ALGEBRAIC NUMBER THEORY-SUMMER SCHOOL NOTES

Contents

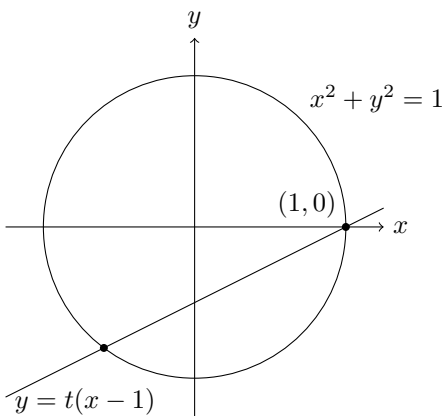
1. Lecture 1: July 30: Introduction

1.1. Diophantine equation.

Example 1.1. Consider the equation

$$x^2 + y^2 = 1$$

in the rational number field $\mathbb{Q}$.



We know that $(1,0)$ is a solution. Any line through this point intersects the unit circle at another point, except the vertical line. Moreover, the point is rational if and only if the slope is rational. Now the slope is $t = \frac{y}{x-1} \in \mathbb{Q}$, and we get

$$x = \frac{t^2-1}{t^2+1}, \quad y = \frac{-2t}{t^2+1}, \quad t \in \mathbb{Q}.$$

In general, if $f(x,y) \in \mathbb{Q}[x,y]$ is a quadratic polynomial, then

$$f(x,y) = 1$$

either has no solutions in $\mathbb{Q}$ or has infinite solutions in $\mathbb{Q}$.

Exercise 1.1. Give a criterion for $f(x,y) = 1$ has a solution in $\mathbb{Q}$.

Exercise 1.2. Solve $x^2 + y^2 = n$ in $\mathbb{Q}$. Hint: consider $n = \mathbf{N}_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy)$.

What about these equations in $\mathbb{Z}$? We may assume that

$$f(x,y) = ax^2 + bxy + cy^2, \quad a,b,c \in \mathbb{Q}.$$

If $f(x,y)$ is positive (negative) definite, then $f(x,y)$ has only finitely many solutions in $\mathbb{Z}$. If $f(x,y)$ is indefinite and irreducible, then if it has a solution in $\mathbb{Z}$, it will has infinitely many solutions in $\mathbb{Z}$.

For example, consider the Pell's equation

$$x^2 - dy^2 = 1,$$

where $d \in \mathbb{Z}_{\geq 2}$ is square-free. Since this is $\mathbf{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x + \sqrt{d}y)$, it's equivalently to say that there are infinitely many $\alpha \in \mathbb{Z}[\sqrt{d}]$ with $\mathbf{N}(\alpha) = 1$, or equivalently to say that $\mathbb{Z}[\sqrt{d}]^\times$ is an infinite abelian group.

Example 1.2. Prove that the equation

$$x^3 + 3y^3 + 9z^3 - 9xyz = 1$$

has infinitely many solutions in $\mathbb{Z}$.

Let $\alpha = \sqrt[3]{3}$. Then the left-hand side is $\mathbf{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x + \alpha y + \alpha^2 z)$. There is a $\gamma \in \mathbb{Z}[\alpha]^\times$ such that $\mathbb{Z}[\alpha]^\times \cong \{\pm 1\} \times \mathbb{Z}$ and $\{\pm\gamma^n\}$ is the set of integral solutions.

The main theorem of this course is

Theorem 1.3 (Catalan's conjecture)**.** *Let $p, q \geq 2$ be integers. Then $x^p - y^q = 1$ has no non-zero solution in $\mathbb{Z}$ except $(x,y,p,q) = (\pm 3, 2, 2, 3)$.*

Remark 1.4. The case $q = 2$ is proved by Lebesgue; the case $p = 2$ is proved by Zhao Ke; when p, q are odd prime, it's proved by Mihailescu.

The Fermat's last theorem is proved by Wiles.

Theorem 1.5 (Wiles)**.** *$x^p + y^p = z^p, p \geq 3$ has no solutions in $\mathbb{Z}$ with $xyz \neq 0$.*

Recall

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!},$$

where the Bernoulli number $B_n \in \mathbb{Q}$, $B_{2n+1} = 0, n \geq 1$.

Definition 1.6. An odd prime p is regular if p does not divide any numerator of B_n for $n = 2, 4, \cdots, p-3$.

Theorem 1.7 (Kummer)**.** *If p is regular, then $x^p + y^p = z^p$ has no solution in $\mathbb{Z}$ with $xyz \neq 0$.*

Remark 1.8. (1) We know that there are infinitely many irregular primes.
(2) We don't know whether there are infinitely many regular primes.
(3) The only irregular primes less than 100 are $37, 59, 67$.

1.2. **Algebraic Integers.**

Definition 1.9. Let $A \subset B$ be an extension of rings. $x \in B$ is called *integral* over A if x satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_i \in A$. B is *integral* over A if all $x \in B$ is integral over A.

Lemma 1.10. *The following are equivalent for $x \in B \supset A$.*

(1) *x is integral over A;*
(2) *$A[x]$ is a finitely generated A-module;*
(3) *there exists a subring $B' \subseteq B$ which is a finitely generated A-module and $x \in B'$.*

Proof. (1)⇒(2) In fact, $A[x] = A + A \cdot x + \cdots + A \cdot x^{n-1}$.
(2)⇒(3) It's trivial, since we can take $B' = A[x]$.
(3)⇒(1) Choose a set of generators $b_1, \cdots, b_n$ of B' as A-module, $xb_i \in B'$, so we have

$$(b_1, \cdots, b_n)x = (b_1, \cdots, b_n)(a_{ij})_{1 \le i,j \le n}.$$

Thus $\det(xI_n - (a_{ij})_{1 \le i,j \le n}) = 0$, which is monic of degree n. So x is integral over A. □

Corollary 1.11. (1) *All elements in B integral over A forms a subring.*
(2) *For $A \subset B \subset C$, if C/B and B/A are integral, then C/A is integral.*

Proof. If $x, y \in B$ are integral over A, then $A[x, y]$ is a finitely generated A-module, so $x \pm y, xy$ are integral over A. This prove (1).

Let $x \in C$, then there exists $f[T] = T^n + b_1T^{n-1} + \cdots + b_n \in B[T]$ s.t $f(x) = 0$. Let $B' = A[b_1, \cdots, b_n] \subseteq B$ be the subring generated by $b_1, \cdots, b_n$, which is a finitely generated A-module, and $B'[x] \subseteq C$ is a finitely generated B'-module, so $C' = B'[x]$ is also a finitely generated A-module. This proves (2). □

Definition 1.12. Let $A \subset B$ as above.

(1) The *integral closure* of A in B is the subring of B consisting of all integral elements over A.
(2) Assume A is a domain. We say A is *integrally closed* is the integral closure of A in $\mathrm{Frac}(A)$ is itself.

Exercise 1.3. All PID (principal ideal domain) are integrally closed, e.g., $\mathbb{Z}, k[x]$.

Let $K/\mathbb{Q}$ be a finite extension and $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K.

Proposition 1.13. *For any $x \in K$, let*

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{Q}[T]$$

be the minimal polynomial of x. Then $x \in \mathcal{O}_K$ if and only if $a_i \in \mathbb{Z}$ for any i.

Proof. Only need to prove the only if part. Let $g(T) \in \mathbb{Z}[T]$ such that $g(x) = 0$. We assume $g(T)$ irreducible in $\mathbb{Z}[T]$. Since $f(T)$ is the minimal polynomial of x, then $g(T) = f(T)\tilde{f}(T)$ in $\mathbb{Q}[T]$. By Gauss lemma, since $g(T)$ is irreducible, $f(T) = g(T)$. □

Exercise 1.4. $K = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ is square-free and $|d| > 1$. Then $\mathcal{O}_K = \mathbb{Z}[\omega_d]$ where

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

1.3. **Discriminant and integral basis.** Let k be a field and A be a finite dimensional k-algebra. For any $x \in A$,

$$\begin{aligned} \ell_x : A &\to A \\ y &\mapsto xy \end{aligned}$$

is an endomorphism of A. Define

$$\mathrm{Tr}_{A/k}(x) = \mathrm{Tr}(\ell_x), \quad \mathbf{N}_{A/k}(x) = \det(\ell_x).$$

Theorem 1.14. *Let L/K be a finite separable field extension. Then*

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

is a non-degenerate K-bilinear form.

Here non-degenerate means that if $\mathrm{Tr}_{L/K}(xy) = 0$ for all $y \in L$, then $x = 0$. Or equivalently to say, $L \simeq \mathrm{Hom}_K(L, K)$ induced by $\mathrm{Tr}_{L/K}$.

Corollary 1.15. *Let L/K be a finite separable extension of degree n. Then $x_1, \ldots, x_n \in L$ form a basis of L/K if and only if $(\mathrm{Tr}_{L/K}(x_i x_j))_{ij}$ is invertible.*

Proof. Consider

$$\begin{array}{ccccc} K^n & \xrightarrow{\phi} & L & \xrightarrow{\psi} & K^n \\ (a_i) & \mapsto & x = \sum a_i x_i & \mapsto & (\mathrm{Tr}(x x_i))_i. \end{array}$$

$\psi \circ \phi$ has matrix form $(\mathrm{Tr}(x_i x_j))_{ij}$. □

Definition 1.16. Let L/K as above and $(\alpha_1, \ldots, \alpha_n)$ a basis of L/K. $(\beta_1, \ldots, \beta_n)$ is called its *dual basis* if

$$\mathrm{Tr}(\alpha_i \beta_j) = \delta_{ij}.$$

Exercise 1.5. Check for which k-algebra A as below, $\mathrm{Tr}_{A/k} : A \times A \to k$ is non-degenerate?

(1) $A = M_n(k)$;
(2) A is the set of upper triangular matrices in $M_n(k)$;
(3) $A = k[x]/(x^n - 1)$, $n \geq 1$.

Let K be a number field.

Definition 1.17. For $x_1, \ldots, x_n \in K$, define

$$\mathrm{disc}(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j)).$$

It's nonzero if and only if $x_1, \ldots, x_n$ form a basis of $K/\mathbb{Q}$.

Proposition 1.18. *(1) If $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ are all embedding of K, then $\mathrm{disc}(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2$.*

(2) If $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)C$ for some $C \in M_n(\mathbb{Q})$, then $\mathrm{disc}(\beta_1, \ldots, \beta_n) = \mathrm{disc}(\alpha_1, \ldots, \alpha_n) \det(C)^2$.

Proof. Since $\mathrm{Tr}(x) = \sum_{i=1}^n \sigma_i(x)$, thus $\mathrm{Tr}(x_i x_j) = \sum_{\ell=1}^n \sigma_\ell(x_i)\sigma_\ell(x_j)$. Hence

$$(\mathrm{Tr}(x_i x_j))_{1 \leq i,j \leq n} = \left((\sigma_\ell(x_i))_{1 \leq i, \ell \leq n} (\sigma_\ell(x_j))^t_{1 \leq \ell, j \leq n}\right)_{1 \leq i,j \leq n}.$$

Take determinant, we get (1).

