Algebraic Number Theory

0. Plan

1. Algebraic integers
2. Dedekind domain
3. Finiteness Thms
4. Valuation Theory

1. Introduction

Examples.

Solve eq. $x^2 + y^2 = z^2$. One can easily deduced that $\begin{cases} x = 2ab \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}$ (with some additional conditions)

Solve $y^2 = x^3 - 2, x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$.

Consider $\mathbb{Z}[\sqrt{-2}]$. This ring is a UFD; its units are ± 1; $\sqrt{-2}$ is irreducible; $gcd(y + \sqrt{-2}, y - \sqrt{-2}) = 1$.

($\begin{aligned} z|y \pm \sqrt{-2} \implies z|2\sqrt{2} \implies \sqrt{-2}|z \implies \sqrt{-2}|y \implies 2|y \\ \implies y^2 = x^3 - 2 \equiv 2 \mod 8 \end{aligned}$ .Contradiction)

Thus $\begin{aligned} x^3 = (y + \sqrt{-2})(y - \sqrt{-2}) \implies y + \sqrt{-2} = \\ (a + b\sqrt{-2})^3 = a(a^2 - 6b^2) + b(3a^2 - 2b^2)\sqrt{-2} \implies b(3a^2 - 2b^2) = 1 \\ \implies (a, b) = (\pm 1, 1); (3, \pm 5) \end{aligned}$

This leads to the first "fake" proof of Fermat's Last Thm. (Error occurs that mathematicians assume that $\mathbb{Z}[\sqrt{-p}]$ is always an UFD which is obviously not true.)

Thus the main aspects we concern is:

1. $\mathbb{Z}[\zeta_p]$ UFD?
2. What is $\mathbb{Z}[\zeta_p]^{\times}$
3. Iwasawa Theory.

General Statement:

Intregral ring of $\mathbb{Q}[\sqrt{-d}]$ in $\mathbb{Z}$ is $\mathcal{O}_k$.

Thm1. (Factorization of Ideals)

Given an ideal $I \subseteq \mathcal{O}_k$,one can decomposite $I = \prod p_i^{\alpha}$ in a uniquely (Primary decomposition)

Thm2. (Finiteness of class number)

$Cl_k = \{fractional\ ideals\}/\{principle\ ideals\}$, which is a F.G. Abelian Group.

This evaluate how far a dedekind domain is from the principal ideal domain.

Thm3. (Dirichlet's Unit Theorem.)

$\mathcal{O}_k^{\times} = W_k \times V_k$, where W_k is finite abelian group, generated by ζ_k, V_k is free abelian group $\mathbb{Z}^{r_1+r_2-1}$, where r_1, r_2 are numbers of real embedding and non-real embedding, resp.

Galois Theory.

L/K a finite extension. $Gal(L/K) = \{\phi : L \to L, iso|\phi|_K = id.\}$

$Gal(L/K) = \mathbb{Z}/2\mathbb{Z}$.

Thm4. Middle field of L/K M,it leads to subgroup of $Gal(L/K)$ $Gal(L/M)$. Conversly a subgroup H leads to L^H.

Thus we need to study $Gal(L/\mathbb{Q})$.

Issue. $Rep(Gal_{\mathbb{Q}})$ is far too complicated, we study $Gal_{\mathbb{Q}_p}$ instead.

(Here $Gal_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q}), Gal_{\mathbb{Q}_p} = Gal(\mathbb{Q}_p/\mathbb{Q})$)

Class Field Theory.

We find that $Gal(L/\mathbb{Q}_p) \cong \mathbb{Q}_p^\times/Nm(L^\times)$

Here $Nm : L \to K, x \in L, \phi_x : y \mapsto xy, take\ Nm(x) = \det$.

This is a local case.

For global cases $I_{\mathbb{Q}} = \prod_v \mathbb{Q}_v^\times$, here v are all valuations (absolute, $p-$adic)

$= \{(x_v)|x_v \in \mathbb{Q}_v^\times, x_v = \mathcal{O}_v^\times for\ all\ but\ finite\ many\ v\}$

Thm. $Gal(L/\mathbb{Q})^{ab} \cong I_{\mathbb{Q}}/Nm(I_L)$

Langlands Conjecture.

2. Algebraic integers

Given a ring extension $A \subseteq B$. Say $x \in B$ integral over A if exists monic polynomial with coefficient in A such that it is the root of this polynomial.

Say B integral over A if $\forall x \in B$ is integral over A.

Prop. $A \subseteq B$, TFAE:

1.x integral; 2.$A[x]$ f.g.$A-$module; 3. x contained in a f.g. $A-$module.

Cor. Integral closure of A in B form a subring of A containing A. ($x+y, xy \in A[x,y]$, while the latter module is f.g. $A-$module)

If the integral closure of a ring is itself, then we say the ring to be integrally closed.(整闭)

If a ring A is an integral domain, then it is integrally closed if it is integrally closed in its fraction field.

Def. $K/\mathbb{Q}$ finite extension, then $\mathcal{O}_k$ is the integral closure of $\mathbb{Z}$ in K.

Trace and Norm.

