

UNIVERSITÄT KONSTANZ

Skriptum zur Vorlesung

Einführung in die Algebra

Private Mitschrift

gelesen von:

Prof. Dr. Markus Schweighofer

Wintersemester 2014/15
Stand vom 24. Januar 2015

Inhaltsverzeichnis

1	Gruppen	5
1.1	Gruppen und Untergruppen	5
2.2	Polynomringe [\rightarrow LA § 3.2]	11
2.4	Primideale und maximale Ideale	16
4	Körper [\rightarrow LA § 4]	19
4.1	Endliche und algebraische Körpererweiterungen	19
4.2	Der algebraische Abschluss	23
4.3	Zerfällungskörper	29
	Literaturverzeichnis	35

§ 1 Gruppen

§ 1.1 Gruppen und Untergruppen

1.1.1 Definition Eine Gruppe ist ein geordnetes Paar (G, \cdot) , wobei G eine Menge ist und $\cdot : G \times G \rightarrow G$ eine meist infix (und manchmal gar nicht) notierte Abbildung mit folgenden Eigenschaften ist:

$$(A) \quad \forall a, b, c \in G : a(bc) = (ab)c \quad \text{„assoziativ“}$$

$$(N) \quad \exists e \in G \quad \forall a \in G : ae = a = ea \quad \text{„neutrales Element“}$$

$$(I) \quad \forall a \in G \quad \exists g \in G : ag = 1 = ba \quad \text{„inverse Elemente“}$$

„ \cdot “ heißt Gruppenmultiplikation oder Gruppenverknüpfung. Gilt zusätzlich

$$(K) \quad \forall a, b \in G : ab = ba$$

so heißt (G, \cdot) abelsch oder kommutativ.

Anmerkung Sind $e, e' \in G$ neutral, so $e = ee' = e'$. Daher gibt es genau ein neutrales Element, für welches man oft „1“ schreibt.

1.1.2 Bemerkung

(a) Sei (G, \cdot) eine Gruppe und $a \in G$. Seien b, b' invers zu a . Dann

$$b \stackrel{(N)}{=} b \cdot 1 \stackrel{(I)}{=} b(ab') \stackrel{(A)}{=} (ba)b' \stackrel{(I)}{=} 1 \cdot b \stackrel{(N)}{=} b'.$$

Daher gibt es zu jedem $a \in G$ genau ein inverses Element in G , welches wir mit a^{-1} bezeichnen.

1 Gruppen

(b) (N) und (I) kann man wie folgt schreiben:

$$(N) \quad \forall a \in G : a1 = a = 1a$$

$$(I) \quad \forall a \in G : aa^{-1} = 1 = a^{-1}a$$

(c) Oft: „Sei G eine Gruppe“, statt: „Sei (G, \cdot) eine Gruppe.“

(d) Sei G eine Gruppe, $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in G$. Dann definiert man $\prod_{i=1}^n a_i := a_1 \cdot \dots \cdot a_n$ als 1 für $n = 0$ und indem man $a_1 \cdot \dots \cdot a_n$ sinnvoll mit Klammern versieht, sonst. Dies hängt nicht von der Wahl der Klammerung da, wie (A) für $n = 3$ besagt. Für $n > 3$ siehe [→ LA 2.1.6] oder mache es als Übung per Induktion. Falls G additiv geschrieben ist, schreibt man $\sum_{i=1}^n a_i$, statt $\prod_{i=1}^n a_i$.

(e) Sei G eine Gruppe, $n \in \mathbb{Z}$ und $a \in G$. Dann definiert man

$$a^n := \begin{cases} \prod_{i=1}^n a, & \text{für } n \geq 0, \\ \prod_{i=1}^n (a^{-1}), & \text{für } n \leq 0. \end{cases}$$

Fall G additiv geschrieben ist, schreibt man na , statt a^n .

1.1.3 Definition Ist (G, \cdot) eine Gruppe, so nennt man $\#G \in \mathbb{N}_0 \cup \{\infty\}$ die Ordnung von (G, \cdot) .

1.1.4 Beispiel

(a) Für jede Menge M bildet die Menge $S_M := \{f \mid f : M \rightarrow M \text{ bijektiv}\}$ mit der durch $fg := f \circ g$ ($f, g \in S_M$) gegebenen Multiplikation eine Gruppe. Man nennt sie die symmetrische Gruppe auf M . Das neutrale Element von S_M ist die Identität auf M und das zu einem $f \in S_M$ inverse Element ist die Umkehrfunktion von f , wodurch die Notation f^{-1} nicht zweideutig ist.

Für $n \in \mathbb{N}_0$ ist $S_n := S_{\{1, \dots, n\}}$ eine Gruppe der Ordnung $n! := \prod_{i=1}^n i$ „ n Fakultät“. Für $n \geq 3$ ist die nicht abelsch, dann die Transpositionen $\tau_{1,2}$ und $\tau_{2,3}$ konvertieren nicht, d.h. $\tau_{1,2}\tau_{2,3} \neq \tau_{2,3}\tau_{1,2}$. In der Tat: $(\tau_{1,2}\tau_{2,3})(1) = \tau_{1,2}(1) = 2$ und $(\tau_{2,3}\tau_{1,2})(1) = \tau_{2,3}(2) = 3$.

(b) Für jeden Vektorraum V ist die Menge $\text{Aut}(V) := \{f \mid f : V \rightarrow V \text{ linear und bijektiv}\}$ mit der Hintereinanderschaltung als Multiplikation eine Gruppe.

(c) Ist R ein kommutativer Ring (z. B. $R = \mathbb{Z}$), so ist $\text{GL}_n(R) := \{A \in R^{n \times n} \mid A \text{ invertierbar}\} = \{A \in R^{n \times n} \mid \det A \in R^\times\}$ eine Gruppe.

1.1.5 Proposition Sei G eine Gruppe und $a, b \in G$.

$$(a) \quad ab = 1 \iff a = b^{-1} \iff b = a^{-1}$$

$$(b) \quad (a^{-1})^{-1} = a$$

$$(c) \quad (ab)^{-1} = b^{-1}a^{-1}$$

Beweis:

$$(a) \quad \text{Gilt } ab = 1, \text{ so } a \stackrel{(N)}{=} a1 \stackrel{(I)}{=} a(bb^{-1}) \stackrel{(A)}{=} (ab)b^{-1} = 1b \stackrel{(N)}{=} b^{-1}. \text{ Gilt } a = b^{-1}, \text{ so } b \stackrel{(N)}{=} 1b \stackrel{(I)}{=} (a^{-1}a)b \stackrel{(A)}{=} a^{-1}(ab) = a^{-1}(b^{-1}b) \stackrel{(I)}{=} a^{-1}1 \stackrel{(N)}{=} a^{-1}. \text{ Gilt } b = a^{-1}, \text{ so } ab = 1.$$

$$(b) \quad \text{Aus } aa^{-1} \stackrel{(I)}{=} 1 \text{ folgt mit (a) } (a^{-1})^{-1} = a.$$

$$(c) \quad \text{Aus } (ab)(b^{-1}a^{-1}) \stackrel{(A)}{=} a(b(b^{-1}a^{-1})) \stackrel{(A)}{=} a((bb^{-1})a^{-1}) \stackrel{(I)}{=} a(1a^{-1}) \stackrel{(N)}{=} aa^{-1} \stackrel{(I)}{=} 1 \text{ folgt mit (a) } (ab)^{-1} = b^{-1}a^{-1}. \quad \square$$

1.1.6 Definition Seien (G, \cdot_G) und (H, \cdot_H) Gruppen. Dann heißt (H, \cdot_H) eine Untergruppe von (G, \cdot_G) , wenn $H \subseteq G$ und $\forall a, b \in H : a \cdot_H b = a \cdot_G b$.

1.1.7 Proposition Sei (G, \cdot_G) eine Gruppe und H eine Menge. Dann ist H genau dann Trägermenge einer Untergruppe von (G, \cdot_G) , wenn $H \subseteq G$, $1_G \in H$, $\forall a, b \in H : a \cdot_G b \in H$ und $\forall a \in H : a^{-1} \in H$.

In diesem Fall gibt es genau eine Abbildung $\cdot_H : H \times H \rightarrow H$ derart, dass (H, \cdot_H) eine Untergruppe von (G, \cdot_G) ist. Es gilt dann $1_H = 1_G$, $\forall a, b \in H : a \cdot_H b = a \cdot_G b$ und $a^{-1} = a^{-1}$ (je in G und H gebildet).

Beweis: Klar oder vgl. LA § 2. \square

1.1.8 Bemerkung

(a) Ist (H, \cdot_H) Untergruppe von (G, \cdot_G) , so schreibt man meist \cdot statt \cdot_H . Oft erwähnt man \cdot_H gar nicht mehr und schreibt einfach „ H ist Untergruppe von G “ oder $H \leq G$.

(b) Untergruppen abelscher Gruppen sind abelsch.

1.1.9 Beispiel

(a) Für $n \in \mathbb{N}_0$ ist $A_n := \{\sigma \in S_n \mid \text{sgn } \sigma = 1\}$ eine Untergruppe von S_n , die man

1 Gruppen

alternierende Gruppe nennt. [\rightarrow LA § 9.1]

Hier fehlt noch etwas ...

2.1.4 Beispiel

- (a) Für jeden Vektorraum V ist die Menge $\text{End}(V) = \{f \mid f : V \rightarrow V \text{ linear}\}$ der Endomorphismen von V mit der punktweisen Addition und der Hintereinanderschaltung als Multiplikation ein Ring mit Einheitengruppe $\text{End}(V)^\times = \text{Aut}(V)$. [\rightarrow LA § 7.1]
- (b) Ist R ein kommutativer Ring, so ist $R^{n \times n}$ ein Ring mit $(R^{n \times n})^\times = \text{GL}_n(R)$.

2.1.5 Definition Seien $(A, +_A, \cdot_A)$ und $(B, +_B, \cdot_B)$ Ringe. Dann heißt $(A, +_A, \cdot_A)$ ein *Unterring* von $(B, +_B, \cdot_B)$, wenn $A \subseteq B$, $1_B \in A$, $\forall a, b \in A : a +_A b = a +_B b$, $\forall a, b \in A : a \cdot_A b = a \cdot_B b$.

2.1.6 Proposition Sei $(B, +, \cdot)$ ein Ring und A eine Menge. Genau dann ist A Trägermenge eines Unterrings von $(B, +, \cdot)$, wenn $\{0, 1\} \subseteq A \subseteq B$, $\forall a, b \in A : a + b \in A$, $a \cdot b \in A$.

2.1.7 Beispiel

- (a) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Dann sind $\blacktriangledown_R^{n \times n} = \{A \in R^{n \times n} \mid A \text{ obere Dreiecksmatrix}\}$, $\blacktriangleleft_R^{n \times n} = \{A \in R^{n \times n} \mid A \text{ untere Dreiecksmatrix}\}$ und $\blacktriangleleft_R^{n \times n} \cap \blacktriangledown_R^{n \times n} = \{A \in R^{n \times n} \mid A \text{ Diagonalmatrix}\}$ Unterringe von $R^{n \times n}$ mit Einheitengruppen $(\blacktriangledown_R^{n \times n})^\times = \blacktriangledown_n(R)$, $(\blacktriangleleft_R^{n \times n})^\times = \blacktriangleleft_n(R)$ und $(\blacktriangleleft_R^{n \times n} \cap \blacktriangledown_R^{n \times n})^\times = \blacktriangledown_n(R) \cap \blacktriangleleft_n(R)$.
- (b) $\{0\}$ ist kein Unterring von \mathbb{Z} , denn $1 \notin \{0\}$.