(2) follows directly from (1). □

Proof of theorem 1.14 We only need to show that for any basis $x_1, \cdots, x_n$, $\mathrm{disc}(x_1, \cdots, x_n) \neq 0$. We know that any finite separable extension is generated by one element. So we may assume $L = K(\theta)$. Then $1, \theta, \cdots, \theta^{n-1}$ form a K-basis of L and $\sigma_i(\theta) \neq \sigma_j(\theta)$ for $i \neq j$. Then we see $(\sigma_i(\theta^{j-1}))_{1 \leq i,j \leq n}$ is a Vandermond matrix, and

$$\mathrm{disc}(1, \theta, \cdots, \theta^{n-1}) = \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta)) \neq 0.$$

Proposition 1.19. *For any basis $(\alpha_1, \ldots, \alpha_n)$ of $K/\mathbb{Q}$, $\mathrm{sign}(\mathrm{disc}(\alpha_1, \ldots, \alpha_n)) = (-1)^{r_2}$, where r_2 is the number of imaginary embedding pairs of K.*

Proof. Since $\mathrm{disc}(\alpha) = \det(\sigma_i(\alpha_j))^2$, $\overline{\mathrm{disc}(\alpha)} = (-1)^{r_2} \mathrm{disc}(\alpha)$. □

Proposition 1.20. *Let $K/\mathbb{Q}$ be a number field of degree n. Then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

Proof. Let $(\alpha_1, \cdots, \alpha_n)$ be a basis of $L/\mathbb{Q}$ and we may assume they all in $\mathcal{O}_K$. Let $(\beta_1, \cdots, \beta_n)$ be its dual basis. For any $x \in \mathcal{O}_K$,

$$x = \sum_{i=1}^n \mathrm{Tr}(x\alpha_i)\beta_i,$$

we see $\sum_{i=1}^n \mathbb{Z} \cdot \alpha_i \subseteq \mathcal{O}_K \subseteq \sum_{i=1}^n \mathbb{Z} \cdot \beta_i$. □

Definition 1.21. A basis of $\mathcal{O}_K$ over $\mathbb{Z}$ is called an *integral basis* of K.

Definition 1.22. The discriminant of K, denoted by $\Delta_K \in \mathbb{Z}$, is the discriminant of an integral basis of K.

Exercise 1.6. Find an integral basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

1.4. **Exercise Sheet 1.**

Exercise 1. *The aim of the exercise is to prove that if $\alpha \in \mathbb{C}$ is an algebraic integer such that $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$, then α must be a root of unity.*

(1) *Show that if $f(X) \in \mathbb{C}[X]$ be a monic polynomial such that all its roots have complex absolute value 1, then the coefficient of X^r in $f(X)$ is bounded by $\binom{n}{r}$.*
(2) *Show that given an integer $n \geq 1$, there exist only finitely many algebraic integers α of degree n such that $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$.*
(3) *Show that an α as in (2) is a root of unity.*

Exercise 2. *Let $f(x) = x^3 + ax + b$ be an irreducible polynomial over $\mathbb{Q}$, and $\alpha \in \mathbb{C}$ be a root of $f(x)$. Set $K = \mathbb{Q}[\alpha]$, and $\mathcal{O}_K$ to be its ring of integers.*

(1) *Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.*
(2) *Find an irreducible polynomial for $2a\alpha + 3b$ over $\mathbb{Q}$.*
(3) *Show that $\mathrm{Disc}_{K/\mathbb{Q}}(1, \alpha, \alpha^2) = -(4a^3 + 27b^2)$.*
(4) *Prove that $f(x)$ is irreducible when $a = b = -1$, and find an integral basis of K.*

Exercise 3. *Consider the number field $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$, and let $\mathcal{O}_K$ be its ring of integers. The aim of this exercise is to show that there exists no algebraic integer α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

(1) *Consider the elements:*

$$\begin{aligned}\alpha_1 &= (1+\sqrt{7})(1+\sqrt{10}),\\ \alpha_2 &= (1+\sqrt{7})(1-\sqrt{10}),\\ \alpha_3 &= (1-\sqrt{7})(1+\sqrt{10}),\\ \alpha_4 &= (1-\sqrt{7})(1-\sqrt{10}).\end{aligned}$$

Show that for any $i \neq j$, the product $\alpha_i\alpha_j$ is divisible by 3 in $\mathcal{O}_K$.
(2) *Let $i \in \{1, 2, 3, 4\}$ and $n \geq 0$ be an integer. Show that*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^n) = \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n \equiv (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^n \pmod 3.$$

Deduce that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i) \equiv 1 \pmod 3$ and hence 3 does not divide α_i in $\mathcal{O}_K$.
(3) *Let α be an algebraic integer. Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α. For all polynomial $g \in \mathbb{Z}[X]$, we denote by $\bar{g} \in \mathbb{F}_3[X]$ its reduction modulo 3. Show that $g(\alpha)$ is divisible by 3 in $\mathcal{O}_K$ if and only if $\bar{g}$ is divisible by $\bar{f}$ in $\mathbb{F}_3[X]$.*
(4) *For $1 \leq i \leq 4$, let $g_i(X) \in \mathbb{Z}[X]$ be such that $\alpha_i = g_i(\alpha)$. Show that there exists an irreducible factor of $\bar{f}$ that divides $\bar{g}_j$ for any $j \neq i$ but does not divide $\bar{g}_i$.*
(5) *Consider the number of irreducible factors of $\bar{f}$ and deduce a contradiction.*

2. Lecture 2: July 31

Lemma 2.1. *Let $\beta_1, \dots, \beta_n$ be n elements of $\mathcal{O}_K$ which form a basis of K. Then $(\beta_1, \dots, \beta_n)$ is not an integral basis if and only if there exists a rational prime p with $p^2 \mid \operatorname{disc}(\beta_1, \dots, \beta_n)$ and some $x_i \in \{0, 1, \dots, p-1\}$ for $1 \le i \le n$ such that not all of x_i are zero and $\frac{1}{p}\sum_i x_i\beta_i \in \mathcal{O}_K$.*

This gives an algorithm to compute integral basis of K.

Proof. We only need to prove the "only if" part. Let $\alpha_1, \cdots, \alpha_n$ be an integral basis, then there exists a matrix $C \in M_n(\mathbb{Z})$ such that

$$(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)C.$$

$\beta_1, \cdots, \beta_n$ is not an integral basis implies that $C \notin \mathrm{GL}_n(\mathbb{Z})$, so there exists a prime $p \mid \det(C)$. Hence $\operatorname{rank}_{\mathbb{F}_p} \overline{C} \le n-1$, here $\overline{C}$ means C modulo p. Take $(\bar{x}_1, \cdots, \bar{x}_n)^t$ be a nonzero solution of $\overline{C}X = 0$ in $\mathbb{F}_p^n$ and let $0 \le x_i \le p-1$ s.t x_i modulo p equals to $\bar{x}_i$. Therefore

$$(\beta_1, \cdots, \beta_n)(x_1, \cdots, x_n)^t = (\alpha_1, \cdots, \alpha_n)C(x_1, \cdots, x_n)^t \equiv 0 \pmod{p},$$

which means $x_1\beta_1 + \cdots x_n\beta_n \in p\mathcal{O}_K$. □

Exercise 2.1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Is $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ an integral basis? Since $\alpha = \frac{\sqrt{2}+\sqrt{3}}{2} \in \mathcal{O}_K$, $2^2 \mid \operatorname{disc}(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$, the answer is no. In fact, $(1, \sqrt{2}, \sqrt{3}, \alpha)$ is an integral basis.

Proposition 2.2. *Let $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Let $f(T) \in \mathbb{Z}[T]$ be its minimal polynomial. Assume for any prime p with $p^2 \mid \operatorname{disc}(1, \alpha, \dots, \alpha^{n-1})$, there is a j such that $f(T+j)$ is Eisenstein for p. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Proof. It suffices to show for any $x_i = 0, 1, \dots, p-1$, $x = \frac{1}{p}\sum x_i\alpha^i \notin \mathcal{O}_K$. We may assume $j = 0$. Put $k := \min\{i \mid x_i \neq 0\}$, then $\sum x_i\alpha^i = \alpha^k \sum_{i=k}^{n-1} x_i\alpha^{i-k}$ and $\mathbf{N}(\alpha) \notin \mathbb{Z}$. □

Exercise 2.2. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $f(T) = T^3 - 2$ and $f(T-1) = T^3 - 3T^2 + 3T - 3$ are Eisenstein. Since $\operatorname{disc}(1, \sqrt[3]{2}, \sqrt[3]{4}) = -3^3 \cdot 2^2$, $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

2.1. **Cyclotomic fields.** For $N \ge 3$, let $\zeta_N = e^{\frac{2\pi i}{N}}$ be a primitive N-th root of unity. Then $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is Galois and

$$\begin{aligned} \varphi : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times, \\ \sigma &\longmapsto a_\sigma \end{aligned}$$

is injective, where $\sigma(\zeta_N) = \zeta_N^{a_\sigma}$.

Proposition 2.3. *φ is an isomorphism. It's equivalently to say that*

$$\prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} (T - \zeta_N^a) = \Phi_N(T)$$

is irreducible in $\mathbb{Q}$.

Proof. By writing a positive integer coprime to N as a product of prime numbers, it suffices to show that if $p \nmid N$, then $\bar{p} \in (\mathbb{Z}/N\mathbb{Z})^\times$ lies in $\mathrm{Im}(\varphi)$.

Let $f(T)$ be the minimal polynomial of ζ_N. Then $T^N - 1 = f(T)g(T)$, where $f, g \in \mathbb{Z}[T]$. Assume that ζ_N^p is not conjugate to ζ_N, then $f(\zeta_N^p) \neq 0$ but $g(\zeta_N^p) = 0$. Thus ζ_N is a root of $g(T^p)$ and $f(T) \mid g(T^p)$. Let $\bar{f}, \bar{g} \in \mathbb{F}_p[T]$ be the reduction of f, g. Then $\bar{f}(T) \mid \bar{g}(T^p) = (\bar{g}(T))^p$ and $\bar{f} \mid \bar{g}$. Thus $T^N - 1 = \bar{f}(T)\bar{g}(T)$ has a multiple root. But $(T^N - 1)' = NT^{N-1}$ is coprime to $T^N - 1$ in $\mathbb{F}_p[T]$, which is a contradiction. □

Corollary 2.4. *(1) $[\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N) := \#(\mathbb{Z}/N\mathbb{Z})^\times$.*

(2) For any $N, M \ge 3$ with $\gcd(N, M) = 1$, $\mathbb{Q}(\mu_N) \cap \mathbb{Q}(\mu_M) = \mathbb{Q}$ and $\mathbb{Q}(\mu_{NM}) = \mathbb{Q}(\mu_N)\mathbb{Q}(\mu_M)$ in $\mathbb{C}$.

Now let's find an integral basis for $\mathbb{Q}(\zeta_N)$. Obviously $\mathcal{O}_{\mathbb{Q}(\zeta_N)} \supseteq \mathbb{Z}[\zeta_N]$.

Lemma 2.5. *$|\operatorname{disc}(1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1})|$ divides $N^{\varphi(N)}$.*

Proof. The left-hand side is $|\mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Phi_N'(\zeta_N))|$. In general, $\operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))$ where $K = \mathbb{Q}(\alpha)$ and f is the minimal polynomial of α.

Since $T^N - 1 = \Phi_N(T)g(T)$, $NT^{N-1} = \Phi_N'(T)g(T) + \Phi_N(T)g'(T)$ and $N\zeta_N^{N-1} = \Phi_N'(\zeta_N)g(\zeta_N)$. Thus

$$\mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Phi_N'(\zeta_N)) = \mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(g(\zeta_N)) \mid \mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(N\zeta_N^{N-1}) = N^{\varphi(N)}.$$

□

Corollary 2.6. *If $N = p^n$, then $\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_{p^n}]$.*

Proof. Because $\Phi_{p^n}(T) = \frac{T^{p^n}-1}{T^{p^{n-1}}-1}$ is Eisenstein. □

For general N, write $N = \prod p_i^{a_i}$ then $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{p_1^{a_1}}) \cdots \mathbb{Q}(\zeta_{p_n^{a_n}})$. We consider the following. Let K, L be two number fields. Clearly $\mathcal{O}_{KL} \supseteq \mathcal{O}_K \mathcal{O}_L$.

