7/01/13

Number Fields ①

Books

Stewart and Tall, Algebraic Number Theory, A.K. Peters 2002

Esmonde and Murty, Problems in Algebraic Number Theory, Springer 1999 (500 problems)

D.A. Marcus, Number Fields, Springer 1977 (lots of exercises)

S. Alaca and K.S. Williams, Introductory Algebraic Number Theory (CUP 2004)

*** A. Baker, A comprehensive course in number theory CUP 2012 (chapters 10-12)

E. Hecke, Lectures on the theory of Algebraic Numbers, Springer 1981

P. Samuel, Algebraic Theory of Numbers, Dover 2008

Some Diophantine Problems

1. If p is a prime, $p \equiv 1 \ (4)$, then p is the sum of two squares.
   $(5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2, \ldots)$
2. Find all integer solutions to $x^2 - 2y^2 = 7$
3. Find all integer solutions to $y^2 = x^3 - 2$

Lemma

$p \equiv 1 \ (4) \Rightarrow x^2 \equiv -1 \ (p)$ for some x i.e. $\left(\frac{-1}{p}\right) = 1$

Proof

$\left(\frac{\mathbb{Z}}{(p-1)\mathbb{Z}}\right) \cong \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times = \mathbb{F}_p^\times$ is a cyclic group of order $p-1$.

$p \equiv 1 \ (4) \Rightarrow 4 \mid p-1 \Rightarrow \mathbb{F}_p^\times$ contains an element of order 4.

i.e. $\exists\, x \in \mathbb{Z}$ such that $x^4 \equiv 1 \ (p)$, but $x^2 \not\equiv 1 \ (p)$ since x has order 4

$\Rightarrow x^2 \equiv -1 \ (p)$. □

(Since $x^4 - 1 \equiv (x^2+1)(x^2-1) \equiv 0 \ (p)$, and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$)

Ring of Gaussian Integers $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$.

Recall from GRM that $\mathbb{Z}[i]$ is Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

Solution of ①

Let $p \equiv 1 \ (4)$. Lemma $\Rightarrow p \mid (x^2+1)$ for $x \in \mathbb{Z}$.

$p \mid (x^2+1) = (x+i)(x-i)$

If p is irreducible in $\mathbb{Z}[i]$, then $p \mid (x+i)$ or $p \mid (x-i)$

$\Rightarrow \frac{x \pm i}{p} \in \mathbb{Z}[i]$, with the correct choice of sign ※

$\therefore p = \alpha\beta$, for some $\alpha, \beta \in \mathbb{Z}[i]$, non-units

If $\alpha = a+bi$, $a,b \in \mathbb{Z}$, then $|\alpha|^2 = a^2+b^2 \in \mathbb{Z}$

α a unit $\Leftrightarrow \frac{1}{\alpha} \in \mathbb{Z}[i] \Leftrightarrow |\alpha| = 1 \Leftrightarrow \alpha \in \{\pm 1, \pm i\}$

Then $p^2 = |\alpha|^2 |\beta|^2$, α, β not units

$\Rightarrow |\alpha|^2 = |\beta|^2 = p$, i.e. $p = a^2+b^2$ as required □

Solution of ②

Work in $\mathbb{Z}[\sqrt{2}]$, Euclidean, hence a UFD.

Define $N: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$, $a+b\sqrt{2} \mapsto a^2-2b^2 = \overset{\alpha}{(a+b\sqrt{2})}\overset{\bar{\alpha}}{(a-b\sqrt{2})}$

The problem is to find all $\alpha \in \mathbb{Z}[\sqrt{2}]$ with $N(\alpha) = \alpha\bar{\alpha} = 7$

We factor 7 into irreducibles. $7 = (3+\sqrt{2})(3-\sqrt{2})$

To check that $3+\sqrt{2}$ is irreducible, suppose that $3+\sqrt{2} = xy$,

$x, y \in \mathbb{Z}[\sqrt{2}]$. $N(3+\sqrt{2}) = 7 = N(x)\,N(y)$

$\Rightarrow N(x) = \pm 1$ or $N(y) = \pm 1$, ~~a unit~~ x or y a unit.

So $3 \pm \sqrt{2}$ are irreducible.

$\therefore \alpha = u(3 \pm \sqrt{2})$, u a unit.

Fact (See later)

The units in $\mathbb{Z}[\sqrt{2}]$ are $\{\pm(1+\sqrt{2})^m : m \in \mathbb{Z}\}$

$\therefore$ The general solution to $x^2 - 2y^2 = 7$ is given by

$x + y\sqrt{2} = \pm(1+\sqrt{2})^{2m}(3 \pm \sqrt{2})$, $m \in \mathbb{Z}$

(if the exponent is odd, this solves $x^2 - 2y^2 = -7$)

Solution to ③

$\mathbb{Z}[\sqrt{-2}]$ is Euclidean, hence a UFD.

The only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

$y^2 = x^3 - 2 \Rightarrow (y + \sqrt{-2})(y - \sqrt{-2}) = x^3$

Suppose $\pi \in \mathbb{Z}[\sqrt{-2}]$ is an irreducible with $\pi \mid (y+\sqrt{-2})$ and

$\pi \mid (y - \sqrt{-2}) \Rightarrow \pi \mid 2\sqrt{-2} = -(\sqrt{-2})^3 \Rightarrow \pi = \pm\sqrt{-2}$

Write $y + \sqrt{-2} = \pm(\sqrt{-2})^{\alpha_1} \pi_1^{\beta_1} \dots \pi_r^{\beta_r}$

$y - \sqrt{-2} = \pm(\sqrt{-2})^{\alpha_1} \bar{\pi}_1^{\beta_1} \dots \bar{\pi}_r^{\beta_r}$

where $\sqrt{-2}, \pi_1, \dots, \pi_r, \bar{\pi}_1, \dots, \bar{\pi}_r$ are distinct irreducibles, coprime

$\Rightarrow x^3 = \pm(\sqrt{-2})^{2\alpha} \pi_1^{\beta_1} \bar{\pi}_1^{\beta_1} \dots \pi_r^{\beta_r} \bar{\pi}_r^{\beta_r}$

Since $\mathbb{Z}[\sqrt{-2}]$ is a UFD, $2\alpha = \beta_1 = \beta_2 = \dots = \beta_r = 0$ (3)

$\Rightarrow y + \sqrt{2} = \pm(u + v\sqrt{-2})^3$, $u, v \in \mathbb{Z}$

$\Rightarrow y + \sqrt{2} = (u + v\sqrt{-2})^3$, $u, v \in \mathbb{Z}$

$= (u^3 - 6uv^2) + (3u^2v - 2v^3)\sqrt{-2}$

$\Rightarrow y = u(u^2 - 6v^2)$, $1 = (3u^2 - 2v^2)v$

$\Rightarrow v = \pm 1$, $3u^2 - 2 = \pm 1$, $y = u(u^2 - 6)$

$\Rightarrow u = \pm 1$, $v = \pm 1$, $u = \pm 5$

The only solutions of $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$

Remark

In each of these problems, we relied on the relevant ring having unique factorisation. Later in this course we solve problems of this sort in cases where the ring does not have unique factorisatio

Recall from GRM:

- Euclidean Domain $\Rightarrow$ PID. Let I be an ideal. We have a Euclidean function ℓ, so take $r \in I$ with $r \neq 0$, $\ell(r)$ minimal, and use the division algorithm to show that $r \mid a$ for $a \in I$
- prime $\Rightarrow$ irreducible
- UFDs satisfy:

(UFD1) For r, non-zero, non-unit, we can write r as a product of irreducibles

(UFD2) The above product is unique up to reordering and multiplying by units

- If R is an integral domain, then R is a UFD $\Leftrightarrow$ UFD1 is satisfied, and all irreducibles are prime
- (r) prime $\Leftrightarrow$ r prime for $r \neq 0$
- (r) proper $\Leftrightarrow$ r a non-unit

7/01/13

Number Fields ①

- For R a PID, $r \in R$, $r \neq 0$, the following are equivalent:

i) r irreducible

ii) (r) prime (so r is prime)

iii) (r) maximal

- With the same conditions as above, r is a product of irreducibles
- By the above, PID $\Rightarrow$ UFD

22/01/13

Number Fields ②

1 Algebraic Numbers and Algebraic Integers

Definition

$\alpha \in \mathbb{C}$ is

i) An *algebraic number* if $f(\alpha) = 0$ for some non-zero polynomial $f \in \mathbb{Q}[X]$

ii) An *algebraic integer* if $f(\alpha) = 0$ for some *monic* polynomial $f \in \mathbb{Z}[X]$.

Lemma 1.1

Let $\alpha \in \mathbb{Q}$. α an algebraic integer $\Leftrightarrow \alpha \in \mathbb{Z}$

Proof

Write $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$, $a_{n-1}, \dots, a_0 \in \mathbb{Z}$.

Since $\alpha \in \mathbb{Q}$, we can write $\alpha = r/s$, $r, s \in \mathbb{Z}$ coprime

$\Rightarrow r^n + a_{n-1}r^{n-1}s + \dots + a_1 r s^{n-1} + a_0 s^n = 0$

$\Rightarrow s \mid r^n$. If p is a prime then $p \mid s$

then $p \mid r^n \Rightarrow p \mid r$ ⚡ as r, s were coprime

$\therefore s = \pm 1 \Rightarrow \alpha = \pm r \in \mathbb{Z}$ □

Remark

Sometimes "algebraic integer" is abbreviated to "integer". To avoid confusion elements of $\mathbb{Z}$ are called "rational integers".

Notation

$R \subset S$ rings, $\alpha_1, \dots, \alpha_m \in S$. $R[\alpha_1, \dots, \alpha_m]$ is the subring of S generated by R and $\alpha_1, \dots, \alpha_m$.

$= \mathrm{Im}\begin{pmatrix} R[x_1,\dots,x_n] \to S \\ x_i \mapsto \alpha_i \end{pmatrix}$

Theorem 1.2

The algebraic numbers form a field.

Proof:

If $0 \neq \alpha \in \mathbb{C}$ is a root of $f \in \mathbb{Q}[x]$, $d = \deg(f)$

Then $\frac{1}{\alpha}$ is a root of $x^d f(\frac{1}{x})$.

So it will suffice to check that α, β algebraic

$\Rightarrow \alpha \pm \beta$, $\alpha\beta$ algebraic.

If α, β satisfy polynomials (with coefficients in $\mathbb{Q}$) of degrees m and n, then $\mathbb{Q}[\alpha, \beta]$ is a $\mathbb{Q}$-vector space of dimension $\leq mn$, since it is spanned by $\{\alpha^i \beta^j \mid 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\}$

If $x \in \mathbb{Q}[\alpha, \beta]$ then the $mn+1$ elements $1, x, x^2, \dots, x^{mn}$ must satisfy a dependence relation $\Rightarrow x$ is algebraic.

Taking $x = \alpha \pm \beta, \alpha\beta$ gives the result. □

Theorem 1.3

The algebraic integers form a ring.

Proof:

It suffices to check closure, i.e. α, β algebraic integers

$\Rightarrow \alpha \pm \beta$, $\alpha\beta$ algebraic integers.

If α, β satisfy monic polynomials (with coefficients in $\mathbb{Z}$) of degrees m and n then $\mathbb{Z}[\alpha, \beta]$ is generated as a $\mathbb{Z}$-module

by $\{\alpha^i \beta^j \mid 0 \le i \le m-1,\ 0 \le j \le n-1\}$

To complete the proof, take $R = \mathbb{Z}$, $S = \mathbb{Z}[\alpha, \beta]$, $x = \alpha \pm \beta, \alpha\beta$ in the following lemma.

Lemma 1.4

Let $R \subset S$ be rings. Suppose that S is finitely generated as an R-module. Then every $x \in S$ is integral over R, i.e.

$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$ for some $a_0, \dots, a_{n-1} \in R$.

Proof

Say $S = \{\sum_{i=1}^{n} \lambda_i w_i \mid \lambda_i \in R\}$ for some $w_1, \dots, w_n \in S$. w_1 is special.

Then $x w_i = \sum_{j=1}^{n} a_{ij} w_j$, some $a_{ij} \in R$.

$\Rightarrow (x I_n - A)\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$ where $A = (a_{ij})$

$\Rightarrow \det(x I_n - A)\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$ ← multiply on the left by $\operatorname{adj}(x I_n - A)$

$\Rightarrow \det(x I_n - A) = 0$ (since $w_1 = 1$)

Then x satisfies a monic-polynomial of degree n with coefficients in R. □

Definition

L/k a field extension (i.e. $L \supset k$ fields). The minimal polynomial of $\alpha \in L$ is the monic polynomial $g \in k[x]$ of least degree such that $g(\alpha) = 0$. (It is clear that g is unique, and that it is irreducible in $k[x]$).

Proposition 1.5

Let $\alpha \in \mathbb{C}$ be an algebraic number, with minimal polynomial $g \in \mathbb{Q}[x]$.

i) For $f \in \mathbb{Q}[x]$, $f(\alpha) = 0 \Leftrightarrow g \mid f$

ii) α an algebraic integer $\Leftrightarrow g \in \mathbb{Z}[x]$

Proof

i) ($\Rightarrow$) By the division algorithm, $f = qg + r$ for some $q, r \in \mathbb{Q}[x]$, with $\deg r < \deg g$

$\Rightarrow f(\alpha) = q(\alpha)\, g(\alpha) + r(\alpha) \quad \Rightarrow r(\alpha) = 0$

This contradicts the definition of g unless $r = 0$, i.e. $g \mid f$.

($\Leftarrow$) is clear.

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

By i) $g \mid f$ in $\mathbb{Q}[x]$. Write $g(x) = \prod_{i=1}^{n} (x - \alpha_i)$, $\alpha_1, \dots, \alpha_n \in \mathbb{C}$

Then $f(\alpha_i) = 0 \Rightarrow \alpha_i$ an algebraic integer

Theorem 1.3 $\Rightarrow$ the coefficients of g are algebraic integers.

But $g \in \mathbb{Q}[x]$, so by Lemma 1.1, $g \in \mathbb{Z}[x]$. $\square$

This proposition is useful for showing that $\alpha \in \mathbb{C}$ is <u>not</u> an algebraic integer.

24/01/13

Number Fields ③

Definition
Let L/k be a field extension. L/k is *finite* if L is finite dimensional as a k-vector space.
The degree of the extension is $[L:k] = \dim_k L$.

