Monday, 26 April 2021 16:10

Beliebigen Dedekind Ring $\mathfrak{o}$ mit Quotientenkörper K und seine ganzen Abschluss $\mathcal{O}$ in L/K.

$\mathfrak{p} \subseteq \mathfrak{o}$ $\quad \mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$

$\mathfrak{P}_i$ heisst ein Primteiler von $\mathfrak{p}$: $\mathfrak{P} | \mathfrak{p}$

$\mathfrak{p} = \mathfrak{P}_i \cap \mathfrak{o}$.

$\underline{(\mathcal{O}/\mathfrak{P}_i)/(\mathfrak{o}/\mathfrak{p})}$

$\mathfrak{o} \to \mathcal{O} \to \mathcal{O}/\mathfrak{P}$ hat Kern $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$

$\Rightarrow \mathfrak{o}/\mathfrak{p} \hookrightarrow \mathcal{O}/\mathfrak{P}$ ist injektiv.

Def $\mathfrak{p}\mathcal{O} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, wir definieren:

(i) e_i heisst Verzweigungindex

(ii) $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}]$ heisst Trägheitsgrad

(iii) $\mathfrak{P}_i$ heisst unverzweigt über $\mathfrak{p}$, falls $e_i = 1$ und $(\mathcal{O}/\mathfrak{P}_i)/(\mathfrak{o}/\mathfrak{p})$ separabel ist

(iv) $\mathfrak{p}$ heisst unverzweigt über L/K, falls $\forall i = 1, \dots, r$: $\mathfrak{P}_i/\mathfrak{p}$ unverzweigt ist

(v) $\mathfrak{p}$ heisst unzerlegt in L/K, falls $r = 1$

(vi) $\mathfrak{p}$ heisst total zerlegt in L/K, falls für alle $i = 1, \dots, r$: $f_i = 1$ und $e_i = 1$

Satz $\sum_{i=1}^{r} e_i f_i = n = [L:K]$

Beweis $\underbrace{\mathcal{O}/\mathfrak{p}\mathcal{O}}_{} \cong \bigoplus_{i=1}^{r} \underbrace{\mathcal{O}/\mathfrak{P}_i^{e_i}}_{}$

Vektorräume über dem Körper $\kappa := \mathfrak{o}/\mathfrak{p}$

27. $\dim_\kappa(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n$ und $\dim_\kappa(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i f_i$

1) Seien $\underline{\omega_1, \dots, \omega_n} \in \mathcal{O}$ Repräsentanten für die Basis $\bar{\omega}_1, \dots, \bar{\omega}_n$ von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ über κ.

Nehme an, dass $\omega_1, \dots, \omega_n$ lin. abhängig sind über K also auch über $\mathfrak{o}$.

Also $\exists\, a_1, \dots, a_n \in \mathfrak{o}$ so, dass

$a_1\omega_1 + \dots + a_n\omega_n = 0$.

Sei $\mathfrak{a} = (a_1, \dots, a_n)$ und finde ein $a \in \mathfrak{a}^{-1}$:

$a \notin \mathfrak{a}^{-1}\mathfrak{p}$ also $a\mathfrak{a} \not\subseteq \mathfrak{p}$.

$aa_1, \dots, aa_n \in \mathfrak{o}$ aber nicht alle gehören zu $\mathfrak{p}$.

$aa_1\omega_1 + \dots + aa_n\omega_n \equiv 0 \mod \mathfrak{p}$

$\Rightarrow \bar{\omega}_1, \dots, \bar{\omega}_n$ sind lin. abhängig über κ ↯

$M := \mathfrak{o}\omega_1 + \dots + \mathfrak{o}\omega_n$ und $N := \mathcal{O}/M$.

$\mathcal{O} = M + \mathfrak{p}\mathcal{O} \Rightarrow \mathfrak{p}N = N$.

