Algebraic Number Theory

Jim Brown
(Notes by Shuai Wei)

September 18, 2023

Contents

Chapter 1

Field Theory

1.1 Definitions

Definition 1.1. A field $\mathcal{F}$ is *algebraically closed* if for any $f \in \mathcal{F}[x]$, f has a root in $\mathcal{F}$, or equivalently, every polynomial in $\mathcal{F}[x]$ splits over $\mathcal{F}$.

Definition 1.2. We say an extension $\mathcal{K}/\mathcal{F}$ is *separable* if $\mathcal{K}$ is algebraic over $\mathcal{F}$ and there exists $[\mathcal{K} : \mathcal{F}]$ distinct embeddings (field homomorphism and $\mathcal{F}$-linear) $\mathcal{K} \hookrightarrow \overline{\mathcal{F}}$.

Remark. If $\sigma : \mathcal{K} \to \overline{\mathcal{F}}$ is an embedding and $\alpha \in \overline{\mathcal{F}}$ is a root of $f \in \mathcal{F}[x]$, then $\sigma(\alpha)$ is a root of f since σ is a field homomorphism and $\mathcal{F}$-linear.

Example 1.3. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable since we have 2 distinct embeddings $\mathbb{Q}(\sqrt{2}) \hookrightarrow \overline{\mathbb{Q}}$ given by $\sigma_1 : \sqrt{2} \mapsto \sqrt{2}$ and $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$. Note that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$.

Example 1.4. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is separable since we have 3 distinct embeddings $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbb{Q}}$ given by $\sigma_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sigma_2 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3$ and $\sigma_3 : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3^2$. Since $\sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2 \notin \mathbb{Q}(\sqrt[3]{2})$, we have $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$ and then it is not a *Galois extension.*

Fact 1.5. (a) $\mathcal{F}(\alpha)/\mathcal{F}$ is separable if and only if m_α has no repeated roots over $\overline{\mathcal{F}}$.

(b) Any extension $\mathcal{K}/\mathcal{F}$ with $\mathcal{F}$ *perfect* is separable.

(c) If $\mathcal{F} \subseteq \mathcal{K} \subseteq \mathcal{L}$, then $\mathcal{L}/\mathcal{F}$ is separable if and only if $\mathcal{L}/\mathcal{K}$ and $\mathcal{K}/\mathcal{F}$ are separable.

(d) $[\mathcal{F}(\alpha) : \mathcal{F}] = \deg(m_\alpha)$.

Example 1.6. In $\mathbb{F}_p$, $f(x) = x^p - a$ has repeated roots since $f'(x) = px^{p-1} = 0$ for any $x \in \mathbb{F}_p$. Hence $\mathbb{F}_p(\sqrt[p]{a}\xi_p)/\mathbb{F}_p$ is not separable.

Lemma 1.7 (Primitive element theorem)**.** If $\mathcal{K}/\mathcal{F}$ is finite and separable, then $\mathcal{K} = \mathcal{F}(\theta)$.

Proof. We assume that $\mathcal{F}$ and $\mathcal{K}$ are infinite. The finite case is left to the reader. It is enough to show $\mathcal{F}(\alpha, \beta)$ can be written as $\mathcal{F}(\theta)$ for some $\theta \in \mathcal{K}$. Let m_α and m_β be the minimal polynomial of α and β over $\mathcal{F}$. Let $\alpha_1, \ldots, \alpha_r$ be the roots of m_α and $\beta_1, \ldots, \beta_s$ be the roots of m_β over $\overline{\mathcal{F}}$. Since $\mathcal{F}$ is infinite, we can choose $c \in \mathcal{F}$ such that $\frac{\alpha_i - \alpha}{\beta_j - \beta} \neq -c$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$. Hence

$\alpha+c(\beta-\beta_j) \neq \alpha_i$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$. Let $\theta = \alpha+c\beta$ and $f(x) = m_\alpha(\theta-cx) \in \mathcal{F}(\theta)[x]$. Observe $f(\beta) = m_\alpha(\theta - c\beta) = m_\alpha(\alpha) = 0$, i.e., β is a root of f. Since $\alpha + c(\beta - \beta_j) \neq \alpha_i$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$, we have $f(\beta_j) = m_\alpha(\theta-c\beta_j) = m_\alpha(\alpha+c(\beta-\beta_j)) \neq 0$ for $j = 2, \ldots, s$. This implies f and m_β only have one root β in common by our choice of c. Let h be the minimal polynomial of β over $\mathcal{F}(\theta)$, then we must have $h \mid m_\beta$ and $h \mid f$. Since $\mathcal{K}/\mathcal{F}$ is separable, we have $\mathcal{F}(\beta)/\mathcal{F}$ is separable. Hence m_β has no repeated roots and then $h(x) = u(x-\beta) \in \mathcal{F}(\theta)[x]$ for some $u \in \mathcal{F}(\theta)^\times$. Hence $\beta \in \mathcal{F}(\theta)$ and thus $\mathcal{F}(\beta) \subseteq \mathcal{F}(\theta)$. Since $\alpha = \theta - c\beta \in \mathcal{F}(\theta)$, $\mathcal{F}(\alpha, \beta) \subseteq \mathcal{F}(\theta)$. Also, since $\theta = \alpha + c\beta \in \mathcal{F}(\alpha, \beta)$, $\mathcal{F}(\theta) \subseteq \mathcal{F}(\alpha, \beta)$. □

Example 1.8. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. The point is

$$\sqrt{3} = \frac{(\sqrt{2} + \sqrt{3}) + (\sqrt{3} - \sqrt{2})}{2} = \frac{\sqrt{2} + \sqrt{3}}{2} + \frac{1}{2(\sqrt{2} + \sqrt{3})} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$ □

Definition 1.9. An *(algebraical) number field* is a finite field extension of $\mathbb{Q}$.

Example 1.10. The fields $\mathbb{C}$ and $\mathbb{R}$ are not number fields.

Fact 1.11. Since all number fields $\mathcal{K}/\mathbb{Q}$ are separable, there are $[\mathcal{K} : \mathbb{Q}]$ distinct embbedings $\sigma : \mathcal{K} \hookrightarrow \overline{\mathbb{Q}}$. Let $\mathcal{K} := \mathbb{Q}(\alpha)$ and $f \in \mathbb{Q}[x]$ the minimal polynomial of α of degree n. Then $\mathcal{K} = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle f\rangle = \mathbb{Q}(x + \langle f\rangle)$. Let $\gamma : \mathbb{Q}[x] \to \mathbb{Q}[x]/\langle f\rangle$ be the natural projection. Then $f(x + \langle f\rangle) = f(\gamma(x)) = \gamma(f(x)) = f + \langle f\rangle = \langle f\rangle = 0$ in $\mathcal{K} \cong \mathbb{Q}[x]/\langle f\rangle$. Since $\mathrm{char}(\mathbb{Q}) = 0$ and f is irreducible with degree $n \geqslant 2$, we have f has n distinct roots $\alpha_1, \ldots, \alpha_n$ in $\overline{\mathbb{Q}}$. Then we get n distinct embeddings $\sigma_i : \mathcal{K} \cong \mathbb{Q}[x]/\langle f\rangle \hookrightarrow \overline{\mathbb{Q}}$ given by $x + \langle f\rangle \mapsto \alpha_i$ ($\mathbb{Q}(\alpha_1) \cong \cdots \cong \mathbb{Q}(\alpha_n)$). There can't be more since $\sigma(x + \langle f\rangle)$ has to be a root of f for any embedding σ.

Definition 1.12. Let σ be an embedding $\sigma : \mathcal{K} \hookrightarrow \overline{\mathbb{Q}}$. We say σ is a *real embedding* if $\sigma(\mathcal{K}) \subseteq \mathbb{R}$. If $\sigma(\mathcal{K}) \subseteq \mathbb{C}$, we say σ is a *complex embedding*. If σ is a complex embedding, so is $\overline{\sigma}$, and hence complex embeddings come in pair. For example, $\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3$ and $\overline{\sigma} : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3^2$.

1.2 Trace, Norm and Determinant

Let $\mathcal{L}/\mathcal{K}$ be a finite field extension of degree n, $\sigma_1, \ldots, \sigma_n$ the distinct embeddings of $\mathcal{L} \hookrightarrow \overline{\mathcal{K}}$ and $\alpha_1, \ldots, \alpha_n$ a basis of $\mathcal{L}/\mathcal{K}$.

Definition 1.13. Let $x \in \mathcal{L} \cong \mathcal{K}^n$. For any $x \in \mathcal{K}$, we have a $\mathcal{K}$-linear transform $f_x : \mathcal{L} \to \mathcal{L}$ given by $y \mapsto xy$. The *trace* of x from $\mathcal{L}$ to $\mathcal{K}$ is the trace of this map and we denote this by $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x)$. The *norm* of x from $\mathcal{L}$ to $\mathcal{K}$ is the determinant of this map and we denote this by $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(x)$.

Example 1.14. Let $\mathcal{L} = \mathbb{Q}(\sqrt{3})$ and $\mathcal{K} = \mathbb{Q}$. Let $x = 6 + 7\sqrt{3}$ and $f_x : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$. Let $\mathcal{B} = \{1, \sqrt{3}\}$. Then $[f_x]_\mathcal{B} = \begin{bmatrix} 6 & 21 \\ 7 & 6 \end{bmatrix}$. Hence $\mathrm{Tr}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(6 + 7\sqrt{3}) = 12$ and $\mathrm{N}_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}(6 + 7\sqrt{3}) = -111$.

Definition 1.15. Let $c_x(t)$ be the characteristic polynomial of $f_x : \mathcal{L} \to \mathcal{L}$. Write

$$c_x(t) = \det(tI_n - A_{f_x}) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in \mathcal{K}[t].$$

Then $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x) = a_1$ and $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(x) = a_n$ and so

$$c_x(t) = \det(tI_n - A_{f_x}) = t^n - \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x)t^{n-1} + \cdots + (-1)^n \mathrm{N}_{\mathcal{L}/\mathcal{K}}(x) \in \mathcal{K}[t].$$

Remark. Note that $f_{x_1+x_2} = f_{x_1} + f_{x_2}$ and $f_{x_1x_2} = f_{x_1}f_{x_2}$.

Theorem 1.16. *Let $\sigma : \mathcal{L} \hookrightarrow \overline{\mathcal{K}}$ vary over the n distinct $\mathcal{K}$-embeddings of $\mathcal{L}$ into $\overline{\mathcal{K}}$. Fix $x \in \mathcal{L}$, then $c_x(t) = \prod_\sigma (t - \sigma(x))$, $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x) = \sum_\sigma \sigma(x)$ and $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(x) = \prod_\sigma \sigma(x)$.*

Proof. It is enough to show $c_x(t) = \prod_\sigma (t - \sigma(x))$. Note $\mathcal{K} \subseteq \mathcal{K}(x) \subseteq \mathcal{L}$. Write $m_x(t) = t^m + a_1t^{m-1} + \cdots + a_m$, with $m = [\mathcal{K}(x) : \mathcal{K}]$. We claim that $c_x(t) = (m_x(t))^d$ with $d = [\mathcal{L} : \mathcal{K}(x)] = \frac{[\mathcal{L}:\mathcal{K}]}{[\mathcal{K}(x):\mathcal{K}]} = \frac{n}{m}$. We have $\mathcal{B} = \{1, x, \ldots, x^{m-1}\}$ is a basis for $\mathcal{K}(x)/\mathcal{K}$. Since $0 = m_x(x) = x^m + a_1x^{m-1} + \cdots + a_m$, we have $x \cdot x^{m-1} = x^m = -a_m - a_{m-1}x - \cdots - a_1x^{m-1}$. Hence $[f_x]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_m \\ 1 & 0 & \cdots & 0 & -a_{m-1} \\ 0 & 1 & \cdots & 0 & -a_{m-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{bmatrix}$, which is the companion matrix A_{f_x} of m_x. Hence the characteristic function of $f_x|_{\mathcal{K}(x)} : \mathcal{K}(x) \to \mathcal{K}(x)$ is m_x. Let $\{\alpha_1, \ldots, \alpha_d\}$ be a basis of $\mathcal{L}/\mathcal{K}(x)$. Then $\mathcal{C} = \{\alpha_1, \alpha_1x, \ldots, \alpha_1x^{m-1}, \ldots, \alpha_d, \alpha_dx, \ldots, \alpha_dx^{m-1}\}$ is a basis for $\mathcal{L}/\mathcal{K}$. Hence $[f_x]_{\mathcal{C}} = \begin{bmatrix} A_{f_x} & 0 & \cdots & 0 \\ 0 & A_{f_x} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & A_{f_x} \end{bmatrix}$. Hence the characteristic polynomial of $f_x : \mathcal{L} \to \mathcal{L}$ is $c_x = m_x^d$. Since $\mathcal{L}/\mathcal{K}$ is separable and $x \in \mathcal{L}$, $\mathcal{K}(x)/\mathcal{K}$ is separable and then m_x has m distinct roots $x_1, \ldots, x_m \in \overline{\mathcal{K}}$. For $i = 1, \ldots, m$ define an emebedding $\sigma_i : \mathcal{K}(x) \hookrightarrow \overline{\mathcal{K}}$ given by $x \mapsto x_i$, we then lift σ_i to $\sigma_i' : \mathcal{L} \to \overline{\mathcal{K}}$ with $\sigma'|_{\mathcal{K}(x)} = \sigma$ and the number of liftings is $[\mathcal{L} : \mathcal{K}(x)] = d$. Then $m_x(t) = \prod_{i=1}^m (t - \sigma_i(x))$ and σ_i's are all the n embeddings $\mathcal{L} \hookrightarrow \overline{\mathcal{K}}$. For $\sigma, \tau \in \mathrm{Hom}_{\mathcal{K}}(\mathcal{L}, \overline{\mathcal{K}})$ 1-1, define an equivalent relation $\sigma \sim \tau$ if and only if $\sigma(x) = \tau(x)$. Then

$$c_x(t) = m_x(t)^d = \prod_{j=1}^m (t - \sigma_j(x))^d = \prod_{j=1}^m \prod_{\sigma \sim \sigma_j} (t - \sigma(x)) = \prod_\sigma (t - \sigma(x)). \qquad \square$$

Corollary 1.17. $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}} : \mathcal{L} \to K$ and $\mathrm{N}_{\mathcal{L}/\mathcal{K}} : L^\times \to \mathcal{K}^\times$ are $\mathcal{K}$-linear transforms.

Corollary 1.18. Let $x \in \mathcal{L}$ then $x \mid \mathrm{N}_{\mathcal{L}/\mathcal{K}}(x)$.

Proof. Note that the identity map belongs to the $\mathcal{K}$-embeddings of $\mathcal{L}$. $\square$

Corollary 1.19. Let $\mathcal{L}/\mathcal{K}$ be Galois. If $x \in \mathcal{L}$, then $\mathrm{Tr}(x) \in \mathcal{K}$.

Proof. Let $\tau \in \mathrm{Gal}(\mathcal{L}/\mathcal{K})$, then since $\{\sigma \mid \sigma \text{ is an embedding } \mathcal{L} \hookrightarrow \overline{\mathcal{K}}\}$ is a finite group,

$$\tau(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x)) = \tau\left(\sum_\sigma \sigma(x)\right) = \sum_\sigma \tau(\sigma(x)) = \sum_\sigma \sigma(x) = \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x).$$

Since the fixed field of $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$ is $\mathcal{K}$, we have $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(x) \in \mathcal{K}$. $\square$

Corollary 1.20. If $\mathcal{K}(\alpha)/\mathcal{K}$ is separable and $x \in \mathcal{K}(\alpha) \smallsetminus \mathcal{K}$, then $c_x = m_x$.

Example 1.21. Consider $\mathcal{L} = \mathbb{Q}(\sqrt{d})$ and $\mathcal{K} = \mathbb{Q}$, where d is square free. For $x = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$,

$$\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d}) + \sigma_2(a + b\sqrt{d}) = a + b\sqrt{d} + a - b\sqrt{d} = 2a$$

and

$$\mathrm{N}_{\mathcal{L}/\mathcal{K}}(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d})\sigma_2(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Corollary 1.22. Let $\mathcal{F} \subseteq \mathcal{K} \subseteq \mathcal{L}$ be a tower of finite field extension. Then $\mathrm{Tr}_{\mathcal{K}/\mathcal{F}} \circ \mathrm{Tr}_{\mathcal{L}/\mathcal{K}} = \mathrm{Tr}_{\mathcal{L}/\mathcal{F}}$ and $\mathrm{N}_{\mathcal{K}/\mathcal{F}} \circ \mathrm{N}_{\mathcal{L}/\mathcal{K}} = \mathrm{N}_{\mathcal{L}/\mathcal{F}}$.

Definition 1.23. The *determinant* of $\{\alpha_1, \ldots, \alpha_n\}$ is defined as

$$d(\alpha_1, \ldots, \alpha_n) = \left(\det(\sigma_i(\alpha_j))\right)^2.$$

Example 1.24. Let $\mathcal{K} = \mathbb{Q}(\sqrt{3})$, $\mathcal{F} = \mathbb{Q}$ and σ_1, σ_2 distinct embeddings with $\sigma_1 = 1$. Let $\mathcal{B} = \{1, \sqrt{3}\}$, then $\sigma_1(1) = 1$, $\sigma_1(\sqrt{3}) = \sqrt{3}$, $\sigma_2(1) = 1$, $\sigma_2(\sqrt{3}) = -\sqrt{3}$, $m_{\sqrt{3}}(x) = x^2 - 3$, $\mathrm{disc}(m_{\sqrt{3}}) = 12$, and $d(1, \sqrt{3}) = \det \begin{bmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{bmatrix}^2 = 12$.

Fact 1.25.

$$\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Theorem 1.26. *The matrix* $\left(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j)\right)$ *is the product of the matrix* ${}^t(\sigma_k(\alpha_i))$ *and* $(\sigma_k(\alpha_i))$. *This gives* $d(\alpha_1, \ldots, \alpha_n) = \det\left((\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j))\right)$.

Proof. It follows from $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$. □

Remark. More generally, let $B \supseteq A$ be rings, and assume $B \cong A^n$, i.e., B is a free A-module of dimension n. Let $\beta_1, \ldots, \beta_m$ be elements of B. We define their *discriminant* to be

$$d(\beta_1, \ldots, \beta_m) = \det\left((\mathrm{Tr}_{B/A}(\beta_i\beta_j))\right).$$

Example 1.27. Let $\mathcal{L} = \mathbb{Q}(\xi_3)$ and $\mathcal{K} = \mathbb{Q}$. Then

$$d(1, \xi_3) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\xi_3) \\ \mathrm{Tr}(\xi_3) & \mathrm{Tr}(\xi_3^2) \end{bmatrix} = \begin{bmatrix} 2 & \xi_3 + \xi_3^2 \\ \xi_3 + \xi_3^2 & \mathrm{Tr}(-1 - \xi_3) \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & -2 - (-1) \end{bmatrix} = -3.$$

Definition 1.28. Define $\psi : \mathcal{L} \times \mathcal{L} \to \mathcal{K}$ by $(x, y) \mapsto \mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(xy)$, which is a (non-degenerate) symmetric bilinear form on $\mathcal{L}$ regarded as a vector space over $\mathcal{K}$, and the discriminant of this form is called the *discriminant* of $\mathcal{L}/\mathcal{K}$.

Remark. Let $M \in \mathrm{Mat}_n(\mathcal{K})$ be nonsingular and $(\gamma_1, \ldots, \gamma_n) = (\alpha_1, \ldots, \alpha_n)M$. Then we have $\left(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\gamma_i\gamma_j)\right) = {}^tM \left(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j)\right) M$. Hence $d(\gamma_1, \ldots, \gamma_n) = (\det(M))^2 d(\alpha_1, \ldots, \alpha_n)$.

Theorem 1.29. *If we have a basis of the form* $\{1, \theta, \ldots, \theta^{n-1}\}$ *of* $\mathcal{L}/\mathcal{K}$, *then* $d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2$, *where* $\theta_i = \sigma_i(\theta)$. *Then* $d(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\binom{n}{2}} \prod_{i \neq j}(\theta_i - \theta_j)$.

Proof. You may use the Vandermant matrix $\begin{bmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{bmatrix}$. □

Example 1.30. Let $\mathcal{L} = \mathbb{Q}(\sqrt{3})$ and $\mathcal{K} = \mathbb{Q}$. Then

$$d(1, \sqrt{3}) = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta))^2 = (\sigma_1(\sqrt{3}) - \sigma_2(\sqrt{3}))^2 = (\sqrt{3} - (-\sqrt{3}))^2 = 12.$$

Lemma 1.31. Let $\{\beta_1, \ldots, \beta_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ be two bases for $\mathcal{L}/\mathcal{K}$. Then $d(\beta_1, \ldots, \beta_n) = u^2 d(\alpha_1, \ldots, \alpha_n)$ for some $u \in \mathcal{K}^\times$, i.e., the discriminant $d(\beta_1 \cdots, \beta_n)$ of a basis $\beta_1, \ldots, \beta_n$ of $\mathcal{L}/\mathcal{K}$ is well-defined up to multiplication by a square of a unit (nonzero square) in $\mathcal{K}$.

Proof. Since $0 \neq \det(M) \in \mathcal{K}$ given that M is the change of basis matrix, we have $\det(M) \in \mathcal{K}^\times$. □

Theorem 1.32. $d(\alpha_1 \cdots \alpha_n) \neq 0$.

Proof. Let θ be a primitive element for $\mathcal{L}/\mathcal{K}$. We have $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of $\mathcal{L}/\mathcal{K}$. The correspoding bilinear form on $\{\alpha_1, \ldots, \alpha_n\}$ has the matrix $M = \left(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\theta^{i-1}\theta^{j-1})\right)_{i=1,\ldots,n;\ j=1,\ldots,n}$. Since $\det(M) = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0$, where $\theta_i = \sigma_i(\theta)$, we have M is nonsingular. Let $\{\alpha_1, \ldots, \alpha_n\}$ be any basis with correspoding matrix $M' = \left(\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\alpha_i\alpha_j)\right)$. Since $\det(M')$ is a unit square multiple of $\det(M)$, we have $0 \neq \det(M') = d(\alpha_1, \ldots, \alpha_n)$. □

Remark. The above conclusions for the discriminant can be generalized to free modules.

Example 1.33. Let $\mathcal{L} = \mathbb{Q}(\sqrt{d})$ and $\mathcal{K} = \mathbb{Q}$, where d is square free.

(a) Let $\mathcal{B}_1 = \{1, \sqrt{d}\}$. Then $d(\mathcal{B}_1) = d(1, \sqrt{d}) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d.$

(b) Let $\mathcal{B}_2 = \left\{1, \frac{1+\sqrt{d}}{2}\right\}$. Similarly, $d(\mathcal{B}_2) = d\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{bmatrix} = d.$

Note that the disciminants differ by 4 and 4 is a square in $\mathbb{Q}^\times$.

1.3 Rings of integers

All rings in this section are nonzero commutative ring with identity. Let $A \subseteq B$ be subrings.

Definition 1.34. We say $b \in B$ is *integral* over A if there is a monic polynomial $f \in A[x]$ such that $f(b) = 0$. We say B is *integral* over A if each $b \in B$ is integral over A.

Example 1.35. Let $B = \mathbb{Z}[i]$ and $A = \mathbb{Z}$. Let $\beta = a+bi \in \mathbb{Z}[i]$ and $f(x) = x^2 - 2ax + a^2 + b^2 \in \mathbb{Z}[x]$. Then $f(a + bi) = 0$. This gives β is integral over $\mathbb{Z}$ and so $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$.

Fact 1.36. Let $A \in \mathrm{Mat}_r(R)$ and A^* be the adjugate matrix. Then $AA^* = A^*A = \det(A)I_r$. Hence if $Av = 0$ for some $v = (v_1, \ldots, v_r) \in R^r$, then $(\det(A)I_r)v = 0$.

Theorem 1.37. *Let $A \subseteq B \subseteq C$ be ring extensions. If C is integral over B and B is integral over A, then C is integral over A.*

Proof. Let $c \in C$, then there exist $b_1, \ldots, b_n \in B$ such that $c^n + b_1 c^{n-1} + \cdots + b_n = 0$. Hence c is integral over $A[b_1, \ldots, b_n]$ and then $A[b_1, \ldots, b_n, c] = A[b_1, \ldots, b_n][c]$ is a finitely generated $A[b_1, \ldots, b_n]$ module. Since B is integral over A and $b_1, \ldots, b_n \in B$, $A[b_1, \ldots, b_n]$ is a finitely generated A-module. Hence $A[b_1, \ldots, b_n, c]$ is a finitely generated A-module and thus c is integral over A. □

Definition 1.38. Let $A \subseteq B$ be ring extension.

$$\overline{A} = \{b \in B \mid b \text{ is integral over } A\}$$

is a subring of B. This is the *integral closure* of A in B. If $\overline{A} = A$, we say A is *integrally closed in* B.

Definition 1.39. If A is an integral domain and A is integrally closed in its field of fractions $Q(A)$, we say A is *integrally closed*.

Theorem 1.40. *UFDs are integrally closed.*

Proof. Method 1. Let R be a UFD. Let $\alpha/\beta \in Q(R)$ with $\beta \neq 0$ and $\gcd(\alpha, \beta) = 1$ be integral over R. Then there exists $n \in \mathbb{N}$ and $r_1, \ldots, r_n \in Q(R)$ such that $(\alpha/\beta)^n + r_1(\alpha/\beta)^{n-1} + \cdots + r_n = 0$, i.e., $\alpha^n + r_1\alpha\beta^{n-1} + \cdots + r_n\beta^n = 0$. Hence $\alpha^n \equiv 0 \pmod{\beta}$. Also, since $\gcd(\alpha, \beta) = 1$, $\beta \in R^\times$. Hence $\alpha/\beta \in R$.

Method 2. Let R be a UFD and $b \in Q(R)$ integral over R. Then there exists monic $f \in R[x]$ such that $f(b) = 0$. Since R is a UFD, $R[x]$ is a UFD. Factor f into irreducible and monic polynomials $f_1 \cdots f_m$ in $R[x]$. Then $f_1(b) \cdots f_m(b) = f(b) = 0$. Since R is an integral domain, $f_i(b) = 0$ for some $i \in \{1, \ldots, n\}$. Hence $x - b \mid f_i(x)$. Also, since f_i is irreducible, $f_i(x) = x - b$. Since $f_i \in R[x]$, $b \in R$. □

Theorem 1.41. *Let A be integrally closed with $\mathcal{K} := Q(A)$. Let $\mathcal{L}/\mathcal{K}$ be a finite separable extension. Let B be the integral closure of A inside $\mathcal{L}$, i.e., $B = \{a \in \mathcal{L} \mid a \text{ is integral over } A\}$. Then B is integrally closed in $\mathcal{L}$.*

Proof. Note $A \subseteq \mathcal{K} \subseteq \mathcal{L}$. Let $\overline{B} = \{b \in \mathcal{L} \mid b \text{ is integral over } B\} \supseteq B$. Since $\overline{B}$ is integral on B and B is integral over A, we have $\overline{B}$ is integral on A. Hence by definition of B and $\overline{B}$, $\overline{B} \subseteq B$. □

Definition 1.42. Let $\mathcal{K}$ be a number field. The *ring of integer* of $\mathcal{K}$, denoted $\mathcal{O}_\mathcal{K}$, is the integral closure of $\mathbb{Z}$ in $\mathcal{K}$, i.e.,

$$\mathcal{O}_\mathcal{K} = \{a \in \mathcal{K} \mid a \text{ is integral over } \mathbb{Z}\}.$$

Remark. Let $\mathcal{K}$ be a number field. Since $\mathbb{Z}$ is integrally closed with $Q(\mathbb{Z}) = \mathbb{Q}$, we have $\mathcal{O}_\mathcal{K}$ is integrally closed in $\mathcal{K} = Q(\mathcal{O}_\mathcal{K})$. Hence $\mathcal{O}_\mathcal{K}$ is integrally closed.

Fact 1.43. Let $\mathcal{K}$ be a number field. Then $\mathcal{O}_\mathcal{K}$ is a $\mathbb{Z}$-module, $\mathcal{K}$ is a (finitely generated) $\mathcal{O}_\mathcal{K}$-module and $\mathbb{Z} \subseteq \mathcal{O}_\mathcal{K} \subseteq \mathcal{K}$ is a chain of $\mathbb{Z}$-submodules.

Lemma 1.44. Let A be integrally closed with $Q(A) = \mathcal{K}$. Let $\mathcal{L}/\mathcal{K}$ be separable of degree n. Then an element $\beta \in \mathcal{L}$ is integral over A if and only if $m_{\beta,\mathcal{K}}(x)$ has coefficients in A.

Proof. $\Longleftarrow$ follows from definition.

$\Longrightarrow$ Assume $\beta \in \mathcal{L}$ is integral over A. Then there exists (monic) $p(x) \in A[x] \subseteq \mathcal{K}[x]$ such that $p(\beta) = 0$. Hence β is algebraic over $\mathcal{K}$. Then $m_{\beta,\mathcal{K}}(x) \mid p(x)$ in $\mathcal{K}[x]$ and so every root of $m_\beta(x)$ is a root of $p(x)$ in $\overline{\mathcal{K}}$. Let $\{\sigma_1, \ldots, \sigma_n\}$ be all the distinct $\mathcal{K}$-embeddings $\mathcal{L} \hookrightarrow \overline{\mathcal{K}}$. Since $\mathcal{L}/\mathcal{K}$ is separable, $\sigma_1(\beta), \ldots, \sigma_n(\beta) \in \overline{\mathcal{K}}$ are the n distinct roots of $m_{\beta,\mathcal{K}}$ and then $m_{\beta,\mathcal{K}}(x) = \prod_{i=1}^{n}(x - \sigma_i(\beta))$. Since β is integral over A, $\sigma_i(\beta)$ is integral over A for $i = 1, \ldots, n$. Hence the coefficients of m_β are integral over A. Thus, since A is integrally closed and the coefficients are in $\mathcal{K} = Q(A)$, the coefficients must lie in A. □

Example 1.45. Let $A = \mathbb{Z}$, $\mathcal{K} = \mathbb{Q}$ and $\mathcal{L} = \mathbb{Q}(\xi_p)$ with p prime. Then $m_{\xi_p}(x) \mid x^p - 1$, and actually $m_{\xi_p}(x) = x^{p-1} + \cdots + 1 \in \mathbb{Z}[x]$.

Example 1.46. Let $\mathcal{L} = \mathbb{Q}(i)$ with $\beta = i$, then $m_\beta(x) = x^2 + 1 \in \mathbb{Z}[x]$.

Lemma 1.47. Let $\mathcal{L}/\mathcal{K}$ be an extension of number fields. If $\beta \in \mathcal{O}_\mathcal{L}$, then $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\beta), \mathrm{N}_{\mathcal{L}/\mathcal{K}}(\beta) \in \mathcal{O}_\mathcal{K}$. In particular, if $\beta \in \mathcal{O}_\mathcal{K}$, then $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\beta),\ \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\beta) \in \mathbb{Z}$.

Proof. By definition, β is integral over $\mathbb{Z} \subseteq \mathcal{O}_\mathcal{K}$. Hence $m_{\beta,\mathcal{K}}(x)$ has coefficients in $\mathcal{O}_\mathcal{K}$. Since $c_\beta(x) = m^d_{\beta,\mathcal{K}}(x)$, where $d = [\mathcal{L} : \mathcal{K}(\beta)]$, we have c_β has coefficients in $\mathcal{O}_\mathcal{K}$. Also, since $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\beta)$ and $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(\beta)$ are both coefficients in c_β, $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(\beta), \mathrm{N}_{\mathcal{L}/\mathcal{K}}(\beta) \in \mathcal{O}_\mathcal{K}$. □

Theorem 1.48. *Let $\mathcal{K}$ be a number field and $\alpha \in \mathcal{O}_\mathcal{K}$. Then $\alpha \in \mathcal{O}_\mathcal{K}^\times$ if and only if $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. "⇒". Assume $\alpha \in \mathcal{O}_\mathcal{K}^\times$. Then $1/\alpha \in \mathcal{O}_\mathcal{K}$ and so $1 = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(1) = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)\,\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(1/\alpha)$. Since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha), \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(1/\alpha) \in \mathbb{Z}$, $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \pm 1$.

"⇐". Assume $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \pm 1$. Then since $\alpha \in \mathcal{O}_\mathcal{K}$, there exist $a_{n-1}, \ldots, a_1 \in \mathbb{Z}$ such that $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1$. Hence $1/\alpha$ is a root of the monic polynomial $g(x) = 1 + a_{n-1}x + \cdots + a_1 x^{n-1} \pm x^n$ and hence $1/\alpha \in \mathcal{O}_\mathcal{K}$. Thus, $\alpha \in \mathcal{O}_\mathcal{K}^\times$. □

Example 1.49. Let $\mathcal{K} = \mathbb{Q}(\sqrt{2})$. We have $\sqrt{2} \in \mathcal{O}_\mathcal{K}$ and $\mathbb{Z}[\sqrt{2}] \subseteq \mathcal{O}_\mathcal{K}$. Since $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$, we can let $x + y\sqrt{2} \in \mathcal{O}_\mathcal{K}$ with $x, y \in \mathbb{Q}$. Hence $2x = \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(x + y\sqrt{2}) \in \mathbb{Z}$. Hence $x = a/2$ for some $a \in \mathbb{Z}$. We also have $x^2 - 2y^2 = \mathrm{N}_{\mathcal{L}/\mathcal{K}}(x + y\sqrt{2}) \in \mathbb{Z}$. If $x \in \mathbb{Z}$, then $2y^2 \in \mathbb{Z}$. This gives $y \in \mathbb{Z}$, and so $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Assume $x \notin \mathbb{Z}$. Then a is odd. Since $(a/2)^2 - 2y^2 \in \mathbb{Z}$, $a^2 - 8y^2 \in 4\mathbb{Z}$ and so $8y^2 \in \mathbb{Z}$. If $y = b/2$ for some $b \in \mathbb{Z}$, then $a^2 - 8(b/2)^2 = a^2 - 2b^2 \in 4\mathbb{Z}$, contradicted by that a is odd and $a^2 - 2b^2$ is even. Hence $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and thus $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{2}]$.

Theorem 1.50. *Let $\mathcal{K}$ be a number field. Then every finitely generated $\mathcal{O}_\mathcal{K}$-submodule of $\mathcal{K}$ is a free $\mathbb{Z}$-module of rank $[\mathcal{K} : \mathbb{Q}]$. In particular, $\mathcal{O}_\mathcal{K} \cong \mathbb{Z}^{[\mathcal{K}:\mathbb{Q}]}$ as $\mathbb{Z}$-module.*

Proof. Let $\{\alpha_1, \ldots, \alpha_d\}$ be a $\mathbb{Q}$-basis of $\mathcal{K}$. We claim that we can choose the α_i's to lie in $\mathcal{O}_\mathcal{K}$. Let $i \in \{1, \ldots, d\}$, let $m_{\alpha_i}(x) = x^k + a_{i,k-1}x^{k-1} + \cdots + a_{i,0}$ with $a_{ij} \in \mathbb{Q}$. Let $D_i \in \mathbb{Z}$ be the least common denominator of the coefficients of $m_{\alpha_i}(x)$. Then

$$0 = D_i^k m_{\alpha_i}(\alpha_i) = D_i^k\alpha_i^k + D_i^k a_{i,k-1}\alpha_i^{k-1} + \cdots + D_i^k a_{i,0} = (D\alpha_i)^k + D_i a_{i,k-1}(D_i\alpha_i)^{k-1} + \cdots + D_i^k a_{i,0}.$$

Hence $D_i\alpha_i$ is a root of a monic $x^k + D_i a_{i,k-1}x^{k-1} + \cdots + D_i^k a_{i,0} \in \mathbb{Z}[x]$. Hence $D_i\alpha_i \in \mathcal{O}_\mathcal{K}$. Let $D = \mathrm{lcm}(D_1, \ldots, D_d)$, then $\{D\alpha_1, \ldots, D\alpha_d\} \subseteq \mathcal{O}_\mathcal{K}$ is a $\mathbb{Q}$-basis of $\mathcal{K}$.

Let $\mathcal{O}_\mathcal{K} \supseteq M_0 := \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d \cong \mathbb{Z}^d$. Since $\{\alpha_1, \ldots, \alpha_d\}$ are $\mathbb{Q}$-linearly independent when $\mathcal{K}$ is a $\mathbb{Q}$-vector space, they are $\mathbb{Z}$-linearly independent when $\mathcal{O}_\mathcal{K}$ is a $\mathbb{Z}$-module. Also, since $\{\alpha_1, \ldots, \alpha_n\}$

is a $\mathbb{Z}$-generating set for M_0, M_0 is a free $\mathbb{Z}$-module of rank d. Hence $\mathcal{O}_\mathcal{K}$ contains a free $\mathbb{Z}$-module of rank d. Set $\Delta = d(\alpha_1, \cdots, \alpha_d)$. Let $a \in \mathcal{O}_\mathcal{K}$. Then $a = b_1\alpha_1 + \cdots + \cdots + b_d\alpha_d \in \mathcal{O}_\mathcal{K}$ for some $b_1, \ldots, b_d \in \mathbb{Q}$. Then $\Delta a \in \Delta\mathcal{O}_\mathcal{K}$ and $\alpha_i a = (\alpha_i\alpha_1)b_1 + \cdots + (\alpha_i\alpha_d)b_d$ for $i = 1, \ldots, d$. Since $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}$ is $\mathbb{Q}$-linear, for $i = 1, \ldots, d$, $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i a) = \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_1)b_1 + \cdots + \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_d)b_d$, i.e., $\begin{bmatrix} \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_1 a) \\ \vdots \\ \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_d a) \end{bmatrix} = \left(\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_j)\right) \begin{bmatrix} b_1 \\ \vdots \\ b_d \end{bmatrix}$. Since $\alpha_i a, \alpha_i\alpha_j \in \mathcal{O}_\mathcal{K}$ for $i = 1, \ldots, d$ and $j = 1, \ldots, d$, we have $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i a), \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$ by Lemma 1.47 for $i = 1, \ldots, d$ and $j = 1, \ldots, d$. Also, by Cramer's rule, $\Delta b_i = \det\left(\left(\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_j)\right)\right)b_i$ is the determinant of the matrix $\left(\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha_i\alpha_j)\right)$ with i^{th} column replaced by $(b_1, \ldots, b_d)^T$ for $i = 1, \ldots, d$. Hence $\Delta b_i \in \mathbb{Z}$ for $i = 1, \ldots, d$. Then

$$\Delta a = (\Delta b_1)\alpha_1 + \cdots + (\Delta b_d)\alpha_d \in \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d = M_0.$$

Hence $\Delta\mathcal{O}_\mathcal{K} \subseteq M_0$ and then $\Delta\mathcal{O}_\mathcal{K}$ is a $\mathbb{Z}$-submodule of M_0 since $\Delta\mathcal{O}_\mathcal{K}$ is a $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, $\Delta\mathcal{O}_\mathcal{K}$ is a free $\mathbb{Z}$-module of rank at most d. Since $0 \neq \Delta \in \mathcal{K}$, we have a $\mathbb{Z}$-module isomorphism $\Delta\mathcal{O}_\mathcal{K} \cong \mathcal{O}_\mathcal{K}$ given by $\Delta x \mapsto x$. Hence $\mathcal{O}_\mathcal{K}$ is a free $\mathbb{Z}$-module of rank at most d. Also, since $M_0 \subseteq \mathcal{O}_\mathcal{K}$ is a $\mathbb{Z}$-submodule, $\mathcal{O}_\mathcal{K}$ is a free $\mathbb{Z}$-module of rank d. Then we have a $\mathbb{Z}$-module isomorphism $\mathcal{O}_\mathcal{K} \otimes_\mathbb{Z} \mathbb{Q} \cong \mathbb{Z}^d \otimes_\mathbb{Z} \mathbb{Q} \cong \mathbb{Q}^d$.

Let $w_1, \ldots, w_r \in \mathcal{K}$ such that $M := \mathcal{O}_\mathcal{K}w_1 + \cdots + \mathcal{O}_\mathcal{K}w_r$. Then for $i = 1, \ldots, r$, there exist $\gamma_{i1}, \ldots, \gamma_{id} \in \mathcal{O}_\mathcal{K}$ and $c_{i1}, \ldots, c_{id} \in \mathbb{Q}$ and such that $w_i = c_{i1}\gamma_{i1} + \cdots + c_{id}\gamma_{id}$. Let $D' = \mathrm{lcm}(c_{11}, \ldots, c_{1d}, \ldots, c_{r1}, \ldots, c_{rd})$. Then $D'c_{11}, \ldots, D'c_{1d}, \ldots, D'c_{r1}, \ldots, D'c_{rd} \in \mathbb{Z}$. Hence we have $D'w_1, \ldots, D'w_r \in \mathcal{O}_\mathcal{K}$ and then $D'M \subseteq \mathcal{O}_\mathcal{K}$ and hence $\Delta D'M \subseteq \Delta\mathcal{O}_\mathcal{K} \subseteq M_0$. Also, since $\Delta D'M$ is a $\mathbb{Z}$-module, we have $\Delta D'M$ is a $\mathbb{Z}$-submodule of M_0. Since $\Delta D' \neq 0$, we have M is a free $\mathbb{Z}$-module of rank at most d similarly. Also, $\mathbb{Z}^d \cong \mathcal{O}_\mathcal{K} \cong \mathcal{O}_\mathcal{K}w_1 \subseteq M$ as a $\mathbb{Z}$-submodule. Hence M is a free $\mathbb{Z}$-module of rank d. □

Definition 1.51. Let $\mathcal{K}$ be a number field, a basis $\{\alpha_1, \ldots, \alpha_m\}$ for $\mathcal{O}_\mathcal{K}$ as a $\mathbb{Z}$-module is called an *integral basis* ($\mathbb{Z}$-basis) for $\mathcal{K}$ or for $\mathcal{O}_\mathcal{K}$.

Remark. An ingtegral basis always exists. By Theorem 1.50, it is can be chose from a $\mathbb{Q}$-basis of $\mathcal{K}$.

Definition 1.52. Let $\mathcal{K}$ be a number field. Define the *discriminant* of $\mathcal{K}$ to be the discriminant of $\mathcal{O}_\mathcal{K}$ down to $\mathbb{Z}$, i.e., given any integral basis $\{\alpha_1, \ldots, \alpha_d\}$,

$$\Delta(\mathcal{O}_\mathcal{K}) = \Delta(\mathcal{K}) = \Delta_\mathcal{K} = \mathrm{disc}(\mathcal{K}) = \mathrm{disc}(\mathcal{O}_\mathcal{K}) = d(\alpha_1, \ldots, \alpha_d) = \left(\det(\sigma_i(\alpha_j))\right)^2.$$

Remark. We check the well-definedness of discriminant of $\mathcal{K}$. If $\{\alpha_1, \ldots, \alpha_r\}$ and $\{\beta_1, \ldots, \beta_r\}$ are two integral bases for $\mathcal{K}$, then $d(\alpha_1, \ldots, \alpha_r) = (\det(M))^2 d(\beta_1, \ldots, \beta_r)$, where $M \in \mathrm{GL}_r(\mathbb{Z})$ is the change of basis. Then M is invertible. Hence $\det(M) \in \mathbb{Z}^\times = \{\pm 1\}$ and then $\Delta_\mathcal{K}$ is a well-defined integer. In this case, the inverse is given by $M^{-1} = \det(M)^{-1}M^{\mathrm{adj}}$.

Theorem 1.53. *Let $\mathcal{K}$ be a field such that $\mathrm{char}(\mathcal{K}) = 0$ and $\mathcal{L} = \mathcal{K}(\beta)$. Let $\sigma_1, \ldots, \sigma_m$ be the distinct embeddings of $\mathcal{L} \hookrightarrow \overline{\mathcal{K}}$. Let f be the minimal polynomial of β over $\mathcal{K}$ of degree m. Then $d(1, \beta^2, \ldots, \beta^{m-1}) = (-1)^{\frac{m(m-1)}{2}} \mathrm{N}_{\mathcal{L}/\mathcal{K}}(f'(\beta))$.*

Proof. Write $f = \prod_{i=1}^{m}(x-\beta_i)$, where $\beta_i = \sigma_i(\beta)$. Then

$$d(1,\beta,\ldots,\beta^{m-1}) = \prod_{i<j}(\beta_i-\beta_j)^2 = (-1)^{\frac{m(m-1)}{2}}\prod_{i\neq j}(\beta_i-\beta_j)$$
$$= (-1)^{\frac{m(m-1)}{2}}\prod_{i=1}^{m} f'(\beta_j) = (-1)^{\frac{m(m-1)}{2}}\,\mathrm{N}_{\mathcal{L}/\mathcal{K}}(f'(\beta)). \qquad \square$$

Example 1.54. Let $\mathcal{K} = \mathbb{Q}(\xi_3)$. Then $m_{\xi_3}(x) = x^2+x+1 = (x-\xi_3)(x-\xi_3^2) = (x-\xi_3)(x-\bar{\xi}_3)$ and we have 2 $\mathcal{K}$-embeddings $\sigma_1 : \xi_3 \to \xi_3$ and $\sigma_2 : \xi_3 \to \bar{\xi}_3$. Note $d(1,\xi_3) = \det\begin{bmatrix}\mathrm{Tr}(1) & \mathrm{Tr}(\xi_3)\\ \mathrm{Tr}(\xi_3) & \mathrm{Tr}(\bar{\xi}_3)\end{bmatrix} = \det\begin{bmatrix}1+1 & \xi_3+\bar{\xi}_3\\ \xi_3+\xi_3 & \bar{\xi}_3+\xi_3\end{bmatrix} = \det\begin{bmatrix}2 & -1\\ -1 & -1\end{bmatrix} = -3$. Since $f'(x) = 2x+1$, $(-1)^{\frac{3(3-1)}{2}}\,\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(2\xi_3+1) = -(2\xi_3+1)(2\bar{\xi}_3+1) = -(4-2+1) = -3$.

Exercise 1.55. Check both for quadratic extension of $\mathbb{Q}$.

Example 1.56. Let $f = x^n + ax + b$ with $a, b \in \mathcal{K}$ be irreducible with a root β. Then $\Delta(\mathcal{K}(\beta)) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)$.

Theorem 1.57. *Let $M \subseteq M'$ be two finitely generated $\mathcal{O}_\mathcal{K}$-submodule of $\mathcal{K}$. Then $[M' : M]$ is finite and satisfies $\Delta(M) = [M' : M]^2\Delta(M')$.*

Proof. See *Abstract Algebra* by Dummit and Foot or Modules over PID. $\square$

Exercise 1.58. Let $M' = \mathbb{Z}^3$ and $M = (2\mathbb{Z})^3$. Work out result for this case and the general case is essentially the same.

Theorem 1.59 (Stickleberger's theorem)**.** *Let $\mathcal{K}$ be a number field, then $\Delta_\mathcal{K} \equiv 0, 1 \pmod 4$.*

Proof. Let $\{\alpha_1,\ldots,\alpha_n\}$ be an integral basis for $\mathcal{K}$ and $\sigma_1,\ldots,\sigma_n$ the distinct embeddings $\mathcal{K} \hookrightarrow \overline{\mathbb{Q}}$. Then $\Delta_\mathcal{K} = (\det((\sigma_i(\alpha_j))))^2 = \left(\sum_{\pi\in A_n}\prod_{i=1}^n \sigma_i(\alpha_{\pi(i)}) - \sum_{\pi\notin A_n}\prod_{i=1}^n \sigma_i(\alpha_{\pi(i)})\right)^2$. Let $P = \sum_{\pi\in A_n}\prod_{i=1}^n \sigma_i(\alpha_{\pi(i)})$ and $N = \sum_{\pi\notin A_n}\prod_{i=1}^n \sigma_i(\alpha_{\pi(i)})$. Then $\Delta_\mathcal{K} = (P-N)^2$. Since $\{\sigma_1,\ldots,\sigma_n\}$ is a finite group, $\sigma_i\{\sigma_1,\ldots,\sigma_n\} = \{\sigma_1,\ldots,\sigma_n\}$ for $i = 1,\ldots,n$. For $i = 1,\ldots,n$, since $\sigma_i(P) = P, \sigma_i(N) = N$ or $\sigma_i(P) = N, \sigma_i(N) = P$, we have $\sigma_i(P+N) = P+N$ and $\sigma_i(PN) = PN$. Hence $P+N, PN \in \mathbb{Q}$. Since $\alpha_j \in \mathcal{O}_\mathcal{K}$ and $\sigma_i(\alpha_j) \in \mathcal{O}_\mathcal{K}$ for $i = 1,\ldots,d$ and $j = 1,\ldots,d$, we have $P+N, PN \in \mathcal{O}_\mathcal{K}$. Then $P+N, PN \in \mathbb{Q}\cap\mathcal{O}_\mathcal{K} = \mathbb{Z}$ and so $\Delta_\mathcal{K} = (P-N)^2 = (P+N)^2 - 4PN \in \mathbb{Z}$. $\square$

Example 1.60. Let $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ with d square free.

(a) Let $d \equiv 2, 3 \pmod 4$. Let $\mathcal{B} = \{1, \sqrt{d}\}$ be a basis of $\mathbb{Z}[\sqrt{d}]$. Then $4d = \Delta(\mathbb{Z}[\sqrt{d}]) = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]]^2\Delta(\mathcal{O}_\mathcal{K})$. Since d is square free, we have $[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]] = 2$ and $\Delta(\mathcal{O}_\mathcal{K}) = d$ or $[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]] = 1$ and $\Delta(\mathcal{O}_\mathcal{K}) = 4d$. If $\Delta(\mathcal{O}_\mathcal{K}) = d$, then $d \equiv 0, 1 \pmod 4$, a contradiction. Thus, $\Delta(\mathcal{O}_\mathcal{K}) = 4d$ and $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{d}]$.

(b) Let $d \equiv 1 \pmod 4$. Note $\frac{1+\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$, but is a root of the polynomial $f = x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$. Hence $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_\mathcal{K}$. A $\mathbb{Z}$-basis for $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_\mathcal{K}$ is $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. Hence $d = d\left(1, \frac{1+\sqrt{d}}{2}\right) = \Delta\left(\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right) = \left[\mathcal{O}_\mathcal{K} : \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right]^2\Delta(\mathcal{O}_\mathcal{K})$. Since d is square-free,

$\left[\mathcal{O}_\mathcal{K} : \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right] = 1$. Thus, $\mathcal{O}_\mathcal{K} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and $\Delta(\mathcal{O}_\mathcal{K}) = d$. Since $4d = \Delta(\mathbb{Z}[\sqrt{d}]) = [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]]^2\Delta(\mathcal{O}_\mathcal{K})$, we have $[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]] = 2$.

In summary,

$$\mathcal{O}_\mathcal{K} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4 \end{cases} \quad \text{and } [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\sqrt{d}]] = \begin{cases} 1 & d \equiv 2,3 \pmod 4 \\ 2 & d \equiv 1 \pmod 4 \end{cases}.$$

Chapter 2

Dedekind domain

$x^n + y^n = z^n$ with $n \in \mathbb{N}^{>2}$ has no solutions in $\mathbb{Z}^3$. Note $z^n = (x+y)(x+\xi_n y)\cdots(x+\xi_n^{n-1}y)$, where ξ_n is the n^{th} primitive root of unity and

(a) terms on right have no common factor;

(b) then each term must be an n^{th} power;

(c) all terms on right are not an n^{th} power.

Definition 2.1. A ring R is said to be *Noetherian* if given any chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists $n \in \mathbb{N}$ such that $I_k = I_n$ for any $k \geqslant n$.

Theorem 2.2. *A ring R is Noetherian if and only if all ideals in R are finitely generated.*

Proof. $\Longrightarrow$ Assume R is Noetherian. Suppose $I \subseteq R$ is not finitely generated. Let $0 \neq x_1 \in I$. Then $\langle x_1\rangle \subsetneq I$. Let $x_2 \in I \smallsetminus \langle x_1\rangle$, then $\langle x_1\rangle \subsetneq \langle x_1, x_2\rangle \subsetneq I$. Continue to get a chain of ideals that does not stabilize, a contradiction.

