Kap 5 Erweiterungen von Dedekindringen

§1 Primideale und Erweiterungen

Sei $K \subset L$ Zahlkörper mit Ganzheitsringen $\mathcal{O}_K \subset \mathcal{O}_L$, und $n = [L:K]$.
Dann ist weiter $K \subset L$ separabel und $\mathcal{O}_K$, $\mathcal{O}_L$ Dedekindringe.

Bem 1: Sei $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ Primideal. Dann ist $\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$.

Bew: $\mathfrak{p} \supsetneq \mathfrak{p}^2$.
Sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$.
$\Rightarrow \pi\mathcal{O}_K \subset \mathfrak{p}$ mit $\operatorname{ord}_{\mathfrak{p}} \pi\mathcal{O}_K = 1$.
$\Rightarrow \pi\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$ mit $\mathfrak{p} + \mathfrak{a}$.
$\Rightarrow \mathfrak{p} + \mathfrak{a} = \mathcal{O}_K$.
Sei $b \in \mathfrak{p}$, $s \in \mathfrak{a}$ mit
$b + s = 1$. ($\Rightarrow \mathfrak{p} + \mathfrak{a}$)
Es ist $s\mathfrak{p} \subset \mathfrak{a}\mathfrak{p} = \pi\mathcal{O}_K$.

Ann $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$.
$\Rightarrow s\mathcal{O}_L = s\mathfrak{p}\mathcal{O}_L \subset \pi\mathcal{O}_L$
$\Rightarrow s = \pi x$ mit $x \in \mathcal{O}_L$
$x = s/\pi \in K$
$\Rightarrow x \in \mathcal{O}_L \cap K = \mathcal{O}_K$
$\Rightarrow s \in \pi\mathcal{O}_K \subset \mathfrak{p}$ $\lightning$ ☐

Kor 2: Sei $0 \neq \mathfrak{p} \subset \mathcal{O}_K$. Dann hat $\mathfrak{p}\mathcal{O}_L$ eine eind. Faktorisierung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \qquad (*)$$

mit $\mathfrak{P}_i \subset \mathcal{O}_L$ prim und $e_i \in \mathbb{N}$.

Die $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ sind genau die $\mathfrak{P} \subset \mathcal{O}_L$ über $\mathfrak{p}$ d.h. mit $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Bew: Die Existenz einer $\mathfrak{P}$-Faktorisierung folgt weil $\mathcal{O}_L$ Dedekind-Ring.

Für jedes $\mathfrak{P}_i$ in $(*)$ gilt

$$\mathfrak{P}_i \supset \mathfrak{p}\mathcal{O}_L$$

$$\Rightarrow \mathfrak{P}_i \cap \mathcal{O}_K \supset (\mathfrak{p}\mathcal{O}_L) \cap \mathcal{O}_K \supset \mathfrak{p}$$

$\overset{\text{Lie}}{\Rightarrow} \mathfrak{P}_i \cap \mathcal{O}_K, \mathfrak{p}$ maximal $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$

Sei umgekehrt $\mathfrak{P} \subset \mathcal{O}_L$ PI mit $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, so gilt

$$\mathfrak{P} \supset \mathfrak{p}\mathcal{O}_L \Rightarrow \mathfrak{P} \cap \mathcal{O}_K \mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$$

$\overset{\text{Eind. von } (*)}{\Rightarrow} \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$

$\overset{\text{Eind.}}{\Rightarrow} \mathfrak{P} = \mathfrak{P}_i$ für ein i. ☐

Def: Ein PI $\mathfrak{P} \subset \mathcal{O}_L$ mit $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ heißt auch Primideal-Teiler von $\mathfrak{p}$.

Der Exponent e_i heißt Verzweigungsordnung von $\mathfrak{P}_i$.

Der Grad der Erw. $\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}$

$$f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

heißt Trägheitsgrad von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Satz 3: Bei obiger Notation gilt

$$\sum_{i=1}^{r} e_i f_i = n.$$

Bew: Nach dem chinesischen Restsatz gilt

$$\mathcal{O}_K/p\mathcal{O}_K \cong \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^{e_i}$$

$\mathcal{O}_K/p\mathcal{O}_K$ und $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ sind VR über $\mathcal{O}_K/p =: k$

$\Rightarrow$ genügt zu zeigen:

1) $\dim_k \mathcal{O}_K/p\mathcal{O}_K = n$

2) $\dim_k \mathcal{O}_K/\mathfrak{p}_i^{e_i} = e_i f_i$

Zu 1: $\mathcal{O}_K$ ist endl. erz. $\mathbb{Z}$-Modul

$\Rightarrow$ z.e. $\mathcal{O}_K$-Modul.

$\Rightarrow \dim_k \mathcal{O}_K/p\mathcal{O}_K < \infty$.

