GESAMTSKRIPT

zur Vorlesung ALGEBRA I

Kapitel IV

Prof. Dr. Salma Kuhlmann

Wintersemester 2020 - 2021

Inhaltsverzeichnis Kapitel IV zur Vorlesung: Algebra 1 (WiSe 2020-2021)

Prof. Dr. Salma Kuhlmann

§21 Die Galois Korrespondenz

§22 Einige Anwendungen der Galois Theorie

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

Prof. Dr. Salma Kuhlmann

Kapitel 4

EINFÜHRUNG IN DIE GALOISTHEORIE

In diesem Kapitel werden wir die basische Begriffe einführen, und die Eigenschaften von Galoiserweiterungen studieren. Wir werden zunächst den Hauptsatz der Galoistheorie beweisen, und danach einige erste Anwendungen vorzeigen (u.a. den Satz vom primitiven Element, den Fundamentalsatz der Algebra, sowie die Charakterisierung von auflösbaren Erweiterungen). In der Vorlesung B4 (Algebra 2 / algebraische Zahlentheorie) im Sommer Semester werden wir unser Studium der Galoistheorie und ihre Anwendungen vertiefen.

Im Skript 23 werden wir das notwendige Werkzeug für den Hauptsatz der Galoistheorie präsentieren. Wir werden zunächst in Proposition 23.4 eine Korrespondenz und ihre allgemeine Eigenschaften etablieren. Der Beweis davon ist routinemäßig. Anspruchsvoller ist es zu untersuchen, wann genau Mengengleichungen (anstatt Mengeninklusionen) gelten. Dafür werden wir am Ende des Skripts zwei Hilfslemmata beweisen. Im Skript 24 werden wir dann die Charakterisierung von Galoiserweiterungen beweisen.

§21: Die Galois Korrespondenz

Sei E/F stets eine Körpererweiterung.

Definition 23.1. Wir bezeichnen mit $\mathrm{Aut}(E)$ die Menge

$$\mathrm{Aut}(E) := \{\sigma \,;\, \sigma : E \to E, \sigma \text{ ist ein bijektive Körperhomomorphismus } \}$$

versehen mit der Verknüpfung $\circ$ (Komposition).
Sie ist tatsächlich eine Gruppe (ÜA), und heißt die *Automorphismengruppe von* E.

Definition 23.2. Die *Galoisgruppe von* E/F ist die Menge

$$\mathrm{Gal}(E/F) := \{\mu \in \mathrm{Aut}(E) \,;\, \mu(\alpha) \,=\, \alpha \;\forall\, \alpha \in F\}\,.$$

Sie ist tatsächlich eine Teilgruppe von $\mathrm{Aut}(E)$ (ÜA).

Definition 23.3. Sei $G \leq \mathrm{Aut}(E)$ eine Teilgruppe. Die Menge

$$\mathrm{Inv}(G) := \{a \in E \,;\, \sigma(a) = a \;\forall\, \sigma \in G\}$$

ist der *G-fixierte Teilkörper* von E oder der *Fixkörper* von G.
Sie ist tatsächlich ein Teilkörper von E (ÜA).

Proposition 23.4. Sei Γ die Menge aller Teilgruppen von $\mathrm{Aut}(E)$ und Σ die Menge aller Teilkörper von E. Die Abbildungen

$$\begin{aligned} \Gamma \to \Sigma, &\quad H \mapsto \mathrm{Inv}(H) \qquad \text{und} \\ \Sigma \to \Gamma, &\quad F \mapsto \mathrm{Gal}(E/F) \end{aligned}$$

haben folgende Eigenschaften:

1. $H_1 \leq H_2 \Rightarrow \mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2)$,
2. $F_1 \subseteq F_2 \Rightarrow \mathrm{Gal}(E/F_1) \geq \mathrm{Gal}(E/F_2)$,
3. $\mathrm{Inv}(\mathrm{Gal}(E/F)) \supseteq F$,
4. $\mathrm{Gal}(E/\mathrm{Inv}(H)) \supseteq H$.

Beweis: ÜA. ÜB.