2.1.8 Definition Seien A und B Ringe. Dann heißt $f : A \rightarrow B$ ein *(Ring-)Homomorphismus* von A nach B , wenn

f ein Gruppenhomomorphismus von A nach B ist,
 $f(1) = 1$ und
 $\forall a, b \in A : f(ab) = f(a)f(b)$ gilt.

Ein Ringhomomorphismus heißt

(Ring-)	(Einbettung oder) Mono-	/ Epi-	/ Isomorphismus
wenn f	injektiv	/ surjektiv	/ bijektiv ist,
in Zeichen	$f : A \hookrightarrow B$	/ $f : A \twoheadrightarrow B$	/ $f : A \xrightarrow{\cong} B$

2.1.9 Bemerkung Ist $f : A \rightarrow B$ ein Ringhomomorphismus, so ist im f ein Unterring von B , jedoch $\ker f$ in aller Regel kein Unterring von A . (Denn $1 \in \ker f \iff f(1) = 0$ in $B \iff 1 = 0$ in B . ζ)

2.1.10 Bemerkung Analog zu 1.2.7 und 1.2.8 führt man das *direkte Produkt* von Ringen durch punktweise Addition und Multiplikation ein.

2.1.11 Definition und Proposition [\rightarrow § ??], [\rightarrow LA § 3.3] Sei R ein Ring. Eine *Kongruenzrelation* auf R ist eine Kongruenzrelation \equiv auf der additiven Gruppe von R [\rightarrow ??], für die zusätzlich gilt:

$$\forall a, a', b, b' \in A : ((a \equiv a' \ \& \ b \equiv b') \implies ab \equiv a'b')$$

Ist \equiv ein Kongruenzrelation auf R , so wird R/\equiv vermöge $\overline{a} + \overline{b} = \overline{a+b}$ und $\overline{ab} = \overline{a}\overline{b}$ ($a, b \in A$) zu einem Ring („*Quotientenring*“, „*Faktoring*“, „*Restklassenring*“).

2.1.12 Definition Sei R ein Ring. Eine Untergruppe I der additiven Gruppe von R heißt (beidseitiges) *Ideal* von R , wenn:

$$\forall a \in R \ \forall b \in I : ab, ba \in I$$

2.1.13 Satz [\rightarrow ??] [\rightarrow LA § 3.3] Sei R ein Ring. Die Zuordnungen

$$\begin{aligned} \equiv & \mapsto \overline{0} \\ \equiv_I & \mapsto I \end{aligned}$$

vermitteln eine Bijektion zwischen der Menge der Kongruenzrelationen auf R und der Menge der Ideale von R .

Beweis. Wenn wir zeigen, dass beide Abbildungen wohldefiniert sind, dann folgt mit ??, dass sie auch invers zueinander sind. Also zu zeigen:

(a) \equiv ist Kongruenzrelation auf $R \implies \overline{0}$ ist Ideal von R

1 Gruppen

(b) I ist Ideal von $R \implies \equiv_I$ ist Kongruenzrelation auf R

Zu (a). Sei \equiv eine Kongruenzrelation auf R . Aus ?? wissen wir schon, dass $\bar{0}$ eine Untergruppe von R ist. Noch zu zeigen: $\forall a \in A : \forall b \in \bar{0} : ab \in \bar{0}$. Sei also $a \in R$ und $b \in \bar{0}$. Dann $ab \stackrel{b \equiv 0}{\equiv} a0 \stackrel{2.1.2(e)}{\equiv} 0$, also $ab \in \bar{0}$ und $ba \equiv 0a \equiv 0$, also $ba \in \bar{0}$.

Zu (b). Sei I eine Ideal von R . Aus ?? wissen wir schon, dass \equiv_I eine Kongruenzrelation der additiven Gruppe von R ist. Noch zu zeigen: $\forall a, a', b, b' \in A : ((a \equiv a' \ \& \ b \equiv b') \implies ab \equiv a'b')$. Seien also $a, a', b, b' \in R$ mit $a \equiv_I a'$ und $b \equiv_I b'$. Dann $ab - a'b' = \underbrace{a(b - b')}_{\in I} + \underbrace{b'(a - a')}_{\in I} \in I$, also $ab \equiv_I a'b'$. \square

2.1.14 Notation & Sprechweise Sei I ein Ideal des Ringes R . Schreibe $R/I := R/\equiv_I := \{a + I \mid a \in R\}$. Man bezeichnet die Kongruenzklasse $\bar{a}^I = a + I$ von $a \in R$ auch als *Restklasse* von a modulo I .

2.1.15 Bemerkung

- (a) Sei I ein Ideal des Ringes R . Dann ist die Abbildung $R \rightarrow R/I, a \mapsto \bar{a}^I$ nach Definition 2.1.11 ein Ringhomomorphismus, genannt *kanonischer Epimorphismus*.
- (b) Sei $f : A \rightarrow B$ ein Ringhomomorphismus. Dann ist $\ker f$ ein Ideal von A , aber im f im Allgemeinen kein Ideal von B . (Betrachte zum Beispiel $\mathbb{Z} \hookrightarrow \mathbb{Q}, a \mapsto a$.)

2.1.16 Homomorphiesatz für Ringe Seien A, B Ringe, I ein Ideal von A und $\varphi : A \rightarrow B$ ein Homomorphismus mit $I \subseteq \ker \varphi$. Dann gibt es genau eine Abbildung $\bar{\varphi} : A/I \rightarrow B$ mit $\bar{\varphi}(\bar{a}^I) = \varphi(a)$ für alle $a \in A$. Diese Abbildung $\bar{\varphi}$ ist ein Homomorphismus. Weiter gilt $\bar{\varphi}$ injektiv $\iff I = \ker \varphi$ und $\bar{\varphi}$ surjektiv $\iff B = \text{im } \varphi$.

Beweis. Mit ?? ist nur noch $\bar{\varphi}(1) = 1$ und $\bar{\varphi}(\bar{a}^I \bar{b}^I) = \bar{\varphi}(\bar{a}^I) \bar{\varphi}(\bar{b}^I)$ f.a. $a, b \in A$ zz zeigen.

Dies ist klar:

$$\begin{aligned} \bar{\varphi}(1) &= \bar{\varphi}(\bar{1}^I) = \varphi(1) = 1 \quad \text{und} \\ \bar{\varphi}(\bar{a}^I \bar{b}^I) &= \bar{\varphi}(\overline{ab}^I) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\bar{a}^I) \bar{\varphi}(\bar{b}^I) \quad \text{für alle } a, b \in A. \end{aligned}$$

\square

2.1.17 Isomorphiesatz für Ringe Seien A, B Ringe und $\varphi : A \rightarrow B$ ein Homomorphismus. Dann ist $\ker \varphi$ ein Ideal von A und $\bar{\varphi} : A/\ker \varphi \rightarrow \operatorname{im} \varphi$ mit $\bar{\varphi}(a^{\ker \varphi}) = \varphi(a)$ für $a \in A$ ein Isomorphismus. Insbesondere $A/\ker \varphi \cong \operatorname{im} \varphi$.

Beweis. Direkt aus 2.1.16. □

§ 2.2 Polynomringe [\rightarrow LA § 3.2]

2.2.1 Notation Sei R ein kommutativer Ring, $n \in \mathbb{N}_0$, $a = (a_1, \dots, a_n) \in R^n$ und $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$. Schreibe dann $|\alpha| = \alpha_1 + \dots + \alpha_n$ und $a^\alpha := a_1^{\alpha_1} + \dots + a_n^{\alpha_n}$.

2.2.2 Definition & Satz Sei A ein Unterring des kommutativen Ringes B .

(a) Sei $n \in \mathbb{N}_0$ und $b = (b_1, \dots, b_n) \in B^n$.

$$A[b] := A[b_1, \dots, b_n] := \left\{ \sum_{\substack{\alpha \in \mathbb{N}_0^n, \\ |\alpha| < d}} a_\alpha b^\alpha \mid d \in \mathbb{N}_0, a_\alpha \in A \right\}$$

ist der kleinste Unterring C von B mit $A \cup \{b_1, \dots, b_n\} \subseteq C$.

(b) Sei $E \subseteq B$. $A[E] = \bigcup \{A[b] \mid n \in \mathbb{N}_0, b \in B^n\}$ ist der kleinste Unterring C von B mit $A \cup E \subseteq C$.

Beweis. Dass die angegebenen Mengen jeweils in jedem solchen Unterring C enthalten sind, ist klar. Zu zeigen ist dann nur noch, dass sie jeweils einen Unterring bilden. Dies ist einfach und wir zeigen exemplarisch nur, dass $A[b]$ aus (a) unter Multiplikation abgeschlossen ist. Seien also $d, d' \in \mathbb{N}_0$, $a_\alpha \in A$ für alle $\alpha \in \mathbb{N}_0^n$ mit $|\alpha| \leq d$ und $a'_\alpha \in A$ für alle $\alpha \in \mathbb{N}_0^n$ mit $|\alpha| \leq d'$. Dann

$$\left(\sum_{|\alpha| \leq d} a_\alpha b^\alpha \right) \left(\sum_{|\alpha| \leq d'} a'_\alpha b^\alpha \right) = \sum_{|\gamma| \leq d+d'} \left(\sum_{\alpha+\beta=\gamma} a_\alpha a'_\beta \right) b^\gamma \in A[b],$$

wobei man $a_\alpha := 0$ für $d < |\alpha| \leq d+d'$ und $a'_\alpha := 0$ für $d' < |\alpha| \leq d+d'$ setzt. □

1 Gruppen

2.2.3 Definition Sei A ein Unterring des kommutativen Ringes B .

- (a) Sei $n \in \mathbb{N}_0$ und $b = (b_1, \dots, b_n) \in B^n$. Es heißen b_1, \dots, b_n *algebraisch unabhängig* über A (in B), wenn für alle $d \in \mathbb{N}_0$ und alle $a_\alpha \in A$ ($\alpha \in \mathbb{N}_0^n, |\alpha| \leq d$) gilt:

$$\sum_{\substack{\alpha \in \mathbb{N}_0^n, \\ |\alpha| \leq d}} a_\alpha b^\alpha = 0 \implies \forall \alpha \in \mathbb{N}_0^n : (|\alpha| \leq d \implies a_\alpha = 0)$$

Es heißt B *Polynomring* über A in b_1, \dots, b_n , wenn $B = A[b_1, \dots, b_n]$ und b_1, \dots, b_n algebraisch unabhängig über A sind.

- (b) Sei $E \subseteq B$. Es heißt E *algebraisch unabhängig* über A (in B), wenn für alle $n \in \mathbb{N}_0$ alle paarweise verschiedenen Elemente $b_1, \dots, b_n \in E$ algebraisch unabhängig über A sind.