Seien $w_1, \dots, w_n \in \mathcal{O}_K$, so dass ihre Restklassen $\bar{w}_1, \dots, \bar{w}_n \in \mathcal{O}_K/p\mathcal{O}_K$ eine k-VR Basis bilden.

Z.z.: $w_1, \dots, w_n$ bilden Basis von L/K.

z.z.: $w_1, \dots, w_n$ K-lin. unabh.

$\Rightarrow \mathcal{O}_K$ lin. unabh.

$\exists\, a_1, \dots, a_n \in \mathcal{O}_K$:

$$a_1 w_1 + \dots + a_n w_n = 0$$

Sei $w = (a_1, \dots, a_n) \in \mathcal{O}_K$.

$w \neq 0 \Rightarrow \exists\, r$

$\Rightarrow \exists\, a \in \mathcal{O}_K \setminus \mathcal{O}_K p$ (d.h. $a \notin p$)

$\Rightarrow a a_1, \dots, a a_n \in \mathcal{O}_K$ sind nicht alle durch p teilbar.

$\Rightarrow \alpha a_1 w_1 + \ldots + \alpha a_m w_m \equiv 0$ (mod $\mathfrak{p}$)

gibt nicht-triviale Lin. Relation. ↯

<u>$w_1, \ldots, w_m$ erzeugen $\mathcal{O}_L$</u>:

Betr. die $\mathcal{O}_K$-Moduln

$M = \mathcal{O}_K w_1 + \ldots + \mathcal{O}_K w_m$, $N = \mathcal{O}_L / M$.

Es ist $M \to \mathcal{O}_L / \mathfrak{p}\mathcal{O}_L$ surj.

$\Rightarrow \mathcal{O}_L = M + \mathfrak{p}\mathcal{O}_L$ als $\mathcal{O}_K$-Moduln.

$\Rightarrow \mathfrak{p}N = (\mathfrak{p}\mathcal{O}_L + M)/M = \mathcal{O}_L/M = N$.

$\mathcal{O}_L$ endl. erz. $\Rightarrow N$ endl. erz.

Seien $\alpha_1, \ldots, \alpha_s$ Erzeuger von N als $\mathcal{O}_K$-Modul.

$N = \mathfrak{p}N \Rightarrow \alpha_i = \sum_{j=1}^{s} a_{ij} \alpha_j$ mit $a_{ij} \in \mathfrak{p}$.

Sei $A = (a_{ij}) - I \in \mathcal{O}_K^{s \times s}$.

Sei $A^* \in \mathcal{O}_K^{s\times s}$ die zu A adj-Matrix, d.h.

$$AA^* = A^*A = \det(A) =: d$$

Es gilt $A\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_s\end{pmatrix} = 0$

$$\Rightarrow 0 = A^*A\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_s\end{pmatrix} = d \cdot \begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_s\end{pmatrix}.$$

$\Rightarrow \quad dN = 0$

$\Rightarrow \quad d\,\mathcal{O}_L \subset M = \mathcal{O}_K w_1 + \ldots + \mathcal{O}_K w_m$.

Wegen $a_{ij} \in \mathfrak{p}$ $\forall i,j$ ist

$d = \det A \equiv (-1)^s$ ($\mathfrak{p}$) $\Rightarrow d \neq 0$.

$\Rightarrow L \cdot \alpha L = K w_1 + \dots + K w_n$.

Also ist $w_1, \dots, w_n$ K-Basis von L.

2) Klar: $\mathcal{O}_L / \mathfrak{p}_i^{e_i} = e_i f_i$.

Für die Kette von $\mathcal{O}_L$-UR:

$$\mathcal{O}_L/\mathfrak{p}_i^{e_i} \supset \mathfrak{p}_i/\mathfrak{p}_i^{e_i} \supset \mathfrak{p}_i^2/\mathfrak{p}_i^{e_i} \supset \dots \supset \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} \supset (0)$$

die Quot $\mathfrak{p}_i^{\nu}/\mathfrak{p}_i^{\nu+1} \cong \mathcal{O}_L/\mathfrak{p}_i$ (klarer).

$$\left(\mathfrak{p}_i^{\nu}/\mathfrak{p}_i^{e_i}\right) / \left(\mathfrak{p}_i^{\nu+1}/\mathfrak{p}_i^{e_i}\right)$$

haben also $\mathcal{O}_L$-UR $\mathfrak{p}_i$.

$\Rightarrow$ Beh. $\square$

L/K sep

$\gamma \in \mathcal{O}_L$ primit. El. [also $L = K(\gamma)$.]

$P(X) \in \mathcal{O}_K[X]$ Min-Pol von γ.

$\mathcal{O}' := \mathcal{O}_K[\gamma] \subset \mathcal{O}_L$ Unterring,

$\mathcal{O}_K$ Unterring v. endl. Index.

