3704 Algebraic Number Theory Notes

Based on the 2012 spring lectures by Dr H Wilton

Algebraic Number Theory

Examples of Algebraic numbers

$\alpha = \sqrt{2},\ \sqrt[3]{2},\ \sqrt[7]{15},\ i$

$f(\alpha) = 0$ for some $f \in \mathbb{Z}[x]$ or $\mathbb{Q}[x]$

An algebraic number field:

eg. $\mathbb{Q}(\sqrt{2})$ = smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{2}$

$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

eg $\mathbb{Q}(i + \sqrt{2})$

$\sigma \subseteq k$ — algebraic intergers / algebraic number field

eg. $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Q}(\sqrt{2})$

Typical questions about σ

1. Does σ have unique factorisation?
2. Is σ a principle ideal domain?
3. If not, then how close it to being a PID?
4. How does a prime p factorise in σ?
   eg in $\mathbb{Z}[i]$, $5 = (2+i)(2-i)$, but 7 does not factorise?
5. What are the units of σ?
   eg in $\mathbb{Z}[\sqrt{2}]$ $(\sqrt{2}+1)(\sqrt{2}-1) = 1$
   $\mathbb{Z}[\sqrt{-5}]$ only 1 and -1 are units

Background Material

Rings - commutative, with 1

k - field

Rings of interest

1. $\mathbb{Z}$
2. $k[x] = \{f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in k\}$

i) units - invertible elements

ii) Reducible elements - $f = gh$, g, h non units

iii) Irreducible elements - everything else.

units of $k[x] = k^{*}$

3 Criteria for irreducibility of $f \in \mathbb{Q}[x]$

i) Gauss Lemma: If it is irreducible in $\mathbb{Z}[x]$, then f is irreducible in $\mathbb{Q}[x]$

Corollary: If f is monic and of deg 2 or 3 then if f is reducible it has a root in $\mathbb{Z}$, which has to divide the constant term of f

eg. x^3+x+1

ii) Eisenstein's criterion:

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

If there is a prime, $p \in \mathbb{Z}$ st

a) $p \mid a_i \quad i<n$

b) $p \nmid a_n$

c) $p^2 \nmid a_0$

then f is irreducible

iii) Reduction mod p

If $f \in \mathbb{Z}[x]$, 'denote' the map $\mathbb{Z}[x] \to (\mathbb{Z}/p)[x]$ by $f \to \bar{f}$

If $\deg f = \deg \bar{f}$ and $\bar{f}$ is irreducible in $(\mathbb{Z}/p)[x]$ then f is irreducible in $\mathbb{Z}[x]$.

Also note that $f \in \mathbb{Z}[x]$ is irreducible iff $f(x+a)$ is irreducible where $a \in \mathbb{Z}$

Euclid's Algorithm

If $f, g \in k[x]$, then we can write $f(x) = q(x)g(x) + r(x)$ where $\deg r < \deg g$

$hcf(f,g) = hcf(g,r) = hcf(h,0)$

Definition:

A ring with a euclidean algorithm is called a Euclidean ring
eg. $\mathbb{Z}$, $k[x]$.

Ideals

Definition:

$I \subseteq R$, $I \neq \emptyset$ is called an ideal if
- $x, y \in I \Rightarrow x+y \in I$
- $x \in I, \lambda \in R \Rightarrow \lambda x \in I$

Example

if $x \in R$, then $(x) = \{\lambda x \mid \lambda \in R\}$ principle ideal
Also $(x_1, \ldots, x_n) = \{\sum_{i=1}^{n} \lambda_i x_i \mid \lambda_i \in R\}$
eg $(4,6) \subseteq \mathbb{Z} = (hcf(4,6)) = (2)$

Definition:

If every ideal in R is principle then R is a PID.

Theorem:

Euclidean rings are principle ideal domains

Proof: $I \subseteq R$ ideal. Take $x \in I \setminus 0$ of minimal degree. Let $y \in I$.
Then $y = qx + r$, $\deg r < \deg x$ $r \in I \Rightarrow r = 0$

Definition:

An ideal $I \subseteq R$ is maximal if, for any ideal J such that
$I \subseteq J \subseteq R$ then either $I = J$ or $J = R$

Remark: $(a) \subseteq (b) \Leftrightarrow b \mid a$

Example: The maximal ideals in $\mathbb{R}[x]$ are all of the form (f) where f is an irreducible polynomial

if $(g) \neq$ where $g = hk$, then $(h) \supsetneq (g)$

Exercise: What are maximal ideals in $\mathbb{Z}$?

Definition:

Let I be an ideal.

Then $(I,+) \subseteq (R,+)$ is a subgroup

We can consider the group $R/I = \{x + I \mid x \in R\}$

- $(x+I)+(y+I) = (x+y)+I$ addition on R/I
- $(x+I)(y+I) = xy + I$ defines multiplication on R/I

R/I is the quotient ring.

Definition:

If R, S are rings, $\varphi : R \rightarrow S$ is a ring homomorphism if

i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$

iii) $\underset{R}{\varphi(1)} = \underset{S}{1}$

Exercise: $\ker\varphi = \{x \in R \mid \varphi(x) = 0\}$ is an ideal.

Lemma:

If R is a field and I is a ideal then $I = \{0\}$ or $I = R$.

Proof: If $x \in I \setminus \{0\}$. Let $y \in R$ arbitrarily. Then $(yx^{-1})x \in I$, $y \in I$ $\square$

Corollary: If $\varphi : R \rightarrow R$, is a ring homomorphism, R a field, R is a ring, then φ is injective.

Proof: $\varphi(1_R) = 1_R$ so $1_R \notin \ker\varphi \Rightarrow \ker\varphi \neq R$. Therefore $\ker\varphi = \{0\}$

Theorem:

An ideal $I \subseteq R$ is maximal iff R/I is a field.

Proof: $\Leftarrow$ Let $\varphi : R \to R/I$ be the quotient homomorphism
$x \mapsto x + I$
Suppose $I \subseteq J \subseteq R$. Then $\varphi(J) \subseteq R/I$ is an ideal (check).
By lemma $\varphi(J) = \{0\} \Rightarrow J = I$
or $\varphi(J) = R/I \Rightarrow J = R$
$\Rightarrow$ Suppose $I \subseteq R$ is maximal and consider $x \in R/I$
We need to show $x + I \in R/I$ has multiplicative inverse
The ideal generated by x and I is R
$1 \in R$. So, there is a $y \in R$ and a z in I st $yx + z = 1$
So $1 \in yx + I = (y+I)(x+I)$
Hence $x + I$ has a multiplicative inverse $\Rightarrow R/I$ is a field

Field Extensions

Definition:

If k, L are fields and $k \subseteq L$ then k is a subfield of L and L is an extension of k

eg. $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$
$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$k \subseteq L \subseteq \mathbb{C}$
This is a naturally occuring example
The fact that this definition depends on $\mathbb{C}$, is unsatisfactory.

Another example $\mathbb{Q}[x]/(x^2 - 2)$

Definition:

An element $\alpha \in L$ is algebraic over k if there exists $f(x) \in k[x]$ such that $f(\alpha) = 0$
Usually $k = \mathbb{Q}$

The ring generated by k and $\alpha \in L$ is denoted $k[\alpha] = \{f(\alpha) \mid f \in k[x]\}$

The field generated by k and $\alpha \in L$ is denoted $k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \middle| \begin{array}{l} f, g \in k[x] \\ g(\alpha) = 0 \end{array} \right\}$

Exercise: check equalities

$k \subseteq k[\alpha] \subseteq k(\alpha)$

Let $I(\alpha) = \{f \in k[x] \mid f(\alpha) = 0\}$.

Lemma:

$I(\alpha)$ is an ideal of $k[x]$

Proof: $f, g \in I(\alpha)$

$(f+g)(\alpha) = f(\alpha) + g(\alpha) = 0 + 0 = 0$

$f \in I(\alpha)$, $g \in k[x]$

$(gf)(\alpha) = g(\alpha) f(\alpha) = g(\alpha) 0 = 0$

$k[x]$ is a PID (it's a euclidean ring)

$I(\alpha) = (m)$

m is well defined up to multiplication by $\lambda \in k^{x}$, because its a minimal degree element of $I(\alpha)$

Definition:

The minimal polynomial of α, m_α, is the unique monic m_α, s.t $I(\alpha) = (m_\alpha)$.

Example: $\alpha = \sqrt{2}$ $k = \mathbb{Q}$ then $m_\alpha(x) = x^2 - 2$

Lemma:

$I(\alpha)$ is a maximal ideal or equivalently m_α is irreducible

Proof: Suppose m_α is reducible.

Then $m_\alpha(x) = a(x) b(x)$ $\Rightarrow$ $m_\alpha(\alpha) = a(\alpha) b(\alpha) = 0$

Therefore, wlog, $a(\alpha) = 0 \Rightarrow a \in I(\alpha) = (m)$

so $m_\alpha | a$, $\deg a = \deg m_\alpha$, so $b(x)$ is constant.
$b(x)$ is a unit in $k[x]$ and therefore m_α is irreducible

Lemma:

A polynomial m is the minimal polynomial of α iff
  i) $m(\alpha) = 0$
  ii) m is monic
  iii) m is irreducible

Proof: $\Rightarrow$ Already proved
$\Leftarrow$ i) $\Rightarrow m \in I(\alpha) = (m_\alpha)$
  $\Rightarrow m_\alpha | m$, ie $m = a m_\alpha$
iii) $a \in k^\times$
comparing highest degree coefficents, $x^n = a x^n \Rightarrow a = 1$
Therefore $m = m_\alpha$.

We just proved that $I(\alpha)$ is a maximal ideal, so $\underbrace{k[x]/I(\alpha)}_{= k[x]/(m_\alpha(x))}$ is a field

Theorem:

Let $\alpha \in L$ be algebraic over k.
Then, $\Phi : k[x]/(m_\alpha) \longrightarrow k(\alpha)$

$f + (m_\alpha) \longrightarrow f(\alpha)$

is a field isomorphism and $k[\alpha] = k(\alpha)$

Proof: First we need to check that Φ is well defined
Suppose $g \in f + (m_\alpha) \Leftrightarrow f - g \in (m_\alpha) \Leftrightarrow (f-g)(\alpha) = 0$
Then $\Phi(g + (m_\alpha)) = g(\alpha) = f(\alpha)$
$= \Phi(f + (m_\alpha))$

Next we should check that Φ is a ring homomorphism Exercise
ie $\Phi(f + g + (m_\alpha)) = \Phi(f + m_\alpha) + \Phi(g + m_\alpha)$, similarly for multi.
Notice that $\operatorname{im} \Phi = k[\alpha]$
But $k[x]/(m_\alpha)$ is a field, so Φ is naturally injective.

So we have

$$k[x]/_{(m_\alpha)} \cong \Phi\left(k[x]/_{(m_\alpha)}\right) \subseteq k[\alpha] \subseteq k(\alpha)$$

$\cup$ k, α

Therefore by definition of $k(\alpha)$ $\Phi\left(k[x]/_{(m_\alpha)}\right) = k[\alpha] = k(\alpha)$ $\square$?

It's normal to abuse notation and write f for $f + I \in k[x]/I$.

Example: $\alpha = \sqrt{2} + \sqrt{3}$.

Can talk about $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\alpha^2 = 5 + 2\sqrt{6}$ so $(\alpha^2 - 5)^2 = 24$

So α is a root of $\underset{m(x)=}{x^4 - 10x^2 + 1} = 0$

Need to show that m is irreducible

It could factorise quadratic $\times$ quadratic or $\underbrace{\text{linear}}_{\text{root which is } \pm 1}$ $\times$ cubic $\alpha(1), \alpha(-1) \neq 0$.

$$m(x) = (x^2 + ax + b)(x^2 + cx + d)$$
$$= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (bc+ad)x + bd.$$

Compare coefficents $a + c = 0 \Rightarrow a = -c$

$ac + b + d = -10 \Rightarrow a^2 = 10 + 2b = \underbrace{8 \text{ or } 12}_{\text{not squares}}$

$bc + ad = 0$

$bd = 1 \Rightarrow b = d \pm 1$

So m is irreducible.

Therefore $\mathbb{Q}[x]/_{(x^4 - 10x^2 + 1)} \cong \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$$f \longmapsto f(\sqrt{2}+\sqrt{3})$$

Degrees of Extensions

$L \supseteq k$

Recall that $l_1 + l_2$ makes sense and kl makes sense but forget that $l_1 l_2$ makes sense.

This realises L as a vector space over k.

Definition:

The degree of L over k is just $\dim L$, thought of L is a vector space over k. It is denoted $[L:k]$.

Example: $\mathbb{C} \supseteq \mathbb{R}$

$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$

$\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$

$[\mathbb{C}:\mathbb{R}] = 2$

Example: Let $f(x) = \sum_{i=0}^{d} a_i x^i$ be an irreducible polynomial over k

$L = k[x]/(f) \supseteq k$

A basis is $\{1, x, \dots, x^{d-1}\} = B$

$x^d = \frac{-1}{a_d} \sum_{i=0}^{d-1} a_i x^i \Rightarrow x^d \in \text{span } B$

Similarly $x^n \in \text{span } B$ for any $n \geq d$

$x^n = x^{n-d} x^d = x^{n-d} \left(\frac{-1}{a_d} \sum_{i=0}^{d-1} a_i x^i \right)$ is of degree $\leq n-1$

and so $x^n \in \text{span } B$ by induction.

But all $g \in \text{span}\{x^n \mid n \geq 0\} = \text{span}\{1, \dots, x^{d-1}\}$.

Suppose $g(x) = \sum_{i=0}^{d-1} b_i x^i = 0$

Then $g \in (f)$. But $\deg g \leq d-1 < d = \deg f$

$\Rightarrow g = 0 \Rightarrow b_i = 0$ for all i.

Therefore $[L:k] = \deg f$.

Therefore if $f = m_\alpha$ for some α algebraic over k, then $[k(\alpha):k] = \deg m_\alpha$

Proposition:

α is algebraic over k if and only if $[k(\alpha):k] < \infty$

Proof: $\Rightarrow$ $[k(\alpha):k] = \deg m_\alpha < \infty$

$\Leftarrow$ Suppose $[k(\alpha):k] = d < \infty$

Then $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^d$ is linearly dependent

$\Rightarrow \exists a_i$ st $\sum_{i=0}^{d} a_i \alpha^i = 0$ □

Tower Theorem:

Suppose $k \subseteq L \subseteq M$. Then $[M:k] = [M:L][L:k]$

Proof: Let $\{a_i\}$ be a basis for L over k
and $\{b_j\}$ be a basis for M over L
claim: $\{a_i b_j\}$ is a basis for M over k.
Proof of claim: Spanning: Let $v \in M$. Then $\exists \lambda_j \in L$ st $v = \sum_j \lambda_j b_j$
$\exists \mu_{ij} \in k$ st $\lambda_j = \sum_i \mu_{ij} a_i$ because $\lambda_j \in L$, so
$v = \sum_{i,j} \mu_{ij} a_i b_j$
Linear independence: Suppose $\sum_{i,j} \underset{\substack{\cap \\ k}}{m_{ij}} a_i b_j = 0$

Let $\lambda_j = \sum_i \overset{\substack{L \\ \cup}}{m_{ij}} a_i$. Then $\sum_j \lambda_j b_j = 0 \Rightarrow \lambda_j = 0$ for all j
so $m_{i,j} = 0$ for all i,j

Corollary:

Let $L \supseteq k$ and let $L^{alg} \subseteq L$ be the set of algebraic over k elements of L. Then L^{alg} is a field.

Proof: Let $\alpha, \beta \in L^{alg}$. Then $[k(\alpha,\beta):k] = \underbrace{[k(\alpha,\beta):k(\alpha)]}_{\leq [k(\beta):k]}[k(\alpha):k] < \infty$ (β still satisfies poly over k)

Let $\theta = \alpha+\beta, \alpha\beta, \alpha-\beta, \alpha/\beta \in k(\alpha,\beta)$
Now $[k(\alpha,\beta):k] = [k(\alpha,\beta):k(\theta)][k(\theta):k]$
Therefore $[k(\theta):k] < \infty$ so $\theta \in L^{alg}$ □

Example: What is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$?
Hopefully its still x^2-3.
Note that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$
$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$
Now $-9(\sqrt{2}+\sqrt{3})$, get $2\sqrt{2}$
$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = \deg(x^4-10x^2+1) = 4$
Therefore $4 = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{=2}$

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

Primative Element Theorem:

Suppose $k \subseteq L \subseteq \mathbb{C}$ and $[L:k] < \infty$. Then $\exists\, \theta \in L$ st $L = k(\theta)$

Proof will use...

Galois' seperability Theorem:

Let $k \subseteq \mathbb{C}$, $f \in k[x]$ irreducible. Then f does not have repeated roots in $\mathbb{C}$.

Proof: Suppose α is a repeated root. Then $f(x) = (x-\alpha)^2 g(x)$ in $\mathbb{C}[x]$

$f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha) g(x)$

$f'(\alpha) = 0$. Then $f' \in I(\alpha) = (f)$

But $\deg f' < \deg f \Rightarrow f' = 0$

Therefore f is constant, contradiction $\square$

Remark: This proof doesn't work over a finite field

eg. $\mathbb{F}_p$ $f = x^p - a$ $f' = px^{p-1} = 0$.

Proof of primative element theorem:

Let $\{1, \gamma_1, \dots, \gamma_{d-1}\}$ be a basis for L over k.

Then $L = k(\gamma_1, \dots, \gamma_{d-1}) = k(\gamma_1, \dots, \gamma_{d-2})k(\gamma_{d-1})$

By induction on d, may assume that $k(\gamma_1 \dots \gamma_{d-2}) = k(\alpha)$

Let $\gamma_{d-1} = \beta$.

Now $L = k(\alpha, \beta)$.

Let $p = m_\alpha$, $q = m_\beta$

Let $\alpha = \alpha_1, \dots, \alpha_m$ be roots of p

$\beta = \beta_1, \dots, \beta_n$ be roots of q

Choose $c \in k$ such that $\alpha_i + c\beta_j \neq \alpha + c\beta$ unless $i = j = 1$

To choose c we use:

i) k is infinite

ii) We have finitely many c's to avoid

iii) Galois' Sep Thm $\Rightarrow \alpha_i = \alpha_{i'} \Leftrightarrow i = i'$

$\beta_j = \beta_{j'} \Leftrightarrow j = j'$

Let $\theta = \alpha + c\beta$. We need to prove that $k(\theta) = k(\alpha, \beta)$

Claim: $\beta \in k(\theta) \Rightarrow \alpha = \theta - c\beta \in k(\theta)$

$\Rightarrow k(\alpha, \beta) \subseteq k(\theta) \subseteq k(\alpha, \beta)$

Proof of claim: Define $r(x) \in k(\theta)[x]$ by $r(x) = p(\theta - cx)$

Then $r(\beta) = p(\theta - c\beta) = p(\alpha) = 0$

On the other hand if $r(\beta_j) = p(\theta - c\beta_j) = 0$ for $j \geq 2$

$\Leftrightarrow \theta - c\beta_j = \alpha_i$ for some i

$\Leftrightarrow \alpha + c\beta = \alpha_i + c\beta_j$ which never happens by choice of c.

Now β satisfies two polynomials over $k(\theta)$, $q(\beta) = 0$ $r(\beta) = 0$

We have just seen that β is the only root that q and r have in common.

Let m be the minimal polynomial of β over $k(\theta)$

$m \mid q$ and $m \mid r$

So any root of m is a root of q and r. The only root of m is β.

