MATH620 - Algebraic Number Theory

Taught by Niranjan Ramachandran
Notes taken by Haoran Li
2020 Spring

Department of Mathematics
University of Maryland

Contents

1 Disciminant

Definition 1.1. An *algebraic number field* K is a finite field extension of $\mathbb{Q}$, its ring of algebraic integers is denoted $\mathcal{O}_K$

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, hook] & K \\ \mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

More generally, if E/F is a finite separable field extension, B, A are their ring of integers

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

Definition 1.2. $[E : F] = n$, then $B \cong A^n$ as an A module, assume $\beta_1, \cdots, \beta_n$ is a basis, define

$$D(\beta_1, \cdots, \beta_n) = \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j)) \in A$$

The *discriminant* $\operatorname{disc}(B/A) = D(\beta_1, \cdots, \beta_n)$ is well-defined in $A/(A^\times)^2$. In particular, $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ is a well-defined integer

Lemma 1.3. $\gamma_1, \cdots, \gamma_n \in \mathcal{O}_K$ is an $\mathbb{Z}$-basis for $\mathcal{O}_K$ iff $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. More generally, if A is integrally closed and Noetherian, $\gamma_1, \cdots, \gamma_n \in B$ is an A-basis of B iff $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(B/A)$

Proof. Write $\gamma_i = \sum c_{ji}\beta_j$, then $\det(\mathrm{Tr}(\gamma_i\gamma_j)) = (\det C)^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$. Thus $D(\gamma_1, \cdots, \gamma_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \Leftrightarrow \det C = \pm 1 \Leftrightarrow C \in \mathrm{GL}_n(\mathbb{Z}) \Leftrightarrow \gamma_1, \cdots, \gamma_n$ is an $\mathbb{Z}$-basis ☐

Example 1.4. $K = \mathbb{Q}(\sqrt{d})$, d is square free. $\mathcal{O}_K$ has $\{1, \sqrt{d}\}$ as an $\mathbb{Z}$-basis if $d \equiv 2, 3 \bmod 4$

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \det \mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}} \begin{pmatrix} 1 & \sqrt{d} \\ \sqrt{d} & d \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$$

$\mathcal{O}_K$ has $\{1, \frac{1+\sqrt{d}}{2}\}$ as an $\mathbb{Z}$-basis if $d \equiv 1 \bmod 4$

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \det \mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}} \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ \frac{1+\sqrt{d}}{2} & \frac{1+2\sqrt{d}+d}{4} \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{2+2d}{4} \end{pmatrix} = d$$

Therefore 7 can never be a discriminant

Proposition 1.5. $\gamma_1, \cdots, \gamma_n \in \mathcal{O}_K$, $N = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_n \leq \mathcal{O}_K$ has finite index in $\mathcal{O}_K$ iff $D(\gamma_1, \cdots, \gamma_n) \neq 0$, $D(\gamma_1, \cdots, \gamma_n) = [\mathcal{O}_K : N]^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$

Proof. Suppose $\beta_1, \cdots, \beta_n$ is an $\mathbb{Z}$-basis, $D(\beta - 1, \cdots, \beta_n) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$, $\gamma_i = \sum c_{ji}\beta_j$, $\det C = [\mathcal{O}_K : N]$ ☐

Proposition 1.6. If $D(\gamma_1, \cdots, \gamma_n)$ is square free, then $\gamma_1, \cdots, \gamma_n$ is an $\mathbb{Z}$-basis

Example 1.7. $K = \mathbb{Q}(\alpha)$, α is a root of irreducible polynomial $x^3 - x - 1$, $D(1, \alpha, \alpha^2) = -23$ which is square free, hence $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 = \mathbb{Z}[\alpha]$

Proposition 1.8. $[E : F] = n$ is separable, Ω is the Galois closure of E, $\mathrm{Hom}_F(E, \Omega) = \{\sigma_1, \cdots, \sigma_n\}$ are distinct F-embeddings of E

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

If $\beta_1, \cdots, \beta_n$ is an F-basis of E, then $D(\beta_1, \cdots, \beta_n) = \det(\sigma_i(\beta_j))^2 \neq 0$

Proof. Deonte $Q = \sigma_i(\beta_j)$, then

$$\begin{aligned} D(\beta_1, \cdots, \beta_n) &= \det(\mathrm{Tr}_{E/F}(\beta_i\beta_j)) \\ &= \det(\sum \sigma_k(\beta_i\beta_j)) \\ &= \det(\sum \sigma_k(\beta_i)\sigma_k(\beta_j)) \\ &= \det(Q^T Q) \\ &= \det(\sigma_i(\beta_j))^2 \\ &\overset{\text{Theorem 1.9}}{\neq} 0 \end{aligned}$$

□

Dedekind's theorem

Theorem 1.9 (Dedekind's theorem). *G is group, Ω is a field, $\sigma_1, \cdots, \sigma_n$ are distinct homomorphisms $G \to \Omega^\times$, then σ_i's are linear independent over Ω*

Definition 1.10. Assume A, B are integrally closed in F, E, $\beta_1, \cdots, \beta_n \in B$ is an F-basis of E, $C = A\beta_1 + \cdots + A\beta_n \leq B$, $C^* = \{\beta \in E | \mathrm{Tr}_{E/F}(\beta\beta_i) \in A\}$, $\beta \in B \Rightarrow \beta\beta_i \in B \Rightarrow \mathrm{Tr}(\beta\beta_i) \in A \Rightarrow C \leq B \leq C^*$, $C^* = A\beta_1' + \cdots + A\beta_n'$, $\beta_1', \cdots, \beta_n'$ is a dual basis. For $\alpha \in E$, $\alpha = \sum \mathrm{Tr}_{E/F}(\alpha\beta_i)\beta_i'$

$$\begin{array}{ccc} B & \hookrightarrow & E \\ \uparrow & & \uparrow \\ A & \hookrightarrow & F \end{array}$$

