GESAMTSKRIPT

zur Vorlesung ALGEBRA I

Prof. Dr. Salma Kuhlmann

Wintersemester 2020 - 2021

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

Prof. Dr. Salma Kuhlmann

Gesamtskript
Kapitel I
zur Vorlesung
Algebra I

Prof.'in Dr. Salma Kuhlmann

Inhaltsverzeichnis für das Gesamtskript Kapitel 1[1] zur Vorlesung: Algebra I (WiSe2020/2021)

Prof. Dr. Salma Kuhlmann

KAPITEL I: Ringe.

[1] Die Seitenzahlen in Klammern geben die Seitenzahl für die Suche mit Adobe Acrobat Reader an (unter dem Menü ANZEIGE – GEHE ZU – SEITE).

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

Prof. Dr. Salma Kuhlmann

Kurze Einleitung:
Für die Vorlesung Algebra 1 (B3) haben wir vier Kapitel vorgesehen. Das erste Teil besteht aus Kapitel 1 (Ringe) und Kapitel 2 (Körpererweiterungen), das zweite Teil aus Kapitel 3 (Gruppen) und Kapitel 4 (Einführung in die Galoistheorie). In der B4 Vorlesung (Algebra 2 und algebraische Zahlentheorie) werden wir unser Studium von Galois Erweiterungen fortsetzen und vertiefen. Das Vorlesungskalender ist zur Orientierung, und enthält eine voraussichtliche Themenplanung.

Kapitel 1

RINGE

In diesem Kapitel werden wir folgende Ringe und Ringkonstruktionen untersuchen (im Stichwort): Faktorringe, Ringe von Brüchen, Lokalisierungen, Euklidische Ringe, Hauptideal Ringe, Faktorielle Ringe, Polynomringe.
In Skript 1, werden wir zunächst einige Begriffe (die wir schon in Lineare Algebra 1 und 2 gesehen haben) in Erinnerung bringen. Danach werden wir Faktorringe einführen.

§ 1 Erinnerungen

Definition 1.1.
Ein Tripel $(R, +, \cdot)$ ist ein *Ring*, falls R ist eine nichtleere Menge und $+, \cdot$ sind Verknüpfungen auf R so dass: :

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element $0 \in R$
- Die Verknüpfung $\cdot$ ist assoziativ
- die Distributivitätsgesetze gelten:

Links: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)\ \forall x, y, z \in R$ und

Rechts: $(y + z) \cdot x = (y \cdot x) + (z \cdot x)\ \forall x, y, z \in R$

Definition 1.2.
Ein Ring $(R, +, \cdot)$ ist
(i) *kommutativ* falls $\forall x, y \in R : x \cdot y = y \cdot x$.
(ii) Ein *Ring mit Eins* wenn es existiert $1 \in R$ $(1 \neq 0)$ so dass $\forall x \in R : x \cdot 1 = 1 \cdot x = x$.

In dieser Vorlesung werden wir kommutative Ringe studieren.

Definition 1.3. Sei R ein kommutativer Ring mit 1.

(1) $a \neq 0; a \in R$ ist ein *Nullteiler*, wenn es $b \neq 0; b \in R$ gibt mit $ab = 0$.

(2) R ist ein *Integerring* oder *Integritätsbereich*, wenn er keine Nullteiler hat.

(3) $u \in R$ ist eine *Einheit*, wenn es ein $v \in R$ gibt mit $uv = 1$.

Notation: $R^\times :=$ Menge der Einheiten von R.

Die folgende Begriffe und Beipiele haben wir in LA I und/oder II schon studiert, wir wiederholen die Aussagen, jedoch nicht die Beweise.

Proposition 1.4.
$R^\times$ ist eine multiplikative Gruppe.

Beispiel 1.5.
Wir bezeichnen $\mathbb{Z}_n^\times$ mit $U(n)$

Es gilt: $a \in U(n) \Leftrightarrow \text{ggT}\ (a, n) = 1$.

Die Euler φ-Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ wird so definiert: $\varphi(n) := \mid U(n) \mid$.

Siehe Übungsblatt für eine ausführliche Ausarbeitung der Eigenschaften von φ:

(1) $\varphi(p^v) = p^v - p^{v-1}$ für p Primzahl und $v \in \mathbb{N}$

(2) φ ist eine multiplikative arithmetische Funktion i.e. $\varphi(ab) = \varphi(a)\varphi(b)$, wenn $\text{ggT}\ (a, b) = 1$.

Definition 1.6.

(1) $S \subseteq R$ ist ein *Teilring*, wenn $S \neq \varnothing; a, b \in S \Rightarrow a - b \in S$ und $ab \in S$.

(2) Seien R, S kommutative Ringe (mit 1_R und 1_S).
Eine Abbildung $\varphi : R \to S$ ist ein *Ringhomomorphismus*, wenn
$\varphi(1_R) = 1_S, \varphi(a + b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$.

(3) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.
Notation: $\varphi : R \simeq S$ oder $R \overset{\varphi}{\simeq} S$ oder $R \simeq S$.

Notation:
$\ker \varphi := \{x \in R; \varphi(x) = 0\}$
$\text{im}\ \varphi := \{y \in S; \exists x \in R \text{ mit } \varphi(x) = y\} := \varphi(R)$.

Bemerkung 1.7.
Sei φ ein Homomorphismus: φ ist injektiv $\Leftrightarrow \ker \varphi = \{0\}$.

Beispiel 1.8.
Sei $n \in \mathbb{N}$
$a \in \mathbb{Z}; \overline{a} :=$ Rest nach Division durch n.

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$

ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Definition 1.9.
Ein Teilring $I \subseteq R$ ist ein *Ideal*, wenn aus $r \in R$ und $x \in I$ folgt: $rx \in I$.
Notation: $I \lhd R$

Beispiel 1.10.
$I = R$ und $I = \{0\}$

Terminologie:
$I \lhd R$ und $I \neq R$ heißt *echtes Ideal*.
$I \lhd R$ und $I \neq \{0\}$ heißt *nicht triviales Ideal*.

Proposition 1.11.
Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gelten:

(1) im φ ist ein Teilring von S.

(2) $\ker\varphi$ ist ein Ideal von R.

Beweis: ÜA.

§ 2 Faktorringe

Sei $I \lhd R$. Wir definieren eine binäre Relation auf R wie folgt:
$\forall x, y \in R : x \sim y \mod I$ genau dann, wenn $x - y \in I$.

Diese ist eine Äquivalenzrelation (siehe Übungsblatt).

Notation:
(i) Für $x \in R$ bezeichnen wir mit $x + I$ die Äquivalenzklasse $[x]$ von x.
(ii) Wir bezeichnen $R/I := \{x + I \mid x \in R\}$ die Menge der *Nebenklassen von R modulo I*.

Proposition 1.12.
R/I ist ein Ring mit den Ringoperationen
$(r + I) + (s + I) := (r + s) + I$ und
$(r + I) \cdot (s + I) := (rs) + I$
für alle $r, s \in R$.

Beweis: siehe Übungsblatt.

Definition 1.13.
R/I ist der *Faktorring* "$R \mod I$".

Satz 1.14. (Isomorphiesatz für Ringe)

(1) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Es gilt $R/\ker\varphi \simeq \text{im}\,\varphi$.

(2) Umgekehrt: Ist $I \lhd R$, dann ist die *kanonische Projektion*

$$\begin{array}{rccc} \pi: & R & \to & R/I \\ & r & \mapsto & r+I \end{array}$$

ein surjektiver Ringhomomorphismus mit $\ker\pi = I$.

Also sind die Ideale genau die Kerne von Ringhomomorphismen.

Beweis:
Setze $I := \ker\varphi$. Wir prüfen unmittelbar dass die Abbildung

$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & \varphi(R) \\ & x+I & \mapsto & \varphi(x) \end{array}$$

wohldefiniert ist, d.h. $x + I = y + I$ impliziert $\varphi(x) = \varphi(y)$.

Es ist außerdem klar, dass Φ surjektiv und ein Ringhomomorphismus ist (ÜA).

Wir berechnen nun $\ker\Phi$:
$\Phi(x+I) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker\varphi \Leftrightarrow x \in I \Leftrightarrow x + I = 0 + I$;
somit ist $\ker\Phi = \{0 + I\}$ (das Nullelement der Faktorring R/I).

Es folgt aus Bemerkung 1.7 dass die Abbildung auch injektiv, und damit ein Isomorphismus.

Der Beweis von (2) ist analog. Siehe Übungsblatt. □

Beispiel 1.15.
Betrachte die Abbildung in Beispiel 1.8:

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & a & \mapsto & \overline{a} \end{array}$$

ist ein Ringhomomorphismus mit $\ker\varphi = \{nz / z \in \mathbb{Z}\} := n\mathbb{Z}$

Es folgt nun aus Satz 1.14 dass $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

Korollar 1.16.
Sei $I \lhd R, J \lhd R$ mit $I \subseteq J$ (insbesondere $I \lhd J$). Dann ist $J/I \lhd R/I$ und $(R/I)/(J/I) \simeq R/J$.

Beweis:
Die Abbildung

$$\begin{array}{rccc} \Phi: & R/I & \twoheadrightarrow & R/J \\ & x+I & \mapsto & x+J \end{array}$$

ist ein surjektiver Ringhomomorphismus mit $\ker\Phi = J/I$. Die Behauptung folgt nun aus Satz 1.14. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst eine wichtige Anwendung vom Isomorphiesatz ableiten; in Korollar 2.1 werden die Ideale von einem Faktorring charakterisieren. Dann werden wir verschiedene allgemeine Idealkonstruktionen einführen (beziehungsweise in Erinnerung bringen). Wir werden bei der Gelegenheit das Lemma von Zorn kennenlernen.

Notation:
$x + I$ wird in dieser Vorlesung auch als $\overline{x}$ geschrieben .

Korollar 2.1.
Sei R ein kommutativer Ring und $I \lhd R$. Sei $\mathcal{T} \coloneqq \{A \subseteq R \,;\, I \subseteq A \subseteq R\}$ die Menge der Teilringe von R die I enthalten und $\mathcal{T}_I$ die Menge der Teilringe von R/I. Es gelten für $A \in \mathcal{T}$:

1. $I \lhd A$,
2. Die Abbildung
$$A \mapsto A/I$$
ist eine bijektive, Inklusionserhaltende Korrespondenz zwischen $\mathcal{T}$ und $\mathcal{T}_{\mathcal{I}}$,
3. $A \lhd R$ genau dann, wenn $A/I \lhd R/I$.

Beweis:
Siehe Übungsblatt. □

Definition 2.2.
Sei $A \subseteq R$ eine beliebige Teilmenge. Das *von A erzeugte Ideal*, mit $< A >$ bezeichnet, ist das kleinste Ideal, das A enthält.

Die folgende Aussage ist als ÜA zu prüfen:

Bemerkung 2.3.

1. $< \varnothing >= \{0\}$.
2. $< A >= \bigcap_{\{A \subseteq J \lhd R\}} J$ (der Durchschnitt aller Ideale, die A enthalten).
3. $< A >= \{\sum_{i=1}^{n} r_i a_i \,;\, n \in \mathbb{N} \,,\, r_i \in R \,,\, a_i \in A\}$
(die Menge aller endlichen R-Linearkombinationen aus Elementen von A).

Konvention: Wenn $A = \{a_1, \ldots, a_l\}$ endlich ist, so schreiben wir einfach $< a_1, \ldots, a_l >$.

Definition 2.4.
Sei $a \in R$, $< a >= \{ra; r \in R\}$ heißt *Hauptideal*, das von a erzeugt ist.

Beispiel 2.5.
$< 1 >= R$ und $< 0 >= \{0\}$.

Proposition 2.6.
Seien R ein kommutativer Ring mit 1, und $I \lhd R$. Es gelten:

(1) $I = R$ genau dann, wenn $I \bigcap R^\times \neq \varnothing$

(2) R ist ein Körper genau dann, wenn die einzigen Ideal R und $\{0\}$ sind.

Beweis:

(1) "$\Rightarrow$" trivial

"$\Leftarrow$" $u \in I$ Einheit $\Rightarrow$ $u^{-1}u \in I$ $\Rightarrow$ $1 \in I$

$\uparrow$

$\in R$ $\Rightarrow$ $r.1 \in I \ \forall \ r \in R$

(2) "$\Rightarrow$" Sei $I \neq \{0\}$ und $u \in I; u \neq 0$. Dann ist u eine Einheit und somit $I = R$.

"$\Leftarrow$" Sei $x \in R, x \neq 0$. Dann ist $< x >= R$, d.h. $1 \in < x >$, also existiert ein $r \in R$ mit $rx = 1$, also $r = x^{-1}$ □

Korollar 2.7.
Sei R ein Körper, S ein Ring und $\varphi : R \to S$ ein Ringhomomorphismus. Ist $\varphi \neq 0$, dann ist φ injektiv.

Beweis:
Proposition 1.11(2) liefert dass $\ker \varphi \lhd R$. Da $\ker \varphi \neq R$ ist, folgt aus Proposition 2.6 dass $\ker \varphi = \{0\}$. Also ist φ injektiv (Bemerkung 1.7). □

Definition 2.8.
$M \lhd R$ ist *maximal*, wenn

(i) $M \neq R$ (M ist echt).

(ii) Ist $I \lhd R$ mit $M \subseteq I \subseteq R$,

dann gilt: $I = M$ oder $I = R$ (i.e. es gibt keine weiteren Ideale strikt zwischen M und R).

Proposition 2.9.
Jedes echte Ideal ist in einem Maximalideal enthalten.

Um Proposition 2.9 zu beweisen, brauchen wir Zorn's Lemma.

Exkurs

Partielle Ordnung
Sei $A \neq \varnothing$ eine Menge. Eine *partielle Ordnung* auf A ist eine Relation $\leq$ auf A mit den Eigenschaften:

(1) $x \leq x$ für alle $x \in A$.

(2) Aus $x \leq y$ und $y \leq x$ folgt $x = y$ für alle $x, y \in A$.

(3) Aus $x \leq y$ und $y \leq z$ folgt $x \leq z$ für alle $x, y, z, \in A$.

(4) $\leq$ ist *total* falls $x \leq y$ oder $y \leq x$ für alle $x, y \in A$.

Definition

(i) Sei $(A, \leq)$ eine partielle Ordnung und $B \subseteq A$. Ein Element $a \in A$ heißt *obere Schranke* für B in A, falls $b \leq a$ für alle $b \in B$.

(ii) $m \in A$ heißt *maximal*, wenn gilt: $m \leq x \Rightarrow m = x$ für alle $x \in A$.

Zorn's Lemma
Sei $A \neq \varnothing$ eine partielle Ordnung mit der Eigenschaft: Jede total angeordnete Teilmenge $B \subseteq A$ hat eine obere Schranke in A. Dann hat A ein maximales Element.

Ende Exkurs.

Beweis von Proposition 2.9:
Sei $I \lhd R$, $I \subsetneq R$. Betrachte
$S :=$ die Menge aller echten Ideale von R, die I enthalten.
$I \in S$, so $S \neq \varnothing$.
S ist partiell geordnet durch Mengeninklusion. Wir behaupten, dass jede total geordnete Teilmenge von S eine obere Schranke in S hat. Sei also $\xi \subseteq S$ eine solche. Setze

$$J := \bigcup_{c \in \xi} C$$

J ist Ideal: $0 \in J$. Seien $a, b \in J$, existieren $C_1, C_2 \in \xi$ mit $a \in C_1$ und $b \in C_2$.
Nun gilt $C_1 \subseteq C_2$ oder $C_2 \subseteq C_1$ (weil ξ total geordnet ist).
In jedem Fall ist $a + b \in J$ (weil $a + b \in C_1$ oder $a + b \in C_2$).
Analog zeigt man: $a \in J$ und $r \in R \Rightarrow ra \in J$.
Nun zeigen wir: $J \subsetneq R$, sonst $1 \in J$, also $1 \in C$ für ein geeignetes $C \in \xi$ - Widerspruch, weil $C \in \xi$ echt sein muss.

Anwendung von Zorn's Lemma ergibt:
S hat maximale Elmente. Wenn M ein solches ist, dann ist klar, dass M ein maximales Ideal ist, welches I enthält, wie behauptet. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Primideale und Maximalideale näher untersuchen. Danach werden wir Produktringe einführen. In diesem Zusammenhang werden wir den Chinesischer Reste-Satz aussagen und beweisen. Damit wird § 2 beendet. In § 3 führen wir Bruchringe ein.

Proposition 3.1.
$M \lhd R$ ist maximal genau dann, wenn R/M ein Körper ist.

Beweis:
M ist maximal, genau dann, wenn $M \subsetneq R$ und es keine Ideale A gibt mit

$$M \subsetneq A \subsetneq R$$

d.h. genau dann, wenn R/M nur $M/M = \{0\}$ und R/M als Ideale hat. Nun Proposition 2.6(2) anwenden. □

Beispiel 3.2.
$n\mathbb{Z} \lhd \mathbb{Z}$ ist maximal genau dann, wenn $\mathbb{Z}/n\mathbb{Z} \backsimeq \mathbb{Z}_n$ ein Körper ist, genau dann, wenn $n = p$ eine Primzahl ist (Lineare Algebra I, 3. Vorlesung).

Definition 3.3.
$P \lhd R$ ist ein Primideal, wenn

(1) P echt ist, i.e. $P \subsetneq R$.

(2) Für alle $a, b, \in R$: Aus $ab \in P$ folgt $a \in P$ oder $b \in P$.

Beispiel 3.4.
$\{0\} \neq p\mathbb{Z} \lhd \mathbb{Z}$ ist Primideal genau dann, wenn p eine Primzahl ist.

Proposition 3.5.
$P \lhd R$ ist Primideal genau dann, wenn R/P ein Integritätsbereich ist.

Beweis:
Per Definition von R/P gilt für $a, b \in R : \overline{ab} = \overline{a}\overline{b}$, und $\overline{a} = \overline{0}$ genau dann, wenn $a \in P$. Dies bedeutet wiederum: P Primideal genau dann, wenn $[\overline{ab} = \overline{a}\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0}$ **oder** $\overline{b} = \overline{0}]$ genau dann, wenn R/P integer ist. □

Aus Proposition 3.1 und 3.5 folgt nun:

Korollar 3.6.
Jedes maximale Ideal ist Primideal.

Definition 3.7.

(1) Seien R, S Ringe. Wir definieren Ringoperationen auf $R \times S$ (koordinatenweise).

$$\left.\begin{array}{rcrcl} (r_1, s_1) & + & (r_2, s_2) & := & (r_1 + r_2, s_1 + s_2) \\ (r_1, s_1) & \times & (r_2, s_2) & := & (r_1 r_2, s_1 s_2) \end{array}\right\} \text{ für alle } r_1, r_2 \in R \text{ und } s_1, s_2 \in S$$

$R \times S$ heißt *Ringprodukt*.

(2) Seien $A, B \lhd R$, setze: $A + B := \{a + b; a \in A, b \in B\}$. A, B sind *teilerfremd*, wenn $A + B = R$

Konvention: In der Bezeichnung $\overline{x}$ für ein Element aus R/I, werden wir zur Erleichterung der Notation das Symbol $\bar{}$ unterbinden, wann immer der Kontext klar ist.

Satz 3.8. (Chinesischer Reste-Satz)
Seien R ein kommutativer Ring mit 1 und $A_1, \ldots, A_k \lhd R$. Die Abbildung

$$\begin{array}{rccc} \varphi: & R & \to & \prod_{i=1}^{k} (R/A_i) \\ & r & \mapsto & (r + A_1, \ldots, r + A_k) \end{array}$$

ist ein Ringhomomorphismus mit $\ker \varphi = \bigcap_{i=1}^{k} A_i$.

Wenn A_i, A_j teilerfremd sind für alle $i \neq j$, dann ist φ surjektiv. In diesem Fall gilt also:

$$R/\bigcap_{i=1}^{k} A_i \simeq \prod_{i=1}^{k} (R/A_i).$$

Beweis:

Ohne Einschränkung $k = 2$ (ÜA). Prüfe, für $r_1, r_2 \in R$ ob $\varphi(r_1 + r_2) \stackrel{?}{=} \varphi(r_1) + \varphi(r_2)$. Wir berechnen:

$$\begin{array}{rcl} \varphi(r_1 + r_2) & = & ((r_1 + r_2) + A_1, (r_1 + r_2) + A_2) \\ & = & ((r_1 + A_1) + (r_2 + A_1), (r_1 + A_2) + (r_2 + A_2)) \\ & = & (r_1 + A_1, r_1 + A_2) + (r_2 + A_1, r_2 + A_2) \\ & = & \varphi(r_1) + \varphi(r_2)\,. \end{array}$$

Analog berechnet man $\varphi(r_1 r_2)$ (ÜA). Also ist φ ein Ringhomomorphismus. Wir berechnen:

$$\begin{array}{rcl} \ker \varphi & = & \{r \in R\,;\, \varphi(r) = 0\} \\ & = & \{r \in R\,;\, \varphi(r) = (A_1, A_2)\} \\ & = & \{r \in R\,;\, r \in A_1 \text{ und } r \in A_2\}. \end{array}$$

Sei nun $A_1 + A_2 = R$. Es existieren also $x \in A_1$ und $y \in A_2$ mit $x + y = 1$.
Es folgt: $x - 1 \in A_2$ und $y - 1 \in A_1$, und somit $\varphi(x) = (0, 1)$ und $\varphi(y) = (1, 0)$.

Sei nun $(r_1 + A_1, r_2 + A_2) \in R/A_1 \times R/A_2$ beliebig. Setze $r := r_2 x + r_1 y$ und berechne:

$$\begin{array}{rcl} \varphi(r) & = & \varphi(r_2 x + r_1 y) \\ & = & \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\ & = & (r_2 + A_1, r_2 + A_2)(0, 1) + (r_1 + A_1, r_1 + A_2)(1, 0) \\ & = & (0, r_2 + A_2) + (r_1 + A_1, 0) \\ & = & (r_1 + A_1, r_2 + A_2). \end{array}$$

Also ist φ surjektiv.
Die letzte Aussage folgt aus Isomorphiesatz. □

§ 3 Bruchringe

Definition 3.9.
Seien R ein kommutativer Ring mit 1 und $D \subseteq R$. D ist multiplikativ, falls $1 \in D$ und $st \in D$ für alle $s, t \in D$.

Beispiel 3.10.

(i) $D = R^\times$

(ii) $D = R \backslash P$ mit $P \lhd R$ Prim.

Konstruktion:
Sei $D \subset R$ eine multiplikative Untermenge, ohne Nullteiler, und so dass $0 \notin D$. (*)

Definiere eine Relation $\sim$ auf $R \times D$:

$$(r, d) \sim (r', d') \Leftrightarrow rd' = dr' .$$

$\sim$ ist Äquivalenzrelation, wir zeigen z.B. die Transitivität:

$$\begin{array}{rccc|c|rcccl} & (r,d) & \sim & (s,e) & \Rightarrow + & re & - & sd & = 0 & \times f \\ \text{und} & (s,e) & \sim & (t,f) & & sf & - & te & = 0 & \times d \end{array} \quad \text{ergibt } (rf - td)e = 0,$$

Außerdem ist e ist kein Nullteiler und $e \neq 0$. Also muss $rf - td = 0$ sein und damit $rf = td$. Also $(r, d) \sim (t, f)$.

Notation:
Schreibe $\frac{r}{d} := [(r, d)]$ (die Äquivalenzklasse von (r, d)) und setze $D^{-1}R :=$ die Menge der Äquivalenzklassen.

Wir Versehen $D^{-1}R$ mit den folgenden Verknüpfungen:

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} := \frac{r_1 d_2 + r_2 d_1}{d_1 d_2} \quad \text{und} \quad \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} := \frac{r_1 r_2}{d_1 d_2}.$$

Im Skript 4 werden wir zeigen dass $D^{-1}R$ ein Ring ist, und werden seine Eigenschaften weiter untersuchen.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript beweisen wir (wie angekündigt am Ende vom Skript 3) Satz 4.2, und liefern wichtige Beispiele. Im Abschnitt 4 untersuchen wir Polynomringe über Ringe; siehe Satz 4.8. Wir beenden mit dem wichtigem Besipiel 4.11.

Definition 4.1. Ein injektiver Ringhomomorphismus heißt eine *Einbettung*.

Ansatz:
R kommutativer Ring mit 1, $D \subset R$ multiplikative Untermenge ohne Nullteiler, $0 \notin D$. (*)

Satz 4.2.
$D^{-1}R$ ist ein kommutativer Ring mit Eins. Die Abbildung

$$\begin{array}{rccc} i: & R & \to & D^{-1}R \\ & r & \mapsto & \frac{r}{1} \end{array}$$

definiert eine Einbettung mit $i(D) \subseteq (D^{-1}R)^\times$.

Beweis:
Wir zeigen, dass die Addition wohldefiniert ist.

Seien also $\frac{a}{b} = \frac{a'}{b'}$, und $\frac{c}{d} = \frac{c'}{d'}$. Wir müssen zeigen dass: $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$.

Wir prüfen:

$$\begin{array}{ccc} \frac{a}{b} = \frac{a'}{b'} & \text{und} & \frac{c}{d} = \frac{c'}{d'} \\ \Downarrow & & \Downarrow \\ ab' = a'b & & cd' = c'd \\ (ad+bc)(b'd') & \stackrel{?}{=} & (a'd'+b'c')(bd) \\ \text{berechne} & & \text{und vergleiche} \\ \| & & \| \\ \underline{ab'}dd' + \underline{\underline{cd'}}bb' & = & \underline{a'b}dd' + \underline{\underline{c'd}}bb' \end{array}$$

Also gilt die Gleichung.

