Universität Konstanz

Skriptum zur Vorlesung

Einführung in die Algebra

Private Mitschrift

gelesen von: Prof. Dr. Markus Schweighofer

Wintersemester 2014/15
Stand vom 1. Februar 2015

Inhaltsverzeichnis

§ 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 $\cdot : G \times G \to G$ eine meist infix (und manchmal gar nicht) notierte Abbildung mit folgenden Eigenschaften ist:

(A) $\forall a, b, c \in G : a(bc) = (ab)c$ *„assoziativ“*

(N) $\exists e \in G \; \forall a \in G : ae = a = ea$ *„neutrales Element“*

(I) $\forall a \in G \; \exists g \in G : ab = 1 = ba$ *„inverse Elemente“*

„$\cdot$“ heißt Gruppenmultiplikation oder Gruppenverknüpfung. Gilt zusätzlich

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

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

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

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

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

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

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

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

(d) Sei G eine Gruppe, $n \in \mathbb{N}_0$ und $a_1, ..., a_n \in G$. Dann definiert man $\prod_{i=1}^{n} a_i := a_1 \cdot ... \cdot a_n$ als 1 für $n = 0$ und indem man $a_1 \cdot ... \cdot a_n$ 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 $S_M := \{f \mid f : M \to M \text{ bijektiv}\}$ 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 $S_n := S_{\{1,...,n\}}$ 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 $\mathrm{Aut}(V) := \{f \mid f : V \to V \text{ linear und bijektiv}\}$ mit der Hintereinanderschaltung als Multiplikation eine Gruppe.

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

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

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

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

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

Beweis:

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

(b) Aus $aa^{-1} \overset{(I)}{=} 1$ folgt mit (a) $\left(a^{-1}\right)^{-1} = a$.

(c) Aus $(ab)(b^{-1}a^{-1}) \overset{(A)}{=} a(b(b^{-1}a^{-1})) \overset{(A)}{=} a((bb^{-1})a^{-1}) \overset{(I)}{=} a(1a^{-1}) \overset{(N)}{=} aa^{-1} \overset{(I)}{=} 1$ folgt mit (a) $(ab)^{-1} = b^{-1}a^{-1}$. □

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 $H \subseteq G$, $1_S \in H$, $\forall a, b \in H : a \cdot_S b \in H$ und $\forall a \in H : a^{-1} \in H$.

In diesem Fall gibt es genau eine Abbildung $\cdot_H : H \times H \to H$ 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. □

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 $A_n := \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\}$ eine Untergruppe von S_n, die man

alternierende Gruppe nennt. [→ LA § 9.1]

`Hier fehlt noch etwas ...`

1.3.4 Definition Sei G eine Gruppe. Zu jedem $H \leq G$ definieren wir Äquivalenzrelationen ${}_H\sim$ und $\sim_H$ auf G durch

$$a\ {}_H\sim b \iff ab^{-1} \in H \qquad (a, b \in G)$$
$$a \sim_H b \iff a^{-1}b \in H \qquad (a, b \in G)$$

Die Äquivalenzklassen

$${}^H\widetilde{a} = \{b \in G \mid a\ {}_H\sim b\} = \{b \in G \mid ab^{-1} \in H\} = \{ha \mid h\ inH\} =: Ha$$
$$\widetilde{a}^H = \{b \in G \mid a \sim_H b\} = \{b \in G \mid a^{-1}b \in H\} = \{ah \mid h \in H\} =: aH$$

nennt man Rechts- bzw. Linksnebenklassen von H nach a ($a \in G$).

1.3.5 Bemerkung Ist $\equiv$ eine Kongruenzrelation auf G, so gilt nach **??** für $H := \overline{1}$ die Gleichheit $(\equiv) = ({}_H\sim) = (\sim_H)$.

1.3.6 Definition Sei G eine Gruppe. Eine Untergruppe N von G heißt Normalteiler von G, in Zeichen $N \triangleleft G$, wenn ${}_H\sim = \sim_H$.

1.3.7 Proposition Sei G eine Gruppe und $H \leq G$. Dann sind äquivalent:

a) $H \triangleleft G$

b) ${}_H\sim = \sim_H$

c) $\forall a \in G : Ha = aH$

d) $\forall a \in G : aHa^{-1} := \{aha^{-1} \mid h \in H\} = H$

e) $\forall a \in G : aHa^{-1} \subseteq H$

f) ${}_H\sim$ ist eine Kongruenzrelation

g) $\sim_H$ ist eine Kongruenzrelation

h) H ist der Kern eines Gruppenhomomorphismus

Beweis. Übung. □

1.3.8 Notation und Proposition Sei G eine Gruppe und $N \triangleleft G$. Dann schreiben wir:

$$(\equiv_N) := ({}_N\sim) = (\sim_N)$$
$$G/N := G/\equiv_N = \{Na \mid a \in G\} = \{aN \mid a \in G\}$$

Weiter bezeichnen wir die Kongruenzklasse $\overline{a} = Na = aN$ von $a \in G$ auch als Nebenklasse von N nach a.

1.3.9 Satz Sei G eine Gruppe. Die Zuordnungen

$$\equiv \mapsto \overline{1}$$
$$\equiv_N \leftarrow\!\shortmid N$$

vermitteln eine Bijektion zwischen der Menge der Kongruenzrelationen auf G und der Menge der Normalteiler von G.

Beweis. Übung. □

1.3.10 Definition und Proposition Sei G eine Gruppe. Ein Isomorphismus $G \to G$ heißt Automorphismus von G. Bezüglich der Hintereinanderschaltung bilden die Automorphismen von G eine Gruppe, die sogenannte Automorphismengruppe $\mathrm{Aut}(G)$ von G. Die Konjugationen $c_a : G \to G, b \mapsto aba^{-1}$ mit $a \in G$ sind offensichtlich Automorphismen von G, die sogenannten inneren Automorphismen von G. Sie bilden den Normalteiler $\mathrm{Inn}(G) := \{c_a \mid a \in G\}$ von $\mathrm{Aut}(G)$. Eine Untergruppe $N \leq G$ ist genau dann ein Normalteiler von G, wenn $f(N) = N$ für alle $f \in \mathrm{Inn}(G)$ gilt. Man nennt $N \leq G$ eine charakteristische Untergruppe von G, wenn $f(N) = N$ sogar für alle $f \in \mathrm{Aut}(G)$ gilt.

Beweis. Zu zeigen:

a) $\forall a \in G : c_a \in \mathrm{Aut}(G)$

b) $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$

Zu (a): Übung.

Zu (b): Sei $a \in G$ und $f \in \mathrm{Aut}(G)$. Zu zeigen: $fc_af^{-1} \in \mathrm{Inn}(G)$. Ist $b \in G$, so $(fc_af^{-1})(b) = f\left(af^{-1}(b)a^{-1}\right) = f(a)bf(a)^{-1}$. Daher $fc_af^{-1} = c_{f(a)} \in \mathrm{Inn}(G)$. □

1.3.11 Beispiel

a) Nicht jeder Normalteiler ist eine charakteristische Untergruppe. Ist zum Beispiel $G \neq \{1\}$ eine Gruppe, so ist $G \times \{1\} \triangleleft G \times G$, aber $G \times \{1\}$ ist keine charakteristische Untergruppe von G, denn $G \times G \to G \times G, (g, h) \mapsto (h, g)$ ist ein Automorphismus von $G \times G$.

b) Sei $n \in \mathbb{N}$, $n \geq 3$. Dann gilt $C_n \triangleleft D_n$. In der Tat: Sei $A \in D_n$ und $B \in C_n$. Zu zeigen: $ABA^{-1} \in C_n$. Dies ist klar, falls $A \in C_n$, denn C_n ist abelsch. Sei nun $A \in D_n \backslash C_n$. Dann ändert die Spiegelung den Drehsinn und somit $ABA^{-1} = B^{-1} \in C_n$.

c) Als Kern des Gruppenhomomorphismus sgn : $S_n \to \{-1, 1\}$ ist A_n ein Normalteiler von S_n.

d) Sei R ein kommutativer Ring als Kern von det : $\mathrm{GL}_n(R_n) \to R^\times$ ist $\mathrm{SL}_n(R) \triangleleft \mathrm{GL}_n(R)$.

e) Ebenso $\mathrm{SO}_n \triangleleft \mathrm{O}_n$.

1.3.12 Bemerkung Wird eine Untergruppe einer Gruppe in einer Weise definiert, die offensichtlich nur auf die Gruppenstruktur Bezug nimmt, so ist nach **??** klar, dass diese Untergruppe charakteristisch und insbesondere ein Normalteiler ist.

