Algebra BIII

– Kuhlmann –

27. Vorlesung am 11.02.2013.

Bemerkung 1: sei $E \mid F$ eine endliche (d.i. endlichdimensionale) separable Erweiterung, dann ist $E \mid F$ endlich erzeugt durch z.B $\{a_1, \dots, a_n\}$; a_i algebraische und separable Elemente.

Sei $f_i(x)$ das Minimalpolynom von a_i; $f_i(x)$ ist separable irreduzible. Setze

$$f(x) := \prod_i f_i(x) \qquad f(x) \text{ ist separable.}$$

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; so

(1) $K \mid F$ ist normal

Anderseits, jede normale Erweiterung von E enthält einen Zerfällungskörper für $f(x)$ über F

(2) also damit enthält eine isomorphe Kopie von K.

(3) Also ist K bis Isomorphie eindeutig bestimmt durch

unabhängig von der Wahl der Erzeugern $\{a_1, \dots, a_n\}$.

Definition 1: K/F ist die normale Hülle von E/F.

Einige Anwendungen der Galois Theorie.

Wir wollen zeigen:

Satz 1. Satz vom primitiven Element.

Es sei E/F eine endliche separable Körpererw.

Dann existiert ein primitives Element zu E/F,

d. h. eine Element $z \in E$ mit $E = F(z)$.

Wir brauchen einen

satz 2. Satz (Hilfssetz).

Sei G eine endliche Untergruppe von $F^\times$ (F Körper).
Dann ist G zyklisch.

Dafür brauchen wir eine Definition und eine Proposition:

Definition: Sei G eine endliche group; $G \neq \{1\}$.

Setze $\gamma(G) :=$ die kleinste $\gamma \in \mathbb{N}$ so daß

$$x^\gamma = 1 \quad \forall\, x \in G.$$

Bemerkung 2 Lagrange $\Rightarrow \gamma(G) \leq |G|$.

Proposition 1 (Char. endl. zyklische Gruppen).

Sei G eine endliche abelsche Gruppe.

Es gilt: G ist zyklisch gdw $\gamma(G) = |G|$.

Für den Beweis brauchen wir wiederum zwei Hilfslemmas.

HL 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 $k := g^r = h^{-r} \in \langle g \rangle \cap \langle h \rangle$,

somit $|k| \mid m$ und $|k| \mid n$ also $|k| = 1$

und $k = 1$. Wir haben gezeigt:

$(gh)^r = 1 \Rightarrow g^r = h^r = 1$. Also $m \mid r$ und $n \mid r$

und somit $mn = kgV(m,n) \mid r$

Anderseits:

$(gh)^{mn} = g^{mn} h^{mn} = 1.$ ∎

HL2: Sei G endliche abelsche Gruppe;
$g \in G$ so daß $|g|$ maximal ist.

Es gelt: $|g| = \gamma(G)$.

Beweis. Sei $h \in G$; wir zeigen $h^{|g|} = 1$.

Schreibe $|g| = p_1^{e_1} \cdots p_s^{e_s}$
$|h| = p_1^{f_1} \cdots p_s^{f_s}$
} p_i verschiedene Primzahlen; $e_i \geq 0$, $f_i \geq 0$

Zum Widerspruch sei $h^{|g|} \neq 1$, dann $\exists i$ s.d

$f_i > e_i$; OE Sei $f_1 > e_1$.

Setze: $g' := g^{p_1^{e_1}}$ und $h' := h^{p_2^{f_2} \cdots p_s^{f_s}}$

und berechne:

$|g'| = p_2^{e_2} \cdots p_s^{e_s}$ und $|h'| = p_1^{f_1}$

$ggT(|g'|, |h'|) = 1 \underset{HL1}{\Rightarrow} |g'h'| = p_1^{f_1} p_2^{e_2} \cdots p_s^{e_s}$

$> |g|$ ↯ ∎

Beweis von Proposition 1.

"$\Rightarrow$" Sei $G = \langle g \rangle$ dann ist $|G| = \langle g \rangle$ und

damit ist $\gamma(G) = |G|$.

