

**Inhaltsverzeichnis zur Vorlesung: Algebra (BIII)**  
**Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont**  
**WS 2012/2013**

**Kapitel 1 Ringe**

1. Vorlesung	22. Oktober 2012	Seite	1
2. Vorlesung	25. Oktober 2012	Seite	5
3. Vorlesung	29. Oktober 2012	Seite	8
4. Vorlesung	05. November 2012	Seite	11
5. Vorlesung	08. November 2012	Seite	14
6. Vorlesung	12. November 2012	Seite	18
7. Vorlesung	15. November 2012	Seite	21

**Kapitel 2 Körpererweiterungen**

7. Vorlesung	15. November 2012	Seite	25
8. Vorlesung	18. November 2012	Seite	30
9. Vorlesung	22. November 2012	Seite	30
10. Vorlesung	26. November 2012	Seite	33
11. Vorlesung	29. November 2012	Seite	37
12. Vorlesung	03. Dezember 2012	Seite	39
13. Vorlesung	10. Dezember 2012	Seite	43

**Kapitel 3 Gruppen**

13. Vorlesung	10. Dezember 2012	Seite	43
14. Vorlesung	13. Dezember 2012	Seite	47
15. Vorlesung	17. Dezember 2012	Seite	51
16. Vorlesung	20. Dezember 2012	Seite	54
17. Vorlesung	7. Januar 2013	Seite	58
18. Vorlesung	10. Januar 2013	Seite	63
19. Vorlesung	14. Januar 2013	Seite	70
20. Vorlesung	17. Januar 2013	Seite	72

**Kapitel 4 Galoistheorie**

20. Vorlesung	17. Januar 2013	Seite	72
21. Vorlesung	21. Januar 2013	Seite	75
22. Vorlesung	24. Januar 2013	Seite	78
23. Vorlesung	28. Januar 2013	Seite	81
24. Vorlesung	31. Januar 2013	Seite	83
25. Vorlesung	4. Februar 2013	Seite	86
26. Vorlesung	7. Februar 2013	Seite	92
27. Vorlesung	11. Februar 2013	Seite	94
28. Vorlesung	14. Februar 2013	Seite	97

## 1. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 22. Oktober 2012

### Kapitel 1

Faktorringer, Homomorphismen, Ideale, Ringe von Brüchen, Quotientenkörper,  
Lokalisierung, Chinesischer Reste-Satz, Euklidische und Hauptideal Ringe,  
Faktorielle Ringe, Polynom-Ringe, Irreduzibilitätskriterien

Alle Ringe in dieser Vorlesung sind kommutativ mit  $1 \neq 0$ .

#### Erinnerungen

Sei  $R$  ein Ring.

- (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) Ein endlicher Integritätsbereich ist ein Körper (siehe Übungsblatt 1, Aufgabe 1.4 (b)).
- (4)  $u \in R$  ist eine *Einheit*, wenn es ein  $v \in R$  gibt mit  $uv = 1$ .

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

#### Proposition

$R^\times$  ist eine multiplikative Gruppe.

#### Beispiele

$\mathbb{Z}_n^\times = U(n)$  (Übungsblatt 3, Aufgabe 2b aus Lineare Algebra 1)

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

Euler  $\varphi$ -Funktion:  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$

$\varphi(n) := |U(n)|$ .

Siehe Übungsblatt für eine ausführliche Ausarbeitung der Eigenschaften von  $\varphi$ :

- (1)  $\varphi(p^v) = p^v - p^{v-1}$  für  $p$  Primzahl und  $v \in \mathbb{N}$
- (2)  $\varphi$  ist eine multiplikative arithmetische Funktion i.e.  $\varphi(ab) = \varphi(a)\varphi(b)$ ,  
wenn  $\text{ggT}(a, b) = 1$ .

**Definition**

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

(2) Seien  $R, S$  Ringe.  $\varphi : R \rightarrow S$  ist ein *Ringhomomorphismus*, wenn  
 $\varphi(1_R) = 1_S$ ,  $\varphi(a + b) = \varphi(a) + \varphi(b)$ ,  $\varphi(ab) = \varphi(a)\varphi(b)$ .

**Notation:**

$$\ker \varphi := \{x \in R; \varphi(x) = 0\}$$

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

(3) Ein *Ringisomorphismus* ist ein bijektiver Ringhomomorphismus.

**Notation:**  $\varphi : R \simeq S$  oder  $R \stackrel{\varphi}{\simeq} S$  oder  $R \cong S$ .

**Bemerkung**

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

**Beispiel**

Sei  $n \in \mathbb{N}$

**Notation**

$a \in \mathbb{Z}; \bar{a} := \text{Rest nach Division durch } n$ .

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n$$

$$a \mapsto \bar{a}$$

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

(siehe Lineare Algebra 1, 2. Vorlesung).

**Definition**

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

**Notation:**  $I \triangleleft R$

**Beispiele**

$$I = R \quad \text{und} \quad I = \{0\}$$

**Terminologie**

$I \triangleleft R$  und  $I \neq R$  heißt *echtes Ideal*.

$I \triangleleft R$  und  $I \neq \{0\}$  heißt *nicht triviales Ideal*.

**Proposition**

Sei  $\varphi : R \rightarrow S$  ein Ringhomomorphismus. Es gelten:

(1)  $\text{im } \varphi$  ist ein Teilring von  $S$ .

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

**Faktoring**

Sei  $I \triangleleft R$ .  $R/I := \{x + I \mid x \in R\}$  die Menge der *Nebenklassen von  $R$  modulo  $I$*  (siehe Übungsblatt 1, Aufgabe 1.2) (also der Äquivalenzklassen  $[x]$  bezüglich  $x \sim y \pmod I$  genau dann, wenn  $x - y \in I$ ).

**Proposition**

$R/I$  ist ein Ring mit den Ringoperationen

$$(r + I) + (s + I) := (r + s) + I \text{ und}$$

$$(r + I) \cdot (s + I) := (rs) + I$$

für alle  $r, s \in R$  (Übungsblatt 1, Aufgabe 1.2).

**Definition**

$R/I$  ist der *Faktoring* " $R$  modulo  $I$ ".

**Satz** (Isomorphiesatz für Ringe)

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

(2) Umgekehrt: Ist  $I \triangleleft R$ , dann ist

$$\pi : R \rightarrow R/I$$

$$r \mapsto r + I$$

ein surjektiver Ringhomomorphismus mit  $\ker \pi = I$  ( $\pi$  ist die *kanonische Projektion*).

Also sind die Ideale genau die Kerne von Ringhomomorphismen.

**Beweis**

**Behauptung** die Abbildung von (1)

$$\Phi : R/I \rightarrow \varphi(R)$$

$$x + I \mapsto \varphi(x)$$

ist wohldefiniert (i.e.  $x + I = y + I$  impliziert  $\varphi(x) = \varphi(y)$ ).

Es ist klar, dass  $\Phi$  surjektiv und ein Ringhomomorphismus ist. Wir berechnen  $\ker \Phi$ .

$$\Phi(x + I) = 0 \Leftrightarrow \varphi(x) = 0 \Leftrightarrow x \in \ker \varphi \Leftrightarrow x \in I \Leftrightarrow x + I = 0 + I;$$

somit ist  $\ker \Phi = \{0 + I\}$  (das Nullelement der Faktoring  $R/I$ ).

Beweis von (2) analog. □

**Beispiel**

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$$

**Korollar 1**

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

**Beweis**

Die Abbildung

$$\begin{aligned} \Phi : R/I &\rightarrow R/J \\ x + I &\mapsto x + J \end{aligned}$$

ist ein surjektiver Ringhomomorphismus mit  $\ker \Phi = J/I$ . □

## 2. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 25. Oktober 2012

### Korollar

Sei  $I \triangleleft R$ . Betrachte die Teilringe  $A$  von  $R$  mit  $I \subseteq A \subseteq R$  einerseits und die Teilringe von  $R/I$  andererseits.

Die Abbildung

$$A \mapsto A/I$$

ist bijektiv und respektiert Inklusion. Ferner gilt für  $I \subseteq A \subseteq R$ , dass  $A \triangleleft R$  genau dann, wenn  $A/I \triangleleft R/I$ .

### Beweis

Siehe Übungsblatt 2. □

### Notation

$x + I$  wird manchmal auch als  $\bar{x}$  geschrieben.

### Definition

Sei  $A \subseteq R$  eine beliebige Teilmenge. Das *von  $A$  erzeugte Ideal* ist das kleinste Ideal, das  $A$  enthält (und wird mit  $\langle A \rangle$  bezeichnet), e.g.  $\langle \emptyset \rangle = \{0\}$ .

### Bemerkung (Übungsaufgabe)

$$\langle A \rangle = \bigcap \{A \subseteq J \triangleleft R\}$$

(ist der Durchschnitt aller Ideale, die  $A$  enthalten) und außerdem ist

$$\langle A \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid n \in \mathbb{N}; r_i \in R; a_i \in A \right\}$$

(also die Menge aller  $R$ -Linearkombinationen aus endlichen Elementen von  $A$ ).

Konvention: Wenn  $A = \{a_1, \dots, a_l\}$  endlich ist, so schreiben wir einfach  $\langle a_1, \dots, a_l \rangle$ .

### Definition

Sei  $a \in R$ .  $\langle a \rangle = \{ra; r \in R\}$  heißt *Hauptideal*, das von  $a$  erzeugt ist.

### Beispiel

$\langle 1 \rangle = R$  und  $\langle 0 \rangle = \{0\}$ .

**Proposition**Sei  $I \triangleleft R$ 

- (1)  $I = R$  genau dann, wenn  $I \cap R^\times \neq \emptyset$
- (2)  $R$  ist ein Körper genau dann, wenn die einzigen Ideale  $R$  und  $\{0\}$  sind.

**Beweis**(1) " $\Rightarrow$ " trivial

$$\begin{array}{lcl}
 u \in I & \Rightarrow & u^{-1}u \in I \Rightarrow 1 \in I \\
 \text{"}\Leftarrow\text{"} & & \uparrow \\
 \text{Einheit} & R & \Rightarrow r \cdot 1 \in I \forall r \in R
 \end{array}$$

(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  $\langle x \rangle = R$ , d.h.  $1 \in \langle x \rangle$ , also existiert ein  $r \in R$  mit  $rx = 1$ , also  $r = x^{-1}$  □

**Korollar**

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

**Beweis** $\ker \varphi = \{0\}$ . □**Definition** $M \triangleleft R$  ist *maximal*, wenn

- (i)  $M \neq R$  ( $M$  ist echt).
- (ii) Ist  $I \triangleleft R$  mit  $M \subseteq I \subseteq R$ ,

dann gilt:  $I = M$  oder  $I = R$ . (Also gibt es keine weiteren Ideale zwischen  $M$  und  $R$ .)**Proposition**

Jedes echte Ideal ist in einem Maximalideal enthalten.

Wir brauchen Zorn's Lemma.

**Exkurs Partielle Ordnung**

Sei  $A \neq \emptyset$  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  $A \neq \emptyset$  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.

**Beweis der Proposition**

Sei  $I \triangleleft R$ ,  $I \subsetneq R$ . Betrachte

$S :=$  die Menge aller echten Ideale von  $R$ , die in  $I$  enthalten sind.

$I \in S$ , so  $S \neq \emptyset$ .

$S$  ist partiell geordnet durch Mengeneinklusion. 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  $\xi$  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 Elemente. Wenn  $M$  ein solches ist, dann ist klar, dass  $M$  ein maximales Ideal ist, welches  $I$  enthält, wie behauptet.  $\square$



### 3. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 29. Oktober 2012

(Korrekturen vom 28. Januar 2016)

#### Proposition

$M \triangleleft R$  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 erste Proposition aus der 2. Vorlesung anwenden.  $\square$

#### Beispiel

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

#### Definition

$P \triangleleft R$  ist ein Primideal, wenn

- (1)  $P$  echt ist, u.i.e.  $P \subsetneq R$ .
- (2) Aus  $ab \in P$  ( $a, b \in R$ ) folgt  $a \in P$  oder  $b \in P$ .

#### Beispiel

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

#### Proposition

$P \triangleleft R$  ist Primideal genau dann, wenn  $R/P$  ein Integritätsbereich ist.

#### Beweis

seien  $a, b \in R$  und  $P \triangleleft R$ . Dann ist  $P$  Primideal genau dann, wenn  $[\overline{ab} = \overline{a}\overline{b} = 0 \Rightarrow \overline{a} = \overline{0}$  oder  $\overline{b} = \overline{0}]$  ( $\overline{a} = \overline{0}$  bedeutet  $a \in P$ ) genau dann, wenn  $R/P$  integer ist.  $\square$

**Korollar**

Jedes maximale Ideal ist Primideal.

**Definition**

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

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

$R \times S$  heißt *Ringprodukt*.

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

**Satz (Chinesischer Reste-Satz)**

Seien  $A_1, \dots, A_k \triangleleft R$ . Die Abbildung

$$\begin{aligned} \varphi : R &\rightarrow \prod_{i=1}^k (R/A_i) \\ r &\mapsto (r + A_1, \dots, r + A_k) \end{aligned}$$

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  $\varphi$  surjektiv. In diesem Fall gilt also (Isomorphiesatz):

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

**Beweis**

Ohne Einschränkung  $k = 2$ . Prüfe, ob  $\varphi(r_1 + r_2) \stackrel{?}{=} \varphi(r_1) + \varphi(r_2)$ .

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

usw.

Also ist  $\varphi$  ein Ringhomomorphismus.

$$\begin{aligned} \ker \varphi &= \{r | \varphi(r) = 0\} \\ &= \{r | \varphi(r) = (A_1, A_2)\} \\ &= \{r | r \in A_1 \text{ und } r \in A_2\}. \end{aligned}$$

Sei nun  $A_1 + A_2 = R$ . Also existieren  $x \in A_1$  und  $y \in A_2$  mit  $x + y = 1$ , insbesondere  $\varphi(x) = (0, 1)$  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  $r := r_2x + r_1y$  und berechne:

$$\begin{aligned}\varphi(r) &= \varphi(r_2x + r_1y) \\ &= \varphi(r_2)\varphi(x) + \varphi(r_1)\varphi(y) \\ &= (r_2 + A_1, r_2 + A_2)(0, 1) + (r_1 + A_1, r_1 + A_2)(1, 0) \\ &= (0, r_2 + A_2) + (r_1 + A_1, 0) \\ &= (r_1 + A_1, r_2 + A_2).\end{aligned}$$

Also ist  $\varphi$  surjektiv. □

## Bruchringe

### Definition

$D \subseteq R$  ist multiplikativ, falls  $1 \in D$  und  $st \in D$  für alle  $s, t \in D$ .

### Beispiele

(i)  $D = R^\times$

(ii)  $D = R \setminus P$  mit  $P \triangleleft R$  Prim.

Sei nun  $D$  multiplikativ, ohne Nullteiler  $0 \notin D$ . Definiere eine Relation  $\sim$  auf  $R \times D$ :

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

$\sim$  ist Äquivalenzrelation

$$\left. \begin{array}{l} \text{(e.g. } (r, d) \sim (s, e) \\ \text{und } (s, e) \sim (t, f) \end{array} \right| \Rightarrow + \begin{array}{l} re - sd = 0 \\ sf - te = 0 \end{array} \left| \begin{array}{l} \times f \\ \times d \end{array} \right. \text{ ergibt } (rf - td)e = 0,$$

$e$  ist kein Nullteiler  $e \neq 0$ . 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.

Versehe  $D^{-1}R$  mit den folgenden Ringoperationen:

$$\frac{r_1}{d_1} + \frac{r_2}{d_2} := \frac{r_1d_2 + r_2d_1}{d_1d_2} \quad \text{und} \quad \frac{r_1}{d_1} \cdot \frac{r_2}{d_2} := \frac{r_1r_2}{d_1d_2}.$$

## 4. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 5. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

**Behauptung** $D^{-1}R$  ist ein Ring mit Null  $\frac{0}{1}$  und Eins  $\frac{1}{1}$ .**Beweis**

Wir zeigen zum Beispiel, dass die Addition wohldefiniert ist.

Zu zeigen:  $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ .

Seien

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{und} \quad \frac{c}{d} = \frac{c'}{d'}$$

 $\Downarrow$ 

$$ab' = a'b$$

 $\Downarrow$ 

$$cd' = c'd$$

$$(ad+bc)b'd' \stackrel{?}{=} (a'd'+b'c')(bd)$$

berechne

berechne

||

||

$$\underline{ab'dd'} + \underline{cd'bb'} = \underline{a'bdd'} + \underline{c'dbb'}$$

usw....

□

**Behauptung**

Die Abbildung

$$i: R \rightarrow D^{-1}R$$

$$r \mapsto \frac{r}{1}$$

definiert einen injektiven Ringhomomorphismus.

**Beweis**

$$i(r) = 0 \Leftrightarrow \frac{r}{1} = \frac{0}{1} \Leftrightarrow r = 0$$

□

**Behauptung**

$$i(D) \subset (D^{-1}R)^\times.$$

**Beweis**

$$d \in D; i(d) = \frac{d}{1} \text{ und damit } [i(d)]^{-1} = \frac{1}{d}$$

□

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

**Beispiel 1**

$R$  ist integer  $\Rightarrow D := R \setminus \{0\}$  erfüllt  $(*)$  und so ist  $D^{-1}R$  ein Körper, den wir mit  $\text{Quot}(R)$  bezeichnen.

Wir identifizieren  $R$  mit  $i(R)$  (i.e.  $r$  mit  $\frac{r}{1}$  für alle  $r \in R$ ).

Wir haben erreicht: Jeder Integritätsbereich lässt sich in einen Körper einbetten.

(Erinnerung: Ein injektiver Ringhomomorphismus heißt eine Einbettung.)

**Korollar**

Der Ring  $R$  lässt sich in einen Körper einbetten genau dann, wenn er integer ist.

**Beispiel 1**

$$(a) \text{Quot}(\mathbb{Z}) = \mathbb{Q}$$

$$(b) \text{Quot}(K[x]) := K(x)$$

der rationale Funktionenkörper einer Variablen über den Körper  $K$ .

**Beispiel 2**

$P$  ist ein Primideal;  $D = R \setminus P$ .

$R_P = D^{-1}R$  ist die Lokalisierung von  $R$  nach  $P$ .

**Zu Beispiel 1 (b):** Polynomringe über Ringe

Sei  $R$  ein kommutativer Ring mit Eins.

$$R[x] := \{p(x) \mid p(x) \text{ Polynom über } R\}$$

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$n \in \mathbb{N}_0 \begin{cases} 0 \neq a_n & := \text{Leitkoeffizient} \\ \deg p & := n \end{cases}$$

Addition: Koordinatenweise (koeffizientenweise)

Multiplikation: Wenn

$$p(x) = \sum a_i x^i \quad \text{und} \quad q(x) = \sum b_j x^j,$$

so ist der Koeffizient von  $x^k$  im Produkt  $p(x)q(x)$  gleich  $\sum_{i=0}^k a_i b_{k-i}$ .

**Bemerkungen:**

$R \subseteq R[x]$  als Teilring der konstanten Polynome (i.e. Polynome  $p$  mit  $\deg p = 0$ ).

**Frage**

Wann ist  $a_m b_m$  Leitkoeffizient vom Produkt  $p(x)q(x)$ ?

**Korollar**

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

**Beweis**

“ $\Leftarrow$ ” Ein Teilring von einem Integritätsbereich ist integer.

“ $\Rightarrow$ ” Sei  $a_n \neq 0$  und  $b_m \neq 0$  für  $p(x) = a_n x^n + \dots + a_0$  und  $q(x) = b_m x^m + \dots + b_0$ , 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.  $\square$

**Beispiel**

Sei  $R$  ein Ring. Betrachte die Abbildung

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

Dann ist  $ev_0$  ein surjektiver Ringhomomorphismus mit  $\ker ev_0 :=$  die Menge der Polynome mit konstantem Term gleich Null.

Also ist  $R[x]/\langle x \rangle \simeq R$ , wobei  $\ker ev_0 = \langle x \rangle = \{xf(x); f(x) \in R[x]\}$

Sei nun  $R = \mathbb{Z}$ , so ist  $\mathbb{Z}[x]/\langle x \rangle \simeq \mathbb{Z}$ .

Wir sehen also:  $\langle x \rangle$  ist ein Primideal in  $\mathbb{Z}[x]$ , aber ist nicht maximal !

## 5. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 8. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### Euklidische Bereiche

#### Definition

- (1) Eine Abbildung  $N : R \rightarrow \mathbb{N}_0$  heißt *Norm*.
- (2) Der Integritätsbereich  $R$  (mit der Norm  $N$  versehen) heißt *euklidisch*, wenn für alle  $a, b \in R$  mit  $b \neq 0$   $q, r \in R$  existieren, so dass  $a = qb + r$ , wobei  $r = 0$  oder  $N(r) < N(b)$ .

**Abkürzung:**  $R$  ist E.R.

#### Beispiele

- (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 Übungsblatt 3.

#### Proposition

Sei  $R$  ein euklidischer Integritätsbereich,  $I \triangleleft R$ , dann ist  $I$  ein Hauptideal.

#### Beweis

Sei  $I \neq \{0\}$  und  $0 \neq d \in I$  mit  $N(d)$  minimal. Es ist klar, dass  $\langle d \rangle \subseteq I$  (siehe (i) unten bei Definition).

Umgekehrt: Sei  $a \in I$  und  $q, r \in R$  mit  $a = qd + r$   $r = 0$  oder  $N(r) < N(d)$ .

Nun ist aber  $r = a - qd \in I$ , also  $N(r) < N(d)$  unmöglich.

Also  $r = 0$  und somit  $a = qd \in \langle d \rangle$ . □

**Teilbarkeit****Definition**

$a, b \in R; b \neq 0$

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

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

(a)  $d|a$  und  $d|b$ , und für  $d' \in R$  gilt:

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

**Bemerkungen**

(i)  $b|a$  genau dann, wenn  $a \in \langle b \rangle$  genau dann, wenn  $\langle a \rangle \subseteq \langle b \rangle$

(ii)  $d$  ist ggT von  $a, b$ , falls  $\langle a, b \rangle \subseteq \langle d \rangle$  und aus  $\langle a, b \rangle \subseteq \langle d' \rangle$  folgt  $\langle d \rangle \subseteq \langle d' \rangle$  (für alle  $d' \in R$ ).

