(\alpha)$.

E.g. $\alpha^8 - 2 = 0$, we need better methods for calculating discriminants.

Lemma 3.26. *If $\{b_1, \ldots, b_d\}$ is any basis then $\Delta\{b_1, \ldots, b_d\} = \det \begin{pmatrix} \sigma_1(b_1) & \ldots & \sigma_d(b_1) \\ \vdots & & \vdots \\ \sigma_1(b_d) & \ldots & \sigma_d(b_d) \end{pmatrix}^2$*

Here $\sigma_1, \ldots, \sigma_d : k \mapsto \mathbb{C}$ are field embeddings.

E.g. $k = \mathbb{Q}(\sqrt{n})$ n not a square

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

If n is square free then the only primes to consider in the algorithm is $p = 2$. So we'd consider the elements $\frac{1}{2}, \frac{\sqrt{n}}{2}, \frac{1+\sqrt{n}}{2}$.

Proof.

$$\begin{pmatrix} \sigma_1(b_1) & \ldots & \sigma_d(b_1) \\ \vdots & & \vdots \\ \sigma_1(b_d) & \ldots & \sigma_d(b_d) \end{pmatrix} \begin{pmatrix} \sigma_1(b_1) & \ldots & \sigma_d(b_1) \\ \vdots & & \vdots \\ \sigma_1(b_d) & \ldots & \sigma_d(b_d) \end{pmatrix}$$

$$= \begin{pmatrix} \sigma_1(b_1 b_1) + \sigma_2(b_1 b_1) + \ldots \sigma_d(b_1 b_1) & \ldots & \sigma_d(b_1 b_d) + \cdots + \sigma_d(b_1 b_d) \\ \vdots & & \vdots \\ \sigma_1(b_d b_1) + \cdots + \sigma_d(b_d b_1) & \ldots & \sigma_d(b_d b_d) + \cdots + \sigma(b_d b_d) \end{pmatrix}$$

$$= \begin{pmatrix} Tr(b_1 b_1) & \ldots & Tr(b_1 b_d) \\ \vdots & \ddots & \vdots \\ Tr(b_d b_1) & \ldots & Tr(b_d b_d) \end{pmatrix}$$

Take determinant of both sides $\det(\sigma_i(b_j))^2 = \Delta\mathcal{B}$ □

Next we'll look at $\Delta\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$, $k = \mathbb{Q}(\alpha)$

Proposition 3.27. *Let $\alpha_1, \ldots, \alpha_d$ be the conjugate of α in $\mathbb{C}$. Then $\Delta\{1, \ldots, \alpha^{d-1}\} = \prod_{i,j=1\ i<j}^{d} (\alpha_i - \alpha_j)^2$*

Proof. By the previous lemma

$$\Delta = \det \begin{pmatrix} \sigma_1(1) & \dots & \sigma_1(\alpha^{d-1}) \\ \vdots & \ddots & \vdots \\ \sigma_d(1) & \dots & \sigma_d(\alpha^{d-1}) \end{pmatrix}^2 \qquad\qquad \sigma_i(\alpha) = \alpha_i$$

$$= \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{d-1} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \dots & \alpha_d^{d-1} \end{pmatrix}$$

$$= \left(\pm \prod_{i,j=1\ i<j}^{d} (\alpha_i - \alpha_j) \right)^2$$

□

Proposition 3.28. $\Delta\{1, \alpha, \dots, \alpha^{d-1}\} = (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha))$ *where m is the minimal polynomial of α, $m'(x)$ is the derivative.*

E.g. Let $k = \mathbb{Q}(\alpha)$ where $\alpha^8 - 2 = 0$

$m_\alpha(x) = x^8 - 2$ (Eisenstein's criterion with $p = 2$)

$m'_\alpha(x) = 8x^7$

By the proposition:

$$\begin{aligned} \Delta\{1, \alpha, \dots, \alpha^7\} &= (-1)^{\frac{8*7}{2}} N(8\alpha^7) \\ &= (-1)^{\frac{8*7}{2}} N(8) N(\alpha)^7 \\ &= 1 * 8^8 * -2^7 \\ &= -2^{31} \end{aligned}$$

$$N(\beta) = \det(A_\beta) = \begin{pmatrix} 8 & & & \\ & 8 & & \\ & & \ddots & \\ & & & 8 \end{pmatrix} \text{(0}s\text{ elsewhere)}$$

$$\begin{aligned} N(\alpha) &= \alpha_1 \dots \alpha_8 \\ &= \text{constant term in } m_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_8) \\ &= -2 \end{aligned}$$

Proof. From the previous proposition:

$$\begin{aligned}\Delta &= \prod_{i,j=1\ i<j}^{d} (\alpha_i - \alpha_j)^2 \\ &= \prod_{i,j=1\ i<j}^{d} (\alpha_i - \alpha_j) * (\alpha_j - \alpha_i) * -1 && \#\text{ of terms } = \frac{d(d-1)}{2} \\ &= (-1)^{\frac{d(d-1)}{2}} \prod_{i,j=1\ i\neq j}^{d} (\alpha_i - \alpha_j)\end{aligned}$$

$$m(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_d).$$

$$\begin{aligned}m'(x) &= (x-\alpha_2)\dots(x-\alpha_d) + (x-\alpha_1)(x-\alpha_3)\dots(x-\alpha_d) + \dots + (x-\alpha_1)(x-\alpha_{d-1}) \\ &= \sum_{i=1}^{d} \prod_{j\neq i}(x-\alpha_j)\end{aligned}$$

$$m'(a_k) = \sum_{i=1}^{d} \underbrace{\prod_{j\neq i}(\alpha_k - \alpha_j)}_{=0 \text{ unless } i=k}$$

$$\begin{aligned}N(m'(\alpha)) &= \prod_i \sigma_i(m'(\alpha)) \\ &= \prod_i m'(\alpha_i) \\ &= \prod_i \prod_{j\neq i}(\alpha_i - \alpha_j)\end{aligned}$$

Therefore $\Delta = (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha))$. □

Note: $F(x) = \Big(x - \sigma_1(\theta)\Big)\dots\Big(x-\sigma_d(\theta)\Big) = x^d - Tr(\theta)x^{d-1} + \dots + (-1)^d N(\theta)$

3.5 Quadratic Fields

$k = \mathbb{Q}(\sqrt{n})$ for $n \neq 1$ and square-free.

Theorem 3.29. *$\mathcal{O}_k = \mathbb{Z}[\alpha]$ where $\alpha \begin{cases} \sqrt{n} & d \not\equiv 1 \ \ (4) \\ \frac{1+\sqrt{n}}{2} & d \equiv 1 \ \ (4) \end{cases}$, and $\{1, \alpha\}$ is an integral basis, then*

$$\Delta\{1,\alpha\} = \begin{cases} 4n & n \not\equiv 1 \ \ (4) \\ n & n \equiv 1 \ \ (4) \end{cases}$$

Proof. Suppose $n \not\equiv 1 \pmod 4$ and let $\mathcal{B} = \{1, \sqrt{n}\}$

$$\begin{aligned}\Delta\mathcal{B} &= \det\begin{pmatrix}\sigma_1(1) & \sigma_1(\sqrt{n}) \\ \sigma_2(1) & \sigma_2(\sqrt{n})\end{pmatrix}^2 \\ \\ &= \det\begin{pmatrix}1 & \sqrt{n} \\ 1 & -\sqrt{n}\end{pmatrix} \\ &= 4n\end{aligned}$$

In the algorithm we get $p = 2$, the only prime whose square divides 4n.

$\theta = \frac{1}{2}, \frac{\sqrt{n}}{2}$ or $\frac{1+\sqrt{n}}{2}$

We know $\frac{1}{2} \notin \mathcal{O}_k$ and $N(\frac{\sqrt{n}}{2}) = -\frac{n}{4} \notin \mathbb{Z}$ because n is square free so $\frac{\sqrt{n}}{2} \notin \mathcal{O}_k$.

Also $N(\frac{1+\sqrt{n}}{2}) = \frac{1}{4}^{-n} \notin \mathbb{Z}$ so $\frac{1+\sqrt{n}}{2} \notin \mathcal{O}_k$ so $\{1, \sqrt{n}\}$ is an integral basis.

Suppose $n \equiv 1 \pmod 4$ so $\frac{1+\sqrt{n}}{2} \in \mathcal{O}_k$. Then $\mathcal{B} = \{1, \frac{1+\sqrt{n}}{2}\}$ and $\Delta\mathcal{B} = \det\begin{pmatrix}1 & \frac{1+\sqrt{n}}{2} \\ 1 & \frac{1-\sqrt{n}}{2}\end{pmatrix} = n$

Since n is square free $\mathcal{B}$ is an integral basis, there are not primes whose square divides $\Delta\mathcal{B}$.

□

3.6 Cubic Fields

Suppose k is a cubic field, i.e. $[k : \mathbb{Q}] = 3$. Let $k = \mathbb{Q}(\alpha)$ with $m_\alpha(x) = x^3 + cx^2 + \dots$

If we let $\beta = \alpha + \frac{c}{3}$ so $k = \mathbb{Q}(\beta)$, the minimal polynomial of β has no x^2 term

$$\begin{aligned}m_\beta(x) &= m_\alpha(x - \frac{c}{3}) \\ &= (x - \frac{c}{3}^3 + c(x - \frac{c}{3})^2 + \dots \\ &= x^3 - cx^2 + \dots + cx^2 + \dots\end{aligned}$$

Let's assume that the minimal polynomial of α is $x^3 + ax + b$.

Proposition 3.30. $\Delta\{1, \alpha, \alpha^2\} = -27b^2 - 4a^3$

We can use this to find an integral basis in k.

E.g. $m_\alpha(x) = x^3 + x + 1$

$m(1) \neq 0$ and $m(-1) \neq 0$ so m_α is irreducible.

$k = \mathbb{Q}(\alpha)$ is a cubic field, $\Delta\{1, \alpha, \alpha^2\} = -27 - 4 = -31$.

This is square free so $\{1, \alpha, \alpha^2\}$ is an integral basis i.e. $\mathcal{O}_k = \mathbb{Z}[\alpha]$.

E.g. $m_\alpha(x) = x^3 - 2x + 3$.

It is irreducible since plugging in $\pm 1, \pm 3$ does not give 0.

By the proposition $\Delta\{1,\alpha,\alpha^2\} = -27b^2 - 4a^3 = -243 + 32 = -211$.

211 prime so $\{1,\alpha,\alpha^2\}$ is an integral basis i.e. $\mathcal{O}_k = \mathbb{Z}[\alpha]$.

Proof.

$m_\alpha(x^3) = x^3 + ax + b$ and we proved last time that $\Delta\{1,\alpha,\ldots,\alpha^{d-1}\} = (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha))$.

$m'(x) = 3x^2 + a$

$\Delta\{1,\alpha,\alpha^2\} = -N(3\alpha^2 + a)$

Let $\alpha,\beta,\gamma \in \mathbb{C}$ be the conjugates of α, $m(x) = (x-\alpha)(x-\beta)(x-\gamma)$.

By comparing coefficients:

- $\alpha + \beta + \gamma = 0$
- $\alpha\beta + \beta\gamma + \gamma\alpha = a$
- $\alpha\beta\gamma = -b$

$$\begin{aligned}\Delta\{1,\alpha,\alpha^2\} &= -N(3\alpha^2 + a)\\ &= -(3\alpha^2+a)(3\beta^2+a)(3\gamma^2+a)\\ &= -(27\alpha^2\beta^2\gamma^2 + 9a(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) + 3a^2(\alpha^2+\beta^2+\gamma^2) + a^3)\end{aligned}$$

Using

$$\begin{aligned}\alpha^2\beta^2\gamma^2 &= b^2\\ \alpha^2+\beta^2+\gamma^2 &= \underbrace{\alpha+\beta+\gamma}_{0} - \underbrace{2(\alpha\beta+\beta\gamma+\gamma\alpha)}_{a} = -2a\\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= (\alpha\beta+\beta\gamma+\gamma\alpha)^2 - 2(\alpha\beta\beta\gamma + \beta\gamma\gamma\alpha + \gamma\alpha\alpha\beta))\\ &= a^2 - 2\alpha\beta\gamma(\alpha+\beta+\gamma)\end{aligned}$$

$\Delta\{1,\alpha,\alpha^2\} = -27b^2 + 9aa^2 + 3a^2(-2a) + a^3 = -27b^2 - 4a^3$ □

Proposition 3.31. *Suppose $m_\alpha(x)$ satisfies Eisenstein's criterion with prime p.*

Let $\theta = \dfrac{x_0 + x_1\alpha + \cdots + x_d\alpha^d}{p}$ for $x_i \in \{0,\ldots,p-1\}$ not all 0.

Then θ is not an algebraic integer.