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

Notation : If $k \subset L$ and $\alpha_1, \dots, \alpha_m \in L$, then $k(\alpha_1, \dots, \alpha_m)$ is the subfield of L generated by $k, \alpha_1, \dots, \alpha_m = \mathrm{Frac}\, k[\alpha_1, \dots, \alpha_m]$.
It is clear that if k is a number field then $k = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_m \in k$ (for example, take $\alpha_1, \dots, \alpha_m$ a basis for k over $\mathbb{Q}$).

By the Primitive Element Theorem (see Galois Theory), we can take $m = 1$, i.e. $k = \mathbb{Q}(\alpha)$, for some $\alpha \in k$.

Example : $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Remark
Many different α define the same field.
e.g. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}\left(\frac{1}{\sqrt{2}} + 7\right) = \mathbb{Q}(\sqrt{2} + 31)$ etc
Let $k = \mathbb{Q}(\alpha)$ a number field.
$[k : \mathbb{Q}] < \infty \Rightarrow 1, \alpha, \alpha^2, \dots$ satisfy a linear-dependence relation over $\mathbb{Q}$.
$\Rightarrow \alpha$ algebraic, an algebraic number
Let $g \in \mathbb{Q}[x]$, the minimal polynomial of α over $\mathbb{Q}$.

The ring homomorphism

$$\begin{aligned} \mathbb{Q}[x] &\to k \\ f(x) &\mapsto f(\alpha) \end{aligned}$$

has kernel (g), and the image is $\mathbb{Q}[\alpha]$.

By the isomorphism theorem for rings, $\mathbb{Q}[x]/(g) \cong \mathbb{Q}[\alpha]$

Recall that $\mathbb{Q}[x]$ is a PID (it is an ED). g is irreducible $\Rightarrow (g)$ is a maximal ideal $\Rightarrow \mathbb{Q}[\alpha]$ is a field.

Remark: The inverse of $f(\alpha) \in \mathbb{Q}[\alpha]$ can be computed by running Euclid's Algorithm on f, g.

Since $\mathbb{Q}(\alpha) = \mathrm{Fac}\,\mathbb{Q}[\alpha]$, and $\mathbb{Q}[\alpha]$ is already a field, we have $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ $(= k)$.

If $\deg g = n$, then $k = \mathbb{Q}(\alpha)$ has basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$
$\Rightarrow [k : \mathbb{Q}] = n = \deg g$.

Lemma 1.6

Let k be a number field of degree n. Then there are exactly n embeddings $k \hookrightarrow \mathbb{C}$.

Proof

Write $k = \mathbb{Q}(\alpha)$. $g \in \mathbb{Q}[x]$ the min. poly. of α
$\deg g = [k : \mathbb{Q}] = n$.
$g \in \mathbb{Q}[x]$ irreducible. $\Rightarrow g, g'$ are coprime
$\Rightarrow g$ has n distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{C}$
These are called the conjugates of α.

The embeddings $k \hookrightarrow \mathbb{C}$ are given by
$k = \mathbb{Q}[x]/(g) \hookrightarrow \mathbb{C}$
$x \mapsto \alpha_i$; (use isomorphism theorem) $\square$

Since g has real coefficients it has r real roots and s pairs of complex conjugate roots with $n = r + 2s$.

$\therefore$ k has r real embeddings and s pairs of complex conjugate embeddings in $\mathbb{C}$.

24/01/13

Number Fields ③

Remark

i) n, r, s depend only on k (and not on the choice of α).
Indeed $n = [k : \mathbb{Q}]$
$r = \#$ real embeddings $k \hookrightarrow \mathbb{R}$.
$s = \frac{1}{2}(n - r)$.

ii) In the definition of a number field, we could demand that $k \subset \mathbb{C}$.
Then one of the embeddings is the identity.

Tower Law

M — L — k

$[M : k] = [M : L][L : k]$

Sketch Proof

If L has k-basis $x_1, \dots, x_m$ and M has L-basis $y_1, \dots, y_n$, then check that M has k basis $\{x_i y_j : 1 \le i \le m, 1 \le j \le n\}$

Lemma 1.7

Let k be a number field. $\beta \in k$, with minimal polynomial $g \in \mathbb{Q}[X]$. Let $\beta_1, \dots, \beta_m \in \mathbb{C}$ be the roots of g (the conjugates of β).

$$d_i = \#\{\sigma : k \hookrightarrow \mathbb{C} \mid \sigma(\beta) = \beta_i\}$$

is independent of i.

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

Proof

Let h be the min. poly. of α over $\mathbb{Q}(\beta)$.

Then $d_i \le \deg(h) = [k : \mathbb{Q}(\beta)]$ (since α must be sent to one of its own conjugates and this determines $\sigma : k \to \mathbb{C}$ entirely)

$\Rightarrow \sum_{i=1}^{m} d_i \le [k : \mathbb{Q}(\beta)]\, m = [k : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$

$= [k : \mathbb{Q}]$

Lemma 1.6 shows that $\sum_{i=1}^{m} d_i = [k : \mathbb{Q}]$

$\therefore d_i = [k : \mathbb{Q}(\beta)]$ $\forall i$ □

Definition
L/k finite extension of fields. Let $x \in L$. There is a k-linear map $\phi_x : L \to L$, $y \mapsto xy$.
The norm of x is
$$N_{L/k}(x) = \det(\phi_x) \in k.$$
The trace of x is
$$\mathrm{Tr}_{L/k}(x) = \mathrm{tr}(\phi_x) \in k.$$

Remark $N_{L/k}(x_1 \cdot x_2) = N_{L/k}(x_1) N_{L/k}(x_2) \quad \forall x_1, x_2 \in L$
$\mathrm{Tr}_{L/k} : L \to k$ is a k-linear map.

29/01/13 Number Fields ④

L/k a finite extension of fields. For $x \in L$, let $\phi_x : L \to L$, $y \mapsto xy$.

Definition

$N_{L/k}(x) = \det(\phi_x)$, $Tr_{L/k} = tr(\phi_x)$.

Remark

For $f \in k[x]$, $f(\phi_x) = \phi_{f(x)}$

Theorem 1.8

Let k be a number field of degree n, $\sigma_1, \ldots, \sigma_n$ distinct embeddings $k \hookrightarrow \mathbb{C}$. For $\beta \in k$, let $\phi_\beta : k \to k$, $y \mapsto \beta y$.

The characteristic polynomial of ϕ_β is $f(x) = \prod_{i=1}^{n} (X - \sigma_i(\beta))$

In particular, $Tr_{k/\mathbb{Q}}(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$.

$N_{k/\mathbb{Q}}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$

Proof

Let g be the minimal polynomial of β over $\mathbb{Q}$, and let $\beta_1, \ldots \beta_r \in \mathbb{C}$ be the roots of g (distinct since g, g' coprime). The characteristic polynomial of ϕ_β and $f(x)$ are both monic polynomials of degree n. We show that they are equal by showing that they are both powers of g. By Linear Algebra, the characteristic polynomial and the minimal polynomial of ϕ_β have the same roots in $\mathbb{C}$.

$\therefore$ they have the same irreducible factors in $\mathbb{Q}[x]$.

(Use Proposition 1.5(i)). But the minimal polynomial of ϕ_β

is the same as the minimal polynomial of β (i.e. g), which is ireducible in $\mathbb{Q}[x]$.

We have $g(x) = \prod_{j=1}^{m} (x - \beta_j)$. By Lemma 1.7, we know that f is a power of g. □

Remark

Let $k \subset \mathbb{C}$ be any subfield. If $[L:k] = n$, and $\sigma_1, \dots, \sigma_n$ the k-embeddings $L \hookrightarrow \mathbb{C}$, then $N_{L/k}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$ and $Tr_{L/k}(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$ with the same proofs. (We can also replace L/k by any finite separable extension).

Corollary 1.9

If $\beta \in K$ is an algebraic integer then $Tr_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$.

Proof

$Tr_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Q}$. Theorems 1.3, 1.8 $\Rightarrow$ They are algebraic integers. Hence they are in $\mathbb{Z}$ by Lemma 1.1.

Definition

Let K be a number field. The ring of integers of K is $\mathcal{O}_K = \{x \in K \mid x \text{ is an algebraic integer}\}$. This is a ring by Theorem 1.3.

Notation

If R is a ring, then R^* is the set of units in R.

Lemma 1.10

Let $x \in \mathcal{O}_K$. Then $x \in \mathcal{O}_K^* \Leftrightarrow N_{K/\mathbb{Q}}(x) = \pm 1$.

Proof

"⇒" Suppose $xy = 1$ for some $y \in \mathcal{O}_K$.

$\Rightarrow N_{K/\mathbb{Q}}(x) N_{K/\mathbb{Q}}(y) = 1 \Rightarrow N_{K/\mathbb{Q}}(x)$ a unit in $\mathbb{Z}$.

i.e. $N_{K/\mathbb{Q}}(x) = \pm 1$.

"⇐" If $N_{K/\mathbb{Q}}(x) = \pm 1$ then $\prod_{i=1}^{n} \sigma_i(x) = \pm 1$

We identify K as a subfield of $\mathbb{C}$ via σ_1:

$\underbrace{\frac{1}{x}}_{\in K} = \pm \underbrace{\prod_{i=2}^{n} \sigma_i(x)}_{\text{an algebraic integer. Hence } \frac{1}{x} \in \mathcal{O}_K}$

and x is a unit. □

Lemma 1.11

If $\beta \in K$ then $\exists\, 0 \neq c \in \mathbb{Z}$ such that $c\beta \in \mathcal{O}_K$. In particular, $K = \mathrm{Frac}\, \mathcal{O}_K$.

Proof

Let β have minimal polynomial $X^m + a_{m-1}X^{m-1} + \dots + a_1 X + a_0$ with $a_i \in \mathbb{Q}$. Let c be the least common multiple of the denominators of the a_i. Then $c\beta$ is a root of $X^m + ca_{m-1}X^{m-1} + \dots + c^{m-1}a_1 X + c^m a_0$, which has coefficients in $\mathbb{Z}$. $\Rightarrow c\beta \in \mathcal{O}_K$ □

Let $[K:\mathbb{Q}] = n$, $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$. For $x_1, \dots, x_n \in K$ we define

$$\Delta(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2$$

$$= \det \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_n(x_1) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_n) & \cdots & \sigma_n(x_n) \end{pmatrix} \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \cdots & \sigma_n(x_n) \end{pmatrix} = \det\left(\underbrace{\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j)}_{\in \mathbb{Q}}\right)$$

If $x_j' = \sum_{i=1}^{n} a_{ij} x_i$ for some $a_{ij} \in \mathbb{Q}$, $A = (a_{ij})$

then $\Delta(x_1', \dots, x_n') = (\det A)^2 \Delta(x_1, \dots, x_n)$ (*)

Recall

The discriminant of a monic polynomial of $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$

is $\operatorname{disc}(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$

Lemma 1.12

Let $k = \mathbb{Q}(\alpha)$ be a number field of degree n, and $f \in \mathbb{Q}[X]$ be the minimal polynomial of α. Then.

i) $\Delta(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \operatorname{disc}(f)$

ii) $x_1, \dots, x_n$ a basis for k over $\mathbb{Q} \iff \Delta(x_1, \dots, x_n) \neq 0$

Proof

i) Let $\alpha_i = \sigma_i(\alpha)$ ← Observe that if $\alpha_i = \alpha_j$ then $\Delta = 0$

$$\Delta(1, \alpha, \dots, \alpha^{n-1}) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}^2$$ is a Vandermonde determinant.

$$= \prod_{i<j} (\alpha_i - \alpha_j)^2 = \operatorname{disc}(f)$$

ii) This follows by (*) and noting that $\operatorname{disc}(f)$ is non-zero.

Theorem 1.13

Let k be a number field of degree n. Then $\exists$ a basis $x_1, \dots, x_n$ for k over $\mathbb{Q}$, such that

$$\mathcal{O}_k = \left\{ \sum_{i=1}^{n} \lambda_i x_i \mid \lambda_i \in \mathbb{Z} \right\}$$

We say that $x_1, \dots, x_n$ is an integral basis.

If $x_j' = \sum a_{ij} x_i$, $A = (a_{ij})$

$\Delta(x_1', \dots, x_n') = (\det A)^2 \Delta(x_1, \dots, x_n)$ (✱)

Theorem 1·13

Let k be a number field of degree n. Then $\exists$ a basis $x_1, \dots, x_n$ for k over $\mathbb{Q}$ such that $\mathcal{O}_k = \{\sum_{i=1}^{n} \lambda_i x_i \mid \lambda_i \in \mathbb{Z}\}$

In particular $\mathcal{O}_k \cong \mathbb{Z}^n$ as a group under $+$.

Proof

Let $x_1, \dots, x_n$ be a basis for k over $\mathbb{Q}$. Clearing denominators (see Lemma 1·11) we may assume that $x_1, \dots, x_n \in \mathcal{O}_k$.

Then $\Delta(x_1, \dots, x_n) \in \mathbb{Z}$ and non-zero by Lemma 1·12. ($= \det(\mathrm{Tr}_{k/\mathbb{Q}}(x_i x_j))$)

We pick $x_1, \dots, x_n$ such that $|\Delta(x_1, \dots, x_n)|$ is minimal.

Let $\theta \in \mathcal{O}_k$. Write $\theta = \sum_{i=1}^{n} \lambda_i x_i$. $\lambda_i \in \mathbb{Q}$. Suppose WLOG $\lambda_1 \notin \mathbb{Z}$, i.e. $\lambda_1 = \lambda + \mu$, $\lambda \in \mathbb{Z}$, $0 < \mu < 1$.

$x_1' = \theta - \lambda x_1 = \mu x_1 + \lambda_2 x_2 + \dots + \lambda_n x_n$

$x_1', x_2, \dots, x_n \in \mathcal{O}_k$ form a basis for k over $\mathbb{Q}$.

Change of basis matrix $\begin{pmatrix} \mu & 0 & \cdots & 0 \\ \lambda_2 & 1 & & \\ \vdots & & \ddots & \\ \lambda_n & 0 & & 1 \end{pmatrix}$

Now $\Delta(x_1', x_2, \dots, x_n) = \mu^2 \Delta(x_1, \dots, x_n)$, but $0 < \mu < 1$ contradicting our choice of $x_1, \dots, x_n$ for minimality of $|\Delta|$. ✱

The theorem follows. □

Definition

The discriminant of k is $D_k = \Delta(x_1, \dots, x_n)$ where $x_1, \dots, x_n$

is an integral basis.

If $x_1, \dots, x_n$ and $x_1', \dots, x_n'$ are integral bases, then the change of basis matrix A in (*) and its inverse both have entries in $\mathbb{Z}$, so $\det A = \pm 1 \Rightarrow D_K$ is independant of the choice of integral basis.