Analog zeigen Sie dass die Multiplikation wohldefiniert ist, dass die Ringaxiome für $D^{-1}R$ gelten, das Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$ sind (ÜA).

Prüfen Sie dass die Abbildung i ein Ringhomomorphismus ist (ÜA). Per Definition von i gilt: $i(r) = 0 \Leftrightarrow \frac{r}{1} = \frac{0}{1} \Leftrightarrow r = 0$. Also ist i injektiv.

Für $d \in D$ ist $i(d) = \frac{d}{1}$ und damit $i(d)^{-1} = \frac{1}{d}$. □

Konvention: Wir identifizieren R mit $i(R)$ (i.e. r mit $\frac{r}{1}$ für alle $r \in R$). Somit wird R mit dem Teilring $i(R)$ von $D^{-1}R$ identifiziert.

Definition 4.3.
$D^{-1}R$ ist der *Ring von Brüchen von R bezüglich D.*

Satz 4.4.
Jeder Integritätsbereich lässt sich in einen Körper einbetten.

Beweis:
Wenn R integer ist, dann erfüllt $D = R\backslash\{0\}$ die Bedingung $(*)$. Dann ist $D^{-1}R$ ein Körper (wenn $0 \neq \frac{r}{d}$ dann ist $r \neq 0$ und $(\frac{r}{d})^{-1} = \frac{d}{r}$). □

Notation: Wenn R integer ist und $D = R\backslash\{0\}$ bezeichnen wir den Körper $D^{-1}R$ mit **Quot (R)**.

Korollar 4.5.
Der Ring R läßt sich in einen Körper einbetten genau dann, wenn er integer ist.

Beispiel 4.6.
Quot $(\mathbb{Z}) = \mathbb{Q}$

Definition 4.7.
P ist ein Primideal; $D = R \setminus P$.
$R_P := D^{-1}R$ bezeichnet die *Lokalisierung von R nach P.*

§ 4 Polynomringe über Ringe

Erinnerung:
• $R[x] := \{p(x) \ ; \ p(x)$ Polynom über $R\}$

$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a, x + a_0$

$n \in \mathbb{N}_0 \left[\begin{array}{rcl} 0 \neq a_n & := & \text{Leitkoeffizient} \\ \deg p & := & n \end{array} \right.$

• $R \subseteq R[x]$ als Teilring der konstanten Polynome (i.e. Polynome p mit $\deg p = 0$).
• Addition: Koordinatenweise (koeffizientenweise)
• Multiplikation: wenn $p(x) = \sum a_i x^i$ und $q(x) = \sum b_j x^j$,
so ist der Koeffizient von x^k im Produkt $p(x)q(x)$ gleich $\sum_{i=0}^{k} a_i b_{k-i}$.
• Wir beantworten nun die Frage: Wann ist $a_n b_m$ Leitkoeffizient vom Produkt $p(x)q(x)$?
Siehe dazu den Beweis vom Satz 4.8.

Satz 4.8.
R ist integer genau dann, wenn $R[x]$ integer ist.

Beweis
"⇐" Ein Teilring von einem Integritätsbereich ist integer.

"⇒" Sei $a_n \neq 0$ und $b_m \neq 0$ für $p(x) = a_n x^n + \cdots + a_o$ und $q(x) = b_m x^m + \cdots + b_o$, dann ist $a_n b_m \neq 0$, weil R integer ist (und damit ist auch $\deg p(x)q(x) = n + m$). Insbesondere ist $p(x)q(x)$ nicht das Nullpolynom. □

Definition 4.9.
Sei K ein Körper. Dann ist Quot $(K[x]) := K(x)$ der *rationale Funtkionenkörper einer Variablen über K.*

Bemerkung 4.10.
Sei R ein Ring. Betrachte die Abbildung

$$\begin{array}{rccc} ev_0: & R[x] & \twoheadrightarrow & R \\ & p(x) & \mapsto & p(0) \quad = \quad \text{der konstante Term von } p(x). \end{array}$$

Dann ist ev_0 ein surjektiver Ringhomomorphismus (ÜA). Wir berechnen:

$$\ker ev_0 =< x >= \{xf(x); f(x) \in R[x]\}$$

(das Ideal der Polynome mit konstantem Term gleich Null).

Es folgt aus Isomorphiesatz dass $R[x]/ < x > \simeq R$.

Beispiel 4.11. Sei nun $R = \mathbb{Z}$, so ist $\mathbb{Z}[x]/ < x > \simeq \mathbb{Z}$.

Wir sehen also (siehe Proposition 3.1 und 3.5): $< x >$ ist ein Primideal in $\mathbb{Z}[x]$, aber ist nicht maximal.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir einige Begriffe (die wir schon in der LA I für den Ring $\mathbb{Z}$ und in der LA II für den Ring $K[x]$ kennengelernt hatten) allgemeiner für kommutative Ringe einführen. Wir werden im Abschnitt 6 Ringe erhalten, die einen Divisionsalgorithmus und Euklidische Algorithmus (zum Berechnen von ggT) besitzen. Im Abschnitt 7 werden wir eine strikt größere Klasse studieren.

§ 5 Teilbarkeit

Sei R stets ein kommutativer Ring mit Eins.

Definition 5.1.
Seien $a, b \in R; b \neq 0$

(i) b *teilt* a, wenn ein $x \in R$ existiert mit $a = bx$. (Bezeichnung: $b|a$)

(ii) $d \in R$ ist ein *gemeinsamer Teiler von a und b* (Bezeichnung: gT von a, b) falls $d|a$ und $d|b$

(iii) $d \in R$ ist ein *ggT von a und b*, falls

(a) d ist ein gT von a und b, und für alle $d' \in R$ gilt:

(b) $d'|a$ und $d'|b$ impliziert $d'|d$.

Bemerkung 5.2.

(i) $b|a$ genau dann, wenn $a \in < b >$ (genau dann, wenn $< a > \subseteq < b >$)

(ii) d ist gT von a, b genau dann, wenn $< a, b > \subseteq < d >$

(iii) d ist ggT von a, b genau dann, wenn d ist gT von a, b und für alle $d' \in R$ gilt: $< a, b > \subseteq < d' >$ impliziert $< d > \subseteq < d' >$.

Aus Bemerkung 5.2 bekommen wir eine hinreichende Bedingung für die $\exists^Z$ eines ggT:

Proposition 5.3.

Seien $a, b \in R$ so dass $< a, b >$ ein Hauptideal ist, i.e. $< a, b > = < d >$, dann ist d ein ggT von a und b.

Die Bedingung ist jedoch nicht notwendig, siehe ÜB.

Definition 5.4.
$x, y \in R$ sind *assoziiert*, falls ein $u \in R^\times$ exisitert mit $xu = y$.

Proposition 5.5. (Eindeutigkeit bis auf Einheiten)

Sei R integer, $d, d' \in R$ und $a, b \in R$.
Es gilt: $< d > = < d' >$ genau dann, wenn d, d' assoziiert sind.
Insbesondere alle ggT von a, b sind zueinander assoziiert.

Beweis:

"$\Leftarrow$" $d' = ud \Leftrightarrow d = d'u^{-1}$ mit $u \in R^\times$. Also $d' = ud \Rightarrow d' \in < d > \Rightarrow < d' > \subseteq < d >$ und umgekehrt aus $d = d'u^{-1}$ folgt auch $< d > \subseteq < d' >$.

"$\Rightarrow$" Seien $d, d' \neq 0$ und $< d > = < d' >$. Also

$$\left.\begin{array}{ll} \exists x \in R & : \ d = xd' \\ \exists y \in R & : \ d' = yd \end{array}\right\| \Rightarrow d = xyd \text{ i.e. } d(1 - xy) = 0$$

R integer und $d \neq 0$ impliziert $1 - xy = 0$, also $xy = 1$.

Die letzte Aussage folgt aus Bemerkung 5.2. □

§ 6 Euklidische Bereiche

Definition 5.6.

(1) Eine Abbildung $N : R \setminus \{0\} \to \mathbb{N}_0$ heißt *Norm.*

(2) Der Integritätsbereich R, versehen mit der Norm N, heißt *euklidisch* (R ist E.R.), wenn er einen Divisionsalgorithmus bezüglich N erlaubt, das heißt:
für $\forall a, b \in R$ mit $b \neq 0$ $\exists q, r \in R$, so dass $a = qb + r$, wobei $r = 0$ oder $N(r) < N(b)$.

Beispiel 5.7.

(i) $\mathbb{Z}$ mit $N(a) := |a|$

(ii) $K[x]$, wenn K *ein Körper* mit $N(p(x)) := \deg p(x)$ ist.

Weitere Beispiele: Siehe ÜB.

Proposition 5.8.
Sei R ein euklidischer Integritätsbereich, $I \lhd R$, dann ist I ein Hauptideal.

Beweis:
Sei $I \neq \{0\}$ und $0 \neq d \in I$, also $< d > \subseteq I$. Wähle d so dass $N(d)$ minimal ist. Sei nun $a \in I$ und $q, r \in R$ mit $a = qd + r$ wobei $r = 0$ oder $N(r) < N(d)$. Da $r = a - qd \in I$, ist $N(r) < N(d)$ nicht möglich. Also $r = 0$ und somit $a = qd \in < d >$. □

Eine wichtige Eigenschaft von E.R. ist die $\exists^Z$ eines ggT sowie eines Algorithmus zum Berechnen von ggT . Die Aussage und Beweis vom Satz 5.9 haben wir im LA I (Rückwärts EA; Skript 3 Seiten 2 und 3) für $R = \mathbb{Z}$ (und in LA II Skripte 3 und 5 für $R = K[x]$) detailliert studiert. Wir wiederholen hier die Beweisschritte nicht ausführlich.

Satz 5.9.
Sei R E.R; $a, b \in R \neq 0$ und $d = r_n$ der letzte ungleich Null Rest in **(DA)**. Dann ist

(1) d ein ggT von a und b

(2) $d = ax + by$ für geeignete $x, y \in R$.

Beweis: Wiederholter Anwendung des Divisionsalgorithmus (DA)
Seien $a, b \in R, b \neq 0$

$$\begin{array}{lllll} a & = & q_0 b & + & r_0 \\ b & = & q_1 r_0 & + & r_1 \\ r_0 & = & q_2 r_1 & + & r_2 \\ \vdots & & & & \\ r_{n-2} & = & q_n r_{n-1} & + & r_n \quad r_n \neq 0 \\ r_{n-1} & = & q_{n+1} r_n & & (*) \end{array}$$

(Da

$$N(b) > N(r_0) > \cdots > N(r_{n-1}) > N(r_n) \geq 0$$

kann der Abstieg nur endlich viele Schritte n haben, das Verfahren muss also zwangläufig mit einer Gleichung $(*)$ anhalten). □

§ 7 Hauptidealbereiche

Definition 5.10.
Ein *Hauptidealbereich* (H.I.R.) ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

Proposition 5.11.
Sei R ein Hauptidealbereich, $a, b \neq 0, a, b \in R$ und d ein Erzeuger von $< a, b >$. Es gelten:

(1) d ist ggT von a, b

(2) $\exists x, y \in R$ mit $d = ax + by$

(3) d ist (bis auf Einheiten) eindeutig.

Beweis:
Folgt aus Proposition 5.2, Bemerkung 2.3 (3) und Proposition 5.5. □

Proposition 5.12.
Jedes Primideal in einem Hauptidealbereich ist auch maximal.

Beweis:
Sei $< p > \neq \{0\}$ Primideal und $M \supseteq < p >, M$ maximal (M existiert vgl. Proposition 2.9).
Nun ist auch $M = < m >$ ein Hauptideal und $p \in < m >$. Also existiert $r \in R$ mit $p = rm$.
Aber $< p >$ prim $\Rightarrow r \in < p >$ oder $m \in < p >$.
1. Fall: $m \in < p > \Rightarrow < m > \subseteq < p > \Rightarrow < p > = M$
2. Fall: $r \in < p > \Rightarrow r = ps \Rightarrow p = psm$, kürzen ergibt: $sm = 1$. Somit ist aber $m \in R^\times$. Das widerspricht, dass M maximal, also echt, ist (vgl. Proposition 2.6(1)). □

Beispiel 5.13.

(1) Alle Ideale in $\mathbb{Z}$ sind Hauptideale der Gestalt $n\mathbb{Z}$, $n\mathbb{Z}$ ist maximal genau dann, wenn $n = p$ eine Primzahl ist.

(2) $\mathbb{Z}[x]$ ist kein Hauptidealbereich, weil $< x >$ prim, aber nicht maximal ist (Beispiel 4.11).

Wir verallgemeinern Beispiel 5.13 (2):

Korollar 5.14.
Sei R integer, $R[x]$ ist ein Hauptidealbereich genau dann, wenn R ein Körper ist.

Beweis:
"$\Leftarrow$" R ist ein Körper $\Rightarrow R[x]$ ist E.R. (s. Beispiel 5.7 (ii)) $\Rightarrow R[x]$ ist H.I.R. (s. Prop. 5.8).

"$\Rightarrow$" $R[x]/ < x > \simeq R$ (vgl. Bemerkung 4.10), also ist $< x >$ Primideal (s. Proposition 3.5).

Nun $R[x]$ Hauptidealbereich $\Rightarrow < x >$ ist ein maximales Ideal (s. Proposition 5.12) $\Rightarrow R[x]/ < x >$ ist ein Körper (s. Proposition 3.1) . □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst prime und irreduzible Elemente in einem integer Ring einführen und studieren. Im Abschnitt 9 werden wir dann unsere Untersuchung über Faktorielle Ringe beginnen.

§ 8 Primelemente, Irreduzible Elemente

Sei R stets ein integer Ring.

Definition 6.1.

(1) Sei $0 \neq p \in R$, p ist *Primelement*, wenn $< p >$ *Primideal* in R ist
(für alle $a, b \in R : p|ab \Rightarrow p|a$ oder $p|b$).

(2) Sei $0 \neq r \in R$; $r \notin R^\times$, p ist *irreduzible* in R, wenn für alle $a, b \in R : r = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$. Sonst ist r *reduzible*.

Proposition 6.2.
Sei $p \in R$, p ist Primelement $\Rightarrow p$ ist irreduzible.

Beweis:
Sei $< p > \neq \{0\}$ Primideal. Also ist $p \notin R^\times$.
Wenn $p = ab$ dann folgt: $ab \in < p > \Rightarrow a \in < p >$ oder $b \in < p >$.
1. Fall: $a \in < p > \Rightarrow a = pr \Rightarrow p = prb$ oder $p(1 - rb) = 0 \Rightarrow 1 = rb$; also $b \in R^\times$.
2. Fall: Analog. □

Proposition 6.3.
Sei R Hauptidealbereich, $p \in R$ irreduzible $\Rightarrow p$ ist Primelement.

Beweis:
Sei $p \notin R^\times; p \neq 0$, p irreduzible.
Sei $M \lhd R$ ein Ideal so dass $< p > \subseteq M$. Nun existiert ein $m \in R$ mit $M = < m >$.
Also $\exists r : p = rm$ und p irreduzible, also

1. Fall		2. Fall
$r \in R^\times$	oder	$m \in R^\times$
$\Downarrow$		$\Downarrow$
$< p >=< m >$		$< m >= R$

Wir haben gezeigt dass $< p >$ maximal, und insbesondere Primideal ist. □

§ 9 Faktorielle Ringe

Definition 6.4.
R ist *faktoriell*, wenn

(1) Für alle $0 \neq r \in R \setminus R^\times$ existiert $p_1, \ldots, p_n \in R$ irreduzibel: $r = p_1 \cdots p_n$ (†)

(2) Diese Darstellung ist *eindeutig bis auf die Reihenfolge und Assoziiertheit*:
D.h. wenn auch $r = q_1 \cdots q_m$ mit $q_1, \ldots, q_m$ irreduzible, dann ist $m = n$
und $\forall$ i $\exists$ j und $u_i \in R^\times$ so dass: $u_i p_i = q_j$.

(3) Also R ist faktoriell wenn für jedes $r \in R$, $r \neq 0$ beliebiges Element, gibt es für r eine Darstellung

$$r = u p_1^{e_1} \cdots p_n^{e_n}$$

mit $u \in R^\times, e_i \in \mathbb{N}_0$, p_i irreduzible, mit $p_i \neq p_j$ für $i \neq j$. (†)

Für faktorielle Ringe gilt auch die Umkehraussage von Proposition 6.2:

Proposition 6.5.
Sei R faktoriell und $p \in R$, es gilt: p irreduzible $\Rightarrow p$ ist Primelement.

Beweis:
Sei $0 \neq p$, $p \in R \setminus R^\times$ irreduzible und $a, b \in R$ mit $p|ab$. Nun $p|ab \Rightarrow ab = pc$ für ein $c \in R$ $(*)$
Schreibe a und b wie in (†).
Da p irreduzibel ist, folgt aus $(*)$ und der Eindeutigkeit in (†): p ist assoziiert mit einem der irreduziblen Faktoren in der Darstellung von a oder von b.
Ohne Einschränkung sei es a, und schreibe $a = (up)p_2 \cdots p_n$; $u \in R^\times$, $p_i \in R$. Somit haben wir bewiesen dass $p|a$. □

Auch für faktorielle Ringe gilt die Existenz eines $ggTs$ (vgl. Satz 5.9):

Proposition 6.6.
Sei R faktoriell, a und $b \in R$. Schreibe:
$a = u p_1^{e_1} \cdots p_n^{e_n}$ (†)
$b = v p_1^{f_1} \cdots p_n^{f_n}$ (‡)

wobei $u, v \in R^\times$, p_i irreduzible, $p_i \neq p_j$ für $i \neq j$, e_i , $f_i \in \mathbb{N}_0$.

Setze $d := p_1^{min(e_1, f_1)} \cdots p_n^{min(e_n, f_n)}$ (††)
Dann ist d ein ggT von a und b.

Beweis:
Aus (††), (‡) und (†) ist klar, dass $d|a$ und $d|b$. Sei $d' \in R$ so dass, $d'|a$ und $d'|b$. Schreibe in der (†) Darstellung, mit q_i irreduzibel:

$$d' = v q_1^{g_1} \cdots q_n^{g_n} .$$

Nun für alle i : $q_i|d' \Rightarrow q_i|a$ und $q_i|b$.
Also für alle i : $q_i|a \Rightarrow$ existiert ein j und $u_i \in R^\times$ so dass $p_j = u_i q_i$.
Also $g_\ell \leq e_\ell$. Analog zeigt man dass $g_\ell \leq f_\ell$. Also $g_\ell \leq min(e_\ell, f_\ell)$. Somit haben wir gezeigt: $d'|d$. □

Satz 6.7.
Sei R ein Hauptidealbereich, dann is R faktoriell.

Beweis:
Sei $0 \neq r \in R \setminus R^\times$. Wir wollen eine Darstellung (†) erreichen.
Ist r irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r = r_1 r_2$, $r_1 \notin R^\times$ und $r_2 \notin R^\times$.
Sind r_1, r_2 irreduzibel, dann ist das Ziel erreicht. Sonst zerlege $r_1 = r_{11} r_{12}$, usw.

Diese Prozedur muss nach endlich vielen Schritten anhalten, da wir sonst eine unendliche (**strikte**) für die Inklusion ansteigende Folge von Idealen bekommen:

$$< r > \subsetneq < r_1 > \subsetneq < r_{11} > \subsetneq \cdots \subseteq R\,.$$

Wir behaupten nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann:

Sei also $I_i \lhd R$ mit $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$.
Setze $I := \bigcup_{i=1}^{\infty} I_i \lhd R$. Da R ein Hauptidealbereich, existiert $a \in R$ mit $I = < a >$.
Nun $a \in I \Rightarrow \exists n \in \mathbb{N} : a \in I_n$. Also $I_n \subseteq I = < a > \subseteq I_n$ und somit $I = I_n$.
Damit ist die Behauptung bewiesen.

Wir haben also die $\exists^Z$ einer Darstellung (†) gezeigt. Die Aussage über die Eindeutigkeit erfolgt per Induktion über n in der Darstellung $r = p_1 \cdots p_n$ (genau so wie in Lineare Algebra II, Skript 5 Seite 3, Beweis vom Satz 5.15). □

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

Prof. Dr. Salma Kuhlmann

Bisher haben wir zwei Hauptthemen untersucht: Wir haben einerseits diese Inklusionen Körper ⊆ Euklidische Bereiche ⊆ Hauptidealbereiche ⊆ Faktorielle Bereiche ⊆ Integritätsbereiche untersucht und andererseits haben wir Polynomringe über Integerringe untersucht. In diesem Skript werden wir diese zweite Untersuchung fortsetzen. Unser Ziel ist es, Satz 4.8 ähnlich für faktorielle Ringe zu zeigen.

§ 10 Polynomringe über faktorielle Ringe

Sei R stets integer.

Lemma 7.1.
$R[x]$ ist faktoriell $\Rightarrow R$ ist faktoriell.

Beweis:
Da R integer ist, wissen wir dass $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ für alle $0 \neq p, q \in R[x]$ $(*)$ (und dass auch $R[x]$ integer ist; siehe Satz 4.8 und seinen Beweis). Aus $(*)$ folgt dass $(R[x])^\times = R^\times$ und $r \in R$ ist irreduzibel in $R[x]$ genau dann, wenn r irreduzibel in R ist. $(**)$ (ÜA).
Sei nun $0 \neq r \in R \setminus R^\times$, per Annahme ist r das Produkt vom Irreduziblen in $R[x]$ (und diese Darstellung ist eindeutig bis auf Reihenfolge und Assoziiertheit). Diese irreduzible Faktoren müssen wegen $(*)$ Grad 0 haben, d.h. die Faktoren sind Elemente aus R. Wegen $(**)$ sind diese Faktoren irreduzible auch in R. Wir haben eine Darstellung wie in Definition 6.4(1) (†) bekommen. Die Eindeutigkeit Bedingung in Definition 6.4(2) wird analog geprüft. □

Um die Umkehrung von Lemma 7.1 zu etablieren (siehe Skript 8) brauchen wir hier das Lemma von Gauß. Hierfür brauchen wir wiederum das Hilfslemma 7.2:

Lemma 7.2.
Sei $I \lhd R$. Dann gelten für das Ideal $< I > \lhd R[x]$:

1. $< I >= I[x] := \{f(x) \in R[x]\,;\ \ f(x) = \sum a_i x^i \text{ mit } a_i \in I\}$
2. $R[x]/I[x] \simeq (R/I)[x]$
3. I ist Primideal in $R \Rightarrow I[x]$ ist Primideal in $R[x]$.

Beweis:
Die 1. Aussage ist leicht zu prüfen. Betrachte nun $\begin{array}{rccc} \varphi: & R[x] & \to & (R/I)[x] \\ & \sum a_i x^i & \mapsto & \sum \overline{a_i} x^i \end{array}$

Es ist leicht zu prüfen dass φ ein Ringhomomorphismus ist; dass φ surjektiv ist; und dass $\ker \varphi = I[x]$. Die 2. und 3. folgen nun aus Isomorphiesatz sowie Proposition 3.5 und Satz 4.8. □

Lemma 7.3. (Lemma von Gauß)
Sei R faktoriell, $F := \text{Quot}(R)$ und $p(x) \in R[x]$. Wenn $p(x)$ reduzibel in $F[x]$ ist, so ist $p(x)$ reduzibel in $R[x]$. Genauer: Wenn

$$p(x) = A(x)B(x), A, B \in F[x], \deg A \geq 1, \deg B \geq 1\,,$$

dann gibt es $0 \neq r, 0 \neq s \in F$ so dass

$$\left.\begin{array}{l} rA(x) := a(x) \\ sB(x) := b(x) \end{array}\right\} \in R[x] \qquad \deg a(x) \geq 1, \deg b(x) \geq 1$$

und $p(x) = a(x)b(x) \in R[x]$.

Beweis:

$$\begin{array}{ccccc} p(x) & = & A(x) & & B(x) \\ \uparrow & & \uparrow & & \uparrow \\ R[X] & & F[x] & & F[x] \end{array}$$

Die Koeffizienten von A, B sind aus der Form $\frac{r_i}{s_i}$ mit $r_i, 0 \neq s_i \in R$. Wir multiplizieren A, B jeweils mit den gemeinsamen Nennern seiner Koeffizienten und bekommen eine Gleichung:

$$\left.\begin{array}{ccccc} dp(x) & = & a'(x) & & b'(x) \\ \uparrow & & \uparrow & & \uparrow \\ d \in R & & \in R[x] & & \in R[x] \end{array}\right\} \text{ mit } d \in R, d \neq 0; \deg a'(x) \geq 1, \deg b'(x) \geq 1; a', b' \in R[x]. \qquad (*)$$

und $a'(x) = \alpha A(x), b'(x) = \beta B(x); \alpha, \beta \in F$.

1. Fall: $d \in R^\times$ ✓ (die Behauptung gilt in diesem Fall).

2. Fall: $d \in R \setminus R^\times$
So schreibe $d = p_1 \cdots p_n$, mit p_i irreduzibel in R für alle i.

- p_1 irreduzibel in $R \Rightarrow I :=< p_1 >$ ist Primideal in R und $d \in I$.
- $I[x] = p_1 R[x]$ Primideal in $R[x]$, $R[x]/I[x] \simeq (R/I)[x]$ und $(R/I)[x]$ ist integer (vgl. Lemma 7.2).