Example of dual basis

Example 1.11. $E = F(\beta)$, $f \in A[x]$ is the minimal polynomial of $\beta \in B$, $\deg f = n$, $C = A[\beta] \leq B$, Euler discovered

$$\mathrm{Tr}_{E/F}(\beta^i/f'(\beta)) = \begin{cases} 0 & 0 \leq i \leq n-1 \\ 1 & i = n-1 \end{cases}, \det \mathrm{Tr}_{E/F}(\frac{\beta^i\beta^j}{f'(\beta)}) = (-1)^n$$

$\dfrac{\beta^{n-1-i}}{f'(\beta)}$ is the dual basis of β^i

Proposition 1.12. In Example 1.11, suppose $f(x) = \prod_{i=1}^n (x - \beta_i) \in \bar{E}[x]$, $f'(x) = \sum_{i=1}^n \prod_{j \neq i}(x - \beta_j)$. Then

$$D(1, \beta, \cdots, \beta^{n-1}) = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 = (-1)^{\frac{n(n-1)}{2}} = N_{E/F}(f'(\beta))$$

Proof.

$$\begin{aligned} D(1, \beta, \cdots, \beta^{n-1}) &= \det(\sigma_i(\beta^j))^2 \\ &= \det(\beta_i^j)^2 \\ &= \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j \neq i} (\beta_i - \beta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_i f'(\beta_i) \\ &= (-1)^{\frac{n(n-1)}{2}} N(f'(\beta)) \end{aligned}$$

□

Remark 1.13. $\Delta = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2$ is the determinant $\mathrm{disc}(f) = \mathrm{disc}(E/F)$

Lemma 1.14. $f(x) = x^n + ax + b$, $\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^n (n-1)^{n-1} a^n)$

Example 1.15. $K = \mathbb{Q}(\beta)$, β is a root of $f(x) = x^5 - x - 1 \in \mathbb{Z}[x]$, $\mathrm{disc}(f) = 2869 = 19 \times 151$ is square free, hence $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 1$, $\mathcal{O}_K = \mathbb{Z}[\beta]$

Definition 1.16. $K = \mathbb{Q}(\alpha)$, $f(x)$ is the minimal polynomial of α, thus $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \dfrac{\mathbb{R}[x]}{(f)} \overset{\text{Chinese remainder theorem}}{\cong} \mathbb{R}^r \times \mathbb{C}^s$, $\alpha_1, \cdots, \alpha_r$ are the real roots of f, $\alpha_{r+1}, \bar{\alpha}_{r+1}, \cdots, \alpha_{r+s}, \bar{\alpha}_{r+s}$ are complex roots of f. $\mathcal{O}_K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^n$ is a lattice

Example 1.17. $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{R} \times \mathbb{R}$ give the two real embeddings. $\mathbb{Q}(\sqrt{-5}) \hookrightarrow \mathbb{C}$ give the two complex embeddings

Proposition 1.18.

(1) $K = \mathbb{Q}(\alpha)$, $\operatorname{sgn}\mathrm{disc}(K/\mathbb{Q}) = (-1)^s$

(2) (Stickelberger) $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0, 1 \bmod 4$

Proof.

(1) $1, \alpha, \cdots, \alpha^n$ is a basis for K, since $disc(K/\mathbb{Q}) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ $\operatorname{sgn} D(1, \alpha, \cdots, \alpha^n) = \operatorname{sgn}\det(\sigma_j(\alpha^i))^2 = \operatorname{sgn}\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)^2 = \operatorname{sgn}\prod_{1\le j\le s}(\alpha_{r+j} - \bar{\alpha}_{r+j})^2 = (-1)^s$

(2) $\beta_1, \cdots, \beta_n$ is an $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \det(\sigma_i(\beta^j))^2$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathrm{Hom}(K, \overline{\mathbb{Q}})$, $K \overset{\sigma}{\hookrightarrow} \overline{\mathbb{Q}} \xrightarrow{\tau} \overline{\mathbb{Q}}$. $\det A = \sum_{\tau\in S_n}\mathrm{sgn}(\tau)\prod_{i=1}^n a_{i\tau(i)} = P - N$, P for those $\tau \in A_n$, N for those aren't, so $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = (P-N)^2 = (P+N)^2 - 4PN$, $\eta \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induce a permutation π_η on $\mathrm{Hom}(K, \overline{\mathbb{Q}})$, if π_η is even, $\pi_\eta(P) = P, \pi_\eta(N) = N$, if π_η is odd, then π_η swich P, N, and $P+N, PN$ are integral over $\mathbb{Z}$, thus $P+N, PN \in \mathbb{Z}$, hence $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0, 1 \bmod 4$

$\square$

Definition 1.19. For any nonzero ideal $I \le \mathcal{O}_K$, since $I \cap \mathbb{Z} = m\mathbb{Z}$, $\mathcal{O}_K/m\mathcal{O}_K \cong (\mathbb{Z}/m\mathbb{Z})^m \to \mathcal{O}_K/I$ is surjective, hence the *norm* $N(I) = |\mathcal{O}_K/I| < \infty$. The *Dedekind zeta function* of an algebraic number field is $\zeta_K(s) = \sum_{I\neq 0}\dfrac{1}{N(I)^s} = \prod_p \dfrac{1}{1 - N(p)^{-s}}$

2 Minkowski's theorem

Definition 2.1. $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n \leq \mathbb{R}^n$ is a lattice, take $D = \{c_1v_1 + \cdots + c_nv_n | 0 \leq c_i \leq 1\}$ L, the *covolume* $\mathrm{covol}(L) = \mathrm{vol}(\mathbb{R}^n/L) = \mathrm{vol}(D)$, $\pi : D \to \mathbb{R}^n/L$ is the quotient map, $\mathrm{covol}(L)^2 = \det(\langle v_i, v_j\rangle)$

Theorem 2.2. If $B \subseteq \mathbb{R}^n$ is bounded, convex, symmetric (i.e. $B = -B$) subset such that either

1. $\mathrm{vol}(B) > 2^n \,\mathrm{covol}(L)$ or
2. $\mathrm{vol}(B) \geq 2^n \,\mathrm{covol}(L)$ and B is closed

Then $(B \cap L) \setminus \{0\} \neq \varnothing$

Proof.

