Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z14: PIZ in normalen Erweiterungen

Stichworte: $L|K$ normal $\Rightarrow$ alle e_i gleich,
und je zwei $\mathfrak{q}_i$ über $\mathfrak{p}$ werden von einem El. $\sigma \in Gal(L|K)$ aufeinander abgebildet.

14.1. **Einleitung:** Wir zeigen im Spezialfall einer normalen ZKerweiterung $L|K$, dass sich jedes Primideal $\mathfrak{p}$ (im ZR von K) im ZR von L als Produkt von Primidealen $\mathfrak{q}_i$ von allesamt derselben Multiplizität, d.h. mit demselben Verzweigungsindex, zerlegen lässt. Das trifft z.B. für quadratische ZK und KTK zu, vgl. Bsp. 13.2 und 13.4.
Die $\mathfrak{q}_i$ werden dabei von Elementen der Galoisgruppe aufeinander abgebildet.

14.2. **Vor.:** In diesem Kapitel seien stets $L|K$ Zahlkörper mit $L|K$ normal, und $A \subseteq B$ die Zahlringe von $K \subseteq L$.

14.3. **Lemma:** Seien $\mathfrak{q}, \mathfrak{q}' \in \mathcal{P}(B)$ mit $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$.
Dann ex. ein $\sigma \in Gal(L|K)$ mit $\sigma\mathfrak{q} = \mathfrak{q}'$.

Bew.: Sei $G := Gal(L|K)$, $\mathfrak{q} \neq \mathfrak{q}'$ und $\mathfrak{p} \subseteq \mathfrak{q} \cap \mathfrak{q}'$ prim in A.
Ann.: $\forall \sigma \in G: \sigma\mathfrak{q} \neq \mathfrak{q}'$.
Nach dem chinesischen Restsatz ex. ein $x \in B = L \cap \mathbb{A}$ mit $x \equiv \begin{cases} 0 \bmod \mathfrak{q}', \\ 1 \bmod \sigma\mathfrak{q} \text{ für alle } \sigma \in G. \end{cases}$
Nun ist
$N_K^L(x) = \prod_{\sigma \in G} \sigma x \in \mathfrak{q}' \cap K = \mathfrak{p} = \mathfrak{q} \cap K$, also $\exists \sigma \in G: \sigma x \in \mathfrak{q}$.
Es folgt: $x \in \sigma^{-1}\mathfrak{q}$, im $\lightning$ zu $x \equiv 1 \pmod{\sigma^{-1}\mathfrak{q}}$. $\square$

14.4. **Kor.:** Sei $L|K$ normal, $A \subseteq B$ seien die Zahlringe von $K \subseteq L$, $\mathfrak{p}$ sei Primideal von A. Dann gilt: Alle $\mathfrak{q} \in \mathcal{P}(B)$ mit $\mathfrak{p} \subseteq \mathfrak{q}$ haben denselben Verzweigungsindex, d.h. $B\mathfrak{p} = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^e$ für ein $e \in \mathbb{N}$, $\mathfrak{q}_i \in \mathcal{P}(B)$.

Bew.: Sei $B\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$. Ist dann $\sigma\mathfrak{q}_i = \mathfrak{q}_j$ für $\sigma \in G$ und $1 \leq i \neq j \leq r$, so folgt wegen $\mathfrak{p} \subseteq K$:
$B\mathfrak{p} = \sigma(B\mathfrak{p}) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_j^{e_i} \cdots \mathfrak{q}_i^{e_j} \cdots \mathfrak{q}_r^{e_r}$, wegen der eind. PIZ also $e_i = e_j$. Induktiv folgt: $e_1 = \ldots = e_r =: e$. $\square$