Proof. Assume $\theta \in \mathcal{O}_k$, let x_i be the first non-zero coefficient.

$$\theta = \frac{x_i\alpha^i + x_{i+1}\alpha^{i+1} + \cdots + x_{d-1}\alpha^{d-1}}{p}$$

Multiply by α^{d-i-1}:

$$\alpha^{d-i-1}\theta = \frac{x_i\alpha^{d-1} + \text{ multiples of } \alpha^d}{p}$$

By Eisenstein's criterion α^d is a multiple of p in $\mathcal{O}_k$:

$$\underbrace{\alpha^{d-i-1}\theta}_{\text{an algebraic integer}} = \frac{x_i\alpha^{d-1}}{p} + \text{ an algebraic integer}$$

$\therefore \frac{x_i\alpha^{d-1}}{p}$ is an algebraic integer. So $N(\frac{x_i\alpha^{d-1}}{p}) \in \mathbb{Z}$.
But $N(\frac{x_i\alpha^{d-1}}{p}) = \dfrac{x_i^d N(\alpha)^{d-1}}{p^d}$ but $x_i \in \{1, \ldots, p-1\}$ coprime to p.
Also by Eisenstein's criterion $N(\alpha)$ is not a multiple of p^2, only a multiple of p.
Therefore $x_i^d N(\alpha)^{d-1}$ is a multiple of p^{d-1} but not p^d. ↯ □

E.g. Let $k = \mathbb{Q}(\alpha)$ $\quad \alpha = 2^{\frac{1}{8}}$ $\quad m(x) = x^8 - 2$

$$\begin{aligned}\Delta\{1, \alpha, \ldots, \alpha^7\} &= (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha)) \\ &= 1 * N(8\alpha^7) \\ &= 8^8 * \underbrace{N(\alpha)^7}_{-2} \\ &= -2^{31}\end{aligned}$$

E.g. Let $k = \mathbb{Q}(\alpha)$ $\quad \alpha$ has minimal polynomial $m(x) = x^3 + 4x + 2$

Irreducible by Eisenstein's criterion with $p = 2$

$$\begin{aligned}\Delta\{1, \alpha, \alpha^2\} &= -27b^2 - 4a^3 \\ &= -27 * 4 - 4 * 64 \\ &= 2^2 * 7 * 13\end{aligned}$$

The only prime whose square divides this is $p = 2$. Therefore $\{1, \alpha, \alpha^2\}$ is an integral basis i.e. $\mathcal{O}_k = \mathbb{Z}[\alpha]$.

E.g. Let $k = \mathbb{Q}(\alpha)$ with minimal polynomial $m(x) = x^3 - 2$.
$\Delta\{1, \alpha, \alpha^2\} = -27b^2 - 4a^3$. $a = 0, b = -2, \alpha = 2^{\frac{1}{3}}$

If $p = 2, 3$ then $p^2 | \Delta\{1, \alpha, \alpha^2\}$, by the proposition we can forget about 2.

$m(x-1) = x^3 - 3x^2 + 3x - 3$

$m(x+2) = x^3 + 6x^2 + 12x + 6$ satisfies Eisenstein's criterion for $p = 2, 3$

$m(x+2)$ is the minimal polynomial of $\alpha - 2 = \beta$ and $\Delta\{1, \beta, \beta^2\} = \Delta\{1, \alpha, \alpha^2\} = -2^3 * 3^3$

Proposition 3.32. *Suppose $\beta = \alpha + 1$ for $x \in \mathbb{Q}$, then $\Delta\{1, \beta, \beta^2, \beta^{d-1}\} = \Delta\{1, \alpha, \dots, \alpha^{d-1}\}$*

By the proposition we can forget about 2 and 3, so $\{1, \beta, \beta^2\}$ is an integral basis.
$\therefore \mathcal{O}_k = \mathbb{Z}[\beta] = \mathbb{Z}[\alpha - 2] = \mathbb{Z}[\alpha]$
$\therefore \{1, \alpha, \alpha^2\}$ is also an integral basis.

Proof. $m_\beta(x) = m_\alpha(X - x)$.
By the chain rule:

$$\begin{aligned} m_\beta(x) &= m_\alpha(X - x) \\ m_\beta(\beta) &= m'_\alpha(\beta - x) = m'_\alpha(\alpha) \\ \\ \Delta\{\beta^i\} &= (-1)^{\frac{d(d-1)}{2}} N(m'_\beta(\beta)) = \Delta\{\alpha^i\} \end{aligned}$$

□

3.7 Cyclotomic Fields

$\zeta = e^{\frac{2\pi i}{n}}$ is the n^{th} primitive root of unity.

Theorem 3.33. *The minimal polynomial of ζ is the cyclotomic polynomial Φ_n with degree $\varphi(n)$.*

Proof. Easy to prove when n is a power of a prime. $\Phi_{n+1}(x)$ will satisfy Eisenstein's criterion. For $n = p^a$:

$$\begin{aligned} \alpha^{p-1} &= \prod_{d | p^a} \Phi_d(x) \\ &= \underbrace{\Phi_1 \Phi_p \dots \Phi_{p^{a-1}}}_{x^{p^{a-1}} - 1} \Phi_{p^a} \end{aligned}$$

$$\Phi_{p^a}(x) = \frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = \underbrace{1 + x^{p^{a-1}} + \dots + x^{(p-1)p^{a-1}}}_{p \text{ terms}}$$

Claim $\Phi_{p^a}(x + 1)$ satisfies Eisenstein's criterion with the prime p.

$$\begin{aligned} (x^{p^{a-1}} - 1)\Phi_{p^a}(x) &= x^{p^a} - 1 \\ ((x + 1)^{p^{a-1}} - 1) &= (x + 1)^{p^a} - 1 \\ (x^{p^{a-1}} + 1^{p^{a-1}} - 1) &\equiv x^{p^a} + 1^{p^a} - 1 \quad (p) \quad \textbf{(*)} \\ \Phi_{p^a}(x + 1) &= x^{p^a - p^{a-1}} \quad (p) \end{aligned}$$

(*) Using that in any ring $(a + b)^p \equiv a^p + b^p \ \ (p)$ and by induction

$(a + b)^{p^n} \equiv a^{p^n} + a^{p^n} + b^{p^n} \ \ (p)$

So all coefficients apart from the leading coefficient are multiples of p. Constant coefficient of $\Phi_{p^n}(x+1)$ is $\Phi_{p^a}(1) = 1 + 1^{p^{a-1}} + 1^{2p^{a-1}} + \cdots + 1^{(p-1)p^{a-1}} = p$.

This is not a multiple of p^2 and so $\Phi_{p^a}(x+1)$ satisfies Eisenstein's criterion.

□

Theorem 3.34. *Let $k = \mathbb{Q}(\zeta)$ and $\zeta = e^{\frac{2\pi i}{n}}$ then $\mathcal{O}_k = \mathbb{Z}[\zeta]$*

Proof. Only in the case where $n = p$ is a prime number.

Notation, let $\lambda = \zeta - 1$.

Recall that $m_\lambda(x) = \Phi_p(x+1)$ which satisfies Eisenstein's criterion with the prime p.

□

Lemma 3.35. *$N(\zeta) = 1$, $N(\lambda) = p$, $[k : \mathbb{Q}] = p - 1$*

Proof. Minimal polynomial of ζ is $\Phi_p(\alpha) = 1 + \alpha + \cdots + \alpha^{p-1} = \frac{x^p - 1}{x - 1}$

$N(\zeta) = (-1)^{p-1} * \Phi_p(0) = 1$

$[k : \mathbb{Q}] = deg(\Phi_p) = p - 1$ □

Theorem 3.36. *Let $k = \mathbb{Q}(\zeta)$, $\zeta = e^{\frac{2\pi i}{n}}$ then $\mathcal{O}_k = \mathbb{Z}[\zeta]$*

Proof. When n is prime

$$\begin{aligned}\Delta\{1, \lambda, \ldots, \lambda^{p-2}\} &= \Delta\{1, \zeta, \ldots, \zeta^{p-2}\} && \text{by the useful trick}\\ &= (-1)^{\frac{d(d-1)}{2}} N(\Phi_p'(\zeta))\\ &= (-1)^{\frac{p-1}{2}} N(\Phi_p'(\zeta))\end{aligned}$$

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

$$\begin{aligned}\Phi_p'(\zeta) &= \frac{p\zeta^{p-1}\lambda - \overbrace{\zeta^p - 1}^{0}}{\zeta^2}\\ &= \frac{p\zeta^{p-1}}{\lambda}\end{aligned}$$

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

The only prime whose square divides this is the prime p but m_λ satisfies Eisenstein's criterion with p, therefore $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is an integral basis.

So $\mathcal{O}_k = \mathbb{Z}[\lambda] = \mathbb{Z}[\zeta] \implies \{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis. □

The proof generalises to the case $n = p^a$ but not to general n.

E.g. $n = 2$

$$\begin{aligned} k &= \mathbb{Q}(\zeta_{20}) & \zeta_{20} &= e^{\frac{2\pi i}{20}} \\ m &= \mathbb{Q}(\zeta_5) & \zeta_5 &= e^{\frac{2\pi i}{5}} = \zeta_{20}^4 \\ &\mathbb{Q} \end{aligned}$$

We can prove using $\Delta\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ that $\{1, \zeta_5, \zeta_5^2, \zeta_5^3\}$ is an integral basis in m. We can also define the discriminant of a basis is for k as vector space over m.

$\Delta_{k/m}\{1, i\} = -4$

Useful Trick: $N(x - \alpha) = m(x)$

4 Factorisation in Rings of Algebraic Integers

Let k be a number field, $\mathcal{O}_k$ might or might not have unique factorisation but $\mathcal{O}_k$ has unique factorisation if ideal.

The main tool for splitting factors of elements in $\mathcal{O}$ is the norm, $N(AB) = N(A)N(B)$.

This shows that $\underbrace{A|B}_{\text{in } \mathcal{O}} \implies \underbrace{N(A)|N(B)}_{\text{in } \mathbb{Z}}$

Proposition 4.1. *For any $A \in \mathcal{O}$, $A|N(A)$*

Proof. Want to show that $\frac{N(A)}{A}$ is an algebraic integer.

If $\sigma_1(A) = A$ then $\frac{N(A)}{A} = \sigma_2(A) \dots \sigma_d(A)$ and each $\sigma_i(A)$ is an algebraic integer so $\frac{N(A)}{A}$ is an algebraic integer. □

Corollary 4.2. *Let $A \in \mathcal{O}$. Then A is a unit iff $N(A) = \pm 1$*

Proof. ($\implies$) A is a unit $\implies A|1 \implies N(A)|N(1) = 1 \implies N(A) = \pm 1$

($\impliedby$) If $N(A) = \pm 1 \implies A| \pm 1 \implies A$ is a unit □

Corollary 4.3. *Let $A \in \mathcal{O}$. If $N(A) = \pm p$ then A must be irreducible.*

Proof. Suppose $A = BC$, $N(B)N(C) = \pm p \implies N(B), N(C) = \pm 1$. So B or C is a unit □

There are also many irreducible elements whose norm is not prime,

E.g. $\mathcal{O} = \mathbb{Z}[i]$, $k = \mathbb{Q}(i)$.

Let $p = 2 + 3i$, $N(p) = 2^2 + 3^2 = 13$, so $2 + 3i$ is irreducible by corollary.

E.g. Let $Q = 3$, then $N(Q) = 9$ but Q is also irreducible.

This is because there are no elements of norm 3, $N(x + iy) = x^2 + y^2 = 3$ ↯

Proposition 4.4. *Let $A \in \mathcal{O}$ and not a unit, then $A = P_1 \dots P_r$ for irreducible elements P_i*

Proof. By induction on $|N(A)|$. If $|N(A)| = 2$ then A is irreducible.

Suppose true for elements B with $|N(B) < |N(A)|$

If A is irreducible then we're done, if not then $A = BC$ and $|N(B) < |N(A)|$, $|N(C) < |N(A)|$.
So B and C factorise into irreducibles hence so does A. □

Examples of non unique factorisation
$k = \mathbb{Q}(\sqrt{-10})$, $\quad -10 \equiv 1 \ \ (4)$

So $\mathcal{O} = \mathbb{Z}[\sqrt{-10}]$

Note that $10 = 2 * 5 = \sqrt{10} * \sqrt{-10}$ and $2, 5, \pm 10$ are all irreducible.

$N(2) = 4$
$N(5) = 25$
$N(\pm\sqrt{10}) = \sqrt{-10} * -\sqrt{-10} = 10$

Are there any elements with norm 2 or 5?

$N(x + y\sqrt{-10}) = x^2 + 10y^2 \neq \pm 2$ or ± 5

$\mathbb{Z}[\sqrt{10}]$ does not have unique factorisation, although 2,5 $\sqrt{-10}$ are all irreducible elements. The ideals (2), (5), $(\sqrt{-10})$ all factorise.