1. $\mathbb{R}^2 \to \mathbb{R}^2/2L$ is not injective by volume, thus $\exists x \neq y \in B$ such that $x - y \in 2L \Rightarrow \frac{1}{2}(x - y) \in B \cap L$ since B is convex and symmetric
2. $C_k = L \cap (1 + \frac{1}{k})B \setminus \{0\} \neq \varnothing$, C_k is discrete and closed, $\cap_{k=1}^{\infty} C_k \neq \varnothing$, thus contains a limit point of B, but B is closed

$\square$

Proposition 2.3. $D_K = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \in \mathbb{Z}$

1. The image of $\mathcal{O}_K$ in $K_{\mathbb{R}}$ is a lattice
2. $\mathrm{covol}(\mathcal{O}_K) = \sqrt{|D_K|}$
3. If I is an ideal of $\mathcal{O}_K$, $\mathrm{covol}(I) = [\mathcal{O}_K : I]\sqrt{|D_K|}$ (union of all members in the coset)

Proof.

1. Need $\mathcal{O}_K \cap B_r$ is finite. $x \in \mathcal{O}_K \cap B_r \Rightarrow |\sigma(x)| \leq r$, for all complex embeddings $\sigma \Rightarrow f_{K/\mathbb{Q}.x}(t) = \prod_\sigma (t - \sigma(x))$, the characteristic monomial with $\mathbb{Z}$ coefficients of degree $[K : \mathbb{Q}]$, since coefficients are bounded, so only finitely many f, finitely many x since conjugates are roots
2. $\alpha_1, \cdots, \alpha_n$ is an $\mathbb{Z}$-basis of $\mathcal{O}_K$, $\mathrm{covol}(\mathcal{O}_K)^2 = \det(\langle\alpha_i, \alpha_j\rangle) = \det(M^T\bar{M})$, $M = (\sigma_i(\alpha_j))$, thus $\mathrm{covol}(\mathcal{O}_K) = \sqrt{|D_K|}$

$\square$

Lemma 2.4. For $m \geq 1$, the number of ideals of $\mathcal{O}_K$ of index less than m is finite, if $[\mathcal{O}_K : I] \leq m$, then $\mathcal{O}_K/I$ is killed by $m!$, thus $m!\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$, but $\mathcal{O}_K/m!\mathcal{O}_K \cong \mathbb{Z}^n/m!\mathbb{Z}^n \cong (\mathbb{Z}/m!)^n$ is finite

Theorem 2.5. For any $g \in \mathrm{Cl}(\mathcal{O}_K)$, $\exists I \subseteq \mathcal{O}_K$ such that $NI = [\mathcal{O}_K : I] \leq (\frac{2}{\pi})^s\sqrt{D_K} \Rightarrow \mathrm{Cl}(\mathcal{O}_K)$ is finite

Proof. J be an ideal representation for g^{-1}, if $0 \neq \alpha \in J$, then $0 \neq (\alpha) \subseteq J \Rightarrow \exists I$ ideal of $\mathcal{O}_K$ such that $(\alpha) = IJ$, so I represents g, $N\alpha = NI \cdot NJ$, for $c = (c_1, \cdots, c_r, c_{r+1}, \cdots, c_{r+s})$, $c_i > 0$

$$B(c) = \{(x_1, \cdots, x_r, x_{r+1}, \cdots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s | |x_i| \leq c_i\}$$

$\mathrm{vol}(B(c)) = (2c_1)\cdots(2c_r)(2\pi c_{r+1}^2)\cdots(2\pi c_{r+s}^2) = 2^n(\frac{\pi}{2})^s c_1 \cdots c_r c_{r+1}^2 \cdots c_{r+s}^2 = 2^n(\frac{\pi}{2})^s\xi$. Pick c such that $\mathrm{vol}(B(c)) = 2^n \,\mathrm{covol}(J)$, by Minkowski's theorem, $B(c) \cap J \setminus \{0\} \neq \varnothing$, pick $\alpha \in B(c) \cap J \setminus \{0\}$, $|N(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_n(\alpha)| \leq \xi$, thus $N\alpha = NI \cdot NJ \leq \xi = (\frac{2}{\pi})^s \,\mathrm{covol}\, J = (\frac{2}{\pi})^s [\mathcal{O}_K : J]\sqrt{|D_K|}$, hence $NI \leq (\frac{2}{\pi})^s \sqrt{|D_K|}$ $\square$

3 Dirichlet's unit theorem

Example 3.1. $K = \mathbb{Q}(\zeta_p)$, $p \nmid rs$, then $\dfrac{\zeta^r - 1}{\zeta^s - 1} \in \mathbb{Z}[\zeta]^\times$

Proposition 3.2. For $\alpha \in \mathcal{O}_K$, $\alpha \in \mathcal{O}_K^\times \Leftrightarrow N_{K/\mathbb{Q}}(\alpha) = \pm 1$

Proof. Let $f = x^m + \cdots + a_0$ be the charateristic polynomial of α, $N\alpha = a_0$, if $N\alpha = \pm 1$, then $g(x) = x^m + a_0^{-1} a_1 x^{m-1} + \cdots + a_0^{-1} a_{m-1} x + a_0^{-1} \in \mathbb{Z}[x]$ has α^{-1} as a root, thus $\alpha \in \mathcal{O}_K^\times$ □

Lemma 3.3. $\mu(K)$ is the set of roots of unity in K which is also the torsion subgroup of $\mathcal{O}_K^\times$. $\mu(K)$ is finite, hence cyclic, $\zeta_m \in K \Rightarrow \varphi(m) | [K : \mathbb{Q}] \Rightarrow$ only finitely many such m

Example 3.4. If $K \hookrightarrow \mathbb{R}$, then $\mu(K) = \{\pm 1\}$. If $K = \mathbb{Q}(\zeta_p)$, then $\mu(K) = \{\pm 1\} \times \langle \zeta_p \rangle$. If $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, then $\zeta_m \in K \Rightarrow \varphi(m) \leq 2 \Rightarrow m = 2, 3, 4, 6$