Lemma 23.5. Sei E ein Zerfällungskörper eines separablen Polynoms $p(x) \in F[x]$. Dann

$$|\mathrm{Gal}(E/F)| = [E : F].$$

Beweis: Wir beweisen eine ähnliche Aussage wie im Beweis vom Satz 12.1; wir werden nämlich folgende Behauptung beweisen:

Sei $\tau: F \to F'$ ein Körperisomorphismus. Sei $p(x) \in F[x]$ separabel. Sei E ein Zerfällungskörper für $p(x)$ und E' ein Zerfällungskörper für $\tau(p)(x)$. Es gibt genau $[E : F]$ Fortsetzungen von τ zu einem Isomorphismus $\sigma: E \to E'$.

Wir führen einen Beweis (eine Aufzälung) per Induktion nach $[E : F]$ aus.
• Wenn $[E : F] = 1$ gilt die Behauptung offensichtlich.
• Sei nun $[E : F] > 1$ und sei $\alpha \in E \setminus F$ eine Nullstelle von $p(x)$ mit Minimalpolynom $m_\alpha(x)$. Sei β Nullstelle von $\tau(m_\alpha)(x)$. Sei

$$\tau_\beta : F(\alpha) \to F'(\beta)$$

der (eindeutige) Isomorphismus der τ durch $\tau_\beta(\alpha) = \beta$ fortsetzt, und sei

$$S_\beta := \text{ die Menge aller Isomorphismen } E \to E' \text{ die } \tau_\beta \text{ fortsetzen.}$$

Wir bemerken dass $S_\beta \cap S_{\beta'} = \varnothing$ wenn $\beta \neq \beta'$.
Der Körper E ist auch ein Zerfällungskörper von $p(x)$ über $F(\alpha)$ und E' ist ein Zerfällungskörper von $\tau_\beta(p)(x)$ über $F'(\beta)$ (s. Definition 11.10). Da $[E : F(\alpha)] < [E : F]$ (s. Satz 10.11), folgt aus der Induktionsvoraussetzung dass

$$|S_\beta| = [E : F(\alpha)].$$

Das Polynom $m_\alpha(x)$ teilt $p(x)$, daher ist $m_\alpha(x)$ separabel und somit ist $\tau(m_\alpha)(x)$ auch separabel (s. Definition 13.2). Es folgt, dass $\tau(m_\alpha)(x)$ genau $[F(\alpha) : F]$ verschiedene Nullstellen hat (s. Proposition 10.6).
Jede Fortsetzung $\sigma : E \to E'$ von τ bildet α auf eine Nullstelle $\beta := \sigma(\alpha)$ von $\tau(m_\alpha)(x)$ ab. Also ist die Einschränkung von σ auf $F(\alpha)$ gleich τ_β. Das heißt, $\sigma \in S_\beta$.

Also gibt es insgesamt genau $[E : F(\alpha)][F(\alpha) : F]$ Isomorphismen $\sigma : E \to E'$ die $\tau : F \to F'$ fortsetzen. Unsere Behauptung wurde hiermit bewiesen.
Die Aussage des Lemmas folgt nun, sobald wir $E = E'$, $F = F'$ und $\tau = \mathrm{id}_F$ setzen. □

Lemma 23.6. Sei $G \leq \mathrm{Aut}(E)$ eine endliche Teilgruppe und setze $F = \mathrm{Inv}(G) \subseteq E$. Dann gilt

$$[E : F] \leq |G|.$$

Beweis: Seien $n = |G|$ und $G = \{\mu_1 = 1, \mu_2, \ldots, \mu_n\}$. Wir werden zeigen dass jede Menge mit $m > n$ Elementen aus E linear abhängig über F ist.

Seien $u_1, \ldots, u_m \in E$. Betrachte folgendes homogenes Gleichungssystem in den Variablen $x_1, \ldots, x_m$

$$\sum_{j=1}^{m} \mu_i(u_j)x_j = 0, \quad 1 \leq i \leq n. \tag{1}$$

Nach [Gesamtscript LA I (2019-2020); Korollar 7.2], hat das System (1) eine nichttriviale Lösung. Sei $(b_1, \ldots, b_m)$ eine nichttriviale Lösung mit der kleinsten Anzahl von $b_j \neq 0$. Nach Umbenennung der Variablen kann man annehmen, dass $b_1 \neq 0$. Weiter, nach Multiplikation mit b_1^{-1} können wir auch annehmen, dass $b_1 = 1$.