$\Longleftarrow$ Assume all ideals in R are finitely generated. Consider a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$. We have $I := \bigcup_{i=1}^{\infty} I_j$ is an ideal, so it is finitely generated and say $I = \langle x_1, \cdots, x_n\rangle$. Pick m such that $x_1, \ldots, x_n \in I_m$. So $I \subseteq I_m \subseteq I_{m+1} \subseteq \cdots \subseteq I$. Thus, for any $k \geqslant m$, $I_m = I = I_k$. □

Fact 2.3. A ring R is Noetherian if and only if every non-empty set Σ of ideals of R contains a maximal element with respect to "$\subseteq$".

Definition 2.4. A *Dedekind domain* is a Noetherian ring and integrally closed, whose nonzero prime ideals are maximal ideals.

Example 2.5. $\mathbb{Z}$ is a Dedekind domain.

Lemma 2.6. Let $\mathcal{L}/\mathcal{K}$ be a field extension, if $\mathfrak{P} \subseteq \mathcal{O}_{\mathcal{L}}$ is a prime ideal, then $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_{\mathcal{K}} \subseteq \mathcal{O}_{\mathcal{K}}$ is also a prime ideal.

Proof. Let $a, b \in \mathcal{O}_{\mathcal{K}}$ and $ab \in \mathfrak{p}$. Then $ab \in \mathfrak{P}$. Since $\mathfrak{P} \subseteq \mathcal{O}_{\mathcal{L}}$ is prime, $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$. Since $a, b \in \mathcal{O}_{\mathcal{K}}$, we have $a \in \mathfrak{P} \cap \mathcal{O}_{\mathcal{K}} = \mathfrak{p}$ or $b \in \mathfrak{P} \cap \mathcal{O}_{\mathcal{K}} = \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime. □

Fact 2.7. Let M be an R-module and $I \subseteq R$ an ideal. Then M has a well-defined R/I-module structure defined by the formula $\bar{r}m := rm$ if and only if $IM = 0$.

Lemma 2.8. Let $\mathcal{K}$ be a number field. Let $\mathfrak{p} \subseteq \mathcal{O}_\mathcal{K}$ be prime and $\langle p \rangle = \mathfrak{p} \cap \mathbb{Z}$. Then $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is a $\mathbb{F}_p$-module given by $(r + \langle p \rangle)(v + \mathfrak{p}) = rv + \mathfrak{p}$.

Proof. Note that $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is a $\mathbb{Z}$-module given by $r(v + \mathfrak{p}) = rv + \mathfrak{p}$. Since $\langle p \rangle = \mathfrak{p} \cap \mathbb{Z}$, we have $\langle p \rangle \cdot \mathcal{O}_\mathcal{K}/\mathfrak{p} = \mathfrak{p}/\mathfrak{p} = 0$. So $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is a $\mathbb{F}_p$-module given by $(r + \langle p \rangle)(v + \mathfrak{p}) = r(v + \mathfrak{p}) = rv + \mathfrak{p}$. □

Theorem 2.9. *Let $\mathcal{K}$ be a number field. The ring $\mathcal{O}_\mathcal{K}$ is a Dedekind domain.*

Proof. Since $\mathcal{O}_\mathcal{K}$ is integrally closed in $\mathcal{K}$, $\mathcal{O}_\mathcal{K}$ is integrally closed.

Since $\mathbb{Z}$ is Noetherian and $\mathcal{O}_\mathcal{K}$ is a finitely generated $\mathbb{Z}$-module, $\mathcal{O}_\mathcal{K}$ is Noetherian.

Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_\mathcal{K}$ be a prime ideal. Then $\mathfrak{p} \cap \mathbb{Z} \subseteq \mathbb{Z}$ is also a prime ideal. Let $0 \neq a \in \mathfrak{p} \subseteq \mathcal{O}_\mathcal{K}$. Then there exist $r_0, \ldots, r_{n-1} \in \mathbb{Z}$ such that $a^n + r_{n-1}a^{n-1} + \cdots + r_1 a + r_0 = 0$ holds at minimum degree. Then $0 \neq r_0 \in \mathbb{Z}$ and $r_0 = -a(a^{n-1} + r_{n-1}a^{n-2} + r_1) \in \mathfrak{p}$. So $0 \neq r_0 \in \mathfrak{p} \cap \mathbb{Z}$ and hence $\mathfrak{p} \cap \mathbb{Z} \neq 0$. Also, since $\mathbb{Z}$ is PID, $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ for some prime $p \in \mathbb{Z}$. Define $\varphi : \mathbb{Z} \to \mathcal{O}_\mathcal{K}/\mathfrak{p}$ by $z \mapsto z + \mathfrak{p}$. Then $\mathrm{Ker}(\varphi) = \mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ and so $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle \cong \mathrm{Im}(\varphi) \subseteq \mathcal{O}_\mathcal{K}/\mathfrak{p}$ as a ideal. Since $\mathfrak{p}$ is prime, $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is an integral domain. Let $\theta + \mathfrak{p} \in \mathcal{O}_\mathcal{K}/\mathfrak{p}$ with $\theta \in \mathcal{O}_\mathcal{K}$. Then there exist $b_0, \ldots, b_{m-1} \in \mathbb{Z}$ such that $\theta^m + b_{m-1}\theta^{m-1} + \cdots + b_1\theta + b_0 = 0$. So

$$\begin{aligned}
&(\theta + \mathfrak{p})^m + (b_{m-1} + \langle p \rangle)(\theta + \mathfrak{p})^{m-1} + \cdots + (b_1 + \langle p \rangle)(\theta + \mathfrak{p}) + (b_0 + \langle p \rangle)(1 + \mathfrak{p}) \\
&= (\theta^m + \mathfrak{p}) + (b_{m-1} + \langle p \rangle)(\theta^{m-1} + \mathfrak{p}) + \cdots + (b_1\theta + \mathfrak{p}) + (b_0 + \mathfrak{p}) \\
&= (\theta^m + \mathfrak{p}) + (b_{m-1}\theta^{m-1} + \mathfrak{p}) + \cdots + (b_1\theta + \mathfrak{p}) + (b_0 + \mathfrak{p}) \\
&= \theta^m + b_{m-1}\theta^{m-1} + \cdots + b_1\theta + b_0 + \mathfrak{p} = \mathfrak{p},
\end{aligned}$$

which is 0 in $\mathcal{O}_\mathcal{K}/\mathfrak{p}$. So $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is integral over $\mathbb{F}_p$. Hence $\mathcal{O}_\mathcal{K}/\mathfrak{p}$ is a field and thus $\mathfrak{p}$ is maximal. □

Definition 2.10. Let R be a commutative ring and $0 \neq \mathfrak{a}, \mathfrak{b} \leqslant R$. We say $\mathfrak{b}$ *divides* $\mathfrak{a}$ and write $\mathfrak{b} \mid \mathfrak{a}$, if $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$ for some $0 \neq \mathfrak{c} \leqslant R$.

Fact 2.11. If $\mathfrak{b} \mid \mathfrak{a}$, then $\mathfrak{b} \supseteq \mathfrak{a}$.

Lemma 2.12. Let R be a commutative ring and $a, b \in R$. Then $a \mid b$ if and only if $\langle a \rangle \mid \langle b \rangle$.

Proof. $\Longrightarrow$ If $a \mid b$, then $ac = b$ for some $c \in R$. So $\langle a \rangle\langle c \rangle = \langle b \rangle$, i.e., $\langle a \rangle \mid \langle b \rangle$.

$\Longleftarrow$ Since $\langle a \rangle \mid \langle b \rangle$, $a\mathfrak{c} = \langle a \rangle\mathfrak{c} = \langle b \rangle$ for some ideal $\mathfrak{c} \subseteq R$. So $ac = b$ for some $c \in \mathfrak{c}$, i.e., $a \mid b$. □

Theorem 2.13. *Let R be a commutative ring and $\mathfrak{p} \subseteq R$ an ideal. Then $\mathfrak{p} \subseteq R$ is prime if and only if for any ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$, $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$.*

Proof. $\Longrightarrow$ Let $\mathfrak{p} \subseteq R$ be prime and $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$. Suppose $\mathfrak{p} \not\supseteq \mathfrak{a}$ and $\mathfrak{p} \not\supseteq \mathfrak{b}$. Then there exist $x \in \mathfrak{a} \setminus \mathfrak{p}$ and $y \in \mathfrak{b} \setminus \mathfrak{p}$ such that $xy \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, a contradiction.

$\Longleftarrow$ Let $x, y \in R$ and $xy \in \mathfrak{p}$, then $\langle x \rangle\langle y \rangle = \langle xy \rangle \subseteq \mathfrak{p}$. So $\langle x \rangle \subseteq \mathfrak{p}$ or $\langle y \rangle \subseteq \langle \mathfrak{p} \rangle$ and hence $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Thus, $\mathfrak{p}$ is prime. □

Assumption 2.14. Assume that $\mathcal{O}$ is a Dedekind domain.

Lemma 2.15. Let $0 \neq \mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be ideals. Then $\mathfrak{b} \supseteq \mathfrak{a}$ if and only if $\mathfrak{b} \mid \mathfrak{a}$.

Proof. We will show it later. □

Corollary 2.16. Let $\mathfrak{p} \subseteq \mathcal{O}$ be an ideal. Then $\mathfrak{p} \subseteq R$ is prime if and only if for any ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$, $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$.

Lemma 2.17. Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be ideals, then $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$, and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$.

Proof. (a) Since $\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{a}$ and $\mathfrak{a} + \mathfrak{b} \supseteq \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{a}$ and $\mathfrak{a} + \mathfrak{b} \mid \mathfrak{b}$. Let $\mathfrak{c} \subseteq \mathcal{O}$ be an ideal and $\mathfrak{c} \mid \mathfrak{a}$ and $\mathfrak{c} \mid \mathfrak{b}$, i.e., $\mathfrak{c} \supseteq \mathfrak{a}$ and $\mathfrak{c} \supseteq \mathfrak{b}$. Then $\mathfrak{c} \supseteq \mathfrak{a} + \mathfrak{b}$, i.e., $\mathfrak{c} \mid \mathfrak{a} + \mathfrak{b}$ and thus $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$.

(b) Since $\mathfrak{a} \supseteq \mathfrak{a} \cap \mathfrak{b}$ and $\mathfrak{b} \supseteq \mathfrak{a} \cap \mathfrak{b}$, we have $\mathfrak{a} \mid \mathfrak{a} \cap \mathfrak{b}$ and $\mathfrak{b} \mid \mathfrak{a} \cap \mathfrak{b}$. Let $\mathfrak{c} \subseteq \mathcal{O}$ be an ideal and $\mathfrak{a} \mid \mathfrak{c}$ and $\mathfrak{b} \mid \mathfrak{c}$, i.e., $\mathfrak{a} \supseteq \mathfrak{c}$ and $\mathfrak{b} \supseteq \mathfrak{c}$. Then $\mathfrak{a} \cap \mathfrak{b} \supseteq \mathfrak{c}$, i.e., $\mathfrak{a} \cap \mathfrak{b} \mid \mathfrak{c}$ and thus $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$. □

Corollary 2.18. Let $0 \neq \mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ be all prime ideals, If $\mathfrak{p} \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$, then $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in \{1, \ldots, r\}$.

Proof. Since $\mathfrak{p} \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$, we have $\mathfrak{p} \mid \mathfrak{p}_i$ for some $i \in \{1, \ldots, r\}$. Then $\mathfrak{p} \supseteq \mathfrak{p}_i \neq 0$. Since $\mathcal{O}$ is a Dedekind domain, $\mathfrak{p}_i$ is maximal and so $\mathfrak{p} = \mathfrak{p}_i$. □

Remark. We can not get a unique factorization of elements in $\mathcal{O}$. For example, let $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_\mathcal{K} = \mathbb{Z}(\sqrt{-5})$, which is not a UFD. But we can uniquely factor any ideal in $\mathcal{O}$ into a product of prime ideals.

Lemma 2.19. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal, then there exist $0 \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ all primes such that $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$, where $\mathfrak{p}_i$ are not necessarily distinct.

Proof. Let $\emptyset \neq S$ be the set of ideals for which the claim is false. Since $\mathcal{O}$ is Noetherian, $\emptyset \neq S$ has a maximal element $\mathcal{M}$ with respect to "$\subseteq$". Then $\mathcal{M}$ is not prime. So there exist $b_1, b_2 \in \mathcal{O}$ such that $b_1 b_2 \in \mathcal{M}$, but $b_1 \notin \mathcal{M}$ and $b_2 \notin \mathcal{M}$. Then $M \subsetneq \mathcal{N}_1 := \langle b_1 \rangle + \mathcal{M} \subseteq \mathcal{O}$ and $M \subsetneq \mathcal{N}_2 := \langle b_2 \rangle + \mathcal{M} \subseteq \mathcal{O}$ as ideals. Since $\mathcal{M}$ is maximal, $\mathcal{N}_1, \mathcal{N}_2 \notin S$. So there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s \subseteq \mathcal{O}$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathcal{N}_1$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathcal{N}_2$. Then we have $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathcal{N}_1 \mathcal{N}_2 = \langle b_1 b_2 \rangle + \mathcal{M} = \mathcal{M}$, a contradiction. Thus $S = \emptyset$. □

Assumption 2.20. Let $\mathcal{K} = \operatorname{Frac}(\mathcal{O})$ be the field of fraction.

Definition 2.21. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal. Define the *inverse* of $\mathfrak{a}$ by

$$\mathfrak{a}^{-1} = \{x \in \mathcal{K} \mid x\mathfrak{a} \subseteq \mathcal{O}\} = (\mathcal{O} :_\mathcal{K} \mathfrak{a}).$$

Fact 2.22. $\mathfrak{a}^{-1}$ is a $\mathcal{O}$-submodule of $\mathcal{K}$.

Theorem 2.23. *Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}$ be prime. Then $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$.*

Proof. By definition, $\mathcal{O} \subseteq \mathfrak{p}^{-1}$. Since $\mathfrak{p} \neq 0$, there exists $a \in \mathfrak{p} \setminus \{0\}$. Then there exist $0 \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ all prime such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle a \rangle \subseteq \mathfrak{p}$, where r is chosen as small as possible. So $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in \{1, \ldots, r\}$. Without loss of generality, assume $\mathfrak{p} = \mathfrak{p}_1$. By the choice of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq \langle a \rangle$. Then there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus \langle a \rangle$ and so $\mathfrak{p} b = \mathfrak{p}_1 b \subseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \langle a \rangle = a\mathcal{O}$. So $a^{-1}\mathfrak{p} b \subseteq \mathcal{O}$ and then $a^{-1} b \in \mathfrak{p}^{-1}$. Since $b \notin \langle a \rangle = a\mathcal{O}$, $a^{-1} b \notin \mathcal{O}$. □

Lemma 2.24. Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}$ be prime. Then $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ for any ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}$.

Proof. Since $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, we have $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1}$. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal. Then $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_n \rangle \mathcal{O}$ for some $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$. Suppose $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$. Let $x \in \mathfrak{p}^{-1}$. Then $\alpha_i x \in \mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ and there exists $a_{ij} \in \mathcal{O}$ such that $x\alpha_i = \alpha_i x = \sum_{j=1}^n a_{ij}\alpha_j$ for $i = 1, \ldots, n$. Since $\mathfrak{a} \neq 0$, we have $0 \neq (\alpha_1, \ldots, \alpha_n) \in \mathcal{O}^n$ and hence $\det(xI_n - (a_{ij})) = 0$, i.e., x is a root of a monic polynomial in $\mathcal{O}[x]$. So x is integral over $\mathcal{O}$. Since $\mathcal{O}$ is integrally closed, we have $x \in \mathcal{O}$ and then $\mathfrak{p}^{-1} \subseteq \mathcal{O}$, which is contradicted by that $\mathcal{O} \subsetneq \mathfrak{p}^{-1}$. □

Lemma 2.25. Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}$ be prime, then $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

Proof. By definition, $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. Since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. □

Theorem 2.26. *Every ideal $0 \neq \mathfrak{a} \subsetneq \mathcal{O}$ admits a unique factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, with $0 \neq \mathfrak{p}_i \subseteq \mathcal{O}$ prime and $e_i \in \mathbb{N}$.*

Proof. Uniqueness. Suppose $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, where primes are not necessarily distinct. Then $\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, i.e., $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s$. So $\mathfrak{p}_1 = \mathfrak{q}_i$ for some $i \in \{1, \ldots, s\}$, without loss of generality, assume $\mathfrak{p}_1 = \mathfrak{q}_1$. Then $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{p}_1^{-1}(\mathfrak{p}_1 \cdots \mathfrak{p}_r) = \mathfrak{p}_1^{-1}(\mathfrak{q}_1 \cdots \mathfrak{q}_s) = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. By induction, we have $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ for $i = 1, \ldots, r$.

Existence. Let $\emptyset \neq S$ be the set of nonzero prime ideals without a prime factorization. Since $\mathcal{O}$ is Noetherian, $\emptyset \neq S$ has a maximal element $\mathcal{M}$ with respect to "$\subseteq$". Then $\mathcal{M}$ is not prime. So $\mathcal{M}$ is not a maximal ideal in $\mathcal{O}$ and then there exists a maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$ such that $\mathcal{M} \subsetneq \mathfrak{p}$. Then $\mathcal{M} \subsetneq \mathcal{M}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Note that $\mathcal{M}\mathfrak{p}^{-1} \neq \mathcal{O}$, otherwise, $\mathcal{M} = \mathcal{M}\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{M}\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}\mathfrak{p} = \mathfrak{p}$, which is a contradiction. So $\mathcal{M} \subsetneq \mathcal{M}\mathfrak{p}^{-1} \subsetneq \mathcal{O}$. Since $\mathcal{M}$ is maximal, $\mathcal{M}\mathfrak{p}^{-1} \notin S$ and so $\mathcal{M}\mathfrak{p}^{-1}$ must have a prime factorization, say $\mathcal{M}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. So $\mathcal{M} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, a contradiction. □

Lemma 2.27. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal, then $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$.

Proof. If $\mathfrak{a} = \mathcal{O}$, it is trivial. Assume $\mathfrak{a} \subsetneq \mathcal{O}$. Let $0 \neq x \in \mathfrak{a}$. Then $x\mathfrak{a}^{-1} \subseteq \mathcal{O}$. Since $0 \neq \mathfrak{a} \subsetneq \mathcal{O}$ is an ideal, we have a unique prime factorization $\mathfrak{a} = \mathfrak{p}_1 \cdots, \mathfrak{p}_r$. Let $\mathfrak{b} := \mathfrak{p}_r^{-1} \cdots \mathfrak{p}_1^{-1}$. Then $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} = (\mathfrak{p}_r^{-1} \cdots \mathfrak{p}_1^{-1})(\mathfrak{p}_1 \cdots \mathfrak{p}_r) = \mathcal{O}$. So by definition, $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Let $x \in \mathfrak{a}^{-1}$, then $x\mathfrak{a} \subseteq \mathcal{O}$ and so $\langle x \rangle = x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$. So $x \in \mathfrak{b}$ and hence $\mathfrak{a}^{-1} \subseteq \mathfrak{b}$. Thus, $\mathfrak{a}^{-1} = \mathfrak{b}$. Since $\mathfrak{a}\mathfrak{b} = \mathcal{O}$, $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. □

Remark. Suppose that there exists an ideal $\mathfrak{b} \subseteq \mathfrak{o}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Then

$$\mathfrak{b} \subseteq (\mathfrak{o} :_{\mathcal{K}} \mathfrak{a}) = (\mathfrak{o} :_{\mathcal{K}} \mathfrak{a})\mathfrak{o} = (\mathfrak{o} :_{\mathcal{K}} \mathfrak{a})\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{o}\mathfrak{b} \subseteq \mathfrak{b}.$$

Hence $\mathfrak{b} = (\mathfrak{o} :_{\mathcal{K}} \mathfrak{a}) = \mathfrak{a}^{-1}$.

Lemma 2.28. Let $0 \neq \mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be ideals. Then $\mathfrak{b} \supseteq \mathfrak{a}$ if and only if there exists an ideal $0 \neq \mathfrak{c} \subseteq \mathcal{O}$ such that $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.

Proof. $\Longleftarrow$ is trivial.

$\Longrightarrow$ If $\mathfrak{b} = \mathcal{O}$, we take $\mathfrak{c} = \mathfrak{a}$. Assume now $\mathfrak{b} \subsetneq \mathcal{O}$. Since $\mathfrak{b}^{-1}$ is an $\mathcal{O}$-submodule of $\mathcal{K}$ and $\mathfrak{a} \subseteq \mathcal{O}$ is an ideal, we have $\mathfrak{c} := \mathfrak{b}^{-1}\mathfrak{a} = \mathfrak{a}\mathfrak{b}^{-1}$ is also an $\mathcal{O}$-submodule of $\mathcal{K}$. Also, since $\mathfrak{b}^{-1}\mathfrak{a} \subseteq \mathfrak{b}^{-1}\mathfrak{b} = \mathcal{O}$, we have $\mathfrak{b}^{-1}\mathfrak{a} \subseteq \mathcal{O}$ is an ideal. Moreover, $\mathfrak{b}\mathfrak{c} = \mathfrak{b}(\mathfrak{b}^{-1}\mathfrak{a}) = \mathfrak{a}$. □

Lemma 2.29. If $\mathcal{O}$ is a UFD, if $\mathfrak{p} \subseteq \mathcal{O}$ is prime, then $\mathfrak{p}$ is principal.

Proof. Since $\mathcal{O}$ is Dedekind, $\mathfrak{p}$ is maximal. Let $0 \neq \alpha \in \mathfrak{p}$. If $\mathfrak{p} = \langle \alpha \rangle$, we are done. Assume $\mathfrak{p} \neq \langle \alpha \rangle$. Then $\mathfrak{p} \supsetneq \langle \alpha \rangle$. Then there exists an ideal $0 \neq \mathfrak{b} \subsetneq \mathcal{O}$ such that $\mathfrak{p}\mathfrak{b} = \langle \alpha \rangle$. So $\mathfrak{b}$ has a prime factorization: $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$. So $\langle \alpha \rangle = \mathfrak{p}\mathfrak{b} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$. Also, since $\mathcal{O}$ is a UFD, the element $\alpha \in \mathcal{O}$ has a unique factorization $\alpha = uw_1 \cdots w_m$ with irreducible elements $w_1, \ldots, w_m \in \mathcal{O}$ and $u \in \mathcal{O}^\times$. So $\langle \alpha \rangle = \langle w_1 \rangle \cdots \langle w_m \rangle$. Also, since $\mathcal{O}$ is a UFD, $\langle w_j \rangle \subseteq \mathcal{O}$ is prime for $i = 1, \ldots, r$. Since the prime factorization of $\langle \alpha \rangle$ is unique, we have $m = r + 1$ and $\mathfrak{p} = \langle w_j \rangle$ for some $j \in \{1, \ldots, m\}$. □

Theorem 2.30. *$\mathcal{O}$ is a PID if and only if $\mathcal{O}$ is a UFD.*

Proof. $\Longrightarrow$ PID implies UFD in general.

$\Longleftarrow$ Suppose $\mathcal{O}$ is a UFD and let $0 \neq \mathfrak{a} \subsetneq \mathcal{O}$ be an ideal. Then $\mathfrak{a}$ can be factored into a product of prime ideals $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ with $e_1, \ldots, e_n \geqslant 1$. Since each prime $\mathfrak{p}_i \subseteq \mathcal{O}$ is principal, so is $\mathfrak{a}$ with the generator for $\mathfrak{a}$ being the product of the these generators. □

Theorem 2.31 (CRT)**.** *Let R be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals in R such that $\mathfrak{a}_i + \mathfrak{a}_j = R$ for any $i \neq j$. Set $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i$. Then $R/\mathfrak{a} \cong \bigoplus_{i=1}^n R/\mathfrak{a}_i$.*

2.1 Fractional ideal

Assumption 2.32. Let $\mathcal{O}$ be a Dedekind domain and $\mathcal{K} = \mathrm{Frac}(\mathcal{O})$ the field of fraction.

Definition 2.33. A *fractional ideal* $I \neq 0$ of $\mathcal{K}$ is an $\mathcal{O}$-submodule of $\mathcal{K}$, such that for some $d \in \mathcal{O} \smallsetminus \{0\}, dI \subseteq \mathcal{O}$ is an ideal. Such a d is called a *common denominator* for I.

Theorem 2.34. *If $0 \neq I$ is a finitely generated $\mathcal{O}$-submodule of $\mathcal{K}$, then I is a fractional ideal.*

Proof. Let $I = \langle x_1, \ldots, x_r \rangle \mathcal{O}$ for some $x_1, \ldots, x_r \in \mathcal{K}$. Since $\mathcal{K} = \mathrm{Frac}(\mathcal{O})$, there is a $d_i \in \mathcal{O} \smallsetminus \{0\}$ such that $d_i x_i \in \mathcal{O}$ for $i = 1, \ldots, r$. Let $d := d_1 \cdots d_r \in \mathcal{O} \smallsetminus \{0\}$, then $dx_i \in \mathcal{O}$ for $i = 1, \ldots, r$ and so $dI \subseteq \mathcal{O}$. □

Theorem 2.35. *$0 \neq I$ is a fractional ideal of $\mathcal{K}$ if and only if $I = \frac{1}{d}\mathfrak{a}$ for some $d \in \mathcal{K}^\times$ (or $\mathcal{O} \smallsetminus \{0\}$ or $\mathbb{Z} \smallsetminus \{0\}$ if $\mathcal{K}$ is a number field) and some ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}$.*

Proof. $\Longrightarrow$ By definition, there exists $d \in \mathcal{O} \smallsetminus 0$ such that $\mathfrak{a} := dI \subseteq \mathcal{O}$ is an ideal and $\mathfrak{a} \neq 0$. So $I = \frac{1}{d}\mathfrak{a}$ with $d \in \mathcal{K}^\times$. Similarly, if $\mathcal{K}$ is a number field, then $d \mid \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(d) \in \mathbb{Z} \smallsetminus \{0\}$, so $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(d) I \subseteq \mathcal{O}$ is an ideal.

$\Longleftarrow$ Since $\mathcal{O}$ is a Dedekind domain and $\mathfrak{a} \subseteq \mathcal{O}$ is an ideal, we have $I = \frac{1}{d}\mathfrak{a}$ is a finitely generated $\mathcal{O}$-module of $\mathcal{K}$. □

Corollary 2.36. *I is a fractional ideal of $\mathcal{K}$ if and only if $I = d\mathfrak{a}$ for some $d \in \mathcal{K}^\times$ and some ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}$.*

Definition 2.37. Nonzero ideals in $\mathcal{O}$ are called *integral ideals*.

Definition 2.38. We denote the *collection of fraction ideals* in $\mathcal{K}$ by $J_{\mathcal{K}}$.

Fact 2.39. When $\mathcal{O}$ is a PID, all fractional ideals in $\mathcal{K}$ are principal and conversely.

Theorem 2.40. *The set $J_{\mathcal{K}}$ forms an abelian group under multipliciton with identity $\mathcal{O}$ and the inverse of $\mathfrak{a} \in J_{\mathcal{K}}$ is given by $\mathfrak{a}^{-1}$.*

Proof. Clearly, $J_{\mathcal{K}}$ is abelian and that $\mathcal{O}$ is the identity. Let $\mathfrak{a}, \mathfrak{b} \in J_{\mathcal{K}}$. Then there are $\alpha_1, \ldots, \alpha_r \in \mathcal{K}$ not all 0 and $\beta_1, \ldots, \beta_s \in \mathcal{K}$ not all 0 such that $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_r \rangle \mathcal{O}$ and $\mathfrak{b} = \langle \beta_1, \ldots, \beta_s \rangle \mathcal{O}$. Then $\mathfrak{ab} = \langle \alpha_1\beta_1, \ldots, \alpha_r\beta_s \rangle \neq 0$ and so $\mathfrak{ab} \in J_{\mathcal{K}}$. Let $\mathfrak{a} \in J_{\mathcal{K}}$. Then there exists $c \in \mathcal{O} \smallsetminus \{0\}$ such that $c\mathfrak{a} \subseteq \mathcal{O}$. Claim. $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1}$. "$\subseteq$". Let $x \in (c\mathfrak{a})^{-1}$, then $(xc)\mathfrak{a} = x(c\mathfrak{a}) \subseteq \mathcal{O}$ and so $xc \in \mathfrak{a}^{-1}$ and hence $x = c^{-1}(xc) \in c^{-1}\mathfrak{a}^{-1}$. "$\supseteq$". Let $x \in c^{-1}\mathfrak{a}^{-1}$, then there exists $y \in \mathfrak{a}^{-1}$ such that $x = c^{-1}y$ and so $x(c\mathfrak{a}) = c^{-1}y(c\mathfrak{a}) = y\mathfrak{a} \in \mathcal{O}$. So $x \in (c\mathfrak{a})^{-1}$. Hence $\mathfrak{a}\mathfrak{a}^{-1} = c\mathfrak{a}c^{-1}\mathfrak{a}^{-1} = (c\mathfrak{a})(c\mathfrak{a})^{-1} = \mathcal{O}$. Assume $\mathfrak{a} = \frac{\mathfrak{a}^*}{d}$ for some $d \in \mathcal{O} \smallsetminus \{0\}$ and some ideal $\mathfrak{a}^* \subseteq \mathcal{O}$. Let $0 \neq x := \frac{a}{d} \in \mathfrak{a}$ with $a \in \mathfrak{a}^*$. Then $dx = a \in \mathfrak{a}^*$. So $\mathfrak{a}^{-1} = (d^{-1}\mathfrak{a}^*)^{-1} = d(\mathfrak{a}^*)^{-1}$. Hence $x\mathfrak{a}^{-1} = (dx)(\mathfrak{a}^*)^{-1} \subseteq \mathcal{O}$. So $\mathfrak{a}^{-1} \in J_{\mathcal{K}}$. At last, the associative law follows from the associativity of $\mathcal{K}$. □

Corollary 2.41. Let $\mathfrak{a} \in J_{\mathcal{K}}$. If there exists $\mathfrak{b} \in J_{\mathcal{K}}$ such that $\mathfrak{ab} = \mathcal{O}$, then $\mathfrak{b} = \mathfrak{a}^{-1}$.

Corollary 2.42. Let $\mathfrak{a}, \mathfrak{b} \in J_{\mathcal{K}}$ be ideals. Then $(\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}$.

Proof. We have $\mathfrak{ab} \in J_{\mathcal{K}}$ and $\mathfrak{a}^{-1}, \mathfrak{b}^{-1} \in J_{\mathcal{K}}$. Hence $\mathfrak{b}^{-1}\mathfrak{a}^{-1} \in J_{\mathcal{K}}$. Since $(\mathfrak{ab})(\mathfrak{b}^{-1}\mathfrak{a}^{-1}) = \mathcal{O}$, we have $(\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}$. □

Corollary 2.43. Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be ideals. Then $(\mathfrak{ab})^{-1} = \mathfrak{b}^{-1}\mathfrak{a}^{-1}$.

Lemma 2.44. Let $\mathfrak{a} \in J_{\mathcal{K}}$. Then $\mathfrak{a}$ can be written as $\mathfrak{a} = \mathfrak{bc}^{-1}$ with $\mathfrak{b}, \mathfrak{c} \subseteq \mathcal{O}$ ideals.

Proof. Since $\mathfrak{a} \in J_{\mathcal{K}}$, there exists $d \in \mathcal{O}_{\mathcal{K}}^{\times}$ and an ideal $\mathfrak{b} \subseteq \mathcal{O}$ such that $\mathfrak{a} = \frac{\mathfrak{b}}{d}$. So $\mathfrak{b} \in J_{\mathcal{K}}$. Let $\mathfrak{c} := d\mathcal{O} \in J_{\mathcal{K}}$, then $\mathfrak{ac} = d\mathfrak{a} = \mathfrak{b}$. Since $J_{\mathcal{K}}$ is a group, $\mathfrak{a} = \mathfrak{bc}^{-1}$. □

Corollary 2.45. Every $\mathfrak{a} \in J_{\mathcal{K}}$ admits a unique representation as a product $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$, where $\mathfrak{p} \subseteq \mathcal{O}$ is prime and $\nu_{\mathfrak{p}} \in \mathbb{Z} \setminus \{0\}$. In other words, $J_{\mathcal{K}}$ is isomorpic to the free abelian group generated by the nonzero prime ideals in $\mathcal{O}$.

Proof. Note that $\mathfrak{a}$ can be written as $\mathfrak{a} = \mathfrak{bc}^{-1}$ with $\mathfrak{b}, \mathfrak{c} \subseteq \mathcal{O}$ ideals. Since $\mathfrak{b}$ and $\mathfrak{c}$ has a unique prime factorization, $\mathfrak{a}$ has a unique prime decomposition of the type stated in the corollary. □

Corollary 2.46. $\mathfrak{a} \in J_{\mathcal{K}}$ is an integral ideal if and only if every exponent of its prime factors is positive in its prime factorization.

Example 2.47. Since $\mathbb{Z}$ is a PID, the fractional ideals in $\mathbb{Q}$ are $\mathbb{Z}$-submodules (subgroups) of $\mathbb{Q}$ having the form $r\mathbb{Z}$ for $r \in \mathbb{Q}^{\times}$. Examples include $\frac{1}{2}\mathbb{Z}$ and $\frac{6}{5}\mathbb{Z} = \frac{6\mathbb{Z}}{5}$.

Definition 2.48. A fractional ideal of the form $x\mathcal{O} = \langle x \rangle$ for some $x \in \mathcal{K}^{\times}$ is called *principal fractional ideal*. The principal fractional ideals form a subgroup $P_{\mathcal{K}}$ of $J_{\mathcal{K}}$.

Definition 2.49. The *ideal class group* of $\mathcal{K}$ is the abelian group $\mathrm{Cl}(\mathcal{K}) = \mathrm{Cl}_{\mathcal{K}} = \mathrm{Cl}(\mathcal{O}) = J_{\mathcal{K}}/P_{\mathcal{K}}$ measures whether $\mathcal{O}$ is a unique factorization domain or principal ideal domain.

Remark. If $\mathrm{Cl}(\mathcal{K}) = \{0\}$, then every fractional ideal is principal. The larger $\mathrm{Cl}(\mathcal{K})$ is the further you are from having all ideals are principal.

Fact 2.50. The *class number*

$$h_{\mathcal{K}} = |\mathrm{Cl}(\mathcal{K})| = [J_{\mathcal{K}} : P_{\mathcal{K}}] < \infty.$$

Example 2.51. $\mathbb{Q}[x]$ is a PID, so it is a Dedekind domain. So $\mathbb{Q}[x]$ is integrally closed with field of fraction $\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in \mathbb{Q}[x] \text{ and } g \neq 0 \right\}$.

Proof. It is similar to the proof for $\mathbb{Z}$. □

Remark. Let $\mathcal{O} = \mathbb{Z}\sqrt{-5}$, which is not a UFD. Since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3 \in \langle 3 \rangle$ but $1 \pm \sqrt{-5} \notin \langle 3 \rangle$, we have but $\langle 3 \rangle$ is not prime. Check that $3 \in \mathcal{O}$ is irreducible.

Definition 2.52. Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal, the absolute norm $\mathfrak{N}$ of $\mathfrak{a}$ is

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}|.$$

Lemma 2.53. Let $0 \neq \alpha \in \mathcal{O}$, then $\mathfrak{N}(\langle \alpha \rangle) = \left| \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) \right|$.

Proof. Exercise. □

Corollary 2.54. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal. Then $\mathfrak{N}(\mathfrak{a}) < \infty$.

Proof. Let $0 \neq \alpha \in \mathfrak{a}$. Since $\mathfrak{a} \subseteq \mathcal{O}$ and $\alpha\mathcal{O} \subseteq \mathcal{O}$ are ideals, we have a surjective map $\mathcal{O}/\alpha\mathcal{O} \to \mathcal{O}/\mathfrak{a}$. Then $\mathfrak{N}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}| \leqslant |\mathcal{O}/\alpha\mathcal{O}| = \mathfrak{N}(\langle\alpha\rangle) = \left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)\right| < \infty$. □

Theorem 2.55. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal, write $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ for prime factorization. Then $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$, i.e., $\mathfrak{N}$ is multiplicative.*

Proof. By CRT, $\mathcal{O}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{p}_1^{\nu_1} \oplus \cdots \oplus \mathcal{O}/\mathfrak{p}_r^{\nu_r}$. We are thus reduced to considering the case where $\mathfrak{a}$ is a prime power $\mathfrak{p}^\nu$. In the chain $\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^\nu$, one has $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ because of the unique prime factorization. Since $\mathfrak{p}\mathfrak{p}^i/\mathfrak{p}^{i+1} = 0$, the quotient $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ is an $\mathcal{O}/\mathfrak{p}$-vector space for $i = 1, \ldots, r$. Let $a \in \mathfrak{p}^i \smallsetminus \mathfrak{p}^{i+1}$ and $\mathfrak{b} := \langle a\rangle + \mathfrak{p}^{i+1}$, then $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{i+1}$. So $\mathfrak{p}^i = \mathfrak{b}$, otherwise, since $\langle a\rangle \subseteq \mathfrak{p}^i$, $\mathfrak{b}' := \mathfrak{b}\mathfrak{p}^{-i} = \langle a\rangle\mathfrak{p}^{-i} + \mathfrak{p} = \langle a\rangle(\mathfrak{p}^i)^{-1} + \mathfrak{p} \subseteq \mathcal{O}$, would be a proper divisor of $\mathfrak{p}$ since $(\mathfrak{p}^i)^{-1} \supsetneq \mathcal{O}$, which is contradicted by $\mathfrak{p}$ is prime. Hence $a + \mathfrak{p}^{i+1}$ is a basis of the $\mathcal{O}/\mathfrak{p}$-vector space $\mathfrak{p}^i/\mathfrak{p}^{i+1} = \langle a\rangle/\mathfrak{p}^{i+1}$. Thus, $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathcal{O}/\mathfrak{p}$ and so $\mathfrak{N}(\mathfrak{p}^\nu) = [\mathcal{O} : \mathfrak{p}^\nu] = [\mathcal{O} : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu] = \mathfrak{N}(\mathfrak{p})^\nu$. □

2.2 Revisit quadratic field

Definition 2.56. A number field $\mathcal{K}/\mathbb{Q}$ is a *quadratic field* if $\deg(\mathcal{K}/\mathbb{Q}) = 2$.

Lemma 2.57. A field $\mathcal{K}/\mathbb{Q}$ is quadratic if and only if there exists $d \in \mathbb{Z} \smallsetminus \{0\}$ square-free such that $\mathcal{K} = \mathbb{Q}(\sqrt{d})$.

Proof. $\Longleftarrow$ Use definition.

$\Longrightarrow$ Let $\alpha \in \mathcal{K} \smallsetminus \mathbb{Q}$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geqslant 2$. Also, since $2 = [\mathcal{K} : \mathbb{Q}] = [\mathcal{K} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \geqslant 2 \cdot [\mathcal{K} : \mathbb{Q}(\alpha)]$, we have $[\mathcal{K} : \mathbb{Q}(\alpha)] = 1$. Since $\alpha \in \mathcal{K} \smallsetminus \mathbb{Q}$, there exists $b', c' \in \mathbb{Q}$ such that $\alpha^2 + b'\alpha + c' = 0$. Then we can choose suitable $a, b, c \in \mathbb{Z}$ with $a \neq 0$ such that $a\alpha^2 + b\alpha + c = 0$. So $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = -\frac{b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a}$ or $\sqrt{b^2 - 4ac} = \pm(2a\alpha + b)$ and so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Let $d' := b^2 - 4ac \in \mathbb{Z}$. Since $\alpha \notin \mathbb{Q}$, d' is not a perfect square. Also, since $d' \neq 0$, d' can be written uniquely in the form $d' = de$, where d is a square-free and e is a perfect square. So $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d'}) = \mathbb{Q}(\sqrt{de}) = \mathbb{Q}(\sqrt{d})$. □

Lemma 2.58. Let $\mathcal{K}$ be a quadratic field and $\alpha \in \mathcal{K}$. $\alpha \in \mathcal{O}_\mathcal{K}$ if and only if $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha),\ \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Proof. $\Longrightarrow$ If $\alpha \in \mathbb{Q}$, it is obvious. Now let $\alpha \in \mathcal{K} \smallsetminus \mathbb{Q}$. Then there exist $a, b \in \mathbb{Z}$ such that $m_\alpha(\alpha) = \alpha^2 + a\alpha + b = 0$. Let $\{\sigma_1, \sigma_2\}$ be the distinct embeddings $\mathcal{K} \hookrightarrow \overline{\mathbb{Q}}$. Then

$$0 = (\alpha - \sigma_1(\alpha))(\alpha - \sigma_2(\alpha)) = \alpha^2 - \alpha(\sigma_1(\alpha) + \sigma_2(\alpha)) - \sigma_1(\alpha)\sigma_2(\alpha) = \alpha^2 - \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha)\alpha + \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha),$$

which is irreducible, otherwise $\alpha \in \mathbb{Q}$. Since the minimal polynomial is unique, $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha) = a \in \mathbb{Z}$ and $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = b \in \mathbb{Z}$.

$\Longleftarrow$ $m_\alpha(x) = x - \alpha \in \mathbb{Z}[x]$ or $m_\alpha(x) = x^2 - \mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(\alpha)x + \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. □

Example 2.59. Let $\mathcal{K} = \mathbb{Q}(i)$. Then $\mathcal{O}_\mathcal{K}$ is a PID.

Proof. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_\mathcal{K}$ be an ideal. Since $\mathrm{Im}(|\mathrm{N}|_{\mathcal{K}/\mathbb{Q}}) \subseteq \mathbb{N}$, we can choose $0 \neq a \in \mathfrak{a}$ with $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right|$ minimal. Let $b \in \mathfrak{a}$. Then $b/a \in \mathbb{Q}(i)$. Choose $c \in \mathcal{O}_\mathcal{K} = \mathbb{Z}[i]$ that is the closest to b/a, then $|c - b/a| \leqslant \sqrt{2}/2$. Let $r := b - ac \in \mathcal{O}_\mathcal{K}$, since $a \neq 0$,

$$\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(r)\right| = |b - ac|^2 = |a|^2|c - b/a|^2 \leqslant |a|^2(\sqrt{2}/2)^2 = \frac{1}{2}|a|^2 = \frac{1}{2}\,\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a) < \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a).$$

Also, since $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right|$ is minimal, we have $r = 0$ and then $b \in \langle a\rangle$ and so $\mathfrak{a} \subseteq \langle a\rangle$. Hence, $\mathfrak{a} = \langle a\rangle$ and thus $\mathcal{O}_\mathcal{K}$ is a PID. □

Remark. Now we want to consider given a prime $p \in \mathbb{Z} \subseteq \mathbb{Z}[i]$, what does $p\mathbb{Z}[i]$ look like? Note $p\mathbb{Z}[i] \lneq \mathbb{Z}[i]$. The ideal $p\mathbb{Z}[i]$ has a prime factorization: $p\mathbb{Z}[i] = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then what are the $\mathfrak{p}_j$'s, e_j's and r?

Example 2.60. Let $\mathcal{K} = \mathbb{Q}(i)$. The ideal $p\mathbb{Z}[i]$ has a prime factorization: $p\mathbb{Z}[i] = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. By CRT,

$$\bigoplus_{j=1}^{r} \mathbb{Z}[i]/\mathfrak{p}_j^{e_j} \cong \mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{Z}[i]/\langle p\rangle \cong \mathbb{Z}[x]/\langle p, x^2+1\rangle \cong \mathbb{F}_p[x]/\langle x^2+1\rangle.$$

To see x^2+1 factors in $\mathbb{F}_p[x]$, we need to see whether -1 is a square module p or not. Since for $p \neq 2$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ if and only if $p \equiv 1 \pmod 4$, we have with $\alpha \in \mathbb{Z}$ and $\alpha^2 \equiv -1 \pmod p$,

$$x^2 + 1 = x^2 - (-1) \equiv \begin{cases} (x+1)^2 \pmod p & \text{if } p = 2, \\ x^2 + 1 \pmod p & \text{if } p \equiv 3 \pmod 4, \\ (x-\alpha)(x+\alpha) \pmod p & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Since $(2, 1+i)\mathbb{Z}[i] = (1+i)\mathbb{Z}[i] = \langle 1+i\rangle$,

$$p\mathbb{Z}[i] = \begin{cases} \langle i+1\rangle^2 & \text{if } p = 2, \\ p\mathbb{Z}[i] & \text{if } p \equiv 3 \pmod 4, \\ \langle p, i+\alpha\rangle\langle p, i-\alpha\rangle & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Thus,

$$\begin{cases} r = 1, e = 2, \\ r = 1, e = 1, \\ r = 2, e_1 = e_2 = 1. \end{cases}.$$

Lemma 2.61. Let $\mathcal{K}$ be a quadratic field and $p \in \mathbb{N}$ an odd prime. Then $p\mathcal{O}_\mathcal{K}$ has a prime factorization:

$$p\mathcal{O}_\mathcal{K} = \begin{cases} \mathfrak{p}^2 & \text{if } p \mid \Delta_\mathcal{K}, \\ \mathfrak{p}_1\mathfrak{p}_2 (\mathfrak{p}_1 \neq \mathfrak{p}_2) & \text{if } \left(\frac{\Delta_\mathcal{K}}{p}\right) = 1, \\ p\mathcal{O}_\mathcal{K} & \textit{otherwise.} \end{cases}$$

Proof. We have there exists $d \in \mathbb{Z} \setminus \{0\}$ square-free such that $\mathcal{K} = \mathbb{Q}(\sqrt{d})$. We have

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

and

$$\Delta_{\mathcal{K}} = \begin{cases} 4d & \text{if } d \equiv 2,3 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4 \end{cases}.$$

Assume the ideal $p\mathbb{Z}[i]$ has a prime factorization: $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

(a) Let $d \equiv 2,3 \pmod 4$. By CRT,

$$\bigoplus_{j=1}^{r} \mathcal{O}_{\mathcal{K}}/\mathfrak{p}_j^{e_j} \cong \mathcal{O}_{\mathcal{K}}/p\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}}/\langle p \rangle \cong \mathbb{Z}[x]/\langle p, x^2 - d \rangle \cong \mathbb{F}_p[x]/\langle x^2 - \bar{d} \rangle.$$

To see $x^2 - d$ factors in $\mathbb{F}_p[x]$, we need to see whether d is a square module p or not. Since for $p \neq 2$, $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{\Delta_{\mathcal{K}}}{p}\right)$ and $(x^2 - d) - (x - d)^2 \equiv -d(d+1) \equiv 0 \pmod 2$, we have with $\alpha \in \mathbb{Z}$ and $\alpha^2 \equiv d \pmod p$,

$$x^2 - d \equiv \begin{cases} (x-d)^2 \pmod p & \text{if } p = 2 \\ x^2 \pmod p & \text{if } p \text{ is odd and } p \mid \Delta_{\mathcal{K}} \\ (x-\alpha)(x+\alpha) \pmod p & \text{if } p \text{ is odd and } \left(\frac{\Delta_{\mathcal{K}}}{p}\right) = 1 \\ x^2 - d \pmod p & \text{otherwise} \end{cases}.$$

So

$$p\mathcal{O}_{\mathcal{K}} = \begin{cases} \langle 2, \sqrt{d} - d \rangle^2 & \text{if } p = 2 \\ \langle \sqrt{d} \rangle^2 & \text{if } p \text{ is odd and } p \mid \Delta_{\mathcal{K}} \\ \langle p, \sqrt{d} - \alpha \rangle \langle p, \sqrt{d} + \alpha \rangle & p \text{ is odd and } \left(\frac{\Delta_{\mathcal{K}}}{p}\right) = 1 \\ p\mathcal{O}_{\mathcal{K}} & \text{otherwise} \end{cases}.$$

- ☐ The *inert* case: $x^2 - d$ is irreducible modulo p. Then

$$\mathcal{O}_{\mathcal{K}}/p\mathcal{O}_{\mathcal{K}} \cong \mathbb{F}_p/\langle x^2 - \bar{d} \rangle = \{a + bx \mid a, b \in \mathbb{F}_p, x^2 = \bar{d}\}$$

  is a field. It is an extension of $\mathbb{F}_p$ of degree 2 which one might denote $\mathbb{F}_p(\sqrt{\bar{d}})$ and hence a finite field with p^2 elements.

- ☐ The *split* case: $x^2 - d$ is a product of two different linear factors modulo p. By CRT, we have an isomorphism

$$\mathcal{O}_{\mathcal{K}}/p\mathcal{O}_{\mathcal{K}} \cong \mathbb{F}_p[x]/\langle (x - \bar{\alpha})(x + \bar{\alpha}) \rangle = \mathbb{F}_p[x]/\langle x - \bar{\alpha} \rangle \times \mathbb{F}_p[x]/\langle x + \bar{\alpha} \rangle \cong \mathbb{F}_p \times \mathbb{F}_p.$$

- ☐ The *ramified* case: $x^2 - d$ is a square modulo p. This happes if $p = 2$ or $p \mid \Delta_{\mathcal{K}} = 4d$. In both cases, $\mathcal{O}_{\mathcal{K}}/p\mathcal{O}_{\mathcal{K}}$ is non-reduced and then has nilpotent elements.

(b) Let $d \equiv 1 \pmod 4$. Let $f(x) = x^2 - x + \frac{1-d}{4} \in \mathbb{Z}[x]$. Since $\Delta = \sqrt{1 - 4\frac{1-d}{4}} = \sqrt{d}$ and d is not a perfect square, f is irreducible. Then $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \cong \mathbb{Z}[x]/\langle f(x) \rangle$. By CRT,

$$\bigoplus_{j=1}^{r} \mathcal{O}_{\mathcal{K}}/\mathfrak{p}_j^{e_j} \cong \mathcal{O}_{\mathcal{K}}/p\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}}/\langle p \rangle \cong \mathbb{Z}[x]/\langle p, f(x) \rangle \cong \mathbb{F}_p[x]/\langle f(x) \rangle.$$

To see $f(x) = x^2 - x + \frac{1-d}{4}$ factors in $\mathbb{F}_p[x]$, we need to see whether d is a square module p or not.

(1) Let $p \neq 2$. Then $\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^2 \left(\frac{d}{p}\right) = \left(\frac{4d}{p}\right) = \left(\frac{\Delta_\mathcal{K}}{p}\right)$. Since $d = \Delta_\mathcal{K}$, we have

$$x^2 - x + \frac{1-d}{4} = \left(x - \frac{1+\sqrt{\Delta_\mathcal{K}}}{2}\right)\left(x - \frac{1-\sqrt{\Delta_\mathcal{K}}}{2}\right)$$
$$\equiv \begin{cases} (x-1/2)^2 \pmod p & \text{if } p \mid \Delta_\mathcal{K} \\ (x-\alpha)(x-\overline{\alpha}) \pmod p & \text{if } \left(\frac{\Delta_\mathcal{K}}{p}\right) = 1 \\ x^2 - x + \frac{1-d}{4} \pmod p & \text{otherwise} \end{cases}.$$

So

$$p\mathcal{O}_\mathcal{K} = \begin{cases} \langle p, \frac{\sqrt{d}}{2}\rangle^2 & \text{if } p \mid \Delta_\mathcal{K} \\ \langle p, \frac{1+\sqrt{d}}{2} - \alpha\rangle\langle p, \frac{1+\sqrt{d}}{2} - \overline{\alpha}\rangle & \text{if } \left(\frac{\Delta_\mathcal{K}}{p}\right) = 1 \\ p\mathcal{O}_\mathcal{K} & \text{otherwise} \end{cases}.$$

(2) Let $p = 2$. Note

$$x^2 - x + \frac{1-d}{4} \equiv \begin{cases} x(x-1) \pmod 2 & \text{if } d \equiv 1 \pmod 8 \\ x^2 - x + 1 \pmod 2 & \text{if } d \equiv 5 \pmod 8 \end{cases}.$$

Alos, since $(2, \frac{1+\sqrt{d}}{2})\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \frac{1+\sqrt{d}}{2}\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, we have

$$2\mathcal{O}_\mathcal{K} = \begin{cases} \langle\frac{1+\sqrt{d}}{2}\rangle\langle\frac{1-\sqrt{d}}{2}\rangle & \text{if } d \equiv 1 \pmod 8 \\ 2\mathcal{O}_\mathcal{K} & \text{if } d \equiv 5 \pmod 8 \end{cases}. \qquad \square$$

Definition 2.62. Let $\mathcal{K}$ be a quadratic field. If $p\mathcal{O}_\mathcal{K} = \mathfrak{p}^2$, we say p *ramifies* in $\mathcal{O}_\mathcal{K}$; if $p\mathcal{O}_\mathcal{K} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$, we say p *splits* in $\mathcal{O}_\mathcal{K}$; if $p\mathcal{O}_\mathcal{K} \subseteq \mathcal{O}_\mathcal{K}$ is prime, we say p is *inert* in $\mathcal{O}_\mathcal{K}$.

