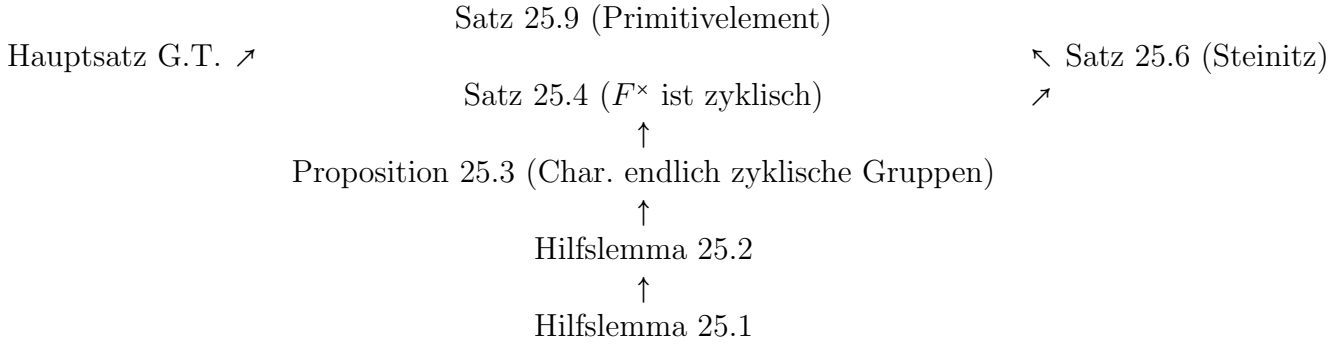
25 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir mit Abschnitt §22 anfangen und unsere erste Anwendungen präsentieren. Das Endziel für diese Vorlesung ist Satz 25.9. Für den Beweis brauchen wir einige, an sich sehr interessante Zwischenschritte. Den Beweisaufbau haben wir in diesem Diagram zusammenfasst:



§22: Einige Anwendungen der Galois Theorie

Ergänzend zu Kapitel 3, fassen wir hier einige einfache Eigenschaften von endlichen Gruppen.

Notation 25.0
Sei $G \neq \{1\}$ eine endliche Gruppe. Setze $\gamma(G) :=$ die kleinste $\gamma \in \mathbb{N}$, so dass $x^\gamma = 1$ für alle $x \in G$. Bemerke dass $\gamma(G) \leq |G|$ (folgt aus Korollar 16.3).

Hilfslemma 25.1.
Sei G eine endliche abelsche Gruppe, und $g, h \in G$ so dass $ggT(|g|, |h|) = 1$. Es gilt: $|gh| = |g||h|$.

Beweis:
Setze $|g| := m$ und $|h| := n$. Sei $r \in \mathbb{N}$, so dass $(gh)^r = 1$. Dann ist $g' := g^r = h^{-r} \in < g > \cap < h >$. Es folt $|g'| \mid m$ und $|g'| \mid n$. Also $|g'| = 1$ und $g' = 1$. Somit haben wir gezeigt: $(gh)^r = 1 \Rightarrow g^r = h^r = 1$. Es folgt: $m \mid r$ und $n \mid r$ und somit $mn = kgV(m, n) \mid r$. Da aber andererseits $(gh)^{mn} = g^{mn}h^{mn} = 1$, folgt die Behauptung. □

Hilfslemma 25.2.
Sei G eine endliche abelsche Gruppe, wähle $g \in G$, so dass $|g|$ maximal ist. Es gilt: $|g| = \gamma(G)$.

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

Schreibe: $\left.\begin{array}{rcl} |g| & = & p_1^{\ell_1}\cdots p_s^{\ell_s} \\ |h| & = & p_1^{f_1}\cdots p_s^{f_s} \end{array}\right\} p_i$ 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 $|h'| = p_1^{f_1}$.
Nun ggT $(|g'|, |h'|) = 1 \underset{HL1}{\Rightarrow} |g'h'| = p_1^{f_1}p_2^{\ell_2}\cdots p_s^{\ell_s} > |g|$. □

Proposition 25.3. Sei G eine endliche abelsche Gruppe. Es gilt: G ist zyklisch $\Leftrightarrow \gamma(G) = |G|$.

Beweis:
"⇒": Sei $G =< g >$, dann ist $|G| = |g|$ und damit ist $\gamma(G) = |G|$.
"⇐": Wähle $g \in G$ mit $|g|$ maximal. HL 25.2 ergibt: $|g| = \gamma(G)$. Es folgt $|g| = |G|$, also $G =< g >$. □

Satz 25.4. Sei F ein Körper, und G eine endliche Untergruppe von $F^\times$. Dann ist G zyklisch.