1.3.13 Definition Sei G eine Gruppe. Dann heißt

$$Z(G) := \{a \in G \mid \forall b \in G : ab = ba\} \triangleleft G$$

das Zentrum von G.

1.3.14 Bemerkung Mit **??** ist klar, dass $Z(G)$ sogar eine charakteristische Untergruppe der Gruppe G ist. Insbesondere ist $Z(G) \triangleleft N$. Letzteres folgt auch mit **??**, denn $Z(G)$ ist der Kern des Gruppenhomomorphismus $G \to \mathrm{Aut}(G)$, $a \mapsto c_a$. (Das Bild von $Z(G)$ ist übrigens $\mathrm{Inn}(G)$.)

1.3.15 Homomorphiesatz für Gruppen [→ LA § 2.3] Seien G und H Gruppen, $N \triangleleft G$ und $f : G \to H$ ein Homomorphismus mit $N \subseteq \ker f$. Dann gibt es genau eine Abbildung $\overline{f} : G/N \to H$ mit $\overline{f}\left(\overline{a}^N\right) = f(a)$ für alle $a \in G$. Die Abbildung $\overline{f}$ ist ein Homomorphismus. Weiter gilt:

$$\begin{aligned} \overline{f} \text{ injektiv} &\iff N = \ker f \\ \overline{f} \text{ surjektiv} &\iff H = \mathrm{im}\, f \end{aligned}$$

Beweis. Eindeutigkeit von $\overline{f}$ ist klar.

Zur Existenz von $\overline{f}$ (Wohldefiniertheit): Seien $a, b \in G$ mit $\overline{a}^N = \overline{b}^N$, d. h. $a \equiv_N b$. Zu zeigen: $f(a) = f(b)$. Wegen $ab^{-1} \in N \subseteq \ker f$ folgt $f(ab^{-1}) = 1$, also $f(a)f\left(b^{-1}\right) = f(a)f(b)^{-1} = 1$. Es folgt $f(a) = f(b)$.

$\overline{f}$ ist ein Homomorphismus: Seien $a, b \in G$. Zu zeigen: $\overline{f}\left(\overline{a}^N\overline{b}^N\right) = \overline{f}\left(\overline{a}^N\right)\overline{f}\left(\overline{b}^N\right)$. Es gilt $\overline{f}\left(\overline{a}^N\overline{b}^N\right) \overset{??}{=} \overline{f}\left(\overline{ab}^N\right) = f(ab) = f(a)f(b) = \overline{f}\left(\overline{a}^N\right)\overline{f}\left(\overline{b}^N\right)$.

$$\begin{aligned}
\overline{f} \text{ injektiv} &\iff \ker\overline{f} = \{1\} \iff \{\overline{a}^N \mid f(a) = 1\} = \{1\} \iff \forall a \in \ker f : \overline{a}^N = \overline{1}^N \\
&\iff \ker f \subseteq N \iff \ker f = N \\
\overline{f} \text{ surjektiv} &\iff H = \operatorname{im}\overline{f} \iff H = \operatorname{im} f
\end{aligned}$$

□

`Hier fehlt noch etwas ...`

2.1.4 Beispiel

(a) Für jeden Vektorraum V ist die Menge $\operatorname{End}(V) = \{f \mid f : V \to V \text{ linear}\}$ der Endomorphismen von V mit der punktweisen Addition und der Hintereinanderschaltung als Multiplikation ein Ring mit Einheitengruppe $\operatorname{End}(V)^\times = \operatorname{Aut}(V)$. [→ LA § 7.1]

(b) Ist R ein kommutativer Ring, so ist $R^{n\times n}$ ein Ring mit $(R^{n\times n})^\times = \mathrm{GL}_n(R)$.

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 $\blacktriangleleft_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ obere Dreiecksmatrix}\}$, $\blacktriangleright_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ untere Dreiecksmatrix}\}$ und

$\mathbb{L}_R^{n\times n} \cap \mathbb{T}_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ Diagonalmatrix}\}$ Unterringe von $R^{n\times n}$ mit Einheitengruppen $(\mathbb{T}_R^{n\times n})^\times = \mathbb{T}_n(R)$, $(\mathbb{L}_R^{n\times n})^\times = \mathbb{L}_n(R)$ und $\left(\mathbb{L}_R^{n\times n} \cap \mathbb{T}_R^{n\times n}\right)^\times = \mathbb{T}_n(R) \cap \mathbb{L}_n(R)$.

(b) $\{0\}$ ist kein Unterring von $\mathbb{Z}$, denn $1 \notin \{0\}$.

2.1.8 Definition Seien A und B Ringe. Dann heißt $f : A \to B$ 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 $f : A \to B$ ein Ringhomomorphismus, so ist $\operatorname{im} f$ 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. $\lightning$)

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 [→ § **??**], [→ LA § 3.3] Sei R ein Ring. Eine *Kongruenzrelation* auf R ist eine Kongruenzrelation $\equiv$ auf der additiven Gruppe von R [→ **??**], 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 $\overline{a}\,\overline{b} = \overline{ab}$ $(a, b \in A)$ zu einem Ring (*„Quotientenring“ „Faktorring“*, *„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 [→ 1.3.9] [→ LA § 3.3] Sei R ein Ring. Die Zuordnungen

$$\equiv \mapsto \overline{0}$$
$$\equiv_I \hookleftarrow I$$

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 1.3.9, dass sie auch invers zueinander sind. Also zu zeigen:

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

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

Zu (a). Sei $\equiv$ eine Kongruenzrelation auf R. Aus 1.3.9 wissen wir schon, dass $\overline{0}$ eine Untergruppe von R ist. Noch zu zeigen: $\forall a \in A : \forall b \in \overline{0} : ab \in \overline{0}$. Sei also $a \in R$ und $b \in \overline{0}$. Dann $ab \overset{b\equiv 0}{\equiv} a0 \overset{2.1.2(e)}{\equiv} 0$, also $ab \in \overline{0}$ und $ba \equiv 0a \equiv 0$, also $ba \in \overline{0}$.

Zu (b). Sei I eine Ideal von R. Aus 1.3.9 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 $ab - a'b' = a\underbrace{(b - b')}_{\in I} + b'\underbrace{(a - a')}_{\in I} \in I$, also $ab \equiv_I a'b'$. □

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 $\overline{a}^I = a + I$ 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 $R \to R/I, a \mapsto \overline{a}^I$ nach Definition 2.1.11 ein Ringhomomorphismus, genannt *kanonischer Epimorphismus*.

(b) Sei $f : A \to B$ ein Ringhomomorphismus. Dann ist $\ker f$ ein Ideal von A, aber $\operatorname{im} f$ 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 $\varphi : A \to B$ ein Homomorphismus mit $I \subseteq ker\varphi$. Dann gibt es genau eine Abbildung $\overline{\varphi} : A/I \to B$ mit $\overline{\varphi}(\overline{a}^I) = \varphi(a)$ für alle $a \in A$. Diese Abbildung $\overline{\varphi}$ ist ein Homomorphismus. Weiter gilt $\overline{\varphi}$ injektiv $\iff I = \ker\varphi$ und $\overline{\varphi}$ surjektiv $\iff B = \operatorname{im}\varphi$.

Beweis. Mit 1.3.15 ist nur noch $\overline{\varphi}(1) = 1$ und $\overline{\varphi}(\overline{a}^I\overline{b}^I) = \overline{\varphi}(\overline{a}^I)\overline{\varphi}(\overline{b}^I)$ f.a. $a, b \in A$ zz zeigen.

Dies ist klar:

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

□

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

Beweis. Direkt aus 2.1.16. □

---

§ 2.2 Polynomringe [→ LA § 3.2]

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

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

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

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

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

(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 angegeben 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. □

2.2.3 Definition Sei A ein Unterring des kommutativen Ringes B.

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

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

Es heißt B *Polynomring* über A in $b_1, ..., b_n$, wenn $B = A[b_1, ..., b_n]$ und $b_1, ..., b_n$ 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 $b_1, ..., b_n \in E$ 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 $\alpha : E \to \mathbb{N}_0$ mit endlichem Träger $supp(\alpha) = \{e \in E \mid \alpha(e) \neq 0\}$. Mache die abelsche Gruppe $A^{\mathbb{N}_0^{(E)}}$ zu einem kommutativen Ring mit der „Faltung“ $*$ als Multiplikation, welche gegeben ist durch

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

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

$$1 : \mathbb{N}_0^{(E)} \to A$$
$$\alpha \mapsto \begin{cases} 1, & \alpha = 0 \\ 0, & sonst \end{cases}$$

und rechnet

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

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

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

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 $\widetilde{(a, s)} = \widetilde{(s, 1)}^{-1}\widetilde{(a, 1)} \in \tilde{S}^{-1}\tilde{A}$. □

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

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 $\varphi : A \to C$ ein Homomorphismus. Genau dann gibt es einen Homomorphismus $\psi : S^{-1}A \to C$ 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. □

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 $\psi : B \to C$ mit $\psi|_A = \mathrm{id}_A$.

