Universität Konstanz

Skriptum zur Vorlesung

Einführung in die Algebra

Private Mitschrift

gelesen von: Prof. Dr. Markus Schweighofer

Wintersemester 2014/15
Stand vom 13. März 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 ab, 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 $S_n := S_{\{1,\ldots,n\}}$ eine Gruppe der Ordnung $n! := \prod_{i=1}^{n} i$ „n Fakultät“. Für $n \geq 3$ ist sie nicht abelsch, denn die Transpositionen $\tau_{1,2}$ und $\tau_{2,3}$ kommutieren 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 $H \subseteq G$, $1_G \in H$, $\forall a, b \in H : a \cdot_G b \in H$ und $\forall a \in H : a^{-1} \in H$.

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

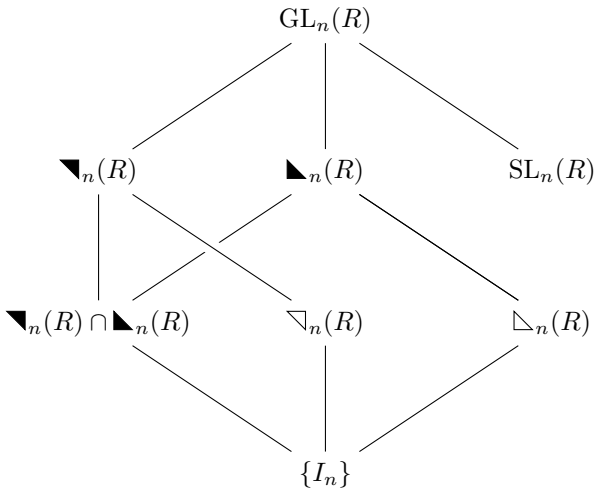
1.1.9 Beispiel

(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]

(b) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Die Mengen

$$\begin{array}{rcl}
\mathrm{SL}_n(R) & := & \{A \in R^{n\times n} \mid \det(A) = 1\} \\
\blacktriangleleft_n(R) & := & \{A \in \mathrm{GL}_n(R) \mid A \text{ obere Dreiecksmatrix}\} \\
\blacktriangleright_n(R) & := & \{A \in \mathrm{GL}_n(R) \mid A \text{ untere Dreiecksmatrix}\} \\
\triangleleft_n(R) & := & \left\{ \begin{pmatrix} 1 & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \in R^{n\times n} \right\} \text{ unipotente obere Dreiecksmatrix} \\
\triangleright_n(R) & := & \left\{ \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ * & \cdots & 1 \end{pmatrix} \in R^{n\times n} \right\} \text{ unipotente untere Dreiecksmatrix}
\end{array}$$

bilden allesamt Untergruppen von $\mathrm{GL}_n(R)$, die wie im folgenden Hasse-Diagramm halbgeordnet sind:



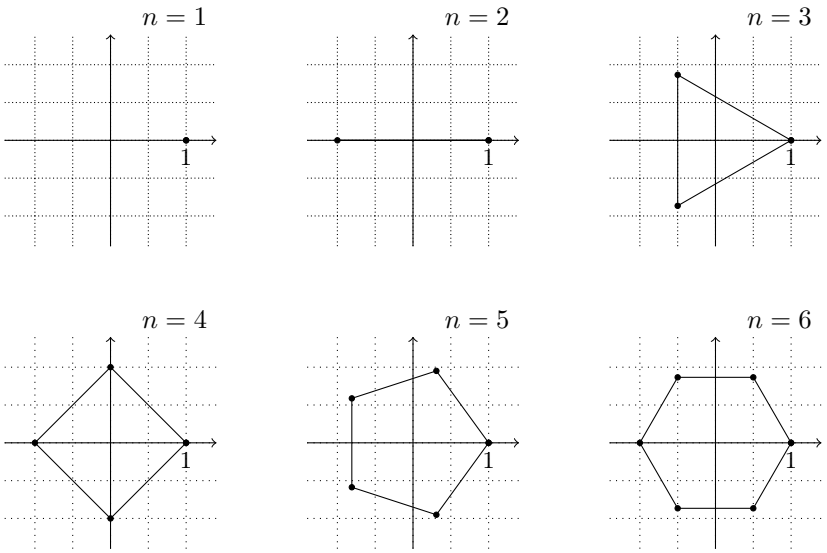
Dies ist alles leicht einzusehen, außer der Tatsache, dass $\blacktriangleleft_n(R)$, $\blacktriangleright_n(R)$, $\triangleleft_n(R)$ und $\triangleright_n(R)$ unter Inversenbildung abgeschlossen sind.

(c) Sei $n \in \mathbb{N}_0$. Dann nennt man die Untergruppe $O_n := \{A \in \mathbb{R}^{n\times n} \mid A^T A = I_n\}$ von $\mathrm{GL}_n(\mathbb{R})$ *orthogonale Gruppe* [→ LA § 11.2]. Man sieht leicht [→ LA 11.2.27]:

$$\mathrm{SO}_2 = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \;\middle|\; \varphi \in \mathbb{R} \right\} \qquad (\text{„Drehungen“})$$

$$O_2 = \mathrm{SO}_2 \;\cup\; \left\{ \begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} \;\middle|\; \varphi \in \mathbb{R} \right\} \qquad (\text{„Drehspiegelungen“})$$

(d) Sei $n \in \mathbb{N}_0$ und $P_n := \left\{ \begin{pmatrix} \cos(\frac{k}{n}2\pi) \\ \sin(\frac{k}{n}2\pi) \end{pmatrix} \;\middle|\; k \in \{0, ..., n-1\} \right\}$ die Ecken eines regulären n-Ecks.



$C_n := \{A \in \mathrm{SO}_2 \mid \forall x \in P_n : Ax \in P_n\}$ ist die *zyklische Gruppe* der Ordnung n („Drehungen des regulären n-Ecks“).

Sei $n \geq 3$. $D_n := \{A \in O_2 \mid \forall x \in P_n : Ax \in P_n\}$ ist die Diedergruppe der Ordnung $2n$ („Drehspiegelungen des regulären n-Ecks).

(e) Setze $P := \left\{ \binom{2}{1}, \binom{-2}{1}, \binom{-2}{-1}, \binom{2}{-1} \right\} \subseteq \mathbb{R}^2$ (Ecken eines nicht quadratischen Rechtecks). $V := \{A \in O_2 \mid \forall x \in P : Ax \in P\}$ ist die Kleinsche Vierergruppe. V hat die Ordnung 4.

1.1.10 Proposition Sei G eine Gruppe und $M \neq \emptyset$ eine Menge von Untergruppen von G. Dann ist auch $\bigcap M$ eine Untergruppe von G.

Beweis. Klar. □

1.1.11 Korollar und Definition Sei G eine Gruppe und $E \subseteq G$. Dann gibt es eine eindeutig bestimmte kleinste Untergruppe H von G mit $E \subseteq H$. Man nennt sie die von E (gemeinsam mit G) *erzeugte Untergruppe* und notiert sie mit $\langle E \rangle$ oder $\langle E \rangle_G$.
Notation: $\langle e_1, ..., e_n \rangle := \langle E \rangle$, falls $E = \{e_1, ..., e_n\}$.

1.1.12 Beispiel

(a) Sei $n \in \mathbb{N}_0$. Die Gruppe S_n ist (in sich selbst) von den Transpositionen erzeugt, das heißt $S_n = \langle \{\tau_{ij} \mid 1 \leq i < j \leq n\} \rangle$. Weiter gilt: $A_n = \langle \{\tau_{ij}\tau_{kl} \mid 1 \leq i < j \leq n,\ 1 \leq k < l \leq n\} \rangle$. [→ LA § 9.1]

(b) Sei K ein Körper und $n \in \mathbb{N}_0$. Die Gruppe $\mathrm{GL}_n(K)$ ist erzeugt von den Matrizen der folgenden zwei Formen:

(1)

$$\begin{pmatrix} 1 & & & 0 \\ & 1 & \lambda = (A)_{ij} & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in K^{n \times n},\ i \neq j,\ \lambda \in K$$

(2)

$$\begin{pmatrix} 1 & & & 0 \\ & \lambda = (A)_{ii} & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in K^{n\times n},\ \lambda \in K^\times$$

Begründung: Alle diese Matrizen liegen offensichtlich in $\mathrm{GL}_n(K)$. Sei $A \in \mathrm{GL}_n(K)$. Zu zeigen: A liegt in der von den fraglichen Matrizen erzeugten Untergruppe H. Nach [→ LA § 5.2] können wir A durch elementare Zeilenoperationen in reduzierte Stufenform $B \in K^{n\times n}$ überführen. Wegen $\ker(B) = \ker(A) = \{0\}$, muss $B = I_n$ sein. Die Zeilenoperationen

$$\begin{cases} z_i \leftarrow z_i + \lambda z_j & (i \neq j) \\ z_i \leftarrow \lambda z_i & (\lambda \in K^\times) \end{cases}$$

entsprechen der Multiplikation mit (1) oder (2) von links. Daher gibt es $C \in H$ mit $CA = B = I_n$. Es folgt $A = C^{-1} \in H$.

(c) Sei $n \in \mathbb{N}$. Dann

$$C_n = \left\langle \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \right\rangle.$$

(d) Sei $n \in \mathbb{N}$, $n \geq 3$. Dann

$$D_n = \left\langle \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, R \right\rangle,$$

wobei $R \in D_n \setminus C_n$ beliebig gewählt ist, zum Beispiel

$$R = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

die Spiegelung an der x-Achse.

(e) Jedes Element aus $V \setminus \{1\}$ erzeugt eine Untergruppe der Ordnung 2. Je zwei Elemente aus $V \setminus \{1\}$ erzeugen schon V.

---

§ 1.2 Gruppenhomomorphismen [→ LA § 2.2]

1.2.1 Definition Seien G und H Gruppen. Eine Abbildung $f : G \to H$ heißt *(Gruppen-)homomorphismus* von G nach H, wenn $f(ab) = f(a)f(b)$ für alle $a, b \in G$.

1.2.2 Proposition und Definition Seien G und H Gruppen und $f : G \to H$ ein Homomorphismus. Dann:

(a) $f(1) = 1$ und $f(a^{-1}) = (f(a))^{-1}$ für alle $a \in G$.

(b) Der Kern $\ker(f) := f^{-1}(\{1\}) = \{a \in G \mid f(a) = 1\}$ ist eine Untergruppe von G.

(c) Das Bild $\mathrm{im}(f) := f(G) = \{f(a) \mid a \in G\}$ ist eine Untergruppe von H.

(d) f injektiv $\iff \ker(f) = \{1\}$.

(e) f surjektiv $\iff \mathrm{im}(f) = H$.

1.2.3 Definition Ein Gruppenhomomorphismus $f : G \to H$ heißt *(Gruppen-)Mono-/Epi-/Isomorphismus*, wenn f injektiv/surjektiv/bijektiv ist, in Zeichen: $f : G \hookrightarrow H$ / $G \twoheadrightarrow H$ / $G \xrightarrow{\cong} H$. Statt (Gruppen-)-Monomorphismus sagt man auch *Einbettung*.

1.2.4 Proposition Hintereinanderschaltung von Gruppenhomomorphismen sind wieder Gruppenhomomorphismen, Umkehrfunktionen von Gruppenisomorphismen sind wieder Gruppenisomorphismen.

Beweis. Klar. □

1.2.5 Definition Zwei Gruppen G und H heißen *isomorph*, wenn es einen Isomorphismus $f : G \to H$ gibt, in Zeichen $G \cong H$.

1.2.6 Bemerkung Ein Gruppenisomorphismus führt die Multiplikationstabelle der einen Gruppe in eine Multiplikationstabelle der anderen über.

Er tauscht die Elemente aus, ohne die „Gruppenstruktur“ (d.h. die in der Multiplikation geregelten Beziehungen der Elemente untereinander) zu verändern. Alle strukturellen (d.h. nur auf die Rolle des Elements in der Gruppe bezogenen) Eigenschaften einer Gruppe übertragen sich daher unter Isomorphismen.

1.2.7 Definition und Satz Sei I eine Menge und sei für jedes $i \in I$ eine Gruppe G_i gegeben. Dann wird

$$\prod_{i\in I} G_i := \left\{ f : I \to \bigcup\{G_i \mid i \in I\} \;\middle|\; \forall i \in I : f(i) \in G_i \right\}$$

durch

$$gh := (i \mapsto g(i)h(i)) \qquad \left(g, h \in \prod_{i\in I} G_i \right)$$

wieder eine Gruppe, genannt das *direkte Produkt* der G_i $(i \in I)$. Für $g \in \prod_{i\in I} G_i$ und $i \in I$ gilt $1(i) = 1_{G_i}$ und $g^{-1}(i) = g(i)^{-1}$. Sind alle G_i $(i \in I)$ abelsch, so auch $\prod_{i\in I} G_i$.

1.2.8 Korollar Seien $G_1, ..., G_n$ Gruppen. Dann wird $\prod_{i=1}^n G_i = G_1 \times ... \times G_n$ durch

$$(a_1, ..., a_n)(b_1, ..., b_n) := (a_1b_1, ..., a_nb_n), \quad a_i, b_i \in G_i,$$

wieder eine Gruppe mit $1 = (1_{G_1}, ..., 1_{G_n})$ und $(a_1, ..., a_n)^{-1} = (a_1^{-1}, ..., a_n^{-1})$ für alle $(a_1, ..., a_n) \in G_1 \times ... \times G_n$. Sind $G_1, ...G_n$ abelsch, so auch $G_1 \times ... \times G_n$.

Beweis. Nehme $I = \{1, ..., n\}$ im Satz 1.2.7. □

1.2.9 Beispiel

(a) Ist $\varphi : M \to N$ bijektiv, so $S_M \cong S_N$, denn $\psi : S_M \to S_N,\ \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ ist ein Isomorphismus.

$$\begin{array}{ccc} M & \xrightarrow{\sigma} & M \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ N & \xrightarrow[\psi(\sigma)]{} & N \end{array} \qquad \text{also} \qquad \begin{array}{c} \varphi \circ \sigma = \psi(\sigma) \circ \varphi \\ \iff \psi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1} \end{array}$$

(b) Für $n \in \mathbb{N}, n \geq 3$:

$$D_n \hookrightarrow S_n,$$
$$A \mapsto \left(\begin{array}{rcl} \{1, ..., n\} & \to & \{1, ..., n\} \\ i & \mapsto & j, \text{ falls } A \begin{pmatrix} \cos(\frac{i}{n}2\pi) \\ \sin(\frac{i}{n}2\pi) \end{pmatrix} = \begin{pmatrix} \cos(\frac{i}{n}2\pi) \\ \sin(\frac{i}{n}2\pi) \end{pmatrix},\ i, j \in \{1, ..., n\} \end{array} \right)$$

Diese Abbildung ist surjektiv genau dann, wenn $n = 3$. Insbesondere $D_3 \cong S_3$.

(c) $\operatorname{sgn} : S_n \to \{-1, 1\} = \mathbb{Z}^\times$ ist ein Gruppenhomomorphismus [→ LA 9.1.4] mit Kern A_n.

(d) Sei R ein kommutativer Ring. Die Gruppe $\blacktriangledown_n(R) \cap \blacktriangle_n(R)$ der invertierbaren Diagonalmatrizen ist isomorph zur Gruppe $(R^\times)^n := R^x \times ... \times R^x$ und daher abelsch. Weiter gilt $\blacktriangledown_n(R) \cong \blacktriangle_n(R)$, denn

$$f : \blacktriangledown_n(R) \to \blacktriangle_n(R),\ (a_{ij})_{1\le i,j\le n} \mapsto (a_{n+1-i}a_{n+1-j})_{1\le i,j\le n}$$

ist ein Isomorphismus. Klar ist, dass f bijektiv ist. Um zu zeigen, dass f ein Homomorphismus ist, seien

$$A = (a_{ij})_{1\le i,j\le n},\ B = (b_{jk})_{1\le j,k\le n} \in \blacktriangledown_n(R).$$

Dann

$$\begin{aligned} f(AB) &= f\left(\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)_{1\le i,k\le n}\right) \\ &= \left(\sum_{j=1}^{n} a_{n+1-i,j}b_{j,n+1-k}\right)_{1\le i,k\le n} \\ &= \left(\sum_{j=1}^{n} a_{n+1-i,n+1-j}b_{n+1-j,n+1-k}\right)_{1\le i,k\le n} \\ &= f(A)f(B) \end{aligned}$$

Dies zeigt $\blacktriangledown_n(R) \cong \blacktriangle_n(R)$ und analog $\triangledown_n(R) \cong \triangle_n(R)$.

(e) Sei $n \in \mathbb{N}_0$. Wir haben $f : S_n \hookrightarrow O_n,\ \sigma \mapsto (e_{\sigma(1)}...e_{\sigma(n)})$. Seien $\sigma, \tau \in S_n$. Dann:

$$f(\sigma\tau) = (e_{(\sigma\tau)(1)}...e_{(\sigma\tau)(n)}) = (f(\sigma)e_{\tau(1)}...f(\sigma)e_{\tau(n)}) = f(\sigma)f(\tau)$$

Injektivität von f ist klar. Das Bild von f besteht gerade aus den Permutationsmatrizen. Für alle $\sigma \in S_n$ gilt $\operatorname{sgn}(\sigma) = \det f(\sigma)$ [→ LA § 9.1]. Daher $f|_{A_n} : A_n \hookrightarrow \mathrm{SO}_n$.

(f) Zur Kleinschen Vierergruppe:

$$f : V \to S_2,$$
$$A \mapsto \begin{cases} 1, \text{falls } A \text{ fixiert Kanten links und rechts,} \\ \tau_{12}, \text{falls } A \text{ vertauscht Kanten links und rechts.} \end{cases}$$

und

$$g : V \to S_2,$$
$$A \mapsto \begin{cases} 1, \text{falls } A \text{ fixiert Kanten oben und unten,} \\ \tau_{12}, \text{falls } A \text{ vertauscht Kanten oben und unten.} \end{cases}$$

sind Homomorphismen. Daher ist $h : V \to S_2 \times S_2,\ A \mapsto (f(A), g(A))$ auch ein Homomorphismus. Es ist h sogar ein Isomorphismus und daher $V \cong S_2 \times S_2 \cong C_2 \times C_2$. Insbesondere ist V abelsch.

1.2.10 Proposition (Satz von Cayley) Jede endliche Gruppe der Ordnung n ist isomorph zu einer Untergruppe von S_n.

Beweis. Sei G eine Gruppe mit $n := \#G \in \mathbb{N}$. Zu zeigen $\exists f : G \hookrightarrow S_n$. Wegen $S_n \cong S_G$, genügt, zu zeigen $\exists f : G \hookrightarrow S_G$. Definiere

$$f : G \to S_G,\ g \mapsto L_g := \begin{pmatrix} G \to G \\ h \mapsto gh \end{pmatrix}.$$

Dies ist wohldefiniert, denn L_g ist bijektiv mit Umkehrfunktion $L_{g^{-1}}$: $L_g \circ L_{g^{-1}} \overset{(A)}{=} L_{gg^{-1}} \overset{(I)}{=} L_1 \overset{(N)}{=} \mathrm{id}_G \overset{(N)}{=} L_1 \overset{(I)}{=} L_{g^{-1}g} \overset{(A)}{=} L_{g^{-1}} \circ L_g$.

f ist homomorph, denn für $g, h, a \in G$ gilt: $f(gh)(a) = (gh)(a) = g(ha) = g\big(f(h)(a)\big) = \big(f(g)\big)\big(f(h)(a)\big) = \big((f(g)) \circ (f(h))\big)(a) = \big(f(g)f(h)\big)(a)$.
f ist injektiv, denn ist $g \in G$ mit $f(g) = 1 = \mathrm{id}_G$, so $g = g \cdot 1 = (f(g))(1) = \mathrm{id}_G(1) = 1$. □

---

§ 1.3 Quotientengruppen

1.3.1 Definition Sei G eine Gruppe. Eine *Kongruenzrelation* auf G ist eine Äquivalenzrelation $\equiv$ auf G, für die gilt:

$$\forall\, a, a', b, b' \in G : ((a \equiv a' \wedge b \equiv b') \implies ab \equiv a'b') \qquad (\star)$$

Für $a \in G$ nennt man $\overline{a} := \overline{\overline{a}} := \{b \in G \mid a \equiv b\}$ statt Äquivalenzklasse auch *Kongruenzklasse* von a bezüglich $\equiv$. Diese Definition wurde gerade so gemacht, dass

$$\cdot : \begin{cases} G/\!\equiv \times\, G/\!\equiv & \to & G/\!\equiv \\ (\overline{a}, \overline{b}) & \mapsto & \overline{ab} \end{cases}, \quad a, b \in G$$

wohldefiniert ist.

1.3.2 Satz und Definition Ist G eine Gruppe und $\equiv$ eine Kongruenzrelation auf G, so wird die Quotientenmenge $G/\!\equiv = \{\overline{a} \mid a \in G\}$ mittels $\overline{a}\,\overline{b} := \overline{ab}$, $(a, b \in G)$ zu einer Gruppe (*Quotientengruppe*, *Faktorgruppe*) in der $1 = \overline{1}$ und $\overline{a}^{-1} = \overline{a^{-1}}$ für $a \in G$ gilt.

Beweis. Einfach, siehe auch [→ LA § 2.3]. □

1.3.3 Bemerkung Sei $\equiv$ eine Kongruenzrelation auf der Gruppe G. Dann $\overline{1} \leq G$ und

$$\forall\, a, b \in G : a \equiv b \iff ab^{-1} \in \overline{1} \iff a^{-1}b \in \overline{1}.$$

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

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

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 1.3.3 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 ${}_N\!\sim = \sim_N$.

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 $a \in G$ 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 $\operatorname{sgn} : S_n \to \{-1,1\}$ ist A_n ein Normalteiler von S_n.

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

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

1.3.12 Bemerkung Wird eine Untergruppe einer Gruppe in einer Weise definiert, die offensichtlich nur auf die Gruppenstruktur Bezug nimmt, so ist nach 1.2.6 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 1.2.6 ist klar, dass $Z(G)$ sogar eine charakteristische Untergruppe der Gruppe G ist. Insbesondere ist $Z(G) \triangleleft G$. Letzteres folgt auch mit 1.3.7(h), denn $Z(G)$ ist der Kern des Gruppenhomomorphismus $G \to \mathrm{Aut}(G),\ a \mapsto c_a$, dessen Bild übrigens $\mathrm{Inn}(G)$ ist.