2.3 Extensions of Dedekind domain

Assumption 2.63. Let $\mathcal{o}$ be a Dedekind domain and $\mathcal{K} = \mathrm{Frac}(\mathcal{o})$. Let $\mathcal{L}$ be finite and separable extension of $\mathcal{K}$. Let $\mathcal{O}$ be integral closure of $\mathcal{o}$ in $\mathcal{L}$.

Remark (Questions)**.** What do prime look like in $\mathcal{O}$? Note $\mathfrak{p} := \mathfrak{P} \cap \mathcal{o} \subseteq \mathcal{o}$ is also prime for every prime $0 \neq \mathfrak{P} \subseteq \mathcal{O}$. Also, $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}$, i.e., $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}$. So the question of how primes $\mathfrak{p}\mathcal{O}$'s with prime $\mathfrak{p} \subseteq \mathcal{o}$ factor when extended to $\mathcal{O}$ answers it.

Remark. We often write $\langle\mathfrak{p}\rangle = \mathfrak{p}\mathcal{O}$.

Theorem 2.64. *$\mathcal{O}$ is a Dedekind domain.*

Proof. Since $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in $\mathcal{L}$, it is integrally closed.

Similar to the proof of Theorem 2.9, we have $\mathcal{O}/\mathfrak{P}$ is an extension of the field $\mathcal{o}/\mathfrak{p}$ and every prime ideal in $\mathcal{O}$ is maximal.

Let $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}$ be a $\mathcal{K}$-basis of the separable extension $\mathcal{L}/\mathcal{K}$. Then $\Delta := \Delta(\alpha_1, \ldots, \alpha_n) \neq 0$. We have $\Delta\mathcal{O} \subseteq \mathcal{o}\alpha_1 + \cdots \mathcal{o}\alpha_n =: M_1$ similar to the proof of Theorem 1.50. So $\mathcal{O} \subseteq \mathcal{o}\frac{\alpha_1}{\Delta} + \cdots + \mathcal{o}\frac{\alpha_n}{\Delta} = \frac{M_1}{\Delta}$. Also, since $\mathcal{o}$ is a Noetherian ring and $\frac{M_1}{\Delta}$ is a finitely generated $\mathcal{o}$-module, $\frac{M_1}{\Delta}$ is a Noetherian $\mathcal{o}$-module. So $\mathcal{O}$ is Noetherian. $\square$

Recall 2.65. Let M be a left R-module, define the *annihilator* of m in R by

$$\mathrm{Ann}_R(m) = \{r \in R \mid rm = 0\},$$

which is an ideal of R. The set of *torsion element* of M is defined by

$$\mathrm{Tor}(M) = \{m \in M \mid \mathrm{Ann}_R(m) \neq \{0\}\} = \{m \in M \mid rm = 0 \text{ for some } r \in R \smallsetminus 0\}.$$

An left R-module M is said to be *torsion free* if $\mathrm{Tor}(M) = \{0\}$. If R is an integral domain, $\mathrm{Tor}(M)$ is a submodule of M.

Fact 2.66. $\mathrm{Frac}(\mathcal{O}) = \mathcal{L}$ and $\mathcal{O}$ is a torsion-free $\mathcal{o}$-module.

Theorem 2.67. *Let $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime, then $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.*

Proof. There exists $\varpi \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$ such that $\mathfrak{p} \supseteq \varpi\mathcal{o}$, i.e, $\mathfrak{p} \mid \varpi\mathcal{o}$. Claim. there exists an ideal $\mathfrak{a} \subseteq \mathcal{o}$ such that $\mathfrak{p}\mathfrak{a} = \varpi\mathcal{o}$ and $\mathfrak{p} \nmid \mathfrak{a}$. Suppose not. Since $\mathfrak{p} \mid \varpi\mathcal{o}$, there exists an ideal $\mathfrak{b} \subseteq \mathcal{o}$ such that $\mathfrak{p}\mathfrak{b} = \varpi\mathcal{o}$, then $\mathfrak{p} \mid \mathfrak{b}$ by assumption, i.e., $\mathfrak{p} \supseteq \mathfrak{b}$. Then $\varpi \in \mathfrak{p}\mathfrak{b} \subseteq \mathfrak{p}^2$, a contradiction. Since $\mathfrak{p} \nmid \mathfrak{a}$, $\mathfrak{p} \subsetneq \mathfrak{p} + \mathfrak{a} \subseteq \mathcal{o}$. Since $\mathfrak{p}$ is maximal, $\mathfrak{p} + \mathfrak{a} = \mathcal{o}$. So there exist $r \in \mathfrak{p}$ and $s \in \mathfrak{a}$ such that $r + s = 1$. Since $\mathfrak{p} \subsetneq \mathcal{o}$, $s \notin \mathfrak{p}$. Suppose $\mathfrak{p}\mathcal{O} = \mathcal{O}$. Then $s\mathcal{O} = s\mathfrak{p}\mathcal{O} = \mathfrak{p}s\mathcal{O} \subseteq \mathfrak{p}\mathfrak{a}\mathcal{O} = \varpi\mathcal{o}\mathcal{O} = \varpi\mathcal{O}$. So $s = \varpi x$ for some $x \in \mathcal{O}$. Since $s\mathfrak{p} = \mathfrak{p}s \subseteq \mathfrak{p}\mathfrak{a} = \varpi\mathcal{o}$, letting $0 \neq y \in \mathfrak{p}$, there exists $z \in \mathcal{o}$ such that $sy = \varpi z$, i.e, $s = \varpi\frac{z}{y}$, i.e., $s = \varpi x'$ for some $x' \in \mathrm{Frac}(\mathcal{o}) = \mathcal{K}$. Also, since $s \neq 0 \neq \varpi$, we have $s = \varpi x$ for some $x \in \mathcal{O} \cap \mathcal{K} = \mathcal{o}$, i.e., $s \in \mathfrak{p}$, a contradcition. Thus, $\mathfrak{p}\mathcal{O} \subsetneq \mathcal{O}$. This means, given a prime $0 \neq \mathfrak{p} \subseteq \mathcal{o}$, we have a unique prime factorization $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. □

Example 2.68. We saw this for $\mathbb{Z}[i]$ by inspection: since $\mathbb{Z}[i] \ni 1 \neq p(a + bi)$, for any $a, b \in \mathbb{Z}$, $p\mathbb{Z} \cdot \mathbb{Z}[i] = p\mathbb{Z}[i] \neq \mathbb{Z}[i]$.

Lemma 2.69. Let $0 \neq \mathfrak{P} \subseteq \mathcal{O}$ be prime and $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime. Then $\mathfrak{P} \mid \mathfrak{p}$ if and only if $\mathfrak{p} = \mathfrak{P} \cap \mathcal{o}$.

Proof. $\Longrightarrow$ Note that $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{o} \subsetneq \mathcal{o}$ and $\mathfrak{p}$ is maximal, so $\mathfrak{p} = \mathfrak{P} \cap \mathcal{o}$.
$\Longleftarrow$ Note that $\mathfrak{p} \subseteq \mathfrak{P}$, so $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O} \supseteq \mathfrak{p}$. □

Definition 2.70. Let $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$. Define the *ramification index* $e(\mathfrak{P}_i/\mathfrak{p}) =: e_i$. Define the *residue class degree* $f(\mathfrak{P}_i/\mathfrak{p})$ by $f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}] =: f_i$.

Definition 2.71. Let $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$. $\mathfrak{p}$ is said to *ramify* in $\mathcal{L}$ if $e_i > 1$ for some $i \in \{1, \ldots, r\}$; otherwise it is *unramified*.

Fact 2.72. (a) $\mathcal{o}_\mathfrak{p}$ is a discrete valuation ring and so a principal ideal domain and hence Dedekind for $\mathfrak{p} \subseteq \mathcal{o}$ prime.

(b) Let $\mathfrak{p} \subseteq \mathcal{o}$ be prime and $U := \mathcal{o} \smallsetminus \mathfrak{p}$. Then $U^{-1}\mathcal{O}$ is the integral closure of $\mathcal{o}_\mathfrak{p}$ in $\mathcal{L}$.

Theorem 2.73 (Fundamental identity)**.** *Let $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Then $[\mathcal{L} : \mathcal{K}] = \sum_{j=1}^r e_j f_j$.*

Proof. By CRT, $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{j=1}^r \mathcal{O}/\mathfrak{P}_j^{e_j}$. Set $\mathfrak{k} = \mathcal{o}/\mathfrak{p}$. For $j = 1, \ldots, r$, since $\mathfrak{p} \cdot \mathcal{O}/\mathfrak{P}^{e_j} = \mathfrak{p}\mathcal{O}/\mathfrak{P}^{e_j} = 0$, we have $\mathcal{O}/\mathfrak{P}_j^{e_j}$ is a $\mathfrak{k}$-vector space. So $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is a $\mathfrak{k}$-vector space. Then it suffices to show $\dim_\mathfrak{k}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = [\mathcal{L} : \mathcal{K}]$ and $\dim_\mathfrak{k}(\mathcal{O}/\mathfrak{P}_j^{e_j}) = e_j f_j$ for $j = 1, \ldots, r$. Since $\mathcal{O}$ is a finitely

generated $\mathcal{O}$-module, $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is also a finitely generated $\mathcal{O}$-module and then $\dim_{\mathfrak{k}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) < \infty$. Let $\{w_1, \ldots, w_m\} \subseteq \mathcal{O}$ be the representatives of a basis $\{\overline{w}_1, \ldots, \overline{w}_m\}$ of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ over $\mathfrak{k}$. Claim. $\{w_1, \ldots, w_m\}$ is a $\mathcal{K}$-basis of $\mathcal{L}/\mathcal{K}$. Suppose $\{w_1, \ldots, w_m\}$ are linearly dependent over $\mathcal{K}$. Then there exists $\underline{a}_1, \ldots, \underline{a}_m \in \mathcal{K}$ such that $\underline{a}_1 w_1 + \cdots + \underline{a}_m w_m = 0$. Let A be the LCM denominators of $\underline{a}_j, \ldots, \underline{a}_m$. Set $a_j = A\underline{a}_j \in \mathcal{O}$ for $j = 1, \ldots, m$. Then $a_1 w_1 + \cdots + a_m w_m = 0$. Set $\mathfrak{a} := \langle a_1, \ldots, a_m \rangle \subseteq \mathcal{O}$. Since $\mathfrak{a}^{-1}\mathfrak{p} \neq \mathfrak{a}^{-1}$, pick $a \in \mathfrak{a}^{-1} \smallsetminus \mathfrak{a}^{-1}\mathfrak{p}$. Then $aa_1, \ldots, aa_m \in \mathcal{O}$. Since $a \notin \mathfrak{a}^{-1}\mathfrak{p}$, $\mathfrak{p} \not\supseteq a\mathfrak{a} = \langle aa_1, \ldots, aa_m \rangle$ and then at least one of $aa_1, \ldots, aa_m$ is not in $\mathfrak{p}$. Since $aa_1 w_1 + \cdots + aa_m w_m = 0$ and $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is a $\mathcal{O}/\mathfrak{p}$-vector space, we have

$$(aa_1 + \mathfrak{p})(w_1 + \mathfrak{p}\mathcal{O}) + \cdots + (aa_m + \mathfrak{p})(w_m + \mathfrak{p}\mathcal{O}) \equiv 0 \pmod{\mathfrak{p}\mathcal{O}},$$

i.e., $(aa_1 + \mathfrak{p})\overline{w}_1 + \cdots + (aa_m + \mathfrak{p})\overline{w}_m = 0$ in $\mathcal{O}/\mathfrak{p}\mathcal{O}$, which gives us a linear dependence among the $\overline{w}_1, \ldots, \overline{w}_m$ over $\mathfrak{k}$, a contradiction. So $w_1, \ldots, w_m$ are linearly independent over $\mathcal{K}$.

Consider the $\mathcal{O}$-module $M := \mathcal{O}w_1 + \cdots + \mathcal{O}w_m \subseteq \mathcal{O}$. Let $N := \mathcal{O}/M$ and $x \in \mathcal{O}$. If $x \in \mathfrak{p}\mathcal{O}$, then $x \in M + \mathfrak{p}\mathcal{O}$. If $x \notin \mathfrak{p}\mathcal{O}$, then $0 \neq x + \mathfrak{p}\mathcal{O} \in \mathcal{O}/\mathfrak{p}\mathcal{O}$ and so there exist $b_1 + \mathfrak{p}, \ldots, b_m + \mathfrak{p} \in \mathfrak{k}$ such that $x + \mathfrak{p}\mathcal{O} = (b_1 + \mathfrak{p})(w_1 + \mathfrak{p}\mathcal{O}) + \cdots + (b_m + \mathfrak{p})(w_m + \mathfrak{p}\mathcal{O}) = b_1 w_1 + \cdots + b_m w_n + \mathfrak{p}\mathcal{O}$, i.e., $x = b_1 w_1 + \cdots + b_m w_n + \mathfrak{p}\mathcal{O} \subseteq M + \mathfrak{p}\mathcal{O}$. So $\mathcal{O} \subseteq M + \mathfrak{p}\mathcal{O}$. Also since $M \subseteq \mathcal{O}$ and $\mathfrak{p}\mathcal{O} \subseteq \mathcal{O}$, we have $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$. Then $N = \frac{\mathcal{O}}{M} = \frac{M + \mathfrak{p}\mathcal{O}}{M} = \mathfrak{p}\frac{\mathcal{O}}{M} = \mathfrak{p}N$. Since $\mathcal{O}$ is a finitely generated $\mathcal{O}$-module, N is also a finitely generated $\mathcal{O}$-module and then there exists $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_s\} \subseteq N$ such that $N = \mathcal{O}(\overline{\alpha}_1, \ldots, \overline{\alpha}_s)$. Since $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_s\} \subseteq N = \mathfrak{p}N = \mathfrak{p}(\overline{\alpha}_1, \ldots, \overline{\alpha}_s)$, we can write $\overline{\alpha}_i = \sum_{j=1}^{s} a_{ij}\overline{\alpha}_j$ with $a_{ij} \in \mathfrak{p}$ for $i = 1, \ldots, s$. Set $A = (a_{ij}) - I_s$ and $B = A^{\mathrm{adj}}$. Then $0 = A(\overline{\alpha}_1, \ldots, \overline{\alpha}_s)^t$ and $BA = dI_s$ with $d = \det(A)$. So $0 = B0 = BA(\overline{\alpha}_1, \ldots, \overline{\alpha}_s)^t = (d\overline{\alpha}_1, \ldots, d\overline{\alpha}_s)^t$ and then $\frac{d\mathcal{O}}{M} = d\frac{\mathcal{O}}{M} = dN = (d\overline{\alpha}_1, \ldots, d\overline{\alpha}_s)\mathcal{O} = 0$. Hence $d\mathcal{O} \subseteq M = \mathcal{O}w_1 + \cdots + \mathcal{O}w_m$. Since $a_{ij} \in \mathfrak{p}$, $d = \det(A) = \det((a_{ij}) - I) \equiv (-1)^s \pmod{\mathfrak{p}}$. So $d \neq 0$. Claim. we can assume $\mathcal{O}$ is a principal ideal domain while calculating $[\mathcal{O}/\mathfrak{p}\mathcal{O} : \mathcal{O}/\mathfrak{p}]$. Let $\mathfrak{q} \subseteq \mathcal{O}$ be prime and $U := \mathcal{O} \smallsetminus \mathfrak{q}$. $\mathcal{O}_{\mathfrak{q}}/\mathfrak{q}\mathcal{O}_{\mathfrak{q}} = (\mathcal{O} \smallsetminus \mathfrak{q})^{-1}\mathcal{O}/(\mathcal{O} \smallsetminus \mathfrak{q})^{-1}\mathfrak{q} \cong (\mathcal{O}/\mathfrak{q})_{\mathfrak{q}} \cong \mathcal{O}/\mathfrak{q}$ since $\mathcal{O}/\mathfrak{q}$ is a field, and $U^{-1}\mathcal{O}/\mathfrak{q}U^{-1}\mathcal{O} \cong U^{-1}(\mathcal{O}/\mathfrak{q}\mathcal{O}) \cong \mathcal{O}/\mathfrak{q}\mathcal{O}$ since $\mathcal{O}/\mathfrak{q}\mathcal{O}$ contains the field $\mathcal{O}/\mathfrak{q}$. So $[U^{-1}\mathcal{O}/\mathfrak{q}U^{-1}\mathcal{O} : \mathcal{O}_{\mathfrak{q}}/\mathfrak{q}\mathcal{O}_{\mathfrak{q}}] = [\mathcal{O}/\mathfrak{q}\mathcal{O} : \mathcal{O}/\mathfrak{q}]$. Hence similar to the proof of Theorem 1.50,

$$\mathcal{L} = d\mathcal{L} \cong d(\mathcal{O} \otimes_{\mathcal{O}} \mathcal{K}) = d\mathcal{O} \otimes_{\mathcal{O}} \mathcal{K} \subseteq (\mathcal{O}w_1 + \cdots + \mathcal{O}w_n) \otimes_{\mathcal{O}} \mathcal{K} \cong \mathcal{K}w_1 + \cdots + \mathcal{K}w_m.$$

So $\mathcal{L} = \mathcal{K}w_1 + \cdots + \mathcal{K}w_m$. Thus, $w_1, \ldots, w_m$ is a $\mathcal{K}$-basis of $\mathcal{L}/\mathcal{K}$. Then $\dim_{\mathfrak{k}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = [\mathcal{L} : \mathcal{K}]$. In order to prove the second identity, let us consider the descending chain of $\mathfrak{k}$-vector spaces: $\mathcal{O}/\mathfrak{P}_j^{e_j} \supseteq \mathfrak{P}_j/\mathfrak{P}_j^{e_j} \supseteq \cdots \supseteq \mathfrak{P}_j^{e_j-1}/\mathfrak{P}_j^{e_j} \supseteq \{0\}$. Let $0 \leqslant \nu \leqslant e_j - 1$ and $\alpha \in \mathfrak{P}_j^{\nu} \smallsetminus \mathfrak{P}_j^{\nu+1}$. Define

$$\begin{aligned} \varphi : \mathcal{O} &\to \mathfrak{P}_j^{\nu}/\mathfrak{P}_j^{\nu+1} \\ a &\mapsto \alpha a + \mathfrak{P}_j^{\nu+1}. \end{aligned}$$

Then φ is a homomorphism with $\mathrm{Ker}(\varphi) = \mathfrak{P}_j$. Since $\mathfrak{P}_j^{\nu}\mathfrak{P}_j = \mathfrak{P}_j^{\nu+1} \subsetneq \mathfrak{P}_j^{\nu} = \mathfrak{P}_j^{\nu}\mathcal{O}$ and $\mathfrak{P}_j \subsetneq \mathcal{O}$ is maximal, there is no proper ideal between $\mathfrak{P}_j^{\nu+1}$ and $\mathfrak{P}_j^{\nu}$. Also, $\mathfrak{P}_j^{\nu} \mid \alpha\mathcal{O}$ and $\mathfrak{P}_j^{\nu} \mid \mathfrak{P}_j^{\nu+1}$, we have $\mathfrak{P}_j^{\nu} = \gcd(\alpha\mathcal{O}, \mathfrak{P}_j^{\nu+1}) = \alpha\mathcal{O} + \mathfrak{P}_j^{\nu+1}$ and then $\mathfrak{P}_j^{\nu}/\mathfrak{P}_j^{\nu+1} = \alpha\mathcal{O}/\mathfrak{P}_j^{\nu+1} = \mathrm{Im}(\varphi)$. Hence φ is surjective and so $\mathfrak{P}_j^{\nu}/\mathfrak{P}_j^{\nu+1} \cong \mathcal{O}/\mathfrak{P}_j$. Thus, $\dim_{\mathfrak{k}}(\mathfrak{P}_j^{\nu}/\mathfrak{P}_j^{\nu+1}) = \dim_{\mathfrak{k}}(\mathcal{O}/\mathfrak{P}_j) = [\mathcal{O}/\mathfrak{P}_j : \mathfrak{k}] = f_j$. Therefore, each quotient in the chain $\mathcal{O} \supseteq \mathfrak{P}_j \supseteq \mathfrak{P}_j^2 \supseteq \cdots \supseteq \mathfrak{P}_j^{e_j}$ has dimension f_j over $\mathfrak{k}$. So each successive quotient in the filtration $\mathcal{O}/\mathfrak{P}_j^{e_j} \supseteq \mathfrak{P}_j/\mathfrak{P}_j^{e_j} \supseteq \mathfrak{P}_j^2/\mathfrak{P}_j^{e_j} \supseteq \cdots \supseteq 0$ has dimension f_j over $\mathfrak{k}$. So

$$\dim_{\mathfrak{k}}(\mathcal{O}/\mathfrak{P}_j^{e_j}) = \sum_{\nu=0}^{e_j-1} \dim_{\mathfrak{k}}(\mathfrak{P}_j^{\nu}/\mathfrak{P}_j^{\nu+1}) = \sum_{\nu=0}^{e_j-1} f_j = e_j f_j. \qquad \square$$

Example 2.74. Let $\mathcal{o} = \mathbb{Z}$ and $\mathcal{K} = \mathbb{Q}$ and $\mathcal{L} = \mathbb{Q}(i)$. Then $\mathcal{O} = \mathbb{Z}[i]$ and $[\mathcal{L} : \mathcal{K}] = 2$. Recall

$$p\mathbb{Z}[i] = \begin{cases} \langle 1+i\rangle^2 & \text{if } p = 2 \\ p\mathbb{Z}[i] & \text{if } p \equiv 3 \pmod 4 \\ \mathfrak{p}_1\mathfrak{p}_2 = \langle p, i+\alpha\rangle\langle p, i-\alpha\rangle & \text{if } p \equiv 1 \pmod 4 \end{cases},$$

with

$$\begin{cases} r = 1, e = 2 \\ r = 1, e = 1 \\ r = 2, e_1 = e_2 = 1 \end{cases}.$$

(a) Let $p = 2$. Since $e(\langle 1+i\rangle/2) = 2$, we have $[\mathbb{Z}[i]/\langle 1+i\rangle : \mathbb{Z}/2\mathbb{Z}] = f(\langle 1+i\rangle/2) = 1$. So $\mathbb{Z}[i]/\langle 1+i\rangle \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. Or we can check this directly. Since $\langle 2\rangle = \langle 1+i\rangle^2$ and the prime factorization is unique, we have $\langle 1+i\rangle \leqslant \mathbb{Z}[i]$ is prime. Or since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(1+i) = 2$ is prime in $\mathbb{Z}$, by the multiplicativity of $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}$, $1+i$ is prime in $\mathbb{Z}[i]$ and so $\langle 1+i\rangle \leqslant \mathbb{Z}[i]$ is prime. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}[i]/\langle 1+i\rangle \\ m &\mapsto m + \langle 1+i\rangle \end{aligned}$$

Since $\varphi(1) = 1 + \langle 1+i\rangle$ and $\varphi(-1) = -1 + \langle 1+i\rangle = i + \langle 1+i\rangle$, we have φ is surjective. Since in $\mathbb{Z}[i]$, $1+i \mid 2$ and then $2\mathbb{Z} \subseteq \mathrm{Ker}(\varphi)$. Let $m \in \mathrm{Ker}(\varphi) \subseteq \mathbb{Z}$. Then $1+i \mid m$. So $2 = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(1+i) \mid \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(m) = m^2$. Hence $2 \mid m$ and so $m \in 2\mathbb{Z}$ and thus $\mathrm{Ker}(\varphi) \subseteq 2\mathbb{Z}$. Or we can check it using

$$\mathbb{Z}[i]/\langle 1+i\rangle \cong \mathbb{Z}[i]/\langle 2, 1+i\rangle \cong \mathbb{Z}[x]/\langle 2, x+1, x^2+1\rangle \cong \mathbb{F}_2[x]/\langle x+\bar{1}, (x+\bar{1})^2\rangle \cong \mathbb{F}_2[x]/\langle x+\bar{1}\rangle \cong \mathbb{F}_2.$$

(b) Let $p = 3$. Since $3\mathbb{Z}[i] \subseteq \mathbb{Z}[i]$ is prime, we have $r = 1$ and $e(3\mathbb{Z}[i]/3) = 1$, So $f(3\mathbb{Z}[i]/3) = 2$. Or we can check it directly: $\mathbb{Z}[i]/3\mathbb{Z}[i] \cong \mathbb{Z}[x]/\langle 3, x^2+1\rangle \cong \mathbb{F}_3[x]/\langle x^2+\bar{1}\rangle$. Since $\left(\frac{-1}{3}\right) = -1$, $x^2+\bar{1}$ is irreducible in $\mathbb{F}_3[x]$ and then $\mathbb{F}_3[x]/\langle x^2+1\rangle$ is a degree 2 extension of $\mathbb{F}_3$, in fact, $\mathbb{F}_3[x]/\langle x^2+1\rangle \cong \{a+b\theta \mid a, b \in \mathbb{F}_3, \theta^2 = -1\} \cong \mathbb{F}_9 \ncong \mathbb{Z}/9\mathbb{Z}$. So $f(3\mathbb{Z}[i]/3) = [\mathbb{F}_9 : \mathbb{F}_3] = 2$.

(c) Let $p = 5$. Then $5\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 = \langle 5, i+2\rangle = \langle i+2\rangle$ and $\mathfrak{p}_2 = \langle 5, i-2\rangle = \langle i-2\rangle$. Since $e(\mathfrak{p}_1/5) = 1 = e(\mathfrak{p}_2/5)$ and $2 = e(\mathfrak{p}_1/5)f(\mathfrak{p}_1/5) + e(\mathfrak{p}_2/5)f(\mathfrak{p}_2/5)$, we have $f(\mathfrak{p}_1/5) = 1 = f(\mathfrak{p}_2/5)$. Or we can check it direcly. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}[i]/\mathfrak{p}_1 \\ m &\mapsto m + \mathfrak{p}_1 \end{aligned}$$

Since $\varphi(1) = 1 + \mathfrak{p}_1$ and $\varphi(-2) = -2 + \mathfrak{p}_1 = i + \mathfrak{p}_1$, we have φ is onto. Similarly, $\mathrm{Ker}(\varphi) = 5\mathbb{Z}$. So $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}[i]/\mathfrak{p}_1$ and thus $f(\mathfrak{p}_1/\langle 5\rangle) = 1$.

2.4 Relative Extensions

Assumption 2.75. Let $\mathcal{o}$ be a Dedekind domain and $\mathcal{K} = \mathrm{Frac}(\mathcal{o})$. Let $\mathcal{L}$ be finite and separable extension of $\mathcal{K}$. Let $\mathcal{O}$ be integral closure of $\mathcal{o}$ in $\mathcal{L}$.

Definition 2.76. $\mathcal{L}/\mathcal{K}$ is called a *relative extension*.

Definition 2.77. We can generalize the application norm as follows: $\mathfrak{N} : J_{\mathcal{L}} \to J_{\mathcal{K}}$ by $\mathfrak{P} \mapsto \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, which is a group homomorphism. This defines a *relative norm* for ideals, which is itself an ideal!

Definition 2.78. (a) We define the *relative discriminant* $\Delta(\mathcal{O}/\mathcal{o})$ of $\mathcal{O}/\mathcal{o}$ be the ideal of $\mathcal{o}$ generated by elements of the form $d(\alpha_1, \dots, \alpha_n)$, where $\{\alpha_1, \dots, \alpha_n\} \subseteq \mathcal{o}_\mathcal{K}$ is a $\mathcal{K}$-basis of $\mathcal{L}$.

(b) Let $A \subseteq B$ be a subring such that $B \cong A^n$. We define the *relative discriminant* $\Delta(B/A)$ of B/A be the ideal of A generated by all A-basis of B.

Remark. The two definitions agree when they both apply.

Proposition 2.79. Assume $\mathcal{O} \cong \mathcal{o}^n$ and $\Delta(\mathcal{O}/\mathcal{o}) \neq 0$. Then $\{\beta_1, \dots, \beta_n\}$ forms an $\mathcal{o}$-basis for $\mathcal{O}$ if and only if $\Delta(\mathcal{O}/\mathcal{o}) = d(\beta_1, \dots, \beta_n)\mathcal{o}$.

Proof. $\Longleftarrow$ We are done.
$\Longrightarrow$ It follows since discriminants of bases differ by a change of basis matrix whose determinant is in $\mathcal{o}^\times$. □

Example 2.80. Let $\mathcal{K}$ be a number field, then $\Delta(\mathcal{o}_\mathcal{K}/\mathbb{Z}) = \Delta_\mathcal{K}\mathbb{Z}$.

Lemma 2.81. Assume $\mathcal{O} \cong \mathcal{o}^n$. Let $\{e_1, \dots, e_n\}$ be an $\mathcal{o}$-basis of $\mathcal{O}$ and $0 \neq \mathfrak{a} \subseteq \mathcal{o}$ an ideal. Then $\{\bar{e}_1, \dots, \bar{e}_n\} = \{e_1 \pmod{\mathfrak{a}\mathcal{O}}, \dots, e_n \pmod{\mathfrak{a}\mathcal{O}}\}$ is a basis of $\mathcal{o}/\mathfrak{a}$-module $\mathcal{O}/\mathfrak{a}\mathcal{O}$. Moreover, $d(\bar{e}_1, \dots, \bar{e}_n) \equiv d(e_1, \dots, e_n) \pmod{\mathfrak{a}}$. So $\Delta(\mathcal{O}/\mathcal{o}) \pmod{\mathfrak{a}} = \Delta\big((\mathcal{O}/\mathfrak{a}\mathcal{O})/(\mathcal{o}/\mathfrak{a})\big)$.

Proof. Since $\{e_1, \dots, e_n\}$ is a $\mathcal{o}$-basis for $\mathcal{O}$, we have an $\mathcal{o}$-module isomorphism $\mathcal{o}^n \to \mathcal{O}$ given by $(a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i e_i$. Since $\mathcal{O}/\mathfrak{a}\mathcal{O} \cong \mathcal{O} \otimes_\mathcal{o} \mathcal{o}/\mathfrak{a} \cong \mathcal{o}^n \otimes_\mathcal{o} \mathcal{o}/\mathfrak{a} \cong (\mathcal{o}/\mathfrak{a})^n$, we have another isomorphism $(\mathcal{o}/\mathfrak{a})^n \to \mathcal{O}/\mathfrak{a}\mathcal{O}$ given by $(a_1 + \mathfrak{a}, \dots, a_n + \mathfrak{a}) \mapsto \sum_{i=1}^n a_i \bar{e}_i$. Thus, $\{\bar{e}_1, \dots, \bar{e}_n\}$ is a basis for $\mathcal{O}/\mathfrak{a}\mathcal{O}$ as an $\mathcal{o}/\mathfrak{a}$-module. For the second part, just use the result on bases and definition of discriminant d. □

Lemma 2.82. Let $A \subseteq B_j$ for $j = 1, \dots, m$ and with B_j an A-module of finite rank. Then $\Delta\big((\prod_{j=1}^m B_j)/A\big) = \prod_{j=1}^m \Delta(B_j/A)$.

Proof. For $j = 1, \dots, m$, choose an A-basis $\epsilon_j = \big\{e_1^{\{j\}}, \dots, e_{n_j}^{\{j\}}\big\}$ for B_j. Then we compute $\Delta\big((\prod_{j=1}^m B_j)/A\big)$ using the basis $\bigcup_{j=1}^m \epsilon_j$. □

Definition 2.83. An *algebra* over a field (often simply called an *algebra*) is a vector space equipped with a bilinear product.

Lemma 2.84. Let $\mathfrak{k}$ be a perfect field and $\mathcal{A}$ a finite $\mathfrak{k}$-algebra. Then $\mathcal{A}$ is reduced (no nilpotent elts) if and only if $\Delta(\mathcal{A}/\mathfrak{k}) \neq \langle 0 \rangle$.

Theorem 2.85. *Let $0 \neq \mathfrak{p} \subseteq \mathcal{o}$ be prime. We have $\mathfrak{p}$ ramifies in $\mathcal{O}$ if and only if $\mathfrak{p} \mid \Delta(\mathcal{O}/\mathcal{o})$.*

Proof. Write $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with distinct prime $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ and $e_1, \dots, e_r \geqslant 1$. CRT gives $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{j=1}^r \mathcal{O}/\mathfrak{P}_j^{e_j}$. Claim. $\mathfrak{p}$ ramifies if and only if $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is not reduced. $\Longleftarrow$ We are done. $\Longrightarrow$ If there exists $e_j > 1$, for example, $e_i = 2$, then there exists $p_i \in \mathfrak{P}_i \smallsetminus \mathfrak{P}_i^2$. So in $\mathcal{O}/\mathfrak{P}_i^2$, $0 \neq p_i + \mathfrak{P}_i^2 \in \mathfrak{P}_i/\mathfrak{P}_i^2 \subseteq \mathcal{O}/\mathfrak{P}_i^2$. Since $p_i^2 \in \mathfrak{P}_i^2$, we have in $\mathcal{O}/\mathfrak{P}_i^2$, $(p_i + \mathfrak{P}_i)^2 = p_i^2 + \mathfrak{P}_i^2 = 0$. So $(0, \dots, p_i + \mathfrak{P}_i, \dots, 0)$ is a nilpotent of $\bigoplus_{j=1}^r \mathcal{O}/\mathfrak{P}_j^{e_j}$ and then $\mathcal{O}/\mathfrak{p}\mathcal{O}$ has a nilpotent element and hence is not reduced. Since $\mathcal{o}/\mathfrak{p}$ is perfect and $[\mathcal{O}/\mathfrak{p}\mathcal{O} : \mathcal{o}/\mathfrak{p}] = [\mathcal{L} : \mathcal{K}]$, we have $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is not reduced if and only if $\Delta\big((\mathcal{O}/\mathfrak{p}\mathcal{O})/(\mathcal{o}/\mathfrak{p})\big) = 0$ if and only if $\Delta(\mathcal{O}/\mathcal{o}) \pmod{\mathfrak{p}} = 0$ if and only if $\mathfrak{p} \mid \Delta(\mathcal{O}/\mathcal{o})$. □

Corollary 2.86. There are finitely many primes of $\mathcal{o}$ that ramify in $\mathcal{O}$.

Proof. Since $\Delta(\mathcal{O}/\mathcal{o})$ is an ideal of $\mathcal{o}$ and $\mathcal{o}$ is a Dedekind domain, $\Delta(\mathcal{O}/\mathcal{o})$ has a unique prime factorization $\Delta(\mathcal{O}/\mathcal{o}) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$. If $\mathfrak{p} \mid \Delta(\mathcal{O}/\mathcal{o})$, then $\mathfrak{p} = \mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_r^{f_r}$ with $0 \leqslant f_i \leqslant e_i$ for $i = 1, \ldots, r$. So there are just finitely many primes of $\mathcal{o}$ that ramify in $\mathcal{O}$. □

Corollary 2.87. A prime $0 \neq p \in \mathbb{Z}$ ramifies in $\mathcal{K}$ if and only if $p \mid \Delta_{\mathcal{K}}$.

Example 2.88. In $\mathbb{Z}[i]$, the only prime which ramifies is 2 and $\langle 2\rangle = \langle 1+i\rangle^2$.

Example 2.89. In $\mathbb{Z}[\sqrt{19}]$, the only primes which ramify are 2 and 19, and $\langle 2\rangle = \langle 2, \sqrt{19}-19\rangle^2$ and $\langle 19\rangle = \langle\sqrt{19}\rangle^2$.

Remark. We saw in quadratic fields p ramifies in $\mathbb{Q}(\sqrt{d}) = \mathcal{K}$ if and only if $\left(\frac{\Delta_{\mathcal{K}}}{p}\right) = 0$.

Lemma 2.90. If $\mathcal{O} = \mathcal{o}[\alpha]$ and f is the minimal polynomial of α over $\mathcal{K}$. Then $\mathcal{o}[x]/\langle f\rangle \cong \mathcal{O}$.

Proof. Since $\alpha \in \mathcal{O}$, $f \in \mathcal{o}[x]$. We have a $\mathcal{o}$-linear ring homomorphism $\varphi : \mathcal{o}[x] \to \mathcal{o}[\alpha] = \mathcal{O}$ given by $x \mapsto \alpha$. Then $\mathrm{Ker}(\varphi) \supseteq \langle f\rangle$. Let $g \in \mathrm{Ker}(\varphi)$ and write $g = qf + r$ with $q, r \in \mathcal{o}[x]$ and $\deg(r) < \deg(f)$. Then $0 = \varphi(g) = \varphi(q)\varphi(f) + \varphi(r)$. Since $\varphi(f) = 0$, $\varphi(r) = 0$. Let $r = a_0 + a_1x + \cdots + a_nx^n$ with $n < \deg(f)$, $a_1, \ldots, a_n \in \mathcal{o}$ and $a_n \neq 0$. Since $0 = \varphi(r) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$, we have $\alpha^n + \cdots + \frac{a_1}{a_n}\alpha + \frac{a_0}{a_n} = 0$. Since f is the minimal polynomial of α, $a_n = 0$, we have $r = 0$. So $g = qf \in \langle f\rangle$ and then $\mathrm{Ker}(\varphi) \subseteq \langle f\rangle$. Thus, $\mathrm{Ker}(\varphi) = \langle f\rangle$ and so $\mathcal{o}[x]/\langle f\rangle \cong \mathcal{o}[\alpha] = \mathcal{O}$. □

Theorem 2.91 (Dedekind factorization criterion)**.** *Suppose $\mathcal{O} = \mathcal{o}[\alpha]$ and let f be the minimal polynomial of α over $\mathcal{K}$. Let $\mathfrak{p} \subseteq \mathcal{o}$ be prime. Write $f \equiv \prod_j g_j^{e_j} \pmod{\mathfrak{p}}$. Then the prime factorization is $\mathfrak{p}\mathcal{O} = \prod_j \langle \mathfrak{p}, g_j(\alpha)\rangle^{e_j}$. Moreover, for any j, the residue field $\mathcal{O}/\langle \mathfrak{p}, g_j(\alpha)\rangle \cong (\mathcal{o}/\mathfrak{p})[x]/\langle \bar{g}_j\rangle$ and so the residue class degree f_j is equal to the degree of $\bar{g}_j$.*

Proof. Since $\mathcal{o}[x]/\langle f\rangle \cong \mathcal{o}[\alpha] = \mathcal{O}$, we have a ring homomorphism

$$\mathcal{O}/\langle\mathfrak{p}\rangle = \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}\otimes_{\mathcal{o}}\mathcal{o}/\mathfrak{p} = \mathcal{o}[\alpha]\otimes_{\mathcal{o}}\mathcal{o}/\mathfrak{p} \cong \mathcal{o}[x]/\langle f\rangle \otimes_{\mathcal{o}}\mathcal{o}/\mathfrak{p} \cong \frac{\mathcal{o}[x]/\langle f\rangle}{\mathfrak{p}\mathcal{o}[x]/\langle f\rangle} = \frac{\mathcal{o}[x]/\langle f\rangle}{\langle\mathfrak{p}\rangle} \cong \mathfrak{k}[x]/\langle\overline{f}\rangle.$$

Or $\mathcal{O}/\langle\mathfrak{p}\rangle \cong \frac{\mathcal{o}[x]/\langle f\rangle}{\langle\mathfrak{p}\rangle} \cong \frac{\mathcal{o}[x]}{\langle\mathfrak{p}, f\rangle} \cong \mathfrak{k}[x]/\langle\overline{f}\rangle$.

Our goal is to find all prime ideals (maximal ideals) in $\mathcal{O}$ containing $\mathfrak{p}\mathcal{O}$, which corresponding to the maximal ideal of $\mathcal{O}/\langle\mathfrak{p}\rangle$ or $\mathfrak{k}[x]/\langle\overline{f}\rangle$. The ideal of $\mathfrak{k}[x]/\langle\overline{f}\rangle$ corresponds the ideal of $\mathfrak{k}[x]$ containing $\overline{f}$, since $\mathfrak{k}[x]$ is a PID, these ideals are actually the ideals $\langle\bar{g}_j\rangle$, where $\bar{g}_j \mid \overline{f}$. Note $\prod_j \bar{g}_j^{e_j} = 0$ in $\mathfrak{k}[x]/\langle\overline{f}\rangle$, but no product with smaller exponents is zero and note

$$\langle\bar{g}_j\rangle + \langle\overline{f}\rangle \longleftrightarrow \langle\bar{g}_j(\alpha)\rangle + \mathfrak{p}\mathcal{O} \text{ in } \mathcal{O}/\mathfrak{p}\mathcal{O},$$

$$\langle\bar{g}_j\rangle \longleftrightarrow \langle\mathfrak{p}, g_j(\alpha)\rangle =: \mathfrak{P}_j \text{ in } \mathcal{O}.$$

So $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ is the complete set of prime ideals containing $\mathfrak{p}\mathcal{O}$ and hence is the complete set of prime divisors of $\mathfrak{p}$. This corresponds to e_j being the power of $\mathfrak{P}_j = \langle\mathfrak{p}, g_j(\alpha)\rangle$, and e_j is characterized by the fact that $\mathfrak{p}\mathcal{O}$ contains $\prod\mathfrak{P}_j^{e_j}$, but it does not contain the product when any e_j is replaced with a smaller value. Thus, e_j is the exponent of $\bar{g}_j$ occuring in the factorization of $\overline{f}$. Since

$$\frac{\mathcal{O}}{\langle\mathfrak{p}, g_j(\alpha)\rangle} = \frac{\mathcal{o}[\alpha]}{\langle\mathfrak{p}, g_j(\alpha)\rangle} = \frac{\mathcal{o}[\alpha]/\mathfrak{p}[\alpha]}{\mathfrak{p}\mathcal{o}[\alpha]/\mathfrak{p}[\alpha] + g_j(\alpha)\mathcal{o}[\alpha]/\mathfrak{p}[\alpha]} \cong \frac{\mathfrak{k}[\alpha]}{\bar{g}_j\mathfrak{k}[\alpha]} = \mathfrak{k}[\alpha]/\langle\bar{g}_j\rangle,$$

we have $f_j = f(\mathfrak{P}_j/\mathfrak{p}) = [\mathcal{O}/\mathfrak{P}_j : \mathcal{o}/\mathfrak{p}] = [\mathcal{o}[\alpha]/\langle\mathfrak{p}, g_j(\alpha)\rangle : \mathcal{o}/\mathfrak{p}] = [\mathfrak{k}[\alpha]/\langle\bar{g}_j\rangle : \mathfrak{k}] = \deg(\bar{g}_j)$. □

Remark. The idea behind Dedekind's criterion is to relate the monic irreducible factorization of $\overline{f}$ in $(\mathcal{o}/\mathfrak{p})[x]$ to the prime ideal factorization of $\mathfrak{p}\mathcal{O}$.

Example 2.92. Let $f = x^3+10x+1 \in \mathbb{Z}[x]$ and α be a root of f and $\mathcal{K} = \mathbb{Q}(\alpha)$. Note $\Delta(1, \alpha, \alpha^2) = -4027$, and since 4027 is prime, the discriminant is square-free. Also, since $\Delta(1, \alpha, \alpha^2) = \Delta(\mathbb{Z}[\alpha]) = [\mathcal{o}_\mathcal{K} : \mathbb{Z}[\alpha]]^2\Delta(\mathcal{o}_\mathcal{K})$, we have $\mathcal{o}_\mathcal{K} = \mathbb{Z}[\alpha]$. A couple of prime factorization is $x^3 + 10x + 1 = (x + 1)(x^2 + x + 1) \pmod 2$. Then $2\mathcal{o}_\mathcal{K} = \langle 2, \alpha + 1\rangle\langle 2, \alpha^2 + \alpha + 1\rangle = \mathfrak{p}_1\mathfrak{p}_2$. So $r = 2$, $e(\mathfrak{p}_1/2) = 1 = e(\mathfrak{p}_2/2)$ and $f(\mathfrak{p}_1/2) = 1,\ f(\mathfrak{p}_2/2) = 2$. Since $3 = 1 \cdot 1 + 1 \cdot 2$, we verified $[\mathcal{K} : \mathbb{Q}] = \sum_{j=1}^r e_j f_j$. Another couple of prime factorization is $x^3 + 10x + 1 = (x + 2215)^2(x + 3624) \pmod{4027}$. Then $4027\mathcal{o}_\mathcal{K} = \langle 4027, \alpha + 2215\rangle^2\langle 4027, \alpha + 3624\rangle = \mathfrak{p}_1^2\mathfrak{p}_2$. So $r = 2$, $e(\mathfrak{p}_1/4027) = 2,\ e(\mathfrak{p}_2/4027) = 1$ and $f(\mathfrak{p}_1/4027) = 1 = f(\mathfrak{p}_2/4027)$. Finally, factorization in $\mathcal{o}_\mathcal{K}$ from this relys on writting $\mathcal{o} = \mathbb{Z}[\alpha]$. If not trivial, let $\mathcal{K} = \mathbb{Q}(\alpha)$, then $\mathbb{Z} \subseteq \mathbb{Z}[\alpha] \subseteq \mathcal{o}_\mathcal{K}$. Can we always use the theorem to find factorization in $\mathbb{Z}[\alpha]$?

Theorem 2.93. *Let $\alpha \in \mathcal{o}_\mathcal{K}$ such that $\mathcal{K} = \mathbb{Q}(\alpha)$. Let f be the minimal polynomial of α over $\mathbb{Q}$. For any $p \nmid [\mathcal{o}_\mathcal{K} : \mathbb{Z}[\alpha]]$, write $f \equiv \prod_{j=1}^r g_j^{e_j} \pmod p$. Then the prime factorization is $p\mathcal{o}_\mathcal{K} = \prod_{j=1}^r \langle p, g_j(\alpha)\rangle^{e_1} \cdots \langle p, g_j(\alpha)\rangle^{e_r}$ with $f_j = \deg(g_j)$.*

Proof. Note $\mathcal{o}_\mathcal{K}/p\mathcal{o}_\mathcal{K} \cong \frac{\mathbb{Z}[x]/\langle f\rangle}{\langle p\rangle} \cong \frac{\mathbb{Z}[x]}{\langle p, f\rangle} \cong \mathbb{F}_p[x]/\langle \overline{f}\rangle$. Let $m = [\mathcal{o}_\mathcal{K} : \mathbb{Z}[\alpha]]$ and assume $p \nmid m$. Then the additive group $\mathcal{o}_\mathcal{K}/\mathbb{Z}[\alpha]$ has order m. So for any $x \in \mathcal{o}_\mathcal{K}$, $m(x + \mathbb{Z}[\alpha]) = \mathbb{Z}[\alpha]$, i.e., $mx \in \mathbb{Z}[\alpha]$. Since $x \in \mathcal{o}_\mathcal{K}$ is arbitrary, $m\mathcal{o}_\mathcal{K} \subseteq \mathbb{Z}[\alpha] \subseteq \mathcal{o}_\mathcal{K}$. Given any prime $l \in \mathbb{Z}$, we have a natural ring homomorphism $\mathbb{Z}[\alpha]/l\mathbb{Z}[\alpha] \to \mathcal{o}_\mathcal{K}/p\mathcal{o}_\mathcal{K}$. (conrad) If we take $l = p$, we claim this is a surjective. Since $p \nmid m$, $\gcd(p, m) = 1$. Then there exists $m' \in \mathbb{Z}$ such that $mm' \equiv 1 \pmod p$. Let $x \in \mathcal{o}_\mathcal{K}$, we have $x \equiv m'mx \pmod{p\mathcal{o}_\mathcal{K}}$. Since $mx \in m\mathcal{o}_\mathcal{K} \subseteq \mathbb{Z}[\alpha]$, $m'mx \in \mathbb{Z}[\alpha]$. Hence $m'mx + p\mathbb{Z}[\alpha]$ maps to $m'mx + p\mathcal{o}_\mathcal{K} = x + p\mathcal{o}_\mathcal{K}$ and so $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{o}_\mathcal{K}/p\mathcal{o}_\mathcal{K}$ is surjective. Since $\mathbb{Z}[\alpha]$ and $\mathcal{o}_\mathcal{K}$ are both free $\mathbb{Z}$-module of rank $[\mathcal{K} : \mathbb{Q}]$, $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ and $\mathcal{o}_\mathcal{K}/p\mathcal{o}_\mathcal{K}$ both have $p^{[\mathcal{K}:\mathbb{Q}]}$ elements. Thus, we have the module isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathcal{o}_\mathcal{K}/p\mathcal{o}_\mathcal{K}$. Now apply the previous theorem. □

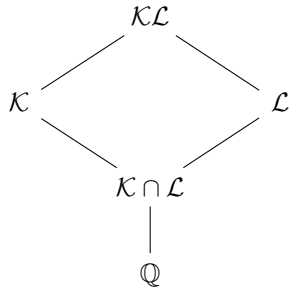
Chapter 3

Ramification Theory

3.1 Galois Theory

Definition 3.1. Let $\mathcal{K}$ and $\mathcal{L}$ be number fields. The *compositive field* of $\mathcal{K}$ and $\mathcal{L}$, denoted $\mathcal{KL}$, is defined to be $\mathcal{KL} = \left\{\sum^{\text{finite}} a_i b_i : a_i \in \mathcal{K}, b_i \in \mathcal{L}\right\}$.

Remark. Note



Remark (Facts)**.** (a) $\deg(\mathcal{KL}/\mathcal{K}) \leqslant \deg(\mathcal{L}/\mathcal{K} \cap \mathcal{L})$ and $\deg(\mathcal{KL}/\mathcal{L}) \leqslant \deg(\mathcal{K}/\mathcal{K} \cap \mathcal{L})$.

(b) $\deg(\mathcal{KL}/\mathbb{Q}) \leqslant \deg(\mathcal{K}/\mathbb{Q}) \deg(\mathcal{L}/\mathbb{Q})$, where the equality is attained when $\mathcal{L}$ and $\mathcal{K}$ are Galois with $\mathcal{L} \cap \mathcal{K} = \mathbb{Q}$.

(c) Since $\mathcal{O}_\mathcal{K} \subseteq \mathcal{O}_{\mathcal{KL}}$ and $\mathcal{O}_\mathcal{L} \subseteq \mathcal{O}_{\mathcal{KL}}$, $\mathcal{O}_\mathcal{K}\mathcal{O}_\mathcal{L} \subseteq \mathcal{O}_{\mathcal{KL}}$.

Theorem 3.2. *Let $\mathcal{K}, \mathcal{L}$ be number fields and $\mathcal{K} \cap \mathcal{L} = \mathbb{Q}$ and $\mathcal{K}/\mathbb{Q}$ and $\mathcal{L}/\mathbb{Q}$ are Galois. Let $d = \gcd(\Delta_\mathcal{K}, \Delta_\mathcal{L})$. Then*

(a) $\mathcal{O}_{\mathcal{KL}} \subseteq \frac{1}{d}\mathcal{O}_\mathcal{K}\mathcal{O}_\mathcal{L}$.

(b) If $d = 1$, then $\mathcal{O}_{\mathcal{KL}} = \mathcal{O}_\mathcal{K}\mathcal{O}_\mathcal{L}$ and $\Delta_{\mathcal{KL}} = \Delta_\mathcal{K}^{\deg(\mathcal{L}/\mathbb{Q})} \cdot \Delta_\mathcal{L}^{\deg(\mathcal{K}/\mathbb{Q})}$.