So $m = (x - \beta)^d$

$d = 1$ by Galois' seperability Theorem $\Rightarrow m = x - \beta \Rightarrow \beta \in k(\theta)$ $\square$

Symmetric Polynomials.

$f(\underline{x}) \in k[x_1, \dots, x_n] \equiv k[\underline{x}]$

S_n = symmetric group on n objects acts:

$\sigma \in S_n$, $\sigma f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$

f is called if $\sigma f = f$ for all $\sigma \in S_n$

$K[\underline{X}]^{S_n} = \{\text{symmetric polynomials}\}$.

NB: If $f, g \in k[\underline{X}]^{S_n}$, $f + g \in k[\underline{X}]^{S_n}$ and $fg \in k[\underline{X}]^{S_n}$

eg. $X + Y$, $X^2 + 3XY + Y^2 \in \mathbb{Q}[X, Y]^{S_2}$

Definition:

Suppose $f(\xi)$ has roots $x_1, \dots x_n$. Then $f(\xi) = \prod_{i=1}^{n} (\xi - x_i)$

$$= \xi^n + \sum_{i=0}^{n-1} (-1)^{i+1} s_{n-i}(\underline{x}) \xi^i$$

(eg. $n = 3$ $(\xi - x)(\xi - y)(\xi - z) = \xi^3 - \overset{s_1}{(x + y - z)}\xi^2 + \overset{s_2}{(xy + yz + zx)}\xi - \overset{s_3}{xyz}$)

The polynomials $s_1, \dots, s_n$ are called the elementary symmetric polynomials in n variable

They enable us to write coefficents of a polynomial in terms of its coefficents

You can also define them as:

$s_1 = x_1 + x_2 + \dots + x_n$

$s_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n = \sum_{i,j} x_ix_j$

$\vdots$

$s_n = x_1 \cdots x_n = \prod_{j=1}^{n} x_j$

The Fundemental Theorem of Symmetric Polynomials
(aka Newton's Theorem)

$k[\underline{X}]^{S_n}$ is generated by k and $\{s_1, \dots, s_n\}$.

Suppose $f(x) \in \mathbb{Z}[x]$ with roots $\alpha_1, \dots, \alpha_n$.
Suppose $\beta \in \mathbb{Q}(\alpha_1, \dots \alpha_n)$ is invarient when you permute $\alpha_1, \dots, \alpha_n \rightsquigarrow \beta \in \mathbb{Q}$

Proof: $f \in k[\underline{X}]^{S_n}$. We want to find some polynomial g st
$f(\underline{X}) = g(s_1(\underline{X}), \dots, s_n(\underline{X}))$
We can break f up into homogeneous pieces.
ie sums of monomials of the same degree
If we can prove for these pieces, it follows for f.
So we may assume that f is homogeneous.
eg. $f = x^2 + y^2$ -homogeneous $f = (x^2+y^2) + (x+y)$ - not homogeneous

Step 1: Decree that $x_1 > x_2 > \dots > x_n$
Order monomials $x_1^{i_1} \dots x_n^{i_n}$ lexicographically.
$x_1^{i_1} \dots x_n^{i_n} > x_1^{j_1} \dots x_n^{j_n}$ iff the first non zero term of the list $i_1 - j_1, i_2 - j_2, \dots, i_n - j_n$ is positive
Because f is homogeneous this orders every pair of monomials.
It now makes sense to talk about the leading term of f
ie the 'biggest' monomial in f in the sense of the lexicographic ordering.
Denote the leading term of f as $a_{\underline{i}} x_1^{i_1} \dots x_n^{i_n}$

Step 2: Compute leading term of $s_1^{k_1}, s_2^{k_2}, \dots s_n^{k_n}$.

The leading term of a product is the product of the leading terms of the factors.

Leading term of $s_1 = x_1$

$$s_2 = x_1 x_2$$
$$s_3 = x_1 x_2 x_3$$
$$\vdots$$
$$s_n = x_1 \cdots x_n$$

The leading term of p is $x_1^{k_1}(x_1 x_2)^{k_2} \cdots (x_1 \cdots x_n)^{k_n}$
$$= x_1^{k_1+\dots+k_n} x_2^{k_2+\dots+k_n} \cdots x_n^{k_n}$$

I want to choose the k_j's such that this is equal to the leading term of f.

$k_1 + \dots + k_n = i_1 \Rightarrow k_1 = i_1 - i_2$

$k_2 + \dots + k_n = i_2 \Rightarrow k_2 = i_2 - i_3$

$k_3 + \dots + k_n = i_3 \Rightarrow k_3 = i_3 - i_4$

$\vdots$

$k_{n-1} + k_n = i_{n-1} \Rightarrow k_{n-1} = i_{n-1} - i_n$

$k_n = i_n$.

$h(x) =$ $s_1^{i_1-i_2} s_2^{i_2-i_3} s_3^{i_3-i_4} \dots s_n^{i_n}$ has the same leading term as f.

Step 3: Let $w(\underline{x}) = f(\underline{x}) - h(\underline{x})$

Then $w(x)$ has a smaller leading term

By induction $w(\underline{x})$ is a polynomial in the elementary symmetric polynomials

$\therefore f(\underline{x}) = w(\underline{x}) + h(\underline{x})$ is too.

Example: $\cancel{x^4+y^4+z^4}$ $\underline{x}^3 + y^3 + z^3$

$s_1 = x + y + z$

$s_2 = xy + yz + xz$

$s_3 = xyz$.

leading term x^3 = leading term of $s_1^{k_1} s_2^{k_2} s_3^{k_3}$ $\quad k_1 = i_1 - i_2 = 3$

$x^3 y^0 z^0 = (x+y+z)^3$ $\quad k_2 = i_2 - i_3 = 0$

next leading term.

$= x^3 + y^3 + z^3 + \Big[3(\underline{x^2 y} + y^2 z + z^2 x$ $\quad k_3 = i_3 = 0$

$+ xy^2 + yz^2 + zx^2)$

$+ 6xyz. \Big]$ f_2

leading term of $f_2 = 3x^2 y z^0$

f_2 has the same leading term as $3s_1^1 s_2^1 s_3^0$

$$3s_1^1 s_2^1 s_3^0 = 3(x+y+z)(xy+yz+zx)$$
$$= 3[x^2y + xyz + zx^2 + xy^2 + y^2z + xyz + xyz + yz^2 + z^2x]$$
$$= 3[\underline{\qquad} + \underline{\qquad}] + 9xyz$$
$$= f_2 + 3xyz$$

$$\left.\begin{aligned} s_1^3 &= f_1 + f_2 \\ 3s_1s_2 &= f_2 + 3s_3 \end{aligned}\right\} \Rightarrow f_1 = s_1^3 - f_2 = s_1^3 - (3s_1s_2 - 3s_3) = s_1^3 - 3s_1s_2 + 3s_3.$$

ALGERAIC NUMBER FIELDS

Field embeddings:

Definition:

An algebraic number field is a finite extension of $\mathbb{Q}$, ie an algebraic extension of $\mathbb{Q}$.

By primitive element theorem, such a thing is always of the form $\mathbb{Q}(\alpha)$

If $m = m_\alpha$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m$ and $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/m$
$$\alpha \mapsto x + (m)$$

Definition:

A field embedding of an algebraic number field k is a homomorphism $\sigma : k \to \mathbb{C}$.

NB σ is necessarily injective.

Lemma: If $\sigma : k \to \mathbb{C}$ is a field embedding and $x \in \mathbb{Q} \subseteq k$, then $\sigma(x) = x$

$$\begin{tikzcd} \mathbb{Q} \arrow[r, "\sigma|_{\mathbb{Q}} = \mathrm{id}"] \arrow[d] & \mathbb{Q} \arrow[d] \\ k \arrow[r, "\sigma"] & \mathbb{C} \end{tikzcd}$$

Proof: $\sigma(0) = 0$, $\sigma(1) = 1$

Now for any $x \in \mathbb{N}$, $\sigma(x) = \sigma(x-1) + \sigma(1)$
$$= \sigma(x-1) + 1$$
$$= (x-1) + 1 = x$$
by induction on x

$0 = \sigma(0) = \sigma(1+(-1)) = \sigma(1) + \sigma(-1) = 1 + \sigma(-1)$
$\Rightarrow \sigma(-1) = 0 - 1 = -1$
$\therefore$ If $x \in \mathbb{Z}$, $x < 0$ then $x = (-1)y$ for some $y \in \mathbb{N}$
$\sigma(x) = \sigma((-1)y) = \sigma(-1)\sigma(y) = (-1)y = -y$
If $x = a/b$, $a, b \in \mathbb{Z}$, then $bx = a \in \mathbb{Z}$

$$\left.\begin{array}{l}\sigma(bx) = \sigma(a) \\ \overset{\shortparallel}{\sigma(b)\sigma(x)}\end{array}\right\} \Rightarrow \sigma(x) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b} = x$$

Lemma:

If $f \in \mathbb{Q}[x]$ and $\sigma : K \to \mathbb{C}$ is a field embedding, then for any $x \in K$, $\sigma(f(x)) = f(\sigma(x))$

Proof: $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \in \mathbb{Q}$.

$$\sigma(f(x)) = \sigma\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \sigma(a_i x^i)$$

$$= \sum_{i=0}^{n} \sigma(a_i)\sigma(x)^i = \sum_{i=0}^{n} a_i \sigma(x)^i$$

$$= f(\sigma(x))$$

$L = \mathbb{Q}(\alpha)$. How many field embeddings $\sigma : K \to \mathbb{C}$ are there?

Lemma:

A field embedding σ $K = \mathbb{Q}(\alpha) \to \mathbb{C}$ is determined by $\sigma(\alpha)$

Proof: For any $x \in \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$, so $x = f(\alpha)$ for some polynomial $f \in \mathbb{Q}[x]$. Now $\sigma(x) = \sigma(f(\alpha)) = f(\sigma(\alpha))$ $\square$

$$x \in \mathbb{Q}(\alpha) \xrightarrow{\sigma} \mathbb{C}$$
$$x \longmapsto \sigma(x)$$

Definition:

Two algebraic numbers α, β are called $\mathbb{Q}$-conjugate, if they have the same minimal polynomial over $\mathbb{Q}$.

eg. $\sqrt{2}, -\sqrt{2}$

$\sqrt[3]{2}$ has $m = x^2 - 2$

This has over roots, $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, $\omega \notin \mathbb{R}$ satisfies $x^3 - 1 = 0$.

Lemma:

Let k be an algebraic number field.
If $\sigma : k \to \mathbb{C}$ is a field embedding and $x \in k$ then x and $\sigma(x)$ are $\mathbb{Q}$-conjugate

Proof:

Let $m = m_x$. Then $m(\sigma(x)) = \sigma(m(x)) = \sigma(0) = 0$
Because m is monic and irreducible, m is also the minimal polynomial of $\sigma(x)$. $\square$

Theorem:

Let k be an algebraic number field and let $d = [k : \mathbb{Q}]$. Then there are exactly d field embeddings, $\sigma_1, \ldots, \sigma_d : k \to \mathbb{C}$.

Proof: By primitive element theorem $k = \mathbb{Q}(\alpha)$ for some α.
Let $m = m_\alpha$ and let $\alpha = \alpha_1, \ldots, \alpha_d$ be the roots of m.
By Galois seperability theorem, $\alpha_1 \ldots \alpha_d$ are all distinct.
Let $\sigma_i : k \to \mathbb{C}$ be defined as follows:

$$k = \mathbb{Q}(\alpha) \xrightarrow[\text{because } m = m_\alpha]{\cong} \mathbb{Q}[x]/(m) \xrightarrow[\text{because } m = m_{\alpha_i}]{\cong} \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}.$$

$$\underbrace{\alpha \longmapsto x + (m) \longmapsto \alpha_i}_{\sigma_i}$$

Let $\sigma : k = \mathbb{Q}(\alpha) \to \mathbb{C}$ be any field embedding.
Then $\sigma(\alpha)$ is $\mathbb{Q}$-conjugate to α, so $\sigma(\alpha) = \underset{= \sigma_i(\alpha)}{\alpha_i}$ for some i
Because σ is determined $\sigma(\alpha)$, $\sigma = \sigma_i$ $\square$

Example: $k = \mathbb{Q}(\sqrt{2})$. The $\mathbb{Q}$-conjugates of $\sqrt{2}$ are $\{\sqrt{2}, -\sqrt{2}\}$
$m_{\sqrt{2}} = x^2 - 2$
The two embeddings $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ are $\sigma_1 : a + b\sqrt{2} \longmapsto a + b\sqrt{2}$
$\sigma_2 : a + b\sqrt{2} \longmapsto a - b\sqrt{2}$

Example: Let $k=\mathbb{Q}(\alpha)$, α root of $m(x)=x^3+2x+2$
Then $x\in\mathbb{Q}(\alpha)$ looks like $x=a+b\alpha+c\alpha^2$, for $a,b,c\in\mathbb{Q}$
because $\{1,\alpha,\alpha^2\}$ is a basis for k over $\mathbb{Q}$.
Let β,γ be the other roots of m.
The three field embeddings are $\sigma_1(x)=a+b\alpha+c\alpha^2$, $\sigma_2(x)=a+b\beta+c\beta^2$
$\sigma_3(x)=a+b\gamma+c\gamma^2$

Norm, Trace and Discriminent.

Definition:

Let k be an algebraic number field and $\sigma_1,\dots,\sigma_d : k \longrightarrow \mathbb{C}$ be all the field embeddings $[d=[k:\mathbb{Q}]]$.
Then for any $x\in k$, define $N(x)=\prod_{i=1}^{d}\sigma_i(x)$, called the norm.
Define $Tr(x)=\sum_{i=1}^{d}\sigma_i(x)$, called the trace of x.

A priori (obviously) : $N(x)\in\mathbb{C}$, $Tr(x)\in\mathbb{C}$.
(Prima facie).

Proposition:

For any $x\in k$, $N(x)\in\mathbb{Q}$, $Tr(x)\in\mathbb{Q}$

Proof: Let $k=\mathbb{Q}(\alpha)$. Then $x=f(\alpha)$ for some $f\in\mathbb{Q}[x]$
Let $\alpha_1,\dots,\alpha_d$ be roots of $m=m_\alpha$
Now $N(x)=\prod_{i=1}^{d}\sigma_i(f(\alpha))=\prod_{i=1}^{d}f(\sigma_i(\alpha))$

$=\prod_{i=1}^{d}f(\alpha_i)$ a symetric polynomial in $\alpha_1,\dots,\alpha_d$

By fundemental theorem of symmetric polynomials
$N(x)=g(s_1(\alpha_1,\dots,\alpha_d),\dots,s_d(\alpha_1,\dots,\alpha_d))$ coeffs of m
But $m(x)=x^d+\sum_{i=0}^{d-1}\underbrace{(-1)^i s_{i+1}(\alpha_1,\dots,\alpha_d)}_{\in\mathbb{Q}}x^i$

$\Rightarrow N(x)\in\mathbb{Q}$

For $Tr(x)$ the argument is the same, but replace $\prod$ by $\sum$

□

Lemma:

For $x, y \in k$, $N(xy) = N(x)N(y)$
$$Tr(x+y) = Tr(x) + Tr(y)$$

Proof: exercise

Example: $k = \mathbb{Q}(\sqrt{2})$ $\quad x = a + b\sqrt{2}$

$\sigma_1 : a + b\sqrt{2} \longmapsto a + b\sqrt{2}$

$\sigma_2 : a + b\sqrt{2} \longmapsto a - b\sqrt{2}$

$$N(a+b\sqrt{2}) = \prod_{i=1}^{2} \sigma_i (a+b\sqrt{2}) = \sigma_1(a+b\sqrt{2})\sigma_2(a+b\sqrt{2})$$
$$= (a+b\sqrt{2})(a-b\sqrt{2})$$
$$= a^2 + 2b^2$$

$$Tr(a+b\sqrt{2}) = \sigma_1(a+b\sqrt{2}) + \sigma_2(a+b\sqrt{2})$$
$$= a+b\sqrt{2} + a - b\sqrt{2}$$
$$= 2a.$$

Definition:

Let B be a basis for k over $\mathbb{Q}$. The discriminent of $B = \{b_1, \dots, b_d\}$ is

$$\Delta(B) = \det(Tr(b_i b_j))_{i,j}$$
$$= \begin{vmatrix} Tr(b_1 b_1) & \cdots & Tr(b_1 b_d) \\ \vdots & & \vdots \\ Tr(b_d b_1) & \cdots & Tr(b_d b_d) \end{vmatrix} \in \mathbb{Q}.$$

Remark: There is a bilinear form $k \times k \longrightarrow \mathbb{Q}$, $(v, w) \longmapsto Tr(vw)$
Then $\Delta(B)$ is just the determinent of the matrix of this bilinear form with respect to B.

Proposition:

Let $\sigma_1, \dots, \sigma_d : k \longrightarrow \mathbb{C}$ be a complete set of field embeddings for k. Then for any B, $\Delta(B) = (\det((\sigma_i(b_j))_{i,j})^2$

Proof: Let $A = (\sigma_i(b_j))_{i,j=1,\dots,d}$

$$(A^T A)_{ij} = \sum_k (A^T)_{ik} A_{kj} = \sum_k \sigma_k(b_i)\sigma_k(b_j)$$

$$= \sum_k \sigma_k(b_i b_j) = Tr(b_i b_j)$$

Therefore $\Delta(B) = \det(A^T A)$

$$= (\det(A))^2$$

$$= (\det(\sigma_i(b_j))_{i,j})^2$$

Example: $K = \mathbb{Q}(\sqrt{2})$ $B = \{1, \sqrt{2}\}$.

By the proposition $\Delta(B) = \left(\det\begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2}\end{pmatrix}\right)^2$

$$= (-2\sqrt{2})^2 = 8$$

Lemma:

If B, $\mathcal{C}$ are both bases for K over $\mathbb{Q}$ and Λ is the change of basis matrix (ie $\Lambda = (\lambda_{ij})$, $c_i = \sum_j \lambda_{ij} b_j$)
then $\Delta(\mathcal{C}) = \det(\Lambda)^2 \Delta(B)$

Proof: $(\sigma_i(c_j)) = (\sigma_i(b_i))\Lambda$

So $\Delta(\mathcal{C}) = \det(\sigma_i(c_j))^2 = (\det(\sigma_i(b_j)\Lambda))^2$

$$= \Delta(B)(\det\Lambda)^2$$

Vandermonde Determinants.

Proposition:

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{d-1} \\ 1 & x_2 & x_2^2 & & x_2^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_d & x_d^2 & & x_d^{d-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j)$$

Proof: By induction on d. Note that it is true for $d=2$.

$$\Rightarrow \begin{vmatrix} 0 & x_1 - x_d & x_1^2 - x_d^2 & \cdots & x_1^{d-1} - x_d^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & x_{d-1} - x_d & x_{d-1}^2 - x_d^2 & & x_{d-1}^{d-1} - x_d^{d-1} \\ 1 & x_d & x_d^2 & & x_d^{d-1} \end{vmatrix} = (-1)^{d-1} \boxed{}$$

$\square$

Note: $x_j^i - x_d^i = (x_j - x_d)(x_j^{i-1} + x_j^{i-2} x_d + \dots + x_j x_d^{i-2} + x_d^{i-1})$

$$= (-1)^{d-1} \prod_{j=1}^{d-1} (x_j - x_d) \begin{vmatrix} 1 & x_1 + x_d & x_1^2 + x_1 x_d + x_d^2 & \dots & x_1^{d-1} + \dots + x_d^{d-1} \\ \vdots & \vdots & & & \vdots \\ 1 & x_{d-1} + x_d & x_{d-1}^2 + x_{d-1} x_d + x_d^2 & \dots & x_{d-1}^{d-1} + \dots + x_d^{d-1} \end{vmatrix}$$

$\prod_{j=1}^{d-1} (x_d - x_j)$

$\xleftarrow{\text{order}}$

$c_2 \to c_2 - x_1 c_1 \quad c_3 \to c_3 - x_d c_2 \quad c_{d-1} \to c_{d-1} - x_d c_{d-2}$

$$= \prod_{j=1}^{d-1} (x_d - x_j) \begin{vmatrix} 1 & x_1 & \dots & x_1^{d-1} \\ \vdots & & & \vdots \\ 1 & x_{d-1} & \dots & x_{d-1}^{d-1} \end{vmatrix}$$

$$= \prod_{j=1}^{d-1} (x_d - x_j) \prod_{1 \le j < i \le d-1} (x_i - x_j)$$

$$= \prod_{1 \le j < i \le d} (x_i - x_j)$$

Recall that if $k = \mathbb{Q}(\alpha)$ and $d = [k : \mathbb{Q}]$ then $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$ is a basis for k over $\mathbb{Q}$.