Es heißt B *Polynomring* über A in E , wenn $B = A[E]$ und E algebraisch unabhängig über A ist.

2.2.4 Beispiel

- (a) Jeder kommutative Ring A ist ein Polynomring über sich selbst in \emptyset .
- (b) Der Nullring $\{0\}$ ist ein Polynomring über sich selbst in 0 .

2.2.5 Satz Sei A ein kommutativer Ring mit $0 \neq 1$. Sei E eine Menge mit $A \cap E = \emptyset$. Dann gibt es einen Polynomring über A in E .

Beweis. Bezeichne $\mathbb{N}_0^{(E)}$ die Menge aller $\alpha : E \rightarrow \mathbb{N}_0$ mit endlichem Träger $\text{supp}(\alpha) = \{e \in E \mid \alpha(e) \neq 0\}$. Mache die abelsche Gruppe $A^{\mathbb{N}_0^{(E)}}$ zu einem kommutativen Ring mit der „Faltung“ $*$ als Multiplikation, welche gegeben ist durch

$$(f * g)(\gamma) := \sum_{\substack{\alpha, \beta \in \mathbb{N}_0^{(E)}, \\ \alpha + \beta = \gamma}} f(\alpha)g(\beta) \quad \left(f, g \in A^{\mathbb{N}_0^{(E)}}, \gamma \in \mathbb{N}_0^{(E)} \right)$$

(Es handelt sich um eine endliche Summe, da $\text{supp}(\gamma)$ endlich. Man sieht sofort $f * g = g * f$, $f * (g + h) = f * g + f * h$ und $1 * f = f$ für

$$1 : \mathbb{N}_0^{(E)} \rightarrow A$$

$$\alpha \mapsto \begin{cases} 1, & \alpha = 0 \\ 0, & \text{sonst} \end{cases}$$

und rechnet

$$\begin{aligned} ((f * g) * h)(\gamma) &= \sum_{\alpha+\beta=\gamma} (f * g)(\alpha)h(\beta) = \sum_{\alpha+\beta=\gamma} \left(\sum_{\delta+\varepsilon=\alpha} f(\delta)g(\varepsilon) \right) h(\beta) \\ &= \sum_{\delta+\varepsilon+\beta=\gamma} f(\delta)g(\varepsilon)h(\beta) = \dots = (f * (g * h))(\gamma) \end{aligned}$$

für alle $f, g, h \in A^{\mathbb{N}_0^{(E)}}$, $\gamma \in \mathbb{N}_0^{(E)}$. \square^1

Hier fehlt noch etwas ...

2.3.6 Satz Sei A ein kommutativer Ring und $S \subseteq A$ eine multiplikative Menge, die keine Nullteiler von A enthält. Dann gibt es einen kommutativen Oberring B von A mit $S \subseteq B^\times$ und $B = S^{-1}A$.

Beweis. Durch $(a, s) \sim (b, t) : \iff at = bs$ ($a, b \in A, s, t \in S$) wird eine Äquivalenzrelation \sim auf $A \times S$ definiert. [Reflexiv und symmetrisch ist klar, transitiv: Seien $a, b, c \in A$ und $s, t, u \in S$ mit $(a, s) \sim (b, t) \sim (c, u)$. Dann $at = bs$ und $bu = ct$, also $atu = bsu = bus = cts$, das heißt $t(au - cs) = 0$ und daher $au = cs$, da $t \in S$ kein Nullteiler ist.] Der Leser zeigt als Übung, dass $+$ und \cdot durch

$$\begin{aligned} \widetilde{(a, s)} + \widetilde{(b, t)} &:= \widetilde{(at + bs, st)} \quad \text{und} \\ \widetilde{(a, s)} \cdot \widetilde{(b, t)} &:= \widetilde{(ab, st)} \end{aligned}$$

wohldefiniert ist und $(A \times S)/\sim$ zu einem kommutativen Ring mit $0 = \widetilde{(0, 1)}$, $1 = \widetilde{(1, 1)}$ machen.

Wegen $A \cong \tilde{A} := \{\widetilde{(a, 1)} \mid a \in A\} \subseteq (A \times S)/\sim$ reicht es zu zeigen, dass $\tilde{S} := \{\widetilde{(s, 1)} \mid s \in S\} \subseteq ((A \times S)/\sim)^\times$ und $(A \times S)/\sim = \tilde{S}^{-1}\tilde{A}$. Sei hierzu $a \in A, s \in S$. Dann $\widetilde{(s, 1)}\widetilde{(1, s)} = \widetilde{(s, s)} = \widetilde{(1, 1)} = 1$, also $\widetilde{(s, 1)}^{-1} = \widetilde{(1, s)}$ und $\widetilde{(a, s)} = \widetilde{(s, 1)}^{-1}\widetilde{(a, 1)} \in \tilde{S}^{-1}\tilde{A}$. \square

2.3.7 Satz Sei A ein Unterring des kommutativen Ringes B , $S \subseteq A \cap B^\times$ multiplikativ und $B = S^{-1}A$. Sei C ein weiterer Ring und $\varphi : A \rightarrow C$ ein Homomorphismus. Genau dann gibt es einen Homomorphismus $\psi : S^{-1}A \rightarrow C$ mit $\varphi = \psi|_A$, wenn $\varphi(S) \subseteq C^\times$. In diesem Fall ist ψ eindeutig bestimmt, denn es gilt $\psi\left(\frac{a}{s}\right) = \frac{\psi(a)}{\psi(s)}$ für $a \in A, s \in S$.

Beweis. Übung. \square

¹Korrektur: Ist der Beweis vollständig? Hier fehlen noch 2.2.6, 2.2.7 und 2.2.8 aus dieser Vorlesung.

1 Gruppen

2.3.8 Satz Sei A ein Unterring des kommutativen Ringes B , $S \subseteq A \cap B^\times$ multiplikativ und $B = S^{-1}A$. Dasselbe gelte mit C statt B . Dann gibt es genau einen Isomorphismus $\psi : B \rightarrow C$ mit $\psi|_A = \text{id}_A$.

Beweis. Wende 2.3.7 mit $\varphi : A \rightarrow C, a \mapsto a$ an, um zu sehen, dass id_A eine eindeutige Fortsetzung zu einem Homomorphismus $\psi : B \rightarrow C$ hat. Zu zeigen ist nur noch, dass ψ ein Isomorphismus ist. Mit 2.3.7 bekommt man aber auch einen Homomorphismus $\varphi : C \rightarrow B$ mit $\varphi|_A = \text{id}_A$. Nun ist $\varphi \circ \psi : C \rightarrow C$ ein Homomorphismus mit $(\varphi \circ \psi)|_A = \text{id}_A$ und daher $\varphi \circ \psi = \text{id}_C$ nach 2.3.7. Ebenso $\psi \circ \varphi = \text{id}_B$. Daher sind φ und ψ bijektiv. \square

2.3.9 Definition Sei A ein kommutativer Ring und $S \subseteq A$ eine multiplikative Menge, die keine Nullteiler von A enthält. Den (nach 2.3.6 existierenden und nach 2.3.8 im Wesentlichen eindeutigen) Oberring B von A mit $S \subseteq B^\times$ und $B = S^{-1}A$ nennt man Ring der Brüche mit Zählern aus A und Nennern aus S (oder Lokalisierung von A nach S).

Ist speziell S die Menge aller Nichtnullteiler von A (vgl. ??), so nennt man $Q(A) = S^{-1}A$ den totalen Quotientenring von A . Offenbar gilt: $Q(A)$ ist Körper $\iff A$ ist Integritätsring. Ist A ein Integritätsring, so nennt man den Körper $\text{qf}(A) := Q(A) = (A \setminus \{0\})^{-1}A$ daher auch den Quotientenkörper von A .

2.3.10 Bemerkung Es folgt nun, dass Integritätsringe genau die Unterringe von Körpern sind.

2.3.11 Definition und Satz (Körperadjunktion, vgl. Ringadjunktion 2.2.2)

(a) Ist K ein Unterring eines Körpers L und K ein Körper, so nennt man

- K einen Unterkörper von L ,
- L einen Oberkörper von K und
- $L|K$ („über“) eine Körpererweiterung.

(b) Sei $L|K$ eine Körpererweiterung. Sind $b_1, \dots, b_n \in L$, so ist $K(b_1, \dots, b_n) := (K[b_1, \dots, b_n] \setminus \{0\})^{-1}K[b_1, \dots, b_n] = \text{qf}(K[b_1, \dots, b_n]) \subseteq L$ der kleinste Unterkörper F von L mit $K \cup \{b_1, \dots, b_n\} \subseteq F$.

Ist $E \subseteq L$, so ist $K(E) := (K[E] \setminus \{0\})^{-1}K[E] = \text{qf}(K[E]) \subseteq L$ der kleinste Unterkörper F von L mit $K \cup E \subseteq F$.

Beweis. Trivial. \square

2.3.12 Definition (vgl. ??) Sei $L|K$ eine Körpererweiterung.

- (a) Sei $n \in \mathbb{N}_0$ und $b_1, \dots, b_n \in L$. Es heißt L ein Körper der rationalen Funktionen über K in b_1, \dots, b_n , wenn $L = K[b_1, \dots, b_n]$ und b_1, \dots, b_n algebraisch unabhängig über K sind.
- (b) Sei $E \subseteq L$. Es heißt L ein Körper von rationalen Funktionen über K in E , wenn $L = K[E]$ und E algebraisch unabhängig über K ist.²

2.3.13 Proposition (vgl. ??) Sei $L|K$ eine Körpererweiterung und $E \subseteq L$ mit $L = K[E]$. Sei R ein Ring und seien $\varphi, \psi : L \rightarrow R$ Homomorphismen mit $\varphi|_{K \cup E} = \psi|_{K \cup E}$. Dann $\varphi = \psi$.

Beweis. $F := \{a \in L \mid \varphi(a) = \psi(a)\}$ ist ein Unterkörper von L , der $K \cup E$ enthält. Also $F = L$. \square

2.3.14 Definition und Proposition Seien K und F Körper.

- (a) K besitzt nur die trivialen Ideale K und $\{0\}$.
- (b) Ist $\varphi : K \rightarrow F$ ein (Ring-)Homomorphismus, so nennt man φ auch einen Körperhomomorphismus. In diesem Fall gilt: Da $\varphi(1) = 1 \neq 0$ in F , liegt 1 nicht im Ideal $\ker \varphi$ von K , womit $\ker \varphi = \{0\}$ nach (a). Es ist daher $\varphi : K \hookrightarrow F$ eine Einbettung und $\varphi : K \xrightarrow{\cong} \text{im } \varphi$ ein Isomorphismus. Insbesondere ist das Bild von φ nicht nur ein Unterring, sondern sogar ein Unterkörper von F . Beachte auch, dass gelten muss $\varphi(-\frac{1}{a}) = \frac{1}{\varphi(a)}$ für alle $a \in K^\times$.³

2.3.15 Satz (vgl. ??) Seien $K(E)$ und $K(F)$ Körper von rationalen Funktionen über K in E bzw. F . Sei $f : E \rightarrow F$ eine Bijektion. Dann gibt es genau einen Isomorphismus $\psi : K(E) \rightarrow K(F)$ mit $\psi|_K = \text{id}_K$ und $\psi|_E = f$.