Although 2, $\sqrt{-10}$ are coprime as elements and the only common factor is a unit, it's not true that:

$$1 = H * 2 + K * \sqrt{-10} \ \text{ for } H, K \in \mathbb{Z}[\sqrt{-10}]$$

i.e. $(2, \sqrt{-10}) \neq \mathbb{Z}[\sqrt{-10}]$

Let $P = (2, \sqrt{-10})$ and $Q = (5, \sqrt{-10})$

$$\begin{aligned} P^2 &= (2, \sqrt{-10}) * (2, \sqrt{-10}) \\ &= (2 * 2, 2 * \sqrt{-10}, -10) \\ &= (4, -10, 2\sqrt{-10}, 2) \\ &= (2) \end{aligned} \qquad \begin{aligned} Q^2 &= (5, \sqrt{-10}) * (5, \sqrt{-10}) \\ &= (25, 5\sqrt{-10}, -10) \\ &= (25, 5\sqrt{-10}, -10, 5) \\ &= (5) \end{aligned}$$

$$\begin{aligned} PQ &= (10, 2\sqrt{-10}, 5, \sqrt{-10}, -10) \\ &= (10, 2\sqrt{-10}, 5, 5\sqrt{-10}, -10, \sqrt{-10}) \\ &= (\sqrt{-10}) \end{aligned}$$

Recall $10 = 2 * 5 = \sqrt{-10} * \sqrt{-10}$ in terms of ideals.
$(10) = (2)(5) = (-\sqrt{10})^2 = P^2Q^2 = (PQ)^2$

Often $\mathcal{O}$ is not a UFD and not a PID.

Instead of factorising elements of $\mathcal{O}$, we factorise ideals.

Theorem 4.5. *Let I be a non-zero ideal of $\mathcal{O}$, then there exists maximal ideals $P_1, \dots, P_r$ of $\mathcal{O}$ unique up to reordering such that $I = P_1 \dots P_r$.*

The proof will involve:

- The norm of an ideal, this is useful for factorising an ideal
- It will also give us a way of proving theorems about ideals by induction

Definition 4.6. *Let $I \subset \mathcal{O}$ be a non-zero ideal. The norm of I is $N(I) = |\mathcal{O}/I|$*

Proposition 4.7. *If I is a non-zero ideal of $\mathcal{O}$ then $N(I)$ is finite.*

Proof. Choose a non-zero element $\beta \in I \implies (\beta) \subseteq I \implies |\mathcal{O}/(\beta)| \geq |\mathcal{O}/I|$ □

Proposition 4.8. *If $\beta \in \mathcal{O}$ is non-zero then* $\underbrace{N\Big((\beta)\Big)}_{\textit{norm of ideal}} = \underbrace{|N(\beta)|}_{\textit{norm of element}}$

Lemma 4.9. *(From Commutative Algebra)*
Let A be a $d \times d$ matrix with entries in $\mathbb{Z}$ and $\det(A) \neq 0$. Then $|\mathbb{Z}^d / A\mathbb{Z}^d| = |\det(A)|$.

Proof. (Prop 4.8)
Let β be an integral basis, this gives us an isomorphisms of additive groups, $\mathbb{Z}^d \cong \mathcal{O}$.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \mapsto x_1 b_1 + \dots + x_d b_d$$

Multiplication by β on $\mathcal{O}$ corresponds to multiplication by A_β on $\mathbb{Z}^d$ where A_β is the standard representation with respect to β.

Then $\mathbb{Z}^d / A_\beta \mathbb{Z}^d \cong \mathcal{O}/(\beta)$.

So by the lemma:

$$\begin{aligned} N\Big((\beta)\Big) &= |\mathcal{O}/(\beta)| \\ &= |\mathbb{Z}^d / A_\beta \mathbb{Z}^d| \\ &= |\det(A_\beta)| \\ &= |N(\beta)| \end{aligned}$$

□

Proof. (Sketch of lemma)

We can do integer row and column operations to A to reduce it to diagonal form.

$A = PDQ \quad P, Q$ are integer matrices with determinant:

$$D = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_d \end{pmatrix} \qquad\qquad P\mathbb{Z}^d = \mathbb{Z}^d$$

$$Q\mathbb{Z}^d = \mathbb{Z}^d$$

$$\begin{aligned} \mathbb{Z}^d/a\mathbb{Z}^d &= \mathbb{Z}^d/PD\underbrace{Q\mathbb{Z}^d}_{\mathbb{Z}^d} \\ &= P\mathbb{Z}^d/PD\mathbb{Z}^d \\ &= \mathbb{Z}^d/D\mathbb{Z}^d \\ &\equiv \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_d\mathbb{Z} \end{aligned}$$

$$\begin{aligned} |\mathbb{Z}^d/A\mathbb{Z}^d| &= |e_1 \dots e_d| \\ &= |\det(D)| \\ &= |det(A)| \end{aligned}$$

□

4.1 Prime ideals and Maximal ideals

Let R be any commutative ring with 1. An ideal $P \subseteq R$ is called a prime ideal if:

- $P \neq R$
- If $xy \in P \implies x \in P$ or $y \in P$

Recall R is an integral domain if:

- $1 \neq 0$ in R
- If $xy = 0$ then $x = 0$ or $y = 0$

Proposition 4.10. *Let P be an ideal in R then P is prime $\iff$ R/P is an integral domain.*

Proof.

$$\begin{aligned} P \neq R &\iff 1 \in P \\ &\iff 1 \neq 0 \ \ (P) \quad \text{1 and 0 are different in } R/P \end{aligned}$$

$$xy \equiv 0 \ \ (P) \iff xy \in P$$

$$x \equiv 0 \ \ (P) \text{ or } y \equiv 0 \ \ (P) \iff x \in P \text{ or } y \in P$$

□

Proposition 4.11. *Recall $I \subseteq R$ is maximal $\iff$ R/I is a field*

Corollary 4.12. *Every maximal ideal is prime*

Proof. Every field is an integral domain. □

There are prime ideals which are not maximal.

E.g. $(0) \subseteq \mathbb{Z}$ is a prime ideal but not maximal, $\mathbb{Z}/(0) \cong \mathbb{Z}$ which is an integral domain but not a field

E.g. $(x) \subseteq \mathbb{C}[x,y]$ is prime but not maximal, $\mathbb{C}[x,y]/(x) \cong \mathbb{C}[y]$ is an integral domain but not a field.
$f(x,y) \mapsto f(0,y)$

Recall every finite integral domain is a field.

Corollary 4.13. *If P is a prime ideal in $\mathcal{O}$ then either $P = (0)$ or P is maximal.*

Proof. Suppose P is a non-zero prime ideal $\mathcal{O}_k/P$ is an integral domain and is finite because $N(P)$ is finite.

Therefore $\mathcal{O}_k/P$ is a field so P is maximal. □

Proof. (of proposition)
Let R be a finite integral domain. Let $x \in R$ with $x \neq 0$.
The powers x^n are not all distincts.

This implies $x^n = x^{n+m}$ for some m, n.

By the cancellation property $1 = x^m$.

Therefore x^{m-1} is an inverse of x. □

Lemma 4.14. *Let $I \subseteq R$ be an ideal, then I is prime iff:*

- *$I \neq R$*
- *Suppose $JK \subset I$ for ideals J, K, then $J \subseteq I$ or $K \subseteq I$*

Definition 4.15. *A prime ideal is one such that:*

- *$I \neq R$*
- *$xy \in I \implies x \in I$ or $y \in I$*

Proof. ($\implies$)

Assume I is prime and assume $J \subseteq I$. We'll show that $K \subseteq I$.
Choose $x \in j \backslash I$.

For $y \in K$ we have $xy \in JK \subseteq I \implies y \in I$.

($\Longleftarrow$)

Assume the property of the lemma, suppose $xy \in I$. Then $(x)(y) = (xy) \subseteq I$.
By the property in the lemma $(x) \subseteq I$ or $(y) \subseteq I$, so $x \in I$ or $y \in I$ □

Remark: Suppose $M_1, \dots M_r$ and $M'_1, \dots M'_s$ are maximal ideals and $M_1 \dots M_r = M'_1 \dots M'_s$.
Also $M_1 \supset M'_1 \dots M'_s$ but M_1 is prime so by the lemma, $M_1 \supseteq M'_i$ for some i and without loss of generality, $M \supseteq M'_1$.

4.2 Fractional Ideals and Unique Factorisation

If $M_1 \dots M_r = M'_1 \dots M'_s$ then $M_1 = M'_i$ for some i, we want a way of cancelling ideals in order to prove uniqueness of factorisation. To give ideal inverses we need something more general than an ideal.

Definition 4.16. *Let k be a number field, $\mathcal{O}_k$ the ring of algebraic integers in k. A fractional ideal in k is a subset $I \subseteq k$ such that there exists $\beta \in \mathcal{O}$, $\beta \neq 0$ such that βI is an ideal of $\mathcal{O}$.*

E.g. If $k \in \mathbb{Q}$ $\quad \mathcal{O}_k = \mathbb{Z}$ the fractional ideals have the form:

$$(x) = \{xy : y \in \mathbb{Z}\} \text{ with } x \in \mathbb{Q}$$

We can multiply fractional ideals in the same way as ideals.

$$IJ = \{\sum_{i,j} x_i y_j : x_i \in I \quad y_j \in J\}$$

This is clearly associative and $(1) = \mathcal{O}_k$ is the identity element.

4.3 Tricky Lemma

Lemma 4.17. *Let $P \subseteq \mathcal{O}_k$ be a maximal ideal. Then there is a fractional ideal P^{-1} such that:*

- *If I is any ideal, $I \subseteq P$ then $P^{-1}I$ is also an ideal which has smaller norm than I. In other words $P^{-1}I$ is an ideal containing I but not equal to I*
- *$PP^{-1} = (1)$*

Using this we'll prove some theorems.

Theorem 4.18. *The non-zero fractional ideals form a group with the operation ×.*

Proof. Remains to show that every element has an inverse.
We'll first show that all ideals have inverses. By induction on $N(I) = 1$ then $I = \mathcal{O}_k = (1)$.

Assume all ideals with norm smaller than I have inverses.

Let P be a maximal ideal containing I, by the tricky lemma, $P^{-1}I$ is an ideal with norm smaller than I.

$P^{-1}I$ has an inverse J. $\underbrace{(JP^{-1})}_{\text{inverse of } I}\ I = (1)$

Now let I be any fractional ideal (non-zero). $\beta I = J$ is an ideal for non-zero $\beta \in \mathcal{O}_k$. Therefore J has an inverse J^{-1}. $\underbrace{\beta J^{-1}}_{\text{inverse of } I}\ I = J^{-1}J = (1)$

□

Theorem 4.19. *Every non-zero ideal $I \subseteq \mathcal{O}_k$ can be factorised as $I = P_1 \dots P_r$ with P_i maximal, unique up to reordering.*

Proof. By induction on $N(I)$, if $N(I) = 1$ then $I = (1)$ so true with $r = 0$.

Assume all ideals with smaller norm than I can be factorised into maximal ideals.

Let P be a maximal ideal containing I, by the tricky lemma, $P^{-1}I$ is an ideal with smaller norm than I.

Therefore $P^{-1}I = P_1 \dots P_r$ (P_i maximal) and $I = PP_1 \dots P_r$.

(Uniqueness of factorisation)

By induction on $N(I)$, if $N(I) = 1$ then $I = (1)$ and nothing to prove.

Assume all ideals with smaller norm than I have a unique factorisation.

Suppose $I = P_1 \dots P_r = Q_1 \dots Q_s$ for P_1, Q_i maximal.

Let P_1 be prime and $P_1 \supseteq Q_1 \dots Q_s$. So $P_i \supset Q_i$ for some i.

Without loss of generality $P_1 \supseteq Q_1$ but Q_i is maximal so $P_1 = Q_1$.

Multiply the equation by $P_1^{-1} \implies P_1^{-1}I = P_2 \dots P_r = Q_2 \dots Q_s$

By the tricky lemma, $P_1^{-1}I$ is an ideal with smaller norm than I.

Therefore P_1^{-1} has only maximal ideals $\implies$ after reordering $P_i = Q_i$ and $r = s$. □

A subset $I \subset k$ is a fractional ideal if $I = \beta^{-1}J$ for $\beta \in \mathcal{O}_k$, $\beta \neq 0$ and J is an ideal.

E.g. in $\mathbb{Q}$, $(\frac{1}{2}) = \{\frac{n}{2} : n \in \mathbb{Z}\}$

Remark: If I is a fractional ideal then I is an ideal $\iff I \subseteq \mathcal{O}_k$

Proof. ($\implies$) trivial

($\impliedby$) βI is an ideal so closed under $+$ and scalar multiplication.