Proposition 3.5. $\alpha \in \mathcal{O}_K$, $|\sigma(\alpha)| = 1$ for all $K \overset{\sigma}{\hookrightarrow} \mathbb{C}$, then $\alpha \in \mu(K)$

Proof. Fix $C, D > 0$

$$E_{C,D} = \{\beta \in \overline{\mathbb{Z}} | \deg(\beta) \leq C, |\sigma(\beta)| \leq D, \forall \mathbb{Q}(\beta) \overset{\sigma}{\hookrightarrow} \mathbb{C}\}$$

$f_\beta(x) \in \mathbb{Z}[x]$ is the monic irreducible polynomial of β. $\deg f_\beta \leq C \Rightarrow \deg f_\beta$ has finitely many choice and coefficients of f_β is bounded by function of $D \Rightarrow$ finitely many choices for $f_\beta \Rightarrow E_{C,D}$ is finite. $\alpha \in E_{n,1}$, $n = [K : \mathbb{Q}]$, $\alpha^2, \alpha^3, \cdots \in E_{n,1} \Rightarrow \alpha \in \mu(K)$ since $E_{n,1}$ is finite, α^n repeats □

Definition 3.6. Define logarithm

$$\begin{aligned} \mathcal{L} : K_{\mathbb{R}}^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s &\to \mathbb{R}^{r+s} \\ (x_1, \cdots, x_{r+s}) &\mapsto (\log|x_1|, \cdots, \log|x_r|, 2\log|x_{r+1}|, \cdots, 2\log|x_{r+s}|) \end{aligned}$$

Note that $1 = |N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)||\sigma_{r+1}(\alpha)||\overline{\sigma_{r+1}(\alpha)}| \cdots |\sigma_{r+s}(\alpha)||\overline{\sigma_{r+s}(\alpha)}|$, thus the image of α is contained in the hyperplane $H = \{a_1 + \cdots + a_{r+s} = 0\}$

Theorem 3.7. (i) $\ker \mathcal{L} = \mu(K) = \mathrm{Tor}(\mathcal{O}_K^\times)$

(ii) $\mathcal{L}(\mathcal{O}_K^\times)$ is a lattice in H

(iii) $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \times \mu(K)$, $\mathcal{O}_K^\times$ is finitely generated

Proof. $\mathbb{C} \xrightarrow{|\cdot|} \mathbb{R}_{>0}$ is a homomorphism, compact $\Leftrightarrow$ image compact, $\mathbb{C}^\times \cong U(1) \times \mathbb{R}^\times$, $\log : \mathbb{R}_{>0} \to \mathbb{R}$, compact $\Leftrightarrow$ image compact

$$\begin{tikzcd} \mathcal{O}_K^\times \arrow[r, hook] & K_{\mathbb{R}}^\times \cong (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \arrow[r, hook, "\mathcal{L}"] \arrow[d, hook] & \mathbb{R}^r \times \mathbb{R}^s \\ \mathcal{O}_K \arrow[r, hook] & K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s & \end{tikzcd}$$

Show $\mathcal{L}(\mathcal{O}_K^\times)$ is discrete in $\mathbb{R}^r \times \mathbb{R}^s$, $\Rightarrow \mathrm{rank}_{\mathbb{Z}} \mathcal{O}_K^\times \leq r + s$. Let $B \subseteq \mathbb{R}^r \times \mathbb{R}^s$ be open bounded, $\mathcal{L}(\mathcal{O}_K^\times) \cap B$ is finite since $\mathcal{L}^{-1}(B)$ is open bounded in $K_{\mathbb{R}} \Rightarrow \mathcal{L}^{-1}(B) \cap \mathcal{O}_K$ is finite $\Rightarrow \mathcal{L}^{-1}(B) \cap \mathcal{O}_K^\times$ is finite $\Rightarrow \mathcal{L}(\mathcal{O}_K^\times) \cap B$ is finite. Two lattices, $\mathcal{O}_K$ is an additive group scheme, $\mathcal{O}_K^\times$ is a multiplicative group scheme □

4 Discrete valuation domain

Definition 4.1. A is a *discrete valuation ring* if A is an integrally closed PID with a unique nonzero prime ideal. $k = A/m$, $m = (\pi)$, π irreducible is unique up to $A^\times$, called the *uniformizer*, $F = \mathrm{Frac}(A) = A[\frac{1}{\pi}]$

Proposition 4.2. A is a DVR, then $m^i - m^{i+1} = A^\times \pi^i$, $A^\times = A - m = \bigsqcup_{i\in\mathbb{N}} A^\times \pi^i$, $F^\times = \bigsqcup_{i\in\mathbb{Z}} A^\times \pi^i$

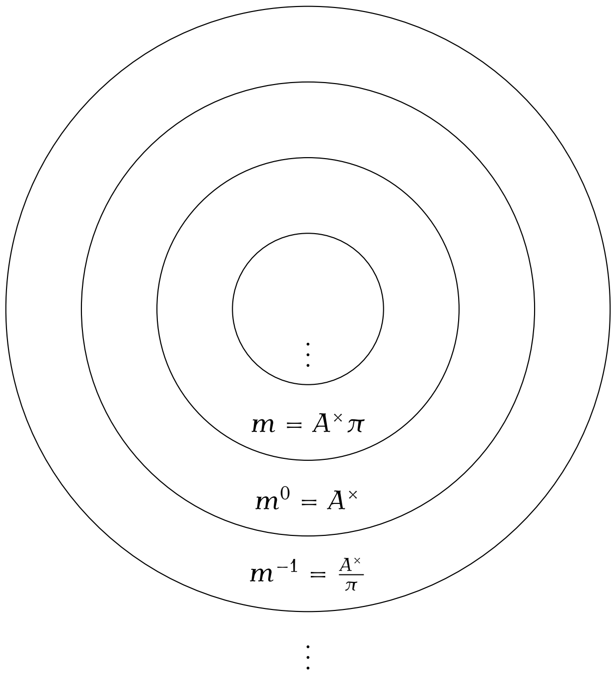


Figure 4.1: Discrete Valuation Ring

DVR

Proposition 4.3. X is a compact Riemann surface, $F = \mathbb{C}(X)$, then $A = \{f \in F | f \text{ is defined at } x\} \subseteq F$ is a DVR