Beweis. Zur Existenz: Nach ?? gibt es einen Isomorphismus $\varphi : K[E] \rightarrow K[F]$ mit $\varphi|_K = \text{id}_K$ und $\varphi_E = f$. Da φ injektiv ist, gilt $\varphi(K[E] \setminus \{0\}) \subseteq K[F] \setminus \{0\} \subseteq K(F)^\times$ und 2.3.7 liefert einen Homomorphismus $\psi : K(E) \rightarrow K(F)$ mit $\psi|_{K[E]} = \varphi$. Da ψ ein Körperhomomorphismus ist, ist ψ injektiv und ψ ist ein Unterkörper von $K(F)$.⁴ Es gilt aber $K \cup F \subseteq \text{im } \varphi \subseteq \text{im } \psi$, weswegen ψ surjektiv ist.

Die Eindeutigkeit folgt aus 2.3.13.

²An Korrektor: War mir hier bzgl. der Klammern und der Namen (Index!) nicht ganz sicher.

³An Korrektor: Gehört da wirklich ein Minus hin?

⁴An Korrektor: Macht so keinen Sinn.

2.3.16 Notation und Sprechweise (vgl. ??) Sei K ein Körper. Schreibt man $K(X_1, \dots, X_n)$, so meint man dabei den (nach 2.3.15 im Wesentlichen eindeutig bestimmen und nach ?? und 2.3.9 existierenden) Körper der rationalen Funktionen in paarweise verschiedenen „unbestimmten“ X_1, \dots, X_n .⁵

2.3.17 Definition und Proposition Sei A ein kommutativer Ring und $S \subseteq A$ eine multiplikative Menge. Wenn S Nullteiler enthält (das heißt, wenn es $s \in S$ und $a \in A$ gibt mit $sa = 0$), dann können wir keinen Oberring $S^{-1}A$ wie in 2.3.6 konstruieren (siehe ??). In diesem Fall (und allgemein) setzten wir $I_S := \{a \in A \mid \exists s \in S : sa = 0\}$. Es ist I_S ein Ideal von A , das S multiplikativ ist. Es ist dann $\bar{S} := \{\bar{s} \mid s \in S\} \subseteq \bar{A} := A/I_S$ multiplikativ und ohne Nullteiler. Man nennt dann den Oberring $\bar{S}^{-1}\bar{A}$ von $\bar{A} = A/I_S$ die Lokalisierung von A nach S , in Zeichen $A_S := \bar{S}^{-1}\bar{A}$. Man hat einen Homomorphismus⁶ $\iota_S(S) \subseteq A_S^\times$ und $\ker \iota_S = I_S$. Oft schreibt man schlampig wieder $S^{-1}A$ und $\frac{a}{s}$ ($a \in A, s \in S$) statt $\bar{S}^{-1}\bar{A}$ und $\frac{\bar{a}}{\bar{s}}$ ($a \in A, s \in S$).

2.3.18 Satz Sei A ein kommutativer Ring und $S \subseteq A$ multiplikativ. Sei B ein weiterer kommutativer Ring und $\varphi : A \rightarrow B$ ein Homomorphismus mit $\varphi(S) \subseteq B^\times$. Dann gibt es genau einen Homomorphismus $\psi : A_S \rightarrow B$ mit $\varphi = \psi \circ \iota_S$.

Beweis. Übung. □

§ 2.4 Primideale und maximale Ideale

2.4.1 Wiederholung Sei R ein kommutativer Ring. Ist $E \subseteq R$, so ist $(E) := \{\sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}, a_i \in R, b_i \in E\}$ das kleinste Ideal von R , welches E enthält und man nennt es das von E (in R) erzeugte Ideal [→ LA 3.3.9, 3.3.10]. Für $b_1, \dots, b_n \in R$ schreibt man auch $(b_1, \dots, b_n) := (b_1, \dots, b_n) = \{\sum_{i=1}^n a_i b_i \mid a_i \in R\}$. Ideale der Form (b) mit $b \in R$ nennt man auch Hauptideale [→ LA 3.3.11]. Es heißt R ein Hauptidealring, wenn R ein Integritätsring ist, in dem jedes Ideal ein Hauptideal ist. \mathbb{Z} und $K[X]$ (K ein Körper, X eine Unbekannte) sind Hauptidealringe [→ LA 3.3.13, 10.2.2] oder [1, § 2.2, § 2.4].

Ist $p \in R$, so heißt p irreduzibel (in R), wenn

$$p \notin R^\times \quad \& \quad \forall a, b \in R : (p = ab \Rightarrow (a \in R^\times \text{ oder } b \in R^\times))$$

⁵An Korrektor: Index für „Körper der rationalen Funktionen“ anpassen.

⁶An Korrektor: Wie sieht der aus? Habe ich mir nicht aufgeschrieben.

und prim (in R), wenn

$$p \notin R^\times \quad \& \quad \forall a, b \in R : (p|ab \Rightarrow (p|a \text{ oder } p|b)).$$

In einem Integritätsring ist jedes Primelement $\neq 0$ irreduzibel. Die Äquivalenzrelation $\hat{=}$ auf R ist definiert durch $a \hat{=} b : \iff (a|b \& b|a) \iff (a) = (b) \ (a, b \in R)$.

Setze $\hat{a} := \frac{a}{a}$ für $a \in R$. Fixiere $\mathbb{P}_R \subseteq R$ mit $\mathbb{P}_R \rightarrow \{a \in R \mid a \text{ prim}, a \neq 0\} / \hat{=} , p \rightarrow \hat{p}$ bijektiv. (Z. B. $\mathbb{P}_{\mathbb{Z}} = \mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}$ für $R = \mathbb{Z}$.) Bezeichne $\mathbb{N}_0^{(\mathbb{P}_R)}$ die Menge der Funktionen $\alpha : \mathbb{P}_R \rightarrow \mathbb{N}_0$ mit endlichem Träger $\text{supp}(\alpha) := \{p \in \mathbb{P}_R \mid \alpha(p) \neq 0\}$.

Für jedes $\alpha \in \mathbb{N}_0^{(\mathbb{P}_R)}$ setze $\mathbb{P}_R^\alpha := \prod_{p \in \text{supp}(\alpha)} p^{\alpha(p)}$. Man nennt $(c, \alpha) \in R \times \mathbb{N}_0^{(\mathbb{P}_R)}$ eine Primfaktorzerlegung von $a \in R$, wenn $a = c\mathbb{P}_R^\alpha$. In Integritätsringen sind Primfaktorzerlegungen eindeutig. Es heißt R ein faktorieller Ring, wenn er ein Integritätsring ist, in dem jedes $a \in R \setminus \{0\}$ eine Primfaktorzerlegung besitzt. Jeder Hauptidealring ist faktoriell. In einem faktoriellen Ring ist jedes irreduzible Element prim. [1, § 2.4]

2.4.2 Definition Sei R ein kommutativer Ring. Ein Ideal \mathfrak{p} von R heißt Primideal von R , wenn

$$1 \notin \mathfrak{p} \quad \& \quad \forall a, b \in R : (ab \in \mathfrak{p} \Rightarrow (a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p})).$$

Ein Ideal I von R heißt echt, wenn $1 \notin I$ (oder äquivalent $I \neq R$). Ein Ideal \mathfrak{m} von R heißt maximales Ideal von R , wenn \mathfrak{m} ein maximales Element der durch Inklusion halbgeordneten Menge aller echten Ideale von R ist.

2.4.3 Bemerkung Sei R ein kommutativer Ring. Die in 2.4.1 wiederholte Definition eines Primelements $p \in R$ kann man offensichtlich wie folgt lesen:

$$1 \notin (p) \quad \& \quad \forall a, b \in R : (ab \in (p) \Rightarrow (a \in (p) \text{ oder } b \in (p))).$$

Es folgt für $p \in R$: p Primelement $\iff (p)$ ist Primideal

2.4.4 Satz Sei I ein Ideal des kommutativen Ringes R . Dann gilt

- (a) I Primideal $\iff R/I$ Integritätsring und
- (b) I maximales Ideal $\iff R/I$ Körper

Beweis. Übung. □

2.4.5 Korollar Jedes maximale Ideal eines kommutativen Rings ist ein Primideal.

Beweis. Jeder Körper ist ein Integritätsring. □

2.4.6 Korollar Seien A, B kommutative Ringe und $\varphi : A \rightarrow B$ ein Homomorphismus. Sei \mathfrak{q} ein Primideal von B . Dann ist $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$ ein Primideal von A .

Beweis. $\psi : A \rightarrow B/\mathfrak{q}, a \mapsto \overline{\varphi(a)}^{\mathfrak{q}}$ ist Hintereinanderschaltung der Homomorphismen $A \xrightarrow{\varphi} B \xrightarrow{b \mapsto \overline{b}^{\mathfrak{q}}} B/\mathfrak{q}$ und daher ein Homomorphismus. Nach Isomorphiesatz 2.1.17 ist $A/\ker \psi \cong \text{im } \psi$. Es ist ψ ein Unterring des Integritätsrings B/\mathfrak{q} und daher auch ein Integritätsring. Somit ist auch $A/\ker \psi$ ein Integritätsring, das heißt $\ker \psi$ ein Primideal von A . Es gilt $\ker \psi = \{a \in A \mid \psi(a) = 0\} = \{a \in A \mid \overline{\psi(a)}^{\mathfrak{q}} = 0\} = \{a \in A \mid \varphi(a) \in \mathfrak{q}\} = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

2.4.7 Beispiel Sei K ein Körper. Im Polynomring $K[X, Y]$ ist (X) ein Primideal, denn $K[X, Y]/(X) \cong K[Y]$ ist ein Integritätsring (betrachte den Einsetzungshomomorphismus $K[X, Y] \rightarrow K[Y], p \mapsto p(0, Y)$ und wende den Isomorphiesatz 2.1.17 an). Es ist (X) kein maximales Ideal, denn $K[X, Y]/(X) \cong K[Y]$ ist kein Körper. Dagegen ist (X, Y) ein maximales Ideal von $K[X, Y]$, denn $K[X, Y]/(X, Y) \cong K$ ist ein Körper (betrachte $K[X, Y] \rightarrow K, p \mapsto (0, 0)$).

2.4.8 Satz In einem Hauptidealring ist jedes Primideal $\neq \{0\}$ ein maximales Ideal.

Beweis. Sei R ein Hauptidealring und $\mathfrak{p} \neq \{0\}$ ein Primideal in R . Sei I ein Ideal von R mit $p \subseteq I$. Zu zeigen: $I = \mathfrak{p}$ oder $I = R$. Wähle $p, a \in R$ mit $\mathfrak{p} = (p)$ und $I = (a)$. Die Bedingung $p \subseteq I$ bedeutet $(p) \subseteq (a)$, d. h. $p \in (a)$. Wähle $b \in R$ mit $p = ab$. Da p gemäß 2.4.3 prim ist und R ein Integritätsring ist, ist p irreduzibel in R . Also gilt $a \in R^\times$ oder $b \in R^\times$, also $I = (a) = R$ oder $I = (a) = (b^{-1}p) \subseteq (p) = \mathfrak{p} \subseteq I$. Also $I = R$ oder $I = \mathfrak{p}$ wie gewünscht.