Proposition 2.7. *Assume that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. Then $\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$ where $d = \gcd(\Delta_K, \Delta_L)$.*

Proof. Let $\mathcal{O}_K = \oplus_{i=1}^n \mathbb{Z}\alpha_i$ and $\alpha_i^\vee$ $(1 \leq i \leq n)$ the dual basis. Similarly, let $\mathcal{O}_L = \oplus_{j=1}^m \mathbb{Z}\beta_j$ and $\beta_j^\vee (1 \leq j \leq m)$ the dual basis. Then it is easy to verify that $\alpha_i^\vee \beta_j^\vee$ $(1 \leq i \leq n, 1 \leq j \leq m)$ is the dual basis of $\alpha_i\beta_j$ for $KL/\mathbb{Q}$. Also note that

$$|\operatorname{disc}_K| = [\oplus \mathbb{Z}\alpha_i^\vee : \oplus \mathbb{Z}\alpha_i].$$

Then the proposition follows directly. □

In particular, $\mathbb{Z}[\zeta_N]$ is the integer ring of $\mathbb{Q}(\zeta_N)$.

2.2. **Exercise sheet 2.**

Exercise 1. *Let ζ_N be a primitive N-th root of unity. Put $\theta = \zeta_N + \zeta_N^{-1}$.*

1. *Show that $\mathbb{Q}(\theta)$ is the fixed field of $\mathbb{Q}(\zeta_N)$ under the automorphism defined by the complex conjugation.*
2. *Put $n = \phi(N)/2$. Show that $\{1, \zeta_N, \theta, \theta\zeta_N, \theta^2, \theta^2\zeta_N, \cdots, \theta^{n-1}, \theta^{n-1}\zeta_N\}$ is an integral basis for $\mathbb{Q}(\zeta_N)$.*
3. *Show that the ring of integers of $\mathbb{Q}(\theta)$ is $\mathbb{Z}[\theta]$.*
4. *Suppose that $N = p$ is an odd prime number. Prove that the discriminant of $\mathbb{Q}(\theta)$ is $\Delta_{\mathbb{Q}(\theta)} = p^{\frac{p-3}{2}}$.*

Exercise 2. *Let A be a local domain with unique maximal ideal $\mathfrak{m} \subset A$ such that each non-zero ideal $I \subseteq A$ admits a unique factorization $I = \prod_i \mathfrak{p}_i^{e_i}$ into products of prime ideals $\mathfrak{p}_i$.*

1. *Show that there exists $x \in \mathfrak{m} \backslash \mathfrak{m}^2$.*
2. *Let $x \in \mathfrak{m}\backslash\mathfrak{m}^2$ and $y \in \mathfrak{m}$. Prove that $(x, y) \subseteq A$ is prime ideal.*
   Hint: Write $(x, y) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ as a product of prime ideals and use $x \notin \mathfrak{m}^2$
3. *Prove $(x) = \mathfrak{m}$.*
   Hint: For $y \in \mathfrak{m}$, show $y \in (x, y^2)$.
4. *Conclude that every element $y \in A\backslash\{0\}$ admits a unique expression $y = ux^e$ with $e \geqslant 0$ and $u \in A^\times$ a unit and that A is a discrete valuation ring.*

Exercise 3. *Let $f(x) \in \mathbb{C}[x]$ be a nonconstant polynomial not of the form $g(x)^2$ for any $g(x) \in \mathbb{C}[x]$. Let $A = \mathbb{C}[x, y]/(y^2 - f(x))$.*

1. *Prove that A is a domain.*
2. *Prove that A is a Dedekind domain if $f(x)$ has only simple roots.*
3. *If we allow the roots of $f(x)$ to have multiplicities, what is the integral closure of A in its fraction field?*

Exercise 4 (Chinese Remainder Theorem)**.** *Let A be a commutative ring, $I, J \subseteq A$ be ideals such that $1 \in I + J$. Consider the natural map $\phi : A/I \cap J \to A/I \oplus A/J$ sending x to $(x \mod I, x \mod J)$.*

1. *Prove that, given any $x \in A$, there exists $y \in I$ such that $y \equiv x \mod J$ (Hint: write $1 = a + b$ for some $a \in I$ and $b \in J$).*
2. *Use (1) to prove ϕ is an isomorphism.*
3. *Suppose that A is a Dedekind domain. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be primes of A such that $\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j$, and $e_1, \cdots, e_r \geqslant 1$ be integers. Prove that*

$$A/\prod_{i=1}^r \mathfrak{p}_i^{e_i} = \bigoplus_{i=1}^r A/\mathfrak{p}_i^{e_i}.$$

3. Lecture 3: August 2

3.1. **Dedekind domain.** A is called a Dedekind domain if A is Noetherian, integrally closed and each nonzero prime ideal is maximal.

Note that localization of a Dedekind domain is also Dedekind. We always have the following setting in this section. Let A be a Dedekind domain, let K be the fractional field of A. Let L/K be a finite separable extension. Let B be the integral closure of A in L.

Proposition 3.1. *Let A be a Dedekind domain, let K be the fractional field of A. Let L/K be a finite separable extension. Let B be the integral closure of A in L. Then B is a Dedekind domain.*

Proof. Of course B is integrally closed. Let $\mathfrak{P}$ be a nonzero prime ideal of B. Since for any nonzero $b \in \mathfrak{P}$, we have $N(b) \in A \cap \mathfrak{P} \neq 0$. Thus $\mathfrak{P} \cap A$ is a nonzero prime ideal of A, hence $\mathfrak{P} \cap A$ is maximal. It follows that $B/\mathfrak{P}$ is integral over $A/\mathfrak{P} \cap A$, thus $B/\mathfrak{P}$ is also a field. (Exercise). This proves $\mathfrak{P}$ is a maximal ideal of B. Since L/K is finite separable, the trace pairing is non-degenerate. Then B is finitely generated as A-modules, (the argument is same as in the number field case). Since A is Noetherian, we have that in particular B is a Noetherian ring. □

Counter-examples:

(1) $\mathbb{C}[[X^{\frac{1}{n}}, n \geq 1]]$ is not Noetherian. Note that this ring is integrally closed and every nonzero prime ideal is maximal.
(2) $\mathbb{Z}[\sqrt{-3}]$ is not integrally closed. Note that this ring is Noetherian and every nonzero prime ideal is maximal.
(3) $\mathbb{Z}[X]$ is Noetherian and integrally closed, but (X) is a prime ideal but not maximal.

Theorem 3.2 (Unique factorization law)**.** *Let A be a Dedekind domain. Then every ideal $I \subseteq A$ has a factorization $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ where each $\mathfrak{p}_i$ non-zero prime, $\mathfrak{p}_i \neq \mathfrak{p}_j$ and $a_i \in \mathbb{Z}_{\geq 1}$. Such a factorization is unique.*

Sketch of the proof.

(1) Show that every non-zero ideal $I \subseteq A$ contains a product of non-zero prime ideals. (Use A is Noetherian.)
(2) Let $K = \mathrm{Frac}(A)$, prove that $\forall\ 0 \neq \mathfrak{p} \subseteq A$ prime, define $\mathfrak{p}^{-1} := \{x \in K : x\mathfrak{p} \subseteq A\} \subseteq K$ and $\mathfrak{p}\mathfrak{p}^{-1} := \{x \in K : x = \sum a_i b_i, a_i \in \mathfrak{p}^{-1}, b_i \in \mathfrak{p}\}$. Then $\mathfrak{p}^{-1}\mathfrak{p} = A$. In fact, $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq A$, $\mathfrak{p}$ maximal implies that either $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{p}^{-1}\mathfrak{p} = A$. If $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$, then $\mathfrak{p}^{-1}$ is integral over A. $(x \in \mathfrak{p}^{-1} \Rightarrow x\mathfrak{p} \subset \mathfrak{p} \Rightarrow \det(xI_n - C) = 0$, where $x(a_1, \cdots, a_n) = (a_1, \cdots, a_n)C)$. Then $\mathfrak{p}^{-1} = A$. To see $\mathfrak{p}^{-1} = A$ impossible, we construct a $x \in \mathfrak{p}^{-1} - A$. In fact, let $x = \frac{a}{b} \in \mathfrak{p}^{-1}$, then $\frac{a}{b} \notin A \Leftrightarrow a\mathfrak{p} \subseteq (b), a \notin (b)$.
(3) Existence. $S := \{I \subset A : I$ is not a product of prime ideals$\}$. If $S \neq \emptyset$, then $\exists$ a maximal element J, which is contained in a maximal ideal $\mathfrak{p}$ and $J \neq \mathfrak{p}$. Then $A \supset J\mathfrak{p}^{-1} \supset J$, hence $\mathfrak{p}^{-1}J \notin S$, which means $\mathfrak{p}^{-1}J = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$, and then $J = \mathfrak{p}\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$, contradiction.

3.2. **Fractional ideal.** Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$.

Definition 3.3. A fractional ideal of A is an A sub-module I of K, s.t. $\exists\ 0 \neq d \in A$ such that $dI \subseteq A$ $(\Rightarrow I \subseteq \frac{1}{d}A)$.

Example 3.4. $A = \mathbb{Z}$, $I = \frac{1}{d}\mathbb{Z}$ is a fractional ideal while $\mathbb{Z}[\frac{1}{d}]$ is not. If I, J are two fractional ideals of A, then so are $I + J, IJ$.

Theorem 3.5 (UFL of factional ideals)**.** *Any fractional ideal I of A has a unique factorization $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, $a_i \in \mathbb{Z}, \mathfrak{p}_i \neq \mathfrak{p}_j, i \neq j$.*

Corollary 3.6. *$\mathcal{I}_A = \{$fractional ideals of $A\}$ form a free abelian group with a basis given by non-zero prime ideals of A.*

Exercise 3.1. If $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \subset A$, then $I^{-1} = \prod_{i=1}^{r} \mathfrak{p}_i^{-a_i}$.

$$\begin{array}{rl} \mathcal{P}_A & := \{\text{principal fractional ideals}\} = \{(x) : x \in K^\times\} \subseteq \mathcal{I}_A; \\ \mathrm{Cl}_A & := \mathcal{I}_A/\mathcal{P}_A \quad \text{ideal class group of A} \end{array}.$$

A is a PID$\Leftrightarrow \mathrm{Cl}_A = 0$.

Theorem 3.7. *If $K/\mathbb{Q}$ is a finite extension, then $\mathrm{Cl}_{\mathcal{O}_K}$ is finite.*

Remark 3.8. There are Dedekind domain A s.t. Cl_A is infinite.

Example 3.9. $A = \mathbb{C}[x,y]/(y^2 - f(x)), f(x) = \prod_{i=1}^{3}(x-a_i), a_i \neq a_j, i \neq j$. A is a Dedekind domain. Is Cl_A infinite?

Corollary 3.10. *For any fractional ideal I of A, $(0) \neq \mathfrak{p} \subseteq A$, then $\dim_{A/\mathfrak{p}}(I/I\mathfrak{p}) = 1$.*

Proof. $\forall x \in I, x \notin I\mathfrak{p}$. $I\mathfrak{p} \subset I\mathfrak{p} + (x) \subseteq I$ and UFL implies $I\mathfrak{p} + (x) = I$. □

Recall if $I = \prod_{i=1}^{r} \mathfrak{p}^{e_i} \subseteq A$ is an ideal, $\mathfrak{p}_i \neq \mathfrak{p}_j, i \neq j$. By Chinese remainder theorem

$$A/I \simeq \bigoplus_i A/\mathfrak{p}_i^{e_i}$$

with each $A/\mathfrak{p}_i^{e_i}$ a local Artinian ring.

Exercise 3.2. $A = \mathbb{Z}[\sqrt{-5}]$, it is a Dedekind domain. $I = (3, \sqrt{-5}) \stackrel{?}{=} \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$.

Since $A/I \simeq \mathbb{Z}[T]/(T^2+5, 3+T) \simeq \mathbb{Z}/((-3)^2+5) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, so $I = \mathfrak{p}_2\mathfrak{p}_7$, $\mathfrak{p}_2 = (2, 3+\sqrt{-5}), \mathfrak{p}_7 = (7, 3+\sqrt{-5})$.