Theorem 4.4. $\operatorname{sgn}\operatorname{disc}(K/\mathbb{Q}) = (-1)^s$

Proof. $\operatorname{disc}(K/\mathbb{Q}) = \det(\mathrm{Tr}(\alpha_i\alpha_j)) = (\det M)^2$, $M = (\sigma_i(\alpha_j))$, $\overline{M} = (\overline{\sigma_i(\alpha_j)})$, $\det \overline{M} = (-1)^s \det M$ ☐

Example 4.5.
- $\mathbb{Z}_{(p)}$ with $\pi = p$
- $\mathbb{C}[t]_{(t-a)}$ with $\pi = t - a$
- $\mathbb{R}[t]_{(t-c)}$ with $\pi = t - c$
- $\mathbb{F}_p[t]_{(t-c)}$ with $\pi = t - c$

Definition 4.6. The additive valuation $\nu : F \to \mathbb{Z} \cup \{\infty\}$, $0 \mapsto \infty$, $u\pi^i \mapsto i$ satisfies

1. $\nu(x) = \infty \Leftrightarrow x = 0$
2. $\nu(xy) = \nu(x) + \nu(y)$
3. $\nu(x + y) \geq \min(\nu(x), \nu(u))$

Any ν on F satisfying 1.-3. knows A, i.e. $A = \{\nu \geq 0\}$, $m = \{\nu > 0\}$, $A^\times = \{\nu = 0\}$

Definition 4.7. F is a field, a *discrete valuation* on F is a function $F \to \mathbb{R} \cup \{\infty\}$ satisfying

1. $\nu(x) = \infty \Leftrightarrow x = 0$
2. $\nu(xy) = \nu(x) + \nu(y)$
3. $\nu(x + y) \geq \min(\nu(x), \nu(u))$

$\nu(F^\times) \subseteq \mathbb{R}$ is a lattice in $\mathbb{R}$. ν is normalized if $\nu(F^\times) = \mathbb{Z}$ is the standard lattice

Remark 4.8. Given a normalized, discrete valuation, we get $A, m, A^\times$ and A is a DVR

Example 4.9. $\mathrm{ord}_p : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$, $\mathrm{ord}_p(x) = r$ if $x = p^r \frac{a}{b}$, $p \nmid ab$, then $A = \{x \in \mathbb{Q} | \mathrm{ord}_p(x) \geq 0\} = \mathbb{Z}_{(p)}$, $m = p\mathbb{Z}_{(p)}$

Exercise 4.10. A is a DVR with valuation ν

1. If $\nu(x) \neq \nu(y)$, then $\nu(x + y) = \min(\nu(x), \nu(y))$
2. If $x_1 + \cdots + x_n = 0$, $n \geq 2$, then $\exists i \neq j$ such that $\nu(x_i) = \nu(x_j) = \min_{1 \leq k \leq n} \nu(x_k)$

Definition 4.11. R is a Noetherian domain, $K = \mathrm{Frac}(R)$, a fractional ideal $I \leq K$ is a sub R-module such that $rI \subseteq R$ for some nonzero $r \in R$, define $I^{-1} = \{x \in K | xI \subseteq R\}$, a principal fractional ideal is xR for some nonzeor $x \in K$, clearly $II^{-1} \subseteq R$

Lemma 4.12. If I, J are fractional ideals, then so are $I^{-1}, IJ, I + J$

Proposition 4.13. F is a field, discrete valuations are in bijective correspondence with DVR subrings of F

Definition 4.14. Consider $\mathrm{Spv}(R) = \{\text{All valuations on } R\}/\sim$, and there is a topology given by $R(f/g) = \{\nu \in \mathrm{Spv}(R) | \nu(f) \leq \nu(g) \neq 0\}$

Hilbert rings and adic spaces

Definition 4.15. I is invertible $II^{-1} = R$

Example 4.16. $R = \mathbb{C}[x, y]$, $I = (x, y)$, $I^{-1} = \mathbb{C}[x, y]$

Proposition 4.17.

1. If $I = (f)$, then $I^{-1} = (f^{-1})$, hence principal fractional ideals are invertible
2. If I is invertible, then I is finitely generated as an R-module. $1 = \sum_{i=1}^n x_i y_i$, $x_i \in I, y_i \in I^{-1}$, so for any $r \in I$, $r =\sim r x_i y_i = \sum x_i (r y_i)$, hence I is finitely generated by $x_1, \cdots, x_n$
3. (R, m) is a local ring, then I invertible $\Rightarrow I$ principal. $1 = \sum_{i=1}^n x_i y_i$, $x_i \in I, y_i \in I^{-1}$ are not all in m, say $x_1 y_1 \notin m$, then $x_1 y_1 = u$ is a unit, let $y_1' = y_1 u^{-1}$, then $1 = x_1 y_1'$, then $r \in I \Rightarrow r = r x_1 y_1' = x_1 (r y_1')$, thus $I = (x_1)$
4. p is a prime of R, (R_p, pR_p) is a local ring, then I fractional invertible $\Rightarrow IR_p$ fractional invertible $\Rightarrow IR_p$ principal
5. I, J invertible $\Rightarrow IJ$ invertible

Definition 4.18. The group of divisors $\mathrm{Div}(R)$ is the set of invertible fractional ideals of R, this becomes an abelian group, R is the neutral element. The set of principal fractional ideals is a subgroup of $\mathrm{Div}(R)$, define the Picard group $\mathrm{Pic}(R) = \mathrm{Div}(R)/\{\text{principal fractional ideals}\}$

