

Algebra II
und
Algebra und Zahlentheorie

Franz Halter-Koch

Contents

| | |
|---|----|
| Chapter 1. Mengenlehre und Kategorien | 3 |
| 1.1. Das Axiomensystem von Zermelo-Fraenkel | 3 |
| 1.2. Wohlordnung, Ordinalzahlen und Zorn'sches Lemma | 6 |
| 1.3. Kardinalzahlen | 11 |
| 1.4. Kategorien und Funktoren | 13 |
| Chapter 2. Modultheorie | 19 |
| 2.1. Definitionen und elementare Eigenschaften | 19 |
| 2.2. Innere direkte Summen und freie Moduln | 25 |
| 2.3. Existenz und Mächtigkeit von Basen | 31 |
| 2.4. Matrizenrechnung | 35 |
| 2.5. Noethersche Moduln und Ringe | 39 |
| 2.6. Moduln über Hauptidealbereichen | 41 |
| Chapter 3. Ring- und Körpertheorie | 47 |
| 3.1. Ganze Ringerweiterungen | 47 |
| 3.2. Quotientenbildung | 50 |
| 3.3. Algebraische Körpererweiterungen | 53 |
| 3.4. Transzendente Körpererweiterungen | 57 |
| 3.5. Affine Algebren: Normalisierungssatz und Nullstellensatz | 60 |
| 3.6. Separabilität | 64 |
| 3.7. Derivationen | 72 |
| Chapter 4. Potenzreste und quadratisches Reziprozitätsgesetz | 79 |
| 4.1. Allgemeines über Potenzreste | 79 |
| 4.2. Quadratisches Reziprozitätsgesetz | 82 |

Mengenlehre und Kategorien

1.1. Das Axiomensystem von Zermelo-Fraenkel

Die ZF-Mengenlehre (Mengenlehre nach Zermelo und Fraenkel) hat zwei undefinierte Grundbegriffe, den Begriff der *Menge* und den Begriff des *Enthaltenseins*.

Die Variablen der Sprache bezeichnen Mengen: a, b, \dots, u, x, \dots

Die Enthaltenseinsrelation ist eine zweistellige Relation zwischen Mengen: $x \in y$. $x \notin y \iff \neg x \in y$.

Definition 1.1.1. Wir formulieren die ZF-Mengenlehre in der Sprache der Prädikatenlogik 1. Stufe mit Identität (das ist die formalisierte mathematische Umgangssprache). Wir geben eine informale (rekursive) Definition, die angibt, welche Ausdrücke wir als *Formeln* bezeichnen. Inhaltliche Bedeutung: Formeln bezeichnen Aussagen der Mengenlehre.

1. $x = y$ und $x \in y$ sind Formeln.
2. Sind φ und ψ Formeln, so sind auch $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \implies \psi$ und $\varphi \iff \psi$ Formeln.
3. Ist φ eine Formel, so sind auch $\exists x\varphi$ und $\forall x\varphi$ Formeln.

Es gibt zwei Möglichkeiten, eine axiomatische Theorie zu lesen:

- *formal-syntaktisch*: Gegenstand der Untersuchung ist das regelgerechte Manipulieren von Formeln ohne Bezug auf deren Bedeutung.
- *inhaltlich-semantisch*: Man tut so, als hätte man die mathematischen Objekte, für die man eine Theorie macht, in der Hand und operiert mit ihnen.

Wir werden die axiomatische Mengenlehre als inhaltlich-semantische Theorie beschreiben und dementsprechend wie folgt beginnen:

Gegeben sei eine nicht-leere Gesamtheit (ein Universum) \mathcal{U} von Objekten, die wir Mengen nennen, und zwischen ihnen eine zweistellige Operation \in , so dass die folgenden Axiome erfüllt sind: ...