Wir reduzieren die Gleichung (*) mod I. Wir bekommen $0 = \overline{a'(x)b'(x)}$ in $(R/I)[x]$. Also ist ohne Einschränkung $\overline{a'(x)} = 0$, das heißt alle Koeffizienten von $a'(x)$ liegen in I sind also durch p_1 teilbar in R. So hat man $a''(x) := \frac{1}{p_1}a'(x) \in R[x], \deg a''(x) \geq 1$ mit $\frac{1}{p_1} \in F$, das heißt wir können die Gleichung (*) um p_1 kürzen und bekommen eine neue Gleichung

$$d'p(x) = a''(x)b''(x) \text{ in } R[x].$$

Aber nun hat d' einen irreduziblen Faktor weniger, i.e. $d' = p_2 \cdots p_n$.

Wiederholung mit $p_2, \ldots, p_n$ (gleiche Argumente) ergibt eine Gleichung schließlich aus der Form

$$\begin{array}{lccll} & p(x) & = & a(x)b(x) & a(x), b(x) \in R[x] \\ \text{mit} & a(x) & = & \alpha' a'(x) & \alpha', \beta' \neq 0 \\ & b(x) & = & \beta' b'(x) & \alpha', \beta' \in F \end{array}$$

$$\text{d.h.} \quad \begin{array}{ccc} a(x) & = & \alpha\alpha' A(x) \\ b(x) & = & \beta\beta' B(x) \end{array} \quad \text{mit } \alpha\alpha' \in F \text{ und } \beta\beta' \in F. \qquad \square$$

Korollar 7.4.
Sei R faktoriell, $F := \text{Quot}\,(R); \deg p \geq 1$, wobei $\sum_{i=0}^{n} a_i x^i =: p(x) \in R[x]$
mit ggT von $\{a_0, \ldots, a_n\} = 1$.
Dann ist $p(x)$ in $R[x]$ irreduzibel genau dann, wenn $p(x)$ in $F[x]$ irreduzibel. Insbesondere ist $p(x) \in R[x]$ normiert und in $R[x]$ irreduzibel, so ist $p(x)$ in $F[x]$ irreduzibel.

Beweis:
GL ergibt: Ist $p(x)$ in $F[x]$ reduzibel, so ist $p(x)$ in $R[x]$ reduzibel. Umgekehrt ist $p(x)$ in $R[x]$ reduzibel, dann ist $p(x) = a(x)b(x)$, wobei $a(x), b(x) \in R[x] \setminus R$ (sonst wäre der ggT der Koeffizient von $p(x)$ in R ungleich 1).
Das heißt $p(x) = a(x)b(x)$ für $a(x), b(x) \in R[x], \deg a(x) \geq 1, \deg b(x) \geq 1$. Insbesondere $p(x) = a(x)b(x)$ für $a(x), b(x) \in F[x], \deg a(x) \geq 1, \deg b(x) \geq 1$, das heißt $p(x)$ ist in $F[x]$ reduzibel. □

Wie angekündigt werden wir im Skript 8 die Umkehrung von Lemma 7.1 zeigen; wir werden wir zeigen dass R faktoriell impliziert $R[x]$ faktoriell. Eigentlich werden wir das Resultat auch für $R[x_1, \ldots, x_n]$ erhalten. Wir beenden Skript 7 mit einem Exkurs. Hier führen wir diesen Ring ein, und fassen einige Begriffe zusammen.

Exkurs $R[x_1, \ldots, x_n] := R[x_1, x_2, \ldots, x_{n-1}][x_n]$.
Notation $= \{p(x_1, \ldots, x_n) | p \in R[x_1, \ldots, x_n]\}$.

Also: *Polynome* in den Variablen $x_1, \ldots, x_n$ werden folgendermaßen definiert:
Es ist eine endliche Sumem von *Monomen*.

$$m(x_1, \ldots, x_n) := a x_1^{d_1} \cdots x_n^{d_n} \qquad a \in R$$

$$\text{Notation} \quad \begin{cases} := a \underline{x}^{\underline{d}} & d_i \in \mathbb{N}_0 \\ (x_1, \ldots, x_n) := \underline{x} \\ (d_1, \ldots, d_n) := \underline{d} \in \mathbb{N}_0^n \end{cases}$$

- d_i ist der *Grad von* x_i in $m(\underline{x})$
- $|\underline{d}| := \sum_{i=1}^{n} d_i$ ist der *Grad von* $m(\underline{x})$ $\deg m(\underline{x}) := |\underline{d}|$
- $\deg p(x_1, \ldots, x_n)$ ist der größte Grad von seinen Monomen.
- Die Summe aller Monomen von $p(x_1, \ldots, x_n)$ vom Grad k heißt die *homogene Komponente von p vom Grad k*.
- Wenn $\deg p = d$, so läßt sich p eindeutig als Summe

$$p = p_0 + p_1 + \cdots + p_d$$

beschreiben, wobei p_k die homogene Komponente vom Grad k ist für $0 \leq k \leq d$ (und $p_k = 0$ vorkommen kann).

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir den im Skript 7 angekündigten Beweis von Satz 8.1 führen. Der letzte Abschnitt 11 im Kapitel 1 wird für Irreduzibilitätsteste und Beispiele gewidmet. Damit beenden wir Kapitel 1.

Sei hier R stets ein integer Ring.

Satz 8.1.
R ist genau dann faktoriell wenn $R[x]$ faktoriell ist.

Beweis:
Die Rückrichtung ist Lemma 7.1 und wurde bereits gezeigt.
Sei R faktoriell. Seien $F = \text{Quot}\,(R)$ und $0 \neq p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. Setze $d = \text{ggT}\{a_0, \ldots, a_n\}$ (d existiert weil R faktoriell ist wegen Proposition 6.6). Schreibe $p(x) = dq(x)$ (für ein geeignetes $q(x) \in R[x]$). Der ggT der Koeffizienten von q ist nun 1.
Da R faktoriell ist lässt sich d in R als Produkt $d = d_1 \cdots d_m$ von Irreduziblen faktorisieren und diese Irreduziblen in R sind auch in $R[x]$ irreduzibel (Beweis Lemma 7.1 $(**)$).
Nun wollen wir $q(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben. Da $F[x]$ faktoriell ist (Beispiel 5.7(ii)), existieren $q_1(x), q_2(x), \ldots, q_n(x) \in F[x]$, irreduzibel in $F[x]$ mit $q(x) = q_1(x) \cdots q_n(x)$. Nach dem Lemma von Gauß können wir annehmen dass $q_i \in R[x]$ für alle $i = 1, \cdots, n$. Da der ggT der Koeffizienten von $q(x)$ 1 ist, ist der ggT der Koeffizienten von q_i auch 1 , für alle $i = 1, \cdots, n$. Nach Korollar 7.4 ist q_i irreduzibel in $R[x]$, für alle $i = 1, \cdots, n$. Wir können also $p(x)$ als Produkt von irreduziblen Polynomen aus $R[x]$ schreiben:
$p(x) = d_1 \cdots d_m q_1(x) \cdots q_n(x)$.
Es bleibt noch zu zeigen, dass diese Faktorisierung eindeutig bis auf Reihenfolge der Faktoren und Multiplikation mit Einheiten ist. Das wird als ÜA gemacht. □

Induktion auf n ergibt:

Korollar 8.2.
Ist R faktoriell so ist $R[x_1, \ldots, x_n]$ auch faktoriell.

Beweis: ÜA.

§ 11 Irreduzibilitätskriterien

Wir untersuchen hier weiter die Irreduzibilität eines Polynoms in einem Integerring. Wir beginnen mit einer Bemerkung:

Bemerkung 8.3. Sei $R = K$ ein Körper, und $0 \neq p(x) \in K[x] \setminus K$. Wenn $\deg p = 1$ dann ist p irreduzibel. Wenn $\deg p = 2$ oder $\deg p = 3$, dann ist p reduzibel genau dann, wenn p einen linearen Faktor in $K[x]$ hat, genau dann, wenn p eine Nullstelle in K hat (s. LA II Skript 4 Korollar 4.1).

Lemma 8.4. Sei $p(x) \in R[x] \setminus R$ ein normiertes Polynom. Dann ist p irreduzible in $R[x]$ genau dann, wenn $p(x)$ kein Produkt $p(x) = a(x)b(x)$ von normierten Polynomen $a(x)$, $b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$ ist.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, so dass $p(x) = a(x)b(x)$ mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Da R integer ist, ist $\deg p(x) = \deg a(x) + \deg b(x)$ (s. Beweis Satz 4.8). Da $\deg p(x) > 0$, sind $\deg a(x) > 0$ und $\deg a(x) > 0$, also sind $a(x) \notin R$ und $b(x) \notin R$. Da $R[x]^\times = R^\times$ (s. Beweis Lemma 7.1 $(**)$) sind insbesondere $a(x) \notin R[x]^\times$ und $b(x) \notin R[x]^\times$. Also ist $p(x)$ reduzibel.

Umgekehrt sei $p(x)$ nicht-konstant, normiert und reduzibel in $R[x]$.
Also gibt es Polynome $a'(x) \in R[x] \setminus R[x]^\times$ und $b'(x) \setminus R[x]^\times$ mit $p(x) = a'(x)b'(x)$. Insbesondere sind $a'(x) \notin R^\times$ und $b'(x) \notin R^\times$. Wir bemerken dass der Leitkoeffizient von $p = 1 = a_m b_n$, wobei $a_m \in R$ der Leitkoeffizient von $a'(x)$ und $b_n \in R$ der Leitkoeffizient von $b'(x)$ sind (s. Beweis Satz 4.8). Also sind $a_m, b_n \in R^\times$ (es gelten $b_n = a_m^{-1}$ und $a_m = b_n^{-1}$). Es folgt dass $a'(x) \notin R$ (sonst wäre $a'(x) = a_m \in R^\times$) und analog $b'(x) \notin R$. Also sind $\deg a'(x) < \deg p(x)$ und $\deg b'(x) < \deg p(x)$.

Nun setze $a(x) := a_m^{-1} a'(x)$ und $b(x) := b_n^{-1} b'(x)$. Dann sind $a(x)$ und $b(x)$ normiert mit $\deg a(x) < \deg p(x)$ und $\deg b(x) < \deg p(x)$. Ferner gilt

$$p(x) = a_m b_n p(x) = b_n^{-1} a_m^{-1} a'(x) b'(x) = a_m^{-1} a'(x) b_n^{-1} b'(x) = a(x)b(x).$$

□

Proposition 8.5.
Sei I ein echtes Ideal in R und sei $p(x)$ ein normiertes Polynom aus $R[x] \setminus R$. Wenn $\varphi(p) = \overline{p}(x)$ in $(R/I)[x]$ sich nicht als Produkt $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$ von Polynomen in $(R/I)[x]$ mit $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$ darstellen lässt, dann ist $p(x)$ irreduzibel in $R[x]$.

Beweis:
Sei $p(x) \in R[x]$ nicht-konstant, normiert und reduzibel. Aus Lemma 8.4 ist $p(x) = a(x)b(x)$, $a(x)$, $b(x) \in R[x]$ normiert und nicht-konstant. Seien $\overline{p}(x), \overline{a}(x)$ und $\overline{b}(x)$ die Bilder von $p(x), a(x)$ und $b(x)$ in $(R/I)[x]$ (s. Beweis Lemma 7.2). Dann $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$. Da I echt ist, $a(x)$ und $b(x)$ normiert und nicht-konstant sind, so sind auch $\overline{a}(x)$ und $\overline{b}(x)$. Es folgt, dass $\deg \overline{a}(x) < \deg \overline{p}(x)$ und $\deg \overline{b}(x) < \deg \overline{p}(x)$. □

Proposition 8.5 kann man anwenden um zu prüfen ob ein Polynom über $\mathbb{Z}$ irreduzibel ist.

Beispiel:
Betrachte das Polynom $x^4 + 9x^3 + 10x^2 + 22x + 1 \in \mathbb{Z}[x]$.
Das Bild in $\mathbb{Z}_2[x]$ ist $x^4 + x^3 + 1$. Dieses Polynom besitzt keine Nullstelle in $\mathbb{Z}_2$ (prüfe 0 und 1). Daher, wenn es reduzibel ist, dann zerfällt es als Produkt zweier irreduziblen Polynomen aus $\mathbb{Z}_2[x]$ von Grad 2. (Wir arbeiten über $\mathbb{Z}_2 = \mathbb{F}_2$ und können Bemerkung 8.3 ausnutzen). Wenn $p(x) \in \mathbb{Z}_2[x]$ irreduzibel von Grad 2 ist, dann ist das Leitkoeffizient 1 und das konstante Koeffizient ist auch 1 (weil 0 keine Nullstelle ist). Das Polynom x^2+1 hat die Nullstelle 1. Somit gibt es nur ein irreduzibles Polynom von Grad 2 aus $\mathbb{Z}_2[x]$, und zwar $x^2 + x + 1$ (prüfe, dass 0 und 1 keine Nullstelle sind). Aber $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Somit ist $x^4 + x^3 + 1$ irreduzibel über $\mathbb{Z}_2$ und, daher ist $x^4 + 9x^3 + 10x^2 + 22x + 1$ irreduzibel über $\mathbb{Z}$.

Leider funktioniert dieses Verfahren nicht immer.

Bemerkung 8.6. Seien $a(x), b(x)$ nicht-konstante Polynome $\in R[x]$ so dass $f(x) := a(x)b(x) = x^n$ für ein $n \in \mathbb{N}$. Dann sind $a(x)$ und $b(x)$ Monome, das heißt, es gibt $\alpha, \beta \in R^\times$ und $p, q \in \mathbb{N}$ so dass $a(x) = \alpha x^p$ und $a(x) = \beta x^q$ (und $\alpha\beta = 1$, $p + q = n$). In der Tat kann man zeigen, dass nur die Leitkoeffiziente von $a(x)$ und $b(x)$ ungleich Null sind. Siehe ÜA.

Hier zeigen wir dass die konstante Koeffiziente gleich Null sind. Bemerke dass der konstante Koeffizient $f(0)$ von $f(x) := a(x)b(x)$ das Produkt der konstante Koeffiziente $a(0)$ und $b(0)$ von $a(x)$ and $b(x)$ ist. Wir behaupten dass $b(0) = a(0) = 0$. In der Tat, $0 = f(0) = a(0)b(0)$. Da R ein Integritätsbereich ist, gilt $a(0) = 0$ oder $b(0) = 0$. Angenommen $a(0) = 0$. Sei $F = \text{Quot}\,(R)$ und $m \in \mathbb{N}$ maximal mit $a(x) = x^m a'(x)$ für gewisses $a'(x) \in F[x]$ (m ist die Vielfachheit der Nullstelle $x = 0$ von $a(x)$). Dann $a'(0) \neq 0$ und somit $a'(x)b(x) = x^{n-m}$. Da $b(x)$ nicht konstant ist, dann gilt $n - m > 0$. Daher $a'(0)b(0) = 0$ also $b(0) = 0$ und die Behauptung wurde bewiesen.

Proposition 8.7. (Eisensteinkriterium)
Seien P ein Primideal in R, $n \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$. Angenommen $a_{n-1}, \ldots, a_0 \in P$ aber $a_0 \notin P^2$. Dann ist $f(x)$ irreduzibel in $R[x]$.

Beweis:
Angenommen $f(x) = a(x)b(x)$ in $R[x]$ wobei $a(x)$ und $b(x)$ nicht-konstante normierte Polynome sind (s. Lemma 8.4).
Seien $\overline{f}(x), \overline{a}(x), \overline{b}(x)$ die Bilder von $f(x), a(x)$ bzw. $b(x)$ in $(R/P)[x]$ (s. Beweis Lemma 7.2). Also $x^n = \overline{f}(x) = \overline{a}(x)\overline{b}(x)$. Dann gilt $\overline{a}(0) = \overline{b}(0) = 0$ (man kann Bemerkung 8.6 anwenden weil R/P ein Integerring ist). Aber dann liegen die konstante Koeffizienten von $a(x)$ und $b(x)$ in P und somit liegt der konstante Koeffizient a_0 von $f(x)$ in P^2. Widerspruch. Somit ist $f(x)$ irreduzibel. □

Korollar 8.8.
Sei p prim in $\mathbb{Z}$, $n \geq 1$ und sei $f(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$. Angenommen p teilt a_i für alle $0 \leq i \leq n-1$ aber p^2 teilt nicht a_0. Dann ist $f(x)$ irreduzibel in $\mathbb{Z}[x]$ sowie in $\mathbb{Q}[x]$.

Beweis:
Für $\mathbb{Z}[x]$: Wende das Eisensteinkriterium auf das Primideal $< p >$ an. Für $\mathbb{Q}[x]$: Korollar 7.4 zu Gauß Lemma anwenden. □

Beispiel:

1. Das Polynom $x^5 + 10x^4 + 25x^2 + 35 \in \mathbb{Z}[x]$ ist irreduzibel nach Eisensteinkriterium auf $p = 5$ angewandt.

2. Sei $f(x) := x^4 + 1 \in \mathbb{Z}[x]$. Wir dürfen das Eisensteinkriterium nicht direkt anwenden. Sei $g(x) = f(x + 1)$, also $g(x) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Nun, nach Eisenstein angewandt auf 2, ist $g(x)$ irreduzibel und, wenn f als Produkt von nicht-konstanten Faktoren zerfällt, dann auch g. Daher ist f irreduzibel.

Gesamtskript
Kapitel II
zur Vorlesung
Algebra I

Prof.'in Dr. Salma Kuhlmann

Inhaltsverzeichnis für das Gesamtskript Kapitel 2[1]
zur Vorlesung: Algebra I (WiSe2020/2021)

Prof. Dr. Salma Kuhlmann

KAPITEL II: KÖRPERERWEITERUNGEN.

[1]Die Seitenzahlen in Klammern geben die Seitenzahl für die Suche mit Adobe Acrobat Reader an (unter dem Menü ANZEIGE – GEHE ZU – SEITE).

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

Prof. Dr. Salma Kuhlmann

Kapitel 2

KÖRPERERWEITERUNGEN

In diesem Kapitel werden wir besondere Körpererweiterungen kennenlernen. Wir werden algebraische Körpererweiterungen untersuchen, wo wir Nullstellen für Polynome finden. Insbesondere werden wir den Zerfällungskörper und den algebraischen Abschluss konstruieren. Wir werden die Vielfachheit einer Nullstelle, die wir schon in LA II gelernt haben, genauer betrachten, um separable Körpererweiterungen zu untersuchen. Im letztem Kapitel 4 werden wir dann Galois Erweiterungen behandeln, nachdem wir im Kapitel 3 zwischendurch die dafür notwendige Gruppentheorie studieren.
In diesem Skript werden wir im Abschnitt 12 algebraische, insbesondere endliche Körpererweiterungen studieren. Wir fangen an mit Erinnerungen (Definition 9.1, Bemerkung 9.2) aus LA I Skript 4.

Definition 9.1.

1. Die *Charakteristik* eines Körpers F, bezeichnet $\mathrm{Char}(F)$, ist die kleinste $n \in \mathbb{N}$ mit $n \cdot 1 = 0$. Falls ein solches n nicht existiert, dann setzen wir $\mathrm{Char}(F) = 0$.
2. Der *Primkörper* eines Körpers F ist der kleinste Teilkörper von F.

Bemerkung 9.2. Für die Charakteristik gilt: entweder $\mathrm{Char}(F) = p$ für eine Primzahl p, oder $\mathrm{Char}(F) = 0$. Wenn $\mathrm{Char}(F) = p$, dann ist der Primkörper $\mathbb{F}_p$, wenn $\mathrm{Char}(F) = 0$, dann ist der Primkörper $\mathbb{Q}$. ÜA.

§ 12 Algebraische Körpererweiterung

Definition 9.3.
Ein Körper K der ein Teilkörper F enthält heißt *Körpererweiterung* von F, bezeichnet mit K/F. Wir nennen F den *Grundkörper*.

Bemerkung 9.4. Ist K/F eine Körpererweiterung, dann ist K ein F-Vektorraum, wobei die Skalarmultiplikation $F \times K \to K$ die auf K definierte Multiplikation ist. ÜA.

Definition 9.5. Der *Grad (oder deg) einer Körpererweiterung* K/F, bezeichnet mit $[K : F]$, ist die Dimension von K als F-Vektorraum. Die Körpererweiterung heißt *endlich* falls $[K : F]$ endlich ist; sonst heißt die Körpererweiterung *unendlich* und wir schreiben $[K : F] = \infty$.

Beispiel 9.6.

1. Sei $F = \mathbb{F}_p$ und $K = \mathbb{F}_p(x) := \text{Quot}\ (\mathbb{F}_p[x])$. Dann ist $[K : F] = \infty$. ÜA.
2. $[\mathbb{C} : \mathbb{R}] = 2$: Jedes Element aus $\mathbb{C}$ lässt sich als Linearkombination von 1 und i darstellen und, wenn $a + bi = 0$ dann $a^2 + b^2 = (a + bi)(a - bi) = 0$; also $a = b = 0$. Somit bilden $1, i$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.
3. $[\mathbb{R} : \mathbb{Q}] = \infty$. Siehe ÜB.

Satz 9.7.
Seien F ein Körper und $p(x) \in F[x]$ ein irreduzibles Polynom. Dann existiert eine Körpererweiterung von F wo $p(x)$ eine Nullstelle besitzt.

Beweis:
Betrachte den Faktorring $\mathbb{K} := F[x]/ < p(x) >$. Da $p(x)$ irreduzibel ist und $F[x]$ ein Hauptidealring ist, ist das von $p(x)$ erzeugte Ideal ein maximales Ideal (Proposition 5.12 und Proposition 6.3). Daher ist $\mathbb{K}$ ein Körper (Proposition 3.1).

Sei $\varphi : F[x] \to \mathbb{K}$ die kanonische Projektion $a(x) \mapsto \overline{a(x)}$. Die Einschränkung $\varphi|F$ von φ auf F ist ein Körperhomomorphismus und daher ist sie injektiv (s. Korollar 2.7). Es folgt, dass F isomorph ist zu seinem Bild $\varphi(F) \subseteq \mathbb{K}$. Nun können wir F mit dem Teilkörper $\varphi(F)$ von $\mathbb{K}$ identifizieren. Somit ist F ein Teilkörper von $\mathbb{K}$, und die Einschränkung $\varphi|F$ ist nun die Identitätsabbildung Id. [1]

Sei $\varphi(x) = \overline{x}$ das Bild von x in $\mathbb{K}$. Es gilt $p(\overline{x}) = \overline{p(x)}$ (weil φ ein Homomorphismus ist mit $\varphi(a) = a$ für alle $a \in F$). Aber $p(x) \in < p(x) >$, also $0 = \overline{p(x)} = p(\overline{x})$. Dann ist $\overline{x} \in \mathbb{K}$ eine Nullstelle des Polynoms $p(x)$. □

Satz 9.8.
Sei $p(x) \in F[x]$ irreduzibel; $\deg p(x) = n, n \in \mathbb{N}$. Setze $\mathbb{K} := F[x]/ < p(x) >$. Es gilt $[\mathbb{K} : F] = n$.

Beweis:
Setze $\overline{x} := \theta$. Wir behaupten $O := \{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ ist eine F-Basis für $\mathbb{K}$.

- Sei $a(x) \in F[x]$. Schreibe $a(x) = q(x)p(x) + r(x)$ mit $r(x) = 0$ oder $\deg r(x) < n$.
  Also $a(x)+ < p(x) >= r(x)+ < p(x) >$,

  $$\begin{array}{lcl} \text{d. h.} & \overline{a(x)} & = & \overline{r(x)} \\ & \shortparallel & & \\ \text{d. h.} & a(\overline{x}) & = & r(\overline{x}) \end{array}$$

  Schreibe $r(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in F$, i.e. $\overline{a(x)} =: r(\theta)$, also $\mathbb{K} \ni \overline{a(x)} \in \text{span}\ O$.

- O ist linear unabhängig über F: Seien $b_0, \dots, b_{n-1} \in F$ mit $\sum b_i \theta^i = 0$.
  Setze $b(x) := \sum b_i x^i$. Es ist: $0 = b(\theta) = \overline{b(x)}$. Also $b(x) \in < p(x) >$ und $\deg b(x) < \deg p(x)$ und damit muss $b(x) = 0$ das Nullpolynom sein, i.e. $b_i = 0$ für alle $i = 0, \dots, n - 1$. □

Bemerkung 9.9.
$\mathbb{K} = \{a(\theta)\ ;\ a(x) \in F[x], a(x) = 0 \text{ oder } \deg a(x) < n\}$, versehen mit den Verknüpfungen:
$a(\theta) + b(\theta) = (a + b)(\theta)$ für alle $a(x), b(x) \in F[x]$ und $a(\theta)b(\theta) = r(\theta)$; wobei $r(x) \in F[x]$ der Rest ist in E.A.: $a(x)b(x) = q(x)p(x) + r(x)$, $\deg r(x) < n$.

[1] Dies ist subtil: was bedeutet F mit seinem Bild in $\varphi(F) \subseteq \mathbb{K}$ zu identifizieren? Für $a \in F$ können wir einfach jedes Element $\varphi(a)$ als a umbenennen. Dies können wir machen weil $\varphi|F$ injektiv ist: für alle $a, a' \in F$: gilt: $\varphi(a) = \varphi(a')$ genau dann, wenn $a = a'$.

Definition 9.10.