Hier fehlt noch etwas ...

§ 4 Körper [→ LA § 4]

§ 4.1 Endliche und algebraische Körpererweiterungen

4.1.1 Definition Sei $L|K$ eine Körpererweiterung [→ 2.3.11]. Die Dimension $[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$ des K -Vektorraums L [→ LA § 6.1] nennt man den (Körper-)Grad von L über K (nicht zu verwechseln mit dem Index aus ??!). Ist $[L : K] < \infty$ ($[L : K] = \infty$), so nennt man L endlich (unendlich) über K und $L|K$ eine endliche (unendliche) Körpererweiterung.

4.1.2 Beispiel

- (a) $[K : K] = 1$ für jeden Körper K .
- (b) $[K(X) : K] = \infty$ für jeden Körper K .
- (c) $[\mathbb{C} : \mathbb{R}] = 2$

4.1.3 Proposition Sei $L|K$ eine Körpererweiterung von V ein L -Vektorraum (und damit auch ein K -Vektorraum). Sei A eine Basis des K -Vektorraums L und B eine Basis des L -Vektorraums V . Dann ist $A \times B \rightarrow AB := \{ab \mid a \in A, b \in B\}$, $(a, b) \mapsto ab$ bijektiv und AB eine Basis des K -Vektorraums V .

Beweis. Zu zeigen:

- (a) $\text{span}_K AB = V$
- (b) Für paarweise verschiedene $a_1, \dots, a_m \in A$ und paarweise verschiedene $b_1, \dots, b_n \in B$ sind $a_1 b_1, \dots, a_1 b_n, \dots, a_m b_1, \dots, a_m b_n$ linear unabhängig.

Zu (a). Für jedes $\lambda \in L$ und $b \in B$ gilt $\lambda \in \text{span}_K A$ und daher $\lambda b \in \text{span}_K Ab \subseteq \text{span}_K AB$. Daraus folgt $V = \text{span}_L B \subseteq \text{span}_K AB \subseteq V$.

Zu (b). Seien $\lambda_{ij} \in K$ ($1 \leq i \leq m, 1 \leq j \leq n$) mit $\sum_{i=1}^m \sum_{j=1}^n \lambda_{ij} a_i b_j = 0$. Dann $\sum_{j=1}^n (\sum_{i=1}^m \lambda_{ij} a_i) b_j = 0$ und daher $\sum_{i=1}^m \lambda_{ij} a_i = 0$ für alle j , also $\lambda_{ij} = 0$ für alle i, j . \square

4.1.4 Sprechweise Ein Zwischenkörper einer Körpererweiterung $L|K$ ist ein Unterkörper von L , der K enthält.

4.1.5 Korollar Sei F ein Zwischenkörper der Körpererweiterung $L|K$. Dann ist $L|K$ endlich genau dann, wenn $L|F$ und $F|K$ beide endlich sind, und in diesem Fall gilt die sogenannte „Gradformel“

$$[L : K] = [L : F][F : K].$$

4.1.6 Definition Sei $L|K$ eine Körpererweiterung. Dann heißt $a \in L$ algebraisch über K , wenn es $f \in K[x] \setminus \{0\}$ gilt mit $f(a) = 0$ [das heißt, wenn a nicht algebraisch unabhängig über K ist, \rightarrow ??]. Es heißt $L|K$ algebraisch, wenn jedes Element von L algebraisch über K ist.

4.1.7 Beispiel

- (a) $\sqrt{2}$ ist algebraisch über \mathbb{Q} , denn $(\sqrt{2})^2 - 2 = 0$.
- (b) i und $i + 1$ sind algebraisch über \mathbb{Q} , denn $i^2 + 1 = 0$ und $(i + 1)^2 - 2(i + 1) + 2 = 0$.
- (c) $K \in K(X)$ ist nicht algebraisch über K . (K ein Körper.)

4.1.8 Definition Sei $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K . Dann ist der Kern von $K[X] \rightarrow L, f \mapsto f(a)$ ein Ideal von $K[X]$, welches von einem eindeutig bestimmten normierten Polynom erzeugt wird \rightarrow LA 10.2.4], dem sogenannten Minimalpolynom $\text{irr}_K(a) \in K[X]$.

4.1.9 Proposition Sei $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K . Dann sind für $f \in K[X]$ äquivalent:

- (a) $f = \text{irr}_K(a)$
- (b) f ist das normierte Polynom kleinsten Grades mit $f(a) = 0$.

(c) f ist normiert und irreduzibel in $K[X]$ und es gilt $f(a) = 0$.

(d) f ist das Minimalpolynom des K -Vektorraumendomorphismus $\lambda_a : L \rightarrow L$, $b \mapsto ab$.

Beweis.

(a) \implies (b): Klar

(b) \implies (c): Gelte (b). Zu zeigen ist f irreduzibel. Es gilt $f \in K[X]^\times = K^\times$, da $f(a) = 0$. Seien $g, h \in K[X]$ mit $f = gh$. Zu zeigen ist $g \in K^\times$ oder $h \in K^\times$. Wegen $g(a)h(a) = (gh)(a) = f(a) = 0$ gilt $g(a) = 0$ oder $h(a) = 0$. Dann gilt aber $\deg g \geq \deg f$ oder $\deg h \geq \deg f$ und daher $h \in K^\times$ oder $g \in K^\times$.

(c) \implies (a): Gelte (c). Wegen $f(a) = 0$ gilt dann $f \in (\text{irr}_K(a))^1$, das heißt, es gibt $g \in K[X]$ mit $f = g \text{irr}_K(a) \in K^\times$. Letzteres ist unmöglich, also $g \in K^\times$ und sogar $g = 1$, da f und $\text{irr}_K(a)$ beide normiert sind.

(a) \iff (d): Es reicht zu zeigen, dass für alle $g \in K[X]$ gilt: $g(a) = 0 \iff g(\lambda_a) = 0$ [\rightarrow LA 10.2.18]. Dies folgt aus $(g(\lambda_a))(b) = (g(a))b$ für alle $b \in L$. \square

4.1.10 Proposition Sei $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K . Dann ist $K[X]/(\text{irr}_K(a))$ ein Körper und $K[X]/(\text{irr}_K(a)) \rightarrow K[a]$, $\bar{f} \mapsto f(a)$ ein Isomorphismus. Insbesondere ist $K[a] = K(a)$ auch ein Körper und $\deg \text{irr}_K(a) = [K(a) : K]$.

Beweis. Nach dem Isomorphiesatz für Ringe und für K -Vektorräume liefert der Einsetzungshomomorphismus $K[X] \twoheadrightarrow K[a]$, $f \mapsto f(a)$ den Ring- und K -Vektorraumisomorphismus $K[X]/(\text{irr}_K(a)) \rightarrow K[a]$, $\bar{f} \mapsto f(a)$.

Da $\text{irr}_K(a)$ irreduzibel im Hauptidealring $K[X]$ ist, ist $K[X]/(\text{irr}_K(a))$ nach ?? (siehe auch ??) ein Körper. Daher ist auch der dazu isomorphe Ring $K[a]$ ein Körper, das heißt $K[a] = K(a)$ [\rightarrow ??]. Setzt man nun $d := \deg \text{irr}_K(a)$, so bilden $\bar{1}, \bar{X}, \dots, \bar{X}^{d-1}$ offensichtlich eine Basis des K -Vektorraumes $K[X]/(\text{irr}_K(a))$ und daher deren Bilder $1, a, \dots, a^{d-1}$ eine Basis des K -Vektorraums $K[a] = K(a)$. Insbesondere ist $d = [K(a) : K]$. \square

4.1.11 Beispiel $\text{irr}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/(X^2 - 2)$ und $1, \sqrt{2}$ bilden eine \mathbb{Q} -Basis von $\mathbb{Q}(\sqrt{2})$.

4.1.12 Satz Sei $L|K$ eine Körpererweiterung und $a \in L$. Dann sind äquivalent:

¹Korrektur: Hier fehlt doch was um die Klammern?

- (a) a ist algebraisch über K
- (b) $K(a)|K$ ist endlich
- (c) $K[a] = K(a)$

Beweis.

(a) \implies (b): Nach 4.1.10.

(b) \implies (a): Ist $d := [K(a) : K] < \infty$, so sind $1, a, \dots, a^d$ linear abhängig im K -Vektorraum $K(a)$

(a) \implies (c): Nach 4.1.10

(c) \implies (a): Ist a nicht algebraisch über K , das heißt a algebraisch unabhängig über K , so ist $K[a]$ ein Polynomring über K und daher $K[a]^\times = K^\times \neq K[a] \setminus \{0\}$. Insbesondere ist dann $K[a]$ kein Körper und daher $K[a] \neq K(a)$. \square

4.1.13 Korollar Jede endliche Körpererweiterung ist algebraisch.

4.1.14 Proposition Sei $L|K$ eine Körpererweiterung und $a_1, \dots, a_n \in L$ algebraisch über K mit $L = K(a_1, \dots, a_n)$. Dann gilt $L = K[a_1, \dots, a_n]$ und $L|K$ ist endlich.

Beweis. Für jedes $i \in \{1, \dots, n\}$ ist a_i insbesondere algebraisch über $K(a_1, \dots, a_{i-1})$ und daher nach 4.1.12 auch $K(a_1, \dots, a_i)$ über $K(a_1, \dots, a_{i-1})$ endlich.

Es folgt mir 4.1.5, dass $L|K$ endlich ist und mit 4.1.12, dass $L = K(a_1) \cdots (a_n) = K[a_1] \cdots [a_n] = K[a_1, \dots, a_n]$. \square

4.1.15 Definition Eine Körpererweiterung $L|K$ heißt endlich erzeugt, wenn es $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in L$ gibt mit $L = K(a_1, \dots, a_n)$.

4.1.16 Korollar Sei $L|K$ eine Körpererweiterung. Dann ist $L|K$ endlich genau dann, wenn $L|K$ endlich erzeugt und algebraisch ist.

4.1.17 Satz (Transitivität der Algebraizität) Sei F ein Zwischenkörper von $L|K$ und $F|K$ algebraisch. Ist $a \in L$ algebraisch über F , so ist a auch algebraisch über K .

Beweis. Bezeichne die Koeffizienten von $\text{irr}_F(a) \in F[X]$ mit $a_1, \dots, a_n \in F$. Dann ist a sogar algebraisch über $K(a_1, \dots, a_n)$.

Da die Körpererweiterung $K(a_1, \dots, a_n)|K$ endlich erzeugt und algebraisch ist, ist sie auch endlich. Da $K(a_1, \dots, a_n)(a)|K(a_1, \dots, a_n)$ auch endlich ist, ist nach 4.1.5 $K(a_1, \dots, a_n, a)|K$ endlich und damit algebraisch. Insbesondere ist a algebraisch über K . \square

4.1.18 Korollar Sei F ein Zwischen Körper von $L|K$. Dann ist $L|K$ algebraisch genau dann, wenn $L|F$ beide algebraisch sind $[\rightarrow \text{vgl. 4.1.5}]$.²

4.1.19 Definition und Satz Sei $L|K$ eine Körpererweiterung. Dann ist $\overline{K}^L := \{a \in L \mid a \text{ algebraisch über } K\}$ ein Zwischenkörper von $L|K$, genannt der (relative) algebraische Abschluss von K über L .