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

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 $\mathrm{qf}(A) := Q(A) = (A \setminus \{0\})^{-1}A$ 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 $b_1, ..., b_n \in L$, so ist $K(b1, ..., b_n) := (K[b_1, ..., b_n] \setminus \{0\})^{-1} K[b_1, ..., b_n] = \mathrm{qf}(K[b_1, ..., b_n]) \subseteq L$ der kleinste Unterkörper F von L mit $K \cup \{b_1, ..., b_n\} \subseteq F$.

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

Beweis. Trivial. □

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

(a) Sei $n \in \mathbb{N}_0$ und $b_1, ..., b_n \in L$. Es heißt L ein Körper der rationalen Funktionen über K in $b_1, ..., b_n$, wenn $L = K[b_1, ..., b_n]$ und $b_1, ..., b_n$ algebraisch unabhängig über $K1$ 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 seiden $\varphi, \psi : L \to R$ Homomorphismen mit $\varphi|_{K \cup E} = \psi|_{K \cup E}$. Dann $\varphi = \psi$.

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

2.3.14 Definition und Proposition Seien K und F Körper.

(a) K besitzt nur die trivialen Ideale K und $\{0\}$.

(b) Ist $\varphi : K \to F$ 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 $\varphi : K \xrightarrow{\cong} \mathrm{im}\, \varphi$ ein Isomorphismus. Insbesondere ist das Bild von φ nicht nur ein Unterring, sondern sogar ein Unterkörper von F. Beachte auch, dass gelten muss $\varphi\left(-\frac{1}{a}\right) = \frac{1}{\varphi(a)}$ für alle $a \in K^\times$.[3]

[2] An Korrektor: War mir hier bzgl. der Klammern und der Namen (Index!) nicht ganz sicher.
[3] An Korrektor: Gehört da wirklich ein Minus hin?

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

Beweis. Zur Existenz: Nach **??** gibt es einen Isomorphismus $\varphi : K[E] \to K[F]$ mit $\varphi|_K = \mathrm{id}_K$ 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 $\psi : K(E) \to K(F)$ 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 $K \cup F \subseteq \mathrm{im}\,\varphi \subseteq \mathrm{im}\,\psi$, weswegen ψ surjektiv ist.

Die Eindeutigkeit folgt aus 2.3.13.

2.3.16 Notation und Sprechweise (vgl. **??**) Sei K ein Körper. Schreibt man $K(X_1, ...X_n)$, 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“ $X_1, ..., X_n$.[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 $\overline{S} := \{\overline{s} \mid s \in S\} \subseteq \overline{A} := A/I_S$ multiplikativ und ohne Nullteiler. Man nennt dann den Oberring $\overline{S}^{-1}\overline{A}$ von $\overline{A} = \overline{A/I_S}$ die Lokalisierung von A nach S, in Zeichen $A_S := \overline{S}^{-1}\overline{A}$. Man hat einen Homomorphismus[6] $\iota_S(S) \subseteq A_S^\times$ 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 $\overline{S}^{-1}\overline{A}$ und $\frac{\overline{a}}{\overline{s}}$ $(a \in A, s \in S)$.

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

Beweis. Übung. □

---

[4] An Korrektor: Macht so keinen Sinn.
[5] An Korrektor: Index für „Körper der rationalen Funktionen“ anpassen.
[6] An Korrektor: Wie sieht der aus? Habe ich mir nicht aufgeschrieben.

§ 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 $b_1, ..., b_n \in R$ schreibt man auch $(b_1, ..., b_n) := (b_1, ..., b_n) = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in R\}$. 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

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

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 $\widehat{=}$ auf R ist definiert durch $a \mathrel{\widehat{=}} b :\iff (a|b \ \& \ b|a) \iff (a) = (b)$ $(a, b \in R)$.

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

Für jedes $\alpha \in \mathbb{N}_0^{\mathbb{P}_R}$ setze $\mathbb{P}_R^\alpha := \prod_{p \in \operatorname{supp}(\alpha)} p^{\alpha(p)}$. 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 Korrolar Jedes maximale Ideal eines kommutativen Rings ist ein Primideal.

Beweis. Jeder Körper ist ein Integritätsring. □

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

Beweis. $\psi : A \to B/\mathfrak{q}, a \mapsto \overline{\varphi(a)}^{\mathfrak{q}}$ 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 $A/\ker\psi \cong \operatorname{im}\psi$. 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 $\ker\psi = \{a \in A \mid \psi(a) = 0\} = \left\{a \in A \mid \overline{\psi(a)}^{\mathfrak{q}} = 0\right\} = \{a \in A \mid \varphi(a) \in \mathfrak{q}\} = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

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 $K[X, Y] \to K[Y], p \mapsto p(0, Y)$ 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 $K[X, Y] \to K, p \mapsto (0, 0)$).

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 mir $p \subseteq I$. 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 ...`

---

§ 3.3 Auflösbare Gruppen

3.3.1 Definition Sei G eine Gruppe. Für $a, b \in G$ nennt man $[a, b] := aba^{-1}b^{-1}$ den Kommutator von a und b. Man nennt $G' := \langle \{[a, b] \mid a, b \in G\} \rangle \leq G$ die Kommutatorgruppe von G. Weiter definiert man für jedes $n \in \mathbb{N}_0$ die n-te Kommutatorgruppe $G^{(n)}$ von G rekursiv durch $G^{(0)} := G$ und $G^{(n+1)} := (G^{(n)})'$ für $n \in \mathbb{N}_0$.

3.3.2 Bemerkung Sei G eine Gruppe.

(a) $\forall a, b \in G : ([a, b] = 1 \iff ab = ba)$

(b) $G' = \{[a_1, b_1] \cdots [a_m, b_m] \mid m \in \mathbb{N}_0,\ a_i, b_i \in G\}$

[„$\supseteq$“ klar; „$\subseteq$“ beachte $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ für $a, b \in G$]

(c) G' ist der kleinste Normalteiler N von G mit G/N abelsch.

[G' ist nach 1.3.12 eine charakteristische Untergruppe und daher ein Normalteiler von G; ist $N \triangleleft G$ mit G/N abelsch, so $\overline{[a, b]}^N = \overline{aba}^{-1}\overline{b}^{-1} = \overline{aa^{-1}}^N\overline{bb^{-1}}^N = 1$ und daher $[a, b] \in N$ für alle $a, b \in G$, woraus $G' \subseteq N$ folgt.]

3.3.3 Definition Sei $n \in \mathbb{N}_0$. Eine Permutation der Form

$$(x_1, ..., x_\ell) := \begin{pmatrix} \{1, ..., n\} \to \{1, ..., n\} \\ \begin{array}{ccc} & x_1 & \\ x_\ell & & x_2 \\ \updownarrow & & \downarrow \\ \ddots & & x_3 \\ & x_4 & \end{array} \\ x \mapsto x \text{ für } x \in \{1, ..., n\} \setminus \{x_1, ..., x_\ell\} \end{pmatrix}$$

mit $\ell \in \{2, ..., n\}$ und paarweise verschiedenen $x_1, ..., x_\ell \in \{1, \dots, n\}$ nennt man einen ℓ-Zykel in S_n. Man nennt 2-Zykel auch Transpositionen [→ LA 9.1.3].

3.3.4 Proposition [→ **??**] Sei $n \in \mathbb{N}_0$. Dann

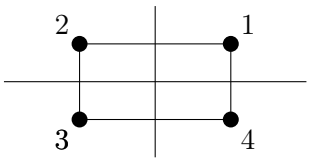
$$A_n = \{\sigma_1 \cdots \sigma_m \mid m \in \mathbb{N}_0,\ \sigma_1, \dots, \sigma_m \text{ 3-Zykel in } S_n\}.$$

Beweis. „$\supseteq$“: Seien $x_1, x_2, x_3 \in \{1, ..., n\}$ paarweise verschieden. Zu zeigen: $(x_1\ x_2\ x_3) \in A_n$. Dies folgt aus $(x_1\ x_2\ x_3) = (x_2\ x_3)(x_1\ x_3)$.