(1) Sei K/F eine Körpererweiterung, und $S \subseteq K$. **Notation:** Setze $F(S)$ = der kleinste Teilkörper von K, der $F \bigcup S$ enthält, d.h. $F(S) := \bigcap\{L \mid L \subseteq K$ Teilkörper $; L \supseteq F \bigcup S\}$. $F(S)$ heißt der *Körper der von S über F erzeugt ist.*

(2) **Notation:** Wenn $S = \{\alpha_1, \ldots, \alpha_n\}$ endlich ist, schreiben wir $L = F(\alpha_1, \ldots, \alpha_n)$. In diesem Fall sagen wir: L ist *endlich erzeugt über F.*

(3) Wenn $S = \{a\}$ heißt $L = F(a)$ eine *einfache Erweiterung* und a heißt ein *primitives Element* für die Körpererweiterung L/F.

Satz 9.11.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, $\alpha \in K$ eine Nullstelle von $p(x)$. Es ist: $F[x]/ < p(x) > \simeq F(\alpha)$.

Beweis: Setze $\mathbb{K} := F[x]/ < p(x) >$. Betrachte die Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{K} & \to & F(\alpha) \subseteq K \\ & a(x)+ < p(x) > & \mapsto & a(\alpha) \end{array}$$

- Das heißt $\varphi|F = Id|F$ (i.e. $\varphi(a) = a$ für alle $a \in F$) und $\varphi(a(\overline{x})) = a(\alpha)$ für alle $a(x) \in F[x]$. Insbesondere ist $\varphi(\overline{x}) = \alpha$.
- φ ist wohldefiniert: $a(x) \equiv b(x) \mod < p(x) > \Leftrightarrow a(x) - b(x) = p(x)q(x)$. Also $a(\alpha) - b(\alpha) = 0$ und damit $a(\alpha) = b(\alpha)$.
- $\varphi \neq 0$, also φ ist ein injektiver Ringhomomorphismus und damit definiert φ einen Isomorphismus $\varphi : F[x]/ < p(x) > \simeq im(\varphi)$. Nun ist $im(\varphi) \subseteq F(\alpha) \subseteq K$ ein Teilkörper von K und enthält $F \bigcup \{\alpha\}$. Somit ist $F(\alpha) \subseteq im(\varphi)$. Also $im(\varphi) = F(\alpha)$. □

Aus Satz 9.11 und Bemerkung 9.9 folgt

Korollar 9.12.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, $\deg p = n$ und $\alpha \in K$ eine Nullstelle von $p(x)$. Es ist $F(\alpha) = \{a(\alpha)\ ;\ a(x) \in F[x]; a(x) = 0$ oder $\deg a(x) < n\}$.

Korollar 9.13.
Sei K/F eine Körpererweiterung, $p(x) \in F[x]$ irreduzibel, und $\alpha, \beta \in K$ Nullstellen von $p(x)$. Es ist $F(\alpha) \simeq F(\beta)$.

Beweis: Aus Satz 9.11 folgt: $F(\alpha) \simeq F[x]/ < p(x) > \simeq F(\beta)$. □

Allgemeiner gilt:

Satz 9.14.
Seien K/F und K'/F' Körpererweiterungen, und $\varphi : F \xrightarrow{\sim} F'$ ein Isomorphismus. Sei $p(x) = \sum a_i x^i \in F[x]$ irreduzibel, und setze $p'(x) := \sum \varphi(a_i)x^i$. Dann ist $p'(x) \in F'[x]$ irreduzibel. Sei $\alpha \in K$ mit $p(\alpha) = 0$ und $\beta \in K'$ mit $p'(\beta) = 0$. Dann läßt sich φ zu einer Isomorphie $\varphi' : F(\alpha) \to F'(\beta)$ fortsetzen (i.e. $\varphi'|F = \varphi$), so dass $\varphi'(\alpha) = \beta$.

Beweis:

Wir betrachten also folgenden Ansatz und Fragestellung:

$$\begin{array}{ccc} F(\alpha) & \overset{?}{\dashrightarrow} & F'(\beta) \\ | & & | \\ F & \xrightarrow[\varphi]{\sim} & F' \end{array}$$

(1) $p'(x)$ ist irreduzibel, weil eine Faktorisierung $p'(x) = a'(x)b'(x)$ mit $\deg a'(x) \geq 1, \deg b'(x) \geq 1, a'(x), b'(x) \in F'[x]$ eine Faktorisierung (durch Anwendung von φ^{-1} auf Koeffizienten) $p(x) = a''(x)b''(x)$ von $p(x)$ in $F[x]$ induziert, mit $\deg(a''(x)) \geq 1, \deg(b''(x)) \geq 1; a''(x), b''(x) \in F[x]$.

(2) $F[x] \simeq F'[x]$ und $< p(x) > \simeq < p'(x) >$ (durch Anwendung von φ auf Koeffizienten). Also $F(\alpha) \simeq F[x]/ < p(x) > \simeq F'[x]/ < p'(x) > \simeq F(\beta)$. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript führen wir algebraische Erweiterungen ein, und untersuchen wir genau den Zusammenhang zwischen algebraische, endliche, und endlich erzeugte Erweiterungen.

Sei K/F stets eine Körpererweiterung.

Definition 10.1.

(1) $\alpha \in K$ ist *algebraisch über* F (alg/F), wenn es ein Polynom $0 \neq f(x) \in F[x]$ gibt mit $f(\alpha) = 0$.

(2) Wenn α nicht algebraisch über F ist, dann heißt α *transzendent* über F.

(3) Die Körpererweiterung K/F heißt *algebraisch*, falls für alle $\alpha \in K$: α ist algebraisch über F.

Beispiel 10.2.
Betrachte die Erweiterung $F(x)/F$. Hier ist $x \in F(x)$ transzendent über F , weil $f(x) = 0 \Leftrightarrow f = 0$ das Nullpolynom ist. ÜA.

Proposition 10.3.
Sei $\alpha \in K$ alg $/F$. Dann gibt ein eindeutiges normiertes irreduzibles Polynom $m_{\alpha,F}(x) \in F[x]$, so dass:

(i) $m_{\alpha,F}(\alpha) = 0$.

(ii) Ist $f(\alpha) = 0$ für ein $f \in F[x]$, dann teilt $m_{\alpha,F}(x)$ das Polynom $f(x)$ in $F[x]$.

Beweis:

- Setze $m(x) := m_{\alpha,F}(x) :=$ normiertes Polynom vom minimalem deg, so dass $m(\alpha) = 0$. Sei $f(x) \in F[x]$, schreibe $f(x) = q(x)m(x) + r(x), \deg r(x) < \deg m(x)$ oder $r(x) = 0$. Wir sehen $0 = f(\alpha) \Leftrightarrow r(\alpha) = 0$. Die Minimalität vom $\deg m(x)$ impliziert $r(x) = 0$, also $m(x)|f(x)$.
- Ist $m'(x)$ normiert vom minimalem deg mit $m'(\alpha) = 0$, dann gilt wie oben $m'(\alpha)|m(\alpha)$, aber auch $m(\alpha)|m'(\alpha), m(\alpha), m'(\alpha)$ normiert $\Rightarrow m'(x) = m(x)$. □

Definition 10.4.
$m_{\alpha,F}(x)$ heißt das *Minimal-Polynom* von α über F. Wir schreiben $m(x)$, wenn klar.

Bemerkung 10.5.
Im Skript 14. LA II (Definition 14.2) hatten wir das Minimal-Polynom von einem Operator T : Das Min.Pol.(T) in $F[x]$ ist der eindeutige normierte Erzeuger vom Annihilator-Ideal von T

$$\mathcal{A}_T := \{f \in F[x] | f(T) = 0\}.$$

Wir können analog $m_{\alpha,F}(x)$ definieren, ÜA.

Proposition 10.6.
Sei $\alpha \in K$ algebraisch über F. Es ist $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$.

Beweis:
Satz 9.11 impliziert $F(\alpha) \simeq F[x]/ < m_{\alpha,F}(x) >$, aus Satz 9.8 folgt $[F(\alpha) : F] = \deg m_{\alpha,F}(x)$. □

Terminologie:
$\deg \alpha/F := \deg m_{\alpha,F}(x) = \deg F(\alpha)/F$.

Der Beweis dieser Bemerkung ist eine ÜA:

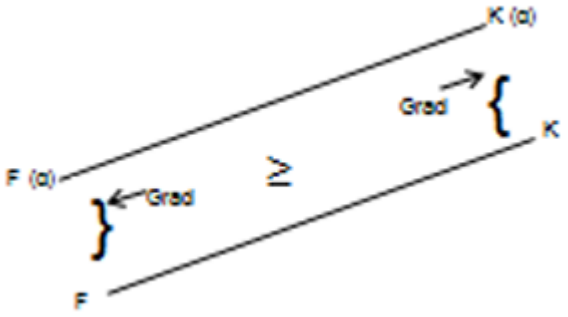
Bemerkung 10.7.
(1) $L \supseteq K \supseteq F, \alpha \in L,$ alg $/F \to \alpha$ alg $/K$ und es gilt

(2) $m_{\alpha,K}(x)$ teilt $m_{\alpha,F}(x)$ in $K[x]$, insbesondere

(3) $\deg m_{\alpha,K}(x) \leq \deg m_{\alpha,F}(x)$. Es gilt ferner

(4) $m_{\alpha,K}(x) = m_{\alpha,F}(x)$ genau dann, wenn $m_{\alpha,F}(x)$ irreduzibel bleibt in $K[x]$.
Wir haben aus (3):

(5) $[K(\alpha) : K] \leq [F(\alpha) : F]$



Wir zeigen nun die Umkehrung von Proposition 10.6.

Proposition 10.8.
Sei $\alpha \in K$, so dass $[F(\alpha) : F] < \infty$. Dann ist α algebraisch über F.

Beweis:
Sei $[F(\alpha) : F] = n$, dann sind $F(\alpha) \ni 1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig über F. Also existieren $b_i \in F$ *nicht alle gleich 0*, so dass $\sum_{i=0}^{n} b_i \alpha^i = 0$. Setze $f(x) := \sum b_i x^i \in F[x]; \not\equiv 0$. Dann gilt $f(\alpha) = 0; \alpha$ alg $/F$. □

Beispiel 10.9.
Die Erweiterung $F(x)/F$ ist endlich erzeugt (eigentlich ist sie eine einfache Erweiterung), aber $[F(x) : F] = \infty$ weil $x \in F(x)$ transzendent ist über F. Wir sehen also: K/F endlich erzeugt $\not\Rightarrow K/F$ endlich.

Korollar 10.10.
K/F ist endlich $\Rightarrow K/F$ algebraisch.

Beweis:
Sei $\alpha \in K$. Es ist $[F(\alpha) : F] \leq [K : F] < \infty$, also ist α algebraisch über F. □

Satz 10.11.
$F \subseteq K \subseteq L$. Es gilt $[L : F] = [L : K][K : F]$. (Also insbesondere ist L/F unendlich genau dann, wenn L/K oder K/F unendlich sind.)

Beweis:
Zunächst nehmen wir an: $[L : K] = m$ mit $\{\alpha_1, \ldots, \alpha_m\}$ Basis für L/K; $[K : F] = n$
mit $\{\beta_1, \ldots, \beta_n\}$ Basis für K/F. Ein Element λ aus L ist also aus der Form $\lambda = \sum_i a_i \alpha_i$
mit $a_i \in K$. $(*)$
Schreibe $a_i = \sum_j b_{ij}\beta_j$ mit $b_{ij} \in F$ $(**)$

$\rightsquigarrow$ Einsetzen von $(**)$ in $(*)$ ergibt $\lambda = \sum_{i,j} b_{ij}\alpha_i\beta_j$. $(***)$

Also ist span $_F\{\alpha_i\beta_j \mid i = 1, \ldots, m, j = 1, \ldots, n\} = L$. Wir zeigen, dass diese Menge auch F-linear unabhängig ist.
Sei also $\sum_{i,j} b_{ij}\alpha_i\beta_j = 0$ für $b_{ij} \in F$. $(\dagger)$
Setze $a_i := \sum_j b_{ij}\beta_j \in K$ und schreibe $(\dagger)$, also $\sum_i a_i\alpha_i = 0$. Nun ist α_i linear unabhängig über $K \Rightarrow a_i = 0$ für alle i, also $\sum_j b_{ij}\beta_j = 0$ für alle i.
Nun ist β_j linear unabhängig über $F \Rightarrow b_{ij} = 0$ für alle j. □

Wir haben gezeigt: $[L : F] = \infty \Rightarrow [L : K] = \infty$ oder $[K : F] = \infty$.
Sei nun $[K : F]$ unendlich, dann ist auch $[L : F]$ unendlich, weil K ein F-Unterraum von L ist.
Sei nun $[L : K] = \infty$, dann ist a fortiori $[L : F] = \infty$ ($\lambda_1, \ldots, \lambda_s$ sind K linear unabhängig $\rightarrow \lambda_1, \ldots, \lambda_s$ sind F-linear unabhängig).

Korollar 10.12.
Seien L/K und K/F Körpererweiterungen so dass L/F endlich ist. Es gilt $[K : F] | [L : F]$.

Wir haben bisher gezeigt, dass α algebraisch über F ist $\Leftrightarrow [F(\alpha) : F] < \infty$. Wir sind nun in der Lage dieses für $F(\alpha_1, \ldots, \alpha_n)$ zu verallgmeinern.

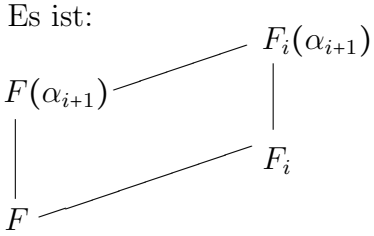
Satz 10.13.
K/F ist endlich $\Leftrightarrow$ K/F ist endlich erzeugt von alg $/F$-Elementen.

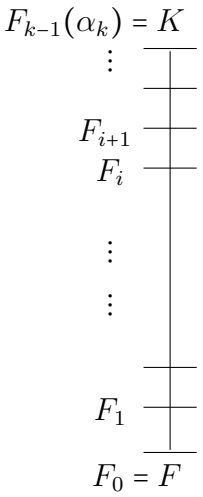
Beweis:

"$\Rightarrow$" Setze $[K : F] = n$. Sei $\{\alpha_1, \ldots, \alpha_n\}$ die F-Basis von K. Jedes α_i ist algebraisch über F. Außerdem ist $K = \text{span}_F\{\alpha_1, \ldots, \alpha_n\} \subseteq F(\alpha_1, \ldots, \alpha_n) \subseteq K$
und damit ist $K = F(\alpha_1, \ldots, \alpha_n)$.

"$\Leftarrow$" Wir bemerken vorab dass für $\alpha, \beta \in K$ gilt allgemein: $F(\alpha, \beta) = F(\alpha)(\beta)$ (folgt unmittelbar aus der Definition 9.10, ÜA). Sei $K = F(\alpha_1, \ldots, \alpha_k)$. Sei α_i algebraisch über F und $\deg \alpha_i = n_i$. Setze $F = F_0$ und $F_1 = F_0(\alpha_1)$. $F_{i+1} := F_i(\alpha_{i+1})$, so $K = F_{k-1}(\alpha_k)$.

Es ist:





Also $[F_{i+1} : F_i] \leq n_{i+1}$. Also (Satz 10.11) $[K : F] = [F_k : F_{k-1}] \cdots [F_1 : F_0] \leq n_1 \cdots n_k$ und damit ist K/F endlich. $\square$

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir zunächst wichtige Begriffe (Zerfällungskörper, normale Erweiterung, Kompositum) einführen und untersuchen. In Abschnitt 13 werden wir die Voraussetzungen erstellen, um dann algebraische Abschlüsse in Skript 12 aufzubauen.

Sei K/F stets eine Körpererweiterung.

Korollar 11.1.
Seien $\alpha, 0 \neq \beta \in K$ algebraisch über F, dann sind $\alpha \pm \beta\,, \alpha\beta\,, \alpha/\beta$ auch algebraisch über F.

Beweis:
Die Erweiterung $F(\alpha,\beta)/F$ ist endlich wegen Satz 10.13. Nun sind $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha,\beta)$. Aus Korollar 10.10 folgt nun unsere Behauptung. □

Korollar 11.2.
Die Menge $\tilde{F} := \{\alpha \in K \mid \alpha \text{ alg } /F\}$ ist ein Teilkörper von K welcher F enthält.

Definition 11.3.
Dieser Teilkörper $\tilde{F}$ heißt der *relative algebraische Abschluss von F in K.*

Beispiel 11.4.
(1) In der Erweiterung $\mathbb{C}/\mathbb{Q}$ ist $\tilde{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ alg } /\mathbb{Q}\}$ der *Körper der algebraischen Zahlen.*

(2) In der Erweiterung $\mathbb{R}/\mathbb{Q}$ ist $\tilde{\mathbb{Q}}^r := \{r \in \mathbb{R} \mid r \text{ alg } /\mathbb{Q}\}$ der *Körper der reellen algebraischen Zahlen.*

Es gilt $\tilde{\mathbb{Q}} \subsetneq \mathbb{C}$ und $\tilde{\mathbb{Q}}^r \subsetneq \mathbb{R}$ (z.B: $\pi, e \in \mathbb{R}\backslash\tilde{\mathbb{Q}}^r$). Eigentlich gilt es ferner: $[\tilde{\mathbb{Q}} : \mathbb{Q}] = [\tilde{\mathbb{Q}}^r : \mathbb{Q}] = \infty$, $|\tilde{\mathbb{Q}}| = |\tilde{\mathbb{Q}}^r| = \aleph_0$ und $|\mathbb{C} \setminus \tilde{\mathbb{Q}}| = |\mathbb{R} \setminus \tilde{\mathbb{Q}}^r| = 2^{\aleph_0}$. Siehe ÜB.

Satz 11.5.

L/K	und	K/F	$\Rightarrow$	L/F
alg		alg		alg

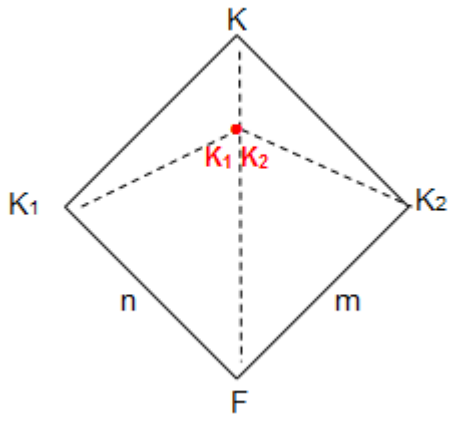
Beweis:
Sei $\alpha \in L$ und $0 \neq k(x) := \sum_{i=0}^{n} a_i x^i \in K[x]$ so dass $k(\alpha) = 0 \qquad (*)$.
Betrachte die folgende Körpererweiterungen:

- $F_1 := F(a_0, \ldots, a_n)\,, F_1 \subseteq K\,, a_i$ alg $/F$, also folgt aus Satz 10.13 dass $[F_1 : F] < \infty$.
- $F_1(\alpha) \subseteq L\,, \alpha$ alg $/F_1$ wegen $(*)$, also folgt aus Satz 10.13 dass $[F_1(\alpha) : F_1] < \infty$.
- Es folgt aus Satz 10.11 dass $[F_1(\alpha) : F] = [F_1(\alpha) : F_1][F_1 : F] < \infty$.

Insbesondere folgt nun aus Proposition 10.8 dass $F_1(\alpha)/F$ algebraisch ist, und damit ist α algebraisch über F. □

Definition 11.6.
Seien K/K_1 und K/K_2 Körpererweiterungen. Der Körper $K_1K_2 := K_1(K_2) = K_2(K_1) \subseteq K$ heißt *das Kompositum von K_1 und K_2 in K.*

Lemma 11.7.
Seien K/K_1 und K/K_2 sowie K_1/F und K_2/F Körpererweiterungen, so dass



$\{\alpha_1, \ldots, \alpha_n\}$ eine F-Basis von K_1 und $\{\beta_1, \ldots, \beta_m\}$ eine F-Basis von K_2 . Es gilt:
$\text{span}_F\{\alpha_i\beta_j / i, j\} = K_1K_2$.

Beweis:
Ohne Einschränkung $\alpha_1 = \beta_1 = 1$. Bemerke, dass $K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m)$. Nun ist $\text{span}_F\{\alpha_i\beta_j / i, j\} \subseteq K_1K_2$ ein **Teilkörper** von K welcher $F \cup \{\alpha_1, \ldots, \alpha_n\} \cup \{\beta_1, \ldots, \beta_m\}$ enthält (ÜA). Also gilt auch $\text{span}_F\{\alpha_i\beta_j / i, j\} \supseteq K_1K_2$. □

Korollar 11.8.
Seien $K/K_1, K/K_2$; $K_1/F, K_2/F$ die Körpererweiterungen wie in Lemma 11.7, setze $[K_1 : F] := n$, $[K_2 : F] := m$. Es gilt $[K_1K_2 : F] \leq nm$.
Ferner gilt: $[K_1K_2 : F] = mn$, wenn α_i linear unabhängig über K_2 bleiben (oder wenn β_j linear unabhängig über K_1 bleiben.)

Beweis:
Dass $[K_1K_2 : F] \leq nm$, folgt direkt aus dem Lemma 11.7. Wir nehmen an, dass $\alpha_1, \ldots, \alpha_n$ linear unabhängig über K_2 sind und wir zeigen, dass die Familie $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ linear unabhängig über F ist. Seien $(\nu_{ij})_{ij} \subseteq F$ so, dass $\sum_{i,j} \nu_{ij}\alpha_i\beta_j = 0$. Man kann diese Summe umschreiben: $\sum_{i=1}^{n} \alpha_i(\sum_{j=1}^{m} \nu_{ij}\beta_j) = 0$. Für alle $i \in \{1, \ldots, n\}$ ist $\sum_{j=1}^{m} \nu_{ij}\beta_j \in K_2$. Nach Annahme muss dann $\sum_{j=1}^{m} \nu_{ij}\beta_j = 0$ gelten für alle $i \in \{1, \ldots, n\}$. Weil $\beta_1, \ldots, \beta_m$ linear unabhängig über F sind, muss dann $\nu_{ij} = 0$ gelten für alle i, j.
(Analog kann man die zweite Aussage beweisen). □

Korollar 11.9.
Seien $[K_1 : F] = n, [K_2 : F] = m$ und ggT $(n, m) = 1$. Es gilt $[K_1K_2 : F] = mn$.

Beweis:
$$\left.\begin{array}{rcl} n & | & [K_1K_2 : F] \\ m & | & [K_1K_2 : F] \end{array}\right\} \Rightarrow kgV(n, m) \mid [K_1K_2 : F]$$

$kgV(n, m) = \frac{nm}{ggT(n,m)} = mn$. Also $mn \leq [K_1K_2 : F] \leq mn$. □

§ 13 Algebraischer Abschluss

Sei K/F stets eine Körpererweiterung.

Definition 11.10.
Sei $f \in F[x]\,, \deg(f) \geq 1$. Der Körper K ist ein *Zerfällungskörper von* f, wenn folgendes gilt:

1. f zerfällt vollständig in lineare Faktoren in $K[x]$, das heißt ist Produkt von linearen Faktoren in $K[x]$.
2. Für alle Körper L mit $F \subseteq L \subsetneq K$ zerfällt f in $L[x]$ **nicht**.

Allgemeiner können wir diesen Begriff für eine Menge von Polynomen erklären:

Bemerkung 11.11.
Sei $\mathcal{E} \subseteq F[x]$. Der Körper K ist ein *Zerfällungskörper von* $\mathcal{E}$ wenn folgendes gilt:

1. Jedes $f \in \mathcal{E}$ mit $\deg(f) \geq 1$ zerfällt vollständig in lineare Faktoren in $K[x]$
2. K wird von den Nullstellen der Polynome in $\mathcal{E}$ erzeugt, also
   $K = F(\{\alpha \in K \mid \exists f \in \mathcal{E} \text{ mit } f(\alpha) = 0\})$

Bemerkung 11.12.
Sei $f \in F[x]$, $\deg(f) \geq 1$. Dann ist K Zerfällungskörper von f genau dann, wenn K Zerfällungskörper von $\mathcal{E} := \{f\}$ ist.

Definition 11.13.
Die Erweiterung K/F ist *normal*, wenn K ein Zerfällungskörper einer Menge $\mathcal{E} \subseteq F[x]$ ist.

Satz 11.14.
Es gibt einen Zerfällungskörper K/F für $f(x)$ über F.

Beweis:
Per Induktion zeigen wir zunächst, dass es eine Körpererweiterung E/F gibt, in der $f(x)$ vollständig zerfällt.
Setze $n = \deg f(x)$. $n = 1, E = F\checkmark$ Induktionsanfang $n > 1$.
Sei $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ (sonst ist wieder $E = F$).
Sei $\alpha \in E_1/F$ eine Nullstelle von $p(x)$ (s. Satz 9.7), über E_1 haben wir also

$$(*) \qquad f(x) = (x - \alpha) f_1(x)$$

$f_1(x) \in E_1[x]; \deg f_1 \leq n - 1$.

Induktionsannahme für f_1 und E_1 ergibt eine E/E_1 und f_1 zerfällt vollständig in $E[x]$. Nun ist auch $\alpha \in E$. Also zerfällt f wie in $(*)$ vollständig über E.
Setze nun $K := \bigcap\{L/F \subseteq L \subseteq E; f \text{ zerfällt vollständig in } L[x]\}$ □

Proposition 11.15.
Sei $\deg f = n \geq 1$, und K/F ein Zerfällungskörper von f über F. Es gilt $[K : F] \leq n!$

Beweis:
Sei $\alpha_1 \in F_1/F$, α_1 ist Nullstelle von f. Dann ist $[F_1 : F] \leq n$ und $f(x) = (x - \alpha_1)f_1(x)$, $f_1(x) \in F[x]$, $\deg f_1 \leq n-1$. Wiederholung des Vorgangs ergibt: Sei $\alpha_2 \in F_2/F_1, \alpha_2$ ist Nullstelle von f_1. Dann ist $[F_2 : F_1] \leq n-1$, und damit $[F_2 : F] \leq n(n-1)$ (wegen Satz 10.11).
Wir verfahren so weiter (ÜA). □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Abschnitt 13 beenden; unser Endresultat ist Korollar 12.6 wo wir die Existenz und Eindeutigkeit für algebraische Abschluss etablieren.