Die Variablen der Sprache bezeichnen dann die Elemente von \mathcal{U} , und Quantoren erstrecken sich (wenn nichts Anderes gesagt wird) über \mathcal{U} . Für jede Formel φ bezeichne $\{x \mid \varphi\}$ die Gesamtheit aller Objekte von \mathcal{U} , für die φ gilt (wie in der naiven Mathematik üblich). Die Teilgesamtheiten von \mathcal{U} der Form $\{x \mid \varphi\}$ heißen *definierbar* und werden *Klassen* genannt. Für Klassen verwenden wir die üblichen Begriffe und Operationen der naiven Mengenlehre (Teilklasse, Vereinigung, Durchschnitt, Differenz etc.). Insbesondere verwenden wir das Enthaltenseinszeichen auch für die Zugehörigkeit zu Klassen: Ist $C = \{x \mid \varphi\} \subset \mathcal{U}$ mit einer Formel φ , so schreiben wir $x \in C$, wenn x zu C gehört (d. h., wenn φ gilt). Demnach hat das Zeichen \in zwei Bedeutungen: Es ist einerseits das formale (axiomatisch zu beschreibende) Relationzeichen zwischen Objekten von \mathcal{U} , andererseits das Elementzeichen der mathematischen Umgangssprache, mit dem wir über unser Universum sprechen.

Axiom 1 (Extensionalität). $a = b \iff \forall x[x \in a \iff x \in b]$. Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente (= Mengen) enthalten.

Für eine Menge a ist $\hat{a} = \{x \mid x \in a\} \subset \mathcal{U}$ eine Klasse (der \in -Vorbereich von a). Aufgrund des Extensionalitätsaxioms gilt: $a = b \iff \hat{a} = \hat{b}$. Daher werden wir im Folgenden nicht zwischen a und \hat{a} unterscheiden, und damit wird auch die Unterscheidung zwischen der formalen und der inhaltlichen Bedeutung von \in obsolet.

Für zwei Klassen A, B bedeutet $A \in B$ insbesondere, dass A eine Menge ist [präzise: Es gibt ein $a \in B$ mit $\hat{a} = A$].

Axiom 2 (Aussonderung). Jede Teilklasse einer Menge ist eine Menge [äquivalent: Für jede Formel φ gilt: $\forall u \exists z \forall x [x \in z \iff x \in u \wedge \varphi]$. Kurzschreibweise: Ist C eine Klasse und $C \subset a$, so ist C eine Menge.

Definition 1.1.2. Für (Mengen) a, b und Klassen A, B definieren wir

- die *Paarklasse* $\{a, b\} = \{x \mid x = a \vee x = b\}$, die *Einerklasse* $\{a\} = \{a, a\}$,
- die *Vereinigungsklasse* $\bigcup A = \{x \mid \exists y [y \in A \wedge x \in y]\}$, $A \cup B = \{x \mid x \in A \vee x \in B\}$.
- die *Schnittklasse* $\bigcap A = \{x \mid \forall y [y \in A \implies x \in y]\}$, $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
- die *Potenzklasse* $\mathbb{P}A = \{x \mid x \subset A\}$.

Für Mengen a, b ist $a \cup b = \bigcup\{a, b\}$ und $a \cap b = \bigcap\{a, b\}$.

Die Klasse $\emptyset = \{x \mid x \neq x\}$ heißt *leere Klasse*.

\emptyset ist eine Menge [nach dem Aussonderungsaxiom, denn: $\emptyset \subset a$], und nach dem Extensionalitätsaxiom gilt: $a = \emptyset \iff \forall x [x \notin a]$

Die Klasse $\mathcal{U} = \{x \mid x = x\}$ heißt *Allklasse*, die Klasse $\mathcal{R} = \{x \mid x \notin x\}$ heißt *Russell-Klasse*.

Axiom 3 (Paarbildungsaxiom) Für alle (Mengen) a, b ist die Paarklasse $\{a, b\}$ eine Menge.

Axiom 4 (Vereinigungsaxiom) Für alle (Mengen) a ist die Vereinigung $\bigcup a$ eine Menge.

Axiom 5 (Potenzmengenaxiom) Für alle (Mengen) a ist die Potenzklasse $\mathbb{P}a$ eine Menge.