I is closed under $+$, scalar multiplication $\implies I$ is an ideal. □

Definition 4.20. *Let I, J be ideals, we'll say $I|J$ if $J = II'$ for some ideal I'*

Corollary 4.21. $I|J \iff I \supseteq J$

Proof. ($\implies$) $\quad J = II' \quad I' \subseteq \mathcal{O}_k$ then $J \subseteq I\mathcal{O}_k = I$

($\impliedby$) Suppose $I \supseteq J$. Let $I' = I^{-1}J \implies J = II'$. Remains to show that $I' \subseteq \mathcal{O}_k$.

$J \subseteq I$

Therefore $I' = I^{-1}J \subseteq I^{-1}I = (1) = \mathcal{O}_k$

I' is an ideal.

□

Definition 4.22. $P^{-1} = \{x \in k : xP \subset \mathcal{O}_k\}$

Let $\beta \in P$, $\beta \neq 0$. We'll see that $\beta P^{-1} \subseteq \mathcal{O}_k$ and is an ideal.

If $x \in P^{-1}$ then $xP \subseteq \mathcal{O}_k$
$\implies x\beta \in \mathcal{O}$
$\implies \beta P^{-1} \subseteq \mathcal{O}_k$

Let $x, y \in P^{-1}$ and $\lambda \in \mathcal{O}_k$, need to check $x + \lambda y \in P^{-1}$.

Let $\delta \in P$

$\implies x\delta \in \mathcal{O}_k$ and $y\delta \in \mathcal{O}_k$

$\implies x\delta + \lambda y\delta \in \mathcal{O}_k$

$\implies (x + \lambda)\delta \in \mathcal{O}_k$

$\implies x + \lambda y \in P^{-1}$

Definition 4.23. $P^{-1} = \{x \in k : xP \subseteq \mathcal{O}_k\} \implies$ *P^{-1} is a fractional ideal.*

Before proving the tricky lemma we'll need:

Lemma 4.24. *Let $I \subseteq \mathcal{O}_k$ for $I = 0$. Then there exists ideals $P_1, \ldots, P_r$ with $I \supseteq P_1 \ldots P_r$*

Proof. By induction on $N(I)$.

If $N(I) = 1$ then $I = \mathcal{O}_k$. Assume true for ideals smaller norm than I.

If I is maximal then let $P_i \in I$.
If I is not maximal then I is no prime. Then there exists $x, y \in \mathcal{O}_k$, $xy \in I$ and $x \notin I$, $y \notin I$.

Let $J = I + (x)$ and $K = I + (y)$

These are bigger than I so they have smaller norm.

$J \supseteq P_1 \ldots P_t$ for P_i maximal
$K \supseteq P_{i+1} \ldots P_r$

Then $JK = \underbrace{I * I}_{\subseteq I} + \underbrace{I * (y)}_{\subseteq I} + \underbrace{I(x)}_{\subseteq I} + \underbrace{(xy)}_{\subseteq I}$

$\implies JK \subseteq I$

$\implies P_1 \dots P_r \subseteq I$

□

Note that $P^{-1} \supseteq \mathcal{O}_k$, if $x \in \mathcal{O}_k$ then $xP \subseteq \mathcal{O}_k$ therefore $x \in P^{-1}$.

The first step in the proof of the tricky lemma will be to show that $P^{-1} \supsetneq \mathcal{O}_k$.

Proof. (Tricky Lemma)

Step 1: Show that $P^{-1} \supsetneq \mathcal{O}_k$.

Choose $a \in P$, $a \neq 0$ such that $(a) \supseteq P_1, \dots P_r$, by the previous lemma with $P_1, \dots, P_r$ maximal.

We'll do this with r minimal.

$P_1 \dots P_r \subseteq (a) \subseteq P$

Since P prime, $P \supseteq P_i$ for some i, without loss of generality, $P \supseteq P_r$ but P_r is maximal.

$\implies P = P_r$

Since r is minimal $(a) \supsetneq P_1 \dots P_{r-1}$ so we can choose $b \in P_1 \dots P_{r-1}$ for $b \in (a)$.

Let $x = \frac{b}{a}$, we'll see that $x \in P^{-1}$ and $x \in \mathcal{O}_k$.

$xP = \frac{b}{a}P \subseteq \frac{1}{a}(P_1 \dots P_{r-1})P = \frac{1}{a}P_1 \dots P_r \subseteq \frac{1}{a}(a) = \mathcal{O}_k$

$\therefore x \in P^{-1}$

Also $b \in (a)$ so b is not a multiple of a, i.e. $\frac{b}{a} \in \mathcal{O}_k$.

Step 2: Let $I \subseteq P$ an ideal, want to show that $P^{-1}I$ is an ideal bigger than I.

$P^{-1}I \subseteq P^{-1}P \subseteq \mathcal{O}_k$, from the definition of P^{-1}.

$\therefore P^{-1}$ is an ideal and $P^{-1} \supseteq \mathcal{O}_k$ so $P^{-1}I \supseteq \mathcal{O}_k I = I$

Suppose $P^{-1}I = I$. Let $x \in P^{-1}$, $x \in \mathcal{O}_k$ then by step 1:

$xI \subseteq I$

$I = Span_{\mathbb{Z}}\{b_1, \dots, b_d\}$

$xb_1 = m_{i1}b_1 + \dots + m_{id}b_d$ $\qquad$ $x\begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} = \left(m_{ij}\right)\begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}$

So x is an eigenvalue of (m_{ij}), $x \in \mathcal{O}_k$ ↯

Step 3: Let $I = P$, by step 2, $P^{-1}P$ is a bigger ideal than P but P is maximal. $P^{-1}P = \mathcal{O}_k$

□

Theorem 4.25. *If k is a number field and $\mathcal{O}_k$ is the ring of algebraic integers in k, then every non-zero ideal I has a unique factorisation $I = P_1 \dots P_r$ for maximal ideal P_i.*

We'll now concentrate on these questions:

1. Given I, how do we find $P_1, \dots P_r$?
2. How do we find $N(I)$?
3. What are the maximal ideals in $\mathcal{O}_k$?

4.4 Norms of Ideals

Definition 4.26. $N(I) = |\mathcal{O}_k/I|$
$N\Big((\beta)\Big) = |N(\beta)|$

Theorem 4.27. *Let I, J be non-zero ideals in $\mathcal{O}_k$ then $N(IJ) = N(I)N(J)$.*

We can use the theorem to calculate $N(I)$ if I is not a principal ideal.

Remark: Suppose $\sigma : k \to k$ is a field homomorphism.

If $\beta \in \mathcal{O}_k$ then $\sigma(\beta) \in \mathcal{O}_k$ because they have the same minimal polynomial, i.e. $\sigma(\mathcal{O}_k) = \mathcal{O}_k$

If I is an ideal, then $\sigma(I)$ is also an ideal.

Also $N(\sigma I) = |\mathcal{O}_k/\sigma(I)| = |\sigma(\mathcal{O}_k)/\sigma(I)| = |\mathcal{O}_k/I| = N(I)$

E.g. Let $k = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$ because $-5 \not\equiv 1 \;\; (4)$
$I = (2, 1 + \sqrt{-5})$ and $\sigma(x + y\sqrt{-5}) = x - y\sqrt{-5}$ then:

$$\begin{aligned}
\sigma(I) &= (2, 1 - \sqrt{-5}) \\
I * \sigma(I) &= (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) \\
&= (\cancel{4}, \cancel{2 - 2\sqrt{-5}}, \cancel{2 + 2\sqrt{-5}}, \cancel{6}) \\
&= (2)
\end{aligned}$$

$$\begin{aligned}
N(I)^2 = N(I * \sigma(I)) &= N\Big((2)\Big) \\
&= |N(2)| \\
&= 4
\end{aligned}$$

$\therefore N(I) = 2$

Theorem 4.28. *N(IJ) = N(I)N(J)*

Proof. Sufficient to prove when $J = P$ is a maximal ideal.

$N(IP) = |\mathcal{O}_k/IP|$

$\mathcal{O}_k \cong (\mathcal{O}_k/IP)\Big/(I/IP)$

$\therefore N(I) = \dfrac{N(IP)}{|I/IP|}$

So we want to prove $|I/IP| = N(P) = |\mathcal{O}_k/P|$.

We'll find an isomorphism $\mathcal{O}_k/P \cong I/IP$ such that $IP \subsetneq I$.

Choose $a \in I$ such that $a \notin IP$.

Define $\Phi : \mathcal{O}_k \to I/IP$ by:
$x \to ax \mod IP$

Then this means $IP \subsetneq IP + (a) \subseteq I$.

Since P is maximal, $IP + (a) = I$.

$\therefore$ Every element of IP is congruent mod IP to a multiple of a.

$\therefore$ Φ is surjective.

$ker(\Phi)$ is an ideal, not just a subgroup of $\mathcal{O}_k$. If $ax \equiv 0 \pmod{IP}$ then for all $y \in \mathcal{O}_k$:

$axy \equiv 0 \pmod{IP}$

So $x \in ker \implies xy \in ker$.

If $x \in P$ then $ax \in IP$, since $a \in I$.

So $\Phi(x) \equiv 0 \pmod{IP}$ i.e. $x \in ker(\Phi)$ and $ker(\Phi)$ is an ideal containing P.

Since P maximal, $ker(\Phi) = P$ or $\mathcal{O}_k$.

But Φ is surjective $\implies \Phi \neq 0 \implies ker(\Phi) \neq \mathcal{O}_k$.

Therefore $ker(\Phi) = P$ and by the first isomorphism theorem:

$\mathcal{O}_k/P \cong I/IP$ so $N(P) = |I/IP|$

□

Corollary 4.29. *If $I \subseteq \mathcal{O}_k$ is a non-zero ideal and $N(I)$ is a prime number then I is maximal.*

E.g. In $\mathbb{Z}[\sqrt{-5}$, the ideal $(2, 1+\sqrt{-5})$ has norm 2 so is maximal.

Proof. $I = P_1 \dots P_r$ for P_i maximal and by the theorem:

$$N(P_1)N(P_2)\dots N(P_r) \text{ is prime}$$

Note that for all $N(P_i)$, $N(P_i) > 1$.
$\therefore r = 1$ so $I = P_1$ □

Lemma 4.30. $N(I) \in I$

Proof. Let n be the order of 1 in the additive group $\mathcal{O}/I$. So

$$n = \underbrace{1+1+1+\cdots+1}_{n} \equiv 0 \ \ (I)$$

By corollary to Lagrange's theorem, $n|N(I)$ so $N(I) \equiv 0 \ \ (I)$, i.e. $N(I) \in I$. □

Corollary 4.31. *There are only finitely many ideals in $\mathcal{O}_k$ with any given norm.*

Proof. Suppose $N(I) = n$, then $n \in I$ by the lemma. Therefore $(n) \subseteq I$ and I is factor of (n).

By uniqueness of factorisation (n) has only finitely many factors. □

Lemma 4.32. *Let $R \subseteq S$ be commutative rings. If $P \subset S$ is a prime ideal then $P \cap R$ is a prime ideal of R.*

Proof. Suppose $xy \in P \cap R$ with $x, y \in R$. $xy \in P \implies x \in P$ or $y \in P$.

Since $x, y \in R$, we have $x \in P \cap R$ or $y \in P \cap R$ □

Let P be a maximal ideal in $\mathcal{O}_k$. By the lemma $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Also $P \cap \mathbb{Z} \neq \{0\}$ because $N(P) \in P$.

Therefore $P \cap \mathbb{Z} = (p)$ for some prime number $p \in \mathbb{Z}$, i.e. $P|(p)$. We'll say "P lies above p and write $P|p$.

This means that to find all the maximal ideals of $\mathcal{O}_k$, we just factorise (P) for each prime number p.

Corollary 4.33. *If $P \subset \mathcal{O}_k$ is maximal then $N(P) = p^r$ for some $r \leq [k : \mathbb{Q}]$ where $P|p$*

Proof. $P|(p)$, therefore $N(P)|N\Big((p)\Big) = p^{[k:\mathbb{Q}]}$ □

4.5 Dedekind's Criterion

Assume $\mathcal{O}_k = \mathbb{Z}[\alpha]$ and let $m(x)$ be the minimal polynomial of α and p be a prime number.

Suppose $m(x) \equiv m_1(x)^{e_1} \dots m_r(x)^{e_r}$ where $m_i \in \mathbb{F}_p[x]$ are irreducible distinct, monic polynomials.

Then $(p) = Q_1^{e_1} \dots Q_r^{e_r}$ where $Q_i = (p, m_i(\alpha))$. The ideals Q_i are distinct and maximal and $N(Q_i) = p^{deg(m_i)}$.