Given a finite extension of fields $L/K, \forall x \in L$. $\phi_x : L \to L, y \mapsto xy$

Define the trace of x is $tr(\phi_x)$, norm is det ϕ_x, where ϕ_x viewed as a $K-$linear transformation. Obv that trace and norm belongs to K.

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

E.g. In $\mathbb{Q}[2+\sqrt{3}]/\mathbb{Q}$, $Nm(2+\sqrt{-3}) = 7$. (Which has a direct relation with the complex cases.)

Prop. L/K finite extensions of fields of char 0. $n = [L:K]$, $\tau : K \to \Omega$ is a fixed embedding into its algebraic closure.

Then $\exists$ n distinct embedding $\sigma_1, \cdots, \sigma_n : L \to \Omega$, s.t. $\sigma_i|_K = \tau$; and all of the embeddings $\sigma_1, \cdots, \sigma_n$ are linear independent.

$$Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

$$Nm_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$$

Pf: Fact $Tr_{L/K}(x) = [L : K(x)]Tr_{K(x)/K}(x)$; $Nm_{L/K}(x) = Nm_{K(x)/K}(x)^{[L:K(x)]}$

Say $f(T) = T^n + \cdots \in K[T]$ is the minimal polynomial of x. Then $Tr_{K(x)/K}(x) = -a_1 = \sum\{roots\ of\ f\} = \sum \sigma_i(x)$, similarly we get similar results for the norms.

Prop. Consider $L \times L \to K : (x, y) \mapsto Tr_{L/K}(xy)$ which leads to a quad. form, it is non-degenerate.

Cor. $\alpha_1, \cdots, \alpha_n$ are $n = [L : K]$ elements of L. Then $(\alpha_1, \cdots, \alpha_n)$ is a $K-$basis of $L \iff \det\left(Tr_{L/K}(\alpha_i\alpha_j)\right) \neq 0$

$$K^n \longrightarrow L \longrightarrow K^n$$

Hint. Consider: $(x_i) \longrightarrow \sum x_i\alpha_i$

$$x \longrightarrow \left(Tr(x\alpha_i)\right)$$

Discriminents

Discriminents. Consider $K/\mathbb{Q}$, $n = [K : \mathbb{Q}]$, $\alpha_1, \cdots, \alpha_n \in K$, define the discriminant $\det\left(Tr(\alpha_i\alpha_j)\right)$.

Lem.(1) $\sigma_1, \cdots, \sigma_n$ are embeddings of K into $\bar{Q}$, then
$Disc(\alpha_1, \cdots, \alpha_n) = \det\left(\sigma_i(\alpha_j)\right)^2$

(2) $(beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)C$**, where** $C \in M_{n\times n}(K)$**, then** $Disc(\beta_1, \cdots, \beta_n) = Disc(\alpha_1, \cdots, \alpha_n)(\det C)^2$

E.g. $f(T) \in \mathbb{Q}[T]$ the minimal polynomial of $\alpha \in K$, then

$$Disc(1, \alpha, \cdots, \alpha^{n-1}) = \begin{cases} 0 & \deg f < n \\ (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f(\alpha)) & \deg f = n \end{cases}$$

Prop. $\mathcal{O}_K$ **is a free abelian group of rank** n**.**

Pf. $(\alpha_1, \cdots, \alpha_n)$ the basis of $K/\mathbb{Q}$

Given $M = \oplus \mathbb{Z}\alpha_i \subseteq \mathcal{O}_K$

Consider the dual basis α_i^* such that $Tr_{K/\mathbb{Q}}(\alpha_i^* \alpha_j) = \delta_{ij}$, thus we get the dual span $M^* = \oplus_i \mathbb{Z}\alpha_i^* = \{x \in K | Tr_{K/\mathbb{Q}}(xy) \in \mathbb{Z} | \forall y \in M\}$, thus $\mathcal{O}_K \subseteq M^*$

Moreover $|M^*/M| = |Disc(\alpha_1, \cdots, \alpha_n)|$ finite, thus $\mathcal{O}_K$ must be a rank n free abelian group.

Definition. A basis $\alpha_1, \cdots, \alpha_n$ **of** $K/\mathbb{Q}$ **is called an integral basis if it is a basis of** $O_K/\mathbb{Z}$

(From the prop. previously shown, it is a reasonable definition)

Definition. $\Delta_K = Disc(integral\ basis) \in \mathbb{Z}$ **is invariant under changes of the integral basis. It is called the discriminent of** K

Invariant property comes from the following fact:

Since $(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)C; (\alpha_1, \cdots, \alpha_n) = (\beta_1, \cdots, \beta_n)D$

Thus $Disc(\beta) = Disc(\alpha)(\det C)^2; Disc(\alpha) = Disc(\beta)(\det D)^2$, since integrality, $Disc(\alpha) = Disc(\beta)$

Prop. $\alpha \in \mathcal{O}_K$ **s.t.** $K = \mathbb{Q}(\alpha)$, $f(T) \in \mathbb{Z}[T]$ **being its minimum polynomial. Assume** $p^2 | Disc(1, \alpha, \cdots, \alpha^{n-1})$。

If $\exists i s.t.\ f(T+i)$ **is a** $p-$**Eisenstein polynomial, then** $\mathcal{O}_K = \mathbb{Z}[\alpha]$

Lem. $\beta_1, \cdots, \beta_n \in \mathcal{O}_K$ s.t. β_i a basis of $K/\mathbb{Q}$, then β_i integral basis $\iff \forall p^2 | Disc(\beta_i)$, $\nexists x_1 \in \{0, \cdots, p-1\}$ s.t. $\exists$ notall 0 coefficients x_i s.t. $\sum x_i \beta_i \in p\mathcal{O}_K$.