Nun zeigen wir per Widerspruch, dass $b_j \in F$ für alle $j = 1, \cdots, m$. Ohne Einschränkung können wir annehmen, dass $b_2 \notin F$ und $\mu_k(b_2) \neq b_2$ für ein $k \in \{1, \cdots, n\}$. Wenn wir μ_k auf (1) anwenden finden wir

$$\sum_{j=1}^{m} (\mu_k\mu_i)(u_j)\mu_k(x_j) = 0, \quad 1 \leq i \leq n. \tag{2}$$

Da $\mu_k\mu_1, \ldots, \mu_k\mu_n$ eine Permutation von $\mu_1, \ldots, \mu_n$ ist, folgt dass (1) und (2) äquivalent sind und

$$(\mu_k(1), \mu_k(b_2), \ldots, \mu_k(b_m)) = (1, \mu_k(b_2), \ldots, \mu_k(b_m))$$

auch eine Lösung von (1) ist. Daher ist auch

$$(0, b_2 - \mu_k(b_2), \ldots, b_m - \mu_k(b_m))$$

auch eine Lösung. Diese Lösung ist nichttrivial weil $b_2 \neq \mu_k(b_2)$, hat aber mehr nulle Einträge als $(b_1, \ldots, b_m)$. Dies widerspricht die Wahl von $(b_1, \ldots, b_m)$.
Es folgt, dass $b_j \in F$ für alle $j = 1, \cdots, m$. Die erste Gleichung vom (1) (mit $\mu_1 = 1$) ergibt

$$\sum_{j=1}^{m} b_j u_j = 0.$$

Somit sind $u_1, \ldots, u_m$ linear abhängig über F. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir (endliche) Galois Erweiterungen definieren und Charakterisieren, und den Hauptsatz der Galoistheorie aussagen und beweisen.

Sei E/F stets eine algebraische Körpererweiterung.

Definition 24.1. Die Körpererweiterung E/F heißt *separabel* falls für jedes $\alpha \in E$, das Minimalpolynom $m_{\alpha,F}(x)$ separabel ist.

Definition 24.2. Die Körpererweiterung E/F heißt *Galoiserweiterung* falls E/F endlich, normal und separabel ist.

Satz 24.3. Sei E/F eine Körpererweiterung. Die folgende Aussagen sind äquivalent:

(i) E ist der Zerfällungskörper eines separablen Polynoms $p(x) \in F[x]$.

(ii) $F = \mathrm{Inv}(G)$ für eine endliche Teilgruppe $G \leq \mathrm{Aut}(E)$.

(iii) E/F ist eine Galoiserweiterung.

Darüberhinaus gelten:

(a) sind E und F wie in (i) und $G = \mathrm{Gal}(E/F)$ dann ist $F = \mathrm{Inv}(G)$
d.h. $\mathrm{Inv}(\mathrm{Gal}(E/F)) = F$

(b) sind G und F wie in (ii) dann ist $G = \mathrm{Gal}(E/F)$
d.h. $\mathrm{Gal}(E/\mathrm{Inv}(G)) = G$.

Beweis: (i)⇒(ii):

• Setze $F' := \mathrm{Inv}(\mathrm{Gal}(E/F))$. Dann ist E auch ein Zerfällungskörper von $p(x)$ über F' . Es gelten: $F \subseteq F'$ und $\mathrm{Gal}(E/F) \geq \mathrm{Gal}(E/F')$ (Proposition 23.4). Per Definition von F' ist auch $\mathrm{Gal}(E/F) \leq \mathrm{Gal}(E/F')$. Also ist $\mathrm{Gal}(E/F) = \mathrm{Gal}(E/F')$.

• Aus Lemma 23.5 folgen $[E : F] = |\mathrm{Gal}(E/F)|$ und $[E : F'] = |\mathrm{Gal}(E/F')|$, also $[E : F] = [E : F']$. Daher ist $[F'/F] = 1$ (s. Satz 10.11). Also $F = F'$ und somit gelten (a) und (ii).