Corollary:

Let $k = \mathbb{Q}(\alpha)$ and let $\alpha = \alpha_1, \dots, \alpha_d$ be the $\mathbb{Q}$ conjugates of α. Then $\Delta(\{1, \alpha, \dots, \alpha^{d-1}\}) = \{\prod_{i > j} (\alpha_i - \alpha_j)\}^2$

Proof: $$\Delta(\{1, \alpha, \dots, \alpha^{d-1}\}) = \left(\det \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{d-1} \\ \vdots & & & \vdots \\ 1 & \alpha_d & \dots & \alpha_d^{d-1} \end{vmatrix} \right)^2 = \prod_{i < j} (\alpha_i - \alpha_j)^2$$

Corollary:

For any B, $\Delta(B) \neq 0$

Proof: The previous corollary shows this for $\{1, \alpha, \dots, \alpha^{d-1}\}$. For any other basis the corollary follows from change of basis formula.

Proof: (again). When $B = \{1, \alpha, \ldots, \alpha^{d-1}\} = \{\alpha^{j-1} : 1 \le j \le d\}$.

In this case $\Delta(B) = (\det(\sigma_i(\alpha^{j-1})))^2$

$\{\underset{\alpha_i}{\underset{\|}{\sigma_i(\alpha)}} : 1 \le i \le d\}$ - the Q conjugate of α, ie roots of m_α.

$$\text{So } \Delta(B) = (\det(\alpha_i^{j-1}))^2$$

$$= \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & & \alpha_2^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \alpha_d^2 & & \alpha_d^{d-1} \end{vmatrix}^2$$

$$= \Big(\underbrace{\prod_{1 \le i \le j \le d} (\alpha_j - \alpha_i)}_{\neq 0}\Big)^2 \neq 0$$

by Vandermonde determinant formula

Galois seperability theorem.

If B' is any basis for K over $\mathbb{Q}$ let Λ be the change of basis matrix from B to B'

Then $\Delta(B') = \det \Lambda^2 \Delta(B)$

$\neq 0$ $\square$

Algebraic Intergers.

$$\begin{array}{ccc} \cancel{\mathbb{Q} \supseteq \mathbb{Z}} & \mathbb{Q} & \supseteq & \mathbb{Z} \\ \cancel{\wr} & \wr & & \wr \\ \cancel{K = \mathbb{Q}(\alpha)} & K = \mathbb{Q}(\alpha) & \supseteq & ? \\ & & & \mathcal{O}_K \end{array}$$

← What goes here? Algebraic Intergers!

$\mathbb{Z}[\alpha]$? Bad definition, want $\mathcal{O}_K$ depends on K not α.

Definition:

Let $L \supseteq \mathbb{Q}$ be a field extension. An element $\alpha \in L$ is called an algebraic interger if there is a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

eg. $\alpha = \sqrt{2}$, $f = x^2 - 2$.

Note: You can take $L = \mathbb{C}$.

Next we need to prove that the set of algebraic intergers is a ring.

Lemma:

$\alpha \in \mathbb{C}$ is an algebraic interger iff $\mathbb{Z}[\alpha]$ is finitely generated as an abelion group. (when equipped with addition)

Remark: $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group if and only if there exists some $b_1, \dots, b_n \in \mathbb{Z}[\alpha]$ st every $x \in \mathbb{Z}[\alpha]$ can be written as $x = \sum_{i=1}^{n} \lambda_i b_i$ where $\lambda_i \in \mathbb{Z}$.

Proof: $\Rightarrow$ Suppose α is an algebraic interger, ie $f(\alpha) = 0$ for some monic $f \in \mathbb{Z}[x]$, and let $d = \deg f$.
I claim that $\{1, \alpha, \dots \alpha^{d-1}\}$ generate $\mathbb{Z}[\alpha]$.
First notice that $\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}, \alpha^d, \dots, \alpha^i, \dots\} = \{\alpha^i \mid i \in \mathbb{N}\}$ generates $\mathbb{Z}[\alpha]$.
Now, it is enough to prove that $\alpha^m = \sum_{i=0}^{d-1} \lambda_i \alpha^i$ for any $m \geq d$. $\lambda_i \in \mathbb{Z}$
The proof of this by induction on m.
Let $f(x) = x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$
$f(\alpha) = 0$ so $\alpha^d = -a_{d-1}\alpha^{d-1} - \dots - a_1 \alpha - a_0$
This is the base case $m = d$ of our induction.
Now multiply by α^{m-d}: $\alpha^m = -a_{d-1}\alpha^{m-1} - \dots - a_1 \alpha^{m-d+1} - a_0 \alpha^{m-d}$
$\in \operatorname{span}_{\mathbb{Z}}\{1, \alpha, \dots, \alpha^{d-1}\}$ by inductive hypothesis

$\Leftarrow$ Suppose $\mathbb{Z}[\alpha]$ is finitely genereated abelion group.
ie $\mathbb{Z}[\alpha] = \operatorname{span}_{\mathbb{Z}}\{b_1 \dots b_N\}$
Each $b_i \in \mathbb{Z}[\alpha]$. Write $b_i = \sum_{j=0}^{m_i} \lambda_{ij} \alpha^j \quad \lambda_{ij} \in \mathbb{Z}$.
Let $M = \max\{M_i\}$
Now I can write $b_i = \sum_{j=0}^{M} \lambda_{ij} \alpha^j$ by setting $\lambda_{ij} = 0$ when $j > m_i$
consider $\alpha^{M+1} \in \mathbb{Z}[\alpha] = \operatorname{span}\{b_1 \dots b_N\}$
so there exists $\mu_i \in \mathbb{Z}$ such that
$$\alpha^{M+1} = \sum_{i=1}^{N} \mu_i b_i = \sum_{i=1}^{N} \mu_i \sum_{j=0}^{M} \lambda_{ij} \alpha^j$$
$$= \sum_{j=0}^{M} \left(\sum_{i=1}^{N} \mu_i \lambda_{ij}\right) \alpha^j$$

We have $\alpha^{M+1} - \sum_{j=0}^{M} r_j \alpha^j = 0$

Therefore α is an algebraic interger.

RECALL

Proposition:

Any subgroup of a finitely generated abelian group is a finitely generated abelian group.

$$\mathbb{Z}^d \oplus \mathbb{Z}/_{m_1} \oplus \mathbb{Z}/_{m_2} \oplus \dots \oplus \mathbb{Z}/_{m_n}$$

Corollary:

The algebraic intergers in $L \supseteq \mathbb{Q}$ form a ring.

Proof: Let α, β be algebraic intergers

Then $\mathbb{Z}[\alpha] = \text{span}_{\mathbb{Z}}\{g_1, \dots, g_m\}$

and $\mathbb{Z}[\beta] = \text{span}_{\mathbb{Z}}\{h_1 \dots h_n\}$.

For any i,j

$$\alpha^i \beta^j = \left(\sum_p \lambda_p g_p\right)\left(\sum_q \mu_q h_q\right) = \sum_{p,q} \lambda_p \mu_q g_p h_q \in \text{span}_{\mathbb{Z}}\{g_p h_q \mid 1 \le p \le m, 1 \le q \le n\}$$

Therefore $\mathbb{Z}[\alpha, \beta] \subseteq \text{span}_{\mathbb{Z}}\{g_p h_q \mid 1 \le p \le m, 1 \le q \le n\}$

$\mathbb{Z}[\alpha, \beta]$ is a finitely generated abelian group, by the group theory proposition.

But $\left.\begin{array}{l}\mathbb{Z}[\alpha+\beta] \\ \mathbb{Z}[\alpha\beta]\end{array}\right\} \subseteq \mathbb{Z}[\alpha, \beta]$ and so are finitely generated.

$\Rightarrow \alpha\beta, \alpha+\beta$ are algebraic intergers.

Definition:

The ring of algebraic intergers in k (a number field) is denoted by $\mathcal{O}_k$ (or $\mathcal{O}$ if k is implicit).

Example: $k = \mathbb{Q}$, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ Why?

Because for any $\alpha \in \mathbb{Q}$ $m_\alpha(x) = x - \alpha \in \mathbb{Z}[x]$ iff $\alpha \in \mathbb{Z}$.

This claim follows from ...

Lemma:

Suppose α is algebraic with minimal polynomial m_α. Then α is an algebraic interger iff $m_\alpha \in \mathbb{Z}[x]$

Proof: $\Leftarrow$ obvious.

$\Rightarrow$ Suppose $f(\alpha)=0$ for f monic, $f\in\mathbb{Z}[x]$

Then $f\in(m_\alpha)$ so $f=q m_\alpha$ for $q\in\mathbb{Q}[x]$

By the Gauss Lemma, there is $c\in\mathbb{Q}^*$ such that $cq\in\mathbb{Z}[x]$ and $c^{-1}m_\alpha\in\mathbb{Z}[x]$

But m_α is monic $\Rightarrow c^{-1}\in\mathbb{Z}$

On the other hand $f=qm_\alpha$ is also monic, so q is monic

But $cq\in\mathbb{Z}[x] \Rightarrow c\in\mathbb{Z}$

Therefore $c=\pm1$, so $m_\alpha\in\mathbb{Z}[x]$ QED

This completes the demonstration that $\mathcal{O}_\mathbb{Q}=\mathbb{Z}$.

Example: $k=\mathbb{Q}(i)=\{a+bi : a,b\in\mathbb{Q}\}$.

Suppose $\alpha=a+bi\in\mathcal{O}_k$ with $b\neq0$.

Now $m_\alpha(x)=(x-\alpha)(x-\bar{\alpha})$

$=x^2-2ax+(a^2+b^2)$

So $\alpha\in\mathcal{O}_K$ iff $2a\in\mathbb{Z} \Rightarrow a=c/2 \quad c\in\mathbb{Z}$

and $a^2+b^2\in\mathbb{Z} \Rightarrow c^2/4+b^2\in\mathbb{Z}$

if c is even then $a\in\mathbb{Z} \Rightarrow b^2\in\mathbb{Z} \Rightarrow b\in\mathbb{Z}$

suppose c is odd

$\Rightarrow c^2\equiv1 \bmod 4$

$\Rightarrow c^2/4\notin\mathbb{Z}$

If $b\in\mathbb{Z} \Rightarrow c^2/4\notin\mathbb{Z}$ so $b\notin\mathbb{Z}$.

Let $b=p/q$, p,q coprime.

If $q=2$ then p is odd

$\Rightarrow b^2=p^2/4$ but $p^2\equiv1\bmod4 \Rightarrow {}^2/4\in\mathbb{Z}$ * X

If $q>2$ then ... !

Step 1: Prove $2b\in\mathbb{Z}$

$4a^2+4b^2\in\mathbb{Z}$

$(2a)^2+(2b)^2\in\mathbb{Z}$

$\Rightarrow(2b)^2=m\in\mathbb{Z}$

Then $2b$ is root of

$x^2-m=0 \quad m\in\mathbb{Z}$

$\overset{\text{Gauss Lemma}}{\Rightarrow} 2b\in\mathbb{Z}$

Step 2: $a,b\in\frac{1}{2}\mathbb{Z}$

Let $a=a'/2 \quad b=b'/2$

If a',b' both even $a,b\in\mathbb{Z}$

* suppose a' odd $\Rightarrow b'$ odd to

$a'=2n+1 \quad b'=2p+1 \quad a^2+b^2=\frac{4n^2+4n+1+4p^2+4p+1}{4}$

$=n^2+p^2+n+p+\frac{1}{2}$

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

Corollary:

Let $x\in\mathcal{O}_K$. Then $N(x), Tr(x)\in\mathbb{Z}$

Furthermore if B is a basis for k over $\mathbb{Q}$ and $B\subseteq\mathcal{O}_K$, then $\Delta(B)\in\mathbb{Z}\setminus\{0\}$.

Proof: Let $\sigma_1, \dots, \sigma_d : K \longrightarrow \mathbb{C}$ be a complete set of field embeddings
The $\mathbb{Q}$ conjugates $\{\sigma_i(x)\}$ are all roots of $m_x \Rightarrow \{\sigma_i(x)\}$ are algebraic intergers.
Now $N(x) = \prod_i \sigma_i(x)$ is an algebraic number and a rational number
$\Rightarrow N(x) \in \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
Similarly $Tr(x) \in \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
$\Delta(B) = \det(Tr(b_i b_j))$ $(B = \{b_i\})$
$\underset{\mathbb{Z}}{\cap}$.
So $\Delta(B) \in \mathbb{Z}$. (already proved $\Delta(B) \neq 0$). QED.

Intergral Bases

Definition:

B a basis for K over $\mathbb{Q}$, is called intergral if $\mathcal{O}_K = \left\{ \sum_{i=1}^{d} \lambda_i b_i : \lambda_i \in \mathbb{Z} \right\}$.

Example: $\{1\}$ is an intergral basis in $\mathbb{Q}$
$\{2\}$ is not an intergral basis in $\mathbb{Q}$, because $1 = \underset{\notin \mathbb{Z}}{\frac{1}{2}} 2$.

Example: We have seen that $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$
$\{1, i\}$ is an intergral basis in $\mathbb{Q}(i)$ exercise: find more than 4
$\{2, i\}$ isn't.

Lemma:

For any $\alpha \in K$, there is $N \in \mathbb{Z} \setminus \{0\}$ such that $N\alpha \in \mathcal{O}_K$

Proof: Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0$ $a_i \in \mathbb{Q}$
Consider $N^d m\left(\frac{x}{N}\right) = x^d + N a_{d-1} x^{d-1} + N^2 a_{d-2} x^{d-2} + \dots + N^d a_0$.
$N \in \mathbb{Z}$
Choose N so that $N a_i \in \mathbb{Z}$ for all i. Then $N^d m(x/N) \in \mathbb{Z}[x]$
$N^d m\left(\frac{N\alpha}{N}\right) = 0$ so $N\alpha$ is a root of $N^d m\left(\frac{x}{N}\right) \Rightarrow N\alpha \in \mathcal{O}_K$ QED.

Proposition:

There is a basis $B \subseteq \mathcal{O}_K$

Proof: Let $B' = \{b_i'\}$ be any basis for K over $\mathbb{Q}$.
For each i let $N_i b_i' \in \mathcal{O}_K$ for $N_i \in \mathbb{Z} \setminus \{0\}$
Now $B = \{N_i b_i\} \in \mathcal{O}_K$.

Recall from last time that if $B \subseteq \mathcal{O}_K$ then $\Delta B \in \mathbb{Z} \setminus \{0\}$.

Theorem:

If $B \subseteq \mathcal{O}_K$ is choosen so that $|\Delta B|$ is minimal among all basis in $\mathcal{O}_K$ then B is an intergral basis.

Proof: Since $B \subseteq \mathcal{O}_K$, $\operatorname{span}_{\mathbb{Z}} B \subseteq \mathcal{O}_K$.
Suppose B is not an intergral basis.
Then $\exists\, \theta \in \mathcal{O}_K$ such that $\theta = \sum_{i=1}^{d} x_i b_i$ with some $x_i \in \mathbb{Q} \setminus \mathbb{Z}$
wlog $i = 1$. Let $\theta' = \sum_{i=1}^{d} \lfloor x_i \rfloor b_i \in \mathcal{O}_K$
Replace θ by $\theta - \theta'$ intergar part
Then we can assume that $0 < x_1 < 1$.
Consider a new basis $\mathcal{C} = \{\theta, b_2 \ldots b_d\}$
The transition matrix from B to $\mathcal{C}$ is

$$\Lambda = \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 1 & & \vdots \\ \vdots & \vdots & \ddots & 0 \\ x_d & 0 & \cdots & 1 \end{pmatrix}$$

Then $\det \Lambda = x_1$ so
$|\Delta \mathcal{C}| = |(\det \Lambda)^2 \Delta B| = x_1^2 |\Delta B| < |\Delta B|$

$0 < x_1 < 1$

QED

The proof gives a procedure for finding an intergral basis
1. Start with any basis $B \in \mathcal{O}_K$
2. Calculate ΔB and let $N \in \mathbb{N}$ be maximal such that N^2 divides $|\Delta B|$
(in the proof N is a possible denominater for x_1)
3. For each $\theta = \sum_{i=1}^{d} \left(\frac{m_i}{N}\right) b_i = \frac{1}{N} \sum_{i=1}^{d} m_i b_i$ with $m_i \in \mathbb{Z}$ $0 \leq m_i < N$ not all zero.

Check whether $\theta \in \mathcal{O}_K$
If so replace b_i by θ for some sutiable i (ie $m_i \neq 0$) and go back to step 2.

4. If no $\theta \in \mathcal{O}_K$ or if $N=1$ then B is an intergral basis.

Example: $k = \mathbb{Q}(\sqrt{-3})$

1. $B_1 = \{1, \sqrt{-3}\} \subseteq \mathcal{O}_K$
2. $\Delta B_1 = \begin{vmatrix} 1 & \sqrt{-3} \\ 1 & -\sqrt{-3} \end{vmatrix}^2 = (-2\sqrt{-3})^2 = -2^2 \times 3$

So $N = 2$

3. Check: $\theta = \frac{1}{2}, \frac{1}{2}\sqrt{-3}, \frac{1}{2}(1+\sqrt{-3})$

$\frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z} \Rightarrow \frac{1}{2} \notin \mathcal{O}_K$

$N(\frac{1}{2}\sqrt{-3}) = (\frac{1}{2}\sqrt{-3})(-\frac{1}{2}\sqrt{-3}) = \frac{3}{4} \notin \mathbb{Z} \Rightarrow \frac{1}{2}\sqrt{-3} \notin \mathcal{O}_K.$

$N(\frac{1}{2}(1+\sqrt{-3})) = \frac{1}{2}(1+\sqrt{-3})\frac{1}{2}(1-\sqrt{-3}) = \frac{1}{4}(1+3) = 1 \in \mathbb{Z}.$

$Tr(\frac{1}{2}(1+\sqrt{-3})) = \frac{1}{2}(1+\sqrt{-3}) + \frac{1}{2}(1-\sqrt{-3}) = 1$

$\Rightarrow m_{\frac{1}{2}(1+\sqrt{-3})}(x) = x^2 - x + 1$

$\Rightarrow \frac{1}{2}(1+\sqrt{-3}) \in \mathcal{O}_K.$

So replace B_1 by $B_2 = \{1, \frac{1}{2}(1+\sqrt{-3})\}$.

$\Delta B_2 = \begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{-3}) \\ 1 & \frac{1}{2}(1-\sqrt{-3}) \end{vmatrix}^2 = (\frac{1}{2}(1-\sqrt{-3}) - \frac{1}{2}(1+\sqrt{-3}))^2$

$= \left(-\frac{2}{2}\sqrt{-3}\right)^2 = -3 \Rightarrow N=1 \Rightarrow B_2$ is an intergral basis.