L/K separabel $\Rightarrow$ $\mathcal{O}$ und N endlich erzeugte $\mathfrak{o}$-Module

Sei $\alpha_1, \dots, \alpha_s$ ein Erzeugendensystem von N

$\alpha_i = \sum_j a_{ij}\alpha_j$ für $a_{ij} \in \mathfrak{p}$

Sei

$A := (a_{ij}) - I_s$ und $B := \operatorname{adj}(A)$

$A(\alpha_1, \dots, \alpha_s)^T = 0$ und $BA = dI$, wo $d = \det(A)$

$\Rightarrow 0 = BA(\alpha_1, \dots, \alpha_s)^T = (d\alpha_1, \dots, d\alpha_s)$

$dN = 0$, $d\mathcal{O} \subseteq M$. $d \neq 0$, weil

$d = \det((a_{ij}) - I_s) \equiv (-1)^s \mod \mathfrak{p}$

$\Rightarrow L = dL = K\omega_1 + \dots + K\omega_m$.

2) $\mathcal{O}/\mathfrak{P}_i^{e_i} \supseteq \mathfrak{P}_i/\mathfrak{P}_i^{e_i} \supseteq \dots \supseteq \mathfrak{P}_i^{e_i-1}/\mathfrak{P}_i^{e_i} \supseteq (0)$

$\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1} \cong \mathcal{O}/\mathfrak{P}_i$

Für $\alpha \in \mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}$: $\mathcal{O} \longrightarrow \mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}$, $a \mapsto a\alpha$

hat Kern $\mathfrak{P}_i$ und es ist surjektiv, weil

$\mathrm{ggT}(\mathfrak{P}_i^{\nu+1}, \alpha\mathcal{O}) = \mathfrak{P}_i^{\nu}$.

$\mathfrak{P}_i^{\nu} = \alpha\mathcal{O} + \mathfrak{P}_i^{\nu+1}$.

$f_i = [\mathcal{O}/\mathfrak{P}_i : K]$ haben wir

$\dim_K(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = f_i$

$\Rightarrow \dim_K(\mathcal{O}/\mathfrak{P}_i^{e_i}) = \sum_{\nu=0}^{e_i-1} \dim_K(\mathfrak{P}_i^{\nu}/\mathfrak{P}_i^{\nu+1}) = e_i f_i$.

□

$\mathbb{Z}_K$, $K = \mathbb{Q}(\theta)$ für ein ganz θ

$p \in \mathbb{Z}$ $\quad p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$, $\mathfrak{P}_i \cap \mathbb{Z} = p\mathbb{Z}$

Satz Sei $\theta \in \mathbb{Z}_K$ eine ganze Zahl von einem Zahlkörper $K = \mathbb{Q}(\theta)$ vom Grad n über $\mathbb{Q}$ und $d = \mathrm{disk}(1, \theta, \dots, \theta^{n-1})$. Sei $p \in \mathbb{Z}$ eine Primzahl, welche zu d teilerfremd ist. Sei $Q(X) \in \mathbb{Z}[X]$ das

Minimalpolynom von θ und nehme an, dass die Reduktion $\bar{Q}(X) \in (\mathbb{Z}/p\mathbb{Z})[X]$ sich wie folgt

$$\bar{Q}(X) = \prod_{i=1}^{r} \bar{Q}_i(X)^{e_i}$$

in irreduzible, paarweise teilerfremde Polynome faktorisiert. Seien $Q_i(X) \in \mathbb{Z}[X]$ die Polynome die auf die $\bar{Q}_i(X)$ sich reduzieren, dann sind

$$\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$$

die verschiedene über (p) liegende Primideale von $\mathbb{Z}_K$. Ferner ist der Trägheitsgrad f_i von $\mathfrak{P}_i$ über (p) gleich den Grad des Polynoms $\bar{Q}_i(X)$ und es gilt

$$p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}.$$

Beweis $\mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\bar{Q}(X))$

1) $1, \theta, \dots, \theta^{n-1}$ bildet eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\theta]$.

$d = \mathrm{disk}(1, \dots, \theta^{n-1}) = \det(\mathrm{tr}(\theta^{i+j}))_{i,j=0,\dots,n-1}$

$\Rightarrow \mathbb{Z}[\theta] \subseteq \mathbb{Z}_K \subseteq \frac{1}{d}\mathbb{Z}[\theta]$.

$(d,p) = 1 \Rightarrow d$ invertierbar in $\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow \mathbb{Z}[\theta] \to \mathbb{Z}_K \to \mathbb{Z}_K/p\mathbb{Z}_K$ ist surjektiv mit Kern $p\mathbb{Z}[\theta] \Rightarrow \mathbb{Z}_K/p\mathbb{Z}_K \cong \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathbb{Z}[X]/(p, Q(X))$

2) $\mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X]/(\bar{Q}(X))$

hat Kern $(p, Q(X))$, $\mathbb{Z}[\theta] = \mathbb{Z}[X]/(Q(X))$

$\Rightarrow \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong (\mathbb{Z}/p\mathbb{Z})[X]/(\bar{Q}(X))$.