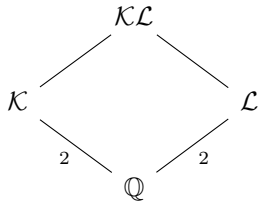
Proof. (a) Let $\{\alpha_1, \ldots, \alpha_m\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_\mathcal{K}$ and $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_\mathcal{L}$. Since $\mathcal{L} \cap \mathcal{K} = \mathbb{Q}$ and $\mathcal{L}/\mathbb{Q}$ and $\mathcal{K}/\mathbb{Q}$ are Galois, $[\mathcal{KL} : \mathbb{Q}] = [\mathcal{K} : \mathbb{Q}][\mathcal{L} : \mathbb{Q}]$. So $\{\alpha_i\beta_j\}$ gives a basis for $\mathcal{KL}/\mathbb{Q}$. Given $\gamma \in \mathcal{O}_{\mathcal{KL}}$, write $\gamma = \sum_{ij} \frac{a_{ij}}{M}\alpha_i\beta_j$ with $a_{ij} \in \mathbb{Z}$ and $M \in \mathbb{Z}$ and $\gcd(a_{11}, \ldots, a_{mn}, M) = 1$. NTS:

$M \mid d = \gcd(\Delta_{\mathcal{K}}, \Delta_{\mathcal{L}})$. Fix $\tau : \mathcal{L} \hookrightarrow \overline{\mathbb{Q}}$, and let $\sigma_1, \ldots, \sigma_m$ be the distinct $\mathbb{Q}$-embeddings $\mathcal{K} \hookrightarrow \overline{\mathbb{Q}}$. Each σ_k extends to an embedding $\tilde{\sigma}_k : \mathcal{KL} \hookrightarrow \overline{\mathbb{Q}}$ such that $\tilde{\sigma}_k|_{\mathcal{L}} = \tau$. Then for $k = 1, \ldots, m$, $\tilde{\sigma}_k(\alpha_i\beta_j) = \tilde{\sigma}_k(\alpha_i)\tilde{\sigma}_k(\beta_j) = \sigma_k(\alpha_i)\tau(\beta_j)$ and then $\tilde{\sigma}_k(\gamma) = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{a_{ij}}{M}\sigma_k(\alpha_i)\tau(\beta_j)$. Set for $i = 1, \ldots, m$, $x_i = \sum_{j=1}^{n} \frac{a_{ij}}{M}\tau(\beta_j) \in \tau(\mathcal{L})$. Then $\tilde{\sigma}_k(\gamma) = \sum_{i=1}^{m} \sigma_k(\alpha_i)x_i$. So $x = (x_1, \ldots, x_m)^t$ is a solution of $(\sigma_k(\alpha_i))x = \begin{pmatrix} \tilde{\sigma}_1(\gamma) \\ \vdots \\ \tilde{\sigma}_m(\gamma) \end{pmatrix}$. Since the $\sigma_k(\alpha_i)$ and $\tilde{\sigma}_k(\gamma)$'s are integral over $\mathbb{Z}$, Cramer's rule gives $\det(\sigma_k(\alpha_i))x_i$ is also integral over $\mathbb{Z}$. Also, since $\det(\sigma_k(\alpha_i))$ is integral over $\mathbb{Z}$, we have $(\det(\sigma_k(\alpha_i)))^2 x_i$ is integral over $\mathbb{Z}$. So $\Delta_{\mathcal{K}} x_i$ is integral over $\mathbb{Z}$. Also, since $\Delta_{\mathcal{K}} x_i \in \tau(\mathcal{L})$, we have $\Delta_{\mathcal{K}} x_i \in \tau(\mathcal{O}_{\mathcal{L}})$ and then $\Delta_{\mathcal{K}} x_i = \sum_{j=1}^{n} \frac{\Delta_{\mathcal{K}} a_{ij}}{M}\tau(\beta_j) \in \tau(\mathcal{O}_{\mathcal{L}})$. Hence $M \mid \Delta_{\mathcal{K}}$ and similarly, $M \mid \Delta_{\mathcal{L}}$. Thus, $M \mid \gcd(\Delta_{\mathcal{K}}, \Delta_{\mathcal{L}})$ and thus $\mathcal{O}_{\mathcal{KL}} \subseteq \frac{1}{d}\mathcal{O}_{\mathcal{K}}\mathcal{O}_{\mathcal{L}}$.

(b) Since $d = 1$, $\mathcal{O}_{\mathcal{K}}\mathcal{O}_{\mathcal{L}} \subseteq \mathcal{O}_{\mathcal{KL}} \subseteq \mathcal{O}_{\mathcal{K}}\mathcal{O}_{\mathcal{L}}$, i.e., $\mathcal{O}_{\mathcal{KL}} = \mathcal{O}_{\mathcal{K}}\mathcal{O}_{\mathcal{L}}$. Since $\{\alpha_i\beta_j\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathcal{KL}}$, by the definition of $\Delta_{\mathcal{KL}}$? $\Delta_{\mathcal{KL}} = \Delta_{\mathcal{K}}^{\deg(\mathcal{L}/\mathbb{Q})} \cdot \Delta_{\mathcal{L}}^{\deg(\mathcal{K}/\mathbb{Q})}$.

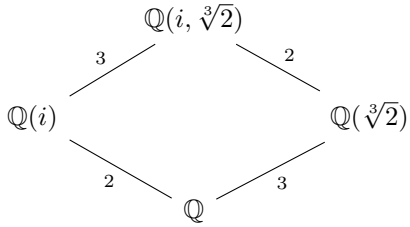
□

Example 3.3. Let $\mathcal{K} = \mathbb{Q}(i)$ and $\mathcal{L} = \mathbb{Q}(\sqrt{-3})$, we have $\mathcal{KL} = \mathbb{Q}(i, \sqrt{-3})$.



Since any degree 2 extension are Galois, $\mathcal{K}/\mathbb{Q}$ and $\mathcal{L}/\mathbb{Q}$ are both Galois. Since $\gcd(\Delta_{\mathcal{K}}, \Delta_{\mathcal{L}}) = \gcd(-4, -3) = 1$, we have $\mathcal{O}_{\mathcal{KL}} = \mathcal{O}_{\mathcal{K}}\mathcal{O}_{\mathcal{L}} = \mathbb{Z}[i]\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}\left[1, i, \frac{1+\sqrt{-3}}{2}, i\frac{1+\sqrt{-3}}{2}\right]$. Also, since $\mathcal{K} \cap \mathcal{L} = \mathbb{Q}$, $\Delta_{\mathcal{KL}} = (-4)^{\deg(\mathcal{L}/\mathbb{Q})}(-3)^{\deg(\mathcal{K}/\mathbb{Q})} = 3^2 \cdot 4^2$. Or use SAGE, we find $\mathcal{KL} \cong \mathbb{Q}[x]/\langle x^4 - 4x^2 + 16\rangle$ and $\Delta_{\mathcal{KL}} = 2^4 \cdot 3^2$.

Example 3.4. Let $\mathcal{K} = \mathbb{Q}(i)$ and $\mathcal{L} = \mathbb{Q}(\sqrt[3]{2})$, we have $\mathcal{L}/\mathbb{Q}$ is not Galois. Note $\mathcal{O}_{\mathcal{L}} = \mathbb{Z}[\sqrt[3]{2}]$. We can factor primes in $\mathcal{L}$, based on how $x^3 - 2$ factors modulo these primes.



It is a degree 6 extension of $\mathbb{Q}$. Only $\mathbb{Q}(i)/\mathbb{Q}$ and $\mathbb{Q}(i, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ are Galois extension.

By SAGE, the minimal polynomial of $\mathcal{KL}/\mathbb{Q}$ is $f = x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$. Then $\mathcal{KL} \cong \mathbb{Q}[x]/\langle f\rangle \equiv \mathbb{Q}(c)$, where c is a root of f. By SAGE,

$$\begin{aligned}\mathcal{O}_{\mathcal{KL}} \cong \mathbb{Z}[&15/22c^5 + 4/11c^4 + 17/22c^3 + 7/22c^2 + 2/11c + 1/22,\\ &1/2c^5 + 1/2c, 1/2c^5 + 1/2c^4 + 1/2c^3 + 1/2c^2, c^3, c^4, c^5].\end{aligned}$$

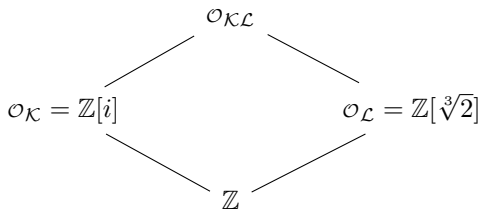
Note $[\mathcal{O}_{\mathcal{KL}} : \mathbb{Z}[c]] = 2^3 \cdot 11$.

(a) Factor in $\mathcal{L}$. Since $\Delta_{\mathcal{L}} = -2^2 \cdot 3^3$, the only primes that ramify are 2 and 3.

- Let $p = 2$. Then $x^3 - 2 \equiv x^3 \pmod 2$ and so $2\mathcal{O}_{\mathcal{L}} = \langle 2, \sqrt[3]{2}\rangle^3 =: \mathfrak{p}^3$. So $r = 1$, $e(\mathfrak{p}/2) = 3$ and $f(\mathfrak{p}/2) = 1$. Since $r = 1$ and $e = [\mathcal{L} : \mathbb{Q}]$, 2 is totally ramified.
- Let $p = 3$. Then $x^3 - 2 \equiv (x + 1)^3 \pmod 3$ and so $3\mathcal{O}_{\mathcal{L}} = \langle 3, \sqrt[3]{2} + 1\rangle =: \mathfrak{p}^3$. So $r = 1$, $e(\mathfrak{p}/3) = 3$ and $f(\mathfrak{p}/3) = 1$. Since $r = 1$ and $e = [\mathcal{L} : \mathbb{Q}]$, 3 is totally ramified.
- Let $p = 5$. Then $x^3 - 2 \equiv (x + 2)(x^2 + 3x + 4) \pmod 5$ and so $5\mathcal{O}_{\mathcal{L}} = \langle 5, \sqrt[3]{2} + 2\rangle\langle 5, \sqrt[3]{2} + 3\sqrt[3]{2} + 4\rangle =: \mathfrak{p}_1\mathfrak{p}_2$. Hence $e(\mathfrak{p}_1/5) = 1 = e(\mathfrak{p}_2/5), f(\mathfrak{p}_1/5) = 1, f(\mathfrak{p}_2/5) = 2$ and $r = 2$. Thus, 5 is not ramified.

(b) Factor in $\mathcal{KL}$. Since $\Delta_{\mathcal{KL}} = -2^8 \cdot 3^6$, the only prime that ramify are 2 and 3.

- Let $p = 2$. Then $f \equiv (x + 1)^6 \pmod 2$ and so $2\mathcal{O}_{\mathcal{KL}} = \langle 2, c + 1\rangle^6 =: \mathfrak{p}^6$. So $r = 1$, $e(\mathfrak{p}/2) = 6$ and $f(\mathfrak{p}/2) = 1$. Since $r = 1$ and $e = [\mathcal{KL} : \mathbb{Q}]$, 2 is totally ramified.
- Let $p = 5$. Then $f \equiv x(x + 4)(x^2 + 2x + 4)(x^2 + 4x + 2) \pmod 5$ and so $5\mathcal{O}_{\mathcal{KL}} = \langle 5, c\rangle\langle 5, c + 4\rangle\langle 5, c^2 + 2c + 4\rangle\langle 5, c^2 + 4c + 2\rangle =: \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. Hence $r = 4, e_1(\mathfrak{p}_1/5) = e_2(\mathfrak{p}_2/5) = e_3(\mathfrak{p}_3/5) = e_4(\mathfrak{p}_4) = 1$ and $f(\mathfrak{p}_1/5) = 1 = f(\mathfrak{p}_2/5), f(\mathfrak{p}_3/5) = 2 = f(\mathfrak{p}_4/5)$. Since $r = 4 > 1$, 5 splits.
- Let $p = 3$. Then $f \equiv (x^2 + 2x + 2)^3 \pmod 3$ and so $3\mathcal{O}_{\mathcal{KL}} = \langle 3, c^2 + 2c + 2\rangle^3 =: \mathfrak{p}^3$. So $r = 1$, $e(\mathfrak{p}/3) = 3$ and $f(\mathfrak{p}/3) = 2$. Since $r = 1$ and $e < [\mathcal{L} : \mathbb{Q}]$, 3 is ramified.



3.2 Ramification Theory

Let $\mathcal{O}$ be dedekind domain and $\mathcal{K}$ be $\mathrm{Frac}(\mathcal{O})$. Let $\mathcal{O}$ be the integral closure of $\mathcal{O}$ in $\mathcal{L}$. $\mathfrak{P} \leqslant \mathcal{O}$ be a prime dividing $\mathfrak{p} \subseteq \mathcal{O}$. Let $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $\mathcal{P}_{\mathfrak{p}} := \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$. Let $\mathcal{L}/\mathcal{K}$ be finite Galois extension with degree n, $G = G_{\mathcal{L}/\mathcal{K}} = \mathrm{Gal}(\mathcal{L}/\mathcal{K})$ and $\sigma \in G$.

Remark. If one takes a prime $\mathfrak{p} \leqslant \mathcal{O}$, what happens when $\mathfrak{p}$ is lifted to $\mathcal{O}$, that is $\mathfrak{p}\mathcal{O}$?

Theorem 3.5. *We have $\sigma|_{\mathcal{O}} : \mathcal{O} \xrightarrow{\cong} \mathcal{O}$ given by $a \mapsto \sigma(a)$.*

Proof. Let $a \in \mathcal{O}$. Then $\sigma(a) \in \mathcal{O}$ and so $\sigma|_{\mathcal{O}}$ is well-defined. Since $\sigma : \mathcal{L} \to \mathcal{L}$ is an isomorphism, $\sigma|_{\mathcal{O}}$ is a homomorphism and 1-1. Let $\alpha \in \mathcal{O}$. Since G is a group, there exists $\sigma^{-1} \in G$ and $\sigma^{-1}(\alpha) \in \mathcal{O}$. By the associativity of group action, $\sigma(\sigma^{-1}(\alpha)) = (\sigma \circ \sigma^{-1})(\alpha) = \alpha$, σ is onto. □

Lemma 3.6. We have $\sigma(\mathfrak{P}) \leqslant \mathcal{O}$ is a prime dividing $\mathfrak{p}$, i.e., $\sigma(\mathfrak{P}) \in \mathcal{P}_\mathfrak{p}$.

Proof. Let $xy \in \sigma(\mathfrak{P})$. Then there exists $z \in \mathfrak{P}$ such that $\sigma(z) = xy$. Then $\mathfrak{P} \ni z = \sigma^{-1}(\sigma(z)) = \sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$. Since $\mathfrak{P} \leqslant \mathcal{O}$ is prime, $\sigma^{-1}(x) \in \mathfrak{P}$ or $\sigma^{-1}(y) \in \mathfrak{P}$. So $x = \sigma(\sigma^{-1}(x)) \in \sigma(\mathfrak{P})$ or $y = \sigma(\sigma^{-1}(y)) \in \sigma(\mathfrak{P})$. Hence $\sigma(\mathfrak{P}) \leqslant \mathcal{O}$ is prime. Since $\mathfrak{p} \leqslant \mathcal{o} \subseteq \mathcal{K}$ and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{o}$, $\mathfrak{p} = \sigma(\mathfrak{p}) = \sigma(\mathfrak{P} \cap \mathcal{o}) \subseteq \sigma(\mathfrak{P})$, i.e., $\sigma(\mathfrak{P}) \mid \mathfrak{p}$. Thus, $\mathfrak{p} = \sigma(\mathfrak{P}) \cap \mathcal{o}$. □

Corollary 3.7. We have a well-defined group action $\varphi : G \times \mathcal{P}_\mathfrak{p} \to \mathcal{P}_\mathfrak{p}$.

Definition 3.8. The prime ideal $\sigma(\mathfrak{P})$ is called the *Galois conjugate* of $\mathfrak{P}$.

Theorem 3.9. *The Galois group G acts transitively on the primes $\mathfrak{P}$ of $\mathcal{O}$ dividing $\mathfrak{p}$, i.e., for any $\mathfrak{P}_i, \mathfrak{P}_j \in \mathcal{P}_\mathfrak{p}$, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, i.e., φ is onto, i.e., there is only one orbit $\mathcal{P}_\mathfrak{p}$.*

Proof. Let $\mathfrak{P}_1, \mathfrak{P}_2 \leqslant \mathcal{O}$ be distinct primes dividing $\mathfrak{p}$. Suppose $\mathfrak{P}_2 \neq \sigma(\mathfrak{P}_1)$, for any $\sigma \in G$. Apply CRT to find $x \in \mathcal{O}$ such that $x \equiv 0 \pmod{\mathfrak{P}_2}$ and $x \equiv 1 \pmod{\sigma(\mathfrak{P}_1)}$ for any $\sigma \in G$. Then $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(x) = \prod_{\sigma\in G} \sigma(x) = x \prod_{\mathrm{id}\neq\sigma\in G} \sigma(x) \in \mathfrak{P}_2 \cap \mathcal{o} = \mathfrak{p}$. Since $x \not\equiv 0 \pmod{\sigma(\mathfrak{P}_1)}$ for any $\sigma \in G$, we have $x \notin \sigma(\mathfrak{P}_1)$ for any $\sigma \in G$. Suppose there exists $\sigma \in \mathfrak{P}_1$ such that $\sigma(x) \in \mathfrak{P}_1$. Then there exists $y \in \mathfrak{P}_1$ such that $\sigma^{-1}(y) = x$ and so $x \in \sigma^{-1}(\mathfrak{P}_1)$, a contrdiction. So $\sigma(x) \notin \mathfrak{P}_1$ for any $\sigma \in G$. Since $\mathfrak{p}$ is a prime ideal, $\mathrm{N}_{\mathcal{L}/\mathcal{K}}(x) = \prod_{\sigma\in G} \sigma(x) \notin \mathfrak{P}_1 \cap \mathcal{o} = \mathfrak{p}$, a contradiction. □

Corollary 3.10. For any $\mathfrak{P}_i, \mathfrak{P}_j \in \mathcal{P}_\mathfrak{p}$, $\mathfrak{P}_i \cong \mathfrak{P}_j$.

Proof. Let $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Then σ is onto. Since $\sigma : \mathcal{L} \to \mathcal{L}$ is an isomorphism, $\sigma|_{\mathfrak{P}_i}$ is a homomorphism and 1-1. □

Definition 3.11. The *decomposition group* of $\mathfrak{P}$ over $\mathcal{K}$ is $G_\mathfrak{P} = D_\mathfrak{P} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \leqslant G$, where $G_\mathfrak{P}$ is the stabilizer of $\mathfrak{P}$ in G. The *decomposition field* $\mathcal{Z}_\mathfrak{P}$ is the fixed field of $G_\mathfrak{P}$, i.e., $\mathcal{Z}_\mathfrak{P} = \mathcal{L}^{G_\mathfrak{P}} = \{x \in \mathcal{L} : \sigma(x) = x, \forall \sigma \in G_\mathfrak{P}\}$.

Remark. $[\mathcal{Z}_\mathfrak{P} : \mathcal{K}] = [G : G_\mathfrak{P}] = r$. $G_\mathfrak{P} = \mathrm{Gal}(\mathcal{L}/\mathcal{Z}_\mathfrak{P})$. If $G_\mathfrak{P} \trianglelefteq G$, then $\mathcal{Z}_\mathfrak{P}/\mathcal{K}$ is also Galois.

Remark. The decomposition group encodes in group-theoretic language the number of different prime ideals into which a prime ideal $\mathfrak{p}$ of $\mathcal{o}$ decomposes in $\mathcal{O}$. By orbit-stabilizer theorem, $\frac{|G|}{|G_\mathfrak{P}|} = [G : G_\mathfrak{P}] = \#\mathcal{P}_\mathfrak{p} = r$. In particular,

$$G_\mathfrak{P} = \{\mathrm{id}\}(\Longleftrightarrow \mathcal{Z}_\mathfrak{P} = \mathcal{L}) \Longleftrightarrow n = r \Longleftrightarrow \mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdots \mathfrak{P}_n \Longleftrightarrow \mathfrak{p} \text{ is totally split,}$$

$$G_\mathfrak{P} = G(\Longleftrightarrow \mathcal{Z}_\mathfrak{P} = \mathcal{K}) \Longleftrightarrow r = 1 \Longleftrightarrow \mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \Longleftrightarrow \mathfrak{p} \text{ ramifies.}$$

Proposition 3.12. The decomposition groups are conjugates of each other. If $\mathcal{L}/\mathcal{K}$ is an abelian extension, then $G_{\sigma(\mathfrak{P})} = G_\mathfrak{P}$, and often this will make people write $G_\mathfrak{p}$ for $G_\mathfrak{P}$.

Proof. By the associativity of group action, we have $\tau \in G_{\sigma(\mathfrak{P})}$ if and only if $\tau(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P})$ if and only if $\sigma^{-1}\tau\sigma(\mathfrak{P}) = \mathfrak{P}$ if and only if $\sigma^{-1}\tau\sigma \in G_\mathfrak{P}$ if and only if $\tau \in \sigma G_\mathfrak{P}\sigma^{-1}$. So $G_{\sigma(\mathfrak{P})} = \sigma G_\mathfrak{P}\sigma^{-1}$. Moreover, If $\mathcal{L}/\mathcal{K}$ is an abelian extension, G and $G_\mathfrak{P}$ are abelian and then $G_{\sigma(\mathfrak{P})} = G_\mathfrak{P}$. □

Corollary 3.13. Let $\mathcal{L}/\mathcal{K}$ be an abelian extension and $\mathfrak{p} \leqslant \mathcal{o}$ be prime. Then $\sigma(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$ for any $\sigma \in G_\mathfrak{p}$.

Proof. Since $\mathfrak{p}\mathcal{O}$ admits a unique prime factorization $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $\sigma(\mathfrak{P}_i) = \mathfrak{P}_i$ for $i = 1, \ldots, r$, $\sigma(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$. □

Remark. The decomposition group regulates the prime decomposition also in the case of a non-Galois extension. For subgroups U and V of a group G, consider the equivalence relation in G defined by $\sigma \sim \sigma' \iff \sigma' = u\sigma v$ for $u \in U, v \in V$.

The correspoding equivalence classes $U\sigma V = \{u\sigma v : u \in U, v \in V\}$ are called the double cosets of G modulo U, V. The set of these double cosets, which form a partition of G, is denoted $U\backslash G/V$.

Definition 3.14. Let $\mathcal{L}^{\text{gal}}$ be the *Galois closure* of $\mathcal{L}$ in some fixed $\overline{K}$. ($\mathcal{L}^{\text{gal}}$ is the smallest Galois extension of $\mathcal{K}$ that contains $\mathcal{L}$.)

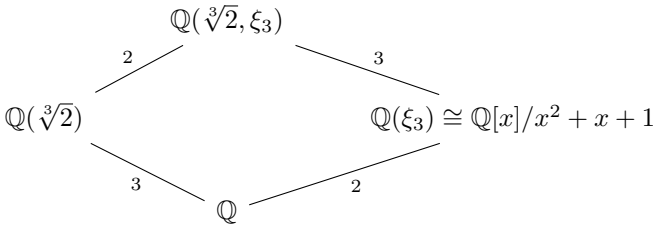
Remark. Since $\text{char}(\mathcal{L}) = \infty$, Galois closure of $\mathcal{L}$ exsits.

Theorem 3.15. *Let $\mathcal{H} = \text{Gal}(\mathcal{L}^{\text{gal}}/\mathcal{L})$. If $\mathfrak{P}$ is a prime ideal of $\mathcal{L}^{\text{gal}}$ over $\mathfrak{p}$, then the rule*

$$\begin{aligned} \mathcal{H}\backslash G/G_{\mathfrak{P}} &\to G_{\mathfrak{P}} \\ \mathcal{H}\sigma G_{\mathfrak{P}} &\mapsto \sigma(\mathfrak{P}) \cap L \end{aligned}$$

gives a well-defined bijection.

Example 3.16. Let ξ_3 be the 3^{rd} root of unity, then $\xi_3^3 = 1$. In $\mathbb{Q}(\sqrt[3]{2})$, we have $x^3 - 2 = (x - \sqrt[3]{2})(x - \xi_3\sqrt[3]{2})(x - \xi_3^2\sqrt[3]{2})$.



Remark. In the Galois case, set $\mathfrak{P} = \mathfrak{P}_1$. Then by previous theorem, for any $\mathfrak{P}_j \in \mathcal{P}_{\mathfrak{p}}$, there exists $\sigma_j \in \text{G}_{\mathcal{L}/\mathcal{K}}$ such that $\mathfrak{P}_j = \sigma_j(\mathfrak{P})$. Then the isomorphism $\sigma_j : \mathcal{O} \to \mathcal{O}$ induces a field homomorphism $\varphi : \mathcal{O}/\mathfrak{P} \to \mathcal{O}/\sigma_j(\mathfrak{P})$ given by $a \pmod{\mathfrak{P}} \mapsto \sigma_j(a) \pmod{\sigma_j(\mathfrak{P})}$. Since $\sigma_j : \mathcal{O} \to \mathcal{O}$ is onto, φ is onto. Since $|\mathcal{O}_{\mathfrak{P}}| = |\mathcal{o}/\mathfrak{p}|^f = |\mathfrak{N}(\mathfrak{p})|^f < \infty$, φ is 1-1. So for $j = 1, \ldots, r$, $f_j = f(\mathfrak{P}_j/\mathfrak{p}) = [\mathcal{O}/\mathfrak{P}_j : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}]$. Then $f_1 = \cdots = f_r =: f$. Furthermore, since $\sigma_j : \mathcal{L} \to \mathcal{L}$ is an isomorphism and $\sigma_j(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$ for $j = 1, \ldots, r$, $\mathfrak{P}^m \mid \mathfrak{p}\mathcal{O} \iff \sigma_j(\mathfrak{P}^m) \mid \sigma_j(\mathfrak{p}\mathcal{O}) \iff (\sigma_j(\mathfrak{P}))^m \mid \mathfrak{p}\mathcal{O}$, i.e., for $j = 1, \ldots, r$, $\mathfrak{P}^m \mid \mathfrak{p}\mathcal{O} \iff (\sigma_j(\mathfrak{P}))^m \mid \mathfrak{p}\mathcal{O}$. So $e_1 = \cdots = e_r =: e$. Thus, $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \left(\prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma(\mathfrak{P})\right)^e$. Also, we have $efr = n$, where $r = [G : G_{\mathfrak{P}}]$ and $n = |G|$.

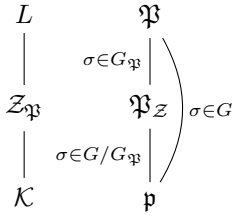
Theorem 3.17. *Let $\mathfrak{P}_{\mathcal{Z}} = \mathfrak{P} \cap \mathcal{Z}_{\mathfrak{P}}$ be the prime ideal of $\mathcal{Z}_{\mathfrak{P}}$ below $\mathfrak{P}$. Then $\mathfrak{P}_{\mathbb{Z}} \mid \mathfrak{p}$ and*

(a) $\mathfrak{P}_{\mathcal{Z}}$ is non-split in $\mathcal{L}$, i.e., $\mathfrak{P}$ is the only prime over $\mathfrak{P}_{\mathcal{Z}}$.

(b) $e(\mathfrak{P}/\mathfrak{P}_{\mathcal{Z}}) = e := e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{P}_{\mathcal{Z}}) = f := f(\mathfrak{P}/\mathfrak{p})$.

(c) $e(\mathfrak{P}_{\mathcal{Z}}/\mathfrak{p}) = 1 = f(\mathfrak{P}_{\mathcal{Z}}/\mathfrak{p})$.

Proof. (a) The prime ideals above $\mathfrak{P}_\mathcal{Z}$ are of the form $\sigma(\mathfrak{P})$ for $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{Z}_\mathfrak{P}) = G_\mathfrak{P}$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$ for any $\sigma \in G$, $\mathfrak{P}$ is the only prime over $\mathfrak{P}_\mathcal{Z}$.



(b) Since $n = efr = ef\frac{|G|}{|G_\mathfrak{P}|} = ef\frac{[\mathcal{L}:\mathcal{K}]}{|G_\mathfrak{P}|} = ef\frac{n}{|G_\mathfrak{P}|}$, we have $|G_\mathfrak{P}| = ef$. Let $e' = e(\mathfrak{P}/\mathfrak{P}_\mathcal{Z})$, $e'' = e(\mathfrak{P}_\mathcal{Z}/\mathfrak{p})$, $f' = f(\mathfrak{P}/\mathfrak{P}_\mathcal{Z})$ and $f'' = e(\mathfrak{P}_\mathcal{Z}/\mathfrak{p})$. Then $\mathfrak{p}\mathcal{O}_{\mathcal{Z}_\mathfrak{P}} = \mathfrak{P}_\mathcal{Z}^{e''}\cdots$ and by (1) we have $\mathfrak{P}_\mathcal{Z}\mathcal{O} = \mathfrak{P}^{e'}$. So $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e'e''}\cdots$. Also, since $\mathfrak{p}\mathcal{O} = \mathfrak{P}^e\cdots$, we have $e = e'e''$. Note $f = [\mathcal{O}/\mathfrak{P} : \mathcal{o}/\mathfrak{p}] = [\mathcal{O}/\mathfrak{P} : \mathcal{o}_{\mathcal{Z}_\mathfrak{P}}/\mathfrak{P}_\mathcal{Z}][\mathcal{o}_{\mathcal{Z}_\mathfrak{P}}/\mathfrak{P}_\mathcal{Z} : \mathcal{o}/\mathfrak{p}] = f'f''$. Since $\mathfrak{P}$ is the only prime over $\mathfrak{P}_\mathcal{Z}$, the fundamental identity for the decomposition of $\mathfrak{P}_\mathcal{Z} \leqslant \mathcal{o}_{\mathcal{Z}_\mathfrak{P}}$ prime in $\mathcal{L}$ then reads $[\mathcal{L} : \mathcal{Z}_\mathfrak{P}] = e(\mathfrak{P}/\mathfrak{P}_\mathcal{Z})f(\mathfrak{P}/\mathfrak{P}_\mathcal{Z})r(\mathfrak{P}/\mathfrak{P}_\mathcal{Z}) = e(\mathfrak{P}/\mathfrak{P}_\mathcal{Z})f(\mathfrak{P}/\mathfrak{P}_\mathcal{Z}) = e'f'$. Also, since $[\mathcal{L} : \mathcal{Z}_\mathfrak{P}] = |G_\mathfrak{P}| = ef$, we have $ef = e'f'$, i.e., $(e'e'')(f'f'') = e'f'$, i.e., $e''f'' = 1$, i.e., $e'' = 1 = f''$. Thus, $e = e',\ f = f'$. □

Corollary 3.18. Let $\mathcal{M}/\mathcal{L}/\mathcal{K}$ be a tower of finite extension, and let $\mathcal{P}, \mathfrak{P}, \mathfrak{p}$ be prime ideals of $\mathcal{M}, \mathcal{L}$ and $\mathcal{K}$, respectively. Then $e(\mathcal{P}/\mathfrak{p}) = e(\mathcal{P}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathcal{P}/\mathfrak{p}) = f(\mathcal{P}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$.

Remark. Let $\sigma \in G_\mathfrak{P}$. Similarly, since $\sigma(\mathfrak{P}) = \mathfrak{P}$, $\sigma : \mathcal{O} \xrightarrow{\cong} \mathcal{O}$ induces an automorphism $\overline{\sigma} : \mathcal{O}/\mathfrak{P} \to \mathcal{O}/\mathfrak{P}$ given by $a \pmod{\mathfrak{P}} \mapsto \sigma(a) \pmod{\mathfrak{P}}$ of the residue class field $\mathcal{O}/\mathfrak{P}$.

Remark (Notation)**.** $\mathfrak{k}(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$ and $\mathfrak{k}(\mathfrak{p}) = \mathcal{o}/\mathfrak{p}$.

Theorem 3.19. *The extension $\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})$ is normal and the map $\pi_\mathfrak{P} : G_\mathfrak{P} \to \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$ with $\pi_\mathfrak{P}(\sigma)(b + \mathfrak{P}) = \sigma(b) + \mathfrak{P}$ is a welll-defined surjective homomorphism.*

Proof. Since $f(\mathfrak{P}_\mathcal{Z}/\mathfrak{p}) = [O_{\mathcal{Z}_\mathfrak{P}}/\mathfrak{P}_\mathcal{Z} : \mathcal{o}/\mathfrak{p}] = 1$, $\mathcal{Z}_\mathfrak{P}$ has the same residue class field $\mathfrak{k}(\mathfrak{p})$ as $\mathcal{K}$ with respect to $\mathfrak{p}$. So assume $K = \mathcal{Z}_\mathfrak{P}$. Then $G_\mathfrak{P} = G$. Let $\overline{\alpha} = \alpha + \mathfrak{P} \in \mathfrak{k}(\mathfrak{P})$, where $\alpha \in \mathcal{O}$ is a representative of $\overline{\alpha}$. Let $f \in \mathcal{o}[x]$ be the minimal polynomial of α over $\mathcal{K}$ and $\overline{f}$ be its image in $(\mathcal{o}/\mathfrak{p})[x]$. Assume $f = \sum_{i=0}^n a_i x^i$, where $a_1, \ldots, a_n \in \mathcal{o}$. Then $f(\alpha) = \sum_{i=0}^n a_i\alpha^i = 0$ and modulo $\mathfrak{P}$, we have $\sum_{i=0}^n (a_i+\mathfrak{p})(\alpha+\mathfrak{P})^i = 0 \pmod{\mathfrak{P}}$. So $\overline{\alpha} = \alpha+\mathfrak{P}$ is a root of $\overline{f}$ and then $m_{\overline{\alpha},\mathfrak{k}(\mathfrak{p})} \mid \overline{f}$. Since $\mathcal{L}/\mathcal{K}$ is Galois and f is irreducible, f splits over $\mathcal{O}$ and then $\overline{f}$ splits over $\mathcal{O}/\mathfrak{P} = \mathfrak{k}(\mathfrak{P})$. So $m_{\overline{\alpha},\mathfrak{k}(\mathfrak{p})}$ splits over $\mathfrak{k}(\mathfrak{P})$ and thus $\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})$ is normal. Let $\sigma \in G_\mathfrak{P}$ and $b, c \in \mathcal{O}$ with $b + \mathfrak{P} = c + \mathfrak{P}$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$, we have $\sigma(b - c) \in \mathfrak{P}$ and then $\sigma(b) + \mathfrak{P} = \sigma(c) + \mathfrak{P}$. So $\pi_\mathfrak{P}(\sigma)(b + \mathfrak{P}) = \pi_\mathfrak{P}(\sigma)(c + \mathfrak{P})$. We have $\pi_\mathfrak{P}(\sigma) \in \mathrm{Aut}(\mathfrak{k}(\mathfrak{P}))$ by such computations as

$$\begin{aligned}\pi_\mathfrak{P}(\sigma)((b + \mathfrak{P})(c + \mathfrak{P})) &= \pi_\mathfrak{P}(\sigma)(bc + \mathfrak{P}) = \sigma(bc) + \mathfrak{P} = \sigma(bc + \mathfrak{P}) = \sigma((b + \mathfrak{P})(c + \mathfrak{P}))\\ &= (\sigma(b) + \mathfrak{P})(\sigma(c) + \mathfrak{P}) = \pi_\mathfrak{P}(\sigma)(b + \mathfrak{P})\pi_\mathfrak{P}(\sigma)(c + \mathfrak{P}).\end{aligned}$$

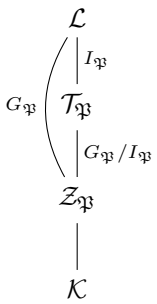
Also, since $\sigma \in G$, σ fixes $\mathcal{o}$ and then σ fixes $\mathfrak{k}(\mathfrak{p})$. So $\pi_\mathfrak{P}(\sigma) \in \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$. Hence $\pi_\mathfrak{P}$ is well-defined. That $\pi_\mathfrak{P}$ is a homomorphism is similarly easily checked. Let $\overline{\theta} = \theta + \mathfrak{P} \in \mathcal{O}/\mathfrak{P}$ be the primitive element for the maximal separable subextension of $\mathcal{O}/\mathfrak{P}$ with θ a representative of $\overline{\theta}$. Let $\overline{\sigma} \in \mathrm{Aut}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$. Let $g \in \mathcal{o}[x]$ be the minimal polynomial of θ and $\overline{g}$ be its image in $(\mathcal{o}/\mathfrak{p})[x]$.

Similarly, $\bar{g}(\bar{\theta}) = 0$ and so $m_{\bar{\theta},\mathfrak{k}(\mathfrak{p})} \mid \bar{g}$. Since $\overline{\sigma}(\bar{\theta})$ is also a root of $m_{\bar{\theta},\mathfrak{k}(\mathfrak{p})}$, $\bar{g}(\sigma(\bar{\theta})) = 0$. So there is an element θ' that is a root of g such that $\theta' + \mathfrak{P} = \overline{\sigma}(\bar{\theta})$. Since both θ and θ' are roots of f, there exists $\sigma \in G = G_{\mathfrak{P}}$ such that $\theta' = \sigma(\theta)$. So $\pi_{\mathfrak{P}}(\sigma)(\bar{\theta}) = \sigma(\theta) + \mathfrak{P} = \theta' + \mathfrak{P} = \overline{\sigma}(\bar{\theta})$ and then $\pi_{\mathfrak{P}}(\sigma) = \bar{\sigma}$ by choice of θ. Thus we have a surjective map $G_{\mathfrak{P}} \to \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$. □

Definition 3.20. The kernel $I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ of the surjective homomorphism $G_{\mathfrak{P}} \to \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$ is called the *inertia group* of $\mathfrak{P}$ over $\mathcal{K}$. Then $I_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}, \forall \alpha \in \mathcal{O}\}$. The fixed field of $I_{\mathfrak{P}}$, denoted $\mathcal{T}_{\mathfrak{P}}$, is called the *inertia field* of $\mathfrak{P}$ over $\mathcal{K}$.

Remark. For any $\sigma \in G$, $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$. The inertia groups are conjugates of each other. Often this will make people write $I_{\mathfrak{p}}$ for $I_{\mathfrak{P}}$.

Remark. The inertia field is the "largest field where $\mathfrak{P}$ is unramified".



Remark. We have the exact sequence

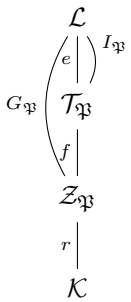
$$1 \to I_{\mathfrak{P}} \xrightarrow{\subseteq} G_{\mathfrak{P}} \xrightarrow{\mathrm{id}} \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})) \to 1.$$

Theorem 3.21. *The extension $\mathcal{T}_{\mathfrak{P}}/\mathcal{Z}_{\mathfrak{P}}$ is normal (Galois), and one has $\mathrm{Gal}(\mathcal{L}/\mathcal{T}_{\mathfrak{P}}) \cong I_{\mathfrak{P}}$ and $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathcal{T}_{\mathfrak{P}}/\mathcal{Z}_{\mathfrak{P}}) \cong \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$. If the residue field extension $\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})$ is separable? then one has $|I_{\mathfrak{P}}| = [\mathcal{L} : \mathcal{T}_{\mathfrak{P}}] = e$ and $[G_{\mathfrak{P}} : I_{\mathfrak{P}}] = [\mathcal{T}_{\mathfrak{P}} : \mathcal{Z}_{\mathfrak{P}}] = f$. In this case, letting $\mathfrak{P}_{\mathcal{T}} := \mathfrak{P} \cap \mathcal{T}_{\mathfrak{P}}$, we have*

(a) $e(\mathfrak{P}/\mathfrak{P}_{\mathcal{T}}) = e$ and $f(\mathfrak{P}/\mathfrak{P}_{\mathcal{T}}) = 1$.

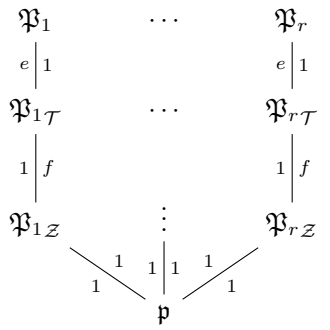
(b) $e(\mathfrak{P}_{\mathcal{T}}/\mathfrak{P}_{\mathcal{Z}}) = 1$ and $f(\mathfrak{P}_{\mathcal{T}}/\mathfrak{P}_{\mathcal{Z}}) = f$.

Proof. The first two statements follow from the identity $|G_{\mathfrak{P}}| = ef$ and the latter statements. Since $\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})$ is separable and normal, $|\mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))| = [\mathfrak{k}(\mathfrak{P}) : \mathfrak{k}(\mathfrak{p})] = [\mathcal{O}/\mathfrak{P} : \mathcal{O}/\mathfrak{p}] = f(\mathfrak{P}/\mathfrak{p}) = f$. Since $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))$, $|I_{\mathfrak{P}}| = \frac{|G_{\mathfrak{P}}|}{|\mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p}))|} = \frac{ef}{f} = e$. Then



Since both $\mathcal{Z}_\mathfrak{P}$ and $\mathcal{T}_\mathfrak{P}$ are fixed field of some subgroup of the Galois group (Or since $I_\mathfrak{P} \subseteq G_\mathfrak{P}$), similarly, $\mathfrak{p} = \mathfrak{P}_\mathcal{Z} \cdots = \mathfrak{P}_\mathcal{T} \cdots = \mathfrak{P}^e \cdots$. So $e(\mathfrak{P}/\mathfrak{P}_\mathcal{T}) = e(\mathfrak{P}/\mathfrak{p}) = e$.

As the inertia group $I_\mathfrak{P}$ of $\mathfrak{P}$ over $\mathcal{K}$ is also the inertia group of $\mathfrak{P}$ over $\mathcal{T}_\mathfrak{P}$, it follows from an application of theorem 3.19 to the extension $\mathcal{L}/\mathcal{T}_\mathfrak{P}$ that $\mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{P}_\mathcal{T})) = 1$. So $\mathfrak{k}(\mathfrak{P}) = \mathfrak{k}(\mathfrak{P}_\mathcal{T})$ and thus $f(\mathfrak{P}|\mathfrak{P}_\mathcal{T}) = 1$ and $f(\mathfrak{P}_\mathcal{T}|\mathfrak{P}_\mathcal{Z}) = f$.



□

Remark. $I_\mathfrak{P} = \{1\} \iff \mathcal{T}_\mathfrak{P} = L \iff e = 1 \iff \mathfrak{p}$ is unramified in $\mathcal{L}$.

Example 3.22. Let $\mathcal{K} = \mathbb{Q}(i)$. Then $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}) = \{1, \tau\} = \langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

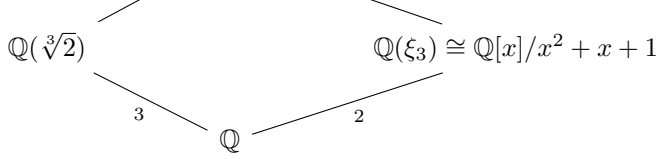
(a) Since $1 + i \mid 2$, $2\mathcal{O}_\mathcal{K} = \langle 1 + i\rangle^2 = \mathfrak{P}^2$. Since $\tau(\mathfrak{P}) = \tau(\langle 1 + i\rangle) = \langle 1 - i\rangle = \langle 1 + i\rangle = \mathfrak{P}$, we have $\tau \in G_\mathfrak{P}$ and so $G_\mathfrak{P} = \{1, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$. Since $|I_\mathfrak{P}| = e = 2$ and $I_\mathfrak{P} \subseteq G_\mathfrak{P}$, we have $I_\mathfrak{P} = G_\mathfrak{P}$.

Alternatively, since $\mathfrak{k}(\langle 1 + i\rangle) = \mathbb{Z}[i]/\langle 1 + i\rangle \cong \mathbb{F}_2$ and $\mathfrak{k}(2) = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$, we have $\mathrm{Gal}(\mathfrak{k}(\langle 1 + i\rangle)/\mathfrak{k}(2)) \cong 1$ and so $I_\mathfrak{P} = \mathrm{Ker}(G_\mathfrak{P} \to 1) \cong \mathrm{Ker}(\mathbb{Z}/2\mathbb{Z} \to 1) = \mathbb{Z}/2\mathbb{Z}$. Note we have a exact sequence $1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1 \to 1$.

(b) We already know $\mathfrak{P} = 3\mathbb{Z}[i]$ is prime. Then $e = 1$ and so $I_\mathfrak{P} = 1$. Since $\mathfrak{k}(3) = \mathbb{Z}/3\mathbb{Z} \cong \mathbb{F}_3$ and $\mathfrak{k}(3\mathbb{Z}[i]) = \mathbb{Z}[i]/3\mathbb{Z}[i] \cong \mathbb{F}_9$, we have $\mathrm{Gal}(\mathfrak{k}(3\mathbb{Z}[i])/\mathfrak{k}(3)) \cong \mathbb{Z}/2\mathbb{Z}$. Since $\tau(3\mathbb{Z}[i]) = 3\mathbb{Z}[i]$, we have $G_\mathfrak{P} = \langle\tau\rangle$. Note we have a exact sequence $1 \to 1 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$.

(c) Recall we saw that $5\mathbb{Z}[i] = \mathfrak{P}_1\mathfrak{P}_2 = \langle 2 - i\rangle\langle 2 + i\rangle$ and $\mathbb{Z}[i]/\langle 2 - i\rangle\mathbb{Z}[i] \cong \mathbb{F}_5$. Since $\tau(\mathfrak{P}_1) = \mathfrak{P}_2$, $\tau(\mathfrak{P}_2) = \mathfrak{P}_1$, $G_{\mathfrak{P}_1} = 1 = G_{\mathfrak{P}_2}$ and hence $I_{\mathfrak{P}_1} = 1 = I_{\mathfrak{P}_2}$. Note we have a exact sequence $1 \to 1 \to 1 \to 1 \to 1$.

Example 3.23. Let $\mathcal{L} = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ be the splitting field of $x^3 - 2 = (x - \sqrt[3]{2})(x - \xi_3\sqrt[3]{2})(x - \xi_3^2\sqrt[3]{2})$.



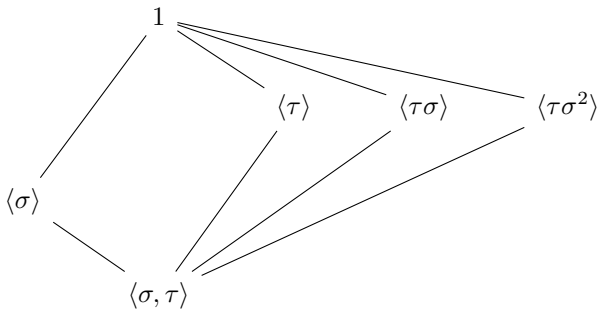
Since $\gcd(2,3)=1$, $\mathcal{L}/\mathbb{Q}$ is Galois extension of degree 6. (Or follow from $\mathrm{char}(\mathbb{Q})=\infty$.) Since $\mathrm{Gal}(\mathcal{L}/\mathbb{Q})$ acts as permutations of the 3 roots of x^3-2, $G \leqslant S_3$. Also, $|G|=6$, $\mathrm{Gal}(\mathcal{L}/\mathbb{Q})=S_3$. In particular, $\mathrm{Gal}(\mathcal{L}/\mathbb{Q}) \cong \langle \sigma, \tau \rangle$, where

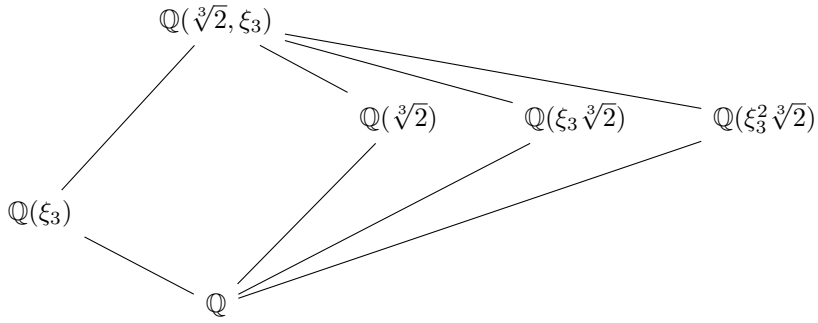
$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto & \xi_3 \sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3 \end{cases}, \quad \tau : \begin{cases} \sqrt[3]{2} \mapsto & \sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3^2 = -1 - \xi_3 \end{cases}.$$

Since $\sigma^2(\sqrt[3]{2}) = \sigma(\xi_3\sqrt[3]{2}) = \sigma(\xi_3)\sigma(\sqrt[3]{2}) = \xi_3^2\sqrt[3]{2}$, we have $\sigma^3(\sqrt[3]{2}) = \sigma(\xi_3^2\sqrt[3]{2}) = \sigma(\xi_3^2)\sigma(\sqrt[3]{2}) = \xi_3^2\xi_3\sqrt[3]{2} = \sqrt[3]{2}$. Also, $\tau^2(\xi_3) = \tau(\xi_3^2) = \tau(\xi_3)^2 = \xi_3^4 = \xi_3$. Then $|\sigma| = 3$. Similarly, $|\tau| = 2$. So $\{1, \sigma, \sigma^2\} \leqslant \mathrm{Gal}(\mathcal{L}/\mathbb{Q})$ and $\{1, \tau\} \leqslant \mathrm{Gal}(\mathcal{L}/\mathbb{Q})$. Also, $\sigma\tau = \tau\sigma^2$. Hence $\mathrm{Gal}(\mathcal{L}/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. We have

$$\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto & \xi_3^2\sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3 \end{cases}, \quad \tau\sigma : \begin{cases} \sqrt[3]{2} \mapsto & \xi_3^2\sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3^2 \end{cases}, \quad \tau\sigma^2 : \begin{cases} \sqrt[3]{2} \mapsto & \xi_3\sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3^2 \end{cases}.$$

From SAGE, we can calculate $\mathcal{L} \cong \mathbb{Q}[x]/\langle f \rangle$, where $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$ and $\Delta_{\mathcal{L}} = -2^4 \cdot 3^7$. So 2 and 3 are the only primes that ramify in $\mathcal{L}$. If α is a root if f, then by SAGE, $[\mathcal{O}_{\mathcal{L}} : \mathbb{Z}[\alpha]] = 3^5$, and so we will avoid 3. We would use SAGE to do all the calculations, but we choose to do these by hand instead. Define $\mathcal{K} := \mathbb{Q}(\xi_3)$. Then $o_{\mathcal{K}} = \mathbb{Z}[\xi_3]$. It is easy to see $\mathcal{K} = \mathbb{Q}(\xi_3) = \mathcal{L}^{\langle\sigma\rangle}$. So $\mathcal{L}/\mathcal{K}$ is Galois. There is 1-1 correspondence between the diagram of subgroups of $\langle \sigma, \tau \rangle$ and subfields for $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$.





The subfields in the second diagram are precisely the fixed fields of the subgroups in the first diagram. Since only the subgroup $\langle\sigma\rangle \trianglelefteq \langle\sigma, \tau\rangle$, the subfield $\mathbb{Q}(\xi_3)$ is the only subfield that is Galois over $\mathbb{Q}$. We can verify $\mathcal{O}_{\mathcal{L}} = \mathbb{Z}[\xi_3, \sqrt[3]{2}] = \mathbb{Z}[\xi_3][\sqrt[3]{2}] = o_{\mathcal{K}}[\sqrt[3]{2}]$.