Intergral Bases in quadratic fields.

Definition:

A number field k is called quadratic if $[k:\mathbb{Q}] = 2$
$\Leftrightarrow k = \mathbb{Q}(\alpha)$ for α a root of some irreducible quadratic polynomial $m(x) = x^2 + bx + c$, $b, c \in \mathbb{Q}$.

We saw
- $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] \Leftrightarrow \{1, i\}$ is an intergral basis
- $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-3})] \Leftrightarrow \{1, \frac{1}{2}(1+\sqrt{-3})\}$ is an intergral basis.

If K is quadratic, $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2}$

so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2-4ac})$

Let $x = b^2 - 4c = \frac{p}{q} \in \mathbb{Q}$ for p, q coprime.

$$\begin{aligned} \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{x}) &= \mathbb{Q}\left(\sqrt{\tfrac{p}{q}}\right) \\ &= \mathbb{Q}\left(q\sqrt{\tfrac{p}{q}}\right) \\ &= \mathbb{Q}(\sqrt{pq}) \\ &= \mathbb{Q}(\sqrt{n}) \text{ for some } n \in \mathbb{Z}. \end{aligned}$$

If $n = m^2 n'$ the

$\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(m\sqrt{n'}) = \mathbb{Q}(\sqrt{n'})$.

So we may assume $K = \mathbb{Q}(\sqrt{n})$ for n some square-free interger ie the only ~~number~~ square number dividing n is one.

We proved:

Proposition:

If K is quadratic then $K = \mathbb{Q}(\sqrt{n})$ for ~~some~~ n some square free interger. (not equal to 1).

Theorem:

Let $n \in \mathbb{Z} \setminus \{1\}$ be a square free interger and $K = \mathbb{Q}(\sqrt{n})$.

- If $n \not\equiv 1 \bmod 4$ then $\{1, \sqrt{n}\}$ is an interger basis.
- If $n \equiv 1 \bmod 4$ then $\{1, \frac{1}{2}(1+\sqrt{n})\}$ is an interger basis

Proof: First assume $n \not\equiv 1 \bmod 4$ and apply algorithm

$B_1 = \{1, \sqrt{n}\} \subseteq \mathcal{O}_K$ ~~wra~~ because $x^2 - n = m_{\sqrt{n}}$.

$$\Delta B = \begin{vmatrix} 1 & \sqrt{n} \\ 1 & -\sqrt{n} \end{vmatrix}^2 = (-\sqrt{n} - \sqrt{n})^2 = 4n \Rightarrow N = 2.$$

Check $\theta = \frac{1}{2}, \frac{1}{2}\sqrt{n}, \frac{1}{2}(1+\sqrt{n})$

$\frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z}$ so $\frac{1}{2} \notin \mathcal{O}_K$.

$N(\frac{1}{2}\sqrt{n}) = (\frac{1}{2}\sqrt{n})(-\frac{1}{2}\sqrt{n}) = \frac{-n}{4} \notin \mathbb{Z}$ because n square free

$\Rightarrow \frac{1}{2}\sqrt{n} \notin \mathcal{O}_K$.

$N(\frac{1}{2}(1+\sqrt{n})) = \frac{1}{2}(1+\sqrt{n})\frac{1}{2}(1-\sqrt{n}) = \frac{1}{4}(1-n) \notin \mathbb{Z}$ because $n \not\equiv 1 \bmod 4$

$\Rightarrow \frac{1}{2}(1+\sqrt{n}) \notin \mathcal{O}_K$

$\Rightarrow B = \{1, \sqrt{n}\}$ is an intergral basis.

Next suppose $n \equiv 1 \bmod 4$

Let $B_2 = \{1, \underbrace{\tfrac{1}{2}(1+\sqrt{n})}_{=\alpha}\}$

$(\alpha - \frac{1}{2})^2 = \frac{n}{4}$ so $m_\alpha(x) = (x - \frac{1}{2})^2 - \frac{n}{4}$

$= x^2 - x + \underbrace{\frac{(1-n)}{4}}_{\in \mathbb{Z} \text{ because } n \equiv 1 \bmod 4}$

$$\Delta B = \begin{vmatrix} 1 & \frac{1}{2}(1+\sqrt{n}) \\ 1 & \frac{1}{2}(1-\sqrt{n}) \end{vmatrix}^2 = \left(\tfrac{1}{2}(1-\sqrt{n}) - \tfrac{1}{2}(1+\sqrt{n})\right)^2 = (-\sqrt{n})^2 = n$$

$\Rightarrow N = 1 \Rightarrow B$. intergral basis.

Cubic fields

Definition:

K is called cubic if $[K:\mathbb{Q}] = 3$ ie $K = \mathbb{Q}(\alpha)$ for some α with $m(x) = m_\alpha(x) = x^3 + ax^2 + bx + c$.

The normalised minimal polynomial is

$m(\alpha + \frac{a}{3}) = m(x - \frac{a}{3}) = x^3 + 0x^2 + \ldots$

Of course $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha + a/3)$.

So we may assume that $m(x) = m_\alpha(x) = x^3 + ax + b$

Also we saw that $\exists N \in \mathbb{Z} \setminus \{0\}$ such that $\alpha' - N\alpha \in \mathcal{O}_K$

Replacing α by α' we may assume that $\alpha \in \mathcal{O}_K$

ie $a, b \in \mathbb{Z}$.

Proposition:

If $K = \mathbb{Q}(\alpha)$, $m_\alpha(x) = x^3 + ax + b$, $a, b \in \mathbb{Q}$ then

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

To prove this proposition we need

Theorem:

If $K = \mathbb{Q}(\alpha)$, α of degree d, with minimal polynomial $m(x)$

$$\Delta\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\} = (-1)^{\frac{d(d-1)}{2}} N(m'(\alpha))$$

Proof of theorem: Let $\alpha_1 \dots \alpha_d$ be the roots of m.

Recall $\Delta\{1, \alpha, \dots, \alpha^{d-1}\} = \prod_{i<j} (\alpha_j - \alpha_i)^2$

$$= (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

Now $N(m'(\alpha)) = \prod_{i=1}^{d} m'(\alpha_i)$

Over $\mathbb{C}$, $m(x) = \prod_{j=1}^{d} (x - \alpha_j)$

By Leibniz's Rule

$$m'(x) = \sum_{j=1}^{d} \prod_{k \neq j} (x - \alpha_k) = \prod_{k \neq i} (x - \alpha_k) + \sum_{j \neq i} \prod_{k \neq j} (x - \alpha_k)$$

So $m'(\alpha_i) = \prod_{k \neq i} (\alpha_i - \alpha_k)$ because $\sum_{j \neq i} \prod_{k \neq j} (\alpha_i - \alpha_k) = 0$

We can rename k as j and this proves theorem. QED.

Proof of proposition: $m(x) = x^3 + ax + b$.

Roots α, β, γ

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

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

$$= -(3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a).$$

$$= -27(\alpha\beta\gamma)^2 - 9a\underbrace{(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2)}_{(\sum\alpha\beta)^2 - 2(\sum\alpha)(\prod\alpha)} - 3a^2\underbrace{(\alpha^2 + \beta^2 + \gamma^2)}_{(\sum\alpha)^2 - 2(\sum\alpha\beta)} - a^3$$

$\alpha\beta\gamma = \prod\alpha = -b$

$\alpha\beta + \beta\gamma + \gamma\alpha = \sum\alpha\beta = a$

$\alpha + \beta + \gamma = \sum\alpha = 0$

So $\Delta\{1, \alpha, \alpha^2\} = -27(-b)^2 - 9a(a^2 - 0) - 3a^2(0 - 2a) - a^3$

$$= -27b^2 - 9a^3 + 6a^3 - a^3$$

$$= -27b^2 - 4a^3 \qquad \text{QED.}$$

Example: Let α be a root of $m(x) = x^3 + 2x + 2$ (other roots β, γ).

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

m irreducible by eisensteins criterion ($p = 2$)

$\Rightarrow [K : \mathbb{Q}] = 3$.

Let $B = \{1, \alpha, \alpha^2\}$ Now $\alpha \in \mathcal{O}_K \Rightarrow \alpha^2 \in \mathcal{O}_K$.

$\Delta B = -27b^2 - 4a^3 = -27 \times 4 - 4 \times 8 = -4 \times 35 = -2^2 \times 5 \times 7$.

$\Rightarrow N = 2$.

Check $\theta = \frac{1}{2}, \frac{1}{2}\alpha, \frac{1}{2}\alpha^2, \frac{1}{2}(1+\alpha), \frac{1}{2}(1+\alpha^2), \frac{1}{2}(\alpha + \alpha^2) (= \frac{1}{2}\alpha(1+\alpha)), \frac{1}{2}(1+\alpha+\alpha^2)$

- $\frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z} \Rightarrow \frac{1}{2} \notin \mathcal{O}_K$.

- $N(\frac{1}{2}\alpha) = (\frac{1}{2}\alpha)(\frac{1}{2}\beta)(\frac{1}{2}\gamma) = \frac{1}{8}(\alpha\beta\gamma) = -\frac{1}{4} \notin \mathbb{Z}. \Rightarrow \frac{1}{2}\alpha \notin \mathcal{O}_K.$
- $N(\frac{1}{2}\alpha^2) = (\frac{1}{2}\alpha^2)(\frac{1}{2}\beta^2)(\frac{1}{2}\gamma^2) = \frac{1}{8}(\alpha\beta\gamma)^2 = \frac{1}{8}(-2)^2 = \frac{1}{2} \notin \mathbb{Z} \Rightarrow \frac{1}{2}\alpha^2 \notin \mathcal{O}_K.$
- $N(\frac{1}{2}(1+\alpha)) = \frac{1}{2}(1+\alpha)\frac{1}{2}(1+\beta)\frac{1}{2}(1+\gamma)$

$\alpha\beta\gamma = -2$

$\alpha\beta+\beta\gamma+\alpha\gamma = 2$

$\alpha+\beta+\gamma = 0.$

$$= \frac{1}{8}(1+\alpha)(1+\beta)(1+\gamma) = \frac{1}{8}m(-1) \text{ !..}$$
$$= \frac{1}{8}(1+\sum\alpha+\sum\alpha\beta+\prod\alpha)$$
$$= \frac{1}{8}(1+0+2+2) = \frac{1}{8} \notin \mathbb{Z} \Rightarrow \frac{1}{2}(1+\alpha) \notin \mathcal{O}_K.$$

$m(x) = (x-\alpha)(x-\beta)(x-\gamma)$

$= -(\alpha-x)(\beta-x)(\gamma-x)$

- $N(\frac{1}{2}(1+\alpha^2)) = \frac{1}{8}(1+\alpha^2)(1+\beta^2)(1+\gamma^2) = \frac{1}{8}((1-\sum\alpha\beta)^2 - (\sum\alpha - \prod\alpha)^2)$

$$= \frac{1}{8}((1-2)^2 - (0-2)^2) = \frac{1}{8}(1-2^2) = -\frac{3}{8} \notin \mathbb{Z} \Rightarrow \frac{1}{2}(1+\alpha^2) \notin \mathcal{O}_K.$$

- $N(\frac{1}{2}(\alpha+\alpha^2)) = \frac{1}{8}\alpha(1+\alpha)\beta(1+\beta)\gamma(1+\gamma)$

$$= (\alpha\beta\gamma)\frac{1}{8}(1+\alpha)(1+\beta)(1+\gamma)$$
$$= (-2)\frac{1}{8} = -\frac{1}{4} \notin \mathbb{Z} \Rightarrow \frac{1}{2}(\alpha+\alpha^2) \notin \mathcal{O}_K.$$

- $N(\frac{1}{2}(1+\alpha+\alpha^2)) = \frac{1}{8}(1+\alpha+\alpha^2)(1+\beta+\beta^2)(1+\gamma+\gamma^2)$

$$= \frac{1}{8}(1-(\sum\alpha\beta) - 2(\prod\alpha) + (\sum\alpha\beta)^2 + (\prod\alpha)(\sum\alpha\beta) + (\prod\alpha)^2)$$
$$= \frac{1}{8}(1-2-2(-2)+2^2+-2\cdot 2+(-2)^2)$$
$$= \frac{1}{8}(1-2+4+4-4+4)$$
$$= \frac{7}{8} \notin \mathbb{Z} \Rightarrow \frac{1}{2}(1+\alpha+\alpha^2) \notin \mathcal{O}_K.$$

OR use trace instead - probably easier.

Corollary: (of previous theorem).

Let $K = \mathbb{Q}(\alpha)$, $d = [K:\mathbb{Q}]$. Then for any $\theta = \alpha + x$, with $x \in \mathbb{Q}$,

$\Delta\{1,\alpha,\ldots\alpha^{d-1}\} = \Delta\{1,\theta,\ldots\theta^{d-1}\}.$

Proof: $m_\theta(X) = m_\alpha(X-x)$

By chain rule $m_\theta'(X) = m_\alpha'(X-x)$

$m_\theta'(\theta) = m_\alpha'(\theta - x) = m_\alpha'(\alpha) \Rightarrow$ the result QED.

More Tricks for Calculating Intergal Bases.

Trick 1: If $\theta = \frac{1}{N}\sum_{i=1}^{d} a_i b_i \in \mathcal{O}_K$, not all a_i divisible by N

then, for some prime $p \mid N$, there exists $\theta' = \frac{1}{p}\sum_{i=1}^{d} a_i' b_i$

not all a_i' divisible by p.

So instead of working with N, we can work with all primes p st $p^2 \mid \Delta B$.

Proof: induction on $N \geq 2$

Base case: If N is prime nothing to prove

Otherwise: Case 1: $\exists$ prime $p \mid N$ and i st $a_i \not\equiv 0 \bmod p$

Then $\theta' = \left(\frac{N}{p}\right)\theta = \frac{1}{p}\sum a_i b_i$ works.

Case 2: $\forall$ prime $p \mid N$ and for all i, $a_i \equiv 0 \bmod p$

Then fix $p' \mid N$ write $a_i = a_i' p$ for $a_i' \in \mathbb{Z}$, $N = N'p$ for $N' \in \mathbb{Z}$

Note that $N' \mid a_i' \Rightarrow N = N'p \mid a_i' p$, so $\exists i$ st $N' \nmid a_i'$

Now $\theta = \frac{1}{N'p}\sum_i p a_i' b_i$ and $N' < N$

So we are done by induction.

Trick 2:

$N(ab) = N(a)N(b)$

$Tr(a+b) = Tr(a) + Tr(b)$

Trick 3:

Let $K = \mathbb{Q}(\alpha)$, $m = m_\alpha$. Then for any $x \in \mathbb{Q}$ $N(x - \alpha) = m(x)$

Proof: $m_{x-\alpha}(X) = (-1)^d m_\alpha(x - X)$

$N(x-\alpha) = (-1)^d \times$ constant term of $m_{x-\alpha}$

$= (-1)^d m_{x-\alpha}(0)$

$= (-1)^d (-1)^d m_\alpha(x - 0)$

$= m_\alpha(x)$ QED.

Trick 4:

Suppose m_α satisfies Eisenstein's Criterion with prime p.

Consider $K = \mathbb{Q}(\alpha)$. Suppose we want to compute

$\Delta\{1, \alpha, \ldots, \alpha^{d-1}\} = \pm N(m_\alpha'(\alpha))$

$m_\alpha(X) \equiv X^d \bmod p$

$\Rightarrow m_\alpha'(x) \equiv d x^{d-1} \bmod p$.

$N(m_\alpha'(\alpha)) \equiv N(d\alpha^{d-1}) = N(d) N(\alpha)^{d-1}$

But $N(\alpha) = m_\alpha(0) \equiv 0 \bmod p$

$\Rightarrow \Delta\{1, \alpha, \dots \alpha^{d-1}\}$ has p as a factor.

Theorem:

Let $K = \mathbb{Q}(\alpha)$, $d = [K:\mathbb{Q}]$, m_α satisfies eisenstien's criterion, with prime p.

Let $\theta = \frac{1}{p} \sum_{i=0}^{d-1} a_i \alpha^i$, $a_i \in \{0, \dots, p-1\}$ not all 0.

Then $\theta \notin \mathcal{O}_K$.

Proof: Let n be minimal such that $a_n > 0$

suppose $\theta = \frac{1}{p} \sum_{i=n}^{d-1} a_i \alpha^i \in \mathcal{O}_K$.

$= \frac{1}{p}(a_n \alpha^n + \underbrace{\alpha^{n+1} \delta}_{\text{higher order terms}})$ for some $\delta \in \mathcal{O}_K$.

$\Rightarrow \alpha^{d-1-n} \theta = \frac{1}{p}(a_n \alpha^{d-1} + \alpha^d \delta) \in \mathcal{O}_K$.

Since m satisfies eisenstien criterion.

$0 = m(\alpha) = \alpha^d - p g(\alpha)$ for some $g(x) \in \mathbb{Z}[x]$ (so $\alpha^d = p g(\alpha)$)

$\Rightarrow \underbrace{\alpha^{d-1-n}\theta}_{\in \mathcal{O}_K} = \frac{a_n \alpha^{d-1}}{p} + \underbrace{g(\alpha)\delta}_{\in \mathcal{O}_K}$

$\Rightarrow \frac{a_n \alpha^{d-1}}{p} \in \mathcal{O}_K$

But $N\left(\frac{a_n \alpha^{d-1}}{p}\right) = \frac{N(a_n)}{N(p)} N(\alpha^{d-1})$ But $N(\alpha) = m_\alpha(0) = pr$ for some r coprime to p.

so $N\left(\frac{a_n \alpha^{d-1}}{p}\right) = \frac{a_n^d}{p^d}(pr)^{d-1}$

$= \frac{a_n r^{d-1}}{p} \in \mathbb{Z}$

$\Rightarrow p | a_n$ or $p | r$

contradiction.

Example: $K = \mathbb{Q}(\alpha)$, α a root of $m(X) = X^p - p$, p prime:

$m'(X) = pX^{p-1}$

So $|\Delta\{1,\ldots,\alpha^{p-1}\}| = N(m'(\alpha))$
$= N(p\alpha^{p-1})$
$= N(p)N(\alpha)^{p-1}$
$= p^p((-1)^p(-p))^{p-1} = p^{2p-1}$

By Trick 4, $\{1,\alpha,\ldots\alpha^{p-1}\}$ is an integral basis.

Example: $f(x) = x^3 - 2$ $\quad \alpha = \sqrt[3]{2}$ $\quad K = \mathbb{Q}(\alpha)$

f is irreducible by Eisenstein's criterion ~~prim~~ with $p=2$

$B = \{1, \alpha, \alpha^2\}$ $\quad \Delta = -27\times(-2)^2 - 4\times 0^3 = -2^2\times 3^3$

So we need to check $p = 2, 3$. But $p=2$ is ok because of Eisenstein's criterion.

Still need to check.