Beweis:
Setze $\gamma(G) := \gamma$. Da G abelsch ist, genügt es zu zeigen (wegen Proposition 25.3) dass $|G| = \gamma$.
Betrachte $f(x) = x^\gamma - 1$. Das Polynom hat $\leq \gamma$ Nullstellen in $F^\times$, insbesondere $\leq \gamma$ Nullstellen in G. Andererseits muss jedes $a \in G$ eine Nullstelle sein, also $|G| \leq \gamma$. □

Korollar 25.5.
Sei F ein endlicher Körper und eine E/F eine endliche Körpererweiterung. Dann hat E/F ein primitives Element.

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

Satz 25.6. [Steinitz]
Sei E/F eine endliche Körpererweiterung. Dann ist E/F einfach $\Leftrightarrow$ es gibt nur endlich-viele Zwischenkörper $F \subseteq K'' \subseteq E$.

Beweis:
"⇒" Sei $E = F(u)$ und $f(x)$ Min. Pol. von u über F. Sei $F \subseteq K \subseteq E$, und $g(x)$ Min. Pol. von u über K. Es gilt $g(x) \mid f(x)$. Sei K' der Zwischenkörper von E/F, der erzeugt ist durch die Koeffizienten von g. Dann ist $K' \subseteq K$, und $g(x)$ ist Min. Pol. von u über K'.

Da $E = K(u) = K'(u)$, haben wir $[E : K] = \deg g(x) = [E : K']$. Also $K' = K$. Also ist jeder Zwischenkörper erzeugt durch die Koeffizienten der normierten Faktoren von $f(x)$. Da es nur endlich viele davon gibt, haben wir die Behauptung bewiesen.

"⇐" Wenn F endlich ist folgt die Behauptung aus Korollar 25.5.

Also ohne Einschränkung ist F unendlich. Wir zeigen, dass $E = F(u, v)$ ein primitives Element hat. (Der allgemeine Fall $E = F(u_1, \ldots, u_k)$ folgt dann per Induktion).

Betrachte die Unterkörper $F(u + av)$ mit $a \in F$. Da es nur endlich viele davon gibt, aber unendlich viele $a \in F$, müssen $a, b\,; a \neq b$ existieren, so dass $F(u + av) = F(u + bv)$. Aber dann ist $v = (a - b)^{-1}(u + av - u - bv) \in F(u + av)$ und $u = u + av - av \in F(u + av)$. Setze $z := u + av$, dann ist $E = F(u, v) = F(z)$. □

Definition 25.7.
Sei E/F eine algebraische Körpererweiterung. Die *normale Hülle K von E/F* ist der Zerfällungskörper der Menge $\{m_{\alpha,F}(x)\,;\,\alpha \in E\}$ von Minimalpolynomen der Elemente in E.

Bemerkung 25.8.
Wir beschreiben die normale Hülle K für eine endliche separable Erweiterung E/F. Da E/F endlich erzeugt ist, seien die Erzeuger $\{a_1, \ldots, a_n\}$, $a_i \in E$ algebraische und separable Elemente. Sei $m_i(x)$ das Minimalpolynom von a_i, $m_i(x)$ ist separabel und irreduzibel. Œ $m_i \neq m_j$ für $i \neq j$. Setze $m(x) \coloneqq \prod_{1\leq i\leq n} m_i(x)$. Dann ist $m(x)$ separabel. Setze $K \coloneqq$ Zerfällungskörper von $m(x)$ über E. Da $K \supseteq F(a_1, \ldots, a_n)$ ist K Zerfällungskörper von $m(x)$ über F ist. Es gelten:

(1) K/F normal (und Galois).

(2) Jede normale Erweiterung von E enthält einen Zerfällungskörper für $m(x)$ über F. Also enthält jede normale Erweiterung von E eine isomorphe Kopie von K (s. Satz 12.1).

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

Satz 25.9. [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 $E = F(z)$.

Beweis:
Sei E/F wie in der Aussage und sei K die normale Hülle von E/F. Dann ist K/F eine endliche Galois Erweiterung (s. Bemerkung 25.8). Es folgt aus Satz 24.5: es gibt nur endlich viele Zwischenkörper $F \subseteq K' \subseteq K$ (weil die genau Inv H sind für eine $H \leq \mathrm{Gal}\,(K/F)$, da aber $\mathrm{Gal}\,(K/F)$ 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. □