Der Beweis von $\mathcal{O}'$ ist der alte

$\mathcal{F} = \{\mathfrak{A} \subset \mathcal{O}_L : \mathfrak{A} \subset \mathcal{O}'\}$

$=$ projektiv Ideal von $\mathcal{O}_L$, welches in $\mathcal{O}'$ liegt.

- $\mathcal{F} \neq \emptyset$, da $\mathcal{O}_L$ e.e. $\mathcal{O}_K$-Modul.

$\Rightarrow$ $\mathfrak{p}$ ist endl. viele Primideale.

Satz 4: Sei $p \in \mathbb{Q}$ PZ, eigentl. zerf. Fall in $\mathcal{O}_L$ (d.h. $p\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$). Sei

$$\bar{P}(X) = \bar{P}_1(X)^{e_1} \cdot \ldots \cdot \bar{P}_r(X)^{e_r}$$

die Faktorisierung von $\bar{P}(X) = P(X)$ mod p in $\mathcal{O}_K/p[X]$ in irred. Pol., wobei $P_i \in \mathcal{O}_K[X]$ normiert mit $\bar{P}_i(X) = P_i(X)$ mod p.
Dann setzt

$$\mathfrak{P}_i = p\mathcal{O}_L + P_i(\Theta)\mathcal{O}_L, \quad i = 1, \ldots, r$$

die ersten r über p.
Der Trägheitsgrad f_i von $\mathfrak{P}_i$ ist $\deg \bar{P}_i(X)$, und

$$p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

Bsp: $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathcal{O}_L = \mathbb{Z}[i]$
$\Theta = i \Rightarrow \mathcal{O}_L' = \mathcal{O}_L$, $\mathfrak{F} = (1)$.

Sei $p = (q) \subset \mathbb{Z}$ PZ ($q \in \mathbb{N}$ PZ)
$P(X) = X^2 + 1 \in \mathbb{Z}[X]$

$$\bar{P}(X) = X^2 + 1 \in \mathbb{Z}_q[X] = \mathbb{F}_q[X]$$

1.) q irred. $\Leftrightarrow -1$ kein Quadrat in $\mathbb{F}_q^\times$
$\Leftrightarrow \mathbb{F}_q^\times \not\cong \mathbb{Z}/4\mathbb{Z}$
$\Leftrightarrow q \not\equiv 3 \pmod 4$
$\overset{\text{Satz 4}}{\Rightarrow}$ $q\mathbb{Z}[i] \subset \mathbb{Z}[i]$ prim.

2.) q red. $\Leftrightarrow -1$ ein Quadrat in $\mathbb{F}_q$
$\Leftrightarrow q \not\equiv 3 \pmod 4$
$\Leftrightarrow q\mathbb{Z}[i] \subset \mathbb{Z}[i]$ nicht prim.

Dann ex $b \in \mathbb{Z}$ mit

$$-1 \equiv b^2 \ (q)$$

$$\Rightarrow \bar{p}(X) = (X+b)(X-b) \in \mathbb{F}_q[X].$$

$$= \begin{cases} (X+b)^2 & \text{falls } q = 2 \\ (X+b)(X-b) & \text{mit coprimen verschiedenen Faktoren falls } q \equiv 1 \ (4). \end{cases}$$

$$\Rightarrow q\mathbb{Z}[i] = \begin{cases} (q, b+i)^2 & , q = 2 \\ (q, b+i)(q, b-i) & , q \equiv 1 \ (4) \\ (q) & , q \equiv 3 \ (4) \end{cases}$$

ist die PI-Faktorisierung von q in $\mathbb{Z}[i]$.

<u>Bew von Satz 4:</u>

Sei $\mathcal{O}_L' = \mathcal{O}_K[\theta]$, $k = \mathcal{O}_K/p$.

1) Es ist $f(\theta) \leftarrow f(X)$ (unabhängig der Vertr.)

$$\mathcal{O}_L/p\mathcal{O}_L \cong \mathcal{O}_L'/p\mathcal{O}_L' \cong k[X]/(\bar{p}(X)) =: R$$

Erstes Iso:

p coprim zu $\mathfrak{F}$ $\Rightarrow p\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$

$\mathfrak{F} \subset \mathcal{O}_L'$

$\Rightarrow \mathcal{O}_L = p\mathcal{O}_L + \mathcal{O}_L'$

$\Rightarrow$ Der Hom $\mathcal{O}_L' \longrightarrow \mathcal{O}_L/p\mathcal{O}_L$ ist surj.