$\theta = 1/3 \in \mathbb{Q}\setminus\mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

$\theta = 1/3\,\alpha$ $\quad N(\theta) = N(1/3)N(\alpha) = \frac{1}{27}\alpha\beta\gamma = \frac{2}{27} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

$\theta = \frac{1}{3}\alpha^2$ $\quad N(\theta) = N(\frac{1}{3})N(\alpha^2) = \frac{1}{27}\times 2^2 = \frac{4}{27} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$

$\theta = \frac{1}{3}(1+\alpha)$ $\quad N(\theta) = -\frac{1}{27}((-1)-\alpha)) = -\frac{1}{27}f(-1) = \frac{3}{27} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

$\theta = \frac{1}{3}(1+\alpha^2)$ $\quad N(\theta) = -\frac{1}{27}(((-1)-\alpha^2) = -\frac{1}{27}m_{\alpha^2}(-1) = \frac{5}{27} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

$\theta = \frac{1}{3}(\alpha+\alpha^2)$ $\quad N(\theta) = N(\frac{1}{3}(\alpha+\alpha^2)) = \frac{1}{27}N(\alpha)N(1+\alpha) = \frac{2}{9} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

$\theta = \frac{1}{3}(1+\alpha+\alpha^2)$

Consider $(\alpha+\alpha^2)^3 = \alpha^3 + 3\alpha^4 + 3\alpha^5 + \alpha^6$
$= 2(1+3\alpha+3\alpha^2+\alpha^3)$
$= 2{\cdot}3(1+\alpha+\alpha^2)$
$= 6(1+\alpha+\alpha^2)$

$N(\theta) = \frac{1}{27}N(1+\alpha+\alpha^2) = \frac{1}{27}N\left(\frac{1}{6}(\alpha(1+\alpha))^3\right)$

$= \frac{1}{27}\left(\frac{1}{6}\right)^3 2^2 3^3 = \frac{1}{27} \notin \mathbb{Z} \Rightarrow \theta \notin \mathcal{O}_K$.

Example: $m(x) = x^p - p$, p prime α root of m $K = \mathbb{Q}(\alpha)$

m irreducible by eisenstien criterion $p = p$

$B = \{1, \alpha, \dots, \alpha^{p-1}\}$

$m'(x) = px^{p-1}$

$\Delta B = N(m'(\alpha)) = N(p\alpha^{p-1})$

$= N(p)N(\alpha)^{p-1}$

$= (p^p)(p^{p-1}) = p^{2p-1}$

The only prime divisor is p which we used in eisenstiens
$\Rightarrow B$ is intergral basis.

Prime Cyclotonic Fields.

Definition:

Let $n \in \mathbb{N}$. $\zeta \in \mathbb{C}$ is an n^{th} root of unity if $\zeta^n = 1$.
If there is no $1 \le r \le n$ with $\zeta^r = 1$ then ζ is a primitive root of unity

eg. $\zeta = e^{\frac{2\pi i}{n}}$

clearly any such ζ is an algebraic interger because it satisfies $x^n - 1 = 0$.

If $r | n$ then $x^r - 1 | x^n - 1$
We will concentrate on $n = p$, p odd prime.
Let $\lambda = \zeta - 1$.

Proposition:

The minimal polynomial of ζ is $m_\zeta(x) = \dfrac{x^p - 1}{x - 1} = 1 + x + \dots + x^{p-1}$

Proof: Equivalently we will prove that
$m_\lambda(x) = m_\zeta(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$

Recall that $p | \binom{p}{i}$ if $1 \le i \le p-1$, so m_λ satisfies eisenshiens criterion $p = p$.

Corollary:

- $[K:\mathbb{Q}] = p-1$
- $N(\lambda) = p$
- $N(\zeta) = 1$

Theorem:

$\Delta\{1, \lambda, \dots \lambda^{p-2}\} = \Delta\{1, \zeta, \dots \zeta^{p-2}\} = (-1)^{\frac{p-1}{2}} p^{p-2}$
and $\{1, \lambda, \dots, \lambda^{p-2}\}$ is an intergral basis in K.
Hence $\mathcal{O}_K = \mathbb{Z}[\lambda] = \mathbb{Z}[\zeta]$.

Proof: $\Delta = (-1)^{\frac{(p-1)(p-2)}{2}} N(m_\zeta'(\zeta))$

$m_\zeta(x) = \dfrac{x^{p}-1}{x-1}$

$m_\zeta'(x) = \dfrac{p x^{p-1}(x-1) - (x^{p}-1)}{(x-1)^2}$

so $m_\zeta'(\zeta) = \dfrac{p\zeta^{p-1}(\zeta-1) - (1-1)}{(\zeta-1)^2}$

$= \dfrac{p\zeta^{p-1}}{\lambda}$

$(-1)^{\frac{p-1}{2}} N(m_\zeta'(\zeta)) = (-1)^{\frac{p-1}{2}} \dfrac{N(p)N(\zeta)^{p-1}}{N(\lambda)} = \dfrac{(-1)^{\frac{p-1}{2}} p^{p-1} 1^{p-1}}{p} = (-1)^{\frac{p-1}{2}} p^{p-2}$

Because the only prime divisor of Δ is p and we used p in eisensteins criterion, $\{1, \lambda, \dots \lambda^{p-2}\}$ is an intergral basis.

$\frac{p^2-3p+2}{2}$

FACTORISATION IN $\mathcal{O}_K$.

Units and irreducibles in $\mathcal{O}_K$.

A ring R with a unit 1 has three sorts of elements:

- units: $x \in R$ such that $\exists y \in R$ st $xy = 1$
- Reducibles: $x \in R$ such that $\exists y, z \in R$, neither units st $x = yz$.
- irreducibles: $x = yz \in R \Rightarrow$ either y or z is a unit.

Proposition:

Let $x \in \mathcal{O}_K$. Then x is a unit iff $N(x) = \pm 1$.

Proof: $\Rightarrow$ If x is a unit then $xy = 1$ for $x \in \mathcal{O}_K$, $y \in \mathcal{O}_K$.

$\underset{\mathbb{Z}}{\underset{\cap}{N(x)}}\,\underset{\mathbb{Z}}{\underset{\cap}{N(y)}} = N(xy) = N(1) = 1 \quad \Rightarrow N(x) = \pm 1$

$\Leftarrow$ $\pm 1 = N(x) = x_1 \ldots x_d$ where $\{x_i\}$ are the $\mathbb{Q}$-conjugates of x

Let $y = x_2 \ldots x_d$. Then $(x = x_1)$ $xy = \pm 1 \Rightarrow x(\pm y) = 1$. QED

Corollary:

If $x \in \mathcal{O}_K$ has $N(x) = p$, prime, then x is irreducible.

Proof: Suppose $x = yz$. Then $p = N(x) = N(y)N(z)$

$\Rightarrow N(y) = \pm 1 \Rightarrow y$ is a unit QED.

Converse is false !

Example: $3 \in \mathbb{Z}[i]$

$N(3) = 9$

Suppose $3 = xy$ for x, y not units

$\Rightarrow |N(x)| = |N(y)| = 3$

But $x = a + bi$ $N(x) = a^2 + b^2 \neq 3$ for any $a, b \in \mathbb{Z}$

Therefore 3 is irreducible.

Theorem:

Let $x \in \mathcal{O}_K \setminus \{0\}$. Then there is a unit $u \in \mathcal{O}_K^{\times}$ and irreducibles

group of units.

$p_1 \cdots, p_n$ such that $x = u p_1 \cdots p_n$.

Proof: By induction on $|N(x)|$

If $|N(x)| = 1$, $x = u$ works

If x is irreducible $x = p_1$ works.

Otherwise x is reducible

$x = yz \Rightarrow |N(x)| = |N(y)||N(z)|$

neither units

$\Rightarrow |N(x)| > |N(y)|, |N(z)|$

By induction theorem holds for y, z.

Multiply to get the decomposition for x.

Definition:

A ring R is a unique factorisation domain if, whenever we have $x = u p_1 \cdots p_r = v q_1 \cdots q_s$ then $r = s$ and for each i, $\exists j$ and a unit u_i st $p_i = u_i q_j$ and vice versa.

eg. $\mathbb{Z}$, $k[x]$,

Example: $k = \mathbb{Q}(\sqrt{-10})$ $\quad O_k = \mathbb{Z}[\sqrt{-10}]$

$10 = 2 \times 5 = -\sqrt{-10} \times \sqrt{-10}$

$N(2) = 4 \quad N(5) = 25 \quad N(\sqrt{-10}) = \sqrt{-10} \times -\sqrt{-10} = 10$

If any of these can be written as yz, for y, z irreducibles, then $\{N(y), N(z)\} \subseteq \{\pm 2, \pm 5\}$

If $y = a + b\sqrt{-10}$, So $N(y) = a^2 + 10b^2$

This never equals ± 2 or ± 5.

So O_k is not a UFD!

Definition:

If $I, J \leq R$ are ideals then $IJ = (xy : x \in I, y \in J)$

eg $I = (a)$, $J = (b)$, $IJ = (ab)$

$I = (a, b)$, $J(c, d)$ $\quad IJ = (ac, ad, bc, bd)$ etc.

We will eventually prove.

Theorem:

Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal.
There are maximal ideals $\mathfrak{p}_1 \dots \mathfrak{p}_r$ of $\mathcal{O}_K$ such that $I = \mathfrak{p}_1 \dots \mathfrak{p}_r$
Furthermore the factorisation is unique up to reordering
ie if $I = \mathfrak{q}_1 \dots \mathfrak{q}_s$ then $r = s$ and there exists a bijection
$\sigma : \{1, \dots, r\} \longrightarrow \{1, \dots, s\}$ st $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$ for all i.

Example: $k = \mathbb{Z}[\sqrt{-10}]$
Consider $\mathfrak{p} = (2, \sqrt{-10})$, $\mathfrak{q} = (5, \sqrt{-10})$

$\mathfrak{p}^2 = (2, \sqrt{-10})(2, \sqrt{-10}) = (4, 2\sqrt{-10}, -10) = (4, 2\sqrt{-10}, -10, 2) = (2)$
$\mathfrak{q}^2 = (5, \sqrt{-10})(5, \sqrt{-10}) = (25, 5\sqrt{10}, -10) = (25, 5\sqrt{10}, -10, 5) = (5)$
$\mathfrak{p}\mathfrak{q} = (2, \sqrt{-10})(5, \sqrt{-10})$
$= (10, 2\sqrt{-10}, 5\sqrt{-10}, -10) = (10, 2\sqrt{-10}, 5\sqrt{-10}, -10, \sqrt{-10}) = (\sqrt{-10})$.
We found $10 = 2 \times 5 = (\sqrt{-10})^2$
As ideals $(10) = (2)(5) = \mathfrak{p}^2\mathfrak{q}^2 = (\mathfrak{p}\mathfrak{q})^2$

Prime Ideals

Definition:

R a commutative ring with 1.
An ideal $\mathfrak{p} \subseteq R$ is prime if $xy \in \mathfrak{p} \Rightarrow$ either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

eg. $\mathfrak{p} = (p) \subseteq \mathbb{Z}$, then this the usual notion of primality for p.

Definition:

R is an intergral domain if $xy = 0 \Rightarrow x = 0$ or $y = 0$.
ie $\{0\}$ is prime.

Examples: $\mathbb{Z}_4$ $2 \times 2 = 4 = 0$, so $\mathbb{Z}_4$ is not an intergral domain

Example: If k is a field then k is an intergral domain
If $xy = 0$, $y \neq 0$, then $x = y^{-1}(xy) = 0$

more generally if $R \subseteq K$, then R is an intergral domain.

Lemma:

An ideal p is prime iff R/p is an intergral domain.

Proof: Exercise (? (commutative)?

Corollary:

Every maximal ideal is prime.

Proof: if $I \subseteq R$ is maximal, then R/I is a field, in particular R/I is a intergral domain, so by lemma I is prime.

The converse is false, there are prime ideals which are not maximal ideals. Let R be a ring which is an intergral domain, but not a field, eg $\mathbb{Z}$. Then $\{0\} \subseteq \mathbb{Z}$ is prime but not maximal

Proposition:

Every finite non-zero intergral domain is a field.

Proof: Let $x \in R \setminus \{0\}$. We need to find a multiplicative inverse for x. Look at $\{x, x^2, x^3, \ldots\}$

Because R finite, $\exists\, m > n \in \mathbb{N}$ st $x^m = x^n$

Then $x^m - x^n = 0$

$x^n(x^{m-n} - 1) = 0$

So $x^n = 0$ or $x^{m-n} = 1$

By induction on n, $x^n \neq 0$

Therefore $x^{m-n} = 1$

$x(x^{m-n-1}) = 1$ QED.

Proposition:

Let K be an algebraic number field. If $I \subseteq \mathcal{O}_K$ is a non zero ideal then $\mathcal{O}_K/I$ is finite.

Proof: Let $x \in I \setminus \{0\}$

$N(x) = x \times (\underbrace{\text{the product of the other } \mathbb{Q}\text{-conjugates of } x}_{\in \mathcal{O}_K})$

$\Rightarrow N(x) \in I \cap \mathbb{Z}$

$n = |N(x)|$, now $(n) \subseteq I$

Therefore $|\mathcal{O}_K / I| \leq |\mathcal{O}_K / (n)|$

As a group $\mathcal{O}_K \cong \mathbb{Z}^d$ (eg pick an intergral basis).

Under isomorphism $(n) \cong n\mathbb{Z}^d$

$|\mathcal{O}_K/(n)| = |\mathbb{Z}^d / n\mathbb{Z}^d| = n^d < \infty$ QED.

Corollary:

Every non-zero prime ideal in $\mathcal{O}_K$ is maximal

Proof: If $\mathfrak{p}$ is prime, then $\mathcal{O}_K/\mathfrak{p}$ is finite.

So $\mathcal{O}_K/\mathfrak{p}$ is a finite intergral domain $\Rightarrow \mathcal{O}_K/\mathfrak{p}$ is a field

$\Rightarrow \mathfrak{p}$ is maximal.

Example: $R = \mathbb{Z}[x]$ contains non-zero prime ideals that are not maximal. eg (x).

Last time we defined IJ for I, J ideals.

Lemma:

Let R be a ~~ring~~ commutative ring with 1.

Then an ideal $\mathfrak{p}$ is prime iff whenever I, J are ideals and $IJ \subseteq \mathfrak{p}$ either $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

Proof: $\Leftarrow$ Set $I = (x)$, $J = (y)$. Now its obvious.

$\Rightarrow$ Suppose $\mathfrak{p}$ is prime, and $IJ \subseteq \mathfrak{p}$.

Suppose $I \not\subseteq \mathfrak{p}$. Then there exists $x \in I \setminus \mathfrak{p}$

Let $y \in J$. Then $xy \in IJ \in \mathfrak{p}$, so either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

But $x \notin \mathfrak{p}$, so $y \in \mathfrak{p}$. Therefore $J \subseteq \mathfrak{p}$ as required QED.

Cautionary Example:

In $\mathbb{Z}[\sqrt{6}]$, $\sqrt{6}$ is irreducible, but not prime.

$N(\sqrt{6}) = -6$

If $\sqrt{6} = xy$, then $N(x) = \pm 2$, $N(y) = \pm 3$

If $x = a + b\sqrt{6}$, $N(x) = a^2 - 6b^2 = +2$

Reduce mod 3, then 2 is a square mod 3. Contradiction etc...

$\sqrt{6}$ irreducible.

But $\sqrt{6}$ not prime, eg $\sqrt{6} | 6 = 2 \times 3$

But $\sqrt{6}$ does not divide 2 or 3.

$N(2) = 4$, $N(3) = 9$ $\Rightarrow \sqrt{6} | 2$ or 3.

Uniqueness of Factorisation into Ideals.

Definition:

A ring R is Noetherian if every ascending chain of ideals stabilizes. In other words if we have ideals

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$$

then there exists N st $\forall n \geq N$ $I_n = I_N$.

Definition:

~~If I is a non-zero ideal~~ If $I \subseteq \mathcal{O}_K$ is a non-zero ideal, then the norm of I is $N(I) = |\mathcal{O}_K / I|$.

This is always a positive interger.

Lemma:

If K is an algebraic number field then $\mathcal{O}_K$ is noetherian.

Proof: Suppose $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$ is a sequence of non-zero ideals. An isomorphism theorem asserts that

$$\mathcal{O}_K / I_{n+1} \cong \frac{(\mathcal{O}_K / I_n)}{(I_{n+1}/I_n)}$$

so $N(I_{n+1}) = N(I_n) / |I_{n+1}/I_n|$

so $N(I_{n+1}) \leq N(I_n)$ with equality iff $I_n = I_{n+1}$

We have $N(I_1) \geq N(I_2) \geq \dots \geq N(I_n) \geq \dots > 0$

a non-increasing sequence of natural numbers

Let N be such that $N(I_n) = N(I_N)$ for $n \geq N$

Then $I_n = I_N$ as required QED.

This is useful, for instance:

Lemma: ~~Let~~

Let $I \subseteq \mathcal{O}_K$ be any non zero ideal. There are maximal ideals $p_1, \dots, p_r$ such that $p_1 \cdot \ldots \cdot p_r \subseteq I$

This is the analogue of the statement "every interger divides a product of primes"

Proof: Suppose I is maximal counterexample; that is if $I \subsetneq J$, then J satisfies the conclusion of the lemma.

If I is a maximal ideal, then $I = p_1$, $r = 1$ satisfies the lemma.

So if I is not a maximal ideal. Therefore, I is not prime.

Therefore there exists A, B such that $A \not\subseteq I$, $B \not\subseteq I$ but $AB \subseteq I$

Let $A' = (A, I)$ $B' = (B, I)$

Then $A'B' = (x_1 a_1 + y_1 i_1)(x_2 b_2 + y_2 i_2) = (x_1 x_2 a_1 b_2 + x_1 y_2 a_1 i_2, \; x_2 b_2 y_1 i_1 + y_1 y_2 i_1 i_2) \in I$

$x_1, y_1 \in \mathcal{O}_K$ $\quad x_2, y_2 \in \mathcal{O}_K$

$a_i \in A$, $i_1 \in I$ $\quad b_2 \in B$, $i_2 \in I$

Let $A' \not\subseteq I$, $B' \not\subseteq I$.

Now $I \subsetneq A'$ so A' satisfies the conclusion of the lemma

Likewise $I \subsetneq B'$ so B' satisfies the conclusion of the lemma.

~~Therefor~~ Therefore there are prime ideals $p_1 \dots p_r$ with $p_1 \dots p_r \subseteq A'$

and there are prime ideals $q_1 \dots q_s$ with $q_1 \dots q_s \subseteq B'$

so $p_1 \dots p_r q_1 \dots q_s \subseteq A'B' \subseteq I$. QED.

Lemma:

Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal.

If $x \in K$ satisfies $xI \subseteq I$ then $x \in \mathcal{O}_K$

Proof: $I \subseteq \mathcal{O}_K$ so $I = \text{span}_{\mathbb{Z}}\{b_1 \dots b_r\}$ for some $b_i \in \mathcal{O}_K$
So let $xb_i = \sum_{j=1}^{r} a_{ij} b_j$ for $a_{ij} \in \mathbb{Z}$.

Let $A = (a_{ij})$

$$x\begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = A\begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} \qquad \text{so} \quad (A - x(Id_{r\times r}))\begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Therefore x is an eigenvalue of A, and so satisfies the characteristic polynomial $\chi_A(x) = 0$
Since this is monic and intergral, $x \in \mathcal{O}_K$ QED.

Definition:

A fractional ideal is a non-empty subset $I \subseteq k$, such that
- I is closed under addition.
- If $x \in \mathcal{O}_K$ and $y \in I$ then $xy \in I$
- There exists $n \in \mathbb{N}\setminus\{0\}$ such that $nI \subseteq \mathcal{O}_K$.

eg. $I = \{\frac{a}{2} \mid a \in \mathbb{Z}\} \subseteq \mathbb{Q}$. $n = 2$. $nI \subseteq \mathcal{O}_{\mathbb{Q}}$.

Lemma:

Let I be an ideal in $\mathcal{O}_K$. Then $N(I) \in I$.

? Proof: Think about $\mathcal{O}_K/I$ $(x \in I)$
$N(I) + I = N(I)N(1+I)$
Legrange's theorem tells us that $o(1+I) \mid |\mathcal{O}_K/I| = N(I)$.
So $N(I) + I = I \iff N(I) \in I$. QED.