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:

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

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

Zur Existenz (Wohldefiniertheit) von $\overline{f}$: Seien $a, b \in G$ mit $\overline{a}^N = \overline{b}^N$, das heißt $a \equiv_N b$. 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, denn: 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 $\overline{f}\left(\overline{a}^N\overline{b}^N\right) \overset{1.3.2}{=} \overline{f}\left(\overline{ab}^N\right) = f(ab) = f(a)f(b) = \overline{f}\left(\overline{a}^N\right)\overline{f}\left(\overline{b}^N\right)$.

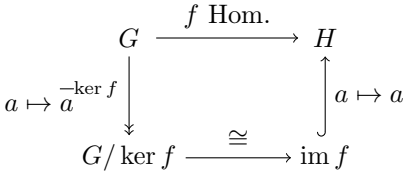
$$\begin{aligned} \overline{f} \text{ injektiv} &\iff \ker \overline{f} = \{1\} \iff \{\overline{a}^N \mid f(a) = 1\} = \{1\} \iff \forall a \in \ker f : \overline{a}^N = \overline{1}^N \\ &\iff \ker f \subseteq N \iff \ker f = N \\ \overline{f} \text{ surjektiv} &\iff H = \operatorname{im} \overline{f}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

□

1.3.16 Isomorphiesatz für Gruppen Seien G und H Gruppen und $f : G \to H$ ein Homomorphismus. Dann ist $N := \ker(f) \triangleleft G$ und $\overline{f} : G/N \to \operatorname{im}(f)$ definiert durch $\overline{f}\left(\overline{a}^N\right) = f(a)$ für $a \in G$ ein Isomorphismus. Insbesondere $G/\ker(f) \cong \operatorname{im}(f)$.

Beweis. Direkte Folgerung aus dem Homomorphiesatz. □

1.3.17 Bemerkung Der Isomorphiesatz klärt uns über die Natur von Homomorphismen auf:



Drei Phasen:

G	$\twoheadrightarrow$	$G/\ker f$	„vergröbern“
$G/\ker f$	$\xrightarrow{\cong}$	$\operatorname{im} f$	„umbenennen“
$\operatorname{im} f$	$\hookrightarrow$	H	„erweitern“

1.3.18 Beispiel

(a) $D_n/C_n \cong C_2$ für $n \geq 3$

$S_n/A_n \cong C_2$ für $n \geq 2$

$\mathrm{GL}_n(R)/\mathrm{SL}_n(R) \cong R^\times$ für $n \geq 1$, R kommutativer Ring

$O_n/\mathrm{SO}_n \cong C_2$ für $n \geq 1$

(b) Ist G eine Gruppe, so $G/Z(G) \cong \mathrm{Inn}(G)$ nach 1.3.14 und dem Isomorphiesatz.

1.3.19 Proposition und Definition Sei G ein Gruppe und $H \leq G$. Dann sind folgende Abbildungen bijektiv:

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}l} H & \to & Ha, & h & \mapsto & ha & \text{für alle } a \in G \\ H & \to & aH, & h & \mapsto & ah & \text{für alle } a \in G \\ G/_H\sim & \to & G/\sim_H, & Ha & \mapsto & a^{-1}H & \text{für alle } a \in G \end{array}$$

Man nennt $[G : H] := \#G/_H\sim = \#G/\sim_H \in \mathbb{N} \cup \{\infty\}$ den *Index* von H in G. Ist G endlich, so gilt der Satz von Lagrange:

$$[G : H] \cdot \#H = \#G$$

Beweis. Sei $a \in G$. Offensichtlich ist $H \to Ha,\ h \mapsto ha$ surjektiv. Um zu zeigen, dass diese Abbildung auch injektiv ist, seien $h, h' \in H$ mit $ha = h'a$. Dann $h = haa^{-1} = h'aa^{-1} = h'$. Also ist $H \to Ha$ bijektiv. Analog zeigt man $H \to aH$ bijektiv. Nach 1.3.4 gilt ${}^H\widetilde{a} = Ha$ und $\widetilde{a}^H = aH$ für $a \in G$.

Es ist $f : G/_H\sim \to G/\sim_H,\ Ha \mapsto a^{-1}H$ wohldefiniert und injektiv, denn für $a, b \in G$ gilt $Ha = Hb \iff ba^{-1} \in H \iff ab^{-1} \in H \iff a^{-1}H = b^{-1}H$. Der Rest folgt nun aus der Tatsache, dass $G/_H\sim$ eine Zerlegung von G in $[G : H]$ viele gleich große Äquivalenzklassen ist. □

1.3.20 Definition Sei G eine Gruppe und $a \in G$. Es heißt

$$\mathrm{ord}(a) := \inf\{n \in \mathbb{N} \mid a^n = 1\} \in \mathbb{N} \cup \{\infty\}$$

die *Ordnung* von a in G.

1.3.21 Proposition Sei G eine Gruppe und $a \in G$ mit $\mathrm{ord}(a) < \infty$. Dann $\langle a\rangle = \{1, a, ..., a^{\mathrm{ord}(a)-1}\}$ und $\#\langle a\rangle = \mathrm{ord}(a)$. Ist G endlich, so ist die Ordnung von a ein Teiler der Ordnung von G.

Beweis.

„$\supseteq$“ ist klar.

„$\subseteq$“ folgt aus $\{1, a, ..., a^{\mathrm{ord}(a)-1}\} \leq G$. $\#\{1, a, ..., a^{\mathrm{ord}(a)-1}\} = \mathrm{ord}(a)$, denn sonst $a^i = a^j$ für gewisse $i, j \in \{0, ..., \mathrm{ord}(a) - 1\}$ und $i < j$, was $a^{j-i} = 1$ und somit $\mathrm{ord}(a) \leq j - i < \mathrm{ord}(a)$ nach sich zöge.

Also nach 1.3.19 $[G : \langle a\rangle] \cdot \mathrm{ord}(a) = \#G$, falls G endlich. □

1.3.22 Definition Eine Gruppe ist *zyklisch*, wenn es $n \in \mathbb{N}$ mit $G \cong C_n$ gibt oder wenn $G \cong (\mathbb{Z}, +)$.

1.3.23 Proposition Eine Gruppe G ist zyklisch genau dann, wenn sie von einem Element erzeugt wird, das heißt, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt.

Beweis.

„$\Longleftarrow$“ ist klar.

„$\Longrightarrow$“ Ist $\mathrm{ord}(a) < \infty$, so $\langle a \rangle \cong C_{\mathrm{ord}(a)}$ nach 1.3.21. Ist $\mathrm{ord}(a) = \infty$, so $\mathbb{Z} \xrightarrow{\cong} \langle a \rangle,\ n \longmapsto a^n$.

---

§ 1.4 Semidirekte Produkte

1.4.1 Notation und Proposition Sei G eine Gruppe, $N \lhd G$ und $H \leq G$. Mit

$$NH := \{ab \mid a \in N,\ b \in H\} \text{ und } HN := \{ba \mid b \in H,\ a \in N\}$$

gilt dann

$$NH = \langle N \cup H \rangle = HN \leq G.$$

Beweis. Für $a, a' \in N$ und $b, b' \in H$ gilt

$$(ab)(a'b') = (a(\underbrace{ba'b^{-1}}_{\in N}))(\underbrace{bb'}_{\in H}) \in NH \tag{$\star$}$$

und

$$(ab)^{-1} = (\underbrace{b^{-1}a^{-1}b}_{\in N})b^{-1} \in NH. \tag{$\star\star$}$$

Zusammen mit $1 = 1 \cdot 1 \in NH$ zeigt dies $NH \leq G$. Somit $HN = H^{-1}N^{-1} = (NH)^{-1} = NH$. Schließlich $\langle N \cup H \rangle \subseteq NH$, da $N \cup H \subseteq NH \leq G$ und $NH \subseteq \langle N \cup H \rangle$. □

1.4.2 Definition Sei G eine Gruppe, $N \lhd G$ und $H \leq G$. Dann heißt die Gruppe G ein *semidirektes Produkt* ihres Normalteilers N und ihrer Untergruppe H, in Zeichen $G = N \rtimes H$, wenn $G = NH$ und $N \cap H = \{1\}$.

1.4.3 Beispiele

(a) Ist $\tau \in S_n$ eine Transposition, so gilt $S_n = A_n \rtimes \langle \tau \rangle$.

(b) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Dann:

$$\mathrm{GL}_n(R) = \mathrm{SL}_n(R) \rtimes \left\{ \begin{pmatrix} a & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix} \;\middle|\; a \in R^\times \right\}, \text{ falls } n \geq 1$$

$$\blacktriangleleft_n(R) = \triangleleft_n(R) \rtimes (\blacktriangleleft_n(R) \cap \blacktriangleright_n(R))$$

Beachte:

$$\begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \begin{pmatrix} b_1 & & * \\ & \ddots & \\ & & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & & * \\ & \ddots & \\ 0 & & a_n b_n \end{pmatrix}$$

für $a_i, b_i \in R$, weswegen $\blacktriangleleft_n(R) \to \blacktriangleleft_n(R) \cap \blacktriangleright_n(R)$,

$$\begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

ein Homomorphismus mit Kern $\triangleleft_n(R)$ ist.

(c) $O_n = \mathrm{SO}_n \rtimes \left\{ \begin{pmatrix} \pm 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \right\}$

(d) $D_n = C_n \rtimes \{1, R\}$ für alle $R \in D_n \setminus C_n$.

(e) $V = \{1, A\} \rtimes \{1, B\}$ für alle $A, B \in V$ mit $\#\{1, A, B\} = 3$, denn $\{1, A\} \lhd V$, da V abelsch, siehe 1.2.9(e), und $\langle 1, A, B\rangle = V$, da $[V : \langle 1, A, B\rangle] \cdot \#\langle 1, A, B\rangle = 4$.

1.4.4 Bemerkung Ist $G = N \rtimes H$, so hat man den Homomorphismus [→ 1.3.10 und 1.3.14]

$$\varphi : H \to \mathrm{Aut}(N),\ b \mapsto c_b|_N : N \to N.$$

Nach $(\star)$ aus 1.4.1 gilt dann $(ab)(a'b') = (a\varphi(b)a')(bb')$ für alle $a, a' \in N$ und $b, b' \in H$.

1.4.5 Definition und Satz Seien N und H Gruppen und $\varphi : H \to \mathrm{Aut}(N)$ ein Homomorphismus. Dann wird die Menge $N \times H$ vermöge $(a, b)(a', b') := (a\varphi(b)(a'), bb')$ $(a, a' \in N,\ b, b' \in H)$ eine Gruppe $N \rtimes_\varphi H$, die man das *semidirekte Produkt* der Gruppe N mit der Gruppe H bezüglich φ nennt.
Vermöge der Einbettung

$$N \to N \rtimes_\varphi H,\ a \mapsto (a, 1)$$

und

$$H \to N \rtimes_\varphi H,\ b \mapsto (1, b)$$

fasst man N und H oft als Untergruppe vom $N \rtimes_\varphi H$ auf.

Beweis. Nachweis der Gruppenaxiome:

(A) $((a, b)(a', b'))(a'', b'') = (a\varphi(b)(a'), bb')\,(a'', b'') = (a\varphi(b))(a')(\varphi(bb')(a''), b, b'b'') =$
$(a\varphi(b)(a'\varphi(b')(a'')), bb'b'') = (a, b)(a'\varphi(b')(a''), b'b'') = (a, b)((a', b')(a'', b''))$,
wobei $\varphi(bb')(a'') = \varphi(b)\varphi(b')(a'') = \varphi(b)(\varphi(b')(a''))$ für alle $(a, b), (a', b'), (a'', b'') \in N \times H$.

(N) $(1, 1)(a, b) = (1\varphi(1)(a), 1b) = (a, b)$ und $(a, b)(1, 1) = (a\varphi(b)(1), b1) = (a, b)$ für alle $(a, b) \in N \times H$.

(I) Wir zeigen $(a, b)(\varphi(b^{-1})(a^{-1}), b^{-1}) = (1, 1) = (\varphi(b^{-1})(a^{-1}), b^{-1})(a, b)$ für alle $(a, b) \in N \times H$, vergleiche $(\star\star)$ in 1.4.1.

Sei also $(a, b) \in N \times H$. Dann: $(a, b)(\varphi(b^{-1})(a^{-1}), b^{-1}) = (a\varphi(b)(\varphi(b^{-1})(a^{-1})), bb^{-1}) =$
$(a(\varphi(b)\varphi(b^{-1}))(a^{-1}), 1) = (a\varphi(bb^{-1})(a^{-1}), 1) = (a\varphi(bb^{-1})(a^{-1}), 1) = (1, 1)$ und
$(\varphi(b^{-1})(a^{-1}), b^{-1})(a, b) = (\varphi(b^{-1})(a^{-1})\varphi(b^{-1})(a^{-1}), bb^{-1}) = (\varphi(b^{-1})(a^{-1}a), 1) = (1, 1)$.

$N \to N \rtimes_\varphi H,\ a \mapsto (a, 1)$ und $H \to N \rtimes_\varphi H,\ b \mapsto (1, b)$ sind Einbettungen: $(a, 1)(a', 1) = (a\varphi(1)(a'), 1 \cdot 1) = (aa', 1)$ und $(1, b)(1, b') = (1\varphi(b)(1), bb') = (1, bb')$ für alle $a, a' \in N$ und $b, b' \in H$ und offensichtlich haben beide Abbildungen trivialen Kern $\ker = \{1\}$.

□

1.4.6 Satz Sei G eine Gruppe $N \leq G$, $H \leq G$ und $\varphi : H \to \mathrm{Aut}(N)$ ein Homomorphismus. Dann sind äquivalent:

(a) $N \lhd G$ und $G = N \rtimes H$ und $\forall b \in H : \varphi(b) = c_b|_N$.

(b) $N \rtimes_\varphi H \to G,\ (a, b) \mapsto ab$ ist ein Isomorphismus.

Beweis. Bezeichne f die Abbildung aus (b)
(a) $\Longrightarrow$ (b): Gelte (a). Für $(a,b),(a',b') \in N \rtimes_\varphi H$ gilt:

$$\begin{aligned} f\big((a,b),(a',b')\big) &= f\big(a\varphi(b)(a'),bb'\big) = a\varphi(b)(a')bb' = a\, c_b(a')bb' \\ &= aba'b^{-1}bb' = aba'b' = f(a,b)f(a',b'). \end{aligned}$$

Also ist f ein Homomorphismus. Wegen $G = NH$ ist f surjektiv und wegen $N \cap H = \{1\}$ ist f injektiv.
(b) $\Longrightarrow$ (a): Gelte (b). Es ist $N \times \{1\}$ der Kern des Homomorphismus $N \rtimes_\varphi H \to H,\ (a,b) \mapsto b$. Daher

$$N \times \{1\} \lhd N \rtimes_\varphi H \text{ und } N = f(N \times \{1\}) \overset{f \text{ Iso.}}{\lhd} G.$$

Weiter ist $G = NH$ wegen der Surjektivität und $N \cap H = \{1\}$ wegen der Injektivität von f. Also $G = N \rtimes H$. Schließlich

$$\begin{aligned} (\varphi(b)(a),b) = (1,b)(a,1) = f^{-1}(b)f^{-1}(a) &\overset{f \text{ Iso}}{\underset{1.2.4}{=}} f^{-1}(ba) \\ = f^{-1}((\underbrace{bab^{-1}}_{\in N})\underbrace{b}_{\in H}) &= (bab^{-1},b), \end{aligned}$$

insbesondere $\varphi(b)(a) = bab^{-1} = c_b(a)$ für alle $a \in N, b \in H$. Es folgt $\forall b \in H : \varphi(b) = c_b|_N$.

1.4.7 Beispiel Sei $n \in N, n \geq 3$. Dann:

$$D_n \cong C_n \rtimes_\varphi C_2, \text{ wobei } \varphi : C_2 \to \mathrm{Aut}(C_n),\ b \mapsto \begin{cases} \mathrm{id}_{C_n}, & \text{falls } b = 1, \\ \begin{pmatrix} C_n \to C_n \\ c \mapsto c^{-1} \end{pmatrix}, & \text{falls } b \neq 1. \end{cases}$$

Begründung: Nach Beispiel 1.4.3(d) ist $D_n = C_n \rtimes \{1,R\}$ für ein beliebiges $R \in D_n \setminus C_n$. Wie in 1.3.11(b):

$$c_R(A) = RAR^{-1} = RAR = A^{-1} \text{ für alle } A \in C_n$$

Nach 1.4.6 also $C_n \rtimes_\psi \{1,R\} \xrightarrow{\cong} D_n, (A,B) \mapsto AB$ mit

$$\psi : \{1,R\} \to \mathrm{Aut}(C_n),\ B \mapsto \begin{cases} \mathrm{id}_{C_n}, & \textit{falls } B = 1, \\ \begin{pmatrix} C_n \to C_n \\ A \mapsto A^{-1} \end{pmatrix}, & \textit{falls } B \neq 1. \end{cases}$$

Da die Konstruktion des semidirekten Produkts offenbar „strukturell" ist (die „Struktur" der resultierenden Gruppe hängt von der „Struktur" der Ausgangsgruppen und dem gegeben Homomorphismus ab, vergleiche 1.2.6), gilt $C_n \rtimes_\varphi C_2 \cong C_n \rtimes_\psi \{1,R\} \cong D_n$.

1.4.8 Korollar Sei G eine Gruppe $H \leq G$, $I \leq G$. Dann sind äquivalent:

(a) $HI = G$ und $H \cap I = \{1\}$ und $\forall a \in H\ \forall b \in I : ab = ba$

(b) $HI = G$ und $H \cap I = \{1\}$ und $H \lhd G$ und $I \lhd G$

(c) $H \times I \xrightarrow{\cong} G,\ (a,b) \mapsto ab$

Beweis.
(b) $\Longrightarrow$ (a): Gelte (b) und seien $a \in H$, $b \in I$. Zu zeigen $ab = ba$, das heißt $aba^{-1}b^{-1} = 1$. Es gilt:

$$aba^{-1}b^{-1} = (\underbrace{aba^{-1}}_{\in I})\underbrace{b^{-1}}_{\in I} = \underbrace{a}_{\in H}(\underbrace{ba^{-1}b^{-1}}_{\in H}) \in H \cap I = \{1\}$$

(a) $\Longrightarrow$ (c): Gelte (a). Nach Satz 1.4.6 angewandt auf $\varphi : I \to \mathrm{Aut}(H),\ b \mapsto \mathrm{id}_H$ ist zu zeigen:

1. $H \triangleleft G$
2. $G = HI$ und $H \cap I = \{1\}$. Dies folgt direkt aus (a).
3. $\forall b \in I : \mathrm{id}_H = c_b$. Dies ist äquivalent zu $\forall a \in H\ \forall b \in I : a = bab^{-1}$ und folgt auch aus (a).

Noch zu zeigen: $H \triangleleft G$. Sei $h \in H$ und $g \in G$. Zu zeigen: $ghg^{-1} \in H$. Wähle $a \in H$ und $b \in I$ mit $g = ab$. Dann $ghg^{-1} = abhb^{-1}a^{-1} \overset{(a)}{=} aa^{-1}bb^{-1}h = h \in H$.
(c) $\implies$ (b): Gelte (c). Da $f : H \times I \to G,\ (a, b) \mapsto ab$ surjektiv ist, gilt $HI = G$. Da f injektiv ist, gilt $H \cap I = \{1\}$. Wegen $H \times \{1\} \triangleleft H \times I$ und f Isomorphismus, ist $H = f(H \times \{1\}) \triangleleft G$. Analog $N \triangleleft G$. $\square$

§ 2 Ringe [→ LA §3]

§ 2.1 Definition und Beispiele

2.1.1 Definition Ein *Ring* ist ein Tripel $(R, +, \cdot)$, wobei $(R, +)$ eine abelsche Gruppe ist und $\cdot : R \times R \to R$ eine Abbildung mit folgenden Eigenschaften:

(D^+) $\forall a, b, c \in R : a(b + c) = (ab) + (ac)$

$({}^+D)$ $\forall a, b, c \in R : (a + b)c = (ac) + (bc)$

$(\dot{A})$ $\forall a, b, c \in R : (ab)c = a(bc)$

$(\dot{N})$ $\exists e \in R : \forall a \in R : ae = a = ea$

Es gibt genau ein neutrales Element bezüglich '$\cdot$', für das man oft nur '1' schreibt. Gilt zusätzlich

$(\dot{K})$ $\forall a, b \in R : ab = ba$,

so heißt $(R, +, \cdot)$ *kommutativ*. (Nicht „abelsch".)

2.1.2 Bemerkung

(a) Manchmal fordert man $(\dot{A})$ bzw. $(\dot{N})$ nicht und bezeichnet dann einen Ring $(R, +, \cdot)$ mit $(\dot{A})$ bzw. $(\dot{N})$ als *assoziativen* bzw. *unitären Ring* mit Eins.

(b) Sprachgebrauch: „Sei R ein Ring", statt: „Sei $(R, +, \cdot)$ ein Ring."

(c) Wegen (A) und $(\dot{A})$ kann man beim Addieren und Multiplizieren in einem Ring die Klammern weglassen. Notation für $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in R$:

$$\sum_{i=1}^{n} a_i = a_1 + \ldots + a_n, \quad \sum_{i=1}^{0} a_i = 0$$

$$\prod_{i=1}^{n} a_i = a_1 \cdot \ldots \cdot a_n, \quad \prod_{i=1}^{0} a_i = 1$$

(d) Konvention: „Punkt vor Strich."

(e) (D^+) besagt, dass für jedes $a \in R$ die Abbildung $R \to R,\ x \mapsto ax$ ein Gruppenhomomorphismus von $(R, +)$ nach $(R, +)$ ist. Daher $a \cdot 0 = 0$ und $a(-b) = -ab$ für alle $a, b \in R$. Analog für $({}^+D)$ und die Multiplikation von rechts zeigt man $0 \cdot a = 0$ und $(-a)b = -ab$ für alle $a, b \in R$.

(f) Sei R ein Ring, dann $\#R = 1 \iff 0 = 1 \in R$.

2.1.3 Definition und Proposition Sei $(R, +, \cdot)$ ein Ring. Elemente von

$$R^\times := \{a \in R \mid \exists b \in R : ab = 1 = ab\}$$

nennt man *Einheiten* oder *invertierbare Elemente* von R. Es ist $(R^\times, \cdot)$ mit $R^\times \times R^\times \to R^\times,\ (a, b) \mapsto ab$ eine Gruppe, die sogenannte *Einheitengruppe* oder *multiplikative Gruppe* von R.