Proposition 4.19. If R is a domain, $\dim R = 1 \Leftrightarrow R$ is a field $\Leftrightarrow$ all primes are maximal. R is a DVR $\Rightarrow \dim R = 1$, $\dim R[t] = 1 + \dim R$

Proposition 4.20. Every prime in $\mathcal{O}_K$ is maximal

Proof. For any nonzero $\alpha \in p$, $0 \neq N\alpha \in p \cap \mathbb{Z}$, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is the minimal polynomial of α, then $a_0 = -a_1\alpha - a_2\alpha^2 - \cdots - \alpha^n \in (p)$. Recall $N(p) = [\mathcal{O}_K : p] = |\mathcal{O}_K/p|$ is finite, $\mathcal{O}_K \cong \mathbb{Z}^n$, thus $\mathcal{O}_K/p$ is a domain $\Rightarrow \mathcal{O}_K/p$ is a field $\Rightarrow p$ is maximal □

Theorem 4.21. R is a domain, then the following are equivalent

1. R is Noetherian, normal, and $\dim R = 1$
2. R is Noetherian, R_p is a DVR for any nonzero prime p
3. All fractional ideals of R are invertible

Such a ring is called a *Dedekind domain*. This is why DVR is sometimes called a local Dedekind domian. $\mathcal{O}_K$ is a Dedekind domain

Theorem 4.22 (DVR recognition theorem)**.** (R, m) is a local domain, the following are equivalent

(1) R is a DVR

(2) R is a PID

(3) R is Noetherian and m is principal

(4) R is a Noetherian and m is invertible

(5) All fractional ideals are invertible

(6) R is Noetherian, normal and $\dim R = 1$

Proof.

$$\begin{array}{ccccccc} (1) & \Longrightarrow & (2) & \Longrightarrow & (3) & \Longrightarrow & (4) \\ \Updownarrow & & \Updownarrow & & & & \\ (6) & & (5) & & & & \end{array}$$

is clear, here (2)⇔(5) uses local rings + invertible fractional ideals ⇒ principal
(3)⇒(1): $m = (\pi)$, $N = \cap_{i=1}^{\infty} m^i = \cap_{i=1}^{\infty} \pi^i R$, N is finitely generated, $mN = N$, by Nakayama's lemma, $N = 0$. Thus for any $r \in R$, $r \in \pi^n R - \pi^{n+1} R$ for some n, hence $R \setminus \{0\} = \sqcup_{n \geq 0} \pi^n R^\times$
(6)⇒(4): $K = \mathrm{Frac}(R)$, need to show $1 \in mm^{-1}$

- Set $s(m) = \{x \in K | xm \subseteq m\}$, $R \subseteq s(m) \subseteq K$, $s(m) \subseteq \mathrm{End}_R(m) \Rightarrow s(m)$ is integral over R (Cayley-Hamilton). Since R is normal, $s(m) = R$, i.e. R is the largest subring of K such that m is an ideal
- $R \subseteq m^{-1}$, $m \subseteq mm^{-1} \subseteq R$, since m is maximal, if $mm^{-1} = R$ then we are done, otherwise $m = mm^{-1} \Rightarrow m^{-1} \subseteq s(m) = R \Rightarrow m^{-1} = R$
- Consider $T = \{I \subseteq R \text{ ideal} | R \subsetneqq I^{-1}\} \ni (0) = K$, since R is Noetherian, T has a maximal element I, $I \subsetneqq R \subsetneqq I^{-1}$, claim I is prime, then I is maximal since $\dim R = 1$, then $I = m$, $R \subsetneqq m^{-1}$. Pf of claim: suppose $r, s \in R$, $rs \in I$, $r \notin I$, let $J = (r) + I \subseteq R$ is an ideal, then $I \subsetneqq J$, $J^{-1} = R$, but $\exists t \in I^{-1} \setminus R$, $tsJ = ts(r) + tsI \subseteq R \Rightarrow ts \in J^{-1} = R$, thus $t((s) + I) \subseteq R$ $\Rightarrow t \in ((s) + I)^{-1} - R$, thus $(s) + I \in I \Rightarrow s \in I$ which is a contradiction

□

R is a Noetherian ring, $X = \mathrm{Spec}\, R$ or any scheme. Consider the category of projective modules, and the subcategory of rank 1 projective R-modules. If M is of rank 1, $M \otimes R_p \cong R_p$ as R_p module, $M \otimes M^* \cong R$, Picard category

Definition 4.23. The *class group* is $\mathrm{Cl}(\mathcal{O}_K) = \{$Fractional ideals/Principal ideals$\}$

Exercise 4.24. Every ideal in $\mathcal{O}_K$ is generated by at most 2 elements

Theorem 4.25. R is a domain, the following are equivalent

1. R is Noetherian, normal and $\dim R = 1$
2. R is Noetherian, R_p is a DVR for any nonzero prime p
3. All nonzero fractional ideals are invertible

Proof. 1.⇒2.: R is Noetherian, so is R_p, $\dim R_p \leq \dim R$, there is a bijection between primes in $S^{-1}R$ and primes in R that doesn't intersect S, thus $\dim R_p = 1$. Claim: R normal $\Rightarrow S^{-1}R$ normal. If $x \in \operatorname{Frac} S^{-1}R = K$ is normal and integral over $S^{-1}R$, then $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, $a_i \in S^{-1}R$, pick $s \in S$, $sa_i \in R$, then $(sx)^n + sa_{n-1}(sx)^{n-1} + \cdots + s^{n-1}a_1(sx) + s^n a_0 = 0$ $\Rightarrow sx$ is integral over $R \Rightarrow sx \in R \Rightarrow x \in S^{-1}R$
2.⇒3.: $I \subseteq R$ is a nonzero fractional ideal, $IR_p \subseteq R_p$ is a nonzero fractional ideal, since R_p is a DVR, IR_p is invertible, $(IR_p)^{-1} = I^{-1}R_p$ is easy, $II^{-1}R_p = (IR_p)(I^{-1}R_p) = R_p$, if $II^{-1} \subsetneqq R$, then $II^{-1} \subseteq p$ for some prime(maximal) $p \Rightarrow II^{-1}R_p \subseteq pR_p$ which is a contradiction
3.⇒1.: $0 \neq I \subseteq R \Rightarrow I$ is invertible $\Rightarrow I$ is a finitely genenrated R-module $\Rightarrow R$ is Noetherian, $x \in K$ integral over R, the subring $B = R[x]$ is a finitely generated R-module $\Rightarrow B$ is a fractional ideal of $R \Rightarrow B$ is invertible, $B = BR = BBB^{-1} = BB^{-1} = R \Rightarrow x \in R$. $p \neq 0$ is a prime in R, $p \subsetneqq m$ is maximal, then $m^{-1} \subseteq p^{-1} \Rightarrow pm^{-1} \subseteq R = pp^{-1}$, $pmm^{-1} = p \Rightarrow p \subseteq m$ or $p \subseteq pm^{-1} \Rightarrow p \supseteq pm^{-1} \Rightarrow m^{-1} \supseteq R \Rightarrow mm^{-1} \subseteq m \Rightarrow R \subseteq m$ which is a contradiction ☐