Beweis. Zu zeigen sind:

- (a) $L \subseteq \overline{K}^L$
- (b) $\forall a, b \in \overline{K}^L : a + b, a \cdot b \in \overline{K}^L$
- (c) $\forall a \in \overline{K}^L \setminus \{0\} : \frac{1}{a} \in \overline{K}^L$

Zu (a). Ist klar.

Zu (b). Sind $a, b \in \overline{K}^L$, so ist $K(a, b)|K$ endlich nach 4.1.14 und damit algebraisch und daher $a + b, a \cdot b \in K(a, b)$ algebraisch über K .

Zu (c). Zeigt man genauso.

4.1.20 Beispiel Den Körper $\overline{\mathbb{Q}}^{\mathbb{C}} (\overline{\mathbb{Q}}^{\mathbb{R}})$ nennt man den Körper der algebraischen (reellen algebraischen) Zahlen.

§ 4.2 Der algebraische Abschluss

4.2.1 Satz von Kronecker Sei K ein Körper und $f \in K[X]$ irreduzibel und normiert. Dann gibt es eine endliche Körpererweiterung $L|K$ und ein $a \in L$ mit $L = K(a)$ und $\text{irr}_K(a) = f$.

²Korrektur: Aussage wahrscheinlich so nicht richtig?

4 Körper [→ LA § 4]

Nach 4.1.10 ist klar, dass der gesuchte Körper, falls er existiert, isomorph zu $K[X]/(f)$ sein muss. $L := K[X]/(f)$ ist nach ?? ein Körper. $K' := \{\bar{b} \mid b \in K\}$ ist ein zu K isomorpher Unterkörper von L , da $K \hookrightarrow L$, $b \mapsto \bar{b}$ und $f' := \varphi(f) \in K'[X]$ mit $\varphi : K[X] \xrightarrow{\cong} K'[X]$, $b \mapsto \bar{b}$ ($b \in K$), $X \mapsto X$.

Es reicht, die Behauptung für (K', f') statt (K, f) zu zeigen. Setzt man $a := \bar{X} \in L$, so ist $f' \in K'[X]$ irreduzibel mit $f'(a) = f'(\bar{X}) = \bar{f} = 0$ und daher $f' = \text{irr}_{K'}(a)$ nach 4.1.9. \square

4.2.2 Korollar Sei K ein Körper und $f \in K[X] \setminus K$. Dann gibt es ein $L|K$ und ein $a \in L$ mit $[L : K] \leq \deg f$ und $f(a) = 0$.

Beweis. Wähle $g \in K[X]$ irreduzibel mit $g|f$. Wende 4.2.1 auf g an.

4.2.3 Beispiel [→ LA § 4.2] Sei K ein Körper, in dem es kein $a \in K$ gibt mit $a^2 = -1$. Dann ist $X^2 + 1$ irreduzibel in $K[X]$ und es gibt $L|K$ und $i \in L$ mit $L = K(i)$ und $\text{irr}_K(i) = X^2 + 1$.

4.2.4 Definition Ein Körper K heißt algebraisch abgeschlossen, wenn jedes Polynom aus $K[X] \setminus K$ eine Nullstelle in K hat.

4.2.5 Bemerkung Der noch zu beweisende Fundamentalsatz der Algebra besagt, dass \mathbb{C} algebraisch abgeschlossen ist [→ LA 4.2.12].

4.2.6 Proposition Sei K ein Körper. Dann sind äquivalent:

- (a) K ist algebraisch abgeschlossen.
- (b) Jedes Polynom aus $K[X] \setminus \{0\}$ zerfällt [→ LA 10.1.13].
- (c) Jedes irreduzible Polynom aus $K[X]$ hat den Grad 1.
- (d) K ist der einzige über K algebraische Oberkörper von K .
- (e) K ist der einzige über K endliche Oberkörper von K .

Beweis.

(a) \implies (b): Durch sukzessives Abspalten von Nullstellen [→ LA 4.2.10].

(b) \implies (c): Klar.

(c) \implies (d): Gelte (c). Sei $L|K$ algebraisch. Zu zeigen ist $L = K$. Sei $a \in L$. Zu zeigen ist $a \in K$. Nach (c) gilt $\text{irr}_K(a) = X - c$ für ein $c \in K$. Dann aber $a - c = 0$, also $a = c \in K$.

(d) \implies (e): Klar nach 4.1.13.

(e) \implies (a): Gelte (e) und sei $f \in K[X] \setminus K$. Nach 4.2.2 gibt es eine endliche Erweiterung L von K und ein $a \in L$ mit $f(a) = 0$. Nach (e) gilt $L = K$ und daher $a \in K$. \square

4.2.7 Lemma Sei K ein Körper. Dann gibt es eine algebraische Körpererweiterung $L|K$ derart, dass jedes Polynom aus $K[X] \setminus K$ in L eine Nullstelle hat.

Beweis. Wir treiben die Beweisidee des Satzes von Kronecker 4.2.1 bis zum Exzess. Definiere $I \rightarrow ??$

$$I := (\{f \in X_f \mid f \in K[X] \setminus K\}) \subseteq K[X_f \mid f \in K[X] \setminus K] =: A^3$$

Wir zeigen $1 \notin I$ und nehmen hierzu an $1 \in I$. Wähle $f_1, \dots, f_n \in K[X] \setminus K$ und $g_1, \dots, g_n \in A$ mit

$$1 = \sum_{i=1}^n g_i f_i X_{f_i}^4 \quad (*)$$

alle f_i (und damit X_{f_i}) paarweise verschieden. Durch n -faches Anwenden von 4.2.2 erhält man sukzessive $L|K$ und $a_1, \dots, a_n \in L$ mit $f_i(a_i) = 0$ für $i \in \{1, \dots, n\}$. Durch Einsetzen von a_i für X_{f_i} und zum Beispiel 0 für die übrigen Unbestimmten in $(*)$, folgt $1 = 0$.

Wegen $1 \notin I$ gibt es nach ?? ein maximales Ideal \mathfrak{m} von A mit $I \subseteq \mathfrak{m}$. Dann ist $L := A/\mathfrak{m}$ nach ?? ein Körper. Definiere $K' := \{\bar{b} \mid b \in K\} \cong K \subseteq L$. Es reicht zu zeigen:

(a) $L|K'$ ist algebraisch.

(b) Jedes Polynom aus $K'[X] \setminus K'$ hat in L eine Nullstelle.

Beweis.

Zu (a). $L = K'[\overline{X}_f \mid f \in K[x] \setminus K] \subseteq \overline{K'}^L$, denn für alle $f \in K[X] \setminus K$ ist \overline{X}_f algebraisch über K' . In der Tat: Definiert man $f' \in K'[X] \setminus K'$ wie im Beweis von 4.2.1, so gilt $f'(\overline{X}_f) = \overline{f(X_f)} = 0$.

Zu (b). Dies zeigt auch (b). \square

³Korrektur: Kann ich nicht lesen.

⁴Korrektur: Kann ich nicht lesen.

4.2.8 Bemerkung Man kann zeigen, dass in der Situation von 4.2.6 der Körper L automatisch algebraisch abgeschlossen ist [1, A 3.7.11] [4, A 8.8]. Dies ist für uns aber noch zu schwierig, weshalb wir den Trick anwenden werden, das Lemma zu iterieren, um die Existenz eines algebraischen Abschlusses im folgenden Sinn zu zeigen:

4.2.9 Definition \rightarrow 4.1.19] Sei $L|K$ eine algebraische Körpererweiterung und L algebraisch abgeschlossen. Dann heißt L ein algebraischer Abschluss von K .

4.2.10 Satz [Ernst Steinitz, geb. 1871, gest. 1928] Jeder Körper besitzt einen algebraischen Abschluss.

Beweis. Sei K ein Körper. Nach 4.2.6 gibt es eine Folge $(K_n)_{n \in \mathbb{N}}$ von Körpern derart, dass $K_0 = K$ und für jedes $n \in \mathbb{N}_0$ $K_{n+1}|K_n$ eine algebraische Körpererweiterung ist mit der Eigenschaft, dass jedes Polynom aus $K_n[X]$ in K_{n+1} eine Nullstelle hat. Definiere einen Körper L durch $L := \bigcup \{K_n \mid n \in \mathbb{N}\}$ und $A +_L b = a +_{K_n} b$ sowie $a \cdot_L b = a \cdot_{K_n} b$ für alle $a, b \in L$ und $n \in \mathbb{N}$ mit $a, b \in K_n$.

Es ist L offensichtlich ein algebraischer Oberkörper von K (denn jedes K_n ist es nach 4.1.18). Schließlich ist L algebraisch abgeschlossen. Ist nämlich $f \in L[X] \setminus L$, so gibt es $n \in \mathbb{N}_0$ mit $f \in K_n[X] \setminus K_n$ und f hat in $K_{n+1} \subseteq L$ eine Nullstelle. \square

4.2.11 Beispiel Falls \mathbb{C} algebraisch abgeschlossen ist (was wir später beweisen werden), so ist \mathbb{C} ein algebraischer Abschluss von \mathbb{R} und $\overline{\mathbb{Q}}^{\mathbb{C}} \rightarrow ??$ ein algebraischer Abschluss von \mathbb{Q} .

4.2.12 Lemma Seien $L|K$ und $L'|K'$ eine Körpererweiterung, $\varphi : K \rightarrow K'$ ein Isomorphismus, $a \in L$ und $b \in L'$. Bezeichne $\tilde{\varphi} : K[X] \rightarrow K'[X]$ den Isomorphismus mit $\tilde{\varphi}|_K = \varphi$ und $\tilde{\varphi}(X) = X$. Dann sind äquivalent:⁵

- (a) Es gibt einen Isomorphismus $\psi : K(a) \rightarrow K'(b)$ mit $\psi|_K = \varphi$ und $\psi(a) = b$.
- (b) Entweder ist sowohl a algebraisch über K als auch b über K' mit $\tilde{\varphi}(\text{irr}_K(a)) = \text{irr}_{K'}(b)$ ⁶ oder weder a ist algebraisch über K noch b über K' .

Beweis.

(a) \implies (b) Ist einfach.

⁵Hier könnte man noch die Grafiken einfügen.

⁶Korrektur: Stand anders in der Vorlage.

(b) \implies (a) Seien zunächst weder a algebraisch über K noch b über K' . Dann ist $K[a]$ (bzw. $K'[b]$) ein Polynomring über K (bzw. K') in der Unabhängigen a (bzw. b). Daher findet man einen Isomorphismus $\psi_0 : K[a] \rightarrow K'[b]$ mit $\psi_0|_K = \varphi$ und $\psi_0(a) = b$. Mit 2.3.7 kann man ψ_0 zu einem Isomorphismus $\psi : K[a] \rightarrow K'[b]$ erweitern.