In Satz 11.14 haben wir die Existenz vom Zerfällungskörper gezeigt, nun zeigen wir die Eindeutigkeit:

Satz 12.1.
Seien F und F' Körper und $\varphi : F \xrightarrow{\sim} F'$ eine Isomorphie, $f(x) \in F[x]$ mit $\deg f \geq 1$ und $\varphi(f) := f'(x) \in F'[x]$ das Bild von f (nach Anwendung von φ auf die f-Koeffiziente). Seien E Zerfällungskörper für f über F und E' ist Zerfällungskörper für f' über F'.
Dann läßt sich φ fortsetzen:

$$\begin{array}{ccc} E & \overset{\sigma}{\xrightarrow{\sim}} & E' \\ | & & | \\ F & \underset{\varphi}{\xrightarrow{\sim}} & F' \end{array}$$

Beweis:
Sei $\deg f := n$. Beweis per Induktion nach n. Es ist klar dass wenn f über F als Produkt von linearen Faktoren zerfällt, dann zerfällt ebenfalls f' über F' als Produkt von linearen Faktoren (ÜA). In diesem Fall $E = F$ und $E' = F'$ und wir setzen $\sigma = \varphi$.

Sei also $p(x)$ ein irreduzibler Faktor von $f(x)$ in $F[x]$ mit $\deg p \geq 2$ und $p' = \varphi(p)$ der entsprechende irreduzibler Faktor von $f'(x)$ in $F'[x]$ (s. Satz 9.14). Sei $\alpha \in E$ eine Nullstelle für $p(x)$ und $\beta \in E'$ eine Nullstelle für $p'(x)$. Setze $F_1 := F(\alpha)$ und $F_1' := F'(\beta)$.

Aus Satz 9.14. folgt, dass ein σ_1 existiert, so dass

$$\begin{array}{ccc} F_1 & \underset{\sigma_1}{\xrightarrow{\sim}} & F_1' \\ | & & | \\ F & \underset{\varphi}{\xrightarrow{\sim}} & F' \end{array}$$

Nun haben wir also den folgenden Ansatz:

$$\sigma_1 : F_1 \xrightarrow{\sim} F_1'$$

und $f(x) = (x-\alpha)f_1(x)$ über F_1, mit $\deg f_1 \leq n-1$. Bemerke dass E ein Zerfällungskörper von f_1 über F_1 ist: $E \supseteq F_1$ und E enthält alle Nullstellen von f_1; und für L mit $E \supsetneq L \supseteq F_1$, ist es unmöglich, dass L alle Nullstellen von f_1 enthält (sonst enthält L auch α und alle Nullstellen von f_1, also alle Nullstellen von f - Widerspricht Minimalität von E als ein Zerfällungskörper von f über F). Analog ist $f'(x) = (x-\beta)f_1'(x)$ über F_1', $\deg f_1' \leq n-1$ und E' ist ein Zerfällungskörper von f_1' über F_1'. Also haben wir nun den Ansatz f_1, F_1, σ_1 mit $\deg f_1 \leq n-1$ für die Induktion.

Die Induktionsannahme liefert ein σ, so dass

$$\begin{array}{ccc} E & \xrightarrow[\sigma]{\sim} & E' \\ | & & | \\ F_1 & \xrightarrow[\sigma_1]{\sim} & F_1' \end{array}$$

Also

$$\begin{array}{ccc} E & \xrightarrow[\sigma]{\sim} & E' \\ | & & | \\ F_1 & \xrightarrow[\sigma_1]{\sim} & F_1' \\ | & & | \\ F & \xrightarrow[\varphi]{\sim} & F' \end{array}$$

□

Korollar 12.2.
Ein Zerfällungskörper von $f \in F[x]$ über F ist bis Isomorphie auf F eindeutig.

Beweis:
Seien K und K' Zerfällungskörper von f über F. Wegen Satz 12.1 gilt:

mit $\sigma|F = Id$

$$\begin{array}{ccc} K & \xrightarrow[\sigma]{\sim} & K' \\ | & & | \\ F & \xrightarrow{Id} & F \end{array}$$

□

Definition 12.3.

(a) $\tilde{F}/F$ ist ein *algebraischer Abschluss* von F, falls
   (a) $\tilde{F}/F$ algebraisch ist;
   (b) jedes $f(x) \in F[x]$ mit $\deg f \geq 1$ zerfällt vollständig als Produkt von linearen Faktoren über $\tilde{F}$.

(b) K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[x]$ mit $\deg f \geq 1$ eine Nullstelle in K hat.

Bemerkung 12.4.
K ist algebraisch abgeschlossen $\Leftrightarrow$ jedes $f \in K[x]$ mit $\deg f \geq 1$ zerfällt vollständig in linearen Faktoren über $K \Leftrightarrow K = \tilde{K}$.

Proposition 12.5.
Sei $\tilde{F}$ ein algebraischer Abschluss von F. Dann ist $\tilde{F}$ algebraisch abgeschlossen.

Beweis:
Sei $f(x) \in \tilde{F}(x)$ $\deg f \geq 1$, α ist Nullstelle von $f(x)$ (in irgend einer Körpererweiterung $K/\tilde{F}$, s. Satz 9.7). Dann ist $\tilde{F}(\alpha)/\tilde{F}$ algebraisch und $\tilde{F}/F$ algebraisch. Also ist auch $\tilde{F}(\alpha)/F$ algebraisch (s. Satz 11.5) und damit ist auch α/F algebraisch.
Sei $m_{\alpha,F}$ das Minimalpolynom von α/F, dann zerfällt $m_{\alpha,F}$ in $\tilde{F}[x]$ und hat $(x-\alpha)$ als linearen Faktor. Es folgt $\alpha \in \tilde{F}$. □

Sei F ein beliebiger Körper. Wir zeigen nun:
Hauptsatz
Es gibt eine algebraische abgeschlossene Körpererweiterung von F.

Beweis:
Setze $F = K_0$. Wir definieren per Induktion nach $n \in \mathbb{N}_0$ eine ansteigende Folge

$$K_0 \subseteq \cdots \subseteq K_j \subseteq K_{j+1} \subseteq \cdots$$

von der Körpererweiterung, so dass jedes Polynom $f \in K_{j-1}[x]$ mit $\deg f \geq 1$ eine Nullstelle in K_j hat. Dann setzen wir $K := \bigcup K_j$. Dann ist K/F eine Körpererweiterung,und wenn $f(x) \in K[x]$ $(\deg f \geq 1)$, dann existiert ein j mit $f(x) \in K_j[x]$ und f hat eine Nullstelle in $K_{j+1} \subseteq K$. Also ist K algebraisch abgeschlossen.

Und nun zur Induktion:
Für $f(x) \in F[x](\deg f \geq 1)$ sei x_f eine neue Variable. Betrachte $F[\cdots, x_f, \cdots]$ (Polynomring in der Variablen x_f ; siehe ÜB) und das Ideal $I :=< \{f(x_f); f \in F[x]\} >$.

Behauptung:
I ist echt. Sonst ist

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})(*)$$

mit $g_i \in F[\cdots, x_f, \cdots]$. Schreibe $x_i := x_{f_i}$ für $i = 1, \ldots, n$ und seien $x_{n+1}, \ldots, x_m$ alle anderen Variablen, die unter den g_i's noch vorkommen. Also ist

$$1 = g_1(x_1, \ldots, x_m) f_1(x_1) + \cdots + g_n(x_1, \ldots, x_m) f_n(x_n)(*)$$

eine polynomiale Gleichung.
Sei F'/F eine Körpererweiterung mit $\alpha_i \in F'$, Nullstelle für $f_i(x)$. Durch Einsetzen von α_i für x_i mit $i = 1, \ldots, n$ und 0 für x_j mit $j = n-1, \ldots, m$ in $(*)$ muss es immer noch eine Gleichung ergeben, die nun im Körper F' gelten muss, das heißt $1 = 0$ in F' - Widerspruch.

I ist echt. Per ZL, sei $\mathcal{M}$ maximal. $\mathcal{M} \lhd F[\cdots, x_f, \cdots]$ und $I \subseteq \mathcal{M}$. Setze $K_1 := F[\cdots, x_f, \cdots]/\mathcal{M}$. K_1/K_0 und $f \in K_0[x]$ hat eine Nullstelle in K_1, weil $f(\overline{x_f}) = \overline{f(x_f)} = 0$ (da $f(x_f) \in I$).
Wiederhole mit K_j/K_{j-1} und setze $K = \bigcup K_j$ wie schon erwähnt. □

Korollar 12.6.
Existenz:: Sei K algebraisch abgeschlossen und $F \subseteq K$. Dann ist der relative algebraische Abschluss von F in K ein algebraischer Abschluss von F.
Eindeutigkeit: (siehe ÜB)
Ein algebraischer Abschluss von F ist bis auf Isomorphie eindeutig.

Beweis:
Per Definition ist $\tilde{F}/F$ algebraisch. Sei $f(x) \in F[x]$ $(\deg f \geq 1)$, da K algebraisch abgeschlossen ist, $K[x] \ni f(x)$ zerfällt vollständig in lineare Faktoren $(x-\alpha)$ in $K[x]$. Aber α ist algebraisch über F und $\alpha \in K$, also $\alpha \in \tilde{F}$. Also zerfällt $f(x)$ in $\tilde{F}[x]$. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Kapitel 2 beenden. Im Abschnitt 14 werden wir LA II Skript 4 ergänzen, indem wir die Vielfachheit der Nullstellen in einem Grundkörper F ($Char(F) = 0$ oder $Char(F) = p$) untersuchen.

§14: Separable und inseparable Körpererweiterung

Definition 13.1.
Sei $f(x) \in F[x]$, mit $f(x) = a_n x^n + \cdots + a_0$, $\deg f \geq 1$, und sei K/F ein Zerfällungskörper für f. Dann ist

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

in $K[x]$; mit $n_i \geq 1$, $\alpha_i \neq \alpha_j$ für $i \neq j$.

- n_i ist die *Vielfachheit* der Nullstelle α_i.
- α_i ist eine *mehrfache* Nullstelle, wenn $n_i > 1$, sonst ist
- α_i eine *einfache* Nullstelle.

Definition 13.2. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$.
(1) f ist *separabel*, wenn es nur einfache Nullstellen hat.
(2) f nicht separabel heißt *inseparabel*.

Definition 13.3. Sei $f(x) = a_n x^n + \cdots + a_0 \in F[x]$, die *Ableitung* Df von f ist
$Df(x) = D(a_n x^n + \cdots + a_0) = n a_n x^{n-1} + \cdots + a_1 \in F[x]$.
$D : F[x] \to F[x]$ ist *Ableitungsoperator* und erfüllt die Produktregel

$$Dfg = gDf + fDg.$$

Bemerkung 13.4.
Sei $f(x) \in F[x]$ mit $\deg f = n \geq 1$.

1. $Df = 0$ oder $\deg Df < \deg f$ gilt immer.
2. Sei Char $F = 0$, dann ist $Df \neq 0$, weil zum Beispiel $na_n \neq 0$, für den Hauptkoeffizient $a_n \neq 0$ von f.
3. Sei p eine Primzahl und Char $F = p$. Betrachte $f(x) = x^p \in F[x]$. Dann ist $\deg f(x) > 1$, jedoch ist $Df(x) = px^{p-1} = 0$.

Proposition 13.5.
Sei $f(x) \in F[x]$ mit $\deg f \geq 1$. Eine Nullstelle α für $f(x)$ ist eine mehrfache Nullstelle genau dann, wenn α auch eine Nullstelle für $Df(x)$ ist. Das heißt,

$$\{x; x \text{ ist eine mehrfache Nullstelle von } f\} = \{x; x \text{ ist eine gemeinsame Nullstelle von } f \text{ und } Df\}.$$

Beweis:

"⇒" Sei α eine mehrfache Nullstelle. Schreibe $f(x) = (x-\alpha)^n g(x)$ mit $n \geq 2$.
Berechne $Df(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n Dg(x)$; $n-1 \geq 1 \Rightarrow \alpha$ ist Nullstelle von $Df(x)$.

"⇐" Sei α eine gemeinsame Nullstelle von $f(x)$ und $Df(x)$.
Schreibe $f(x) = (x-\alpha)h(x)$. $(*)$
Also ist $Df(x) = h(x) + (x-\alpha)Dh(x)$. Beim Einsetzen von α für x, ergibt das $h(\alpha) = 0$.
Zurück in $(*)$ ergibt es $f(x) = (x-\alpha)^2 h_1(x)$. □

Bemerkung 13.6. Sei $f(x) \in F[x]$ mit $\deg f \geq 1$; α eine Nullstelle, und $m_{\alpha,F} \in F[x]$ das minimal Polynom. Dann ist α auch Nullstelle von $Df(x) \Leftrightarrow m_{\alpha,F} \,/\, Df(x)$.

Lemma 13.7.
Die gemeinsamen Nullstellen von f und Df sind die Nullstellen von ggT (f, Df).

Beweis:

"⇐" α ist Nullstelle von ggT $(f, Df) \to \alpha$ ist Nullstelle von f und Df. Ist klar, ÜA.

"⇒" Sei α eine Nullstelle von f und Df. Da $m_{\alpha,F} \,/\, f$ und $m_{\alpha,F} \,/\, Df$, $m_{\alpha,F} /$ ggT (f, Df) auch.
Da α Nullstelle von $m_{\alpha,F}$ ist, folgt nun α ist Nullstelle von ggT (f, Df). □

Korollar 13.8.
Sei $f \in F[x]$ mit $\deg f \geq 1$ ein normiertes Polynom. Dann ist f separabel genau dann, wenn ggT $(f, Df) = 1$.

Beweis:

"⇐" Folgt aus Proposition 13.5 und Lemma 13.7.

"⇒" f separabel $\Rightarrow$ f hat keine gemeinsame Nullstelle mit Df (s. Proposition 13.5)
$\Rightarrow$ ggT $(f, Df) = 1$ (ÜA). □

Korollar 13.9.
Sei $f(x)$ mit $\deg f \geq 1$ ein irreduzibles Polynom. Es gilt: f ist inseparabel genau dann, wenn $Df = 0$.

Beweis:
α ist eine mehrfache Nullstelle von $f \Leftrightarrow m_{\alpha,F}$ ist gT von f und Df (s. Bemerkung 13.6). Nun f irreduzibel $\Rightarrow \deg m_{\alpha,F} = \deg f$. Also $m_{\alpha,F} \,/\, Df \Leftrightarrow Df = 0$ (s. Bemerkung 13.4 (1)). □

Beispiel 13.10.

(1) Sei $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.
Berechne $Df(x) = p^n x^{p^n-1} - 1 = -1$.
Df hat gar keine Nullstelle, also ist f separabel.

(2) Sei F so dass Char $F = 0$ oder Char $F := p \nmid n$. Sei $f(x) = x^n - 1$, berechne $Df(x) = nx^{n-1}$.
Dann ist $Df \neq 0$ und hat 0 als einzige Nullstelle, 0 ist aber keine Nullstelle von f, also ist f separabel und die Gleichung $x^n - 1 = 0$ hat n paarweise verschiedene Nullstellen. Diese Nullstellen heißen die $n$te *Einheitswurzel*.

(3) Sei nun F so dass Char $F = p | n$. Für $f(x) = x^n - 1$, $Df(x) = nx^{n-1} = 0 \Rightarrow f$ ist inseparabel.

Korollar 13.11.
Sei Char $F = 0$, und $f \in F[x]$ mit $\deg f \geq 1$.

1. Wenn f irreduzibel, dann ist f separable.
2. Allgemeiner gilt: $f(x)$ ist separabel genau dann, wenn die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

Beweis:

1. $f \neq 0 \Rightarrow Df \neq 0$ (weil Char $F = 0$).
2. "$\Leftarrow$" Wegen Eindeutigkeit des minimal Polynoms, können verschiedene irreduzible, normierte Polynome in $F[x]$ keine gemeinsame Nullstelle in K haben (ÜA). In der Primfaktorisierung
   $$f = c\prod_{i=1}^{k} p_i(x) \qquad p_i \neq p_j$$
   haben außerdem keiner der Faktoren eine mehrfache Nullstelle (folgt aus 1.). Also hat f keine mehrfache Nullstelle, f ist separabel.

"$\Rightarrow$": Analog (ÜA). □

Beispiel 13.12.
$f = x^2 - t \in \mathbb{F}_2(t)[x]$. f ist irreduzibel, weil $\sqrt{t} \notin \mathbb{F}_2(t)$ (ÜA).
$Df = 0$, also ist f irreduzibel, aber inseparabel.

Bemerkung 13.13.
Sei Char $F = p > 0$; $g \in F[x]$, $\deg g \geq 1$. Setze $f(x) := g(x^p)$, schreibe

$$f(x) = \gamma_m(x^p)^m + \cdots + \gamma_1 x^p + \gamma_0 \qquad (*) .$$

Dann ist $Df(x) = 0$ und f ist inseparabel.
Umgekehrt: $f(x) \in F[x](\deg f \geq 1)$ mit $Df = 0$ muss die Gestalt $(*)$ haben, i.e. $f(x) = g(x^p)$ mit $g(x) \in F[x]$. (ÜA).

Proposition 13.14. Sei Char $F = p > 0$.

Es gelten $(a+b)^p = a^p + b^p$ für alle $a, b \in F$

$(ab)^p = a^p b^p$

und $\varphi : F \to F$, $a \mapsto a^p$

ist ein injektiver Körper-Homomorphismus (Frobenius).

Beweis: (ÜB).

Korollar 13.15.
$\mathbb{F}$ ist endlich $\Rightarrow \varphi : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$
ist auch surjektiv, also ein Automorphismus. Das heißt $\mathbb{F} = \mathbb{F}^p := \{a^p; a \in \mathbb{F}\}$.

Beweis:
$\mathbb{F}$ ist endlich, also endlich dimensional über den Primkörper $\mathbb{F}_p$ und kann also nicht isomorph sein zu einem echten Unterraum (vgl. LA I Skript 13). □

Korollar 13.11. gilt also auch für endliche Körper.

Proposition 13.16. Sei $\mathbb{F}$ ein endlicher Körper.

1. Jedes irreduzible Polynom $f \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel.
2. Ein Polynom $f(x) \in \mathbb{F}[x]\,(\deg f \geq 1)$ ist separabel $\Leftrightarrow$ die Primfaktorisierung von f in $F[x]$ diese Gestalt hat:

   $f = c\prod_{i=1}^{k} p_i(x)$; $0 \neq c \in F$, $p_i \in F[x]$ sind irreduzibel und normiert, **und** $p_i \neq p_j$ für $i \neq j$.

Beweis:
(1) Sei Char $\mathbb{F} := p > 0$, $f \in \mathbb{F}[x](\deg f \geq 1)$, f irreduzibel.

- f inseparabel $\Leftrightarrow Df = 0 \Leftrightarrow f(x) = g(x^p)$. Berechne:

$$\begin{aligned} f(x) = g(x^p) &= a_m(x^p)^m &+\cdots+ &\quad a_1x^p + a_0 \\ &= b_m^p(x^m)^p &+\cdots+ &\quad b_1^p x^p + b_0^p \\ &= (b_m x^m)^p &+\cdots+ &\quad (b_1 x)^p + b_0^p \\ &= (b_m x^m &+\cdots+ &\quad b_1 x + b_0)^p \end{aligned}$$

Widerspruch.
(2) Analog zum Beweis vom Korollar 13.11. (ÜA). □

Bemerkung 13.17.
Im Beweis von Proposition 13.16 haben wir die wichtige Eingenschaft $\mathbb{F}^p = \mathbb{F}$ benutzt (s.Korollar 13.15).

Definition 13.18.
Ein Körper F heißt *perfekt*, falls Char $F = 0$ oder Char $F = p > 0$ und $F = F^p$.

Bemerkung 13.19.
Proposition 13.16. gilt allgemeiner für F perfekt (anstatt $\mathbb{F}$ endlich).

Beweis: (ÜB).

GESAMTSKRIPT

zur Vorlesung ALGEBRA I

Kapitel III

Prof. Dr. Salma Kuhlmann

Wintersemester 2020 - 2021

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

Prof. Dr. Salma Kuhlmann

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

Prof. Dr. Salma Kuhlmann

Kapitel 3

GRUPPEN

In LA I und II haben wir schon Gruppen studiert. Insbesondere haben wir die symmetrische und alternierende Gruppen S_n in Zusammenhang mit Determinanten kennengelernt. In diesem Kapitel, setzen wir das Studium der Gruppentheorie fort, mit Schwerpunkt endliche Gruppen. Die Gruppentheorie die wir entfalten ist für die Grundlagen der Galoistheorie in Kapitel 4 unerlässig. Wir fangen damit an in diesem Skript und studieren Zyklische Gruppen.

§15: Zyklische Gruppen

Definition 14.1.
Sei G eine Gruppe. Eine Untermenge $H \subseteq G$ ist eine *Untergruppe*, oder *Teilgruppe*, falls H (versehen mit der Verknüpfung von G) eine Gruppe ist, das heißt:
$H \neq \varnothing$; und $\forall x, y \in G : x, y \in H \Rightarrow xy \in H$ und $x^{-1} \in H$.

Notation: Sei G eine gruppe, $x \in G$.

1. $< x >:= \{x^k \mid k \in \mathbb{Z}\}$ (additiv geschrieben $< x >:= \{kx \mid k \in \mathbb{Z}\}$) bezeichnet die Untergruppe die von x erzeugt ist.
2. $|G| := \begin{cases} \text{Anzahl} & \text{der Elemente in } G, \text{ falls } G \text{ endlich} \\ \infty & \text{sonst} \end{cases}$

Definition 14.2.

Sei G eine Gruppe und $x \in G$. Die *Ordnung von x*, die wir mit $|x|$ bezeichnen, ist so definiert:

$$|x| := \begin{cases} \text{kleinste } n \in \mathbb{N} \text{ mit } x^n = 1 \text{ falls vorhanden} \\ \infty \qquad \text{sonst} \end{cases}$$

Proposition 14.3.
Sei G eine Gruppe, $x \in G$. Es gilt $|x| = |< x >|$.

Beweis:

1. Sei $n \in \mathbb{N}$, und $|x| = n$. Wir behaupten dass $< x >= \{x^i ; i = 0, \ldots, n-1\}$ (und damit ist $|< x >| = n$). Wenn $x^i = x^j$ mit $0 \leq i < j < n$, dann $x^{j-i} = 1$ mit $0 < j - i < n$. Widerspruch. Sei nun $k \in \mathbb{Z}$ und $x^k \in < x >$; schreibe $k = qn + r$ mit $0 \leq r < n$. Berechne $x^k = x^{nq+r} = (x^n)^q x^r = x^r$.
   Analog zeigt man dass wenn $|< x >| = n$, dann ist $|x| = n$ (ÜA).

2. Sei nun $|x| = \infty$. Wir behaupten dass $x^i \neq x^j$ für alle $i, j \in \mathbb{Z}$ mit $i \neq j$ (und damit ist $|< x >| = \infty$): wenn $x^i = x^j$ mit $i < j \in \mathbb{Z}$, dann ist $x^{j-i} = 1$, also $|x| \leq j - i$. Widerspruch.
   Analog zeigt man dass wenn $|< x >| = \infty$, dann ist $|x| = \infty$ (ÜA).

□

Proposition 14.4.
Sei G eine Gruppe, $x \in G$ und $m, n \in \mathbb{Z}$, setze $d := \text{ggT}(m, n)$. Es gilt:

$$x^n = 1 \text{ und } x^m = 1 \Rightarrow x^d = 1 .$$

Insbesondere gilt für $m \in \mathbb{Z} : x^m = 1 \Rightarrow |x| \,|\, m$.

Beweis:
• Setze $d = mr + ns$. Berechne $x^d = (x^m)^r (x^n)^s = 1$.
• Sei nun $x^m = 1$. Setze $|x| = n$. Schreibe $m = qn+r$ mit $0 \leq r < n$. Berechne $x^m = (x^n)^q x^r \Rightarrow x^r = 1$. Widerspruch. Also $r = 0$. □

Definition 14.5.

G ist *zykisch*, wenn ein $x \in G$ existiert mit $G =< x >$, in diesem Fall ist x ein *Erzeuger* der Gruppe G.

Bemerkung 14.6.
Eine zyklische Gruppe ist abelsch. (ÜA)

Definition 14.7.
(*i*) Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ ist ein *Gruppenhomomorphismus*, wenn $\varphi(xy) = \varphi(x)\varphi(y)$ ist für alle $x, y \in G$.
(*ii*) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

Proposition 14.8.
Zyklische Gruppen derselben Ordnung sind isomorph.

Beweis:
(1) Sei $|G| = |H| = n$, $G =< x >$ und $H =< y >$. Betrachte die Abbildung:

$$\begin{array}{rccc} \varphi : & G & \to & H \\ & x^k & \mapsto & y^k \end{array}$$

• φ ist wohldefiniert, weil $x^r = x^s \Rightarrow x^{r-s} = 1 \Rightarrow n | r - s \Rightarrow nt = (r - s)$
$\Rightarrow y^{(r-s)} = (y^n)^t = 1 \Rightarrow y^r y^{-s} = 1 \Rightarrow y^r = y^s$.