Wir bekommen damit eine hinreichende Bedingung für die  $\exists^Z$  eines ggT:

**Proposition 2**

Ist  $\langle a, b \rangle$  ein Hauptideal, u.e.  $\langle a, b \rangle = \langle d \rangle$ , dann ist  $d$  ein ggT von  $a$  und  $b$ .

**Definition**

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

**Proposition** (Eindeutigkeit bis auf Einheiten)

Sei  $R$  integer,  $d, d' \in R$  und  $a, b \in R$ .

Es gilt:  $\langle d \rangle = \langle d' \rangle$  genau dann, wenn  $d' = ud$  mit  $u \in R^\times$ .

Insbesondere alle ggT von  $a, b$  sind zueinander assoziiert.

**Beweis**

“ $\Leftarrow$ ”  $d' = ud \Leftrightarrow d = d'u^{-1}$  mit  $u \in R^\times$ . Also  $d' = ud \Rightarrow d' \in \langle d \rangle \Rightarrow \langle d' \rangle \subseteq \langle d \rangle$  und umgekehrt aus  $d = d'u^{-1}$  folgt auch  $\langle d \rangle \subseteq \langle d' \rangle$ .

“ $\Rightarrow$ ” Seien  $d, d' \neq 0$  und  $\langle d \rangle = \langle d' \rangle$ . Also

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

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



Eine wichtige Eigenschaft von E.R. ist der  
**Algorithmus zum Berechnen von ggT:**

Seien  $a, b \in R, b \neq 0$

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$\vdots$

$$r_{n-2} = q_n r_{n-1} + r_n \quad r_n \neq 0$$

$$r_{n-1} = q_{n+1} r_n$$

$$\underbrace{N(b) > N(r_0) > \dots > N(r_{n-1}) > N(r_n) > 0}_{\text{endlich viele Schritte im Abstieg !}}$$

Wir fassen zusammen:

### Satz

Sei  $R \in D; a, b \in R \neq 0$  und  $d = r_n$  (wie oben), so ist

- (1)  $d$  ein ggT von  $a$  und  $b$
- (2)  $d = ax + by$  für geeignete  $x, y \in R$ .

## Hauptidealbereiche

### Definition

Ein *Hauptidealbereich* ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

**Abkürzung:** H.I.R.

### Proposition 4

Sei  $R$  ein Hauptidealbereich,  $a, b \neq 0, a, b \in R$  und  $d$  ein Erzeuger von  $\langle a, b \rangle$ . 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

Siehe Proposition 2

□

**Proposition 5**

Jedes Primideal in einem Hauptidealbereich ist auch maximal.

**Beweis**

Sei  $\langle p \rangle \neq \{0\}$  Primideal und  $M \supseteq \langle p \rangle = M$  maximal (wir wissen  $M$  existiert!). Nun ist auch  $M = \langle m \rangle$  ein Hauptideal;  $p \in \langle m \rangle$  also existiert  $r \in R$  mit  $p = rm$ .

Aber  $\langle p \rangle$  prim  $\Rightarrow r \in \langle p \rangle$  oder  $m \in \langle p \rangle$ .

1. Fall:  $m \in \langle p \rangle \Rightarrow \langle m \rangle \subseteq \langle p \rangle \Rightarrow \langle p \rangle = M$

2. Fall:  $r \in \langle p \rangle \Rightarrow r = ps \Rightarrow p = rm = psm$  oder  $sm = 1$ .

Somit ist aber  $m \in R^\times$ . Das widerspricht, dass  $M$  maximal (also echt) ist.  $\square$

**Beispiele**

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

(2)  $\mathbb{Z}[x]$  ist kein Hauptidealbereich, weil  $\langle x \rangle$  prim, aber nicht maximal ist.

Wir verallgemeinern: Sei  $R$  integer. Es gilt:

**Korollar**

$R[x]$  ist ein Hauptidealbereich genau dann, wenn  $R$  ein Körper ist.

**Beweis**

" $\Leftarrow$ "  $R$  ist ein Körper  $\Rightarrow R[x]$  ist E.R.  $\Rightarrow R[x]$  ist H.I.R.

" $\Rightarrow$ "  $R[x]/\langle x \rangle \cong R$ ,  $\langle x \rangle$  Primideal.

Nun  $R[x]$  Hauptidealbereich  $\Rightarrow \langle x \rangle$  maximales Ideal  $\Rightarrow R[x]/\langle x \rangle$  ist ein Körper.  $\square$

## 6. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 12. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### Definition

Sei  $R$  integer.

- (1)  $0 \neq p \in R$  ist *Primelement*, wenn  $\langle p \rangle$  *Primideal* ist  
(für alle  $a, b \in R : p|ab \Rightarrow p|a$  oder  $p|b$ ).
- (2)  $0 \neq r \in R; r \notin R^\times$  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 1

Sei  $R$  integer und  $p \in R$ .  $p$  ist Primelement  $\Rightarrow p$  ist irreduzible.

### Beweis

Sei  $\langle p \rangle \neq \{0\}$  Primideal. Also ist  $p \notin R^\times$ .

Sei  $p = ab; ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$  oder  $b \in \langle p \rangle$ .

1. Fall:  $a \in \langle p \rangle \Rightarrow a = pr \Rightarrow p = prb$  oder  $p(1 - rb) = 0 \Rightarrow 1 = rb$ ; also  $b \in R^\times$ .
2. Fall: Analog. □

### Proposition 2

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

### Beweis

Sei  $p \notin R^\times; p \neq 0$ ,  $p$  irreduzible.

Sei  $M \triangleleft R$  mit  $\langle p \rangle \subseteq M$ . Nun existiert ein  $m \in R$  mit  $M = \langle m \rangle$ .

$\exists r : p = rm$  und  $p$  irreduzible, also

$$\begin{array}{ccc}
 \text{1. Fall} & & \text{2. Fall} \\
 r \in R^\times & \text{oder} & m \in R^\times \\
 \Downarrow & & \Downarrow \\
 \langle p \rangle = \langle m \rangle & & \langle m \rangle = R
 \end{array}$$

Also  $\langle p \rangle$  ist maximal, insbesondere Primideal. □

**Definition**

Sei  $R$  integer.  $R$  ist *faktoriell*, wenn

(1) Für alle  $0 \neq r \in R \setminus R^\times$  existiert  $p_1, \dots, p_n \in R$  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  $q_1, \dots, q_m$  irreduzible, dann ist  $m = n$  und  $\forall i \exists j$  und  $u_i \in R^\times : u_i p_i = q_j$ .)

Ist  $R$  faktoriell und  $r \neq 0$  beliebiges Element, so hat  $r$  also eine Darstellung

$$r = up_1^{e_1} \cdots p_n^{e_n}$$

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

**Proposition 3**

Sei  $R$  faktoriell und  $p \in R$  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 ist  $p|ab \Rightarrow ab = pc$  für ein  $c \in R$  (\*)

Schreibe  $a$  und  $b$  wie in (†).

Aus (\*) und Eindeutigkeit in (†) folgt:  $p$  ist assoziiert mit einem der irreduziblen Faktoren in der Darstellung von  $a$  oder von  $b$ .

Ohne Einschränkung sei es  $a$ . Also  $a = (up)p_2 \cdots p_n; u \in R^\times, p_i \in R$  und damit  $p|a$ . □

**Proposition 4**

Sei  $R$  faktoriell,  $0 \neq a$  und  $b \in R$ .

$$a = up_1^{e_1} \cdots p_n^{e_n} \quad (\dagger)$$

$$b = vp_1^{f_1} \cdots p_n^{f_n} \quad (\ddagger)$$

$u, v \in R^\times, p_i$  irreduzible (Prim),  $p_i \neq p_j$  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  $d' \in R, d'|a$  und  $d'|b$ . Schreibe

$$d' = vq_1^{g_1} \cdots q_n^{g_n}.$$

für alle  $iq_i|d' \Rightarrow q'_i|a$  und  $q_i|b$ . Also für alle  $i$  existiert ein  $j: q_i|p_j$ , so dass  $p_j = u_i q_i$  mit  $u_i \in R^\times$ .

Also  $\{p_1, \dots, p_n\} \supseteq \{u_1 q_1, \dots, u_n q_n\}$ . Analog zeigt man  $g_\ell \leq \min(e_\ell, f_\ell)$ . Also  $d'|d$ . □

**Satz**

Sei  $R$  ein Hauptidealbereich, dann ist  $R$  faktoriell.

**Beweis**

Sei  $0 \neq r \in R \setminus R^\times$ . Wir wollen eine Darstellung  $(\dagger)$  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.

Wir wollen zeigen, dass diese Prozedur nach endlich vielen Schritten anhält, sonst bekommen wir eine unendliche (**strikte**) für die Inklusion ansteigende Folge von Idealen:

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \cdots \subseteq R$$

**Behauptung**

Wir zeigen nun, dass dieses in einem Hauptidealbereich nicht der Fall sein kann.

Sei also  $I_i \triangleleft R$  mit  $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq R$ .

Setze  $I := \bigcup_{i=1}^{\infty} I_i \triangleleft R$ . Da  $R$  ein Hauptidealbereich, existiert  $a \in R$  mit  $I = \langle a \rangle$ .

Nun  $a \in I \Rightarrow \exists n \in \mathbb{N} : a \in I_n$ . Also  $I_n \subseteq I = \langle a \rangle \subseteq I_n$  und somit  $I = I_n$ .

Damit ist die Behauptung bewiesen.

Wir haben also die  $\exists^Z$  einer Darstellung  $(\dagger)$  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, Vorlesung 5 vom 30.04.2012).  $\square$

## 7. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 15. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

Körper  $\subsetneq$  Euklidische Bereiche  $\subsetneq$  Hauptidealbereiche  $\subsetneq$  Faktorielle Bereiche  $\subsetneq$  Integritätsbereiche

### Konvention

deg von Nullpolynom ist = 0.

### Proposition 1 (Zusammenfassung)

Sei  $R$  integer und  $p, q \in R[x]$ . Es gelten:

1.  $\deg p(x)q(x) = \deg p(x) + \deg q(x)$
2.  $(R[x])^\times = R^\times$
3.  $R[x]$  ist integer
4.  $R[x]$  ist E.R.  $\Leftrightarrow R$  ist Körper
5.  $\text{Quot}(R[x]) := R(x) := \{\frac{p}{q} \mid p, q \in R[x], q \neq 0\}$  ist Körper.

**Notation:**  $I \triangleleft R$

### Bemerkung

$I[x] := \langle I \rangle \in R[x] = \{f(x) \in R[x] \mid f(x) = \sum a_i x^i \text{ mit } a_i \in I\}$

### Proposition 2

$R[x]/I[x] \simeq (R/I)[x]$

### Bemerkung

$$\begin{aligned} \varphi: R[x] &\rightarrow (R/I)[x] \\ \sum a_i x_i &\mapsto \sum \bar{a}_i x^i \end{aligned}$$

ist ein Ringhomomorphismus; surjektiv;  $\ker \varphi = I[x]$ .

**Korollar**

$P$  ist Primideal in  $R \Rightarrow P[x]$  ist Primideal in  $R[x]$ .

**Exkurs**  $R[x_1, \dots, x_n] := R[x_1, x_2, \dots, x_{n-1}][x_n]$ .

Notation =  $\{p(x_1, \dots, x_n) | p \in R[x_1, \dots, x_n]\}$ .

Also: *Polynome* in den Variablen  $x_1, \dots, x_n$  werden folgendermaßen definiert:

Es ist eine endliche Summe von *Monomen*.

$$m(x_1, \dots, x_n) := ax_1^{d_1} \dots x_n^{d_n} \quad a \in R$$

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

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

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

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

**Lemma 1**

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

**Beweis**

$$(R[x])^\times = R^\times \quad (*)$$

Sei  $0 \neq r \in R \setminus R^\times$ .  $r$  ist das Produkt von Irreduziblen in  $R[x]$  und diese (deg Bedingungen) müssen  $\deg = 0$  haben, d.h. sind Elemente aus  $R$ . Beachte ferner, dass  $r \in R$  irreduzibel in  $R[x] \Rightarrow$  irreduzibel in  $R$ , sonst  $r = ab$ ;  $a, b \in R \setminus R^\times$ . Aber wegen (\*):  $r = ab$ ;  $a, b \in R[x] \setminus (R[x])^\times$  - Widerspruch.  $\square$

Für die Umkehrung von Lemma 1 brauchen wir ein Hilfslemma.

**Lemma von Gauß**

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

Das heißt:  $p(x) = A(x)B(x)$  mit  $A, B \in F[x]$ ,  $\deg A \geq 1, \deg B \geq 1$ , dann gibt es  $0 \neq r, 0 \neq s \in F$  mit

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

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 der Form

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

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

1. Fall:  $d \in R^\times \quad \checkmark$

2. Fall:  $d \in R \setminus R^\times$

So schreibe  $d = p_1 \cdots p_n$ .  $p_i$  ist irreduzibel in  $R$ .

- $p_1$  irreduzibel  $\Rightarrow I = \langle p_1 \rangle$  ist Primideal in  $R$  und  $d \in I$   
(also ist auch  $I[x] = p_1 R[x]$  Primideal).
- $(R / \langle p_1 \rangle)[x]$  ist integer.

(\*) reduziere  $\text{mod } \langle p_1 \rangle$ . Wir bekommen  $0 = \overline{a'(x)b'(x)}$  in  $(R / \langle p_1 \rangle)[x]$ . Also ist ohne Einschränkung  $\overline{a'(x)} = 0$ , das heißt alle Koeffizienten von  $a'(x)$  liegen in  $\langle p_1 \rangle$  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

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

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



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

$$p(x) = a(x)b(x) \quad a(x), b(x) \in R[x]$$

$$\text{mit } a(x) = \alpha' a'(x) \quad \alpha', \beta' \neq 0$$

$$b(x) = \beta' b'(x) \quad \alpha', \beta' \in F$$

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

### Korollar

$R$  ist 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  $\{a_0, \dots, a_n\} = 1$ .

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

" $\Rightarrow$ " 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. □

## 1. TERMINOLOGY ENGLISH/GERMAN

Unique factorisation domain - faktorieller Ring  
 Field - Körper  
 Field of fractions - Quotientenkörper  
 Principal ideal domain - Hauptidealbereich  
 Field extension - Körpererweiterung  
 Prime subfield of a field - Primkörper eines Körpers

## 2. UFD'S AND IRREDUCIBLE POLYNOMIALS OVER INTEGRAL DOMAINS

From the last lecture we have the following lemma and corollary:

**Lemma 2.1** (Gauss' lemma). *Let  $R$  be a unique factorisation domain (in German: faktorieller Ring) with field of fractions  $F$  and  $p(x) \in R[x]$ . If  $p(x) = A(x)B(x)$  for some non-constant polynomials  $A(x), B(x) \in F[x]$  then there exist  $r, s \in F$  such that  $rA(x) = a(x)$  and  $sB(x) = b(x)$  are both in  $R[x]$  and  $p(x) = a(x)b(x)$ .*

**Corollary 2.2.** *Let  $R$  be a unique factorisation domain with field of fractions  $F$  (in German: Quotientenkörper) and let  $p(x) \in R[x]$ . Suppose that the greatest common divisor of the coefficients of  $p(x)$  is 1. Then  $p(x)$  is irreducible in  $R[x]$  if and only if it is irreducible in  $F[x]$ . In particular, if  $p(x)$  is a monic polynomial that is irreducible in  $R[x]$  then  $p(x)$  is irreducible in  $F[x]$ .*

**Theorem 2.3.** *A ring  $R$  is a unique factorisation domain if and only if  $R[x]$  is a unique factorisation domain.*

*Proof.* The reverse direction was covered in the last lecture.

Suppose  $R$  is a UFD (unique factorisation domain),  $F$  is the field of fractions of  $R$  and  $p(x) \in R[x]$  is non-zero.

Let  $d$  be the greatest common divisor of the coefficients of  $p(x)$  (NOTE: The greatest common divisor exists because  $R$  is a UFD) and write  $p(x) = dq(x)$ . The greatest common divisor of the coefficients of  $q$  is 1. Since  $R$  is a UFD,  $d$  can be factored in  $R$  into irreducibles and irreducibles in  $R$  remain irreducible in  $R[x]$  (this is simply because if  $d \in R \setminus \{0\}$  and  $d = a(x)b(x)$  then  $\deg(a(x)) = \deg(b(x)) = 0$ ; so  $a(x), b(x) \in R$ ).

We now attempt to write  $q(x)$  as a product of irreducibles in  $R[x]$ . Since  $F[x]$  is a UFD, there exist  $q_1(x), q_2(x), \dots, q_n(x) \in F[x]$  irreducible in  $F[x]$  such that  $q(x) = q_1(x) \cdots q_n(x)$ . Gauss' lemma means we may assume these factors are in  $R[x]$ . Since the greatest common divisor of the coefficients of  $q(x)$  is 1, the greatest common divisor of the

coefficients of each of the  $q_i$ s is also 1. Thus by corollary 2.2 each of these factors is irreducible in  $R[x]$ . Thus we can write  $p$  as a product of irreducible elements in  $R[x]$ :

$$d_1 \cdots d_m q_1(x) \cdots q_n(x)$$

where  $d = d_1 \cdots d_m$  and each  $d_i$  is irreducible in  $R$ .

It remains to show that this factorisation is unique up to ordering and multiplication by units. This is UB4 exercise 4. □

**Corollary 2.4.** *If  $R$  is a UFD then so is  $R[x_1, \dots, x_n]$ .*

*Proof.* Use induction on  $n$ . □

We will give two methods for testing the irreducibility of a polynomial over an integral domain.

**Proposition 2.5.** *Let  $I$  be a proper ideal of an integral domain (in German: Integritätsbereich)  $R$  and let  $p(x)$  be a non-constant monic (in German: normierte) polynomial in  $R[x]$ . If the image of  $p(x)$  in  $(R/I)[x]$  can't be factored in  $(R/I)[x]$  into two polynomials of smaller degree, then  $p(x)$  is irreducible.*

*Proof.* Suppose  $p(x)$  is non-constant, monic and reducible. Then  $p(x) = a(x)b(x) \in R[x]$  with  $a(x), b(x)$  non-constant (if either  $a(x)$  or  $b(x)$  were constant then would be a unit, since  $p(x)$  is monic). We may assume that  $a(x)$  and  $b(x)$  are monic since  $p(x)$  is monic.

Let  $\bar{p}(x)$ ,  $\bar{a}(x)$  and  $\bar{b}(x)$  be the images of  $p(x)$ ,  $a(x)$  and  $b(x)$  in  $(R/I)[x]$ . Then  $\bar{p}(x) = \bar{a}(x)\bar{b}(x)$  and since  $a(x)$  and  $b(x)$  are monic and non-constant,  $\bar{a}(x)$  and  $\bar{b}(x)$  are non-constant and monic. By comparing degrees  $\bar{a}(x)$  and  $\bar{b}(x)$  are polynomials of smaller degree than  $\bar{p}(x)$ . □

The most common application of this result is to prove that a polynomial over  $\mathbb{Z}$  is irreducible. For instance consider the polynomial  $X^4 + 9X^3 + 10X^2 + 22X + 1 \in \mathbb{Z}[X]$ .

Its image in  $\mathbb{Z}_2[X]$  is  $X^4 + X^3 + 1$ . It is clear that this polynomial does not have a root in  $\mathbb{Z}_2$  (check 0 and 1). Thus if it were irreducible, it must factor as a product of two polynomials in  $\mathbb{Z}_2[x]$  of degree 2. If  $p(x) \in \mathbb{Z}_2[X]$  is irreducible of degree 2 then its leading term is 1 and its constant term is also 1 since 0 is not a root. The polynomial  $X^2 + 1$  has root 1. Therefore, there is only one irreducible polynomial of degree 2 in  $\mathbb{Z}_2[X]$ . That is  $X^2 + X + 1$  (check it has no roots). But  $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ . So  $X^4 + X^3 + 1$  is irreducible over  $\mathbb{Z}_2$ . Thus  $X^4 + 9X^3 + 10X^2 + 22X + 1$  is irreducible over  $\mathbb{Z}$ .

Unfortunately this does not always work.

**Proposition 2.6.** (*Eisenstein's Criterion*) Let  $\mathfrak{p}$  be a prime ideal of an integral domain  $R$ ,  $n \geq 1$  and let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  be a polynomial in  $R[x]$ . Suppose  $a_{n-1}, \dots, a_0 \in \mathfrak{p}$  and  $a_0 \notin \mathfrak{p}^2$ . Then  $f(x)$  is irreducible in  $R[x]$ .

*Proof. Claim:* If  $a(x), b(x)$  are non-constant polynomials over an integral domain  $R$  with  $a(x)b(x) = x^n$  and  $n > 0$  then  $b(0) = a(0) = 0$ .

**Proof of claim:** Since  $R$  is an integral domain either  $a(0) = 0$  or  $b(0) = 0$ . Suppose  $a(0) = 0$ . Let  $m$  be maximal such that  $a(x) = x^m a'(x)$  for some  $a'(x) \in R[x]$ . Thus  $a'(0) \neq 0$ . So now  $a'(x)b(x) = x^{n-m}$ . Since  $b(x)$  is non-constant  $n - m > 0$ . Therefore  $a'(0)b(0) = 0$ . So  $b(0) = 0$ . So we have proved the claim.

Suppose  $f(x) = a(x)b(x)$  in  $R[x]$  where  $a(x)$  and  $b(x)$  are non-constant polynomials. It is easy to see that the constant term of  $f(x)$  is the product of the constant term of  $a(x)$  and the constant term of  $b(x)$ .

Let  $\bar{f}(x), \bar{a}(x), \bar{b}(x)$  be the images of  $f(x), a(x)$  and  $b(x)$  in  $(R/\mathfrak{p})[x]$ . Then  $x^n = \bar{f}(x) = \bar{a}(x)\bar{b}(x)$ . Thus  $\bar{a}(0) = \bar{b}(0) = 0$  since  $R/\mathfrak{p}$  is an integral domain. But this means that the constant terms of  $a(x)$  and  $b(x)$  are in  $\mathfrak{p}$ . Thus the constant term of  $f(x)$  is in  $\mathfrak{p}^2$  contradicting our assumptions. Therefore  $f(x)$  is irreducible. □

**Corollary 2.7.** Let  $p$  be a prime in  $\mathbb{Z}$ ,  $n \geq 1$  and let  $f(x) := x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ . Suppose that  $p$  divides  $a_i$  for all  $0 \leq i \leq n-1$  but  $p^2$  does not divide  $a_0$ . Then  $f(x)$  is irreducible in both  $\mathbb{Z}[x]$  and  $\mathbb{Q}[x]$ .