Er hat Kern $\mathcal{O}_L' \cap p\mathcal{O}_L = p\mathcal{O}_L'$. ✓

$p\mathcal{O}_L' \subset \mathcal{O}_L' \cap p\mathcal{O}_L$ klar.

$$\mathcal{O}_L' \cap p\mathcal{O}_L \overset{(p + \mathfrak{F} \cap \mathcal{O}_K) = 1}{=} (p + \mathfrak{F} \cap \mathcal{O}_K) \cdot \mathcal{O}_L' \cap p\mathcal{O}_L$$

$$= \underbrace{p(\mathcal{O}_L' \cap p\mathcal{O}_L)}_{\subset p\mathcal{O}_L'} + \underbrace{\mathfrak{F} \cap \mathcal{O}_K (\mathcal{O}_L' \cap p\mathcal{O}_L)}_{\subset \mathfrak{F} p\mathcal{O}_L = p\mathfrak{F} \subset p\mathcal{O}_L'}$$

($\mathfrak{F} \subset \mathcal{O}_L'$ Ideal)

$$\begin{array}{ccc} L & \supset & \mathcal{O}_L \\ | & & | \\ K & \supset & \mathcal{O}_K \supset \mathfrak{p} \end{array} \qquad k = \mathcal{O}_K/\mathfrak{p}$$

$p(X) \in \mathcal{O}_K[X]$ Reste von Θ über $\mathcal{O}_L$.

$\bar{p}(X) = \bar{p}_1^{e_1} \cdots \bar{p}_r^{e_r} \in k[X]$

$$\begin{array}{ccc} \mathcal{O}_K[X]/(p(X)) & \xrightarrow{f \mapsto f(\Theta)}_{\sim} & \mathcal{O}_K[\Theta] = \mathcal{O}_L \\ \downarrow & & \downarrow \\ \left(\mathcal{O}_K[X]/(\mathfrak{p}, p(X))\right) & \xrightarrow{\sim} & \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L'/\mathfrak{p}\mathcal{O}_L' \\ \downarrow z & & \\ R = k[X]/(\bar{p}(X)) & & \downarrow s \quad \text{CRS} \\ \downarrow z \text{ CRS} & & \\ \bigoplus_{i=1}^{r} k[X]/(\bar{p}_i(X)^{e_i}) & \xrightarrow{\sim} & \bigoplus_{i=1}^{r} \mathcal{O}_L/\mathfrak{P}_i^{e_i} \\ \updownarrow \text{i-th place} & & \uparrow \\ (\bar{p}_i(X) + (\bar{p}_i(X))^{e_i}) & \longrightarrow & \overline{\mathfrak{P}_i} + \mathfrak{P}_i^{e_i} \\ & & \| \\ & & (p_i(\Theta) + \mathfrak{P}_i^{e_i}) \end{array}$$

primeideal

Zweites Ziel:

Habe surj. Hom

$\mathcal{O}_K[X] \longrightarrow \mathcal{O}_K[X]/(\bar{p}(X))$ $(\mathcal{O} = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$

Kern $= \mathfrak{p}\mathcal{O}_K[X] + (p(X)) = (\mathfrak{p}, p(X))$.

$\Rightarrow \mathcal{O}_K[X]/(\mathfrak{p}, p(X)) \xrightarrow{\sim} \mathcal{O}[X]/(\bar{p}(X))$

Analogerweise: $\mathcal{O}' = \mathcal{O}_K[\theta] = \mathcal{O}_K[X]/(p(X))$

$\Rightarrow \mathcal{O}'/\mathfrak{p}\mathcal{O}' \cong \mathcal{O}_K[X]/(\mathfrak{p}, p(X))$

2) Wegen $\bar{p}(X) = \bar{p}_1(X)^{e_1} \cdot \ldots \cdot \bar{p}_r(X)^{e_r}$ erhält man aus 1 mit dem Chin. RS:

$R := \mathcal{O}[X]/(\bar{p}(X)) \cong \prod_{i=1}^{r} \mathcal{O}[X]/(\bar{p}_i(X))^{e_i}$

$\bar{p}_i(X) \in \mathcal{O}[X]$ sind

$\Rightarrow$ · die $\mathfrak{P}_i$ in R sind die Hauptideale $(\bar{p}_i(X))$ erz. von den $\bar{p}_i(X)$ mod $\bar{p}(X)$, $i = 1, \ldots, r$.

· $[R/\mathfrak{P}_i : \mathcal{O}] = \operatorname{grad}(\bar{p}_i)$

· $(0) = (\bar{p}(X)) = \prod_{i=1}^{r} (\bar{p}_i)^{e_i}$ in R.

3) Wegen des Isos

$R = \mathcal{O}[X]/(\bar{p}(X)) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}\mathcal{O}$

$f(X) \mapsto f(\theta)$

folgt im $\mathcal{O}/\mathfrak{p}\mathcal{O}$ die analoge Aussage.