$\bar{Q}(X) = \prod_{i=1}^{r} \bar{Q}_i(X)^{e_i}$

$$\underbrace{(\mathbb{Z}/p\mathbb{Z})[X]/(\bar{Q}(X))} \cong \bigoplus_{i=1}^{r} (\mathbb{Z}/p\mathbb{Z})[X]/(\bar{Q}_i(X))^{e_i}$$

$=: R$

Alle Primideale von R sind die Hauptideale $(\bar{Q}_i)$, die erzeugt von $\bar{Q}_i(X) \bmod \bar{Q}(X)$ sind (für $i = 1, \dots, r$)

$[R/(\bar{Q}_i) : \mathbb{Z}/p\mathbb{Z}] = \deg(\bar{Q}_i(X))$ und

$$(0) = (\bar{Q}) = \bigcap_{i=1}^{r} (\bar{Q}_i)^{e_i}.$$

$R \cong \mathbb{Z}_K/p\mathbb{Z}_K$, $f(X) \mapsto f(\theta)$

$\bar{\mathfrak{P}}_i \in \mathbb{Z}_K/p\mathbb{Z}_K$ ~~sind~~ $(\bar{Q}_i)$ und sind erzeugt von den $Q_i(\theta) \bmod p\mathbb{Z}_K$.

$[(\mathbb{Z}_K/p\mathbb{Z}_K)/\bar{\mathfrak{P}}_i : \mathbb{Z}/p\mathbb{Z}] = \deg(\bar{Q}_i(X))$

$$\Rightarrow (0) = \bigcap_{i=1}^{r} \bar{\mathfrak{P}}_i^{e_i}.$$

$\mathfrak{P}_i = p\mathbb{Z}_K + Q_i(\theta)\mathbb{Z}_K$ ist das Vorbild von $\bar{\mathfrak{P}}_i$ bezüglich den Homo $\mathbb{Z}_K \to \mathbb{Z}_K/p\mathbb{Z}_K$.

Für $i = 1, \dots, r$ variiert $\mathfrak{P}_i$ über den Primidealen von $\mathbb{Z}_K$ über p.

$f_i = [\mathbb{Z}_K/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}] = \deg(\bar{Q}_i(X))$

$\mathfrak{P}_i^{e_i}$ ist das Vorbild von $\bar{\mathfrak{P}}_i^{e_i}$, weil

$e_i = \#\{\bar{\mathfrak{P}}^{\nu} \mid \nu \in \mathbb{N}\}$ und

$p\mathbb{Z}_K \supseteq \bigcap_{i=1}^{r} \mathfrak{P}_i^{e_i}$ so, dass $p\mathbb{Z}_K \mid \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$

$$\sum_{i=1}^{r} e_i f_i = n \quad \Rightarrow p\mathbb{Z}_K = \prod_{i=1}^{r} P_i^{e_i} .$$ $\square$

Bem $d = (-1)^{n(n-1)/2} \operatorname{disk}(Q(X)) = \operatorname{Res}\left(Q(X), \frac{d}{dX} Q(X)\right)$

Seit $(p,d) = 1 \Rightarrow \bar{Q}(X)$ hat keine mehrfache Nullstelle $\Rightarrow \forall i : e_i = 1$ und also p ist unverzweigt.

Bsp $\theta = \sqrt[3]{2}$, $Q(X) = X^3 - 2 \in \mathbb{Z}[X]$

$$X^3 - 2 \equiv \underbrace{\overset{\bar{Q}_1}{(X+2)}}\ \underbrace{\overset{\bar{Q}_2}{(X^2+3X+4)}} \mod (5)$$

irreduzibel und teilfremd über $\mathbb{Z}/5\mathbb{Z}$

5 und $d = -108$ sind teilerfremd.

$$5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} = P_1 P_2 = \left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{2}+2)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right) \cdot \left(5\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})} + (\sqrt[3]{4} + 3\sqrt[3]{2} + 4)\mathbb{Z}_{\mathbb{Q}(\sqrt[3]{2})}\right) .$$