Seien nun sowohl a algebraisch über K als auch b über K' und es gelte $\tilde{\varphi}(\text{irr}_K(a)) = \text{irr}_{K'}(b)$. Wähle nun ψ so, dass das folgende Diagramm kommutiert.

$$\begin{array}{ccc}
 K & \xrightarrow[\varphi]{\cong} & K' \\
 \cap \downarrow \cdots & & \downarrow \cdots \cap \\
 K[X] & \xrightarrow[\tilde{\varphi}, X \rightarrow X]{\cong} & K'[X] \\
 \downarrow & & \downarrow \\
 K[X]/(\text{irr}_K(a)) & \xrightarrow[\Phi \text{ aus 2.1.17}]{\cong} & K'[X]/(\text{irr}_{K'}(b)) \\
 \wr \downarrow & \xleftarrow{4.1.10} & \downarrow \wr \\
 K[a] & \xrightarrow[\psi]{\cong} & K'[b] \\
 \parallel \downarrow \cdots & \xleftarrow{4.1.10} & \downarrow \cdots \parallel \\
 K(a) & & K(b)
 \end{array}$$

□

4.2.13 Definition Seien $L|K$ und $L'|K$ Körpererweiterungen. Ein K -Homomorphismus (oder Homomorphismus über K) von L nach L' ist ein Homomorphismus $\varphi : L \rightarrow L'$ mit $\varphi|_K = \text{id}_K$. Ein K -Isomorphismus (oder Isomorphismus über K) ist ein surjektiver (und damit bijektiver, siehe ?? K -Homomorphismus. Man nennt L und L' K -isomorph (oder isomorph über K), in Zeichen $L \equiv_K L'$, wenn es einen K -Isomorphismus $L \rightarrow L'$ gibt.

4.2.14 Proposition Seien $L|K$ und $L'|K$ Körpererweiterungen und $\varphi : L \rightarrow L'$ ein Körperhomomorphismus. Dann ist φ ein K -Homomorphismus genau dann, wenn φ ein K -Vektorraumhomomorphismus ist.

Beweis. Es gilt:

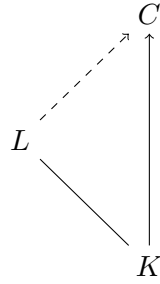
$$\begin{aligned}\varphi|_K = \text{id}_K &\iff \forall a \in K : \varphi(a) = a \\ &\iff \forall a \in K : \forall b \in L : \varphi(a)\varphi(b) = a\varphi(b) \\ &\iff \forall a \in K : \forall b \in L : \varphi(ab) = a\varphi(b)\end{aligned}$$

□

4.2.15 Korollar Seien $L|K$ und $L'|K$ Körpererweiterungen, $a \in L$ und $b \in L'$. Dann sind äquivalent:

- (a) Es gibt einen K -Isomorphismus $\psi : K(a) \rightarrow K(b)$ mit $\psi(a) = b$.
- (b) Entweder sind a und b beide algebraisch über K mit demselben Minimalpolynom oder weder a noch b sind algebraisch über K .

4.2.16 Satz Sei $L|K$ eine Körpererweiterung, C ein algebraisch abgeschlossener Körper und $\varphi : K \rightarrow C$ ein Homomorphismus. Dann gibt es einen Homomorphismus $\psi : L \rightarrow C$ mit $\psi|_K = \varphi$.



Beweis. Auf $M := \{(F, \alpha) \mid F \text{ Zwischenkörper von } L|K, \alpha : F \rightarrow C \text{ Homomorphismus}\}$ definieren wir eine Halbordnung \preceq durch $(F, \alpha) \preceq (F', \alpha') : \iff (F \subseteq F' \text{ \& } \alpha'|_F = \alpha)$. Sei K eine Kette in M . Ist $K = \emptyset$, so ist (K, φ) eine obere Schranke von K in (M, \preceq) . Ist $K \neq \emptyset$, so sieht man leicht, dass (G, β) , definiert durch $G := \bigcup \{F \mid \exists \alpha : (F, \alpha) \in K\}$ und $\beta : G \rightarrow C, a \mapsto \alpha(a)$ für $(F, \alpha) \in K$ mit $a \in F$, eine obere Schranke (G, β) von K in (M, \preceq) definiert.

Insgesamt besitzt also in (M, \preceq) jede Kette eine obere Schranke. Nach dem Lemma von Zorn besitzt (M, \preceq) ein maximales Element (H, γ) . Es genügt, $H = L$ zu zeigen. Sei hierzu $a \in L$. Zu zeigen, dass $a \in H$. Bezeichne $\tilde{\gamma} : H[X] \rightarrow (\gamma(H))[X]$ den Homomorphismus mit $\tilde{\gamma}|_H = \gamma$ und $\tilde{\gamma}(X) = X$. Da $\tilde{\gamma}$ ein Isomorphismus ist, ist mit $p := \text{irr}_H(a)$ auch $q := \tilde{\gamma}(\text{irr}_K(a)) \in (\gamma(H))[X]$ irreduzibel und normiert. Da L algebraisch abgeschlossen

ist, können wir $b \in C$ mit $q(b) = 0$ wählen. Nach 4.2.12 gibt es also einen Homomorphismus $\delta : H(a) \rightarrow C$ mit $\delta|_H = \gamma$ und $\delta(a) = b$. Insbesondere $(H(a), \delta) \in M$ und $(H, \gamma) \preceq (H(a), \delta)$. Aus der Maximalität von (H, γ) folgt $(H, \gamma) = (H(a), \delta)$, insbesondere $H = H(a)$, das heißt $a \in H$, wie gewünscht. \square

4.2.17 Korollar Seien $L|K$ und $C|K$ Körpererweiterungen. Sei $L|K$ algebraisch und C algebraisch abgeschlossen. Dann gibt es einen K -Homomorphismus $\varphi : L \rightarrow C$, das heißt, L ist K -isomorph zu einem Zwischenkörper von $L|K$.

4.2.18 Satz [Ernst Steinitz] Je zwei algebraische Abschlüsse eines Körper K sind zueinander K -isomorph.

Beweis. Seien L und L' algebraische Abschlüsse von K . Dann ist L K -isomorph zu einem Zwischenkörper F von $L'|K$ nach 4.2.17. Mit L ist auch F algebraisch abgeschlossen. Da $L'|F$ algebraisch ist, folgt also aus ??, dass $L' = F$. \square

4.2.19 Sprechweise und Notation Sei K ein Körper. Da nach 4.2.10 der algebraische Abschluss von K existiert und er nach 4.2.18 bis auf K -Isomorphie eindeutig ist, spricht man auch von *dem* algebraischen Abschluss \overline{K} von K . Die algebraischen Overkörper von K sind bis auf K -Isomorphie nach 4.2.17 genau die Zwischenkörper von $\overline{K}|K$.

§ 4.3 Zerfällungskörper

4.3.1 Sprechweise Sei K ein kommutativer Ring mit $0 \neq 1$, zum Beispiel ein Körper. Man sagt dann oft „über K “, statt „in $K[X]$ “. Beispiele: „Sei f ein Polynom über K “, statt: „Sei $f \in K[X]$.“ – „ f zerfällt über K “, statt: „ f zerfällt in $K[X]$.“ – „ f ist irreduzibel über K “, statt: „ f ist irreduzibel in $K[X]$.“

4.3.2 Definition Sei $L|K$ eine Körpererweiterung und $A \subseteq K[X] \setminus \{0\}$. Dann heißt L ein Zerfällungskörper von A über K , wenn jedes Polynom aus A über L zerfällt und $L = K(\{a \in L \mid \exists f \in A : f(a) = 0\})$.⁷

⁷Korrektur: Konnte Klammerung hier nicht richtig lesen.

4.3.3 Bemerkung Ist $L|K$ eine Körpererweiterung und $E \subseteq \overline{K}^L$, so:

$$\begin{aligned} K(E) &\stackrel{2.3.11}{=} \bigcup_{2.2.2} \{K(a_1, \dots, a_n) \mid n \in \mathbb{N}_0, a_i \in E\} \\ &\stackrel{4.1.14}{=} \bigcup \{K[a_1, \dots, a_n] \mid n \in \mathbb{N}_0, a_i \in E\} \\ &= K[E] \end{aligned}$$

Insbesondere kann man in 4.3.2 Ring-, statt Körperadjunktion verwenden.

4.3.4 Definition und Proposition Sei $L|K$ eine Körpererweiterung und $f \in K[X] \setminus \{0\}$. Dann heißt L ein Zerfällungskörper von f über K , falls L ein Zerfällungskörper von $\{f\}$ über K ist. Genau dann ist also L ein Zerfällungskörper von f über K , wenn es $c \in K^\times$, $n \in \mathbb{N}_0$ und a_1, \dots, a_n gibt, mit $f = c \prod_{i=1}^n (X - a_i)$ und $L = K(a_1, \dots, a_n)$ (oder $L = K[a_1, \dots, a_n]$).

4.3.5 Beispiel

- (a) \mathbb{C} ist ein Zerfällungskörper von $X^2 + 1$ über \mathbb{R} .
- (b) $\mathbb{Q}(\sqrt{2})$ ist ein Zerfällungskörper von $X^2 - 2$ über \mathbb{Q} .
- (c) $\mathbb{Q}(e^{\frac{2\pi i}{6}})$ ist ein Zerfällungskörper von $X^6 - 1$ über \mathbb{Q} .
- (d) $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ ist ein Zerfällungskörper von $X^3 - 2$, denn

$$X^3 - 2 = \left(X - \sqrt[3]{2}\right) \left(X - \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}\right) \left(X - \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}\right)$$

$$\text{und } \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}, \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}\right) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right).$$

4.3.6 Bemerkung Sei $L|K$ eine Körpererweiterung und $A \subseteq K[X] \setminus \{0\}$.

- (a) Jeder Zerfällungskörper L von A über K ist offensichtlich algebraisch über K , denn er entsteht aus K durch Adjunktion von über K algebraischen Elementen und ist damit nach 4.1.19 in \overline{K}^L enthalten und damit gleich \overline{K}^L . Ist zusätzlich A endlich, ist nach 4.1.16 $L|K$ sogar endlich.
- (b) Zerfällt jedes Polynom aus A über L , so gibt es offensichtlich genau einen Zwischenkörper F von $L|K$, der ein Zerfällungskörper von A über K ist, nämlich $F = K(\{a \in L \mid \exists f \in A : f(a) = 0\})$.

4.3.7 Satz Sei K ein Körper und $A \subseteq K[X] \setminus \{0\}$. Dann gibt es bis auf K -Isomorphie genau einen Zerfällungskörper von A über K .

Beweis.

Existenz: Nehme $K(\{a \in \overline{K} \mid \exists f \in A : f(a) = 0\})$ im nach 4.2.10 existierenden algebraischen Abschluss \overline{K} von K .