Quadratic Fields

$[K:\mathbb{Q}] = 2 \Rightarrow K = \mathbb{Q}(\sqrt{d})$ for some $d \neq 0, 1$, a square-free integer. K has $\mathbb{Q}$-basis $1, \sqrt{d}$.

$$\mathrm{Tr}_{K/\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d}) + (x - y\sqrt{d})$$
$$= \mathrm{tr}\begin{pmatrix} x & dy \\ y & x \end{pmatrix} = 2x$$

$$N_{K/\mathbb{Q}}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = \det\begin{pmatrix} x & dy \\ y & x \end{pmatrix} = x^2 - dy^2$$

Proposition 1.14

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

N.B. d squarefree, $d \neq 0$ (

Proof

If $x + y\sqrt{d} \in \mathcal{O}_K$, then $2x, x^2 - dy^2 \in \mathbb{Z}$.

$\Rightarrow 4dy^2 \in \mathbb{Z}$. Since d is square-free, $x = \frac{u}{2}$, $y = \frac{v}{2}$, for some $u, v \in \mathbb{Z}$. Moreover, $u^2 - dv^2 \equiv 0 \ (4)$.

i) If $d \equiv 2, 3 \ (4)$, then since squares are $0, 1 \ (4)$, u, v are both even $\Rightarrow x, y \in \mathbb{Z}$. $\therefore \mathcal{O}_K$ has integral basis $1, \sqrt{d}$.

ii) If $d \equiv 1 \ (4)$, then u, v have the same parity, so $1, \frac{1+\sqrt{d}}{2}$ is an integral basis. N.B. $\frac{1+\sqrt{d}}{2}$ is a root of

$$X^2 - X + \frac{1-d}{4} = 0$$

Trace: 1; Norm: $\frac{1-d}{4} \in \mathbb{Z}$, as $d \equiv 1 \ (4)$

□

31/01/13

Number Fields ⑤

Remark

$$D_K = \begin{cases} \left|\frac{1}{\sqrt{d}} - \frac{1}{\sqrt{d}}\right|^2 = 4d & , d \equiv 2, 3 \ (4) \\ \left|\frac{1}{\frac{1+\sqrt{d}}{2}} \ \frac{1}{\frac{1-\sqrt{d}}{2}}\right|^2 = d & , d \equiv 1 \ (4) \end{cases}$$

Lemma 1.15

Let $M \subset \mathbb{Z}^n$ be a subgroup. Then $M \cong \mathbb{Z}^r$ for some $r \leq n$.

If $r = n$, and A is an $n \times n$ matrix whose rows are a $\mathbb{Z}$-basis for M, then M has finite index : $(\mathbb{Z}^n : M) = |\det A|$

Proof

We construct an $n \times n$ upper triangular matrix $A = (a_{ij})$ whose rows generate M. We choose $(0, 0, \dots, 0, a_{jj}, a_{jj+1}, \dots, a_{jn}) \in M$ with $a_{jj} > 0$ minimal such that. (If no such exists, then take the j^{th} row to be 0)

If $x = (x_1, \dots, x_n) \in M$, then subtracting a multiple of the first row of A gives $x_1 = 0$, subtracting a multiple of the second row of A gives $x_2 = 0$, and so on. This shows that x is a $\mathbb{Z}$-linear combination of rows of A. $\therefore M \cong \mathbb{Z}^r$ where $r = \#$ non-zero rows in A

For the last part, $\mathbb{Z}^n/M$ has coset representatives $(\lambda_1, \dots, \lambda_n)$ with $0 \leq \lambda_i < a_{ii} \Rightarrow (\mathbb{Z}^n : M) = \prod_{i=1}^{n} a_{ii} = \det A$

Changing our basis for M can only change the sign of $\det A$ □

Corollary 1.16

If $x_1, \dots, x_n \in \mathcal{O}_K$ a basis for $K/\mathbb{Q}$, and $M = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$ then $\Delta(x_1, \dots, x_n) = (\mathcal{O}_K : M)^2 D_K$

Proof

This follows by Lemma 1.15 and (*)

In particular, if $\Delta(x_1, \ldots, x_n) = k^2 d$, $k, d \in \mathbb{Z}$, d squarefree, then $M \subset \mathcal{O}_K \subset \frac{1}{k} M$

05/02/13 Number Fields ⑥

Chapter 2: Ideals

Example

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. $\mathcal{O}_K$ is not a UFD

e.g. $3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$. But $3, 7, 1 \pm 2\sqrt{-5}$ are irreducible and not associates: $\mathcal{O}_K^\times = \{\pm 1\}$

For example, if $\alpha\beta = 3$, $\alpha, \beta \in \mathcal{O}_K$, $N(\alpha)N(\beta) = 9$

But $x^2 + 5y^2 = \pm 3$ has no solutions for $x, y \in \mathbb{Z}$.

Ideals were introduced by Kummer, Dedekind, ..., to restore the property of unique factorisation.

Recall

$\underline{\underline{a}} \subset \mathcal{O}_K$ is an ideal if

i) $\underline{\underline{a}}$ is a (non-zero) group under $+$ ii) $r \in \mathcal{O}_K$, $s \in \underline{\underline{a}} \Rightarrow rs \in \underline{\underline{a}}$

Theorem 1.13 $\Rightarrow \mathcal{O}_K \cong \mathbb{Z}^n$ as a group under $+$. So if $\underline{\underline{a}} \subset \mathcal{O}_K$ is an ideal then by Proposition 1.15, $\underline{\underline{a}}$ is a finitely generated $\mathbb{Z}$-module $\Rightarrow \underline{\underline{a}}$ is a finitely generated $\mathcal{O}_K$-module. This proves:

Lemma 2.1

$\mathcal{O}_K$ is a Noetherian ring.

Notation

$\underline{\underline{a}} = (\alpha_1, \ldots, \alpha_r)$ means that $\underline{\underline{a}} = \{\sum_{i=1}^{r} \lambda_i \alpha_i \mid \lambda_i \in \mathcal{O}_K\}$

Definition

$\underline{\underline{a}}$ is principal if $\underline{\underline{a}} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$.

Note that $(\alpha) = (\beta) \Leftrightarrow \alpha/\beta \in \mathcal{O}_K^*$ (α, β are associates)

Definition

The product of ideals $\underline{\underline{a}}$ and $\underline{\underline{b}}$ is

$\underline{\underline{a}}\,\underline{\underline{b}} = \{ \sum_{i=1}^{m} \alpha_i \beta_i \mid \alpha_i \in \underline{\underline{a}}, \beta_i \in \underline{\underline{b}} \}$

If $\underline{\underline{a}} = (\alpha_1, \ldots, \alpha_r)$, $\underline{\underline{b}} = (\beta_1, \ldots, \beta_s)$, then

$\underline{\underline{a}}\,\underline{\underline{b}} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_r\beta_s)$. We say that $\underline{\underline{b}}$ divides $\underline{\underline{a}}$ if $\underline{\underline{a}} = \underline{\underline{b}}\,\underline{\underline{c}}$ for some ideal $\underline{\underline{c}}$.

Theorem 2.2

Let $\underline{\underline{a}} \subset \mathcal{O}_K$ be a non-zero ideal. Then, $\exists$ a non-zero ideal $\underline{\underline{b}}$ such that $\underline{\underline{a}}\,\underline{\underline{b}}$ is principal.

Lemma 2.3

For $\underline{\underline{a}} \subset \mathcal{O}_K$ an ideal, $\exists\ 0 \neq c \in \underline{\underline{a}} \cap \mathbb{Z}$, and $\mathcal{O}_K/\underline{\underline{a}}$ is finite

Proof

i) Pick $0 \neq \alpha \in \underline{\underline{a}}$. α has min. poly. $g(x) = x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0$

$g(x) \in \mathbb{Z}[x]$. $c_0 \neq 0$ (since g is irreducible), and $c_0 \in \mathbb{Z}$.

$c_0 = -\alpha(\alpha^{m-1} + c_{m-1}\alpha^{m-2} + \ldots + c_1) \in \underline{\underline{a}} \cap \mathbb{Z}$.

ii) If $0 \neq c \in \underline{\underline{a}} \cap \mathbb{Z}$, then $\mathcal{O}_K/(c) \twoheadrightarrow \mathcal{O}_K/\underline{\underline{a}}$ is surjective.

Theorem 1.13 $\Rightarrow \mathcal{O}_K \cong \mathbb{Z}^n$ as a groups under $+$.

$\Rightarrow \mathcal{O}_K/(c) \cong (\mathbb{Z}/c\mathbb{Z})^n$ is finite $\square$

Recall

An ideal $\underline{\underline{p}} \in \mathcal{O}_K$ is prime if $\mathcal{O}_K/\underline{\underline{p}}$ is an integral domain.

i.e. $\underline{\underline{p}} \neq \mathcal{O}_K$ and $x, y \in \mathcal{O}_K$, $xy \in \underline{\underline{p}} \Rightarrow x$ or $y \in \underline{\underline{p}}$

05/02/13

Number Fields ⑥

Lemma 2.4

Let $\underline{\underline{\mathfrak{p}}}$ be a prime ideal. If $\underline{\underline{\mathfrak{a}}}$ and $\underline{\underline{\mathfrak{b}}}$ are ideals, with $\underline{\underline{\mathfrak{a}}}\,\underline{\underline{\mathfrak{b}}} \subset \underline{\underline{\mathfrak{p}}}$, then $\underline{\underline{\mathfrak{a}}} \subset \underline{\underline{\mathfrak{p}}}$ or $\underline{\underline{\mathfrak{b}}} \subset \underline{\underline{\mathfrak{p}}}$

Proof

Suppose not. Then $\exists x \in \underline{\underline{\mathfrak{a}}} \setminus \underline{\underline{\mathfrak{p}}}$, $y \in \underline{\underline{\mathfrak{b}}} \setminus \underline{\underline{\mathfrak{p}}}$. Then $xy \in \underline{\underline{\mathfrak{a}}}\,\underline{\underline{\mathfrak{b}}} \subset \underline{\underline{\mathfrak{p}}}$ yet $x \notin \underline{\underline{\mathfrak{p}}}$, $y \notin \underline{\underline{\mathfrak{p}}}$. But $\underline{\underline{\mathfrak{p}}}$ was a prime ideal ⚔ □

Lemma 2.5

Every non-zero prime-ideal $\underline{\underline{\mathfrak{p}}} \subset \mathcal{O}_K$ is maximal.

Proof

If R is a finite integral domain, and $0 \neq x \in R$, then $R \to R$, $y \mapsto xy$ is injective. Hence this is surjective (by counting), $\Rightarrow \exists y \in R$ with $xy = 1$. $\therefore R$ is a field.

$\underline{\underline{\mathfrak{p}}}$ prime $\Rightarrow \mathcal{O}_K/\underline{\underline{\mathfrak{p}}}$ is an integral domain.

$\overset{\text{Lemma 2.3}}{\Rightarrow}$ $\mathcal{O}_K/\underline{\underline{\mathfrak{p}}}$ is a field $\Rightarrow \underline{\underline{\mathfrak{p}}}$ maximal. □

Conventions

For this course, a "prime ideal" means a "non-zero prime ideal".

Lemma 2.6

Every non-zero ideal $\underline{\underline{\mathfrak{a}}} \subset \mathcal{O}_K$ contains a product of prime ideals

Proof

Suppose not. Since $\mathcal{O}_K$ is Noetherian, $\exists\, \underline{\underline{\mathfrak{a}}} \subset \mathcal{O}_K$ that is maximal subject to not having this property i.e. $\underline{\underline{\mathfrak{a}}}$ does not contain a product of prime ideals.

$\mathfrak{a}$ not prime $\Rightarrow \exists x, y \in \mathcal{O}_K$ with $xy \in \mathfrak{a}$, but $x, y \notin \mathfrak{a}$.

$\mathfrak{a} \subsetneq \mathfrak{a} + (x)$ $\overset{\text{choice of } \mathfrak{a}}{\Rightarrow}$ $\mathfrak{P}_1 \dots \mathfrak{P}_r \subset \mathfrak{a} + (x)$ for $\mathfrak{P}_i$ prime.

$\mathfrak{a} \subsetneq \mathfrak{a} + (y) \Rightarrow \mathfrak{q}_1 \dots \mathfrak{q}_s \subset \mathfrak{a} + (y)$ for $\mathfrak{q}_i$ prime.

$\Rightarrow \mathfrak{P}_1 \dots \mathfrak{P}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subset (\mathfrak{a} + (x))(\mathfrak{a} + (y)) \subset \mathfrak{a}$ (since $xy \in$

$\lightning$ of choice of $\mathfrak{a}$. $\square$

Lemma 2.7

Let $\mathfrak{a} \subsetneq \mathcal{O}_K$, an ideal. Then, $\exists x \in K$ such that $x\mathfrak{a} \subset \mathcal{O}_K$ but $x \notin \mathcal{O}_K$.

Proof

WLOG $\mathfrak{a}$ is maximal, and hence prime, say $\mathfrak{a} = \mathfrak{P}$. Pick $0 \neq \alpha \in$

Lemma 2.6 $\Rightarrow \mathfrak{P}_1 \dots \mathfrak{P}_r \subset (\alpha)$, $\mathfrak{P}_i$ prime. We take r to be minimal. Lemma 2.4 $\Rightarrow \mathfrak{P}_i \subset \mathfrak{P}$ for some i.

Lemma 2.5 $\Rightarrow \mathfrak{P}_i = \mathfrak{P}$, since $\mathfrak{P}_i$ is prime, hence maximal.

WLOG, $\mathfrak{P} = \mathfrak{P}_1$. Choice of $r \Rightarrow \mathfrak{P}_2 \dots \mathfrak{P}_r \notin (\alpha)$.

Pick $\tau \in \mathfrak{P}_2 \dots \mathfrak{P}_r \setminus (\alpha)$. Then $\tau \mathfrak{P} \subset (\alpha)$, yet $\tau \notin (\alpha$

$\Rightarrow \frac{\tau}{\alpha} \mathfrak{P} \subset \mathcal{O}_K$ yet $\frac{\tau}{\alpha} \notin \mathcal{O}_K$. Take $x = \frac{\tau}{\alpha}$ $\square$

07/02/13 Number Fields (7)

Lemma 2.8

Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. If $x \in K$ with $x\mathfrak{a} \subset \mathfrak{a}$ then $x \in \mathcal{O}_K$.