(ii)⇒(iii):

• Nach Lemma 23.6 ist E/F endlich.

• Sei $\alpha \in E$. Sei $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m\}$ die Bahn von α unter der Wirkung $(\sigma, \alpha) \mapsto \sigma(\alpha)$ von G. Setze $g(x) = \prod_{i=1}^{m}(x - \alpha_i)$. Für alle $\sigma \in G$ gilt $\sigma(g)(x) = \prod_{i=1}^{m}(x - \sigma(\alpha_i)) = g(x)$ (weil σ die Elemente $\alpha_1, \ldots, \alpha_m$ permutiert). Also $g(x) \in F[x]$ (weil die Koeffiziente von g in $\mathrm{Inv}(G)$ liegen).

Aus $g(\alpha) = 0$ und $g(x) \in F[x]$ folgt, dass das Minimalpolynom m_α von α über F das Polynom g teilt. Da (per Definition) g separabel und daher, ist auch m_α separabel. Es folgt, dass E/F separabel ist.

• Außerdem liegen alle Nullstellen von m_α in E. Daher ist E/F normal (E ist der Zerfällungskörper der Minimalpolynomen über F aller $\alpha \in E$).

(iii)⇒(i):

• E/F ist normal und endlich, also E ist der Zerfällungskörper von endlich vielen Polynomen $p_1, \dots, p_n \in F[x]$. Ohne Einschränkung können wir annehmen, dass die p_i paarweise verschieden, normiert und irreduzibel über F sind. Somit ist jedes p_i das Minimalpolynom über F von einem $\alpha_i \in E$. Da E/F separable ist, ist jedes p_i separable. Da die p_i verschieden sind, haben sie auch keine gemeinsame Nullstelle. Das Produkt $p_1 \cdots p_n$ ist somit auch separabel (s. Definition 13.2) und E ist sein Zerfällungskörper. Dies zeigt (i).

• Zu (b). Sei $F = \mathrm{Inv}(G)$ für eine endliche Gruppe $G \leq \mathrm{Aut}(E)$. Lemma 23.6 liefert $[E : F] \leq |G|$. Da (i) gilt, Lemma 23.5 liefert, dass $|\mathrm{Gal}(E/F)| = [E : F]$. Es gilt $G \leq \mathrm{Gal}(E/F)$ (Proposition 23.4) und daraus folgt nun $G = \mathrm{Gal}(E/F)$. □

Bemerkung 24.4. Die Erweiterung E/F ist normal wenn E enthält ein Zerfällungskörper für das Minimalpolynom m_α (von α über F) , für jedes $\alpha \in E$. Das heißt, jedes irreduzibles Polynom $p(x) \in F[x]$ das eine Nullstelle $\alpha \in E$ hat zerfällt als Produkt von linearen Faktoren in $E[x]$. Die Erweiterung ist normal und separable wenn jedes irreduzibles Polynom $p(x) \in F[x]$ das eine Nullstelle $\alpha \in E$ hat zerfällt als Produkt von verschiedenen linearen Faktoren in $E[x]$. ÜA

Satz 24.5 (Hauptsatz der Galoistheorie)**.** Sei E/F eine Galoiserweiterung. Setze $G := \mathrm{Gal}(E/F)$. Seien Γ die Menge aller Teilgruppen $H \leq G$ und Σ die Menge aller Zwischenkörper K mit $F \subseteq K \subseteq E$. Die Abbildungen

$$\begin{aligned} \Gamma &\to \Sigma, \quad H \mapsto \mathrm{Inv}(H) \\ \Sigma &\to \Gamma, \quad K \mapsto \mathrm{Gal}(E/K) \end{aligned}$$

sind bijektiv und Inverse voneinander.
Darüberhinaus gelten die folgende Eigenschaften:

(i) $H_1 \supseteq H_2 \iff \mathrm{Inv}(H_1) \subseteq \mathrm{Inv}(H_2)$;

(ii) $|H| = [E : \mathrm{Inv}(H)]$ und $[G : H] = [\mathrm{Inv}(H) : F]$;

(iii) $H \trianglelefteq G \iff \mathrm{Inv}(H)/F$ normal ist. In diesem Fall gilt $\mathrm{Gal}(\mathrm{Inv}(H)/F) \simeq G/H$.