• Es ist klar, dass φ ein Homomorphismus und auch surjektiv ist. Da beide Gruppen die gleiche Ordnung haben und endlich sind, folgt das φ injektiv ist (ÜA).

(2) Sei nun $|G| = |H| = \infty$.

$$\begin{array}{rccc} \varphi: & G & \to & H \\ & x^k & \mapsto & y^k \end{array}$$

ist ein surjektiver Homomorphismus und ferner injektiv, weil $x^i \neq x^j \Leftrightarrow i \neq j \Leftrightarrow y^i \neq y^j$. □

Beispiel 14.9.

(1) $|G| = n$ und G ist zyklisch $\Rightarrow G \simeq \mathbb{Z}_n$

(2) $|G| = \infty$ und G ist zyklisch $\Rightarrow G \simeq \mathbb{Z}$

Die folgende Proposition wird im Übungsblatt bearbeitet:

Proposition 14.10. Sei G eine Gruppe mit $x \in G$ und $j \in \mathbb{Z}$ mit $j \neq 0$. Es gelten

(1) $|x| = \infty \Rightarrow |x^j| = \infty$

(2) $|x| = n < \infty \Rightarrow |x^j| = \frac{n}{ggT(n,j)}$

(3) $|x| = n < \infty$ und $j|n \Rightarrow |x^j| = \frac{n}{|j|}$.

Proposition 14.11.
Sei $H = < x >$ und $j \in \mathbb{N}$.

(1) $|x| = \infty$, dann ist x^j Erzeuger von H genau dann, wenn $j = \pm 1$

(2) $|x| = n < \infty$, dann ist x^j Erzeuger von H genau dann, wenn ggT $(j, n) = 1$.

Beweis:

(1) ÜA.

(2) x^j Erzeuger $\Leftrightarrow |H| = |x^j|$. Also $\Leftrightarrow |x^j| = |x| \Leftrightarrow \frac{n}{ggT(j,n)} = n \Leftrightarrow ggT(j, n) = 1$. □

Korollar 14.12.
Sei H zyklisch mit $|H| = n$; dann ist die Anzahl der Erzeuger von $H = \phi(n)$ (Euler).

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

Prof. Dr. Salma Kuhlmann

In diesem skript werden wir Abschnitt 15 beenden, indem wir die zyklische Untergruppen studieren. Im Abschnitt 16 werden wir Homomorphismen und Faktorgruppen untersuchen, dabei werden wir normale Untergruppen kennenlernen.

Notation: Seien K, H und G stets Gruppen. Wir schreiben $K \leq H$ für: K ist eine Untergruppe von H.

Satz 15.1.
Sei $H =< x >$ zyklisch

(1) Sei $K \leq H$, dann ist K zyklisch.

(2) Wenn $|H| = \infty$, dann sind $< x^j > \neq < x^i >$ für $i \neq j$ und $\{< x^i > ; \, i \in \mathbb{N}_0\}$ ist die Menge aller Teilgruppen von H.

(3) Wenn $|H| = n$ und $a \in \mathbb{N}$ mit $a \,|\, n$, dann gibt es eine eindeutige Teilgruppe der Ordnung a, nämlich $< x^{n/a} >$. Die Menge aller nicht-trivialen Teilgruppen von H ist $\{< x^d >; d \in \mathbb{N}, d|n\}$.

Beweis:

(1) $K = \{1\}$ ist zyklisch, also ohne Einschränkung $K \neq \{1\}$.
Sei $k \in \mathbb{N}$ die kleinste, so dass $x^k \in K$. Also ist $< x^k > \leq K$.
Sei $x^a \in K; DA \Rightarrow a = qk + r$ mit $0 \leq r < k$ und $x^r = x^a x^{-qk} \in K$.
Da k minimal gewählt ist, muss $r = 0$ sein. Also $a = qk$ und $x^a = (x^k)^q \in < x^k >$.
Also $K \leq < x^k >$.

(2) ÜA.

(3) Sei $d := \frac{n}{a}$, also $d|n$ und $|x^d| = \frac{n}{ggT(n,d)} = n/d = n/(n/a) = a$. Somit ist $| < x^d > | = a$.
Eindeutigkeit: Sei $K \leq H$ mit $|K| = a$ und $b \in \mathbb{N}$ kleinste, so dass $K = < x^b >$. Wir berechnen $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{ggT(n,b)}$. Daraus folgt $d = ggT(n, b)$, insbesondere $d|b$. Also $x^b \in < x^d >$ und $K = < x^b > \leq < x^d >$.
Da aber $|K| = a = | < x^d > |$, folgt nun $K = < x^d >$. □

§16: Faktorgruppen

Proposition 15.2.
Sei $\mathcal{A}$ eine nichtleere Menge von Teilgruppen von H, dann ist $\bigcap \mathcal{A}$ auch eine Teilgruppe.

Beweis:
Setze $K := \bigcap \mathcal{A}; a, b \in K \Rightarrow ab^{-1} \in A$, für alle $A \in \mathcal{A}$ (weil $A \leq H$), also $ab^{-1} \in K$ und damit $K \leq H$. □

Definition 15.3.
Sei $S \subseteq H$ eine Untermenge; $\mathcal{A} := \{K \leq H; S \subseteq K\}$.
Definiere $< S >= \bigcap \mathcal{A}$. Dann ist $< S >$ die (für die Inklusion) kleinste Teilgruppe von H, die S enthält. $< S >$ heißt die *Teilgruppe, die von S erzeugt ist.*
Konvention: $< \varnothing >= \{1\}$
Notation: $S = \{a_1, \ldots, a_n\}; < S >=< a_1, \ldots, a_n >$ (wenn S endlich ist).

Proposition 15.4.
Sei $S \neq \varnothing$. Dann ist $< S >= \{a_1^{\varepsilon_1} \ldots a_n^{\varepsilon_n}; n \in \mathbb{N}; a_i \in S; \varepsilon_i = \pm 1\}$.

Beweis:
Diese Menge ist eine Teilgruppe (ÜA). Sie enthält S und muss in jeder Teilgruppe, die S enthält enthalten sein. □

Der Beweis dieser Proposition ist analog wie für Ringhomomorphismen und wird als ÜA überlassen:

Proposition 15.5.
Sei $\varphi : G \to H$ ein Homomorphismus. Es gelten
(1) $\varphi(1) = 1$
(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$
(3) $\varphi(g^n) = \varphi(g)^n$ für alle $n \in \mathbb{Z}$
(4) $\ker \varphi := \{g \in G; \varphi(g) = 1\} \leq G$
(5) $\text{im } \varphi := \{h \in H; \exists g \in G : \varphi(g) = h\} \leq H$

Wir wollen Faktorengruppen definieren.

Definition 15.6.
Sei $H \leq G$ und $g \in G$. Dann ist $gH := \{gh \mid h \in H\}$ ist die *linke Nebenklasse von g bezüglich H* und $Hg := \{hg \mid h \in H\}$ ist die *rechte Nebenklasse von g bezüglich H.*
Additive Notation: $g + H$ und $H + g$

Proposition 15.7.
Sei $H \leq G$. Es gelten:

(1) Die Menge der linken Nebenklassen bilden eine Partition von G i.e. $G = \bigcup_{g \in G} gH$ und $uH \cap vH \neq \varnothing \Rightarrow uH = vH$.
(2) Für alle $u, v \in G : uH = vH \Leftrightarrow v^{-1}u \in H$.

Beweis:
(1) $1 \in H$, also $g \in gH$ für alle $g \in G$. Also $G = \bigcup gH$. Sei $uH \cap vH \neq \varnothing$. Sei $x \in uH, x \in vH$, also $x = uh_1 = vh_2$ für geeignete $h_1, h_2 \in H$. Also $u = v \underbrace{h_2 h_1^{-1}}_{\in H}$.
Sei $t \in H$. Es gilt also $ut = v(h_2 h_1^{-1})t = v(h_2 h_1^{-1} t) \in vH$, somit $uH \subseteq vH$.
Analog: $uH \supseteq vH$.
(2) $uH = vH$ genau dann, wenn $u \in vH$ genau dann, wenn $u = vh$ für ein $h \in H$ genau dann, wenn $v^{-1}u \in H$. □

Proposition 15.8.
Sei $N \leq G$. Die Verknüpfung

$$(uN)(vN) := (uv)N$$

ist wohldefiniert genau dann, wenn

(*) $$gng^{-1} \in N \text{ für alle } g \in G; \text{ für alle } n \in N$$

Beweis:
"⇒" Wohldefiniert →

$$\left.\begin{array}{l} u, u_1 \in uN \\ v, v_1 \in vN \end{array}\right\} \Rightarrow (uv)N = (u_1v_1)N$$

Sei $g \in G, n \in N$, dann setze $u = 1, v = g^{-1}, u_1 = n, v_1 = g^{-1} \Rightarrow 1g^{-1}N = ng^{-1}N$ i.e. $g^{-1}N = ng^{-1}N$.

Nun: $ng^{-1} \in ng^{-1}N$, also $ng^{-1} \in g^{-1}N$. Also $ng^{-1} = g^{-1}n_1$ für geeignetes $n_1 \in N$. Also $gng^{-1} = n_1 \in N$.

"⇐" Sei $u, u_1 \in uN, v, v_1 \in vN$. Zu zeigen: $(uv)N = (u_1v_1)N$.
Schreibe $u_1 = un, v_1 = vm; n, m \in N$. Wir zeigen: $u_1v_1 \in (uv)N$.
Wir berechnen: $u_1v_1 = (un)(vm) = u(vv^{-1})nvm = uv(\underbrace{v^{-1}nv}_{:=n_1 \in N})m = uvn_1m = uv(\underbrace{n_1m}_{\in N})$ □

Zusatz zu Proposition 15.8.
Wenn wohldefiniert, dann definiert die Verknüpfung $(uN)(vN) := (uv)N$ eine Gruppenoperation auf die Menge der linken Nebenklassen. (ÜA).

Definition 15.9.
1. Sei $N \leq G$. N ist *normal*, falls $(*)$ in Proposition 15.8. gilt. Wir schreiben dafür: $N \trianglelefteq G$.
2. Für $N \trianglelefteq G$ bezeichnen wir G/N *die Gruppe der linken Nebenklassen* .

Beispiel:
Sei φ ein Homomorphismus, $N := \ker\varphi$ ist normal, weil

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = 1\,.$$

Also $gng^{-1} \in N$ für alle $g \in G$ und $n \in N$.

Die Umkehrung gilt auch (ÜA):

Proposition 15.10.
Für $N \trianglelefteq G$ ist die kanonische Projektion $\begin{array}{rccc} \varphi: & G & \longrightarrow & G/N \\ & g & \mapsto & gN \end{array}$
ein surjektiver Gruppenhomomorphismus mit $\ker\varphi = N$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript wollen wir die Menge der Nebenklassen, normale Teilgruppen, sowie Faktorgruppen weiter untersuchen. Im Abschnitt 17 werden wir zunächst die Anzahl der Nebenklassen allgemein berechnen; insbesondere bestimmen wir die Kardinalität einer Faktorgruppe. Im Abschnitt 18 werden wir diesbezüglich den ersten von insgesamt vier Isomorphiesätze studieren.

§17: Satz von Lagrange

Definition 16.1. Der *Index* einer Teilgruppe H in einer Gruppe G, bezeichnet mit $[G : H]$, ist die Anzahl der Linksnebenklassen von H in G
($[G : H]$ ist entweder eine natürliche Zahl oder unendlich).

Satz 16.2 (Lagrange)**.** Seien G eine endliche Gruppe und H eine Teilgruppe von G. Dann:

1. $|H|$ teilt $|G|$
2. Es gilt $[G : H] = \frac{|G|}{|H|}$.
3. Insbesondere für $H \trianglelefteq G$ ist $|G/H| = \frac{|G|}{|H|}$.

Beweis. Die Menge der linken Nebenklassen bilden eine Partition von G (Proposition 15.7). Da G endlich ist, ist also $n := [G : H]$ eine natürliche Zahl und es existieren $g_1, \ldots, g_n \in G$ mit

- $G = \bigcup_{i=1}^{n} g_i H$
- für alle $1 \leq i < j \leq n$ gilt $g_i H \cap g_j H = \varnothing$.

Es genügt also zu zeigen, dass jede Nebenklasse von H in G Kardinalität $|H|$ hat.
Sei also $g \in G$. Die Abbildung

$$\phi_g : H \to gH; \quad h \mapsto gh$$

ist surjektiv, nach Definition. Sie ist auch injektiv, denn, wenn für $h_1, h_2 \in H$ gilt

$$gh_1 = \phi_g(h_1) = \phi_g(h_2) = gh_2$$

dann ergibt Multiplikation mit g^{-1} die Gleichheit $h_1 = h_2$. Es folgt, dass für alle Nebenklassen gH von H

$$|gH| = |H|$$

gilt. Daher

$$|G| = \sum_{i=1}^{n} |g_i H| = \sum_{i=1}^{n} |H| = [G : H]|H|$$

woraus (i) und (ii) folgen. □

Bemerkung: Im obigen Beweis hätten wir auch mit Rechtsnebenklassen arbeiten können. Daher, die Anzahl der Linksnebenklassen von H ist gleich wie die von Rechtsnebenklassen. Allgemeiner, die Abbildung $gH \mapsto Hg^{-1}$ ist eine Bijektion zwischen die Menge der Links- und Rechtsnebenklassen von H in G. (ÜA)

Korollar 16.3. Sei G eine endliche Gruppe. Für alle $x \in G$ teilt $|x|$ die Ordnung $|G|$. Insbesondere gilt für alle $x \in G$: $x^{|G|} = 1$.

Beweis. Nach Proposition 14.3. und Satz 16.2 gilt $|x| = |\langle x \rangle| \mid |G|$. □

Beispiel: Die Umkehrung des Satzes von Lagrange gilt nicht. Es gibt endliche Gruppen G und $m \in \mathbb{N}$ so dass $m \mid |G|$, jedoch besitzt G keine Teilgruppe der Ordnung m: Sei $G = A_4$. Die Elemente von A_4 sind alle gerade Permutationen auf 4 Elementen:

$$A_4 = \{e,\ (123),\ (132),\ (234),\ (243),\ (134),\ (143), (124),\ (142),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Es gilt $|A_4| = 12$, und $6 \mid 12$, aber A_4 hat keine Teilgruppe der Ordnung 6. (ÜA)

Korollar 16.4. Jede Gruppe primer Ordnung ist zyklisch.

Beweis. Sei G eine endliche Gruppe mit $|G|$ prim. Sei $x \in G\,, x \neq 1$. Nach Korollar 16.3 teilt $|x|$ die Ordnung $|G|$. Da $|G|$ prim ist, folgt entweder $|x| = |G|$ oder $|x| = 1$. Aus $x \neq 1$ folgt $|x| \neq 1$ also $|x| = |G|$ und somit $\langle x \rangle = G$. □

Wir betrachten nun weitere Gruppenkonstruktionen, die wir später im §18 für die Isomorphiesätze brauchen.

Bezeichnung 16.5. Sei G eine Gruppe und seien S, T Teilmenge von G. Schreibe:

$$ST := \{st : s \in S,\ t \in T\}.$$

Proposition 16.6. Sei G eine endliche Gruppe und seien H, K Teilgruppe. Dann gilt

$$|HK||H \cap K| = |H||K|.$$

Beweis. Definiere eine Abbildung

$$\phi\colon H \times K \to HK,\ (h,k) \mapsto hk.$$

Nach Definition ist ϕ surjektiv.

Behauptung: für alle $(h,k) \in H \times K$ gilt $\phi^{-1}(hk) = \{(hd^{-1}, dk) : d \in H \cap K\}$.
Beweis der Behauptung:
"$\supseteq$": offensichtlich, wenn $d \in H \cap K$ dann auch $d^{-1} \in H \cap K$ somit $h' = hd^{-1} \in H$ und $k' = dk \in K$ und $h'k' = hk$.
"$\subseteq$": seien $h' \in H$ und $k' \in K$ mit $h'k' = hk$. Dann $d := k'k^{-1} = h'^{-1}h \in H \cap K$ und $h' = hd^{-1}$ und $k' = dk$. Die Behauptung ist damit bewiesen.

Es folgt, dass für alle $x \in HK$, $|\phi^{-1}(x)| = |H \cap K|$ gilt und somit

$$|HK||H \cap K| = |H \times K| = |H||K|.$$

□

Proposition 16.7. Sei G eine Gruppe und seien H, K Teilgruppen. Die Menge HK ist genau dann eine Teilgruppe wenn $HK = KH$.

Beweis. Wir bemerken die folgende allgemeine Tatsache: Seien $h \in H$ und $k \in K$. Dann $hk \in HK$ und $(hk)^{-1} = k^{-1}h^{-1} \in KH$. Also $g \in HK \iff g^{-1} \in KH$.

Sei nun HK eine Teilgruppe und sei $g := hk \in HK$. Dann ist $g^{-1} \in HK$, und somit $g = (g^{-1})^{-1} \in KH$. Somit $HK \subseteq KH$. Die Inklusion $KH \subseteq HK$ wird analog bewiesen.

Umgekehrt sei nun $HK = KH$. Bemerke dass $HK \neq \varnothing$. Seien $h_1, h_2 \in H$ und $k_1, k_2 \in K$. Betrachte $h_1k_1h_2k_2$. Da $k_1h_2 \in KH = HK$ gilt, dann existieren $h_3 \in H$ und $k_3 \in K$ mit $k_1h_2 = h_3k_3$. Daher $h_1(k_1h_2)k_2 = (h_1h_3)(k_3k_2) \in HK$. Also HK ist bezüglich Multiplikation abgeschlossen. Wir haben weiterhin oben gemerkt, dass $g \in HK$ impliziert $g^{-1} \in KH$. Da $KH = HK$ ist also HK auch bezüglich Inversen abgeschlossen, und somit eine Teilgruppe. □

Definition 16.8. Sei A eine Teilgruppe von G. Der *Normalisator* von A in G, bezeichnet $N_G(A)$, ist die Menge

$$N_G(A) = \{x \in G : xAx^{-1} = A\}$$

Bemerkung 16.9. $N_G(A)$ ist eine Teilgruppe von G die A enthält, A ist genau dann normal in G wenn $G = N_G(A)$ (ÜA).

Korollar 16.10. Seien H, K Teilgruppen von G mit $H \leq N_G(K)$. Dann ist HK eine Teilgruppe von G. Insbesondere, wenn $K \trianglelefteq G$ dann $HK \leq G$ für alle $H \leq G$.

Beweis. Es genügt zu zeigen, dass $HK = KH$. Seien $h \in H$ und $k \in K$. Dann $h^{-1}kh, hkh^{-1} \in K$ weil $H \leq N_G(K)$. Daher $hk = (hkh^{-1})h \in KH$ und $kh = h(h^{-1}kh) \in HK$. Somit $HK = KH$. □

§18: Isomorphiesätze

Satz 16.11 (Erster Isomorphiesatz)**.** Sei $\phi: G \to H$ ein Gruppenhomomorphismus. Dann $\ker\phi \trianglelefteq G$ und

$$G/\ker\phi \simeq \operatorname{Im}\,\phi.$$

Beweis. Es wurde bereits bewiesen, dass der Kern eines Gruppenhomomorphismus normal ist (s. Skript 15; Beispiel nach Definition 15.9).
Definiere $f: G/\ker\phi \to H$ durch $f(a\ker\phi) = \phi(a)$.

- f ist wohldefiniert, denn wenn $a\ker\phi = b\ker\phi$ dann $ab^{-1} \in \ker\phi$ also $1 = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1}$ und somit $\phi(a) = \phi(b)$.
- f ist ein Gruppenhomomorphismus, denn

$$f((a\ker\phi)(b\ker\phi)) = f(ab\ker\phi) = \phi(ab) = \phi(a)\phi(b) = f(a\ker\phi)f(b\ker\phi).$$

- $\operatorname{Im} f = \operatorname{Im}\phi$. Klar.
- f ist injektiv: Seien $f(a\ker\phi) = f(b\ker\phi)$. Dann $\phi(a) = \phi(b) \Rightarrow \phi(ab^{-1}) = 1 \Rightarrow ab^{-1} \in \ker\phi \Rightarrow a\ker\phi = b\ker\phi$.

Also $f: G/\ker\phi \to \operatorname{Im}\phi$ ist also ein bijektiver Gruppenhomomorphismus (ein Isomorphismus). □

Korollar 16.12. Sei $\phi: G \to H$ ein Gruppenhomomorphismus. Dann

1. ϕ ist genau dann injektiv wenn $\ker \phi = 1$;
2. $[G : \ker \phi] = |\text{Im } \phi|$.

Beweis. 1. Die Hinrichtung folgt direkt aus der Definition von Injektivität.

Für die Rückrichtung, sei $\ker \phi = 1$ und seien $a, b \in G$ mit $\phi(a) = \phi(b)$. Dann $\phi(ab^{-1}) = 1 \Rightarrow ab^{-1} \in \ker \phi \Rightarrow ab^{-1} = 1 \Rightarrow a = b$.

2. Aus dem ersten Isomorphiesatz, folgt $[G : \ker \phi] = |G/\ker \phi| = |\text{Im } \phi|$.

□

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

Prof. Dr. Salma Kuhlmann

In diesem Skript wollen wir weitere Isomorphiesätze kennenlernen, und damit §18 beenden.

Wir ergänzen Bemerkung 16.9:

Bemerkung 17.1. Seien $A \leq B \leq G$ Gruppen. Der Normalisator $N_G(A)$ von A in G ist die größte Teilgruppe von G in der A normal ist; A ist genau dann normal in B wenn $B \leq N_G(A)$. (siehe ÜB).

Satz 17.2 (Zweiter Isomorphiesatz)**.** Sei G eine Gruppe und seien A, B Teilgruppen mit $A \leq N_G(B)$. Dann ist AB eine Teilgruppe von G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ und $AB/B \simeq A/(A \cap B)$.

Beweis. Aus $A \leq N_G(B)$ folgt $AB \leq G$ (Korollar 16.10). Aus $B \leq N_G(B)$ folgt $AB \leq N_G(B)$, also $B \trianglelefteq AB$ (Bemerkung 17.1).

Sei nun $\pi\colon AB \to (AB)/B$ die kanonische Projektion, und betrachte die Einschränkung $\pi|_A$ von π auf A. Für $a \in A$ mit $\pi(a) = 1$ gilt auch $a \in B$, daher $a \in A \cap B$. Also ist $\ker(\pi|_A) = A \cap B$, und daher $A \cap B \trianglelefteq A$.

Seien nun $a \in A$ und $b \in B$. Es gilt $\pi(a) = \pi(ab)$. Also ist $\pi|_A$ surjektiv, d.h., Im $(\pi|_A) = (AB)/B$. Der erste Isomorphiesatz (Satz 16.11) ergibt nun $A/(A \cap B) \simeq (AB)/B$. □

Satz 17.3 (Dritter Isomorphiesatz)**.** Sei G eine Gruppe und seien $H, K \trianglelefteq G$ normale Teilgruppen mit $H \leq K$. Dann $K/H \trianglelefteq G/H$ und

$$(G/H)/(K/H) \simeq G/K.$$

Beweis. Definiere die Abbildung $f\colon G/H \to G/K$ durch $f(gH) = gK$.

- f ist wohldefiniert, da für $g_1, g_2 \in G$ mit $g_1H = g_2H$ gilt $g_1^{-1}g_2 \in H$ und $g_1^{-1}g_2 \in K$. Also $g_1K = g_2K$ (s. Proposition 15.7).
- f ist ein Gruppenhomomorphismus:

$$f(aHbH) = f(abH) = abK = aKbK = f(aH)f(bH).$$

- f ist surjektiv: klar.
- Bemerke dass $H \trianglelefteq K$, so dass K/H eine Gruppe ist, also $K/H \leq G/H$ ist eine Untergruppe (s. Proposition 15.8). Wir behaupten dass $\ker f = K/H$. In der Tat, sei $a \in G$. Dann $f(aH) = 1K \iff aK = 1K \iff a \in K$. Daher $K/H = \ker f$. Also $K/H \trianglelefteq G/H$ und (s. Satz 16.11) es folgt:

$$(G/H)/(K/H) \simeq G/K.$$

□

Satz 17.4. (Gitter Isomorphiesatz / Korrespondenzsatz) Sei G eine Gruppe und N eine normale Teilgruppe von G. Für eine Teilgruppe A die N enthält, sei $\bar{A} := A/N$. Sei $\pi: G \to G/N$ die kanonische Projektion.

Die Abbildung $A \mapsto \pi(A) = \bar{A}$ ist eine Bijektion zwischen der Menge der Teilgruppen von G die N enthalten und der Menge der Teilgruppen von G/N.

Weiter, für $A, B \leq G$ mit $N \leq A$ und $N \leq B$ gelten:

1. $A \leq B \iff \bar{A} \leq \bar{B}$; in diesem Fall, gilt $[B : A] = [\bar{B} : \bar{A}]$.
2. $A \trianglelefteq B \iff \bar{A} \trianglelefteq \bar{B}$; in diesem Fall, gilt $B/A \simeq \bar{B}/\bar{A}$.
3. $\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$.
4. $\overline{A \cap B} = \bar{A} \cap \bar{B}$.