Proof

Let $\mathfrak{a}$ have $\mathbb{Z}$-basis $w_1, \dots, w_n$. Then $xw_i = \sum_{j=1}^{n} a_{ij} w_j$, for some $a_{ij} \in \mathbb{Z}$. $A = (a_{ij}) \Rightarrow (xI_n - A)\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = 0$

Multiply on the left by $\operatorname{adj}(xI_n - A)$, and use that $w_i \neq 0$ for some i. $\Rightarrow \det(xI_n - A) = 0$

$\Rightarrow x$ satisfies a monic polynomial in $\mathbb{Z}[x]$. $\therefore x \in \mathcal{O}_K$ □

Example

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (9, 3(1-\sqrt{-5}), 3(1+\sqrt{-5}), 6) = (3)$ (not principal)

Definition

$\mathfrak{a} \subset K$ is a fractional ideal if $\exists\, 0 \neq c \in K$ such that $c\mathfrak{a} \subset \mathcal{O}_K$ is an ideal. N.B. fractional ideals need not be ideals.

Lemma 2.9

Let $\mathfrak{a} \subset K$. $\mathfrak{a}$ a fractional ideal $\Leftrightarrow \mathfrak{a}$ is a finitely generated $\mathcal{O}_K$ mod

Proof

"$\Rightarrow$" Use that $\mathcal{O}_K$ is Noetherian (Lemma 2.1).

"$\Leftarrow$" Use that $K = \operatorname{Frac} \mathcal{O}_K$ (Lemma 1.11). □

The original ideals are called integral ideals.

Multiplication of fractional ideals is defined as before.

Definition

A fractional ideal $\mathfrak{a}$ is *invertible* if $\exists$ a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\cdot\mathfrak{b} = (1) = \mathcal{O}_K$

Example (continued)

$(3, \mathfrak{a}) = (3, 1+\sqrt{-5})$, $(1, \mathfrak{a}^{-1}) = (1, \frac{1-\sqrt{-5}}{3})$

$= (1)$

Theorem 2·2 is equivalent to the statement that "every non-zero fractional ideal is invertible."

Remark

If $\mathfrak{a}$ is invertible, then it is easy to show that

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

Proof of Theorem 2·2

Suppose that this is false. Since $\mathcal{O}_K$ is Noetherian, $\exists$ an integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ maximal subject to not being invertible.

Let $\mathfrak{b} = \{x \in K : x\mathfrak{a} \in \mathcal{O}_K\}$. To see that $\mathfrak{b}$ is a fractional ideal, take $0 \neq \alpha \in \mathfrak{a}$. Then $\alpha\mathfrak{b} \subset \mathcal{O}_K$.

We have $\mathcal{O}_K \subset \mathfrak{b} \Rightarrow \mathfrak{a} \subset \mathfrak{a}\cdot\mathfrak{b}$.

If $\mathfrak{a} = \mathfrak{a}\cdot\mathfrak{b}$, then Lemma 2·8 $\Rightarrow \mathfrak{b} \subset \mathcal{O}_K$. But Lemma 2·7 constructs $x \in \mathfrak{b} \setminus \mathcal{O}_K$ ⚡

$\therefore \mathfrak{a} \subsetneq \mathfrak{a}\cdot\mathfrak{b} \subset \mathcal{O}_K$.

By choice of $\mathfrak{a}$, $\mathfrak{a}\cdot\mathfrak{b}$ is invertible $\Rightarrow \mathfrak{a}$ is invertible ⚡ □

Corollary 2·10

Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be integral ideals with $\mathfrak{c}$ non-zero.

i) $\mathfrak{b} \mid \mathfrak{a} \iff \mathfrak{b}\cdot\mathfrak{c} \mid \mathfrak{a}\cdot\mathfrak{c}$

07/02/13

Number Fields (7)

$\mathfrak{b} \mid \mathfrak{a}$ $\overset{(i)}{\iff}$ $\mathfrak{b}\cdot\mathfrak{c} \mid \mathfrak{a}\cdot\mathfrak{c}$

$\Downarrow$ (iii) $\qquad$ (ii) $\Updownarrow$

$\mathfrak{a} \subset \mathfrak{b}$ $\iff$ $\mathfrak{a}\cdot\mathfrak{c} \subset \mathfrak{b}\cdot\mathfrak{c}$

"To contain, is to divide."

(i) and (ii) "$\Rightarrow$" is clear. "$\Leftarrow$" Multiply by the fractional ideal $\mathfrak{c}^{-1}$

iii) "$\Downarrow$" is clear. "$\Uparrow$" By i), ii) and Theorem 2·2, we may assume that $\mathfrak{b}$ is principal. Say $\mathfrak{b} = (\beta) \supset \mathfrak{a} = (\alpha_1, \dots, \alpha_r)$

Let $\mathfrak{d} = (\alpha_1/\beta, \dots, \alpha_r/\beta) \subset \mathcal{O}_K$. Then $\mathfrak{b}\cdot\mathfrak{d} = \mathfrak{a} \Rightarrow \mathfrak{b} \mid \mathfrak{a}$ ∎

Theorem 2·11

Every non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ can be written uniquely as a product of prime ideals.

Proof (Existence)

We claim that if $\mathfrak{a} \subsetneq \mathcal{O}_K$ is not prime, then $\mathfrak{a} = \mathfrak{b}\cdot\mathfrak{c}$ for some $\mathfrak{a} \subsetneq \mathfrak{b}$, $\mathfrak{a} \subsetneq \mathfrak{c}$. Then apply the same argument to $\mathfrak{b}$ and $\mathfrak{c}$, and so on. This process stops, since $\mathcal{O}_K$ is Noetherian.

To prove the claim, $\mathfrak{a} \subset \mathfrak{p}$ for some $\mathfrak{p}$ maximal $\Rightarrow \mathfrak{p}$ prime.

By Corollary 2·10 (ii), $\mathfrak{a} = \mathfrak{p}\cdot\mathfrak{b}$ for some integral ideal $\mathfrak{b}$.

$\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a} \subset \mathfrak{b}$. If $\mathfrak{a} = \mathfrak{p}$, then $\mathfrak{a}$ is prime ✗

If $\mathfrak{a} = \mathfrak{b}$, then multiplying by $\mathfrak{a}^{-1}$, we get $\mathfrak{p} = \mathcal{O}_K$ ✗

$\therefore \mathfrak{a} \subsetneq \mathfrak{p}$, $\mathfrak{a} \subsetneq \mathfrak{b}$.

(Uniqueness)

Lemma 2·4 now says "$\mathfrak{p} \mid \mathfrak{a}\cdot\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$"

Suppose that $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$

Then $\mathfrak{p}_1 \mid \mathfrak{q}_1 \dots \mathfrak{q}_r \Rightarrow \mathfrak{p}_1 \mid \mathfrak{q}_i$ for some $i \Rightarrow \mathfrak{p}_1 = \mathfrak{q}_i$, Lemma 2-5

Renumbering, WLOG $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying by $\mathfrak{p}_1^{-1}$ gives

$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s$, and repeat. □

Theorem 2·12

The non-zero fractional ideals of K form a group I_K under multiplication. It is a free abelian group on the primes, i.e. every $\mathfrak{a} \in I_K$ can be written uniquely as $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_r^{\alpha_r}$ where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals and $\alpha_1, \dots, \alpha_r \in \mathbb{Z}$.

Remark

$\mathfrak{a} \subset \mathcal{O}_K \iff \alpha_i \geq 0 \ (\forall i)$

Proof:

The difficult part in checking that I_K is a group is checking inverses. (See Theorem 2-2). We may write any fractional ideal in the form $\mathfrak{b} \cdot \mathfrak{c}^{-1}$, where $\mathfrak{b}, \mathfrak{c}$ are integral ideals. Now use Theorem 2·11. □

There is a group homomorphism

$K^* \to I_K \quad , \quad x \mapsto (x) \leftarrow$ fractional ideal

with kernel $\mathcal{O}_K^*$ and image P_K, the group of principal fractional ideals.

Definition

The class group is $Cl_K = I_K / P_K$

12/02/13 Number Fields (8)

Let k be a number field. We define an equivalence relation on the ideals in $\mathcal{O}_k$:

$\underline{a} \sim \underline{b} \Leftrightarrow \exists\, 0 \neq r, s \in \mathcal{O}_k$ such that $r\underline{a} = s\underline{b}$

Notation

$[\underline{a}]$ = the equivalence class of $\underline{a}$

The equivalence classes form the group Cl_k under $[\underline{a}]\cdot[\underline{b}] = [\underline{ab}]$

(Exercise: Check that this is well defined and satisfies the group axioms)

Proposition 2.13

The following are equivalent:

i) $\mathcal{O}_k$ is a PID.

ii) $\mathcal{O}_k$ is a UFD

iii) Cl_k is trivial.

Proof

i) $\Rightarrow$ ii) See GRM

ii) $\Rightarrow$ i). Let $\underline{p} \subset \mathcal{O}_k$, prime. Let $0 \neq x \in \underline{p}$ and write $x = \pi_1 \dots \pi_r$, π_i irreducible.

$\pi_1 \dots \pi_r \in \underline{p} \Rightarrow \pi_i \in \underline{p}$, for some $i \Rightarrow (\pi_i) \subset \underline{p}$

$\Rightarrow (\pi_i) = \underline{p}$, by Lemma 2.5.

Then by theorem 2.11, $\mathcal{O}_k$ is a PID

i) $\Leftrightarrow$ iii) by definition of Cl_k.

Remark

For $\mathfrak{a}, \mathfrak{b}$ ideals, $\mathfrak{a}+\mathfrak{b} = \{x+y \mid x \in \mathfrak{a},\ y \in \mathfrak{b}\}$

It is the smallest ideal containing (dividing) both $\mathfrak{a}$ and $\mathfrak{b}$ i.e. the gcd of $\mathfrak{a}$ and $\mathfrak{b}$. We may think of $\mathfrak{a} = (\alpha_1, \dots, \alpha_r)$ as the gcd of $\alpha_1, \dots, \alpha_r$.

Norm of Ideals

Definition

Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. For $\alpha, \beta \in \mathcal{O}_K$, write $\alpha - \beta \in \mathfrak{a}$ as $\alpha \equiv \beta \pmod{\mathfrak{a}}$. The ideal norm is the number of equivalence classes, $N(\mathfrak{a}) = \left| \mathcal{O}_K / \mathfrak{a} \right|$ (finite by Lemma 2.3). By Lagrange, $N(\mathfrak{a}) \in \mathfrak{a} \cap \mathbb{Z}$.

$0(1) \mid N(\mathfrak{a}) \Rightarrow N(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{a}}$ by definition

Proposition 2.14

Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ be ideals. Then $N(\mathfrak{a} \cdot \mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$

Proof

By theorem 2.11, it suffices to prove that this holds when $\mathfrak{b} = \mathfrak{p}$ is prime. By the Isomorphism Theorem:

$$\frac{\mathcal{O}_K / \mathfrak{a}\mathfrak{p}}{\mathfrak{a} / \mathfrak{a}\mathfrak{p}} \xrightarrow{\sim} \mathcal{O}_K / \mathfrak{a}$$

$$\Rightarrow N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a}) \cdot \left| \mathfrak{a} / \mathfrak{a}\mathfrak{p} \right|$$

Pick $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}$. We claim that there is an isomorphism $\mathcal{O}_K / \mathfrak{p} \to \mathfrak{a} / \mathfrak{a}\mathfrak{p}$ (as groups under $+$).

$x \bmod \mathfrak{p} \mapsto \alpha x \bmod \mathfrak{a}\mathfrak{p}$

Injective

Write $(\alpha) = \mathfrak{a}\mathfrak{c}$, for some ideal $\mathfrak{c} \subset \mathcal{O}_K$.

If $x \in \mathcal{O}_K$ with $\alpha x \in \mathfrak{a}\mathfrak{P}$, then $\mathfrak{a} \subseteq (x) \subset \mathfrak{a}\mathfrak{P}$

$\Rightarrow$ either $\mathfrak{a} \subset \mathfrak{P}$ or $x \in \mathfrak{P}$

$\alpha \in \mathfrak{a}\mathfrak{P}$ $\quad$ $x \equiv 0 \bmod \mathfrak{P}$

Surjective

Choice of $\alpha \Rightarrow \mathfrak{a}\mathfrak{P} \subsetneq \mathfrak{a}\mathfrak{P} + (\alpha) \subset \mathfrak{a}$

So $\mathfrak{a} \mid \mathfrak{a}\mathfrak{P} + (\alpha) \mid \mathfrak{a}\mathfrak{P}$

$\Rightarrow \mathfrak{a}\mathfrak{P} + (\alpha) = \mathfrak{a}$ since $\mathfrak{P}$ is prime.

This proves the claim.

So $N(\mathfrak{a}\mathfrak{P}) = N(\mathfrak{a}) \left| \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{P}} \right| = N(\mathfrak{a}) N(\mathfrak{P})$ $\square$

Lemma 2.15

Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. Then, $\exists$ a basis $r_1, \dots, r_n$ for K over $\mathbb{Q}$ such that $\mathfrak{a} = \left\{ \sum_{i=1}^{n} \lambda_i r_i \mid \lambda_i \in \mathbb{Z} \right\}$

Moreover, $\Delta(r_1, \dots, r_n) = (N(\mathfrak{a}))^2 D_K$

Proof

If $0 \neq m \in \mathfrak{a} \cap \mathbb{Z}$ then $m\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$.

Lemma 1.15 $\Rightarrow \mathfrak{a} \cong \mathbb{Z}^n$ (as a group under $+$). because ideals have finite index, and are subgroups $\cong \mathbb{Z}^n$

For the last part, write $r_j = \sum_{i=1}^{n} a_{ij} x_i$, where $x_1, \dots, x_n$ are an integral basis, and $a_{ij} \in \mathbb{Z}$. $A = (a_{ij})$ some $r \in n$.

$\Delta(r_1, \dots, r_n) = (\det A)^2 \Delta(x_1, \dots, x_n)$

Lemma 1.15 $\Rightarrow |\det A| = (\mathcal{O}_K : \mathfrak{a})$

$\therefore \Delta(r_1, \dots, r_n) = (N(\mathfrak{a}))^2 D_K$ $\square$

Proposition 2.16

If $0 \neq \alpha \in \mathcal{O}_K$, then $N(\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$

Proof

Let $x_1, \ldots, x_n$ be an integral basis. If $r_i = \alpha x_i$, then

$$\Delta(r_1, \ldots, r_n) = \det(\sigma_i(\alpha x_j))^2 = \prod_{i=1}^{n} \sigma_i(\alpha)^2 \, \Delta(x_1, \ldots, x_n)$$

$$= (N_{K/\mathbb{Q}}(\alpha))^2 D_K$$

Lemma 2.15 $\Rightarrow N_{K/\mathbb{Q}}(\alpha)^2 = (N(\alpha))^2$

$\Rightarrow |N_{K/\mathbb{Q}}(\alpha)| = N(\alpha)$ □

Example

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$$\mathfrak{a} = (3, 1+\sqrt{-5})$$

$$= \{3a + (1+\sqrt{-5})b : a, b \in \mathcal{O}_K\}$$

$$= \{3a + (1+\sqrt{-5})b : a, b \in \mathbb{Z}\}$$ ↙ calculation

$$\therefore \mathfrak{a} = \ker\left(\begin{array}{l}\mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_3 \\ x + y\sqrt{-5} \mapsto x - y \bmod 3\end{array}\right)$$

$\Rightarrow N\mathfrak{a} = 3$

But $x^2 + 5y^2 = \pm 3$ has no solutions for $x, y \in \mathbb{Z}$

$\therefore$ By proposition 2.16, $\mathfrak{a}$ is not principal.