Beweis:
Benenne die Abbildungen:

$$\begin{array}{lccll} & \Sigma & \overset{\gamma}{\to} & \Gamma & \\ & K & \mapsto & \mathrm{Gal}(E/K) & (\leq \mathrm{Gal}(E/F)) \\ \text{und} & \Gamma & \overset{i}{\to} & \Sigma & \\ & H & \mapsto & \mathrm{Inv}\, H & (\subseteq E \text{ und } \supseteq F) \end{array}$$

• Wir behaupten also dass

$$i \circ \gamma = \mathrm{id} \text{ und } \gamma \circ i = \mathrm{id}$$

d.h.

$$\mathrm{Gal}(E/\mathrm{Inv}\, H) = H \text{ und } \mathrm{Inv}(\mathrm{Gal}(E/K)) = K \quad (\dagger)$$

d.h.

$$(\gamma \circ i)(H) = H \text{ und } (i \circ \gamma)(K) = K\,.$$

Das ist aber gerade die letzte Aussage in Satz 24.3 (weil H endlich ist), genauer:

- $H \leq G$, also $F := \operatorname{Inv} G \subseteq \operatorname{Inv} H$ und $K = \operatorname{Inv} H$ ist eine Zwischenerweiterung $F \subseteq K \subseteq E$. Die Anwendung von Satz 24.3 (b) (mit H anstatt mit G) liefert $\operatorname{Gal}(E/\operatorname{Inv} H) = H$. Es gilt auch $|H| = |\operatorname{Gal}(E/\operatorname{Inv} H)| = [E : \operatorname{Inv} H]$ (s. Lemma 23.5). Das ist die erste Aussage in (ii).

- Sei nun $F \subseteq K \subseteq E$ und $H := \operatorname{Gal}(E/K)$, dann ist $H \leq G$.
  Nun ist E immer noch Zerfällungskörper über K von einem separablen Polynom (‡) (ÜA).
  Also liefert die Anwendung von Satz 24.3 (a) für E und K

$$K = \operatorname{Inv} H = \operatorname{Inv}(\operatorname{Gal}(E/K))$$

- (i) ist eine unmittelbare Folgerung der allgemeinen Eigenschaften:
  $H_1 \supseteq H_2 \Rightarrow \operatorname{Inv} H_1 \subseteq \operatorname{Inv} H_2$.
  Umgekehrt wenn $\operatorname{Inv} H_1 \subseteq \operatorname{Inv} H_2$ dann ist $H_1 = \operatorname{Gal}(E/\operatorname{Inv} H_1) \supseteq \operatorname{Gal}(E/\operatorname{Inv} H_2) = H_2$.

- Die erste Aussage in (ii) haben wir schon bewiesen: $|H| = [E : \operatorname{Inv} H]$. Wir berechnen $|G| = [E : F] = [E : \operatorname{Inv} H][\operatorname{Inv} H : F] = |H|[\operatorname{Inv} H : F]$, aber auch $|G| = |H|[G : H]$ (vergleiche: $|G| = |H|[\operatorname{Inv} H : F]$ und $|G| = |H|[G : H]$) $\Rightarrow [G : H] = [\operatorname{Inv} H : F]$. Dies ist die zweite Aussage in (ii).

Zu (iii):
Sei $H \in \Gamma$ und $K := \operatorname{Inv} H$. Dann gilt, für alle $\eta \in G$:

$$\operatorname{Inv}(\eta H \eta^{-1}) = \eta(K)$$

[ÜA; für alle ξ gilt nämlich: $\xi(k) = k \Rightarrow (\eta\xi\eta^{-1})(\eta(k)) = \eta(k)$.]

Es folgt: $H \trianglelefteq G \Leftrightarrow \eta(K) = K$ für alle $\eta \in G$ (∗) (ÜA).

[i.e. K ist *mengenweise invariant*].