E.g. $k = \mathbb{Q}(\sqrt{6})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{6}]$, $\alpha = \sqrt{6}$, $m(x) = x^2 - 6$

x	$m(x) = x^2 - 6$
0	-6 = -2*3
±1	-5
±2	-2
±3	3

$m(x) \equiv x^2 \ \ (2)$ so $(2) = Q_2^2$ where $Q_2 = (2, m_i(\sqrt{6}))$.
$m_i(x) = x$ so $Q_2 = (2, \sqrt{6})$

$m(x) \equiv x^2 \ \ (3)$
$(3) = Q_3^2$ where $Q_3 = (3, \sqrt{6})$.

$m(x) \equiv (x-1)(x+1) \ \ (5)$
$(5) = Q_5 Q_5'$ where $Q_5 = (5, \sqrt{6}+1)$ and $Q_5' = (5, \sqrt{6}-1)$.

$m(x) \equiv m(x) \ \ (7)$
(7) is a maximal ideal in $\mathbb{Z}[\sqrt{6}]$.

Proof.

$\mathcal{O}_k = \mathbb{Z}[\alpha]$
$\mathcal{O}_k \cong \mathbb{Z}[x]/(m)$
$\alpha \leftarrow x \mod m$

For each Q_i we have:

$$\begin{aligned} \mathcal{O}_k/Q_i &\cong \mathbb{Z}[x]/(m, p, m_i(x)) \\ &\cong \mathbb{F}_p[x]/(m, m_i) \\ &\cong \mathbb{F}_p[x]/(m_i) \text{ because } m_i | m \text{ in } \mathbb{F}_p[x] \end{aligned}$$

But m_i is irreducible in $\mathbb{F}_p[x]$

$$\begin{aligned} &\implies (m_i) \text{ is maximal in } \mathbb{F}_p[x] \\ &\implies \mathbb{F}_p[x]/(m_i) \text{ is a field} \\ &\implies \mathcal{O}_k/Q_i \text{ is a field} \\ &\implies Q_i \text{ is maximal} \end{aligned}$$

Also

$$\begin{aligned} N(Q_i) &= |\mathcal{O}_k/Q_i| \\ &= |\mathbb{F}_p[x]/(m_i)| \\ &= p^{deg(m_i)} \end{aligned}$$

We'll next show that $(p) = Q_1^{e_1} \dots Q_r^{e_r}$:

$$\begin{aligned} Q_1^{e_1} \dots Q_r^{e_r} &= (p, m_1(\alpha))^{e_1} \dots (p, m_r(\alpha))^{e_r} \\ &= (m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r}, \text{ multiples of } p) \end{aligned}$$

But $m_1(\alpha)^{e_1} \dots m_r(\alpha)^{e_r} \equiv \underbrace{m(\alpha)}_{0} \mod p$

This shows that $Q_1^{e_1} \dots Q_r^{e_r} =$ (multiples of p), therefore $Q_1^{e_1} \dots Q_r^{e_r} \subseteq (p)$

To show that they are equal, we'll show that they have the same norm:

$$\begin{aligned} N(Q_1^{e_1} \dots Q_r^{e_r}) &= N(Q_1)^{e_1} \dots N(Q_r)^{e_r} \\ &= (p^{deg(m_1)})^{e_1} \dots (p^{deg(m_r)})^{e_r} \\ &= p^{e_1 deg(m_1) + \dots + e_r deg(m_r)} \\ &= p^{deg(m)} \\ &= N\Big((p)\Big) \end{aligned}$$

Therefore $(p) = Q_1^{e_1} \dots Q_r^{e_r}$.

Remains to show that Q_i are distinct $\mathcal{O}_k / Q_i \cong \mathbb{F}_p[x]/(m_i)$ with $\alpha \mapsto x$.

Suppose $Q_i = Q_j$ then $m_j(\alpha) \in Q_i$.

Then $m_j(\alpha) \equiv 0 \ \ (Q_i)$ and $m_j(x) \equiv 0 \ \ (m_i)$ in $\mathbb{F}_p[x]$.

So $m_i | m_j$ in $\mathbb{F}_p[x]$ □

E.g. We'll factorise $(12 + 7\sqrt{6})$ into maximal ideals in $\mathcal{O}_k$

$$\begin{aligned} N\Big((12 + 7\sqrt{6})\Big) &= |12^2 - 6 * 7^2| \\ &= |144 - 294| \\ &= |150| \\ &= 2 * 3 * 5^2 \end{aligned}$$

Recall that
$(2) = Q_2^2$,
$(3) = Q_3^2$,
$(5) = Q_5 Q_5'$

with norms:
$N(Q_2) = 2$
$N(Q_3) = 3$,
$N(Q_5) = N(Q_5') = 5$ where

$Q_2 = (2, \sqrt{6})$
$Q_3 = (3, \sqrt{6})$
$Q_5' = (5, \sqrt{6} + 1)$
$Q_5' = (5, \sqrt{6} - 1)$

and $(7)^2$ is a prime ideal with norm 7^2.

The ideals with norm 150 are $Q_2Q_3Q_5^2$, $Q_2Q_3Q_5Q_5'$ or $Q_2Q_3Q_5'^2$.

Note that (5) is not a factor of $(12+7\sqrt{6})$.

If Q_5 is a factor then $(12+7\sqrt{6}) = Q_2Q_3Q_5^2$
If Q_5' is a factor then $(12+7\sqrt{6}) = Q_2Q_3Q_5^2$

Is $12+7\sqrt{6}$ in Q_5 or Q_5'?

$12+7\sqrt{6} = 5+7(\sqrt{6}+1) \in Q_5$

In this case Q_2, Q_3, Q_5 are all principal.

$N(x+y\sqrt{6}) = x^2-6y^2$

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

Therefore:
$(2+\sqrt{6}) = Q_2$
$(3+\sqrt{6}) = Q_3$
$(1+\sqrt{6}) = Q_5$
$(1-\sqrt{6}) = Q_5'$

E.g. Let $\mathbb{Q}(\sqrt{\alpha})$, $\alpha^3 = \sqrt{2}$, $\mathcal{O} = \mathbb{Z}[\alpha]$, $m(x) = x^3-2$

$$\begin{aligned} m(x) &= x^3 \quad (2) \\ &= (x+1) \equiv (x+1)^3 \quad (3) \\ &= (x+2)\ \underbrace{(x^2-2x-1)}_{\text{irreducible mod 5}} \quad (5) \\ &= \text{ irreducible mod 7} \end{aligned}$$

x	$m(x)$
0	-2
1	-1
-1	3
2	6=2*3
-2	-10=-2*5
3	25=5*5
-3	-29

$(2) = P_2^3$	$P_2 = (2, \alpha)$	Norm 2
$(3) = P_3^3$	$P_3 = (3, \alpha + 1)$	Norm 3
$(5) = P_5 P_{25}$	$P_5 = (5, \alpha + 2)$	Norm 5
	$P_{25} = (5, \alpha^2 - 2\alpha - 1)$	Norm 25

(7) is prime with norm 7^3

4.6 Ramified Primes

Suppose p is a prime number and $(p) = Q_1^{e_1} \dots Q_r^{e_r}$ for Q_i distinct prime ideals in $\mathcal{O}_k$. Then p is ramified if the powers $e_1, \dots, e_r$ are not all 1.

For example 2 and 3 are ramified in $\mathbb{Z}[\sqrt[3]{2}]$.

Also in $\mathbb{Q}(\sqrt{7})$, 2 and 7 are ramified and all the other primes are unramified.

This folllows then:

Theorem 4.34. *p ramified $\iff$ $p|\Delta$ where Δ is the discriminant of an integral basis.*

Proof. (Sketch)

Assuming $\mathcal{O}_k = \mathbb{Z}[\alpha]$

($\implies$) Assume p is ramified, suppose $Q^2|(p)$ where Q is a maximal ideal. $Q = (p, m_1(\alpha))$.

By Dedekind's criterion, $m_1(x)^2$ is a factor of $m(x)$ in $\mathbb{F}_p(x)$. Then:

$$\begin{aligned} m(x) &\equiv m_1(x)^2 f(x) \ \ (p) \\ m'(x) &\equiv m_1(x) g(x) \ \ (p) \\ m'(\alpha) &\equiv m_1(\alpha) g(\alpha) \ \ (p) \in Q \end{aligned}$$

$N(m'(\alpha))$ is a multiple of $N(Q)$ which is a power of p.

($\Longleftarrow$) We can reverse the argument. □

Let k be a quadratic field, p unramified in k.

$$(p) = \begin{cases} Q_1 Q_2 & Q_i \text{ norm p} \\ \text{prime} & \text{of norm } p^2 \end{cases}$$

Call these two split or inert respectively.

Recall the Decomposition Theorem, let $k = \mathbb{Q}(\sqrt{n}$ where n square free and let p be prime which is unramified. If:

$\left(\dfrac{n}{p}\right) = 1$ then p splits	2 splits $\iff n \equiv 1 \ \ (8)$
$\left(\dfrac{n}{p}\right) = -1$ then p is inert	2 inert $\iff n \equiv 5 \ \ (8)$

We no longer need to assume $\mathcal{O}_k$ is a UFD.

4.7 Quadratic Fields

Let $k = \mathbb{Q}(\sqrt{n})$ for $n \neq 1$ square-free, $\mathcal{O}_k = \mathbb{Z}[\alpha]$ and

$$\alpha = \begin{cases} \sqrt{n} & n \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{n}}{2} & n \equiv 1 \pmod 4 \end{cases} \qquad \Delta = \begin{cases} 4n & n \not\equiv 1 \pmod 4 \\ n & n \equiv 1 \pmod 4 \end{cases}$$

Suppose p is a prime number, then:

- p is ramified $\implies (p) = Q^2 \qquad N(Q) = p$
- p is split $\implies (p) = Q_1 Q_2 \qquad Q_1 \neq Q_2 \; N(Q_i) = p$
- p is inert $\implies (p)$ prime with norm p^2

Theorem 4.35. *Let p be unramified in $\mathbb{Q}(\sqrt{n})$. If p is odd then:*

$$\left(\frac{n}{p}\right) = 1 \text{ then } p \text{ splits} \qquad 2 \text{ splits} \iff n \equiv 1 \pmod 8$$

$$\left(\frac{n}{p}\right) = -1 \text{ then } p \text{ is inert} \qquad 2 \text{ inert} \iff n \equiv 5 \pmod 8$$

and ramified in other cases.

Proof. Suppose p odd, let $f(x) = x^2 - n$ be the minimal polynomial of $\sqrt{n}$ and $g(x) = \frac{1}{4}$ be the minimal polynomial of $\frac{1+\sqrt{n}}{2}$.

2 is invertible mod p, so f factorises mod p if and only if g factorise mod p.

$\iff x^2 - n \equiv 0 \pmod p$

$\iff \left(\frac{n}{p}\right) = 1$

If $n \equiv 1 \pmod 8$:

$$\begin{aligned} g(x) &= x^2 - x + \frac{1-d}{4} \\ &= x^2 + x \pmod 2 \\ &= x(x+1) \pmod 2 \end{aligned} \qquad \text{split in this case}$$

If $n \equiv 5 \pmod 8$:

$$g(x) = x^2 + x + 1 \pmod 2 \qquad \text{irreducible}$$

□

E.g. If $k = \mathbb{Q}(\sqrt{5})$ and $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, how does (199) factorise?

$$\left(\frac{5}{199}\right) = \left(\frac{199}{5}\right) = \left(\frac{4}{5}\right) = 1$$

Therefore $(199) = Q_1 Q_2$ where $N(Q_1) = N(Q_2) = 199$

4.8 Cyclotomic Fields

Let ζ be the primitive n^{th} root of unity and $k = \mathbb{Q}(\zeta)$ then $[k : \mathbb{Q}] = \varphi(n)$, the Euler totient function.

Also $\Phi(x)$ is the minimal polynomial of ζ

Theorem 4.36. *Let ζ be the primitive n^{th} root of unity with p prime not dividing n and let $f =$ order of p in $(\mathbb{Z}/n)^\times$ and $fg = \varphi(n)$.*

Then p is unramified in $\mathbb{Q}(\zeta)$ and $(p) = Q_1 \dots Q_g$ where Q_i is a prime ideal with norm p^f

E.g. $n = 5$ and $\varphi(5) = 4$

$p \mod n$	f order ($p \bmod 5$)	g	Factorisation of (p)
1	1	4	$Q_1Q_2Q_3Q_4$
2	4	1	(p) is prime with norm p^4
3	4	1	(p) is prime with norm p^4
4	2	2	Q_1Q_2 Q_i prime with norm p^2

Proof.

Let p be a prime $p \not| n$, $\Phi_n(x) | x^n - 1 = g(x)$.

To show that p is unramified, we'll show that g has no repeated factors in $\mathbb{F}_p[x]$.