„$\subseteq$“: Sind $x_1, x_2, x_3, x_4 \in \{1, ..., n\}$ paarweise verschieden, so $(x_1\ x_2)(x_3\ x_4) = (x_1\ x_3\ x_2)(x_1\ x_3\ x_4)$. Sind $x_1, x_2, x_3 \in \{1, \dots, n\}$ paarweise verschieden, so $(x_1\ x_2)(x_2\ x_3) = (x_1\ x_2\ x_3)$. Sind $x_1, x_2 \in \{1, \dots, n\}$ mit $x_1 \neq x_2$, so $(x_1\ x_2)(x_1\ x_2) = 1$. □

3.3.5 Proposition Sei $n \in \mathbb{N}_0$. Dann $S_n' = A_n$ und

$$A_n' = \begin{cases} \{1\} & \text{falls } n \leq 3, \\ V_4 := \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V & \text{falls } n = 4, \\ A_n & \text{falls } n \geq 5. \end{cases}$$



[→ **??**]

Beweis.

$\underline{S_n' \subseteq A_n}$: Nach **??** genügt es zu zeigen, dass S_n/A_n abelsch ist. Dies ist klar, da $S_n/A_n \cong C_2$ für $n \geq 2$ **??** und $S_n/A_n \cong C_1$ für $n \in \{0, 1\}$.

$\underline{A_n \subseteq S_n'}$: Nach 3.3.4 genügt es zu zeigen, dass jeder 3-Zykel in S_n' liegt. Seien hierzu x_1, x_2, x_3 paarweise verschieden. Dann

$$(x_1\ x_2\ x_3) = (x_1\ x_3)(x_2\ x_3)(x_1\ x_3)^{-1}(x_2\ x_3)^{-1} = [(x_1\ x_3), (x_2\ x_3)] \in S_n'.$$

$\underline{A_n' = \{1\} \text{ für } n \leq 3}$: Für $n \leq 3$ ist $A_n \cong A_n/\{1\}$ abelsch, da $\#A_n \leq \#A_3 = \frac{\#S_3}{2} = \frac{3!}{2} = 3$.

$\underline{A_4' = V_4}$: „$\subseteq$“ Wegen $\#A_4 = \frac{4!}{2} = 4 \cdot 3 = 12$ gilt $\#(A_4/V_4) = 3$ und A_4/V_4 ist abelsch.

„$\supseteq$“ Ist $\{x_1, x_2, x_3, x_4\} = \{1, 2, 3, 4\}$, so nach 3.3.4

$$\begin{aligned}(x_1\ x_2)(x_3\ x_4) &= (x_1\ x_2\ x_3)(x_1\ x_2\ x_4)(x_1\ x_2\ x_3)^{-1}(x_1\ x_2 x_4)^{-1}\\ &= [\underbrace{(x_1\ x_2\ x_3)}_{\in A_4}, \underbrace{(x_1\ x_2\ x_3)}_{\in A_4}] \in A_4'.\end{aligned}$$

$\underline{A_n' = A_n \text{ falls } n \geq 5}$: Sei $n \geq 5$. Zu zeigen: $A_n \subseteq A_n'$. Seien $x_1, x_2, x_3 \in \{1, ..., n\}$ paarweise verschieden. Zu zeigen: $(x_1\ x_2\ x_3) \in A_n'$. Wähle $x_4, x_5 \in \{1, ..., n\} \setminus \{x_1, x_2, x_3\}$ mit $x_4 \neq x_5$. Dann

$$(x_1\ x_2\ x_3) = (x_1\ x_2\ x_4)(x_1\ x_3\ x_5)(x_1\ x_2\ x_4)^{-1}(x_1\ x_3\ x_5)^{-1} = [(x_1\ x_2\ x_4), (x_1\ x_3\ x_5)] \in A_n'.$$

□

3.3.6 Definition Sei G eine Gruppe. Es heißt $(G_0, ..., G_n)$ eine Normalreihe von G, wenn $G = G_0 \triangleright G_1 \triangleright ... \triangleright G_n = \{1\}$. In diesem Fall heißen die Gruppen G_k/G_{k+1} $(k \in \{0, ...n-1\})$ die Faktoren dieser Normalreihe. Es heißt G auflösbar, wenn G eine Normalreihe mit (lauter) abelschen Faktoren besitzt.

3.3.7 Satz Sei G eine Gruppe. Dann

$$G \text{ auflösbar} \iff \exists n \in \mathbb{N}_0 : G^{(n)} = \{1\}.$$

Beweis. „$\Longleftarrow$“ Ist $n \in \mathbb{N}_0$ mit $G^{(n)} = \{1\}$, so ist $(G^{(0)}, ..., G^{(n)})$ eine Normalreihe von G mit abelschen Faktoren.

„ $\Longrightarrow$ “ Sei $(G_0, ..., G_n)$ eine Normalreihe von G mit abelschen Faktoren. Wir zeigen durch Induktion nach $k \in \{0, ..., n\}$, dass $G^{(k)} \subseteq G_k$:

$\underline{k = 0:}$ $G^{(0)} = G = G_0$

$\underline{k \to k+1 \quad (k \in \{0, ..., n-1\})}$ $\quad G^{(k+1)} = (G^{(k)})' \underset{G^{(k)} \subseteq G_k}{\overset{\text{IV}}{\subseteq}} G_k' \overset{\substack{G_k/G_{k+1}\\ \text{abelsch}}}{\subseteq} G_{k+1}$ □

3.3.8 Satz S_n ist auflösbar für $n \leq 4$, nicht aber für $n \geq 5$.

Beweis. Nach Proposition 3.3.5 gilt $S_n^{(2)} = A_n' = \{1\}$ für $n \leq 3$,

$$S_4^{(3)} = A_4^{(2)} = V_4' \overset{\substack{V_4 \cong V \cong C_2 \times C_2\\ \text{abelsch}}}{=} \{1\}$$

und $S_n^{(1)} = S_n^{(2)} = ... = A_n \neq \{1\}$ für $n \geq 5$. □

3.3.9 Proposition Sei G eine Gruppe.

(a) Ist G auflösbar und $H \leq G$, so ist auch H auflösbar.

(b) Ist $N \triangleleft G$, so

$$G \text{ auflösbar} \iff (N \text{ auflösbar } \& \ G/N \text{ auflösbar}).$$

Beweis.

zu (a): Klar, da man durch Induktion $H^{(n)} \subseteq G^{(n)}$ für alle $n \in \mathbb{N}_0$ zeigt.

zu (b): Gelte $N \triangleleft G$. Durch Induktion zeigt man $(G/N)^{(n)} = (G^{(n)}N)/N$ für alle $n \in \mathbb{N}_0$ **??**:

$\underline{n = 0}$: $G/N = \underbrace{(GN)}_{=G}/N$

$\underline{n \to n+1 \ (n \in \mathbb{N}_0)}$:

$$\begin{aligned}
(G/N)^{(n+1)} &= ((G/N)^{(n)})' \overset{\text{IV}}{=} ((G^{(n)}N)/N)' \\
&\overset{??}{=} \{[\overline{a_1 n_1}^N, \overline{a_1' n_1'}^N] \cdots [\overline{a_m n_m}^N, \overline{a_m' n_m'}^N] \mid m \in \mathbb{N}_0,\ a_i, a_i' \in G^{(n)},\ n_i, n_i' \in \mathbb{N}\} \\
&= \{\overline{[a_1, a_1'] \cdots [a_m, a_m']}^N \mid m \in \mathbb{N}_0,\ a_i, a_i' \in G^{(n)}\} \\
&\overset{??}{=} \{\overline{g}^N \mid g \in G^{(n+1)}\} = \{\overline{gn}^N \mid g \in G^{(n+1)},\ n \in N\} = (G^{(n+1)}N)/N
\end{aligned}$$

„$\Longrightarrow$“ Ist $n \in \mathbb{N}$ mit $G^{(n)} = \{1\}$, so $(G/N)^{(n)} = (G^{(n)}N)/N = N/N = \{1\}$.

„$\Longleftarrow$“ Ist $n \in \mathbb{N}$ mit $N^{(n)} = \{1\}$ und $(G/N)^{(n)} = \{1\}$, so $(G^{(n)}N)/N = N/N$, also $G^{(n)} \subseteq N$ und $G^{(2n)} \subseteq N^{(n)} = \{1\}$. □

3.3.10 Satz Sei $p \in \mathbb{P}$. Jede p-Gruppe ist auflösbar.

Beweis. Wir zeigen durch Induktion nach $e \in \mathbb{N}_0$, dass alle Gruppen G mit $\#G = p^e$ auflösbar sind.