(a) Consider $\mathcal{O}_\mathcal{K}/2\mathcal{O}_\mathcal{K} = \mathbb{Z}[\xi_3]/\langle 2\rangle \cong \mathbb{Z}[x]/\langle x^2+x+1, 2\rangle \cong \mathbb{F}_2[x]/\langle x^2+x+1\rangle$, where $m_{\xi_3,\mathbb{Q}}(x) = x^2+x+1$ is irreducible modulo 2. So $\mathfrak{p} = 2\mathcal{O}_\mathcal{K} \leqslant \mathcal{O}_\mathcal{K}$ is prime with $r = 1$, $e(\mathfrak{p}/2) = 1$ and $f(\mathfrak{p}/2) = 2$. Then $|I_\mathfrak{p}| = e(\mathfrak{p}/2) = 1$ and since $r = 1$, $G_\mathfrak{p} = \mathrm{Gal}(\mathcal{K}/\mathbb{Q}) = \langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathrm{Gal}(\mathfrak{k}(\mathfrak{p})/\mathfrak{k}(2)) \cong \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$, we have an exact sequence

$$1 \to 1 \to \langle\tau\rangle \to \langle\tau\rangle \to 1.$$

Since $[\mathcal{L} : \mathcal{K}] = 3$, $m_{\sqrt[3]{2},\mathcal{K}}(x) = x^3 - 2$ and then $\mathcal{L} \cong \mathcal{K}[x]/\langle x^3-2\rangle \cong \mathcal{K}(\sqrt[3]{2})$. Since $\sqrt[3]{2} \in \mathcal{O}_\mathcal{L}$, we have $\mathcal{O}_\mathcal{L}/\langle\mathfrak{p}\rangle = \mathcal{O}_\mathcal{K}[x]/\langle x^3-2, \mathfrak{p}\rangle \cong \frac{\frac{\mathcal{O}_\mathcal{K}}{\mathfrak{p}}[x]}{\langle x^3-2\rangle} = \frac{\frac{\mathcal{O}_\mathcal{K}}{2\mathcal{O}_\mathcal{K}}[x]}{\langle x^3-2\rangle} \cong \frac{\mathbb{F}_4[x]}{\langle x^3-2\rangle}$. Since $x^3 - 2 \equiv x^3 \pmod{2\mathcal{O}_\mathcal{K}}$, we have $2\mathcal{O}_\mathcal{L} = 2\mathcal{O}_\mathcal{K}\mathcal{O}_\mathcal{L} = \mathfrak{p}\mathcal{O}_\mathcal{L} = \langle\mathfrak{p}, \sqrt[3]{2}\rangle^3 =: \mathfrak{P}^3$. So $r = 1$, $e(\mathfrak{P}/\mathfrak{p}) = 3$ and $f(\mathfrak{P}/\mathfrak{p}) = 1$. Since $r = 1$, $G_{\mathfrak{P}/\mathfrak{p}} = \mathrm{Gal}(\mathcal{L}/\mathcal{K}) = \langle\sigma\rangle$. Since $e(\mathfrak{P}/\mathfrak{p}) = 3$, $I_{\mathfrak{P}/\mathfrak{p}} = \langle\sigma\rangle$. Since $\frac{\mathcal{O}_\mathcal{L}}{\mathfrak{P}} = \frac{\mathcal{O}_\mathcal{K}[\sqrt[3]{2}]}{\langle\mathfrak{p}, \sqrt[3]{2}\rangle} \cong \frac{\frac{\mathcal{O}_\mathcal{K}}{\mathfrak{p}}[\sqrt[3]{2}]}{\langle\sqrt[3]{2}\rangle} \cong (\mathcal{O}_\mathcal{K}/\mathfrak{p})^{\deg(x)} = \mathcal{O}_\mathcal{K}/\mathfrak{p}$, $\mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})) \cong 1$. Note we have an exact sequence

$$1 \to \langle\sigma\rangle \to \langle\sigma\rangle \to 1 \to 1.$$

Since $\mathfrak{P} \leqslant \mathcal{O}_\mathcal{L}$, $\sqrt[3]{2} \in \mathfrak{P}$ and $\xi_3 \in \mathcal{O}_\mathcal{K} \subseteq \mathcal{O}_\mathcal{L}$, $\xi_3\sqrt[3]{2}$, $\xi_3^2\sqrt[3]{2} \in \mathfrak{P}$ and then $\sigma(\mathfrak{P}) = \mathfrak{P}$. Similarly, since $\xi^2 \notin \mathfrak{P}$, $\tau(\mathfrak{P}) = \mathfrak{P}$ and then $\langle\sigma,\tau\rangle \leqslant G_\mathfrak{P} \leqslant \mathrm{Gal}(\mathcal{L}/\mathbb{Q}) = \langle\sigma,\tau\rangle$. Hence $G_\mathfrak{P} = \langle\sigma,\tau\rangle \cong S_3$. Since $e(\mathfrak{P}/2) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/2) = 3$, $|I_\mathfrak{P}| = 3$. Also, since the only subgroup of $G_\mathfrak{P}$ of order 3 is $\langle\sigma\rangle$, $I_\mathfrak{P} = \langle\sigma\rangle \cong \mathbb{Z}/3\mathbb{Z}$. Similarly, $f(\mathfrak{P}/2) = 2$. Note we have an exact sequence

$$1 \to \langle\sigma\rangle \to \langle\sigma,\tau\rangle \to \langle\tau\rangle \to 1.$$

Thus, we have

$$\begin{array}{c}
\mathfrak{P} \\
{\scriptstyle 3}\,\big|\,{\scriptstyle 1} \\
\mathfrak{p}_\mathcal{T} \\
{\scriptstyle 1}\,\big|\,{\scriptstyle 1} \\
\mathfrak{p}_\mathcal{Z} \\
{\scriptstyle 1}\,\big|\,{\scriptstyle 1} \\
\mathfrak{p} \\
{\scriptstyle 1}\,\big|\,{\scriptstyle 1} \\
2_\mathcal{T} \\
{\scriptstyle 1}\,\big|\,{\scriptstyle 2} \\
2_\mathcal{Z} \\
{\scriptstyle 1}\,\big|\,{\scriptstyle 1} \\
2
\end{array}$$

(b) Consider $\mathcal{O}_\mathcal{K}/\mathfrak{p} = \mathcal{O}_\mathcal{K}/3\mathcal{O}_\mathcal{K} \cong \frac{\mathbb{Z}[x]}{\langle 3, x^2+x+1\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^2+x+1\rangle}$, where $x^2+x+1 \equiv (x-1)^2 \pmod 3$. So $3\mathcal{O}_\mathcal{K} = \langle 3, \xi_3 - 1\rangle^2 =: \mathfrak{p}^2$. So $r = 1$, $e(\mathfrak{p}/3) = 2$ and $f(\mathfrak{p}/3) = 1$. Then $|I_\mathfrak{p}| = e(\mathfrak{p}/3) = 2$ and since

$r = 1$, $G_{\mathfrak{p}} = \mathcal{K}/\mathbb{Q} = \langle\tau\rangle$. Since $I_{\mathfrak{p}} \leqslant G_{\mathfrak{p}}$ and $|I_{\mathfrak{p}}| = |G_{\mathfrak{p}}|$, $I_{\mathfrak{p}} = \langle\tau\rangle$. Since $\frac{\mathcal{O}_{\mathcal{K}}}{\mathfrak{p}} = \frac{\mathbb{Z}[\xi_3]}{\langle 3, \xi_3 - 1\rangle} \cong \frac{\mathbb{F}_3[\xi_3]}{\xi_3 - 1} \cong \mathbb{F}_3$, we have $\mathrm{Gal}(\mathfrak{k}(\mathfrak{p})/\mathfrak{k}(3)) \cong 1$. Note we have an exact sequence

$$1 \to \langle\tau\rangle \to \langle\tau\rangle \to 1 \to 1.$$

Since $x^3 - 2 \equiv x^3 + 1 \equiv (x+1)^3 \pmod{3\mathcal{O}_{\mathcal{K}}}$, we have $3\mathcal{O}_{\mathcal{L}} = \langle 3, \sqrt[3]{2} + 1\rangle^3 =: \mathfrak{P}^3$. So $r = 1$, $e(\mathfrak{P}/\mathfrak{p}) = 3$ and $f(\mathfrak{P}/\mathfrak{p}) = 1$. Since $r = 1$, $G_{\mathfrak{P}} = \mathrm{Gal}(\mathcal{L}/\mathcal{K}) = \langle\sigma\rangle$. Since $e(\mathfrak{P}/\mathfrak{p}) = 3$, $|I_{\mathfrak{P}}| = 3$. Since $\frac{\mathcal{O}_{\mathcal{L}}}{\mathfrak{P}} \cong \frac{\mathcal{O}_{\mathcal{K}}[\sqrt[3]{2}]}{\langle \mathfrak{p}, \sqrt[3]{2}+1\rangle} \cong \frac{\frac{\mathcal{O}_{\mathcal{K}}}{\mathfrak{p}}[\sqrt[3]{2}]}{\langle \sqrt[3]{2}+1\rangle} \cong \mathcal{O}_{\mathcal{K}}/\mathfrak{p}$, $\mathrm{Gal}(\mathfrak{k}(\mathfrak{P})/\mathfrak{k}(\mathfrak{p})) \cong 1$. Note we have an exact sequence

$$1 \to \langle\sigma\rangle \to \langle\sigma\rangle \to 1 \to 1.$$

Since $e(\mathfrak{P}/2) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/2) = 6$ and $f(\mathfrak{P}/2) = f(\mathfrak{P}/\mathfrak{p})f(\mathfrak{p}/2) = 1$, we have an exact sequence

$$0 \to \langle\sigma, \tau\rangle \to \langle\sigma, \tau\rangle \to 1 \to 1.$$

Thus, we have

$$\begin{array}{c} \mathfrak{P} \\ {\scriptstyle 3}\big| {\scriptstyle 1} \\ \mathfrak{p}_{\mathcal{T}} \\ {\scriptstyle 1}\big| {\scriptstyle 1} \\ \mathfrak{p}_{\mathcal{Z}} \\ {\scriptstyle 1}\big| {\scriptstyle 1} \\ \mathfrak{p} \\ {\scriptstyle 2}\big| {\scriptstyle 1} \\ 3_{\mathcal{T}} \\ {\scriptstyle 1}\big| {\scriptstyle 1} \\ 3_{\mathcal{Z}} \\ {\scriptstyle 1}\big| {\scriptstyle 1} \\ 3 \end{array}$$

(c) Consider $\mathcal{O}_{\mathcal{K}}/7\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\xi_3]/\langle 7\rangle \cong \mathbb{Z}[x]/\langle x^2 + x + 1, 2\rangle \cong \mathbb{F}_7[x]/\langle x^2 + x + 1\rangle$, where $m_{\xi_3,\mathbb{Q}}(x) = x^2 + x + 1 = (x-2)(x+3) \pmod 7$. So $7\mathcal{O}_{\mathcal{K}} = \langle 7, \xi_3 - 2\rangle\langle 7, \xi_3 + 3\rangle =: \mathfrak{p}_1\mathfrak{p}_2$. Then $r = 2$, $e(\mathfrak{p}_1/7) = 1 = e(\mathfrak{p}_2/7)$, as is expected since $7 \nmid \Delta_{\mathcal{L}}$ and $f(\mathfrak{p}_1/7) = 1 = f(\mathfrak{p}_2/7)$. Note $\tau(\xi_3 + 3) = -1 - \xi_3 + 3 = 2 - \xi_3$. If $\tau(\mathfrak{p}_2) = \mathfrak{p}_2$, then $2 - \xi_3 \in \mathfrak{p}_2$, which means $(2 - \xi_3) + (3 + \xi_3) = 5 \in \mathfrak{p}_2$. Then $5, 7 \in \mathfrak{p}_2$. Since $\mathbb{Z}[\xi_3]$ is a ED, $1 = \gcd(5, 7) \in \mathfrak{p}_2$, a contradiction. So $\tau(\mathfrak{p}_2) = \mathfrak{p}_1$. Similarly, $\tau(\mathfrak{p}_1) = \mathfrak{p}_2$. Hence $G_{\mathfrak{p}_1} = 1 = G_{\mathfrak{p}_2}$ and so $I_{\mathfrak{p}_1} = 1 = I_{\mathfrak{p}_2}$. Note we have an exact sequence

$$1 \to 1 \to 1 \to 1 \to 1.$$

Now we consider $\mathfrak{p}_1\mathcal{O}_{\mathcal{L}}$ and $\mathfrak{p}_2\mathcal{O}_{\mathcal{L}}$. We can easily check that $x^3 - 2$ is irreducible modulo 7. Let $j \in \{1, 2\}$. To factor $\mathfrak{p}_j$ in $\mathcal{L}$, we want to factor $x^3 - 2 \pmod{\mathfrak{p}_j}$. Since $f(\mathfrak{p}_j/7) = 1$, $\mathcal{O}_{\mathcal{K}}/\mathfrak{p}_j \cong \mathbb{F}_7$. Since $x^3 - 2$ is irreducible modulo 7, $x^3 - 2$ is irreducible modulo $\mathfrak{p}_j$ as well. So $\mathfrak{P}_j := \mathfrak{p}_j\mathcal{O}_{\mathcal{L}}$ is

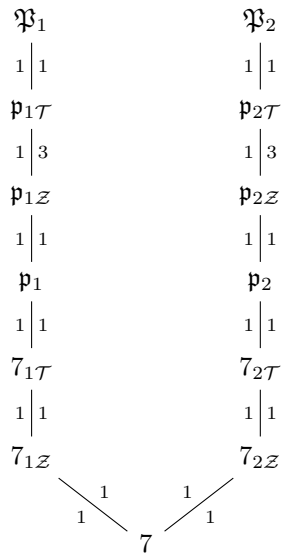
prime and then $r = 1$, $e(\mathfrak{P}_j/\mathfrak{p}_j) = 1$ and $f(\mathfrak{P}_j/\mathfrak{p}_j) = 3$. Since $e(\mathfrak{P}_j/\mathfrak{p}_j) = 1$, $I_{\mathfrak{P}_j/\mathfrak{p}_j} = 1$. Since $f(\mathfrak{P}_j/\mathfrak{p}_j) = 3$, $\mathrm{Gal}(\mathfrak{k}(\mathfrak{P}_j)/\mathfrak{k}(\mathfrak{p}_j)) = \langle\sigma\rangle$. So $G_{\mathfrak{P}_j/\mathfrak{p}_j} = \langle\sigma\rangle$. Note we have an exact sequence

$$1 \to 1 \to \langle\sigma\rangle \to \langle\sigma\rangle \to 1.$$

Since $e(\mathfrak{P}_j/2) = e(\mathfrak{P}_j/\mathfrak{p}_j)e(\mathfrak{p}_j/2) = 1$ and $f(\mathfrak{P}_j/2) = f(\mathfrak{P}_j/\mathfrak{p}_j)f(\mathfrak{p}_j/2) = 3$, we have an exact sequence

$$0 \to 1 \to \langle\sigma\rangle \to \langle\sigma\rangle \to 1.$$

Thus, we have



(d) Consider $\mathcal{O}_\mathcal{K}/5\mathcal{O}_\mathcal{K} = \mathbb{Z}[\xi_3]/\langle 5\rangle \cong \mathbb{Z}[x]/\langle x^2 + x + 1, 2\rangle \cong \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$, where $m_{\xi_3,\mathbb{Q}}(x) = x^2 + x + 1$ is irreducible modulo 5. So $\mathfrak{p} = 5\mathcal{O}_\mathcal{K} \leqslant \mathcal{O}_\mathcal{K}$ is prime with $r = 1$, $e(\mathfrak{p}/2) = 1$ and $f(\mathfrak{p}/2) = 2$. So $|I_\mathfrak{p}| = e(\mathfrak{p}/2) = 1$ and since $r = 1$, $G_\mathfrak{p} = \mathrm{Gal}(\mathcal{K}/\mathbb{Q}) = \langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathrm{Gal}(\mathfrak{k}(\mathfrak{p})/\mathfrak{k}(2)) \cong \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$, we have an exact sequence

$$1 \to 1 \to \langle\tau\rangle \to \langle\tau\rangle \to 1.$$

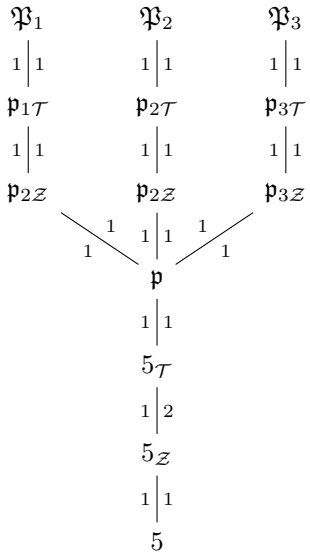
Since $[\mathcal{L} : \mathcal{K}] = 3$, $m_{\sqrt[3]{2},\mathcal{K}}(x) = x^3 - 2$ and then $\mathcal{L} \cong \mathcal{K}[x]/\langle x^3 - 2\rangle \cong \mathcal{K}(\sqrt[3]{2})$. Since $\sqrt[3]{2} \in \mathcal{O}_\mathcal{L}$, we have $\mathcal{O}_\mathcal{L}/\langle\mathfrak{p}\rangle = \mathcal{O}_\mathcal{K}[x]/\langle x^3 - 2, \mathfrak{p}\rangle \cong \frac{\mathcal{O}_\mathcal{K}/\mathfrak{p}[x]}{\langle x^3-2\rangle} = \frac{\mathcal{O}_\mathcal{K}/5\mathcal{O}_\mathcal{K}[x]}{\langle x^3-2\rangle}$. Since 2 is a multiple root and $\mathcal{L}/\mathcal{K}$ is Galois, $x^3 - 2 \equiv (x + 2)(x + \alpha(\xi_3))(x + \beta(\xi_3)) \pmod{5\mathcal{O}_\mathcal{K}}$ for some $\alpha(\xi_3), \beta(\xi_3) \in 5\mathbb{Z}[\xi_3]$. Then $5\mathcal{O}_\mathcal{L} = \langle 2, \sqrt[3]{2} + 2\rangle\langle 2, \sqrt[3]{2} + \alpha(\xi_3)\rangle\langle\sqrt[3]{2} + \beta(\xi_3)\rangle =: \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$. So $r = 3$, $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ and $f(\mathfrak{P}_i/\mathfrak{p}) = 1$ for $j = 1, 2, 3$. Let $j \in \{1, 2, 3\}$. Since $e(\mathfrak{P}_j/\mathfrak{p}) = 1$, $I_{\mathfrak{P}_j/\mathfrak{p}} = 1$. Since $f(\mathfrak{P}_j/\mathfrak{p}) = 1$, $\mathrm{Gal}(\mathfrak{k}(\mathfrak{P}_1)/\mathfrak{k}(\mathfrak{p})) = 1$. Note we have an exact sequence

$$1 \to 1 \to 1 \to 1 \to 1.$$

Since $e(\mathfrak{P}_j/2) = e(\mathfrak{P}_j/\mathfrak{p})e(\mathfrak{p}/2) = 1$ and $f(\mathfrak{P}_j/2) = f(\mathfrak{P}_j/\mathfrak{p})f(\mathfrak{p}/2) = 2$, we have an exact sequence

$$1 \to 1 \to \langle\tau\rangle \to \langle\tau\rangle \to 1.$$

Thus, we have


$\mathfrak{P}_1$
$\mathfrak{P}_2$
$\mathfrak{P}_3$
$\mathfrak{p}_{1\mathcal{T}}$
$\mathfrak{p}_{2\mathcal{T}}$
$\mathfrak{p}_{3\mathcal{T}}$
$\mathfrak{p}_{2\mathcal{Z}}$
$\mathfrak{p}_{2\mathcal{Z}}$
$\mathfrak{p}_{3\mathcal{Z}}$
$\mathfrak{p}$
$5_{\mathcal{T}}$
$5_{\mathcal{Z}}$
5

Chapter 4

Cyclotomic Extension

4.1 Roos of Units

Definition 4.1. Let $\mathcal{K}$ be a field. An n^{th} root of unity in $\mathcal{K}$ is a root of the polynomial $x^n - 1$. Since $x^n - 1$ has at most n roots in any field, there are at most n different n^{th} roots of unity. We say an n^{th} root of unity ξ_n is primitive if $\xi_n^n = 1$ and $\xi_n^m \neq 1$ for $1 \leqslant m < n$, i.e., ξ_n is an element of order n in $\mathcal{K}^\times$.

Remark. Any two primitive n^{th} roots of unity in a field $\mathcal{K}$ are powers of each other.

Example 4.2. (a) The n^{th} roots of unity in $\mathbb{R}$ are $\{\pm 1\}$.

(b) The n^{th} roots of unity in $\mathbb{C}$ are the numbers $\left\{e^{\frac{2\pi i m}{n}},\ 0 \leqslant m \leqslant n-1\right\}$.

(c) The p^{th} roots of unity in $\mathbb{F}_p$ are $\{1\}$ since $0 = x^p - 1 = (x-1)^p$ in $\mathbb{F}_p$. So the map $\mathbb{F}_p \to \mathbb{F}_p$ given by $x \mapsto x^p$ is 1-1.

Theorem 4.3. *Let $\mathcal{K}$ be field. Then any finite subgroup of $\mathcal{K}^\times = \mathcal{K} \smallsetminus \{0\}$ is cyclic. In particular, the group of n^{th} roots of unity in $\mathcal{K}$ is cyclic.*

Proof. Let $\mathcal{K}$ be a field and G be a finite subgroup of the abelian group $\mathcal{K}^\times$. Let $m \in G$ have maximal order N. Suppose there exists $g \in G$ with $|g| \nmid N$. Since $|gm| = \operatorname{lcm}(|g|, |m|) > |m| = N$, a contradiction. So for any $g \in G$, we have $|g| \mid N$. Hence for any $g \in G$, g is a root of $x^N - 1$. Then $\#G \leqslant N$. Also, since $N \mid |G|$, we have $\#G = N$. Thus, $G = \langle m \rangle$. □

Example 4.4. (a) The group of n^{th} roots of unity in $\mathbb{C}$ is cyclic with generator $e^{2\pi i/n}$.

(b) Any subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

(c) Since $\mathbb{Z}/p^r\mathbb{Z}$ for $r > 1$ is not a field, $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is not necessarily cyclic. For example, $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic.

(d) $\mathbb{Z}/n\mathbb{Z}$ is an additive cyclic group for any $n \in \mathbb{N}$ and there are $\varphi(n)$ primitive n^{th} roots of unity.

(e) $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 1, 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k \geqslant 1$. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, there are $\varphi(\varphi(n))$ primitive $\varphi(n)^{\text{th}}$ roots of unity mod n, i.e., there are $\varphi(\varphi(n))$ elements of order $\varphi(n)$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, there are $\varphi(p-1)$ primitive $(p-1)^{\text{th}}$ roots of unity in $(\mathbb{Z}/p\mathbb{Z})^\times$. For example, 3 is a primitive 6^{th} root of unity but 2 is not.

Corollary 4.5. Let $\xi_n = e^{\frac{2\pi i}{n}}$ be the n^{th} root of unity. Then $\xi_n^m = e^{\frac{2\pi i}{n}m}$ is a primitive n^{th} root of unity if and only if $\gcd(m, n) = 1$.

Proof. Follow from $\mathcal{K}^\times$ is a group. □

4.2 Properties

Definition 4.6. We say an extension $\mathcal{L}/\mathcal{K}$ is *cyclotomic* if $\mathcal{L} = \mathcal{K}(\xi_n)$ for some n^{th} root of unity $\xi_n \in \overline{\mathcal{K}}$.

Remark. The term cyclotomic means "circle-dividing" which comes from the fact that the n^{th} roots of unity in $\mathbb{C}$ divide a cicle into n arcs of equal length

Remark. The important algebraic fact we will explore is that cyclotomic extensions of every field have an abelian Galois group. Other constructions of abelian extensions are Kummer extensions, Artin-Schreier-Witt extension and Carlitz extensions, but these all require special conditions on the base field.

Remark. Consider a cyclotomic extension $\mathcal{K}(\xi_n)/\mathcal{K}$ with ξ_n a primitive n^{th} root of unity. Then $x^n - 1$ has every power of ξ_n as a root, so it has n different roots. Hence $x^n - 1$ is separable over $\mathcal{K}$. Conversely, if $x^n - 1$ is separable over $\mathcal{K}$, then it has n different roots, so they form a cyclic group under multiplication. Then there is a (primitive) root of unity of order n among the n^{th} roots of unity. Therefore, when we construct cyclotomic extensions $\mathcal{K}(\xi_n)/\mathcal{K}$, little is lost by assuming $x^n - 1$ is separable over $\mathcal{K}$ if and only if $x^n - 1$ and nx^{n-1} have no common roots if and only if $n \neq 0$ in $\mathcal{K}$: $\text{char}(\mathcal{K}) = 0$, or $\text{char}(\mathcal{K}) = p$ and $(p, n) = 1$.

Remark. In a field $\mathcal{K}$, if there are n different n^{th} roots of unity, we denote the group of them by μ_n. For instance, in $\mathbb{C}$ we have $\mu_2 = \{1, -1\}$ and $\mu_4 = \{1, -1, i, -i\}$. In $\mathbb{F}_7$, we have $\mu_3 = \{1, 2, 4\}$. A generator of μ_n is denoted ξ_n which is a primitive n^{th} root of unity. Let $a \in \mathbb{Z}$. Since $|\xi_n| = n$, we have $|\xi_n^a| = \frac{n}{(n,a)}$. So ξ_n^a is a generator if and only if $(n, a) = 1$. So when a field contains n different n^{th} roots of unity.

Remark. When $x^n - 1$ is separable over $\mathcal{K}$, $\mathcal{K}(\xi_n)/\mathcal{K}$ is Galois since $\mathcal{K}(\xi_n)$ is the splitting field of $x^n - 1$ over $\mathcal{K}$.

Lemma 4.7. For $\sigma \in \text{Gal}(\mathcal{K}(\xi_n)/\mathcal{K})$, there is $a_\sigma \in \mathbb{Z}$ with $(n, a_\sigma) = 1$ such that $\sigma(\xi_n) = \xi_n^{a_\sigma}$.

Proof. Since $\xi_n^n = 1$ and $\xi_n^j \neq 1$ for $1 \leqslant j < n$, we have $\sigma(\xi_n)^n = 1$ and $\sigma(\xi_n) \neq 1$ for $1 \leqslant j < n$. So $\sigma(\xi_n)$ is a primitive n^{th} root of unity. Then $\sigma(\xi_n) = \xi_n^{a_\sigma}$ for some $a_\sigma \in \mathbb{Z}$ with $(n, a_\sigma) = 1$. □

Example 4.8. In $\mathbb{Q}$, the primitive 7^{th} roots of unity are the 7^{th} roots of unity besides 1 and they are all roots of $f(x) = x^6 + \cdots + x + 1$. This polynomial is irreducible over $\mathbb{Q}$ becasue it becomes Eisenstein at 7 when we replace x with $x+1$: $f(x) = x^7 + 7x^5 + 21x^4 + 35x^3 + 35x^2 + 21x + 7$. This implies, for instance, that ξ_7 and ξ_7^2 have the same minimal polynomial over $\mathbb{Q}$. Since $\mathbb{Q}(\xi_7) = \mathbb{Q}(\xi_7^2)$, there is an automorphism $\sigma \in \text{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q})$ that sends ξ_7 to ξ_7^2.

Theorem 4.9. *The mapping*

$$\Psi : \mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma \mapsto a_\sigma$$

is an injective group homomorphism, where $\sigma(\xi_n) = \xi_n^{a_\sigma}$.

Proof. Let $\sigma, \tau \in \mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K})$. Then $(\sigma \circ \tau)(\xi_n) = \sigma(\xi_n^{a_\tau}) = \sigma(\xi_n)^{a_\tau} = (\xi_n^{a_\sigma})^{a_\tau} = \xi_n^{a_\sigma a_\tau}$. Also, since $(\sigma \circ \tau)(\xi_n) = \xi_n^{a_{\sigma\circ\tau}}$, we have $\xi_n^{a_{\sigma\circ\tau}} = \xi_n^{a_\sigma a_\tau}$. So $a_{\sigma\circ\tau} \equiv a_\sigma a_\tau \pmod n$. Hence $\Psi(\sigma \circ \tau) \equiv \Psi(\sigma)\Psi(\tau) \pmod n$. Thus, Ψ is an homomorphism. Since $\mathrm{Ker}(\Psi) = \{\sigma \in \mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K}) : a_\sigma \equiv 1 \pmod n\} = \{\sigma \in \mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K}) : \sigma(\xi_n) = \xi_n\} = 1$, we have Ψ is 1-1. □

Remark. Since $(\mathbb{Z}/n\mathbb{Z})^\times$, the embedded subgroup $\mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K})$ is abelian. So cyclotomic extensions are always abelian.

Example 4.10. Complex conjugation is an automorphism of $\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_n)$ with order 2. Under the embedding of $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ into $(\mathbb{Z}/n\mathbb{Z})^\times$, complex conjugation corresponds to -1 mod n since $\overline{\sigma}(\xi_n) = \overline{\xi}_n = \xi_n^{-1}$.

Remark. The embedding of $\mathrm{Gal}(\mathcal{K}(\xi_n)/\mathcal{K})$ into $(\mathbb{Z}/n\mathbb{Z})$ may not be surjective; that depends on $\mathcal{K}$. For instance, if $\mathcal{K} = \mathbb{R}$ and $n \geqslant 3$, then $\mathcal{K}(\xi_n)/\mathcal{K} = \mathbb{C}/\mathbb{R}$ is a quadratic extension. The nontrivial $\mathbb{R}$-automorphism of $\mathbb{C}$ is complex conjugation, whose effect on roots of unity in $\mathbb{C}$ is to invert them: $\overline{\xi} = \xi^{-1}$. Therefore the embedding $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ for $n \geqslant 3$ has image $\{\pm \bmod n\}$, which is smaller than $(\mathbb{Z}/n\mathbb{Z})^\times$ unless $n = 2, 3, 4$ or 6.

Proposition 4.11. If $f \in \mathbb{Z}[x]$ is monic and $g \mid f$ where $g \in \mathbb{Q}[x]$ is monic, then $g \in \mathbb{Z}[x]$.

Proof. Let $f = gh$. Then $h \in \mathbb{Q}[x]$ is also monic. So there exists $\alpha, \beta \in \mathbb{Q}$ such that $\alpha g, \beta h \in \mathbb{Z}[x]$ are primitive. By Gauss's lemma, $\alpha\beta gh = (\alpha g)(\beta h) \in \mathbb{Z}[x]$ is also primitive. Then $\alpha\beta = \pm 1$. So $\alpha = \pm 1 = \beta$. Hence $g \in \mathbb{Z}[x]$. □

Corollary 4.12. Let $\mathcal{K}$ be a number field and $\alpha \in \mathcal{O}_\mathcal{K}$. If β is a root of $m_\alpha(x)$, then $m_\beta \in \mathbb{Z}[x]$.

Theorem 4.13. *The embedding* $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ *is an isomorphism.*

Proof. To prove $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is a surjection, it is enough to show for all $a \in \mathbb{Z}$ such that $(a, n) = 1$ that ξ_n and ξ_n^a are $\mathbb{Q}$-conjugate: their minimal polynomial over $\mathbb{Q}$ agree. Wlog., take $a > 0$ and in fact $a > 1$. Write $a = p_1 \cdots p_r$, where p_i's are not necessarily distinct. Then $p_i \nmid n$ for $i = 1, \ldots, r$. To show ξ_n and ξ_n^a have the same minimal polynomial over $\mathbb{Q}$, it suffices to show, for each prime p not dividing n, that any primitive n^{th} root of unity and its p^{th} power have the same minimal polynomial over $\mathbb{Q}$, since then the successive pairs of primitive n^{th} roots of unity $\xi_n, \xi_n^{p_1}, \xi_n^{p_1p_2}, \ldots, \xi_n^{p_1\cdots p_r} = \xi_n^a$ have the same minimal polynomial over $\mathbb{Q}$ since each is a prime power of the previous one. Suppose ξ_n and ξ_n^p were not $\mathbb{Q}$-conjugate for prime $p \nmid n$. Let $f(x) = m_{\xi_n,\mathbb{Q}}(x)$ and $g(x) = m_{\xi_n^p,\mathbb{Q}}(x)$. Then $f \neq g$. Since f, g are monic, $x^n - 1 \in \mathbb{Z}[x]$, $f \mid x^n - 1$ and $g \mid x^n - 1$, by previous proposition, $f, g \in \mathbb{Z}[x]$. Write $x^n - 1 = fgh$ for $h \in \mathbb{Q}[x]$. Then h is monic and similarly, we have $h \in \mathbb{Z}[x]$. Reducing the above equation modulo p, $x^n - \overline{1} = \overline{f}\overline{g}\overline{h}$. Since $p \nmid n$, $x^n - \overline{1}$ is separable in $\mathbb{F}_p[x]$. Then $\overline{f}$ and $\overline{g}$ are relatively prime in $\mathbb{F}[x]$. Since f and g are monic, $\deg(\overline{f}) = \deg(f)$ and $\deg(\overline{g}) = \deg(g)$. So $\overline{f}$ and $\overline{g}$ are nonconstant. Since $g(\xi_n^p) = 0$, $g(x^p)$ has ξ_n as a root and then $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$. Write $g(x^p) = f(x)k(x)$ for some $k \in \mathbb{Z}[x]$. Reducing the above equation modulo p and use the formula $\overline{g}(x^p) = \overline{g}(x)^p$ in $\mathbb{F}_p[x]$ to get $\overline{g}(x)^p = \overline{f}\overline{k}$. Thus, any irreducible factor of the nonconstant $\overline{f}$ is a factor of $\overline{g}$, which contradicts relative primality of $\overline{f}$ and $\overline{g}$. □

Theorem 4.14. *The p^{th} power map $\varphi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $\varphi(t) = t^p$ generates* $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Proof. Since $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of $x^{p^n} - x$, which is separable, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. By Fermat little theorem, $a^p = a$ for any $a \in \mathbb{F}_p$. So φ_p fixes $\mathbb{F}_p$ pointwisely. Also, Since φ_p is a field homomorphism and $\varphi_p(1) = 1$, it is 1-1 and then onto. So $\varphi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Since $\#\,\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, it is enough to show $|\varphi_p| = n$. For $r \in \mathbb{Z}^+$ and $t \in \mathbb{F}_{p^n}$, $\varphi_p^r(t) = t^{p^r}$. Let φ_p^r be the identity map. Then $t^{p^r} = t$ for all $t \in \mathbb{F}_{p^n}$, i.e., $t^{p^r} - t = 0$ for any $t \in \mathbb{F}_{p^n}$. So $p^r \geqslant p^n$, i.e., $r \geqslant n$. Hence $|\varphi_p| \geqslant n$. Since $\#\,\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = n$ and $\varphi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, $|\varphi_p| = n$. □

Theorem 4.15. *When $p \nmid n$, the image of $\Psi : \mathrm{Gal}(\mathbb{F}_p(\xi_n)/\mathbb{F}_p) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is $\langle p \rangle$. In particular, $[\mathbb{F}_p(\xi_n) : \mathbb{F}_p]$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Since $p \nmid n$, $x^n - 1$ is separable in $\mathbb{F}_p[x]$. So $[\mathbb{F}_p(\xi_n) : \mathbb{F}_p] = d$ for some $d < n$. By previous theorem, $\mathrm{Gal}(\mathbb{F}(\xi_n)/\mathbb{F}_p)$ is generated by the p^{th} power map φ_p. So $\varphi_p(\xi_n) = \xi_n^p$. Also, by definition, $\Psi(\varphi_p) = a_{\varphi_p}$, where $\varphi_p(\xi_n) = \xi_n^{a_{\varphi_p}}$. Hence $\xi_n^{a_{\varphi_p}} = \xi_n^p$, i.e., $a_{\varphi_p} \equiv p \pmod n$. Thus, $\Psi(\varphi_p) = p \bmod n$. Also, since $\mathrm{Gal}(\mathbb{F}_p(\xi_n)/\mathbb{F}_p) = \langle \varphi_p \rangle$, we have $d = [\mathbb{F}_p(\xi_n) : \mathbb{F}_p] = \#\,\mathrm{Gal}(\mathbb{F}_p(\xi_n)/\mathbb{F}_p)$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Remark. The field extension $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is Galois of degree $\varphi(n)$. Then for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, it permutes the set of **primitive** n^{th} roots of unity in $\mathcal{K}^\times$, i.e., $\mathrm{Gal}(\mathbb{Q}(\xi_n/\mathbb{Q})) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Remark. If $2 \nmid n$ and $n = p_1^{a_1} \cdots p_k^{a_k}$, $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to a product of cyclic group, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times \cong \mathbb{Z}(p_1^{a_1} - p_1^{a_1-1})/\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k^{a_k} - p_k^{a_k-1})\mathbb{Z}$.

Theorem 4.16. *Let $m, n \in \mathbb{Z}^{\geqslant 1}$, then $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{\mathrm{lcm}(m,n)})$.*

Proof. Since $\xi_{\mathrm{lcm}(m,n)}^{\frac{n}{\gcd(m,n)}}$ is a primitive m^{th} root of unity, $\mathbb{Q}(\xi_m) \subseteq \mathbb{Q}(\xi_{\mathrm{lcm}(m,n)})$. Similarly, $\mathbb{Q}(\xi_n) \subseteq \mathbb{Q}(\xi_{\mathrm{lcm}(m,n)})$. So $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) \subseteq \mathbb{Q}(\xi_{\mathrm{lcm}(m,n)})$. Since $\xi_m\xi_n$ is a primitive $\mathrm{lcm}(m,n)^{\text{th}}$ root of unity, $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) \supseteq \mathbb{Q}(\xi_{\mathrm{lcm}(m,n)})$. □

Theorem 4.17. *Let $m, n \in \mathbb{Z}^{\geqslant 1}$, then $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{\gcd(m,n)})$. In particular, if* $\gcd(m,n) = 1$*, then $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}$.*

Proof. Recall from elementary number theory, $\varphi(n) = n\prod_{p|n}(1 - 1/p)$ for any $n \in \mathbb{Z}^+$. Then if $m, n \in \mathbb{Z}^+$ with $(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. If $d \mid n$, since $\xi_d = \xi_n^{\frac{n}{d}}$, $\mathbb{Q}(\xi_d) \subseteq \mathbb{Q}(\xi_n)$. So $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) \supseteq \mathbb{Q}(\xi_{\gcd(m,n)})$. Recall if $\mathcal{L}_1/\mathcal{K}$ and $\mathcal{L}_2/\mathcal{K}$ are Galois, then $[\mathcal{L}_1\mathcal{L}_2 : \mathcal{K}] = \frac{[\mathcal{L}_1:\mathcal{K}][\mathcal{L}_2:\mathcal{K}]}{[\mathcal{L}_1\cap\mathcal{L}_2:\mathcal{K}]}$. By previous theorem, $[\mathbb{Q}(\xi_{\mathrm{lcm}(m,n)}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\xi_m):\mathbb{Q}][\mathbb{Q}(\xi_n):\mathbb{Q}]}{[\mathbb{Q}(\xi_m)\cap\mathbb{Q}(\xi_n):\mathbb{Q}]}$. Then

$$\begin{aligned}
[\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}] &= \frac{\varphi(m)\varphi(n)}{\varphi(\mathrm{lcm}(m,n))} = \frac{m\prod_{p|m}(1-1/p)\cdot n\prod_{p|n}(1-1/p)}{\mathrm{lcm}(m,n)\prod_{p|\mathrm{lcm}(m,n)}(1-1/p)} \\
&= \frac{mn}{\mathrm{lcm}(m,n)}\frac{\prod_{p|m}(1-1/p)\cdot\prod_{p|n}(1-1/p)}{\prod_{p|\mathrm{lcm}(m,n)}(1-1/p)} \\
&= \gcd(m,n)\prod_{p|\gcd(m,n)}(1-1/p) = \varphi(\gcd(m,n)).
\end{aligned}$$

Hence $[\mathbb{Q}(\xi_m)\cap\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(\xi_{\gcd(m,n)}) = [\mathbb{Q}(\xi_{\gcd(m,n)}) : \mathbb{Q}]$ and so $\mathbb{Q}(\xi_m)\cap\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{\gcd(m,n)})$. □

Corollary 4.18. For $m, n \in \mathbb{Z}^+$, $\varphi(m)\varphi(n) = \gcd(m,n)\operatorname{lcm}(m,n)$.

Corollary 4.19. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the decomposition of n into distinct prime powers. Then $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\xi_{p_1^{a_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\xi_{p_k^{a_k}})/\mathbb{Q})$, i.e., $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \cdots (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times$, which is the CRT. Note $(\mathbb{Z}/2^k\mathbb{Z})$ is not cyclic unless $k = 0, 1, 2$, but for $k > 2$, $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.

Proof. By previous theorem, we have $\mathbb{Q}(\xi_{p_1^{a_1}}) \cdots \mathbb{Q}(\xi_{p_k^{a_k}}) = \mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_{p_1^{a_1}}) \cap \cdots \cap \mathbb{Q}(\xi_{p_k^{a_k}}) = \mathbb{Q}$. Note that since $[\mathbb{Q}(\xi_{p_i^{a_i}}) : \mathbb{Q}] = \varphi(p_i^{a_i})$ for $i = 1, \ldots, k$ and $\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_k^{a_k})$, $[\mathbb{Q}_{\xi_n} : \mathbb{Q}] = [\mathbb{Q}(\xi_{p_1^{a_1}}) : \mathbb{Q}] \cdots [\mathbb{Q}(\xi_{p_k^{a_k}}) : \mathbb{Q}]$. □

4.3 Möbius Function

Definition 4.20. For $n \in \mathbb{N}$, define the *Möbius function* $\mu_n : \mathbb{N} \to \mathbb{N}$ by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has a squared prime factor} \\ -1 & \text{if } n \text{ has odd number of prime factors} \\ 1 & \text{if } n \text{ has even number of prime factors} \end{cases}.$$

Remark (Facts)**.** (a) The Möbius function is multiplicative, i.e., $\mu(mn) = \mu(m)\mu(n)$ whenever $(m, n) = 1$.

(b)

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}.$$

This equality leads to the important Möbius inversion formula: if g and f are arithmetic functions satisfying $g(n) = \sum_{d|n} f(d)$ for each $n \in \mathbb{N}$, then $f(n) = \sum_{d|n} \mu(d)g(n/d)$ for each $n \in \mathbb{N}$. Well, we also have a multiplicative version of the above: $f(n) = \prod_{d|n} g(n/d)^{\mu(d)}$. The two sequences are said to be Möbius transforms of each other.

4.4 Cyclotomic Polynomial

Definition 4.21. The n^{th} *cyclotomic polynomial* Φ_n is defined to be $\Phi_n(x) = (x - \varpi_1) \cdots (x - \varpi_r)$, where $\varpi_1, \ldots, \varpi_r$ are all the primitive n^{th} root of unity. By previous theorem, we can write $\Phi_n(x) = \prod_{1 \leqslant k \leqslant n, \gcd(k,n)=1} (x - \xi_n^k)$. Then $\Phi(n)$ is monic of degree $\varphi(n)$ and $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$ and $\Phi_4(x) = x^2 + 1$.

Theorem 4.22. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof. Let ξ be an n^{th} root of unity with $|\xi| = d$, then $d \mid n$ and so ξ is a primitive d^{th} root of unity. Hence ξ is root of the RHS. Let $d \mid n$ and ξ_d be the primitive d^{th} root of unity, then ξ_d is a n^{th} root of unity. Since the polynomials on LHS and RHS are monic, they are equal. □

Corollary 4.23. $\Phi_n(x) = \frac{x^n - 1}{\prod_{k|n, k \neq n} \Phi_k(x)} = \sum_{d|n} \mu(n/d)(x^d - 1) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$.

Corollary 4.24. $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$.

Theorem 4.25. $\Phi_n(x) \in \mathbb{Q}[x]$.

Proof. Let ξ_n be a primitive n^{th} root of unity. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_n))$. Since $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, σ send distinct primitive n^{th} roots of unity to distinct primitive n^{th} roots of unity. So σ just shuffles the linear factor of $\Phi_n(x)$, i.e., $\sigma(\Phi_n(x)) = \Phi_n(x)$. Hence by Galois theory, the coefficient of Φ_n must lie in $\mathbb{Q}$, i.e., $\Phi_n(x) \in \mathbb{Q}[x]$. □

Theorem 4.26 (Gauss)**.** $\Phi_n \in \mathbb{Q}[x]$ *is irreducible.*

Proof. (Sketch). Assume $\Phi_n(x) = fg$, where $f, g \in \mathbb{Q}[x]$ is irreducible. Since $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_n))$ permutes among roots of irreducible polynomials, $\phi_n(x)$ is irreducible. □

Corollary 4.27. Φ_n is the minimal polynomial of the **primitive** n^{th} roots of unity.

Corollary 4.28. Φ_n is the minimal polynomial of the non-identity n^{th} roots of unity.

Theorem 4.29. *If* $m \mid n$*, then* $\Phi_n(x) = \Phi_m(x^{n/m})$.

Proof. Note

$$\begin{aligned}\Phi_n(x) &= \prod_{d|n}(x^d-1)^{\mu(n/d)} = \prod_{d|n}(x^{n/d}-1)^{\mu(d)} = \prod_{d|m}((x^{n/m})^{m/d}-1)^{\mu(d)} \\ &= \prod_{d|m}((x^{n/m})^d-1)^{\mu(m/d)} = \Phi_m(x^{n/m}).\end{aligned}$$ □

Lemma 4.30. We have

(a) $\Phi_n(x) = x^{\varphi(n)}\Phi_n(1/x),\ n \geqslant 2$.

(b) $\Phi_{2n}(x) = \Phi_n(-x),\ n \equiv 1 \pmod 2$ and $n \geqslant 3$.

(c) $\Phi_{p^r}(x) = \Phi_p(x^{p^{r-1}})$ and $\Phi_{p_1^{a_1}\cdots p_r^{a_r}} = \Phi_{p_1\cdots p_r}(x^{p_1^{a_1-1}\cdots p_r^{a_r-1}})$.

(d) If $\gcd(p,m) = 1$, $\Phi_{p^r m}(x) = \frac{\Phi_m(x^{p^r})}{\Phi_m(x^{p^{r-1}})}$.

Proof. These identities can be checked by showing the RHS has the correct degree and one correct root to be the cyclotomic polynomial on LHS. Then use that two monic irreducible polynomials with a common root are equal.

(a) Since

$$\Phi_n(x) = \prod_{1\leqslant k\leqslant n,\gcd(k,n)=1}(x-\xi_n^k) = x^{\varphi(n)}\prod_{1\leqslant k\leqslant n,\gcd(k,n)=1}(1-\xi_n^k/x),$$

and $x^{\varphi(n)}\Phi_n(1/x) = x^{\varphi(n)}\prod_{1\leqslant k\leqslant n,\gcd(k,n)=1}(1/x-\xi_n^k)$ are irreducible and have the same degree and one same root, we have the equality.

(b) Note

$$\Phi_{p^r}(x) = \frac{x^{p^r}-1}{\prod_{d|p^r,d\neq p^r}\Phi_d(x)} = \frac{x^{p^r}-1}{\prod_{d|p^{r-1}}\Phi_d(x)} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = \frac{(x^{p^{r-1}})^p-1}{x^{p^{r-1}}-1} = \Phi_p(x^{p^{r-1}}).$$

Or follow from previous theorem.

(c) If $d \mid m$, since m is odd, d is also odd. Note $\Phi_2(-x) = -x+1 = -\Phi_1(x)$ and by induction,

$$\begin{aligned}\Phi_{2m}(x) &= \frac{x^{2m}-1}{\prod_{d\mid 2m, d \text{ odd}} \Phi_d(x) \cdot \prod_{d\mid 2m, d\neq 2m, d \text{ even}} \Phi_d(x)} = \frac{x^{2m}-1}{\prod_{d\mid m} \Phi_d(x) \cdot \prod_{d\mid m, d<m} \Phi_{2d}(x)} \\ &= \frac{x^{2m}-1}{-(x^m-1)\prod_{d\mid m, d<m} \Phi_d(-x)} = -\frac{x^m+1}{\prod_{d\mid m, d<m} \Phi_d(-x)} = \frac{(x^m+1)\Phi_m(-x)}{-(-x)^m+1} = \Phi_m(-x).\end{aligned}$$

(d) Since $\gcd(p,m)=1$, $\mu(pm/d) = -\mu(m/d)$ and then

$$\begin{aligned}\Phi_{pm}(x) &= \prod_{d\mid pm} (x^d-1)^{\mu(pm/d)} = \prod_{d\mid pm, p\mid d} (x^d-1)^{\mu(pm/d)} \prod_{d\mid pm, p\nmid d} (x^d-1)^{\mu(pm/d)} \\ &= \prod_{d\mid m} (x^{pd}-1)^{\mu(m/d)} \prod_{d\mid m} (x^d-1)^{\mu(pm/d)} = \Phi_m(x^p) \prod_{d\mid m} (x^d-1)^{-\mu(m/d)} = \frac{\Phi_m(x^p)}{\Phi_m(x)}. \quad \square\end{aligned}$$

Example 4.31. $\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1$.

Theorem 4.32. *For any $n \in \mathbb{Z}^+$, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. Since $\Phi_n(x) \mid x^n - 1$ and $\Phi_n(x)$ and x^n-1 are both monic, we have $\Phi_n(x) \in \mathbb{Z}[x]$. $\square$

Remark. How does p factor in $\mathcal{O}_{\mathbb{Q}(\xi_{p^r})}$? Since $\gcd(p,1)=1$ and $x^{p^r} - 1 \equiv (x-1)^{p^r} \pmod p$ and $x^{p^{r-1}} - 1 \equiv (x-1)^{p^{r-1}} \pmod p$, we have

$$\Phi_{p^r}(x) = \frac{(x-1)^{p^r}}{(x-1)^{p^{r-1}}} = (x-1)^{p^r - p^{r-1}} = (x-1)^{\varphi(p^r)} = (x-1)^{[\mathbb{Q}[\xi_{p^r}]:\mathbb{Q}]} \text{ in } \mathbb{F}_p[x].$$

Hence once we see that $\mathcal{O}_{\mathbb{Q}(\xi_{p^r})} = \mathbb{Z}[\xi_{p^r}]$, since $\mathcal{O}_{\mathbb{Q}(\xi_{p^r})}/p\mathcal{O}_{\mathbb{Q}(\xi_{p^r})} \cong \frac{\mathbb{Z}[x]}{\langle p, \Phi_{\xi_{p^r}}\rangle} \cong \frac{\mathbb{F}_p[x]}{\langle \Phi_{\xi_{p^r}}\rangle}$, we have $p\mathbb{Z}[\xi_{p^r}] = \langle p, 1-\xi_{p^r}\rangle^{\varphi(p^r)}$. Since $1-\xi_{p^r} \mid p$ and $p\mathbb{Z}[\xi_{p^r}] = \langle 1-\xi_{p^r}\rangle^{\varphi(p^r)}$, we have $r(\langle 1-\xi_{p^r}\rangle/p) = 1$, $e(\langle 1-\xi_{p^r}\rangle/p) = \varphi(p^r)$ and $f(\langle 1-\xi_{p^r}\rangle/p) = 1$.

4.5 Ramification

Lemma 4.33. Let $n = p^r$ and $d = \varphi(p^r)$ and ξ_n be the n^{th} root of unity. Then $p\mathcal{O}_{\mathbb{Q}(\xi_n)} = \langle 1-\xi_n\rangle^d$. Furthermore, the basis $\{1, \xi_n, \ldots, \xi_n^{d-1}\}$ of $\mathbb{Q}(\xi_n)/\mathbb{Q}$ has the discriminant $d(1,\xi_n,\ldots,\xi_n^{d-1}) = \pm p^s$, where $s = p^{r-1}(rp-r-1)$.