Corollary 2.17

Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime ideal. Then $\exists$ a unique rational prime p such that $\mathfrak{P} \mid p$ (i.e. $\mathfrak{P} \mid (p)$). Moreover, $N\mathfrak{P}$ is a power of p.

Proof

$\mathfrak{P}$ prime $\Rightarrow \mathfrak{P} \cap \mathbb{Z}$ prime (non-empty by Lemma 2.3)

$\therefore$ ~~$\mathfrak{P}$ prime~~ $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p.

Remark

For $a \in \mathbb{Z}$, $a \in \mathfrak{P} \Leftrightarrow a \in p\mathbb{Z}$, or $\mathfrak{P} \mid a \Leftrightarrow p \mid a$

We have $\mathfrak{P} \mid p \Rightarrow \mathfrak{P}\mathfrak{b} = (p)$ for some ideal $\mathfrak{b} \subset \mathcal{O}_K$.

$\Rightarrow N\mathfrak{P}\, N\mathfrak{b} = p^n \qquad (n = [K : \mathbb{Q}])$

$\Rightarrow N\mathfrak{P}$ is a power of p. $\square$

Let p be a rational prime.

Aim

Compute the factorisation of $(p) = p\mathcal{O}_K$ into prime ideals.

$\mathcal{O}_K \xrightarrow{q} \frac{\mathcal{O}_K}{p\mathcal{O}_K}$. $\{\text{prime ideals in } \frac{\mathcal{O}_K}{p\mathcal{O}_K}\} \leftrightarrow \{\text{ideals in } \mathcal{O}_K \text{ containing } p\}$ (dividing)

$I \mapsto q^{-1}(I)$. Since $\mathcal{O}_K/p\mathcal{O}_K$ is a finite ring, we could compute its prime ideals by trying all subsets.

Fortunately, we can do better.

Dedekind's Criterion

Let $\alpha \in \mathcal{O}_K$ with minimal polynomial $g \in \mathbb{Z}[x]$. Suppose $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ has finite index, coprime to p. If $\bar{g} \in \mathbb{F}_p[x]$ factors into irreducibles $\bar{g} = \phi_1^{e_1} \phi_2^{e_2} \cdots \phi_r^{e_r}$

then $p = \underline{p}_1^{e_1} \underline{p}_2^{e_2} \dots \underline{p}_r^{e_r}$, factoring into prime ideals, with $\underline{p}_i = (p, \phi_i(\alpha))$

Proof

1) Case where $\mathcal{O}_K = \mathbb{Z}[\alpha]$

There are surjective ring homomorphisms

$\mathbb{Z}[x] \to \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]}$, $f(x) \mapsto f(\alpha) \bmod p$

$\mathbb{Z}[x] \to \frac{\mathbb{F}_p[x]}{(\bar{g})}$ $f(x) \mapsto \bar{F}(x) \bmod \bar{g}$

each with kernel $(p, g(x))$. We claim that the map

$$\mathcal{O}_K \twoheadrightarrow \frac{\mathcal{O}_K}{p\mathcal{O}_K} = \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} \xrightarrow{\sim} \frac{\mathbb{F}_p[x]}{(\bar{g})} \twoheadrightarrow \frac{\mathbb{F}_p[x]}{(\bar{\phi}_i)}$$

has kernel $\underline{p}_i = (p, \phi_i(\alpha))$

Indeed, $p \mapsto 0$ and $\phi_i(\alpha) \to 0$, so $\underline{p}_i$ is contained in the kernel.

Conversely, if $f \in \mathbb{Z}[x]$ with $f(\alpha) \mapsto 0$, then $\phi_i \mid F$

$\Rightarrow f(x) = q(x)\phi_i(x) + ph(x)$, $q, h \in \mathbb{Z}[x]$

$\Rightarrow f(\alpha) \in (p, \phi_i(\alpha)) = \underline{p}_i$.

$\phi_i \in \mathbb{F}_p[x]$ irreducible $\Rightarrow \frac{\mathbb{F}_p[x]}{(\phi_i)}$ is a field $\Rightarrow \underline{p}_i$ prime

Moreover, $N\underline{p}_i = \left|\frac{\mathbb{F}_p[x]}{(\phi_i)}\right| = p^{f_i}$ where $f_i = \deg(\phi_i)$

Remark

$$[K:\mathbb{Q}] = \deg(\bar{g}) = \sum_{i=1}^{r} e_i \deg(\phi_i) = \sum_{i=1}^{r} e_i f_i \qquad (*)$$

Now $\underline{p}_i = (p, \phi_i(\alpha)) \Rightarrow \underline{p}_i^{e_i} \subset (p, \phi_i(\alpha)^{e_i})$

$\Rightarrow \underline{p}_1^{e_1} \dots \underline{p}_r^{e_r} \subset (p, \phi_1(\alpha)^{e_1} \dots \phi_r(\alpha)^{e_r}) = (p, g(\alpha))$

$= (p)$ since $g(\alpha) = 0$

To prove equality, we take ideal norms.

$N(\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}) = p^{\sum e_i f_i} \overset{(*)}{=} p^{[K:\mathbb{Q}]} = N(p)$

Note

If $i \neq j$, then $\phi_i, \phi_j \in \mathbb{F}_p[x]$ coprime

$\Rightarrow \mathfrak{P}_i + \mathfrak{P}_j = (p, \phi_i(\alpha), \phi_j(\alpha)) = \mathcal{O}_K \Rightarrow \mathfrak{P}_i \neq \mathfrak{P}_j$

2) General case (i.e. not assuming that $\mathcal{O}_K = \mathbb{Z}[\alpha]$)

$\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ has index coprime to p.

$\Rightarrow \frac{\mathcal{O}_K}{\mathbb{Z}[\alpha]} \xrightarrow{\times p} \frac{\mathcal{O}_K}{\mathbb{Z}[\alpha]}$ is an isomorphism

$\Rightarrow \begin{cases} \mathbb{Z}[\alpha] \cap p\mathcal{O}_K = p\mathbb{Z}[\alpha] \\ \mathbb{Z}[\alpha] + p\mathcal{O}_K = \mathcal{O}_K \end{cases}$ look at both kernels

$\Rightarrow \frac{\mathbb{Z}[\alpha]}{p\mathbb{Z}[\alpha]} \to \frac{\mathcal{O}_K}{p\mathcal{O}_K}$ is an isomorphism.

The proof in 1) now applies. □

Quadratic Fields

$K = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$, d a squarefree integer

$\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$ has index 1 or 2.

Let p be an odd prime. By Dedekind's Criterion, there are 3 cases.

i) $X^2 - d$ has two distinct roots mod p (i.e. $\left(\frac{d}{p}\right) = +1$)

Then $(p) = \mathfrak{P}\mathfrak{P}'$, $N\mathfrak{P} = N\mathfrak{P}' = p$, $\mathfrak{P} \neq \mathfrak{P}'$

i.e. p splits in $K/\mathbb{Q}$

ii) $X^2 - d$ has a repeated root mod p (i.e. $p \mid d$)

Then $(p) = \mathfrak{P}^2$, $N\mathfrak{P} = p$. We say that p ramifies in $K/\mathbb{Q}$.

iii) $X^2 - d$ is irreducible mod p (i.e. $\left(\frac{d}{p}\right) = -1$)

Then $(p) = \mathfrak{P}$, $N\mathfrak{P} = p^2$. We say that p is inert in $K/\mathbb{Q}$

For K any number field, p a rational prime.

$p\mathcal{O}_K = (p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, $N\mathfrak{p}_i = p^{f_i}$

$e_1, \ldots, e_r$ are called <u>ramification indices</u>.

$f_1, \ldots, f_r$ are called <u>residue class degrees</u>.

Taking ideal norms $\Rightarrow \sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}]$

<u>Terminology</u>

p ramifies in $K/\mathbb{Q}$ $\Leftrightarrow$ some $e_i > 1$

p inert in $K/\mathbb{Q}$ $\Leftrightarrow$ $r = 1$, $e_1 = 1$

p splits completely in $K/\mathbb{Q}$ $\Leftrightarrow$ $e_i = f_i = 1 \ \forall i$

3 Class Groups and Units

Definition

A subset $X \subset \mathbb{R}^n$ is *discrete* if $\forall x \in X \ \exists \varepsilon > 0$ such that $B(x, \varepsilon) \cap X = \{x\}$

Lemma 3.1

Let $\Lambda \subset \mathbb{R}^n$. The following are equivalent:

i) $\Lambda = \{ \sum_{i=1}^{m} a_i x_i \mid a_i \in \mathbb{Z} \}$ for some $\mathbb{R}$-linearly independent $x_1, \dots, x_m \in \mathbb{R}^n$.

ii) Λ is a discrete subgroup of $(\mathbb{R}^n, +)$.

If these conditions hold, then Λ is called a *lattice*.

Proof

Both of the conditions are invariant under all linear automorphisms of $\mathbb{R}^n$. Replacing $\mathbb{R}^n$ by a subspace, we may assume that Λ spans $\mathbb{R}^n$.

i) $\Rightarrow$ ii) WLOG, $\Lambda = \mathbb{Z}^n$. Take $\varepsilon = \frac{1}{2}$.

ii) $\Rightarrow$ i) WLOG, $\Lambda \supset \mathbb{Z}^n$. Let $X = \{(a_1, \dots, a_n) \in \mathbb{R}^n \mid 0 \le a_i \le 1\}$

X closed and bounded, hence compact. Λ discrete, X compact $\Rightarrow \Lambda \cap X$ is finite.

$\Rightarrow \Lambda / \mathbb{Z}^n$ is finite, say of order d.

Then $\mathbb{Z}^n \subset \Lambda \subset \frac{1}{d}\mathbb{Z}^n$. Lemma 1.15 $\Rightarrow \Lambda \cong \mathbb{Z}^n$

$M \subset \mathbb{Z}^n$ a subgroup $\Rightarrow M \cong \mathbb{Z}^r$, $r \le n$

Say $\Lambda = \{ \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{Z} \}$, for some $x_1, \dots, x_n \in \mathbb{R}^n$

Recall that Λ spans $\mathbb{R}^n \Rightarrow x_1, \dots, x_n$ span $\mathbb{R}^n$

$\Rightarrow x_1, \dots, x_n$ linearly independent $\square$

Recall (from GRM)

If A is a finitely generated abelian group, then $A \cong T \times \mathbb{Z}^r$ where T is a finite group (the torsion subgroup) and r is the rank of A.

Let K be a number field. $[K:\mathbb{Q}] = n = r + 2s$

$\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$. $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+1}, \dots, \overline{\sigma}_{r+s} : K \hookrightarrow \mathbb{C}$

There is a group homomorphism

$$L : \mathcal{O}_K^* \to \mathbb{R}^{r+s}, \quad u \mapsto (\log|\sigma_1(u)|, \dots, \log|\sigma_{r+s}(u)|)$$

Lemma 3.2

If $B \subset \mathbb{R}^{r+s}$ bounded, then $L^{-1}(B)$ is finite.

Proof:

If $u \in L^{-1}(B)$ then $|\sigma_i(u)|$ is bounded $\forall i$.

$\Rightarrow f(x) = \prod_{i=1}^{n} (x - \sigma_i(u))$ has bounded coefficients,

and $f(x) \in \mathbb{Z}[x] \Rightarrow$ only finitely many possibilities for f

(f a power of the min. poly.)

$\Rightarrow$ only finitely many possibilities for u □

By Lemma 3.2, $\ker(L)$ is finite (and hence consists of roots of unity) (finite order elements) and $\mathrm{Im}(L)$ is a discrete subgroup of $\mathbb{R}^{r+s}$ (a finite subgroup of $\mathcal{O}_K^*$)

~~because $\cong \mathbb{Z}^{r+s} \times T$~~ ? finiteness of $L^{-1}(B)$

Lemma 3.1 $\Rightarrow \mathcal{O}_K^*$ is a finitely generated abelian group of rank $\leq r+s$.

Lemma 1.10 says that $u \in \mathcal{O}_K^*$

$\Rightarrow \prod_{i=1}^{n} \sigma_i(u) = N_{K/\mathbb{Q}}(u) = \pm 1$.

$\therefore \mathrm{Im}(L) \subset \{(x_1, \dots, x_r, y_1, \dots, y_s) \in \mathbb{R}^{r+s} \mid \sum x_i + 2\sum y_i = 0\}$.

We deduce the following.

Proposition 3.3

$\mathcal{O}_K^*$ is a finitely generated abelian group of rank $\leq r+s-1$

Dirichlet's Unit Theorem is the statement that equality holds in Proposition 3.3. ($\rho = r+s-1$)

i.e. $\exists$ units $\varepsilon_1, \ldots, \varepsilon_\rho \in \mathcal{O}_K^*$ such that every $u \in \mathcal{O}_K^*$ can be written uniquely in the form $u = \zeta \varepsilon_1^{m_1} \cdots \varepsilon_\rho^{m_\rho}$ where ζ is a root of unity, and $m_1, \ldots, m_\rho \in \mathbb{Z}$.

We call $\varepsilon_1, \ldots, \varepsilon_\rho$ a set of fundamental units.

Units in Quadratic Fields

$K = \mathbb{Q}(\sqrt{d})$, $d \neq 0, 1$, squarefree integer

$d \equiv 1 \ (4)$, $\mathcal{O}_K^* = \left\{ x + y\left(\frac{1+\sqrt{d}}{2}\right) \mid x, y \in \mathbb{Z}, \left(x + \frac{y}{2}\right)^2 - \frac{d}{4} y^2 = \pm 1 \right\}$

$d \equiv 2, 3 \ (4)$, $\mathcal{O}_K^* = \{ x + y\sqrt{d} \mid x, y \in \mathbb{Z}, x^2 - dy^2 = \pm 1 \}$

i) $d < 0$. K is an imaginary quadratic field.