*Proof.* Apply Eisenstein at the prime ideal  $\langle p \rangle$ . □

The polynomial  $X^5 + 7 + 10X^4 + 25X^2 + 35 \in \mathbb{Z}[X]$  is irreducible by Eisenstein's theorem applied at 5.

**Extra example:**

Consider the polynomial  $f(X) := X^4 + 1 \in \mathbb{Z}[X]$ . We can't apply Eisenstein's theorem directly. Let  $g(X) = f(X+1)$ . So  $g(X) = X^4 + 4X^3 + 6X^2 + 4X + 2$ . Now, by Eisenstein applied at 2,  $g(x)$  is irreducible and if  $f$  could be factored as a product of non-constant polynomials then so could  $g$ . Thus  $f$  is irreducible.

### 3. FIELDS

A reminder from linear algebra:

**Definition 3.1.** The characteristic of a field  $F$ , denoted  $\text{char}(F)$  is the smallest strictly positive integer  $n$  such that  $n \cdot 1_F = 0$ . If such an integer does not exist we say the characteristic is zero.

Note that the characteristic of a field will always be zero or a primes (Check you know why?).

**Definition 3.2.** *The prime subfield (Primkörper eines Körpers) of a field  $F$  is the smallest subfield of  $F$ . Note that the prime subfield is always  $\mathbb{Q}$  (when  $F$  has characteristic zero) or  $\mathbb{F}_p$  (when  $F$  has positive characteristic  $p$ ).*

Note that a field of characteristic  $p$  may well have infinitely many elements. For example consider the field of fractions of  $\mathbb{F}_p[x]$ .

**Definition 3.3.** *If  $K$  is a field containing a subfield  $F$  then  $K$  is called an extension field (in German: Körpererweiterung) of  $F$ , denoted  $K/F$ . We refer to  $F$  as the base field.*

*If  $K/F$  is a field extension, then the multiplication defined in  $K$  makes  $K$  as a vector space over  $F$ .*

*The degree of a field extension (Grad einer Körpererweiterung)  $K/F$ , denoted  $[K : F]$ , is the dimension of  $K$  as a vector space over  $F$ . The extension is called finite if  $[K : F]$  is finite and is called infinite otherwise.*

**Examples:** The field extension  $\mathbb{C}/\mathbb{R}$  has degree 2. Every element of  $\mathbb{C}$  can be written as a linear combination of 1 and  $i$  and if  $a + bi = 0$  then  $a^2 + b^2 = (a + bi)(a - bi) = 0$ ; so  $a = b = 0$ . So  $1, i$  are a basis for  $\mathbb{C}$  as a vector space over  $\mathbb{R}$ .

**Remark 3.4.** *A homomorphism of fields is always injective.*

*Proof.* Let  $\varphi : F \rightarrow K$  be a homomorphism between fields  $F$  and  $K$ . The kernel of  $\varphi$  is an ideal of  $F$ . The only ideals of  $F$  are  $\{0\}$  and  $F$ . Since  $\varphi(1_F) = 1_K \neq 0$ ,  $\ker \varphi = 0$ . So  $\varphi$  is injective.  $\square$

**Theorem 3.5.** *Let  $F$  be a field and  $p(x) \in F[x]$  be irreducible. There exists a field  $K$  extension  $F$  of  $F$  in which  $p(x)$  has a root.*

*Proof.* Consider the quotient  $F[x]/\langle p(x) \rangle$ . Since  $p(x)$  is irreducible and  $F[x]$  is a PID (Hauptidealbereich), the ideal generated by  $p(x)$  is maximal. Therefore  $F[x]/\langle p(x) \rangle$  is a field.

Let  $\varphi : F[x] \rightarrow F[x]/\langle p(x) \rangle$  be the canonical homomorphism. The restriction of  $\varphi$  to  $F$  is a homomorphism of fields and thus is injective. Thus  $F$  is isomorphic to its image  $\varphi(F)$  in  $F[x]$ . We may now identify  $F$  with its image in  $F[x]/\langle p(x) \rangle$ .

This is a subtle point: what does it mean to identify  $F$  with its image in  $F[x]/\langle p(x) \rangle$ ?

If  $\psi : F \rightarrow K$  is a homomorphism of fields (with  $K$  and  $F$  disjoint as sets) we simply relabel each element  $\varphi(f)$  for  $f \in F$  as  $f$ . We can do

this because  $\psi$  is injective; i.e. if  $\psi(f) = \psi(g)$  then  $f = g$ . Now  $F$  as a set is a subset of  $K$ . Because  $\psi$  is a homomorphism  $\psi(0) = 0$ ,  $\psi(1) = 1$  and for all  $f, g \in F$ ,  $f + g = \psi(f) + \psi(g)$  and  $f \cdot g = \psi(f) \cdot \psi(g)$ . Thus  $F$  is also a subfield of  $K$ .

Back to the proof: Let  $\bar{x}$  be the image of  $x$  in  $F[x]/\langle p(x) \rangle$ . We now have that  $p(\bar{x}) = \overline{p(x)}$  since  $\varphi$  is a homomorphism. But  $p(x) \in \langle p(x) \rangle$ , so  $\overline{p(x)} = 0$ . Thus  $\bar{x}$  is a root of the polynomial  $p(x)$  in  $K$ .  $\square$

### 9. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 22. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

#### Satz 1

Sei  $p(x) \in F[x]$  irreduzibel;  $\deg p(x) = n$ . Es gilt  $[K : F] = n$ , wobei  $K := F[x]/\langle p(x) \rangle$ .

#### Beweis

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

- 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  $a(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle$ ,

$$\text{d. h. } \overline{a(x)} = \overline{r(x)}$$

||

$$\text{d. h. } a(\bar{x}) = r(\bar{x})$$

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

- $O$  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  $b(x) \in \langle p(x) \rangle$  und  $\deg b(x) < \deg p(x)$

und damit muss  $b(x) = 0$  das Nullpolynom sein, i.e.  $b_i = 0$  für alle  $i = 0, \dots, n-1$ .  $\square$

#### Bemerkung

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

#### Definition

- (1) Sei  $K/F$  eine Körpererweiterung;  $S \subseteq K$ .

**Notation:**  $F(S) =$  der kleinste Unterkörper von  $K$ , der  $F \cup S$  enthält  $= \bigcap \{L \mid L \subseteq K \text{ Unterkörper}; L \supseteq F \cup S\}$ .

$F(S)$  heißt der Körper der von  $S$  über  $F$  erzeugt ist.

- (2) Wenn  $S = \{\alpha_1, \dots, \alpha_n\}$  endlich ist, schreiben wir  $L = F\{\alpha_1, \dots, \alpha_n\}$  und sagen:  $L$  ist endlich erzeugt über  $F$ .
- (3) Wenn  $S = \{\alpha\}$  heißt  $L = F(\alpha)$  eine einfache Erweiterung und  $\alpha$  heißt ein primitives Element für die Körpererweiterung  $L/F$ .

**Satz 2**

Sei  $p(x) \in F[x]$  irreduzibel;  $\alpha \in K/F$  eine Nullstelle. Es ist:  $F(\alpha) \simeq F[x]/\langle p(x) \rangle$ .

**Beweis**

Betrachte

$$\begin{aligned} \varphi : F[x]/\langle p(x) \rangle &\rightarrow F(\alpha) \subseteq K \\ a(x) + \langle p(x) \rangle &\mapsto a(\alpha) \end{aligned}$$

- Es ist  $\varphi|_F = Id|_F$  (i.e.  $\varphi(r) = r$  für alle  $r \in F$ ) und  $\varphi(x) = \alpha$ .
- $\varphi$  ist wohldefiniert:  $a(x) \equiv b(x) \pmod{\langle p(x) \rangle} \Leftrightarrow a(x) - b(x) = p(x)q(x)$ . Also  $a(\alpha) - b(\alpha) = 0$  und damit  $a(\alpha) = b(\alpha)$ .
- $\varphi \neq 0$  (e.g.  $\varphi|_F = id|_F$ ), also  $\varphi$  ist ein injektiver Ringhomomorphismus und damit ist  $\varphi : F[x]/\langle p(x) \rangle \simeq Bi(\varphi) \subseteq F(\alpha) \subseteq K$  ein Unterkörper. Also ist  $Bi(\varphi)$  ein Unterkörper von  $K$  und enthält  $F \cup \{\alpha\}$  und somit ist  $F(\alpha) \subseteq Bi(\varphi)$ . Also  $Bi(\varphi) = F(\alpha)$ .  $\square$

**Korollar 1**

$K/F$  ist eine Körpererweiterung;  $\alpha \in K$  ist Nullstelle vom irreduziblen  $p(x) \in F[x]$ ;  $\deg p = n$ .  
Es ist  $F(\alpha) = \{a(\alpha) \mid a(x) \in F[x]; \deg a(x) < n\}$ .

**Korollar 2**

$\alpha, \beta \in K/F$ ;  $p(x) \in F[x]$  ist irreduzibel mit  $p(\alpha) = p(\beta) = 0$ .  
Es ist  $F(\alpha) \simeq F[x]/\langle p(x) \rangle \simeq F(\beta)$ .

Allgemeiner betrachten wir folgenden Absatz:

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

**Satz 3**

Seien  $F, F'$  Körper.  $\varphi : F \xrightarrow{\sim} F'$  und  $p(x) \in F[x]$  irreduzibel.

Setze  $p(x) = \sum a_i x^i$  und  $p'(x) := \sum \varphi(a_i) x^i$  (Anwendung von  $\varphi$  auf Koeffizienten). Dann ist  $p'(x) \in F'[x]$  irreduzibel.

Sei  $\alpha \in K/F$  mit  $p(\alpha) = 0$  und  $\beta \in K'/F'$  mit  $p'(\beta) = 0$ . Dann läßt sich  $\varphi$  zu einer Isomorphie  $\varphi'$  fortsetzen

$$\begin{aligned} \varphi' : F(\alpha) &\rightarrow F'(\beta) \\ \varphi' | F = \varphi &\text{ und } \varphi'(\alpha) = \beta \end{aligned}$$



**Beweis**

- (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  $\varphi^{-1}$  auf Koeffizienten)  $p(x) = a''(x)b''(x)$  von  $p(x)$  in  $F[x]$  induziert.  
 $\deg(a''(x)) \geq 1$ ,  $\deg(b''(x)) \geq 1$ ;  $a''(x), b''(x) \in F[x]$ .
- (2)  $F[x] \simeq F'[x]$  und  $\langle p(x) \rangle \simeq \langle p'(x) \rangle$  (durch Anwendung von  $\varphi$  auf Koeffizienten). Also  $F(\alpha) \simeq F[x]/\langle p(x) \rangle \simeq F'[x]/\langle p'(x) \rangle \simeq F(\beta)$ .  $\square$

## 10. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 26. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### Definition

- (1)  $\alpha \in K/F$  ist *algebraisch über  $F$*  (*alg/ $F$* ), wenn es ein Polynom  $0 \neq f(x) \in F[x]$  gibt mit  $f(\alpha) = 0$ .
- (2) Wenn  $\alpha$  nicht algebraisch ist, dann heißt  $\alpha$  *transzendent* über  $F$ .
- (3) Die Körpererweiterung  $K/F$  heißt *algebraisch*, falls für alle  $\alpha \in K$ :  $\alpha$  ist algebraisch über  $F$ .

### Proposition 1

Sei  $\alpha$  alg /  $F$ . Es gibt ein eindeutiges normiertes 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  $r(x) \equiv 0$ , 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  $\Rightarrow m'(x) = m(x)$ . □

### Bemerkung

Vergleiche mit 13. Vorlesung "Lineare Algebra II" vom 1. Juni 2012:

Das Minimal-Polynom vno  $T$  in  $F[x]$  ist der eindeutige normierte Erzeuger vom Annihilator-Ideal von  $T$

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

**Definition**

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

**Proposition 2**

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

**Beweis**

$$F(\alpha) \simeq F[x] / \langle m(x) \rangle$$

□

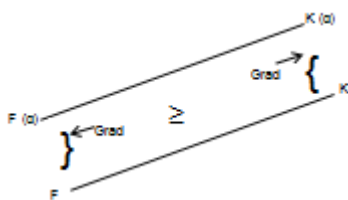
**Terminologie**

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

**Bemerkung**

- (1)  $L \supseteq K \supseteq F, \alpha \in L$ ,  $\text{alg } /F \rightarrow \alpha \text{ alg } /K$  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)  $[K(\alpha) : K] \leq [F(\alpha) : F]$

Für  $\alpha \in L$   $\text{alg } /F \subseteq K \subseteq L$ :



Wir zeigen nun die Umkehrung von Proposition 2.

(**Erinnerung:**  $K/F$  ist endlich, wenn  $[K : F] < \infty$ , sonst unendlich.)

**Proposition 3**

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

**Beweis**

Sei  $[F(\alpha) : F] = n$ , dann sind  $F(\alpha) \ni 1, \alpha, \alpha^2, \dots, \alpha^n$  linear abhängig über  $F$ . Also existiert  $b_i \in F$  nicht alle gleich 0, so dass  $\sum_{i=0}^n b_i \alpha^i = 0$ . Setze  $f(x) := \sum b_i x^i \in F[\alpha]; \neq 0$ . Dann gilt  $f(\alpha) = 0; \alpha \text{ alg } / F$ .  $\square$

**Bemerkung**

$x \in F(x)$  ist transzendent über  $F$  (weil  $f(x) = 0 \Leftrightarrow f = 0$  das Nullpolynom ist). Wir sehen, dass  $F(x)/F$  eine endlich erzeugte (eigentlich eine einfache) Erweiterung ist, aber  $[F(x) : F] = \infty$ . Also i.a.:  $K/F$  endlich erzeugt  $\not\Rightarrow K/F$  endlich.

**Korollar**

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

**Beweis**

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

**Satz 1**

$F \subseteq K \subseteq L$ . 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  $\{\alpha_1, \dots, \alpha_m\}$  Basis für  $L/K$ ;  $[K : F] = n$  mit  $\{\beta_1, \dots, \beta_n\}$  Basis für  $K/F$ . Ein Element  $\lambda$  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  $\text{span}_F \{\alpha_i \beta_j \mid i = 1, \dots, m, j = 1, \dots, n\} = L$ . 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  $\alpha_i$  linear unabhängig über

$K \Rightarrow a_i = 0$  für alle  $i$ , also  $\sum_j b_{ij} \beta_j = 0$  für alle  $i$ .

Nun ist  $\beta_j$  linear unabhängig über  $F \Rightarrow b_{ij} = 0$  für alle  $j$ .  $\square$

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  $[L : F] = \infty$  ( $\lambda_1, \dots, \lambda_s$  sind  $K$  linear unabhängig  $\rightarrow \lambda_1, \dots, \lambda_s$  sind  $F$ -linear unabhängig).

**Korollar**

Sei  $L/K/F$  und  $L/F$  endlich. Es gilt  $[K : F] | [L : F]$ .

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

**Bemerkung**

$F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) \subseteq K$  (folgt unmittelbar aus der Definition von  $F(\alpha_1, \alpha_2)$ ).

**Satz 2**

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

**Beweis**

“ $\Rightarrow$ ” Setze  $[K : F] = n$ . Sei  $\{\alpha_1, \dots, \alpha_n\}$  die  $F$ -Basis von  $K$ . Jedes  $\alpha_i$  ist algebraisch über  $F$ .

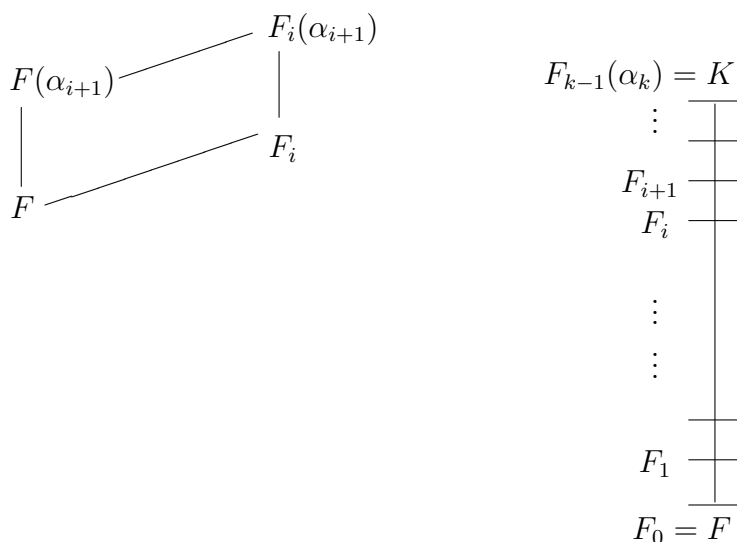
Außerdem ist  $K = \text{span}_F \{\alpha_1, \dots, \alpha_n\} \subseteq F(\alpha_1, \dots, \alpha_n) \subseteq K$

und damit ist  $K = F(\alpha_1, \dots, \alpha_n)$ .

“ $\Leftarrow$ ” Sei  $K = F(\alpha_1, \dots, \alpha_k)$ . Sei  $\alpha_i$  algebraisch über  $F$  und  $\text{deg } \alpha_i = n_i$ . 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 1)  $[K : F] = [F_k : F_{k-1}] \cdots [F_1 : F_0] \leq n_1 \cdots n_k$  und damit ist  $K/F$  endlich. □

### 11. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 29. November 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

#### Korollar 1

$\alpha, \beta$  sind algebraisch über  $F \rightarrow \alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$  sind auch algebraisch über  $F$ .

#### Beweis

$F(\alpha, \beta)/F$  ist endlich und  $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$  für  $\beta \neq 0$ . □

#### Korollar 2

Sei  $L/F$  ist eine beliebige Körpererweiterung. Die Menge  $\{\alpha \in L \mid \alpha \text{ alg } /F\}$  ist ein Unterkörper von  $L$  (und enthält  $F$ ).

#### Definition

Dieser Unterkörper heißt der *relative algebraische Abschluss von  $F$  in  $L$* .

#### Beispiele

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

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

Es gilt  $\tilde{\mathbb{Q}} \subsetneq \mathbb{C}$  und  $\tilde{\mathbb{Q}}^r \subsetneq \mathbb{R}$ . Eigentlich gilt es ferner  $|\tilde{\mathbb{Q}}| = |\tilde{\mathbb{Q}}^r| = \chi_0$  und  $|\mathbb{C} \setminus \tilde{\mathbb{Q}}| = |\mathbb{R} \setminus \tilde{\mathbb{Q}}^r| = 2^{\chi_0}$  (siehe Ausarbeitung dazu im Weihnachtsübungsblatt!)

#### Satz 1

$$\begin{array}{ccc} L/K & \text{und} & K/F \Rightarrow L/F \\ \text{alg} & & \text{alg} \quad \text{alg} \end{array}$$

#### Beweis

Sei  $\alpha \in L, k(x) \in K[x]; k(\alpha) = 0$ . Setze  $k(x) := \sum_{i=0}^n a_i x^i$  mit  $a_i \in K$  nicht alle Null. Betrachte  $F_1 := F(a_0, \dots, a_n)$  und  $F_1(\alpha), F_1 \subseteq K, F_1(\alpha) \subseteq L; a_i \text{ alg } /F$  und  $\alpha \text{ alg } /F_1$ .

Also  $[F_1 : F] < \infty$  und  $[F_1(\alpha) : F_1] < \infty \Rightarrow [F_1(\alpha) : F] = [F_1(\alpha) : F_1][F_1 : F] < \infty$ .

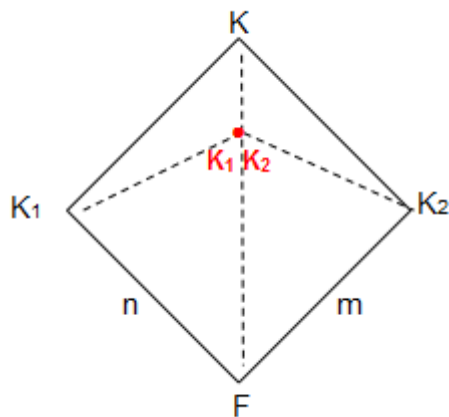
Insbesondere  $F_1(\alpha)/F$  algebraisch und damit  $\alpha$  algebraisch über  $F$ .

#### Definition

Sei  $K/K_1$  und  $K/K_2$  eine Körpererweiterung.  $K_1K_2 := K_1(K_2) = K_2(K_1) \subseteq K$  heißt das Kompositum von  $K_1$  und  $K_2$  in  $K$ .

**Lemma**

Sei



$\{\alpha_1, \dots, \alpha_n\}$  eine  $F$ -Basis von  $K_1$  und  $\{\beta_1, \dots, \beta_m\}$  eine  $F$ -Basis von  $K_2$  ohne Einschränkung mit  $\alpha_1 = \beta_1 = 1$ . Es ist  $\text{span}_F\{\alpha_i\beta_j/i, j\} = K_1K_2$ .

**Beweis**

$K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ , so dass  $\text{span}_F\{\alpha_i\beta_j/i, j\} \subseteq K_1K_2$ . Umgekehrt müssen wir nun prüfen, dass  $\text{span}_F\{\alpha_i\beta_j/i, j\}$  ein Unterkörper von  $K$  ist (der offensichtlich  $F \cup \{\alpha_1, \dots, \alpha_n\} \cup \{\beta_1, \dots, \beta_m\}$  enthält) und damit  $\text{span}_F\{\alpha_i\beta_j/i, j\} \supseteq K_1K_2$ .

Aber es ist klar, dass  $\text{span}_F\{\alpha_i\beta_j/i, j\}$  ein Unterkörper ist, weil zum Beispiel

$$\alpha_i^k \in F(\alpha_1, \dots, \alpha_n) = \text{span}_F\{\alpha_1, \dots, \alpha_n\} = K_1$$

$$\text{und } \beta_j^l \in F(\beta_1, \dots, \beta_m) = \text{span}_F\{\beta_1, \dots, \beta_m\} = K_2$$

und damit ist er abgeschlossen unter Multiplikation.

Analog ist er abgeschlossen unter Inversen.

Außerdem ist er abgeschlossen unter Addition und Subtraktion (weil er ein  $F$ -Vektorraum ist).

□

## 12. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 3. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

(A) Wir haben bewiesen:

Sei  $\{\alpha_1, \dots, \alpha_n\}$  eine  $F$ -Basis von  $K_1/F$  und  $\{\beta_1, \dots, \beta_m\}$  eine  $F$ -Basis von  $K_2/F$ . Dann ist  $\text{span}_F\{\alpha_i\beta_j/i, j\} = K_1K_2$ . Also ist  $[K_1K_2 : F] \leq mn$ .