Proposition 3.11. *If A is a Dedekind domain with finitely main prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, then A is a PID.*

Proof. $A/\prod_{i=1}^{r} \mathfrak{p}_i^2 \simeq \bigoplus_{i=1}^{r} A/\mathfrak{p}_i^2$, so there exists $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$ and $x \equiv 1 \pmod{\mathfrak{p}_i^2}, \forall i \neq 1$. Claim $(x) = \mathfrak{p}_1$. Indeed, $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$ and $x \notin \mathfrak{p}_i, \forall i \neq 1$. By UFL, the claim holds. □

3.3. **Localization.** .

Proposition 3.12. *Let A be a Dedekind domain, $S \subseteq A - \{0\}$ be a multiplicative set, $A' = S^{-1}A = \left\{\frac{a}{s} : a \in A, s \in S\right\}$.*

1. *If $\mathfrak{p} \subset A$ maximal, $\mathfrak{p}' = \mathfrak{p}A'$. Then $\mathfrak{p}'$ is a maximal ideal of A' iff $S \cap \mathfrak{p} = \emptyset$.*
2. *If I is a fractional ideal with decomposition $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, then $I' = \prod_{i=1}^{r} \mathfrak{p}_i'^{a_i}$.*

3.4. **Extension of Dedekind domains.** Setup: A Dedekind, $K = \mathrm{Frac}(A), L/K$ finite separable extension, B the integral closure of A in L. As we have known, B is Dedekind.

$\mathfrak{p} \subset A$ a non-zero prime ideal, $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$.

Proposition 3.13. $[L:K] = \sum_{i=1}^{r} e_i f_i$.

Proof. Step 1. Reduce to the case where B is free over A by localization. Then

$$\sum \dim_{k(\mathfrak{p})}(B/\mathfrak{P}^{e_i}) = \dim_{k(\mathfrak{p})}(B/\mathfrak{p}B) = \mathrm{rank}_A(B) = n.$$

Step 2. Consider the filtration $\mathfrak{P}_i^{e_i} \subseteq \mathfrak{P}_i^{e_i-1} \subseteq \cdots \subseteq B$, $\mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ is a 1-dimensional vector space over $k(\mathfrak{P}_i)$. Therefore $\dim_{k(\mathfrak{p})} B/\mathfrak{P}_i^{e_i} = e_i f_i$. □

Theorem 3.14 (Kummer)**.** *Let $\alpha \in B$ s.t. $B/\mathfrak{p}B = \kappa(\mathfrak{p})[\bar{\alpha}]$. Let $f[T] \in A[T]$ be the minimal polynomial of α. Assume $f(T) \equiv \prod_{i=1}^{g} h_i(T)^{e_i} \pmod{\mathfrak{p}A[T]}$, where $i \geq 1, h_i(T) \in A[T]$ are monic polynomial which is irreducible in $k(\mathfrak{p})[T]$, distinct. Then $\mathfrak{Q}_i = \mathfrak{p}B + h_i(\alpha)B$ is a maximal ideal of B and $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{Q}_i^{e_i}$ is the prime decomposition of $\mathfrak{p}B$.*

Remark 3.15. $B/\mathfrak{p}B = k(\mathfrak{p})[\overline{\alpha}]$ is much weaker than $B = A[\alpha]$.

Proof. $B/\mathfrak{Q}_i = B/(\mathfrak{p}B + h_i(\alpha)B) = k(\mathfrak{p})[T]/h_i[T]$ is a field, i.e. $\mathfrak{Q}_i$ is maximal.

$$B/\mathfrak{p}B = k(\mathfrak{p})[\bar{\alpha}] = k(\mathfrak{p})[T]/(f(T)) \simeq \prod_{i=1}^{r} k(\mathfrak{p})[T]/h_i(T)^{e_i} = \prod_{i=1}^{r} B/(\mathfrak{p}B + h_i(\alpha)^{e_i}).$$

To complete the proof, it suffices to show $\mathfrak{Q}_i^{e_i} = \mathfrak{p}B + h_i(\alpha)^{e_i}B$. In fact

$$(\mathfrak{p}B + h_i(\alpha)B)^{e_i} \subseteq \mathfrak{p}B + h_i(\alpha)^{e_i}B \text{ and } e_i f_i = \dim_{k(\mathfrak{p})} B/\mathfrak{Q}_i^{e_i} = \dim_{k(\mathfrak{p})} B/(\mathfrak{p}B + h_i(\alpha)^{e_i}B).$$ □

Example 3.16. $K = \mathbb{Q}(\sqrt{d})$ with d square free, then

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

$p \in \mathbb{Z}$ be a prime,

(1) p ramified in K, i.e. some $e_i > 1$, iff

$$p \mid \Delta_K = \begin{cases} 4d & d \equiv 2, 3 \pmod 4 \\ d & d \equiv 1 \pmod 4 \end{cases}$$

(2) If $p \geq 3$ and unramified in K, then p splits in K i.e. $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1 \neq \mathfrak{p}_2$ iff $\left(\frac{d}{p}\right) = 1$.

(3) If $p = 2$ is unramified in K (equivalently, $d \equiv 1 \pmod 4$), then 2 is split in K iff $d \equiv 1 \pmod 8$.

3.5. **Exercise sheet 3.**

Exercise 1. *Let $f(x) \in \mathbb{C}[x]$ be a nonconstant polynomial not of the form $g(x)^2$ for any $g(x) \in \mathbb{C}[x]$. Let $A = \mathbb{C}[x, y]/(y^2 - f(x))$.*

(1) *Prove that A is a domain.*
(2) *Prove that A is a Dedekind domain if $f(x)$ has only simple roots. (*Hint: mimic the case of $\mathbb{Q}(\sqrt{d})$ to prove that A is integrally closed*)*
(3) *If we allow the roots of $f(x)$ to have multiplicities, what is the integral closure of A in its fraction field?*

Exercise 2. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha^3 = \alpha + 1$.*

(1) *Show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*
(2) *Find the explicit decomposition of primes $p = 3, 5, 23$ in $\mathcal{O}_K$.*
(3) *Prove that $\sqrt{\alpha}, \sqrt[3]{\alpha} \notin K$. (Hint: try to find prime p such that there exists a surjective map $\mathcal{O}_K \twoheadrightarrow \mathbb{F}_p$ such that the image of α can not has square or cubic root.)*

Exercise 3. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha^5 = 2$.*

(1) *Determine all the primes p that are ramified in K.*
(2) *Prove that $\mathcal{O}_K = \mathcal{Z}[\alpha]$.*
(3) *Prove that if p is a prime unramified in K and $5 \nmid (p^2 - 1)$, then p decomposes in $\mathcal{O}_K$ as $(p) = \mathfrak{p}\mathfrak{p}'$ with $f(\mathfrak{p}|p) = 1$ and $f(\mathfrak{p}'|p) = 4$.*

Exercise 4. *Let A be a Dedekind domain. Let $I \subset A$ be a nonzero ideal with prime decomposition $I = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$. Prove that $I^{-1} = \prod_{i=1}^r (\mathfrak{p}_i^{-1})^{e_i}$ and $I^{-1}I = A$.*

*(*Remark: This is one of intermediate steps to deduce the UFL for fractional ideals from UFL for ideals. So you can only use UFL for ideals and the fact that $\mathfrak{p}^{-1}\mathfrak{p} = A$ for any nonzero prime $\mathfrak{p}$*)*

4. Lecture 4: August 5

Let L/K be a finite extension of number fields with integer ring B and A, and $\mathfrak{p} \neq 0$ be a prime of $\mathcal{O}_K$. We have a prime decomposition

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Definition 4.1. A prime $\mathfrak{p} \subset A$ is unramified in B if $\forall \mathfrak{P}_i \mid \mathfrak{p}$, $e(\mathfrak{P}_i/\mathfrak{p}) = 1$.

Proposition 4.2. *Let $K/\mathbb{Q}$ be finite, $p \in \mathbb{Q}$ prime, then p is unramified in $\mathcal{O}_K$ (or in K) iff $p \mid \Delta_K$.*

Proof. p is unramified in $K \Leftrightarrow \mathcal{O}_K \simeq \oplus_{i=1}^g \mathcal{O}_K/\mathfrak{P}_i^{e_i}$ is reduced.
Fact: If R is a finite dimensional commutative k-algebra, then R is a direct sum of finite separable extension of k iff

$$\mathrm{Tr}_{R/k} : R \times R \to k$$
$$(x, y) \mapsto \mathrm{Tr}_{R/k}(xy) \text{ is non-degenerate.}$$

So p is unramified $\Leftrightarrow \mathrm{Tr}_{\mathcal{O}_K/p} : \mathcal{O}_K/p \times \mathcal{O}_K/p \to \mathbb{F}_p$ is non-degenerate $\Leftrightarrow p \nmid \Delta_K$. □

Remark 4.3. From geometric point of view, $e(\mathfrak{P}/\mathfrak{p}) > 1$ if $\mathfrak{P} \in \mathrm{Supp}(\Omega^1_{B/A})$. $\Omega^1_{B/A} \otimes_B L = \Omega^1_{L/K} = 0$ implies Supp is finite module.

4.1. **Galois extension.** Assume L/K is Galois, $G = \mathrm{Gal}(L/K)$. For all $\sigma \in G$, $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ implies $\mathfrak{p}B = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g}$. If $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j \Rightarrow e_i = e_j$, and $B/\mathfrak{P}_i \xrightarrow{\sigma} B/\mathfrak{P}_j$ is an isomorphism.

Proposition 4.4. (1) *The action of G in $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ is transitive.*
(2) *$e = e_1 = \cdots = e_g$, $f = f(\mathfrak{P}_1/\mathfrak{p}) = \cdots = f(\mathfrak{P}_g/\mathfrak{p})$.*

Proof. Let $\mathfrak{P}' \notin G$-orbit of $\mathfrak{P} = \mathfrak{P}_1$, then $\exists x \in \mathfrak{P}'$ but $x \notin \sigma(\mathfrak{P}_1)$ for all $\sigma \in G$, then get $\sigma(x) \notin \mathfrak{P}_1$ for all $\sigma \in G$.

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P}_1 \cap \mathcal{O}_K = \mathfrak{p}.$$ □

Definition 4.5. For $\mathfrak{P} \mid \mathfrak{p}$, define

$$D(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

and call it the decomposition group at $\mathfrak{P}$ relative to $\mathfrak{p}$. We get thus a homomorphism

$$\varphi_{\mathfrak{P}} : D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

We define

$$I(\mathfrak{P} \mid \mathfrak{p}) := \mathrm{Ker}(\varphi_{\mathfrak{P}}) = \{\sigma \in D(\mathfrak{P} \mid \mathfrak{p}) \mid \sigma(x) \equiv x \bmod \mathfrak{P},\ \forall x \in \mathcal{O}_L\},$$

and call it the inertia group.

Proposition 4.6. (1) $1 \to I(\mathfrak{P} \mid \mathfrak{p}) \to D(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(p)) \to 1$.
(2) $\#I(\mathfrak{P} \mid \mathfrak{p}) = e$, $\#D(\mathfrak{P} \mid \mathfrak{p}) = ef$.