$\underline{e = 0}$: ✓

$\underline{0, ..., e-1 \to e \quad (e \in \mathbb{N})}$: Sei G eine Gruppe mit $\#G = p^e$. Nach **??** gilt $\#Z(G) > 1$. Nach dem Satz von Lagrange **??** gibt es also $d \in \{0, ..., e-1\}$ mit $\#(G/Z(G)) = p^d$ (siehe auch 1.3.14). Nach Induktionsvoraussetzung ist $G/Z(G)$ auflösbar. Da $Z(G)$ abelsch und daher auch auflösbar ist, folgt mit **??**, dass auch G auflösbar ist. □

3.3.11 Proposition Sei G eine Gruppe und $N \triangleleft G$. Bezeichne $\pi : G \to G/N,\ a \mapsto \overline{a}^N$ den kanonischen Epimorphismus. Dann wird durch die Zuordnungen

$$\begin{aligned} I &\mapsto \pi(I) = I/N \qquad \text{und} \\ \pi^{-1}(J) &\hookleftarrow J \end{aligned}$$

eine Bijektion zwischen der Menge der Untergruppen (Normalteiler) I von G mit $N \subseteq I$ und der Menge der Untergruppen (Normalteiler) von G/N definiert.

Beweis. Übung. □

3.3.12 Satz Sei G eine endliche Gruppe und $(G_0, ..., G_m)$ eine Normalreihe von G mit abelschen Faktoren. Dann gibt es eine Normalreihe $(H_0, ..., H_n)$ von G mit $\{G_0, ..., G_m\} \subseteq \{H_0, ..., H_n\}$, deren Faktoren H_k/H_{k+1} alle zyklisch von Primzahlordnung sind.

Beweis. Ohne Einschränkung

$$G = G_0 \underset{\neq}{\triangleright} G_1 \underset{\neq}{\triangleright} \ldots \underset{\neq}{\triangleright} G_m = \{1\}.$$

Sei $k \in \{0, \ldots, m-1\}$ mit $\#(G_k/G_{k+1}) \notin \mathbb{P}$. Dann gibt es sicher J mit

$$\{1\} \underset{\text{echt}}{<} J \underset{\text{echt}}{<} G_k/G_{k+1}$$

(z.B. wegen **??** oder indem man J einfach als geeignete zyklische Untergruppe von G_k/G_{k+1} wählt). Da G_{k+1}/G_k abelsch ist, gilt

$$\{1\} \underset{\neq}{\triangleleft} J \underset{\neq}{\triangleleft} G_k/G_{k+1}.$$

Für $I := \pi^{-1}(J)$ mit $\pi : G_k \to G_k/G_{k+1}$ kanonisch gilt nach 3.3.11 dann

$$G_k \underset{\neq}{\triangleright} I \underset{\neq}{\triangleright} G_{k+1}.$$

Es ist I der Kern von $G_k \twoheadrightarrow G_k/G_{k+1} \twoheadrightarrow (G_k/G_{k+1})/J$ und daher $G_k/I \cong \underbrace{\underbrace{(G_k/G_{k+1})}_{\text{abelsch}}/J}_{\text{abelsch}}$ abelsch. Weiter ist $I/G_{k+1} \leq \underbrace{G_k/G_{k+1}}_{\text{abelsch}}$ auch abelsch. Mache nun so weiter... □

§ 4 Körper [→ LA § 4]

§ 4.1 Endliche und algebraische Körpererweiterungen

4.1.1 Definition Sei $L|K$ eine Körpererweiterung [→ 2.3.11]. Die Dimension $[L : K] := \dim_K L \in N \cup \{\infty\}$ 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 $A \times B \to AB := \{ab \mid a \in Ab \in B\},\ (a, b) \mapsto ab$ bijektiv und AB eine Basis des K-Vektorraums V.

Beweis. Zu zeigen:

(a) $\operatorname{span}_K AB = V$

(b) Für paarweise verschiedene $a_1, ..., a_m \in A$ und paarweise verschiedene $b_1, ..., b_n \in B$ sind $a_1b_1, ..., a_1b_n, ..., a_mb_1, ..., a_mb_n$ linear unabhängig.

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

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 $\sum_{j=1}^n \left(\sum_{i=1}^m \lambda_{ij} a_i\right) b_j = 0$ und daher $\sum_{i=1}^m \lambda_{ij} a_i = 0$ für alle j, also $\lambda_{ij} = 0$ für alle i, j. □

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, [→ **??**]]. 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 $\left(\sqrt{2}\right)^2 - 2 = 0$.

(b) $\mathring{\imath}$ und $\mathring{\imath} + 1$ sind algebraisch über $\mathbb{Q}$, denn $\mathring{\imath}^2 + 1 = 0$ und $(\mathring{\imath} + 1)^2 - 2(\mathring{\imath} + 1) + 2 = 0$.

(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 $K[X] \to L,\ f \mapsto f(a)$ ein Ideal von $K[X]$, welches von einem eindeutig bestimmten normierten Polynom erzeugt wird [→ LA 10.2.4], dem sogenannten Minimalpolynom $\operatorname{irr}_K(a) \in K[X]$.

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) $f = \operatorname{irr}_K(a)$

(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 $\lambda_a : L \to L,\ b \mapsto ab$.

Beweis.

(a) $\Longrightarrow$ (b): Klar

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

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

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

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 $K[X]/(\mathrm{irr}_K(a)) \to K[a],\ \overline{f} \mapsto f(a)$.

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

4.1.11 Beispiel $\mathrm{irr}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/(X^2 - 2)$ 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:

[1] Korrektur: 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) $\Longrightarrow$ (b): Nach 4.1.10.

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

(a) $\Longrightarrow$ (c): Nach 4.1.10

(c) $\Longrightarrow$ (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 $K[a] \neq K(a)$. □

4.1.13 Korollar Jede endliche Körpererweiterung ist algebraisch.

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

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

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

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

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 $\mathrm{irr}_F(a) \in F[X]$ mit $a_1, ..., a_n \in F$. Dann ist a sogar algebraisch über $K(a_1, ..., a_n)$.

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

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 [→ 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 $\mathrm{irr}_K(a) = f$.

[2] Korrektur: Aussage wahrscheinlich so nicht richtig?

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. $K' := \{\overline{b} \mid b \in K\}$ ist ein zu K isomorpher Unterkörper von L, da $K \hookrightarrow L,\ b \mapsto \overline{b}$ und $f' := \varphi(f) \in K'[X]$ mit $\varphi : K[X] \overset{\cong}{\to} K'[X],\ b \mapsto \overline{b}\ (b \in K),\ X \mapsto X$.

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

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 $\mathring{\imath} \in L$ mit $L = K(\mathring{\imath})$ und $\mathrm{irr}_K(\mathring{\imath}) = X^2 + 1$.

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

(b) $\Longrightarrow$ (c): Klar.

(c) $\Longrightarrow$ (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 $\mathrm{irr}_K(a) = X - c$ für ein $c \in K$. Dann aber $a - c = 0$, also $a = c \in K$.

(d) $\Longrightarrow$ (e): Klar nach 4.1.13.

(e) $\Longrightarrow$ (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 $a \in K$. □

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 [→ **??**]

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

Wir zeigen $1 \; not \in I$ und nehmen hierzu an $1 \in I$. Wähle $f_1, ..., f_n \in K[X] \setminus K$ und $g_1, ..., g_n \in A$ mit

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

alle f_i (und damit X_{f_i}) paarweise verschieden. Durch n-faches Anwenden von 4.2.2 erhält man sukzessive $L|K$ und $a_1, ..., a_n \in L$ mit $f_i(a_i) = 0$ für $i \in \{1, ..., n\}$. 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 $K' := \{\overline{b} \mid b \in K\} \cong K \subseteq L$. 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). □

[3] Korrektur: Kann ich nicht lesen.
[4] Korrektur: 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 [→ 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 $K_n[X]|K_n$ 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. □

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 $\overline{\mathbb{Q}}^{\mathbb{C}}$ [→ **??**] ein algebraischer Abschluss von $\mathbb{Q}$.

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

(a) Es gibt einen Isomorphismus $\psi : K(a) \to K'(b)$ mit $\psi|_K = \varphi$ und $\psi(a) = b$.

(b) *Entweder* ist sowohl a algebraisch über K als auch b über K' mit $\tilde{\varphi}(\mathrm{irr}_K(a)) = \mathrm{irr}_{K'}(b)$[6] *oder* weder a ist algebraisch über K noch b über K'.