Theorem 4.26. *If A is a Dedekind domain, then so is B*

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

Proof. B is normal, B is a finitely generated A-module. $I \subseteq B$ is an ideal $\Rightarrow I$ is a finitely generated A-module $\Rightarrow I$ is a finitely generated B-module $\Rightarrow B$ is Noetherian. Pick $p \neq 0$ prime in B, $A \cap p \subseteq A$ is prime, $A/A \cap p \hookrightarrow B/p$. $0 \neq \alpha \in p$, $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, $a_i \in A$ minimal so that $a_0 \neq 0$, $0 \neq a_0 \in A \cap p \Rightarrow A \cap p$ is maximal, $k = A/A \cap p$, B/p is a k-algebra, finite dimensional vector space, $0 \neq y \in B/p$, $B/p \xrightarrow{\times y} B/p$ is injective, this an isomorphism, hence $1 = yy^{-1}$
R is a Dedekind domain, $0 \neq p$ maximal, $K = \operatorname{Frac}(R)$, R_p is a DVR with valuation v_p, $a \in K^\times$, $aR_p = p^{v_p(a)}R_p = (pR_p)^{v_p(a)}$. I is a fractional ideal of R, $v_p(I) = n$ if $IR_p = p^n R_p = (pR_p)^n$, $n \in \mathbb{Z}$, it is enough to check

- $v_p(IJ) = v_p(I) + v_p(J)$
- $v_p(I + J) = \min\{v_p(I), v_p(J)\}$
- $v_p(I \cap J) = \max\{v_p(I), v_p(J)\}$
- $I \subseteq J \Rightarrow v_p(J) \leq v_p(I)$

☐

Example 4.27. $A = \mathbb{C}[t]$, PID $\Rightarrow$ Dedekind domain, $F = \mathbb{C}(t)$, $v_\infty : F \to \mathbb{Z} \cup \{\infty\}$, $v_\infty(0) = \infty$, $v_\infty(f/g) = \deg g - \deg f$. Normalized valuations on $\mathbb{C}(t) \leftrightarrow \mathbb{CP}^1$

Theorem 4.28. *A is a Dedekind domain, then any nonzero ideal I can be written as a product of prime ideals in a unique way, thus A is a UFD $\Leftrightarrow$ A is a PID*

Proof. The abelian group of invertible ideals of A is a free abelian group generated by $\operatorname{Spec} A$. I is a nonzero ideal, $I_0 = I$, if $I_{k-1} = A$, then set $I_k = A$, otherwise, $\exists p_k \supseteq I_{k-1}$, set $I_k = p_k^{-1}I_{k-1}$, then $I_{k-1} \subseteq I_k \subseteq A$. Since $I_{k-1} \subsetneqq A$, $I_{k-1} \subsetneqq I_k$, $I = I_0 \subsetneqq I_1 \subsetneqq \cdots \subsetneqq I_{n-1} \subsetneqq I_n = A = \cdots$, so $I_0 = p_1 \cdots p_n In = p_1 \cdots p_n$. For fractional ideal I, $aI \subseteq A$, $aI = \cdots$ and $(a) = \cdots \Rightarrow I = \cdots$
Uniqueness: $q \in \operatorname{Spec} A$, $q_1, \cdots, q_s \neq q$, $q + q_i = A$, $(q+q_1)^{f_1} \cdots (q+q_s)^{f_s} = A \Rightarrow q + q_1^{f_1} \cdots q_s^{f_s} = A$, $f_i \geq 0 \Rightarrow q_1^{f_1} \cdots q_s^{f_s} A_q$ is not in qA_{q_1} thus not in $A_q \Rightarrow 0 = v_q(q_1^{f_1} \cdots q_s^{f_s}) \Rightarrow v_q(q^{f_0} q_1^{f_1} \cdots q_s^{f_s}) = f_0 = v_q(q^{f_0})$ ☐

Remark 4.29.

$$1 \to A^\times \to F^\times \xrightarrow{\oplus v_p} \bigoplus_{p \in \operatorname{Spec} A} \mathbb{Z} \to \mathrm{Cl}(A) \to 0$$

$$\cdots \to K_1(A) \to K_1(F) \to \bigoplus_{p \in \operatorname{Spec} A} K_0(A/p) \to \cdots$$

is the localization sequence in K-theory

Lemma 4.30. A is a Dedekind domain, $\operatorname{Spec} A$ has closed points and a unique generic point (0)

Example 4.31. $A = \mathbb{C}[x]$ is a PID, $F = \mathbb{C}(x)$, $\mathrm{Cl}(A)$ is trivial

$$\begin{tikzcd} B = \dfrac{\mathbb{C}[x,y]}{(y^2 - x^3 - 1)} \arrow[r, hook] & \dfrac{\mathbb{C}(x)[y]}{(y^2 - x^3 - 1)} \\ A = \mathbb{C}[x] \arrow[r, hook] \arrow[u, hook] & F = \mathbb{C}(x) \arrow[u, hook] \end{tikzcd}$$