(B) Wir betrachten ferner  $\text{span}_{K_1}\{\beta_j; j = 1, \dots, m\} = K_1K_2$ , weil man  $\lambda \in K_1K_2$  mit Hilfe von (A) als

$$\lambda = \sum \nu_{ij}\alpha_i\beta_j = \sum \underbrace{(\nu_{ij}\alpha_i)}_{\in K_1} \beta_j$$

mit  $\nu_{ij} \in F$  schreibt.

Ferner gilt:  $\{\beta_j; j = 1, \dots, m\}$  ist eine Basis für  $K_1K_2/K_1$ , falls  $\{\beta_j; j = 1, \dots, m\}$  über  $K_1$  linear unabhängig ist.

(C) Analog zeigt man  $\text{span}_{K_2}\{\alpha_i; i = 1, \dots, n\} = K_1K_2$  und  $\{\alpha_i; i = 1, \dots, n\}$  ist eine  $K_2$ -Basis für  $K_1K_2$ , falls  $\{\alpha_i; i = 1, \dots, n\}$  linear unabhängig über  $K_2$  bleibt.

Wir haben bewiesen:

### Korollar 1

Seien  $F \subseteq K_1, K_2 \subseteq K; [K_1 : F] := n; [K_2 : F] := m$ . Es gilt  $[K_1K_2 : F] \leq nm$  und  $[K_1K_2 : F] := mn$ , falls  $\beta_j$  linear unabhängig über  $K_1$  bleiben (oder  $\alpha_i$  linear unabhängig über  $K_2$  bleiben).

### Korollar 2

Seien  $F \subseteq K_1, K_2 \subseteq K$  mit  $[K_1 : F] = n, [K_2 : F] = m$  und  $\text{ggT}(n, m) = 1$ .

Es gilt  $[K_1K_2 : F] = mn$ .

### Beweis

$$\left. \begin{array}{l} n \mid [K_1K_2 : F] \\ m \mid [K_1K_2 : F] \end{array} \right\} \Rightarrow \text{kgV}(n, m) \mid [K_1K_2 : F]$$

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



## Zerfällungskörper

### Definition 1

$K/F$  ist ein Zerfällungskörper von  $f(x) \in F[x]$ , falls

- (i)  $f(x)$  vollständig in lineare Faktoren in  $K[x]$  zerfällt ( $\deg f \geq 1$ ) und
- (ii)  $F \subseteq L \subsetneq K \Rightarrow f(x)$  **nicht** vollständig in linearen Faktoren in  $L(x)$  zerfällt.

### Satz 1

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  $n = \deg f(x)$ .  $n = 1, E = F$  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  $p(x)$ , über  $E_1$  haben wir also

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

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

Induktionsanfang 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  $K := \bigcap \{L/F \subseteq L \subseteq E; f \text{ zerfällt vollständig in } L[x]\}$  □

### Definition 2

$K/F$  ist *normal*, falls

- (i)  $K/F$  algebraisch ist
- (ii) und  $K$  ein Zerfällungskörper über  $F$

einer Familie von Polynomen  $f(x) \in F[x]$ .

### Proposition

Sei  $\deg f = n$   $K/F$  ein Zerfällungskörper von  $f$  über  $F$ . Es gilt  $[K : F] \leq n!$

### Beweis

Sei  $\alpha_1 \in F_1/F$ ,  $\alpha_1$  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:  $\alpha_2 \in F_2/F_1$ ,  $\alpha_2$  ist Nullstelle von  $f_1$ .

Dann ist  $[F_2 : F_1] \leq n - 1$  und damit  $[F_2 : F] \leq n(n - 1)$  usw. □

**Satz 2** (Eindeutigkeit bis auf Isomorphie)

Sei  $\varphi : F \xrightarrow{\sim} F'$  eine Isomorphie.

$f(x) \in F[x] \rightsquigarrow f'(x) \in F'[x]$  ( $\deg f \geq 1$ ).

$E$  ist Zerfällungskörper für  $f$  über  $F$  -  $E'$  ist Zerfällungskörper für  $f'$  über  $F'$ .

Dann läßt sich  $\varphi$  fortsetzen:

$$\begin{array}{ccc} E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

**Beweis**

Sei  $\deg f := n$ . Induktion nach  $n$ . Wenn  $f$  über  $F$  erfällt, dann zerfällt  $f'$  über  $F'$  und  $\sigma = \varphi$ . Sei also  $p(x)$  ein irreduzibler Faktor von  $f(x)$  in  $F[x]$  mit  $\deg p \geq 2$  und  $p' = \varphi(p)$  der entsprechende Faktor von  $f'(x)$  in  $F'[x]$ .

$\alpha \in E$  ist Nullstelle für  $p(x)$  und  $\beta \in E'$  ist Nullstelle für  $p'(x)$ . Setze  $F_1 := F(\alpha)$  und  $F'_1 := F'(\beta)$ .

Aus Satz 3 der 9. Vorlesung (22.11.2012) folgt, dass ein  $\sigma_1$  existiert, so dass

$$\begin{array}{ccc} F_1 & \xrightarrow{\sim} & F'_1 \\ \downarrow & \sigma_1 & \downarrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

Wir haben also den folgenden Ansatz:

$$\sigma_1 : F_1 \xrightarrow{\sim} F'_1$$

$f(x) = (x - \alpha)f_1(x)$  über  $F_1$ ,  $\deg f_1 \leq n - 1$  und  $E$  ist ein Zerfällungskörper von  $f_1$  über  $F_1$ , weil  $E \supseteq F_1$  und alle Nullstellen von  $f_1$  und für  $E \supsetneq L \supseteq F_1$  ist es unmöglich, dass  $L$  alle Nullstellen von  $f_1$  enthält (sonst enthält  $L$   $\alpha$  und alle Nullstellen von  $f_1$ , also alle Nullstellen von  $f$  - Widerspruch. Minimalität von  $E$  als ein Zerfällungskörper von  $f$  über  $F$ ).

$f'(x) = (x - \beta)f'_1(x)$  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  $f_1, F_1, \sigma_1$  mit  $\deg f_1 \leq n - 1$ .

Die Induktionsannahme liefert ein  $\sigma$ , 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

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

### Beweis

Seien  $K$  und  $K'$  Zerfällungskörper von  $f$  über  $F$ . Es gilt

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

$$\sigma \upharpoonright F = Id$$

□

### Definition

(a)  $\tilde{F}/F$  ist ein *algebraischer Abschluss* von  $F$ , falls

(a)  $\tilde{F}/F$  algebraisch ist;

(b)  $f(x) \in F[x]$  vollständig in lineare Faktoren über  $\tilde{F}$  zerfällt für alle  $f \in F[x]$ .

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

### Bemerkung

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

### 13. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 10. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

#### Proposition 1

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

#### Beweis

Sei  $f(x) \in \tilde{F}(x)$ ;  $\alpha$  ist Nullstelle von  $f(x)$ . Dann ist  $\tilde{F}(\alpha)/\tilde{F}$  algebraisch und  $\tilde{F}/F$  algebraisch. Also ist auch  $\tilde{F}(\alpha)/F$  algebraisch und damit ist auch  $\alpha/F$  algebraisch.

Sei  $m_{\alpha,F}$  ein Minimalpolynom von  $\alpha/F$ , dann zerfällt  $m_{\alpha,F}$  in  $\tilde{F}[x]$  und hat  $(x - \alpha)$  als linearen Faktor. Es folgt  $\alpha \in \tilde{F}$ .  $\square$

Sei  $F$  ein beliebiger Körper. Wir zeigen nun:

#### Satz 1

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  $K := \bigcup K_j$ .

$K/F$  ist dann eine Körpererweiterung, wenn  $f(x) \in K[x]$  ( $\deg f \geq 1$ ), so dass ein  $j$  existiert 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  $F[\cdots, x_f, \cdots]$  (Polynom in der Variablen  $x_f$ ) und das Ideal  $I := \langle f(x_f); f \in F[x] \rangle$ .

**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  $i = 1, \dots, n$  und seien  $x_{n+1}, \dots, x_m$  alle anderen Variablen, die unter den  $g_i$ 's noch vorkommen. Also ist

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

eine polynomiale Gleichung.

Sei  $F'/F$  eine Körpererweiterung mit  $\alpha_i \in F'$ , Nullstelle für  $f_i(x)$ . Durch Einsetzen von  $\alpha_i$  für  $x_i$  mit  $i = 1, \dots, n$  und 0 für  $x_j$  mit  $j = n+1, \dots, m$  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. Sei  $\mathcal{M}$  maximal.  $\mathcal{M} \triangleleft F[\cdots, x_f, \cdots]$  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  $f(\bar{x}_f) = \overline{f(x_f)} = 0$  (da  $f(x_f) \in I$ ).

Wiederhole mit  $K_j/K_{j-1}$  und setze  $K = \bigcup K_j$  wie schon erwähnt.  $\square$

**Korollar 1**

$\exists^Z$ : Sei  $K$  algebraisch abgeschlossen und  $F \subseteq K$ . Dann ist der relative algebraische Abschluss von  $F$  in  $K$  (siehe Korollar 2 aus der 11. Vorlesung vom 29.11.2012) ein algebraischer Abschluss von  $F$ .

**Eindeutigkeit:** (Übungsaufgabe siehe Übungsblatt))

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  $\alpha$  ist algebraisch über  $F$  und  $\alpha \in K$ , also  $\alpha \in \tilde{F}$ . Also zerfällt  $f(x)$  in  $\tilde{F}[x]$ .  $\square$

## § Separable und inseparable Körpererweiterung

### Bemerkung

Sei  $f(x) \in F[x]$ ,  $K/F$  ein Zerfällungskörper für  $f$ . Also  $f(x) = (x - \alpha_1)^{n_1} (x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$  in  $K[x]$ ;  $n_i \geq 1$ ;  $\alpha_i \neq \alpha_j$  für  $i \neq j$ .

### Definition 1

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

### Definition 2

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

### Definition 3

$Df(x) = D(a_n x^n + \cdots + a_0) = na_n x^{n-1} + \cdots + a_1 \in F[x]$ .

$D : F[x] \rightarrow F[x]$  ist ein *Ableitungsoperator* und erfüllt die Produktregel

$$Dfg = gDf + fDg.$$

### Bemerkung

- (i)  $\deg Df < \deg f$  immer !
- (ii)  $f(x) = x^p \in F[x]$ ;  $p$  ist Primzahl;  $\text{Char } F = p$ . Dann ist  $f(x) \neq 0$ ,  
aber  $Df(x) = px^{p-1} \equiv 0$ .
- (iii)  $f(x) \in F[x]$  ( $\deg f \geq 1$ ) und  $\text{Char } F = 0 \Rightarrow Df \neq 0$  (weil zum Beispiel  $na_n \neq 0$ , falls  $a_n \neq 0$  ist).

### Proposition 2

Sei  $f(x) \in F[x]$  ( $\deg f \geq 1$ ). Eine Nullstelle  $\alpha$  für  $f(x)$  ist eine mehrfache Nullstelle genau dann, wenn  $\alpha$  auch eine Nullstelle für  $Df(x)$  ist. Das heißt, dass die Menge { mehrfache Nullstelle von  $f$  } = { gemeinsame Nullstelle von  $f$  und  $Df$  } ist.

**Beweis**

" $\Rightarrow$ " Sei  $\alpha$  eine mehrfache Nullstelle.  $f(x) = (x - \alpha)^n g(x)$  mit  $n \geq 2$ .

$$Df(x) = n(x - \alpha)^{n-1}g(x) + (x - \alpha)^n Dg(x); n - 1 \geq 1 \Rightarrow \alpha \text{ ist Nullstelle von } Df(x).$$

" $\Leftarrow$ " Sei  $\alpha$  eine gemeinsame Nullstelle von  $f(x)$  und  $Df(x)$ .

$$\text{Schreibe } f(x) = (x - \alpha)h(x). \quad (*)$$

Also ist  $Df(x) = h(x) + (x - \alpha)Dh(x)$ . Beim Einsetzen von  $\alpha$  für  $x$ , ergibt das  $h(\alpha) = 0$ .

$$\text{Zurück in } (*) \text{ ergibt es } f(x) = (x - \alpha)^2 h_1(x). \quad \square$$

**Bemerkung**

Die mehrfachen Nullstellen von  $f$  stimmen überein mit den gemeinsamen Nullstellen von  $f$  und  $DF$ , das heißt mit den Nullstellen von  $\text{ggT}(f, Df)$ .

**Beweis**

" $\Leftarrow$ "  $\alpha$  ist Nullstelle von  $\text{ggT}(f, DF) \rightarrow \alpha$  ist Nullstelle von  $f$  und  $Df$ . Ist klar.

" $\Rightarrow$ " Sei  $\alpha$  eine Nullstelle von  $f$  und  $DF \in F[x]$ . Also gilt  $m_{\alpha, F}/f$  und  $m_{\alpha, F}/Df$  und damit  $m_{\alpha, F}/\text{ggT}(f, Df)$  auch. Da  $\alpha$  Nullstelle von  $m_{\alpha, F}$ , folgt nun  $\alpha$  ist Nullstelle von  $\text{ggT}$ .  $\square$

**Korollar 2**

$f \in F[x]$  ( $\deg f \geq 1$ ) ist separabel genau dann, wenn  $\text{ggT}(f, Df) = 1$ .

**Beweis**

" $\Leftarrow$ " Folgt aus der Bemerkung.

" $\Rightarrow$ "  $f$  separabel  $\Rightarrow$  keine gemeinsame Nullstelle mit  $Df \Rightarrow \text{ggT}(f, Df) = 1$ .  $\square$

## 14. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 13. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### Erinnerung

$f(x) \in F[x]$  ( $\deg f \geq 1$ );  $\alpha$  ist eine mehrfache Nullstelle  $\Leftrightarrow \alpha$  ist Nullstelle von  $Df(x) \Leftrightarrow m_{\alpha,F} | f(x)$  und  $m_{\alpha,F} | Df(x)$ .

### Korollar 1

Sei  $f(x)$  ( $\deg f \geq 1$ ) irreduzibel. Es gilt:  $f$  ist inseparabel genau dann, wenn  $Df = 0$ .  
(Das heißt, dass  $f$  eine mehrfache Nullstelle hat  $\Leftrightarrow Df = 0$ ).

### Beweis

$\alpha$  ist eine mehrfache Nullstelle  $\Leftrightarrow m_{\alpha,F}$  ggT von  $f$  und  $Df$ .

Nun ist  $f$  irreduzibel  $\Rightarrow \deg m_{\alpha,F} = \deg f > \deg Df$ . Also  $m_{\alpha,F} | Df \Rightarrow Df \equiv 0$ . □

### Beispiel

$$(1) f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$$

$$Df(x) = p^n x^{p^n-1} - 1 = -1$$

$Df$  hat gar keine Nullstelle, also ist  $f$  separabel.

$$(2) f(x) = x^n - 1; Df(x) = nx^{n-1}$$

Annahme:  $\text{Char } F = 0$  oder  $\text{Char } F := p \nmid n$ . 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. (Sie heißen die  $n$  te Einheitswurzel.)

$$(3) f(x) = x^n - 1; \text{Char } F = p | n; Df(x) = nx^n - 1 \equiv 0 \Rightarrow f \text{ ist inseparabel.} \quad \square$$

### Korollar 2

Sei  $\text{Char } F = 0$ .

(i) Sei  $f \in F[x]$  irreduzibel (mit  $\deg f \geq 1$ ). Dann ist  $f$  separabel. Allgemeiner

(ii)  $f(x)$  ist separabel genau dann, wenn  $f = c \prod p_i(x); 0 \neq c \in F; p_i \neq p_j$  für  $i \neq j$   $p_i$  ist irreduzibel normiert.



**Beweis**

(i)  $f \neq 0 \Rightarrow Df \neq 0$  (weil  $\text{Char } F = 0$ ).

(ii) Verschiedene Irreduzible (normierte) können keine gemeinsame Nullstelle wegen Eindeutigkeit des Minimal-Polynoms in der Primfaktorisation

$$f = c \prod_{i=1}^k p_i(x) \quad p_i \neq p_j$$

haben. Außerdem hat keiner der Faktoren eine mehrfache Nullstelle (folgt aus (i)). Also hat  $f$  keine mehrfache Nullstelle.  $\square$

**Beispiel**

(4)  $f = x^2 - t \in \mathbb{F}_2(t)[x]$ .  $f$  ist irreduzibel, weil  $\sqrt{t} \notin \mathbb{F}_2(t)$ .

$Df \equiv 0$ , also ist  $f$  irreduzibel, aber inseparabel.

**Bemerkung**

Sei  $f(x) = g(x^p) \in F[x]$   $\text{Char } F = p > 0$ ;  $\deg f \geq 1$

i.e.  $f(x) = \gamma_m(x^p)^m + \dots + \gamma_1 x^p + \gamma_0$ . (\*)

Also  $Df(x) \equiv 0$  und  $f$  ist inseparabel.

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

**Proposition 1** (Übungsaufgabe)

Sei  $\text{Char } F = p > 0$ .

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

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

und  $\varphi : F \rightarrow F$

$$a \mapsto a^p$$

ist ein injektiver Körper-Homomorphismus (Frobenius).

**Korollar 3**

$\mathbb{F}$  ist endlich  $\Rightarrow \varphi : \mathbb{F} \rightarrow \mathbb{F}$

$$a \mapsto a^p$$

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 (siehe Korollar 4 aus "Lineare Algebra I", 13. Vorlesung vom 2.12.2011).

**Proposition 2**

Jedes irreduzible Polynom über einen endlichen Körper  $\mathbb{F}$  ist separabel. Ein Polynom  $f(x) \in \mathbb{F}[x]$  ( $\deg f \geq 1$ ) ist separabel  $\Leftrightarrow$  Produkt von paarweise verschiedenen irreduziblen Polynomen. (Korollar 2 gilt also auch für endliche Körper.)

**Beweis**

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

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

Berechne:

$$\begin{aligned} f(x) = g(x^p) &= a_m(x^p)^m + \cdots + a_1x^p + a_0 \\ &= b_m^p(x^m)^p + \cdots + b_1^p x^p + b_0^p \\ &= (b_mx^m)^p + \cdots + (b_1x)^p + b_0^p \\ &= (b_mx^m + \cdots + b_1x + b_0)^p \end{aligned}$$

Widerspruch. □

**Bemerkung**

Wichtig war:  $\mathbb{F}^p = \mathbb{F}$ .

**Definition**

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

**Proposition 3**

Proposition 2 gilt für  $F$  perfekt (anstatt  $\mathbb{F}$  endlich).

### Kapitel 3: (Endliche Gruppen)

#### Definition 1

Sei  $G$  eine Gruppe.  $H \subseteq G$  ist eine *Untergruppe*, falls  $H$  eine Gruppe ist (mit der Verknüpfung von  $G$ ), das heißt  $H \neq \emptyset; x, y \in H \Rightarrow xy \in H, x^{-1} \in H$ .

#### Definition 2

(i) Seien  $G, H$  Gruppen. Eine Abbildung  $\varphi : G \rightarrow H$  ist ein *Gruppenhomomorphismus*, wenn  $\varphi(xy) = \varphi(x)\varphi(y)$  ist für alle  $x, y \in G$ .

(ii) Ein bijektiver Homomorphismus heißt *Isomorphismus*.

**Notation:**  $|G| := \begin{cases} \# & \text{der Elemente in } G, \text{ falls } G \text{ endlich} \\ \infty & \text{sonst} \end{cases}$

### 15. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 17. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

#### Definition

(1)  $G$  ist eine Gruppe mit  $x \in G$ .

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

$|x|$  ist die *Ordnung von  $x$* , per Konvention  $|x^0| = 1$ .

(2)  $H$  ist *zyklisch*, wenn ein  $x \in H$  existiert mit

$$H = \langle x \rangle := \{x^n \mid n \in \mathbb{Z}\}$$

und  $x$  heißt *Erzeuger* der Gruppe  $H$  (additiv  $H = \langle x \rangle = \{nx \mid n \in \mathbb{Z}\}$ ).

#### Bemerkung

Eine zyklische Gruppe ist abelsch.

#### Proposition 1

$H = \langle x \rangle \Rightarrow |x| = |H|$ , das heißt

(1)  $|H| = n < \infty$  für  $n \in \mathbb{N}_0 \Leftrightarrow x^n = 1$  und  $x^i \neq x^j$  für  $i \neq j; i, j \in \{0, \dots, n-1\}$

(2)  $|H| = \infty$  genau dann, wenn  $x^i \neq x^j$  für alle  $i, j \in \mathbb{N}_0$  mit  $i \neq j$ .

#### Beweis

(1)  $|x| = n < \infty$ , wenn  $x^i = x^j$  mit  $0 \leq i < j < n \Rightarrow x^{j-i} = 1$  mit  $0 < j-i < n$  - Widerspruch.

Sei  $x^k \in \langle x \rangle; k = qn + r$  mit  $0 \leq r < n$ , also  $x^k = x^{nq+r} = (x^n)^q x^r = x^r$ .

(2)  $|x| = \infty$  und  $x^i = x^j$  mit  $i \neq j \Rightarrow x^{j-i} = 1$ . Also  $|x| \leq j-i$  - Widerspruch.  $\square$

#### Proposition 2

Sei  $G$  eine Gruppe mit  $x \in G$  und  $m, n \in \mathbb{Z}$ . Es gelten  $x^n = 1$  und  $x^m = 1 \Rightarrow x^d = 1$  für  $d = \text{ggT}(m, n)$ . Insbesondere  $x^m = 1$  mit  $m \in \mathbb{Z} \Rightarrow |x| \mid m$ .

#### Beweis

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

**Proposition 3**

Zyklische Gruppen derselben Ordnung sind isomorph.

**Beweis**

(1) Sei  $|G| = |H| = n$ ,  $G = \langle x \rangle$  und  $H = \langle y \rangle$ . Betrachte

$$\begin{aligned} \varphi : G &\rightarrow H \\ x^k &\mapsto y^k \end{aligned}$$

$\varphi$  ist wohldefiniert, weil  $x^r = x^s \Rightarrow x^{r-s} = 1 \Rightarrow n|r-s \Rightarrow nr = ns$   
 $\Rightarrow y^{(r-s)} = (y^n)^t = 1 \Rightarrow y^r y^{-s} = 1 \Rightarrow y^r = y^s$ .