$\Rightarrow$ Die $\mathfrak{P}_i$ $\bar{\mathfrak{P}}_i = \mathcal{O}/\mathfrak{p}\mathcal{O}$

entsprechen den PI $(\bar{p}_i) \subset \bar{R}$, sie sind Hauptideale, erz. von

$$p_i(\theta) \text{ und } p\mathcal{O}_L,$$

und $\left[(\mathcal{O}_L/p\mathcal{O}_L)/\bar{P}_i : k\right] = \operatorname{grad} \bar{p}_i(X)$.

Sei $P_i = p\mathcal{O}_L + p_i(\theta)\mathcal{O}_L$ das Urbild von $\bar{P}_i$ bezügl. des kan. Hom $\mathcal{O}_L \to \mathcal{O}_L/p\mathcal{O}_L$.

Dann sind die P_i, $i=1,\dots,r$, die PI in $\mathcal{O}_L$ über p,
$f_i = [\mathcal{O}_L/P_i : k] = \operatorname{grad}(\bar{p}_i(X))$.

$P_i^{e_i}$ ist das Urbild von $\bar{P}_i^{e_i}$. Übung
$\Rightarrow p\mathcal{O}_L = \prod_{i=1}^{r} P_i^{e_i}$. □

Sei $p \subset \mathcal{O}_K$ prim,

(*) $p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$, $\quad \sum_{i=1}^{r} e_i f_i = n$

die PI-Zerlegung in $\mathcal{O}_L$. $n = [L:K]$.

- p heißt vollständig zerlegt in L, falls $r = n$.
  Dann gilt $e_i = f_i = 1 \ \forall i$.
- p heißt unzerlegt, falls $r = 1$.
  Dann ist
  $$p\mathcal{O}_L = P^e$$
- Ein PI P_i in (*) heißt unverzweigt über K, falls $e_i = 1$.

- Ist $e_i > 1$, so heißt P_i verzweigt.
  Ist $e_i > 1$ und $f_i = 1$, so heißt
- P_i total verzweigt über K.

- $L|K$ heißt unverzweigt, falls alle PI $p \subset O_K$ unverzweigt in L sind.

Satz 5: Es gibt nur endl. viele PI $p \subset O_K$, die in L verzweigt sind.

Bew 5: Sei $\Theta \in O_L$ prim. El. für $L|K$.
Sei $p(X) \in O_K[X]$ das Minpo von Θ,
$d = d(1, \Theta, \dots, \Theta^{n-1}) = \prod_{i<j} (\Theta_i - \Theta_j)^2 \in O_K$
die Diskriminante von p (Vandermonde Det, $\Theta_i = \tau_i(\Theta) \in \mathbb{C}$)

Es gilt $d = 0 \iff p(X)$ hat mehrfache Nullst.
Also $d \neq 0$.
Sei $p \subset O_K$ PI, coprim zu d und zum Führer F von $O_K[\Theta]$.
Dann ist p unverzweigt.
Bew: Nach Satz 4 entsprechen die Exp. e_i in

$$pO_L = P_1^{e_1} \cdots P_r^{e_r}$$

den Exp in

$$O_K[X] \ni p(X) = p_1(X)^{e_1} \cdots p_r(X)^{e_r},$$

wobei $\bar{p}_i \in O_K/p[X]$ irred. [illegible]

$\mathfrak{p}, (d)$ coprim
$\Rightarrow 0 \neq \bar{d} \in \mathcal{O}_K/\mathfrak{p}$

$\Rightarrow \bar{f}(X) \in \mathcal{O}_K/\mathfrak{p}\,[X]$ hat keine mehrfachen Nullst. in alg. Abschluss
$\Rightarrow e_1 = \dots = e_r = 1$.
$\Rightarrow \mathfrak{p}$ unverzweigt. $\square$

Def: Die Diskriminante von L/K ist das Ideal $\mathfrak{d} \subset \mathcal{O}_K$, erzeugt von allen

$d(\omega_1, \dots, \omega_n)$,

wobei $(\omega_1, \dots, \omega_n)$ durch alle ganzen Basen von L/K läuft.

Es ist $\mathfrak{d} \neq 0$.

Bem 6: $\mathfrak{p} \subset \mathcal{O}_K$ ist verzweigt in $L \iff \mathfrak{p} \mid \mathfrak{d}$.

Bew: Neukirch Kap. III §2.

Bsp: $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$
$\mathfrak{p} = (q) \subset \mathbb{Z}$, $q \in \mathbb{N}$ Primzahl

(q) verzweigt in $L \iff q = 2$
(vollst.) zerlegt " " $\iff q \equiv 1\ (4)$
unzerlegt " " $\iff q \equiv 3\ (4)$

M: p 92 # 33–39
N: p 53 # 1, 2, 8

§2 Weitere Verzweigungstheorie

Annahme: L/k sei Galois-
Erweiterung vom Zahlkörper,
$[L:k] = n$

$G = Gal(L/k)$.