Beweis. Einfach. Vergleiche [→ LA § 4.1]. □

2.1.4 Beispiel

(a) Für jeden Vektorraum V ist die Menge $\mathrm{End}(V) = \{f \mid f : V \to V \text{ linear}\}$ der Endomorphismen von V mit der punktweisen Addition und der Hintereinanderschaltung als Multiplikation ein Ring mit Einheitengruppe $\mathrm{End}(V)^\times = \mathrm{Aut}(V)$. [→ 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 $A \subseteq B$, $1_B \in A$, $\forall a, b \in A : a +_A b = a +_B b$ und $\forall a, b \in A : a \cdot_A b = a \cdot_B b$.

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

2.1.7 Beispiel

(a) Sei R ein kommutativer Ring und $n \in \mathbb{N}_0$. Dann sind

$$\begin{aligned}
\blacktriangledown_R^{n\times n} &= \{A \in R^{n\times n} \mid A \text{ obere Dreiecksmatrix}\},\\
\blacktriangle_R^{n\times n} &= \{A \in R^{n\times n} \mid A \text{ untere Dreiecksmatrix}\},\\
\blacktriangle_R^{n\times n} \cap \blacktriangledown_R^{n\times n} &= \{A \in R^{n\times n} \mid A \text{ Diagonalmatrix}\}
\end{aligned}$$

Unterringe von $R^{n\times n}$ mit Einheitengruppen

$$\begin{aligned}
(\blacktriangledown_R^{n\times n})^\times &= \blacktriangledown_n(R),\\
(\blacktriangle_R^{n\times n})^\times &= \blacktriangle_n(R),\\
\left(\blacktriangle_R^{n\times n} \cap \blacktriangledown_R^{n\times n}\right)^\times &= \blacktriangledown_n(R) \cap \blacktriangle_n(R).
\end{aligned}$$

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

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 ist $\ker f$ 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 [→ § 1.3], [→ LA § 3.3] Sei R ein Ring. Eine *Kongruenzrelation* auf R ist eine Kongruenzrelation $\equiv$ auf der additiven Gruppe von R [→ 1.3.1], 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 $\overline{a} \cdot \overline{b} = \overline{ab}$ $(a, b \in A)$ 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 $\forall a \in R \ \forall b \in I : \{ab, ba\} \subseteq I$.

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: $\forall a \in A \ \forall b \in \overline{0} : \{ab, ba\} \subseteq \overline{0}$. 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 und 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

$$\overline{\varphi} : A/I \to B \quad \text{mit} \quad \overline{\varphi}(\overline{a}^I) = \varphi(a)$$

für alle $a \in A$. Diese Abbildung $\overline{\varphi}$ ist ein Homomorphismus. Weiter gelten:

$$\overline{\varphi} \text{ injektiv} \iff I = \ker \varphi$$

$$\overline{\varphi} \text{ surjektiv} \iff B = \operatorname{im} \varphi$$

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

$$\overline{\varphi}(1) = \overline{\varphi}(\overline{1}^I) = \varphi(1) = 1$$

und

$$\overline{\varphi}(\overline{a}^I \overline{b}^I) = \overline{\varphi}(\overline{ab}^I) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a}^I)\overline{\varphi}(\overline{b}^I)$$

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

$$\overline{\varphi} : A/\ker \varphi \to \operatorname{im} \varphi \quad \text{mit} \quad \overline{\varphi}(\overline{a}^{\ker \varphi}) = \varphi(a)$$

für $a \in A$ ein Isomorphismus. Insbesondere gilt $A/\ker \varphi \cong \operatorname{im} \varphi$.

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 und 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 $E \subseteq B$. $A[E] = \bigcup \{A[b] \mid n \in \mathbb{N}_0, b \in E\}$ 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 $\emptyset$. („Konstante Polynome“)

(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. In der Vorlesung, jedoch nicht im Skript. □

2.2.6 Proposition Sei A ein Unterring des kommutativen Ringes C und $E \subseteq C$ mit $C = A[E]$. Sei B ein weiterer Ring und seien $\varphi, \psi : C \to B$ Homomorphismen mit $\varphi|_{A \cup E} = \psi|_{A \cup E}$. Dann $\varphi = \psi$.

Beweis. $D := \{a \in C \mid \varphi(a) = \psi(a)\}$ ist ein Unterring von C, der $A \cup E$ enthält. Also $D = C$. □

2.2.7 Satz Sei A ein kommutativer Ring und $A[E]$ ein Polynomring über E. Sei B ein weiterer kommutativer Ring, $\varphi : A \to B$ ein Homomorphismus und $f : E \to B$ eine Abbildung. Dann gibt es genau einen Homomorphismus $\psi : A[E] \to B$ mit $\psi|_A = \varphi$ und $\psi|_E = f$.

Beweis. Da $A[E]$ ein Polynomring ist, ist

$$\begin{aligned} \psi : A[E] &\to B, \\ \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ |\alpha| \leq d}} a_\alpha X^\alpha &\mapsto \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ |\alpha| \leq d}} \varphi(a_\alpha) f(X_1)^{\alpha_1} ... f(X_n)^{\alpha_n} \end{aligned}$$

($n, d \in \mathbb{N}_0$, $X_1, ..., X_n \in E$ paarweise verschieden, $X = (X_1, ..., X_n)$, $a_\alpha \in A$ für $\alpha \in N_0^n$ mit $|\alpha| \leq d$) als Abbildung wohldefiniert. Man rechnet stur nach, dass ψ ein Homomorphismus ist. Die Eindeutigkeit folgt aus 2.2.6.

2.2.8 Korollar Sei A ein Unterring des kommutativen Ringes B, $A[E]$ ein Polynomring über A in E und $f : E \to B$ eine Abbildung. Dann gibt es genau einen Homomorphismus $\psi : A[E] \to B$ mit $\psi|_A = \mathrm{id}_A$ und $\psi|_E = f$.

2.2.9 Korollar Seien $A[E]$ und $A[F]$ Polynomringe über A in E bzw. F. Sei $f : E \to F$ eine Bijektion. Dann gibt es genau einen Isomorphismus $\psi : A[E] \to A[F]$ mit $\psi|_A = \mathrm{id}_A$ und $\psi|_E = f$.

Beweis. Eindeutigkeit ist klar mit 2.2.6. Nach 2.2.8 gibt es einen Homomorphismus $\varphi : A[E] \to A[F]$ und $\psi : A[F] \to A[E]$ mit $\varphi|_A = \psi|_A = \mathrm{id}_A$, $\varphi|_E = f$ und $\psi|_F = f^{-1}$. Dann ist $\psi \circ \varphi$ ein Endomorphismus von $A[E]$ mit $(\psi \circ \varphi)|_A = \mathrm{id}_A$ und $(\psi \circ \varphi)|_E = \mathrm{id}_E$. Mit 2.2.6 folgt $\psi \circ \varphi = \mathrm{id}_{A[E]}$ und analog $\varphi \circ \psi = \mathrm{id}_{A[F]}$. Daher sind φ und ψ bijektiv.

2.2.10 Notation und Definition Sei A ein kommutativer Ring mit $0 \neq 1$. Schreibt man $A[X_1, ..., X_n]$, so meint man dabei in aller Regel den (nach 2.2.8 im Wesentlichen eindeutig bestimmten und nach 2.2.5 existierenden) *Polynomring* über A in paarweise verschiedenen $X_1, ..., X_n$. (Allgemeiner $A[X_i \mid i \in I]$ für den Polynomring über A in $\{X_i \mid i \in I\}$ mit paarweise verschiedenen X_i $(i \in I)$.) Man nennt dann die X_i *Unbestimmte* oder *Variablen* und die Elemente von $A[X_1, ..., X_n]$ *Polynome*.

Jedes Polynom $p \in A[X_1, ..., X_n] \setminus \{0\}$ hat eine eindeutige Darstellung der Form

$$p = \sum_{k=0}^{d} \sum_{\substack{\alpha \in \mathbb{N}_0^n \\ |\alpha|=k}} a_\alpha \underline{X}^\alpha \qquad (*)$$

mit $\underline{X} := (X_1, ..., X_n)$ derart, dass $\sum_{|\alpha|=d} a_\alpha \underline{X}^\alpha \neq 0$. Es heißt dann d der *Grad* von p, in Zeichen $\deg(p)$ und $\sum_{|\alpha|=d} a_\alpha \underline{X}^\alpha$ die *Leitform* von p. Man setzt $\deg(0) := -\infty$.

Ist A ein Unterring des kommutativen Ringes B und $b_1, ..., b_n \in B$ und bezeichnet $\psi : A[X_1, ..., X_n] \to B$ den nach 2.2.8 eindeutig bestimmten Homomorphismus ψ mit $\psi|_A = \mathrm{id}_A$ und $\psi(X_i) = b_i$ für $i \in \{1, ..., n\}$ (*„Einsetzungshomomorphismus“*), so schreibt man meist $p(b_1, ..., b_n)$, statt $\psi(p)$, denn es gilt mit $(*)$ und $b := (b_1, ..., b_n)$: $p(b_1, ...b_n) = \sum_{k=0}^{d} \sum_{|\alpha|=k} a_\alpha b^\alpha$. Ähnlich für $A[X_i \mid i \in I]$.

2.2.11 Proposition Sei A ein kommutativer Ring mit $0 \neq 1$. Dann $A[X_1]...[X_n] \cong A[X_1, ..., X_n]$.

Beweis. Durch n-maliges Anwenden von 2.2.7 erhält man einen Homomorphpismus $\varphi : A[X_1]...[X_n] \to A[X_1, ..., X_n]$ mit $\varphi(X_i) = X_i$ für $i \in \{1, ..., n\}$. Durch Anwenden von 2.2.8 erhält man einen Homomorphismus $\psi : A[X_1, ..., X_n] \to A[X_1]...[X_n]$ mit $\psi(X_i) = X_i$ für $i \in \{1, ..., n\}$. Nach 2.2.6 gilt $\varphi \circ \psi = \mathrm{id}_{A[X_1,...,X_n]}$ und $\psi \circ \varphi = \mathrm{id}_{A[X_1]...[X_n]}$, vgl. Beweis von 2.2.9. Daher sind φ und ψ isomorph.

2.2.12 Bemerkung, Erinnerung und Definition Sei R ein kommutativer Ring. Die *Teilerrelation* auf R ist gegeben durch:

$$a|b :\iff \exists c \in \mathbb{R} : ac = b \quad (a, b \in R)$$

Für alle $a \in R$ gilt $a|0$, denn $a \cdot 0 = 0$. Daher sagt man nur dann, dass $a \in R$ ein *Nullteiler* in R ist, wenn es ein $c \in R \setminus \{0\}$ gibt, mit $ac = 0$. Ist $0 \neq 1$ in R, so ist 0 ein Nullteiler in R. Man sagt daher, dass R nullteilerfrei ist, wenn kein $a \in R \setminus \{0\}$ ein Nullteiler ist. Man nennt R einen *Integritätsring*, wenn R nullteilerfrei ist und $0 \neq 1$ in R gilt.

Man nennt R einen *Körper*, wenn $R^\times = R \setminus \{0\}$. [→ LA 4.1.4] Jeder Unterring eines Körper ist ein Integritätsring.

2.2.13 Proposition Ist A ein Integritätsring, so auch jeder Polynomring über A.

Beweis. Da in jedem Polynom nur endlich viele Variablen vorkommen, reicht es, $A[X_1, ..., X_n]$ zu betrachten. Dort ist es durch Betrachten der Leitkoeffizienten klar. □

2.2.14 Korollar Sei R ein Integritätsring und $p, q \in R[X_1, ..., X_n] \setminus \{0\}$. Dann ist die Leitform von pq gleich dem Produkt der Leitformen von p und q. Insbesondere gilt $\deg(pq) = \deg(p) + \deg(q)$.

§ 2.3 Ringe von Brüchen

2.3.1 Definition Sei R ein kommutativer Ring. Eine Menge $S \subseteq R$ heißt *multiplikativ*, wenn $1 \in S$ und $\forall s,t \in S : st \in S$.

2.3.2 Beispiel Sei R ein kommutativer Ring.

(a) Ist $a \in R$, so ist $\{a^n \mid n \in \mathbb{N}_0\}$ multiplikativ.

(b) $\{0,1\} \subseteq R$ ist multiplikativ.

(c) Die Nichtnullteiler von R (d.h. die Elemente von R, die keine Nullteiler von R sind) bilden eine multiplikative Menge in R.

(d) Die $R = \mathbb{Z}$ und $p \in \mathbb{P} := \{2,3,5,7,11,...\}$, so ist $\{n \in \mathbb{Z} \mid p \not| n\}$ multiplikativ. [→ LA 4.1.8]

2.3.3 Notation Ist R ein kommutativer Ring, $a \in R$ und $s \in R^\times$, so $\frac{a}{s} := s^{-1}a$.

2.3.4 Definition und Proposition Sei A ein Unterring des kommutativen Rings B und $S \subseteq A \cap B^\times$ multiplikativ. Dann ist

$$S^{-1}A := \left\{ \frac{a}{s} \;\middle|\; a \in A,\ s \in S \right\}$$

ein Unterring von B. Man nennt $S^{-1}A$ den Ring der Brüche mit Zählern aus A und Nennern aus S (oder Lokalisierung von A nach S) in B.

Beweis. Offenbar reicht es, zu zeigen, dass $S^{-1}A$ unter Addition und Multiplikation abgeschlossen ist. Seien hierzu $a,b \in A$, $s,t \in S$. Dann $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \in S^{-1}A$, denn $st\left(\frac{a}{s} + \frac{b}{t}\right) = at + bs$ und $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$, denn $st\frac{a}{s}\frac{b}{t} = ab$. □

2.3.5 Bemerkung Eine Einheit in einem kommutativen Ring ist niemals Nullteiler in diesem Ring (und damit auch in keinem Unterring). [Beachte: Im Nullring ist 0 eine Einheit, aber kein Nullteiler.] In der Situation von 2.3.4 enthält also S keine Nullteiler von B (und damit auch keine Nullteiler von A).

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

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. 2.3.2(c), 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 [→ 2.2.3] 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 K sind.

(b) Sei $E \subseteq L$. Es heißt L ein *Körper von rationalen Funktionen* über K in E, wenn $L = K[E]$ und E algebraisch unabhängig über K ist.

2.3.13 Proposition [→ 2.2.6] Sei $L|K$ eine Körpererweiterung und $E \subseteq L$ mit $L = K[E]$. Sei R ein Ring und seien $\varphi, \psi : L \to R$ Homomorphismen mit $\varphi|_{K \cup E} = \psi|_{K \cup E}$. Dann $\varphi = \psi$.

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

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 Ringhomomorphismus, so nennt man φ auch einen *Körperhomomorphismus*. In diesem Fall: 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 $a \in K^\times$.

2.3.15 Satz (vgl. 2.2.9) 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 2.2.9 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 $\operatorname{im} \psi$ ist ein Unterkörper von $K(F)$. 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. □

2.3.16 Notation und Sprechweise (vgl. 2.2.10) 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 2.3.5 und 2.3.9 existierenden) Körper der rationalen Funktionen in paarweise verschiedenen „unbestimmten“ $X_1, ..., X_n$.

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 2.3.5.

In diesem Fall (und allgemein) setzen wir $I_S := \{a \in A \mid \exists s \in S : sa = 0\}$. Es ist I_S ein Ideal von A, da 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 $\iota_S : A \to A_S,\ a \mapsto \overline{a}$ mit $\iota_S(S) \subseteq A_S^\times$ 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

$$(E) := \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; n \in \mathbb{N},\ a_i \in R,\ b_i \in E \right\}$$

das kleinste Ideal von R, welches E enthält. Man nennt es das von E (in R) *erzeugte Ideal* [→ LA 3.3.9], [→ LA 3.3.10]. Für $b_1, ..., b_n \in R$ schreibt man auch:

$$(b_1, ..., b_n) := (b_1, ..., b_n) = \left\{ \sum_{i=1}^{n} a_i b_i \;\middle|\; a_i \in R \right\}$$

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], [→ LA 10.2.2] oder [1, § 2.2, § 2.4].

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

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

und prim (in R), wenn

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

In einem Integritätsring ist jedes Primelement $\neq 0$ irreduzibel.

Die Äquivalenzrelation $\widehat{=}$ („*Assoziiertheit*“) 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 $\mathbb{P}_R \to \{a \in R \mid a \text{ prim},\ a \neq 0\}/\widehat{=},\ p \to \widehat{p}$ bijektiv. (Zum Beispiel $\mathbb{P}_\mathbb{Z} = \mathbb{P} = \{2, 3, 5, 7, 11, 13, ...\}$ 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, siehe [1, § 2.4].

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

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

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:

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

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 gelten:

(a) I Primideal $\iff$ R/I Integritätsring

(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

$$A \xrightarrow{\varphi} B \xrightarrow{b \to \bar{b}^{\mathfrak{q}}} B/\mathfrak{q}$$

und daher ein Homomorphismus. Nach Isomorphiesatz 2.1.17 ist $A/\ker\psi \cong \operatorname{im}\psi$. Es ist $\operatorname{im}\psi$ 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:

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

□

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 mit $\mathfrak{p} \subseteq I$. Zu zeigen: $I = \mathfrak{p}$ oder $I = R$. Wähle $p, a \in R$ mit $\mathfrak{p} = (p)$ und $I = (a)$. Die Bedingung $\mathfrak{p} \subseteq I$ 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.

2.4.9 Korollar Sei R ein Hauptidealring und $p \in R$ irreduzibel. Dann ist $R/(p)$ ein Körper.

Beweis. Wegen $0 = \overbrace{0}^{\notin R^\times} \cdot \overbrace{0}^{\notin R^\times}$ ist 0 nicht irreduzibel in R. Es ist $(p) \neq \{0\}$ ein Primideal von R nach 2.4.1 und 2.4.3. Nach 2.4.8 ist also (p) ein maximales Ideal von R, also $R/(p)$ ein Körper nach 2.4.4. □

2.4.10 Beispiel

(a) Ist $p \in \mathbb{P}$, so ist $\mathbb{Z}/(p)$ ein Körper. [→ LA 4.1.7]

(b) Ist K ein Körper und $p \in K[X]$ irreduzibel, so ist $K[X]/(p)$ ein Körper.

2.4.11 Satz Seien A und B kommutative Ringe und $\varphi : A \to B$ ein Epimorphismus. Die Zuordnungen

$$\begin{aligned} I &\mapsto \varphi(I) \\ \varphi^{-1}(J) &\hookleftarrow J \end{aligned}$$

vermitteln eine Bijektion zwischen der Menge der Ideale / Primideale / maximalen Ideale I von A mit $\ker(\varphi) \subseteq I$ und der Menge der Ideale / Primideale / maximalen Ideale von B.

Beweis. Übung. □

2.4.12 Satz Sei A ein kommutativer Ring und $S \subseteq A$ multiplikativ. Die Zuordnungen

$$\begin{aligned} \mathfrak{p} &\mapsto \overline{S}^{-1}\iota_s(\mathfrak{p}) := \left\{ \frac{\overline{a}}{\overline{s}} \;\middle|\; a \in \mathfrak{p},\ s \in S \right\} \\ \iota_s^{-1}(\mathfrak{q}) &\hookleftarrow \mathfrak{q} \end{aligned}$$

vermitteln eine Bijektion zwischen der Menge der Primideale $\mathfrak{p}$ von A mit $\mathfrak{p} \cap S = \emptyset$ und der Menge der Primideale von A_S [→ 2.3.17].

Beweis. Übung. □

2.4.13 Satz Jeder kommutative Ring außer dem Nullring bestitzt ein maximales Ideal.

Beweis. Wir benutzen das Lemma von Zorn, welches besagt, dass halbgeordnete Mengen, in der jede Kette eine obere Schranke besitzt, mindestens ein maximales Element besitzt. Genauer benutzen wir folgendes Korollar: Sei M eine durch Inklusion halbgeordnete nichtleere Menge von Mengen derart, dass für jede nichtleere Kette $C \subseteq M$ gilt: $\bigcup C \in M$. Dann besitzt M ein maximales Element. Noch genauer: Sei A ein kommutativer Ring und $M := \{I \mid I \text{ Ideal von A},\ 1 \notin I\}$. □

2.4.14 Korollar Sei R ein kommutativer Ring.

(a) Sei I ein Ideal von R mit $1 \notin I$. Dann gibt es ein maximales Ideal $\mathfrak{m}$ von R mit $I \subseteq \mathfrak{m}$.

(b) Sei $S \subseteq R$ multiplikativ mit $0 \notin S$. Dann gibt es ein Primideal $\mathfrak{p}$ von R mit $\mathfrak{p} \cap S = \emptyset$.

Beweis.

(a) Wegen $R/I \neq \{0\}$ gibt es ein max. Ideal J von R/I. Dann ist nach 2.4.11 $\mathfrak{m} := \{a \in R \mid \overline{a}^I \in J\}$ ein maximales Ideal von R. Offensichtlich gilt $I \subseteq \mathfrak{m}$.

(b) Wegen $0 \notin S$ ist $I_S := \{a \in A \mid \exists s \in S : sa = 0\}$ [→ 2.3.17] echt, also $R/I_S \neq \{0\}$ und damit $R_S \neq \{0\}$. Es besitzt R_S also ein maximales Ideal $\mathfrak{m}$. Dann ist nach 2.4.12 $\mathfrak{p} := \iota_s^{-1}(\mathfrak{m})$ ein Primideal von R mit $\mathfrak{p} \cap S = \emptyset$. □

2.4.15 Definition Sei I ein Ideal des kommutativen Ringes R. Dann heißt das Ideal

$$\sqrt{I} := \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ Primideal von R},\ I \subseteq \mathfrak{p}\}$$

das *Radikal* von I.

2.4.16 Beispiel $\sqrt{(X^2)} = (X)$ in $\mathbb{R}[X]$, denn (X) ist ein Primideal von $\mathbb{R}[X]$, vergleiche 2.4.7 und jedes Primideal von $\mathbb{R}[X]$, welches (X^2) enthält, enthält auch (X).
Genauso $\sqrt{(3)} = \sqrt{(9)} = \sqrt{(27)} = (3)$ in $\mathbb{Z}$.

2.4.17 Satz Sei I ein Ideal des kommutativen Ringes R. Dann $\sqrt{I} = \{a \in R \mid \exists n \in \mathbb{N}_0 : a^n \in I\}$.

Beweis. Nach 2.4.11 entsprechen die Primideale von R, die I enthalten, den Primidealen von P/I. Indem man R und I durch R/I und $\{0\}$ austauscht, reicht es daher zu zeigen, dass für jeden kommutativen Ring R gilt:

$$\bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ Primideal von } R\} = \{a \in R \mid \exists n \in \mathbb{N}_0 : a^n = 0\}$$

„$\supseteq$“ ist einfach.