Corollary 4.7. *Let M/K be a subextension of L/K, $H = \mathrm{Gal}(L/M)$. Let $\mathfrak{P}$ be a prime of L, $\mathfrak{P}_M = \mathfrak{P} \cap M$, $\mathfrak{p} = \mathfrak{P} \cap K$. Then $e(\mathfrak{P}_M/\mathfrak{p}) = 1 \Leftrightarrow I(\mathfrak{P}/\mathfrak{p}) \subset H$.*

Proof. $e(\mathfrak{P} \mid \mathfrak{p}) = 1 \Leftrightarrow e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{P}_M)e(\mathfrak{P}_M \mid \mathfrak{p})$, then $e(\mathfrak{P}_M \mid \mathfrak{p}) = 1 \Leftrightarrow e(\mathfrak{P} \mid \mathfrak{p}) = e(\mathfrak{P} \mid \mathfrak{P}_M) \Leftrightarrow \#I(\mathfrak{P} \mid \mathfrak{p}) = \#I(\mathfrak{P} \mid \mathfrak{P}_M) \Leftrightarrow I(\mathfrak{P} \mid \mathfrak{p}) \subset H$. □

Corollary 4.8. *Let L_1/K, L_2/K be two extensions. Let $\mathfrak{p} \subset A$ be a prime. Then $\mathfrak{p}$ is unramified in both L_1 and L_2 iff $\mathfrak{p}$ is unramified in L_1L_2.*

Proof. Choose a finite Galois extension L/K containing L_1L_2. Let H_i denote the subgroups of $\mathrm{Gal}(L/K)$ that fix L_i respectively. Then L_1L_2 is the fixed field of $H_1 \cap H_2$. Then by the proposition above, $\mathfrak{p}$ is unramified in L_1L_2 iff $I(\mathfrak{P} \mid \mathfrak{p}) \subset H_1 \cap H_2$ for every prime $\mathfrak{P}$ of L above $\mathfrak{p}$, or equivalently $I(\mathfrak{P} \mid \mathfrak{p}) \subset H_1$ and $I(\mathfrak{P} \mid \mathfrak{p}) \subset H_2$, which is equivalent to that $\mathfrak{p}$ is unramified in L_1 and L_2. □

Assume all the residue fields of A are finite fields (e.g. $A = \mathcal{O}_K$, $K/\mathbb{Q}$ finite extension). Assume $e(\mathfrak{P} \mid \mathfrak{p}) = 1$, then $D(\mathfrak{P} \mid \mathfrak{p}) \xrightarrow{\simeq} \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Let $q = N(\mathfrak{p})$, and $q^f = N(\mathfrak{P})$. Then $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \simeq \mathbb{Z}/f\mathbb{Z}$ with a canonical generator given by $\sigma_q : x \mapsto x^q$ for any $x \in k(\mathfrak{P})$. We denote by

$$\phi_{\mathfrak{P}|\mathfrak{p}} \in D(\mathfrak{P} \mid \mathfrak{p})$$

corresponds to σ_q. Then we have following properties:
(1) $\phi_{\sigma(\mathfrak{P})|\mathfrak{p}} = \sigma\phi_{\mathfrak{P}|\mathfrak{p}}\sigma^{-1}$ for all $\sigma \in G$.

(2) $\phi_{\mathfrak{P}|\mathfrak{p}}|_M = \phi_{\mathfrak{P}_M|\mathfrak{p}}$.
(3) $\phi_{\mathfrak{P}|\mathfrak{P}_M} = \phi_{\mathfrak{P}|\mathfrak{p}}^{f(\mathfrak{P}|\mathfrak{p})}$.

4.2. **Chebotarev density theorem.**

Definition 4.9. Let $K/\mathbb{Q}$ be finite extension, $I \subset \mathcal{O}_K$ ideal, define $N(I) = \#(\mathcal{O}_K/I)$.

We have $N(IJ) = N(I)N(J)$ and $N(\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$.

Definition 4.10. Let $\Sigma_K = \{\mathfrak{p} \subset \mathcal{O}_K, \text{non-zero prime ideals}\}$. A subset S of Σ_K has density $\rho \in [0,1]$ if

$$\lim_{t\to\infty} \frac{\#\{\mathfrak{p} \in S \mid N(\mathfrak{p}) \le t\}}{\#\{\mathfrak{p} \in \Sigma_K \mid N(\mathfrak{p}) \le t\}} = \rho.$$

Theorem 4.11 (Chebotarev)**.** *Let L/K be a finite Galois extension of number fields, $G = \mathrm{Gal}(L/K)$, then for $\forall$ conjugacy class $C \subset G$, the set*

$$\{\mathfrak{p} \in \Sigma_K \mid \mathfrak{p} \text{ unramified in } L/K,\ \text{Frob. conjugacy class of } \mathfrak{p} \text{ in } G \text{ is } C\}$$

has density $\frac{|C|}{|G|}$.

Question: For which prime p the equation $x^3 = 2$ has a solution in $\mathbb{F}_p$, what is the density of such primes?
Answer: $x^3 \equiv 2 \bmod p$ has a solution in $\mathbb{F}_p$ is "almost" equivalent to $\exists \mathfrak{p} \mid p$ in $K = \mathbb{Q}(\sqrt[3]{2})$ unramified, $f(\mathfrak{p} \mid p) = 1$ (by Kummer's theorem).

There are two cases:
(1) p (totally) splits in K;
(2) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $f(\mathfrak{p}_1 \mid p) = 1$, $f(\mathfrak{p}_2 \mid p) = 2$.

Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, then $G := \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle / \langle \sigma^3 = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$. The actions are given by $\sigma(\sqrt[3]{2}) = \sqrt{2}[3]\zeta_3$, $\sigma(\zeta_3) = \zeta_3$; $\tau(\sqrt{2}[3]) = \sqrt[3]{2}$, $\tau(\zeta_3) = \zeta_3^2$.

There exists $\mathfrak{p}$ of K such that $f(\mathfrak{p} \mid p) = 1 \Leftrightarrow \exists \mathfrak{P} \mid \mathfrak{p}$ in L such that $\phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(L/K) = \langle \tau \rangle \Leftrightarrow \exists \mathfrak{P} \mid \mathfrak{p}$ in L such that $\phi_{\mathfrak{P}|p} = 1$ or τ. If $\phi_{\mathfrak{P}|p} = 1$, conjugacy class: $\{1\}$, the density is $\frac{1}{6}$. If $\phi_{\mathfrak{P}|p} = \tau$, conjugacy class is $\{\tau, \sigma\tau, \sigma^{-1}\tau\}$, the density is $\frac{3}{6} = \frac{1}{2}$. In all, the density is $\frac{1}{6} + \frac{1}{2} = \frac{2}{3}$.

4.3. **Applications to cyclotomic fields.** Let $N \ge 3$ and $N \not\equiv 2 \bmod 4$.

Proposition 4.12. *A prime p is ramified in $\mathbb{Q}(\zeta_N)$ iff $p \mid N$. Write $N = p^e M$ with $(M, p) = 1$. Then the ramification index of p is $p^{e-1}(p-1)$.*

Proof. Since $\Delta_{\mathbb{Q}(\zeta_M)} \mid M^{\varphi(M)}$, $p \nmid \Delta_{\mathbb{Q}(\zeta_M)}$ unramified in $\mathbb{Q}(\zeta_M)$. And by Kummer's theorem, p is totally ramified in $\mathbb{Q}(\zeta_{p^e})$. Assume $p \nmid N$, then the Frob. elements at p is given by

$$\varphi : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\simeq} (\mathbb{Z}/N\mathbb{Z})^\times$$
$$\phi_{\mathfrak{p}|p} \mapsto p.$$

The reason is $\phi_{\mathfrak{p}|p}(x) \equiv x^p \bmod \mathfrak{p}$ for $\forall x \in \mathcal{O}_{\mathbb{Q}(\zeta_N)}$, then $\phi_{\mathfrak{p}|p}(\zeta_N) = \zeta_N^{\varphi(\phi_{\mathfrak{p}|p})} \equiv \zeta_N^p \bmod \mathfrak{p}$. But $x^N - 1$ has no multiple solutions in $\mathbb{F}_p$, it follows that $\varphi(\phi_{\mathfrak{p}|p}) = p$. □

Corollary 4.13. *If $p \nmid N$, $D_p = \langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^\times$, let $f \ge 1$ be the least integer such that $p^f \equiv 1 \pmod N$, then p splits into $\frac{\varphi(N)}{f}$ primes in $\mathbb{Q}(\zeta_N)$ and any $\mathfrak{p} \mid p$ has degree f.*

Theorem 4.14 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_N)$.*

Fact: For $p \ge 3$, put $p^* = (-1)^{\frac{p-1}{2}}p$, then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_p)$.

Theorem 4.15 (Quadratic Reciprocity)**.** *For $\forall p, q \ge 3$ primes, we have*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. It's equivalent to prove $\left(\frac{p^*}{q}\right) = 1 \Leftrightarrow \left(\frac{q}{p}\right) = 1$, this is the same to say $x^2 = p^* \bmod q$ has a solution in $\mathbb{F}_q \Leftrightarrow q$ splits in $\mathbb{Q}(\sqrt{p^*}) \Leftrightarrow q \in (\mathbb{F}_q^\times)^2 \Leftrightarrow \left(\frac{q}{p}\right) = 1$. □

Exercise 4.1. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

4.4. **Exercise sheet 4.**

Exercise 1. *Use the cyclotomic extension $\mathbb{Q}(\zeta_8)$ to show the quadratic reciprocity law for 2: if p is an odd prime, 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 8$.*

Exercise 2. *Let $K = \mathbb{Q}(\zeta_{25})$.*

(1) *Prove that K has a unique subfield M of degree 5 over $\mathbb{Q}$, and find an explicit $\alpha \in K$ such that $M = \mathbb{Q}(\alpha)$.*
(2) *Find the decompositions of the primes $p = 2, 3, 5$ in $M/\mathbb{Q}$, and their corresponding decomposition subfields.*
(3) *Prove that p splits in M if and only if $p \equiv \pm 1, \pm 7 \mod 25$.*

Exercise 3. (1) *Prove that there exists a unique cubic Galois extension $K/\mathbb{Q}$ which is unramified outside 13. (*Hint: use Kronecker–Weber's theorem.*)*
(2) *Find an explicit irreducible cubic polynomial $f(T) \in \mathbb{Q}[T]$ such that $K = \mathbb{Q}[T]/(f(T))$.*

Exercise 4. *In this exercise, we provide an elementary argument to show a weaker version of a special case of Chebotarev density theorem.*

(1) *Let $f(X) \in \mathbb{Z}[X]$ be a non-constant polynomial. Prove that there exist infinitely many primes p such that the image of $f(X)$ in $\mathbb{F}_p[X]$ has a root in $\mathbb{F}_p$.*
Hint: Consider the prime factors of $f(n!a_0)$ for some large n with $a_0 = f(0)$.
(2) *Show that given an integer $N \geqslant 3$, there exist infinitely many primes p such that $p \equiv 1 \pmod{N}$.*
Hint: Apply (1) to the cyclotomic polynomial $\Phi_N(X)$.

Exercise 5. *Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial. For a prime number p, let $n(p)$ be the number of distinct zeros of $(f \mod p)$ in $\mathbb{F}_p$. Prove that the average of $n(p)$, taken over all prime numbers p, is equal to the number of distinct monic irreducible factors of f in $\mathbb{Q}[X]$. (*Hint: Your solution should include a rigorous definition of that average.*)*

5. Lecture 5: August 6

Let K be a number field and

$$\mathrm{Cl}_K = \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}$$

where $\mathcal{I}_{\mathcal{O}_K}$ is the free group generated by fractional ideals of $\mathcal{O}_K$ with $\mathcal{P}_{\mathcal{O}_K}$ the subgroup consisting of principal fractional ideals.

Theorem 5.1. *The abelian group Cl_K is a finite group.*

Remark 5.2. We give some remarks about the history.

- Gauss (1801). For each integer $d \in \mathbb{Z}$, consider the set of integral binary quadratic forms of discriminant d

  $$\mathrm{BQF}_d = \left\{ ax^2 + bxy + cy^2 \middle| d = b^2 - 4ac, a, b, c \in \mathbb{Z} \right\}.$$

  Then the group $\mathrm{SL}_2(\mathbb{Z})$ acts on BQF_d. Gauss showed that

  $$h_d = \#\left(\mathrm{BQF}_d/\mathrm{SL}_2(\mathbb{Z})\right)$$

  is finite. Assume d is the discriminant of a quadratic field K. If K is imaginary, then the $\mathrm{SL}_2(\mathbb{Z})$ orbits of BQF_d is one-to-one corresponding to Cl_K. If K is real, then the orbits is one-to-one corresponding to $\mathrm{Cl}_K^+ = \mathcal{I}_{\mathcal{O}_K}/\mathcal{P}_{\mathcal{O}_K}^+$ where $\mathcal{P}_{\mathcal{O}_K}^+$ consisting of principal fractional ideals (x) with $x \in K^\times$ and totally positive.
- Dedekind (1897) proved the finiteness of class groups for general number fields in his book *Theory of Algebraic Numbers*.
- Minkowski (1901) gave another proof and it is the one we shall discuss later.
- Chevalley gave a proof in the language of adèles, idèles.