G operiert $\Rightarrow$ symmetrische Eigenschaften.

- G op. auf L.
- $a \in \mathcal{O}_L$, $\sigma \in G \Rightarrow \sigma a \in \mathcal{O}_L \Rightarrow G$ op. auf $\mathcal{O}_L$
- G op auf Teilen $A \subset \mathcal{O}_L$
  $\sigma A = \{\sigma a ; a \in A\}$.
- " " Primideale.
- Sei $P \subset \mathcal{O}_L$ PI über $p = P \cap \mathcal{O}_k \subset \mathcal{O}_k$.
  $\Rightarrow \sigma P \subset \mathcal{O}_L$ " " "
  $\Rightarrow G$ op auf PI über p.

Bem 1:
G operiert transitiv auf der Menge der PI $P \subset \mathcal{O}_L$ über $p \subset \mathcal{O}_k$.

Bew: Sei $P, P' \subset \mathcal{O}_L$ PI über p.
Ang. $\sigma P \neq P'$ $\forall \sigma \in G$.
Dann $\exists \Rightarrow \exists x \in \mathcal{O}_L$ s.d.
i) $x \equiv 0 \pmod{P'}$
ii) $x \equiv 1 \pmod{\sigma P}$ $\forall \sigma \in G$.

$N_{L/k}(x) = \prod_{\sigma \in G} \sigma(x) \overset{(i)}{\in} P' \cap \mathcal{O}_k = p$.

Anderungen:

(ii) $\nu \nmid r \Rightarrow \nu \nmid \sigma r \quad \forall \sigma \in G_K$.

$\Rightarrow \sigma \nu \nmid \mathfrak{P} \quad \forall \sigma \in G_K$.

$\Rightarrow N_{L/K}(\nu) = \prod_{\sigma \in G_K} \sigma(\nu) \nmid \mathfrak{P} \cap O_K = p$. ↯

Def: Sei $\mathfrak{P} \subset O_L$ PI.

Der Zerlegungsgruppe

$$G_{\mathfrak{P}} = \{\sigma \in G_K : \sigma \mathfrak{P} = \mathfrak{P}\} \leq G_K$$

von $\mathfrak{P}$ heißt Zerlegungsgruppe von $\mathfrak{P}$ über K.

Der Fixkörper

$$Z_{\mathfrak{P}} = \{x \in L : \sigma x = x \ \forall \sigma \in G_{\mathfrak{P}}\}$$

heißt Zerlegungskörper von $\mathfrak{P}$ über K.

Satz 2: Hilbert Zerlegung

L/K GE $\Rightarrow$ $\mathfrak{P}$ in O_L eindeutig.

$G_{\mathfrak{P}} \mapsto \sigma \mathfrak{P}$

$\cdot$ $|G_K : G_{\mathfrak{P}}| = \#$ $\mathfrak{P}$ in O_L über p.

$\cdot$ $G_{\mathfrak{P}} = 1 \Leftrightarrow p$ ein Hilbert Zerlegt

$\Leftrightarrow Z_{\mathfrak{P}} = L$

$\cdot$ $G_{\mathfrak{P}} = G_K \Leftrightarrow p$ ist unverzweigt $\Leftrightarrow Z_{\mathfrak{P}} = K$

Satz 3: $G_{\sigma \mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$.

Satz 4: Sei $p \in O_K$ PI unverz.

$$p O_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

Sei P Z.-Zerlegung in $\mathcal{O}_L$.
Seien $\mathfrak{f}_1, \dots, \mathfrak{f}_r$ die Trägheitsgrade
über p.
Es gelte $e_1 = \dots = e_r =: e$ und
$f_1 = \dots = f_r =: f$.
$n = efr$.

Satz: Sei $P = \mathfrak{P}_1$ und
$\mathfrak{P}_i = \sigma_i(\mathfrak{P})$ mit $\sigma_i \in G$.
$\sigma_i : \mathcal{O}_L \to \mathcal{O}_L$ Isomorph.
Ind. $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\sigma_i\mathfrak{P}$

$\Rightarrow f_i = [\mathcal{O}_L/\sigma_i\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = f = f_1$ b.i.

2) Aus $\sigma_i(p\mathcal{O}_L) = p\mathcal{O}_L$ folgt

$\mathfrak{P}^\nu \mid p\mathcal{O}_L \iff \sigma_i(\mathfrak{P})^\nu \mid p\mathcal{O}_L$

$\Rightarrow e_i = e_1$ b.i.

3) $n = efr$ folgt aus §1, Satz 3.