Dirichlet $\Rightarrow \mathcal{O}_K^*$ has rank $r+s-1 = 0$ ($r=0, s=1$)

If $d = -1$, $\mathcal{O}_K = \mathbb{Z}[i]$, $\mathcal{O}_K^* = \{\pm 1, \pm i\}$

If $d = -3$, $\mathcal{O}_K = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$, $\mathcal{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\}$

If $d < -3$, then $\mathcal{O}_K^* = \{\pm 1\}$

ii) $d > 0$. K is a real quadratic field.

Dirichlet $\Rightarrow \mathcal{O}_K^*$ has rank $r+s-1 = 1$ ($\begin{matrix} r=2 \\ s=0 \end{matrix}$)

$K \subset \mathbb{R} \Rightarrow$ only roots of unity are ± 1

$\therefore \mathcal{O}_K^* = \{ \pm \varepsilon^m : m \in \mathbb{Z} \}$ for some $\varepsilon > 1$ called the fundamental unit. (unique, c.f. Number Theory)

$K = \mathbb{Q}(\sqrt{7})$. $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$. $\varepsilon = 8 + 3\sqrt{7}$

$N_{K/\mathbb{Q}}(\varepsilon) = 1$. We claim that ε is the fundamental unit.

If not, $\exists\ u = a + b\sqrt{7}$ $(a, b \in \mathbb{Z})$, $u \in \mathcal{O}_K^*$, and $1 < u < \varepsilon$. Let $\bar{u} = a - b\sqrt{7}$. $u\bar{u} = \pm 1 \Rightarrow |\bar{u}| < 1$

$\Rightarrow u \pm \bar{u} > 0$. $\Rightarrow a > 0,\ b > 0$.

But $a + b\sqrt{7} < 8 + 3\sqrt{7}$.

$\Rightarrow$ Only finitely many a, b to consider.

N.B. $a^2 - 7b^2 = \pm 1$.

$b = 1 \Rightarrow a^2 = 7 \pm 1$ ✗

$b = 2 \Rightarrow a^2 = 28 \pm 1$ ✗

$b \geq 3 \Rightarrow a \geq 8$ ✗ to $u < \varepsilon$

$\therefore \mathcal{O}_K^* = \{ \pm (8 + 3\sqrt{7})^m \}_{m \in \mathbb{Z}}$

Number Fields (II)

Remarks

i) Proposition 3.3 says that $\mathcal{O}_k^* / \{\pm 1\}$ is either trivial or infinite cyclic. This can be proved more simply along the lines of the example (with $k = \mathbb{Q}(\sqrt{7})$).

ii) Finding units in $\mathbb{Z}[\sqrt{d}]$ is equivalent to solving the Pell equation $x^2 - dy^2 = 1$ and (where possible) the negative Pell equation $x^2 - dy^2 = -1$. These equations can be solved using continued fractions (c.f. Number Theory)

Remark (used in proofs of Lemma 3.1)

$\Lambda \subset (\mathbb{R}^n, +)$ a discrete subgroup $\Rightarrow \Lambda \subset \mathbb{R}^n$ closed

Proof:

Λ a discrete subgroup $\Rightarrow \exists \varepsilon > 0$ such that $d(x, y) > \varepsilon$ $\forall x, y \in \Lambda$ discrete. So every sequence in Λ convergent in $\mathbb{R}^n$ must be eventually constant. $\square$

Let $\Lambda \in \mathbb{R}^n$ be a lattice spanned by the rows of an $n \times n$, non-singular matrix A.

Definitions

i) The <u>determinant</u> (or covolume) of Λ is $d(\Lambda) = |\det A|$ (depends on the lattice Λ, but not on A).

ii) A subset $X \subset \mathbb{R}^n$ is <u>convex</u> if $x, y \in X \Rightarrow \lambda x + (1-\lambda) y \in X$ $\forall \lambda \in [0, 1]$, and <u>symmetric about 0</u> if $x \in X \Rightarrow -x \in X$.

Minkowski's Theorem

Let S be a measurable subset of $\mathbb{R}^n$ that is convex and symmetric about 0. Suppose that either

i) volume $(S) > 2^n d(\Lambda)$

ii) $\text{vol}(S) \geq 2^n d(\Lambda)$, and S is compact.

Then S contains a non-zero element of Λ. We deduce this from:

Blichfeldt's Theorem

If X is a measurable subset of $\mathbb{R}^n$ with $\text{vol}(X) > d(\Lambda)$ then $\exists\, x, y \in X$ such that $0 \neq x - y \in \Lambda$

Blichfeldt $\Rightarrow$ Minkowski

i) Let $X = \frac{1}{2}S$. Then $\exists\, x, y \in X$ with $0 \neq x - y \in \Lambda$.

$2x, 2y \in S$. Convex, Symmetric $\Rightarrow \frac{1}{2}(2x - 2y) \in S$

So $x - y \in S$.

ii) Construct $0 \neq x_n \in \Lambda$ ~~such that~~ by applying i) to $(1 + \frac{1}{n})S$.

Write $x_n = (1 + \frac{1}{n}) y_n$. S compact $\Rightarrow$ passing to a subsequence, the y_n converge, to a limit $x \in S$, and $x \in \Lambda$.

Proof of Blichfeldt

Let Λ have a basis $x_1, \ldots, x_n$. Let $F = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; 0 \leq a_i \leq 1 \right\}$.

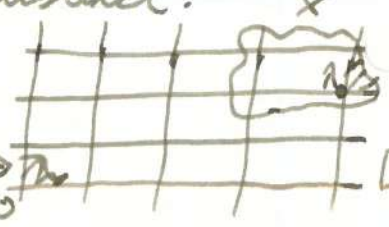
For $\lambda \in \Lambda$ let $X_\lambda = \{x \in F : \lambda + x \in X\}$

$$\sum_{\lambda} \text{vol}(X_\lambda) = \text{vol}(X) \underset{\text{hypothesis}}{>} d(\Lambda) = \text{vol}(F)$$

$\therefore X_\lambda \cap X_{\lambda'} \neq \emptyset$ for some λ, λ', distinct.

$\exists\, u \in F$ such that $\underbrace{\lambda + u}_{x}, \underbrace{\lambda' + u}_{y} \in X$

Then $0 \neq x - y = \lambda - \lambda' \in \Lambda$. □



Number Fields (11)

k a number field, $[k:\mathbb{Q}] = n = r + 2s$

Theorem 3.4

If $\mathfrak{a} \subset \mathcal{O}_k$, a non-zero ideal, then $\exists\, 0 \neq \alpha \in \mathfrak{a}$ such that $|N_{k/\mathbb{Q}}(\alpha)| \leq c\, N\mathfrak{a}\, \sqrt{|D_k|}$ where c is a constant depending only on n, r and s (in fact, $c = 1$ works).

Proof ($c = (\frac{2}{\pi})^s$)

$\sigma_1, \dots, \sigma_r : k \hookrightarrow \mathbb{R}$, $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+1}, \dots, \overline{\sigma}_{r+s} : k \hookrightarrow \mathbb{C}$

Lemma 2.15 $\Rightarrow$ $\mathfrak{a}$ has a $\mathbb{Z}$-basis $\gamma_1, \dots, \gamma_n$ with

$\Delta(\gamma_1, \dots, \gamma_n) = (N\mathfrak{a})^2 D_k$

$\Rightarrow |\det(\sigma_i(\gamma_j))| = N\mathfrak{a}\, \sqrt{|D_k|}$

The image of $\mathfrak{a} \to (\mathbb{R}^r \times \mathbb{C}^s) \cong \mathbb{R}^{r+2s} = \mathbb{R}^n$, $\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r+s}(\alpha))$

$\alpha \mapsto (x_1, \dots, x_r, y_1, \dots, y_s) \mapsto (x_1, \dots, x_r, \mathrm{Re}(y_1), \mathrm{Im}(y_1), \dots, \mathrm{Re}(y_s), \mathrm{Im}(y_s))$

(r coordinates, $2s$ coordinates)

is a lattice Λ in $\mathbb{R}^n$.

This lattice has determinant $d(\Lambda) = 2^{-s} N\mathfrak{a}\, \sqrt{|D_k|}$

N.B. $\begin{pmatrix} z \\ \bar{z} \end{pmatrix} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} \mathrm{Re}(z) \\ \mathrm{Im}(z) \end{pmatrix}$, explains the factor of 2. ($|\det| = 2$)

Pick $\lambda_1, \dots, \lambda_{r+s} \in \mathbb{R}_{>0}$ such that $\left(\prod_{i=1}^{r} \lambda_i\right)\left(\prod_{i=r+1}^{r+s} \lambda_i^2\right) = \left(\frac{4}{\pi}\right)^s d(\Lambda)$

Let S be the image of $\{(x_1, \dots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \mid |x_i| \leq \lambda_i\ \forall\, 1 \leq i \leq r+s\}$ under $\mathbb{R}^r \times \mathbb{C}^s \xrightarrow{\sim} \mathbb{R}^n$. Then $\mathrm{vol}(S) = \left(\prod_{i=1}^{r} 2\lambda_i\right)\left(\prod_{i=r+1}^{r+s} \pi \lambda_i^2\right)$

$= 2^r \pi^s \prod_{i=1}^{r+s} \lambda_i \prod_{i=r+1}^{r+s} \lambda_i^2 = 2^r \pi^s \left(\frac{4}{\pi}\right)^s d(\Lambda) = 2^r d(\Lambda)$

Minkowski $\Rightarrow \exists\, 0 \neq \alpha \in \mathfrak{a}$ such that $|\sigma_i(\alpha)| \leq \lambda_i$, $1 \leq i \leq r+s$

But $N_{k/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \Rightarrow |N_{k/\mathbb{Q}}(\alpha)| \leq \left(\prod_{i=1}^{r} \lambda_i\right)\left(\prod_{r+1}^{r+s} \lambda_i^2\right)$

$|N_{k/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s d(\Lambda) = \left(\frac{2}{\pi}\right)^s N\mathfrak{a}\, \sqrt{|D_k|}$ $\square$

Recall $Cl_K = P_K / I_K$

I_K = fractional ideals, P_K = principal fractional ideals (Both abelian groups so the quotient is allowed).

Theorem 3.5

Every ideal class contains an ideal $\underline{b} \subset \mathcal{O}_K$ with $N\underline{b} \leq c\sqrt{|D_K|}$ (where c is as in Theorem 3.4).

In particular, Cl_K is finite.

Proof

Let $\underline{a}$ be an integral ideal representing the inverse of the given ideal class. Theorem 3.4 $\Rightarrow \exists\, 0 \neq \alpha \in \underline{a}$ such that $|N_{K/\mathbb{Q}}(\alpha)| \leq c N\underline{a} \sqrt{|D_K|}$. Then $(\alpha) \subset \underline{a} \Rightarrow \underline{a} \mid (\alpha)$

$\Rightarrow (\alpha) = \underline{a} \cdot \underline{b}$ for some ideal $\underline{b} \subset \mathcal{O}_K$.

$\Rightarrow N\underline{a}\, N\underline{b} = |N_{K/\mathbb{Q}}(\alpha)| \leq c N\underline{a} \sqrt{|D_K|}$

$\Rightarrow N\underline{b} \leq c\sqrt{|D_K|}$ □

(For the final statement, note that there are only finitely many integral ideals of given norm. Since for example if $N\underline{b} = m$ $\Rightarrow m \in \underline{b}$, $\underline{b} \mid (m)$.)

Remark

Theorems 3.4, 3.5 in fact hold with $c = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$, called the "Minkowski Constant". The proof of theorem 3.4 is refined using the AM-GM inequality.

Definition

The class number h_K is the order of Cl_K. So proposition 2.13 says that $h_K = 1 \Leftrightarrow \mathcal{O}_K$ is a UFD.

Example

$D_K = -20$

$K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Every ideal class contains an ideal $\underline{b}$ with $N\underline{b} \leq \frac{2}{\pi}\sqrt{20} = \frac{4\sqrt{5}}{\pi} < 3$

$\Rightarrow N\underline{b} = 1$ or 2. $N\underline{b} = 1 \Rightarrow \underline{b} = (1)$

If $N\underline{b} = 2$, $\underline{b} \mid (2)$. But $(2) = \underline{p}^2$, $\underline{p} = (2, 1+\sqrt{-5})$
$\Rightarrow \underline{b} = \underline{p}$. $\underline{p}$ is not principal since $x^2 + 5y^2 = \pm 2$ has no solutions for $x, y \in \mathbb{Z}$.
$\therefore Cl_K \cong \mathbb{Z}/2\mathbb{Z}$, $h_K = 2$.

Remark
$x, y \in \mathbb{Z}$
$N(x + y\sqrt{-5}) = x^2 + 5y^2$. $N(2x + (1+\sqrt{-5})y) = (2x+y)^2 + 5y^2$
$(2x+y)^2 + 5y^2 = 2(2x^2 + 2xy + 3y^2)$, $2 = N\underline{p}$
In Number Theory, the class number $h(d)$ for $d < 0$ was defined as the number of $SL_2(\mathbb{Z})$ equivalence classes of integer binary quadratic forms with discriminant d. For $d = -20$ the class number is two with representatives $x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$. This is not a coincidence.

Example
i) p prime, $p \neq 2, 5$, $\left(\frac{-5}{p}\right) = 1$.
Dedekind's Criterion $\Rightarrow p$ splits in $k = \mathbb{Q}(\sqrt{-5})$
i.e. $(p) = \underline{p_1}\,\underline{p_2}$, $N\underline{p_1} = N\underline{p_2} = p$.
Either $\underline{p_1}$ is principal, or $\underline{p}\,\underline{p_1}$ is principal.
$p = x^2 + 5y^2, x, y \in \mathbb{Z}$ or $\underline{p}\,\underline{p_1} = (2x + (1+\sqrt{-5})y)$, $x, y \in \mathbb{Z}$
$p = 2x^2 + 2xy + 3y^2$

ii) We compute the class group of $\mathbb{Q}(\sqrt{-17}) = k$. $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$.
$D_K = -4 \cdot 17$. Minkowski $\Rightarrow$ every ideal class contains $\underline{b}$ with
$N\underline{b} \leq \frac{2}{\pi}\sqrt{4 \cdot 17} < \frac{4\sqrt{17}}{\pi} < \frac{4 \cdot 5}{3} < 7$
$\therefore Cl_K$ is generated by prime ideals dividing 2, 3, 5.
Let $f(x) = x^2 + 17$.
$f(x) = (x+1)^2 \pmod 2 \Rightarrow (2) = \underline{p}^2$, $\underline{p} = (2, 1+\sqrt{-17})$
$f(x) = (x+1)(x-1) \pmod 3 \Rightarrow (3) = \underline{q_1}\,\underline{q_2}$
$\underline{q_1} = (3, 1+\sqrt{-17})$, $\underline{q_2} = (3, 1-\sqrt{-17})$
$f(x) = x^2 + 2 \pmod 5$, irreducible
$\Rightarrow (5)$ is prime, 5 is inert.