Eindeutigkeit: Seien L und L' Zerfällungskörper von A über K . Zu zeigen ist $L \cong_K L'$. Da L und L' über K algebraisch sind, sind \overline{L} und \overline{L}' nach 4.1.17 algebraische Abschlüsse von K und daher nach 4.2.18 K -isomorph. Wähle einen K -Isomorphismus $\varphi : \overline{L} \rightarrow \overline{L}'$. Dann sind $\varphi(L)$ und L' beides Zwischenkörper $\overline{L}'|K$, die ein Zerfällungskörper von A über K sind. Nach ?? gilt $\varphi(L) = L'$, weshalb φ einen K -Isomorphismus $L \rightarrow L'$ induziert. \square

4.3.8 Definition Sei $L|K$ eine Körpererweiterung. Ein Automorphismus von $L|K$ (oder ein K -Automorphismus von L über K) ist ein K -Isomorphismus von L nach L [→ 4.2.13].

Es bezeichne $\text{Aut}(L|K) := \{\varphi \mid \varphi \text{ ist Automorphismus von } L|K\}$ die Gruppe aller Automorphismen von $L|K$.

4.3.9 Definition Sei K ein Körper. Betrachte die natürliche Wirkung von $\text{Aut}(\overline{K}|K)$ auf \overline{K} und die dazugehörige Äquivalenzrelation \sim_K auf \overline{K} , definiert durch $a \sim_K b : \iff \exists \varphi \in \text{Aut}(\overline{K}|K) : \varphi(a) = b$ ($a, b \in \overline{K}$). Für $a, b \in \overline{K}$ nennt man a und b über K zueinander konjugiert, wenn $a \sim_K b$.

4.3.10 Proposition Sei $L|K$ eine algebraische Körpererweiterung und $\varphi : L \rightarrow L$ ein K -Homomorphismus. Dann ist $\varphi \in \text{Aut}(L|K)$.

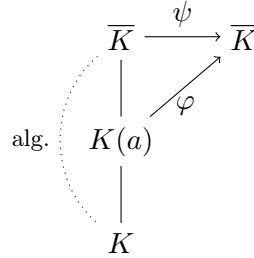
Beweis. Nach ?? ist φ injektiv. Also ist noch zu zeigen, dass φ surjektiv ist. Sei $b \in L$ und zeige also $\exists a \in L : \varphi(a) = b$. Wähle $p \in K[X] \setminus \{0\}$ mit $p(b) = 0$. Für die endliche Menge $A := \{a \in L \mid p(a) = 0\}$ gilt dann $\varphi(A) \subseteq A$ und daher $\varphi(A) = A$. Wegen $b \in A$ gibt es also $a \in A \subseteq L$ mit $\varphi(a) = b$.

4.3.11 Proposition Sei K ein Körper und $a, b \in \overline{K}$. Dann gilt $a \sim_K b \iff \text{irr}_K(a) = \text{irr}_K(b)$.

Beweis. „ \implies “: Klar

⁸Korrektur: Kann ich nicht lesen.

„ \Leftarrow “: Nach 4.2.15 gibt es einen K -Homomorphismus $\varphi : K(a) \rightarrow \overline{K}$ mit $\varphi(a) = b$, den wir nach 4.2.16 fortsetzen zu einem K -Homomorphismus $\psi : \overline{K} \rightarrow \overline{K}$. Nach 4.3.10 gilt $\psi \in \text{Aut}(\overline{L}|K)$.



□

4.3.12 Definition Eine Körpererweiterung $L|K$ heißt normal, wenn L ein Zerfällungskörper einer Menge $A \subseteq K[X] \setminus \{0\}$ ⁹ über K ist.

4.3.13 Beispiel Jede Körpererweiterung $L|K$ vom Grad 2 ist normal. Wählt man nämlich $a \in L \setminus K$, so ist $L = K(a)$ und L der Zerfällungskörper von $\text{irr}_K(a)$ über K , denn $\deg \text{irr}_K(a) = 2$.

4.3.14 Satz Sei $L|K$ eine algebraische Körpererweiterung. Dann sind äquivalent:

- (a) $L|K$ ist normal.
- (b) Jedes irreduzible Polynom aus $K[X]$ mit einer Nullstelle in L zerfällt über L .
- (c) L ist Vereinigung von Äquivalenzklassen von \sim_K .
- (d) Für jeden K -Homomorphismus $\varphi : L \rightarrow \overline{L}$ gilt $\varphi(L) = L$.
- (e) $\forall \varphi \in \text{Aut}(\overline{L}|K) : \varphi(L) = L$

Beweis.

(a) \implies (d) Sei L Zerfällungskörper von $A \subseteq K[X] \setminus \{0\}$ und $\varphi : L \rightarrow \overline{L}$ ein K -Homomorphismus. Mit L ist auch der dazu K -isomorphe Körper $\varphi(L)$ ein Zerfällungskörper von A über K . Da beide Zwischenkörper von $\overline{L}|K$ sind, folgt aber dann $\varphi(L) = L$ nach ??.

⁹Korrektur: Konnte ich nicht lesen.

(d) \implies (e) Klar.

(e) \implies (c) Gelte (e). Wir zeigen $L = \bigcup \left\{ \tilde{a}^K \mid a \in \bar{L}, \tilde{a}^K \cap L \neq \emptyset \right\}$.

„ \subseteq “: Sei $a \in L$. Dann ist $a \in \tilde{a}^K \cap L$, also $\tilde{a}^K \cap L \neq \emptyset$ und $a \in \tilde{a}^K$.

„ \supseteq “: Sei $a \in \bar{L}$ mit $\tilde{a}^K \cap L \neq \emptyset$. Zu zeigen ist $\tilde{a}^K \subseteq L$. Sei ohne Einschränkung $a \in L$. Sei $b \in \tilde{a}^K$. Zu zeigen ist $b \in L$. Wegen $a \sim_K b$ gibt es $\varphi \in \text{Aut}(\bar{L}|K)$ mit $b = \varphi(a) \in \varphi(L) = L$.

(c) \implies (b) Gelte (c) und sei $p \in K[X]$ irreduzibel mit einer Nullstelle in L . Da nach 4.3.11 alle Nullstellen von p in \bar{L} zueinander konjugiert sind, liegen diese alle in L wegen (c).

(b) \implies (a) Gelte (b) und setze $A := \{p \in K[X] \mid p \text{ irreduzibel, } \exists a \in L : p(a) = 0\}$. Nach (b) zerfällt jedoch jedes Polynom aus A über L . Da $L|K$ algebraisch ist, gilt $E := \{a \in L \mid \exists p \in A : p(a) = 0\} = L$, denn jedes Element von L ist Nullstelle eines Minimalpolynoms über K und daher natürlich $L = k(E)$.¹⁰

4.3.15 Beispiel

- (a) Nach dem Kriterium von Eisenstein ?? sind $X^4 - 2$ und $X^2 - 2$ irreduzibel in $\mathbb{Q}[X]$ (und in $\mathbb{Z}[X]$). Daraus folgt $\text{irr}_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$ und $\text{irr}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, also $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Somit sind $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ beides Körpererweiterungen vom Grad 2 und daher normal nach 4.3.13.

Aber $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ ist nicht normal, da das irreduzible Polynom $X^4 - 2 \in \mathbb{Q}[X]$ über $\mathbb{Q}(\sqrt[4]{2})$ nicht zerfällt, obwohl es eine Nullstelle hat. In der Tat: $i\sqrt[4]{2}$ ist eine Nullstelle dieses Polynoms, welche nicht in $\mathbb{Q}(\sqrt[4]{2})$, ja nicht einmal in \mathbb{R} , liegt.

- (b) Für jeden Körper K ist \bar{K} über K normal.

¹⁰Korrektur: Kann ich nicht lesen / ist mir nicht klar.

Literaturverzeichnis

- [1] BOSCH, Siegfried: *Algebra* -. 5. überarb. Aufl. Berlin, Heidelberg : Springer, 2004. – ISBN 978-3-540-40388-3
- [2] JACOBSON, Nathan: *Basic Algebra I - Second Edition*. Second Edition. Courier Corporation, 2012. – ISBN 978-0-486-13522-9
- [3] JANTZEN, Jens C. ; SCHWERMER, Joachim: *Algebra* -. 2. Aufl. Berlin Heidelberg New York : Springer-Verlag, 2014. – ISBN 978-3-642-40533-4
- [4] LORENZ, Falko ; LEMMERMEYER, Franz: *Algebra 1 - Körper und Galois-theorie*. 4. Aufl. 2007. Heidelberg : Spektrum Akademischer Verlag, 2007. – ISBN 978-3-827-41609-4

Index

- algebraisch
 - e Körpererweiterung, 20
 - es Element, 20
 - unabhängig, 12
- algebraisch abgeschlossen, 24
- algebraischer Abschluss, 26, 29
 - relativer, 23
- Automorphismus
 - über Körpererweiterungen, 31
 - Vektorraum-, 6
- Direktes Produkt
 - von Ringen, 9
- Einbettung
 - Ring-, 9
- Endomorphismus
 - Vektorraum-, 8
- Epimorphismus
 - Ring-, 9
 - kanonischer, 10
- Faktoring, 9
- Fakultät, 6
- General Linear Group, 6
- Grad
 - einer Körpererweiterung, 19
- Gradformel, 20
- Gruppe, 5
 - nmultiplikation, 5
 - nverknüpfung, 5
 - abelsche, 5
 - alternierende, 8
 - kommutative, 5
 - symmetrische, 6
 - Unter-, 7
- Hauptideal, 16
- Hauptidealring, 16
- Homomorphiesatz
 - für Ringe, 10
- Homomorphismus
 - über Körpererweiterungen, 27
 - Körper-, 15
 - Ring-, 8
- Ideal, 9
 - echtes, 17
 - erzeugtes, 16
 - maximales, 17
- irreduzibel, 16
- isomorph
 - über Körpererweiterung, 27
- Isomorphiesatz
 - für Ringe, 11
- Isomorphismus
 - über Körpererweiterungen, 27
 - Ring-, 9
- Körper
 - der (reellen) algebraischen Zahlen, 23
 - der rationalen Funktionen, 15
 - in Unbestimmten, 16
 - Oberkörper, 14
 - Unterkörper, 14
 - kleinster, 14
 - von rationalen Funktionen, 15

Index

- Zwischenkörper, 20
- Körpererweiterung, 14
 - endlich erzeugte, 22
 - endliche, 19
 - Grad, 19
 - normale, 32
 - unendliche, 19
- Kongruenzrelation, 9
- konjugiert, 31
- Lokalisierung, 16
- Minimalpolynom, 20
- Monomorphismus
 - Ring-, 9
- Nenner, 14
- Ordnung, 6
- Polynom
 - Minimal-, 20
- Polynomring, 12
- prim, 17
- Primfaktorzerlegung, 17
- Primideal, 17
- Produkt
 - direktes
 - von Ringen, 9
- Quotientenring, 9
 - totaler, 14
- Restklasse, 10
- Restklassenring, 9
- Ring
 - der Brüche, 14
 - Faktor-, 9
 - faktorieller, 17
 - Polynom-, 12
 - Quotienten-, 9
 - Restklassen-, 9
 - Unter-, 8
- Steinitz, Ernst, 29
- supp*, 17
- Träger, 7, 17
- unabhängig
 - algebraisch, 12
- Unterring, 8
- Zähler, 14
- Zerfällungskörper, 29, 30