Satz 5: Sei $\mathfrak{P}_Z = \mathfrak{P} \cap \mathbb{Z}_p$ die $\mathfrak{P}$-
un $\mathcal{O}_{\mathbb{Z}_p} = \mathcal{O}_L \cap \mathbb{Z}_p$ maximal, $\mathfrak{P} \subset \mathcal{O}_L$.
i) $\mathfrak{P}_Z$ ist unverzweigt in L.
(d.h. $\mathfrak{P}\mathcal{O}_L = \mathfrak{P}$)
ii) $\mathfrak{P}$ hat über $\mathbb{Z}_p$ Vertretersystem
$1, \alpha, \dots, \alpha^{f-1}$ und Trägheitsgrad f.
iii) $\mathfrak{P}_Z$ hat über $\mathbb{Z}_p$ Verzweigungs-
index e und Trägheitsgrad 1.

Beweis: i) $Z_\mathfrak{P} = L^{G_\mathfrak{P}}$

$\Rightarrow \mathrm{Gal}(L/Z_\mathfrak{P}) = G_\mathfrak{P}$

Satz 1 $\Rightarrow$ Primideale $\subset \mathcal{O}_L$ über $\mathfrak{P}_Z$ sind $\sigma\mathfrak{P}$ für $\sigma \in G_\mathfrak{P}$.

Davon ist eins $= \mathfrak{P}$.

(ii+iii) L/K Galois $\Rightarrow e_i = e \quad \forall i$,

$f_i = f \quad \forall i$, $n = efr$.

Es ist $n = \#G$

Satz 2 $\Rightarrow r = [G : G_\mathfrak{P}]$

$$\Rightarrow [L : Z_\mathfrak{P}] = \#G_\mathfrak{P} = \frac{\#G}{[G:G_\mathfrak{P}]} = \frac{efr}{r} = ef.$$

Sei e' = Verzweigungsindex von $\mathfrak{P}$ über $Z_\mathfrak{P}$

e'' = " " $\mathfrak{P}_Z$ " K

$\Rightarrow \mathfrak{p} = \mathfrak{P}_Z^{e''}$ enthält $\mathfrak{P}_L$ in $Z_\mathfrak{P}$

$\mathfrak{P}_Z = \mathfrak{P}^{e'}$ in L

$\Rightarrow \mathfrak{p} = \mathfrak{P}^{e'e''}$ ... in L

$\Rightarrow e = e'e''$

Eine analoge Aussage gilt für den Trägheitsgrad:

$f = f'f''$

L. P. Satz 4 für $L/Z_\mathfrak{P} \Rightarrow [L : Z_\mathfrak{P}] = e'f'$

!! ef

$Z_\mathfrak{P}$ $\mathfrak{P}_Z$ $\Rightarrow e''f'' = 1$ $\qquad ef = e'f'e''f''$

" " " $\Rightarrow e'' = f'' = 1$ und $e = e'$, $f = f'$. ☐

K. p

Bem 6 Jedes $\sigma \in G_\mathfrak{p}$ induziert einen Automorphismus

$$\bar{\sigma}: \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$$
$$a \bmod \mathfrak{P} \to \sigma a \bmod \mathfrak{P}$$

des Restklassenkps $\mathcal{O}_L/\mathfrak{P}$,

da $\sigma \mathcal{O}_L = \mathcal{O}_L$ und $\sigma \mathfrak{P} = \mathfrak{P}$.

Satz 7 Setze $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ und $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$.

Die Erweiterung $\kappa(\mathfrak{P}) \mid \kappa(\mathfrak{p})$ ist normal, und man hat einen surjektiven Homomorphismus

$$G_\mathfrak{P} \to G(\kappa(\mathfrak{P}) \mid \kappa(\mathfrak{p})).$$

Beweis: Der Trägheitsgrad von $\mathfrak{P}_Z$ über K ist gleich 1,

d.h. $Z_\mathfrak{P}/\mathfrak{P}_Z = K/\mathfrak{p} = \kappa(\mathfrak{p})$.

Also OE $Z_\mathfrak{P} = K$, $G_\mathfrak{P} = G$.

Sei $\theta \in \mathcal{O}_L$ Repräsentant v. $\bar{\theta} \in \kappa(\mathfrak{P})$

mit Mipo v. θ über K $f(X)$ und v. $\bar{\theta}$ über $\kappa(\mathfrak{p})$ gleich $\bar{g}(X)$

Dann ist $\bar{\theta} = \theta \bmod \mathfrak{p}$ NS von $\bar{f}(X) = f(X) \bmod \mathfrak{p}$

$\Rightarrow \bar{g}(X) \mid \bar{f}(X)$.

Da L/K normal zerfällt $f(X)$ über $\mathcal{O}_L$ in Linearfaktoren

also zerfällt auch $\bar{f}(X)$ und folglich auch $\bar{g}(X)$ über

$\kappa(\mathfrak{P})$ in Linearfaktoren. $\Rightarrow \kappa(\mathfrak{P}) \mid \kappa(\mathfrak{p})$ normal.