$g'(x) = nx^{n-1}$ is coprime to $g(x)$ because $n \not\equiv 0 \pmod{p}$

Therefore $\Phi_n(x)$ has no repeated factors in $\mathbb{F}_p[x]$ and by Dedekind's criterion p is unramified.

Let Q be a prime ideal above p.
Then $N(Q) = p^r$. Sufficient to prove $r = f$.

Step 1 ($r \geq f$): We'll first show that ζ has order n in $(\mathcal{O}_k/Q)^\times$
By a corollary to Lagrange's theorem, $n | \underbrace{N(Q) - 1}_{p^r-1}$, i.e. $p^r \equiv 1 \pmod{n}$.

So $r \geq f$.

We know $\zeta^n \equiv 1 \pmod{Q}$. Suppose $\zeta^d \equiv 1 (Q)$ where d is a proper factor of n.

ζ is a common root in $\mathcal{O}_k/Q$ of Φ_n, $x^d - 1$.

Therefore ζ is a repeated root of $x^n - 1$ in $\mathcal{O}_k/Q$ which is a contradiction since $g(x), g'(x)$ are coprime mod p.

Step 2 ($r \leq f$): We'll show that every element of the field $\mathcal{O}_k/Q$ is a root of $x^{p^f} - x \implies |\mathcal{O}_k/Q| \leq p^f$ and then $p^r = N(Q)$

By Fermat's little theorem if $x \in \mathbb{Z}$ then:

$$\begin{aligned} x^p &\equiv x \pmod{p} \\ x^{p^f} &\equiv x \pmod{p} \\ x^{p^f} &\equiv x \pmod{Q} \end{aligned}$$

Also $p^f \equiv 1 \pmod{n}$ and $\zeta^{p^f} = \zeta$.

Note that in any ring $(x+y)^p \equiv x^p + y^p \pmod{p} \implies (x+y)^{p^f} \equiv x^{p^f} + y^{p^f}$ for p prime

Let $\beta = x_0 + x_1\zeta + \cdots + x_r\zeta^r \in \mathbb{Z}[\zeta]$. Then:

$$\begin{aligned} \beta^{p^f} &\equiv x_0^{p^f} + (x_1\zeta)^{p^f} + \cdots + (x_r\zeta^r)^{p^f} \pmod{p} \\ &\equiv x_0 + x_1\zeta^{p^f} + \cdots + x_r\zeta^{rp^f} \pmod{p} \\ &\equiv \beta \pmod{p} \end{aligned}$$

Therefore $\beta^{p^f} \equiv B \pmod{Q}$ because $Q|(p)$.

□

5 Class Groups

Let k be a number field.

Definition 5.1. $\mathcal{I}_k$ = {*non-zero fractional ideals in* k}

$\mathcal{I}$ is a group under multiplication of fractional ideals..

A principal ideal is one of the form:

$$(\beta) = \{\beta\gamma : \gamma \in \mathcal{O}_k\} \quad (\beta \in k)$$

$$(\beta_1)(\beta_2) = (\beta_1\beta_2)$$

Let $\mathcal{P}_k$ be the set of principal fractional ideals, $\mathcal{P}$ is a subgroup.

The class group of k is $Cl_k = \mathcal{I}_k/\mathcal{P}_k$. Elements of the class group are called ideal closure.

If I and J are in the same ideal class we'll write $I \sim J$. This is equivalent to saying $I = (\beta)J$ for some $\beta \in k^\times$.

If $\mathcal{O}_k$ is PID $\iff$ $Cl_k = \{1\}$ then factorisation of elements is unique. So the size of the class group tells us how far $\mathcal{O}_k$ is from having unique factorisation or being PID.

Recall $x^5 = y^2 + 33$, if (x, y) is any solution in integers then $(y + \sqrt{-33}) = I^5$ for some ideal I. It would be nice to be able to say that I is a principal ideal.

$I^5 \sim (1)$ in Cl_k so the ideal class of I has order 1 or 5 in Cl_k. If Cl_k has no elements of order 5 then $I \sim (1)$ so I is a principal ideal.

Theorem 5.2. *Cl_k is finite, then there exists a constant M_k depending only on k.*

Lemma 5.3. *Let I be a non zero ideal of $\mathcal{O}_k$ then there exists $\beta \in I$ such that $|N(\beta)| \leq M_k N(I)$*

Proof. Theorem 5.2

We'll show that every ideal class contains an ideal with norm $\leq M_k$. Since there are only finitely many ideals with a specific norm, there are only finitely many ideal classes.

Let I be a fractional ideal, $(\beta)I \subseteq \mathcal{O}_k$ for some non-zero $\beta \in \mathcal{O}_k$.

Since $I \sim (\beta)I$ every ideal class contains an ideal. Let J be an ideal in the class of I^{-1}.

By the key lemma, there exists $\beta \in J$, $\beta \neq 0$ such that $|N(\beta)| \leq M_k N(J)$.

Since $\beta \in J$, $(\beta) \subseteq J \implies J|(\beta) \implies (\beta) = J * I'$ for some ideal I'.

This means $I'J \sim (1)$ so $I' \sim J^{-1} \sim I$ and $N(I') = \frac{N\left((\beta)\right)}{N(J)} \leq M_k$

□

5.1 How to Calculate the Class Group

First we need to know the constant M_k.

$$M_k = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d}\sqrt{|\Delta|} \quad d = [k:\mathbb{Q}], \text{ Minkowski bound}$$

Δ is the discriminant of the integral basis
s is the number of pairs of complex field embeddings / roots of $m_\alpha(x)$

If $\sigma_1, \dots, \sigma_d : k \hookrightarrow \mathbb{C}$, reorder these so that $\sigma_1, \dots, \sigma_r : k \hookrightarrow \mathbb{R}$. Call these real embeddings. Similarly, $\sigma_{r+1}, \dots, \sigma_{r+s} : k \hookrightarrow \mathbb{C}$ such that:

$$\sigma_{r+s+1} = \bar{\sigma}_{r+1}$$
$$\vdots$$
$$\sigma_{r+2s} = \bar{\sigma}_{r+s}$$

Call these complex embeddings. Note that these complex embeddings are in complex conjugate pairs.

E.g. $k = \mathbb{Q}(\sqrt{5})$, $s \equiv 1 \pmod 4$ so $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $\Delta = 5$, $d = 2$, $s = 0$.
Then $M_k = \frac{2!}{2^2}\sqrt{5} = \sqrt{\frac{5}{4}} < 2$.

We showed that ever ideal class contains an ideal with norm $< M_k$. In this case the only ideal with norm $< M_k$ is (1), therefore $Cl_k = \{(1)\}$
So $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ is a UFD and a PID.

E.g. $k = \mathbb{Q}(\sqrt{-5})$, $\Delta = -20$.

Then $M_k = \frac{4}{\pi}^1 \frac{2!}{2^2}\sqrt{20} = \frac{\sqrt{80}}{\pi} < \frac{9}{\pi} < 3$.

So every ideal class contains an ideal of norm 1 or 2. (1) has norm 1.

$x^2 + 5 \equiv (x+1)^2 \pmod 2$ which means $(2) = P_2^2$ and $N(P_2) = 2$ where $P_2 = (2,, \sqrt{-5}+1)$.

So the ideals with norm $< M_k$ are $(1), P_2$.

Since $N(x + y\sqrt{-5}) = x^2 + 5y^2 \neq 2$, there are no elements of norm 2 so $P_2 \not\sim (1)$ and $Cl_k = \{(1), P2\}$. This is a cyclic group of order 2 and not a PID.

In many cases we can show that $\mathcal{O}$ is a PID, to do this, we just show that each ideal with norm M_k is principal, equivalently, any maximal ideals with norm M_k is principal.

E.g. $k = \mathbb{Q}[\sqrt{6}]$, $\Delta = 24$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{6}]$, $d = 2$, $s = 0$

$M_k = \frac{4}{\pi}\frac{2!}{2^2}\sqrt{24} = \sqrt{6} < 3$.

This means every ideal class contains an ideal or norm 1 or 2.

$2|24$ so $(2) = P_2^2$ and the ideals of norm 1 or 2 are $(1), P_2$.

Now we need to check if P_2 is a principal ideal.

$N(x + y\sqrt{6}) = x^2 - 6y^2$
$N(2 + \sqrt{6}) = -2$
So $P_2 = 2 + \sqrt{6} \implies P_2 \sim (1)$ and $Cl_k = \{(1)\}$.

If we want to show whether $|x^2 - 6y^2| = n$ has a solution, this is equivalent to asking whether there is an ideal of norm n.

We can check this by factorising n and using the decomposition theorem.

E.g. $k = \mathbb{Q}(\sqrt[3]{2})$, $\mathcal{O} = \mathbb{Z}[\sqrt[3]{2}]$, $m(x) = x^3 - 2$, $s = 1$, $d = 3$

$\Delta = 27b^2 - 4a^3 = -108$ so 2 and 3 will be ramified.

$M_k = \frac{4}{\pi} * \frac{3!}{3^3}\sqrt{108} < \frac{4*2*11}{\pi*3^2} < 4$

x	$x^3 - 2$	$(x - \alpha)$
0	-2	P_2
1	-1	(1)
-1	-3	P_3

$$\begin{aligned} m(x) = x^3 - 2 &\equiv x^3 \quad (2) & (2) &= P_2^3 \text{ where } P_2 = (0 - \alpha) \sim (1) \\ &\equiv (x+1)^3 \quad (3) & (3) &= P_3^3 \text{ where } P_3 = (-1 - \alpha) \sim (1) \end{aligned}$$

All ideals of norm < 4 are principal ideals so $\mathbb{Z}[\sqrt[3]{2}2]$ is a PID.

This allows us to solve $\det \begin{pmatrix} x & 2z & 2y \\ y & x & 2z \\ z & y & x \end{pmatrix} = n$

Consider $x^3 = y^2 + y + 8 = (y + \alpha)(y + \bar{\alpha})$ for $\alpha = \frac{1+\sqrt{-31}}{2}$. Show that the ideals $(y + \alpha)(y + \bar{\alpha})$ are coprime as ideals then using the "Ideal Descent Lemma", $(y + \alpha) = I^3$ for some ideal I.

5.2 Ideal Descent Lemma

Lemma 5.4. *Suppose $I, J, K \subseteq \mathcal{O}_k$ are ideals $IJ = K^n$ for I, J coprime. Then $I = I_0^n$ and $J = J_0^n$ for some ideals I_0, J_0.*

E.g. Suppose that $y + \alpha = (a + b\alpha)^3 = a^3 + 3a^2b\alpha + 3ab^2(\alpha - 8) + b^3(-7\alpha - 8)$ for $a, b \in \mathbb{Z}$.

Consider $x^3 = y^2 + y + 8$ and $1 = 3a^2b + 3ab^2 - 7b^3$.

$b|1$ so if $b = 1 \implies 3a^2 + 3a - 8 = 0$ ↯

If $b = -1$:

$$\begin{aligned} -3a^2 + 3a + 6 &= 0 \\ a^2 - a - 2 &= 0 \\ (a-2)(a+1) &= 0 \\ a &= 2, -1 \end{aligned}$$

$\implies x = 1, y = 31$ or $x = 10, y = -32$

We missed the solution $x = 2, y = 0$ and $x = 2, y = -1$. We missed it because we assumed that if $y + \alpha = I^3$ then I must be a principal ideal. I can be an element of order 3 in the class group.

E.g. $k = \mathbb{Q}(-\sqrt{3})$, $\mathcal{O}_k = \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{-31}}{2}$.

We'll calculate the class group.

$d = 2$, $s = 1$, $\Delta = 31$

$M_k = \left(\frac{4}{\pi}\right)\left(\frac{2!}{2^2}\right)\sqrt{31} = \frac{2}{\pi}\sqrt{31} < 4$

$$\begin{aligned} m(x) &= x^2 - x + 8 \\ &\equiv x(x+1) \ \ (2) \end{aligned}$$

irreducible mod 3 (from the table)

x	$x^2 - x + 8$
0	8
1	8
2	10=2*5

Ideals of norm $< M_k$ are $(1), P_2, P_2'$ where $P_2 = (2, \alpha)$ and $P_2' = (2, \alpha + 1)$.

$N(x + y\alpha) = x^2 + xy + 8y^2 \geq 7y^2$.

If $N(x + y\alpha) \leq 6$ then $y = 0 \implies$ no elements of norm 2.

Suppose $P_2 \sim P_2'$, $P_2 P_2' = (2) \sim (1)$.

There are no elements of norm 2 so if $P_2 \sim P_2'$ then $P_2^2 \sim (1)$.