The starting point of Minkowski's proof is the following observation. Given $c > 0$, there exist only finitely many nonzero ideals I of $\mathcal{O}_K$ with norm less than c. (Proof: Given an integer $M > 0$ and assume I is an ideal of norm M, then $M\mathcal{O}_K \subset I \subset \mathcal{O}_K$. As $\mathcal{O}_K/M\mathcal{O}_K$ is finite, there are only finite many such ideals) It then suffices to show that there exists a constant $C > 0$, such that for any fractional ideal I, there exists $\alpha \in K^\times$ such that $\alpha I^{-1} \subset \mathcal{O}_K$ and $N(\alpha I^{-1}) \leq C$.

For this, Minkowski introduced the following trick. Let $\sigma_1, \ldots, \sigma_{r_1}$ be (all) distinct embeddings $K \hookrightarrow \mathbb{R}$ and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ be (half of) distinct embeddings $K \hookrightarrow \mathbb{C}$ such that $\overline{\sigma_{r_1+i}} \neq \sigma_{r_1+j}$ for any $1 \leq i, j \leq r_2$. Write $n = r_1 + r_2$. Consider the map

$$\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n, \quad x \mapsto ((\sigma_i(x))_i, (\sigma_{r_1+j}(x))_j) \mapsto ((\sigma_i(x))_i, (\mathrm{Re}\sigma_{r_1+j}(x), \mathrm{Im}\sigma_{r_1+j}(x))_j).$$

Lemma 5.3. *For any fractional ideal I, $\lambda(I)$ is a full lattice in $\mathbb{R}^n$ and*

$$\mathrm{Vol}(\mathbb{R}^n/\lambda(I)) = \frac{\sqrt{|\Delta_K|}N(I)}{2^{r_2}}$$

where Δ_K is the discriminant of K.

Proof. As I is a free $\mathbb{Z}$-module of rank n, we may write $I = \sum_{i=1}^n \mathbb{Z}\alpha_i$. Then $\lambda(I)$ is a full lattice in $\mathbb{R}^n$ if and only if $\lambda(\alpha_1), \ldots, \lambda(\alpha_n)$ are ($\mathbb{R}$-) linearly independent in $\mathbb{R}^n$ if and only if the discriminant of the matrix $(\lambda(\alpha_1), \ldots, \lambda(\alpha_n))$ is nonzero.

Example. Consider the case $r_1 = r_2 = 1$. Then the matrix $(\lambda(\alpha_1), \lambda(\alpha_2), \lambda(\alpha_3))$ equals

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \sigma_1(\alpha_3) \\ \mathrm{Re}\,\sigma_2(\alpha_1) & \mathrm{Re}\,\sigma_2(\alpha_2) & \mathrm{Re}\,\sigma_2(\alpha_3) \\ \mathrm{Im}\,\sigma_2(\alpha_1) & \mathrm{Im}\,\sigma_2(\alpha_2) & \mathrm{Im}\,\sigma_2(\alpha_3) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 1/2i & -1/2i \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \sigma_1(\alpha_3) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \sigma_2(\alpha_3) \\ \overline{\sigma_2}(\alpha_1) & \overline{\sigma_2}(\alpha_2) & \overline{\sigma_2}(\alpha_3) \end{pmatrix}.$$

We have

$$\det(\lambda(\alpha_1), \ldots, \lambda(\alpha_n)) = \frac{1}{2^{r_2}} \det(\sigma_i(\sigma_j)).$$

Recall that

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 = \Delta_K N(I)^2$$

which is nonzero. Therefore, $\det(\lambda(\alpha_1), \ldots, \lambda(\alpha_n)) \neq 0$ and

$$\mathrm{Vol}(\mathbb{R}^n/\lambda(I)) = \left| \det(\lambda(\alpha_1), \ldots, \lambda(\alpha_n)) \right| = \frac{\sqrt{|\Delta_K|}N(I)}{2^{r_2}}$$

□

Lemma 5.4. *Let Λ be a full lattice of $\mathbb{R}^n$. Assume $X \subset \mathbb{R}^n$ be a convex, centrally symmetric, connected region. Assume*

$$\mathrm{Vol}(X) > 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda) = \mathrm{Vol}(\mathbb{R}^n/2\Lambda)$$

then $X \cap \Lambda$ contains a nonzero element.

Proof. As $\mathrm{Vol}(X) > \mathrm{Vol}(\mathbb{R}^n/2\Lambda)$, there exist $x_1, x_2 \in X$, such that $x_1 \neq x_2$ and $x_1 - x_2 \in 2\Lambda$. As X is convex and centrally symmetric, there is a nonzero element

$$\frac{x_1 - x_2}{2} \in \Lambda \cap X.$$

□

Exercise 5.1. Try to generalize this statement to a general locally compact topological group.

Theorem 5.5. *For any fractional ideal I, there exists a nonzero element $\alpha \in I$ such that*

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| < C_K N(I)$$

where the Minkowski constant

$$C_K = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot \sqrt{|\delta_K|}.$$

Proof. For any real $t > 0$, consider the following convex, centrally symmetric, connected region in $\mathbb{R}^n$

$$B_t = \left\{ (y, z \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \Big| \sum_i |y_i| + 2\sum_j |z_j| < t \right\}.$$

Then

$$\mathrm{Vol}(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Note that $\mathrm{Vol}(B_t) > 2^n \mathrm{Vol}(\mathbb{R}^n/\lambda(I))$ if and only if

$$t > t_0 = \left(n! \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|} N(I) \right)^{\frac{1}{n}}.$$

By the previous lemma, if $t > t_0$, there exists a nonzero $\alpha \in B_t \cap \lambda(I)$. Note that

$$\begin{aligned}
\left|N_{K/\mathbb{Q}}(\alpha)\right| &= \prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{j=1}^{r_2} |\sigma_{r_1+j}(\alpha)|^2 \\
&\leq \frac{1}{n^n} \left(\sum_i |\sigma_i(\alpha)| + \sum_j |\sigma_{r_1+j}(\alpha)| \right)^n \\
&\leq \frac{t^n}{n^n}.
\end{aligned}$$

Take the limit $t \to t_0$, we obtain that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq C_K N(I).$$

Finally, note that we may choose α independent on t. We obtain the theorem. □

Example 5.6. Consider $K = \mathbb{Q}(\sqrt{-14})$. Then $n = 2$ with $r_1 = 0$ and $r_2 = 1$. The discriminant $\Delta_K = -56$. The Minkowski constant

$$C_K = \left(\frac{4}{\pi}\right) \cdot \frac{2}{2^2} \cdot \sqrt{56} \approx 4.765 < 5.$$

Therefore, every ideal class contains an ideal of norm less than 4. If I is an ideal with $N(I) = 2$, by the unique factorization law of ideals, we have $I = \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ with $N(\mathfrak{p}) = 2$. Now $(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (2, \sqrt{-14})$. Then $I = \mathfrak{p}_2$ which is not principal (otherwise $\mathfrak{p}_2 = (x + \sqrt{-14}y)$ for some $x, y \in \mathbb{Z}$ which is impossible by taking norm). Similarly, if $N(I) = 3$, then $I = \mathfrak{p}_3$ or $\overline{\mathfrak{p}_3}$ where $\mathfrak{p}_3 = (3, 1 + \sqrt{-14})$ and $\overline{\mathfrak{p}_3} = (3, 1 - \sqrt{-14})$ are both non-principal. Hence, the possible representatives in Cl_K are $\mathcal{O}_K, \mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}_3}$. Finally, we have the relation $\mathfrak{p}_2\mathfrak{p}_3^2 = (2 - \sqrt{-14})$ and we obtain $\mathrm{Cl}_K = \mathbb{Z}/4\mathbb{Z}$.

Note that for any number field K, the Minkowski constant $C_K \geq 1$ (Proof: for any ideal I and nonzero element $\alpha \in I$, we have $1 \leq |N_{K/\mathbb{Q}}(\alpha)| \leq C_K N(I)$. Now take $I = \mathcal{O}_K$). This implies that

$$\sqrt{|\Delta_K|} \geq a_n = \left(\frac{\pi}{4}\right)^{n/2} \cdot \frac{n^n}{n!}.$$

For the family $\{a_n\}_n$, we have $a_2 > 1$, $a_{n+1} > a_n$ and $\lim_{n\to+\infty} a_n = +\infty$.

Corollary 5.7. *(1) For any number field K with $n = r_1 + r_2 \geq 2$, $|\Delta_K| > 1$. (2) If $K/\mathbb{Q}$ is unramified everywhere, then $K = \mathbb{Q}$.*

Theorem 5.8 (Hermite)**.** *Fix $\Delta \in \mathbb{Z}$, then there are only finitely many number fields K with $\Delta_K = \Delta$.*

This theorem is the main ingredient to prove the following one

Theorem 5.9. *Let K be a number field. Let S be a finite set of maximal ideals of $\mathcal{O}_K$. Then for any $n \geq 1$, there are only finitely many field extensions L/K such that $[L : K] = n$ and every prime $\mathfrak{p} \notin S$ is unramified in L.*

Example 5.10. Let $G_K = \mathrm{Gal}(\bar{K}/K) = \varprojlim_{L/K\text{finite}} \mathrm{Gal}(L/K)$. Let p be a prime. Then

$$\dim_{\mathbb{F}_p} \mathrm{Hom}(G_K, \mathbb{F}_p) = +\infty.$$

Let S be a finite set of maximal ideals of $\mathcal{O}_K$ and write $G_{K,S} = \varprojlim_L \mathrm{Gal}_{L/K}$ where L runs over finite field extension of K unramified outside S. Then

$$\dim_{\mathbb{F}_p} \mathrm{Hom}(G_{K,S}, \mathbb{F}_p) < \infty.$$

Idea of proof of Hermite's theorem. We need to show that if Δ_K is bounded, then there exists $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$ while its minimal polynomial has bounded coefficients. For this, we shall choose a convex, centrally symmetric, connected region $X_{\leq} \subset \mathbb{R}^n$ such that $\mathrm{Vol}(X_{\leq}) > 2^n \mathrm{Vol}(\mathbb{R}^n/\lambda(\mathcal{O}_K))$. By previous lemma, there is a nonzero element $\alpha \in X_{\leq} \cap \lambda(\mathcal{O}_K)$.

Consider the case $r_1 > 0$. Let $\underline{C} = (C_i)_{1\leq i\leq r_1+r_2} \in \mathbb{R}_{>0}^{r_1+r_2}$, and consider $X_{\underline{C}}$ of the following form

$$X_{\underline{C}} = \left\{(y, z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \middle| |y_1| \leq C_1, \ldots, |z_j| \leq C_{r_1+j}\right\}.$$

Then

$$\mathrm{Vol}(X_{\underline{C}}) = \prod_{i=1}^{r_1} 2C_1 \prod_{j=1}^{r_2} \pi C_{r_1+j}^2.$$

Take C_i with $C_i < 1$ for $i > 1$ and $\mathrm{Vol}(X_{\underline{C}}) > 2\mathrm{Vol}(\mathbb{R}^n/\lambda(\mathcal{O}_K))$. Let α be a nonzero element in $\lambda(\mathcal{O}_K) \cap X_{\underline{C}}$. Then $|\sigma_i(\alpha)| \leq C_i < 1$ for any $i > 1$. Then

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \left(\prod_{i=2}^{r_1} |\sigma_i(\alpha)| \prod_j |\sigma_{r_1+j}(\alpha)|^2\right).$$

This implies that $\sigma_1(\alpha) > 1$ and $\sigma_j(\alpha) \neq \sigma_1(\alpha)$ for any $j \neq 1$.

The case for $r_1 = 0$ is similar. □

We give further questions for the class group Cl_K.