„$\subseteq$“ Wir zeigen: Ist $a \in R$ mit $\forall n \in \mathbb{N} : a^n \neq 0$, so gibt es ein Primideal $\mathfrak{p}$ von R mit $a \notin \mathfrak{p}$. Sei hierzu $S := \{a^n \mid n \in \mathbb{N}_0\}$ und es gelte $0 \notin S$. Es ist $S \subseteq R$ multiplikativ [→ 2.3.2(a)]. Nach 2.4.14(b) gibt es ein Primideal $\mathfrak{p}$ von R mit $\mathfrak{p} \cap S = \emptyset$. □

---

§ 2.5 Der Satz von Gauß

2.5.1 Definition Sei K ein Körper. Dann heißt eine Funktion $v : K \to \mathbb{Z} \cup \{\infty\}$ eine *diskrete Bewertung* auf K, wenn $v(0) = \infty$, $v|_{K^\times}$ ein Gruppenhomomorphismus von $(K^\times, \cdot)$ nach $(\mathbb{Z}, +)$ ist und $v(a+b) \geq \min\{v(a), v(b)\}$ für alle $a, b \in K$ (oder äquivalent für alle $a, b \in K^\times$ mit $a + b \neq 0$).

2.5.2 Beispiel Sei K ein Körper. Dann ist die Gradbewertung $v_\infty : K(X) \to \mathbb{Z} \cup \{\infty\}$ durch

$$v_\infty\left(\frac{f}{g}\right) := \begin{cases} \infty, & \text{falls } f = 0 \text{ und } g \in K[X] \setminus \{0\}, \\ (\deg(g)) - (\deg(f)), & \text{falls } f, g \in K[X] \setminus \{0\}, \end{cases}$$

wohldefiniert und eine diskrete Bewertung auf $K[X]$.

Begründung: Benutze 2.2.14 für die Wohldefiniertheit. Dass $v_\infty(0) = \infty$ ist klar nach Definition und $v_\infty|_{K(X)^\times} : K(X)^\times \to \mathbb{Z}$ ein Homomorphismus ist klar. Sind $f, g, h \in K[X] \setminus \{0\}$ mit $f + g \neq 0$, so:

$$\begin{aligned} v_\infty\left(\frac{f}{h} + \frac{g}{h}\right) &= v_\infty\left(\frac{f+g}{h}\right) = \deg h - \deg(f+g) \\ &\geq \deg h - \max\{\deg f, \deg g\} = \min\{\deg h - \deg f, \deg h - \deg g\} \\ &= \min\left\{v_\infty\left(\frac{f}{h}\right), v_\infty\left(\frac{g}{h}\right)\right\} \end{aligned}$$

2.5.3 Notation, Proposition, Definition Sei R ein faktorieller Ring, $K := \mathrm{qf}(R)$. Bezeichne $\mathbb{Z}^{(\mathbb{P}_R)}$ die Menge der Funktionen $\alpha : \mathbb{P}_R \to \mathbb{Z}$, mit endlichem Träger $\mathrm{supp}(\alpha) := \{p \in \mathbb{P}_R \mid \alpha(p) \neq 0\}$. Für jedes $\alpha \in \mathbb{Z}^{(\mathbb{P}_R)}$ setze $\mathbb{P}_R^\alpha := \prod_{p \in \mathrm{supp}(\alpha)} p^{\alpha(p)} \in K^\times$. Dann gibt es zu jedem $a \in K^\times$ genau ein $(c_a, \alpha_a) \in R^\times \times \mathbb{Z}^{(\mathbb{P}_R)}$, mit $a = c_a \mathbb{P}_R^\alpha$. Für jedes $p \in \mathbb{P}_R$ ist die Abbildung

$$v_p : K \to \mathbb{Z} \cup \{\infty\},\ a \mapsto \begin{cases} \infty, & \text{falls } a = 0, \\ \alpha_a(p), & \text{falls } a \neq 0, \end{cases}$$

eine Bewertung auf K, genannt die p-Bewertung auf K.

Beweis. Übung. □

2.5.4 Beispiel In $\mathbb{Q} = \mathrm{qf}(\mathbb{Z})$ gilt $v_3\left(-\frac{189}{18}\right) = v_3\left((-1)\frac{3^3 \cdot 7}{3^2 \cdot 2}\right) = 3 - 2 = 1$.

2.5.5 Proposition und Definition Sei K ein Körper und v eine diskrete Bewertung auf K. Dann ist $\mathscr{O}_v := \{a \in K \mid v(a) \geq 0\}$ ein Unterring von K, genannt der *Bewertungsring* von v. Es gilt $\mathscr{O}_v^\times = \{a \in K \mid v(a) = 0\}$ und $\mathscr{O}_v$ hat genau ein maximales Ideal, nämlich $\mathfrak{m}_v := \{a \in K \mid v(a) > 0\}$. Man nennt $\mathfrak{m}_v$ das *maximale Ideal* von v und $\mathscr{O}_v/\mathfrak{m}_v$ den *Restklassenkörper* von v.

Beweis. Dass $\mathscr{O}_v$ ein Unterring von K ist und $\mathfrak{m}_v$ ein echtes Ideal ist, ist klar.
Zu zeigen: $\mathscr{O}_v^\times = \{a \in K \mid v(a) = 0\}$

- $\subseteq$ Sei $a \in \mathscr{O}_v^\times$. Wähle $b \in \mathscr{O}_v$ mit $ab = 1$. Dann sind $a, b \in K\backslash\{0\}$ und daher $0 = v(1) = v(ab) = v(a) + v(b)$. Wegen $v(a) \geq 0$ und $v(b) \geq 0$ folgt $v(a) = v(b) = 0$.
- $\supseteq$ Sei $a \in K$ mit $v(a) = 0$. Dann ist $a \in K^\times$ und $v(\frac{1}{a}) = -v(a) = 0$, also $a, \frac{1}{a} \in \mathscr{O}_v$ und somit $a \in \mathscr{O}_v^\times$.

Zu zeigen: $\mathfrak{m}_v$ ist das größte echte Ideal von $\mathscr{O}_v$. Sei I ein echtes Ideal von $\mathscr{O}_v$. Zu zeigen: $I \subseteq \mathfrak{m}_v$. Dies ist aber klar, da $I \subseteq \mathscr{O}_v\backslash\mathscr{O}_v^\times = \mathfrak{m}_v$. □

2.5.6 Beispiel Sei $p \in \mathbb{P}$. Betrachte die p-Bewertung $v := v_p$ auf $\mathbb{Q} = \mathrm{qf}(\mathbb{Z})$. Dann ist $\mathscr{O}_v = \{\frac{a}{s} \mid a \in \mathbb{Z},\ s \in \mathbb{N},\ p \nmid s\} = S^{-1}\mathbb{Z}$ mit $S := \{s \in \mathbb{N} \mid p \nmid s\}$ [→ 2.3.2(d)]. Weiter ist $\mathfrak{m}_v = \{\frac{pa}{s} \mid a \in \mathbb{Z},\ s \in \mathbb{N},\ p \nmid s\}$. Wir behaupten $\mathscr{O}_v/\mathfrak{m}_v \cong \mathbb{Z}/(p)$. Betrachte hierzu den Homomorphismus

$$\varphi : \mathbb{Z} \to \mathscr{O}_v/\mathfrak{m}_v,\ n \mapsto n := 1 + \cdots + 1$$

Wegen $p \in \ker\varphi$ liefert der Homomorphiesatz 2.1.16 den Homomorphismus

$$\psi : \mathbb{Z}/(p) \to \mathscr{O}_v/\mathfrak{m}_v,\ \overline{n}^{(p)} \mapsto n \quad (n \in \mathbb{Z})$$

Für alle $s \in \mathbb{N}$ mit $p \nmid s$ gilt

$$\overline{s}^{\mathfrak{m}_v} = s = \psi(\overline{s}^{(p)}) \in \psi((\mathbb{Z}/(p))^\times) \subseteq (\mathscr{O}_v/\mathfrak{m}_v)^\times$$

und daher

$$\overline{\left(\frac{a}{s}\right)}^{\mathfrak{m}_v} = \frac{\overline{a}^{\mathfrak{m}_v}}{\overline{s}^{\mathfrak{m}_v}} = \frac{\psi(\overline{a})}{\psi(\overline{s})} = \psi\left(\frac{\overline{a}}{\overline{s}}\right) \in \mathrm{im}\,\psi$$

für alle $a \in \mathbb{Z}$. Es folgt $\mathrm{im}\,\psi = \mathscr{O}_v/\mathfrak{m}_v$. Es ist also ψ ein surjektiver Körperhomomorphismus [→ 2.3.14(b)] und daher ein Isomorphismus.

2.5.7 Satz und Definition Sei K ein Körper und v eine diskrete Bewertung auf K. Dann gibt es genau eine diskrete Bewertung w auf $K(X)$ mit

$$w\left(\sum_{i=0}^{d} a_i X^i\right) = \min\{v(a_i) \mid i \in \{0, \ldots, d\}\}$$

für alle $d \in \mathbb{N}_0$ und $a_0, \ldots, a_d \in K$. Es gilt $w|_K = v$ und man nennt w die (klassische) *Gauß-Fortsetzung* von v.

Beweis. Übung. □

2.5.8 Notation und Definition Sei R ein faktorieller Ring und $K = \mathrm{qf}(R)$. Für jedes $p \in \mathbb{P}_R$ bezeichne $w_p : K(X) \to \mathbb{Z} \cup \{\infty\}$ die Gauß-Fortsetzung der p-Bewertung auf K. Dann heißt $f \in R[X]$ *primitiv*, wenn $w_p(f) = 0$ für alle $p \in \mathbb{P}_R$. [Oder äquivalent: Wenn 1 der größte gemeinsame Teiler aller Koeffizienten von f ist.]

2.5.9 Lemma von Gauß Sei R ein faktorieller Ring und $K := \mathrm{qf}(R)$.

(a) Seien $f, h \in K[X]$ und $g \in R[X]$ primitiv mit $f = gh$. Dann gelten:

$$f \in R[X] \iff h \in R[X]$$
$$f \text{ primitiv in } R[X] \iff h \text{ primitiv in } R[X]$$

(b) Sei $f \in R[X]$ mit $\deg f \geq 1$. Dann gilt:

$$f \text{ irreduzibel in } R[X] \implies f \text{ irreduzibel in } K[X]$$

(c) $\{p \mid \text{prim in } R[X]\} = \big\{p \mid \text{prim in } R\big\} \cup \big\{p \mid p \text{ prim in } K[X] \text{ und primitiv in } R[X]\big\}$

Beweis.

(a) $f \in R[X] \iff \forall p \in \mathbb{P}_R : w_p(f) \geq 0 \iff h \in R[X]$,
$f \in R[X]$ primitiv $\iff \forall p \in \mathbb{P}_R : w_p(f) = 0 \iff h \in R[X]$ primitiv

(b) Sei f irreduzibel in $R[X]$ und $g, h \in K[X]$ mit $f = gh$. Zu zeigen: $g \in K^\times$ oder $h \in K^\times$
Œ$g \in R[X]$ primitiv (beachte $f \neq 0$). Dann ist $h \in R[X]$ nach (a). Somit ist $g \in R[X]^\times = R^\times \subseteq K^\times$ oder $h \in R[X]^\times = R^\times \subseteq K^\times$.

(c) Für alle $p \in R$ gilt $R[X]/(p)_{R[X]} \cong (R/(p)_R)[X]$, denn der Homomorphismus $\varphi : R[X] \to (R/(p))[X]$ mit $\varphi(a) = \overline{a}$ für $a \in R$ und $\varphi(X) = X$ aus 2.2.7 ist surjektiv und hat den Kern $(p)_{R[X]}$, wie man leicht sieht. Mit 2.4.4(a) folgt

$$\forall p \in R : (p \text{ prim in } R[X] \iff p \text{ prim in } R) \qquad (\star)$$

Ist p prim in $K[X]$ und primitiv in $R[X]$, so hat der Homomorphismus $\varphi : R[X] \to K[X]/(p)$, $f \mapsto \overline{f}$ den Kern $(p)_{R[X]}$, denn sind $f \in R[X]$ und $g \in K[X]$ mit $f = gp$, so ist $g \in R[X]$ nach (a). Damit ist wegen $(\star)$ schon „$\supseteq$“ gezeigt.

Um „$\subseteq$“ zu zeigen, genügt es wegen $(\star)$, ein $p \in R[X] \backslash R$ zu betrachten, welches prim in $R[X]$ ist. Da $R[X]$ Integritätsring ist, ist p irreduzibel in $R[X]$. Nach (b) ist p irreduzibel in $K[X]$. Da $K[X]$ faktoriell ist (K ist ein Körper und daher ist $K[X]$ sogar ein Hauptidealring), ist p daher prim in $K[X]$. Wäre p nicht primitiv in $R[X]$, so gäbe es $a \in \mathbb{P}_R$ und $q \in R[X]$ mit $p = aq$ und es folgte $a \in R[X]^\times = R^\times$ oder $q \in R[X]^\times = R^\times$, was absurd ist.

□

2.5.10 Satz von Gauß Ist R ein faktorieller Ring, so auch jeder Polynomring über R.

Beweis. Nach 2.2.13 ist nur noch zu zeigen, dass jedes Element ungleich 0 des Polynomringes eine Primfaktorzerlegung besitzt. Da in jedem Polynom nur endlich viele Variablen vorkommen, reicht es zu $R[X_1, \ldots, X_n]$ zu betrachten, vgl. Anfang des Beweises von 2.5.9(c).

Nach 2.2.11 gilt aber $R[X_1, \ldots, X_n] \cong R[X_1][X_2] \ldots [X_n]$ und per Induktion reicht es $R[X]$ zu betrachten. Setze $K := \mathrm{qf}(R)$ und sei $f \in R[X] \backslash \{0\}$. Da $K[X]$ als Hauptidealring faktoriell ist, gibt es $a \in K^\times$, $n \in \mathbb{N}_0$ und $g_1, \ldots, g_n \in K[X]$ prim mit $f = ag_1 \cdots g_n$. Œ $g_1, \ldots, g_n$ primitiv und $a \in R$ nach 2.5.9(a).

Nach 2.5.9(c) sind nun $g_1, \ldots, g_n$ prim in $R[X]$, was zu einer Primfaktorzerlegung von f in $R[X]$ führt, wenn man a in R (und nach 2.5.9(c) damit in $R[X]$) in Primfaktoren zerlegt. □

§ 2.6 Irreduzibilitätskriterien

2.6.1 Satz (Reduktionskriterium) Sei R ein faktorieller Ring, $p \in R$ irreduzibel und $f \in R[X]$ ein Polynom mit $\deg f \geq 1$, dessen Leitkoeffizient nicht von p geteilt wird. Bezeichne $\varphi : R[X] \to (R/(p))[X]$ den Homomorphismus mit $\varphi(a) = \overline{a}$ für $a \in R$ und $\varphi(X) = X$. Dann gilt: Ist $\varphi(f)$ irreduzibel in $(R/(p))[X]$, so ist f irreduzibel in $\mathrm{qf}(R)[X]$.

Ist f zusätzlich primitiv in $R[X]$, so ist f irreduzibel in $R[X]$.

Beweis. Beachte, dass $R/(p)$ nach 2.4.1, 2.4.3 und 2.4.4(a) ein Integritätsring ist. Sei ab nun $\varphi(f)$ irreduzibel in $(R/(p))[X]$. Wegen der Voraussetzung $\deg f \geq 1$ ist f natürlich keine Einheit in $\mathrm{qf}(R)[X]$ und schon gar nicht in $R[X]$.

Sei nun zunächst f zusätzlich als primitiv in $R[X]$ vorausgesetzt. Um zu zeigen, dass f irreduzibel in $R[X]$ ist, seien $g, h \in R[X]$ mit $f = gh$. Zu zeigen: $g \in R[X]^\times = R^\times$ oder $h \in R[X]^\times = R^\times$. Es gilt $\varphi(f) = \varphi(g)\varphi(h)$. Wegen der Voraussetzung an den Leitkoeffizienten von f gilt $\deg \varphi(f) = \deg f$ und folglich $\deg \varphi(g) = \deg g$ und $\deg(\varphi(h)) = \deg h$. Aus der Irreduzibilität von $\varphi(f)$ erhalten wir aber Œ $\varphi(g) \in (R/(p))[X]^\times = (R/(p))^\times$, also $\deg g = \deg \varphi(g) = 0$. Somit $g \in R$ und daher $g \in R^\times$ wegen der Primitivität von f.

Im allgemeinen Fall schreiben wir $f = cf_0$ mit $c \in R$ und $f_0 \in R[X]$ primitiv. Es teilt p weder c noch den Leitkoeffizienten von f_0. Daher $\varphi(c) \in (R/(p))^\times$, denn $\varphi(f) = \varphi(c)\varphi(f_0)$ ist irreduzibel in $(R/(p))[X]$, aber $\varphi(f_0) \notin (R/(p))[X]^\times$, denn $\deg \varphi(f_0) = \deg \varphi(f) = \deg f \geq 1$. Deswegen ist mit $\varphi(f)$ auch $\varphi(f_0)$ irreduzibel. Dann ist aber f_0 nach dem schon Bewiesenen irreduzibel in $R[X]$. Wegen $\deg f_0 = \deg f \geq 1$ ist nach dem Lemma von Gauß 2.5.9(b) f_0 irreduzibel in $(\mathrm{qf}(R))[X]$. Wegen $c \in (\mathrm{qf}(R))^\times$ ist somit f irreduzibel in $(\mathrm{qf}(R))[X]$. □

2.6.2 Beispiel Es ist $f = 20X^3 + 6X^2 - 8X - 20$ irreduzibel in $\mathbb{Q}[X]$. Reduziert man nämlich die Koeffizienten modulo 3, genügt es zu zeigen, dass das Polynom $2X^3 + X + 1$ in $\mathbb{F}_3[X]$ irreduzibel ist, wobei $\mathbb{F}_3 = \mathbb{Z}/(3)$. Da dieses Polynom Grad 3 hat und $\mathbb{F}_3$ ein Körper ist, müsste es aber eine Nullstelle in $\mathbb{F}_3$ haben, wenn es in $\mathbb{F}_3$ reduzibel wäre, was man durch Einsetzen sofort ausschließt.

In $\mathbb{Z}[X]$ ist f dagegen reduzibel, denn $f = 2g$ mit $g := 10X^3 + 3X^2 - 4X - 10 \in \mathbb{Z}[X]$. Da g primitiv ist, zeigt man wieder mit Reduktion der Koeffizienten modulo 3 (der Leitkoeffizient darf nicht verschwinden), dass g sowohl in $\mathbb{Q}[X]$, als auch in $\mathbb{Z}[X]$ irreduzibel ist.

2.6.3 Satz (Kriterium von Eisenstein) Es sei R ein faktorieller Ring und $f := a_n X^n + ... + a_0 \in R[X]$ primitiv, $a_i \in R$. Weiter sei $p \in R$ prim und ein gemeinsamer Teiler von $a_0, \ldots, a_{n-1}$, aber p^2 kein Teiler von a_0. Dann ist f irreduzibel in $R[X]$ und in $(\mathrm{qf}(R))[X]$.

Beweis. Beachte zunächst, dass $p \neq 0$ ist (wegen $0 = 0^2$) und p nicht a_n teilt (insbesondere $\deg f \geq 1$), denn sonst wäre f nicht primitiv.

Wieder ist $R/(p)$ ein Integritätsring und wir bezeichnen mit $\varphi : R[X] \to (R/(p))[X]$ den Homomorphismus gegeben durch $\varphi(a) = \overline{a}$ für $a \in R$ und $\varphi(X) = X$. Nach dem Lemma von Gauß 2.5.9(b) reicht es zu zeigen, dass f irreduzibel in $R[X]$ ist. Wegen $\deg f \geq 1$ ist natürlich f keine Einheit von $R[X]$. Seien also $g, h \in R[X]$ mit $f = gh$. Zu zeigen ist nur noch, dass $g \in R[X]^\times = R^\times$ oder $h \in R[X]^\times = R^\times$ ist. Wegen der Primitivität von f in $R[X]$ reicht es aber $g \in R$ oder $h \in R$ zu zeigen.

Es gilt wieder $\varphi(f) = \varphi(g)\varphi(h)$ und wegen der Eigenschaft des Leitkoeffizienten von f hat man wieder $\deg \varphi(f) = \deg f$ und folglich $\deg \varphi(g) = \deg g$ und $\deg \varphi(h) = \deg h$. Somit reicht es $\varphi(g) \in R/(p)$ oder $\varphi(h) \in R/(p)$ zu zeigen.

Betrachte den Quotientenkörper $K := \mathrm{qf}(R/(p))$. Es ist $K[X]$ faktoriell (sogar ein Hauptidealring), weswegen aus $X^n \widehat{=} \varphi(g)\varphi(h)$ in $K[X]$ nun die Existenz eines $k \in \{0, \ldots, n\}$ mit $\varphi(g) \widehat{=} X^k$ und $\varphi(h) \widehat{=} X^{n-k}$ in $K[X]$ folgt. Ist $k \in \{0, n\}$, so sind wir fertig. Andernfalls wäre aber $\varphi(g)(0) = 0$ und $\varphi(h)(0) = 0$, also ist p ein Teiler sowohl von $g(0)$ als auch von $h(0)$. Dann wäre aber p^2 ein Teiler von $g(0)h(0) = f(0) = a_0$ im Widerspruch zur Voraussetzung. □

2.6.4 Beispiel

(a) Sei K ein Körper und $n \in \mathbb{N}$. Dann ist $X^n - Y$ irreduzibel in $K(Y)[X]$. Es ist nämlich Y prim im faktoriellen Ring $K[Y]$, $X^n - Y$ primitiv in $K[Y][X]$ und man kann das Kriterium von Eisenstein anwenden.

(b) Sei $p \in \mathbb{P}$. Dann ist das p-te Kreisteilungspolynom: $\Phi_p := X^{p-1} + \cdots + 1$ irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$.

---

§ 2.7 Hilbertscher Basissatz

2.7.1 Sprechweise Sei $(M, \preceq)$ eine halbgeordnete Menge. Man sagt $\left\{ \begin{array}{c} a_1 \preceq a_2 \preceq \dots \\ a_1 \succeq a_2 \succeq \dots \end{array} \right\}$ ist eine $\left\{ \begin{array}{c} \text{auf-} \\ \text{ab-} \end{array} \right\}$ steigende Kette in M und meint damit eine Folge $(a_n)_{n\in\mathbb{N}}$ in M mit $\forall n \in \mathbb{N} : \left\{ \begin{array}{c} a_n \preceq a_{n+1} \\ a_n \succeq a_{n+1} \end{array} \right\}$.