Pf: Take α_i a integral basis, assume β_i is not a integral basis, $(\beta_i) = (\alpha_i)C$, then $|\det C| \neq 1$. Take $p \mid |\det C|$, consider $\bar{C} = C \mod p$, $\exists \bar{x}_i \in \mathbb{F}_p$, $\bar{C}\bar{x} = 0$

Then we get $\sum x_i \beta_i \in p\mathcal{O}_k$.

Conversely if $\sum x_i \beta_i \in p\mathcal{O}_K$, then $p | \det C$, thus $\det C \neq 1$.

Now back to the prop.

For $x = \dfrac{1}{p} \displaystyle\sum_{i=0}^{n-1} x_i \alpha^i$, we need to show $x \notin \mathcal{O}_K$. Take $j = \min\{i | x_i \neq 0\}$,

$$N_{K/\mathbb{Q}}(x) = \frac{N_{K/\mathbb{Q}}(\alpha^j)}{p^n} N_{K/\mathbb{Q}}(\textstyle\sum_{i=j}^{n-1} x_i \alpha^{i-j})$$

Since $\dfrac{N_{K/\mathbb{Q}}(\alpha^j)}{p^n} = \dfrac{((-1)^n a_n)^j}{p^n}$, $p || a_n$, we only need to show $p \nmid N_{K/\mathbb{Q}}(\sum_{i=j}^{n-1} x_i \alpha^{i-j})$

However $N_{K/\mathbb{Q}}(\sum_{i=j}^{n-1} x_i \alpha^{i-j}) = \prod_{k=1}^{n} (x_j + x_{j-1} \sigma_k(\alpha)^{i-j} \cdots)$, from calculating we get the result, thus $N_{K/\mathbb{Q}}(x) \notin \mathbb{Z}$, hence the result.

E.g. Cyclotomic Extension.

Consider $p^2 | Disc(1, \cdots, \zeta_{p^n}^{p^n - p})$, $\Phi_{p^n}(x+1)$ Eisesnstein, thus $\mathcal{O}_{K[\zeta_{p^n}]} = \mathbb{Z}[\zeta_{p^n}]$

Prop. Assume $K \cap L = \mathbb{Q}, d = \gcd(\Delta_K, \Delta_L)$, then $\mathcal{O}_{KL} \subset \dfrac{1}{d}\mathcal{O}_K\mathcal{O}_L$

Pf. Take $(\alpha_i), (\beta_i)$ a integral basis of $\mathcal{O}_K, \mathcal{O}_L,$ let $x \in \mathcal{O}_{KL}$, then $x = \sum_{i,j} \dfrac{x_{ij}}{r}\alpha_i\beta_j$

We need to show $r|d$, i.e. $r|\Delta_K$

3. Ideal Class Group

Def. (Fractional ideal) A fractional ideal is a sub $\mathcal{O}_K-$mod of K, say I, s.t.
$\exists d \in \mathcal{O}_K, dI \subseteq \mathcal{O}_K$

Prop. Define $I^{-1} = \{x \in K | xI \subseteq \mathcal{O}_k\}$, then I^{-1} is also a fractional ideal.

Given a fractional ideal I, exists integral ideal s.t. $I = I_1 I_2^{-1}$.

Def. (Ideal Class Group) $Cl_K = \{fractional\ ideals\}/\{principle\ ones\}$

Thus Cl_K measures how far a Dedekind domain is from a PID.

Norm

Def. $I \subseteq \mathcal{O}_K$, **define** $N(I) = \#(\mathcal{O}_K/I)$

Prop. $I = (x), N(I) = N_{K/\mathbb{Q}}(x); N(IJ) = N(I)N(J);$
$\forall n,\ \exists finite\ many\ I, N(I) = n$

Proof of the Main Theorem

Theorem. (Minkowski Bound)

$K, n = [K : \mathbb{Q}], r_2 =$ pairs of complex inclusion.$(\sigma, \bar{\sigma})$, $r_1 =$ numbers of real inclusion. Thus $n = r_1 + 2r_2$.

$\forall$ ideal class contains an integral ideal $\mathfrak{a}$, s.t. $N(\mathfrak{a}) \leq (4/\pi)^r_2 \cdot n!/n^n \cdot \sqrt{|\Delta_K|}$.

Lem. Given a lattice $\Lambda \subseteq \mathbb{R}^n$, $X \subseteq \mathbb{R}^n$ centrally symmetric convex connected space, $\mu(X) > 2^n \mu(\mathbb{R}^n/\Lambda)$