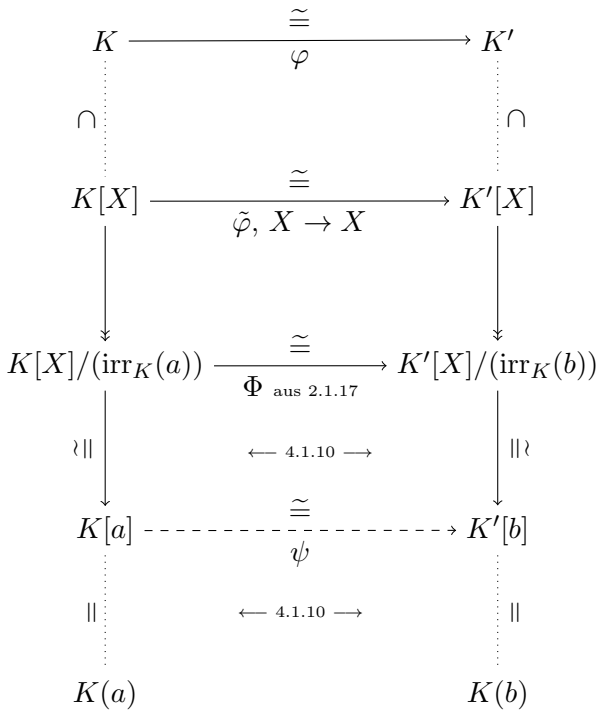
Beweis.

(a) $\Longrightarrow$ (b) Ist einfach.

[5] Hier könnte man noch die Grafiken einfügen.
[6] Korrektur: Stand anders in der Vorlage.

(b) $\Longrightarrow$ (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 $\psi_0 : K[a] \to K'[b]$ mit $\psi_0|_K = \varphi$ und $\psi_0(a) = b$. Mit 2.3.7 kann man ψ_0 zu einem Isomorphismus $\psi : K[a] \to K'(b)$ erweitern.

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



□

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 $\varphi :\to L'$ mit $\varphi|_K = \mathrm{id}_K$. 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 $L \to L'$ gibt.

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

Beweis. Es gilt:

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

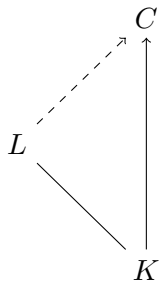
□

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 $\psi : K(a) \to K(b)$ 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 $\varphi : K \to C$ ein Homomorphismus. Dann gibt es einen Homomorphismus $\psi : L \to C$ mit $\psi|_K = \varphi$.



Beweis. Auf $M := \{(F, \alpha) \mid F$ Zwischenkörper von $L|K$, $\alpha : F \to C$ Homomorphismus$\}$ definieren wir eine Halbordnung $\preceq$ durch $(F, \alpha) \preceq (F', \alpha') :\iff (F \subseteq F' \;\&\; \alpha'|_F = \alpha)$. 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 $\beta : G \to C,\ a \mapsto \alpha(a)$ für $(F, \alpha) \in K$ mit $a \in F$, eine obere Schranke (G, β) von K in $(M, \preceq)$ definiert.

Inesgesamt beseitzt also in $(M, \preceq)$ jede Kette eine obere Schranke. Nach dem Lemma von Zorn besitzt $(M, \preceq)$ ein maximales Element (H, γ). Es günugt, $H = L$ zu zeigen. Sei hierzu $a \in L$. Zu zeigen, dass $a \in H$. Bezeichne $\tilde{\gamma} : H[X] \to (\gamma(H))[X]$ den Homomorphismus mir $\tilde{\gamma}|_H = \gamma$ und $\tilde{\gamma}(X) = X$. Da $\tilde{\gamma}$ eine Isomorphismus ist, ist mit $p := \mathrm{irr}_H(a)$ auch $q := \tilde{\gamma}(\mathrm{irr}_K(a)) \in (\gamma(H))[X]$ 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 Homomorphimus $\delta : H(a) \to C$ 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 $(H, \gamma) = (H(a), \delta)$, inesbesondere $H = H(a)$, das heißt $a \in H$, wie gewünscht. □

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 $\varphi : L \to C$, 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 $L' = F$. □

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]

[7] Korrektur: Konnte Klammerung hier nicht richtig lesen.

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

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

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 $a_1, ..., a_n$ gibt, mit $f = c\prod_{i=1}^{n}(X - a_i)$ und $L = K(a_1, ..., a_n)$ (oder $L = K[a_1, ..., a_n]$).

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) $\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$ ist ein Zerfällungskörper von $X^3 - 2$, denn

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

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 Ajunktion von über K algebraischen Elementen und ist damit nach 4.1.19 ist $\overline{K}^L$ enthalten und damit gleich $\overline{K}^L$. Ist zusätzlich A endlich, ist 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 aus K-Isomorphie geanu 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 $\varphi : \overline{L} \to \overline{L}'$. 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 $L \to L'$ induziert. □

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

4.3.9 Definition Sei K ein Körper. Betrachte die natürliche Wirkung von $\mathrm{Aut}(\overline{K}|K)$ auf $\overline{K}$ und die dazugehörige Äquivalenzrelation $\sim_K$ auf $\overline{K}$, definiert durch $a \sim_K b :\iff \exists\ \varphi \in \mathrm{Aut}(\overline{K}|K) : \varphi(a) =??$[8] $(a, b \in \overline{K})$. 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 $\varphi : L \to L$ ein K-Homomorphismus. Dann ist $\varphi \in \mathrm{Aut}(L|K)$.

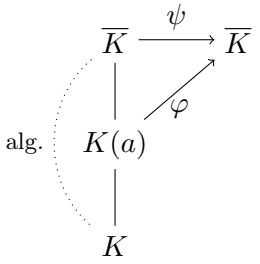
Beweis. Nach **??** ist φ injektiv. Also ist noch zu zeigen, dass φ surjektiv ist. Sei $b \in L$ und zeige also $\exists\ a \in L : \varphi(a) = b$. Wähle $p \in K[X] \setminus \{0\}$ mit $p(b) = 0$. Für die endliche Menge $A := \{a \in L \mid p(a) = 0\}$ gilt dann $\varphi(A) \subseteq A$ und daher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

Beweis. „$\Longrightarrow$“: Klar

[8] Korrektur: Kann ich nicht lesen.

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



□

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 $\mathrm{irr}_K(a)$ über K, denn $\deg \mathrm{irr}_K(a) = 2$.

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 $\varphi : L \to \overline{L}$ gilt $\varphi(L) = L$.

(e) $\forall\, \varphi \in \mathrm{Aut}(\overline{L}|K) : \varphi(L) = L$

Beweis.

(a) $\Longrightarrow$ (d) Sei L Zerfällungskörper von $A \subseteq K[X] \setminus \{0\}$ und $\varphi : L \to \overline{L}$. 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 **??**.

[9] Korrektur: Konnte ich nicht lesen.

(d) $\Longrightarrow$ (e) Klar.

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

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

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

(c) $\Longrightarrow$ (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 $\overline{L}$ zueinander konjugiert sind, liegen diese alle in L wegen (c).

(b) $\Longrightarrow$ (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 $\mathrm{irr}_{\mathbb{Q}}(\sqrt[4]{2}) = X^4 - 2$ und $\mathrm{irr}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, 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: $\mathring{\imath}\sqrt[4]{2}$ 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 $\overline{K}$ über K normal.

---

§ 4.4 Endliche Körper

4.4.1 Definition Ist R ein Ring, so heißt die eindeutig bestimmte Zahl $n \in \mathbb{N}_0$, welche den Kern des eindeutig bestimmten Ringhomomorphismus' $\mathbb{Z} \to R$ als Ideal erzeugt, die Charakterisitk von R, in Zeichen $\mathrm{char}\, R$.[11]

[10] Korrektur: Kann ich nicht lesen / ist mir nicht klar.
[11] $\varphi : \mathbb{Z} \to R,\ ...,\ -1 \mapsto -1,\ 0 \mapsto 0,\ 1 \mapsto 1,\ 2 \mapsto 2,\ ...$

4.4.2 Bemerkung

(a) Ist R ein Ring, so gibt es genau einen Homomorphismus $\mathbb{Z}/(\operatorname{char} R) \to R$. Dieser ist eine Einbettung und sein Bild ist der kleinste Unterring von R.

(b) ist R ein Integritätsring, so gilt $\operatorname{char} R \in \{0\} \cup \mathbb{P}$.

(c) Ist K ein Körper und $p := \operatorname{char} K$, so hat man im Fall $p = 0$ ($p \in \mathbb{P}$) genau einen Homomorphismus $\mathbb{Q} \to K$ [→ 2.3.7] ($\mathbb{F}_p = \mathbb{Z}/(p) \to K$). Dessen Bild ist der kleinste Unterkörper von K, welchen man auch Primkörper von K nennt. Jeder Körper enthält also einen zu $\mathbb{Q}$ oder $\mathbb{F}_p$ ($p \in \mathbb{P}$) isomorphen Unterkörper.