Beachte: $\{a_n \mid n \in \mathbb{N}\}$ *ist dann eine Kette, also eine halbgeordnete Teilmenge von* M.
Man sagt: Eine auf- oder absteigende Kette $(a_n)_{n\in\mathbb{N}}$ in M wird *stationär*, wenn es ein $k \in \mathbb{N}$ gibt mit $\forall n \in \mathbb{N} : (k \leq n \Rightarrow a_n = a_{k+n})$.

2.7.2 Proposition Sei $(M, \preceq)$ eine halbgeordnete Menge. Dann sind äquivalent:

(a) Jede aufsteigende Kette in M wird stationär.

(b) Jede nichtleere Teilmenge von M besitzt ein maximales Element.

2.7.3 Erinnerung Sei A ein Integritätsring. Dann ist A faktoriell genau dann, wenn in A jedes irreduzible Element prim ist und jede aufsteigende Kette von Hauptidealen in A stationär wird.

2.7.4 Definition Sei A ein kommutativer Ring. Dann heißt A *noethersch*, wenn in ihm jede aufsteigende Kette von Idealen stationär wird. Ein Ideal I von A heißt *endlich erzeugt* (e.e.), wenn es $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in A$ gibt mit $I = (a_1, \dots, a_n)$. [→ 2.4.1]

2.7.5 Proposition Sei A ein kommutativer Ring. Dann ist A noethersch genau dann, wenn in A jedes Ideal endlich erzeugt ist.

Beweis.
„$\Longrightarrow$“ zeigen wir durch Kontraposition: Es gebe in A ein Ideal I, welches nicht endlich erzeugt ist. Zu zeigen: Es gibt eine aufsteigende nicht stationäre Kette $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ von Idealen in A. Setze $I_0 := (0) \subseteq I$. Da I nicht endlich erzeugt ist, gilt $I_0 \subset I$, das heißt, dass es ein $a_1 \in I \backslash I_0$ gibt. Setze $I_1 := (a_1) \subseteq I$. Wieder gilt $I_1 \subset I$. Wähle $a_2 \in I \backslash I_1$ und setze $I_2 := (a_1, a_2) \subseteq I$. Setzt man diesen Prozess fort, so erhält man $I_k = (a_1, \dots, a_k) \subseteq I$ und $I_0 \subset I_1 \subset I_2 \subset \dots$.
„$\Longleftarrow$“: Sei in A jedes Ideal endlich erzeugt und $I_1 \subseteq I_2 \subseteq \dots$ eine Kette von Idealen von A. Zu zeigen: Diese aufsteigende Kette wird stationär. Betrachte hierzu $I := \bigcup\{I_k \mid k \in \mathbb{N}\}$ von A, weswegen es $a_1, \dots, a_m \in A$ mit $I = (a_1, \dots, a_m)$ gibt. Wähle $N \in \mathbb{N}$ mit $a_1, \dots, a_m \in I_N$. Dann folgt

$$\forall n \in \mathbb{N} : (n \geq N \implies I = (a_1, \dots, a_m) \subseteq I_N \subseteq I_n \subseteq I),$$

und daher $\forall n \in \mathbb{N} : (n \geq N \implies I_n = I)$. □

2.7.6 Beispiel Jeder Hauptidealring ist noethersch.

2.7.7 Proposition Sei A ein noetherscher kommutativer Ring.

a) Ist $I \subseteq A$ ein Ideal, so ist A/I noethersch.

b) Ist $S \subseteq A$ multiplikativ, so ist A_S noethersch.

Beweis: Übung. □

2.7.8 Hilbertscher Basissatz Sei A ein kommutativer Ring mit $0 \neq 1$. Dann gilt: A noethersch $\implies$ $A[X]$ noethersch.

Beweis. Wir zeigen die Kontraposition: Sei also $A[X]$ nicht noethersch. Zu zeigen: A ist nicht noethersch. Wähle ein Ideal J von $A[X]$, welches nicht endlich erzeugt ist. Dann gibt es eine Folge $(f_n)_{n\in\mathbb{N}}$ mit $f_n \in J\backslash(f_1,\ldots,f_{n-1})$ und $\deg(f_n) = \min\{\deg(g) \mid g \in J\backslash(f_1,\ldots,f_{n-1})\}$ für alle $n \in \mathbb{N}$. Für jedes $n \in \mathbb{N}$ bezeichne a_n den Leitkoeffizienten von f_n. Wir behaupten, dass $I := (\{a_n \mid n \in \mathbb{N}\})$ nicht endlich erzeugt in A ist. Andernfalls gäbe es ein $N \in \mathbb{N}$ mit $I = (a_1,\ldots,a_N)$, insbesondere $a_{N+1} = b_1a_1 + \ldots + b_Na_N$ für gewisse $b_1,\ldots,b_n \in A$. Setzte man dann $h := b_1f_1X^{d_1} + \cdots + b_Nf_NX^{d_N} \in (f_1,\ldots,f_N)$ mit

$$d_n := \deg f_{N+1} - \deg f_n \overset{!}{\geq} 0 \text{ für } n \in \{1,\ldots,N\},$$

so stimmten die Grade und die Leitkoeffizienten von f_{N+1} und h überein. Daher hätte $g := f_{N+1} - h \in J\backslash(f_1,\ldots,f_N)$ einen kleineren Grad als f_{N+1} im Widerspruch zur Wahl von f_{N+1}. □

2.7.9 Korollar Sei A ein noetherscher Unterring eines kommutativen Ringes B und $b_1,\ldots,b_n \in B$ mit $B = A[b_1,\ldots,b_n]$. Dann ist B noethersch.

Beweis. Ist $0 = 1$ in A, so auch in B und $B = A$ und es ist nichts zu zeigen. Also $0 \neq 1$ in A. Dann existiert der Polynomring $A[X_1,\ldots,X_n]$ und $\varphi : A[X_1,\ldots,X_n] \to A[b_1,\ldots,b_n]$, $f \mapsto f(b_1,\ldots,b_n)$ ist ein Epimorphismus. Nach dem Isomorphiesatz gilt $A[b_1,\ldots,b_n] \cong A[X_1,\ldots,X_n]/I$ mit $I = \ker\varphi$. Nach 2.7.7(a) reicht es daher zu zeigen, dass $A[X_1,\ldots,X_n] = A[X_1][X_2]\ldots[X_n]$ noethersch ist. Dies folgt durch Induktion aus dem Hilbertschen Basissatz 2.7.8. □

2.7.10 Beispiel $\mathbb{R}[X_i \mid i \in \mathbb{N}]$ ist nicht noethersch, denn $(\{X_i \mid i \in \mathbb{N}\})$ ist nicht endlich erzeugt.

---

§ 2.8 Der Chinesische Restsatz

2.8.1 Definition und Proposition Sei A ein kommutativer Ring, $n \in \mathbb{N}_0$ und $I_1,\ldots,I_n$ Ideale von A. Dann nennt man die Ideale

$$\sum_{k=1}^{n} I_k := I_1 + \cdots + I_n := \{a_1 + \cdots + a_n \mid a_1 \in I_1,\ldots,a_n \in I_n\} \qquad \text{und}$$

$$\prod_{k=1}^{n} I_k := I_1 \cdots I_n := (\{a_1 \cdots a_n \mid a_1 \in I_1,\ldots,a_n \in I_n\})$$

$$= \begin{cases} \left\{ \sum_{i=1}^{m} a_{i1} \cdots a_{in} \;\middle|\; a_{i1} \in I_1,\ldots,a_{in} \in I_n \right\}, & \text{falls } \geq 1, \\ A, & \text{falls } n = 0, \end{cases}$$

die *Summe* bzw. das *Produkt* der Ideale $I_1,\ldots,I_n$.

2.8.2 Beispiel Sei A ein kommutativer Ring.

(a) Ist $n \in \mathbb{N}_0$ und sind $a_1, \ldots, a_n \in A$, so ist $(a_1) + \cdots + (a_n) = (a_1, \ldots, a_n)$ und $(a_1) \cdots (a_n) = (a_1 \cdots a_n)$.

(b) Ist $n \in \mathbb{N}$ und sind $I_1, \ldots, I_n$ Ideale von A, so ist $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$, aber im Allgemeinen herrscht hier nicht Gleichheit. (Zum Beispiel $(2)(2) = (4) \subset (2) = (2) \cap (2)$ in $\mathbb{Z}$.)

2.8.3 Definition Sei A ein kommutativer Ring. Zwei Ideale I und J von A heißen *koprim*, wenn $1 \in I + J$.

2.8.4 Lemma Sei $n \in \mathbb{N}_0$ und $I_1, \ldots, I_n$ paarweise koprime Ideale des kommutativen Ringes A. Dann sind I_k und $\prod\limits_{j \neq k} I_j$ für alle $k \in \{1, \ldots, n\}$ koprim.

Beweis. Sei $k \in \{1, \ldots, n\}$. Wähle für alle $j \in \{1, \ldots, n\} \backslash \{k\}$ ein $a_j \in I_k$ und $b_j \in I_j$ mit $1 = a_j + b_j$. Dann ist:

$$1 = 1^{n-1} = \prod_{j \neq k} (a_j + b_j) \in I_k + \prod_{j \neq k} I_j$$

□

2.8.5 Chinesischer Restsatz Seien $n \in \mathbb{N}$ und $I_1, \ldots, I_n$ paarweise koprime Ideale des kommutativen Ringes A. Dann ist der Ringhomomorphismus

$$\begin{aligned} A &\to \prod_{k=1}^{n} A/I_k \\ a &\mapsto (\overline{a}^{I_1}, \ldots, \overline{a}^{I_n}) \end{aligned}$$

surjektiv mit Kern $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$. Insbesondere $A/(I_1 \cdots I_n) \cong A/I_1 \times \cdots \times A/I_n$.

Beweis. Per Induktion nach $n \in \mathbb{N}$:

$\underline{n = 1:}$ Trivial.

$\underline{n = 2:}$ Seien I und J koprime Ideale von A. Zu zeigen:

(a) $\forall b, c \in A\ \exists a \in A : (a \equiv_I b \wedge a \equiv_J c)$

(b) $IJ = I \cap J$

Wähle $i \in I$ und $j \in J$ mit $1 = i + j$.

(a) Seien $b, c \in A$. Setze $a := bj + ci$. Dann ist $a = bj + ci \underset{j \equiv 1}{\overset{i \equiv_I 0}{\equiv_I}} b$ und $a = bj + ci \underset{j \equiv 0}{\overset{i \equiv_I 0}{\equiv_J}} c$.

(b) „$\subseteq$“ ist klar.

„$\supseteq$“: Sei $a \in I \cap J$. Dann ist $a = 1a = (i + j)a = \underset{\in I \in J}{i\,a} + \underset{\in J \in I}{j\,a} \in IJ$.

$\underline{n - 1 \to n\ (n \geq 3)}$: Seien $I_1, \ldots, I_n$ paarweise koprime Ideale von A. Dann sind $I := I_1$ und $J := \prod_{k=2}^{n} I_k$ nach Lemma 2.8.4 koprim. Nach der Induktionsvoraussetzung gilt: $J = I_2 \cdots I_n = I_2 \cap \cdots \cap I_n$ und nach dem Fall $n = 2$ gilt $IJ = I \cap J$, woraus sich ergibt: $I_1 \cdots I_n = IJ = I \cap J = I_1 \cap I_2 \cap \cdots \cap I_n$.

Es ist klar, dass $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ der Kern von $A \to \prod_{k=1}^{n} A/I_k$, $a \mapsto (\overline{a}^{I_1}, \ldots, \overline{a}^{I_n})$ ist. Zu zeigen ist noch Surjektivität, das heißt $\forall b_1, \ldots, b_n \in A : \exists a \in A : (a \equiv_{I_2} b_1 \wedge \ldots \wedge a \equiv_{I_n} b_n)$. Seien also $b_1, \ldots, b_n \in A$. Nach Induktionsvoraussetzung gibt es ein $b \in A$ mit $b \equiv_{I_2} b_2 \wedge \ldots \wedge b \equiv_{I_n} b_n$. Nach dem Fall $n = 2$ gibt es $a \in A$ mit $a \equiv_{I_1} b_1$ und $a \equiv_J b$. Wegen $J \subseteq I_k$ folgt $a \equiv_{I_k} b$ für $k \in \{2, \ldots, n\}$ und daher $a \equiv_{I_k} b \equiv_{I_k} b_k$ für $k \in \{2, \ldots, n\}$. □

2.8.6 Korollar Seien $n \in \mathbb{N}_0$ und $p_1, \ldots, p_n$ paarweise nicht assoziierte irreduzible Elemente des Hauptidealringes A und $\alpha_1, \ldots \alpha_n \in \mathbb{N}_0$. Dann ist

$$\begin{aligned} A &\to \prod_{k=1}^{n} A/(p_k^{\alpha_k}) \\ a &\mapsto (\overline{a}^{(p_1^{\alpha_1})}, \ldots, \overline{a}^{(p_n^{a_n})}) \end{aligned}$$

surjektiv mit Kern $(p_1^{\alpha_1} \cdots p_n^{\alpha_n})$. Insbesondere ist $A/(p_1^{\alpha_1} \cdots p_n^{\alpha_n}) \cong A/(p_1^{\alpha_1}) \times \cdots \times A/(p_n^{\alpha_n})$.

Beweis. Mit dem Beispiel 2.8.2(a) und dem Chinesischen Restsatz 2.8.5 reicht es zu zeigen, dass die $(p_k^{\alpha_k})$ paarweise koprim sind. Da A ein Hauptidealring ist, gibt es ein $a \in A$ mit $(p_k^{\alpha_k}) + (p_l^{\alpha_l}) = (a)$. Dann ist a ein Teiler sowohl von $p_k^{\alpha_k}$ als auch von $p_l^{\alpha_l}$. Wegen $p_k \neq 0$ gilt $a \neq 0$, weswegen a eine Primfaktorzerlegung besitzt, in der dann jeder Primfaktor sowohl zu p_k als auch p_l assoziiert ist, womit es wegen $p_k \widehat{\neq} p_l$ gar keinen Primfaktor von a gibt. Daher ist $a \in A^\times$ und $(p_k^{\alpha_k}) + (p_l^{\alpha_l}) = (a) = A$. □

2.8.7 Korollar Seien $n \in \mathbb{N}_0$, $p_1, \ldots, p_n \in \mathbb{P} \subseteq \mathbb{Z}$ paarweise verschieden und $\alpha_1, \ldots, \alpha_n \in N_0$. Dann ist

$$C_{p_1^{\alpha_1}} \times \cdots \times C_{p_n^{\alpha_n}} \cong C_{p_1^{\alpha_1} \cdots p_n^{\alpha_n}}$$

und

$$(\mathbb{Z}/(p_1^{\alpha_1}))^\times \times \cdots \times (\mathbb{Z}/(p_n^{\alpha_n}))^\times \cong (\mathbb{Z}/(p_1^{\alpha_1} \cdots p_n^{\alpha_n}))^\times.$$

§ 3 Strukturtheorie von Gruppen

§ 3.1 Wirkungen

3.1.1 Definition Eine *Wirkung* (auch *Operation* oder *Aktion* genannt) einer Gruppe G auf einer Menge M ist eine (meist infix oder gar nicht notierte) Abbildung $\cdot : G \times M \to M$ mit $1 \cdot x = x$ für alle $x \in M$ und $(gh)x = g(hx)$ für alle $g, h \in G$ und $x \in M$.

- Gilt zusätzlich $\forall x, y \in M : \exists g \in G : gx = y$, so heißt diese Wirkung *transitiv*.
- Gilt $\forall g \in G : \forall x \in M : (gx = x \implies g = 1)$, so heißt sie *frei*.
- Gilt $\forall g \in G((\forall x \in M : gx = x) \implies g = 1)$, so heißt sie *treu*.

3.1.2 Sprechweise „G wirkt auf M (durch ...)“, heißt etwa: „Sei $\cdot : G \times M \to M$ eine Wirkung (definiert durch ...)“ und so weiter.

3.1.3 Beispiel

(a) Sei $n \in \mathbb{N}_0$. Dann wirkt S_n in natürlicher Weise (d.h. durch $\sigma \cdot k := \sigma(k)$ für $k \in \{1, \ldots, n\}$) transitiv und treu auf $\{1, \ldots, n\}$. Nur für $n \leq 2$ ist diese Wirkung frei.

(b) Sei $n \in \mathbb{N}_0$. Die Gruppen O_n und SO_n wirken in natürlicher Weise treu auf $\mathbb{R}^n$. Nur für $n = 0$ sind die Wirkungen transitiv bzw. frei. Diese beiden Gruppen wirken aber auch auf der Einheitssphäre des $\mathbb{R}^n$. Dort wirken sie transitiv.

(c) Sei $n \geq 3$ und

$$P_n := \left\{ \begin{pmatrix} \cos\left(\frac{k}{n} 2\pi\right) \\ \sin\left(\frac{k}{n} 2\pi\right) \end{pmatrix} \;\middle|\; k \in \{0, \ldots, n-1\} \right\}.$$

Dann wirken C_n und D_n transitiv und treu auf P_n. Sie wirken auch treu auf dem Einheitskreis $S^1 \subseteq \mathbb{R}^2$, aber nicht transitiv. C_n wirkt frei auf P_n und auf S^1, D_n nicht.

(d) Jede Gruppe G wirkt auf ihre Trägermenge durch Linkstranslation, das heißt: $G \times G \to G$, $(g, x) \mapsto gx$ ist eine Wirkung. Diese Wirkung ist treu, frei und transitiv. Ebenso für die Wirkung durch Rechtstranslation: $G \times G \to G$, $(g, x) \mapsto xg^{-1}$ ist eine Wirkung. (Diese Wirkung ist treu, frei und transitiv.)

(e) Jede Gruppe G wirkt auf G durch Konjugation, d.h. $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$ ist eine Wirkung.

3.1.4 Satz Sei G eine Gruppe und M eine Menge. Die Zuordnungen

$$\cdot \mapsto \begin{pmatrix} G & \to & S_M \\ g & \mapsto & \begin{pmatrix} M & \to & M \\ x & \mapsto & g \cdot x \end{pmatrix} \end{pmatrix}$$

$$\begin{pmatrix} G \times M & \to & M \\ (g, x) & \mapsto & (\varphi(g))(x) \end{pmatrix} \hookleftarrow \varphi$$

vermitteln eine Bijektion zwischen der Menge der Wirkungen von G auf M und der Menge der Gruppenhomomorphismen von G nach S_M. [→ 1.1.4(a)]

Beweis. Übung. □

3.1.5 Beispiel Eine Gruppenwirkung von G auf M ist treu genau dann, wenn sie aufgefasst als Homomorphismus $G \to S_M$ injektiv ist.

3.1.6 Definition Die Gruppe G wirke auf der Menge M. Wir definierten dann eine Äquivalenzrelation $\sim$ auf M durch

$$x \sim y :\iff \exists g \in G : gx = y \qquad (x, y \in M)$$

Die Äquivalenzklassen

$$\tilde{x} = \{y \in M \mid \exists g \in G : gx = y\} = \{gx \mid g \in G\} =: Gx$$

nennt man die *Bahn* (auch *Orbit*) von $x \in M$. Schreibe auch M/G statt $M/\sim$.

3.1.7 Beispiel $\mathbb{R}^n/O_n = \{\{x \in \mathbb{R}^n \mid ||x|| = r\} \mid r \in \mathbb{R}_{\geq 0}\} = \mathbb{R}^n/\operatorname{SO}_n$ für $n \geq 2$.

3.1.8 Definition G wirke auf M und es sei $x \in M$. Dann heißt $G_x := \{g \in G \mid gx = x\} \leq G$ *Stabilisator* von x.

3.1.9 Bahnengleichung Wirkt G auf der endlichen Menge M, so ist $\#M = \sum\limits_{B \in M/G} \#B$.

3.1.10 Bahnenformel Wirkt G auf M und ist $x \in M$, so ist

$$\begin{aligned} G/{\sim_{G_x}} = \{gG_x \mid g \in G\} &\to Gx \\ gG_x &\mapsto gx \end{aligned}$$

wohldefiniert und bijektiv [→ 1.3.4]. Ist zusätzlich G endlich, so folgt die *Bahnenformel*

$$(\#Gx)(\#G_x) = \#G,$$

insbesondere $\#Gx \mid \#G$ für alle $x \in M$ [→ 1.3.19].

Beweis. Seien $g, h \in G$. Dann ist $gG_x = hG_x \overset{1.3.19}{\iff} \tilde{g}^{G_x} = \tilde{h}^{G_x} \iff g \sim_{G_x} h \iff g^{-1}h \in G_x \iff (g^{-1}h)x = x \iff g^{-1}(hx) = x \iff hx = gx \iff gx = hx$. „$\Longrightarrow$“ ist die Wohldefiniertheit und „$\Longleftarrow$“ die Injektivität. □

3.1.11 Definition Wirkt G auf M, so nennt man die Elemente von $M^G := \{x \in M \mid \forall g \in G : gx = x\}$ die *Fixpunkte* dieser Wirkung (oder die *G-invarianten Elemente* von M).

3.1.12 Beispiel $\mathbb{R}^{n^{\mathrm{O}_n}} = \mathbb{R}^{n^{\mathrm{SO}_n}} = \{0\}$ für $n \geq 2$ [→ 3.1.7].

3.1.13 Fixpunktformel Die Gruppe G wirke auf der endlichen Menge M und es seien $Gx_1, \ldots, Gx_m$ ($x_i \in M$) genau diejenigen paarweise verschiedenen Bahnen, die nicht einelementig sind. Dann:

$$\#M = \#M^G + \sum_{i=1}^{m} [G : G_{x_i}]$$

Beweis. Dies ist klar mit der Bahnengleichung und der Bahnenformel. □

3.1.14 Definition Sei $p \in \mathbb{P}$. Eine endliche Gruppe G heißt *p-Gruppe*, wenn es ein $e \in \mathbb{N}_0$ gibt mit $\#G = p^e$.

3.1.15 Fixpunktsatz Wirkt eine p-Gruppe G ($p \in \mathbb{P}$) auf der endlichen Menge M, so gilt $\#M \equiv_{(p)} \#M^G$. Insbesondere besitzt M einen Fixpunkt, wenn p kein Teiler von $\#M$ ist.