$\mathrm{Cl}(B)$ is uncountable, $\mathbb{C}^2/\Gamma$

5 Ramification

Definition 5.1. A, B are Dedekind domains, F, E are fractional field

$$\begin{tikzcd} B \arrow[r, hook] & E \\ A \arrow[u, hook] \arrow[r, hook] & F \arrow[u, hook] \end{tikzcd}$$

$\beta \in B$ is maximal $\Rightarrow \beta \cap A$ is maximal in A. $pB = \beta_1^{e_1} \cdots \beta_r^{e_r}$, $e_i > 0$. $k_p = A/p \to B/\beta = k_\beta$, B is a finitely generated A-module, B/β is a finitely generated k_p vector space, $f_i = [k_\beta : k_p]$

- p is *ramified* if $e_i > 1$ for some i
- p is *inert* if pB is a prime
- p *total split* if $e_i = 1, f_i = 1$

Proposition 5.2. Suppose $pB = \beta_1^{e_1} \cdots \beta_r^{e_r}$, $e_i > 0$

1. $B/pB \cong \prod_{i=1}^r B/\beta_i^{e_i}$
2. $[E : F] = \dim_{k_p}(B/pB) = \sum_{i=1}^r e_i f_i \Rightarrow r \leq [E : F]$, (totally split $\Leftrightarrow$ "=")

Proof.

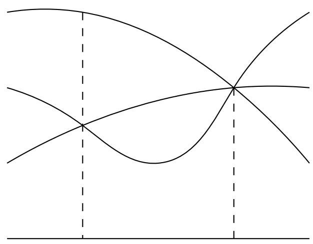
1. Chinese remainder theorem
2. If $B \cong A^n$, then $B/pB \cong A^n pA^n \cong (A/p)^n \cong k_p^n$

$\square$

Example 5.3. $2\mathbb{Z}[i] = (1 + i)^2$ is ramified, $3\mathbb{Z}[i]$ is prime inert, $5\mathbb{Z}[i] = (2 - i)(2 + i)$ totally split

$$\begin{tikzcd} \mathbb{Z}[i] \arrow[r, hook] & \mathbb{Q}[i] \\ \mathbb{Z} \arrow[u, hook] \arrow[r, hook] & \mathbb{Q} \arrow[u, hook] \end{tikzcd}$$

Example 5.4. $f : \operatorname{Spec} B \to \operatorname{Spec} A$, $f(\beta) = \beta \cap A$, If $pB = \beta_1^{e_1} \cdots \beta_r^{e_r}$, then $f^{-1}(p) = T_p = \{\beta_1, \cdots, \beta_r\}$. If $\beta \cap A = p$, then $\beta \supseteq pB = \beta_1^{e_1} \cdots \beta_r^{e_r}$, since β, β_i are maximal, $\beta = \beta_i$ for some i. $pB \subseteq \beta_i \Rightarrow pB \cap A = p \subseteq \beta_i \cap A \Rightarrow \beta_i \cap A = p$



In general, A_p is a DVR $\Rightarrow$ PID, $A_p/pA_p \cong A/p \cong k_p$, $B_p = B \otimes_A A_p$ is torsion free since $B_p \subseteq E$, B_p is finitely generated and torsion free over PID $A_p \Rightarrow B_p \cong A_p^n \Rightarrow B_p/pB_p \cong (A_p/pA_p) \cong k_p^n$

Theorem 5.5. If E/F is Galois, then $G = \mathrm{Gal}(E/F)$ acts on $f^{-1}(p) = \{\beta_1, \cdots, \beta_r\}$ transitively, thus $n = \sum_{i=1}^r e_i f_i = ref$, $e, f, r | n$

Proof. For any $\sigma \in G$, $f(\beta) = f(\sigma(\beta))$, preserving e_i, f_i

$$\begin{tikzcd} k_p \arrow[r, hook] \arrow[d, equal] & B/\beta \arrow[d, "\sigma"] \\ k_p \arrow[r, hook] & B/\sigma(\beta) \end{tikzcd}$$

Suppose β, β' are not related by G, then $\exists x \in B$ such that

$$x \equiv \begin{cases} 1 \bmod \sigma\beta & \forall \sigma \in G \\ 0 \bmod \tau\beta' & \forall \tau \in G \end{cases}$$

Thus

$$A \ni N_{B/A}(x) = N_{E/F}(x) = \prod_{\sigma \in G} \sigma(x) \equiv \begin{cases} 1 \bmod \sigma\beta \\ 0 \bmod \sigma\beta' \end{cases}$$

$$\Rightarrow N_{B/A}(x) \equiv \begin{cases} 0 \bmod \sigma\beta \cap A = p \\ 1 \bmod \sigma\beta' \cap A = p \end{cases}$$

Fix β, define $D_\beta = \{\sigma \in G | \sigma\beta = \beta\}$, $D_{\tau(\beta)} = \tau D_\beta \tau^{-1}$, $|D_\beta| = ef$. p totally splits in $B \Leftrightarrow D_\beta = \{1\}$ for any β

If G is abelian, D_β depends only on p, not β since $\tau D_\beta \tau^{-1} = D_\beta$

$$\begin{tikzcd} 0 \arrow[r] & \beta \arrow[r] \arrow[d] & B \arrow[r] \arrow[d, "\sigma"] & k_\beta \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \sigma\beta \arrow[r] & B \arrow[r] & k_{\sigma\beta} \arrow[r] & 0 \end{tikzcd}$$

If $\sigma \in D_\beta$, $k_\beta \to k_\beta$ is an automorphism $\Rightarrow D_\beta \to \mathrm{Aut}(k_\beta/k_p) \Rightarrow \ker = I_\beta$, the inertia group of β, $I_{\tau\beta} = \tau I_\beta \tau^{-1}$ $\square$

Theorem 5.6. p ramifies in $\mathcal{O}_K \Leftrightarrow p | \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$

References

Index