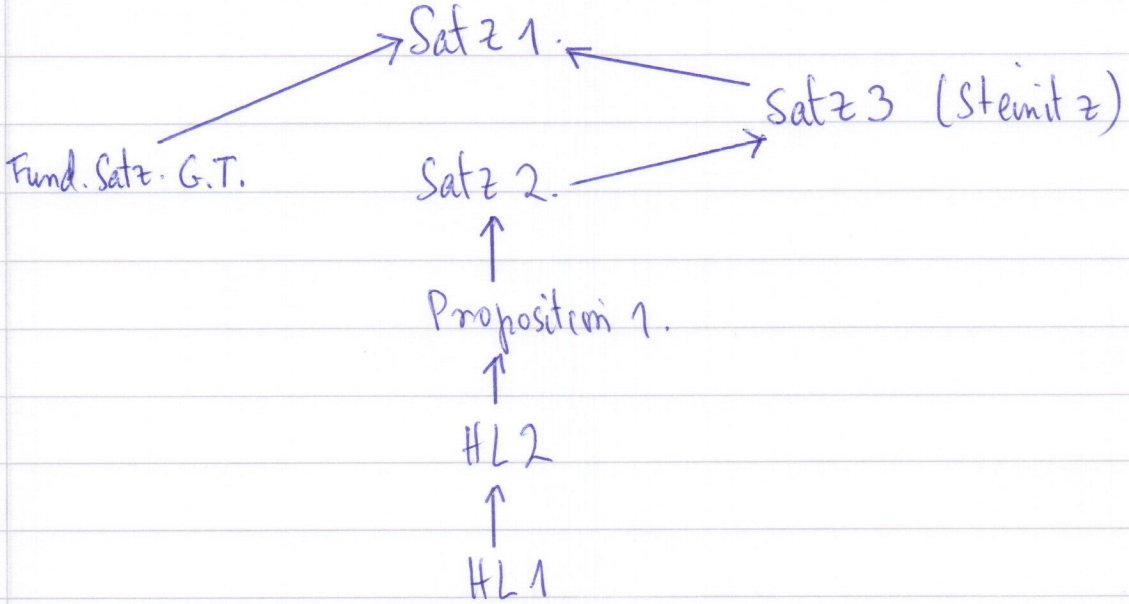
"$\Leftarrow$" Sei G endl. abelsch mit $\gamma(G) = |G|$.

HL 2 $\Rightarrow \exists\, g \in G$ mit $|g| = \gamma(G)$

($|g|$ maximal). Also

$|g| = |G|$ und damit

ist $G = \langle g \rangle$. ∎



Beweis von ~~Proposition 2~~ Satz (Hilfssatz)

G ist abelsch. Wir zeigen $|G| = \gamma(G) := \gamma$ (Prop. 1).

Betrachte $f(x) = x^\gamma - 1$; das Polynom hat

$\leq \gamma$ NS in $F^\times$ also $\leq \gamma$ NS in G;

Anderseits muss jedes $a \in G$ eine NS sein;

also $|G| \leq \gamma$. □

Korollar 1.

Sei F endlicher Körper und E/F endl.

dim. Körpererw., dann hat E/F

ein Primitivelement.

Beweis: $E^\times$ ist zyklisch weil E endlich

ist; sei $E^\times = \langle z \rangle$;

dann ist $E = F(z)$. □

Wir brauchen noch einen Satz:

Satz 3 (Steinitz Char. von einfachen Erw.).

Sei $E|F$ endl. dim; dann ist $E|F$ einfach

$\Leftrightarrow$ es nur endlich viele Zwischenkörper $F \subseteq K'' \subseteq E$ gibt.

Beweis: in der 28. Vor.

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 (Galois: $F \subseteq E \subseteq K$)

Damit gibt es nur endlich viele Zwischenkörper

$F \subseteq K' \subseteq K$ (weil die genau $\mathrm{Inv}\, H$

sind für eine $H \leq \mathrm{Gal}(K|F)$ (Fund. Satz 6.T)

da aber $\mathrm{Gal}(K|F)$ endlich ist; gibt es nur

endlich viele solche Untergruppen H).

A fortiori gibt es nur endl. viele Zwischenkörper

$F \subseteq K'' \subseteq E$. Steinitz impliziert nun daß $E|F$ einfach ist. ∎