Firstly, we view Cl_K as a set and focus on the class number $h_K = \#\mathrm{Cl}_K$. Consider the Dedekind zeta function

$$\zeta_K(s) = \sum_{I\subset\mathcal{O}_K} \frac{1}{N(I)^s}, \quad \mathrm{Re}(s) \gg 1$$

which has a meromorphic continuation to the whole s-plane with a simple pole at $s = 1$. The residue satisfies the following class number formula

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|\Delta_K|}}$$

where w_K is the number of roots of unity in K and R_K is the regulator of K (will discuss in the next talk).

Secondly, we view Cl_K as a group. We have the following special case of class field theory.

Theorem 5.11. *For a number field K, there exists a unique finite extension H_K/K, called the Hilbert class field, which is maximal among all finite abelian Galois extensions of K, that are everywhere unramified over K. Moreover, one has an isomorphism*

$$\mathrm{Gal}(H_K/K) \xrightarrow{\sim} \mathrm{Cl}_K$$

such that for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the Frobenius element at $\mathfrak{p}$ corresponds to the ideal class of $\mathfrak{p}$ in Cl_K.

To have an idea why this theorem is extremely useful, we state the following corollary, which seems to be quite hard to be proved without using class field theory.

Corollary 5.12. *If L/K is an extension of number fields such that there exists a prime of K totally ramified in L, then $h_K \mid h_L$.*

Proof. Let H_K and H_L be the Hilbert class fields of K and L. Then $H_K L \subset H_L$. By the assumption, $H_K \cap L = K$. Hence $h_L = [H_L : L] = [H_L : H_K L] h_K$. □

Example 5.13. Let $K = \mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{-14})$ respectively. Then $H_K = \mathbb{Q}(\sqrt{10}, \sqrt{2})$, $\mathbb{Q}(\sqrt{-23}, \alpha)$ and $\mathbb{Q}(\sqrt{-14}, \sqrt{2\sqrt{2}-1})$ respectively. Here, α satisfies $\alpha^3 - \alpha - 1 = 0$.

Question 5.14. For a number field K, how to construct its Hilbert class field H_K explicitly?

This is one of the most important open questions in class field theory nowadays. When K is an imaginary field, this is done by the theory of complex multiplication using j-invariant.

5.1. **Exercise sheet 5.**

Exercise 1. *Some simple applications of Minkowski bound:*

1. *Find the class number of $\mathbb{Q}(\sqrt{m})$ for $m = 5, 6, -5, -13$.*
2. *Show that the ideal class group of $\mathbb{Q}(\sqrt{-23})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$, and find explicitly an ideal that generates the ideal class group.*

Exercise 2. *Let $K = \mathbb{Q}(\sqrt[3]{m})$.*

1. *Show that $\mathbb{Z}[\sqrt[3]{m}]$ is the ring of integers of K if m is square free and m is not congruent to ± 1 modulo 9.*
2. *Prove that $\mathbb{Z}[\sqrt[3]{m}]$ is a principal ideal domain for $m = 3, 5, 6$, and that the class number of $\mathbb{Q}(\sqrt[3]{7})$ is 3.*

Exercise 3. *The aim of this exercise is to prove that the pairs $(17, \pm 70)$ are the only solutions in $\mathbb{Z}^2$ to the equation*

$$y^2 + 13 = x^3. \tag{5.1}$$

We denote $A = \mathbb{Z}[\sqrt{-13}]$, and let $(x, y) \in \mathbb{Z}^2$ be a solution.

1. *Show that no prime ideals of A contain both $y + \sqrt{-13}$ and $y - \sqrt{-13}$.*
2. *Show that there exist $(a, b) \in \mathbb{Z}^2$ such that*

$$y + \sqrt{-13} = (a + b\sqrt{-13})^3.$$

Conclude that $(x, y) = (17, \pm 70)$. (You may use directly the fact that $\mathbb{Q}(\sqrt{-13})$ has class number 2).

Exercise 4. *Let K be a number field, and S be a finite set of maximal ideals of $\mathcal{O}_K$. Fix an algebraic closure $\overline{K}$ of K. Let K^S/K be the maximal subextension of $\overline{K}/K$ that is unramified outside S, and put $G_{K,S} = \mathrm{Gal}(K^S/K)$.*

1. *Prove that for any finite abelian group M, $\mathrm{Hom}(G_{K,S}, M)$ is a finite abelian group as well.*
2. *For $K = \mathbb{Q}$ and $S = \{5, 13, 31, 101\}$, compute the dimension of $\mathrm{Hom}(G_{\mathbb{Q},S}, \mathbb{F}_5)$ over $\mathbb{F}_5$. (*Hint: use Kronecker–Weber's theorem*)*

6. Lecture 6: August 9

6.1. **Variation of the class numbers in families.** We continue our discussion on questions about ideal class groups of number fields. We are interested in the following

Question 6.1. Let K_n be a family of number fields, h_{K_n} be their class numbers. How does h_{K_n} vary as $n \to \infty$?

For example, we can consider the family of quadratic fields $\{\mathbb{Q}(\sqrt{d}) : d \text{ is a square free integer}\}$. Then in this case, we have the following celebrate

Conjecture 6.2 (Gauss)**.** *Let d be a square-free integer, and let h_d denote the class number of $\mathbb{Q}(\sqrt{d})$.*

1 *If $d < 0$, then $h_d \to \infty$ when $d \to -\infty$.*
2 *If $d > 0$, then there exist infinity many real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $h_d = 1$.*

Remark 6.3. Gauss conjecture for imaginary quadratic fields was first proved by Heilbronn in 1934, but for real quadratic fields, Gauss conjecture is still open.

Theorem 6.4 (Littlewood)**.** *Assume GRH, then*

1 *When $d < 0$, then $h_d = O(\sqrt{|d|} \log\log |d|)$,*
2 *When $d > 0$, then $h_d = O(\sqrt{d} \frac{\log\log d}{\log d})$.*

Remark 6.5. These upper bounds are optimal.

Corollary 6.6. *Given an integer $m \geq 1$, there exists only finitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ with $h_d \leq m$.*

In view of this corollary, a natural question is the following

Question 6.7. Given an integer $m \geq 1$, how to determine all $d < 0$ with $h_d = m$?

For $m = 1$, Heegner proved in 1952 that $h_d = 1$ if and only if $d = -1, -2, -3, -7, -11, -43, -67, -163$. Actually, Heegner's solution was not immediately recognized by the mathematical community, because his article contained a gap. Stark and Baker then filled Heegner's gap in 1971, and they also solved the problem for $m = 2$ as well. For general m, this question was finally solved in 1985 by combining the work of by Goldfeld and Gross-Zagier.

Theorem 6.8 (Goldfeld,[1])**.** *Let $d < 0$ be a square-free integer. Suppose that there exists an elliptic curve $E/\mathbb{Q}$ such that $\mathrm{ord}_{s=1} L(E/\mathbb{Q}(\sqrt{d}), s) \geq 4$. Then for any $\epsilon > 0$, there exist an effective constant $C_\epsilon(E) > 0$, such that*

$$h_d > C_\epsilon(E)(\log |d|)^{1-\epsilon}.$$

The key point of this Theorem is that the constant $C_\epsilon(E)$ is explicitly computable in terms of the elliptic curve E. Then Gross-Zagier's work then gives an effective way to produce elliptic curves with large analytic rank over $\mathbb{Q}(\sqrt{d})$. Based on the theorem above, Watkins gives a complete list of $d < 0$ with $h_d = m$ when $m \leq 100$.

Another important family of number fields is provided by $\mathbb{Z}_p$-extensions.

Definition 6.9. Let p be a prime number, K be a number field, a $\mathbb{Z}_p$-extension of K is an infinite Galois extension L/K such that $L = \bigcup_n L_n$, with $L_n \subset L_{n+1}$ and $\mathrm{Gal}(L_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for each n.

The previous example of family of quadratic fields can be considered as a horizontal family in the sense that the degrees of the number fields in the family remain the same but the ramification locus varies, while the $\mathbb{Z}_p$-extensions can be considered as vertical families in which the ramification locus is bounded but the degrees go to the infinity.

Example 6.10. Let $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_n \mathbb{Q}(\zeta_{p^n})$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$. Via the p-adic logarithm map, we have

$$\mathbb{Z}_p^\times \simeq \begin{cases} \mu_{p-1} \times \mathbb{Z}_p, & \text{if } p > 2, \\ \mu_2 \times \mathbb{Z}_2, & \text{if } p = 2. \end{cases}$$

It follows that $\mathbb{Q}(\zeta_p^\infty)$ contains a (unique) subfield $\mathbb{Q}_\infty$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$, called the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For general number field K, define $K_\infty = K\mathbb{Q}_\infty$, called the cyclotomic $\mathbb{Z}_p$-extension of K.

Theorem 6.11 (Iwasawa). *Let K_∞/K be a $\mathbb{Z}_p$-extension of number field K, A_n be the p-Sylow-subgroup of ideal class group of K_n. Then there exist integers $\mu, \lambda \geq 0$ and c such that for $n \gg 0$,*

$$\log_p(\#A_n) = \mu p^n + \lambda n + c.$$

Conjecture 6.12 (Conjecture by Iwasawa). *Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension of a number field K. Then we have $\mu(K_\infty/K) = 0$.*

Theorem 6.13 (Ferrero-Washington). *If $K/\mathbb{Q}$ is abelian, then Iwasawa's conjecture is true.*

Remark 6.14. There exists $\mathbb{Z}_p$-extension K_∞/K with μ-invariant arbitrarily large.

The key to prove Theorem 6.11 is to consider the natural actions of $\Gamma := \mathrm{Gal}(K_\infty/K)$ on A_n. We put

$$\mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma_n],$$

where $\Gamma_n = \mathrm{Gal}(K_n/K)$. Then it is not hard to see that if $\gamma \in \Gamma \cong \mathbb{Z}_p$ is a topological generator, then one has an isomorphism

$$\mathbb{Z}_p[[T]] \xrightarrow{\sim} \mathbb{Z}_p[\Gamma]$$

sending T to $[\gamma] - 1$. We put $A := \varprojlim_n A_n$, where the transition maps are induced by relative norms of fractional ideals. Since A_n can be viewed as an $\mathbb{Z}_p[\Gamma_n]$-module, A is a $\mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma_n]$-module. A key step to proving Theorem 6.11 is the following result

Proposition 6.15. *A is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module.*

Note that $\mathbb{Z}_p[[\Gamma]]$ is a regular local ring of dimension 2. There is a satisfactory classification for finitely generated modules over such rings, according to which a finitely generated torsion module M over $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ is, modulo the subcategory of $\mathbb{Z}_p[[T]]$-modules of finite length, equivalent to a module of the form $\mathbb{Z}_p[[T]]/(p^\mu g(T))$, where $g(T)$ is a monic polynomial of degree λ with coefficients in $\mathbb{Z}_p$. Theorem 6.11 then follows easily from this description.

For the $\mathbb{Z}_p[[\Gamma]]$-module A, the corresponding ideal $\mathrm{Char}_{\mathbb{Z}_p[[\Gamma]]}(A) := (p^\mu g(T))$ is usually called the characteristic ideal of A. It is intimately related to the L-functions of the Galois group of K. Roughly speaking, one has the following conjecture:

Conjecture 6.16 (Iwasawa Main Conjecture).

$$\mathrm{Char}_{\mathbb{Z}_p[[\Gamma]]}(A) = \text{“}p\text{-adic } L\text{-functions”}.$$

6.2. **Dirichlet's unit theorem.** Let K be a number field, $\mathcal{O}_K^\times$ be its unit group. Then we observed that

- Let $\alpha \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K^\times$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$,
- $(\mathcal{O}_K^\times)_{\mathrm{tor}} = \{\alpha \in \mathcal{O}_K | \alpha^m = 1, \text{for some } m\} = \{\alpha \in K | \alpha^m = 1, \text{for some } m\} =: W_K$.