Lemma:

Let I be a non-zero ideal and define $I^{-1} = \{y \in k \mid yI \subseteq \mathcal{O}_K\}$
Then I^{-1} is a fractional ideal.

Proof: We need to check:
a) I^{-1} is closed under addition
b) If $x \in \mathcal{O}_K$ and $y \in I^{-1}$ then $xy \in I^{-1}$

c) There exists $n \in \mathbb{N} \setminus \{0\}$ such that $nI^{-1} \subseteq \mathcal{O}_K$.

a) is obvious.

b) Let $x \in \mathcal{O}_K$, $y \in I^{-1}$. Then $xyI \subseteq x\mathcal{O}_K = \mathcal{O}_K$.

c) Let $n = N(I)$. Suppose $y \in I^{-1}$.

$ny = yn \in yI \subseteq \mathcal{O}_K$ QED.

Remark: If $I \subseteq J$ are ideals then $J^{-1} \subseteq I^{-1}$

In particular for any I we have $I \subseteq \mathcal{O}_K$ so $\mathcal{O}_K^{-1} \subseteq I^{-1}$

By lemma above $\mathcal{O}_K^{-1} = \mathcal{O}_K$, so $\mathcal{O}_K \subseteq I^{-1}$

Analogy: If $n \in \mathbb{Z} \setminus \{0\}$ then $n^{-1} \leq |1|$.

Lemma:

~~Let~~ If $I \subseteq \mathcal{O}_K$ is an ideal and $I \neq \mathcal{O}_K$ then $I^{-1} \neq \mathcal{O}_K$.

Proof: Let $I \subseteq I'$ where I' is a maximal ideal

If $(I')^{-1} \neq \mathcal{O}_K$ then $I^{-1} \supseteq (I')^{-1} \supsetneq \mathcal{O}_K$ so $I^{-1} \neq \mathcal{O}_K$

So we may assume that I is a maximal ideal.

Let $a \in I$ so therefore $(a) \supseteq p_1 \dots p_r$ which p_i's prime ideals

Choose a so that r is as small as possible.

Now $I \supseteq (a) \supseteq p_1 \dots p_r$

But I is prime, so $p_i \subseteq I$ for some i

But p_i is maximal so $p_i = I$, wlog $i = 1$.

But $(a) \not\supseteq p_2 \dots p_r$ by minimality of r, so there exists some

$b \in p_2 \dots p_r \setminus (a)$

We will prove that $b/a \in I^{-1} \setminus \mathcal{O}_K$.

$(b)I = I(b) \subseteq p_1 p_2 \dots p_r \subseteq (a)$

so $b/a \, I \in \mathcal{O}_K \Rightarrow b/a \in I^{-1}$

But $b \notin (a)$ so $b/a \notin \mathcal{O}_K$.

Lemma:

If $p \subseteq \mathcal{O}_K$ is a maximal ideal then $p^{-1}p = \mathcal{O}_K$.

?

Proof: By definition of p^{-1}, $p^{-1}p \subseteq O_K$.
So $p^{-1}p$ is an ideal in O_K. On the other hand $p \subseteq p^{-1}p \subseteq O_K$
so either $p^{-1}p = O_K$ or $p^{-1}p = p$ *
By an earlier lemma if * occured then $p^{-1} \subseteq O_K \Rightarrow p^{-1} = O_K$, contradiction.

Theorem:

Let $I \subseteq O_K$ be a non-zero ideal. Then there are maximal ideals $p_1, \dots, p_r$ unique up to reordering, such that
$$I = p_1 \cdots p_r.$$

Proof: (Existance).
Suppose I is a maximal counterexample.
Clearly I is not a prime ideal, but $I \subsetneq p$ for some prime ideal p. Now $I \subseteq p^{-1}I \subseteq p^{-1}p = O_K$.
Also $p^{-1}I \neq I$, so because I is a maximal counter example, there exists prime ideals $p_2 \dots p_r$ such that $p^{-1}I = p_2 \dots p_r$
Therefore $I = O_K I = (pp^{-1})I = p p_2 \dots p_r$.
This proves existance.
(Uniqueness) Suppose $p_1 \dots p_r = q_1 \dots q_s$ all prime ideals
Then $p_1 \dots p_r \subseteq q_1$, so $p_i \subseteq q_1$ for some i wlog $i=1$
Because p_1 is maximal $p_1 = q_1$
So $(p_1^{-1}p_1)p_2 \dots p_r = (q_1^{-1}q_1)q_2 \dots q_s$ and proceed by induction

We want to investigate when O_K is a PID. Morally? how far O_K is from being a PID is measurable by the class group Cl_K.
Roughly $Cl_K = \{\text{fractional ideals}\}/\{\text{principle ideals}\}$.

Let $\mathcal{I}_K$ be the group of fractional ideals in O_K.
Multiplication of two fractional ideals is defined as it is for ideals:
If I, J are fractional ideals then $IJ = \{\text{finite sums of } ab \mid a \in I, b \in J\}$
$$= \{\textstyle\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J\}.$$
This is the fractional ideal "generated" by products of elements of I and J.
Note that IJ is really a fractional ideal:
If $mI \subseteq O_K$, $nJ \subseteq O_K$ then $mn\, IJ \subseteq O_K$.

The identity ~~of~~ in $\mathcal{L}_K$ is $\mathcal{O}_K$
Associativity is obvious.

We still need to prove that inverses exist.
Last time we proved that if $\mathfrak{p}$ is maximal then $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$.

Theorem:

If $I \in \mathcal{L}_K$ then there exists $I' \in \mathcal{L}_K$ such that $II' = \mathcal{O}_K$.

Proof: By definition, $\exists n \in \mathbb{N}$ such that $nI \subseteq \mathcal{O}_K$, so nI is an ideal
Let $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ be maximal ideals such that $nI = \mathfrak{p}_1 \cdots \mathfrak{p}_m$
Let $I' = (n)\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$
Now $II' = I(n)\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$
$= nI\,\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1}$
$= (\mathfrak{p}_1 \cdots \mathfrak{p}_m)(\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_m^{-1})$
$= \mathcal{O}_K.$ QED.

So $\mathcal{L}_K$ is a group.

So what does it mean to say $I \mid J$?
There are two sensible definitions.
1. $I \supseteq J$
2. $\exists I'$ an ideal such that $J = II'$

Corollary:

If I, J be ideals in $\mathcal{O}_K$. Then $I \supseteq J$ if and only if there exists an ideal I' such that $J = II'$.
In either case we write $I \mid J$.

Proof: $\Leftarrow$ easy.
$\Rightarrow$ Suppose $I \supseteq J$. Set $I' = I^{-1}J$.
We need to prove $I' \subseteq \mathcal{O}_K$, so it is a genuine ideal
But $I'I = J \subseteq I$, so $\forall x \in I'$ $xI \subseteq I \Rightarrow x \in \mathcal{O}_K$ by earlier lemma
Therefore $I' \subseteq \mathcal{O}_K$, so it is an ideal as required. QED

Norms of Ideals

Theorem:

If $I, J \subseteq \mathcal{O}_K$ are ideals, $N(IJ) = N(I)N(J)$.

Proof: Write $J = \mathfrak{p}_1 \cdots \mathfrak{p}_m$. Suppose we have already proved that $N(I\mathfrak{p}) = N(I)N(\mathfrak{p})$ for $\mathfrak{p}$ maximal.

Then $N(IJ) = N(I\mathfrak{p}_1 \cdots \mathfrak{p}_m)$
$= N(I\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1})N(\mathfrak{p}_m)$
$\vdots$
$= N(I)N(\mathfrak{p}_1)\cdots N(\mathfrak{p}_m)$ by induction on m.

Similarly by induction on m $N(J) = N(\mathfrak{p}_1)\cdots N(\mathfrak{p}_m)$

So $N(IJ) = N(I)N(\mathfrak{p}_1)\cdots N(\mathfrak{p}_m)$
$= N(I)N(J)$.

So it is enough to prove theorem with $J = \mathfrak{p}$ maximal.

We want to prove $N(I\mathfrak{p}) = N(I)N(\mathfrak{p})$.

$$|\mathcal{O}_K / I\mathfrak{p}| = |\mathcal{O}_K / I|\underbrace{|\mathcal{O}_K / \mathfrak{p}|}$$

← enough to prove this equality.

By an isomorphism theorem,

$$|\mathcal{O}_K / I| = |\mathcal{O}_K / I\mathfrak{p}| \,/\, |I / I\mathfrak{p}|$$

Let $a \in I \setminus I\mathfrak{p}$

Define $\Phi : \mathcal{O}_K \longrightarrow I / I\mathfrak{p}$

$x \longmapsto ax + I\mathfrak{p}$.

Its clear that this is a homomorphism of additive groups.

We are going to prove

1. Φ is surjective
2. $\operatorname{Ker} \Phi = \mathfrak{p}$.

1. There are no ideals $I \supsetneq J \supsetneq I\mathfrak{p}$.

If $I \supseteq J \supseteq I\mathfrak{p} \Rightarrow \mathcal{O}_K \supseteq I^{-1}J \supseteq \mathfrak{p}$
$\Rightarrow I^{-1}J = \mathcal{O}_K$ or $\mathfrak{p}$
$\Rightarrow J = I$ or $J = I\mathfrak{p}$.

Therefore $I = (a, I\mathfrak{p})$. so for all $x \in I$, $\exists y \in \mathcal{O}_K$ such that $x \in ay + I\mathfrak{p}$.

Therefore $\Phi(y) = ay + I\mathfrak{p} = x + I\mathfrak{p}$

Φ is surjective.

2. $\Phi : x \longmapsto \underset{\overset{\cap}{I}}{a}x + I\mathfrak{p}$

If $x \in \mathfrak{p}$ then $\Phi(x) = ax + I\mathfrak{p} = I\mathfrak{p} \Rightarrow \operatorname{Ker}\Phi \supseteq \mathfrak{p}$.

But $\Phi(1) = a + I\mathfrak{p} \neq I\mathfrak{p}$ $\therefore$ $\operatorname{Ker}\Phi \neq \mathcal{O}_K \Rightarrow \operatorname{Ker}\Phi = \mathfrak{p}$.

Hence by an isomorphism theorem $I/I\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}$, so they have the same cardinality QED.

Next time: $\{N((\alpha))\} = |N(\alpha)|$

We will use a theorem from another course:

Theorem: Let $H \subseteq \mathbb{Z}^d$ be a subgroup such that $|\mathbb{Z}^d/H| < \infty$. Then there exists linearly independent $c_1, \dots, c_d \in \mathbb{Z}^d$ such that $H = \mathrm{span}_{\mathbb{Z}}\{c_1 \dots c_d\}$

Furthermore $|\mathbb{Z}^d/H| = |\det(c_1 \dots c_d)|$.

Proposition:

Let $I \subseteq \mathcal{O}_K$ be a non-zero ~~basis~~ ideal with $I = \mathrm{span}_{\mathbb{Z}}\{c_1 \dots c_d\}$

Let B be an intergral basis for $\mathcal{O}_K$ and let $\mathcal{C} = \{c_1 \dots c_d\}$.

Then $N(I) = \sqrt{\dfrac{\Delta\mathcal{C}}{\Delta B}}$

Proof: B and $\mathcal{C}$ are both basis for k over $\mathbb{Q}$. Let M be the transition matrix from B to $\mathcal{C}$.

By the theorem $N(I) = |\mathcal{O}_K/I| = |\det(c_1 \dots c_d)| = |\det M|$.

On the other hand $\Delta\mathcal{C} = \det M^2 \Delta B$

$= N(I)^2 \Delta B$. as required QED.

Corollary: If $a \in \mathcal{O}_K$ then $N((a)) = |N(a)|$

Proof: Let B be an intergral basis. Let $\mathcal{C} = aB$, a $\mathbb{Z}$-basis for (a).

$$\begin{aligned}
\text{Then } \Delta\mathcal{C} = \Delta aB &= (\det \sigma_i(ab_j)) \\
&= (\det \sigma_i(a)\sigma_i(b_j)) \\
&= (\textstyle\prod_i \sigma_i(a))^2 (\det \sigma_i(b_j))^2 \\
&= (N((a)))^2 \Delta B
\end{aligned}$$

Therefore $|N(a)| = \sqrt{\dfrac{\Delta\mathcal{C}'}{\Delta B}} = N((a))$ QED.

Corollary:

There are only finitely many ideals with a given norm, ie. for each n, $|\{I \subseteq O_K \mid N(I)=n\}| < \infty$.

Proof: Suppose $N(I)=n$. Then $n \in I$, by a previous lemma.
So $(n) \subseteq I \Leftrightarrow I \mid (n)$
Let $(n) = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorisation in O_K
Then $I = p_1^{f_1} \cdots p_r^{f_r}$ for $f_i \leq e_i$.

Norms of Prime Ideals

In order to understand factorisation of intergers (ie $\mathbb{Z}$) into maximal ideals we need to be able to factorise primes $p \in \mathbb{Z}$ into a product of maximal ideals in O_K.
In this section we will prove Dedekind's Prime Factorisation Theorem, which tells us how to do this.

Proposition:

Let $R \subseteq S$ are both commutative rings with 1.
If $\mathfrak{p} \in S$ is a prime ideal, then $\mathfrak{p} \cap R \subseteq R$ is a prime ideal in R.

Proof: Notice that $\mathfrak{p} \cap R$ is an ideal in R
If $x, y \in R$ and $xy \in \mathfrak{p} \cap R$, then x or $y \in \mathfrak{p} \Rightarrow x$ or $y \in \mathfrak{p} \cap R$. QED.

Therefore if $\mathfrak{p} \subseteq O_K$ is a prime ideal then $\mathfrak{p} \cap \mathbb{Z}$ is prime in $\mathbb{Z}$.
$\Rightarrow \mathfrak{p} \cap \mathbb{Z} = (p)$.

Definition:

We say $\mathfrak{p}$ lies above p and write $\mathfrak{p} \mid p$

Hence every prime $\mathfrak{p} \subseteq O_K$ lies above some prime $p \in \mathbb{Z}$, so to find all the prime ideals of O_K we simply need to factorise the primes $p \in \mathbb{Z}$.

Proposition:

Let $\mathfrak{p}$ be an ideal in O_K. Then if $N(\mathfrak{p})$ is prime then $\mathfrak{p}$ is prime.

Proof: ~~If $xy \in \mathfrak{p}$ then $(x)(y) \subseteq \mathfrak{p}$~~ Let $\mathfrak{p} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ be the factorisation into maximal ideals. Then $N(\mathfrak{p}) = N(\mathfrak{p}_1)^{e_1} \dots N(\mathfrak{p}_r)^{e_r}$

$\Rightarrow r = 1,\ e_1 = 1$ because $N(\mathfrak{p})$ prime.

$\mathfrak{p} = \mathfrak{p}_1 \Rightarrow \mathfrak{p}$ prime.

Proposition:

Norms of Prime Ideals

If $\mathfrak{p}$ is prime then $N(\mathfrak{p}) = p^r$ for some prime $p \in \mathbb{Z}$ and some $1 \le r \le [K:\mathbb{Q}]$.

Proof: Suppose $\mathfrak{p}$ lies above p. Then $(p) \subseteq \mathfrak{p}$. $\Rightarrow \mathfrak{p} \mid (p)$

$\Rightarrow (p) = \mathfrak{p} I$

$\Rightarrow N((p)) = N(\mathfrak{p}) N(I)$

so $N(\mathfrak{p}) \mid N(p) = p^d$

$\Rightarrow N(\mathfrak{p}) = p^r \quad 1 \le r \le d$ as required. QED.

Dedekind's Prime Factorisation Theorem

Suppose $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α.

Let $m = m_\alpha$. Let $p \in \mathbb{Z}$ be a prime. Let $\bar{m} \in \mathbb{F}_p[x]$ be the reduction of m mod p.

Suppose $\bar{m} = \bar{m}_1^{e_1} \dots \bar{m}_r^{e_r}$ is the unique factorisation of $\bar{m} \in \mathbb{F}_p[x]$ into irreducibles with each $\bar{m}_i$ monic and $\bar{m}_i \ne \bar{m}_j$ unless $i=j$

Then (p) factorises in $\mathcal{O}_K$ as:

$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$

where $\mathfrak{p}_i = (p, m_i(\alpha))$ where $m_i \in \mathbb{Z}[x]$ is monic and reduces mod p to $\bar{m}$.

Each $\mathfrak{p}_i$ is maximal and $N(\mathfrak{p}_i) = p^{\deg m_i}$.

Furthermore $\mathfrak{p}_i \ne \mathfrak{p}_j$ unless $i \ne j$

Proof: Recall we showed that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(m_\alpha)$

~~In exactly the same way~~ As a consequence we have $\mathcal{O}_K = \mathbb{Z}[\alpha] \overset{\Phi}{\cong} \mathbb{Z}[x]/(m)$

$\alpha \longmapsto x + (m_\alpha)$

Therefore for each i, we have an isomorphism

$$\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}[x]/(m, p, m_i)$$

$$\cong \mathbb{F}_p[x]/(\bar{m}, \bar{m}_i)$$

$= \mathbb{F}_p[x]/(\bar{m}_i) \cong \mathbb{F}_{p^{\deg \bar{m}_i}}$

$\bar{m}_i$ is irreducible in $\mathbb{F}_p[x] \Rightarrow (\bar{m}_i)$ is maximal in $\mathbb{F}_p[x]$

$\Rightarrow \mathbb{F}_p[x]/(\bar{m}_i)$ is a field $\Rightarrow \mathcal{O}_K/\mathfrak{p}_i$ is a field

$\Rightarrow \mathfrak{p}_i$ is maximal in $\mathcal{O}_K$.

Also $N(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = p^{\deg \bar{m}_i} = p^{\deg m_i}$

The next step is to prove that: $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq (p)$

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

$= (p \times \text{stuff}, \prod_{i=1}^{r} m_i(\alpha)^{e_i})$

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

But mod p,

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

so because α is a root of m $\prod_{i=1}^{r} m_i(\alpha)^{e_i} \equiv 0 \bmod p$.

Therefore $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq (p, \prod_{i=1}^{r} m_i(\alpha)^{e_i}) = (p)$.

To prove that $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = (p)$ we will show that there norms are the same.

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

$= \prod_{i=1}^{r} p^{e_i \deg m_i}$

$= p^{\sum e_i \deg m_i}$

$= p^{\sum \deg(\bar{m}_i^{e_i})}$

$= p^{\deg \bar{m}}$

$= p^{\deg m} = N(p)$

$= N((p))$.

Because $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq (p)$ and they have the same norm it follows $\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = (p)$

It only remains to ~~show~~ prove that $\mathfrak{p}_i \neq \mathfrak{p}_j$ unless $i = j$

Suppose $\mathfrak{p}_i = \mathfrak{p}_j$

Then $\mathcal{O}_K/\mathfrak{p}_i = \mathcal{O}_K/\mathfrak{p}_j$

$\qquad \cong \qquad\qquad \cong$

$\mathbb{F}_p[x]/(\bar{m}_i) \quad \mathbb{F}_p[x]/(\bar{m}_j)$.

$\Rightarrow \bar{m}_i(x) \in (\bar{m}, (x)) \subseteq \mathbb{F}_p[x]$

$\Rightarrow \bar{m}_j \mid \bar{m}_i$

But $\bar{m}_i$ irreducible in $\mathbb{F}_p[x]$

$\Rightarrow \bar{m}_j = \bar{m}_i \Rightarrow i = j$ QED.