Nehmen wir nun an, dass $H \trianglelefteq G$. Aus (∗) folgt, dass $\overline{\eta} := \eta|_K$ ein Automorphismus von K über F ist. Betrachte also nun die Erweiterung K/F und den Homomorphismus

$$\begin{array}{rccc} \nu: & G & \to & \operatorname{Gal}(K/F) \\ & \eta & \mapsto & \overline{\eta} \end{array}$$

Wir bezeichnen $\nu(G) := \overline{G}$. Wir berechnen Bild(ν) und Kern(ν).

Bemerke dass ν surjective ist, also $\overline{G} = \operatorname{Gal}(K/F)$. In der Tat, läßt sich jede $\tau \in \operatorname{Gal}(K/F)$ zu eine $\eta \in \operatorname{Gal}(E/F)$ fortsetzen. Das folgt aus (‡) und Satz 12.1 (ÜA).

Der Kern ist die Menge aller $\eta \in G$ mit $\eta|_K = \mathrm{id}$. Das heißt, dass der Kern ist $\operatorname{Gal}(E/K)$, also $\ker \nu = H$, wegen (†). Wir bekommen nun $\overline{G} = \operatorname{Gal}(K/F) \simeq G/H$ (s. Satz 16.11).
Der Fixkörper von $\overline{G}$ in K ist F (ÜA). Also ist K/F eine normale Erweiterung (Satz 24.3).

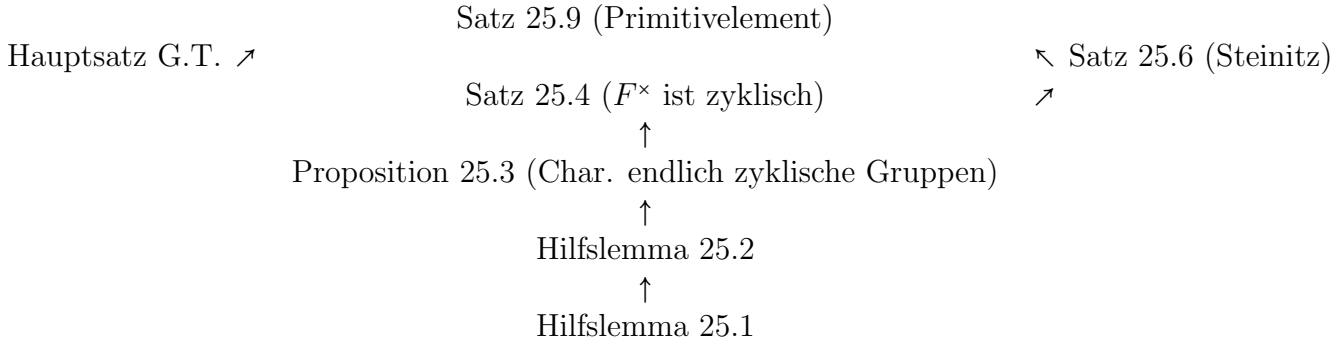
Umgekehrt: Sei K/F normal. Sei $a \in K$ und $f(x)$ sein Minimalpolynom, $f(x)$ zerfällt in Linearfaktoren über $K[x]$. Dann ist $f(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$ in $K[x]$ mit $a = a_1$.
Sei $\eta \in G$, dann ist $0 = \eta(f(a)) = f(\eta(a))$. Also ist $\eta(a)$ eine Nullstelle und somit existiert ein i mit $\eta(a) = a_i$. Insbesondere ist $\eta(a) \in K$.

Wir haben gezeigt: $\eta(K) \subseteq K$ für alle $\eta \in G$ und damit ist durch (∗) $H := \operatorname{Gal}(E/K) \trianglelefteq G$. □

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 $|g'| \,|\, m$ und $|g'| \,|\, n$. Also $|g'| = 1$ und $g' = 1$. Somit haben wir gezeigt: $(gh)^r = 1 \Rightarrow g^r = h^r = 1$. Es folgt: $m|r$ und $n|r$ und somit $mn = kgV(m,n)|r$. 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 endliche 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 $\operatorname{Inv} H$ sind für eine $H \leq \operatorname{Gal}(K/F)$, da aber $\operatorname{Gal}(K/F)$ 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. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zwei weitere Anwendungen der Galoistheorie präsentieren. In der Folgevorlesung Algebra 2 werden wir die Galoistheorie und ihre Anwendungen fortsetzen und vertiefen, insbesondere auf endliche Körper, Radizierbare Körpererweiterungen, und Kreisteilungskörper.