$N_{K/\mathbb{Q}}(1+\sqrt{-17}) = 18 \Rightarrow (1+\sqrt{-17}) = \underline{p}\,\underline{q_1}^2$, $\underline{p}\,\underline{q_1}\,\underline{q_2}$
or $\underline{p}\,\underline{q_2}^2$

$(1+\sqrt{-17}) \neq \underline{P}\,\underline{q_1}\,\underline{q_2}$ since $(3) \nmid (1+\sqrt{-17})$

N.B. $1+\sqrt{-17} \in \underline{q_1}$, but not $\underline{q_2}$.

$\Rightarrow \underline{q_1} \mid (1+\sqrt{-17})$, $\underline{q_2} \nmid (1+\sqrt{-17})$

$(1+\sqrt{-17}) = \underline{P}\,\underline{q_1}^2$.

$\underline{P}^2 \sim 1$ $\quad$ $\underline{q_1}\,\underline{q_2} \sim 1$ $\quad$ $\underline{P}\,\underline{q_1}^2 \sim 1$

$\Rightarrow Cl_K$ is generated by $\underline{q_1}$. Moreover, $\underline{P} \sim \underline{q_1}^2$, and $\underline{q_1}^4 \sim 1$.

$x^2 + 17y^2 = \pm 2$ has no solutions for $x, y \in \mathbb{Z}$, so $\underline{P}$ is not principal. $\Rightarrow \underline{q_1}^2$ is not principal.

$\therefore$ $[\underline{q_1}]$ has order 4 in Cl_K.

$\therefore Cl_K \cong \mathbb{Z}/4\mathbb{Z}$, $h_K = 4$.

Remark

If $a_n := \left(\frac{4}{\pi}\right)^{n/2} \frac{n!}{n^n}$ then $\left(\frac{a_n}{a_{n+1}}\right)^2 = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} > 1$

$\Rightarrow a_n$ is a decreasing sequence

$\Rightarrow c < 1$ for all $n \geq 2$.

$\Rightarrow |D_K| > 1$ for all $K \neq \mathbb{Q}$ by Theorem 3.5.

Example

1) Find all integer solutions to $x^2 - 7y^2 = 9$.

Let $k = \mathbb{Q}(\sqrt{7})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{7}]$

Recall that $\mathcal{O}_k^* = \{\pm(8+3\sqrt{7})^m : m \in \mathbb{Z}\}$

We seek all $\alpha \in \mathcal{O}_k$ with $N_{k/\mathbb{Q}}(\alpha) = 9$.

Dedekind's Criterion $\Rightarrow$ $(3) = (3, 1+\sqrt{7})(3, 1-\sqrt{7})$ $\quad P_1 \quad P_2$

The ideals of norm 9 are P_1^2, $P_1 P_2 = (3)$, P_2^2.

$P_1 = (2-\sqrt{7})$, $N_{k/\mathbb{Q}}(2-\sqrt{7}) = -3$

$P_2 = (2+\sqrt{7})$

Solution: $x + y\sqrt{7} = \begin{cases} \pm(2\pm\sqrt{7})^2(8+3\sqrt{7})^m \\ \pm 3(8+3\sqrt{7})^m \end{cases}$ $\quad m \in \mathbb{Z}$

ii) Find all integer solutions to $y^2 + 5 = x^3$.

Recall that $k = \mathbb{Q}(\sqrt{-5})$ has class number $h_k = 2$.

$\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$. $\quad (y+\sqrt{-5})(y-\sqrt{-5}) = x^3 \quad (*)$

Suppose $P \subset \mathcal{O}_k$ is a prime ideal, $P \mid y+\sqrt{-5}$, $P \mid y-\sqrt{-5}$

$\Rightarrow (P \mid 2y)$ and $P \mid 2\sqrt{-5} \Rightarrow P \mid 2$ or $P \mid 5$

i) $P \mid 2 \Rightarrow (P \mid x^3 \Rightarrow x$ even$)$

$\Rightarrow y^2 \equiv -1 \ (4)$ $\quad \not\Rightarrow$

ii) If $P \mid 5$ then $P \mid x^3 \Rightarrow 5 \mid x$

$\Rightarrow y^2 \equiv -5 \ (25)$ $\quad \not\Rightarrow$

By $(*)$ and unique factorisation into prime ideals

$(y+\sqrt{-5}) = \mathfrak{q}^3$, for some ideal $\mathfrak{q} \subset \mathcal{O}_k$

Remark

As an alternative to i), ii), we could note that 2, 5 ramify in k. (see lecture 1)

Since $3 \nmid h_K$, $\mathfrak{a}^3$ principal $\Rightarrow \mathfrak{a}$ principal

$y + \sqrt{-5} = \pm (a + b\sqrt{-5})^3$, $a, b \in \mathbb{Z}$
(switch signs of a, b)

$y + \sqrt{-5} = a^3 + 3a^2 b\sqrt{-5} - 15ab^2 - 5\sqrt{-5}b^3$

$\Rightarrow y = a(a^2 - 15b^2)$, $1 = b(3a^2 - 5b^2)$

$\Rightarrow b = \pm 1$, $3a^2 = 5 \pm 1$ ⨉

So there are no integer solutions to $y^2 + 5 = x^3$

Hermite's Theorem

There are only finitely many number fields $k/\mathbb{Q}$ of degree n and given discriminant D.

Proof (for k totally complex, other cases are similar)

$n = 2s$, $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s : k \hookrightarrow \mathbb{C}$

$\mathcal{O}_k \to \mathbb{C}^s \xrightarrow{\sim} \mathbb{R}^n$, $x \mapsto (\sigma_1(x), \ldots, \sigma_s(x))$
$(x_1, \ldots, x_n) \mapsto (\mathrm{Re}(x_1), \mathrm{Im}(x_1), \ldots, \mathrm{Re}(x_n), \mathrm{Im}(x_n))$

The image is a lattice Λ with $d(\Lambda) = 2^{-s}\sqrt{|D|}$

Let $S \subset \mathbb{R}^n$ be the image of

$\{(x_1, \ldots, x_s) \in \mathbb{C}^s \mid |\mathrm{Im}(x_1)| < c, |\mathrm{Re}(x_1)| < 1, |x_j| < 1 \ \forall 2 \le j \le s\}$

under $\mathbb{C}^s \xrightarrow{\sim} \mathbb{R}^n$. We pick c (only depending on n, D) such that $\mathrm{vol}(S) > 2^n d(\Lambda)$

Minkowski $\Rightarrow \exists\, 0 \neq \alpha \in \mathcal{O}_k$ such that

$|\mathrm{Im}(\sigma_1(\alpha))| < c$, $|\mathrm{Re}(\sigma_1(\alpha))| < 1$, $|\sigma_j(\alpha)| < 1 \ \forall 2 \le j \le s$.

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

Proof of Claim

$\prod_{i=1}^{s} |\sigma_i(\alpha)|^2 = |N_{k/\mathbb{Q}}(\alpha)| \geq 1$ ← non-zero rational integer

$\Rightarrow |\sigma_1(\alpha)| > 1 \Rightarrow \mathrm{Im}\, \sigma_1(\alpha) \neq 0$

$\Rightarrow \sigma_1(a) \neq \bar{\sigma}_1(\alpha)$

$\therefore \sigma_1(\alpha) \neq \sigma(\alpha)$ $\forall$ embeddings $\sigma : k \hookrightarrow \mathbb{C}$, $\sigma \neq \sigma_1$.

Lemma 1.7 $\Rightarrow \sigma_1(\alpha), \bar{\sigma}_1(\alpha), \ldots, \sigma_s(\alpha), \bar{\sigma}_s(\alpha)$ are distinct.

$\Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq n = [k : \mathbb{Q}] \Rightarrow k = \mathbb{Q}(\alpha)$.

The conjugates of α are bounded by constants depending only on n, D $\Rightarrow$ coefficients of the min. poly. of α are bounded (and in $\mathbb{Z}$), $\Rightarrow$ only finitely many possibilities for the min. poly., and therefore for α, and finally for k. $\square$

4 Cyclotomic Fields

Let ζ_n be a primitive n^{th} root of unity (e.g. $\zeta_n = e^{2\pi i/n}$)

Proposition 4.1

Let $k = \mathbb{Q}(\zeta_n)$, where $n = p^r$, a prime power.

Then i) $[k : \mathbb{Q}] = \varphi(n) = p^{r-1}(p-1)$

ii) p is totally ramified in $k/\mathbb{Q}$ i.e. $(p) = \mathfrak{p}^{[k:\mathbb{Q}]}$

Proof

Let $f(x) = \dfrac{x^n - 1}{x^{n/p} - 1} = \prod_{i=0,\, p \nmid i}^{n-1} (x - \zeta_n^i)$

Then $[k : \mathbb{Q}] \leq \deg(f) = \varphi(n)$

On the other hand, $p = f(1) = \prod_{i=0,\, p \nmid i}^{n-1} (1 - \zeta_n^i)$

For i, j coprime to n, $\dfrac{1-\zeta_n^i}{1-\zeta_n^j} \in \mathcal{O}_k^*$ (see sheet 2)

$\Rightarrow (p) = (1 - \zeta_n)^{\varphi(n)}$

Norms $\Rightarrow p^{[k:\mathbb{Q}]} = |N_{k/\mathbb{Q}}(1 - \zeta_n)|^{\varphi(n)}$

$\Rightarrow \varphi(n) \leq [k : \mathbb{Q}]$. Statements i), ii) follow immediately. $\square$

Remark 4.2

If $p \nmid n$, then $\gcd(X^n - 1, nX^{n-1}) = 1$ in $\mathbb{F}_p[X]$.

$\therefore X^n - 1$ has no repeated roots in any field of characteristic p.

Lemma 4.3

Let k be a number field. Suppose that $\mu_n \subset k$. Let $\mathfrak{P} \subset \mathcal{O}_k$ be a prime ideal. If $\mathfrak{P} \nmid n$ then $N\mathfrak{P} \equiv 1 \pmod{n}$

Proof

Let $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$

$p \nmid n \underset{\text{Remark 4.2}}{\Rightarrow} X^n - 1$ has no repeated roots in $\mathcal{O}_k/\mathfrak{P}$

$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) \quad \Rightarrow \mu_n \hookrightarrow (\mathcal{O}_k/\mathfrak{P})^*$

$\Rightarrow N\mathfrak{P} \equiv 1 \pmod{n}$ □

Theorem 4.4

Let $k = \mathbb{Q}(\zeta_n)$. Suppose that $n \not\equiv 2 \pmod{4}$

p ramifies in $k \iff p \mid n$.

Proof

"$\Leftarrow$" If $p \mid n$, then $\mathbb{Q}(\zeta_p) \subset k$. Proposition 4.1 $\Rightarrow p$ ramifies in $\mathbb{Q}(\zeta_p)$

$\Rightarrow p$ ramifies in k.

If $p = 2$ then consider $\mathbb{Q}(i) \subset k$.

"$\Rightarrow$" We show that if $p \nmid n$, then p is unramified in k.

Let $g \in \mathbb{Z}[X]$ be the min. poly. of ζ_n over $\mathbb{Q}$.

$g(X) = \prod_{i \in I} (X - \zeta_n^i)$ for some $I \subset \{0, 1, \ldots, n-1\}$

If $\mathfrak{P} \mid p$, then $\bar{g}(x) \in \mathbb{F}_p[X]$ splits completely into linear factors over $\mathcal{O}_k/\mathfrak{P}$ and has no repeated roots by Remark 4.2.

$\Rightarrow \operatorname{disc}(\bar{g}) \neq 0 \quad \Rightarrow p \nmid \operatorname{disc}(g) = (\mathcal{O}_K : \mathbb{Z}[\zeta_n])^2 D_K$

$\Rightarrow p \nmid (\mathcal{O}_K : \mathbb{Z}[\zeta_n])$

Dedekind's Criterion now gives the factorisation of $p\mathcal{O}_K$ in terms of the factorisation $\bar{g}$ into ireducibles in $\mathbb{F}_p[X]$.

Remark 4.2 $\Rightarrow \bar{g}$ is a product of distinct ireducibles in $\mathbb{F}_p[X]$.

$\Rightarrow p$ is unramified in $k/\mathbb{Q}$ $\square$.

From now on, $k = \mathbb{Q}(\zeta_p)$, p an odd prime.

Lemma 4.5

The roots of unity in k are $\{\pm\zeta_p^j \mid 0 \leq j < p\}$

Proof

i) If $\zeta_q \in k$, q an odd prime, $q \neq p$

$\Rightarrow \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{pq})$ $\not\in$ to Theorem 4.4

ii) If $i \in k$ then $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{4p})$ $\not\in$ to Theorem 4.4

iii) If $\zeta_{p^2} \in k$, then $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{p^2})$ $\not\in$ to Proposition 4.1 $\square$

Remark

Lemma 4.5 also follows from $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, c.f Galois Theory

Lemma 4.6

$q \neq p$, q prime. Then $q\mathcal{O}_K$ factors as a product of $r = \frac{p-1}{f}$ distinct prime ideals, each of norm q^f, where f is the order of q in $(\mathbb{Z}/p\mathbb{Z})^*$.

Proof

Sheet 2 $\Rightarrow \mathcal{O}_K = \mathbb{Z}[\zeta_p]$. By Dedekind's Criterion, it suffices to show that every ireducible factor $h \in \mathbb{F}_q[X]$ of

$\frac{X^p-1}{X-1} \in \mathbb{F}_q[X]$ has $\deg(h) = f$.

i) $\underline{\underline{q}} = (q, h(\zeta_n))$ has $N\underline{\underline{q}} = q^{\deg(h)}$

Lemma 4.3 $\Rightarrow q^{\deg(h)} \equiv 1 \pmod{p} \Rightarrow \deg(h) \geq f$

ii) We quote (c.f. Galois Theory) that for every prime power, $\exists$ a finite field of that order. Let k be a field with q^f elements

i.e. $[k : \mathbb{F}_q] = f$. $q^f \equiv 1 \pmod{p} \Rightarrow p \mid q^f - 1, p \mid |k^*|$

$\Rightarrow k$ contains a primitive p^{th} root of unity.

$\Rightarrow \frac{X^p-1}{X-1}$ splits completely into linear factors over k.