Es ist klar, dass  $\varphi$  ein Homomorphismus und auch surjektiv ist. Da beide Gruppen die gleiche Ordnung haben und endlich sind, folgt das  $\varphi$  injektiv ist.

(Eine Abbildung  $\varphi : S \rightarrow S$  ( $S$  ist eine endliche Menge) ist injektiv  $\Leftrightarrow$  sie ist surjektiv  $\Leftrightarrow$  sie ist bijektiv).

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

$$\begin{aligned} \varphi : G &\rightarrow H \\ x^k &\mapsto y^k \end{aligned}$$

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

**Beispiel**

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

**Erzeuger****Proposition 4** (Übungsblatt)

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

**Proposition 5**

Sei  $H = \langle x \rangle$  und  $j \in \mathbb{N}$ .

- (1)  $|x| = \infty$ , dann ist  $x^j$  Erzeuger genau dann, wenn  $j = \pm 1$
- (2)  $|x| < \infty$ , dann ist  $x^j$  Erzeuger genau dann, wenn  $|x| = n$  und  $\text{ggT}(j, n) = 1$ .

**Beweis**

(1) Übungsaufgabe

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

**Korollar 6**

$|H| = n$ ;  $H$  ist zyklisch, dann ist die Anzahl der Erzeuger von  $H = \varphi(x)$  (Euler).

**Satz 7**

Sei  $H = \langle x \rangle$  zyklisch.

- (1)  $K \leq H \Rightarrow K$  zyklisch, das heißt  $K = \langle x^d \rangle$  (oder  $K = \{1\}$ ), wobei  $d$  die kleinste  $d \in \mathbb{N}$  mit  $x^d \in K$ .
- (2)  $|H| = \infty \Rightarrow \langle x^j \rangle \neq \langle x^i \rangle$  für  $i \neq j; i, j \in \mathbb{N}_0$ .
- (3)  $|H| = n < \infty; j \in \mathbb{N}_0; j|n \Rightarrow \exists! K \leq H; K$  zyklisch;  $|K| = j$  und  $K = \langle x^{\frac{n}{j}} \rangle$

## 16. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 20. Dezember 2012

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### Satz 1

Sei  $H = \langle x \rangle$  zyklisch

- (1) Sei  $K \leq H$ , dann ist  $K$  zyklisch.
- (2) Wenn  $|H| = \infty$ , dann sind  $\langle x^j \rangle \neq \langle x^i \rangle$  für  $i \neq j$  und  $\{\langle x^i \rangle \mid i \in \mathbb{N}_0\}$  ist die Menge aller Teilgruppen von  $H$ . (Übungsaufgabe).
- (3) Wenn  $|H| = n < \infty$  und  $a \in \mathbb{N}$  mit  $a|n$ , dann gibt es eine eindeutige Teilgruppe der Ordnung  $a$ , nämlich  $\langle x^{n/a} \rangle$  und  $\{\langle x^d \rangle \mid d|n\}$  ist die Menge aller Teilgruppen von  $H \neq \{1\}$ .

### 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  $\langle x^k \rangle \leq K$ .

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  $x^a = (x^k)^q \in \langle x^k \rangle$ .

Also  $K \leq \langle x^k \rangle$ .

- (3) Sei  $d := \frac{n}{a}$ , also  $d|n$  und  $|x^d| = \frac{n}{\text{ggT}(n,d)} = n/d = n/(n/a) = a$ . Somit ist  $|\langle x^d \rangle| = a$ .

**Eindeutigkeit:** Sei  $K \leq H$  mit  $|K| = a$  und  $b \in \mathbb{N}$  kleinste, so dass  $K = \langle x^b \rangle$ . Wir berechnen  $\frac{n}{d} = a = |K| = |x^b| = \frac{n}{\text{ggT}(n,b)}$ . Daraus folgt  $d = \text{ggT}(n,b)$ , insbesondere  $d|b$ . Also  $x^b \in \langle x^d \rangle$  und  $K = \langle x^b \rangle \leq \langle x^d \rangle$ .

Da aber  $|K| = a = |\langle x^d \rangle|$ , folgt nun  $K = \langle x^d \rangle$ . □

### Proposition 2

Sei  $\mathcal{A}$  eine nichtleere Menge von Teilgruppen, 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 1**

Sei  $S \subseteq H$  eine Untermenge;  $\mathcal{A} := \{K \leq H; S \subseteq K\}$ .

Definiere  $\langle S \rangle = \bigcap \mathcal{A}$ .  $\langle S \rangle$  ist die (für die Inklusion) kleinste Teilgruppe von  $H$ , die  $S$  enthält.  $\langle S \rangle$  heißt die *Teilgruppe, die von  $S$  erzeugt ist*.

**Konvention:**  $\langle \emptyset \rangle = \{1\}$

**Notation:**  $S = \{a_1, \dots, a_n\}; \langle S \rangle = \langle a_1, \dots, a_n \rangle$  (wenn  $S$  endlich ist).

**Proposition 3**

Sei  $S \neq \emptyset$ .  $\langle S \rangle = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}; n \in \mathbb{N}; a_i \in S; \varepsilon_i = \pm 1\}$ .

**Beweis**

Übungsaufgabe zu zeigen: Diese Menge ist eine Teilgruppe. Sie enthält  $S$  und muss in jeder Teilgruppe, die  $S$  enthält enthalten sein.  $\square$

Spezialfall: Wenn  $H$  abelsch. (Übungsaufgabe, Übungsblatt).

**Proposition 4**

Sei  $\varphi : G \rightarrow H$  ein Homomorphismus. Es gelten

$$(1) \varphi(1) = 1$$

$$(2) \varphi(g^{-1}) = \varphi(g)^{-1}$$

$$(3) \varphi(g^n) = \varphi(g)^n \text{ für alle } n \in \mathbb{Z}$$

$$(4) \ker \varphi := \{g \in G; \varphi(g) = 1\} \leq G$$

$$(5) \operatorname{im} \varphi := \{h \in H; \exists g \in G : \varphi(g) = h\} \leq H$$

Wir wollen Faktorengruppen definieren.

**Definition 2**

Sei  $H \leq G$  und  $g \in G$ .

$gH := \{gh \mid h \in H\}$  ist die linke Nebenklasse von  $g$  bezüglich  $H$  und  $Hg := \{hg \mid h \in H\}$  ist die rechte Nebenklasse.

**Additive Notation:**  $g + H$  und  $H + g$

**Proposition 5**

Sei  $H \leq G$ . Es gelten:

$$(1) \text{ Die Menge der linken Nebenklassen bilden eine Partition von } G \text{ i.e. } G = \bigcup_{g \in G} gH$$

$$\text{und } uH \cap vH \neq \emptyset \Rightarrow uH = vH.$$

$$(2) \text{ Für alle } u, v \in G : uH = vH \Leftrightarrow v^{-1}u \in H.$$



**Beweis**

(1)  $1 \in H$ , also  $g \in gH$  für alle  $g \in G$ . Also  $G = \bigcup gH$ . Wenn  $uH \cap vH \neq \emptyset$ . 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  $ut = v(h_2 h_1^{-1} t) = v(h_2 h_1^{-1} t) \in vH$ , so dass  $uH \subseteq vH$ .

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  $v^{-1}u \in H$ .  $\square$

**Proposition 6**

Sei  $N \leq G$ . Die Verknüpfung

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

ist wohldefiniert genau dann, wenn

$$ghg^{-1} \in N \text{ für alle } g \in G; \text{ für alle } h \in N \quad (*)$$

**Beweis**

“ $\Rightarrow$ ” Wohldefiniert  $\rightarrow$

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

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 geeignete  $n_1 \in N$ . Also  $gn_1g^{-1} = n_1 \in N$ .

“ $\Leftarrow$ ” Sei  $u, u_1 \in uN, v, v_1 \in vN$ . Zu zeigen:  $(uv)N = (u_1 v_1)N$ .

Schreibe  $u_1 = un, v_1 = vm; n, m \in N$ . Wir zeigen:  $u_1 v_1 \in (uv)N$ .

Wir berechnen:  $u_1 v_1 = (un)(vm) = u(vv^{-1})nvm = uv \underbrace{(v^{-1}nv)}_{:=n_1 \in N} m = uvn_1 m = uv \underbrace{(n_1 m)}_{\in N} \square$

**Zusatz zu Proposition 6**

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

**Definition**

Sei  $N \leq G$ .  $N$  ist normal, falls (\*) in Proposition 6 gilt. Schreibe  $N \triangleleft G$ .

**Beispiel**

Sei  $\varphi$  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  $n \in N$ .

Umgekehrt: Sei  $G/N$  die Gruppe der linken Nebenklassen für ein  $N \triangleleft G$ .

**Proposition 7**

$$\varphi: G \rightarrow G/N$$

$$g \mapsto gN$$

ist ein surjektiver Gruppenhomomorphismus mit  $\ker \varphi = N$ .

# 1 Lagrange's theorem

**Definition 1.1.** The *index* of a subgroup  $H$  in a group  $G$ , denoted  $[G : H]$ , is the number of left cosets of  $H$  in  $G$  ( $[G : H]$  is a natural number or infinite).

**Theorem 1.2** (Lagrange's Theorem). If  $G$  is a finite group and  $H$  is a subgroup of  $G$  then  $|H|$  divides  $|G|$  and

$$[G : H] = \frac{|G|}{|H|}.$$

*Proof.* Recall that (see lecture 16) any pair of left cosets of  $H$  are either equal or disjoint. Thus, since  $G$  is finite, there exist  $g_1, \dots, g_n \in G$  such that

- $G = \cup_{i=1}^n g_i H$  and
- for all  $1 \leq i < j \leq n$ ,  $g_i H \cap g_j H = \emptyset$ .

Since  $n = [G : H]$ , it is enough to now show that each coset of  $H$  has size  $|H|$ .

Suppose  $g \in G$ . The map  $\varphi_g : H \rightarrow gH : h \mapsto gh$  is surjective by definition. The map  $\varphi_g$  is injective; for whenever

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

, multiplying on the left by  $g^{-1}$ , we have that  $h_1 = h_2$ . Thus each coset of  $H$  in  $G$  has size  $|H|$ .

Thus

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

□

Note that in the above proof we could have just as easily worked with right cosets. Thus if  $G$  is a finite group and  $H$  is a subgroup of  $G$  then the number of left cosets is equal to the number of right cosets. More generally, the map  $gH \mapsto Hg^{-1}$  is a bijection between the set of left cosets of  $H$  in  $G$  and the set of right cosets of  $H$  in  $G$ .

**Corollary 1.3.** *Let  $G$  be a finite group. For all  $x \in G$ ,  $|x|$  divides  $|G|$ . In particular, for all  $x \in G$ ,  $x^{|G|} = 1$ .*

*Proof.* By Lagrange's theorem  $|x| = |\langle x \rangle|$  divides  $|G|$ . □

**Corollary 1.4.** *Every group of prime order is cyclic.*

*Proof.* Let  $G$  be a finite group with  $|G|$  prime. Take  $x \in G \setminus \{1\}$ . By Lagrange,  $|x|$  divides  $|G|$  and thus, since  $|G|$  is prime,  $|x| = |G|$  or  $|x| = 1$ . Since  $x \neq 1$ ,  $|x| \neq 1$ . Thus  $|x| = |G|$  and so,  $\langle x \rangle = G$ . □

**Example:** The converse of Lagrange's theorem does not hold. The group  $A_4$  is of size 12 and has no subgroup of size 6. See exercise sheet 8 (Recall from linear algebra that  $A_4$  is the group of all even permutations on 4 elements concretely: the set of permutations

$(123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23), e$ ).

**Definition 1.5.** *Let  $G$  be a group and  $S, T$  subsets of  $G$ . We write*

$$ST := \{st \mid s \in S \text{ and } t \in T\}.$$

**Proposition 1.6.** *If  $K$  and  $H$  are subgroups of a finite group  $G$  then*

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

*Proof.* Let  $\varphi : H \times K \rightarrow HK$  be the map defined by  $\varphi(h, k) := hk$ . This map is surjective by definition.

**Claim:** If  $h \in H$  and  $k \in K$  then  $\varphi^{-1}(hk) = \{(hd^{-1}, dk) \mid d \in K \cap H\}$ .

Clearly, if  $d \in K \cap H$  and  $h' = hd^{-1}, k' = dk$  then  $h' \in H, k' \in K$  and  $h'k' = hk$ . Conversely, if  $h' \in H, k' \in K$  and  $h'k' = hk$  then  $k'k^{-1} = h'^{-1}h \in K \cap H, h' = h(h'^{-1}h)^{-1}$  and  $k' = (h'^{-1}h)k$ . This proves the claim.

Therefore for each  $x \in HK$ ,  $|\varphi^{-1}(x)| = |H \cap K|$ . So,

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

□

**Proposition 1.7.** *Let  $H$  and  $K$  be subgroups of a group  $G$ . The set  $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ .*

*Proof.* Suppose  $h \in H$  and  $k \in K$ . Then  $(hk)^{-1} = k^{-1}h^{-1} \in KH$ . Thus  $g \in HK$  if and only if  $g^{-1} \in KH$ . So, if  $HK$  is a subgroup then  $HK = KH$ .

Suppose  $HK = KH$ . Take  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ . Consider  $h_1k_1h_2k_2$ . Since  $k_1h_2 \in KH = HK$ , there exist  $h_3 \in H$  and  $k_3 \in K$  such that  $k_1h_2 = h_3k_3$ . Thus  $h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 \in HK$ . So  $HK$  is closed under multiplication.

From above we know that if  $g \in HK$  then  $g^{-1} \in KH = HK$ . Thus, since  $HK$  is non-empty, it is a subgroup of  $G$ .  $\square$

**Definition 1.8.** *Let  $G$  be a group and  $A$  a subgroup of  $G$ . The normaliser,  $N_G(A)$ , of  $A$  in  $G$  is the set of  $x \in G$  such that  $xAx^{-1} = A$ .*

**Remark 1.9.** *Let  $A \leq B \leq G$  be groups. Note that  $N_G(A)$  is a subgroup of  $G$  containing  $A$ ; in fact, it is the largest subgroup of  $G$  in which  $A$  is normal.*

*The subgroup  $A$  is normal in  $B$  if and only if  $B \leq N_G(A)$ . In particular,  $A$  is normal in  $G$  if and only if  $N_G(A) = G$ . (Please convince yourself that this is true)*

**Corollary 1.10.** *If  $H$  and  $K$  are subgroups of  $G$  and  $H \leq N_G(K)$ , then  $HK$  is a subgroup of  $G$ . In particular, if  $K \trianglelefteq G$  then  $HK \leq G$  for any  $H \leq G$ .*

*Proof.* It is enough to show that  $HK = KH$ . Suppose that  $h \in H$  and  $k \in K$ . Then  $h^{-1}kh, hkh^{-1} \in K$  since  $H \leq N_G(K)$ . Thus  $hk = (hkh^{-1})h \in KH$  and  $kh = h(h^{-1}kh) \in HK$ . Thus  $HK = KH$ .  $\square$

## 2 Isomorphism theorems

**Theorem 2.1.** *If  $\varphi : G \rightarrow H$  is a homomorphism of groups, then  $\ker\varphi \trianglelefteq G$  and*

$$G/\ker\varphi \cong \text{im}\varphi.$$

*Proof.* We have already seen that the kernel of a homomorphism of groups is normal.

Define  $f : G/\ker \varphi \rightarrow H$  by  $f(a \ker \varphi) = \varphi(a)$ .

This map is well-defined since: if  $a \ker \varphi = b \ker \varphi$  then  $ab^{-1} \in \ker \varphi$ .

So  $1 = \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}$ . Thus  $\varphi(a) = \varphi(b)$ .

The map  $f$  is a homomorphism since:

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

The image of  $f$  is clearly equal to the image of  $\varphi$ . Lastly,  $f$  is injective for if  $f(a \ker \varphi) = f(b \ker \varphi)$  then  $\varphi(a) = \varphi(b)$  and so  $\varphi(ab^{-1}) \in \ker \varphi$  i.e.  $a \ker \varphi = b \ker \varphi$ .

Thus  $f$  gives a bijective group homomorphism from  $G/\ker \varphi$  to  $\text{im} \varphi$ .  $\square$

**Corollary 2.2.** *Let  $\varphi : G \rightarrow H$  be a homomorphism of groups.*

1.  $\varphi$  is injective if and only if  $\ker \varphi = 1$
2.  $|G : \ker \varphi| = |\varphi(G)|$

*Proof.* (1) The forward direction follows directly from the definition of injective. Suppose  $\ker \varphi = 1$  and  $\varphi(a) = \varphi(b)$ . Then  $\varphi(ab^{-1}) = 1$ . So  $ab^{-1} = 1$  and thus  $a = b$ .

(2)  $|G : \ker \varphi| = |G/\ker \varphi| = |\varphi(G)|$ .  $\square$

**Theorem 2.3** (The second isomorphism theorem). *Let  $G$  be a group and let  $A$  and  $B$  be subgroups of  $G$  with  $A \leq N_G(B)$ . Then  $AB$  is a subgroup of  $G$ ,  $B \trianglelefteq AB$ ,  $A \cap B \trianglelefteq A$  and  $AB/B \cong A/A \cap B$ .*

*Proof.* Since  $A \leq N_G(B)$ ,  $AB$  is a subgroup of  $G$ . Since  $B \leq N_G(B)$ ,  $AB \leq N_G(B)$ ; that is  $B$  is normal in  $AB$ .

Consider the canonical projection  $\pi : AB \rightarrow AB/B$ . If  $a \in A$  and  $\varphi(a) = 1$  then  $a \in B$ . Thus  $a \in A \cap B$ . So  $\pi$  restricted to  $A$  has kernel  $A \cap B$  (and thus is normal). Now suppose  $a \in A$  and  $b \in B$ . We have that  $\pi(a) = \pi(ab)$ . Thus  $\pi$  restricted to  $A$  is surjective i.e.  $\text{im} \pi|_A = AB/B$ . So by first iso theorem  $AB/B \cong A/A \cap B$ .  $\square$

**Theorem 2.4** (The third isomorphism theorem). *Let  $G$  be a group and let  $H$  and  $K$  be normal subgroups with  $H \leq K$ . Then  $K/H \trianglelefteq G/H$  and*

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

*Proof.* Consider the map  $f : G/H \rightarrow G/K$  defined by  $f(gH) = gK$ . This map is well defined: If  $g_1H = g_2H$  then  $g_1^{-1}g_2 \in H$  and thus  $g_1^{-1}g_2 \in K$ . So  $g_1K = g_2K$ .

This map is a group homomorphism since

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

It is clearly surjective. Suppose  $a \in G$ . Then  $f(aH) = 1K$  if and only if  $aK = 1K$ ; that is if and only if  $a \in K$ . Thus  $K/H$  is the kernel of  $f$  and so  $K/H$  is normal in  $G/H$  and

$$(G/H)/(K/H) \cong G/K$$

□

# 1 Useful English/German Vocabulary

simple group -einfache Gruppe  
 normal series - Normalreihe  
 composition series - Kompositionsreihe  
 refinement - Verfeinerung

# 2 Isomorphism theorems continued

**Theorem 2.1** (Lattice isomorphism theorem). *Let  $G$  be a group and let  $N$  be a normal subgroup of  $G$ . If  $A$  is a subgroup of  $G$  containing  $N$ , let  $\bar{A} := A/N$ . Let  $\pi : G \rightarrow G/N$  be the canonical projection.*

*The map  $A \mapsto \pi(A) = \bar{A}$  is a bijection between the set of subgroups of  $G$  containing  $N$  and the set of subgroups of  $G/N$ .*

*Moreover, if  $A, B \leq G$  with  $N \leq A$  and  $N \leq B$  then:*

1.  $A \leq B$  if and only if  $\bar{A} \leq \bar{B}$ ; and in this case  $[B : A] = [\bar{B} : \bar{A}]$
2.  $A \triangleleft B$  if and only if  $\bar{A} \triangleleft \bar{B}$ ; and in this case  $B/A \cong \bar{B}/\bar{A}$
3.  $\overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$
4.  $\overline{A \cap B} = \bar{A} \cap \bar{B}$

*Proof.* UB9

□

**Theorem 2.2** (Butterfly Lemma /Zassenhaus Lemma). *Let  $a \triangleleft A$  and  $b \triangleleft B$  be subgroups of a group  $G$ . Then*

- $a(A \cap b)$  is a normal in  $a(A \cap B)$ ,
- $b(B \cap a)$  is normal in  $b(B \cap A)$ ,
- $(A \cap b)(B \cap a)$  is normal in  $(A \cap B)$



and

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

*Proof.* Note first that since  $A \leq N_G(a)$  and  $B \leq N_G(b)$ , we have that

$$A \cap b \leq A \cap B \leq N_G(a)$$

and

$$B \cap a \leq A \cap B \leq N_G(b).$$

Thus  $a(A \cap b)$ ,  $a(A \cap B)$ ,  $b(B \cap a)$  and  $b(B \cap A)$  are subgroups of  $G$  (see lecture 17 corollary 1.10).

We first show that

$$(A \cap b)(B \cap a) \text{ is normal in } (A \cap B).$$

First note that  $A \cap b$  and  $B \cap a$  are normal in  $A \cap B$ ; if  $g \in A \cap B$  and  $c \in A \cap b$  then  $gcg^{-1} \in b$  since  $b \triangleleft B$  and  $gcg^{-1} \in A$  since  $g, c \in A$ . Thus  $(A \cap b)(B \cap a)$  is a subgroup of  $A \cap B$ . In fact it is a normal subgroup since if  $c_1 \in A \cap b$ ,  $c_2 \in B \cap a$  and  $g \in A \cap B$  then  $gc_1c_2g^{-1} = gc_1g^{-1}gc_2g^{-1} \in (A \cap b)(B \cap a)$ .

If  $x \in a(A \cap B)$  then  $x = \alpha\gamma$  where  $\alpha \in a$  and  $\gamma \in A \cap B$ . Define

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

by

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

The map  $f$  is well-defined for if  $\alpha\gamma = \alpha'\gamma'$  with  $\alpha, \alpha' \in a$  and  $\gamma, \gamma' \in A \cap B$  then  $\gamma'\gamma^{-1} = (\alpha')^{-1}\alpha \in a \cap A \cap B = a \cap B \leq (A \cap b)(B \cap a)$ ; i.e.