Beweis. In der Fixpunktformel gilt $G_{x_i} \neq G$ (da sonst Gx_i einelementig ist) und nach dem Satz von Lagrange 1.3.19 $[G : G_{x_i}] \cdot \#G_{x_i} = \#G$ folgt, dass es $e_i \in \mathbb{N}$ gibt mit $[G : G_{x_i}] = p^{e_i}$ für $i \in \{1, \ldots, m\}$, denn $\mathbb{Z}$ ist faktoriell. □

3.1.16 Beispiel *Klassengleichung* Wie in 3.1.3(e) wirke G auf sich selber durch Konjugation. Der nach 3.1.4 dementsprechende Homomorphismus $G \to S_G$ ist

$$G \to \mathrm{Inn}(G) \lhd \mathrm{Aut}(G) \subseteq S_G,\ a \mapsto c_a$$

aus 1.3.14 (vgl. auch 1.3.10). Die Bahn $\{gxg^{-1} \mid g \in G\}$ von $x \in G$ wird *Konjugationsklasse* von x in G genannt. Die Fixpunkte sind genau die Elemente des Zentrums $Z(G)$ [→ 1.3.13]. Der Stabilisator von $x \in G$ ist in diesem Fall der sogenannte *Zentralisator* $Z_G(x) := \{a \in G \mid ax = xa\}$ von x in G. Die Fixpunktformel 3.1.13 wird zur sogenannten *Klassengleichung*.

3.1.17 Klassengleichung Sei G eine endliche Gruppe und seien $K_1, \ldots, K_r$ deren verschiedene Konjugationsklassen mit mindestens zwei Elementen sowie $a_i \in K_i$ für $i \in \{1, \ldots, r\}$. Dann ist:

$$\#G = \#Z(G) + \sum_{i=1}^{r} [G : Z_G(a_i)]$$

3.1.18 Korollar Ist G eine p-Gruppe ($p \in \mathbb{P}$), so gilt $\#Z(G) > 1$.

Beweis. Wäre $\#Z(G) = 1$, so wäre $\#G \equiv_{(p)} 1$. Widerspruch! □

---

§ 3.2 Der Satz von Sylow

3.2.1 Definition [→ 1.3.4] Sei G eine Gruppe. Zu $H \leq G$ und $I \leq G$ definieren wir eine Äquivalenzrelation ${}_H\sim_I$ auf G durch

$$a\ {}_H\sim_I\ b :\Longleftrightarrow\ \exists h \in H\ \exists i \in I : a = hbi \qquad (a, b \in G)$$

[Für ${}_H\sim$ und $\sim_I$ aus 1.3.4 gilt also $({}_H\sim) = ({}_H\sim_{\{1\}})$ und $(\sim_I) = ({}_{\{1\}}\sim_I)$.] Die Äquivalenzklassen ${}^{H\sim_I}a = \{hai \mid h \in H,\ i \in I\} =: HaI$ nennt man *Doppelnebenklassen* von H und I nach a ($a \in G$).

3.2.2 Lemma Seien G eine endliche Gruppe, $H, I \leq G$ und $Hg_1I, \ldots, Hg_mI$ ($g_i \in G$) die verschiedenen Doppelnebenklassen von H und I. Dann gilt:

$$\#G = \sum_{i=1}^{m} \frac{(\#H)(\#I)}{(\#(H \cap g_i I g_i^{-1}))}$$

Beweis. Die Doppelnebenklassen sind gerade die Bahnen der Wirkung von $H \times I$ auf G, die durch $(h, i)g := hgi^{-1}$ ($(h, i) \in H \times I$, $g \in G$) gegeben ist [→ 3.1.3(d),(e)]. Für den Stabilisator $(H \times I)g$ von $g \in G$ gilt

$$\begin{aligned}(H \times I)g &= \{(h, i) \in H \times I \mid hgi^{-1} = g\} \\ &= \{(h, i) \in H \times I \mid h = gig^{-1}\},\end{aligned}$$

also $\#((H \times I)g) = \#(H \cap gIg^{-1})$. Nun folgt alles aus der Bahnengleichung und Bahnenformel. □

3.2.3 Definition Sei G eine Gruppe. Eine Untergruppe von G, die eine p-Gruppe ist ($p \in \mathbb{P}$) nennt man eine *p-Untergruppe* von G. Ist G endlich mit $\#G = p^e q$ ($p \in \mathbb{P},\ e \in \mathbb{N}_0,\ q \in \mathbb{N},\ p \nmid q$) und $P \leq G$ mit $\#P = p^e$, so heißt P eine *p-Sylowgruppe* (oder *p-Sylowuntergruppe*) von G. Mit $\mathrm{Syl}_p(G)$ bezeichnen wir die Menge der p-Sylowgruppen von G ($p \in \mathbb{P}$).

3.2.4 Beispiel Sei $p \in \mathbb{P}$. Betrachte den Körper $\mathbb{F}_p := \mathbb{Z}/(p)$. Es gilt

$$\#\,\mathrm{GL}_n(\mathbb{F}_p) = (p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{n-1})$$

und daher ist

$$v_p(\#\,\mathrm{GL}_n(\mathbb{F}_p)) = 0 + 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2},$$

das heißt $\#\,\mathrm{GL}_n(\mathbb{F}_p) = p^{\frac{n(n-1)}{2}} q$ mit $q \in \mathbb{N},\ p \nmid q$.
Die Untergruppen

$$\diagdown_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & & \star \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathbb{F}_p^{n\times n} \right\} \qquad \text{und}$$

$$\diagup_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ \star & & 1 \end{pmatrix} \in \mathbb{F}_p^{n\times n} \right\} \qquad [\to 1.1.9(\mathrm{b})]$$

sind also wegen $\#\diagdown_n(\mathbb{F}_p) = p^{\frac{n(n-1)}{2}} = \#\diagup_n(\mathbb{F}_p)$ p-Sylowgruppen von $\mathrm{GL}_n(\mathbb{F}_p)$.

3.2.5 Lemma Sei G eine endliche Gruppe, $H \leq G$ und P eine p-Sylowgruppe von G. Dann gibt es ein $g \in G$ mit $H \cap gPg^{-1} \in \mathrm{Syl}_p(H)$.

Beweis. Seien $Hg_1P, \ldots, Hg_mP$ ($g_i \in G$) die verschiedenen Doppelnebenklassen von H und P. Nach Lemma 3.2.2 gilt

$$p \nmid [G : P] = \sum_{i=1}^{m} [H : (g_i P g_i^{-1} \cap H)],$$

also $p \nmid [H : (H \cap g_i P g_i^{-1})]$ für ein $i \in \{1, \ldots, m\}$. Wegen $c_{g_i} \in \mathrm{Aut}(G)$ ist $g_i P g_i^{-1} \in \mathrm{Syl}_p(G)$ und $H \cap g_i P g_i^{-1} \leq g_i P g_i^{-1}$ eine p-Gruppe. Somit $H \cap g_i P g_i^{-1} \in \mathrm{Syl}_p(H)$. □

3.2.6 Satz von Sylow Sei G eine endliche Gruppe, $p \in \mathbb{P}$ und $n_p := \#\,\mathrm{Syl}_p(G)$.

(a) Ist H eine p-Untergruppe von G (z.B. $H = \{1\}$), so gibt es $P \in \mathrm{Syl}_p(G)$ mit $H \leq P$.

(b) $\forall P, Q \in \mathrm{Syl}_p(G) : \exists g \in G : P = gQg^{-1}$

(c) $p \mid (n_p - 1)$ und $n_p \mid \#G$.

Beweis.

(a) Setze $n := \#G$. Nach dem Satz von Cayley 1.2.10 ist G isomorph zu einer Untergruppe von S_n. Nun ist aber S_n analog zu 1.2.9(d) isomorph zu einer Untergruppe von $\mathrm{GL}_n(\mathbb{F}_p)$. Insgesamt sei $\text{Œ}\, G \leq GL_n(\mathbb{F}_p)$.

Nun ist aber $\diagdown_n(\mathbb{F}_p) \in \mathrm{Syl}_p(\mathrm{GL}_n(\mathbb{F}_p))$ nach Beispiel 3.2.4 und nach Lemma 3.2.5 gibt es $A \in \mathrm{GL}_n(\mathbb{F}_p)$ mit $Q := G \cap A\diagdown_n(\mathbb{F}_p)A^{-1} \in \mathrm{Syl}_p(G)$. Sei jetzt $H \leq G$ eine p-Untergruppe. Wieder mit Lemma 3.2.5 gibt es $g \in G$ mit $H \cap gQg^{-1} \in \mathrm{Syl}_p(H)$. Da H eine p-Gruppe ist, folgt für $P := gQg^{-1}$, dass $H \cap P = H$,d.h. $H \leq P$.

(b) Sei $P, Q \in \mathrm{Syl}_p(G)$. Wähle mit 3.2.5 ein $g \in G$ mit $P \cap gQg^{-1} \in \mathrm{Syl}_p(P)$. Da P eine p-Gruppe ist, folgt $P \cap gQg^{-1} = P$, also $gQg^{-1} \supseteq P$. Wegen $\#(gQg^{-1}) = \#Q = \#P$ folgt $gQg^{-1} = P$.

(c) Nach (b) wirkt G durch Konjugation transitiv auf $\mathrm{Syl}_p(G)$. Nach (a) gilt $\mathrm{Syl}_p(G) \neq \emptyset$.

Wähle $P \in \mathrm{Syl}_p(G)$. Nach der Bahnenformel aus 3.1.10 gilt: $n_p := \#\mathrm{Syl}_p(G) = [G : H]$, wobei $H := \{g \in G \mid P = gPg^{-1}\}$ der Stabilisator von P ist. Mit dem Satz von Lagrange 1.3.19 folgt also $n_p = [G : H] \mid \#G$.

Seien $Hg_1P, \ldots, Hg_mP$ ($g_i \in G, g_1 = 1$) die verschiedenen Doppelnebenklassen von H und P. Nach Lemma 3.2.2 gilt:

$$n_p = [G : H] = \sum_{i=1}^{m} \frac{\#P}{\#(H \cap g_iPg_i^{-1})}$$

Als p-Gruppe ist $H \cap g_iPg_i^{-1}$ nach (a) in einer p-Sylowgruppe von H enthalten. Nach der Definition von H ist wegen (b) aber P die einzige p-Sylowgruppe von H, also ist $H \cap g_iPg_i^{-1} \subseteq P$. und daher $H \cap g_iPg_i^{-1} = P \cap g_iPg_i^{-1}$. Es folgt:

$$n_p = \sum_{i=0}^{m} \frac{\#P}{\#(P \cap g_iPg_i^{-1})} = 1 + \sum_{i=2}^{m} [P : P \cap g_iPg_i^{-1}]$$

Aber für $i \in \{2, \ldots, m\}$ ist p ein Teiler von $[P : P \cap g_iPg_i^{-1}]$, denn P ist eine p-Gruppe und $g_iPg_i^{-1} \neq P$. (Sonst ist $g_i \in H$ und $Hg_iP = HP = Hg_1P$. Widerspruch!)

□

3.2.7 Bemerkung Sei G eine endliche Gruppe und $p \in \mathbb{P}$.

(a) Da die Konjugation $c_a : G \to G$, $b \mapsto aba^{-1}$ für jedes $a \in G$ ein Automorphismus von G ist [→ 1.3.10], ist für jedes $P \in \mathrm{Syl}_p(G)$ auch $aPa^{-1} = c_a(P) \in \mathrm{Syl}_p(G)$. Daher wirkt G auf $\mathrm{Syl}_p(G)$ durch Konjugation, d.h. $G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$, $(g, P) \mapsto gPg^{-1}$ ist eine Wirkung. Teil (b) des Satzes von Sylow besagt, dass diese Wirkung transitiv ist.

(b) $\forall P \in \mathrm{Syl}_p(G) : (P \lhd G \iff \#\mathrm{Syl}_p(G) = 1)$

(c) Schreibe $\#G = p^e q$ mit $e \in \mathbb{N}_0$, $q \in \mathbb{N}$, $p \nmid q$. Aus 3.2.6(c) folgt dann für $n_p := \#\mathrm{Syl}_p(G)$ sogar $p \mid (n_p - 1)$ und $n_p \mid q$, denn $p \in \mathbb{P}$ und $p \nmid n_p$.

---

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

[„$\supseteq$“ ist 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 $N \lhd G$ 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

$$(x_1, ..., x_\ell) := \left(\begin{array}{l} \{1, ..., n\} \to \{1, ..., n\} \\ \\ \begin{array}{ccccc} & & x_1 & & \\ & \nearrow & & \searrow & \\ x_\ell & & & & x_2 \\ \uparrow & & & & \downarrow \\ \ddots & & & & x_3 \\ & \nwarrow & & \swarrow & \\ & & x_4 & & \end{array} \\ \\ x \mapsto x \text{ für } x \in \{1, ..., n\} \setminus \{x_1, ..., x_\ell\} \end{array} \right)$$

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

3.3.4 Proposition [→ 1.1.12] Sei $n \in \mathbb{N}_0$. Dann:

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

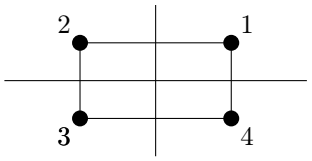
Beweis.

„$\supseteq$“: 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 $x_1, x_2, x_3 \in \{1, \ldots, n\}$ paarweise verschieden, so $(x_1\ x_2)(x_2\ x_3) = (x_1\ x_2\ x_3)$. Sind $x_1, x_2 \in \{1, \ldots, n\}$ 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

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



[→ 1.1.9(e)]

Beweis.

$\underline{S_n' \subseteq A_n}$: Nach 3.3.2(c) genügt es zu zeigen, dass S_n/A_n abelsch ist. Dies ist klar, da $S_n/A_n \cong C_2$ für $n \geq 2$ 1.3.18 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 $G^{(k)} \subseteq G_k$:
$\underline{k = 0:}$ $G^{(0)} = G = G_0$

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

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.

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

(b) Gelte $N \triangleleft G$. Durch Induktion zeigt man $(G/N)^{(n)} = (G^{(n)}N)/N$ für alle $n \in \mathbb{N}_0$ 1.4.1:
$\underline{n = 0:}$ $G/N = \underbrace{(GN)}_{=G}/N$
$\underline{n \to n+1 \ (n \in \mathbb{N}_0):}$

$$\begin{aligned}
(G/N)^{(n+1)} &= ((G/N)^{(n)})' \overset{\text{IV}}{=} ((G^{(n)}N)/N)' \\
&\overset{??}{=} \{[\overline{a_1 n_1}^N, \overline{a'_1 n'_1}^N] \cdots [\overline{a_m n_m}^N, \overline{a'_m n'_m}^N] \mid m \in \mathbb{N}_0,\ a_i, a'_i \in G^{(n)},\ n_i, n'_i \in \mathbb{N}\} \\
&= \{\overline{[a_1, a'_1] \cdots [a_m, a'_m]}^N \mid m \in \mathbb{N}_0,\ a_i, a'_i \in G^{(n)}\} \\
&\overset{??}{=} \{\overline{g}^N \mid g \in G^{(n+1)}\} = \{\overline{gn}^N \mid g \in G^{(n+1)},\ n \in N\} = (G^{(n+1)}N)/N
\end{aligned}$$

„$\Longrightarrow$“ 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 3.1.18 gilt $\#Z(G) > 1$. Nach dem Satz von Lagrange 1.3.19 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 3.3.9(b), dass auch G auflösbar ist. □

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

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

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

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

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 3.2.6(a) 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

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

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

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

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 *Körpergrad* oder *Grad* von L über K. (Nicht zu verwechseln mit dem Index aus 1.3.19!)

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 $\lambda_{ij} \in K$ $(1 \le i \le m, 1 \le j \le n)$ 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 $f \in K[X] \setminus \{0\}$ gibt mit $f(a) = 0$. (Das heißt, wenn a nicht algebraisch unabhängig über K ist, [→ 2.2.3(a)].) 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) $X \in K(X)$ 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 $f \in (\operatorname{irr}_K(a))$, das heißt, es gibt $g \in K[X]$ mit $f = g \operatorname{irr}_K(a)$. Da f irreduzibel ist, gilt $a \in K^\times$ oder $\operatorname{irr}_K(a) \in K^\times$. Letzteres ist unmöglich, also $g \in K^\times$ und sogar $g = 1$, da f und $\operatorname{irr}_K(a)$ beide normiert sind.
(a) $\Longleftrightarrow$ (d): Es reicht zu zeigen, dass für alle $g \in K[X]$ gilt: $g(a) = 0 \iff g(\lambda_a) = 0$ [→ 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 sei $a \in L$ algebraisch über K. Dann ist $K[X]/(\operatorname{irr}_K(a))$ ein Körper und $K[X]/(\operatorname{irr}_K(a)) \to K[a],\ \overline{f} \mapsto f(a)$ ein Isomorphismus. Insbesondere ist $K[a] = K(a)$ auch ein Körper und $\deg \operatorname{irr}_K(a) = [K(a) : K]$.

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

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

Da $\operatorname{irr}_K(a)$ irreduzibel im Hauptidealring $K[X]$ ist, ist $K[X]/(\operatorname{irr}_K(a))$ nach 2.4.9, siehe auch 2.4.10(b), ein Körper. Daher ist auch der dazu isomorphe Ring $K[a]$ ein Körper, das heißt $K[a] = K(a)$ [→ 2.3.11(b)].

Setzt man nun $d := \deg \operatorname{irr}_K(a)$, so bilden $\overline{1}, \overline{X}, ..., \overline{X}^{d-1}$ offensichtlich eine Basis des K-Vektorraumes $K[X]/(\operatorname{irr}_K(a))$ 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:

(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 mit 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 Zwischenkörper von $L|K$. Dann ist $L|K$ algebraisch genau dann, wenn $L|F$ und $F|K$ beide algebraisch sind [→ vgl. 4.1.5].

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 $a+b, a \cdot b \in \overline{K(a,b)}$ 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 $\operatorname{irr}_K(a) = f$.

Beweis. [Nach 4.1.10 ist klar, dass der gesuchte Körper, falls er existiert, isomorph zu $K[X]/(f)$ sein muss.] Es ist $L := K[X]/(f)$ nach 2.4.9 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 $\varphi : K[X] \xrightarrow{\cong} K'[X],\ b \mapsto \overline{b}\ (b \in K),\ X \mapsto X$.
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 [→ 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 [→ 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 [→ 2.2.10]

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

Wir zeigen $1 \notin I$ 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

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

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 2.4.14(a) ein maximales Ideal $\mathfrak{m}$ von A mit $I \subseteq \mathfrak{m}$. Dann ist $L := A/\mathfrak{m}$ nach 2.4.4(b) 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.

Zu (a): $L = K'\left[\overline{X}_f \mid f \in K[x] \setminus K\right] \subseteq \overline{K'}^L$, 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). □

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 von Steinitz 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 $\overline{\mathbb{Q}}^{\mathbb{C}}$ [→ 4.1.10] 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:

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

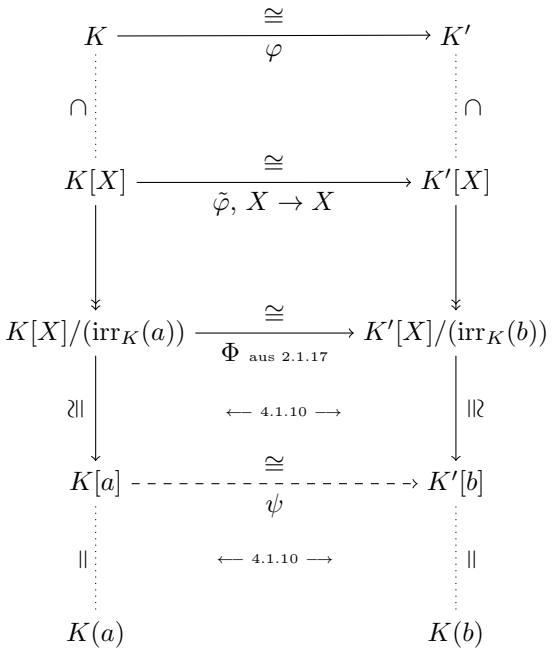
(b) *Entweder* ist sowohl a algebraisch über K als auch b über K' mit $\tilde{\varphi}(\mathrm{irr}_K(a)) = \mathrm{irr}_{K'}(b)$ *oder* weder a ist algebraisch über K noch b über K'.

Beweis.

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

(b) $\implies$ (a) Seien zunächst weder a algebraisch über K noch b über K'. Dann ist $K[a]$ (bzw. $K'[b]$) ein Polynomring über K (bzw. K') in der Unabhängigen a (bzw. b). Daher findet man einen Isomorphismus $\psi_0 : K[a] \to K'[b]$ 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 2.3.14(b)) 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:

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

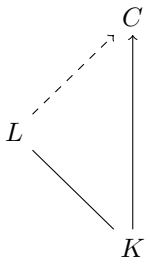
□

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 von 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 4.2.6(d), 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

$$L = K(\{a \in L \mid \exists\ f \in A : f(a) = 0\}).$$

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 von $\overline{L}'|K$, die ein Zerfällungskörper von A über K sind. Nach 4.3.6(b) 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 $L|K$.

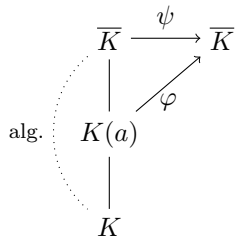
4.3.9 Definition Sei K ein Körper. Betrachte die natürliche Wirkung von $\mathrm{Aut}(\overline{K}|K)$ auf $\overline{K}$ und die dazugehörige Äquivalenzrelation $\sim_K$ auf $\overline{K}$, definiert durch $a \sim_K b :\iff \exists\, \varphi \in \mathrm{Aut}(\overline{K}|K) : \varphi(a) = b$ $(a, b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

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

Beweis. Nach 2.3.14(b) 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.
„$\Longleftarrow$“: 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 $A \subseteq K[X] \setminus \{0\}$ 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 4.3.6(b).
(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 $L = K(E)$.

4.3.15 Beispiel

(a) Nach dem Kriterium von Eisenstein 2.6.3 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' $\mathbb{Z} \to R,\ n \mapsto n \cdot 1$ als Ideal erzeugt, die *Charakterisitk* von R, in Zeichen $\operatorname{char} R$.

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 $\Phi_R : R \to R,\ a \mapsto a^p$ 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 2.5.3 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 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 $n = 0$. 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): Es 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:

$$\begin{aligned} p \nmid \mu(a, f) &\implies \mu(a, f') = \mu(a, f') = \mu(a, f) - 1 \\ p \mid \mu(a, f) &\implies \mu(a, f') = \mu(a, f') \geq \mu(a, f) \end{aligned}$$

[Beachte, dass für $p = 0$ gilt

$$\begin{aligned} p \nmid \mu(a, f) &\iff \mu(a, f) \geq 1 \iff f(a) = 0 && \text{und} \\ p \mid \mu(a, f) &\iff \mu(a, f) = 0 \iff f(a) \neq 0 && .] \end{aligned}$$

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 $\mu(a, f) \geq 2$.

