Universität Konstanz

Skriptum zur Vorlesung

Einführung in die Algebra

Private Mitschrift

gelesen von: Prof. Dr. Markus Schweighofer

Wintersemester 2014/15
Stand vom 17. Januar 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"*

„·" 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 [$\rightarrow$ 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 $S_n := S_{\{1,...,n\}}$ 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 $\mathrm{Aut}(V) := \{f \mid f : V \rightarrow V \text{ linear und bijektiv}\}$ mit der Hintereinanderschaltung als Multiplikation eine Gruppe.

(c) Ist R ein kommutativer Ring (z. B. $R = \mathbb{Z}$), so ist $\mathrm{GL}_n(R) := \{A \in R^{n\times n} \mid A \text{ invertierbar}\} = \{A \in R^{n\times n} \mid \det A \in R^\times\}$ 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. [$\to$ LA § 9.1]

`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 $\operatorname{End}(V)^\times = \operatorname{Aut}(V)$. [$\to$ 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 $\text{◥}_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ obere Dreiecksmatrix}\}$, $\text{◣}_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ untere Dreiecksmatrix}\}$ und $\text{◣}_R^{n\times n} \cap \text{◥}_R^{n\times n} = \{A \in R^{n\times n} \mid A \text{ Diagonalmatrix}\}$ Unterringe von $R^{n\times n}$ mit Einheitengruppen $(\text{◥}_R^{n\times n})^\times = \text{◥}_n(R)$, $(\text{◣}_R^{n\times n})^\times = \text{◣}_n(R)$ und $\left(\text{◣}_R^{n\times n} \cap \text{◥}_R^{n\times n}\right)^\times = \text{◥}_n(R) \cap \text{◣}_n(R)$.

(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

$$
\begin{aligned}
&f \text{ ein Gruppenhomomorphismus von } A \text{ nach } B \text{ ist,}\\
&f(1) = 1 \text{ und}\\
&\forall a, b \in A : f(ab) = f(a)f(b) \text{ gilt.}
\end{aligned}
$$

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. ↯)

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 [→ **??**] [→ LA § 3.3] Sei R ein Ring. Die Zuordnungen

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

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

(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 $\overline{0}$ 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 **??** 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 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 **??** 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:

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

□

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 $|\alpha| \le d$ und $a'_\alpha \in A$ für alle $\alpha \in \mathbb{N}_0^n$ mit $|\alpha| \le d'$. Dann

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

wobei man $a_\alpha := 0$ für $d < |\alpha| \le d + d'$ und $a'_\alpha := 0$ für $d' < |\alpha| \le d + d'$ 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 $a_\alpha \in A(\alpha \in \mathbb{N}_0^n, |\alpha| \le d)$ gilt:

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

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

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

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 $\varphi : A \to C$ 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. $\square$

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

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 $\varphi : K \xrightarrow{\cong} \operatorname{im}\varphi$ 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]

2.3.15 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 $K \cup F \subseteq \operatorname{im}\varphi \subseteq \operatorname{im}\psi$, weswegen ψ surjektiv ist.

Die Eindeutigkeit folgt aus 2.3.13.

[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?
[4] An Korrektor: Macht so keinen Sinn.

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. □

---

§ 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

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

[5] An Korrektor: Index für „Körper der rationalen Funktionen“ anpassen.
[6] An 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 $\mathrel{\widehat{=}}$ auf R ist definiert durch $a \mathrel{\widehat{=}} b :\Longleftrightarrow (a|b \;\&\; b|a) \iff (a) = (b)$ $(a, b \in R)$.

Setze $\widehat{a} := \overset{\widehat{=}}{a}$ 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. $\square$

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 $\ker\psi = \{a \in A \mid \psi(a) = 0\} = \left\{a \in A \mid \overline{\psi(a)}^{\mathfrak{q}} = 0\right\} = \{a \in A \mid \varphi(a) \in \mathfrak{q}\} = \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. $\square$

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 ...`

---

§ 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. $\square$

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, [→ **??**]]. 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) $\iff$ (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 $b \in L$. $\square$

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 $d = [K(a) : K]$. $\square$

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

(b) $\implies$ (a): Ist $d := [K(a) : K] < \infty$, so sind $1, a, ..., a^d$ 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 $K[a] \neq K(a)$. □

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 $f' = \operatorname{irr}_{K'}(a)$ 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 [$\rightarrow$ 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 $\operatorname{irr}_K(\mathring{\imath}) = X^2 + 1$.

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 [$\rightarrow$ 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 [$\rightarrow$ 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.

<u>(a) $\Longrightarrow$ (b)</u>: Durch sukzessives Abspalten von Nullstellen [$\rightarrow$ 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 $\mathrm{irr}_K(a) = X - c$ 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 $f \in K[X] \backslash K$. 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 [→ **??**]

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

Wir zeigen $1 \ \mathit{not} \in I$ 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

$$1 = \sum_{i=1}^{n} g_i f_i X_{f_i} \text{[4]} \tag{$*$}$$

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 $\mathbb{Q}$.

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