Bemerkung 1.1.3. \mathcal{R} und \mathcal{U} sind keine Mengen. [denn: Wäre \mathcal{R} eine Menge, so würde gelten: $\mathcal{R} \in \mathcal{R} \iff \mathcal{R} \notin \mathcal{R}$. Daher ist \mathcal{R} keine Menge, und wegen $\mathcal{R} \subset \mathcal{U}$ ist auch \mathcal{U} keine Menge].

Definition 1.1.4.

1. Für (Mengen) a, b sei $(a, b) = \{\{a\}, \{a, b\}\}$, $(a, b, c) = ((a, b), c)$, $(a, b, c, d) = ((a, b, c), d)$, etc.
2. Für Klassen A, B heißt $A \times B = \{z \mid \exists x \exists y [z = (x, y) \wedge x \in A \wedge y \in B]\}$ die *Produktklasse*.
3. Eine *Relation* ist eine Klasse R mit $R \subset \mathcal{U} \times \mathcal{U}$. Ist R eine Relation, so definiert man

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}, \mathcal{D}(R) = \{x \mid \exists y (x, y) \in R\} \text{ und } \mathcal{W}(R) = \{y \mid \exists x (x, y) \in R\}.$$

$\mathcal{D}(R)$ heißt *Definitionsbereich* und $\mathcal{W}(R)$ heißt *Wertebereich* von R . Die Relation R^{-1} heißt die zu R *inverse Relation*.

Wichtige Relationen: \emptyset , $\text{Id} = \{(x, x) \mid x \in \mathcal{U}\}$, $\mathbb{E} = \{(x, y) \mid x \in y\}$

4. Sei R eine Relation und A eine Klasse. Dann heißt $R \upharpoonright A = R \cap A \times \mathcal{U}$ die *Einschränkung* von R auf A und $R[A] = \mathcal{W}(R \upharpoonright A)$ das *Bild* von A unter R . Die Relation $\text{Id}_A = \text{Id} \upharpoonright A$ heißt *Identität* auf A . Die Relation R heißt *Relation auf A* , wenn $R \subset A \times A$.
5. Sind R und S Relationen, so definiert man $R \circ S = \{(x, z) \mid \exists y [(x, y) \in S \wedge (y, z) \in R]\}$.

6. Eine Relation R heißt *Funktion*, wenn für alle x, y, y' gilt: $(x, y) \in R \wedge (x, y') \in R \implies y = y'$. Eine Funktion F heißt *injektiv*, wenn F^{-1} ebenfalls eine Funktion ist. \emptyset und Id sind injektive Funktionen. $\mathcal{D}(\emptyset) = \mathcal{W}(\emptyset) = \emptyset$, $\emptyset^{-1} = \emptyset$, $\mathcal{D}(\text{Id}) = \mathcal{W}(\text{Id}) = \mathcal{U}$, $\text{Id}^{-1} = \text{Id}$, $\mathcal{D}(\mathbb{E}) = \mathcal{U}$, $\mathcal{W}(\mathbb{E}) = \mathcal{U} \setminus \{\emptyset\}$.

Ist F eine Funktion und $(x, y) \in F$, so schreibt man $y = F(x)$. Vorsicht! $y = F[x]$ bedeutet etwas Anderes! Im üblichen mathematischen Gebrauch (wo Verwechslungen nicht zu befürchten sind) schreibt man auch $F(X)$ an Stelle von $F[X]$.

7. Seien A, B, F Klassen. F heißt *Abbildung* von A nach B (Schreibweise $F: A \rightarrow B$), wenn F eine Funktion mit $\mathcal{D}(F) = A$ und $\mathcal{W}(F) \subset B$ ist. Die leere Funktion ist eine Abbildung $\emptyset: \emptyset \rightarrow B$ (die *leere Abbildung*).
8. Eine Abbildung $F: A \rightarrow B$ heißt *surjektiv*, wenn $\mathcal{W}(F) = B$, und *bijektiv*, wenn sie injektiv und surjektiv ist.