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 endlichdimensionaler 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) $\Longrightarrow$ (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 1.3.21. Es folgt $a^{p^n} = a$ für alle $a \in K$. Es folgt $X^{p^n} - X = \prod_{a \in K}(X - a)$. Wegen $K = \mathbb{F}_p(K)$ folgt (b).
(b) $\Longrightarrow$ (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 $K \cong L \iff \#K = \#L$.

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 1.3.19 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 $\mathbb{F}_p$. Für jedes $n \in \mathbb{N}$ bezeichne $\mathbb{F}_{p^n}$ den nach 4.3.6(b) und 4.4.14 eindeutig bestimmten Zwischenkörper von $\overline{\mathbb{F}}_p|\mathbb{F}_p$ mit genau p^n Elementen.

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 $\operatorname{ord}(ab) = mn$. Wähle $s, t \in \mathbb{Z}$ mit $1 = sm + tn$. Ist $k \in \mathbb{Z}$ mit $(ab)^k = 1$, so gilt

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

und analog $1 = a^k$, woraus $m \mid k$ und $n \mid k$ folgt, das heißt $k \in (m) \cap (n) \overset{2.8.5}{=} (m)(n) \overset{2.8.2}{=} (mn)$. 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 2.4.9 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 4.4.15(b). □

---

§ 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:

$$f \text{ separabel} \iff \underset{K[X]}{\gcd}(f, f') = 1 \iff 1 \in (f, f')_{K[X]} \iff \underset{\overline{K}[X]}{\gcd}(f, f') = 1$$

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

(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 $b_i^{p^n} - a_i = 0$. □

4.5.6 Definition [→ 4.1.6] Sei $L|K$ eine Körpererweiterung. Dann heißt $a \in L$ *separabel* über K, wenn es ein separables $f \in K[X]$ gibt mit $f(a) = 0$. Es heißt $L|K$ *separabel*, wenn jedes Element von L separabel über K ist.

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

(a) a ist separabel über K.

(b) a ist algebraisch über K mit separablem Minimalpolynom.

Beweis.
(a) $\implies$ (b): Teiler von separablen Polynomen sind separabel.
(b) $\implies$ (a): Trivial. □

4.5.8 Beispiel

(a) Sei $p \in \mathbb{P}$. Nach dem Kriterium von Eisenstein 2.6.3 ist $F := X^p - T$ irreduzibel in $(\mathbb{F}_p(T))[X]$ und in $(qf(\mathbb{F}_p[T]))[X] = (\mathbb{F}_p(T))[X]$. Nach 4.5.5(b) ist f nicht separabel über $\mathbb{F}_p(T)$.

Wie in 4.5.5(c) gibt es aber ein irreduzibles, separables $g \in (\mathbb{F}_p(T))[X]$ und $n \in \mathbb{N}$ mit $f = g(X^{p^n})$, nämlich $g = X - T$ und $n = 1$.

Wählt man $a \in \overline{\mathbb{F}_p(T)}$ mit $a^p = T$, so $\mu(a, f) = p$. Es gilt $\mathrm{irr}_{\mathbb{F}_p(T)}(a) = f$. Nach 4.5.7 ist a also nicht separabel über $\mathbb{F}_p(T)$.

(b) Nach 4.5.5 und 4.5.7 ist jede algebraische Körpererweiterung in Charakteristik 0 separabel.

4.5.9 Lemma Ein Vektorrraum V über einem Körper mit mindestens m Elementen ($m \in \mathbb{N}_0$) ist niemals Vereinigung von m Untervektorräumen $\neq V$.

Beweis. Sei V ein K-Vektorraum, $m \in \mathbb{N}_0, U_1, ..., U_m \subsetneq V$ Untervektorräume von V mit $V = U_1 \cup ... \cup U_m$. Zu zeigen: $\#K \leq m - 1$.
Gelte ohne Einschränkung $U_1 \not\subseteq U_2 \cup ... \cup U_m$. Wähle $n \in U_1 \backslash (U_2 \cup ... \cup U_m)$. Wähle $v \in V \backslash U_1$. Keines der Elemente $\lambda u + v$ ($\lambda \in K$) ist in U_1 enthalten und es sind nicht zwei dieser Elemente in demselben U_i enthalten. Damit gibt es höchstens $m - 1$ dieser Elemente. Es folgt $\#K \leq m - 1$. □

4.5.10 Korollar Ein Vektorraum über einem unendlichen Körper ist niemals Vereinigung von endlich vielen Untervektorräumen $\neq V$.

4.5.11 Lemma Sei F ein Zwischenkörper der algebraischen Körpererweiterung $L|K$ und $\overline{K}$ ein algebraischer Abschluss von K. Seien $\varphi, \psi : F \to \overline{K}$ K-Homomorphismen. Dann gibt es eine Bijektion von $\{\tilde{\varphi} \mid \tilde{\varphi} : L \to \overline{K}\text{-Homomorphismus}\ ,\ \tilde{\varphi}|_F = \varphi\}$ nach $\{\tilde{\psi} \mid \tilde{\psi} : L \to \overline{K}\text{-Homomorphismus},\ \tilde{\psi}|_F = \psi\}$.

Beweis. Setze den Homomorphismus $\psi \circ \varphi^{-1} : \varphi(F) \to \overline{K}$ mit 4.2.16 fort zu einem Homomorphismus $\sigma : \overline{K} \to \overline{K}$. Nach 4.3.10 gilt $\sigma \in \mathrm{Aut}(\overline{K}|K)$.
Wir behaupten, dass die Zuordnungen $\tilde{\varphi} \mapsto \sigma \circ \tilde{\varphi}$ und $\tilde{\psi} \mapsto \sigma^{-1} \circ \tilde{\psi}$ eine wunschgemässe Bijektion vermitteln. Zu zeigen:

(a) Ist $\tilde{\varphi} : L \to \overline{K}$ ein Homomorphismus mit $\tilde{\varphi}|_F = \varphi$, so $(\sigma \circ \tilde{\varphi})|_F = \psi$ und $\sigma^{-1} \circ \sigma \circ \tilde{\varphi} = \tilde{\varphi}$

(b) Ist $\tilde{\psi} : L \to \overline{K}$ ein Homomorphismus mit $\tilde{\psi}|_F = \psi$, so $(\sigma^{-1} \circ \tilde{\psi})|_F = \varphi$ und $\sigma \circ \sigma^{-1} \circ \tilde{\psi} = \psi$.

Beides ist klar. □

4.5.12 Definition [→ 4.1.1] Sei $L|K$ eine algebraische Körpererweiterung und $\overline{K}$ ein algebraischer Abschluss von K. Dann heißt

$$[L : K]_s := \#\{\varphi \mid \varphi : L \to \overline{K} \text{ ist } K\text{-Homomorphismus}\} \in \mathbb{N} \cup \{\infty\}$$

der *Separabilitätsgrad* von $L|K$. [Beachte, dass $[L : K]_s$ nach 4.2.17 in der Tat ≥ 1 ist und wegen 4.2.18 nicht von gewähltem $\overline{K}$ abhängt.]

4.5.13 Proposition [→ 4.1.10] Sei $L|K$ eine Körpererweiterung und $a \in L$ algebraisch über K. Dann

$$\begin{aligned}[K(a) : K]_s &= \#\{b \in \overline{K(a)} \mid a \sim_K b\} \\ &= \#\{b \in \overline{K(a)} \mid (\mathrm{irr}_K(a))(b) = 0\}\end{aligned}$$

[→ 4.3.9, 4.3.11]. Setzt man $p := \mathrm{char}(K)$, so gibt es $n \in \mathbb{N}_0$ mit $[K(a) : K]_s \cdot p^n = [K(a) : K]$. Insbesondere gilt$[K(a) : K]_s = [K(a) : K]$, falls $p = 0$.

Beweis. Da $K(a)|K$ algebraisch ist, ist $\overline{K(a)}$ ein algebraischer Abschluss von K. Wir zeigen zunächst, dass

$$\{\varphi \mid \varphi : K(a) \to \overline{K(a)} \text{ ist } K\text{-Homomorphismus}\} \to \{b \in \overline{K(a)} \mid a \sim_k b\},\ \varphi \mapsto \varphi(a)$$

wohldefiniert und bijektiv ist. Wohldefiniertheit und Surjektivität folgen aus:

$$\begin{aligned}\{b \in \overline{K(a)} : a \sim_k b\} &\overset{4.3.11}{=} \{b \in \overline{K(a)} \mid \mathrm{irr}_K(a) = \mathrm{irr}_K(b)\} \\ &\overset{4.2.15}{=} \{b \in \overline{K(a)} \mid \exists\ K\text{-Isomorphismus } \psi : K(a) \to K(b) : \psi(a) = b\} \\ &= \{b \in \overline{K(a)} \mid \exists\ K\text{-Homomorphismus } \varphi : K(a) \to \overline{K(a)} : \varphi(a) = b\}\end{aligned}$$

Injektivität ist klar, da ein K-Homomorphismus $\varphi : K(a) \to \overline{K(a)}$ durch seinen Wert auf a eindeutig festgelegt ist.
Nun folgen

$$[K(a) : K]_s = \#\{b \in \overline{K(a)} \mid a \sim_K b\}$$

und

$$\{b \in \overline{K(a)} \mid a \sim_K b\} = \{b \in \overline{K(a)} \mid \mathrm{irr}_K(a) = \mathrm{irr}_K(b)\} \overset{4.1.9}{=} \{b \in \overline{K(a)} \mid (\mathrm{irr}_K(a))(b) = 0\}.$$

Nach 4.5.5(c) gibt es $n \in \mathbb{N}_0$ derart, dass für alle $b \in \overline{K(a)}$ mit $(\mathrm{irr}_K(a))(b) = 0$ gilt $\mu(b, \mathrm{irr}_k(a)) = p^n$, woraus

$$\#\{b \in \overline{K(a)} \mid (\mathrm{irr}_K(a))(b) = 0\} \cdot p^n = \deg(\mathrm{irr}_K(a)) \overset{4.1.10}{=} [K(a) : K]$$

folgt. □

4.5.14 Lemma Sei $L|K$ Körpererweiterung un $a \in L$. Dann gilt:

$$a \text{ separabel über } K \iff [K(a):K]_s = [K(a):K] < \infty$$

Beweis.
„$\Longrightarrow$“: Sei a separabel über K und $f := \mathrm{irr}_K(a)$. Dann ist nach 4.5.7 f separabel und

$$[K(a):K]_s \overset{4.5.13}{=} \#\{b \in \overline{K(a)} \mid f(b) = 0\} \overset{f \text{ sep.}}{=} \deg(f) \overset{4.1.10}{=} [K(a):K].$$

„$\Longleftarrow$“: Gelte $[K(a):K]_s = [K(a):K] < \infty$. Nach 4.1.13 ist a algebraisch über K. Wir zeigen, dass $f := \mathrm{irr}_K(a)$ separabel ist. Dies folgt aus:

$$\#\{b \in \overline{K(a)} \mid f(b) = 0\} \overset{4.5.12}{=} [K(a):K]_s = [K(a):K] \overset{4.1.10}{=} \deg(f)$$

□

4.5.15 Proposition [→ 4.1.15] Sei F ein Zwischenkörper der algebraischen Körpererweiterung $L|K$. Dann gilt

$$[L:K]_s < \infty \iff \big([L:K]_s < \infty \text{ und } [F:K]_s < \infty\big)$$

und falls $[L:K]_s < \infty$, so

$$[L:K]_s = [L:F]_s \cdot [F:K]_s.$$

Beweis. Ist $\varphi : F \to \overline{K}$ ein Homomorphismus, so gilt nach 4.5.11

$$\#\{\tilde{\varphi} \mid \tilde{\varphi} : L \to \overline{K} \text{ Homomorphimus}, \tilde{\varphi}|_F = \varphi\} = [L:F]_s,$$

denn man kann ohne Einschränkung $\overline{K} = \overline{F}$ nehmen und dann gilt mit $\psi := \mathrm{id}_F : F \to \overline{F}$, dass

$$\#\{\tilde{\psi} \mid \tilde{\psi} : L \to \overline{K},\ \tilde{\psi}|_F = \psi\} = \#\{\tilde{\psi} \mid \tilde{\psi} : L \to \overline{F}\ F\text{-Homomorphismus}\} \overset{4.5.12}{=} [L:F]_s.$$

Daraus folgt alles. □

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

(a) $L|K$ ist endlich und separabel.

(b) $[L:K]_s = [L:K] < \infty$

(c) Es gibt $n \in \mathbb{N}_0$ und über K separabel $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$. [→ 4.1.14]

(d) Es gibt ein über K separables $a \in L$ mit $L = K(a)$. [Man nennt a in dieser Situation oft ein *primitives Element* von $L|K$ und „$a \implies d$“ den *Satz vom primitiven Element.*]

Beweis.
(a) $\implies$ (c) Trivial.
(c) $\implies$ (b) Durch Induktion nach $n \in \mathbb{N}_0$ zeigen wir, dass für alle über K separablen $a_1, ..., a_n \in L$ gilt:

$$[K(a_1, ..., a_n):K]_S = [K(a_1, ..., a_n):K] < \infty$$

$n = 0$

$$[K:K]_S = 1 = [K:K]$$

$n - 1 \to n (n \in \mathbb{N})$

$$[K(a_1, ..., a_n):K]_S \overset{4.5.15}{=} [K(a_1, ..., a_n):K(a_1, ..., a_{n-1})]_S [K(a_1, ..., a_{n-1}):K]_S$$
$$\overset{4.5.14}{\underset{\text{IV}}{=}} [K(a_1, ..., a_n):K(a_1, ..., a_{n-1})][K(a_1, ..., a_{n-1}):K] \overset{4.1.5}{=} [K(a_1, ..., a_n):K] < \infty$$

(b) $\Longrightarrow$ (d) Gelte (b). Dann ist nach 4.5.14 jedes $a \in L$ mit $L = K(a)$ automatisch separabel über K. Ist K endlich, so auch L und es gibt ein solches a nach 4.4.20.

Sei also K unendlich. Bezeichnet man die $n := [L : K]_S = [L : K]$ verschiedenen K-Homomorphismen $L \to \overline{K}$ mit $\varphi_1, ..., \varphi_n$, so kann man nach 4.5.10 ein $a \in L$ wählen mit $\varphi_i(a) \neq \varphi_j(a)$ für $i, j \in \{1, ..., n\}$ mit $i \neq j$, denn $\{a \in L \mid \varphi_i(a) = \varphi_j(a)\}$ ist ein echter K-Untervektorraum von L für $i \neq j$. Es folgt

$$n \leq [K(a) : K]_S \overset{4.5.13}{\leq} [K(a) : K] \leq [L : K] = n,$$

also $[K(a) : K] = n = [L : K]$ und daher $L = K(a)$.

(d) $\Longrightarrow$ (a) Sei $a \in L$ separabel über K und gelte $L = K(a)$. Sei $b \in L$. Zu zeigen: b ist separabel über K. Wäre b nicht separabel über K, so $[K(b) : K]_S < [K(b) : K]$ und daher

$$[K(a) : K]_S \overset{4.5.15}{=} [K(a) : K(b)]_S [K(b) : K]_S < [K(a) : K(b)][K(b) : K] \overset{4.1.5}{=} [K(a) : K],$$

womit nach 4.5.14 auch a nicht separabel über K wäre. □

4.5.17 Satz (*„Transitivität der Separabilität“*) [→ 4.1.17] Sei F ein Zwischenkörper von $L|K$ und $F|K$ separabel. Ist $a \in L$ separabel über F, so ist a auch separabel über K.

Beweis. Sei $a \in L$ und $f \in F[X] \setminus 0$ mit $f(a) = 0$. Bezeichne die Koeffizienten von f mit $a_1, ..., a_n$. Dann ist a sogar separabel über $K(a_1, ..., a_n)$. Es folgt:

$$\begin{aligned}[K(a_1, ..., a_n, a) : K]_S &\overset{4.5.15}{=} [K(a_1, ..., a_n, a) : K(a_1, ..., a_n)]_S [K(a_1, ..., a_n) : K]_S \\ &\overset{4.5.16}{=} [K(a_1, ..., a_n, a) : K(a_1, ..., a_n)][K(a_1, ..., a_n) : K] \overset{4.1.5}{=} [K(a_1, ..., a_n, a) : K] < \infty\end{aligned}$$

Nach 4.5.16 ist also $K(a_1, ..., a_n, a)|K$ separabel. Insbesondere ist a separabel über K. □

4.5.18 Korollar [→ 4.1.18] Sei F ein Zwischenkörper von $L|K$. Dann ist $L|K$ separabel genau dann, wenn $L|F$ und $F|K$ beide separabel sind.

4.5.19 Definition und Satz [→ 4.1.9] Sei $L|K$ eine Körpererweiterung. Dann ist

$$\overline{K}^{sL} := \{a \in L \mid a \text{ separabel über } K\}$$

ein Zwischenkörper von $L|K$, genannt der *(relative) separable Abschluss* von K in L.

Beweis. Klar mit 4.5.16 *(c)* $\Longrightarrow$ *(a)*, vgl. Beweis von 4.1.19. □

4.5.20 Definition Ein Körper K heißt *vollkommen*, wenn jedes irreduzible Polynom in $K[X]$ separabel ist.

4.5.21 Satz Sei K ein Körper und $p := \operatorname{char} K$. Dann sind äquivalent:

(a) K ist vollkommen.

(b) Jede algebraische Körpererweiterung $L|K$ ist separabel.

(c) Jede endliche Körpererweiterung $L|K$ ist separabel.

(d) $\overline{K}|K$ ist separabel.

(e) $p = 0$ oder $(p \in \mathbb{P}$ & $\forall a \in K : \exists b \in K : a = b^p)$

(f) $p = 0$ oder $(p \in \mathbb{P}$ & $\Phi_K \in \operatorname{Aut}(K))$ [→ 4.4.3]

Beweis. (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (d) sind klar.

(d) $\Longrightarrow$ (e) Gelte (d) und $p \in \mathbb{P}$. Zu zeigen: $\forall a \in K : a = b^p$. Sei $a \in K$. Wegen $\Phi_{\overline{K}} \in \mathrm{Aut}(\overline{K})$ gibt es genau ein $b \in \overline{K}$ mit $b^p = a$. Es folgt $X^p - a = (X-b)^p$. Setze $f := \mathrm{irr}_K(b)$. Dann ist f ein Teiler von $X^p - a$ in $K[X]$ und damit auch in $\overline{K}[X]$. Somit $f = (X-b)^k$ für ein $k \in \{1, ..., p\}$. Da b über K separabel ist, ist aber f separabel, das heißt $k = 1$. Daher $X - b = f \in K[X]$ und daher $b \in K$.

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

(f) $\Longrightarrow$ (a) Nach 4.5.5(a) ist nichts zu zeigen, falls $p = 0$. Sei also $p \in \mathbb{P}$ und $\Phi_K \in \mathrm{Aut}(K)$. Sei $f \in K[X]$ irreduzibel. Zu zeigen: f separabel. Wähle $a \in \overline{K}$ mit $f(a) = 0$. Dann $f = \mathrm{irr}_K(a)$ nach 4.1.9. Nach 4.5.7 reicht es also zu zeigen, dass a sep. über K ist. Nach 4.5.5(c) gibt es zumindest $n \in \mathbb{N}_0$ derart, dass $(\Phi_{\overline{K}})^n(a) = a^{p^n}$ separabel über K ist. Dann ist $a = (\Phi_{\overline{K}})^{-n}((\Phi_{\overline{K}})^n(a)) = \Phi_{\overline{K}}^{-n}(a^{p^n})$ separabel über $(\Phi_{\overline{K}})^{-n}(K) = (\Phi_K)^{-n}(K) = K$. □

4.5.22 Beispiel Endliche Körper sind vollkommen, da Bedingung (f) aus 4.5.21 erfüllt ist.

4.5.23 Satz Sei $L|K$ eine algebraische Körpererweiterung. Dann $[L : K]_S = [\overline{K}^{sL} : K]$.

Beweis. Da $\overline{K}^{sL}|K$ separabel ist, gilt $[\overline{K}^{sL} : K] = [\overline{K}^{sL} : K]_S$. (Falls $\overline{K}^{sL}|K$ endlich, direkt aus 4.5.16. Sonst durch Betrachtung von über K endlichen Zwischenkörpern von $\overline{K}^{sL}|K$.) Mit 4.5.15 reicht es daher $[L : \overline{K}^{sL}]_S = 1$ zu zeigen.

Ist $p := \mathrm{char}\, K = 0$, so ist K vollkommen und daher $L = \overline{K}^{sL}$. Sei $p \in \mathbb{P}$. Sei nun $\varphi : L \to \overline{L}$ ein $\overline{K}^{sL}$-Homomorphismus. Zu zeigen: $\varphi = \mathrm{id}_L$. Sei $a \in L$. Zu zeigen: $\varphi(a) = a$. Nach 4.5.5(c) gibt es $n \in \mathbb{N}_0$ mit $a^{p^n} \in \overline{K}^{sL}$. Dann $(\varphi(a))^{p^n} = \varphi(a^{p^n}) = a^{p^n}$, also $(\Phi_{\overline{L}})^n(\varphi(a)) = (\Phi_{\overline{L}})^n(a)$ und daher $\varphi(a) = a$. □

§ 5 Galoistheorie [Évariste Galois, geb. 1811, gest. 1832]

§ 5.1 Galoissche Körpererweiterungen

5.1.1 Definition Sei L ein Körper und $G \leq \mathrm{Aut}(L)$. Dann wirkt G in natürlicher Weise auf L durch $\varphi a = \varphi(a)$ für alle $\varphi \in G$ und $a \in L$. Die Menge $L^G = \{a \in L \mid \forall \varphi \in G : \varphi(a) = a\}$ der Fixpunkte dieser Wirkung [→ 3.1.11] ist dann offensichtlich ein Unterkörper von L, den wir den *Fixkörper* von G nennen. Ist K ein Unterkörper von L und $G \leq \mathrm{Aut}(L|K)$ [→ 4.3.8], so ist L^G natürlich ein Zwischenkörper von $L|K$.

5.1.2 Lemma Sei L ein Körper, $G \leq \mathrm{Aut}(L)$, $K := L^G$ und $a \in L$ mit $\#Ga < \infty$ [→ 3.1.6]. Dann ist a algebraisch über K mit $\mathrm{irr}_K(a) = \prod_{b \in Ga}(X - b)$.