Example: Let $\sigma : k \to k$ be a field isomorphism.
Then $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ and so

$$N(\sigma(I)) = |\mathcal{O}_K / \sigma(I)|$$
$$= |\sigma(\mathcal{O}_K)/\sigma(I)|$$
$$= |\mathcal{O}_K / I|$$
$$= N(I).$$

So suppose $k = \mathbb{Q}(\sqrt{3})$

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

$$N(2, 1+\sqrt{3})^2 = N((2, 1+\sqrt{3})(2, 1-\sqrt{3}))$$
$$= N(4, 2(1+\sqrt{3}), 2(1-\sqrt{3}), -2)$$
$$= N(2)$$
$$= 4$$

$\Rightarrow N(2, 1+\sqrt{3}) = 2.$

Number field with ring of intergers $\mathcal{O}_K$.

$\mathfrak{p}$ prime ideal $\quad \mathfrak{p} \cap \mathbb{Z} = (p)$ prime ideal in $\mathbb{Z}$, p prime

How to factorise (p) in $\mathcal{O}$.

Dedekind Factorisation ~~Lemma~~ Thm:

Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let f be the minimal polynomial of α over $\mathbb{Z}$ ($f(x) \in \mathbb{Z}[x]$).
Let p be prime. Factorise $f(x) = f_1(x)^{e_1} f_2(x)^{e_2} \dots f_r(x)^{e_r} \pmod p$ in the field $\mathbb{F}_p$, where f_i's are irreducible in $\mathbb{F}_p[x]$, f_i monic, $f_i \neq f_j$.
Then $(p) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_k^{e_r}$, $\mathfrak{p}_i = (p, f_i(\alpha))$ prime = maximal in $\mathcal{O}$.
$\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ $(i, j = 1 \dots r)$.
$N(\mathfrak{p}_i) = p^{e_i}$

Example: $F = \mathbb{Q}(\sqrt{6})$ $\quad \mathcal{O} = \mathbb{Z}[\sqrt{6}]$

$p = 2, 3, 5, 7, 11$

$\alpha = \sqrt{6}$, $\quad f(x) = x^2 - 6$

$x^2 - 6 \equiv x^2 \pmod 2$

$x^2 - 6 \equiv x^2 \pmod 3$

$x^2 - 6 \equiv (x+1)(x-1) \pmod 5$

x	$f(x)$
0	-6
± 1	-5
± 2	-2
± 3	3
± 4	10
± 5	19

$x^2-6 \equiv x^2-6 \pmod 7$
$x^2-6 \equiv x^2-6 \pmod{11}$.

Second approach: $x^2 \equiv 6 \pmod 5$ squares mod 5
$\equiv 1 \pmod 5$ $0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4 \ldots$

$x^2-6 \equiv x^2-1 = (x+1)(x-1)$

mod 7, squares mod 7: $0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 2,\ 4^2 \equiv 2 \ldots$

$f_1(x) = x \quad e_1 = 2$

$(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (2, f_1(\sqrt{6})) = (2, \sqrt{6})$

$N(\mathfrak{p}_2) = p^{\deg f_1} = 2$.

$(3) = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = (3, f(\sqrt{6})) = (3, \sqrt{6})$

$N(\mathfrak{p}_3) = 3^{\deg f_1} = 3$

~~(5) NF~~

(5) $f_1(x) = x+1$ $f_2(x) = x-1$ $e_1 = e_2 = 1$

$(5) = \mathfrak{p}_{5,1}^1 \mathfrak{p}_{5,1}^1$ with $\mathfrak{p}_{5,1} = (5, f_1(\sqrt{6})) = (5, \sqrt{6}+1)$

$\mathfrak{p}_{5,2} = (5, f_2(\sqrt{6})) = (5, \sqrt{6}-1)$

$N(\mathfrak{p}_{5,1}) = 5^1 = 5$ $N(\mathfrak{p}_{5,2}) = 5^1 = 5$.

mod 7 irreducible $f(x) = f_1(x)$ $e_1 = 1$

$(7) = (7, f\sqrt{6}) = (7, 0) = (7) = \mathfrak{p}_7$ prime. $N(\mathfrak{p}_7) = 7^{\deg f_1} = 7^2 = 49$

mod 11 irreducible $f(x) = f_1(x)$ $e_1 = 1$.

$(11) = (11, f(\sqrt{6})) = (11, 0) = (11) = \mathfrak{p}_{11}$

$N(\mathfrak{p}_{11}) = \cancel{7}\,11^{\deg f_1} = 11^2 = 121$.

Example: $\mathbb{Q}(\sqrt[3]{2})$ with $\mathcal{O} = \mathbb{Z}[\sqrt[3]{2}]$ $\alpha = \sqrt[3]{2}$. $p = 2, 3, 5, 7$

$f(x) = x^3 - 2$ minimal polynomial.

x	$f(x)$
0	-2
1	-1
2	6
3	25
-1	-3
-2	-10
-3	-29

$x^3 - 2 \equiv x^3 \pmod 2$

$x^3 - 2 \equiv x^3 + 1 \pmod 3$

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

$= (x+1)(x^2 + 2x + 1)$

$= (x+1)^3$

mod 5, 3 is a root (-2).

$$x^3 - 2 = (x+2)\underbrace{(x^2 - 2x + 4)}_{\text{irreducible.}}$$

	x^3	x^2	x	1
	1	0	0	-2
-2	↓	-2	-4	-8
	1	-2	-4	-10

x	$x^2 - 2x + 4$
0	4
1	3
2	4
3	$7 = 2$
4	$12 = 2$.

mod 7 x^3-2 has no root, is irreducible mod 7

$(2) = \wp_2^3$ with $\wp_2 = (2, f_1(\sqrt[3]{2})) = (2, \sqrt[3]{2})$

$x^3 = \cancel{f_2} f_1^3$ $N(\wp_2) = 2^{\deg f_1} = 2$

$(3) = \wp_3^3$ with $\wp_3 = (3, f_1(\sqrt[3]{2})) = (3, \sqrt[3]{2}+1)$

$(x+1)^3 = f_1^3$ $N(\wp_3) = 3^{\deg f_1} = 3.$

$(5) = \wp_{51} \cdot \wp_{52}$ $e_1 = e_2 = 1$ $f_1(x) = x+2$ $f_2(x) = x^2-2x+4$

$\wp_{51} = (5, f_1(\sqrt[3]{2}))$

$= (5, \sqrt[3]{2}+2)$ $N(\wp_{51}) = 5^1 = 5$

$\wp_{52} = (5, f_2(\sqrt[3]{2}))$

$= (5, \sqrt[3]{4} - 2\sqrt[3]{2}+4)$ $N(\wp_{52}) = 5^{\deg f_2} = 5^2 = 25.$

mod 7 x^3-2 irreducible

$(7) = \wp_7 = (7, f(\sqrt[3]{2})) = (7)$

$N(\wp_7) = 7^{\deg f} = 7^3.$

How to factorise an ideal I into maximal prime ideals:

1. Compute $N(I)$
2. Factor $N(I)$ over $\mathbb{Z}$. For each p prime factor of $N(I)$ factor (p) over $\mathcal{O}$
3. Consider all possible combinations giving norm $= N(I)$.
4. Find ~~each~~ which combinations is the right one.

   Recall $I \subset J \Leftrightarrow J \mid I$

   $\wp \mid I$ then $I \subset \wp$ it is enough to check whether generators of I are in $\wp$.

Example: $R = \mathbb{Q}(\sqrt{6})$ $I = (12 + 7\sqrt{6})$

$N(I) = |N(12+7\sqrt{6})|$

$= |(12+7\sqrt{6})(12-7\sqrt{6})|$

$= |144 - 7^2 6|$

$= |144 - 49 \cdot 6|$

$= |144 - 294|$

$= |150|$

$150 = 25 \cdot 6 = 5^2 \cdot 2 \cdot 3$

$(2) = \mathfrak{p}_2^2 \quad N(\mathfrak{p}_2) = 2$

$(3) = \mathfrak{p}_3^2 \quad N(\mathfrak{p}_3) = 3$

$(5) = \mathfrak{p}_{51}\mathfrak{p}_{52} \quad N(\mathfrak{p}_{51}) = N(\mathfrak{p}_{52}) = 5.$

Recall $N(I_1 I_2) = N(I_1)N(I_2)$

$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{51}^2$ or $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{51}\mathfrak{p}_{52}$ or $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{52}^2$

But $\mathfrak{p}_{51}\mathfrak{p}_{52} = (5)$, $\mathfrak{p}_{51}\mathfrak{p}_{52} = (5) \mid I$

$\iff I \subset (5)$

Impossible $12+7\sqrt{6} \in (5)$ since coeffs ~~do~~ not divisible by 5.

So $I \neq \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{51}\mathfrak{p}_{52}$

$\mathfrak{p}_{51} = (5, \sqrt{6}+1) \quad \mathfrak{p}_{52} = (5, \sqrt{6}+2).$

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

$\iff (12+7\sqrt{6}) \subset (5, \sqrt{6}+1) = \mathfrak{p}_{51}$

$\iff \mathfrak{p}_{51} \mid (12+7\sqrt{6}) = I$

$\implies I = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{51}^2$

Class group is $\dfrac{\text{all fraction ideals}}{\text{all principle fractional ideals.}}$

The Class Group.

k-number field

How close is $\mathcal{O}_k$ to being a principle ideal domain?

NB: If $\mathcal{O}_k$ is a PID then it is also a UFD ~~state~~ because we can always factorise uniquely into ideals.

$\mathcal{I}_k$ = group of non-zero fractional ideals with multiplication.

$\mathcal{P}_k$ = subgroup generated by principle ideals.

$$\boxed{Cl_k = \mathcal{I}_k / \mathcal{P}_k \text{ is the class group of } k.}$$

If $Cl_k = 0$ then $\mathcal{O}_k$ is a PID and a UFD.

Theorem:

Cl_K is finite.

Key Lemma:

There is a constant c depending only on K, such that for any non-zero ideal $I \subseteq K$ there exists non-zero $x \in I$ satisfying $|N(x)| \leq c N(I)$.

Proof of theorem (using key lemma):

Let $I \subseteq K$ be any fractional ideal. Then there exists $n \in \mathbb{N}$ such that $(n)I \subseteq \mathcal{O}_K \Rightarrow (n)I$ is an ideal.
Because (n) is principle ideal I and $(n)I$ represent the same element of Cl_K. So every element of Cl_K is represented by an ideal.
Now let $I \subseteq \mathcal{O}_K$ be an ideal.
We will prove that there is an ideal J that represents the same element of Cl_K with $N(J) \leq c$.
Let J' be an ideal in the class ~~proof~~ of I^{-1}. By the key Lemma $\exists x \in J' \setminus \{0\}$ such that $|N(x)| \leq c N(J')$.
We have $(x) \subseteq J' \Leftrightarrow J' \mid (x)$

$\Leftrightarrow \exists$ ideal J such that $J \cdot J' = (x)$

In the class group we have $J' \sim I^{-1}$ but $J \cdot J' \sim id$
so $J \sim (I^{-1})^{-1} = I$
Now $c N(J') \geq |N(x)| = N((x)) = N(JJ') = N(J)N(J')$
$\Rightarrow c \geq N(J)$.

In conclusion every element of the class group is represented by an ideal with norm $\leq c$. Will use this to compute Cl_K.

But there are only finitely many such ideals because there are only finitely many ideals of each norm.
Therefore $|Cl_K| < \infty$.

The Minkowski Constant

c is called the minkowski constant.
To compute Cl_K we need to be able to compute c.
Recall that we have field embeddings $\sigma_1 \dots \sigma_d : K \hookrightarrow \mathbb{C}$.
If $\sigma_i(K) \subseteq \mathbb{R}$ then we call σ_i a real embedding
Otherwise σ_i is complex.

eg. $k = \mathbb{Q}(\sqrt[3]{2})$

$\sigma_1 : \sqrt[3]{2} \longmapsto \sqrt[3]{2}$ is real

$\sigma_2 : \sqrt[3]{2} \longmapsto \omega\sqrt[3]{2}$ is complex ($\omega = e^{2\pi i/3}$)

Let r = # of real embeddings

$2s$ = # of complex embeddings. (because the are in complex conjugate pairs)

Then $d = r + 2s$.

Let B be any intergral basis for k.

Then $c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta(B)|}$

Example : $k = \mathbb{Q}(i)$

$\mathcal{O}_k = \mathbb{Z}[i]$ $B = \{1, i\}$. $\Delta B = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4$.

$s = 1$ because $\sigma : i \longmapsto i$

$\bar{\sigma} : i \longmapsto -i$ is a pair of complex embeddings $k \to \mathbb{C}$.

So $c = \left(\frac{2}{\pi}\right)^1 \sqrt{|-4|} = \frac{2 \times 2}{\pi} < 2$ (because $\pi > 2$).

If I represents a non-trivial class in Cl_k, then I is equivalent to some ideal J with $N(J) \leq c < 2$.

$\Rightarrow N(J) = 1 \Rightarrow J = \mathcal{O}_k$.

This contradicts the hypothesis that I represented a non-trivial element of Cl_k

Therefore $Cl_k = 0$.

Example: $k = \mathbb{Q}(\sqrt{6})$

$\mathcal{O}_k = \mathbb{Z}[\sqrt{6}]$ $B = \{1, \sqrt{6}\}$ $\Delta B = \begin{vmatrix} 1 & \sqrt{6} \\ 1 & -\sqrt{6} \end{vmatrix}^2 = -24$

$s = 0$

$c = \left(\frac{2}{\pi}\right) \sqrt{|-24|} = \sqrt{24} < 5$

So we are only interested in ideals with norms > 1 and < 5, ie $2, 3, 4 = 2 \times 2$

Recall that in $\mathcal{O}_k$ we have the following ideals of small norm

$(2) = \mathfrak{p}_2^2$ where $\mathfrak{p}_2 = (2, \sqrt{6})$ $N(\mathfrak{p}_2) = 2$

$(3) = \mathfrak{p}_3^2$ where $\mathfrak{p}_3 = (3, \sqrt{6})$ $N(\mathfrak{p}_3) = 3$.

$(5) = \mathfrak{p}_5 \mathfrak{q}_5$ where $\mathfrak{p}_5 = (5, \sqrt{6} - 1)$ $\mathfrak{q}_5 = (5, \sqrt{6} + 1)$ $N(\mathfrak{p}_5) = N(\mathfrak{q}_5) = 5$.

So the ideals of norm $2, 3, 4$ are

$\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_2^2 \neq (2)$

Want non PID.

Now we have to decide whether $\mathfrak{p}_2, \mathfrak{p}_3$ are principle.

NB: $\mathfrak{p}_2 = (x) \Leftrightarrow N(\mathfrak{p}_2) = |N(x)|$ and $x \in \mathfrak{p}_2$.

$\mathfrak{p}_2(2, \sqrt{6})$ $\quad N(2+\sqrt{6}) = (2+\sqrt{6})(2-\sqrt{6})$
$= -2.$

$|N(2+\sqrt{6})| = N(\mathfrak{p}_2) \Rightarrow \mathfrak{p}_2 = (2+\sqrt{6})$.

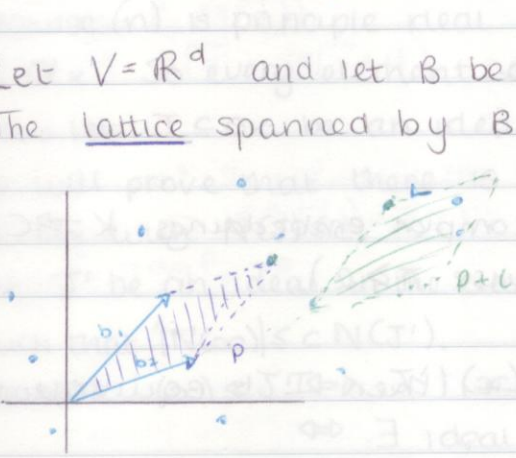
$\mathfrak{p}_3 = (3, \sqrt{6})$ $\quad N(3+\sqrt{6}) = (3+\sqrt{6})(3-\sqrt{6})$
$= 9-6 = 3$

$\Rightarrow \mathfrak{p}_3 = (3+\sqrt{6})$.

Therefore $Cl_K = 0$.

The Geometry of Numbers and Minkowski's Lemma.

Let $V = \mathbb{R}^d$ and let B be a basis for V.
The lattice spanned by B is $L = \operatorname{span} B = \{ \sum_{i=1}^{d} a_i b_i \mid a_i \in \mathbb{Z} \}$.



The fundemental cell P of L is $P = \{ \sum_{i=1}^{d} a_i b_i \mid 0 \le a_i < 1 \}$.

Recall that $\operatorname{Vol} P = |\det(b_1 \cdots b_d)|$.

Note that every $v \in V$ can be written uniquely as $v = l + p$ where $l \in L$, $p \in P$.

Therefore $V = \bigcup_{l \in L} (P + l)$. and this union is disjoint

ie if $(P+l) \cap (P+l') \neq \emptyset$ then $l = l'$

ie P is a set of coset representatives for $L \subseteq V$

There is a map $pr : V \to P$
$v = l + p \mapsto p$.

Lemma:

Let $U \subseteq V$ be a subset with a volume and suppose that $\operatorname{Vol}(U) > \operatorname{Vol}(P)$.
Then there are two points $v \neq w$ in U with $v - w \in L$
$\Leftrightarrow pr(v) = pr(w)$

Sketch proof: (Avoiding measure theory bits).

For a contradiction suppose that $pr|_U$ is injective.

We can write $U = \bigcup_{l \in L} U_l$ where $U_l = U \cap (P + l)$, as a disjoint union.

Fix $l \in L$. On U_l $pr|_{U_l}(u) = u - l$.

So $pr(U_l) = U_l - l$.

By hypothesis $pr(U) = \bigcup_{l \in L} (U_l - l)$ as a disjoint union.

Therefore ~~the volume~~

$$\mathrm{Vol}(U) = \sum_{l \in L} \mathrm{Vol}(U_l) = \sum_{l \in L} \mathrm{Vol}(U_l - l) = \mathrm{Vol}\Big(\bigcup_{l \in L}(U_l - l)\Big)$$
$$= \mathrm{Vol}(\underbrace{pr(U)}_{\subseteq P}) \leq \mathrm{Vol}(P)$$

This is a contradiction

QED

Definition:

A subset $U \subseteq V$ is convex if for any $u, v \in U$ and $\lambda \in [0,1]$
$\lambda u + (1-\lambda) v \in U$.

Definition:

$U \subseteq V$ is symmetric if $u \in U \Rightarrow -u \in U$.

Minkowski's Lemma

Let $U \subseteq V$ be convex and symmetric. If $\mathrm{Vol}(U) > \underbrace{2^d \mathrm{Vol}(P)}_{= \mathrm{Vol}(2P)}$ then there is a non-zero point of L in U.

Proof: Because $\mathrm{Vol}(U) > \mathrm{Vol}(2P)$ by the previous Lemma $\exists$ distinct $v, w \in U$ with $v - w \in 2L \Rightarrow \frac{1}{2}(v-w) \in L$. Also $\frac{1}{2}(v-w) \neq 0$.

We $v \in U$ and $w \in U \underset{\text{symmetry}}{\Rightarrow} -w \in U$

$\underset{\text{convexity}}{\Rightarrow} \frac{1}{2}(v-w) \in U$.

The Minkowski space

Idea: field $k \rightsquigarrow$ vector space k_∞

(of proof key lemma) ideal $I \rightsquigarrow$ lattice L.

Find some suitable U that only contains points with small norm

Then apply Minkowski's Lemma to find a $\neq 0$ point of L in U.

We have field embeddings $\sigma_1 \dots \sigma_d : k \longrightarrow \mathbb{C}$.

Reorder numbering, so $\sigma_1 \dots \sigma_r$ are all real.