The only elements of norm 4 are ± 2. These generate $(2) = P_2 P_2'$ not P_2^2

	(1)	P_2	P_2'
(1)	(1)	P_2	P_2'
P_2	P_2	P_2'	(1)
P_2'	P_2'	(1)	P_2

5.3 Calculating Class Groups

E.g. $k = \mathbb{Q}(\sqrt{10})$, $\quad \mathcal{O} = \mathbb{Z}[\sqrt{10}]$, $\quad m(x) = x^2 - 10$

$\Delta = 4 * 10 = 40$, $\quad d = [k : \mathbb{Q}] = 2$, $\quad s = 0$

$M_k = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d} \sqrt{|\Delta|} = 10 < 4$

Every ideal class contains an ideal with norm < 4

x	$x^2 - 10$	$(x^2 - \sqrt{10})$
0	-10 = 2*5	
± 1	-9 = -3*3	
+2	-6 = 2*3	$P_2 P_3$
-2	-6 = 2*3	$P_2 P_3'$
± 3	-1	
± 4	6=2*3	

$$\begin{aligned} m(x) &= x^2 \ \ (2) \\ &\equiv (x+1)(x-1) \ \ (3) \end{aligned}$$

This means $(2) = P_2^2$, $(3) = P_3 P_3'$ where $P_2 = (2, \sqrt{10})$, $P_3 = (3, \sqrt{10} + 1)$ and $P_3' = (3, \sqrt{10} - 1)$.

So the relations in the class group are:

$$\begin{aligned} P_2^2 &\sim (1) & P_2 &\sim P_2^{-1} \\ P_3 P_3' &\sim (1) & P_3' &\sim P_3^{-1} \\ P_2 P_3 &\sim (1) & P_2 &\sim P_3^{-1} \sim P_3' \\ P_2 P_3' &\sim (1) & P_2 &\sim P_3'^{-1} \end{aligned}$$

There are at most 2 ideal classes, $1, P_2$.

Remains to check whether $P_2 \sim (1)$ or not, check whether P_2 is a principal ideal.

Suppose $N(x + y\sqrt{10}) = \pm 2, \quad x^2 - 10y^2 = \pm 2 \implies x^2 \equiv \pm 2 \ \ (5)$, which has no solutions. $\lightning$

$P_2 \nsim (1) \implies Cl_k = \{(1), P_2\}$

E.g. $k = \mathbb{Q}(-\sqrt{-30}, \quad \mathcal{O}_k = \mathbb{Z}[-\sqrt{-30}]$

$\Delta = -120, \quad d = [k : \mathbb{Q}] = 2, \quad s = 1$

Note that $2, 3, 5$ are ramified.

$M_k = \left(\frac{4}{\pi}\right) * \frac{1}{2}\sqrt{120} = \frac{2*\sqrt{120}}{\pi} < \frac{2*11}{3} < 8$

$m(x) = x^2 \ \ (2), (3), (5)$ and is irreducible mod 7.

x	$x^2 + 30$	$(x - \sqrt{30})$
0	30 = 2*3*5	$P_2 P_3 P_5$
± 1	31	
± 2	34 = 2*17	
± 3	39 = 3*13	

This means $(2) = P_2^2, \quad (3) = P_3^2, \quad (5) = P_5^2$ and (7) is prime with norm 49.

The ideals with norm $< M_k$ are $(1), P_2, P_3, P_2^2 \sim (1), P_5, P_2P_3$. Then $|Cl_k| \leq 5$.

Relations in the class group are:

$$\begin{aligned} P_2^2 \sim P_3^2 \sim P_5^2 &\sim (1) \\ P_2P_3P_5 &\sim (1) \\ P_2P_3 \sim P_5^{-1} &\sim P_5 \end{aligned}$$

So Cl_k has at most 4 elements, $(1), P_2, P_3, P_5$.

Are any of these equivalent? $N(x + y\sqrt{-30}) = x^2 + 30y^2 \neq 2, 3, 5, 6, 10, \ldots$

$P_2 \not\sim (1)$, $P_3 \not\sim (1)$, $P_5 \not\sim (1)$, $P_2P_3 \sim (1)$.
Using these relations, we can then determine that $P_2 \sim P_3^{-1}$, $P_2 \not\sim P_3$.

Also $P_2^2 \sim (1)$ so P_2 has order 2 in Cl_k, therefore $|Cl_k|$ is even and $Cl_k = 4$.
So $Cl_k = \{(1), P_2, P_3, P_5\}$ and the group table is:

	(1)	P_2	P_3	P_5
(1)	(1)	P_2	P_3	P_5
P_2	P_2	(1)	P_5	P_3
P_3	P_3	P_5	(1)	P_2
P_5	P_5	P_3	P_2	(1)

E.g. $k = \mathbb{Q}(\sqrt{-29}$, $\quad \mathcal{O}_k = \mathbb{Z}[\sqrt{-29}]$, $\quad m(x) = x^2 + 29$,
$\Delta = -116$, $d = 2$, $s = 1$

$M_k = \left(\frac{4}{\pi}\right)\frac{1}{2}\sqrt{16} < 8$

x	$x^2 + 29$	$(x - \sqrt{29})$
0	24	
1	30 = 2*3*5	$P_2P_3'P_5'$
-1	30 = 2*3*5	$P_2P_3'P_5$
±2	33=3*11	
±3	38 = 2*19	

$$\begin{aligned} m(x) &\equiv (x+1)^2 \quad (2) \\ &\equiv (x+1)(x-1) \quad (2) \\ &\text{irreducible mod 7} \end{aligned}$$

This means $(2) = P_2^2$, $(3) = P_3P_3'$, $(5) = P_5P_5'$ and (7) is prime with norm 49 where
$P_3 = (3, \sqrt{-29} + 1)$
$P_3' = (3, \sqrt{-29} - 1)$

$P_5 = (5, \sqrt{-29} + 1)$
$P_5' = (5, \sqrt{-29} - 1)$
The ideals with norm < 8 are: $(1), P_2, P_3, P_3', P_2^2 \sim (1), P_5, P_5', P_2P_3, P_2P_3'$.
We know $|Cl_k| \leq 8$, this must mean that there must be classes in the class group which are equivalent to each other, find these by determining the relations between them.

$$\begin{array}{rr} P_2^2 \sim (1) & P_2P_3P_5 \sim P_2P_3'P_5' \sim (1) \\ P_3P_3' \sim (1) & P_2P_3 \sim P_5'^{-1} \sim P_5 \\ P_5P_5' \sim (1) & P_2P_3 \sim P_5^{-1} \sim P_5' \end{array}$$

So $|Cl_k| \leq 6$.

$N(x + y\sqrt{-29}) = x^2 + 29y^2 \neq 2, 3, 5, 6$
The additional relations are:

$$\begin{array}{rrrr} P_2 \sim (1) & P_3' \nsim (1) & P_2P_3 \nsim (1) & P_2P_3 \nsim (1) \\ P_3 \nsim (1) & P_5 \nsim (1) & P_3 \nsim (1) & P_2 \nsim P_3 \\ P_5 \nsim (1) & & & \end{array}$$

$P_2P_5' \nsim (1)$ so $P_5P_5' \sim P_2$.

The remaining ideal classes are $(1), P_2, P_3, P_3', P_5, P_5'$.
We have at least 3 ideal classes because $(1), P_2, P_3$ are all distinct, $P_2^2 \sim (1)$ so P_2 has order 2 therefore $|Cl_k| = 4$ or 6.

$P_3P_5, P_3'P_5, P_3, P_5', P_3'P_5'$ are not principal.

$\therefore P_5, \nsim P_3'$

So we have at least 4 distinct ideal closures, $(1), P_2, P_3, P_5$
Is $P_3 \sim P_3'$?
This would mean $P_3^2 \sim (1)$.

Elements of norm 9 are ± 3, these generate P_3P_3' so $P_3^2 \nsim (1)$ and $|Cl_k| = 6$

We know that $P_2P_3P_5 = (1 + \sqrt{-29})$ and $P_2P_3P_5' = (1 - \sqrt{29})$. So,

$$P_2P_3 \sim P_5^{-1} \sim P_5' \qquad P_3P_5 \sim P_2 \qquad P_3'P_5 \sim P_2$$

This means $P_3^2 \sim P_3'$ or P_5. Suppose $P_3^2 \sim P_3' \sim P_3^{-1}$ then $P_3 \sim (1)$ which is a contradiction since there are no elements of norm 3.

Also note that there is an element of norm 45, $(4 + \sqrt{-29}) = P_3^2 * P_5'$ so $P_3^2 \sim P_5'^{-1} \sim P_5$.

This results in the group table:

	1	P_2	P_3	P_3'	P_5	P_5'
1	(1)	P_2	P_3	P_3'	P_5	P_5'
P_2	P_2	(1)	P_5'	P_5	P_3'	P_2
P_3	P_3	P_5'	P_5	(1)	P_2	P_3'
P_3'	P_3'	P_5	(1)	P_5'	P_3	P_2
P_5	P_5	P_3'	P_2	P_3	P_5'	(1)
P_5'	P_5'	P_3	P_3'	P_2	(1)	P_5

Consider the minimal polynomial $x^2 - x + 41$, for $x = 0, \dots, 40$, the numbers are all prime. For $m(41) = 41^2$ it is not prime.

x	$m(x)$
0	41
1	41
-1,2	43
-2,3	47
-3,4	53
-4,5	61

Gauss discovered that $Cl_k = \{(1)\}$ in several complex quadratic fields, the last of these is $k = \mathbb{Q}(\sqrt{-163})$.

Gauss conjectured that this is the last one which is now proved.

$-163 \equiv 1 \ \ (4)$ so $\mathcal{O}_k = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-163}}{2}$

α has minimal polynomial $m(x) = x^2 - x + 41$. It's easy to show that this is a UFD.

$s = 1$, $d = 2$, $\Delta = -163$

$M_k = \left(\frac{4}{\pi}\right) * \frac{1}{2}\sqrt{163} = \frac{2\sqrt{163}}{\pi} < \frac{2*13}{3} < 9.$

From the table 2,3,5,7 are inert ideals of norm < 9.

$(1), (2)$ are both principle ideals so $Cl_k = \{(1)\}$.

We'll now see that $Cl_k = (1)$, the other values $m(x)$ for $x \leq 40$ are also prime. Suppose that $m(x)$ factorises, let p be a prime factor.

$p \leq \sqrt{m(x)} < \sqrt{41^2}$ so $p < 41$.

Therefore $m(x)$ has a root mod p so there is an ideal Q with norm p.

This must be a principal ideal since $Cl_k = \{(1)\}$, there is an element of norm $p < 41$.

$$\begin{aligned} N(x + y\alpha) &= x^2 - xy + 41y^2 \\ &= (x - \frac{1}{2}y)^2 + (41 - \frac{1}{4}y)^2 \end{aligned}$$

If $y \neq 0$ then this is $\geq 41 - \frac{1}{4}$ ↯so this is not p.

If $y = 0$ then this is x^2 so this is not p.

No element has norm a prime number < 41 ↯

$m(x)$ is prime $x = 1, 2, \ldots, 40$. Suppose $m(x)$ factorises let p be a prime factor $p \leq \sqrt{m(x)} < \sqrt{41^2}$

5.4 Using Class Groups in Diophantine Equations

E.g. $x^3 = y^2 + 13 = (y + \alpha)(y - \alpha)$ for $\alpha = \sqrt{-13}$.
Want to show that $(y + \alpha), (y - \alpha)$ are coprime as ideals.

If $\mathbb{Z}[\sqrt{-13}]$ isn't a UFD $\implies$ cannot use the Descent Lemma.

By the Ideal Descent Lemma, $(y + \alpha) = I^3$ for some ideal.

$I^3 \sim (1)$ so I has order 1 or 3 in Cl_k.

If Cl_k has no elements of order 3 then $I \sim (1)$.

Why are $(y + \alpha), (y - \alpha)$ coprime ideals?

Let P be a common factor which is a prime ideal, so $y + \alpha, y - \alpha \in P \implies 2\alpha \in P$.

Since $P | y + \alpha, y - \alpha$, this means $P | 2\alpha$ and $P | (2\alpha)$ and $N(P) | N(2\alpha) = 4 * 13$.

If $2 | N(P)$, $(P) | (y + \alpha)$ and $N(P) | N(y + \alpha) = x^3$ then $2 | x^3$ which implies $2 | x$.

So $y^2 + 13 \equiv 0 \;\; (8) \implies y^2 \equiv -1 \;\; (4)$ ↯

If $13 | N(P)$ then $13 | x$ by a similar argument and $y^2 + 13 \equiv 0 \;\; (13^2)$ which is irreducible mod 13^2. ↯

Calculating the class group: $M_k = \left(\frac{4}{\pi}\right) * \frac{1}{2}\sqrt{52} < \frac{2*8}{3} < 6$

x	$x^2 + 13$
0	13
± 1	14=2*7
± 2	17
± 3	22=2*11

$m(x) \equiv (x + 1)^2 \;\; (2)$ and irreducible mod 3,5

$(2) = P_2^2$ and so the ideals with norm < 6 are $(1), P_2, (2)$.