Beweis. Siehe ÜB. □

Satz 17.5. (Schmetterlingslemma / Lemma von Zassenhaus) Seien $a \trianglelefteq A$ und $b \trianglelefteq B$ Teilgruppen einer Gruppe G. Dann

1. $a(A \cap b) \trianglelefteq a(A \cap B)$
2. $b(B \cap a) \trianglelefteq b(B \cap A)$
3. $(A \cap b)(B \cap a) \trianglelefteq A \cap B$
4. $$\frac{a(A \cap B)}{a(A \cap b)} \simeq \frac{A \cap B}{(A \cap b)(B \cap a)} \simeq \frac{b(B \cap A)}{b(B \cap a)}$$

Beweis. Aus $A \leq N_G(a)$ beziehungsweise $B \leq N_G(b)$ folgen :

$$A \cap b \leq A \cap B \leq N_G(a) \quad \text{beziehungsweise} \quad B \cap a \leq A \cap B \leq N_G(b).$$

(s. Bemerkungen 16.9 und 17.1).

• Daher sind $a(A \cap b), a(A \cap B), b(B \cap a)$ und $b(A \cap B)$ Teilgruppen von G (s. Korollar 16.10).

Zunächst zeigen wir 3.

• Bemerke, dass $A \cap b$ und $B \cap a$ normale Teilgruppen von $A \cap B$ sind. Wir führen den Beweis für $A \cap b$ (der Beweis für $B \cap a$ ist analog): Für $g \in A \cap B$ und $c \in A \cap b$ gelten $gcg^{-1} \in b$ (weil $b \trianglelefteq B$) und $gcg^{-1} \in A$ weil $c, g \in A$.

• Also ist $(A \cap b)(B \cap a) \leq A \cap B$ (s. Korollar 16.10). Es folgt übrigens dass $(A \cap b)(B \cap a) = (B \cap a)(A \cap b)$ (s. Proposition 16.7).

• Jetzt prüfen wir dass $(A \cap b)(B \cap a)$ eine normale Teilgruppe von $A \cap B$ ist: für $c \in A \cap b$ und $d \in B \cap a$ gilt $gcdg^{-1} = gcg^{-1}gdg^{-1} \in (A \cap b)(B \cap a)$.

Jetzt zeigen wir 4 (und zugleich 1. beziehungsweise 2.).

Ein Element $x \in a(A \cap B)$ lässt sich als $x = \alpha\gamma$ darstellen mit $\alpha \in a$ und $\gamma \in A \cap B$. Definiere

$$f: a(A \cap B) \to \frac{A \cap B}{(A \cap b)(B \cap a)}$$

durch

$$x \mapsto \gamma(A \cap b)(B \cap a).$$

• f ist wohldefiniert: sei $\alpha\gamma = \alpha'\gamma'$. Dann $\gamma'\gamma^{-1} = (\alpha')^{-1}\alpha \in a \cap B \cap A = a \cap B \leq (A \cap b)(B \cap a)$, d.h.:

$$\gamma'(A \cap b)(B \cap a) = \gamma(A \cap b)(B \cap a).$$

• f ist ein Gruppenhomomorphismus: seien $\alpha, \alpha' \in a$ und $\gamma, \gamma' \in A \cap B$. Dann $\alpha, \gamma\alpha'\gamma^{-1} \in a$ weil $a \lhd A$. Also

$$f(\alpha\gamma\alpha'\gamma') = f((\alpha\gamma\alpha'\gamma^{-1})\gamma\gamma') = \gamma\gamma'(A \cap b)(B \cap a)$$

und da $(A \cap b)(B \cap a) \lhd A \cap B$ folgt

$$f(\alpha\gamma)f(\alpha'\gamma') = \gamma(A \cap b)(B \cap a)\gamma'(A \cap b)(B \cap a) = \gamma\gamma'(A \cap b)(B \cap a).$$

• f ist surjektiv: nach Definition.

• Es gilt $\ker f = a(A \cap b)$. In der Tat, seien $\alpha \in a$ und $\gamma \in A \cap B$ mit $f(\alpha\gamma) = 1(A \cap b)(B \cap a)$, d.h., $\gamma \in (A \cap b)(B \cap a)$. Seien $x \in (A \cap b)$ und $y \in (B \cap a)$ mit $\gamma = xy$. Dann $\alpha\gamma = (\alpha x)y \in a(A \cap b)$. Umgekehrt, seien $\alpha \in a$ und $\gamma \in A \cap B$ mit $\alpha\gamma \in a(A \cap b)$. Dann existieren $t \in a,\ s \in A \cap b$ mit $\alpha\gamma = ts$. Nun $\alpha^{-1}t \in a$ und aus $\gamma, s \in B$ folgt $\alpha^{-1}t = \gamma s^{-1} \in B$. Also $\alpha^{-1}ts = \gamma \in (B \cap a)(A \cap b) = (A \cap b)(B \cap a)$ und somit $\alpha\gamma \in \ker f$.

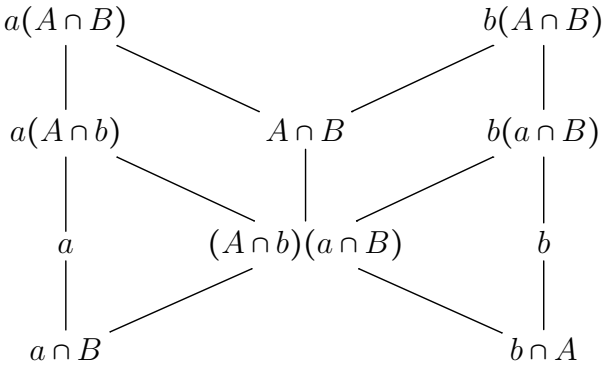
• Nach dem ersten Isomorphiesatz ist $a(A \cap b)$ normal in $a(A \cap B)$ (was 1. zeigt) und

$$\frac{a(A \cap B)}{a(A \cap b)} \simeq \frac{(A \cap B)}{(A \cap b)(B \cap a)}.$$

• Wenn wir nun A und B und, entsprechend, a und b umtauschen und den gleichen Beweis durchführen bekommen wir 2. und

$$\frac{b(A \cap B)}{b(B \cap a)} \simeq \frac{(A \cap B)}{(A \cap b)(B \cap a)}.$$

Das Schmetterlingsdiagramm:



□

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Abschnitt §19 beginnen; Normalreihen einführen, Satz 17.5 benutzen um den Verfeinerungssatz von Schreier sowie den Satz von Jordan-Hölder zu beweisen.

§19: Einfache und auflösbare Gruppen

Definition 18.1. Sei G eine Gruppe.

1. Eine normale Teilgruppe $N \trianglelefteq G$ heißt auch *Normalteiler* von G. Wir schreiben auch $G \trianglerighteq N$ dafür.
2. G ist *einfach* falls G nicht-trivial ist (i.e. $G \neq 1$) und 1 und G die einzige Normalteiler von G sind.

Proposition 18.2. Eine nicht-triviale abelsche Gruppe G ist genau dann einfach wenn $G \simeq \mathbb{Z}_p$ für eine Primzahl p (i.e. G ist zyklisch von primer Ordnung p).

Beweis. 1. Sei G eine abelsche Gruppe. Dann ist jede Teilgruppe N von G normal (weil die Bedingung $(*)$ in Proposition 15.8 stets für N erfüllt ist, wenn G abelsch ist). G ist also genau dann einfach wenn ihre einzige Teilgruppen 1 und G sind. (Insbesondere ist $\mathbb{Z}_p$ einfach, wegen Lagrange's Satz).

2. Sei nun G einfach. Aus 1. folgt, dass G von jedem nicht-trivialen Element erzeugt ist, also G ist zyklisch. Wenn G zyklisch und unendlich ist, und x ein Erzeuger von G, dann ist z.B. x^2 kein Erzeuger von G (s. Proposition 14.11). Es folgt: G ist endlich und zyklisch und jedes Element $x \neq 1$ erzeugt G.

   Sei nun $x \neq 1$ ein Erzeuger von G, $p \in \mathbb{N}$ eine Primzahl die $|x|$ teilt. Dann ist $|x^p| < |x|$ (s. Proposition 14.11) und daher ist x^p kein Erzeuger, also ist $x^p = 1$. Daraus folgt $|G| = p$.

□

Definition 18.3. Sei G eine Gruppe.

1. Eine Kette von Teilgruppen

$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$

   heißt *Normalreihe* falls $G_i \trianglelefteq G_{i+1}$ für alle $i = 0, \cdots, s$ gilt.

2. Die Quotienten G_{i+1}/G_i für $i = 0, \ldots, s-1$ heißen *Faktorgruppen*, oder die *Faktoren* oder die *Quotienten* der Normalreihe.
3. Eine Normalreihe heißt *Kompositionsreihe* falls alle Faktorgruppen einfach sind.
4. In diesem Fall heißen die Faktorgruppen *Kompositionsfaktoren* von G.

5. Eine Normalreihe
$$1 = G_0 \leq G_1 \leq \ldots \leq G_s = G$$
heißt *Verfeinerung* einer anderen Normalreihe
$$1 = H_0 \leq H_2 \leq \ldots \leq H_r = G$$
falls $H_0, \ldots, H_r$ eine Teilkette von $G_0, \ldots, G_s$ ist.

Beispiel: Die Gruppe A_4 ist normal in S_4, weil $[S_4 : A_4] = 2$ (s. ÜB). Im ÜB wird ferner gezeigt, dass die Teilgruppe (die *kleinsche Vierergruppe*)
$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$
ein Normalteiler von A_4 ist. Somit ist
$$\{1\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$$
eine Normalreihe für S_4.

Definition 18.4. Zwei Normalreihen heißen *äquivalent* falls es eine Bijektion zwischen ihren Faktorgruppen gibt, und entsprechende Faktorgruppen isomorph sind. Das heißt zwei Reihen
$$H_0 \trianglelefteq \cdots \trianglelefteq H_i \trianglelefteq H_{i+1} \trianglelefteq \cdots \trianglelefteq G$$
und $\quad K_0 \trianglelefteq \cdots \trianglelefteq K_j \trianglelefteq K_{j+1} \trianglelefteq \cdots \trianglelefteq G$
sind äquivalent, wenn es eine Bijektion $i \to j$ gibt, so dass die korrespondierenden Faktoren isomorph sind: $H_{i+1}/H_i \simeq K_{j+1}/K_j$.

Beispiel: Betrachte die folgende Kompositionsreihen für $\mathbb{Z}_{30}$:
$$\mathbb{Z}_{30} \geq \langle 5\rangle \geq \langle 10\rangle \geq \{0\}$$
$$\mathbb{Z}_{30} \geq \langle 3\rangle \geq \langle 6\rangle \geq \{0\}.$$
Die Kompositionsfaktoren der ersten Reihe sind $\mathbb{Z}_{30}/\langle 5\rangle \simeq \mathbb{Z}_5$, $\langle 5\rangle/\langle 10\rangle \simeq \mathbb{Z}_2$ und $\langle 10\rangle/\langle 0\rangle \simeq \mathbb{Z}_3$.
Die Kompositionsfaktoren der ersten Reihe sind $\mathbb{Z}_{30}/\langle 3\rangle \simeq \mathbb{Z}_3$, $\langle 3\rangle/\langle 6\rangle \simeq \mathbb{Z}_2$ und $\langle 6\rangle/\langle 0\rangle \simeq \mathbb{Z}_5$.
Daher sind die zwei Kompositionsreihen äquivalent.

Satz 18.5 (Verfeinerungssatz von Schreier)**.** Zwei Normalreihen einer Gruppe G haben äquivalente Verfeinerungen.

Beweis. Seien

(1) $$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G$$

und

(2) $$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = G$$

Normalreihen. Sei $G_{i,j} := G_i(G_{i+1} \cap H_j)$ für $0 \leq j \leq r$. Dann
$$G_{i,0} = G_i\{1\} = G_i \quad \text{und} \quad G_{i,r} = G_i(G_{i+1} \cap G) = G_{i+1}.$$
(also haben wir r weitere Glieder zwischen G_i und G_{i+1} eingefügt).
Da $G_i \trianglelefteq G_{i+1}$ und $H_j \trianglelefteq H_{j+1}$, aus dem Lemma von Zassenhaus (mit $a = G_i$, $A = G_{i+1}$, $b = H_j$ und $B = H_{j+1}$) folgt
$$G_{i,j} = G_i(G_{i+1} \cap H_j) \trianglelefteq G_i(G_{i+1} \cap H_{j+1}) = G_{i,j+1}.$$

Somit ist die folgende Normalreihe eine Verfeinerung von (1):

$$\{1\} \trianglelefteq G_{0,0} \trianglelefteq G_{0,1} \trianglelefteq \ldots \trianglelefteq G_{0,r} = G_{1,0} \trianglelefteq G_{1,1} \trianglelefteq \ldots \trianglelefteq G_{s-1,r} = G_s = G.$$

Sei nun $H_{i,j} := H_i(H_{i+1} \cap G_j)$ für $0 \leq j \leq s$. Ähnlich wie oben, ist

$$\{1\} \trianglelefteq H_{0,0} \trianglelefteq H_{0,1} \trianglelefteq \ldots \trianglelefteq H_{0,s} = H_{1,0} \trianglelefteq H_{1,1} \trianglelefteq \ldots \trianglelefteq H_{r-1,s} = H_r = G.$$

eine Verfeinerung von (2). Nun, aus dem Lemma von Zassenhaus (mit $a = G_i$, $A = G_{i+1}$, $b = H_j$ und $B = H_{j+1}$) folgt

$$\frac{G_i(G_{i+1} \cap H_{j+1})}{G_i(G_{i+1} \cap H_j)} \simeq \frac{H_j(H_{j+1} \cap G_{i+1})}{H_j(H_{j+1} \cap G_i)}$$

das heißt:

$$G_{i,j+1}/G_{i,j} \simeq H_{j,i+1}/H_{j,i}.$$

□

Satz 18.6 (Satz von Jordan-Hölder)**.** Sei G eine endliche Gruppe mit $G \neq 1$. Dann gelten

1. G hat eine Kompositionsreihe
2. alle Kompositionsreihen von G sind äquivalent.

Beweis. 1. Wenn G einfach ist, dann ist $\{1\} \trianglelefteq G$ bereits eine Kompositionsreihe.

Sei nun G nicht einfach. Da G endlich ist, hat sie einen maximalen echten Normalteiler N. Dann ist G/N einfach, nach dem Korrespondenzsatz 17.4. Nach Induktion auf $|G|$ hat G eine Kompositionsreihe. ÜA.

2. Nach dem Korrespondenzsatz 17.4 haben Kompositionsreihen keine echte Verfeinerungen; wenn $G_i \trianglelefteq N \trianglelefteq G_{i+1}$ dann $N/G_i \trianglelefteq G_{i+1}/G_i$ und wenn G_{i+1}/G_i einfach ist, dann gilt $N = G_i$ oder $N = G_{i+1}$. Nun, nach dem Verfeinerungssatz von Schreier haben zwei beliebige Kompositionsreihen äquivalente Verfeinerungen. Somit sind zwei beliebige Kompositionsreihen bereits äquivalent.

□

Definition 18.7.
G heißt *auflösbar*, wenn es eine *Normalreihe mit abelschen Faktoren hat.*

Bemerkung 18.8.
Jede abelsche Gruppe ist trivialerweise auflösbar. Betrachte $G \triangleright \{1\}$.

Erinnerung (s. LA II, Kapitel II, § 6; Skripte 6 und 7.) Sei $n \geq 3$, dann ist

1. $|S_n/A_n| = 2$
2. S_n ist nicht abelsch
3. A_n ist nicht abelsch für $n > 3$
   (Begründung: (123) und (234) kommutieren nicht!)

Beispiel 18.9.
S_n ist auflösbar für $n \leq 4$: S_1 und S_2 sind abelsch also auflösbar. Wir betrachten nun:

1. $S_3 \trianglerighteq A_3 \trianglerighteq \{1\}$

   $| S_3/A_3 | = 2$ $| A_3/\{1\} | = 3$: Diese zwei Gruppen haben als Ordnung eine Primzahl. Es folgt aus Lagrange, dass die Gruppen zyklisch sind, also abelsch.

2. $S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq W \trianglerighteq \{1\}$, wobei V die kleinsche Vierergruppe ist und $W := \{1, (12)(34)\}$.

   $| S_4/A_4 | = 2$ $| A_4/V | = 3$ $| V/W | = 2$.

   Die Faktorgruppen sind also $\mathbb{Z}_2$ und $\mathbb{Z}_3$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir auflösbare Gruppen weiter untersuchen, und eine Charakterisierung erzielen in Satz 19.6. Dafür werden wir neue Definitionen und Begriffe (z.B. iterierte Kommutatoren) benötigen. Auflösbare Gruppen spielen in Kapitel 4 eine wesentliche Rolle.

Sei $G \neq \{1\}$ stets eine Gruppe.

Definition 19.1.

1. Für $g, h \in G$ definiere $(g,h) := g^{-1}h^{-1}gh \in G$; (g,h) heißt *Kommutator* von g und h.
2. $G' := (G,G)$ ist die *Kommutatorgruppe* von G und ist die Untergruppe, die durch
$$S := \{(g,h); g,h \in G\}$$
erzeugt wird.
3. Wir definieren die iterierte Kommutatoren per Induktion über $k \in \mathbb{N}, k \geq 2$:
$G'' := (G')'$, $G^{(k)} := (G^{(k-1)})'$.

Bemerkung 19.2.

1. G ist abelsch genau dann, wenn $(G,G) = \{1\}$.
2. $gh = hg(g,h)$
3. $(g,h) = (h,g)^{-1}$, also ist $< S >= \{s_1 \cdots s_n \mid n \in \mathbb{N};\ s_i \in S\}$.
4. Wenn $H \leq G$, dann ist $H^{(l)} \leq G^{(l)}$ für alle $l \in \mathbb{N}$.

Beweis: ÜA.

Wir werden nun die iterierte Kommutatoren genauer untersuchen, und sie für unsere Charakterisierung für auflösbare Gruppen ausnutzen.

Proposition 19.3.
Seien G, K Gruppen und $\eta : G \to K$ ein Homomorphismus. Es gelten

1. $\eta(g,h) = (\eta(g), \eta(h))$
2. $\eta(G') \subseteq K'$
3. Wenn η surjektiv ist, gilt ferner: $\eta(G') = K'$
4. Insbesondere für einen beliebigen Homomorphismus η gilt: $\eta(G') = \eta(G)'$ und
5. Allgemeiner gilt $\eta(G^{(k)}) = \eta(G)^{(k)}$ für alle $k \in \mathbb{N}$

Beweis:

1. Wir berechnen: $\eta(g,h) = \eta(g^{-1}h^{-1}gh) = \eta(g)^{-1}\eta(h)^{-1}\eta(g)\eta(h) = (\eta(g),\eta(h))$.
2. Aus 1. folgt unmittelbar $\eta(G') \subseteq K'$.
3. Wenn η surjektiv ist, folgt aus 1. dass für alle $x, y \in K : (x,y) \in \eta(G')$. Es folgt also auch $\eta(G') \supseteq K'$, und damit ist die Gleichheit bewiesen.
4. Klar, da $\eta : G \to \eta(G)$ surjektiv ist.
5. Für $k = 1$ gilt die Behauptung wie in 4.

   Nun betrachte $\eta : G' \to K$ und 4. nochmal angewendet ergibt:

   $$\begin{array}{lrcl} & \eta((G')') & = & \eta(G')' \\ \text{i.e.} & \eta(G'') & = & (\eta(G)')' = \eta(G)'' . \end{array}$$

   (Usw. per Induktion fortsetzen, ÜA). □

Proposition 19.4.
Wenn $K \trianglelefteq G$, dann ist $K' \trianglelefteq G$. Insbesondere ist $G' \trianglelefteq G$.

Beweis:
Sei $a \in G$ fest und betrachte die Abbildung $\eta_a : K \to K$, $k \mapsto aka^{-1}$.
Da K ein Normalteiler ist, ist η_a wohldefiniert. Außerdem ist η_a ein Homomorphismus (ÜA).
Aus Proposition 19.3 folgt: $\eta_a(K') \subseteq K'$ für alle $a \in G$, i.e. $K' \trianglelefteq G$. □

Wir erhalten also eine Kette:

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq G^{(k+1)} \trianglerighteq \cdots .$$

Für den Beweis von Satz 19.6 brauchen wir noch:

Lemma 19.5.
Sei $K \trianglelefteq G$. Es gilt G/K ist abelsch $\Leftrightarrow K \geq G'$. Insbesondere ist G/G' abelsch.
(In der Tat ist G' ist die kleinste normale Untergruppe mit dieser Eigenschaft).
Allgemeiner gilt: $G^{(k)}/G^{(k+1)}$ ist abelsch für alle $k \in \mathbb{N}$.

Beweis:
Aus Bemerkung 19.2 folgt: G/K ist abelsch $\Leftrightarrow (G/K)' = \{1\} \Leftrightarrow (gK, hK) = 1$ für alle $g, h \in G$.
Aber $(gK,hK) = (gK)^{-1}(hK)^{-1}gKhK = (g^{-1}h^{-1}gh)K = (g,h)K$. Also ist G/K abelsch $\Leftrightarrow$ $(g,h)K = K$ für alle $g,h \in G \Leftrightarrow (g,h) \in K$ für alle $g,h \in G \Leftrightarrow G' \leq K$.
Die letzte Aussage folgt per Induktion nach $k \in \mathbb{N}$. □

Satz 19.6.
G ist auflösbar $\Leftrightarrow \exists k \in \mathbb{N}$ mit $G^{(k)} = 1$.

Beweis:
"$\Leftarrow$" Folgt unmittelbar aus Lemma 19.5: Die Normalreihe $G \trianglerighteq G' \trianglerighteq \cdots \trianglerighteq G^{(k)} = 1$ hat abelsche Faktoren.

"⇒" Sei $G = G_1 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$ eine Normalreihe mit abelschen Faktoren G_i/G_{i+1}.

Lemma 19.5 $\Rightarrow G_{i+1} \supseteq G_i'$ für alle i.

Wir prüfen per Induktion dass $G_i \supseteq G^{(i)}$ für alle i:

- für $i = 1$ gilt $G = G_1 \supseteq G'$ ✓
- Induktionsannahme für k ✓
- Induktionsschritt für $k+1$: $G_{k+1} \supseteq (G_k)' \supseteq (G^{(k)})' = G^{(k+1)}$

Schließlich, da $G_{s+1} = \{1\}$ folgt insbesondere $G^{(s+1)} = \{1\}$ □

Satz 19.7.
Sei G auflösbar.

(1) Sei $H \leq G$. Dann ist H auflösbar.

(2) Sei $\eta : G \twoheadrightarrow H$ ein surjektiver Homomorphismus, dann ist H auflösbar.

(3) Sei G eine beliebige Gruppe und $K \trianglelefteq G$, so dass K und G/K auflösbar sind, dann ist G auch auflösbar.

Beweis: Für den Beweis, benutzen wir stillschweigend Proposition 19.3 und Satz 19.6:

(1) $H \leq G \Rightarrow H^{(i)} \leq G^{(i)}$, also $G^{(k)} = \{1\} \Rightarrow H^{(k)} = \{1\}$.

(2) $\eta(G^{(i)}) = \eta(G)^{(i)}$. Also $G^{(k)} = \{1\} \Rightarrow \eta(G)^{(k)} = \{1\}$. Also $H^{(k)} = \{1\}$.

(3) Sei $\pi : G \twoheadrightarrow G/K$ die kanonische Projektion. Es gilt $\pi(G^{(i)}) = (G/K)^{(i)}$.

Nun G/K auflösbar $\Rightarrow \exists k$ mit $\pi(G^{(k)}) = (G/K)^{(k)} = \{1\}$. Also: für alle $x \in G^{(k)}$ gilt $xK = K$. Es folgt: für alle $x \in G^{(k)}$ gilt $x \in K$, i.e. $G^{(k)} \subseteq K$.

Nun ist aber auch K auflösbar, also existiert ℓ mit $K^{(\ell)} = \{1\}$. Wir berechnen: $G^{(k+\ell)} = (G^{(k)})^{\ell} \subseteq K^{(\ell)} = \{1\}$. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir eine Charakterisierung für endliche auflösbare Gruppen beweisen. Wir werden ferner (ergänzend zu Beispiel 18.9) die Gruppen A_n und S_n für $n \geq 5$ untersuchen, damit werden wir Abschnitt §19 beenden. Im Abschnitt §20 werden wir die Sylow Sätze aussagen, und die notwendige Begriffe und Werkzeug für deren Beweise einführen.

Sei $G \neq \{1\}$ stets eine Gruppe.

Bemerkung 20.1.
G ist auflösbar und einfach $\Rightarrow G$ ist abelsch (weil $G \trianglerighteq \{1\}$ die einzig mögliche Normalreihe ist).

Satz 20.2.
Sei G eine endliche Gruppe. Dann ist G auflösbar $\Leftrightarrow$ jeder (nicht-trivialer) Kompositionsfaktor einer Kompositionsreihe ist zyklisch mit Primordnung.

Beweis:

"$\Rightarrow$" Sei G auflösbar; und $G = G_1 \trianglerighteq \cdots \trianglerighteq G_{s+1} = \{1\}$ eine Kompositionsreihe. Per Definition ist G_i/G_{i+1} einfach, für alle i. Außerdem ist G_i/G_{i+1} auch auflösbar, für alle i (s. Satz 19. 7). Es folgt: G_i/G_{i+1} ist abelsch, für alle i (s. Bemerkung 20.1), also entweder trivial oder zyklisch mit Primordnung (s. Proposition 18.2).