Theorem 6.17 (Dirichlet, 1846). *There exists a free abelian subgroup $V \subset \mathcal{O}_K^\times$ of rank $r_1 + r_2 - 1$, such that*

$$\mathcal{O}_K^\times = W_K \times V \simeq \mathbb{Z}/w_K\mathbb{Z} \times \mathbb{Z}^{r_1+r_2-1},$$

where $w_K := \#W_K$.

Corollary 6.18. *Let R be a commutative ring, which is finitely generated as a $\mathbb{Z}$-module. Then $R^\times$ is a finitely generated abelian group.*

Proof. Let J be the nilpotent radical of R, and $R_0 = R/J$. Then the kernel of the map $R^\times \to R_0^\times$ is $1 + J$, which is a finitely generated abelian group since J is a finitely generated $\mathbb{Z}$-module. To prove the corollary, it is suffice to show that $R_0^\times$ is finitely generated. Up to replacing R by R_0, we may assume that R is reduced. Let $R_{\mathrm{tors}} \subset R$ be the torsion submodule of R. Then $(R_{\mathrm{tors}})^\times$ is finite, and torsion-free. In this case, $R \otimes \mathbb{Q} \simeq \prod_i K_i$, a finite direct product of number fields, since R is integral over $\mathbb{Z}$, we have $R \subset \prod_i \mathcal{O}_{K_i}$, then $R^\times \subset \prod_i \mathcal{O}_{K_i}^\times$, hence it is finitely generated. □

Proof of theorem. First we notice that

- If X is a compact topological space and Γ be a closed discrete group in X, then Γ must be finite,
- Let $f : X \to Y$ be a continuous map between topological spaces, C be a compact subset of X, then $f(C)$ is also compact.

Let $\lambda : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} =: V$, V is a $\mathbb{R}$-algebra, and $V^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. For any element $(y_i, z_j) \in V^\times$, define norm to be $N(y_i, z_j) = \prod_i |y_i| \prod_j |z_j|^2$. Then for any $\alpha \in \mathcal{O}_K$, $N(\lambda(\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$. So the image of $\mathcal{O}_K^\times$ under the map λ is contained in the subgroup $G := \{(y_i, z_j) \in V^\times | N(y_i, z_j) = 1\}$. So $\lambda : \mathcal{O}_K^\times \hookrightarrow G$ is a group homomorphism. Moreover, $\lambda(\mathcal{O}_K^\times)$ is discrete in G because $\lambda(\mathcal{O}_K^\times)$ is discrete in V.

Proposition 6.19. *$G/\lambda(\mathcal{O}_K^\times)$ is compact.*

Proof. By Minkowski's lemma, we fix $C \subset V$ a compact, convex, centrally symmetric, connected subset with volume $\mu(C) > 2^n \mathrm{Vol}(V/\lambda(\mathcal{O}_K))$. Then $C \cap \lambda(\mathcal{O}_K)$ contains a non-zero element $\alpha \in \lambda(\mathcal{O}_K)$. For any $g \in G$, we have $\mu(gC) = N(g)\mu(C) = \mu(C)$, so there is a non-zero element $\alpha_g \in gC \cap \lambda(\mathcal{O}_K)$. Note that

$$\#\mathcal{O}_K/\alpha_g\mathcal{O}_K = N(\alpha_g) \in N(gC) \cap \mathbb{Z},$$

and $N(gC) \cap \mathbb{Z} = N(C) \cap \mathbb{Z}$ is both compact and discrete, hence is finite. However, there are only finitely many ideals of $\mathcal{O}_K$ with bounded norm. So there exist finitely many elements $\alpha_1, ..., \alpha_k \in \mathcal{O}_K - \{0\}$, such that for any $g \in G$, $(\alpha_g) = (\alpha_i)$ for some i, namely $\alpha_g \in \alpha_i \mathcal{O}_K^\times$. Then for any $g \in G$, $\alpha_g \in gC \Leftrightarrow g^{-1} \in \alpha_g^{-1} C \subset \alpha_i^{-1} \mathcal{O}_K^\times C$, therefore $g \in \cup_{i=1}^k \alpha_i^{-1} \mathcal{O}_K^\times C$, namely the image of $\cup_{i=1}^k \alpha_i^{-1} C$ cover $G/\lambda(\mathcal{O}_K^\times)$, which implies that $G/\lambda(\mathcal{O}_K^\times)$ is compact. □

$$\begin{array}{ccccc} \mathcal{O}_K^\times & \xhookrightarrow{\lambda} & G & \xrightarrow{\log} & H = \{x \in \mathbb{R}^{r_1+r_2} | \sum_i x_i = 0\} \\ \downarrow & & \downarrow & & \downarrow \\ K^\times & \xhookrightarrow{\lambda} & V^\times & \xrightarrow{\log} & \mathbb{R}^{r_1+r_2} \end{array}$$

Denote $\ell_K = \log \circ \lambda : \mathcal{O}_K^\times \to H$, clearly

- $\log(G) = H$,
- $\mathrm{Ker}(\ell_K) = (\mathcal{O}_K^\times)_{\mathrm{tor}}$.

Using the above proposition, $\lambda(\mathcal{O}_K^\times)$ is discrete and co-compact in G, so $\ell_K(\mathcal{O}_K^\times)$ is discrete and co-compact in H. Notice that a discrete and co-compact subgroup Γ in $\mathbb{R}^n$ must be a full lattice, in particular, $\mathrm{rank}_{\mathbb{Z}}(\Gamma) = n$. Therefore

$$\mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_K^\times) = r_1 + r_2 - 1.$$ □

Definition 6.20. Let $\epsilon_1, \cdots, \epsilon_r \in \mathcal{O}_K^\times$ be a basis in $\mathcal{O}_K^\times / W_K$, where $r = r_1 + r_2 - 1$. Let $\vec{n} = \frac{1}{r_1+r_2}(1, 1, \cdots, 1) \in \mathbb{R}^{r_1+r_2} \setminus H$, we define the regulator of K to be $R_K = |\det(\vec{n}, \ell_K(\epsilon_1), \cdots, \ell_K(\epsilon_r))|$.

Example 6.21.

1. $r_1 + r_2 - 1 = 0$ iff $r_1 = 0, r_2 = 1$ or $r_1 = 1, r_2 = 0$, namely $K = \mathbb{Q}$ or imaginary quadratic field, and for negative square-free d, $K = \mathbb{Q}(\sqrt{d})$,
$$\mathcal{O}_K^\times \begin{cases} \{\pm 1 \pm \sqrt{-1}\}, & \text{if } d = -1, \\ \{\pm\zeta_3^{\pm}, \pm 1\}, & \text{if } d = -3 \\ \{\pm 1\}, & \text{otherwise} \end{cases}$$
2. $r_1 + r_2 - 1 = 1$ iff $r_1 = 2, r_2 = 0$ or $r_! = 1, r_2 = 1$ or $r_1 = 0, r_2 = 2$. For example, real quadratic fields and pure cubic fields $\mathbb{Q}(\sqrt[3]{m})$. In this case, $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \epsilon^{\mathbb{Z}}$, the generator ϵ is called the fundamental unit of K.

To compute the fundamental unit, for real quadratic case, it is equivalent to solve a Pell equation, then we can use continuous fraction. For cubic case, we have the following theorem.

Theorem 6.22 (Artin)**.** *Suppose $[K : \mathbb{Q}] = 3$ and $r_1 = 1$, fix an embedding $K \hookrightarrow \mathbb{R}$. If $v \in \mathcal{O}_K^\times$ with $v > 1$, then*

$$|\Delta_K| < 4v^3 + 24.$$

Corollary 6.23. *For any $u \in \mathcal{O}_K^\times$, if $4u^{3/m} + 24 \leq |\Delta_K|$ for an integer $m \geq 2$. Then $u = \epsilon^k$ for some $1 \leq k < m$. In particular, if $m = 2$, then u must be the fundamental unit.*

Example 6.24. $K = \mathbb{Q}(\sqrt[3]{2})$, we have $\epsilon = \sqrt[3]{2} - 1$.

6.3. **Exercise sheet 6.**

Exercise 1. *The aim of this exercise is to give a proof of the finiteness of the ideal class group of a number field K following Dedekind.*

As explained in class, we have to show that there exists a constant C_K, which depends only on K, such that for all ideal $I \subseteq \mathcal{O}_K$, there exists $\alpha \in I\backslash\{0\}$ such that $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant C_K \mathrm{N}(I)$. Let $n = [K : \mathbb{Q}]$. We choose an integral basis $(\alpha_1, \cdots, \alpha_n)$ for $\mathcal{O}_K$.

(1) *Prove that there exist integers $x_i \in [-\sqrt[n]{\mathrm{N}(I)}, \sqrt[n]{\mathrm{N}(I)}]$ with $1 \leqslant i \leqslant n$ such that not all x_i are zero and $\alpha := \sum_i x_i\alpha_i \in I$.*
(2) *Prove that there exists a constant $C_K > 0$ such that $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leqslant C_K \mathrm{N}(I)$.*

Exercise 2. *Let $K = \mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field, where p is an* odd *prime, and $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Denote respectively by U_K and U_{K^+} the group of units in K and K^+.*

(1) *Let u be a unit of K. Show that $u/\bar{u}$ is a root of unity.*
(2) *Let u be as in (1), write $u/\bar{u} = \pm\zeta_p^k$ for some $k \in \mathbb{Z}$. Show that it is impossible to have $-$ sign.*
(3) *Show that $U_K = U_{K^+} \times \langle\zeta_p\rangle$, i.e. every unit u in K writes uniquely as $u = \varepsilon \cdot \zeta_p^k$ with $\varepsilon \in U_{K^+}$. (Hint: Consider the map $\phi : U_K \to U_{K^+}$ given by $u \mapsto u/\bar{u}$.)*

Exercise 3. *Let K be a number field. We say an element $\alpha \in K$ is* totally positive *if $\sigma(\alpha) > 0$ for every real embedding $\sigma : K \hookrightarrow \mathbb{R}$. Denote by $\mathcal{I}_K$ the group of fractional ideals of K, and by $\mathcal{P}_K^+$ the subgroup of principal ideals generated by a totally positive element. Define the strict ideal class group of K as*

$$\mathrm{Cl}_K^+ = \mathcal{I}_K/\mathcal{P}_K^+.$$

(1) *Show that the kernel of the natural surjection $f : \mathrm{Cl}_K^+ \to \mathrm{Cl}_K$ has at most 2^{r_1-1} elements, where r_1 denotes the number of real embeddings of K. Conclude that Cl_K^+ is a finite abelian group.*
(2) *Assume that K is real quadratic. Let u denote the fundamental unit of K. Prove that $\mathrm{Ker}(f)$ has order 2 if $\mathrm{N}_{K/\mathbb{Q}}(u) = 1$, and $\mathrm{Ker}(f) = \{1\}$ if $\mathrm{N}_{K/\mathbb{Q}}(u) = -1$.*

Exercise 4. *Let K be a real quadratic field with discriminant d_K. Then fundamental unit of K is defined to be the unique unit ε of K such that $\varepsilon > 1$ and $U_K = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$.*

(1) *Let $u > 1$ be a unit of K. Show that $u \geqslant (\sqrt{d_K} + \sqrt{d_K - 4})/2$ if $\mathrm{N}_{K/\mathbb{Q}}(u) = -1$, and $u \geqslant (\sqrt{d_K} + \sqrt{d_K + 4})/2$ if $\mathrm{N}_{K/\mathbb{Q}}(u) = 1$. (Hint: consider $\mathrm{Disc}_{K/\mathbb{Q}}(1, u)$ and use the equality that $\mathrm{Disc}_{K/\mathbb{Q}}(1, u) \geqslant d_K$.)*
(2) *Show that if d_K is divisible by a prime number p with $p \equiv 3 \mod 4$, then K does not contain any units u with $\mathrm{N}_{K/\mathbb{Q}}(u) = -1$.*
(3) *Find the fundamental unit of $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$.*

References

[1] Goldfeld, Dorian *Gauss' Class Number Problem For Imaginary Quadratic Fields.*