4.4.3 Proposition Sei R ein kommutativer Ring mit $p := \operatorname{char} R \in \mathbb{P}$. Dann ist der Frobenius-Endomorphismus [Ferdinand Georg Frobenius, geb. 1849, gest. 1917] $\Phi_R : R \to R,\ a \mapsto a^p$ ein Endomorphismus.

Beweis. Strittig könnte nur sein, ob $(a+b)^p = a^p + b^p$ für alle $a, b \in R$ gilt. Durch Ausmultiplizieren und Zusammenfassen der linken Seite erhält man $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$, wobei $\binom{p}{k}$ das Bild des Binomialkoeffizienten $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ unter $\mathbb{Z} \to R$ bezeichnet. Für $k \in \{1, ..., p-1\}$ ist p kein Teiler von $k!(p-k)!$, aber $k!(p-k)!$ ein Teiler von $p!$ und damit von $(p-1)!$. Es folgt, dass $\binom{p}{k} = p\frac{(p-1)!}{k!(p-k)!} \in (p)$ und daher $\binom{p}{k} = 0$ in R für $k \in \{1, ..., p-1\}$. □

4.4.4 Definition Sei K ein Körper, $f \in K[X]$ und $a \in K$. Dann heißt $\mu(a, f) := \sup\{n \in \mathbb{N}_0 \mid (X-a)^n \text{ teilt } f \text{ in } K[X]\} \in \mathbb{N}_0 \cup \{\infty\}$ die Vielfachheit von a in f.

4.4.5 Bemerkung Sei K ein Körper, $f \in K[X]$ und $a \in K$.

(a) $\mu(a, f) = \infty \iff f = 0$

(b) $\mu(a, f) \geq 1 \iff f(a) = 0$

(c) Die Definition stimmt überein mit der in [→ LA 10.1.13] gegebenen Definition der Vielfachheit einer Nullstelle $a \in K$ eines Polynoms $f \in K[X] \setminus \{0\}$.

(d) $\mu(a, f) = v_{X-a}(f)$, wobei v_{X-a} die in **??** definierte $(X-a)$-Bewertung auf $K(X) = \operatorname{qf}(K[X])$ bezeichne.

4.4.6 Konvention Ist R ein Ring und $n \in \mathbb{Z}$, so schreibt man oft n und meint damit das Bild von n unter dem eindeutig bestimmten Ringhomomorphismus $Z \to R$.

4.4.7 Definition Sei K ein Körper. Dan durch $1' = 0$ und $(X^n)' = nX^{n-1}$ für $n \in \mathbb{N}$ gegebenen K-Vektorraumhomomorphismus $K[X] \to K[X],\ f \mapsto f'$ nennt[12] man formale Ableitung [→ LA 6.3.2 f].

4.4.8 Proposition Sei K ein Körper. Für alle $f, g \in K[X]$ gilt:

(a) $(fg)' = f'g + fg'$ („Produktregel“)

(b) $(f(g))' = (f'(g))g'$ („Kettenregel“)

Beweis.

zu (a): Die Abbildung $b : K[X] \to K[X]$, $(f, g) \mapsto (fg)' - f'g - fg'$ ist bilinear. Daher reicht es zu zeigen, dass $b(X^m, X^n) = 0$ für alle $m, n \in \mathbb{N}$. Dies ist klar für $m = 0$ oder $n = 0$.[13] Seien also $m, n \in \mathbb{N}$. Dann ist $b(X^m, X^n) = (m+n)X^{m+n-1} - mX^{m-1}X^n - X^m nX^{n-1} = 0$.

zu(b): Er reicht für $n \in \mathbb{N}$ zu zeigen, dass für alle $g \in K[X]$ gilt: $(g^n)' = (ng^{n-1})g'$, was wir durch Induktion nach $n \in \mathbb{N}$ machen: $n = 1$ ist klar, also $n \to n+1$ ($n \in \mathbb{N}$): Sei $g \in K[X]$. Dann $(g^{n+1})' = (gg^n)' = g'g^n + g(g^n)' = g'g^n + gng^{n-1}g' = (n+1)g^n g'$. □

4.4.9 Proposition Sei K ein Körper, $p := \operatorname{char} K$, $f \in K[X] \setminus \{0\}$ und $a \in K$. Dann gilt

$$p \nmid \mu(a, f) \implies \mu(a, f') = \mu(a, f') = \mu(a, f) - 1$$

$$p \mid \mu(a, f) \implies \mu(a, f') = \mu(a, f') \geq \mu(a, f)$$

[Beachte, dass für $p = 0$ gilt: $p \nmid \mu(a, f) \iff \mu(a, f) \geq 1 \iff f(a) = 0$ und $p \mid \mu(a, f) \iff \mu(a, f) = 0 \iff f(a) \neq 0$.]

Beweis. Setze $n := \mu(a, f)$ und schreibe $f = (X-a)^n g$ mit $g \in K[X]$. Dann gilt $g(a) \neq 0$. Ist $n = 0$, so $p \mid n$ und es ist nichts zu zeigen. Sei also $n > 0$. Dann:

$$f' = (X-a)^n g' + n(X-a)^{n-1}g = (X-a)^{n-1} \underbrace{((X-a)g' + ng)}_{=:h}$$

Gilt $p \mid n$, so $h = (X-a)g'$ und $f' = (X-a)^n g'$. Gilt $p \nmid n$, so $h(a) = ng(a) \neq 0$. □

4.4.10 Definition Sei K ein Körper, $f \in K[X]$ und $a \in K$. Dann heißt a eine mehrfache Nullstelle von f, wenn $\mu(a, f) \geq 2$.

[12] Korrektur: Kann ich nicht lesen.
[13] Korrektur: Kann ich nicht lesen.

4.4.11 Proposition Sei K ein Körper, $f \in K[X]$ und $a \in K$. Dann ist a eine mehrfache Nullstelle von f genau dann, wenn $f(a) = f'(a) = 0$.

Beweis. Gilt $\mu(a, f) \geq 2$, so $\mu(a, f') \geq 1$ nach 4.4.9. Gilt umgekehrt $f(a) = f'(a) = 0$, so ist natürlich $\mu(a, f) \geq 1$. Wäre $\mu(a, f) = 1$, so $\operatorname{char} K \nmid \mu(a, f)$ und daher $\mu(a, f') = 0$ nach 4.4.9 im Widerspruch zu $f'(a) = 0$. □

4.4.12 Beispiel Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Das Polynom $X^{p^n} - X \in \mathbb{F}_p[X]$ hat keine mehrfachen Nullstellen im algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$, denn $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$.

4.4.13 Bemerkung Sei K ein endlicher Körper. Dann gilt $p := \operatorname{char} K \in \mathbb{P}$ und K ist ein endlich-dimensionaler Vektorraum über seinem zu $\mathbb{F}_p$ isomorphen Primkörper. Es folgt $\#K = p^n$ für ein $n \in \mathbb{N}_{\geq 1}$.

4.4.14 Satz Sei $p \in \mathbb{P}$, $K|\mathbb{F}_p$ eine Körpererweiterung und $n \in \mathbb{N}$. Dann sind äquivalent:

(a) $\#K = p^n$

(b) K ist Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

Beweis.

(a) $\implies$ (b): Gelte $\#K = p^n$. Dann $\#K^\times = p^n - 1$ und daher $a^{p^n - 1} = 1$ für alle $a \in K^\times$ nach **??**. Es folgt $a^{p^n} = a$ für alle $a \in K$. Es folgt $X^{p^n} - X = \prod_{a \in K}(X - a)$. Wegen $K = \mathbb{F}_p(K)$[14] folgt (b).

(b) $\implies$ (a): Gelte (b). Setzt man $F := \{a \in K \mid a^{p^n} - a = 0\}$, so besteht F genau aus den Nullstellen von $X^{p^n} - X$ in K, woraus mit (b) und 4.4.12 folgt $\#F = p^n$. Andererseits ist $F = \{a \in K \mid \Phi_K^n(a) = a\}$ ein Zwischenkörper von $K|\mathbb{F}_p$, denn Φ_K und damit Φ_K^n ist ein $\mathbb{F}_p$-Endomorphismus von K. Es folgt $K = \mathbb{F}_p(F) = F$. □

4.4.15 Korollar

(a) Ist $m \in \mathbb{N}$, so gibt es genau dann einen Körper K mit $\#K = m$, wenn es $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $m = p^n$ gibt.