Zwei Mengen A, B heißen *gleichmächtig*, $A \approx B$, wenn es eine bijektive Abbildung $F: A \rightarrow B$ gibt. \approx ist eine Äquivalenzrelation auf \mathcal{U} .

Satz 1.1.5.

1. Genau dann ist $(a, b) = (a', b')$, wenn $a = a'$ und $b = b'$.
2. Für alle (Mengen) a, b sind auch $a \cup b$, (a, b) und $a \times b$ Mengen.
3. Eine Relation R ist genau dann eine Menge, wenn $\mathcal{D}(R)$ und $\mathcal{W}(R)$ Mengen sind.
4. Seien R und S Relationen. Dann ist $\mathcal{D}(R \circ S) = S^{-1}[\mathcal{D}(R)]$. Sind R und S Funktionen, so ist auch $R \circ S$ eine Funktion, und für jede Klasse C ist auch $R \upharpoonright C$ eine Funktion.

BEWEIS. 1. und 4. Nach Definition (Übung!).

2. Sind a, b Mengen, so sind auch $\{a, b\}$, $\{a\} = \{a, a\}$ Mengen, und daher sind auch $a \cup b = \bigcup \{a, b\}$ und $(a, b) = \{\{a\}, \{a, b\}\}$ Mengen. Wegen $a \times b \subset \mathbb{P}\mathbb{P}(a \cup b)$ ist $a \times b$ eine Menge.

3. Es ist $\mathcal{D}(R) \subset \bigcup \bigcup R$, $\mathcal{W}(R) \subset \bigcup \bigcup R$ und $R \subset \mathcal{D}(R) \times \mathcal{W}(R)$. □

Axiom 6 (Ersetzungsaxiom). Ist F eine Funktion und a eine Menge, so ist $F[a]$ eine Menge.

Bemerkung 1.1.6. Axiom 6 \implies Axiom 2 [denn: Ist $C \subset a$, so ist $C = \text{Id}_C[a]$].

Satz 1.1.7.

1. Eine Funktion F ist genau dann eine Menge, wenn $\mathcal{D}(F)$ eine Menge ist.
2. Sind a und b Mengen, so ist auch die Klasse $\text{Abb}(a, b)$ aller Abbildungen von a nach b eine Menge.
3. (Existenz fremder Exemplare) Sind a und b Mengen, so gibt es eine Menge a' mit $a' \approx a$ und $a' \cap b = \emptyset$.

BEWEIS. 1. Sei F eine Funktion. Ist F eine Menge, so auch $\mathcal{D}(F)$ nach Satz 1.1.5.3. Ist $\mathcal{D}(F)$ eine Menge, so ist nach dem Ersetzungsaxiom auch $\mathcal{W}(F) = F[\mathcal{D}(F)]$ eine Menge, und daher ist nach Satz 1.1.5.3 auch F eine Menge.

2. $\text{Abb}(a, b) \subset \mathbb{P}(a \times b)$.

3. Es genügt, zu zeigen: Es gibt ein x mit $(a \times \{x\}) \cap b = \emptyset$ [dann ist $a' = a \times \{x\} \approx a$]. Angenommen, das sei falsch. Dann ist $\{x \mid (a \times \{x\}) \cap b \neq \emptyset\} = \mathcal{U}$ und $b_0 = \{z \mid z \in b, z = (u, x) \text{ mit } u \in a\} \subset b$. Dann ist b_0 eine Menge und $f = \{(u, x), x \mid (u, x) \in b_0\}$ eine Funktion mit $f[b_0] = \mathcal{U}$, ein Widerspruch! □

Axiom 7 (Regularitätsaxiom). Für jede nicht-leere Menge b gilt: $\exists u [u \in b \wedge u \cap b = \emptyset]$.

Satz 1.1.8. Aus $x \in y$ folgt $y \notin x$. Insbesondere ist $x \notin x$.

BEWEIS. Nach dem Regularitätsaxiom, angewandt auf die Menge $\{x, y\}$. \square

Definition 1.1.9. Sei I eine Menge.