Beweis. Für jedes $\varphi \in G$ bezeichne $\tilde{\varphi}$ den Automorphismus von $L[X]$ mit $\tilde{\varphi}|_L = \varphi$ und $\tilde{\varphi}(X) = X$. Für $f := \prod_{b \in Ga}(X - b)$ gilt dann $\tilde{\varphi}(f) = \prod_{b \in Ga}(X - \varphi(b)) = f$ für alle $\varphi \in G$ und daher $f \in L^G[X] = K[X]$. Für alle $\varphi \in G$ ist aber mit a auch $\varphi(a)$ eine Nullstelle von $\mathrm{irr}_K(a)$, womit $f = \mathrm{irr}_K(a)$ folgt. □

5.1.3 Definition Eine Körpererweiterung $L|K$ heißt *galoissch*, wenn $L|K$ normal und separabel ist. Die Automorphismengruppe $\mathrm{Aut}(L|K)$ von $L|K$ nennt man dann auch die *Galoisgruppe* von $L|K$. Eine *Galoiserweiterung* ist eine galoissche Körpererweiterung.

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

(a) $L|K$ ist galoissch.

(b) L ist ein Zerfällungskörper über K einer Menge von separablen Polynomen aus $K[X]$.

(c) $L|K$ algebraisch und $L^{\mathrm{Aut}(L|K)} = K$.

(d) $\forall a \in L \setminus K : \ 2 \leq \#\{\varphi(a) \mid \varphi \in \mathrm{Aut}(L|K)\} < \infty$

Beweis.

(b) $\Longrightarrow$ (a): Klar mit Satz 4.5.19 und Definition 4.3.12.

(a) $\Longrightarrow$ (c): Gelte (a). Dann ist $L|K$ natürlich algebraisch. Sei $a \in L \setminus K$. Zu zeigen $a \ni L^{\mathrm{Aut}(L|K)}$. Nach 4.5.7 ist $f = \mathrm{irr}_K(a)$ separabel und nach 4.3.14(b) zerfällt f über L.

Wegen $a \in L \setminus K$ gilt $\deg(f) \geq 2$ und es gibt $b \in L$ mit $b \neq a$ und $f(b) = 0$. Nach 4.3.11 gilt $a \sim_K b$, das heißt, es gibt $\varphi \in \mathrm{Aut}(L|K)$ mit $\varphi(a) = b$. Nach 4.3.14(e) gilt $\varphi|_L \in \mathrm{Aut}(L|K)$. Wegen $\varphi|_L(a) = b \neq a$ folgt $a \in L^{\mathrm{Aut}(L|K)}$.

(c) $\Longrightarrow$ (d): „$< \infty$“ folgt aus „algebraisch“ und „≥ 2“ aus „$L^{\mathrm{Aut}(L|K)} = K$“.

(d) $\Longrightarrow$ (b): Aus „≥ 2“ folgt $K = L^{\mathrm{Aut}(L|K)}$ und aus „$< \infty$“ folgt mit Lemma 5.1.2, dass jedes $a \in L$ Nullstelle eines separablen Polynoms aus $K[X]$ ist, welches über L zerfällt. □

5.1.5 Proposition Sei $L|K$ eine endliche Körpererweiterung. Dann gilt:

(a) $\#\operatorname{Aut}(L|K) \leq [L:K]_S \leq [L:K]$

(b) $\#\operatorname{Aut}(L|K) = [L:K]_S \iff L|K$ normal

(c) $[L:K]_S = [L:K] \iff L|K$ separabel

Beweis.

(a) $\#\operatorname{Aut}(L|K) \leq [L:K]_S$ ist klar nach Definition des Separabilitätsgrades 4.5.12. $[L:K]_S \leq [L:K]$ ist klar nach 4.5.23.

(b) $\#\operatorname{Aut}(L|K) = [L:K]_S \iff \operatorname{Aut}(L|K) = \{\varphi \mid \varphi : L \to \overline{L}\ K\text{-Homomorphismus}\} \iff$ für jeden K-Homomorphismus $\varphi : L \to \overline{L}$ gilt $\varphi(L) = L \iff L|K$ ist normal nach 4.3.14.

(c) Ist Teil von 4.5.16.

□

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

(a) $L|K$ ist galoissch und endlich.

(b) L ist Zerfällungskörper über K eines separablen Polynoms aus $K[X]$.

(c) L ist Zerfällungskörper über K eines irreduziblen und separablen Polynoms aus $K[X]$.

(d) $[L:K] = \#\operatorname{Aut}(L|K) < \infty$

Beweis. (c) $\implies$ (b) $\implies$ (a) sind klar.
(a) $\implies$ (d): Mit 5.1.5(b), (c).
(a) $\implies$ (c): Gelte (a). Nach dem Satz vom primitiven Element 4.5.16 gibt es $a \in L$ mit $L = K(a)$. Dann ist $f = \operatorname{irr}_K(a) \in K[X]$ irreduzibel und separabel. Nach 4.3.14(b) zerfällt f über L. Also ist L Zerfällungskörper von f über K. □

---

§ 5.2 Der Hauptsatz der Galoistheorie

5.2.1 Satz Sei L ein Körper, $G \leq \operatorname{Aut}(L)$ endlich und $K = L^G$. Dann ist $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe G.

Beweis. Für alle $b \in L$ gilt $\#Gb \leq \#G < \infty$. Daher gibt es ein $a \in L$ mit $\#Ga = \max\{\#Gb \mid b \in L\} =: n$. Wir behaupten: $L = K(a)$. Sei hierzu $c \in L$. Zu zeigen $c \in K(a)$. Nach Lemma 5.1.2 ist $L|K$ separabel, womit $K(a,c)|K$ endlich und separabel ist und es nach dem Satz vom primitiven Element 4.5.16 ein $b \in K(a,c)$ gibt mit $K(a,c) = K(b)$. Nach Lemma 5.1.2 gilt:

$$\begin{aligned}[K(b):K] &= \deg \operatorname{irr}_K(b) = \#Gb \\ &\leq \#Ga = \deg \operatorname{irr}_K(a) = [K(a):K] \\ &\leq [K(a,c):K] = [K(b):K],\end{aligned}$$

also $K(a) = K(b) = K(a,c)$, insbesondere $c \in K(a)$. Da also $L = K(a)$ gilt und nach Lemma 5.1.2 $f = \operatorname{irr}_K(a)$ separabel vom Grad n ist und über L zerfällt, ist L als Zerfällungskörper von f über K galoissch vom Grad n. Es folgt

$$n = \#Ga \leq \#G \leq Aut(L|K) = [L:K] = n$$

und daher $\operatorname{Aut}(L|K) = G$.

5.2.2 Hauptsatz der Galoistheorie Sei $L|K$ eine endliche Galoiserweiterung. Dann vermitteln die Zuordnungen

$$H \mapsto L^H$$
$$\mathrm{Aut}(L|F) \hookleftarrow F$$

eine Bijektion zwischen der Menge der Untergruppen von $G := \mathrm{Aut}(L|K)$ und der Menge der Zwischenkörper von $L|K$.
Seien $H, H' \geq G$ und $F := L^H$, $F' := L^{H'}$. (Oder äquivalent: F, F' Zwischenkörper von $L|K$ und $H := \mathrm{Aut}(L|F)$, $H' := \mathrm{Aut}(L|F')$.) Dann gilt:

(a) $H \subseteq H' \iff F' \subseteq F$ (*„inklusionsumkehrend“*)

(b) Gilt $H \subseteq H'$, so $[H' : H] = [F : F']$.

(c) Ist $\varphi \in G$, so $H' = \varphi H \varphi^{-1} \iff F' = \varphi(F)$ (*„konjugationserhaltend“*)

(d) Gilt $H \subseteq H'$, so $H \lhd H' \iff F|F'$ normal (*„normalitätserhaltend“*)

(e) Ist $H \lhd H'$, so ist $F|F'$ galoissch mit Galoisgruppe isomorph zu H'/H, genauer

$$H'/H = \mathrm{Aut}(L|F')/\mathrm{Aut}(L|F) \xrightarrow{\cong} \mathrm{Aut}(F|F'),\ \overline{\varphi} \longmapsto \varphi|_F \qquad (\varphi \in \mathrm{Aut}(L|F')).$$

Beweis. Beachte, dass G natürlich endlich ist (siehe zum Beispiel 5.1.6). Nach 5.2.1 gilt also $H = \mathrm{Aut}(L|L^H)$ für alle $H \leq \mathrm{Aut}(L|K)$. Für jeden Zwischenkörper F von $L|K$ ist auch $L|F$ galoissch und nach 5.1.4 daher $F = L^{\mathrm{Aut}(L|F)}$. Diese beiden Tatsachen bedeuten, dass die beiden Abbildungen zueinander invers sind.

(a) Ist klar.

(b) Gelte $H \subseteq H'$.

$$[H' : H] = \frac{\#H'}{\#H} \overset{5.2.1}{\underset{5.1.6}{=}} \frac{[L : L^{H'}]}{[L : L^H]} = \frac{[L : F']}{[L : F]} = \frac{[L : F][F : F']}{[L : F]} = [F : F']$$

(c) Sei $\varphi \in G$.

$$\begin{aligned} H' = \varphi H \varphi^{-1} &\iff L^{H'} = L^{\varphi H \varphi^{-1}} \\ &\iff F' = \{a \in L \mid \forall \psi \in H : (\varphi\psi\varphi^{-1})(a) = a\} \\ &\iff F' = \{\varphi(a) \mid a \in L,\ \forall \psi \in H : (\varphi\psi)(a) = \varphi(a)\} \\ &\iff F' = \{\varphi(a) \mid a \in L,\ \forall \psi \in H : \psi(a) = a\} \\ &\iff F' = \varphi(L^H) \\ &\iff F' = \varphi(F) \end{aligned}$$

(d) Gelte $H \subseteq H'$.

$$\begin{aligned} H \lhd H' &\overset{1.3.7}{\iff} \forall \varphi \in H' : \varphi H \varphi^{-1} = H \\ &\overset{(c)}{\iff} \forall \varphi \in H' : \varphi(F) = F \\ &\iff \forall \varphi \in \mathrm{Aut}(L|F') : \varphi(F) = F \\ &\overset{4.3.14}{\iff} \forall \varphi : L \to \overline{L},\ \varphi\ F'\text{-Homomorphismus} : \varphi(F) = F \\ &\overset{4.2.16}{\iff} \forall \varphi : F \to \overline{L},\ \varphi\ F'\text{-Homomorphismus} : \varphi(F) = F \\ &\overset{4.3.14}{\iff} F|F' \text{ normal} \end{aligned}$$

(e) Gelte $H \lhd H'$. Gemäß (d) ist dann $F|F'$ normal und daher galoissch. (Denn mit $L|K$ ist auch $F|F'$ separabel.) Nach 4.3.14(d) ist

$$\begin{aligned} \mathrm{Aut}(L|F) &\to \mathrm{Aut}(F|F') \\ \varphi &\mapsto \varphi|_F \end{aligned}$$

wohldefiniert. Diese Abbildung ist offensichtlich ein Homomorphismus und surjektiv nach 4.2.16 und 4.3.14. Ihr Kern ist $\mathrm{Aut}(L|F)$. Wende nun den Isomorphiesatz 1.3.16 an.

□

5.2.3 Bemerkung Nach 5.1.6 und 4.3.4 ist $L|K$ genau dann eine endliche Galoiserweiterung, wenn es ein $n \in \mathbb{N}56$ und paarweise verschiedene $a_1, ..., a_n \in L$ gibt mit $\prod_{i=1}^{n}(X - a_i) \in K[X]$ und $L = K(a_1, ..., a_n)$ (oder äquivalent $L = K[a_1, ..., a_n]$).

Man fixiere nun solche Daten. Dann wirkt die Galoisgruppe $G := \mathrm{Aut}(L|K)$ treu auf $\{a_1, ..., a_n\}$ [→ 3.1.1], das heißt, man hat nach 3.1.5 eine Einbettung $G \hookrightarrow S_{\{a_1,...,a_n\}} \cong S_n,\ \varphi \mapsto \varphi|_{\{a_1,...,a_n\}}$. Indem man

$$S_{\{a_1,...,a_n\}} \xrightarrow[1.2.9]{\cong} S_n,\ \varphi \mapsto \begin{pmatrix} \{1,...,n\} & \to \{1,...,n\} \\ i & \mapsto j \text{ falls } \varphi(a_i) = a_j \end{pmatrix}$$

dahinterschaltet, erhält man eine Einbettung

$$G \hookrightarrow S_n,\ \varphi \mapsto \begin{pmatrix} \{1,...,n\} & \to \{1,...,n\} \\ i & \mapsto j \text{ falls } \varphi(a_i) = a_j \end{pmatrix}$$

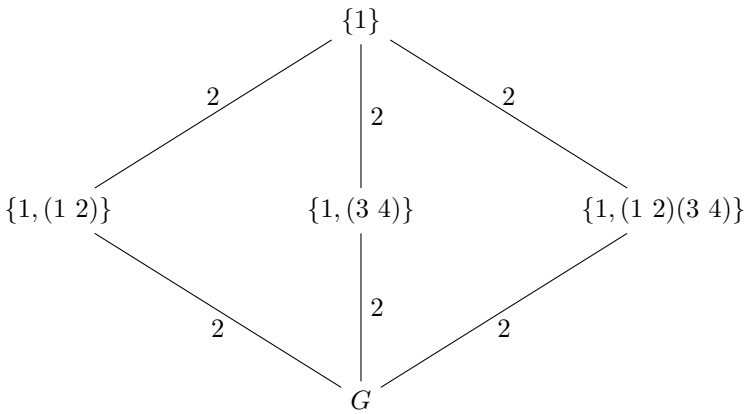
und identifiziert oft G mit seinem Bild unter dieser Abbildung.

5.2.4 Beispiel Um die Unterkörper von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ zu bestimmen, setzt man $a_1 = \sqrt{2}$, $a_2 = -\sqrt{2}$, $a_3 = \sqrt{3}$, $a_4 = -\sqrt{3}$, denn dann gilt, dass $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(a_1, a_2, a_3, a_4)$ und $\prod_{i=1}^{4}(X - a_i) = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$. Es ist also $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ galoissch und $G := \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})$ können wir als Untergruppe von S_n auffassen.

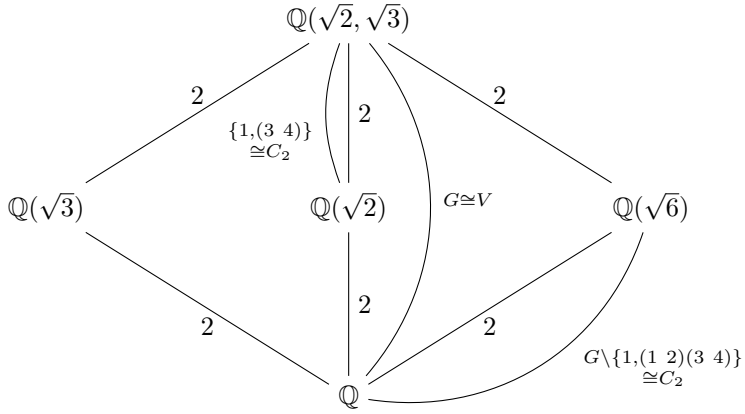
Da die Polynome $X^2 - 2 = (X - a_1)(X - a_2)$ und $X^2 - 3 = (X - a_3)(X - a_4)$ in $\mathbb{Q}[X]$ liegen, folgt $\varphi(\{1, 2\}) = \{1, 2\}$ und $\varphi(\{3, 4\}) = \{3, 4\}$ für alle $\varphi \in G$ und da dieselben Polynome nach dem Kriterium von Eisenstein 2.6.3 irreduzibel sind, gibt es nach 4.3.11 sowohl ein $\varphi \in G$ mit $\varphi(1) = 2$ als auch ein $\varphi \in G$ mit $\varphi(3) = 4$. Es folgt $(1\ 2)(3\ 4) \in G$.

Wäre $\#G = 2$, so $G = \{1, (1\ 2)(3\ 4)\}$ und daher $\sqrt{6} = a_1a_3 = a_2a_4 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})^G = \mathbb{Q}$ im Widerspruch zur Irreduzibilität nach Eisenstein von $X^2 - 6$ in $\mathbb{Q}[X]$. Also $G = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \cong V$ [→ 1.1.9(c)] [→ vgl. auch 3.3.5].

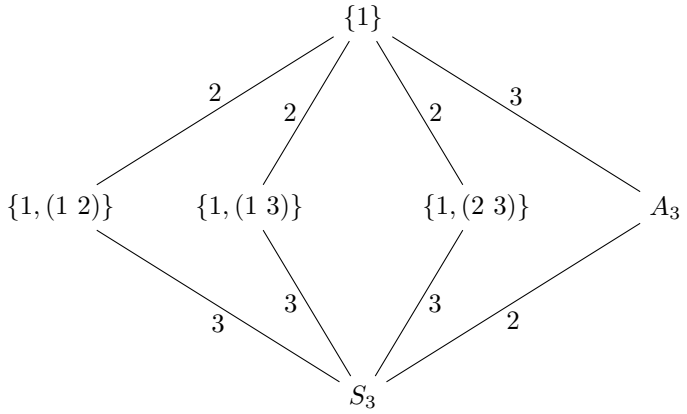
Das auf den Kopf gestellte Diagramm der Untergruppen von G mit den Indizes im Sinne von 1.3.19 an den Kanten liefert nun mit Galois 5.2.2 das Diagramm aller Zwischenkörper von $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ mit den Körpergraden im Sinne von 4.1.1 an den Kanten.



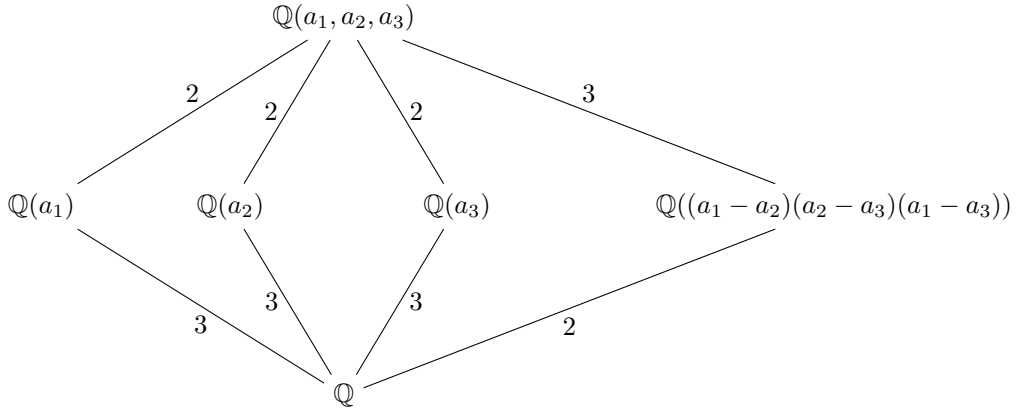
Zeichnet man in einem solchen Diagramm von Zwischenkörpern einer Körpererweiterung einen Bogen zwischen zwei Zwischenkörpern, so meint man damit in der Regel, dass eine Galoiserweiterung vorliegt. Den Bogen beschriftet man oft mit der entsprechenden Galoisgruppe oder einer dazu isomorphen Gruppe.



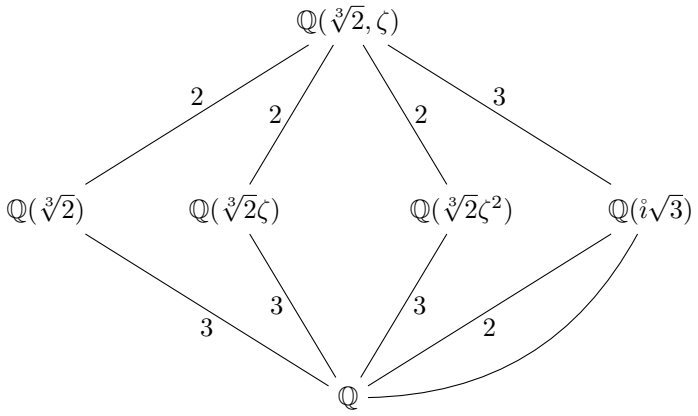
5.2.5 Beispiel Für $f := X^3 - 2 \in \mathbb{Q}[X]$ gilt mit $\zeta := e^{\frac{2\pi i}{3}}$ und $a_1 := \sqrt[3]{2}$, $a_2 := \zeta\sqrt[3]{2}$, $a_3 := \zeta^2\sqrt[3]{2}$, dass $f = \prod_{i=1}^{3}(X - a_i)$. Es ist also $\mathbb{Q}(\sqrt[3]{2},\zeta) = \mathbb{Q}(a_1,a_2,a_3)$ galoissch über $\mathbb{Q}$.
Für $G := \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2},\zeta)|\mathbb{Q}) \subseteq S_3$ gilt $(2\ 3) \in G$ (denn $a_1^* = a_1$ und $a_2^* = a_3$). Da f nach Eisenstein irreduzibel ist, gibt es nach 4.3.11 ein $\varphi \in G$ mit $\varphi(a_1) = a_2$, also $(1\ 2) \in G$ (und damit $(1\ 2\ 3) = (1\ 2)(2\ 3) \in G$) oder $(1\ 2\ 3) \in G$, woraus leicht $G = S_3$ folgt. Nun hat man



und nach Galois dementsprechend



denn $(a_1 - a_2)(a_2 - a_3)(a_1 - a_3)$ wird von A_3 fixiert und liegt nicht in $\mathbb{Q}$, sondern auf der imaginären Achse, wie man durch komplexes Konjugieren sieht. Vereinfache $(a_1 - a_2)(a_1 - a_3)(a_2 - a_3) = (\sqrt[3]{2})^3(1 - \zeta)(\zeta - \zeta^2)(1 - \zeta^2) = 2\zeta(1 - \zeta)^2(1 - \zeta^2) = 2\zeta(1 + 2\zeta + 2\zeta^2)(1 - \zeta^2) = 2\zeta(1 - 2\zeta + \zeta^2 - \zeta^2 + 2 - 3) = 6\zeta(1 - \zeta)$. Wegen $(\zeta(1 - \zeta))^2 = \zeta^2(1 - 2\zeta + \zeta^2) = \zeta^2 - 2 + \zeta = \zeta^2 + \zeta + 1 - 3 = \frac{\zeta^3 - 1}{\zeta - 1} - 3 = -3$ gilt $\mathbb{Q}((a_1 - a_2)(a_2 - a_3)(a_1 - a_3)) = \mathbb{Q}(i\sqrt{3})$. Also ist



das Diagramm aller Zwischenkörper von $\mathbb{Q}(\sqrt[3]{2}, \zeta)|\mathbb{Q}$. Von den vier echten Zwischenkörper ist $\mathbb{Q}(i\sqrt{3})$ der einzige, der galoissch über $\mathbb{Q}$ ist.

§ 6 Der Fundamentalsatz der Algebra

Diesen Paragraphen gibt es geTEXt auf der Vorlesungshomepage.

§ 7 Konstruktionen mit Zirkel und Lineal

Diesen Paragraphen gibt es geTEXt auf der Vorlesungshomepage.

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