Fundamentaler Satz der Algebra.

Bemerkung 26.1. Wir werden die folgenden (aus der Analysis bekannte) Eigenschaften von $\mathbb{R}$ und $\mathbb{C}$ benötigen. [1]

(i) Es ist $[\mathbb{C} : \mathbb{R}] = 2$, da $\mathbb{C} = \mathbb{R}(\sqrt{-1})$.

(ii) $a \in \mathbb{R}$ mit $a \geq 0$ hat eine Quadratwurzel in $\mathbb{R}$.

(iii) Jedes $f \in \mathbb{R}[x]$ ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.

Daraus folgt:

Lemma 26.2. (i) Jedes Polynom zweiten Grades aus $\mathbb{C}[x]$ hat eine Nullstelle in $\mathbb{C}$.

(ii) Insbesondere hat $\mathbb{C}$ keine quadratische Erweiterungen, d.h. keine Körpererweiterung L von $\mathbb{C}$ mit $[L : \mathbb{C}] = 2$.

Beweis: Dafür genügt es zu zeigen, dass $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ hat.
Sei also $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$. Wir wollen $a, b \in \mathbb{R}$ finden so dass:
$z = x + iy = (a + ib)^2 = (a^2 - b^2) + i2ab$, also so dass $x = a^2 - b^2$ und $y = 2ab$ $(*)$
Betrachte

$$a^2 = \frac{1}{2}\,(x + \sqrt{x^2 + y^2})$$
$$b^2 = \frac{1}{2}\,(-x + \sqrt{x^2 + y^2}).$$

Bemerke dass $(x+\sqrt{x^2 + y^2}) \geq 0$ und $(-x+\sqrt{x^2 + y^2}) \geq 0$ (weil $\sqrt{x^2 + y^2} \geq \sqrt{x^2} = |x|$). Bemerkung 26.1(i) impliziert: es gibt eine Lösung $a, b \in \mathbb{R}$. Man prüft: $x = a^2 - b^2$ und $y^2 = 4a^2b^2$ (die Gleichungen $(*)$ sind abgesehen von der Wahl des Vorzeichens von a und b, dazu äquivalent). □

[1] Diese Eigenschaften werden allgemeiner für reell abgeschlossene Körper und ihre algebraische Abschlüsse in der Vorlesung "Reelle algebraische Geometrie I " gezeigt.

Satz 26.3.
$\mathbb{C}$ ist algebraich abgeschlossen.

Beweis:

Es genügt zu zeigen das $\mathbb{C}$ keine echte endliche Körpererweiterung hat.
Sei also $L/\mathbb{C}$ endlich und betrachte $\mathbb{R} \subseteq \mathbb{C} \subseteq L$, ist. Zu zeigen: $L = \mathbb{C}$.

Setze $[L : \mathbb{R}] = 2^k m$ mit $k \in \mathbb{N}$ und $2 \nmid m$ (s. Bemerkung 26.1(i)).

Ohne Einschränkung ist $L/\mathbb{R}$ Galois (ggfs. L durch ist die Normalhülle von $L/\mathbb{R}$ ersetzen, siehe Bemerkung 25.8). Setze $G := \mathrm{Gal}(L/\mathbb{R})$. Dann ist $|G| = 2^k m$ (Satz 24.5).

Nun enthält G eine 2-Sylow $H \leq G$ (Sylow 1; Skript 20). Satz 24.5 impliziert dass $[L : \mathrm{Inv}\, H] = |H| = 2^k$ beziehungsweise $[\mathrm{Inv}\, H : \mathbb{R}] = m$.

Da aber jedes reelle Polynom ungeraden Grades eine Nullstelle in $\mathbb{R}$ hat (Bemerkung 26.1 (ii)), ergibt sich notwendig $m = 1$ (benutze Satz 25.9). Also $[L : \mathbb{R}] = 2^k$ und somit ist $[L : \mathbb{C}] = 2^{k-1}$. Wir müssen nun zeigen dass $k = 1$.