(b) Sind K und L endliche Körper, so $K \cong L \iff \#K = \#L$.

[14] Korrektur: Stimmt das so?

Beweis.

zu (a): Benutze 4.4.13 und die Existenz von Zerfällungskörpern aus 4.3.7.

zu (b): Seien K und L endliche Körper mit $\#K = \#L$. Zu zeigen $K \cong L$. Nach 4.4.13 gibt es $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $\#K = \#L = p^n$. Aus dem Satz von Lagrange **??** folgt dann, dass K und L jeweils einen zu $\mathbb{F}_p$ isomorphen Primkörper besitzen.

Ohne Einschränkung sei $\mathbb{F}_p$ sogar gleich dem Primkörper sowohl von K also auch von L. Nach 4.4.14 sind K und L dann beide ein Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$. Mit 4.3.7 folgt $K \cong L$.

4.4.16 Notation Sei $p \in \mathbb{P}$. Fixiere einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$ den nach **??** und 4.4.14 eindeutig bestimmten Zwischenkörper von $\overline{\mathbb{F}}_p|\mathbb{F}_p$ mit genau p^n Elementen.[15]

4.4.17 Proposition

(a) $\overline{\mathbb{F}}_p = \bigcup\{\mathbb{F}_{p^n} \mid n \in \mathbb{N}\}$

(b) $\forall\, m, n \in \mathbb{N} : (\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n)$

Beweis.

zu (a): Sei $a \in \overline{\mathbb{F}}_p$ und setze $n := [\mathbb{F}_p(a) : \mathbb{F}_p] < \infty$. Dann ist $\#F_p(a) = p^n$ und daher $a \in \mathbb{F}_p(a) = \mathbb{F}_{p^n}$.

zu (b): Seien $m, n \in \mathbb{N}$. Gilt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, so ist $\mathbb{F}_{p^n}$ ein $\mathbb{F}_{p^m}$-Vektorraum der Dimension $k := [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$ und daher $p^n = (p^m)^k$, das heißt $n = mk$. Gilt umgekehrt $m \mid n$, das heißt $p^n = (p^m)^k$ für ein $k \in \mathbb{N}$, so ist jede Nullstelle von $X^{p^m} - X$ auch eine Nullstelle von $X^{p^n} - X$.

4.4.18 Lemma Sei G eine endliche Gruppe und $a, b \in G$. Gelte $ab = ba$ und $1 \in (\operatorname{ord} a, \operatorname{ord} b)$. Dann $\operatorname{ord}(ab) = \operatorname{ord}(a) \operatorname{ord}(b)$.

Beweis. Setze $m := \operatorname{ord} a$ und $n := \operatorname{ord} b$. Zu zeigen ist $\operatorname{ord}(ab) = mn$. Wärte $s, t \in \mathbb{Z}$ mit $1 = sm + tn$. Ist $k \in \mathbb{Z}$ mit $(ab)^k = 1$, so gilt[16]

$$1 = ((ab)^k)^{sm} = (a^m)^{ks}(b^{sm})^k = (b^{??})^k = b^k$$

[15] Korrektur: Macht irgendwie keinen Sinn.
[16] Korrektur: Kann ich nicht lesen.

und analog $1 = a^k$, woraus $m \mid k$ und $n \mid k$ folgt, das heißt $k \in (m) \cap (n) \overset{??}{=} (m)(n) \overset{??}{=} (mn)$. Schließlich $(ab)^m = (a^m)^n (b^n)^m = 1$. Somit $\operatorname{ord}(ab) = mn$. □

4.4.19 Satz Endliche Untergruppen der multiplikativen Gruppe eines Körper sind zyklisch.

Beweis. Sei K ein Körper, $G \leq K^\times$ mit $d := \#G < \infty$ und schreibe $d = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ mit $n \in \mathbb{N}_0$, $p_1, ..., p_n \in \mathbb{P}$ paarweise verschieden und $\alpha_1, ..., \alpha_n \in \mathbb{N}$. Sei $i \in \{1, ..., n\}$. Da das Polynom $X^{\frac{d}{p_i}} - 1$ höchstens $\frac{d}{p_i} < d$ Nullstellen hat, gibt es $a_i \in G$ mit $a_i^{\frac{p}{d_i}} \neq 1$. Setze $b_i := a^{\frac{d}{p_i^{\alpha_i}}} \in G$. Wegen $b_i^{p_i^{\alpha_i}} = a_i^d = 1$, da $\operatorname{ord} a_i \mid \#G = d$, gilt $\operatorname{ord} b_i \mid p_i^{\alpha_i}$. Setzt man schließlich $b := b_1, ..., b_n$, so folgt mit 4.4.18, dass $\operatorname{ord}(b) = p_1^{\alpha_1} \cdots p_n^{\alpha_n} = d$, also $\langle b \rangle = G$. □

4.4.20 Korollar Multiplikative Gruppen endlicher Körper sind zyklisch.

4.4.21 Satz Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Dann gibt es ein irreduzibles Polynom vom Grad n in $\mathbb{F}_p[X]$ und für jedes solche Polynom f gilt $\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(f)$.

Beweis. Wähle gemäß 4.4.19 ein $a \in \mathbb{F}_{p^n}^\times$ mit $\langle a \rangle = \mathbb{F}_{p^n}^\times$. Dann gilt insbesondere $\mathbb{F}_p(a) = \mathbb{F}_{p^n}$. Dann ist $f := \operatorname{irr}_{\mathbb{F}_p}(a) \in \mathbb{F}_p[X]$ irreduzibel vom Grad $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Sei nun $f \in \mathbb{F}_p[X]/(f)$ nach **??** ein Körper. Da $\overline{1}, \overline{X}, ..., \overline{X}^{n-1}$ eine Basis des $\overline{F}_p$-Vektorraumes $\mathbb{F}_p[X]/(f)$ ist, gilt $\#\mathbb{F}_p[X]/(f) = p^n$ und daher $\mathbb{F}_p[X]/(f) \cong \mathbb{F}_{p^n}$ nach **??**. □

---

§ 4.5 Separable Körpererweiterungen

4.5.1 Definition Sei K ein Körper. Ein Polynom $f \in K[X]$ heißt separabel, wenn f im algebraischen Abschluss $\overline{K}$ von K keine mehrfachen Nullstellen hat.

4.5.2 Warnung Sei K ein Körper. Viele Autoren nennen ein Polynom $f \in K[X]$ auch dann separabel über K, wenn jeder irreduzible Teiler von f in $K[X]$ in unserem Sinne separabel ist.

4.5.3 Proposition Sei K ein Körper und $f \in K[X]$. Dann gilt f separabel $\iff$ $\gcd_{K[X]}(f, f') = 1 \iff 1 \in (t, t')_{K[X]} \iff \gcd_{\overline{K}[X]}(f, f') = 1$.

Beweis. Klar mit 4.4.11.

4.5.4 Korollar Sei K ein Körper und $f \in K[X]$ irreduzibel. Dann gilt f separabel $\iff f' \neq 0$.

4.5.5 Korollar Sei K ein Körper der Charakteristik $p \in \mathbb{P} \cup \{0\}$ und $f \in K[X]$ irreduzibel. Dann gilt:

(a) $p = 0 \implies f$ separabel

(b) $p \in \mathbb{P} \implies (f$ separabel $\iff f \notin K[X^p])$

(c) Es gibt ein irreduzibles separables $g \in K[X]$ und ein $n \in N_0$ mit $f = g(X^{p^n})$. Hierbei sind g und n durch f eindeutig bestimmt und für alle $a \in \overline{K}$ mit $f(a) = 0$ gilt $\mu(a, f) = p^n$.

Beweis. (a) und (b) direkt aus 4.5.4.

(c) direkt aus (a), falls $p = 0$. Dann $n = 0$ und $g = f$. (c) durch iteriertes Anwenden von (b), falls $p \in \mathbb{P}$. (Ist $g = \prod_{i=1}^{d}(X - a_i)$ mit $a_i \in \overline{K}$, so $f = \prod_{i=1}^{d}(X^{p^n} - a_i) = \prod_{i=1}^{d}(X^{p^n} - b_i^{p^n}) \overset{4.4.3}{=} \prod_{i=1}^{d}(X - b_i)^{p^n})$, wobei man $b_i \in \overline{K}$ wählt mit $b_i^{p^n} - a_i = 0$.) $\square$

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 Galoistheorie.* 4. Aufl. 2007. Heidelberg : Spektrum Akademischer Verlag, 2007. – ISBN 978–3–827–41609–4

Index