Proof. Since $\Phi_{p^r}(x) = \frac{\Phi_1(x^{p^r})}{\Phi_1(x^{p^{r-1}})} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = \sum_{j=0}^{p-1} x^{p^{r-1}j}$, we have $\Phi_n(1) = p$. Then $p = \Phi_n(1) = \prod_{1\leqslant k\leqslant n, \gcd(k,n)=1}(1-\xi_n^k)$. Let $\epsilon_k = \frac{1-\xi_n^k}{1-\xi_n} = \sum_{i=0}^{k-1} \xi_n^i \in \mathcal{O}_{\mathbb{Q}(\xi_n)}$ with $\gcd(k,n)=1$. Then there exists $k' \in \mathbb{Z}$ such that $kk' \equiv 1 \pmod n$, so $\frac{1-\xi_n}{1-\xi_n^k} = \frac{1-(\xi_n^k)^{k'}}{1-\xi_n^k} = 1 + \xi_n^k + \cdots + (\xi_n^k)^{k'-1} \in \mathcal{O}_{\mathbb{Q}(\xi_n)}$ and hence $\epsilon_k \in \mathcal{O}_{\mathbb{Q}(\xi_n)}^\times$. So $\epsilon := \prod_{1\leqslant k\leqslant n, \gcd(k,n)=1} \epsilon_k \in \mathcal{O}_{\mathbb{Q}(\xi_n)}^\times$. Also, since $1-\xi_n^k = \epsilon_k(1-\xi_n)$, $p = \prod_{1\leqslant k\leqslant n, \gcd(k,n)=1}(1-\xi_n^k) = \epsilon(1-\xi_n)^{\varphi(n)}$. Then $p\mathcal{O}_{\mathbb{Q}(\xi_n)} = \langle 1-\xi_n\rangle^{\varphi(p^r)} = \langle 1-\xi_n\rangle^d$. Let $\eta_1, \ldots, \eta_d$ be the primitive n^{th} roots of unity, i.e., the Galois conjugate of ξ_n. Then $\Phi_n(x) = \prod_{j=1}^d (x-\eta_j)$

and so $\Phi_n'(x) = \sum_{i=1}^d \prod_{k\neq i,k=1}^d (x-\eta_k)$. Hence $\Phi_n'(\eta_j) = \prod_{k\neq j,k=1}^d (\eta_j - \eta_k)$. Since $\Phi_n' \in \mathbb{Q}[x]$ and $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\pm d(1,\xi_n,\ldots,\xi_n^{d-1}) = \prod_{i\neq j}(\xi_i-\xi_j) = \prod_{j=1}^d \Phi_n'(\xi_j) = \prod_\sigma \sigma(\Phi_n'(\xi_n)) = \mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\Phi_n'(\xi_n)).$$

Let $\gamma = p^{r-1}$. Since $1 \neq \xi_n^\gamma$ is primitive p^{th} root of unity, $m_{\xi_n^\gamma}(x) = \Phi_p(x) = x^{p-1}+\cdots+1$. So $m_{\xi_n^\gamma - 1}(x) = m_{\xi_n^\gamma}(x+1) = (x+1)^{p-1}+\cdots+1 = xf(x)+p$, where $f \in \mathbb{Q}[x]$. Consider the tower of field extension $\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_n^\gamma)/\mathbb{Q}$, so $c_{\xi_n^\gamma-1} = m_{\xi_n^\gamma-1}^{[\mathbb{Q}(\xi_n):\mathbb{Q}(\xi_n^\gamma)]}$. Also, since $[\mathbb{Q}(\xi_n):\mathbb{Q}(\xi_n^\gamma)] = \frac{[\mathbb{Q}(\xi_n):\mathbb{Q}]}{[\mathbb{Q}(\xi_n^\gamma):\mathbb{Q}]} = \frac{\varphi(p^r)}{\varphi(p)} = \frac{p^r-p^{r-1}}{p-1} = p^{r-1} = \gamma$, we have $c_{\xi_n^\gamma-1}(x) = (xf(x)+p)^{p^{r-1}} = xg(x)+p^\gamma$ and then $\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^\gamma - 1) = \pm p^{p^{r-1}}$. Since ξ_n is the primitive n^{th} root of unity, $c_{\xi_n} = m_{\xi_n} = \Phi_n(x) = \sum_{j=0}^{p-1} x^{p^{r-1}j}$. So $\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n) = 1$ and then $\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n^{-1}) = 1/\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\xi_n) = \pm 1$. Since $c_{1-\xi_n}(x) = m_{1-\xi_n}(x) = m_{\xi_n}(1-x) = \Phi_n(1-x) = \sum_{j=0}^{p-1}(1-x)^{p^{r-1}j}$, $\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(1-\xi_n) = \pm p$. Also, since $p = \epsilon(1-\xi_n)^{\varphi(n)}$,

$$\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(p^r) = \mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}^r(p) = (\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\epsilon)\,\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(1-\xi_n))^{r\varphi(n)} = \pm p^{r\varphi(n)}.$$

Since $(x^{p^{r-1}}-1)\Phi_n(x) = x^{p^r}-1$, differentiating it, $p^{r-1}x^{p^{r-1}-1}\Phi_n(x)+(x^{p^{r-1}}-1)\Phi_n'(x) = p^r x^{p^r-1}$. So $p^{r-1}\xi_n^{p^{r-1}-1}\Phi_n(\xi_n) + (\xi_n^{p^{r-1}}-1)\Phi_n'(\xi_n) = p^r\xi_n^{p^r-1}$, i.e., $(\xi_n^{p^{r-1}}-1)\Phi_n'(\xi_n) = p^r\xi_n^{-1}$. Taking $\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}$ on both sides, we have $\pm p^{p^{r-1}}\,\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\Phi_n'(\xi_n)) = p^{r\varphi(p^r)}\cdot(\pm 1)$. Thus, $d(1,\xi_n,\ldots,\xi_n^{d-1}) = \pm\,\mathrm{N}_{\mathbb{Q}(\xi_n)/\mathbb{Q}}(\Phi_n'(\xi_n)) = \pm p^{r\varphi(p^r)-p^{r-1}} = \pm p^{p^{r-1}(rp-r-1)} = \pm p^s$. □

Theorem 4.34. $\mathcal{O}_{\mathbb{Q}(\xi_n)} = \mathbb{Z}[\xi_n]$.

Proof. We first prove this for $n = p^r$. Let $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\xi_n)}$. Then $p^s\mathcal{O} \subseteq \mathbb{Z}[\xi_n] \subseteq \mathcal{O}$. Let $\mathfrak{P} := \langle 1-\xi_n\rangle$. We saw before $e(\mathfrak{P}/p) = \varphi(n)$ and $f(\mathfrak{P}/p) = 1$. Since $[\mathbb{Q}[\xi_n]:\mathbb{Q}]) = \varphi(n)$, this is true in $\mathcal{O}$ as well and then $1-\xi_n$ is prime in $\mathcal{O}$. Let $\lambda := 1-\xi_n$. Then $\mathcal{O}/\lambda\mathcal{O} = \mathcal{O}/\mathfrak{P} \cong \mathbb{Z}/p\mathbb{Z}$. Let $\alpha \in \mathcal{O}$, then there exists $z \in \mathbb{Z}$ such that $\alpha + \lambda\mathcal{O} = z + \lambda\mathcal{O}$, i.e., $\alpha = z + \lambda\mathcal{O}$. So $\mathcal{O} = \mathbb{Z} + \lambda\mathcal{O} = \mathbb{Z}[\xi_n] + \lambda\mathcal{O}$ and then $\lambda\mathcal{O} = \lambda\mathbb{Z}[\xi_n] + \lambda^2\mathcal{O}$. Hence $\mathcal{O} = \mathbb{Z}[\xi_n] + \lambda^2\mathcal{O}$ and by inductive argument, $\mathcal{O} = \mathbb{Z}[\xi_n] + \lambda^t\mathcal{O}$ for any $t \in \mathbb{Z}^+$. Pick $t = s\varphi(p^r)$, since $p\mathcal{O} = \lambda^{\varphi(p^r)}\mathcal{O}$, we have $\mathcal{O} = \mathbb{Z}[\xi_n] + \lambda^{s\varphi(p^r)}\mathcal{O} = \mathbb{Z}[\xi_n] + p^s\mathcal{O} = \mathbb{Z}[\xi_n]$. Hence, if $n = p^r$, we have the result. Note $\{1,\xi_n,\ldots,\xi_n^{\varphi(p^r)-1}\}$ forms an integral basis of $\mathbb{Q}(\xi_n)/\mathbb{Q}$ when $n = p^r$. More generally, write $n = p_1^{m_1}\cdots p_r^{m_r}$. Then for $i = 1,\ldots,r$, set $\eta_i = \eta_n^{n/p_i^{m_i}}$. Note that for $i = 1,\ldots,r$, η_i is a primitive $p_i^{m_i}$-th root of unity. Since $\mathrm{lcm}(p_1^{m_1},\ldots,p_r^{m_r}) = n$, $\mathbb{Q}(\xi_n) = \mathbb{Q}(\eta_1)\cdots\mathbb{Q}(\eta_r)$. Since $\gcd(p_i^{m_i}, p_j^{m_j}) = 1$ for any $1 \leqslant i \neq j \leqslant r$, $\mathbb{Q}(\eta_1)\cap\cdots\cap\mathbb{Q}(\eta_r) = \mathbb{Q}$. For $i = 1,\ldots,r$, $\{1,\eta_i,\ldots,\eta_i^{\varphi(p_i^{m_i})-1}\}$ forms an integral basis of $\mathbb{Q}(\eta_i)/\mathbb{Q}$. Since for $i = 1,\ldots,r$, $d(1,\eta_i,\ldots,\eta_i^{d_i-1}) = p_i^{s_i}$ with $s_i = p_i^{m_i}(m_ip_i - m_i - 1)$, they are pairwisely prime. Then $\{\eta_1^{j_1}\cdots\eta_r^{j_r}\}_{j_i=0,\ldots,\varphi(p_i^{m_i})-1,\forall i=1,\ldots,r}$ forms an integral basis of $\mathbb{Q}(\xi_n)/\mathbb{Q}$. By the definition of η_i's, each one of these elements in the basis is a power of ξ_n, so every $\alpha \in \mathcal{O}$ may be written as $\alpha = f(\xi_n)$ with $f \in \mathbb{Z}[x]$. Since $\deg_{\mathbb{Q}}(\xi_n) = \varphi(n)-1$, the degree of any $f(\xi_n)$ with $f \in \mathbb{Z}[x]$ may be reduced to $\varphi(n)-1$. In this way for $\alpha \in \mathcal{O}$, one obtains a representation $\alpha = a_0 + a_1\xi_n + \cdots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1}$. Thus, $\{1,\xi_n,\ldots,\xi_n^{\varphi(n)-1}\}$ is indeed an integral basis of $\mathbb{Q}(\xi_n)/\mathbb{Q}$. □

Lemma 4.35. Let p be prime with $p \nmid n$. The monic irreducible factors of $\Phi_n(x)$ modulo p are distinct and all of them have degree equal to the order of p modulo n.

Proof. Since $p \nmid n$, $x^n - 1$ has distinct roots modulo p. Let α be a root of $\Phi_n(x)$ modulo p. Since $\Phi_n(x) \mid x^n - 1$ in $\mathbb{F}_p[x]$, α is an n^{th} root of unity in $\mathbb{F}_p$. Suppose $\alpha^m = 1$ in $\mathbb{F}_p$ for some $1 \leqslant m < n$. Then α is a root of $x^m - 1 = \prod_{k|m, k\neq m} \Phi_k(x)$ in $\mathbb{F}_p$. So there exists a proper divisor d of n such that $\Phi_d(\alpha) = 0$ in $\mathbb{F}_p$. But then α is a root of $\Phi_n(x)$ and $\Phi_d(x)$ in $\mathbb{F}_p$. So $x^n - 1 = \prod_{d|n} \Phi_n(x) = \Phi_n(x)\Phi_d(x)\prod_{k|n,k\neq d,n} \Phi_d(x)$ in $\mathbb{F}_p$, i.e., α is a multiple root of $x^n - 1$ in $\mathbb{F}_p$, a contradiction since $x^n - 1$ is separable over $\mathbb{F}_p$. Hence α is a primitive n^{th} root of unity in $\mathbb{F}_p$. Let g be an irreducible factor of $\Phi_n(x)$ in $\mathbb{F}_p[x]$ such that $g(\alpha) = 0$. Since $\mathbb{F}_p[x]/\langle g\rangle \cong \mathbb{F}_p(\alpha)$, $\deg(g) = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ is the order of p modulo n, i.e., the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Theorem 4.36. *Let $n = \prod q^{\nu_q}$ be the prime factorization. For each prime p, let f_p be the smallest positive integer such that $p^{f_p} \equiv 1 \pmod{n/p^{\nu_p}}$. Then one has the prime factorization $p\mathbb{Z}[\xi_n] = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct and all have degree f_p.*

Proof. Since $\mathcal{O}_{\mathbb{Q}(\xi_n)} = \mathbb{Z}[\xi_n]$, every $p\mathbb{Z}[\xi_n]$ decomposes into prime ideals in exactly the same way as the minimal polynomial $\Phi_n(x)$ of ξ_n factors into irreducible polynomial modulo p. Write $n = q^{\nu_q}m$ with $q \nmid m$. Let δ_i run over the primitive roots of unity of order m and η_j run over the primitive roots of unity of order q^{ν_q}. Let $1 \leqslant s < n = \operatorname{lcm}(q^{\nu_q}, m)$, wlog., assume s is not a multiple of q^{ν_q}. Then sm is not a multiple of q^{ν_q}. So $(\delta_i\eta_j)^{sm} = \delta_i^{sm}\eta_j^{sm} = \eta_j^{sm} \neq 1$. Hence $(\delta_i\eta_j)^s \neq 1$. So $\delta_i\eta_j$ runs over the primitive n^{th} roots of unity, i.e., over $\mathbb{Z}[\xi_n]$: $\Phi_n(x) = \prod_{i,j}(x - \delta_i\eta_j)$. Let $\mathfrak{p} \mid \langle p\rangle$. Since $x^{q^{\nu_q}} - 1 \equiv (x-1)^{q^{\nu_q}} \pmod{\mathfrak{p}}$, we have $0 \equiv \eta_j^{q^{\nu_q}} - 1 \equiv (\eta_j - 1)^{q^{\nu_q}} \pmod{\mathfrak{p}}$ for $j = 1, \ldots, \varphi(q^{\nu_q})$. So for $j = 1, \ldots, \varphi(q^{\nu_q})$, $\eta_j \equiv 1 \pmod{\mathfrak{p}}$. Hence

$$\begin{aligned}\Phi_n(x) &= \prod_{i,j}(x - \delta_i\eta_j) \equiv \prod_{i,j}(x - \delta_i) \pmod{\mathfrak{p}} \equiv \prod_i (x - \delta_i)^{\varphi(q^{\nu_q})} \pmod{\mathfrak{p}} \\ &\equiv \left(\prod_i x - \delta_i\right)^{\varphi(q^{\nu_q})} \pmod{\mathfrak{p}} \equiv \Phi_m(x)^{\varphi(q^{\nu_q})} \pmod{\mathfrak{p}} \equiv \Phi_m(x)^{\varphi(q^{\nu_q})} \pmod{p}.\end{aligned}$$

Since f_p is the smallest positive integer such that $p^{f_p} \equiv 1 \pmod{m}$, p has order f_p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Observe this congruence reduces us to the case where $p \nmid m$, apply previous theorem to decompose $\Phi_m(x)$, then we have the irreducible decomposition for $\Phi_n(x)$ modulo p. □

Example 4.37. Let $n \in \mathbb{N}$ and $2 \nmid n$, then $f(2)$ is the order of 2 mod n. Since $\mathcal{O}[x]/\langle 2\rangle \cong \mathbb{Z}[\xi_n][x]/\langle 2\rangle \cong \mathbb{Z}[x]/\langle \phi_n(x), 2\rangle \cong \mathbb{F}_2[x]/\langle \phi_n(x)\rangle = g_1 \pmod 2 \cdots g_r \pmod 2$, we have $2\mathcal{O} = \langle 2, g_1(\xi_n)\rangle \cdots \langle 2, g_r(\xi_n)\rangle$. Then $G_2 = \{\langle 2, g_1(\xi_n) \pmod 2\rangle, \cdots, \langle 2, g_r(\xi_n) \pmod 2\rangle\}$. Let $\sigma_2 \in \operatorname{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ such that $\sigma_2(\xi_n) = \xi_n^2$. Since $2 \nmid n$, $\gcd(2, n) = 1$ and then there exists $x \in \mathbb{Z}$ such that $2x \equiv 1 \pmod n$. So $2xk \equiv k \pmod n$ for any $k \in \mathbb{Z}^+$. Then $(\xi_n^{2k})^x = \xi_n^k$ and so $\mathbb{Q}(\xi_n^k) = \mathbb{Q}(\xi_n^{2k})$ for any $k \in \mathbb{Z}^+$. So for any $g(x) \in \mathbb{Q}[x]$, $\mathbb{Q}(g(\xi_n)) = \mathbb{Q}(g(\xi_n^2))$, i..e., $\langle g(\xi_n)\rangle = \langle g(\xi_n^2)\rangle$, i.e., $\langle g(\xi_n) \pmod 2\rangle = \langle g(\xi_n^2) \pmod 2\rangle$. Thus, $\sigma_2\langle 2, g_i(\xi_n) \pmod 2\rangle = \langle 2, \sigma_2(g_i(\xi_n))\rangle = \langle 2, \sigma_2(g_i(\xi_n))\rangle = \langle 2, \overline{g_i(\xi_n^2)}\rangle = \langle 2, \overline{g_i(\xi_n)}^2\rangle = \langle 2, \overline{g_i(\xi_n)}\rangle$ for $i = 1, \ldots, r$.

4.6 Quadratic Fields

Remark (Recall)**.**

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & x^2 \equiv a \pmod p \text{ has a solution,} \\ -1 & x^2 \equiv a \pmod p \text{ has no solution,} \\ 0 & p \mid a. \end{cases}$$

If p is odd prime, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. If $p \nmid b$, $\frac{b^2}{p} = 1$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and if $a \equiv r \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$. If l and p are odd prime and $l \neq p$, then $\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\frac{p-1}{2}}$.

Theorem 4.38. *Let l and p be odd prime. Set $l^* = (-1)^{\frac{l-1}{2}} l$ and let ξ_l be a primitive l^{th} root of unity. Then p splits completely in $\mathbb{Q}(\sqrt{l^*})$ if and only if p splits into an even number of prime ideals in $\mathbb{Q}(\xi_l)$.*

Proof. Define the Gauss sum $\tau := \sum_{a\in(\mathbb{Z}/l\mathbb{Z})^\times} \left(\frac{a}{l}\right)\xi_l^a$. Let a, b, c vary over $(\mathbb{Z}/l\mathbb{Z})^\times$. Since l is prime, $0 = \sum_c \left(\frac{c}{l}\right) = \left(\frac{1}{l}\right) + \sum_{c\neq 1}\left(\frac{c}{l}\right) = 1 + \sum_{c\neq 1}\left(\frac{c}{l}\right)$, i.e., $\sum_{c\neq 1}\left(\frac{c}{l}\right) = -1$. When $c \not\equiv -1 \pmod l$, since $\gcd(c+1, l) = 1$, we have ξ_l^{c+1} is primitive l^{th} root of unity. Thus,

$$\begin{aligned}
\tau^2 &= \sum_a \left(\frac{a}{l}\right)\xi_l^a \sum_b \left(\frac{b}{l}\right)\xi_l^b = \sum_{a,b}\left(\frac{ab}{l}\right)\xi_l^{a+b} = \sum_{a,b}\left(\frac{ab^{-1}}{l}\right)\xi_l^{a+b} = \sum_{b,c}\left(\frac{c}{l}\right)\xi_l^{b(c+1)} \\
&= \sum_{c\neq -1}\left(\frac{c}{l}\right)\sum_b (\xi_l^{c+1})^b + \sum_b \left(\frac{-1}{l}\right) = \sum_{c\neq -1}\left(\frac{c}{l}\right)(-1) + (l-1)\left(\frac{-1}{l}\right) \\
&= 0 - \left(\frac{-1}{l}\right)(-1) + (l-1)\left(\frac{-1}{l}\right) = l\left(\frac{-1}{l}\right) = (-1)^{\frac{l-1}{2}} l = l^*.
\end{aligned}$$

So $\sqrt{l^*} = \pm\tau \in \mathbb{Z}[\xi_l] \subseteq \mathbb{Q}(\xi_l)$. Thus, $\mathbb{Q}(\sqrt{l^*}) \subseteq \mathbb{Q}(\xi_l)$.

$\Longrightarrow$ Assume p splits completely in $\mathbb{Q}(\sqrt{l^*})$, say $p\mathcal{O}_{\mathbb{Q}(\sqrt{l^*})} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_l)/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$ and transforms the set of all prime ideals lying above $\mathfrak{p}_1$ bijectively into the set of prime ideals above $\mathfrak{p}_2$. So the number of prime ideals of $\mathbb{Q}(\xi_l)$ above p is even.

$\Longleftarrow$ Assume $p\mathbb{Z}[\xi_l]$ has an even number of prime factors. Then $[Z_\mathfrak{p} : \mathbb{Q}] = r$ is even. Since $\mathrm{Gal}(\mathbb{Q}(\xi_l)/\mathbb{Q})$ is cyclic of order $l-1$ and it has a unique subgroup of order $\frac{l-1}{2}$, i.e., $\mathrm{Gal}(\mathbb{Q}(\xi_l)/\mathbb{Q})$ has a unique subgroup of index 2, which corresponds to $\mathbb{Q}(\xi_l)^{\langle c\rangle}$, where c is the complex conjugate. Also, since $\mathbb{Q}(\sqrt{l^*}) \subseteq \mathbb{Q}(\xi_l)$ and $\mathbb{Q}(\sqrt{l^*}) : \mathbb{Q}] = 2$, we have $\mathbb{Q}(\xi_l)^{\langle c\rangle} = \mathbb{Q}(\sqrt{l^*}) \subsetneq Z_\mathfrak{p} \subseteq \mathbb{Q}(\xi_l)$. We have before that for $\mathfrak{p} \mid p$, $e(\mathfrak{p} \cap Z_\mathfrak{p}/p) = 1$. So $e(\mathfrak{p} \cap \mathbb{Q}(\sqrt{l^*})/p) = 1$. □

Corollary 4.39. Let $n = p_1^{a_1}\cdots p_k^{a_k}$ be a distinct prime decomposition. Then $\mathbb{Q}(\xi_n)$ contains the quadractic subfield $\mathbb{Q}(\sqrt{p_1^*\cdots p_k^*})$.

Proof. Since $\mathbb{Q}(\sqrt{p_i^*}) \subseteq \mathbb{Q}(\xi_{p_i}) \subseteq \mathbb{Q}(\xi_n)$ for $i = 1, \ldots, k$, $\mathbb{Q}(\sqrt{p_1^*\cdots p_k^*}) = \mathbb{Q}(\sqrt{p_1^*}\cdots\sqrt{p_k^*}) \subseteq \mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_k^*}) \subseteq \mathbb{Q}(\xi_n)$. □

Lemma 4.40. Let a be square-free and p be odd. Then $\left(\frac{a}{p}\right) = 1$ if and only if p splits completely in $\mathbb{Q}(\sqrt{a})$.

Proof. Recall $\mathcal{O}_{\mathbb{Q}(\sqrt{a})} = \begin{cases} \mathbb{Z}[\sqrt{a}] & \text{if } a \equiv 2,3 \pmod a \\ \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] & \text{if } a \equiv 1 \pmod a \end{cases}$, and note

$$\left(\frac{a}{p}\right) = 1 \iff p \nmid a \text{ and } x^2 - a \equiv (x+\sqrt{a})(x-\sqrt{a}) \pmod p \iff p \nmid a \text{ and } \sqrt{a} \in \mathbb{F}_p$$
$$\iff p \nmid a \text{ and } -\sqrt{a} \neq \sqrt{a} \in \mathbb{F}_p \iff p \nmid a \text{ and } \frac{1-\sqrt{a}}{2} \neq \frac{1+\sqrt{a}}{2} \in \mathbb{F}_p$$
$$\iff p \nmid a \text{ and } x^2 - x + \frac{1-a}{4} \equiv \left(x - \frac{1-\sqrt{a}}{2}\right)\left(x - \frac{1+\sqrt{a}}{2}\right) \pmod p.$$

Since $[\mathcal{O}_{\mathbb{Q}(\sqrt{a})} : \mathbb{Z}[a]]$ is 1 or 2, $p \nmid [\mathcal{O}_{\mathbb{Q}(\sqrt{a})} : \mathbb{Z}[a]]$ and we can factor $p\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$ via the minimal polynomials modulo p. □

Theorem 4.41 (QR)**.** *Let p, l be distinct odd primes. Then $\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}\frac{p-1}{2}}$.*

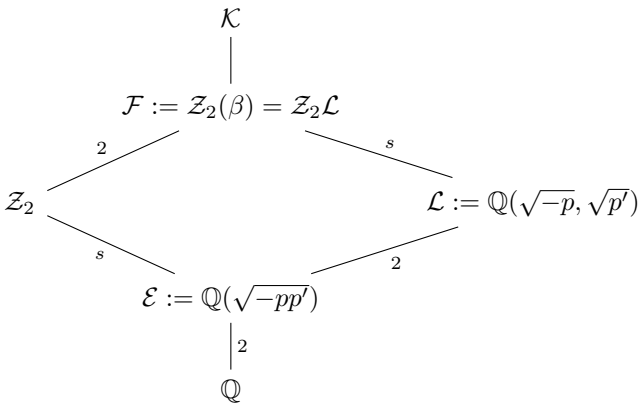
Proof. Let $l^* = (-1)^{\frac{l-1}{2}} l$. Since $\left(\frac{l^*}{p}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{l-1}{2}}\left(\frac{l}{p}\right) = (-1)^{\frac{l-1}{2}\frac{p-1}{2}}\left(\frac{l}{p}\right)$, it is enough to show $\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$. By previous theorem and lemma, $\left(\frac{l^*}{p}\right) = 1$ if and only if p decomposes into an even number of primes in $\mathbb{Q}(\xi_l)$. In the prime decomposition of l, the prime power of p is 0, by previous theorem, $e(p) = \varphi(p^0) = 1$. So $r(p) = \frac{[\mathbb{Q}(\xi_l):\mathbb{Q}]}{e(p)f(p)} = \frac{l-1}{f(p)}$. Hence $r(p)$ is even if and only if $f(p)$ divides $\frac{l-1}{2}$. Recall $f(p)$ is the smallest positive integer such that $p^{f(p)} \equiv 1 \pmod l$. So $f(p)$ divides $\frac{l-1}{2}$ if and only if $p^{\frac{l-1}{2}} \equiv 1 \pmod l$ if and only if $\left(\frac{p}{l}\right) = 1$. Thus, $\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$. □

Remark. We want to study $\mathbb{Q}(\xi_p)/\mathbb{Q}$, in particular, we want to know about the class group of $\mathbb{Q}(\xi_p)$. Iwasawa theory: Instead of focusing on $\mathbb{Q}(\xi_p)$, stick this field in a tower of fields and study the tower instead: $\mathbb{Q} \subseteq \mathbb{Q}(\xi_p) \subseteq \mathbb{Q}(\xi_{p^2}) \subseteq \cdots \subseteq \mathbb{Q}(\xi_{p^r}) \subseteq \cdots$. Set $\mathbb{Q}(\xi_{p^\infty}) = \bigcup_{n\geqslant 0} \mathbb{Q}(\xi_{p^n})$. We have $\mathrm{Gal}(\mathbb{Q}(\xi_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^\times$. Set $K_n = \mathbb{Q}(\xi_{p^n})^{(\mathbb{Z}/p\mathbb{Z})^\times}$. Then $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$ and $\mathbb{Q} = K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_n \subseteq \cdots$. Define the cyclotomic $\mathbb{Z}_p$-extension over $\mathbb{Q}$ by $\mathbb{Q}_\infty = \bigcup_{n\geqslant 1} K_n$, where $\mathbb{Z}_p$ is the p-adic integer. Then $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \mathrm{Gal}(\cup_{n\geqslant 1} K_n/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(K_n/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \cong Z_p$. We can form a large group X that has quotients which is the p-parts of the class groups of $\mathbb{Q}(\xi_p)$. It helps since X is pro-p, so $\mathbb{Z}_p$ acts on X. We also have p acts on X. We have X is a $\mathbb{Z}_p[\Gamma] \cong \mathbb{Z}_p[[\Gamma]]$-module. This gives lots of new tools. Use these tools to get information about the class group of $\mathbb{Q}(\xi_{p^n})$.

4.7 Applications

Example 4.42. Let $p \equiv 3 \pmod 8$ and $p' \equiv 5 \pmod 8$. Let $\mathcal{K} = \mathbb{Q}(\xi_N)$, where $N = p^l p'^{l'}$ with $l, l' \in \mathbb{N}$. Since $\mathcal{K} \cong (\mathbb{Z}/N\mathbb{Z})^\times$ and $2 \nmid N$, $f := f(2)$ is the order of 2 mod N. Let t, t' be the orders of 2 mod p^l and 2 mod $p'^{l'}$, respectively. Since $p' \equiv 5 \pmod 8$, $2^2 \mid\mid t'$. Also, since $f = \mathrm{lcm}(t, t')$ and $2^2 \nmid t$, we have $2^2 \mid\mid f$. Since $\varphi(N) = \varphi(p^l)\varphi(p'^{l'}) = p^{l-1}(p-1)p'^{l'-1}(p'-1)$, $2^3 \mid\mid \varphi(N)$, we have $r = \frac{\varphi(N)}{f}$ is even and $s := \frac{r}{2} = \frac{\varphi(N)}{2f}$ is odd. Let $\mathcal{Z}_2$ be the decomposition field of 2 in $\mathcal{K}$. Then $[\mathcal{Z}_2 : \mathbb{Q}] = r = 2s$. By previous corollary, $\mathcal{E} := \mathbb{Q}(\sqrt{-pp'}) \subseteq \mathcal{K}$. Then $[\mathcal{Z}_2 : \mathcal{E}] = \frac{[\mathcal{Z}_2:\mathbb{Q}]}{[\mathcal{E}:\mathbb{Q}]} = s$.

Since $-pp' \equiv 1 \pmod 4$, $\mathcal{O}_\mathcal{E} = \mathbb{Z}\left[\frac{1+\sqrt{-pp'}}{2}\right]$. Note $\mathcal{O}_\mathcal{E}/\langle 2\rangle \cong \frac{\mathbb{Z}[x]}{\langle 2, x^2-x+\frac{1+pp'}{4}\rangle} \cong \frac{\mathbb{F}_2[x]}{\langle x^2-x+\frac{1+pp'}{4}\rangle}$. Since $x^2 - x + \frac{1+pp'}{4} \equiv x^2 - x \pmod 2$, 2 splits in $\mathcal{E}$. Let $\beta \in \mathcal{O}_K \setminus \mathcal{O}_{\mathcal{Z}_2}$ and $\beta^2 \in \mathcal{O}_{\mathcal{Z}_2}$. Then $m_{\beta,\mathcal{Z}_2}(x) = x^2 - \beta^2$ and so $[\mathcal{Z}_2(\beta) : \mathcal{Z}_2] = 2$.



Since $p \equiv 3 \pmod 8$, $\sqrt{-p} = \sqrt{p^*} = \sum_{i\in\mathbb{Z}_p^\times} \left(\frac{i}{p}\right) \xi_p^i$. So

$$\sigma^4(\sqrt{-p}) = \sigma^4\left(\sum_{i\in\mathbb{Z}_p^\times} \left(\frac{i}{p}\right) \xi_p^i\right) = \sum_{i\in\mathbb{Z}_p^\times} \left(\frac{4i}{p}\right) \xi_p^{4i} = \sum_{i\in\mathbb{Z}_p^\times} \left(\frac{i}{p}\right) \xi_p^i = \sqrt{-p}.$$

Similarly, $\sigma^2(\sqrt{p'}) = \sqrt{p'}$. So σ^2 fixes $\mathcal{L}$ pointwisely and thus $\mathcal{L} \subseteq \mathcal{F}$. Since $p \equiv 3 \pmod 8$ and $p' \equiv 5 \pmod 8$, $\left(\frac{2}{p}\right) = -1 = \left(\frac{2}{p'}\right)$. So

$$\begin{aligned}\sigma^2(\sqrt{-pp'}) = \sigma(\sqrt{-p})\sigma(\sqrt{p'}) = \sigma(\sqrt{p^*})\sigma(\sqrt{p'^*}) &= \sigma^2\left(\sum_{i\in\mathbb{Z}_p^\times} \left(\frac{i}{p}\right) \xi_p^i\right) \sigma^2\left(\sum_{j\in\mathbb{Z}_{p'}^\times} \left(\frac{j}{p'}\right) \xi_{p'}^i\right) \\ = \sum_{i\in\mathbb{Z}_p^\times} \left(\frac{2i}{p}\right) \xi_p^{2j} \sum_{j\in\mathbb{Z}_{p'}^\times} \left(\frac{2i}{p'}\right) \xi_{p'}^{2i} &= \sum_{i\in\mathbb{Z}_p^\times} \left(\frac{i}{p}\right) \xi_p^i \sum_{j\in\mathbb{Z}_{p'}^\times} \left(\frac{j}{p'}\right) \xi_{p'}^i = \sqrt{p^*}\sqrt{p'^*} = \sqrt{-pp'}.\end{aligned}$$

So $\mathcal{E} \subseteq \mathcal{D}$. Since $\mathcal{E} \subseteq \mathcal{L}$ and $\sigma^2(\sqrt{-p}) = -\sqrt{-p}$, $\mathcal{E} \subsetneq \mathcal{L}$. Also, since $[\mathcal{E} : \mathbb{Q}] = 2$, $[\mathcal{L} : \mathbb{Q}] \leqslant 4$ and $[\mathcal{E} : \mathbb{Q}] \mid [\mathcal{L} : \mathbb{Q}]$, we have $[\mathcal{L} : \mathbb{Q}] = 4$ and then $[\mathcal{L} : \mathcal{E}] = 2$. Since $\gcd(2, s) = 1$, $[\mathcal{Z}_2 : \mathcal{L}] = 2$ and $[\mathcal{Z}_2\mathcal{L} : \mathcal{L}] = s$. Also, since $[\mathcal{F} : \mathcal{Z}_2] = 2$, we have $\mathcal{F} = \mathcal{Z}_2\mathcal{L}$.

Chapter 5

Class Group and Unit

5.1 Lattices

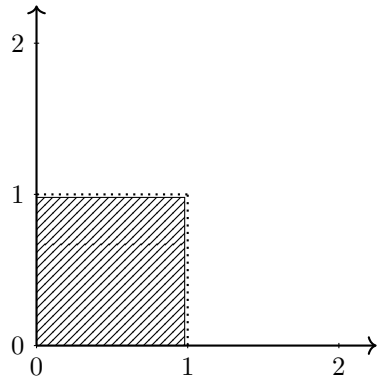
Remark. Recall $\mathbb{Z}[i] \subseteq \mathbb{Q}(i) \subseteq \mathbb{C}$. Goal: generalize this to other ring of integers.

Definition 5.1. Let V be an n-dimensional $\mathbb{R}$-vector space. A *lattice* in V is a additive subgroup Γ of V the form $\Gamma = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$, where $m \leqslant n$ and $v_1, \ldots, v_m \in V$ are linearly independent over $\mathbb{R}$. The set $\{v_1, \ldots, v_m\}$ is called a *basis* of the lattice. The set $\Phi = \{x_1v_1 + \cdots + x_mv_m : 0 \leqslant x_i < 1\}$ is called the *fundamental mesh* of Γ. If $m = n$, we say Γ is a complete lattice or a $\mathbb{Z}$-structure on V.

Remark. The completeness of the lattice Γ is equivalent to the fact that the set of all translate $\Phi + \gamma, \gamma \in \Gamma$ covers the entire space V, i.e., $V = \bigcup_{\gamma\in\Gamma}(\Phi + \gamma)$.

Example 5.2. For any $\mathbb{R}$-basis of V, the subgroup of all linear combinations with integer coefficients of the basis vector forms a lattice.

Example 5.3. Let $V = \mathbb{R}(i) \cong \mathbb{R}^2$ and $\Gamma = \mathbb{Z}[i]$. Then Γ is complete. The fundamental mesh Φ of Γ is $\{x_1 + x_2i : 0 \leqslant x_1, x_2 < 1\} \cong [0, 1) \times [0, 1)$.



Example 5.4. $\Gamma = \mathbb{Z} \cong \mathbb{Z} \times 0 \subseteq \mathbb{R}^2$ is a lattice but not a complete lattice. Note $\Phi = [0, 1)$.

Definition 5.5. Let V be a group and $W \subseteq V$. If each $w \in W$ is an isolated point in the sense that there exists a neighbourhood which contains no other points of W, then W is a discrete group of V.

Remark. If Γ is complete, the collection of all translates $\Phi + \gamma, \gamma \in \Gamma$ covers all of V.

Theorem 5.6. *A **subgroup** $\Gamma \subseteq V \cong \mathbb{R}^n$ is a lattice if and only if it is discrete.*

Proof. "$\Rightarrow$". Assume $\Gamma \subseteq V$ is a lattice. Then there exists $1 \leqslant m \leqslant n$ and $v_1, \ldots, v_m \in V$ independent such that $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$. Let $\gamma \in \Gamma$. Then there exists $a_1, \ldots, a_m \in \mathbb{Z}$ such that $\gamma = a_1v_1 + \cdots + a_mv_m$. Extend $\{v_1, \ldots, v_m\}$ to a basis $\{v_1, \ldots, v_n\}$ of V. Let $U_\gamma = \{x_1v_1 + \cdots + x_nv_n : x_i \in \mathbb{R}, |a_i - x_i| < 1, i = 1, \ldots, m\}$ be a neighborhood of γ. Since $U_\gamma \cap \Gamma = \{\gamma\}$, Γ is a discrete group of V.

"$\Leftarrow$". Assume Γ is discrete subgroup of V. Let U be any open neighborhood of 0. Then there exists a neighborhood $U' \subseteq U$ of 0 such that the difference of any two elements in U' is in U. Suppose there exists $x \in \overline{\Gamma} \setminus \Gamma$, then there exists a sequence $\{x_n\} \subseteq \Gamma$ such that $x_n \to x$. So any open neighborhood of x contains infinitely many points of Γ. In particular, this open neighborhood $x + U'$ contains infinitely many points of Γ. So there exist two distinct $\gamma_1, \gamma_2 \in (x + U') \cap \Gamma$. Since $\gamma_1 - x, \gamma_2 - x \in U'$, by definition of U', $0 \neq \gamma_1 - \gamma_2 = (\gamma_1 - x) - (\gamma_2 - x) \in U$. Since Γ is a group, $\gamma_1 - \gamma_2 \in \Gamma$. So $U \cap \Gamma \neq \{0\}$, a contradiction since Γ is discrete. Hence Γ is closed. Let V_0 be $\mathbb{R}$-spanned by the set Γ. Then V_0 is a subspace of V. Let $m = \dim_{\mathbb{R}} V_0$ and we can pick $u_1, \ldots, u_m \in \Gamma$ such that $\{u_1, \ldots, u_m\}$ is a $\mathbb{R}$-basis of V_0. Let $\Gamma_0 := \mathbb{Z}u_1 + \cdots \mathbb{Z}u_m \leqslant \Gamma$. Then by definition, Γ_0 is a complete lattice of V_0. Let $\gamma' \in \Gamma$ vary over a system of representatives of the cosets in Γ/Γ_0. Let Φ_0 be the fundamental mesh of Γ_0. Since Γ_0 is complete in V_0, $V_0 = \bigcup_{\gamma_0 \in \Gamma_0}(\Phi_0 + \gamma_0)$. Since $\gamma' \in \Gamma \subseteq V_0$, we can write $\gamma' = \mu + \gamma_0$ for some $\mu \in \Phi_0$ and $\gamma_0 \in \Gamma_0 \subseteq T$. Then $\mu = \gamma' - \gamma_0 \in \Gamma$. So $\mu \in \Phi_0 \cap \Gamma = \overline{\Phi}_0 \cap \Gamma$. Since Φ_0 is bounded, $\overline{\Phi}_0$ is bounded and closed. Since $V \cong \mathbb{R}^n$ is a finite dimensional, $\overline{\Phi}_0$ is compact. Also, since Γ is discrete, $\overline{\Phi}_0 \cap \Gamma$ is finite. Hence the number of distinct cosets Γ/Γ_0 is finite. So $q := [\Gamma : \Gamma_0]$ is finite. Then the additive group Γ/Γ_0 has order q. So for any $\gamma + \Gamma_0 \in \Gamma/\Gamma_0$, $q(\gamma + \Gamma_0) = \Gamma_0$, i.e., $q\gamma \in \Gamma_0$. Since $\gamma \in \Gamma$ was arbitrary, $q\Gamma \subseteq \Gamma_0$. So $\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\frac{u_1}{q} + \cdots + \mathbb{Z}\frac{u_m}{q}$. By the FTFGAG, there exists an $\mathbb{Z}$-basis $\{v_1, \ldots, v_r\} \subseteq \Gamma$ with $r \leqslant m$ such that $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r$. Since $\Gamma \cong \mathbb{Z}^m$ and $\Gamma_0 \cong \mathbb{Z}^r$, $\mathbb{R}^r \cong \Gamma \otimes_{\mathbb{Z}} \mathbb{R} \supseteq \Gamma_0 \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^m$ and then $r \geqslant m$. Thus, $r = m$ and then $v_1, \ldots, v_r$ spans the m-dimensional $\mathbb{R}$ vector space V_0. So $v_1, \ldots, v_r$ are also $\mathbb{R}$-linearly independent. □

Lemma 5.7. A lattice Γ in V is complete if and only if there exists a bounded subset $M \subseteq V$ such that the collection of all translates $M + \gamma, \gamma \in \Gamma$ cover the whole space V.

Proof. "$\Rightarrow$". Set $M = \Phi$.

"$\Leftarrow$". Let $M \subseteq V$ be a bounded set whose translates $M + \gamma, \gamma \in \Gamma$ cover V. Let V_0 be the $\mathbb{R}$-spanned subspace of V by Γ. Then it is enough to show $V = V_0$. Let $v \in V$. Since $V = \bigcup_{\gamma \in \Gamma}(M + \gamma)$, and $nv \in V$ for any $n \in \mathbb{N}$, we may write for each $n \in \mathbb{N}$, $nv = a_n + \gamma_n$, $a_n \in M, \gamma_n \in \Gamma \subseteq V_0$. Since M is bounded, $\frac{a_n}{n} \to 0$ as $n \to \infty$. Then $\lim_{n\to\infty} \frac{\gamma_n}{n} = \lim_{n\to\infty} \frac{a_n}{n} + \lim_{n\to\infty} \frac{\gamma_n}{n} = \lim_{n\to\infty} \frac{a_n+\gamma_n}{n} = \lim_{v\to\infty} v = v$. Since V_0 is closed and $\frac{\gamma_n}{n} \in V_0$ for any $n \in \mathbb{N}$, $v \in V$. Thus, $V = V_0$. □

We now assume that our V is a Euclidean vector space, i.e., an $\mathbb{R}$-vector space of finite dimension n equipped with a symmetric, positive definite bilinear form $\langle , \rangle : V \times V \to \mathbb{R}$. Then we have on V a notion of volume - more precisely a Haar measure. The cube spanned by an orthonormal

basis $e_1, \dots, e_n$ has volume 1 and more generally, the parallelepiped $\Phi = \{x_1v_1 + \cdots + x_nv_n : x_i \in \mathbb{R}, 0 \leqslant x_i < 1\}$ spanned by n linearly independent vectors $v_1, \dots, v_n$, has volume $\mathrm{vol}(\Phi) = |\det(A)|$, where $A = (a_{ij})$ is the change of basis matrix from $e_1, \dots, e_n$ to $v_1, \dots, v_n$, i.e., $v_i = \sum_j a_{ij}e_j$. Since $(\langle v_i, v_j\rangle) = \left(\sum_{k,l} a_{ik}a_{jl}\langle e_k, e_l\rangle\right) = (\sum_k a_{ik}a_{jk}) = AA^t$, we have $\mathrm{vol}(\Phi) = |\det(A)| = |\det(AA^t)|^{\frac{1}{2}} = |\det(\langle v_i, v_j\rangle)|^{\frac{1}{2}}$. Let Γ be the lattice spanned by n linearly independent vectors $v_1, \dots, v_n$, then Φ is a fundamental mesh of Γ and write for short $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$. This does not depend on the choice of a basis $\{v_1, \dots, v_n\}$ of the lattice since if we change a basis, we hit $v_1, \dots, v_n$ by an element of $\mathrm{GL}_n(\mathbb{Z})$, but elements of $\mathrm{GL}_n(\mathbb{Z})$ have determinant ± 1 and so they don't impact the volume.

Definition 5.8. A subset $X \subseteq V$ is called *centrally symmetric* if given any $x \in X$ we have $-x \in X$. X is called *convex* if given any $x, y \in X$, the whole line segment $\{ty + (1-t)x : 0 \leqslant t \leqslant 1\} \subseteq X$.

Theorem 5.9 (Minkowski's Lattice Point Theorem)**.** *Let Γ be a complete lattice in the Euclidean vector space V with dimenson n and X a centrally symmetric, convex subset of V. If $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$, then X contains at least one nonzero lattice point $\gamma \in \Gamma$.*

Proof. It is enough to show that there exist two distinct $\gamma_1, \gamma_2 \in \Gamma \subseteq V$ such that $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$. In fact, choosing a point in this intersection: $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$ with $x_1, x_2 \in X$, we obtain $0 \neq \gamma := \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1$. Since $\gamma_1, \gamma_2 \in \Gamma$, $\gamma = \gamma_1\gamma_2 \in \Gamma$. Since X is a centrally symmetric and convex, $\gamma = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X$. So $\gamma \in X \cap \Gamma$. Now, suppose the sets $\{\frac{1}{2}X + \gamma, \gamma \in \Gamma\}$ were pairwise disjoint. Then $\mathrm{vol}(\Phi) \geqslant \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi \cap (\frac{1}{2}X + \gamma)\right)$. Also, since $\Phi - \gamma, \gamma \in \Gamma$ cover V,

$$\mathrm{vol}(\Gamma) \geqslant \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi \cap (\frac{1}{2}X + \gamma)\right) = \mathrm{vol}(\Phi) \geqslant \sum_{\gamma\in\Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{vol}(X),$$

i.e., $\mathrm{vol}(X) \leqslant 2^n \mathrm{vol}(\Gamma)$, a contradiction. □

5.2 Minkowski Theory and Geometry number

Let $\mathcal{K}/\mathbb{Q}$ be a number field of dimension n.

Definition 5.10. Let $\mathcal{K}_{\mathbb{C}} = \prod_\tau \mathbb{C}$, where τ runs over the embeddings $\mathcal{K} \hookrightarrow \mathbb{C}$. We have a natural embedding $j : \mathcal{K} \to \mathcal{K}_{\mathbb{C}}$ given by $a \mapsto (\tau(a))$.

Remark. We have an isomorphism $\mathcal{K}_{\mathbb{C}} \cong \mathcal{K} \otimes_{\mathbb{Q}} \mathbb{C}$ given by $j(a)z \leftarrow\!\shortmid a \otimes z$.

Definition 5.11. Let V be an $\mathcal{F}$-vector space. A *sesquilinear form* $\varphi : V \times V \to \mathcal{F}$ is a map that is linear in the first variable and conjugate linear in the second variable.

Definition 5.12. A sesquilinear form φ on V is said to be *Hermitian* if $\varphi(v, w) = \overline{\varphi(w, v)}$ for any $v, w \in V$.

Remark. The $\mathbb{C}$-vector space $\mathcal{K}_{\mathbb{C}}$ is equipped with the Hermitian scalar product $\langle , \rangle : \mathcal{K}_{\mathbb{C}} \times \mathcal{K}_{\mathbb{C}} \to \mathbb{C}$ given by $\langle (x_\tau), (y_\tau)\rangle \mapsto \sum_\tau x_\tau \overline{y}_\tau$. Actually, it is an inner product.

Remark. Given an embedding $\tau : \mathcal{K} \to \mathbb{C}$, we have a conjugate embedding $\overline{\tau}$ defined by $\overline{\tau}(a) = \overline{\tau(a)}$ for any $a \in \mathcal{K}$. If $\tau(\mathcal{K}) \subseteq \mathbb{R}$, then $\tau = \overline{\tau}$. If $\tau(\mathcal{K}) \not\subseteq \mathbb{R}$, then $\tau \neq \overline{\tau}$.

Definition 5.13. Define an *involution* ($\tau^2 = \mathrm{id}$ for any τ) $c : \mathcal{K}_{\mathbb{C}} \to \mathcal{K}_{\mathbb{C}}$ given by $z = (z_\tau) \mapsto c(z) = (c(z)_\tau) = (\overline{z}_{\overline{\tau}})$.

Example 5.14. If $\mathcal{K}_{\mathbb{C}} = \mathbb{C}$, define $c : \mathbb{C} \to \mathbb{C}$ by $z \mapsto \overline{z}$.

Example 5.15. If $\mathcal{K}_{\mathbb{C}} = \mathbb{C} \times \mathbb{C}$, define $c : \mathbb{C} \times \mathbb{C} \to \mathbb{C} \times \mathbb{C}$ by $(z_1, z_2) \mapsto (\overline{z}_2, \overline{z}_1)$.

Proposition 5.16. The scalar product $\langle , \rangle$ is equivariant under c, that is $\langle c(x), c(y)\rangle = c(\langle x, y\rangle)$.

Proof. Note $\langle c(x), c(y)\rangle = \langle (\overline{x}_{\overline{\tau}}), (\overline{y}_{\overline{\tau}})\rangle = \sum_\tau \overline{x}_{\overline{\tau}} y_{\overline{\tau}} = \sum_\tau \overline{x}_\tau y_\tau = \sum_\tau c(x_\tau \overline{y}_\tau) = c\left(\sum_\tau x_\tau \overline{y}_\tau\right) = c(\langle x, y\rangle)$. □

Definition 5.17. We have $\mathrm{Tr} : \mathcal{K}_{\mathbb{C}} \to \mathbb{C}$ given by $(z_\tau) \mapsto \sum_\tau z_\tau$.

Remark. The composite $\mathcal{K} \xrightarrow{j} \mathcal{K}_{\mathbb{C}} \xrightarrow{\mathrm{Tr}} \mathbb{C}$ gives the usual trace of $\mathcal{K}/\mathbb{Q}$, $\mathrm{Tr}_{\mathcal{K}/\mathbb{Q}}(a) = \mathrm{Tr}(j(a))$.

Example 5.18. Let $\mathcal{K} = \mathbb{Q}(i)$ and define $c : \mathcal{K} \to \mathcal{K}$ by $a + bi \mapsto a - bi$. Then we have $\mathcal{K}_{\mathbb{C}} \cong \mathbb{C} \times \mathbb{C}$ and $j : \mathcal{K} \to \prod_\tau \mathbb{C}$ given by $a + bi \mapsto (a + bi, a - bi)$. Let $x = (x_\tau) = (a + bi, c + di)$ and $y = (y_\tau) = (e + fi, g + hi)$. Then $\langle x, y\rangle = x_{\mathrm{id}} \overline{y}_{\mathrm{id}} + x_c \overline{y}_c = (a + bi)(e - fi) + (c + di)(g - hi)$. So

$$\begin{array}{ccccc} \mathcal{K} & \xrightarrow{\quad j \quad} & \mathcal{K}_{\mathbb{C}} & \xrightarrow{\qquad\mathrm{Tr}\qquad} & \mathbb{C} \\ a + bi & \mapsto & (a + bi, a - bi) & \mapsto & (a + bi) + (a - bi) = 2a, \end{array}$$

or

$$\begin{array}{ccc} \mathcal{K} & \xrightarrow{\mathrm{Tr}(\mathcal{K}/\mathbb{Q})} & \mathbb{Q} \subseteq \mathbb{C} \\ a + bi & \longmapsto & 2a. \end{array}$$

Definition 5.19. Label the embeddding with integers in $\mathbb{R}$ as $\rho_1, \ldots, \rho_r$ and refer to them as *real embeddings*. The embedding that does not map $\mathcal{K}$ into $\mathbb{R}$ are called *complex embeddings* and they come in pairs $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$. Note that $n = r + 2s$.

Definition 5.20. Define the *c-invariant points* of $\mathcal{K}_{\mathbb{C}}$ by

$$\mathcal{K}_{\mathbb{R}} = \{(z_\tau) \in \mathcal{K}_{\mathbb{C}} : z_\rho \in \mathbb{R}, \forall \rho \in \{\rho_1, \ldots, \rho_r\},\ z_{\overline{\sigma}} = \overline{z}_\sigma, \forall \sigma \in \{\sigma_1, \ldots, \sigma_s\}\}.$$

Corollary 5.21. $\mathcal{K}_{\mathbb{R}} = \{(z_\tau) \in \mathcal{K}_{\mathbb{C}} : (z_{\overline{\tau}}) = (\overline{z}_\tau)\}$.

Proof. $c(z) = z$ if and only if $(\overline{z}_{\overline{\tau}}) = (z_\tau) \iff (z_{\overline{\tau}}) = (\overline{z}_\tau)$. □

Remark. We have

$$\begin{array}{ccc} \mathcal{K}_{\mathbb{C}} & \xrightarrow{\cong} & \mathcal{K} \otimes_{\mathbb{Q}} \mathbb{C} \\ \uparrow & & \uparrow \\ \mathcal{K}_{\mathbb{R}} & \xrightarrow{\cong} & \mathcal{K} \otimes_{\mathbb{Q}} \mathbb{R} \end{array}$$

The inclusion $\mathcal{K}_{\mathbb{R}} \subseteq \mathcal{K}_{\mathbb{C}}$ corresponds to the canonical mapping $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{R} \to \mathcal{K} \otimes_{\mathbb{Q}} \mathbb{C}$, which is induced by the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$. c corresponds to $c(a \otimes z) = a \otimes \overline{z}$.

