25. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehéricy, Simon Müller

WS 2016/2017: 14. Februar 2017

Bemerkung 1

Sei E/F eine endliche (i.e. endlich dimensionale) separable Erweiterung, dann ist E/F endlich erzeugt durch zum Beipsiel $\{a_1, \dots, a_n\}$, a_i algebraische und separable Elemente.
Sei $f_i(x)$ das Minimalpolynom von a_i, $f_i(x)$ ist separabel irreduzibel. Œ $f_i \neq f_j$ für $i \neq j$.
Setze $f(x) := \prod_{1 \leq i \leq n} f_i(x)$. $f(x)$ ist separabel.
Setze $K :=$ Zerfällungskörper von $f(x)$ über E. Da $K \supseteq F(a_1, \dots, a_n)$ ist es klar, dass K auch Zerfällungskörper von $f(x)$ über F ist.

(1) So ist K/F normal. Andererseits enthält jede normale Erweiterung von E einen Zerfällungskörper für $f(x)$ über F.

(2) Also damit enthält jede normale Erweiterung von E eine isomorphe Kopie von K.

(3) Also ist K bis Isomorphie eindeutig bestimmt durch E unabhängig von der Wahl der Erzeuger $\{a_1, \dots, a_n\}$

Definition 1

K/F ist die *normale Hülle* von E/F.

Kapitel 6: Einige Anwendungen der Galois Theorie

Satz 1 Satz vom primitiven Element
Es sei E/F eine endliche separable Körpererweiterung. Dann existiert ein primitives Element zu E/F, das heißt ein Element $z \in E$ mit $E = F(z)$.

Wir brauchen einen
Satz 2 (Hilfssatz) (F-Körper)
Sei F ein Körper. Sei G eine endliche Untergruppe von $F^\times$. Dann ist G zyklisch.

Dafür brauchen wir eine Definition und eine Proposition.

Definition
Sei G eine endliche Gruppe $G \neq \{1\}$. Setze $\gamma(G) :=$ die kleinste $\gamma \in \mathbb{N}$, so dass $x^\gamma = 1$ für alle $x \in G$.
Bemerkung: Lagrange $\Rightarrow \gamma(G) \leq |G|$.

Proposition 1 (Char endlich zyklische Gruppen)
Sei G eine endliche abelsche Gruppe. Es gilt: G ist zyklisch genau dann, wenn $\gamma(G) = |G|$.

Für den Beweis brauchen wir wiederum zwei Hilfslemmas.

Hilfslemma 1
Seien $g, h \in G$, wobei G eine endliche abelsche Gruppe ist. Wir nehmen an: $ggT(|g|, |h|) = 1$.
Es gilt: $|gh| = |g||h|$.

Beweis
Setze $|g| := m$ und $|h| := n$. Sei $r \in \mathbb{N}$, so dass $(gh)^r = 1$.
Dann ist $k := g^r = h^{-r} \in < g > \cap < h >$, somit $|k||m$ und $|k||n$. Also $|k| = 1$ und $k = 1$.
Wir haben gezeigt: $(gh)^r = 1 \Rightarrow g^r = h^r = 1$. Also $m|r$ und $n|r$ und somit $mn = kgV(m, n)|r$.
Andererseits: $(gh)^{mn} = g^{mn}h^{mn} = 1$. □

Hilfslemma 2
Sei G eine endliche abelsche Gruppe und $g \in G$, so dass $|g|$ maximal ist. Es gilt: $|g| = \gamma(G)$.

Beweis

Sei $h \in G$. Wir zeigen: $h^{|g|} = 1$.

$$\text{Schreibe:}\quad \left.\begin{array}{rcl} |g| & = & p_1^{\ell_1} \cdots p_s^{\ell_s} \\ |h| & = & p_1^{f_1} \cdots p_s^{f_s} \end{array}\right\} p_i \text{ verschiedene Primzahlen; } \ell_i \geq 0, f_i \geq 0$$

Zum Widerspruch sei $h^{|g|} \neq 1$, dann existiert i, so dass $f_i > \ell_i$. Ohne Einschränkung sei $f_1 > \ell_1$. Setze $g' := g^{p_1^{\ell_1}}$ und $h' := h^{p_2^{f_2} \cdots p_s^{f_s}}$. Wir berechnen: $|g'| = p_2^{\ell_2} \cdots p_s^{\ell_s}$ und $|h'| = p_1^{f_1}$,
ggT $(|g'|, |h'|) = 1 \underset{HL1}{\Rightarrow} |g'h'| = p_1^{f_1} p_2^{\ell_2} \cdots p_s^{\ell_s} > |g|$. - Widerspruch $\square$

Beweis von Proposition 1

"$\Rightarrow$" Sei $G =< g >$, dann ist $|G| = |g|$ und damit ist $\gamma(G) = |G|$.

"$\Leftarrow$" Sei G endlich abelsch mit $\gamma(G) = |G|$.

Hilfslemma 2 ergibt: Es existiert ein $g \in G$ mit $|g| = \gamma(G)$ ($|g|$ maximal). Also ist $|g| = |G|$ und damit ist $G =< g >$. $\square$

$$\begin{tikzcd}
 & \text{Satz 1} & \\
\text{Fund. Satz G.T.} \arrow[ur] & & \text{Satz 3 (Steinitz)} \arrow[ul] \\
 & \text{Satz 2} \arrow[ur] & \\
 & \text{Proposition 1} \arrow[u] & \\
 & \text{Hilfslemma 2} \arrow[u] & \\
 & \text{Hilfslemma1} \arrow[u] &
\end{tikzcd}$$

Beweis von Satz 2 (Hilfssatz)

G ist abelsch. Wir zeigen $|G| = \gamma(G) := \gamma$ (Proposition 1). Betrachte $f(x) = x^\gamma - 1$. Das Polynom hat $\leq \gamma$ Nullstellen in $F^\times$, also $\leq \gamma$ Nullstellen in G. Andererseits muss jedes $a \in G$ eine Nullstelle sein, also $|G| \leq \gamma$. $\square$

Korollar 1

Sei F ein endlicher Körper und eine E/F endlich dimensionierte Körpererweiterung. Dann hat E/F ein primitives Element.

Beweis

$E^\times$ ist zyklisch, weil E endlich ist. Sei $E^\times =< z >$, dann ist $E = F(z)$. $\square$

Wir brauchen noch einen Satz:

Satz 3 (Steinitz Char. von einfachen Erweiterungen)

Sei E/F endlich dimensioniert, dann ist E/F einfach $\Leftrightarrow$ es nur endliche viele Zwischenkörper $F \subseteq K'' \subseteq E$ gibt.

Beweis

Siehe nächstes Vorlesungsscript

Beweis von Satz 1

Sei E/F wie in der Aussage und sei K die normale Hülle von E/F, dann ist K/F Galois ($F \subseteq E \subseteq K$, wobei K/F Galois). Dann gibt es nur endlich viele Zwischenkörper $F \subseteq K' \subseteq K$ [weil die genau Inv H sind für eine $H \leq \text{Gal}\ (K/F)$ (Fundamentaler Satz der Galois Theorie). Da aber Gal (K/F) endlich ist, gibt es nur endlich viele solcher Untergruppen H.]

A fortiori gibt es nur endlich viele Zwischenkörper $F \subseteq K'' \subseteq E$. Steinitz impliziert nun, dass E/F einfach ist. $\square$