1. Eine *Familie* mit Indexmenge I ist eine Funktion X mit $\mathcal{D}(X) = I$ [dann ist X eine Menge; für $i \in I$ schreibt man $X_i = X(i)$, und $X = (X_i)_{i \in I}$].
2. Ist $(X_i)_{i \in I}$ eine Familie, so bezeichne

$$\prod_{i \in I} X_i \subset \mathbb{P}(I \times \bigcup \mathcal{W}(X)) \quad \text{die Menge aller Familien } (x_i)_{i \in I}, \text{ so dass } \forall i \in I [x_i \in X_i].$$

Im Falle $I = \emptyset$ ist $\prod_{i \in I} X_i = \{\emptyset\}$.

Axiom 8 (Auswahlaxiom). Ist X eine Familie mit Indexmenge I , so gilt :

$$\forall i \in I [X_i \neq \emptyset] \implies \prod_{i \in I} X_i \neq \emptyset.$$

Satz 1.1.10 (Auswahlsatz).

1. Zu jeder Menge a mit $\emptyset \notin a$ gibt es eine Funktion f mit $\mathcal{D}(f) = a$, so dass $\forall x \in a [f(x) \in x]$. Man sagt f ist eine *Auswahlfunktion* für das Mengensystem a .
2. Sei R eine Relation, $\mathcal{D}(R)$ eine Menge, und für alle $x \in \mathcal{D}(R)$ sei $R[\{x\}]$ eine Menge. Dann gibt es eine Funktion f mit $\mathcal{D}(f) = \mathcal{D}(R)$ und $f \subset R$.

BEWEIS. 1. Sei $\emptyset \notin a$ und $X = \text{Id} \upharpoonright a$, also $X = (x)_{x \in a}$. Ist nun $f \in \prod_{x \in a} x$, so ist f eine Funktion mit $\mathcal{D}(f) = a$ und $f(x) \in x$ für alle $x \in a$.

2. Für alle $x \in \mathcal{D}(R)$ ist $R[\{x\}] \neq \emptyset$. Ist $f \in \prod_{x \in \mathcal{D}(R)} R[\{x\}]$, so ist f eine Funktion, $\mathcal{D}(f) = \mathcal{D}(R)$ und $f \subset R$. \square

1.2. Wohlordnung, Ordinalzahlen und Zorn'sches Lemma

Definitionen und Bemerkungen 1.2.1. Sei X eine Klasse und $< \subset X \times X$ eine Relation. Für $x, y \in X$ schreiben wir $x < y$ an Stelle von $(x, y) \in <$. $<$ heißt *Teilordnung* auf X , wenn für alle $x, y, z \in X$ gilt :

O1. $x \not< x$.

O2. $x < y \wedge y < z \implies x < z$.

Ist $<$ eine Teilordnung auf X , so definiert man die Relationen \leq , $>$ und \geq sowie die Begriffe *nach oben* [unten] *beschränkt*, *obere* [untere] *Schranke*, *größtes* [kleinstes] *Element*, *Maximum* [Minimum], *Supremum* [Infimum] wie üblich.

Eine Teilordnung $<$ auf X heißt

- *Totalordnung*, wenn für alle $x, y \in X$ gilt: $x \neq y \implies x < y \vee y < x$;
- *Wohlordnung* auf X , wenn jede nicht-leere Teilmenge von X ein Minimum besitzt.

Jede Wohlordnung auf X ist eine Totalordnung auf X [denn: für $x, y \in X$ mit $x \neq y$ ist entweder $\min\{x, y\} = x$, also $x < y$, oder $\min\{x, y\} = y$, also $y < x$].

Ist $<$ eine Teilordnung [Totalordnung, Wohlordnung] auf X und $S \subset X$, so ist $< \cap (S \times S)$ eine Teilordnung [Totalordnung, Wohlordnung] auf S (die wieder mit $<$ bezeichnet wird). Ist $<$ eine Totalordnung auf S , so nennt man S eine *Kette*.