$\sigma_{r+1} \dots \sigma_{r+2s=d}$ are all complex

with $\sigma_{r+s+i} = \overline{\sigma_{r+i}}$ for $1 \le i \le s$.

$\underbrace{\sigma_1, \dots, \sigma_r}_{\text{real}}, \underbrace{\sigma_{r+1}, \dots, \sigma_{r+s}}_{\text{one-representative for each complex pair}}, \underbrace{\sigma_{r+s+1} \dots \sigma_{r+2s}}_{\text{other complex embeddings.}}$

Let $k_\infty = \mathbb{R}^r \oplus \mathbb{C}^s$ a $d = (r+2s)$-dimensional real vector space.

Define $\underline{\sigma} : k \longrightarrow k_\infty$

$$x \longmapsto \begin{pmatrix} \sigma_1(x) \\ \sigma_2(x) \\ \vdots \\ \sigma_r(x) \\ \vdots \\ \sigma_{r+s}(x) \end{pmatrix}$$

Messy Lemma:

If B is a basis for k over $\mathbb{Q}$ then $\underline{\sigma}(B)$ is a basis for k_∞ over $\mathbb{R}$.

Furthermore the volume of the fundemental cell is

$$\mathrm{Vol}(P) = 2^{-s}\sqrt{|\Delta B|}$$

Proof: The elements of $\underline{\sigma}(B)$ can be arranged into a matrix.

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & & \sigma_r(b_d) \\ \mathrm{Re}\,\sigma_{r+1}(b_1) & & \mathrm{Re}\,\sigma_{r+1}(b_d) \\ \mathrm{Im}\,\sigma_{r+1}(b_1) & & \mathrm{Im}\,\sigma_{r+1}(b_d) \\ \vdots & & \vdots \\ \mathrm{Re}\,\sigma_{r+s}(b_1) & & \mathrm{Re}\,\sigma_{r+s}(b_d) \\ \mathrm{Im}\,\sigma_{r+s}(b_1) & & \mathrm{Im}\,\sigma_{r+s}(b_d) \end{pmatrix} = \Lambda$$

Its enough to prove that $|\det \Lambda| = 2^{-s}\sqrt{|\Delta B|}$

Add $i \times \text{row}(r+2j)$ to $\text{row}(r+2j-1)$ for $1 \le j \le s$.

$$\begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_d) \\ \vdots & \vdots \\ \sigma_r(b_1) & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & \sigma_{r+1}(b_d) \\ \operatorname{Im}\sigma_{r+1}(b_1) & \operatorname{Im}\sigma_{r+1}(b_d) \\ \vdots & \vdots \\ \sigma_{r+s}(b_1) & \sigma_{r+s}(b_d) \\ \operatorname{Im}\sigma_{r+s}(b_1) & \operatorname{Im}\sigma_{r+s}(b_d) \end{pmatrix}$$ Doesn't change det.

Multiply $\text{row}(r+2j)$ by $-2i$ for $1 \le j \le s$. Now we get $(-2i)^s \det \Lambda$

Add $\text{row}(r+2j+1)$ to $\text{row}(r+2j)$ for $1 \le j \le s$. Doesn't change det

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_r(b_1) & & \sigma_r(b_d) \\ \sigma_{r+1}(b_1) & & \sigma_{r+1}(b_d) \\ \overline{\sigma_{r+1}}(b_1) & & \overline{\sigma_{r+1}}(b_d) \\ \vdots & & \vdots \\ \sigma_{r+s}(b_1) & & \sigma_{r+s}(b_d) \\ \overline{\sigma}_{r+s}(b_1) & & \overline{\sigma}_{r+s}(b_d) \end{pmatrix} = \Lambda'$$

$$\begin{array}{r} a+bi \\ -2bi \\ \hline a-bi \end{array}$$

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_d) \\ \vdots & & \vdots \\ \sigma_d(b_1) & \cdots & \sigma_d(b_d) \end{pmatrix} = \Lambda'$$

$\det \Lambda' = \sqrt{\Delta B}$

But $|\det \Lambda'| = 2^s |\det \Lambda|$.

$|\det \Lambda| = 2^{-s}\sqrt{|\Delta B|}$

Proof of Key Lemma:

Let $\mathcal{C} \subseteq I$ be a $\mathbb{Q}$-basis for K such that $I = \operatorname{span}_{\mathbb{Z}} \mathcal{C}$.

Now $\sigma(I) = L$ is a lattice in K_∞ and the volume of the ~~discriminant~~ of the fundemental cell P is $\operatorname{vol}(P) = 2^{-s}\sqrt{|\Delta \mathcal{C}|}$ by Messy Lemma

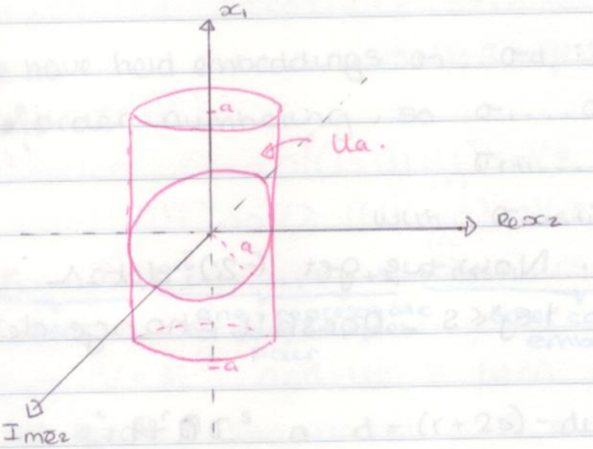
Recall that $N(I) = \sqrt{\left|\frac{\Delta \mathcal{C}}{\Delta B}\right|}$ where B is an intergral basis.

Therefore $\operatorname{vol}(P) = 2^{-s}\sqrt{|\Delta B|}\, N(I)$.

Step 1: Let $c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta B|}$. We will prove that for all $b > cN(I)$ there exists $x \in I \setminus \{0\}$ with $|N(x)| < b$.

Let $a = \sqrt[d]{b}$ so $a^d = b$ and $U_a = \{(\underbrace{x_1, \dots x_r}_{\mathbb{R}}, \underbrace{x_{r+1}, \dots x_{r+s}}_{\mathbb{C}}) \in K_\infty \mid |x_i| < a \text{ for all } i\}$

eg: $r = s = 1$ $K_\infty = \{(x_1, x_2) \in \mathbb{R} \times \mathbb{C}\}$.



- U_a is symmetric
- U_a is convex
- $$\begin{aligned} \mathrm{Vol}(U_a) &= (2a)^r (\pi a^2)^s \\ &= 2^r \pi^s a^{r+2s=d} \\ &= 2^r \pi^s b. \\ &> 2^r \pi^s c N(I). \\ &= 2^r \pi^s \left(\tfrac{2}{\pi}\right)^s \sqrt{|\Delta B|}\, N(I) \\ &= 2^{r+s} \sqrt{|\Delta B|}\, N(I) \\ &= 2^d \left(2^{-s} \sqrt{|\Delta B|}\, N(I)\right). \\ &= 2^d \mathrm{Vol}(P)\, N(I). \end{aligned}$$

U_a = product of r intervals and s discs.

By Minkowski's Lemma there is $x \in I \setminus \{0\}$ such that $\sigma(x) \in U_a = \{(y_i) \mid |y_i| < a\}$

$\sigma(x) = (\sigma_1(x), \dots \sigma_r(x), \sigma_{r+1}(x), \dots \sigma_{r+s}(x)) \Rightarrow |\sigma_i(x)| < a$ for all $1 \leq i \leq d$

Therefore $|N(x)| = \prod_{i=1}^{d} |\sigma_i(x)| < a^d = b$ This completes step 1.

We have $x \in I \setminus \{0\}$ such that $|N(x)| < b$ for each $b > cN(I)$

Step 2: Let $N_{min} = \min_{x \in I \setminus \{0\}} |N(x)|$.

Let $x_{min} \in I \setminus \{0\}$ such that $N_{min} = |N(x_{min})|$

Now for each $b > cN(I)$, we have

$|N(x_{min})| \leq |N(x)| < b$.

i.e. $b \to cN(J)$ from above it follows that $|N(x_{min})| \leq cN(I)$.

Recall we proved that every ideal I which is not principle is equivalent in the ideal class group to an ideal J with

$N(J) \leq c = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta B|}$

Because there are only finitely many positive intergers $\leq c$, and only finitely many ideals with norm equal to each interger, we can find non-trivial elements of the class group in practice and compute the elements of Cl_K.

Example: $k = \mathbb{Q}(\sqrt{-14})$ $B = \{1, \sqrt{-14}\}$ because $-14 \not\equiv 1 \bmod 4$.

$\Delta B = 4 \times -14$, $s = 1$.

$c = \left(\frac{2}{\pi}\right)^1 \sqrt{|4 \times -14|} = \frac{2}{\pi} 2\sqrt{14} < \frac{4 \times 4}{\pi} < \frac{18}{3} < 6$

$= \frac{1}{\pi} \sqrt{4 \times 4 \times 14} < \frac{\sqrt{15^2}}{\pi} < \frac{15}{\pi} < 5$ $\quad 4 \times 4 \times 14 = 15^2 - 1$.

Non trivial elements of ~~the~~ Cl_k can have representatives with norm 2, 3, 4, 5.

The relevant primes are 2, 3, 5.

$m_{\sqrt{-14}}(x) = x^2 + 14$

prime

2 $\quad x^2 \quad (2) = \mathfrak{p}_2^2, \ \mathfrak{p}_2 = (2, \sqrt{-14}) \quad N(\mathfrak{p}_2) = 2^1 = 2$.

3 $\quad x^2 - 1 \equiv (x-1)(x+1) \quad (3) = \mathfrak{p}_3 \mathfrak{q}_3, \ \mathfrak{p}_3 = (3, \sqrt{-14} - 1) \ \mathfrak{q}_3 = (3, \sqrt{-14} + 1)$.

$N(\mathfrak{p}_3) = N(\mathfrak{q}_3) = 3$.

5 $\quad x^2 - 1 \equiv (x-1)(x+1) \quad (5) = \mathfrak{p}_5 \mathfrak{q}_5 \quad \mathfrak{p}_5 = (5, \sqrt{-14} - 1) \ \mathfrak{q}_5 = (5, \sqrt{-14} + 1)$.

$N(\mathfrak{p}_5) = N(\mathfrak{q}_5) = 5$.

Non-trivial elements of the class group could be represented by $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3, \mathfrak{p}_5, \mathfrak{q}_5, \cancel{\mathfrak{p}_2^2}$
$(\overset{\shortparallel}{(2)})$.

- $\mathfrak{p}_2$ is principle iff $\mathfrak{p}_2 = (2a + \sqrt{-14}\, b) \iff 2 = |N(2a + \sqrt{-14}\, b)|$.

$\iff \pm 2 = (2a + \sqrt{-14}\, b)(2a - \sqrt{-14}\, b) = 4a^2 + 14b^2 \geq 4$ whenever a or $b \geq 4$

Contradiction. Therefore $\mathfrak{p}_2$ is not principle.

- $x = 3a + (\sqrt{-14} - 1)b$
$= (3a \mp b) + \sqrt{-14}\, b$

$\pm 3 = N(x) = (3a - b)^2 + 14b^2$

Contradiction $\Rightarrow \mathfrak{p}_3$ not principle.

- Similarly $\mathfrak{q}_3$ is not principle.

- For $\mathfrak{p}_5$, $x = 5a + (\sqrt{14} - 1)b$
$= (5a - b) + \sqrt{-14}\, b$

$\pm 5 = N(x) = (5a - b)^2 + 14b^2$

$\Rightarrow b = 0 \Rightarrow \pm 5 = (5a)^2$ contradiction

$\mathfrak{p}_5$ is not principle.

- Similarly $\mathfrak{q}_5$ is not principle.

Now need to work out whether $\mathfrak{p}_2\mathfrak{p}_3$ is principal.

- $\mathfrak{p}_2\mathfrak{p}_3 = (2, \sqrt{-14})(3, \sqrt{-14}-1) = (6, \underbrace{3\sqrt{-14}, 2(\sqrt{-14}+1)}_{2+\sqrt{-14}}, \underbrace{14+\sqrt{-14}}_{2\times 6 + (2+\sqrt{-14})}).$

$N(\mathfrak{p}_2\mathfrak{p}_3) = N(\mathfrak{p}_1)N(\mathfrak{p}_2) = 2\times 3 = 6.$

$x = (\cancel{3}\sqrt{-14})a + (2+\sqrt{-14})b.$

For general $x = a + \sqrt{-14}\,b \in k$

$N(x) = a^2 + 14b^2 \neq \pm 2 \pm 3, \pm 5$

$\therefore \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3, \mathfrak{p}_5, \mathfrak{q}_5$ non-principle.

Possible representations of non trivial elements of Cl_k $\mathfrak{p}_2$ $\cancel{\mathfrak{q}}$ $\mathfrak{p}_3, \mathfrak{q}_3, (\mathfrak{p}_5, \mathfrak{q}_5)$

$\Rightarrow Cl_k \cong \mathbb{Z}_2, \cancel{\mathbb{Z}_3}, \cancel{\mathbb{Z}_2 \oplus \mathbb{Z}_2}, \mathbb{Z}_4, (\cancel{\mathbb{Z}_5}, \cancel{\mathbb{Z}_6})$ $\quad \mathfrak{p}_2^2 = e$, element of order 2.

Notice $N(1+\sqrt{-14}) = 1^2 + 14 = 15$

There fore $(1+\sqrt{-14}) = \mathfrak{p}_3\mathfrak{p}_5 / \mathfrak{p}_3\mathfrak{q}_5 / \mathfrak{q}_3\mathfrak{p}_5 / \mathfrak{q}_3\mathfrak{q}_5$.

$\Rightarrow$ ~~$\mathfrak{p}_5, \mathfrak{q}_5$~~ $\{\mathfrak{p}_3, \mathfrak{q}_3\} \sim \{\mathfrak{q}_3, \mathfrak{q}_5\}$. eg if $\mathfrak{p}_3\mathfrak{p}_5$ is principal $\Rightarrow \mathfrak{p}_5 \sim \mathfrak{q}_3^{-1} \sim \mathfrak{q}_3$

$\Rightarrow \mathfrak{q}_{\cancel{5}} \sim \mathfrak{p}_3$.

Suppose $Cl_k \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \Rightarrow \mathfrak{q}_3 \sim \mathfrak{p}_3^{-1} \sim \mathfrak{p}_5 \Rightarrow |Cl_k| \leq 3$ contradiction.

$Cl_k \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

If $Cl_k \cong \mathbb{Z}_2$ then $\mathfrak{p}_2 \sim \mathfrak{p}_3 \sim \cancel{\mathfrak{p}}\mathfrak{q}_3$ $\therefore$ ~~$\mathfrak{p}_2\mathfrak{q}$~~ $\mathfrak{p}_2\mathfrak{p}_3$ is principle

But no algebraic integers in $\mathcal{O}_k$ have norm equal to ± 6

$\therefore \mathfrak{p}_2\mathfrak{p}_3$ is not principle, contradiction.

Therefore $Cl_k \cong \mathbb{Z}_4$.

The element of order 2 is represented by $\mathfrak{p}_2$

The elements of order 4 are represented by $\mathfrak{p}_3$ and $\mathfrak{q}_3$.

~~$\Rightarrow \mathfrak{p}_2\mathfrak{q}_3^2$ is principle.~~

$\Rightarrow \mathfrak{p}_2\mathfrak{p}_3^2$

Example:

$k = \mathbb{Q}(\sqrt{15})$ $B = \{1, \sqrt{15}\}$ $\Delta = -60$ $s=0$

$c = \sqrt{60} < 8$

Primes 2, 3, 5, 7

Factorise small primes:

$(2) = \mathfrak{p}_2^2$ $\mathfrak{p}_2 = (2, \sqrt{15}+1)$ norm = 2

$(3) = \mathfrak{p}_3^2$ $\mathfrak{p}_3 = (3, \sqrt{15})$ norm = 3

$(5) = \mathfrak{p}_5$ $\mathfrak{p}_5 = (5, \sqrt{15})$ norm = 5

$(7) = \mathfrak{p}_7 \mathfrak{q}_7$, $\left.\begin{array}{l}\mathfrak{p}_7 = (7, \sqrt{15}-1) \\ \mathfrak{p}_7 = (7, \sqrt{15}+1)\end{array}\right\}$ norm = 7.

Possible non trivial elements $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_7, \mathfrak{q}_7$.

For arbitrary $x = a + b\sqrt{15}$, $N(x) = a^2 - 15b^2 \equiv a^2 \bmod 5$

$\therefore N(x)$ is square mod 5

$\Rightarrow N(x) \equiv 0, 1, 4 \bmod 5$.

$\therefore N(x) \not\equiv \pm 2, \pm 3, \pm 7 \bmod 5 \Rightarrow \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_7, \mathfrak{q}_7$ are all non-principal

$N(3+\sqrt{15}) = 3^2 - 15 = -6 \Rightarrow (3+\sqrt{15}) = \mathfrak{p}_2\mathfrak{p}_3 \Rightarrow \mathfrak{p}_3 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2$.

$N(5+\sqrt{15}) = 5^2 - 15 = 10 \Rightarrow (5+\sqrt{15}) = \mathfrak{p}_2\mathfrak{p}_5 \Rightarrow \mathfrak{p}_5 \sim \mathfrak{p}_2$

$N(1+\sqrt{15}) = 1^2 - 15 = -14 \Rightarrow (1+\sqrt{15}) = \mathfrak{p}_2\mathfrak{p}_7$ or $\mathfrak{p}_2\mathfrak{q}_7$

If $\mathfrak{p}_2\mathfrak{p}_7$ is principle then $\mathfrak{p}_7 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_3$ and $\mathfrak{q}_7 \sim \mathfrak{p}_7^{-1} \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2$.

and similarly if $\mathfrak{p}_2\mathfrak{q}_7$ is principle.

Therefore the $Cl_k \cong \mathbb{Z}_2$. The non trivial element is $\mathfrak{p}_2$.

Example:

$K = \mathbb{Q}(\sqrt{14})$ $\quad B = \{1, \sqrt{14}\}$ $\quad \Delta = -4 \times 14 = -56$ $\quad s = 0$

$c = \sqrt{56} < 8.$

Primes 2, 3, 5, 7.

$(2) = \mathfrak{p}_2^2 \quad \mathfrak{p}_2 = (2, \sqrt{14}) \quad$ norm $= 2$

(3) is prime of norm 9

$(5) = \mathfrak{p}_5 \mathfrak{q}_5 \quad \mathfrak{p}_5 = (5, \sqrt{14} - 2) \quad \mathfrak{q}_5 = (5, \sqrt{14} + 2) \quad$ norm $= 5$

$(7) = \mathfrak{p}_7^2 \quad \mathfrak{p}_7 = (7, \sqrt{14}) \quad$ norm $= 7.$

$N(4 + \sqrt{14}) = 4^2 - 14 = 2$

$\Rightarrow (4 + \sqrt{14}) = \mathfrak{p}_2$. So $\mathfrak{p}_2$ principle.

$N(3 + \sqrt{14}) = 3^2 - 14 = -5$

$\Rightarrow (3 + \sqrt{14}) = \mathfrak{p}_5$ or $\mathfrak{q}_5 \Rightarrow \mathfrak{p}_5$ and $\mathfrak{q}_5$ are both principle...

$N(7 + 2\sqrt{14}) = 49 - 4 \cdot 14 = -7$

$\Rightarrow (7 + 2\sqrt{14}) = \mathfrak{p}_7.$

Therefore Cl_K is the trival group.