Remark. Let $a \in \mathcal{K}$. Since $\overline{\tau}(a) = \overline{\tau(a)}$, $c(j(a)) = c(\tau(a)) = \left(\overline{\tau(a)}_{\overline{\tau}}\right) = \left(\overline{\overline{\tau(a)}}_{\tau}\right) = (\tau(a)) = j(a)$. So $j(a) \in \mathcal{K}_{\mathbb{R}}$. Then this yields a mapping $j : \mathcal{K} \to \mathcal{K}_{\mathbb{R}}$. The restriction of the hermitian scalar product $\langle , \rangle$ from $\mathcal{K}_{\mathbb{C}}$ to $\mathcal{K}_{\mathbb{R}}$ gives a scalar product $\langle , \rangle : \mathcal{K}_{\mathbb{R}} \times \mathcal{K}_{\mathbb{R}} \to \mathbb{R}$ on the $\mathbb{R}$-vector space $\mathcal{K}_{\mathbb{R}}$. Indeed, for $x, y \in \mathcal{K}_{\mathbb{R}}$, since $c(\langle x, y\rangle) = \langle c(x), c(y)\rangle = \langle x, y\rangle$, we have $\langle x, y\rangle \in \mathbb{R}$. So $\langle x, y\rangle = \overline{\langle x, y\rangle} = \langle y, x\rangle$. Thus, this is a symmetric positive definite bilinear form on $\mathcal{K}_{\mathbb{R}}$.

Definition 5.22. We call the Euclidean vector space $\mathcal{K}_{\mathbb{R}}$ the *Minkowski space*, its scalar product $\langle , \rangle$ the canonical metric, and the associated Haar measure the canonical measure.

Example 5.23. Set $\mathcal{K} = \mathbb{Q}(\sqrt[3]{2})$, then $n = 3, r = 1, s = 1$. Note that $\rho = \mathrm{id} : \sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sigma : \sqrt[3]{2} \mapsto \xi_3\sqrt[3]{2}$ and $\overline{\sigma} : \sqrt[3]{2} \mapsto \bar{\xi}_3\sqrt[3]{2} = \xi_3^2\sqrt[3]{2}$. So $\overline{\sigma}(\sqrt[3]{2}) = \overline{\sigma(\sqrt[3]{2})}$. Note $\mathcal{K}_{\mathbb{C}} \cong \mathbb{C}^3$ and $\mathcal{K}_{\mathbb{R}} = \{(z_\tau) \in \mathbb{C}^3 : z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z_\sigma}\} = \{(z_1, z_2, z_3) \in \mathbb{C}^3 : z_1 \in \mathbb{R}, z_3 = \bar{z}_2\} = \{(z_1, z_2, \bar{z}_2) \in \mathbb{C}^3, z_1 \in \mathbb{R}\} \cong \mathbb{R} \times \mathbb{C}$. Let $z \in \mathcal{K}_{\mathbb{C}}$ with $z = (z_\rho, z_\sigma, z_{\overline{\sigma}})$. Then $c(z) = (\bar{z}_{\overline{\rho}}, \bar{z}_{\overline{\sigma}}, \bar{z}_{\overline{\overline{\sigma}}}) = (\bar{z}_\rho, \bar{z}_{\overline{\sigma}}, \bar{z}_\sigma)$. So if $z = (z_1, z_2, z_3) \in \mathcal{K}_{\mathbb{C}}$, then $c(z) = (\bar{z}_1, \bar{z}_3, \bar{z}_2)$. Thus, if $z = (z_1, z_2, z_3) \in \mathcal{K}_{\mathbb{R}}$, then $z_1 \in \mathbb{R}$ and $z_3 = \bar{z}_2$ and so $c(z) = (\bar{z}_1, \bar{z}_3, \bar{z}_2) = (z_1, z_2, z_3) = z$.

Remark (Exercise)**.** Write down what c looks like in $\mathcal{K}_{\mathbb{C}}$. Show $\mathcal{K}_{\mathbb{R}} \cong \mathcal{K}_{\mathbb{C}}^{\langle c\rangle}$.

Theorem 5.24. *There is an isomorphism $f : \mathcal{K}_{\mathbb{R}} \to \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$ given by $(z_\tau) \mapsto (x_\tau)$, where $x_\rho = z_\rho$, $x_\sigma = \mathrm{Re}(z_\sigma)$, $x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma)$. This isomorphism transforms the canonical metric $\langle , \rangle$ into the scalar product $\langle a, b\rangle = \sum_\tau \alpha_\tau a_\tau b_\tau$, where $\alpha_\tau = \begin{cases} 1 & \text{if } \tau \in \{\rho_1, \dots, \rho_r\} \\ 2 & \text{otherwise} \end{cases}$.*

Proof. The map is clearly an isomorphism. Let $z = (z_\tau) = (x_\tau + iy_\tau)$, $z' = (z'_\tau) = (x'_\tau + iy'_\tau) \in \mathcal{K}_{\mathbb{R}}$. Then $z_\rho \bar{z}'_\rho = x_\rho x'_\rho$. Since $x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma) = y_\sigma$ and $x'_{\overline{\sigma}} = y'_\sigma$, $\mathrm{Re}(z_\sigma \bar{z}'_\sigma) = \mathrm{Re}((x_\sigma + ix_{\overline{\sigma}})(x'_\sigma - ix'_{\overline{\sigma}})) = x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}}$. Since $z, z' \in \mathcal{K}_{\mathbb{R}}$, $z_\sigma \bar{z}'_\sigma + z_{\overline{\sigma}} \bar{z}'_{\overline{\sigma}} = z_\sigma \bar{z}'_\sigma + \bar{z}_\sigma z'_\sigma = 2\,\mathrm{Re}(z_\sigma \bar{z}'_\sigma) = 2(x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}})$. So $\langle z, z'\rangle = \sum_\rho x_\rho x'_\rho + \sum_\sigma (z_\sigma \bar{z}'_\sigma + z_{\overline{\sigma}} \bar{z}'_{\overline{\sigma}}) = \sum_\rho x_\rho x'_\rho + \sum_\sigma 2(x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}}) = \sum_\tau \alpha_\tau x_\tau x'_\tau$. □

Remark. The scalar product $\langle x, y\rangle = \sum_\tau \alpha_\tau x_\tau y_\tau$ transfers the canonical measure from $\mathcal{K}_{\mathbb{R}}$ to $\mathbb{R}^{r+2s}$. It obviously dif and only ifers from the standard Lebesgue measure by $\mathrm{vol}_{\mathrm{can}}(X) = 2^s \,\mathrm{vol}_{\mathrm{Leb}}(f(X))$.

Theorem 5.25. *Let $0 \neq \mathfrak{a} \leqslant \mathcal{O}_{\mathcal{K}}$. Then $\Gamma = j(\mathfrak{a})$ is a complete lattice in $\mathcal{K}_{\mathbb{R}}$. Its fundamental mesh has volume* $\mathrm{vol}(\Gamma) = \sqrt{|\Delta_{\mathcal{K}}|}[\mathcal{O}_{\mathcal{K}} : \mathfrak{a}]$.

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Then $\Gamma = \mathbb{Z}j(\alpha_1) + \cdots + \mathbb{Z}j(\alpha_n)$. Let $\{\tau_1, \dots, \tau_n\}$ be the embeddings of $\mathcal{K} \hookrightarrow \mathbb{C}$ and set $A = (\tau_i(\alpha_j))$. Recall $(\det(A))^2 = d(\alpha_1, \dots, \alpha_n) = \Delta(\mathfrak{a}) = [\mathcal{O}_{\mathcal{K}} : \mathfrak{a}]^2 \Delta(\mathcal{O}_{\mathcal{K}})$. Note $(\langle j(\alpha_i), j(\alpha_k)\rangle) = (\sum_{l=1}^n \tau_l(\alpha_i)\overline{\tau}_l(\alpha_k)) = A\overline{A}^t$. Since $\{j(\alpha_1), \dots, j(\alpha_n)\}$ is a $\mathbb{Z}$-basis of $j\mathfrak{a}$, $\mathrm{vol}(\Gamma) = |\det(\langle j(\alpha_i), j(\alpha_k)\rangle)|^{\frac{1}{2}} = |\det(A)| = \sqrt{|\Delta_{\mathcal{K}}|}[\mathcal{O}_{\mathcal{K}} : \mathfrak{a}]$. □

Theorem 5.26. *Let $0 \neq \mathfrak{a} \leqslant \mathcal{O}_{\mathcal{K}}$. Let $c_\tau > 0$ so that $c_\tau = c_{\overline{\tau}}$ for each embedding $\mathcal{K} \hookrightarrow \mathbb{C}$ and $\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_{\mathcal{K}}|}[\mathcal{O}_{\mathcal{K}} : \mathfrak{a}]$. Then there exists $0 \neq a \in \mathfrak{a}$ such that for each embedding $\tau : \mathcal{K} \hookrightarrow \mathbb{C}$, $|\tau(a)| < c_\tau$.*

Proof. Let $X = \{(z_\tau) \in \mathcal{K}_{\mathbb{R}} : |z_\tau| < c_\tau\}$. Then X is centrally symmetric and convex. Its volume $\mathrm{vol}(X)$ can be computed via the map $f : \mathcal{K}_{\mathbb{R}} \xrightarrow{\cong} \prod_\tau \mathbb{R}$ given by $(z_\tau) \mapsto (x_\tau)$. With $f(X) =$

$\{(x_\tau) \in \prod_\tau \mathbb{R} : |x_\rho| < c_\rho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\}$, it comes out

$$\begin{aligned}\operatorname{vol}(X) &= 2^s \operatorname{vol}_{\mathrm{Leb}}(f(X)) = 2^s \prod_\rho (2c_\rho) \prod_\sigma (\pi c_\sigma^2) = 2^{r+s}\pi^s \prod_\tau c_\tau \\ &> 2^{r+s}\pi^s \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}[\mathcal{O}_\mathcal{K} : \mathfrak{a}] = 2^n \operatorname{vol}(\Gamma).\end{aligned}$$

This shows X satisfies the hypothesis of Minkowski's lattice point theorem. Also since $\Gamma = j(\mathfrak{a})$ is a complete lattice in $\mathcal{K}_\mathbb{R}$, there exists a lattice point $j(a) \in X$ with $0 \neq a \in \mathfrak{a}$, i.e., $|\tau(a)| < c_\tau$ for any embedding $\tau : \mathcal{K} \hookrightarrow \mathbb{C}$. □

Example 5.27. Work out for $\mathcal{K} = \mathbb{Q}(i)$.

5.3 The Class Number

Let $\mathcal{K}$ be a number field and $\mathcal{O} = \mathcal{O}_\mathcal{K}$.

Remark. If $\mathrm{Cl}(\mathcal{K}) = J_\mathcal{K}/P_\mathcal{K}$ is finite, set $h_\mathcal{K} = |\mathrm{Cl}(\mathcal{K})|$, which is the class number, then $h_\mathcal{K} = 1$ if and only if $\mathcal{O}_\mathcal{K}$ is a UFD.

Lemma 5.28. Let $\mathcal{K} = \mathbb{Q}(\sqrt{d})$. For $d < 0$, $h_\mathcal{K} = 1$ if and only if

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Example 5.29. Let $\mathfrak{a} \in J_\mathcal{K}$. If m is the smallest positive integer such that $\mathfrak{a}^m$ is principal, then m is the smallest positive integer such that $(\mathfrak{a} + \mathcal{P}_\mathcal{K})^m = \mathcal{P}_\mathcal{K}$, and so $m \mid h_\mathcal{K}$.

Remark (Conjecture, Gauss)**.** (a) $\lim_{d\to\infty} h_{\mathbb{Q}(\sqrt{d})} = \infty$, which is solved by Heilbronn, 1934.

(b) There are infinitely many $d > 0$ such that $h_{\mathbb{Q}(\sqrt{d})} = 1$, where about 75.446% of the real quadratic fields has class number 1.

Remark. In general, there are not nice patterns in the sizes of class groups except in cyclomatic fields $\mathbb{Q}(\xi_{p^n})$.

Proof. p-sylow subgroup of $\mathrm{Cl}_{\mathcal{K}_n}$. □

Remark. For our case (or if $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ is abelian), it is known that $\mu = 0$.

Remark. Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be ideals, then $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$. It may therefore be extended to a homomorphism

$$\begin{aligned}\mathfrak{N} : J_\mathcal{K} &\to \mathbb{R}_{>}0 \\ \mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}} &\mapsto \prod_\mathfrak{p} \mathfrak{N}(\mathfrak{p})^{\nu_\mathfrak{p}}.\end{aligned}$$

Lemma 5.30. Let $0 \neq \mathfrak{a} \leqslant \mathcal{O}$, then there exists $0 \neq a \in \mathfrak{a}$ such that $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{\Delta_\mathcal{K}}\mathfrak{N}(\mathfrak{a})$, i.e., $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right|\mathfrak{N}(\mathfrak{a}^{-1}) = \left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right|\mathfrak{N}(\mathfrak{a})^{-1} \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{\Delta_\mathcal{K}}$.

Proof. Given $\varepsilon > 0$, we choose $c_\tau \in \mathbb{R}_{>0}$ with the embedding $\tau : \mathcal{K} \hookrightarrow \mathbb{C}$ such that $c_\tau = c_{\overline{\tau}}$ and $\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}\mathfrak{N}(\mathfrak{a})+\varepsilon$. Then there exists $0 \neq a \in \mathfrak{a}$ such that $|\tau(a)| < c_\tau$ for each embedding $\tau : \mathcal{K} \hookrightarrow \mathbb{C}$. So $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right| = \prod_\tau |\tau(a)| < \prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}\mathfrak{N}(\mathfrak{a}) + \varepsilon$, which is true for all $\varepsilon > 0$. Also, since $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right| \in \mathbb{N}$, there exists $0 \neq a \in \mathfrak{a}$ such that $\left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a)\right| \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}\mathfrak{N}(\mathfrak{a})$. □

Theorem 5.31. $h_\mathcal{K} < \infty$.

Proof. Let $0 \neq \mathfrak{p} \leqslant \mathcal{O}$ be prime. Then there exists prime $0 \neq p \in \mathbb{Z}$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Let $f := f(\mathfrak{p}/p) = [\mathcal{O}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}] \geqslant 1$. Since $\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_p^f$, $\mathfrak{N}(\mathfrak{p}) = [\mathcal{O} : \mathfrak{p}] = |\mathcal{O}/\mathfrak{p}| = p^f$. Note there are at most $[\mathcal{K} : \mathbb{Q}]$ primes $\mathfrak{p} \leqslant \mathcal{O}$ such that $\mathfrak{p} \mid \langle p\rangle$. Fix $N \in \mathbb{N}$, since there are only finitely many rational primes less than N, there are only finitely many primes $\mathfrak{p} \leqslant \mathcal{O}$ with $\mathfrak{N}(\mathfrak{p}) \leqslant N$, which are at most $[\mathcal{K} : \mathbb{Q}] \cdot \#\{p \mid p \leqslant N\}$ such $\mathfrak{p}$. Since every $0 \neq \mathfrak{a} \leqslant \mathcal{O}$ admits a representation $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$, where $\nu_i > 0$, $\sum_{i=1}^r \nu_i \leqslant n$ and $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \cdots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}$, there are together only a finite number of ideals $\mathfrak{a}$ of $\mathcal{O}$ with $\mathfrak{N}(\mathfrak{a}) \leqslant N$. It therefore suffices to show that each class $\bar{\mathfrak{a}} = \mathfrak{a}P_\mathcal{K} \in \mathrm{Cl}(\mathcal{K})$ contains $\mathfrak{a}_1 \leqslant \mathcal{O}$, which is one of the representatives, such that $\mathfrak{N}(\mathfrak{a}_1) \leqslant N := \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}$. Choose a representative $\mathfrak{a}$ of $\bar{\mathfrak{a}}$. Since $\mathfrak{a}^{-1} \in J_\mathcal{K}$, there exists $\gamma \in \mathcal{O} \smallsetminus \{0\}$ such that $\mathfrak{b} := \gamma\mathfrak{a}^{-1} \subseteq \mathcal{O}$. Then by previous lemma, there exists $0 \neq \alpha \in \mathfrak{b} \leqslant \mathcal{O}$ such that

$$\mathfrak{N}(\alpha\mathfrak{b}^{-1}) = \mathfrak{N}(\langle\alpha\rangle\mathfrak{b}^{-1}) = \mathfrak{N}(\langle\alpha\rangle)\mathfrak{N}(\mathfrak{b}^{-1}) = \left|\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha)\right|\mathfrak{N}(\mathfrak{b}^{-1}) \leqslant \left(\frac{2}{\pi}\right)^s = N.$$

The ideal $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} = \mathfrak{a}(\alpha\gamma^{-1}\mathcal{O}) \in \mathfrak{a}P_\mathcal{K} = \bar{\mathfrak{a}}$ therefore has the required property. Thus, the class group is given by $\mathrm{Cl}_\mathcal{K} = \left\{\bar{\mathfrak{a}} : \mathfrak{a} \leqslant \mathcal{O}, \mathfrak{N}(\mathfrak{a}) \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{\Delta_\mathcal{K}}\right\}$. □

Remark. By previous proof, we have each ideal class contains an ideal $\mathfrak{a} \leqslant \mathcal{O}$ with $\mathfrak{N}(\mathfrak{a}) \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{\Delta_\mathcal{K}}$. Since $\mathfrak{a} \leqslant \mathcal{O}$ has a prime decomposition $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$ with $\nu_i \in \mathbb{N}$ and $\mathfrak{N}(\mathfrak{a}) = (\mathfrak{N}(\mathfrak{p}_1))^{\nu_1} \cdots (\mathfrak{N}(\mathfrak{p}_r^{\nu_r}))$, to actually calculate the class group, we just need to look at the group generated by $\bar{\mathfrak{p}}$ with $\mathfrak{p} \leqslant \mathcal{O}$ and $\mathfrak{N}(\mathfrak{p}) \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_\mathcal{K}|}$ or just need to look at the rational primes that is less than $\left(\frac{2}{\pi}\right)^s \sqrt{\Delta_\mathcal{K}}$.

Example 5.32. Let $\mathcal{K} = \mathbb{Q}(\sqrt{-7})$. Then $|\Delta_\mathcal{K}| = 7$ and $s = 1$. Since $\left(\frac{2}{\pi}\right)^1 \sqrt{7} \approx 1.684$, $\mathfrak{N}(\mathfrak{p}) \leqslant 1.684$. Also, since $\mathfrak{N}(\mathfrak{p}) \in \mathbb{Z}_{>0}$, $\mathfrak{N}(\mathfrak{p}) = 1$. So $\mathrm{Cl}_\mathcal{K} = \{\mathrm{id}\}$ and then $h_\mathcal{K} = 1$.

Example 5.33. Let $\mathcal{K} = \mathbb{Q}(\sqrt{5})$. Then $|\Delta_\mathcal{K}| = 5$ and $s = 0$. So $\mathfrak{N}(\mathfrak{p}) \leqslant \left(\frac{2}{\pi}\right)^0 \sqrt{5} \approx 2.236$. Since $m_{\sqrt{5}}(x) = x^2 - x - 1$, which is irreducible modulo 2, we have $\langle 2\rangle$ is irreducible. So $\mathrm{Cl}_\mathcal{K} = \{\mathrm{id}\}$.

Example 5.34. Let $\mathcal{K} = \mathbb{Q}(\sqrt{-5})$. Then $|\Delta_\mathcal{K}| = -20$ and $s = 1$. So $\mathfrak{N}(\mathfrak{p}) \leqslant \left(\frac{2}{\pi}\right)^1 \sqrt{20} \approx 2.847$. Since $m_{\sqrt{5}}(x) = x^2 + 5 \equiv (x + 1)^2 \pmod 2$, $\langle 2\rangle = \langle 2, \sqrt{-5} + 1\rangle^2$. Note $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Suppose $\mathfrak{p} := \langle 2, \sqrt{-5} + 1\rangle = \langle x + y\sqrt{-5}\rangle$ for some $x, y \in \mathbb{Z}$. Since $2 \in \mathfrak{p}$, then $x + y\sqrt{-5} \mid 2$. So $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(x+y\sqrt{-5}) \mid \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(2)$, i.e., $\mathrm{N}_{\mathcal{K}\mathbb{Q}}(x+y\sqrt{-5}) \mid 4$. Similarly, since $\sqrt{-5}+1 \in \mathfrak{p}$, $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(x+y\sqrt{-5}) \mid 6$. Also, since $x + y\sqrt{-5} \notin \mathcal{O}^\times$, $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(x + y\sqrt{-5}) = 2$, i.e., $x^2 + 5y^2 = 2$, a contraction (or because $x^2+5y^2 \neq 2^1 = 2$). Hence $\mathfrak{p} \notin P_\mathcal{K}$, i.e., $\bar{\mathfrak{p}} \neq \mathrm{id}$. Since $\bar{\mathfrak{p}}^2 = \overline{\langle 2\rangle} = \mathrm{id}$ and then $\mathrm{Cl}_\mathcal{K} = \{\mathrm{id}, \bar{\mathfrak{p}}\} \cong \mathbb{Z}/2\mathbb{Z}$.

Example 5.35. Let $\mathcal{K} = \mathbb{Q}(\sqrt{82})$. Then $\Delta_\mathcal{K} = 4 \cdot 82$ and $s = 0$. Since $\left(\frac{2}{\pi}\right)^0 \sqrt{4 \cdot 82} \approx 18.11$, we

need to consider primes over the rational primes $2, 3, 5, 7, 11, 13, 17$.

p	$T^2 - 82 \pmod p$	$\langle p \rangle$
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	irreducible	prime
7	irreducible	prime
11	$(T+4)(T+7)$	$\mathfrak{p}_{11}\mathfrak{p}_{11}'$
13	$(T+2)(T-2)$	$\mathfrak{p}_{13}\mathfrak{p}_{13}'$
17	irreducible	prime

Since $\langle 5\rangle, \langle 7\rangle, \langle 17\rangle \in P_{\mathcal{K}}$ are irreducible, we don't need to consider primes over $5, 7, 17$. So $\mathrm{Cl}_{\mathcal{K}}$ is generated by $\bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_3, \bar{\mathfrak{p}}_3', \bar{\mathfrak{p}}_{11}$ and $\bar{\mathfrak{p}}_{13}$. Since $\mathfrak{p}_3\mathfrak{p}_3' = \langle 3\rangle \in P_{\mathcal{K}}$, $\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_3' = \overline{\langle 3\rangle} = \mathrm{id}$, i.e., $\bar{\mathfrak{p}}_3' = \bar{\mathfrak{p}}_3^{-1}$. Similarly, $\bar{\mathfrak{p}}_2^2 = \overline{\mathfrak{p}_2^2} = \mathrm{id}$. Since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(7+\sqrt{82}) = -1\cdot 3\cdot 11$, $\langle 7+\sqrt{82}\rangle = \mathfrak{p}_3\mathfrak{p}_{11}$. Similarly, $\bar{\mathfrak{p}}_{11} = \bar{\mathfrak{p}}_3^{-1}$. Since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(11+\sqrt{82}) = 3\cdot 13$, $\langle 11+\sqrt{82}\rangle = \mathfrak{p}_3\mathfrak{p}_{13}$. Similarly, $\bar{\mathfrak{p}}_{13} = \bar{\mathfrak{p}}_3^{-1}$. Since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(10+\sqrt{82}) = 18 = 2\cdot 3^2$, $\langle 10+\sqrt{82}\rangle$ can only be divisible by $\mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_3'$. Since $3 \nmid 10+\sqrt{82}$ and $\mathfrak{p}_3\mathfrak{p}_3' = \langle 3\rangle$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ can't both divide $\langle 10+\sqrt{82}\rangle$. We say $\mathfrak{p}_3'$ is the one that divides $10+\sqrt{82}$, so $\langle 10+\sqrt{82}\rangle = \mathfrak{p}_2\mathfrak{p}_3'^2$. Hence, $\bar{\mathfrak{p}}_2 = \overline{\mathfrak{p}_3'^{2-1}} = \overline{\mathfrak{p}_3'}^{-2} = \bar{\mathfrak{p}}_3^2$. Thus, $\mathrm{Cl}_{\mathcal{K}} = \langle \bar{\mathfrak{p}}_3\rangle$. Since $\mathrm{id} = \bar{\mathfrak{p}}_2^2 = \overline{\mathfrak{p}_3^2}^2 = \bar{\mathfrak{p}}_3^4$, $\bar{\mathfrak{p}}_3$ has order dividing 4. Suppose $\bar{\mathfrak{p}}_2 = \mathrm{id}$, since $\mathcal{O} = \mathbb{Z}[\sqrt{82}]$, there exists $a, b \in \mathbb{Z}$ such that $\mathfrak{p}_2 = \langle a+b\sqrt{82}\rangle$. Then $\langle 2\rangle = \mathfrak{p}_2^2 = \langle (a+b\sqrt{82})^2\rangle$. Since $\mathcal{O}$ is an integral domain, there exists $u \in \mathcal{O}^\times$ such that $2 = (a+b\sqrt{82})^2 u$. Taking norms, we have $\mathrm{N}(u) > 0$. Also, since $\mathrm{N}(u) = \{\pm 1\}$, $\mathrm{N}(u) = 1$. Since $\mathcal{O}^\times \cong \pm(9+\sqrt{82})^{\mathbb{Z}}$ and $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(9+\sqrt{82}) = -1$, the positive units of norm 1 are the integral powers of $(9+\sqrt{82})^2$, which are all squares. So μ as a unit square can be absorbed into the $(a+b\sqrt{82})^2$ term with $a, b \in \mathbb{Z}$. Then we have to solve $2 = (a+b\sqrt{82})^2$. But then $\sqrt{2} \in \mathbb{Z}[\sqrt{82}]$, a contradiction. Hence $\bar{\mathfrak{p}}_2 \neq \mathrm{id}$ and then $\bar{\mathfrak{p}}_3$ has order 4. Thus, $\mathrm{Cl}_{\mathcal{K}} \cong \mathbb{Z}/4\mathbb{Z}$.

Example 5.36. Let $\mathcal{K} = \mathbb{Q}(\sqrt{-30})$. Then $s = 1$ and $\Delta_{\mathcal{K}} = -120$. Since $\left(\frac{2}{\pi}\right)^s \sqrt{|-120|} \approx 6.97$, the class group is generated by primes dividing 2,3 and 5.

p	$T^2 + 30 \pmod p$	$\langle p \rangle$
2	T^2	$\mathfrak{p}_2^2$
3	T^2	$\mathfrak{p}_3^2$
5	T^2	$\mathfrak{p}_5^2$

So $\bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_3$ and $\bar{\mathfrak{p}}_5$ each have order dividing 2 in $\mathrm{Cl}_{\mathcal{K}}$. Also, $f(\mathfrak{p}_2/2) = f(\mathfrak{p}_3/3) = f(\mathfrak{p}_5/5) = 1$. For $a, b \in \mathbb{Z}$, $\mathfrak{N}(\langle a+b\sqrt{-30}\rangle) = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(a+b\sqrt{-30}) = a^2+30b^2$ which is never 2^1, 3^1 or 5^1. So $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5 \notin P_{\mathcal{K}}$ and then $\bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_3$ and $\bar{\mathfrak{p}}_5$ each have order 2 in $\mathrm{Cl}_{\mathcal{K}}$. Moreover, since $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\sqrt{-30}) = 30 = 2\cdot 3\cdot 5$, $\langle\sqrt{-30}\rangle = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$, i.e., $\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_5 = \mathrm{id}$. So $\bar{\mathfrak{p}}_2$ and $\bar{\mathfrak{p}}_3$ generate the class group. Also, since $\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3 = \bar{\mathfrak{p}}_5^{-1} = \bar{\mathfrak{p}}_5 \neq \mathrm{id}$, we have $\bar{\mathfrak{p}}_2 \neq \bar{\mathfrak{p}}_3^{-1}$. Thus, $\mathrm{Cl}_{\mathcal{K}} \cong C_2 \times C_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where C_2 is the cyclic group of order 2.

Remark (Exer)**.** Show that if $d > 0$ and $\left|\mathrm{disc}(\mathbb{Q}(\sqrt{d}))\right| \leqslant d$, then $\mathbb{Q}(\sqrt{d})$ has class number 1.

5.4 Dirichlet's Unit Theorem

The group of units $\mathcal{O}_{\mathcal{K}}^\times$ contains the finite group $\mu(\mathcal{K})$ of the roots of unity that lie in $\mathcal{K}$, but in general is not itself finite. Its size is in fact determined by the number r of real embeddings

$\rho : \mathcal{K} \hookrightarrow \mathbb{R}$ and the number s of pairs $\sigma, \overline{\sigma} : \mathcal{K} \hookrightarrow \mathbb{C}$ of complex conjugate embeddings. To describe the group, we use the following commutative diagrams from Minkowski's theorem,

$$\begin{array}{ccccc} & & \overset{\lambda}{\frown} & & \\ \mathcal{K}^\times & \xrightarrow{j} & \mathcal{K}_{\mathbb{R}}^\times & \xrightarrow{l} & [\prod_\tau \mathbb{R}]^+ \\ \downarrow{\scriptstyle \mathrm{N}_{\mathcal{K}/\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow{\log||} & \mathbb{R} \end{array}$$

In the upper part of the diagram we consider the subgroups. The group of units: $\mathcal{O}_\mathcal{K}^\times = \{\varepsilon \in \mathcal{O}_\mathcal{K} : \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\varepsilon) = \pm 1\}$. The "norm-one surface": $S = \{y \in \mathcal{K}_\mathbb{Q}^\times : \mathrm{N}(y) = \pm 1\}$. The "trace 0" hyperplane: $H = \left\{x \in [\prod_\tau \mathbb{R}]^+ : \mathrm{Tr}(x) = 0\right\}$. We obtain the homomorphisms

$$\begin{array}{ccccc} & & \overset{\lambda}{\frown} & & \\ \mathcal{O}_\mathcal{K}^\times & \xrightarrow{j} & S & \xrightarrow{l} & H \end{array}$$

and the composite $\lambda := l \circ j : \mathcal{O}_\mathcal{K}^\times \to H$. Set $\Gamma = \lambda(\mathcal{O}_\mathcal{K}^\times) \leqslant H$, which is what we want to work with.

Theorem 5.37. *We have the exact sequence:*

$$1 \to \mu(\mathcal{K}) \to \mathcal{O}_\mathcal{K}^\times \xrightarrow{\lambda} \Gamma \to 0.$$

Lemma 5.38. Up to multiplication by units, there are only finitely many elements $\alpha \in \mathcal{O}_\mathcal{K}$ of given norm $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\alpha) = \alpha$.

Theorem 5.39. *The group Γ is a complete lattices in the $(r+s-1)$-dimensional vector space H and is therefore isomorphism to $\mathbb{Z}^{r+s-1}$.*

Corollary 5.40. $\mathcal{O}_\mathcal{K}^\times \cong \mu(\mathcal{K}) \times \mathbb{Z}^{r+s-1}$. In other words, there exists units $\varepsilon_1, \ldots, \varepsilon_{r+s-1}$, called fundamental units, such that any other unit ε can be written uniquely as a product $\varepsilon = \xi \varepsilon_1^{\nu_1} \cdots \varepsilon_{r+s-1}^{\nu_{r+s-1}}$, with a root of unity ξ.

Example 5.41. Let $\mathcal{K} = \mathbb{Q}(i)$. Then $r = 0$ and $s = 1$ and so $\mathcal{O}_\mathcal{K}^\times \cong \mu(\mathbb{Q}(i)) \times \mathbb{Z}^{1+0-1} \cong \mu(\mathbb{Q}(i))$. Since $\deg(\mathbb{Q}(i)/\mathbb{Q}) = 2$, any $\xi_p \in \mathcal{O}_\mathcal{K}^\times$ must have the minimal polynomial of degree at most 2. Note that $\{\pm 1, \pm i\} \subseteq \mathcal{O}_\mathcal{K}^\times$. Check explicitly that $\xi_3 \notin \mathbb{Z}[i]$. So $\mathcal{O}_\mathcal{K}^\times = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Example 5.42. Let $\mathcal{K} = \mathbb{Q}(\sqrt{2})$. Then $r = 2$ and $s = 0$ and so $\mathcal{O}_\mathcal{K}^\times \cong \mu(\mathbb{Q}(\sqrt{2})) \times \mathbb{Z}^{2+0-1} \cong \{\pm 1\} \times \mathbb{Z}$. Note $\varepsilon \in \mathcal{O}_\mathcal{K}^\times$ if and only if $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\varepsilon) = \pm 1$. Let $\epsilon = x + y\sqrt{2} \in \mathcal{O}_\mathcal{K}^\times$. Then there exists $\epsilon' \in \mathcal{O}_\mathcal{K}^\times$ such that $\varepsilon\varepsilon' = \pm 1$. Solve the equation $\pm 1 = \mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\varepsilon) = x^2 - 2y^2$. By inspection, we have $x = y = 1$ and so $\varepsilon = 1 + \sqrt{2}$. This is the "simplest" solution, up to sign, so it is fundamental and hence $\mathcal{O}_\mathcal{K}^\times \cong \pm(1+\sqrt{2})^\mathbb{Z}$. Suppose we didn't see the solution via inspection. Consider the equation $x^2 - 2y^2 = 1$. Use continued fractions to find a fundamental solution $x = 3, y = 2$. Then $u = 3 + 2\sqrt{2} \in \mathcal{O}_\mathcal{K}^\times$. Suppose there is an $\varepsilon = a + b\sqrt{2} \in \mathcal{O}_\mathcal{K}^\times$ with $\mathrm{N}_{\mathcal{K}/\mathbb{Q}}(\varepsilon) = -1$ and $\varepsilon^2 = 3 + 2\sqrt{2}$. Then we get $\epsilon = 1 + \sqrt{2}$ and so $\mathcal{O}_\mathcal{K}^\times \cong \pm(1+\sqrt{2})^\mathbb{Z} = \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}$.

5.5 Kummer's theorem

We will mostly prove the following theorem.

Theorem 5.43. *Let $p > 3$ with $p \nmid h_{\mathbb{Q}(\xi_p)}$. Then $x^p + y^p = z^p$ has no nontrivial solution with $p \nmid xyz$.*

Definition 5.44. The prime p with $p \nmid h_{\mathbb{Q}}(\xi_p)$ are called *regular prime.*

Remark (Conjecture)**.** There are infinitely many regular prime. In fact, most primes should be regular.

Theorem 5.45. *There are infinitely many irrgular primes.*

We will study $\mathbb{Q}(\xi_p)$.

Definition 5.46. The *cyclotomic units* of $\mathbb{Z}[\xi_p]$ are elements of the form $\frac{\xi_p^b-1}{\xi_p^a-1}$ with $p \nmid ab$.

Remark. Since $p \nmid ab$, there exists $c \in \mathbb{Z}$ such that $b \equiv ac \pmod p$. Then $\frac{\xi_p^b-1}{\xi_p^a-1} = \frac{\xi_p^{ac}-1}{\xi_p^a-1} = 1 + \xi_p^a + \cdots + \xi_p^{a(c-1)} \in \mathbb{Z}[\xi_p]$.

Remark. For $p \nmid ab$, $\left(\frac{\xi_p^b-1}{\xi_p^a-1}\right)^{-1} = \frac{\xi_p^a-1}{\xi_p^b-1} \in (\mathbb{Z}[\xi_p])^\times$. So the cyclotomic units form a subgroup of $\mathbb{Z}[\xi_p]$.

Lemma 5.47. For $p \nmid k$, $\langle 1 - \xi_p \rangle = \langle 1 - \xi_p^k \rangle$.

Proof. $\frac{1-\xi_p^k}{1-\xi_p} \in (\mathbb{Z}[\xi_p])^\times$. □

Lemma 5.48. The prime decomposition of $\langle p \rangle$ is $\langle 1 - \xi_p \rangle^{p-1}$, and hence $\langle 1 - \xi_p \rangle$ is prime in $\mathcal{O}_\mathcal{K}$.

Proof. Since $1 + x + \cdots + x^{p-1} = \Phi_p(x) = \prod_{j=1}^{p-1}(x - \xi_p^j)$, $p = \Phi_p(1) = \prod_{j=1}^{p-1}(1 - \xi_p^j)$. So $\langle p \rangle = \prod_{j=1}^{p-1}\langle 1 - \xi_p^j \rangle$. For $j = 1, \ldots, p-1$, since $p \nmid j$, by previous lemma, $\langle 1 - \xi_p \rangle = \langle 1 - \xi_p^j \rangle$. Hence $\langle p \rangle = \prod_{j=1}^{p-1}\langle 1 - \xi_p \rangle = \langle 1 - \xi_p \rangle^{p-1}$. Furthermore, since $[\mathcal{K} : \mathbb{Q}] = p - 1$, $\langle p \rangle$ can have at most $p - 1$ prime factors, thus in fact it is a prime decomposition, so we also get $\langle 1 - \xi_p \rangle \leqslant \mathcal{O}_\mathcal{K}$ is prime. □

Lemma 5.49. Suppose $\alpha = a_0 + a_1\xi_p + \cdots + a_{p-1}\xi_p^{p-1}$ with $a_i \in \mathbb{Z}$. If $a_i = 0$ for some $i = 1, \ldots, p-1$, then if there exists $n \in \mathbb{Z}$ such that $n \mid \alpha$, then $n \mid a_j$ for all $j = 1, \ldots, p-1$.

Proof. If $a_i = 0$ for some $i = 1, \ldots, p-1$, then let $\{1, \xi_p, \ldots, \widehat{\xi_p^i}, \ldots, \xi_p^{p-1}\}$ be a basis of $\mathbb{Z}[\xi_p]$. So α is written in terms of a basis and thus if $n \mid \alpha$, n divides all the coefficients. □

Lemma 5.50. Let $\alpha \in \mathbb{Z}[\xi_p]$. Then α^p is congruent to an element of $\mathbb{Z}$ modulo p.

Proof. Let $\alpha \in \mathbb{Z}[\xi_p]$ and write $\alpha = a_0 + a_1\xi_p + \cdots + a_{p-2}\xi_p^{p-2}$ with $a_i \in \mathbb{Z}$. Then $\alpha^p \equiv a_0^p + a_1^p\xi_p^p + \cdots + a_{p-2}^p\xi_p^{(p-2)p} \equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \pmod p$. □

Remark. Given any prime p, $\mathcal{K} = \mathbb{Q}(\xi_p) \subseteq \mathbb{C}$, but $\mathcal{K}$ is not contained in $\mathbb{R}$. For any $\sigma \in \mathrm{Gal}(\mathcal{K}/\mathbb{Q})$, σ never sends $\mathbb{Q}(\xi_p)$ into $\mathbb{R}$. Furthermore, one of the automorphisms in $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$ is the complex conjugation $c : \mathcal{K} \to \mathcal{K}$ with c fixing $\mathbb{Q}$, so $c \in \mathrm{Gal}(\mathcal{K}/\mathbb{Q})$ and $\mathcal{K}^+ := \mathcal{K}^{\langle c \rangle}$. Since the automorphisms have a group structure, we can pair each automorphism $\sigma \in \mathrm{Gal}(\mathcal{K}/\mathbb{Q})$ with its conjugate. Note that this is equivalent in pairing elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ with their additive inverse. However, there is a large subfield $\mathcal{K}^+ \in \mathbb{Q}(\xi_p)$ which sits insider of $\mathbb{R}$, properties of $\mathcal{K}$ and $\mathcal{K}^+$ gives us information on the number of independents of each field and relates the corresponding rings of integers $\mathcal{O}_\mathcal{K}$ and $\mathcal{O}_{\mathcal{K}^+}$ with the use of Dirichlet's Unit Theorem, stated below. Since $c^2 = 1$, $|\langle c \rangle| = 2$ and then $[\mathcal{K} : \mathcal{K}^+] = 2$.

Theorem 5.51 (Dirachlet's Unit Theorem)**.** *For any number field $\mathcal{K}$,* $\mathrm{rank}(\mathcal{O}_\mathcal{K}^\times) = r + s - 1$.

Theorem 5.52. *Let $p > 2$ and $\mathcal{K} = \mathbb{Q}(\xi_p)$. Then*

(a) $\mathcal{K}$ is totally complex field, i.e., $r = 0$ and $s = \frac{p-1}{2}$.

(b) The maximal totally real subfield of $\mathcal{K}$, i.e., the largest subfield fixed by complex conjugations is $\mathcal{K}^+ = \mathbb{Q}(\xi_p + \xi_p^{-1}) = \mathcal{K} \cap \mathbb{R}$. Furthermore, $\mathcal{O}_{\mathcal{K}^+} = \mathbb{Z}[\xi_p + \xi_p^{-1}]$ and $[\mathcal{K} : \mathcal{K}^+] = 2$.

(c) $\mathcal{K}$ and $\mathcal{K}^+$ have the same unit rank, i.e., $\mathcal{O}_\mathcal{K}^\times$ and $\mathcal{O}_{\mathcal{K}^+}^\times$ have the same rank. In particular, the embedding $\mathcal{O}_{\mathcal{K}^+} \hookrightarrow \mathcal{O}_\mathcal{K}^\times$ has finite index.

Proof. (a) Let $\sigma : \mathcal{K} \hookrightarrow \mathbb{C}$ be an embedding. Since all nontrivial p^{th} roots of unity are primitive, $\sigma(\xi_p) = \xi_p^k$ for some k with $p \nmid k$. Since $p > 2$, $\xi_p^k \notin \mathbb{R}$ for any k with $p \nmid k$. So $r = 0$ and $2s = p - 1$.

(b) Since the imaginary coefficients of ξ_p and ξ_p^{-1} are additive inverses, $\xi_p + \xi_p^{-1} \in \mathbb{R}$ and then $\mathbb{Q}(\xi_p + \xi_p^{-1}) \subseteq \mathcal{K}^+$. Since $x - \xi_p \notin \mathbb{Q}(\xi_p + \xi_p^{-1})[x]$ and ξ_p is a root of $f(x) = x^2 - (\xi_p + \xi_p^{-1})x + 1 \in \mathbb{Q}(\xi_p + \xi_p^{-1})[x]$, we have f is the minimal polynomial for ξ_p over $\mathbb{Q}(\xi_p + \xi_p^{-1}) = \mathcal{K}^+$ and so $[\mathcal{K} : \mathcal{K}^+] = 2$. Since $\mathcal{K}$ is not totally real, $\mathbb{Q}(\xi_p + \xi_p^{-1})$ must be the maximal real subfield in $\mathcal{K}$.

(c) By Dirichlet's Unit Theorem, $\mathrm{rank}_\mathbb{Z}(\mathcal{O}_\mathcal{K}{}^\times) = r + s - 1 = \frac{p-1}{2} - 1$. Furthermore, $[\mathcal{K}^+ : \mathbb{Q}] = \frac{[\mathcal{K}:\mathbb{Q}]}{[\mathcal{K}:\mathcal{K}^+]} = \frac{p-1}{2}$ and as $\mathcal{K}^\times$ is totally real, $\mathrm{rank}_\mathbb{Z}(\mathcal{O}_{\mathcal{K}^+}{}^\times) = r + s - 1 = [\mathcal{K}^+ : \mathbb{Q}] + 0 - 1 = \frac{p-1}{2} - 1$. □

Remark. Units in $\mathcal{O}_\mathcal{K}^\times$ can be easily described in terms of units in $\mathcal{O}_{\mathcal{K}^+}^\times$ since the maximal real subfield is rather large in such a manner that the index of the unit groups is finite. we show in the following Proposition that any unit of $\mathcal{K}$ can be decomposed into a product of p^{th} root of unity and a totally real unit in $\mathcal{O}_{\mathcal{K}^+}^\times$.

Proposition 5.53. For any $u \in \mathcal{O}_\mathcal{K}^\times$, there exist $v \in \mathcal{O}_\mathcal{K}^\times$ and $r \in \mathbb{Z}$ such that $u = \xi_p^r v$. In particular, this gives $[\mathcal{O}_\mathcal{K}^\times : \mathcal{O}_{\mathcal{K}^+}^\times] = p$.

Proof. Not given. □

Remark. Note $z^p = x^p + y^p = (x + y)(x + \xi_p y) \cdots (x + \xi_p^{p-1} y)$. Want to consider this in terms of ideals: $\langle z \rangle^p = \langle x + y \rangle \langle x + \xi_p y \rangle \cdots \langle x + \xi_p^{p-1} y \rangle$.

Lemma 5.54. Let (x, y, z) be a nontrivial solution to $x^p + y^p = z^p$. The ideals $\langle x + \xi_p^j y \rangle$ for $j = 0, \ldots, p - 1$ are either relatively prime (will be when $p \nmid xyz$) or have exactly one common factor $\langle 1 - \xi_p \rangle$ so that the ideals $\langle \frac{x + \xi_p^j y}{1 - \xi_p} \rangle$ for $j = 0, \ldots, p - 1$ are relatively prime.

Proof. Wlog., we can assume $\gcd(x,y,z)=1$. Suppose there exists $\mathfrak{p} \leqslant \mathbb{Z}[\xi_p]$ prime such that $\mathfrak{p} \mid \langle x+\xi_p^j y\rangle$ and $\mathfrak{p} \mid \langle x+\xi_p^j y\rangle$ for $0 \leqslant i \neq j \leqslant p-1$. Then $\mathfrak{p} \mid \langle x+\xi_p^i y\rangle - \langle x+\xi_p^j y\rangle$. Since $0 \leqslant i,j \leqslant p-1$ and $i \neq j$, $p \nmid i-j$ and $p \nmid j-i$. Also, since $\xi_p^i \in \mathbb{Z}[\xi_p]^\times$, $\mathfrak{p} \mid \langle x+\xi_p^i y\rangle - \langle x+\xi_p^j y\rangle = \langle \xi_p^i y - \xi_p^j y\rangle = \langle \xi_p^i(1-\xi_p^{j-i})y\rangle = \langle 1-\xi_p\rangle\langle y\rangle$. So $\mathfrak{p} \mid \langle 1-\xi_p\rangle$ or $\mathfrak{p} \mid \langle y\rangle$. Since $\xi_p^{j-i} \in \mathbb{Z}[\xi_p]^\times$, $\langle x+\xi_p^i y\rangle = \langle \xi_p^{j-i}\rangle\langle x+\xi_p^i y\rangle = \langle \xi_p^{j-i}x+\xi_p^j y\rangle$. So $\mathfrak{p} \mid \langle \xi_p^{j-i}x+\xi_p^j y\rangle - \langle x+\xi_p^j y\rangle = \langle 1-\xi_p\rangle\langle x\rangle$. Similarly, we have $\mathfrak{p} \mid \langle 1-\xi_p\rangle$ or $\mathfrak{p} \mid \langle x\rangle$. Hence either $\mathfrak{p} \mid \langle 1-\xi_p\rangle$ or $\mathfrak{p} \mid \langle x\rangle$ and $\mathfrak{p} \mid \langle y\rangle$. Since $\gcd(x,y)=1$, we get $\mathfrak{p} \mid \langle 1-\xi_p\rangle$. Also, since $\langle 1-\xi_p\rangle$ is prime, $\mathfrak{p} = \langle 1-\xi_p\rangle$. Furthermore, since $(x+\xi_p^{j+1}y) = (x+\xi_p^j y)+\xi_p^j(\xi_p-1)y$, if $\langle 1-\xi_p\rangle \mid \langle x+\xi_p^j y\rangle$, then $\langle 1-\xi_p\rangle \mid \langle x+\xi_p^{j+1}y\rangle$. Hence if $\langle 1-\xi_p\rangle$ is a factor of $\langle x+\xi_p^i y\rangle$ for one $i \in \mathbb{Z}$, then it is a factor of it for all $i \in \mathbb{Z}$. In particular, if $\langle 1-\xi_p\rangle$ is a common factor, then $x+\xi_p^0 y = x+y \equiv 0 \pmod{\langle 1-\xi_p\rangle}$. Since $1-\xi_p \mid x+y$, we have $\mathrm{N}(1-\xi_p) \mid \mathrm{N}(x+y)$, i.e., $p \mid (x+y)^p$. So $p \mid x+y$. So $z^p \equiv x^p+y^p \equiv (x+y)^p \equiv x+y \equiv 0 \pmod p$ and then $z \equiv 0 \pmod p$, i.e., $p \mid z$, i.e., $p \mid xyz$. If $p \nmid z$, then we've arrived at a contradiction and we are done and so $\langle x+\xi_p^j y\rangle$ for $j=0,\dots,p-1$ are relatively prime. Assume now $p \mid z$ and then we can assume $p \nmid y$, otherwise, $p \mid x$ since $p \mid x+y$, which is contradicted to $\gcd(x,y,z)=1$. Since $1-\xi_p \mid p \nmid y$, we have $(1-\xi_p)^2 \nmid (x+\xi_p^i y)$ for any $i \in \mathbb{Z}$. So $\langle 1-\xi_p\rangle^2 \nmid \langle x+\xi_p^i y\rangle$ for any $i \in \mathbb{Z}$. Thus, the ideals $\langle \frac{x+\xi_p^i y}{1-\xi_p}\rangle$ for $j=0,\dots,p-1$ are relatively prime. (Note $\langle x+\xi_p^j y\rangle$ and $\langle x+\xi_p^i y\rangle$ are both divisible by $\langle 1-\xi_p\rangle^2$.) □

Remark. New proof: If $p \nmid h_p$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\xi_p)) \to \mathrm{GL}_1$. If $p \mid h_p$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\xi_p)) \to \mathrm{GL}_2$.

Lemma 5.55 (Kummer's Lemma)**.** Suppose $p>3$ is a regular prime and $u \in \mathcal{O}_{\mathcal{K}}^\times$ satisfies u is congruent to an integer modulo p. Then u is a p^{th} power of an element in $\mathcal{O}_{\mathcal{K}}^\times$.

Theorem 5.56. *Let $p>3$ be regular. Then $x^p+y^p=z^p$ has no nontrivial integer solution with $p \nmid xyz$.*

Proof. We can assume if (x,y,z) is a solution, then $\gcd(x,y,z)=1$. Claim we can assume $x \not\equiv y \pmod p$. Suppose $x \equiv y \equiv -z \pmod p$. Then $z \equiv z^p \equiv x^p+y^p \equiv x+y \pmod p$. So $3z \equiv 0 \pmod p$ and then $p \mid 3$ or $p \mid z$, which is contradicted by $p>3$ and $p \nmid xyz$. We must have either $x \not\equiv y \pmod p$ or $y \not\equiv -z \pmod p$. Suppose $x \equiv y \pmod p$, then $y \not\equiv -z \pmod p$, i.e., $x \not\equiv -z \pmod p$. If (x,y,z) is a solution to $x^p+y^p=z^p$, then $x^p-z^p=-y^p$, i.e., $x^p+(-z)^p=(-y)^p$. So $(x,-z,-y)$ is a solution with the first two entries not congruent modulo p. Suppose we have a nontrivial solution with $p \nmid xyz$, then $\langle z\rangle^p = \langle x+y\rangle\langle x+\xi_p y\rangle\cdots\langle x+\xi_p^{p-1}y\rangle$. Since $p \nmid z$, by previous proof, the ideals $\langle x+\xi_p^j y\rangle$ are relatively prime. Since this decomposition is equal to the p^{th} power of the ideal generated by z, each $\langle x+\xi_p^j y\rangle$ for $j=1,\dots,p-1$ must be a power of an ideal I_i. Then $\langle x+\xi_p^j y\rangle = I_j^p$ for $j=0,\dots,p-1$. So $I_j^p \in \mathcal{P}_{\mathcal{K}}$ for $j=0,\dots,p-1$. Hence $I_j^p+\mathcal{P}_{\mathcal{K}}$ is the identity of $\mathrm{Cl}_{\mathcal{K}}$ for $j=0,\dots,p-1$ and then the order of $I_j+\mathcal{P}_{\mathcal{K}} \in \mathrm{Cl}_{\mathcal{K}}$ must divide p for $j=0,\dots,p-1$. Since p is regular, $p \nmid h_{\mathcal{K}} = |\mathrm{Cl}_{\mathcal{K}}|$ and the order of $I_j+\mathcal{P}_{\mathcal{K}}$ is 1 for $j=0,\dots,p-1$. So $I_j \in \mathcal{P}_{\mathcal{K}}$ for $j=0,\dots,p-1$. For $j=0,\dots,p-1$, write $I_j=\langle \alpha_j\rangle$ for some $\alpha_j \in \mathbb{Z}[\xi_p]$. Then $\langle x+\xi_p^j y\rangle = I_j^p = \langle \alpha_j^p\rangle$ for $j=0,\dots,p-1$. So for $j=0,\dots,p-1$, $x+\xi_p^j y = u_j\alpha_j^p$ for some $u_j \in \mathcal{O}_{\mathcal{K}}^\times$. For $j=0,\dots,p-1$, by previous proposition, we can write $u_j = \xi_p^{r_j} v_j$ for some $r_j \in \mathbb{Z}$ and $v_j \in \mathcal{O}_{\mathcal{K}^+}^\times$. For $j=0,\dots,p-1$, since $\alpha_j \in \mathbb{Z}[\xi_p]$, by previous lemma, such that $\alpha_j^p \equiv a_j \pmod p$ for some $a_j \in \mathbb{Z}$. Then for $j=0,\dots,p-1$, $x+\xi_p^j y = u_j\alpha_j^p = \xi_p^{r_j} v_j \alpha_j^p \equiv \xi_p^{r_j} v_j a_j \pmod p$. Also, for $j=0,\dots,j-1$, since $x,y \in \mathbb{Z}$ and $v_j \in \mathcal{O}_{\mathcal{K}^+}^\times \subseteq \mathcal{K}^+ \subseteq \mathbb{R}$,

$$x+\xi_p^{-j}y = \overline{x+\xi_p^j y} = \overline{\xi_p^{r_j} v_j \alpha_j^p} = \xi_p^{-r_j}\overline{v}_j\overline{\alpha}_j^p = \xi_p^{-r_j} v_j \overline{\alpha}_j^p \equiv \xi_p^{-r_j} v_j \bar{a}_j \equiv \xi_p^{-r_j} v_j a_j \pmod p,$$

i.e., $v_j a_j \equiv \xi_p^{r_j}(x+\xi_p^{-j}y) \pmod p$. So for $j=0,\dots,p-1$, $x+\xi_p^j y \equiv \xi_p^{r_j} v_j a_j \equiv \xi_p^{2r_j}(x+\xi_p^{-j}y) \pmod p$, i.e., $p \mid x + y\xi_p^j - x\xi_p^{2r_j} - y\xi_p^{2r_j-j}$. Actually, for $j=1,\dots,p-1$, we can find a contradiction and so let $1 \leqslant j \leqslant p-1$. If $1, \xi_p^j, \xi_p^{2r_j}, \xi_p^{2r_j-j}$ are distinct, then by previous lemma, $p \mid x$ and $p \mid y$, a contradiction. Since $0 < j < p$, $1 \neq \xi_p^j$ and $\xi_p^{2r_j} \neq \xi_p^{2r_j-j}$.