Sei $G' := \mathrm{Gal}(L/\mathbb{C})$. Wenn $L \neq \mathbb{C}$, also wenn $k \geq 2$, liefert Satz Sylow 1 eine Teilgruppe $H' \leq G'$ mit $|H'| = 2^{k-2}$. Also ist $[L : \mathrm{Inv}\, H'] = 2^{k-2}$, und somit $[\mathrm{Inv}\, H' : \mathbb{C}] = 2$.
Widerspruch (s. Lemma 26.2(ii)). □

Auflösbare Erweiterungen.

Satz 26.4. [Galoisgruppe als Untergruppen von S_n]
Sei K ein Körper, und $f \in K[x]$ separabel, mit $\deg f = n \in \mathbb{N}$. Sei L/K der Zerfällungskörper von f über K, und $a_1, \ldots, a_n \in L$ die Nullstellen von f. Die Abbildung

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(L/K) & \longrightarrow & Sym\{a_1, \ldots, a_n\} \\ & \delta & \longmapsto & \delta \,|\, \{a_1, \ldots, a_n\} \end{array}$$

definiert einen injektiven Gruppenhomomorphismus.

Beweis:
$\delta \in \mathrm{Gal}(L/K), f(a_i) = 0 \Rightarrow 0 = \delta(f(a_i)) = f(\delta(a_i))$, da δ die Koeffizienten von f fest lässt. Also ist $\delta(a_i)$ eine Nullstelle von f. Da δ injektiv ist, und $\delta : \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}$, ist δ bijektiv. Damit ist φ wohldefiniert. Außerdem ist φ ein Gruppenhomomorphismus (ÜA).

Da $L = K(a_1, \ldots, a_n)$ und $\delta \in \mathrm{Gal}(L/K)$ bereits eindeutig durch seine Werte auf $\{a_1, \ldots, a_n\}$ bestimmt ist (ÜA), ist φ injektiv.

□

Korollar 26.5.
Sei L/K eine endliche Galois Erweiterung vom Grad n, so lässt sich $\mathrm{Gal}(L/K)$ als Untergruppe von S_n auffassen.

Definition 26.6.
Eine endliche Körpererweiterung L/K ist *auflösbar*, wenn es einen Oberkörper $E \supset L$ gibt, so dass E/K eine endlische Galois Erweiterung mit auflösbarer $\mathrm{Gal}(E/K)$ ist.

Korollar 26.7.
Sei L/K eine separable Erweiterung vom Grad ≤ 4, dann ist L/K auflösbar.

Beweis:

Satz 25.9 impliziert dass $L = K(a)$ eine einfache Erweiterung ist. Sei $f \in K[x]$ das $Min.Pol._K a$. Sei L' ein Zerfällungskörper von f über K. Die Galoisgruppe $\mathrm{Gal}(L'/K)$ lässt sich als Untergruppe von S_4 auffassen (s. Korollar 26.5). Da S_4 und alle ihre Untergruppen auflösbar sind (s. Beispiel 18.9), so sind L'/K und L/K auflösbar. □

Korollar 26.8.
Es gibt endlich separable Körpererweiterungen, die nicht auflösbar sind.

Beweis:
Sei F ein Körper und setze $L := F(T_1, \ldots, T_n) = \mathrm{Quot}\ (F[T_1, \ldots, T_n])$
(der Körper der rationalen Funktionen in endlich vielen Variablen $T_1, \ldots, T_n$).

Jede $\pi \in S_n$ definiert einen Automorphismus von L, in dem man π auf die Variablen $T_1, \ldots, T_n$ anwendet:

$$\begin{array}{ccc} F(T_1, \ldots, T_n) & \longrightarrow & F(T_1, \ldots, T_n) \\ \frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} & \longmapsto & \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})} \end{array}$$

Sei $K := \mathrm{Inv}\, S_n \subseteq L$. Es ist (s. Satz 24.3) L/K Galois und $\mathrm{Gal}(L/K) = S_n$. Wähle nun $n \geq 5$, dann ist $\mathrm{Gal}(L/K)$ nicht auflösbar (s. Korollar 20.4). □