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

The map is a homomorphism: if  $\alpha, \alpha' \in a$  and  $\gamma, \gamma' \in A \cap B$  then  $\alpha, \gamma\alpha'\gamma^{-1} \in a$  since  $a \triangleleft A$ . So

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

and since  $(A \cap b)(B \cap a)$  is normal in  $A \cap B$

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

The map  $f$  is surjective by definition.

It remains to find the kernel: if  $\alpha \in a$  and  $\gamma \in A \cap B$  are such that  $f(\alpha\gamma) = 1(A \cap b)(B \cap a)$  then  $\gamma \in (A \cap b)(B \cap a) = (B \cap a)(A \cap b)$ . Take  $x \in (B \cap a)$  and  $y \in (A \cap b)$  such that  $\gamma = xy$ . Then  $\alpha\gamma = (\alpha x)\gamma \in a(A \cap b)$ .

Conversely, if  $\alpha \in a$  and  $\gamma \in A \cap B$  with  $\alpha\gamma \in a(A \cap b)$  then there exist  $t \in a$  and  $s \in A \cap b$  such that  $\alpha\gamma = ts$ . Now  $\alpha^{-1}t \in a$  and since  $\gamma, s \in B$ ,  $\alpha^{-1}t = \gamma s^{-1} \in B$ . Thus  $\alpha^{-1}ts = \gamma \in (A \cap b)(B \cap a)$ . So  $\alpha\gamma \in \ker f$ .

So by the first isomorphism theorem,  $a(A \cap b)$  is normal in  $a(A \cap B)$  and

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

Exchanging the roles of  $A$  and  $B$  respectively  $a$  and  $b$ , we get that  $b(B \cap a)$  is normal in  $b(B \cap A)$  and

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

□

### 3 Jordan-Hölder and Simple and Solvable groups

**Definition 3.1.** A group  $G$  is simple if  $|G| > 1$  and the only normal subgroups of  $G$  are 1 and  $G$ .

**Remark:** A non-trivial abelian group  $G$  is simple if and only if its only subgroups are 1 and  $G$  (recall: all subgroups of abelian groups are normal).

Thus, if  $G$  is simple and abelian then it is generated by every non-identity element of  $G$ . So  $G$  is cyclic. Recall that if  $G$  is infinite and  $x$  generates  $G$  then  $x^2$  does not generate  $G$  (lecture 15 Proposition 5(1)). Thus  $G$  is finite. Moreover, if  $p \in \mathbb{N}$ , a prime, divides  $|x|$  then  $|x^p| < |x|$  (see lecture 15 Proposition 4(3)) and therefore  $x^p = 1$ . Thus  $|G| = p$ . Thus an abelian group is simple if and only if it is finite and of prime order.

**Definition 3.2.** Let  $G$  be a group. A sequence of subgroups

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

is called a **normal series** if  $G_i$  is normal in  $G_{i+1}$ ; we call the quotient groups  $G_{i+1}/G_i$  **factor groups** of the series.

A normal series is called a **composition series** if each of the quotient groups  $G_{i+1}/G_i$  are simple; in this case we call the quotient groups **composition factors** of  $G$  (we will see later that the factor groups really do only depend on  $G$ ).

A normal series

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_s = G$$

is a **refinement** of a normal series

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_r = G$$

if  $H_0, \dots, H_r$  is a subsequence of  $G_0, \dots, G_s$ .

**Example:** Since  $A_4$  is index 2 in  $S_4$ ,  $A_4$  is normal in  $S_4$ . You will show on the exercise sheet that the subgroup

$$V := \{(12)(34), (13)(24), (14)(23), e\}$$

is normal in  $A_4$ . So

$$\{1\} \triangleleft V \triangleleft A_4 \triangleleft S_4$$

is a normal series for  $S_4$ . Its factor groups are  $\mathbb{Z}_2$  and  $\mathbb{Z}_3$ . So it is in fact a composition series.

**Definition 3.3.** *Two normal series are said to be **equivalent** if there is a bijection between their factor groups such that corresponding factor groups are isomorphic.*

**Example:**

Consider the following two composition series of  $\mathbb{Z}_{30}$ :

$$\mathbb{Z}_{30} \geq \langle 5 \rangle \geq \langle 10 \rangle \geq \{0\}$$

$$\mathbb{Z}_{30} \geq \langle 3 \rangle \geq \langle 6 \rangle \geq \{0\}$$

The composition factors of the first series are  $\mathbb{Z}_{30}/\langle 5 \rangle \cong \mathbb{Z}_5$ ,  $\langle 5 \rangle/\langle 10 \rangle \cong \mathbb{Z}_2$  and  $\langle 10 \rangle/\{0\} \cong \mathbb{Z}_3$ .

The composition factors of the second series are  $\mathbb{Z}_{30}/\langle 3 \rangle \cong \mathbb{Z}_3$ ,  $\langle 3 \rangle/\langle 6 \rangle \cong \mathbb{Z}_2$  and  $\langle 6 \rangle/\{0\} \cong \mathbb{Z}_5$ .

So the above composition series are equivalent.

**Theorem 3.4** (Schreier Refinement Theorem). *Any two normal series of a group  $G$  have equivalent refinements.*

*Proof.* Let

$$1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_s = G$$

and

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_r = G$$

be normal series.

Let  $G_{i,j} := G_i(G_{i+1} \cap H_j)$  for  $0 \leq j \leq r$ . So

$$G_{i,0} = G_i\{1\} = G_i \text{ and } G_{i,r} = G_i(G_{i+1} \cap G) = G_{i+1}.$$

Since  $G_i \triangleleft G_{i+1}$  and  $H_j \triangleleft H_{j+1}$ , by Zassenhaus (with  $a = G_i$ ,  $A = G_{i+1}$ ,  $b = H_j$  and  $B = H_{j+1}$ ),

$$G_{i,j} = G_i(G_{i+1} \cap H_j) \triangleleft G_i(G_{i+1} \cap H_{j+1}) = G_{i,j+1}.$$

Thus the following series is a refinement of the first normal series:

$$\{1\} = G_{0,0} \triangleleft G_{0,1} \triangleleft \dots \triangleleft G_{0,r} = G_{1,0} \triangleleft G_{1,1} \triangleleft \dots \triangleleft G_{s-1,r} = G_s = G$$

Let  $H_{i,j} := H_i(H_{i+1} \cap G_j)$  for  $0 \leq j \leq s$ .

Exactly as above,

$$\{1\} = H_{0,0} \triangleleft H_{0,1} \triangleleft \dots \triangleleft H_{0,s} = H_{1,0} \triangleleft H_{1,1} \triangleleft \dots \triangleleft H_{r-1,s} = H_r = G$$

is a refinement of the second normal series.

It remains now just to note that by the Zassenhaus lemma (with  $a = G_i$ ,  $A = G_{i+1}$ ,  $b = H_j$  and  $B = H_{j+1}$ )

$$G_i(G_{i+1} \cap H_{j+1})/G_i(G_{i+1} \cap H_j) \cong H_j(H_{j+1} \cap G_{i+1})/H_j(H_{j+1} \cap G_i);$$

that is

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

□

**Theorem 3.5** (Jordan-Hölder Theorem). *Let  $G$  be a finite group with  $G \neq \{1\}$ . Then*

1.  *$G$  has a composition series and*
2. *all composition series of  $G$  are equivalent.*

*Proof.* (1) Suppose  $G$  is not simple. If  $N$  is a maximal normal subgroup of  $G$  then, by the correspondence theorem,  $G/N$  is simple. If  $G$  is finite  $G$  has a maximal normal subgroup. Thus, by induction on  $|G|$ , every finite group has a composition series.

(2) Composition series have no refinements by the correspondence theorem; that is, if  $G_{i+1} \triangleright N \triangleright G_i$  then  $N/G_i \triangleleft G_{i+1}/G_i$  and if  $G_{i+1}/G_i$  is simple then  $N = G_{i+1}$  or  $N = G_i$ . By the Schreier Refinement Theorem, every two normal series have equivalent refinements. Thus every two composition series of  $G$  are equivalent.

□

## 19. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 14. Januar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

In dieser Vorlesung wurde hauptsächlich die 18. Vorlesung kurz wiederholt und die Begriffe auf Deutsch nochmals zusammengefasst.

### Definition 1

(1) Eine Gruppe  $G \neq \{1\}$  ist *einfach*, wenn die einzigen Normalteiler nur  $\{1\}$  und  $G$  sind.

(2)  $\{1\} = H_0 \leq \dots \leq H_s = G$  ist eine *Normalreihe*, wenn  $H_i \triangleleft H_{i+1}$ .

**Notation:**  $H \triangleleft G$  "H Normalteiler in G" wird auch so bezeichnet:  $G \triangleleft H$  "H  $\leq G$  ist Normateiler"

(3)  $H_{i+1}/H_i; i = 0, \dots, s_1$  sind die *Faktorgruppen* oder die *Faktoren* oder die *Quotienten* der Normalreihe

(4) Die Normalreihe heißt *Kompositionsreihe*, falls alle Faktoren einfach sind.

(5) Zwei Reihen

$$H_0 \triangleleft \dots, \triangleleft H_i \triangleleft H_{i+1} \triangleleft \dots \triangleleft G$$

$$\text{und } K_0 \triangleleft \dots, \triangleleft K_j \triangleleft K_{j+1} \triangleleft \dots \triangleleft G$$

sind *äquivalent*, wenn es eine Bijektion  $i \rightarrow j$  gibt, so dass die korrespondierenden Faktoren isomorph sind:  $H_{i+1}/H_i \simeq K_{j+1}/K_j$ .

(Ende der Wiederholung der 18. Vorlesung.)

### Definition 2

$G$  heißt *auflösbar* (englisch: solvable), wenn es eine *Normalreihe mit abelschen Faktoren* hat.

### Erinnerung

(i)  $S_n$  ist nicht abelsch für  $n \geq 3$ .

(ii)  $A_n$  ist nicht abelsch für  $n \geq 4$ .

Begründung: (123) und (234) kommutieren nicht.

**Beispiele**

$S_n$  ist auflösbar für  $n \leq 4$

(a)  $S_3 \triangleright A_3 \triangleright \{1\}$

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

(b)  $S_4 \triangleright A_4 \triangleright V \triangleright W \triangleright \{1\}$ , wobei  $V = \{(1), (12)(34), (13)(24), (14)(23)\}$  die *kleinsche Vierergruppe* ist und  $W := \{1, (12)(34)\}$ .

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



## 20. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 17. Januar 2013

Wir werden später zeigen, dass  $S_n$  nicht auflösbar ist für  $n \geq 5$  (Galois).

### Bemerkung

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

Wir wollen nun auflösbare Gruppen charakterisieren.

### Definition 1

(a) Für  $g, h \in G$  definiere  $(g, h) := g^{-1}h^{-1}gh \in G$ .  $(g, h)$  heißt *Kommutator* von  $g$  und  $h$ .

#### Bemerkung 1

(i)  $gh = hg(g, h)$

(ii)  $(G, G)$  ist die *Kommutatorgruppe* von  $G$  und ist die Untergruppe, die durch  $S := \{(g, h); g, h \in G\}$  erzeugt wird.

#### Bemerkung 2

(i)  $(g, h) = (h, g)^{-1}$ , also ist  $\langle S \rangle = \{S_1 \cdots S_n \mid n \in \mathbb{N}; S_i \text{ ist ein Kommutator in } G\}$ .

(ii)  $G$  ist abelsch genau dann, wenn  $(G, G) = \{1\}$ .

**Notation:**  $(G, G) := G'$ .

(b) Wir definieren die iterierte Kommutatoren folgendermaßen:  $G'' := (G')'$ .

Per Induktion über  $k \in \mathbb{N}$ :  $G^{(k)} := (G^{(k-1)})'$ .

Wir werden nun die iterierte Kommutatoren ausnutzen, um unsere Charakterisierung zu geben.

### Proposition 1

Seien  $G, \bar{G}$  Gruppen und  $\eta : G \rightarrow \bar{G}$  ein Homomorphismus. Es gelten

1.  $\eta(g, h) = (\eta(g), \eta(h))$

2.  $\eta(G') \subseteq \bar{G}'$

3. Wenn  $\eta$  surjektiv ist, gilt ferner:  $\eta(G') = \bar{G}'$

4. Insbesondere für einen beliebigen Homomorphismus  $\eta$  gilt:  $\eta(G') = \eta(G)'$

**Zusatz:** 5. Allgemeiner gilt  $\eta(G^{(k)}) = \eta(G)^{(k)}$  für alle  $k \in \mathbb{N}$

**Beweis 1**

1.  $\eta(g, h) = \eta(g^{-1}h^{-1}gh) = \eta(g)^{-1}\eta(h)^{-1}\eta(g)\eta(h) = (\eta(g), \eta(h))$ .
2. Also aus 1. folgt unmittelbar  $\eta(G') \subseteq \overline{G'}$ .
3. Wenn  $\eta$  surjektiv ist, folgt aus 1. dass jeder Kommutator in  $\overline{G}$  liegt in  $\eta(G')$ . Es folgt also aus Bemerkung 2, dass  $\eta(G') \supseteq \overline{G'}$  und damit ist die Gleichheit bewiesen.
4. Klar, da  $\eta : G \rightarrow \eta(G)$  surjektiv ist.
5.  $\eta(G') = \eta(G)'$  ist 4.

Nun betrachte  $\eta : G' \rightarrow \overline{G}$  und 4. nochmal angewendet ergibt:

$$\eta((G')') = \eta(G')'$$

$$\text{i.e. } \eta(G'') = (\eta(G'))' = \eta(G)''$$

usw. per Induktion fortsetzen. □

**Proposition 2**

$K \triangleleft G \Rightarrow K' \triangleleft G$  (insbesondere:  $G' \triangleleft G$ ).

**Beweis**

Sei  $a \in G$  fest und betrachte  $\eta_a : K \rightarrow K$  wohldefiniert (weil  $K$  ein Normalteiler) und ein Homomorphismus  $k \mapsto aka^{-1}$ .

Aus Proposition 1 folgt:  $\eta_a(K') \subseteq K'$  für alle  $a \in G$ , aber das bedeutet  $K' \triangleleft G$ . □

Wir haben also  $G \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(k)} \triangleright G^{(k+1)} \triangleright \dots$ .

Wir wollen zeigen, dass  $G$  auflösbar ist  $\Leftrightarrow \exists k \geq 1$  mit  $G^{(k)} = \{1\}$ .

Dafür brauchen wir:

**Lemma**

Sei  $K \triangleleft G$ . Es gilt  $G/K$  ist abelsch  $\Leftrightarrow K \supseteq G'$ . Insbesondere  $G/G'$  ist abelsch und  $G'$  ist die kleinste normale Untergruppe mit dieser Eigenschaft.

**Beweis**

Aus Bemerkung 1 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  $g, h \in G \Leftrightarrow G' \subseteq K$ .

**Bemerkung 3**

Wir erhalten  $G^{(k)}/G^{(k+1)}$  ist abelsch für alle  $k \in \mathbb{N}$ .

**Satz 1**

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

**Beweis**

In der nächsten Vorlesung.

#### **Bemerkung 4**

“ $\Leftarrow$ ” folgt unmittelbar aus Bemerkung 3.

#### **Bemerkung 5**

Sei  $H \leq G$ . Es folgt  $H^{(l)} \leq G^{(l)}$  für alle  $l \in \mathbb{N}$ .

## 21. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 21. Januar 2013

### Satz 1

$G$  ist auflösbar  $\Leftrightarrow$  es existiert ein  $k \in \mathbb{N}$  mit  $G^{(k)} = 1$ .

### Beweis

“ $\Leftarrow$ ” Die Normalreihe  $G \triangleright G' \triangleright \dots$  hat abelsche Faktoren.

“ $\Rightarrow$ ” Sei  $G = G_1 \triangleright \dots \triangleright G_s \triangleright G_{s+1} = \{1\}$  eine Normalreihe mit abelschen Faktoren  $G_i/G_{i+1}$ .

Lemma (20. Vorlesung)  $\Rightarrow G_{i+1} \supseteq G'_i$  für alle  $i$ .

**Behauptung**  $G_i \supseteq G^{(i)}$  für alle  $i$ . Bei  $i = 1$  gilt  $G = G_1 \supseteq G'$  ✓

Induktionsannahme für  $k$  ✓

Induktionsschritt für  $k + 1$  :  $G_{k+1} \supseteq (G_k)' \supseteq (G^{(k)})' = G^{(k+1)}$

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

### Satz 2

Sei  $G$  auflösbar.

- (1) Sei  $H \leq G$ . Dann ist  $H$  auflösbar.
- (2) Sei  $\eta : G \rightarrow H$  eine surjektive Homorphie, dann ist  $H$  auflösbar.
- (3) **Zusatz:** Sei  $G$  eine beliebige Gruppe und  $K \triangleleft G$ , so dass  $K$  und  $G/K$  auflösbar sind, dann ist  $G$  auch auflösbar.

### Beweis

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

(2)  $\eta(G^{(i)}) = \eta(G)^{(i)}$  (siehe Proposition 1 (5), 20. Vorlesung). Also  $G^{(k)} = \{1\} \Rightarrow \eta(G)^{(k)} = \{1\}$ . Also  $H^{(k)} = \{1\}$ .

(3) Sei  $\pi : G \rightarrow G/K$  die kanonische Projektion. Es gilt  $\pi(G^{(i)}) = (G/K)^{(i)}$ . Nun ist  $G/K$  auflösbar  $\Rightarrow \exists k$  mit  $\pi(G^{(k)}) = (G/K)^{(k)} = \{1\}$ , i.e. für alle  $x \in G^{(k)}$  gilt  $xK = K$ , i.e. für alle  $x \in G^{(k)}$  gilt  $x \in K$ , i.e.  $G^{(k)} \subseteq K$ . Nun ist aber auch  $K$  auflösbar, also existiert  $\ell$  mit  $G^{(k+\ell)} = (G^{(k)})^\ell \subseteq K^{(\ell)} = \{1\}$ . □

**Bemerkungen**

1. Eine endliche abelsche Gruppe  $G \neq \{1\}$ , die einfach ist, ist zyklisch mit Primordnung.

**Beweis** Da jede Untergruppe normal ist,  $G$  aber einfach, folgt daraus, dass die einzigen Untergruppen  $\{1\}$  und  $G$  sind. Sei  $x \neq 1$  mit  $x \in G$ , also  $\langle x \rangle = G$ , so ist  $G$  zyklisch. Wenn  $|G|$  **keine** Primzahl ist, dann gibt es eine Primzahl  $p$  mit  $p \mid |G|$  und damit  $1 < |H| = p < |G|$  - Widerspruch.  $\square$

2.  $G$  ist auflösbar und einfach  $\Rightarrow G$  ist abelsch.

**Beweis**  $G \triangleright \{1\}$  ist die einzig mögliche Normalreihe.  $\square$

**Satz 3**

Eine endliche Gruppe ist auflösbar  $\Leftrightarrow$  jeder Kompositionsfaktor einer Kompositionsreihe ist zyklisch mit Primordnung.

**Beweis**

" $\Rightarrow$ "  $G$  ist auflösbar. Sei  $G = G_1 \triangleright \dots \triangleright G_{s+1} = \{1\}$  eine Kompositionsreihe. Nun ist auch  $G_i/G_{i+1}$  auflösbar (siehe Satz 2 Nr. (1) und (2)) und einfach  $\Rightarrow G_i/G_{i+1}$  sind abelsch, also zyklisch mit Primordnung (siehe Bemerkungen 1. und 2.).

" $\Leftarrow$ " Sei

$$G = G_1 \triangleright \dots \triangleright G_{s+1} = \{1\} \quad (*)$$

eine Kompositionsreihe (ex. wegen Jordan Hölder) mit  $G_i/G_{i+1}$  zyklisch mit Primordnung. Dann ist insbesondere  $G_i/G_{i+1}$  abelsch und damit ist die Reihe (\*) sogar eine auflösbare Reihe.  $\square$ .

**Erinnerung**

Ex. 4.1 (b) Lineare Algebra II:  $n \geq 3$ .  $A_n$  ist von 3-Zykeln erzeugt.

**Satz 4**

$A_n$  ist einfach für  $n \geq 5$ .

**Beweis**

Sei  $K \neq \{1\}$ ,  $K \triangleleft A_n$ . Zu zeigen:  $K = A_n$ .

**Behauptung 1** Wenn  $K$  ein 3-Zykel entht, dann enthlt  $K$  alle 3-Zykeln.

**Beweis** Sei  $(123) \in K$  und  $(ijk)$  beliebig.

$$\gamma := \begin{pmatrix} 12345 \cdots \\ ijk lm \cdots \end{pmatrix} \quad \text{Es gilt } \gamma(123)\gamma^{-1} = (ijk) \quad (*)$$

Ohne Einschrnkung gilt  $\gamma \in A_n$  (sonst ersetze durch  $(lm)\gamma$ ).

Nun ist  $K$  normal  $\Rightarrow (ijk) \in K$  wegen  $(*)$ .  $\square$

**Behauptung 2**  $K$  enthlt ein 3-Zykel.

**Beweis** Sei  $\alpha \in K \triangleleft A_n; \alpha \neq 1$  mit maximaler Anzahl von Fixpunkten.

Wir zeigen:  $\alpha$  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)  $\alpha$  noch zwei Zahlen bewegen muss, sonst ist  $\alpha = (123k)$  eine ungerade Permutation - Widerspruch.)

Setze  $\beta := (345)$  und betrachte  $\alpha_1 := \beta\alpha\beta^{-1}$  ( $\alpha_1 \in K$ , weil  $\alpha \in K$  und  $K \triangleleft A_n$ ).

Direktes Rechnen zeigt:

$$\alpha_1 = (124 \cdots) \cdots \text{ im Fall (a) und}$$

$$\alpha_1 = (12)(45) \cdots \text{ im Fall (b).}$$

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

Nun ist jede  $\ell > 5$  durch  $\beta$  fixiert. Beobachte, dass falls  $\ell$  auch durch  $\alpha$  fixiert ist,  $\ell$  auch durch  $\alpha_2$  fixiert ist.

Direktes Rechnen im Fall (a) zeigt  $\alpha_2(2) = 2$  und auerdem bewegt  $\alpha$  im Fall 1, 2, 3, 4, 5. Also hat  $\alpha_2$  einen extra Fixpunkt (nämlich 2) und  $\alpha_2 \in K$  - Widerspruch.

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

### Korollar

$S_n$  ist **nicht** auflsbar fr  $n \geq 5$ .