Sei $<$ eine Totalordnung auf X . Eine Teilklasse $Y \subset X$ heißt *Anfangsstück*, wenn für alle $x \in X$ und $y \in Y$ gilt: $x < y \implies x \in Y$. Für $a \in X$ sei $X(a) = \{x \in X \mid x < a\}$ (das durch a bestimmte Anfangsstück).

Eine teilgeordnete [totalgeordnete, wohlgeordnete] Menge ist ein Paar $(X, <)$, bestehend aus einer Menge X und einer Teilordnung [Totalordnung, Wohlordnung] $<$ auf X .

Satz 1.2.2. Sei $<$ eine Totalordnung auf der Klasse X .

1. Ist Ω eine Menge von Anfangsstücken von X , so sind auch $\bigcup \Omega$ und $\bigcap \Omega$ Anfangsstücke von X .
2. Sei $Y \subsetneq X$ ein Anfangsstück und $a = \min(X \setminus Y)$. Dann ist $Y = X(a)$.
3. Sind A und B Anfangsstücke von X , so ist $A \subset B$ oder $B \subset A$.

BEWEIS. 1. und 2. Übung!

3. Sei $A \not\subset B$ und $a \in A \setminus B$. Ist $x \in B$, so folgt $x < a$ [denn aus $x \geq a$ folgt $a \in B$]. Daher ist $x \in A$, also $B \subset A$. \square

Definition 1.2.3. Sei A eine Klasse und $\mathbb{E}_A = \mathbb{E} \cap (A \times A)$ die Enthaltensrelation auf A .

1. A heißt *transitiv*, wenn $x \in A \implies x \subset A$.
2. A heißt *Ordinalklasse*, wenn A transitiv ist, und \mathbb{E}_A eine Totalordnung auf A ist [äquivalent: $\forall a, b \in A [a = b \vee a \in b \vee b \in a]$. Für $a, b \in A$ definieren wir $a < b \iff a \in b$.
3. A heißt *Ordinalzahl*, wenn A eine Ordinalklasse und eine Menge ist. Ord bezeichne die Klasse aller Ordinalzahlen.

Beispiele: $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \in \text{Ord}$.

Satz 1.2.4. A sei eine Ordinalklasse und $B \subset A$.

1. $A \subset \text{Ord}$.
2. Für $z \in B$ gilt: $z = \min(B) \iff z \cap B = \emptyset$.
3. Ist $B \neq \emptyset$, so besitzt B ein Minimum. Insbesondere ist $<$ eine Wohlordnung auf A .
4. Ist $B \subsetneq A$ und B transitiv, so folgt $B = \min(A \setminus B) \in A$.
5. Ist A' eine weitere Ordinalklasse, so folgt $A \subset A'$ oder $A' \subset A$.

BEWEIS. 1. Sei $a \in A$. Dann ist $a \subset A$ und $\mathbb{E}_a = \mathbb{E}_A \cap (a \times a)$ eine Totalordnung auf a . Wir zeigen, dass a transitiv ist, das heißt, $x \in a \wedge y \in x \implies y \in a$. Ist $x \in a$ und $y \in x$, so folgt $x \in A$, also $x \subset A$ und daher $y \in A$. Also folgt $a, x, y \in A$, $y \in x$ und $x \in a$, also $y \in a$.

2. Sei $z \in B$. $z = \min(B) \iff \forall x \in B [x = z \vee z \in x] \iff \forall x \in B [x \not\subset z] \iff z \cap B = \emptyset$.

3. Sei $a \in B$. Ist $a \cap B = \emptyset$, so ist $a = \min(B)$. Sei also $a \cap B \neq \emptyset$. Nach dem Regularitätsaxiom gibt es ein $z \in a \cap B$ mit $z \cap a \cap B = \emptyset$. Ist $y \in z \cap B$, so folgt $y \in z \wedge z \in a$, also $y \in a$. Daher ist $z \cap a \cap B = z \cap B = \emptyset$ und $z = \min(B)$.