"$\Leftarrow$" Da G endlich ist, existiert wegen Jordan Hölder eine Kompositionsreihe

$$(*) \qquad G = G_1 \trianglerighteq \cdots \trianglerighteq G_{s+1} = \{1\}$$

Per Annahme sind die (nicht-triviale) G_i/G_{i+1} zyklisch mit Primordnung. Dann ist insbesondere G_i/G_{i+1} abelsch und damit ist die Reihe $(*)$ sogar eine auflösbare Reihe. $\square$.

Satz 20.3.
A_n ist einfach für $n \geq 5$.

Beweis:
Aus Lineare Algebra II, ÜB5 Aufgabe 5.3 (b) wissen wir dass A_n von 3-Zykeln erzeugt ist, für $n \geq 3$. Sei $K \neq \{1\}, K \trianglelefteq A_n$. Zu zeigen: $K = A_n$.

Behauptung 1: Wenn K ein 3-Zykel enthält, dann enthält K alle 3-Zykeln.

Beweis: Sei OE $(123) \in K$ und (ijk) beliebig. Betrachte γ darunter (OE ist $\gamma \in A_n$ sonst ersetze durch $(lm)\gamma$):

$$\gamma := \begin{pmatrix} 1\,2\,3\,4\,5\cdots \\ i\,j\,k\,l\,m\cdots \end{pmatrix}. \quad \text{Wir berechnen: } \gamma(123)\gamma^{-1} = (ijk) \qquad (*)$$

Da K normal ist folgt nun wegen $(*)$ dass $(ijk) \in K$. $\square$

Behauptung 2: K enthält ein 3-Zykel.

Beweis: • Sei $\alpha \in K\,; \alpha \neq 1$. Wähle α mit maximaler Anzahl von Fixpunkten. Bemerke dass α keine Transposition ist. Wir zeigen: α ist ein 3-Zykel. Sonst schreibe:

(a) $\alpha = (123\cdots)\cdots$

oder

(b) $\alpha = (12)(34)\cdots$

als Produkt disjunkter Zykeln.

• Beobachte, dass im Fall (a) α noch zwei Zahlen bewegen muss (ohne Einschränkung 4, 5), sonst ist $\alpha = (123k)$ eine ungerade Permutation - Widerspruch.

• Setze $\beta := (345)$ und $\alpha_1 := \beta\alpha\beta^{-1}$. Dann ist $\alpha_1 \in K$, weil $\alpha \in K$ und $K \trianglelefteq A_n$.

Direktes Rechnen zeigt:
$\alpha_1 = (124\cdots)\cdots$ im Fall (a) und $\alpha_1 = (12)(45)\cdots$ im Fall (b).

Auf jeden Fall ist $\alpha_1 \neq \alpha$ und damit $\alpha_2 := \alpha_1\alpha^{-1} \neq 1$ und $\alpha_2 \in K$.

Nun ist jede $\ell > 5$ durch β fixiert. Beobachte, dass falls ℓ auch durch α fixiert ist, ℓ auch durch α_2 fixiert ist. Also sind die Fixpunkte von α und α_2 die größer als 5 sind, identisch.

Direktes Rechnen im Fall (a) zeigt $\alpha_2(2) = 2$ und außerdem bewegt α in diesem Fall $1, 2, 3, 4, 5$ (wie oben beobachtet). Also hat α_2 einen extra Fixpunkt (nämlich 2). Da $\alpha_2 \in K$ ist es ein Widerspruch.

Direktes Rechnen im Fall (b) zeigt $\alpha_2(1) = 1$ und $\alpha_2(2) = 2$ - Widerspruch. □

Korollar 20.4.
S_n ist **nicht** auflösbar für $n \geq 5$.

Beweis:
Sonst wäre wegen Satz 19.7 auch A_n auflösbar. Da aber A_n einfach ist folgt wegen Bemerkung 20.1 dass A_n abelsch ist - Widerspruch (s. Erinnerung, S. 3 Skript 18). □

§20: Die Sylow Sätze.

Unser nächstes Ziel ist es, die Sylow Sätze zu beweisen. Diese sind Sonderfälle, für die die Umkehrung von Lagrange gilt. Die Sylow Sätze werden wir für die Galoistheorie in Kapitel 4 benötigen.

Sei G stets eine endliche Gruppe.

Sylow 1:

Sei p Primzahl und $k \in \mathbb{N}$, so dass $p^k \,||G|$, dann hat G eine Teilgruppe H der Ordnung p^k.

Definition 20.5.
Eine solche Teilgruppe H mit $H = p^m$, wobei m maximal ist, heißt eine *Sylow-p-Untergruppe.*

Sylow 2:

1. Sylow-p-Untergruppen H_1 und H_2 sind zueinander konjugiert, das heißt es existiert $a \in G$ mit $H_2 = aH_1a^{-1}$.
2. Die Anzahl der Sylow-p-Untergruppen ist ein Divisor von $[G : H]$ für eine (jede) Sylow-p-Untergruppe H und ist $\equiv 1 \mod p$.
3. Jede Untergruppe der Ordnung p^k ist enthalten in einer Sylow-p-Untergruppe.

Für die Beweise der Sylow-Sätze brauchen wir Gruppenaktionen:

Definition 20.6.
Sei G eine Gruppe und $S \neq \varnothing$ eine Menge. Eine Abbildung

$$\begin{array}{ccc} G \times S & \to & S \\ (g, x) & \mapsto & gx \end{array}$$

so dass

(i) $1x = x$ für alle $x \in S$

(ii) $g_1g_2x = g_1(g_2x)$ für alle $x \in S$ und für alle $g_1, g_2 \in G$

heißt *Gruppenaktion*. Wir sagen G *operiert auf* S.

Definition 20.7.
Angenommen G operiert auf S und S'. Die Aktionen heißen *äquivalent*, wenn es eine Bijektion

$$\nu : S \to S'$$

gibt so dass

$$\nu(gx) = g\nu(x)$$

für alle $g \in G$ und $x \in S$.

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir Gruppenaktionen genauer untersuchen, einige wichtige Beispiele und Begriffe dazu lernen, und eine Charakterisierung von transitiven Aktionen beweisen in Satz 21.12. Der Satz ergibt mehrere Korollare, u.a. die wichtige Bahngleichung in Skript 22.

Seien stets $S \neq \varnothing$ eine Menge, G eine Gruppe.

Notation: $Sym\ S$ bezeichnet die Gruppe der Permutationen von S.

Definition 21.1.
$H \leq Sym\ S$ heißt Permutationsgruppe.

Proposition 21.2. Sei G eine Gruppe. Angenommen G operiert auf S. Sei $g \in G$.

1. Definiere die Abbildung
$$\begin{array}{rccc} T(g): & S & \longrightarrow & S \\ & x & \mapsto & gx \end{array}$$
Dann ist $T(g) \in Sym\ S$.

2. Die Abbildung
$$\begin{array}{rccc} T: & G & \longrightarrow & SymS \\ & g & \mapsto & T(g) \end{array}$$
ist ein Gruppenhomomorphismus.

Beweis: ÜA. □

Definition 21.3.
Ansatz wie in Proposition 21.2, $\ker T \trianglelefteq G$ heißt der *Kern der Aktion von G auf S*. Die Aktion heißt *effektiv*, wenn $\ker T = \{1\}$.

Bemerkung 21.4.

1. G operiert auf S und $H \leq G \Rightarrow H$ operiert auf S (durch Einschränkung).
2. G operiert auf S und $\varnothing \neq \mathcal{O} \subseteq S \Rightarrow G$ operiert auf $\mathcal{O}$
(wann immer die Einschränkung wohldefiniert ist.)

Beweis: (ÜA) □

Beispiel 21.5 (samt Definitionen).

(i) Nehme $S = G$. Definiere die effektive Aktion "*linke Multiplikation*" μ_L :
$(g, x) \mapsto \underbrace{gx}_{\text{Produkt in } G}$, für alle $g, x \in G$.

(ii) Dual dazu μ_R: "*rechte Multiplikation*".

(iii) Nehme $S = G$. Definiere die Aktion "*Konjugation*" κ_j:
$(g, x) \mapsto gxg^{-1}$, für alle $g, x \in G$.

Der Kern dieser Aktion ist die normale Untergruppe $C_G \trianglelefteq G$ und heißt *Zentrum von* G:
$$\begin{aligned} C_G &= \{g \mid \forall x \in G : gxg^{-1} = x\} \\ &= \{g \mid \forall x \in G : gx = xg\} \end{aligned}$$

Satz 21.6. (Satz von Cayley)
Jede Gruppe ist isomorph zu einer Permutationsgruppe.

Beweis:
Setze $S = G$, G operiert auf S mit μ_L. Betrachte den Gruppenhomomorphismus T wie in Proposition 21.2 : $\begin{array}{rccc} T: & G & \longrightarrow & Sym\ G \\ & g & \mapsto & T(g) \end{array}$.
Dann ist offensichtlich $\ker T = \{1\}$. Also $G \simeq T(G) \leq Sym\ G$. □

Aktionen induzieren Äquivalenzrelation. Wir nehmen an: G operiert auf S.

1. Seien $x, y \in S$. Setze $x \underset{G}{\sim} y$, wenn es ein $g \in G$ gibt, s.d. $y = gx$.
   $\underset{G}{\sim}$ ist eine Äquivalenzrelation auf S.
2. $[x] := Gx := \{gx \mid g \in G\}$ heißt die *Orbit* oder *Bahn von* x in S.
3. Es folgt: $S = \bigsqcup_{x \in S} Gx$.

Beispiel 21.7 (samt Definitionen).

(iv) Sei $H \leq G$, setze $S = G$. Dann operiert H auf G durch μ_L (s. Bemerkung 21.4). Wir berechnen für $x \in G$:
$$[x] = \{hx \mid h \in H\} = Hx\,,$$
also die rechte Nebenklasse von x bezüglich H.

(v) Analog für μ_R . Hier bekommen wir $[x] = xH$, die linke Nebenklasse von x bezüglich H.

(vi) Für die Aktion κ_j , und $x \in G$ ist $[x] = \{gxg^{-1} \mid g \in G\}$ die *Konjukationsklasse* von x.

Proposition 21.8.
(i) Die Konjugationsklasse von x ist $\{x\}$ genau dann, wenn $x \in C_G$.

(ii) Also ist das Zentrum von G die Vereinigung solcher Konjugationsklassen.

Beweis: ÜA

□

Wir nehmen an: G operiert auf S.

Definition 21.9.
1. *G operiert transitiv auf S*, oder *die Aktion von G auf S ist transitiv* wenn es nur eine Bahn gibt, das heißt für alle $x, y \in S : x \underset{G}{\sim} y$.
2. Sei $x \in S$, der *Stabilisator von x in G* ist die Untergruppe von G
$$Stab_x := \{g \in G\ ;\ gx = x\ .\}$$

3. Für die Aktion κ_j von G auf G und $x \in G$ heißt

$$Stab_x = \{g \in G \mid gxg^{-1} = x\} = C(x) = \{g \in G \mid gx = xg\} ,$$

der *Zentralisator von x in G.*

Bemerkung 21.10.

(i) Wir nehmen an: G operiert auf S. Seien $x, y \in S$ und $g \in G$. Es gilt:

$$y = gx \Rightarrow Stab_x = g^{-1}(Stab_y)g .$$

(ii) Es folgt: wenn G auf S transitiv operiert, dann gilt:

$$\forall x, y \in S \exists g \in G : Stab_y = g(Stab_x)g^{-1} .$$

Beweis: ÜA □

Beispiel 21.11. [**Transitive Aktion:**]
Sei $H \leq G$ und setze $\overline{G} := \{xH \mid x \in G\}$ die menge der linken Nebenklassen von H in G. Dann operiert G auf $\overline{G}$ durch linke Multiplikation: $g(xH) := (gx)H$. Die Aktion ist transitiv: seien xH und $yH \in \overline{G}$, setze $g = yx^{-1}$. Dann ist $g(xH) = (gx)H = (yx^{-1}x)H = yH$.

Wir zeigen nun, dass bis auf Äquivalenz von Aktionen, alle transitive Aktionen von G auf eine Menge $S \neq \varnothing$ diese Gestalt haben:

Satz 21.12.
Wir nehmen an dass G transitiv auf S operiert. Sei $s \in S$ fest und setze $H := Stab_s$. Dann ist die angegebene transitive Aktion von G auf S äquivalent zur Aktion von G auf $\overline{G} := \{xH \mid x \in G\}$ durch linke Multiplikation.

Beweis:
Definierte $\nu : \overline{G} \to S$ mit $\nu(xH) := xs$. Laut Definition 20.7 müssen wir Folgendes prüfen:

- ν ist wohldefiniert weil $xH = yH$ gdw $y^{-1}x \in H$ gdw $(y^{-1}x)s = s$ gdw $xs = ys$ (*)
- Die Aktion ist transitiv $\Rightarrow \nu$ ist surjektiv.
- ν ist injektiv (auch wegen (*)).
- Wir berechnen: $\nu(g(xH)) = \nu((gx)H) = (gx)s = g(xs) = g\nu(xH)$.

□

Korollar 21.13.
Es sei G eine endliche Gruppe und $S \neq \varnothing$ eine Menge so dass G auf S transitiv operiert. Dann ist $|S| = [G : Stab_s]$ für ein (jedes) $s \in S$. Insbesondere ist S endlich und $|S| \mid |G|$.

Beweis:
Es folgt nun aus Satz 21.12 und Satz 16.2. □

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

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir die Bahn Gleichung und die Sylow Sätze beweisen. Damit beenden wir Kapitel 3.

Seien $S \neq \varnothing$ eine Menge, G eine Gruppe, so dass G auf S operiert.

Wir wollen nun Korollar 21.13 für eine beliebige Aktion verallgemeinern:

Korollar 22.1. [Bahngleichung]
Sei S endlich; wähle ein Vertretersystem $\{x_1, \ldots, x_r\}$ der Bahnen. Es gilt

$$|S| = \sum_{i=1}^{r} [G : Stab_{x_i}] .$$

Beweis:
Seien $\mathcal{O}_1, \ldots, \mathcal{O}_r$ alle Bahnen. Es ist leicht zu sehen (s. Bemerkung 21.4), dass die Aktion von G auf $\mathcal{O}_i$ transitiv ist für jedes $i = 1, \ldots, r$. Es folgt aus Korollar 21.13 dass $|\mathcal{O}_i| = [G : Stab_{x_i}]$. Nun ist $S = \bigsqcup_{i=1}^{r} \mathcal{O}_i$, also $|S| = \sum_{i=1}^{r} |\mathcal{O}_i|$. □

Korollar 22.2. [Klassengleichung I]
Sei G endlich; wähle ein Vertretersystem $\{x_1, \ldots, x_k\}$ der Konjugationsklassen von G. Es gilt

$$|G| = \sum_{i=1}^{k} [G : C(x_i)] .$$

Beweis:
G operiert auf G durch die Konjugation κ_j und $Stab_{x_i} = C(x_i)$ per Definition 21.9. Wir können Korollar 22.1 also direkt anwenden. □

Korollar 22.3. [Klassengleichung II]
Sei G endlich; wähle ein Vertretersystem $\{y_1, \ldots, y_\ell\}$ für die Konjugationsklassen in $G \backslash C_G$. Es gilt:

$$|G| = |C_G| + \sum_{i=1}^{\ell} [G : C(y_i)] \qquad (*)$$

Beweis:
Die Konjugationsklasse von x ist $\{x\}$ gdw $x \in C_G$ genau dann, wenn $C(x) = G \quad (**)$
(s. Proposition 21.8). In Korollar 22.2 wird also in der Formel $1 = [G : G] = [G : C(x_i)]$ so oft summiert wie es Elemente in C_G gibt. Also erhalten wir $|C_G|$ als ersten Summand. □

Korollar 22.4.
Sei G endlich, $|G| = p^k, p$ ist Primzahl und $k \in \mathbb{N}$. Es gilt $C_G \neq \{1\}$.

Beweis: Siehe ÜB.

Proposition 22.5. Sei G eine endliche abelsche Gruppe, $p \in \mathbb{N}$ eine Primzahl und $p \mid |G|$. Dann existiert ein $x \in G$ mit $|x| = p$.

Beweis: Siehe ÜB.

Beweise der Sylow-Sätze.

Beweis von Sylow 1:
Sei p Primzahl und $k \in \mathbb{N}$, so dass $p^k \mid |G|$. Wir werden per Induktion nach $|G|$ zeigen dass G eine Teilgruppe H der Ordnung p^k hat.

• $|G| = 2$ ist klar.

• Induktionsannahme: Sylow 1 gilt für alle Gruppen der Ordnung $< |G|$.

• Induktionsschritt: Wir werden Lagrange's Satz, die Klassengleichung II, und Proposition 22.5 (für die abelsche Gruppe $C := C_G$) anwenden.

Zwei Fälle sind zu betrachten:

Fall 1: $p \nmid |C|$. In diesem Fall wegen $(*)$ $\exists j$ mit $p \nmid [G : C(y_j)]$.
Aber $p^k \mid |G|$ und $|G| = [G : C(y_j)] \mid C(y_j) \mid$.
Also $p^k \mid |C(y_j)|$. Wegen $(**)$ ist $|C(y_j)| < |G|$, da $y_j \notin C$ ist.
Induktionsannahme $\Rightarrow C(y_j)$ besitzt eine Teilgruppe der Ordnung p^k. $\square_{Fall1}$

Fall 2: $p \mid |C|$. In diesem Fall liefert Proposition 22.5 ein Element $c \in C$ der Ordnung p.
Nun ist $< c > \trianglelefteq C, | < c > | = p$. Betrachte die Gruppe $G/ < c >$ der Ordnung $\frac{|G|}{|<c>|} = \frac{|G|}{p}$.
Also $p^{k-1} \mid |\frac{G}{<c>}|$. Induktionsannahme $\Rightarrow \exists$ eine Teilgruppe von $G/ < c >$ der Ordnung p^{k-1}.

Nun haben wegen Satz 17.4 die Teilgruppen von $G/ < c >$ die Gestalt $H/ < c >$, wobei $H \leq G$ und $< c > \leq H$. Also existiert $H \leq G$ mit $|\frac{H}{<c>}| = p^{k-1}$. Wir berechnen:
$|H| = |\frac{H}{<c>}| \ | < c > | = p^{k-1} \, p = p^k$. $\square_{Fall2}$ $\square_{Sylow1}$

Wir wollen nun Sylow 2 beweisen.

Bemerkung 22.6. Sei $H \leq G$ und $g \in G$. Dann ist $gHg^{-1} \leq G$. G operiert also durch Konjugation auf $\Gamma :=$ die Menge der Teilgruppen von G. Wir müssen diese Aktion besser verstehen. Für $H \in \Gamma$ berechnen wir:

(i) $Stab_H = \{g \in G \,;\, gHg^{-1} = H\}$. Somit erkennen wir dass $Stab_H = N_G(H)$ der Normalisator von H in G (s. Definition 16.8). Zur Erleichterung der Notation schreiben wir hier $N(H)$ anstatt $N_G(H)$. Wir erinnern dass $H \trianglelefteq N(H)$ (s. Bemerkung 17.1).

(ii) Die Bahnn von H : $\mathcal{O}_H = \{gHg^{-1} \ ; \ g \in G\}$. Korollar 21.13 liefert $|\mathcal{O}_H| = [G : N(H)]$. Da $[G : H] = [G : N(H)][N(H) : H]$, so ist $|\mathcal{O}_H| \mid [G : H]$.

(iii) Wir betrachten diese Aktion auf die Mengen $\Pi \subseteq \Gamma$ der Sylow-p-Untergruppen von G. Die Aktion auf Π ist wohldefiniert, weil $gHg^{-1} \in \Pi$, wenn $H \in \Pi$. (s. Bemerkung 21.4)

Wir bekommen ein Hilfslemma.

Lemma 22.7. (i) Sei $P \in \Pi, H \leq N(P)$ so dass $|H| = p^j$ für ein $j \in \mathbb{N}$. Dann ist $H \leq P$.

(ii) P ist die einzige Sylow-p-Untergruppe von $N(P)$.

Beweis:

$$\left.\begin{array}{ll} H \leq N(P) & \text{und} \\ P \trianglelefteq N(P) & \end{array}\right\} \Rightarrow HP \text{ ist Untergruppe und } HP/P \simeq H/(H \cap P)$$

(Isomorphie-Satz 17.2). Also ist HP/P isomorph zu einer Faktorgruppe von H und damit hat sie die Ordnung $|HP| = p^k$ für ein geeignetes $k \in \mathbb{N}$. Da aber P eine Sylow-p-Untergruppe ist, folgt: $HP = P$, so dass $H \leq P$. Damit haben wir (i) bewiesen, (ii) folgt unmittelbar aus (i). □

Beweis von Sylow 2:
Betrachte eine Bahn $\sum$ für die Aktion in Bemerkung 22.6. Sei $P \in \Pi$, dann operiert P auf die Bahn $\sum$ (s. Bemerkung 21.4). Wir bekommen eine Partition von $\sum$ in P-Bahnen (i.e. Äquivalenzklassen bezüglich dieser Aktion von P auf $\sum$).

Fall 1: Sei $P \in \sum$.

- Betrachte die P-Bahn von P. Die ist offensichtlich $\{P\}$ (weil $xPx^{-1} = P$ für alle $x \in P$).
- Wir behaupten, dass $\{P\}$ die einzige P-Bahn der Kardinalität 1 ist:
  Sei $\{P'\}$ eine P-Bahn. Dann gilt $xP'x^{-1} = P'$ für alle $x \in P$, das heißt $P \leq N(P')$ und Lemma 22.7(ii) liefert $P = P'$ (weil P' die einzige Sylow-p-Untergruppe von $N(P')$ ist und P ist eine Sylow-p-Untergruppe von $N(P')$).
- Beachte, dass jede P-Bahn Kardinalität eine Potenz von p hat, da diese Kardinalität die Kardinalität $|P|$ teilen muss (siehe Korollar 21.13). Also ist $|\sum| \equiv 1 \mod p$.

Dieses beweist die zweite Aussage von Sylow 2 (2).

Nun beweisen wir Sylow 2 (1). Wir müssen zeigen, dass $\sum$ die einzige Bahn für die Aktion in Bemerkung 22.6. Sonst gibt es $P \in \Pi$ mit

Fall 2: $P \notin \sum$.

Analog wie Fall 1 sehen wir, dass es überhaupt keine P-Bahnen der Kardinalität 1 gibt (die einzige Möglichkeit, nämlich $\{P\}$ scheidet nun aus, weil $P \notin \sum$ ist). Also ist $|\sum| \equiv 0 \mod p$ - Widerspruch. So $\sum = \Pi$ und damit ist Sylow 2 (1) bewiesen.

Es ist $|\Pi| = [G : N(P)]$ für alle $P \in \Pi$ (Korollar 21.13). Also ist die Anzahl der Sylow-p-Untergruppen ein Divisor (s. Bemerkung 22.6). Das beweist die erste Aussage in Sylow 2 (2).

Nun beweisen wir Sylow 2 (3). Sei $H \leq G, |H| = p^k$. Betrachte die Aktion von H auf Π. Die H-Bahnen haben Kardinalität ein Divisor von $|H|$ (Korollar 21.13), also haben die H-Bahnen Kardinalität eine Potenz von p.
Nun ist aber $|\Pi| \equiv 1 \mod p$, also gibt es eine H-Bahn $\{P\}$ mit nur einem Element, das heißt $H \leq N(P)$ und damit $H \leq P$ (s. Lemma 22.7 (i)). □

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).

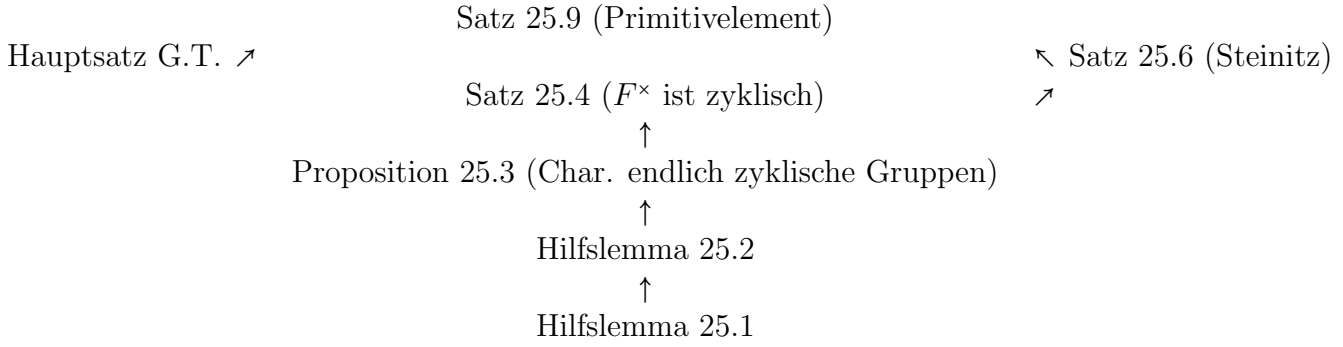
Umgekehrt: Sei K/F normal. Sei $a \in K$ und $f(x)$ sein Minimalpolynom, $f(x)$ zerfällt in Linearfaktoren über $K[x]$. Dann ist $f(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$ in $K[x]$ mit $a = a_1$.
Sei $\eta \in G$, dann ist $0 = \eta(f(a)) = f(\eta(a))$. Also ist $\eta(a)$ eine Nullstelle und somit existiert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