### Beweis

Sonst wre  $A_n$  auflsbar, aber  $A_n$  ist einfach  $\Rightarrow A_n$  ist abelsch - Widerspruch.  $\square$

## 22. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 24. Januar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

Unser nächstes Ziel ist es, die Sylow Sätze zu beweisen (Sonderfälle, für die die Umkehrung von Lagrange gilt).

### Sylow 1

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

### Definition 1

Eine solche Teilgruppe  $H$  mit  $|H| = p^m$ ,  $m$  maximal, ist eine *Sylow- $p$ -Untergruppe*.

### Sylow 2

- (1) Sylow- $p$ -Untergruppen sind 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  $\equiv 1 \pmod{p}$ .
- (3) Jede Untergruppe der Ordnung  $p^k$  ist enthalten in einer Sylow- $p$ -Untergruppe.

Für die Beweise der Sylow-Sätze brauchen wir Gruppenaktionen:

### Definition 2

Sei  $G$  eine Gruppe und  $S$  eine Menge ( $S \neq \emptyset$ ).

$$G \times S \rightarrow S$$

$$(g, x) \mapsto gx$$

ist eine Abbildung, so dass

$$(i) \quad 1x = x \text{ für alle } x \in S$$

$$(ii) \quad g_1g_2x = g_1(g_2x) \text{ für alle } x \in S \text{ und für alle } g_1, g_2 \in G.$$

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

**Definition 3**

Sei  $G$  operiert auf  $S$  und auf  $S'$ . Die Aktionen heißen *äquivalent*, wenn es eine Bijektion  $v : S \rightarrow S'$  gibt pd.  $v(gx) = gv(x)$  für alle  $g \in G$  und  $x \in S$ .

**Proposition 1**

Sei  $G$  operiert auf  $S$ . Definiere

$$\begin{aligned} T(g) : S &\longrightarrow S \\ x &\mapsto gx \end{aligned}$$

Dann ist  $T(g)$  eine Permutation auf  $S$ .

**Notation**

$Sym S$  bezeichnet die Gruppe der Permutationen von  $S$ .

Fortsetzung mit Ansatz von Proposition 1:

**Proposition 2**

Die Abbildung

$$\begin{aligned} T : G &\longrightarrow Sym S \\ g &\mapsto T(g) \end{aligned}$$

ist ein Gruppenhomomorphismus.

**Definition 4**

$\ker T \triangleleft G$  heißt der *ker* der Aktion. Die Aktion heißt *effektiv*, wenn  $\ker T = \{1\}$ .

**Beispiele**

(0)  $G$  operiert auf  $S$  und  $H \leq G \Rightarrow H$  operiert auf  $S$  (durch Einschränkung)

$G$  operiert auf  $S$  und  $\mathcal{O} \subseteq S \Rightarrow G$  operiert auf  $\mathcal{O}$  (auch Einschränkung, wenn wohldefiniert!)

(i)  $S = G$ . Definiere die Aktion "*linke Multiplikation*":

$$(g, x) \mapsto \underbrace{gx}_{\text{Produkt in } G} \text{ ist eine effektive Aktion.}$$

(ii) Dual dazu "*rechte Multiplikation*"

(iii) Konjugation:  $S = G$ ;  $(g, x) \mapsto gxg^{-1}$ .

Was ist hier der *ker* dieser Aktion?

$$\begin{aligned} \ker T &= \{g \mid \forall x \in G : gxg^{-1} = x\} \\ &= \{g \mid \forall x \in G : gx = xg\} \\ &:= C_G \end{aligned}$$

$C_G$  heißt *Zentrum von G* und ist eine normale Untergruppe.

**Definition 5**

$H \leq Sym S$  heißt *Permutationsgruppe*.



**Satz (Cayley)**

Jede Gruppe ist isomorph zu einer Permutationsgruppe.

**Beweis**

$S = G$  operiert mit der linken Multiplikation auf  $G$ .

$$T : G \longrightarrow \text{Sym } G$$

$$g \mapsto T(g)$$

hat trivialen  $\ker T = \{1\}$ . Also  $G \simeq T(G) \leq \text{Sym } G$ . □

**Äquivalenzrelation durch Aktion induziert**

1. Seien  $x, y \in S$ . Setze  $x \underset{G}{\sim} y$ , wenn es ein  $g \in G$  gibt, pd.  $y = gx$ .

$\underset{G}{\sim}$  ist eine Äquivalenzrelation.

2.  $[x] := Gx := \{gx \mid g \in G\}$  heißt die *Orbit* oder *Bahn* von  $x$ .

3.  $S = \bigsqcup_{x \in S} Gx$ .

**Beispiele** (Fortsetzung)

(i) Sei  $H \leq G, S = G$ .  $H$  operiert durch linke Multiplikation  $[x] = Hx = \{hx \mid h \in H\}$  (die Nebenklasse von  $x$ ).

(ii)  $G$  operiert auf  $G$  durch Konjugation  $[x] = \{gxg^{-1} \mid g \in G\}$  heißt die *Konjugationsklasse*.

**Proposition 3**

(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.

### 23. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 28. Januar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

#### Definition 1

1.  $G$  operiert transitiv auf  $S$ , wenn es nur eine Bahn gibt, das heißt für alle  $x, y \in S : x \underset{G}{\sim} y$ .
2. Der Stabilisator  $Stab_x := \{g \in G \mid gx = x\}$  ist eine Untergruppe von  $G$  für jedes  $x \in S$ .

#### Beispiel 1

$G$  operiert auf  $G$  durch Konjugation  $\Rightarrow$

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

#### Bemerkung

- (i) Wenn  $y = ax$ , dann ist  $Stab_x = a^{-1}(Stab_y)a$ .
- (ii) Also wenn  $G$  auf  $S$  transitiv operiert, gilt für alle  $x, y \in S$ , dass  $a \in G$  existiert, so dass  $Stab_y = a(Stab_x)a^{-1}$

#### Beispiel 2

$H \leq G$  operiert transitiv auf  $S := \{xH \mid x \in G\}$  mit  $g(xH) := (gx)H$ .

#### Beweis

Seien  $xH, yH \in S$ . Setze  $g := yx^{-1}$ , dann gilt  $gxH = yH$ . □

Wir zeigen, dass bis auf Äquivalenz von Aktionen, alle transitive Aktionen so sind.

#### Satz 1

Es sei  $G$  operiert transitiv auf  $S \neq \emptyset$ . Sei  $x \in S$  und  $H := Stab_x$ . Dann ist die Aktion äquivalent zur Aktion auf  $S' := \{gH \mid g \in G\}$ .

#### Beweis

Definierte  $\bar{\alpha} : \bar{G} \rightarrow S$  mit  $\bar{\alpha}(\bar{g}) := gx$ , wobei  $\bar{g} := \{a \in G \mid ax = gx\} = \{a \in G \mid g^{-1}a \in H\} = gH$  und  $\bar{G} := \{\bar{g} \mid g \in G\}$  ist. Die Aktion ist transitiv  $\Rightarrow \bar{\alpha}$  surjektiv.

**Übungsaufgabe**

$\bar{\alpha}$  ist wohldefiniert und bijektiv. Wir müssen noch prüfen, ob  $\bar{\alpha}(h\bar{g}) \stackrel{?}{=} h\bar{\alpha}(\bar{g})$ .

**Korollar 1**

Es sei  $G$  endlich, operiert transitiv auf  $S$ . Dann ist  $|S| = [G : \text{Stab}_x]$  für ein (jedes)  $x \in S$ , insbesondere ist  $S$  endlich und  $|S| \mid |G|$ .

Allgemeiner können wir ein Resultat für eine beliebige Aktion herleiten:

**Korollar 2** (Bahngleichung)

Es sei  $G$  endlich operiert auf  $S$  endlich. Es gilt  $|S| = \sum_{i=1}^r [G : \text{Stab}_{x_i}]$ , wobei  $\{x_1, \dots, x_r\}$  ein Vertretersystem der Bahnen ist.

**Beweis**

Seien  $\mathcal{O}_1, \dots, \mathcal{O}_r$  alle Bahnen. Es ist leicht zu sehen, dass die Aktion auf  $\mathcal{O}_i$  transitiv ist für jedes  $i = 1, \dots, r$ . Also gilt  $|\mathcal{O}_i| = [G : \text{Stab}_{x_i}]$ . Nun ist  $S = \bigsqcup_{i=1}^r \mathcal{O}_i$ , also  $|S| = \sum |\mathcal{O}_i|$ .  $\square$

**Korollar 3** (Klassengleichung)

Sei  $G$  eine endliche Gruppe. Es gilt  $|G| = \sum_{i=1}^k [G : C(x_i)]$ , wobei  $\{x_1, \dots, x_k\}$  ein Vertretersystem der Konjugationsklassen ist.

**Beweis**

$G$  operiert auf  $G$  durch Konjugation und  $\text{Stab}_{x_i} = C(x_i)$  in diesem Fall.  $\square$

**Korollar 4** (Klassengleichung Bis.)

$|G| = |C_G| + \sum_{i=1}^{\ell} [G : C(y_i)]$ , wobei  $\{y_1, \dots, y_{\ell}\}$  ein Vertretersystem für die Konjugationsklassen in  $G \setminus C_G$  ist.

**Beweis**

Die Konjugationsklassen von  $x$  ist  $\{x\}$  genau dann, wenn  $x \in C_G$  genau dann, wenn  $C(x) = G$ . In Korollar 3 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.  $\square$

**Korollar 5**

Sei  $G$  endlich,  $|G| = p^k$ ,  $p$  ist Primzahl und  $k \in \mathbb{N}$ . Es gilt  $C_G \neq \{1\}$ .

## 24. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 31. Januar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

### § Beweise der Sylow-Sätze

#### Beweis von Sylow 1

Induktion nach  $|G|$ .  $|G| = 1$  - klar.

Induktionsannahme: Sylow 1 gilt für alle Gruppen der Ordnung  $< |G|$ .

Induktionsschritt: Wir werden "Cauchy's Satz" benutzen und Aufgabe 9.4 benötigen.

Sei  $G$  eine endliche abelsche Gruppe,  $p \in \mathbb{N}$  eine Primzahl und  $p \mid |G|$ . Dann existiert ein  $x \in G$  mit  $|x| = p$ . Betrachte die Klassengleichung  $|G| = |C_G| + \sum_{y_i \notin C_G} [G : C(y_i)]$  und beachte, dass

$C := C_G$  abelsch ist. Zwei Fälle sind zu betrachten:

#### Fall 1

$p \nmid |C| \Rightarrow \exists j$  mit  $p \nmid [G : C(y_j)]$ . Aber  $p^k \mid |G| = [G : C(y_j)] \mid |C(y_j)|$ . Also  $p^k \mid |C(y_j)|$ . Nun ist  $|C(y_j)| < |G|$ , da  $y_j \notin C$  ist.

Induktionsannahme  $\Rightarrow C(y_j)$  besitzt eine Untergruppe der Ordnung  $p^k$ .

#### Fall 2

$p \mid |C| \Rightarrow$  Cauchy's Satz liefert ein Element  $c$  der Ordnung  $p$ .

Nun ist  $\langle c \rangle \triangleleft G$ ,  $|G / \langle c \rangle| = p$ . Betrachte die Gruppe  $G / \langle c \rangle$  der Ordnung  $\frac{|G|}{|\langle c \rangle|} = \frac{|G|}{p}$ . Also  $p^{k-1} \mid \frac{|G|}{p}$ .

Induktionsannahme  $\Rightarrow \exists$  eine Untergruppe von  $G / \langle c \rangle$  der Ordnung  $p^{k-1}$ . Nun haben die Untergruppen von  $G / \langle c \rangle$  die Gestalt  $H / \langle c \rangle$ , wobei  $H \leq G$  und  $\langle c \rangle \leq H$ .

Also existiert  $H \leq G$  mit  $|H / \langle c \rangle| = p^{k-1}$  und damit ist

$|H| = |H / \langle c \rangle| \cdot |\langle c \rangle| = p^{k-1} \cdot p = p^k$ . □

**Beweis von Sylow 2**

Wir benötigen eine

**Bemerkung**

Sei  $H \leq G$  und  $g \in G$ , dann ist  $gHg^{-1}$  auch eine  $\leq G$ . Also haben wir eine Aktion von  $G$  auf  $\Gamma :=$  die Menge der Untergruppen von  $G$  durch Konjugation.

- Für die Aktion berechnen wir  $(H \in \Gamma) \text{ Stab}_H := \{g \in G \mid gHg^{-1} = H\} := N(H)$  der Normalisator von  $H$  in  $G$ .
- Beachte:  $H \triangleleft N(H)$ .
- Wir berechnen die Bahnen  $\mathcal{O}_H = \{gHg^{-1} \mid g \in G\}, H \in \Gamma$ .  
Korollar 1 (23. Vorlesung) liefert  $|\mathcal{O}_H| = [G : N(H)]$   
und  $[G : H] = [G : N(H)][N(H) : H]$ , so ist  $|\mathcal{O}_H| \mid [G : H]$ .
- Zum Spezialisieren dieser Aktion auf die Mengen  $\Pi \subseteq \Gamma$  der Sylow- $p$ -Untergruppen von  $G$ . Die Aktion auf  $\Pi$  ist wohldefiniert, weil  $gHg^{-1} \in \Pi$ , wenn  $H \in \Pi$ .

Wir bekommen ein:

**Hilfslemma**

- (i) Sei  $P \in \Pi, H \leq N(P)$  und  $|H| = p^j$ , dann ist  $H \leq P$ . Es folgt:  
(ii)  $P$  ist eine Sylow- $p$ -Untergruppe von  $N(P)$  und die einzige.

**Beweis**

$$\left. \begin{array}{l} H \leq N(P) \quad \text{und} \\ P \triangleleft N(P) \end{array} \right\} \Rightarrow HP \text{ ist Untergruppe und } HP/P \simeq H/(H \cap P)$$

(Isomorphie-Satz). Also ist  $HP/P$  isomorph zu einer Faktorgruppe von  $H$  und damit hat sie die Ordnung  $|HP/P| = p^k$  für ein geeignetes  $k$ . Also  $|HP| = p^k |P|$ . Da aber  $P$  eine Sylow- $p$ -Untergruppe ist, müssen wir  $k = 0$  haben, i.e.  $HP = P$ , so dass  $H \leq P$ . □

**Beweis von Sylow 2** - Fortsetzung

Wir betrachten eine Bahn  $\Sigma$ .

**Fall 1**

Sei  $P \in \Sigma$  und betrachte die Aktion von  $P$  auf  $\Sigma$ . Wir bekommen eine Partition von  $\Sigma$  in  $P$ -Bahnen.

- Betrachte die Bahn von  $P$ . Die ist offensichtlich  $\{P\}$  (weil  $xPx^{-1} = P$  für alle  $x \in P$ ).
- Wir behaupten, dass  $\{P\}$  die einzige Bahn der Kardinalität 1 ist:  
Sei  $\{P'\}$  eine  $P$ -Bahn. Dann gilt  $xP'x^{-1} = P'$  für alle  $x \in P$ , das heißt  $P \subseteq N(P')$  und Hilfslemma (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 1, 23. Vorlesung). Also ist  $|\Sigma| \equiv 1 \pmod{p}$ .

Dieses beweist die zweite Aussage von Sylow 2 (2).

Nun beweisen wir Sylow 2 (1). Wir zeigen, dass  $\Sigma$  die einzige Bahn ist, sonst gibt es  $P \in \Pi$  mit

**Fall 2**

$P \notin \Sigma$ . Betrachte wieder die Aktion von  $P$  auf  $\Sigma$ . 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  $P \notin \Sigma$  ist).

Also ist  $|\Sigma| \equiv 0 \pmod{p}$  - Widerspruch.

So  $\Sigma = \Pi$  und damit ist (1) bewiesen.

Also ist  $|\Pi| = [G : N(P)]$  für alle  $P \in \Pi$  (Korollar 1, 23. Vorlesung). Also ist die Anzahl der Sylow- $p$ -Untergruppen ein Divisor.

Das beweist die erste Aussage in Sylow (2).

Nun beweisen wir Sylow 2 (3)

Sei  $H \leq G$ ,  $|H| = p^k$ . Betrachte die Aktion von  $H$  auf  $\Pi$ . Die  $H$ -Bahnen haben Kardinalität ein Divisor von  $|H|$  (Korollar 1, 23. Vorlesung), also haben die  $H$ -Bahnen-Kardinalität eine Potenz von  $p$ .

Nun ist aber  $|\Pi| \equiv 1 \pmod{p}$ , also gibt es eine  $H$ -Bahn  $\{P\}$  mit nur einem Element, das heißt  $H \leq N(P)$  und damit  $H \leq P$  (Hilfslemma (i)).  $\square$

## Useful English/German Vocabulary

Splitting field - Zerfällungskörper

Field extension - Körpererweiterung

**Definition 0.1.** Let  $E/F$  be a field extension. The **Galois group**, denoted  $\text{Gal}(E/F)$ , of  $E/F$  is the group of automorphisms of  $E$  which fix  $F$  pointwise i.e. the automorphisms  $\mu$  of  $E$  such that for all  $\alpha \in F$ ,  $\mu(\alpha) = \alpha$ .

**Definition 0.2.** Let  $F$  be a field and  $G$  be a subgroup of the group of automorphisms of  $F$ . The set

$$\text{Inv}(G) := \{a \in F \mid \sigma(a) = a \text{ for all } \sigma \in G\}$$

is a subfield of  $F$ . We call it the  **$G$ -fixed subfield** of  $F$ .

Let  $E$  be a field and  $G$  the group of automorphisms of  $E$ . Let  $\Gamma$  be the set of subgroups of  $G$  and  $\Sigma$  the set of subfields of  $E$ . The maps

$$\Gamma \rightarrow \Sigma, H \mapsto \text{Inv}(H)$$

and

$$\Sigma \rightarrow \Gamma, F \mapsto \text{Gal}(E/F)$$

have the following properties:

- (i)  $G_1 \subseteq G_2 \Rightarrow \text{Inv}(G_1) \supseteq \text{Inv}(G_2)$
- (ii)  $F_1 \subseteq F_2 \Rightarrow \text{Gal}(E/F_1) \supseteq \text{Gal}(E/F_2)$
- (iii)  $\text{Inv}(\text{Gal}(E/F)) \supseteq F$
- (iv)  $\text{Gal}(E/\text{Inv}(G)) \supseteq G$

See exercise 1 sheet 12.

**Lemma 0.3.** Let  $E/F$  be a splitting field of a separable polynomial with coefficients in  $F$ . Then

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

*Proof.* What we will actually show is the following:

Let  $\tau : F \rightarrow F'$  be an isomorphism of fields. Let  $p(x) \in F[x]$  be a separable. Let  $E$  be a splitting field for  $p(x)$  and  $E'$  be a splitting field for  $\tau(p)(x)$ . There exist exactly  $[E : F]$  extensions of  $\tau$  to an isomorphism  $\sigma : E \rightarrow E'$ .

We proceed by induction on  $[E : F]$ . If  $[E : F] = 1$  the statement is clear.

Fix  $\alpha$  a root of  $p(x)$  in  $E \setminus F$  with minimal polynomial  $m_\alpha(x)$ . For each  $\beta$  a root of  $\tau(m_\alpha)(x)$ , let  $\tau_\beta : F(\alpha) \rightarrow F'(\beta)$  be the (unique) isomorphism extending  $\tau$  with  $\tau_\beta(\alpha) = \beta$ .

For each root  $\beta$  of  $\tau(m_\alpha)(x)$  let  $S_\beta$  be the set of isomorphisms  $E \rightarrow E'$  extending  $\tau_\beta$ . If  $\beta \neq \beta'$  then  $S_\beta \cap S_{\beta'} = \emptyset$ .

The field  $E$  remains the splitting field of  $p(x)$  over  $F(\alpha)$  and  $E'$  remains the splitting field of  $\tau_\beta(p)(x)$  over  $F'(\beta)$ . Since  $[E : F(\alpha)] < [E : F]$ , by the induction hypothesis,

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

Since  $m_\alpha(x)$  divides  $p(x)$ ,  $m_\alpha(x)$  is separable and thus, so is  $\tau(m_\alpha)(x)$ . Thus  $\tau(m_\alpha)(x)$  has  $[F(\alpha) : F]$  distinct roots.

Each isomorphism  $\sigma : E \rightarrow E'$  extending  $\tau$  maps  $\alpha$  to a root of  $\tau(m_\alpha)(x)$ . Thus each  $\sigma$  restricts to some  $\tau_\beta$ . So each  $\sigma$  is in  $S_\beta$  for some  $\beta$  a root of  $\tau(m_\alpha)(x)$ .

Thus there are exactly  $[E : F(\alpha)][F(\alpha) : F]$  isomorphisms  $\sigma : E \rightarrow E'$  extending  $\tau : F \rightarrow F'$ . So we have proved our claim.

Setting  $E = E'$ ,  $F = F'$  and  $\tau$  equal to the identity homomorphism we get our lemma as stated.

□



**Lemma 0.4.** *Let  $G$  be a finite group of automorphisms of a field  $E$  and let  $F = \text{Inv}(G)$ . Then*

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

**Remark/Reminder from linear algebra:** A system of  $n$  homogeneous linear equations over a field  $E$  in  $m$  variables with  $n < m$  has a non-trivial solution. (See LA I, Korollar 2, 7. Vorlesung am 11.11.11)

*proof of lemma.* Let  $n = |G|$  and  $G = \{\mu_1 = 1, \mu_2, \dots, \mu_n\}$ . We need to show that any  $m > n$  elements of  $E$  are linearly dependent over  $F$ . Let  $u_1, \dots, u_m \in E$ . Consider the system of linear equations in variables  $x_1, \dots, x_m$

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

Let  $(b_1, \dots, b_m)$  be a non-trivial solution with the least number of  $b_i \neq 0$ . By permuting the variables  $x_i$  we may assume  $b_1 \neq 0$  and by multiplying through by  $b_1^{-1}$  we may assume  $b_1 = 1$ .

We now show by contradiction that each  $b_i \in F := \text{Inv}(G)$ . Without loss of generality we may suppose  $b_2 \notin F$  and  $1 \leq k \leq n$  is such that  $\mu_k(b_2) \neq b_2$ .

Applying  $\mu_k$  to 1 we get that

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

Since  $\mu_k \mu_1, \dots, \mu_k \mu_n$  is just a permutation of  $\mu_1, \dots, \mu_n$ ,

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

is a solution to 1.