$|Cl_k| \leq 2$
$N(x + y\sqrt{-13}) = x^2 + 13y^2 \neq 2 \implies P_2 \not\sim (1)$

So $|Cl_k| = 2$.

So there are no elements of order 3, $I^3 \sim (1) \implies I \sim (1)$ so I is a principal ideal as $y + \alpha = (r + s\alpha)^3$.

As elements $y + \alpha = \text{unit} * (r + s\alpha)^3$.

The units in $\mathbb{Z}[\sqrt{-13}]^\times$ are $\{\pm 1\}$.

Every unit is a cube so without loss of generality $y + \alpha = (r + s\alpha)^3$ resulting in the equation:

$$y + \alpha = r^3 + 3r^2 s\alpha + 3rs^2(-13) - 135s^3\alpha$$

$$y = r^3 - 39rs^2 \qquad\qquad \begin{aligned} 1 &= 3r^2 s - 135s^3 \\ &= (3r^2 - 13rs^2)s \\ \implies s &= \pm 1 \end{aligned}$$

If $s = 1, \implies 3r^2 = 14 \lightning$

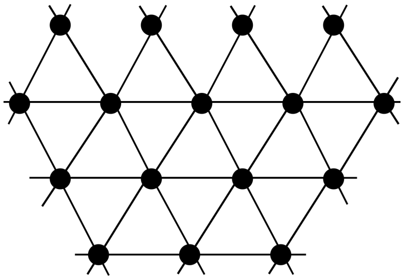
If $s = -1$, $\implies 3r^2 = 12$ and so $r = \pm 2$.

So the final solutions to the equation are $(x, y) = (17, \pm 70)$.

5.5 Geometry of Numbers

(Never understood this chapter so expect a lot of typos)

Let $V = \mathbb{R}^d$ and $\mathcal{B} = \{b_1, \ldots, b_d\}$ be a basis for V. The lattice spanned by $\mathcal{B}$ is $L = Span_{\mathbb{Z}}(\mathcal{B}) = \{x_1 b_1 + \cdots + x_d b_d : x_i \in \mathbb{Z}\}$



Example lattice with two basis vectors.

Also let the fundamental cell $P = \{\sum x_i b_i : x_i \in [0, 1)\}$. We can think of P as a set of coset representatives for L in V, every $v \in V$ is congruent mod L to a unique point in P.

$Vol(p) = |\det(b_1 \ldots b_d)|$ is called the covolume of L.

Lemma 5.5. *Suppose $U \subseteq V$ with $Vol(U)$ well defined if $Vol(U) > Vol(P)$ then there exists $u, v \in U$ $u \neq v$ such taht $u - v \in L$.*

$U = \bigcup_{l \in L} U_l$ where $U_l = U \cap (P + l)$

Proof. Suppose $u \not\equiv v \ \ (l)$ for all $u, v \in U$, $u \neq v$. Therefore $U_l - l \cap (U_m - m) = \emptyset$ for $l, m \in L$.

Then $Vol(u) = \sum Vol(U_l) = \sum Vol(u_l - l) = Vol(\bigcup_{l \in L}(u_l - l)) \leq Vol(P) \lightning$ □

Definition 5.6. *A subset $U \leq V$ is convex if for all $u, v \in U$, $\lambda \in [0, 1]$ $\lambda u + (1 - \lambda)v \in U$*

Definition 5.7. *A subset $U \leq V$ is symmetric if for all $u \in U$, $-u \in U$*

5.5.1 Minkowski's Lemma

Lemma 5.8. *Suppose $U \subseteq V$ is convex and symmetric and $Vol(U) > 2^d Vol(P)$, then U contains a non-zero point of L.*

Proof. $Vol(U) > 2^d Vol(P) = Vol(2P)$

$2P$ is the fundamental cell for the lattice $2L = \{2l : l \in L\}$.

By the previous lemma, there exists $u, v \in U$ such that $u - v \in 2L$ $(u \neq v)$.

U symmetric $\implies -V \in U$ and U convex $\implies \frac{U-V}{2} \in U$, $U - V \in U$ but $U - V \in 2L$ so $\frac{U-V}{2} \in L$. □

What does this have to do with Algebraic Number Theory?

Want to think of I (an ideal) as a lattice in some vector space. Minkowski's lemma will show that I contains some non-zero element of a big enough convex symmetric set. Choose a convex symmetric set where we have a bound on the norm.

5.5.2 Minkowski Space

Let k be an algebraic number field, we have field embeddings:

$$\begin{aligned} \sigma_1, \dots \sigma_r &: k \hookrightarrow \mathbb{R} & \qquad \sigma_{r+s+i} = \bar{\sigma}_{r+i} \\ \sigma_{r+1}, \dots \sigma_{r+s} &: k \hookrightarrow \mathbb{C} \end{aligned}$$

Define $k_\infty = \mathbb{R}^r \times \mathbb{C}^s$ as the Minkowski space. There is a map $\underline{\sigma} : k \hookrightarrow k_\infty$ by:

$$\begin{aligned} \beta \mapsto & \sigma_1(\beta) \\ & \vdots \\ & \sigma_r(\beta) \\ & \sigma_{r+1}(\beta) \\ & \vdots \\ & \sigma_{r+s}(\beta) \end{aligned}$$

We'll use $\underline{\sigma}$ to think of k as a subset of $k\infty$

Lemma 5.9. *Suppose β is a basis for k over $\mathbb{Q}$. Then $\underline{\sigma}(\beta)$ is a basis for k_∞ over $\mathbb{R}$. The lattice generated by $\underline{\sigma}(\beta)$ has covolume $2^{-s}\sqrt{|\Delta\beta|}$*

Proof. If $s = 0$ (i.e. all field embeddings are real) then this is very easy.

$$\textit{covol} = |\det\Big(\sigma(b_1)\dots\sigma(b_d)\Big)| \qquad \text{for } \mathcal{B} = \{b_1, \dots, b_d\}$$

Just knowing that this determinant is $\neq 0$ proves that $\sigma(b_1), \dots, \sigma(b_d)$ is a basis so just need to prove formula for covolume.

Recall $\Delta = \det(\sigma_i(b_j))^2 = (covol)^2$ as long as $s = i$.

$$covolume = |\det \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_d(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ Re(\sigma_{r+1}(b_1)) & \dots & Re(\sigma_{r+1}(b_d)) \\ Im(\sigma_{r+1}(b_1)) & \dots & Im(\sigma_{r+1}(b_d)) \\ \vdots & & \vdots \\ Re(\sigma_{r+s}(b_1)) & \dots & Re(\sigma_{r+s}(b_d)) \\ Im(\sigma_{r+s}(b_1)) & \dots & Im(\sigma_{r+s}(b_d)) \end{pmatrix} |$$

Add $i*$ row $Im(\sigma_{r+1})$ to row $Re(\sigma_{r+1})$:

$$= |\det \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_d(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \dots & \sigma_{r+1}(b_d) \\ Im(\sigma_{r+1}(b_1)) & \dots & Im(\sigma_{r+1}(b_d)) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \dots & \sigma_{r+s}(b_d) \\ Im(\sigma_{r+s}(b_1)) & \dots & Im(\sigma_{r+s}(b_d)) \end{pmatrix}$$

$$= 2^{-s} |\det \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_d(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \dots & \sigma_{r+1}(b_d) \\ -2Im(\sigma_{r+1}(b_1)) & \dots & -2Im(\sigma_{r+1}(b_d)) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \dots & \sigma_{r+s}(b_d) \\ -2Im(\sigma_{r+s}(b_1)) & \dots & -2Im(\sigma_{r+s}(b_d)) \end{pmatrix} |$$

$$= 2^{-s} |\det \begin{pmatrix} \sigma_1(b_1) & \dots & \sigma_d(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & \dots & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \dots & \sigma_{r+1}(b_d) \\ \bar{\sigma}_{r+1}(b_1) & \dots & \bar{\sigma}_{r+1}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & \dots & \sigma_{r+s}(b_d) \\ \bar{\sigma}_{r+s}(b_1) & \dots & \bar{\sigma}_{r+s}(b_d) \end{pmatrix} |$$

$$= 2^{-s}\sqrt{|AB|}$$

□

Lemma 5.10. *Let $I \subseteq \mathcal{O}_k$ be a non-zero ideal. Then $\underline{\sigma}(I)$ is a lattice in k_∞ with covolume $2^{-s}N(I)\sqrt{|\Delta|}$, where Δ is the discriminant of an integral basis.*

Proof. Let $\mathcal{B}$ be an integral basis, $\mathcal{C}$ be a $\mathbb{Z}-basis$ for I, i.e. $I = Span_{\mathbb{Z}}(\mathcal{C})$

Let $c_i = \sum m_{ij} b_j$ for $m_{ij} \in \mathbb{Z}$ and $M = (m_{ij})$ the transition matrix.

$N(I) = |\mathcal{O}_k/I| = |\mathbb{Z}^d/M\mathbb{Z}^d| = |\det(M)|$

$\Delta(\mathcal{C}) = \det(M)^2 \Delta\mathcal{B} = N(I)^2\Delta\mathcal{B}$

$Covol(I) = 2^{-s}\sqrt{|\Delta\mathcal{C}|} = 2^{-s}N(I)\sqrt{|\Delta\mathcal{B}|}$

□

Definition 5.11. *Let* $u(a) = \{ \begin{pmatrix} x_1 \\ \cdots \\ x_r \\ z_1 \\ \cdots \\ z_s \end{pmatrix} \in k_\infty : \sum |x_i| + 2\sum |z_i| < a\}$

5.6 Messy Lemma

Lemma 5.12. *$u(a)$ is convex and symmetric and* $Vol(u(a)) = \dfrac{2^r(\frac{\pi}{2})^s a^d}{d!}$

Proof. Clearly symmetric, suppose $u = \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ z_1 \\ \vdots \\ z_s \end{pmatrix}$ and $v' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_r \\ z'_1 \\ \vdots \\ z'_s \end{pmatrix}$

$u, v \in u(a)$

Let $\lambda \in (0,1)$. Need to show $\lambda u + (1-\lambda)v' \in u(a)$

$$\sum |x_i| + 2\sum |z_i| \leq a$$

$$\begin{aligned}
\sum |\lambda x_i + (1-\lambda)x'_i| + 2\sum |\lambda z_i + (1-\lambda)z_i| &\leq \sum |\lambda x_i| + 2\sum |\lambda z_i| + \sum |(1-\lambda)x'_i| + 2\sum |(1-\lambda)z'_i| \\
&\leq \lambda(\sum |x_i| + 2\sum |z_i|) + (1-\lambda)(\sum |x_i| + 2\sum |z'_i|) \\
&\leq \lambda a + (1-\lambda)a = a
\end{aligned}$$

Therefore $u(a)$ is convex.

□

Lemma 5.13. *Let I be a non-zero ideal then there exists $\beta \in I$ $\beta \neq 0$ such that $|N(\beta)| < M_k * N(I)$*

Proof. I is a lattice in k_∞ with covolume $2^{-s}\sqrt{|\Delta|}N(I)$, $u(a)$ is convex, symmetric with volume $\dfrac{2^r\frac{\pi}{2}^s a^d}{d!}$ as long as $Vol(u(a)) > 2^d covol(I)$, then there is a non-zero element of I in $u(a)$ by Minkowski's Lemma. Let's solve the inequality:

$$\begin{aligned}\frac{2^r\frac{\pi}{2}^s a^d}{d!} &> 2^d 2^{-s}\sqrt{|\Delta|}N(I)\\ a^d &> \frac{2^d 2^{-s} 2^{-r} 2^s d!}{\pi^s}\sqrt{|\Delta|}N(I)\end{aligned}$$

Since $d = r + 2s \implies d - r = 2s$, then

$$a^d > \frac{4}{\pi}^s d!\sqrt{|\Delta|}N(I)$$

If this is the case then we have an element $\beta \neq 0$, $\beta \in I$ such that $\beta \in u(a)$

$$\begin{aligned}\sum_{i=1}^{r}|\sigma_i(\beta)| + 2\sum_{i=1}^{s}|\sigma_{r+i}(\beta)| &\leq a\\ \sum_{i=1}^{d}|\sigma_i(\beta)| &\leq a\\ \frac{1}{d}\sum|\sigma_i(\beta)| &\leq \frac{a}{d}\end{aligned}$$

By the AM-GM inequality, $\sqrt[d]{\prod|\sigma_i(\beta)|} < \frac{a}{d}$.

Then $|N(\beta)| \leq \frac{a^d}{d^d}$, so there is an element $\beta \neq 0$ in I such that:

$$N(\beta) \leq \underbrace{\left(\frac{4}{\pi}\right)^s \frac{d!}{d^d}\sqrt{|\Delta|}}_{M_k} N(I)$$

□

ggwp