$\Rightarrow h(X)$ has a root in k.

$\Rightarrow \deg(h) \leq [k : \mathbb{F}_q] = f$. $(\Rightarrow \deg h = f)$ $\square$

Lemma 4.7

Let K be a number field, $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$. If $0 \neq x \in \mathcal{O}_K$ satisfies $|\sigma_i(x)| \leq 1 \ \forall i$, then x is a root of unity.

Proof

Let $g(X) \in \mathbb{Z}[X]$ be the min. poly. of x. $|\sigma_i(x)| \leq 1 \ \forall i$

$\Rightarrow$ coefficients of g are bounded

$\Rightarrow$ only finitely many choices for $g \Rightarrow$ only finitely many for x.

But $1, x, x^2, \ldots$ satisfy the same bounds

$\therefore x^r = x^s$ for some $r \neq s \Rightarrow$ either $x = 0$, or x is a root of unity $\square$

Lemma 4.8

Every $\varepsilon \in \mathcal{O}_K^*$ can be written as $\varepsilon = \zeta_p^j u$ for some $0 \leq j < p$ and $u \in \mathbb{R}$.

Proofs

Write $\varepsilon = f(\zeta_p)$, $f \in \mathbb{Z}[x]$. Then ε has conjugates $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{p-1}$ ($\varepsilon = \varepsilon$, $\bar{\varepsilon} = \varepsilon_{p-1}$)

where $\varepsilon_i = f(\zeta_p^i)$.

$\varepsilon/\bar{\varepsilon}$ has conjugates $\varepsilon_i/\varepsilon_{p-i} = \varepsilon_i/\bar{\varepsilon_i}$ (has absolute value 1.)

Lemma 4.7 $\Rightarrow$ $\varepsilon/\bar{\varepsilon}$ is a root of unity.

Lemma 4.8

For $k = \mathbb{Q}(\zeta_p)$, p an odd prime, every $\varepsilon \in \mathcal{O}_k^*$ can be written in the form $\zeta_p^i u$ where $0 \le i < p$ and $u \in \mathbb{R}$

Proof (continued)

We proved that $\varepsilon/\bar{\varepsilon}$ is a root of unity. Lemma 4.5 $\Rightarrow \frac{\varepsilon}{\bar{\varepsilon}} = \pm\zeta_p^i$ for some $0 \le i < p$. Since p is odd, $\exists j \in \mathbb{Z}$ such that $2j \equiv i \ (p)$

$\therefore \zeta_p^{-j}\varepsilon = \pm\zeta_p^{j}\bar{\varepsilon}$ (*)

Let $\pi = 1 - \zeta_p$. $\mathcal{O}_k/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$

$\therefore \varepsilon \equiv a \pmod{\pi}$ for some $a \in \mathbb{Z}$.

$\Rightarrow \bar{\varepsilon} \equiv a \pmod{\pi}$ (since $(\pi) = (\bar{\pi})$)

Now (*) $\Rightarrow a \equiv \pm a \pmod{\pi} \Rightarrow a \equiv \pm a \pmod{p}$ since $a \in \mathbb{Z}$

But ε is a unit, so $a \not\equiv 0 \ (p)$. Since p is odd, we must have '+' in

(*) $\Rightarrow \zeta_p^{-j}\varepsilon \in \mathbb{R}$ □

5 Fermat's Last Theorem

The equation $x^n + y^n = z^n$, $(n \ge 3)$ has no solutions in non-zero integers x, y, z.

The case $n = 4$ was proved by Fermat himself, so it suffices to take $n = p$, an odd-prime. We may assume that x, y, z are pairwise coprime. There are two cases:

i) $p \nmid xyz$

ii) $p \mid xyz$ (i.e. p divides exactly one of them)

Kummer proved Fermat's Last Theorem for p a regular prime. i.e. $p \nmid$ the class number of $\mathbb{Q}(\zeta_p)$. This includes all primes < 100

except for 37, 59, 67.

The proofs of Fermat's Last Theorem for all primes p (Wiles, Taylor-Wiles, 1993) is far beyond the scope of this course.

Theorem 5.1

Let p be an odd, regular prime. If x, y, z are integers coprime to p satisfying $x^p + y^p = z^p$ (†) then $x \equiv y \ (p)$

Remark

Rewriting (†) in the more symmetric form $x^p + y^p + (-z)^p = 0$, the theorem shows that $x \equiv y \equiv -z \ (p) \Rightarrow 3x^p \equiv 0 \ (p)$

$\Rightarrow p = 3$. But Fermat's Last Theorem, case i), $p = 3$ is resolved by working mod 9. Indeed, $x^3 + y^3 + (-z)^3 \equiv \pm 1 \pm 1 \pm 1 \ (9)$.

Proofs of 5.1

WLOG, x, y, z are pairwise coprime. $k = \mathbb{Q}(\zeta_p)$, $\zeta_p = \zeta$

$\mathcal{O}_k = \mathbb{Z}[\zeta]$.

$(\dagger) \Rightarrow (x+y)(x+\zeta y) \dots (x+\zeta^{p-1} y) = z^p$

Suppose $\mathfrak{q} \subset \mathcal{O}_k$ is a prime ideal with $\mathfrak{q} \mid (x+\zeta^j y)$ and $\mathfrak{q} \mid (x+\zeta^k y)$, $j \neq k$.

$\Rightarrow \mathfrak{q} \mid (\zeta^j - \zeta^k) y$

$\Rightarrow \mathfrak{q} \mid p$ or $\mathfrak{q} \mid y$.

$\Rightarrow p \mid z$ ✱ $\qquad \Rightarrow \mathfrak{q} \mid x$ ✱ to x, y coprime.

By unique factorisation into prime ideals, (also applies to other terms in (†))

$(x+\zeta y) = \mathfrak{a}^p$ for some $\mathfrak{a} \in \mathcal{O}_k$.

$p \nmid h_k$, so $\mathfrak{a}^p$ principal $\Rightarrow \mathfrak{a}$ principal.

Write $x + \zeta y = \varepsilon \alpha^p$, $\varepsilon \in \mathcal{O}_K^*$, $\alpha \in \mathcal{O}_K$.

Lemma 4.8 $\Rightarrow \varepsilon = \zeta^i u$, $0 \le i < p$, $u \in \mathcal{O}_K^*$, u real.

$\therefore x + \zeta y = \zeta^i u \alpha^p$

Let $\pi = 1 - \zeta$ $\quad \mathcal{O}_K/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$ $\quad \therefore \alpha = a \ (\pi)$, $a \in \mathbb{Z}$

$\Rightarrow \alpha^p - a^p = \prod_{i=0}^{p-1} (\alpha - \zeta^i a) \equiv 0 \pmod{\pi^p}$

But $(p) = (\pi)^{p-1}$ $\quad \therefore \alpha^p \equiv a^p \pmod p$ (i.e. $\bmod p\mathcal{O}_K$)

$\therefore \zeta^{-i}(x + \zeta y) \equiv \underbrace{u a^p}_{\text{real}} \pmod p$ ↖ take complex conjugates, equation still holds

$\Rightarrow \zeta^{-i}(x + \zeta y) \equiv \zeta^i (x + \zeta^{-1} y) \pmod p$

$\Rightarrow \zeta^i x + \zeta^{1-i} y \equiv \zeta^i x + \zeta^{i-1} y \pmod p$

If $\pm i$, $\pm(i-1)$ are distinct mod p, this contradicts that $\mathcal{O}_K = \mathbb{Z}[\zeta]$ – If $i \equiv 0 \pmod p$ $\Rightarrow (\zeta - \zeta^{-1}) y \equiv 0 \pmod p$

$\Rightarrow \pi \mid y \Rightarrow p \mid y$ ⁂

– If $i \equiv 1 \pmod p$ $\Rightarrow (\zeta - \zeta^{-1}) x \equiv 0 \pmod p$

$\Rightarrow \pi \mid x \Rightarrow p \mid x$ ⁂

– If $2i \equiv 1 \ (p)$

$\Rightarrow (\zeta^i - \zeta^{-i})(x - y) \equiv 0 \pmod p$

$\Rightarrow \pi \mid x - y \Rightarrow p \mid (x - y)$, i.e. $x \equiv y \ (p)$ $\quad \square$

Lemma 5.2 (needed for case ii))

$K = \mathbb{Q}(\zeta_p)$, p an odd, regular prime. $\alpha \in \mathcal{O}_K^*$, $\pi = 1 - \zeta_p$.

α is a p^{th} power $\Leftrightarrow$ α is a p^{th} power mod π^p.

Proof (Omitted)

Example

$p = 3$. $k = \mathbb{Q}(\sqrt{-3})$. $\mathcal{O}_k^* = \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\}$

$N \nearrow \quad \left(\mathcal{O}_k / 3\mathcal{O}_k\right)^*$

Books

Borevich and Shafarevich, Number Theory, Academic Press 1966

Swinnerton-Dyer, A Brief Guide to Algebraic Number Theory, CUP 2001

$k = \mathbb{Q}(\zeta)$, $\mathcal{O}_k = \mathbb{Z}[\zeta]$, $\zeta = \zeta_p$,

$(p) = (\pi)^{p-1}$, $\pi = 1 - \zeta$

Theorem 5.1

Let p be an odd regular prime and let $\alpha, \beta, \gamma \in \mathcal{O}_k^*$. Then there are no solutions to $\alpha x^p + \beta y^p = \gamma z^p$, with $x, y, z \in \mathcal{O}$, and $\pi \nmid x$, $\pi \nmid y$, $\pi \mid z$.

Proof

$\pi \nmid x \Rightarrow (x) + (\pi^p) = \mathcal{O}_k \Rightarrow x$ has an inverse mod π^p

$\Rightarrow \alpha/\beta$ is a p^{th} power mod π^p.

Lemma 5.2 $\Rightarrow$ WLOG, $\alpha = \beta = 1$.

Factoring the left hand side, $\prod_{j=0}^{p-1} (x + \zeta^j y) = \gamma z^p$

We have $x + \zeta^j y \equiv x + \zeta^k y \pmod{\pi}$ $\forall j, k$

$\pi \mid z \Rightarrow \pi \mid (x + \zeta^j y)$ $\forall j$.

For $j \neq k$, $(\zeta^i - \zeta^k) = (\pi)$

$\Rightarrow$ the $\frac{x + \zeta^j y}{\pi}$ are distinct mod π.

But there are p residue classes of $\mathcal{O}_k/\pi$. So exactly one of these is $\equiv 0 \pmod{\pi}$.

i.e. $\pi^2 \mid (x + \zeta^j y)$ for exactly one j. WLOG, $j = 0$.

For $j \neq k$, $(x + \zeta^j y, x + \zeta^k y) \subset (x, y) = \mathfrak{a}$

$\pi \mid (x + \zeta^j y, x + \zeta^k y)$, $\pi \nmid \mathfrak{a}$ (since $\pi \nmid x$, $\pi \nmid y$)

$\pi \mid \mathfrak{a} \subseteq (\pi x, \pi y)$

$\therefore$ the gcd of $(x+\zeta^j y)$ and $(x+\zeta^k y)$ is $\pi \mathfrak{a}$

Unique factorisation into prime ideals

$\Rightarrow (x+\zeta^j y) = \pi \mathfrak{a} \mathfrak{b}_j^p \quad \forall j \in \{0,1,\dots,p-1\}$ for some $\mathfrak{b}_j \in C$

Let $\mathfrak{a} \in C\mathcal{O}_K$ be an ideal with $\mathfrak{a}\mathfrak{b}_0 \in$ principal.

Since (π) is principal, WLOG $\pi \nmid \mathfrak{a}$.

$\mathfrak{a}\mathfrak{b}_0^p \sim 1$, $\mathfrak{a}\mathfrak{b}_0 \mathfrak{a} \sim 1$, $\mathfrak{a}^p \mathfrak{b}_0^p \mathfrak{a}^p \sim 1$

$\Rightarrow \mathfrak{a}^{p-1}\mathfrak{a}^p = (\beta)$, for some $\beta \in \mathcal{O}_K$.

$\Rightarrow \beta(x+\zeta^j y) = \pi(\mathfrak{a}\mathfrak{b}_j\mathfrak{a})^p$

Since $p \nmid h_K$, $\beta(x+\zeta^j y) = \varepsilon_j \pi \alpha_j^p \quad \forall 0 \le j \le p-1$

for some $\varepsilon_j \in \mathcal{O}_K^*$, $\alpha_j \in \mathcal{O}_K$.

$$(x+\zeta y)+\zeta(x+\zeta^{-1}y) = (1+\zeta)(x+y)$$

Eliminating x and y from the equations with $j = 0, 1, p-1$ gives

$$\underbrace{\varepsilon_1}_{\text{unit}} \alpha_1^p + \underbrace{\zeta \varepsilon_{p-1}}_{\text{unit}} \alpha_{p-1}^p = \underbrace{(1+\zeta)}_{\text{unit}} \varepsilon_0 \alpha_0^p$$

Claims

i) $\pi \nmid \alpha_1$, $\pi \nmid \alpha_{p-1}$, $\pi \mid \alpha_0$

ii) The power of π dividing (α_0) is strictly less than the power of π dividing (z).

Proofs of Claims

Let $v_\pi(x)$ = power of π dividing (x).

If $n = v_\pi(z) \ge 1$, then $v_\pi(x+\zeta^j y) = \begin{cases} np-(p-1) & \text{if } j=0 \\ 1 & \text{if } j \neq 0 \end{cases}$

$\Rightarrow v_\pi(\alpha_j) = \begin{cases} n-1 & \text{if } j=0 \\ 0 & \text{if } j \neq 0 \end{cases}$ (subtract 1, divide by p).

Note that $\pi^2 \mid (x+y) \Rightarrow n \ge 2$.

By starting with a solution with $v_\pi(z) \geq 1$, and minimal, we obtain a contradiction. □

Definition

The zeta function of a number field k is

$$\zeta_k(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_k} \frac{1}{(N\mathfrak{a})^s} = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_k \\ \text{prime}}} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}$$

This converges for to an analytic function for $\{\mathrm{Re}(s) > 1\}$.

Analytic Class Number Formula:

$$\lim_{s \downarrow 1} (s-1)\zeta_k(s) = \frac{2^r (2\pi)^{s'} h R}{\#\mu(k) \sqrt{|D_k|}}$$

where h = class number of k.

$\mu(k)$ = roots of unity in k.

R = covolume of lattice in the proof of Proposition 3.3

Regulator

Using this formula (and much more), Kummer showed that

p is regular $\Leftrightarrow$ the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ are not divisible by p.

B_n is defined by $\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$