Thus

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

is a solution to 1 and is non-trivial since  $b_2 - \mu_k(b_2) \neq 0$ . But this solutions has fewer zero entries than our original solution. So we have a contradiction. Thus each  $b_i \in F$  and from the first equation in 1:

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

Thus  $u_1, \dots, u_m$  are linearly dependent over  $F$ . □

**Definition 0.5.** We say an algebraic field extension  $E/F$  is **separable** if the minimal polynomial of every element of  $E$  over  $F$  is separable.

**Theorem 0.6.** Let  $E/F$  be a field extension. The following are equivalent:

1.  $E$  is a splitting field of a separable polynomial  $p(x) \in F[x]$ .
2.  $F = \text{Inv}(G)$  for some finite group of automorphisms of  $E$ .
3.  $E$  is a finite dimensional, normal and separable over  $F$ .

Moreover, if  $E$  and  $F$  are as in (1) and  $G = \text{Gal}(E/F)$  then  $F = \text{Inv}(G)$  and if  $G$  and  $F$  are as in (2), then  $G = \text{Gal}(E/F)$ .

*Proof.* (1) $\Rightarrow$ (2) Let  $F' = \text{Inv}(\text{Gal}(E/F))$  and note  $F' \supseteq F$ . Clearly  $E$  is a splitting field of  $p(x)$  over  $F'$  and since  $\text{Gal}(E/F)$  fixes  $F'$  pointwise,  $\text{Gal}(E/F) = \text{Gal}(E/F')$ .

By lemma 0.3,  $[E : F] = |\text{Gal}(E/F)|$  and  $[E : F'] = |\text{Gal}(E/F')|$ . Thus, since  $[E : F] = [E : F'][F' : F]$ ,  $[F' : F] = 1$ . Thus  $F = F'$ . So (2) holds.

Note we have also shown that  $F := \text{Inv}(G)$  for  $G := \text{Gal}(E/F)$ , which is the first part of the moreover.

(2)  $\Rightarrow$  (3)  $E$  is finite dimensional over  $F$  by lemma 0.4. Let  $\alpha \in E$ . Let  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$  be the orbit of  $\alpha$  under the action of  $G$ . Let  $g(x) = \prod_{i=1}^m (x - \alpha_i)$ . For any  $\sigma \in G$ ,

$$\sigma(g)(x) = \prod_{i=1}^m (x - \sigma(\alpha_i)) = g(x)$$

since  $\sigma$  just permutes the elements of  $\{\alpha_1, \dots, \alpha_m\}$ . Thus  $g(x) \in F[x]$ .

Since  $g(\alpha) = 0$  and  $g(x) \in F[x]$ , the minimal polynomial of  $\alpha$  over  $F$  divides  $g$ . Since the  $\alpha_i$ s are all different,  $g$  is separable and thus the minimal polynomial of  $\alpha$  is separable. So  $E/F$  is separable.

Moreover, all roots of the minimal polynomial of  $\alpha$  are in  $E$ . Thus  $E$  is a normal over  $F$  (it is the splitting field of the minimal polynomials over  $F$  of all elements  $\alpha \in E$ ).

(3)  $\Rightarrow$  (1) Since  $E/F$  is normal and finite dimensional,  $E$  is the splitting field of a finite number of polynomials  $p_1, \dots, p_n \in F[x]$ . We may as well assume that each of these polynomials is monic, irreducible over  $F$  and that no two are equal. Thus, each polynomial  $p_i$  is the minimal polynomial of some  $\alpha \in E$  over  $F$ . Thus, since they are non-equal, they also have no common roots. Therefore, their product  $p_1 \cdots p_n$  is separable and  $E$  is its splitting field.

We now prove the second part of the "moreover". Suppose  $F = \text{Inv}(G)$  for some finite group of automorphisms of  $E$ . Then by lemma 0.4,  $[E : F] \leq |G|$ . Since (1) holds, lemma 0.3 says that  $\text{Gal}(E/F) = [E : F]$ . So, since  $G$  is a subgroup of  $\text{Gal}(E/F)$ ,  $G = \text{Gal}(E/F)$ . □

**Definition 0.7.** We call a field extension  $E/F$  which satisfies any (and hence all) the equivalent conditions of the above theorem a **Galois extension**.

**Theorem 0.8** (Fundamental theorem of Galois theory). *Let  $E/F$  be a Galois extension with  $G := \text{Gal}(E/F)$ . Let  $\Gamma$  be the set of subgroups of  $G := \text{Gal}(E/F)$  and let  $\Sigma$  be the set of intermediate fields between  $E$  and  $F$ . The maps*

$$H \mapsto \text{Inv}(H)$$

$$K \mapsto \text{Gal}(E/K)$$

*are inverse bijective maps. Moreover, we have the following properties:*

(i)  $H_1 \supseteq H_2 \Leftrightarrow \text{Inv}(H_1) \subseteq \text{Inv}(H_2)$ .

(ii)  $|H| = [E : \text{Inv}(H)]$ ,  $[G : H] = [\text{Inv}(H) : F]$

(iii)  $H$  in  $G$  is normal if and only if  $\text{Inv}(H)$  is normal over  $F$ . In this case

$$\text{Gal}(\text{Inv}(H)/F) \cong G/H$$

## 26. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 7. Februar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

**Beweis** Fundamentalersatz der Galois Theorie (siehe Satz 0.8, 25. Vorlesung)

Sei  $E/F$  eine endliche Galoiserweiterung. Betrachte die Abbildungen

$$\Sigma \xrightarrow{\gamma} \Gamma$$

$$K \mapsto \text{Gal}(E/K) \quad (\subseteq \text{Gal}(E/F))$$

und  $\Gamma \rightarrow \Sigma$

$$H \mapsto \text{Inv } H \quad (\subseteq E \text{ und } \supseteq F)$$

wobei  $\Gamma :=$  die Menge der Untergruppen von  $G := \text{Gal}(E/F)$  ist und  $\Sigma :=$  die Menge der Zwischenkörper  $F \subseteq K \subseteq E$  ist.

Wir behaupten  $i \circ \gamma = \text{Id}$  und  $\gamma \circ i = \text{Id}$ , i.e.  $\text{Gal}(E/\text{Inv } H) = H$  und  $\text{Inv}(\text{Gal}(E/K)) = K$ , das heißt  $(\gamma \circ i)(H) = H$  und  $(i \circ \gamma)(K) = K$ .

Das ist aber die letzte Aussage in Satz 0.6 der 25. Vorlesung (weil  $H$  endlich ist), genauer:

- $H \leq G$ , also  $F := \text{Inv } G \subseteq \text{Inv } H$  und  $K = \text{Inv } H$  ist eine Zwischenerweiterung  $F \subseteq K \subseteq E$ . Die Anwendung von Satz 0.6 mit  $H$  anstatt mit  $G$  liefert  $\text{Gal}(E/\text{Inv } H) = H$ . Also  $|H| = |\text{Gal}(E/\text{Inv } H)| = [E : \text{Inv } H]$  (siehe Lemma 0.3, 25. Vorlesung)
- Sei nun  $K$  ein Unterkörper von  $E/F$  (i.e.  $F \subseteq K \subseteq E$ ) und  $H := \text{Gal}(E/K)$ , dann ist  $H \leq G (= \text{Gal}(E/F))$ .

Nun ist  $E$  immer noch Zerfällungskörper über  $K$  von einem separablen Polynom (weil  $E$  über  $F$  so ist). Also liefert die Anwendung von Satz 0.6 für  $E$  und  $K$

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

- (i) ist eine unmittelbare Folgerung der allgemeinen Eigenschaften (Übungsblatt, Aufgabe 12.1):  $H_1 \supseteq H_2 \Rightarrow \text{Inv } H_1 \subseteq \text{Inv } H_2$ . Nun ist  $\text{Inv } H_1 \subseteq \text{Inv } H_2$ , dann ist  $H_1 = \text{Gal}(E/\text{Inv } H_1) \supseteq \text{Gal}(E/\text{Inv } H_2) = H_2$ .
- Die erste Aussage in (ii) haben wir schon bewiesen:  $|H| = [E : \text{Inv } H]$ . Wir berechnen  $|G| = [E : F] = [E : \text{Inv } H][\text{Inv } H : F] = |H|[\text{Inv } H : F]$ , aber auch  $|G| = |H|[G : H]$  (vergleiche:  $|H|[\text{Inv } H : F]$  und  $|G| = |H|[G : H]) \Rightarrow [G : H] = [\text{Inv } H : F]$ . Dies ist die zweite Aussage in (ii).

Zu (iii):

Sei  $H \in \Gamma$  und  $K := \text{Inv } H$ . Dann ist  $\text{Inv } (\eta H \eta^{-1}) = \eta(K)$  (für  $\eta \in G$ ), weil für alle  $\xi$  gilt:  
 $\xi(k) = k \Rightarrow (\eta \xi \eta^{-1})(\eta(k)) = \eta(k)$ .

Es folgt:  $H \triangleleft G \Leftrightarrow \eta(K) = K$  für alle  $\eta \in G$  (\*)

(i.e.  $K$  ist (mengenweise) invariant). Nehmen wir nun an, dass  $H \triangleleft G$ . Aus (\*) folgt, dass  $\bar{\eta} := \eta|_K$  ein Automorphismus von  $K$  über  $F$  ist. Betrachte also nun den Homomorphismus

$$\begin{aligned} \text{Gal}(E/F) = G &\rightarrow \text{Gal}(K/F) \\ \eta &\mapsto \bar{\eta} \end{aligned}$$

und berechne das Bild  $\bar{G}$  und den Kern davon.

Bemerke, dass  $\text{Inv } \bar{G} = F$  und  $\bar{G} = \text{Gal}(K/F)$ . Der Kern ist die Menge aller  $\eta \in G$  mit  $\eta|_K = \text{Id}$ . Das heißt, dass der Kern genau  $\text{Gal}(E/K) = H$  ist. Wir bekommen nun  $\bar{G} = \text{Gal}(K/F) \simeq G/H$ . Da  $F = \text{Inv } \bar{G}$ ,  $K/F$  ist eine normale Erweiterung (Satz 0.6, 2., 25. Vorlesung).

Umgekehrt: Sei  $K/F$  normal. Sei  $a \in K$  und  $f(x) := \text{Min.Pol.}_{F,a}$ .  $f(x)$  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 (\*)  $H := \text{Gal}(E/K) \triangleleft G$ .  $\square$

**27. Script zur Vorlesung: Algebra (B III)**

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

**WS 2012/2013: 11. Februar 2013**

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

**Bemerkung 1**

Sei  $E/F$  eine endliche (i.e. endlich dimensionale) separable Erweiterung, dann ist  $E/F$  endlich erzeugt durch zum Beispiel  $\{a_1, \dots, a_n\}$ ,  $a_i$  algebraische und separable Elemente.

Sei  $f_i(x)$  das Minimalpolynom von  $a_i$ ,  $f_i(x)$  ist separabel irreduzibel.

Setze  $f(x) := \prod_{1 \leq i \leq n} f_i(x)$ .  $f(x)$  ist separabel.

Setze  $K :=$  Zerfällungskörper von  $f(x)$  über  $E$ . Da  $K \supseteq F(a_1, \dots, a_n)$  ist es klar, dass  $K$  auch Zerfällungskörper von  $f(x)$  über  $F$  ist.

- (1) So ist  $K/F$  normal. Andererseits enthält jede normale Erweiterung von  $E$  einen Zerfällungskörper für  $f(x)$  über  $F$ .
- (2) Also damit enthält jede normale Erweiterung von  $E$  eine isomorphe Kopie von  $K$ .
- (3) Also ist  $K$  bis Isomorphie eindeutig bestimmt durch  $E$  unabhängig von der Wahl der Erzeuger  $\{a_1, \dots, a_n\}$

**Definition 1**

$K/F$  ist die *normale Hülle* von  $E/F$ .

**Einige Anwendungen der Galois Theorie****Satz 1** Satz vom primitiven Element

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

Wir brauchen einen

**Satz 2** (Hilfssatz)

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

Dafür brauchen wir eine Definition und eine Proposition.

**Definition**

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

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

**Proposition 1** (Char endlich zyklische Gruppen)

Sei  $G$  eine endliche abelsche Gruppe. Es gilt:  $G$  ist zyklisch genau dann, wenn  $\gamma(G) = |G|$ .

Für den Beweis brauchen wir wiederum zwei Hilfslemmas.

**Hilfslemma 1**

Seien  $g, h \in G$ , wobei  $G$  eine endliche abelsche Gruppe ist. Wir nehmen an:  $\text{ggT}(|g|, |h|) = 1$ .

Es gilt:  $|gh| = |g||h|$ .

**Beweis**

Setze  $|g| := m$  und  $|h| := n$ . Sei  $r \in \mathbb{N}$ , so dass  $(gh)^r = 1$ .

Dann ist  $k := g^r = h^{-r} \in \langle g \rangle \cap \langle h \rangle$ , somit  $|k| |m|$  und  $|k| |n|$ . Also  $|k| = 1$  und  $k = 1$ .

Wir haben gezeigt:  $(gh)^r = 1 \Rightarrow g^r = h^r = 1$ . Also  $m|r$  und  $n|r$  und somit  $mn = \text{kgV}(m, n)|r$ .

Andererseits:  $(gh)^{mn} = g^{mn}h^{mn} = 1$ . □

**Hilfslemma 2**

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

**Beweis**

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

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

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

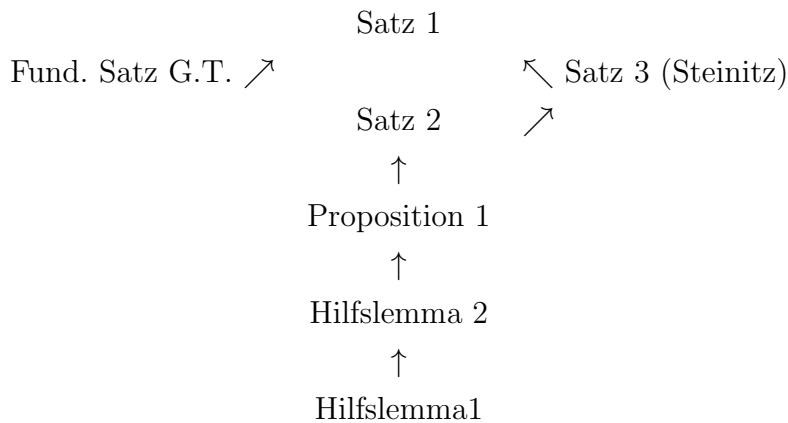
**Beweis von Proposition 1**

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

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

Hilfslemma 2: Es existiert ein  $g \in G$  mit  $|g| = \gamma(G)$  ( $|g|$  maximal). Also ist  $|g| = |G|$  und damit ist  $G = \langle g \rangle$ . □



**Beweis von Satz 2** (Hilfssatz)

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

**Korollar 1**

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

**Beweis**

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

Wir brauchen noch einen Satz:

**Satz 3** (Steinitz Char. von einfachen Erweiterungen)

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

**Beweis**

Siehe 28. Vorlesung

**Beweis von Satz 1**

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

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

## 28. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 14. Februar 2013

**Beweis** (Steinitz)

" $\Rightarrow$ "  $E = F(u)$ . Sei  $F \subseteq K \subseteq E$ ,  $f(x)$  Min. Pol. von  $u$  über  $F$  und  $g(x)$  Min. Pol. von  $u$  über  $K$ .

Es ist  $g(x)/f(x)$ . Sei  $K'$  ein Unterkörper von  $E/F$ , erzeugt durch die Koeffizienten von  $g$ .  $K' \subset K$  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  $K' = K$ . Jeder Zwischenkörper ist erzeugt durch die Koeffizienten der normierten Faktoren von  $f(x)$ . Da es nur endlich viele davon gibt, haben wir die Behauptung bewiesen.

" $\Leftarrow$ " Fall 1:

$F$  ist endlich (siehe Korollar 1, 27. Vorlesung).

Also ohne Einschränkung Fall 2:

$F$  ist unendlich

Wir zeigen, dass  $E = F(u, v)$  ein primitives Element hat. Der allgemeine Fall

$E = F(u_1, \dots, u_k)$  folgt dann per Induktion.

Betrachte die Unterkörper  $F(u + av)$  mit  $a \in F$ . Da es nur endlich viele davon gibt, aber unendlich viele  $a \in F$ , muss  $a \neq b$  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  $E = F(u, v) = F(z)$ .  $\square$

## Fundamentaler Satz der Algebra

### Satz

$\mathbb{C}$  ist algebraisch abgeschlossen.

### Beweis

Wir werden die folgenden Eigenschaften von  $\mathbb{R}$  benötigen (diese werden allgemeiner für reell abgeschlossene Körper in der Vorlesung "Reelle algebraische Geometrie I" im 7. Semester gezeigt).

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

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

**Behauptung:** (i) hat zur Folge, dass jedes Polynom zweiten Grades aus  $\mathbb{C}[x]$  eine Nullstelle in  $\mathbb{C}$  hat. 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 lösen:

$$z = x + iy = (a + ib)^2 = (a^2 - b^2) + i2ab \text{ mit } a, b \in \mathbb{R}. \text{ Also } x = a^2 - b^2 \text{ und } y = 2ab.$$

Die Gleichungen sind, abgesehen von der Wahl des Vorzeichens von  $a$  und  $b$ , äquivalent zu

$$a^2 = 1/2x \pm 1/2\sqrt{x^2 + y^2}$$

$$b^2 = 1/2x \pm 1/2\sqrt{x^2 + y^2},$$

wobei  $\pm$  bedeutet, dass man für beide Gleichungen einheitlich entweder das + oder das - auswählt.

Betrachte nun  $\mathbb{R} \subseteq \mathbb{C} \subseteq L$ , wobei  $L/\mathbb{C}$  endlich ist. Es ist  $[\mathbb{C} : \mathbb{R}] = 2$ . Zu zeigen:  $L = \mathbb{C}$ . Ohne Einschränkung ist  $L/\mathbb{R}$  Galois.

Setze  $G := \text{Gal}(L/\mathbb{R})$ . Es ist  $[L : \mathbb{R}] = |G| = 2^k m$  mit  $k \in \mathbb{N}$  und  $2 \nmid m$ .  $G$  enthält eine 2-Sylow  $H \leq G$ . Fundamentaler Satz der Galois Theorie  $\Rightarrow [L : \text{Inv } H] = |H| = 2^k$  beziehungsweise  $[\text{Inv } H : \mathbb{R}] = m$ .

Da aber jedes reelle Polynom ungeraden Grades eine Nullstelle in  $\mathbb{R}$  hat, ergibt sich unter Benutzung des Satzes vom primitiven Element notwendig  $m = 1$ .

Also  $[L : \mathbb{R}] = 2^k$  und  $[L : \mathbb{C}] = 2^{k-1}$ .

Sei  $G' := \text{Gal}(L/\mathbb{C})$ . Wenn  $L \neq \mathbb{C}$ , also  $k \geq 2$ . Sylow 1 liefert  $H' \leq G'$  mit  $|H'| = 2^{k-2}$ .

Also ist  $[L : \text{Inv } H'] = 2^{k-2}$ , so  $[\text{Inv } H' : \mathbb{C}] = 2$ . - Widerspruch. □

## Auflösbare Erweiterungen

### Definition

$L/K$  endlich ist *auflösbar*, wenn es einen Oberkörper  $E \supset L$  gibt, so dass  $E/K$  eine endliche Galois Erweiterung mit auflösbarer Gal ( $E/K$ ) ist.

**Satz** (Galois Gruppe als Untergruppen von  $S_n$ )

Sei  $f \in K[x]$  separabel,  $\deg f = n \in \mathbb{N}$  und  $L/K$  Zerfällungskörper. Seien  $a_1, \dots, a_n \in L$  Nullstellen von  $f$ , so definiert

$$\begin{aligned} \varphi : \text{Gal}(L/K) &\longrightarrow \text{Sym}\{a_1, \dots, a_n\} \\ \delta &\longmapsto \delta|_{\{a_1, \dots, a_n\}} \end{aligned}$$

einen injektiven Gruppenhomomorphismus.

### Beweis

$\delta \in \text{Gal}(L/K)$ ,  $f(a_i) = 0 \Rightarrow 0 = \delta(f(a_i)) = f(\delta(a_i))$ , da  $\delta$  die Koeffizienten von  $f$  fest lässt. Also ist  $\delta(a_i)$  eine Nullstelle von  $S$ .

Da nun  $\delta$  injektiv ist, ist auch  $\delta : \{a_1, \dots, a_n\} \rightarrow \{a_1, \dots, a_n\}$  surjektiv, also bijektiv. Damit ist  $\varphi$  wohldefiniert.

Da  $L = K(a_1, \dots, a_n)$  und  $\delta \in \text{Gal}(L/K)$  bereits eindeutig durch seine Werte auf  $\{a_1, \dots, a_n\}$  bestimmt ist, ist  $\varphi$  injektiv. □

### Korollar 1

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

### Korollar 2

Sei  $L/K$  eine separable Erweiterung vom Grad  $\leq 4$ , dann ist  $L/K$  auflösbar.

### Beweis

Satz vom primitiven Element  $\Rightarrow L = K(a)$ . Sei  $f \in K[x] \text{Min.Pol.}_K a$ . Sei  $L'$  ein Zerfällungskörper von  $f$  über  $K$ .  $\text{Gal}(L'/K)$  lässt sich als Untergruppe von  $S_4$  auffassen. Da  $S_4$  und alle ihre Untergruppen auflösbar sind, so sind  $L'/K$  und  $L/K$  auflösbar. □

**Korollar 3**

Es gibt endlich separable Körpererweiterungen, die nicht auflösbar sind.

**Beweis**

Sei  $k$  ein Körper und  $L = k(T_1, \dots, T_n) = \text{Quot}(k[T_1, \dots, T_n])$  Körper der rationalen Funktion in endlich vielen Variablen  $T_1, \dots, T_n$ .

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

$$\begin{aligned} k(T_1, \dots, T_n) &\longrightarrow k(T_1, \dots, T_n) \\ \frac{g(T_1, \dots, T_n)}{h(T_1, \dots, T_n)} &\longmapsto \frac{g(T_{\pi(1)}, \dots, T_{\pi(n)})}{h(T_{\pi(1)}, \dots, T_{\pi(n)})} \end{aligned}$$

Sei  $K := \text{Inv } S_n \subseteq L$ . Es ist (Satz 0.6, 25. Vorlesung)  $L/K$  Galois und  $\text{Gal}(L/K) = S_n$ .

Wähle nun  $n \geq 5$ , dann ist  $\text{Gal}(L/K)$  nicht auflösbar.  $\square$