(a) Let $1 = \xi_p^{2r_j}$. Then $p \mid x + y\xi_p^j - x - y\xi_p^{-j} = y(\xi_p^j - \xi_p^{-j})$. So $p \mid y$, a contradiction.

(b) Let $\xi_p^j = \xi_p^{2r_j-j} = \xi_p^{2r_j}\xi_p^{-j}$. Since $p > 2$, $\xi_p^{2r_j} \neq 1$. Also, since $p \mid x - x\xi_p^{2r_j}$, we have $p \mid x$, a contradiction.

(c) Let $1 = \xi_p^{2r_j-j}$, then $\xi_p^j = \xi_p^{2r_j}$ and so $p \mid x-y+(y-x)\xi_p^j$. Then $p \mid x-y$, which is contradicted by $x \not\equiv y \pmod p$. □

Remark. What if $p \mid xyz$? By dividing out $\gcd(x,y,z)$, we can assume p only divides one of x, y, z. Claim. We can assume p only divide z. If (x_0, y_0, z_0) is a solution with $p \mid x_0$ and $p \nmid y_0 z_0$, then $x_0^p + y_0^p = z_0^p$, i.e., $(-z_0)^p + y_0^p = (-x_0)^p$. So $(x_1, y_1, z_1) = (-z_0, y_0, -x_0)$ is another solution with $p \mid z_1$ and $p \nmid x_1 y_1$.

Lemma 5.57. Let $\alpha \in \mathcal{O}_\mathcal{K} \smallsetminus \langle 1-\xi_p\rangle$. Then there exist l, a such that $\xi_p^l \alpha \equiv a \pmod{\langle 1-\xi_p\rangle^2}$.

Proof. Since $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\xi_p] = \mathbb{Z}[1-\xi_p]$, powers of $1-\xi_p$ form a $\mathbb{Z}$-basis. Then there exist $a_0, a_1 \in \mathbb{Z}$ such that $\alpha \equiv a_0 + a_1(1-\xi_p) \pmod{\langle 1-\xi_p\rangle^2}$. Since $\alpha \notin \langle 1-\xi_p\rangle$ and $1-\xi_p \mid p$, we have $a_0 \not\equiv 0 \pmod p$. So there exists $l \in \mathbb{Z}$ such that $a_1 \equiv a_0 l \pmod p$. Since $\xi_p = 1-(1-\xi_p)$, $\xi_p^l \equiv 1 - l(1-\xi_p) \pmod{\langle 1-\xi_p\rangle^2}$. Thus, since $1-\xi_p \mid p \mid a_1 - l a_0$,

$$\xi_p^l \alpha \equiv (1-l(1-\xi_p))\,(a_0 + a_1(1-\xi_p)) \equiv a_0 + (a_1 - l a_0)(1-\xi_p) \equiv a_0 \pmod{\langle 1-\xi_p\rangle^2}. \qquad \square$$

Theorem 5.58. *Let $p > 3$ be regular. Then $x^p + y^p = z^p$ with $p \mid z$ has no nontrivial solution.*

Proof. We prove a stronger statement: there are no nontrivial solutions to $x^p + y^p = u(1-\xi_p)^{kp} z_0^p = u\left((1-\xi_p)^k z_0\right)^p$, with $x, y, z_0 \in \mathcal{O}_\mathcal{K}$ relatively prime and $u \in \mathcal{O}_\mathcal{K}^\times$ and $k \geqslant 1$. In particular, let $u = 1$ and $z = p^j z_0$ with $p \nmid z_0$ and $j \geqslant 1$. Since $p = (1-\xi_p)^{p-1}$, letting $k = j(p-1)$, $z = p^j z_0 = (1-\xi_p)^{j(p-1)} z_0 = (1-\xi_p)^k z_0$. Suppose we have a solution (x, y, z_0), then $\langle u(1-\xi_p)^{kp} z_0^p\rangle = \langle x+y\rangle \cdots \langle x+\xi_p^{p-1}y\rangle$. Since $k > 0$ and $\langle 1-\xi_p\rangle$ is prime, $\langle 1-\xi_p\rangle \mid \langle x+\xi_p^j y\rangle$ for some j. By previous proof, $\langle 1-\xi_p\rangle \mid \langle x+\xi_p^i y\rangle$ for each i. By previous theorem, we also have $\langle \frac{x+\xi_p^j y}{1-\xi_p}\rangle$ for $j = 0, \dots, p-1$ are relatively prime. Since $1-\xi_p \mid p \nmid x$ and $1-\xi_p \mid p \nmid y$, $x, y \in \mathcal{O}_\mathcal{K} \smallsetminus \langle 1-\xi_p\rangle$. By previous lemma, there exist $l, j \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$ such that $\xi_p^l x \equiv a \pmod{\langle 1-\xi_p\rangle^2}$ and $\xi_p^j y \equiv b \pmod{\langle 1-\xi_p\rangle^2}$. Then $\xi_p^l x + \xi_p^j y \equiv a + b \pmod{\langle 1-\xi_p\rangle^2}$. Since $(\xi_p^l x)^p + (\xi_p^j y)^b = x^p + y^p = u\left((1-\xi_p)^k z_0\right)^p$, we have $(\xi_p^l x, \xi_p^j y, z_0)$ is a new solution. Replace (x, y, z_0) with $(\xi_p^l x, \xi_p^j y, z_0)$, we have $x + y \equiv a + b \pmod{\langle 1-\xi_p\rangle^2}$, i.e., $(1-\xi_p)^2 \mid (x+y) - (a+b)$. Since $1-\xi_p \mid x + \xi_p^0 y = x + y$, we have $1-\xi_p \mid a+b$. Then like before, since $a+b \in \mathbb{Z}$, we have $p \mid a+b$ and then $\langle 1-\xi_p\rangle^p = \langle p\rangle \mid \langle a+b\rangle$. Since $p > 2$, $(1-\xi_p)^2 \mid a+b$ and so $(1-\xi_p)^2 \mid x+y$. If $k = 1$, then $1-\xi_p \mid z_0$. But since $1-\xi_p \mid p \nmid z_0$, $1-\xi_p \nmid z_0$, a contradiction. Our goal now is to apply infinite descent to the power k. We just showed $k \geqslant 2$. Pick our solution to have the minimum k. Then we will construct a new solution with a smallest k, giving the contradiction. Since $\langle \frac{x+\xi_p^j y}{1-\xi_p}\rangle$ for $j = 0, \dots, p-1$ are relatively prime and $\langle 1-\xi_p\rangle^2 \mid \langle x+y\rangle$, $\langle 1-\xi_p\rangle \mid\mid \langle x+\xi_p^j y\rangle$ for $j = 1, \dots, p-1$. So $\langle 1-\xi_p\rangle^{p-1} \mid\mid \langle x+\xi_p y\rangle \cdots \langle x+\xi_p^{p-1} y\rangle$.

Also, $\langle 1-\xi_p\rangle^{kp} \mid\mid \langle z^p\rangle = \langle x^p+y^p\rangle$. So $\langle 1-\xi_p\rangle^{kp-p+1} \mid\mid \langle x+y\rangle$, i.e., $\langle 1-\xi_p\rangle^{(k-1)p} \mid\mid \langle \frac{x+y}{1-\xi_p}\rangle$. Consider

$$\langle (1-\xi_p)^{k-1}z_0\rangle^p = \langle \frac{x+y}{1-\xi_p}\rangle \cdots \langle \frac{x+\xi_p^{p-1}y}{1-\xi_p}\rangle.$$

Since $\langle \frac{x+\xi_p^{p-1}y}{1-\xi_p}\rangle$ for $j=0,\ldots,p-1$ are relatively prime, the same argument as in previous version of Kummer's theorem (put where we have $p \nmid h_{\mathcal{K}}$) gives each ideal is the p^{th} power of a primitive ideal. So for $j=0,\ldots,p-1$, there exists $\alpha_j \in \mathcal{O}_{\mathcal{K}}$ and $u_j \in \mathcal{O}_{\mathcal{K}}^{\times}$ such that $\frac{x+\xi_p^y}{1-\xi_p} = u_j\alpha_j^p$. Since $\alpha_0^p,\ldots,\alpha_{p-1}^p$ are relatively prime, $\alpha_0,\ldots,\alpha_{p-1}$ are relatively prime. Since $\langle 1-\xi_p\rangle \mid\mid \langle x+\xi_p^j y\rangle$ for $j=1,\ldots,p-1$, we have $1-\xi_p \nmid \alpha_j$ for $j=1,\ldots,p-1$. Also, since $1-\xi_p \nmid z_0$, $\langle 1-\xi_p\rangle^{k-1} \mid\mid \langle \alpha_0\rangle$. So we can write $\alpha_0 = (1-\xi_p)^{k-1}\beta$ with $1-\xi_p \nmid \beta$. Since

$$y = \frac{(x+y)-(x+\xi_p y)}{1-\xi_p} = \frac{x+y}{1-\xi_p} - \frac{x+\xi_p y}{1-\xi_p} = u_0\alpha_0^p - u_1\alpha_1^p = u_0(1-\xi_p)^{(k-1)p}\beta^p - u_1\alpha_1^p,$$

and

$$y = \frac{(x+\xi_p^{-1}y)-(x+y)}{\xi_p^{-1}(1-\xi_p)} = \xi_p\left(\frac{x+\xi_p^{-1}y}{1-\xi_p} - \frac{x+y}{1-\xi_p}\right) = \xi_p u_{p-1}\alpha_{p-1}^p - \xi_p u_0(1-\xi_p)^{(k-1)p}\beta^p,$$

we have $u_1\alpha_1^p + \xi_p u_{p-1}\alpha_{p-1}^p = (1+\xi_p)u_0(1-\xi_p)^{(k-1)p}\beta^p$, i.e., $\alpha_1^p + \frac{\xi_p u_{p-1}}{u_1}\alpha_{p-1}^p = \frac{(1+\xi_p)u_0}{u_1}(1-\xi_p)^{(k-1)p}\beta^p$. Since $1+\xi_p = \frac{1-\xi_p^2}{1-\xi_p}$, $1+\xi_p \in \mathcal{O}_{\mathcal{K}}^{\times}$. So $v := \frac{\xi_p u_{p-1}}{u_1} \in \mathcal{O}_{\mathcal{K}}^{\times}$ and $\tilde{v} := \frac{(1+\xi_p)u_0}{u_1} \in \mathcal{O}_{\mathcal{K}}^{\times}$. Then $\alpha_1^p + v\alpha_{p-1}^p = \tilde{v}(1-\xi_p)^{(k-1)p}\beta^p$. Since $p \mid (1-\xi_p)^{p-1}$, $\alpha_1^p + v\alpha_{p-1}^p \equiv 0 \pmod p$. Then there exist $a_1, a_{p-1} \in \mathbb{Z}$ such that $\alpha_1^p \equiv a_1 \pmod p$ and $\alpha_{p-1}^p \equiv a_{p-1} \pmod p$. So $a_1 + va_{p-1} \equiv 0 \pmod p$. Since $p \nmid \alpha_{p-1}$, $p \nmid a_{p-1}$. Also, since $a_1 \in \mathbb{Z}$, $v \equiv b \pmod p$ for some $b \in \mathbb{Z}$. By Kummer's Lemma, $v = w^p$ for some $w \in \mathcal{O}_{\mathcal{K}}^{\times}$. Set $x' = \alpha_1$ and $y' = w\alpha_{p-1}$ and $z_0' = \beta$. Then $x'^p + y'^p = \tilde{v}(1-\xi_p)^{(k-1)p}z_0'^p$. This contradicts the minimality of k and gives an contradiction. $\square$

Chapter 6

Zeta Functions and L-series

6.1 Riemann Zeta function

Definition 6.1. Define the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$, where $s = \sigma + it \in \mathbb{C}$.

Remark. Consider $\zeta(s)$ on $\mathbb{R}$. Then

- $\zeta(1)$ is not defined since it is the divergent harmonic series.
- $\zeta(\sigma)$ converges for $\sigma \in \mathbb{R}_{>1}$. ($p$-series)
- $\zeta(\sigma)$ diverges for $\sigma \in \mathbb{R}_{<1}$. ($p$-series)

Remark. For $r \in \mathbb{R} \setminus 0$, since $\operatorname{Arg}(r) = 0$, we have

$$\left|\frac{1}{r^s}\right| = \left|\frac{1}{e^{s\operatorname{Log}(r)}}\right| = \frac{1}{\left|e^{s(\ln|r| + i\operatorname{Arg}(r))}\right|} = \left|\frac{1}{e^{(\sigma+it)\ln|r|}}\right| = \frac{1}{e^{\sigma\ln|r|}} = \frac{1}{|r|^{\sigma}}.$$

Theorem 6.2. *$\zeta(s)$ converges absolutely for $\operatorname{Re}(s) > 1$ and uniformly on $\operatorname{Re}(s) \geqslant 1 + \delta$ for any $\delta \in \mathbb{R} -> 0$.*

Proof. Apply Weierstrass's M-test with $M_n = \frac{1}{n^{1+\delta}}$. □

Remark. From calculus, given $f(x)$ that is infinitely many differentiable at a point $x = a$, then we have a taylor series $f(x) = \sum_{n=0}^{\infty} a_n(x-a)^n$ that converges for some $x \in B_\delta(a)$.

Definition 6.3. A zero of a function $f(x)$ is a value such that $f(a) = 0$. If z_0 is a zero of $1/f$, then it is a pole of f.

Definition 6.4. A function f is *meromorphic* in a $B_\delta(z_0) \subseteq \mathbb{C}$ if either f or $1/f$ is holomorphic in some $B_\delta(z_0)$.

Definition 6.5. If f is a function that is meromorphic in $B_\delta(z_0) \subseteq \mathbb{C}$, then there exists $n \in \mathbb{N}$ such that $\frac{f(z)}{(z-z_0)^n}$ is holomorphic and nonzero in a neighborhood of z_0.

(a) If $n > 0$, then z_0 is a zero of order (or multiplicity) n.

(b) If $n < 0$, then z_0 is a pole of order $|n|$.

Simple zero and simple pole are zeroes and poles of order 1.

Theorem 6.6. *In $B_\delta(z_0)$, a nonzero meromorphic function f can be written as a Laurent series*

$$f(z) = \sum_{k=-n} a_k(z - z_0)^k \text{ for some } n \in \mathbb{Z} \text{ and } a_{-n} \neq 0.$$

(a) If $n > 0$, z_0 is a pole of order n and the residue at $z = z_0$ is a_{-1}.

(b) If $n < 0$, z_0 is a zero of order $|n|$.

Remark. In complex analysis, analytic continuation is a technique to extend the domain of a given analytic function. Analytic continuation oftn succeeds in defining further values of a function, for example in a new region where an infinite series representation in terms of which it is initially defined becomes divergent.

Definition 6.7. Given a function f that is analytic on some domain $S \subseteq \mathbb{C}$, we say g is the *analytic continuation* of f to $R \supseteq S$ (really just need $R \cap S$ contains an open ball) if g is analytic on R and $g|_{R\cap S} = f$.

Definition 6.8. Let σ_0 be the smallest real number for which the series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges for $\mathrm{Re}(s) > \sigma_0$. The number σ_0 is called the abscissa of convergence.

Remark (Partial summation)**.** Let $\{a_n\}_{n\geqslant 1}$ and $\{b_n\}_{n\geqslant 1}$ be two sequences. Let $A_m = \sum_{k=0}^{m} a_k$. Then since $a_0 = A_0$, $\sum_{k=0}^{N} a_k b_k = a_0 b_0 + \sum_{k=1}^{N}(A_k - A_{k-1})b_k = A_N b_N + \sum_{k=0}^{N-1} A_k(b_k - b_{k+1})$. So for $n \geqslant m$, we have $\sum_{k=m+1}^{n} a_k b_k = A_n b_n - A_m b_m + \sum_{k=m}^{n-1} A_k(b_k - b_{k+1})$.

Theorem 6.9. *Let $A_n = \sum_{k=1}^{n} a_k$. Assume there exist $c, \sigma_1 \in \mathbb{R}_{>0}$ so that $|A_n| \leqslant cn^{\sigma_1}$ for any $n \in \mathbb{N}$. Then the abscissa of convergence $\sigma_0 \leqslant \sigma_1$.*

Proof. Set $P_n(s) = \sum_{k=1}^{n} \frac{a_k}{k^s} = \sum_{k=1}^{n} a_k k^{-s}$, assume $n \geqslant m$, then

$$\begin{aligned} P_n(s) - P_m(s) &= A_n n^{-s} - A_m m^{-s} + \sum_{k=m}^{n-1} A_k \left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right) \\ &= \frac{A_n}{n^s} - \frac{A_m}{m^s} + \sum_{k=m}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}} dx. \end{aligned}$$

Let $\delta > 0$. Then for $\mathrm{Re}(s) \geqslant \sigma_1 + \delta$, we have for $k \in \mathbb{N}$,

$$\left| A_k \int_k^{k+1} \frac{1}{x^{s+1}} dx \right| \leqslant ck^{\sigma_1} \int_k^{k+1} \left| \frac{1}{x^{s+1}} \right| dx = ck^{\sigma_1} \int_k^{k+1} \frac{1}{x^{\sigma+1}} dx = \frac{ck^{\sigma_1}}{\sigma} \left(\frac{1}{k^\sigma} - \frac{1}{(k+1)^\sigma}\right).$$

So

$$\begin{aligned}|P_n(s)-P_m(s)| &\leqslant \frac{|A_n|}{|n^s|}+\frac{|A_m|}{|m^s|}+\sum_{k=m}^{n-1}|s|\left|A_k\int_k^{k+1}\frac{1}{x^{s+1}}dx\right| \\ &\leqslant \frac{cn^{\sigma_1}}{n^\sigma}+\frac{cm^{\sigma_1}}{m^\sigma}+\sum_{k=m}^{n-1}|s|\frac{ck^{\sigma_1}}{\sigma}\left(\frac{1}{k^\sigma}-\frac{1}{(k+1)^\sigma}\right) \\ &\leqslant \frac{c}{n^{\sigma-\sigma_1}}+\frac{c}{m^{\sigma-\sigma_1}}+\frac{c|s|}{\sigma}\sum_{k=m}^{n-1}\left(\frac{1}{k^{\sigma-\sigma_1}}-\frac{1}{(k+1)^{\sigma-\sigma_1}}\left(\frac{k}{k+1}\right)^{\sigma_1}\right).\end{aligned}$$

If $\sigma>\sigma_1$, this can be made arbitrarily small by choosing m,n large. Thus, we have the result. □

Theorem 6.10. *$\zeta(s)$ has analytic continuation to $\mathrm{Re}(s)>0$ except for a simple pole at $s=1$ with residue 1.*

Proof. The previous theorem gives the abscissa of convergence is 1. For $n\in\mathbb{N}$ and $s\in\mathbb{R}_{>1}$, we have $\int_n^{n+1}\frac{1}{x^s}dx\leqslant\frac{1}{n^s}\leqslant\int_{n-1}^n\frac{1}{x^s}dx$. So

$$\frac{1}{s-1}=\int_1^\infty\frac{1}{x^s}dx\leqslant\zeta(s)\leqslant 1+\sum_{n=2}^\infty\int_{n-1}^n\frac{1}{x^s}dx=1+\sum_{n=1}^\infty\int_n^{n+1}\frac{1}{x^s}dx=1+\frac{1}{s-1},$$

i.e., $1\leqslant(s-1)\zeta(s)\leqslant s$. Once we prove that $\zeta(s)$ has analytic continuation to $\sigma>0$ except a possible pole at $s=1$, this equality shows it has a single pole at $s=1$ of residue 1. Set $\zeta_2(s)=\sum_{n=1}^\infty(-1)^{n+1}n^{-s}$. Let $a_n=(-1)^{n+1}$ for any $n\in\mathbb{N}$ and $A_n=\sum_{i=1}^n a_i$. Then $|A_n|\leqslant 1$. By previous theorem, $\zeta_2(s)$ is analytic for $\sigma>0$ (right half plane). Note $\frac{2}{2^s}\zeta(s)+\zeta_2(s)=\zeta(s)$. So $\zeta_2(s)=\left(1-\frac{1}{2^{s-1}}\right)\zeta(s)$. This gives the only possible pole of $\zeta(s)$ are when $2^{s-1}=1$, i.e., $s=\frac{2\pi in}{\ln 2}+1$. Set

$$\zeta_r(s)=\sum_{n=1}^\infty(-1)^{n+1}\sum_{j=(n-1)(r-1)+1}^{n(r-1)}\frac{1}{j}.$$

Let $a_n=1$ if $\lfloor n/r\rfloor$ is even and $a_n=-1$ otherwise, for any $n\in\mathbb{N}$ and $A_n=\sum_{i=1}^n a_i$. Then $|A_n|\leqslant r$. By previous theorem, $\zeta_r(s)$ is analytic for $\mathrm{Re}(s)>0$ (right half plane). Note that $\frac{r}{r^s}\zeta(s)+\zeta_r(s)=\zeta(s)$. So $\zeta_r(s)=\left(1-\frac{1}{r^{s-1}}\right)\zeta(s)$. This gives the only possible pole of $\zeta(s)$ are when $r^{s-1}=1$, i.e., the only poles are $s=\frac{2\pi ir}{\ln 3}+1$. The only pole of $\zeta(s)$ with $s\neq 1$ gives $2^m=r^n$ for $r\geqslant 3$ and for some $m,n\in\mathbb{N}$, a contradiction. Thus, $s=1$ is the only pole of $\zeta(s)$. □

Theorem 6.11. *For $\mathrm{Re}(s)>1$, one has Euler product $\zeta(s)=\prod_p\frac{1}{1-p^{-s}}=E(s)$.*

Proof. Let $\{a_n\}_{n\geqslant 1}\subseteq\mathbb{C}$ be a sequence. We say $\prod_{n=1}^\infty a_n$ converges if $\prod_{i=1}^n a_i$ has nonzero limit. This is the case if and only if the series $\sum_{n=1}^\infty\mathrm{Log}\,a_n$ converges. The product is called absolutely convergent if the series converges absolutely. In this case the product converges to the same limit even after a reordering of its terms a_n. Observe if $\mathrm{Re}(s)=\sigma\geqslant 1+\delta$ for some $\delta>0$, then

$$\begin{aligned}|\mathrm{Log}\,E(s)| &= \left|\sum_p\sum_{n=1}^\infty\frac{1}{np^{ns}}\right|\leqslant\sum_p\sum_{n=1}^\infty\frac{1}{np^{n\sigma}}\leqslant\sum_p\sum_{n=1}^\infty\frac{1}{p^{n\sigma}} \\ &\leqslant\sum_p\sum_{n=1}^\infty\left(\frac{1}{p^{1+\delta}}\right)^n=\sum_p\frac{1}{p^{1+\delta}-1}\leqslant 2\sum_p\frac{1}{p^{1+\delta}}.\end{aligned}$$

So $\operatorname{Log} E(s)$ and thus $E(s)$ converges absolutely for $\operatorname{Re}(s) \geqslant 1+\delta$. Let $N \in \mathbb{N}$. For all prime $p_1, \ldots, p_r \leqslant N$, write $\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \cdots$. Then

$$\prod_{p \leqslant N} \frac{1}{1-p^{-s}} = \sum_{\nu_1, \ldots, \nu_r = 0}^{\infty} \frac{1}{(p_1^{\nu_1} \cdots p_r^{\nu_r})^s} = \sum_n{}' \frac{1}{n^s},$$

where $\sum'$ denotes the sum over all natural numbers which are divisible only by prime numbers $p \leqslant N$. Since for any $n \leqslant N$, n must be divisible only by prime $p \leqslant N$, we have

$$\prod_{p \leqslant N} \frac{1}{1-p^{-s}} = \sum_{n \leqslant N} \frac{1}{n^s} + \sum_{n > N}{}' \frac{1}{n^s}.$$

So

$$\left| \prod_{p \leqslant N} \frac{1}{1-p^{-s}} - \zeta(s) \right| \leqslant \left| \sum_{n > N, p_i | n} \frac{1}{n^s} \right| \leqslant \sum_{n > N} \frac{1}{n^{1+\delta}},$$

where the right hand side goes to zero as $N \to \infty$. □

Definition 6.12. For $\operatorname{Re}(s) > 0$, define the gamma function

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}.$$

Proposition 6.13. (a) $\Gamma(s)$ is analytic on $operatorname Re(s) > 0$ and has meromorphic continuation to all of $\mathbb{C}$.

(b) $\Gamma(s) \neq 0$ on $\operatorname{Re}(s) > 0$ and has simple poles at $s = -n$ for all $n \in \mathbb{Z}_{\leqslant 0}$ with resiude $\frac{(-1)^n}{n!}$. These are the only poles.

(c) It satisfies functional equations

(1) $\Gamma(s+1) = s\Gamma(s)$,

(2) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$,

(3) $\Gamma(s)\Gamma(s+1/2) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s)$. (Legendre's duplication formula)

(4) It has the special values $\Gamma(1/2) = \sqrt{\pi}$, $\Gamma(1) = 1$ and $\Gamma(k+1) = k!$ for any $k \in \mathbb{N}$.

Remark. Under which conditions, integrals and sums can be interchanged? This is given by a special case of Fubini's theorem.

Theorem 6.14. *Suppose $f_n \in L^1(\mathbb{R})$ for all $n \in \mathbb{Z}$ and that $f_n(t) \in l^1$ for all $t \in \mathbb{R}$. If either*

$$\int_{\mathbb{R}} \sum_{n \in \mathbb{Z}} |f_n(t)| dt < \infty \text{ or } \sum_{n \in \mathbb{Z}} \int_{\mathbb{R}} |f_n(t)| dt < \infty,$$

then

$$\int_{\mathbb{R}} \sum_{n \in \mathbb{Z}} |f_n(t)| dt = \sum_{n \in \mathbb{Z}} \int_{\mathbb{R}} |f_n(t)| dt.$$

Remark. To relate the gamma function to the zeta function, start with the substitution $y \mapsto \pi n^2 y$, which gives

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Then

$$\pi^{-s}\Gamma(s)\zeta(2s) = \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Since

$$\sum_{n=1}^\infty \int_0^\infty \left| e^{-\pi n^2 y} y^s \right| \frac{dy}{y} = \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^{\operatorname{Re}(s)} \frac{dy}{y} = \pi^{-\operatorname{Re}(s)}\Gamma(\operatorname{Re}(s))\zeta(2\operatorname{Re}(s)) < \infty,$$

we have

$$\pi^{-s}\Gamma(s)\zeta(2s) = \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y} = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 y} y^s \frac{dy}{y}.$$

Note $g(y) = \sum_{n=1}^\infty e^{-\pi n^s y}$ aries from Jacobi's classical theta series

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z} = 1 + 2\sum_{n=1}^\infty e^{\pi i n^2 z},$$

i.e., we gave $g(y) = \frac{1}{2}(\theta(iy) - 1)$.

Remark. Let $\vartheta(z) = \theta(2z) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 z}$. Then for any

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod 4 \right\},$$

and for any $z \in \mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$, one has the formula $\vartheta\left(\frac{az+b}{cz+d}\right) = j(\gamma, z)\vartheta(z)$, where $j(\gamma, z) = \left(\frac{c}{d}\right)\varepsilon_d^{-1}(cz+d)^{1/2}$, where

$$\left(\frac{c}{d}\right) = \begin{cases} -\left(\frac{c}{|d|}\right) & \text{if } c < 0, d < 0 \\ \left(\frac{c}{|d|}\right), & \text{otherwise} \end{cases}, \quad \varepsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4 \\ i & \text{if } d \equiv 3 \pmod 4 \end{cases}.$$

So Jacobi's theta function $\vartheta(z)$ is an example of a modular form of weight $1/2$ for the group $\Gamma_0(4)$.

Definition 6.15. Define the completed Riemann function as $\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$.

Remark. The completed Riemann function implies $\zeta(s) = 0$ whenever $\Gamma(s/2)$. Since $\Lambda(s)$ has simple poles only at $s = 0, 1$ and Γ has simple poles at $s = -n$ for all $n \in \mathbb{Z}_{\leqslant 0}$, we have $\zeta(s/2)$ must have zero at $s/2 = -n$ for all $n \in \mathbb{Z}_{\leqslant -1}$, i.e., $\zeta(s)$ must have zero at all $-2\mathbb{Z} \smallsetminus \{0\}$. These are the "trivial zeros of $\zeta(s)$".

Theorem 6.16. *The function $\Lambda(s)$ has analytic continuation to $\mathbb{C}$ except for simple poles at $s = 0$ and $s = 1$ with residue -1 and 1. It satisfies a functional equation $\Lambda(s) = \Lambda(1-s)$, i.e., $\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s)$.*

Remark. All our L-functions will have

- momermorphic function,
- Euler product,
- functional equation.

Remark. By Euler product, $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$. Then by functional equation, $\zeta(s) \neq 0$ for $s < 0$ except for $n \in -2\mathbb{Z} \setminus \{0\}$, we have other zeros have to lie in the critical strip $0 \leqslant \mathrm{Re}(s) < 1$.

Remark (Riemann Hypothesis)**.** All the nontrivial zeroes of $\zeta(s)$ satisfies $\sigma = 1/2$.

Definition 6.17. Define the *Bernoulli number* as B_k, where $\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$.

Remark. $B_{2k+1} = 0$ for all $k \in \mathbb{N}$. $B_0 = 1$, $B_2 = 1/6$, $B_4 = -1/30$ and $B_6 = 1/42$.

Theorem 6.18. *For every $k \in \mathbb{N}$, $\zeta(1-k) = -\frac{B_k}{k}$.*

Corollary 6.19. For every $k \in \mathbb{N}$, $\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}$.

Remark. The values $\zeta(2k-1)$ for $k \in \mathbb{Z}_{\geqslant 2}$ forms a higher K-groups $K_i(\mathbb{Z})$ from algebraic K-theory, which take the lead. In fact one has a mysterious canonical isomorphism $r : K_{4k-1}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\cong} \mathbb{R}$. The image R_{2k} of a nonzero element in $K_{4k-1} \otimes_{\mathbb{Z}} \mathbb{Q}$ is called the $2k^{\text{th}}$ regulator. It is well-determined up to a rational factor, i.e., it is an element of $R^*/\mathbb{Q}*$, and one has $\zeta(2k-1) \equiv R_{2k} \pmod{\mathbb{Q}}^*$. This is part of the Beilinson-Bloch conjecture.

Theorem 6.20. *$p \mid h_{\mathbb{Q}(\xi_p)}$ if and only if $p \mid B_j$ for some $j = 2, 4, \ldots, p-3$.*

Chapter 7

Finite Fields

Theorem 7.1. *For a prime p and a monic irreducible $f \in \mathbb{F}_p[x]$ of degree n, the ring $\mathbb{F}_p[x]/\langle f\rangle$ is a field of order p^n.*

Proof. The cosets modulo f are represented by remainders $c_0 + \cdots + c_{n-1}x^{n-1}$ with $c_0, \ldots, c_{n-1} \in \mathbb{F}_p$. Note there are p^n remainders. Since $\mathbb{F}_p[x]$ is a UFD and f is irreducible, we have f is prime and then $\langle f\rangle$ is a prime ideal. Since $\mathbb{F}_p[x]$ is a PID, $\langle f\rangle$ is maximal ideal and then $\mathbb{F}_p[x]/\langle f\rangle$ is a field. □

Remark. We will see that every finite field is isomorphic to a field of the form $\mathbb{F}_p[x]/\langle f\rangle$. However, not every finite field is literally of the form $\mathbb{F}_p[x]/\langle f\rangle$. For instance, $\mathbb{Z}[\sqrt{2}]/\langle 3\rangle$ is another field of size 9, which is isomorphic to $\mathbb{F}_3[x]/\langle x^2 - 2\rangle = \mathbb{F}_3[x]/\langle x^2 + 1\rangle$.

Remark. For a finite field, the multiplicative group $F^\times$ is cyclic but the additive group of F is usually not cyclic. When F contains $\mathbb{F}_p$, since $p = 0$ in $\mathbb{F}_p$, every nonzero element of F has additive order p, so $F = \mathbb{F}_{p^r}$ is not additively cyclic unless $r = 1$.

Theorem 7.2. *Every finite field is isomorphic to $\mathbb{F}_p[x]/\langle f\rangle$ for some prime p and some monic irreducible $f \in \mathbb{F}_p[x]$.*

Proof. Let F be a finite field. Then F has order p^n for some $n \in \mathbb{N}$, there is a field embedding $\mathbb{F}_p \hookrightarrow F$ and $F^\times$ is cyclic. Let $F^\times = \langle\gamma\rangle$. Define an evaluation at γ: $\mathrm{evl}_\gamma : \mathbb{F}_p[x] \to F$ given by $f(x) \mapsto f(\gamma)$. Then evl_γ is a ring homomorphism that fixes $\mathbb{F}_p$. Since $\mathrm{evl}_\gamma(0) = 0$ and for any $t \in F \setminus \{0\}$, t is a power of γ, evl_γ is onto. So $\mathbb{F}_p[x]/\operatorname{Ker}(\mathrm{evl}_\gamma) \cong F$. Since $\mathbb{F}_p[x]$ is a PID and F is field, $\operatorname{Ker}(\mathrm{evl}_\gamma) = \langle g\rangle$ for some monic irreducible $g \in \mathbb{F}_p[x]$. □

7.1 Finite fields as splitting fields

Lemma 7.3. A field of prime power order p^n is a splitting field over $\mathbb{F}_p$ of $x^{p^n} - x$.

Proof. Let F be a field of order p^n. From the proof of previous theorem, F contains a subfield isomorphic to $\mathbb{Z}/\langle p\rangle = \mathbb{F}_p$. Explicitly, the subring of F generated by 1 is a field of order p. Since $|F^\times| = p^n - 1$, $t^{p^n-1} = 1$ for any $t \in F^\times$. So $t^{p^n} = t$ for any $t \in F$. Since the polynomial $x^{p^n} - x$ has every element of F as a distinct root, F is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. □

Theorem 7.4. *For every prime power p^n, a field of order p^n exists.*

Proof. Let F be a field extension of $\mathbb{F}_p$ over which $x^{p^n} - x$ splits completely. Inside F, the roots of $x^{p^n} - x$ form the set $S = \{t \in F : t^{p^n} = t\}$. Since $x^{p^n} - x$ is separable, $|S| = p^n$. Since S is a subfield of F, S is a field of order p^n. □

Theorem 7.5. *Any irreducible $f(x)$ in $\mathbb{F}_p[x]$ of degree n divides $x^{p^n} - x$ and is separable.*

Proof. Since the field $\mathbb{F}_p[x]/\langle f\rangle$ has order p^n, $t^{p^n} = t$ for any $t \in \mathbb{F}_p[x]/\langle f\rangle$. In particular, $x^{p^n} \equiv x \pmod f$, so $f \mid (x^{p^n} - x)$ in $\mathbb{F}_p[x]$. Since $x^{p^n} - x$ is separable in $\mathbb{F}_p[x]$, its factor f is separable. □

Remark. For finite field $\mathbb{F}_{p^n}$,

- it contains a unique subfield isomorphic to $\mathbb{F}_p$;
- $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$;
- it is a splitting field of $x^{p^n} - 1$.

Remark. Although $x^{p^n} - x$ has degree p^n, its splitting field over $\mathbb{F}_p$ has degree n, not p^n since $x^{p^n} - x$ is reducible.

Theorem 7.6. *Any finite fields of the same size are isomorphic.*

Proof. Follow from that any two splitting fields are isomorphic. □

Theorem 7.7. *For each $d \mid n$, $\mathbb{F}_{p^n}$ has a subfield $\mathbb{F}_{p^d}$.*

Chapter 8

Rings

Let R be a ring.

Definition 8.1. Let $I, J \leqslant R$. The sum of I and J is the ideal $I + J = \{x + y, x \in I, y \in J\}$. If I and J are right (respectively left) ideals, so is their sum.

Definition 8.2. Let R be a commutative ring with identity. $I, J \leqslant R$ are relatively prime (coprime) if $I + J = R$.

Lemma 8.3. Let R be a commutative ring with identity. If $I, J \leqslant R$ and $I + J = R$, then $IJ = I \cap J$.

Proof. Clearly, $IJ \subseteq I \cap J$. Suppose $u \in I \cap J$. Since $I + J = (1) = R$, there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Since R is commutative, $u = u(i + j) = ui + uj = iu + uj \in IJ$. □

Lemma 8.4. Let $I, J \leqslant R$ be two distinct maximal ideals, then I, J are coprime, i.e., $I + J = R$.

Proof. Note $I + J$ is also a maximal ideal. Since $I \neq J$, $I \subsetneq I + J \subseteq R$. Since I is maximal, $I + J = R$. □

Definition 8.5. If $a, b \in R$ and $I \leqslant R$, we say a is congruent to b modulo I if $a - b \in I$.

Theorem 8.6 (Chinese Remainder Theorem)**.** *Let R be a ring with 1 and $I_1, \ldots, I_n \leqslant R$ such that $I_i + I_j = R$ for any $i \neq j$.*

(a) Let $a_1, \ldots, a_n \in R$. Then there exists $a \in R$ such that $a \equiv a_i \pmod{I_i}$ for $i = 1, \ldots, n$.

(b) Let $b \in R$ and a be given from (1). Then $b \equiv a_i \pmod{I_i}$ for $i = 1, \ldots, n$ if and only if $b \equiv a \pmod{\bigcap_{i=1}^n I_i}$.

(c) We have $R/\cap_{i=1}^n I_i \cong \prod_{i=1}^n R/I_i \cong \bigoplus_{i=1}^n R/I_i$.

Proof. (a) Since $I_1 + I_j = R$ for $j = 2, \ldots, n$, there exists $b_j \in I_1$ and $d_j \in I_j$ such that $b_j + d_j = 1$ for $j = 2, \ldots, n$. Then

$$1 = (b_2+d_2)(b_3+d_3)\cdots(b_n+d_n) = (b_2b_3+b_2d_3+d_2b_3+d_2d_3)\cdots(b_n+d_n) = (b+d_2d_3)\cdots(b_n+d_n),$$

where $b := b_2b_3 + b_2d_3 + d_2b_3 \in I_1$. By induction, we have $c_1 := d_2 \cdots d_n \in I_2 \cdots I_n = I_2 \cap \cdots I_n$ and $c_1 \equiv 1 \pmod{I_1}$. Then $c_1 \in I_j$, i.e., $c_j \equiv 0 \pmod{I_j}$ for $j = 2, \ldots, n$. More generally, for $i = 1, \ldots, n$, we can find c_i with $c_i \equiv 1 \pmod{I_i}$ and $c_i \equiv 0 \pmod{I_j}$ for any $1 \leqslant j \neq i \leqslant n$. Let $a = a_1c_1 + \cdots + a_nc_n$. Then for $i = 1, \ldots, n$, $a - a_i \equiv a - a_ic_i \equiv 0 \pmod{I_i}$.

(b) For all $i = 1, \ldots, n$, $b \equiv a_i \pmod{I_i}$ if and only if $b \equiv a \pmod{I_i}$ if and only if $b - a \pmod{I_i}$, which finally is equivalently to $b - a \in \bigcap_{i=1}^n I_i$.

(c) Define the ring homomorphism $f : R \mapsto \prod_{i=1}^n R/I_i$ given by $a \mapsto (a + I_1, \ldots, a + I_n)$. Let $(a_1 + I_1, \ldots, a_n + I_n) \in \prod_{i=1}^n R/I_i$. Then by (1), there exists $a \in R$ such that $a_i \equiv a \pmod{I_i}$ and so $f(a) = (a + I_1, \ldots, a + I_n) = (a_1 + I_1, \ldots, a_n + I_n)$. Thus, it is onto. Moreover,

$$\begin{aligned}\mathrm{Ker}(f) &= \{a \in R : f(a) = (I_1, \ldots, I_n)\} = \{a \in R : (a + I_1, \ldots, a + I_n) = (I_1, \ldots, I_n)\} \\ &= \{a \in R : a \in I_i, i = 1, \ldots, n\} = \bigcap_{i=1}^n I_i.\end{aligned}$$

□

Remark. The Chinese remainder theorem says that a ring element can be specified by giving its congruence class modulo each ideal in a collection of pairwise relatively prime ideals, and this element is unique modulo the product (intersection) of the ideals.

Lemma 8.7. Let R be a commutative ring with identity, $I, J \leqslant R$ and $I + J = R$, then for any $m, n \in \mathbb{N}$, $I^m + J^n = R$.

Proof. Let $m, n \in \mathbb{Z}^{>0}$. Since $I + J = R$, there exist $a \in I$ and $b \in J$ such that $a + b = 1$. Then

$$\begin{aligned}1 = 1^{m+n-1} = (a + b)^{m+n-1} &= \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} \\ &= \sum_{k=0}^{m-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} + \sum_{k=m}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k}.\end{aligned}$$

Since $m + n - 1 - k \geqslant n$ for any $0 \leqslant k \leqslant m - 1$ and $k \geqslant m$ for any $m \leqslant k \leqslant m + n - 1$, we have $b^n \mid b^{m+n-1-k}$ for any $0 \leqslant k \leqslant m - 1$ and $a^m \mid b^{m+n-1-k}$ for any $m \leqslant k \leqslant m + n - 1$. So

$$\sum_{k=0}^{m-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} \in b^n \text{ and } \sum_{k=m}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} \in a^m.$$

Hence

$$1 = \sum_{k=0}^{m-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} + \sum_{k=m}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k} \in I^m + J^n.$$

Since $I^m + J^n$ is an ideal, $I^m + J^n = 1$. □

Corollary 8.8. Let R be a commutative ring and $\mathfrak{p}_1, \mathfrak{p}_2 \leqslant R$ be distinct primes, then for any $m, n \in \mathbb{N}$, $\mathfrak{p}_1^m + \mathfrak{p}_2^n = R$ and $\mathfrak{p}_1^m\mathfrak{p}_2^n = \mathfrak{p}_1^m \cap \mathfrak{p}_2^n$. Thus, $R/\mathfrak{p}_1^m\mathfrak{p}_2^n \cong R/\mathfrak{p}_1^m \oplus R/\mathfrak{p}_2^n$.

Corollary 8.9. Let $n = p_1^{a_1} \cdots p_k^{e_k}$ be the distinct prime decomposition. Then $f(x) \equiv 0 \pmod{n}$ has a solution if and only if $f(x) \equiv 0 \pmod{p_i^{a_i}}$ for $i = 1, \ldots, k$ has a solution.

Proof. "⇒". It is clear.

"⇐". Assume $f(x_i) \equiv 0 \pmod{p_i^{a_i}}$. Since $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$ for any $1 \leqslant i \neq j \leqslant k$, by Chinese Remainder Theorem, there exists $x \in \mathbb{Z}$ such that $x \equiv x_i \pmod{n}$. Then $f(x) \equiv f(x_i) \equiv 0 \pmod{n}$. □

Definition 8.10. If $R_1, \ldots, R_n$ are commutative rings with identity, the direct product of the R_i is defined as the ring of n-tuples $(a_1, \ldots, a_n), a_i \in R_i$, with componentwise addition and multiplication. The zero element is $(0, \ldots, 0)$ and the identity is $(1, \ldots, 1)$.

Theorem 8.11. *Let R be a Noetherian ring, then for any ideal $\mathfrak{a} \leqslant A$, $\mathfrak{a}$ contains a product of nonzero prime ideals.*

Proof. Suppose not and since R is Noetherian, we can choose a $\mathfrak{a} \leqslant R$ be such that $\mathfrak{a}$ does not contains a product of nonzero prime ideals and no bigger ideal that contains $\mathfrak{a}$ properly. Then $\mathfrak{a}$ can not be prime and so there exists $x, y \in R$ such that $xy \in \mathfrak{a}$ but $x, y \notin \mathfrak{a}$. Note that the ideals $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ strictly contains $\mathfrak{a}$, but their product is contained in $\mathfrak{a}$. By assumption, $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contains a product of prime ideals and so $\mathfrak{a}$ contains a product of prime ideals, a contradiction. □

Chapter 9

Product

Remark. Let X_i's be algebraic structures, for instance, groups, rings, modules and vector spaces. Since direct products do not have the restriction that all but finitely many coordinates must be zero, $\bigoplus_{i=1}^{\infty} X_i \subseteq \prod_{i=1}^{\infty} X_i$.

Remark. (a) Cartesian product takes multiple sets and returns a set. No structure on the sets s assumed. For example for sets A and B, their Cartesian product $C = A \times B = \{(a, b) : a \in A, B \in B\}$.

(b) One often writes $f : A \times B \to C$ meaning that the argument of the function f is a tuple (a, b), where $a \in A$ and $b \in B$, and function values lie in C. This is a typical use case of the Cartesian product.

(c) If sets A and B carry some algebraic structure (e.g. they are groups), then we can define a suitable structure on the product set as well. For example, if $(A, \cdot)$ and $(B, \cdot)$ are groups, their direct product $(A \times B, \cdot)$ forms a group with $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$. Direct product is closely related to direct sum. If the number of operands is finite, they are just the same thing. For example, $A \oplus B$ and $A \times B$ are the same things. The choice of the symbol is usually dicated by the kind of group operation used (addition or multiplication).

(d) The motication for introducing tensor product comes from the study of multilinear maps. If A has a basis $\{e_1, \ldots, e_m\}$ and B has a basis $\{f_1, \ldots, f_n\}$, then $A \otimes B$ has a basis $\{e_i \otimes f_j : i = 1, \ldots, m, j = 1, \ldots, n\}$. For example, $\mathbb{R}^m \otimes \mathbb{R}^n \cong \mathbb{R}^{mn}$. That's how one could build a basis in the space of $m \times n$ matrices of rank 1.

Chapter 10

Orders in Arithmetic

Remark. Euler's theorem tell us that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for all $m \geqslant 2$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Depending on the value of a, it's possible for a smaller power than the $\varphi(n)^{\text{th}}$ power to be congruent to 1 mod n. There are exactly $\varphi(\varphi(n))$ such a's such that $\varphi(n)$ is the order of a mod n.

Theorem 10.1. *Let $a_1 \bmod m$ and $a_2 \bmod m$ have respective orders n_1 and n_2. If $\gcd(n_1, n_2) = 1$, then $a_1 a_2 \bmod m$ has order $n_1 n_2$.*

Proof. Let n be the order of $a_1 a_2 \pmod{m}$. Since $\mathbb{Z}/m\mathbb{Z}$ is commutative, $(a_1 a_2)^{n_1 n_2} \equiv (a_1^{n_1})^{n_2} (a_2^{n_2})^{n_1} \equiv 1 \pmod{m}$. So $n \mid n_1 n_2$. Since $(a_1 a_2)^n \equiv 1 \pmod{m}$, $(a_1^{n_2} a_2^{n_2})^n \equiv 1 \pmod{m}$, i.e., $a_1^{n n_2} \equiv 1 \pmod{m}$. So $n_1 \mid n n_2$. Since $\gcd(n_1, n_2) = 1$, $n_1 \mid n$. Similarly, $n_2 \mid n$. Also, since $\gcd(n_1, n_2) = 1$, $n_1 n_2 \mid n$. Thus, $n = n_1 n_2$. □

Theorem 10.2. *Let $a_1 \bmod m$ and $a_2 \bmod m$ be two units with respective orders n_1 and n_2. For some k_1, k_2, $a_1^{k_1} a_2^{k_2} \bmod m$ has order $\operatorname{lcm}(n_1, n_2)$.*

Proof. Let $n = \operatorname{lcm}(n_1, n_2)$. Then $\gcd(n/n_1, n/n_2) = 1$. Let $n = n_1 \frac{n_2}{\gcd(n_1, n_2)} := n_1 m_2$. Then $\gcd(n_1, m_2) = 1$. Also, since $a_1 \bmod m$ has order n_1 and $a_2^{\gcd(n_1, n_2)} \bmod m$ has order m_2, by previous theorem, $a_1 a_2^{\gcd(n_1, n_2)}$ has order $n_1 m_2 = \operatorname{lcm}(n_1, n_2)$. □

Proposition 10.3. Let g be a primitive root modulo p. Then $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. In particular, $\left(\frac{g}{p}\right) = -1$.

Proof. By FLT, $g^{p-1} \equiv 1 \pmod{p}$, so $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Since the order of g mod p is $p - 1$, $g^{\frac{p-1}{2}} = 1$. Suppose $g \equiv h^2 \pmod{p}$ for some $h \in \mathbb{Z}$. Then $g^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$, a contradiction. Or follow from Euler's Criterion. □

Remark. Let g be a primitive root modulo p. If $p \equiv 1 \pmod{4}$, then $4 \mid (p - 1)$, so $(g^{\frac{p-1}{4}})^2 = g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ and thus $\left(\frac{-1}{p}\right) = 1$.

Corollary 10.4. $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$.

Proof. Let g be a primitive root modulo p. Let $a \in \mathbb{Z}$. Then $a = g^i$ for some $i \in \mathbb{N}$. Then $\left(\frac{a}{p}\right) = \left(\frac{g^i}{p}\right)$. If i is odd, $\left(\frac{g^i}{p}\right) = \left(\frac{g}{p}\right) = 1$; if i is even, $\left(\frac{g^i}{p}\right) = \frac{g^2}{p} = 1$. Thus, $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{g^i}{p}\right) = 0$. □

Theorem 10.5. *If $p \equiv 5 \pmod 8$, letting t be the order of 2 modulo p, then $2^2 \mid\mid t$.*

Proof. Let $p = 8k + 5$ for some $k \in \mathbb{Z}$ and t be the order of 2 moduloe p. Then $2^t \equiv 1 \pmod p$. Since $2^{p-1} \equiv 1 \pmod p$, $t \mid p - 1$, i.e., $t \mid 8k + 4$. So $t = 1, 2, 4$ or $t \mid 2k + 1, 2(2k + 1), 4(2k + 1)$. If $t = 1, 2$, $2^t = 2, 4 \not\equiv 1 \pmod p$ for any $p \equiv 5 \pmod 8$. If $t = 4$, $2^t = 16 \equiv 1 \pmod 5$. Assume $t \mid 2k + 1, 2(2k + 1), 4(2k + 1)$. Now to show $2^2 \mid\mid t$, it is equivalent to show $t \mid 8k + 4$ and then it suffices to show $2^{2(2k+1)} \not\equiv 1 \pmod p$. Since $2(2k + 1) = \frac{p-1}{2}$, by Euler's Criterion, $2^{2(2k+1)} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv -1 \pmod p$. □