Sei $\bar{\theta}$ ein primitives Element für $k(\mathfrak{P})|k(\mathfrak{p})$ ~~(separabel!)~~ (falls $k(\mathfrak{P})|k(\mathfrak{p})$ sep. sonst für max. sep. Teilerweiterung) und sei

$$\bar{\sigma} \in G(k(\mathfrak{P})|k(\mathfrak{p})) = G(k(\mathfrak{p})(\bar{\theta})|k(\mathfrak{p})).$$

Dann ist $\bar{\sigma}\bar{\theta}$ NS von $\bar{g}(X)$, also, da $\bar{f}(X) | \bar{g}(X)$, von $\bar{f}(X)$.
Es gibt also eine NS θ' von $f(X)$ mit

$$\theta' \equiv \bar{\sigma}\bar{\theta} \bmod \mathfrak{P},$$

Man hat $\theta' = \sigma\theta$ mit einem $\sigma \in G(L|K)$.
Wegen $\sigma\theta \equiv \bar{\sigma}\bar{\theta} \bmod \mathfrak{P}$ wird σ auf $\bar{\sigma}$ abgebildet, also ist der Homomorphismus surjektiv. □

Def: Der Kern $J_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$ des Homomorphismus

$$G_{\mathfrak{P}} \to G(k(\mathfrak{P})|k(\mathfrak{p}))$$

heißt Trägheitsgruppe von $\mathfrak{P}$ über K.

Der Fixkp. $T_{\mathfrak{P}} = \{x \in L \mid \sigma x = x \quad \forall \sigma \in J_{\mathfrak{P}}\}$

heißt Trägheitskp. von $\mathfrak{P}$ über K.

Bem 8 $K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$

nun hat man eine exakte Sequenz

$$1 \to J_{\mathfrak{P}} \to G_{\mathfrak{P}} \to G(k(\mathfrak{P})|k(\mathfrak{p})) \to 1$$

Lz 9 Die Kp.erweiterung $T_\mathfrak{P} | Z_\mathfrak{P}$ ist normal und es gilt

$$G(T_\mathfrak{P} | Z_\mathfrak{P}) \cong G(\kappa(\mathfrak{P}) | \kappa(\mathfrak{p})), \quad G(L | T_\mathfrak{P}) = J_\mathfrak{P}.$$

Es sei nun $\kappa(\mathfrak{P}) | \kappa(\mathfrak{p})$ separabel.

Man hat dann

$$\# J_\mathfrak{P} = [L : T_\mathfrak{P}] = e,$$

$$(G_\mathfrak{P} : J_\mathfrak{P}) = [T_\mathfrak{P} : Z_\mathfrak{P}] = f,$$

und für das unter $\mathfrak{P}$ liegende Primideal $\mathfrak{P}_T$ von $T_\mathfrak{P}$ gilt:

(i) Der Verzweigungsidx. von $\mathfrak{P}$ über $\mathfrak{P}_T$ ist e und der Trägheitsgrad ist 1.

(ii) Der Verzweigungsidx. von $\mathfrak{P}_T$ über $\mathfrak{P}_Z$ ist 1 und der Trägheitsgrad ist f.

Bew: Wegen $\# G_\mathfrak{P} = ef$ genügt es, (i) und (ii) zu zeigen.

Wir zeigen zunächst $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$:

Die Trägheitsgrp. $J_\mathfrak{P}$ von $\mathfrak{P}$ über k ist gleichzeitig die Trägheitsgrp. von $\mathfrak{P}$ über $T_\mathfrak{P}$.

Satz 7 auf $L | T_\mathfrak{P}$ hier $\kappa(\mathfrak{P})$ und $\kappa(\mathfrak{P}_T)$
" $L/\mathfrak{P}$ $T_\mathfrak{P}/\mathfrak{P}_T$

$\Rightarrow G(\kappa(\mathfrak{P}) | \kappa(\mathfrak{P}_T)) = 1$

also $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P})$.

Mit der Gln $n = ef$ folgen nun (i) und (ii).

□

Verzweigungsideal

$$K \overset{1}{\underset{1}{\rightarrow}} Z_{\mathfrak{P}} \overset{1}{\underset{f}{\rightarrow}} T_{\mathfrak{P}} \overset{e}{\underset{1}{\rightarrow}} L$$

Trägheitsgrade

- Es gilt, falls $k(\mathfrak{P})/k(\mathfrak{p})$ separabel,

  $f_{\mathfrak{P}} = 1 \iff T_{\mathfrak{P}} = L \iff \mathfrak{p}$ ist unverzweigt in L

  in diesem Fall kann man

  $G(k(\mathfrak{P})/k(\mathfrak{p})) \simeq G_{\mathfrak{P}}$ als Untergrpp. von $G = G(L/K)$ auffassen.