4. Sei $z = \min(A \setminus B)$. Dann ist $z \cap (A \setminus B) = \emptyset$. Aus $z \in A$ folgt $z \subset A$, also $z \subset B$, und wir zeigen $z = B$. Wäre $z \subsetneq B$ und $y \in B \setminus z$, also $y \notin z$, so folgt $y = z$ oder $z \in y$. Da B transitiv ist, folgt $y \subset B$, also $z \in B$, ein Widerspruch.

5. Wir nehmen im Gegenteil an, es sei $A \not\subset A'$ und $A' \not\subset A$. Dann folgt $A \cap A' \subsetneq A$, also $A \cap A' \in A$ nach 4., und ebenso $A \cap A' \in A'$, also $A \cap A' \in A \cap A'$, ein Widerspruch. \square

Satz 1.2.5 (Klassifikationssatz für Ordinalklassen).

1. Ord ist eine Ordinalklasse und keine Menge.
2. Für eine Klasse A sind äquivalent:
 - (a) $A \in \text{Ord}$.
 - (b) A ist eine Ordinalklasse, und $A \neq \text{Ord}$.
 - (c) $A \subsetneq \text{Ord}$ ist ein Anfangsstück.

BEWEIS. 1. Ord ist transitiv nach Satz 1.2.4.1. Für alle $x, y, z \in \text{Ord}$ gilt: $x \notin x$, und aus $x \in y$ und $y \in z$ folgt $y \subset z$ und daher $x \in z$. Daher ist \in eine Teilordnung auf Ord. Seien nun $x, y \in \text{Ord}$ und $x \neq y$. Nach Satz 1.2.4 ist dann entweder $x \subsetneq y$, also $x \in y$, oder $y \subsetneq x$, also $y \in x$.

Daher ist Ord eine Ordinalklasse. Wäre Ord eine Menge, so folgte $\text{Ord} \in \text{Ord}$, ein Widerspruch!

2. (a) \Rightarrow (b) Klar.

(b) \Rightarrow (c) Nach Satz 1.2.4.1 ist $A \subsetneq \text{Ord}$. Ist $x \in A$ und $y \in x$, so ist $y \in A$. Also ist A ein Anfangsstück.

(c) \Rightarrow (a) Da A ein Anfangsstück ist, ist A transitiv und daher $A \in \text{Ord}$ nach Satz 1.2.4.4. \square

Definition 1.2.6. Für eine Menge x sei $x^+ = x \cup \{x\}$. Eine Ordinalzahl x heißt

- *Nachfolgerzahl*, wenn es ein $z \in \text{Ord}$ gibt mit $x = z^+$;
- *Limeszahl*, wenn x keine Nachfolgerzahl ist.
- *endliche Ordinalzahl*, wenn jede nicht-leere Teilmenge von x ein Maximum besitzt. ω bezeichne die Klasse aller endlichen Ordinalzahlen.

Eine Menge x heißt

- *endlich*, wenn es ein $n \in \omega$ gibt mit $x \approx n$;
- *unendlich*, wenn sie nicht endlich ist;
- *abzählbar*, wenn $x \approx \omega$;
- *überabzählbar*, wenn x unendlich, aber nicht abzählbar ist;
- *höchstens abzählbar*, wenn x endlich oder abzählbar ist.

Satz 1.2.7. Seien $x, y \in \text{Ord}$.

1. $x \leq y \iff x \subset y \iff x = y \vee x \in y$.
2. $x^+ \in \text{Ord}$, und $x^+ = \min\{z \in \text{Ord} \mid z > x\}$.
3. $x^+ \leq y^+ \implies x \leq y$. Insbesondere: $x^+ = y^+ \implies x = y$.
4. Ist y eine Nachfolgerzahl, so existiert $\max(y)$, und $\max(y)^+ = y$.
5. Ist y eine Limeszahl, so ist $y = \sup(y) \notin y$. Insbesondere hat y kein Maximum.

BEWEIS. 1. Nach Definition.

2. $z \in x^+ = x \cup \{x\} \implies z = x \vee z \in x \implies z \subset x \subset x^+$. Daher ist $x^+ \subsetneq \text{Ord}$ eine transitive Menge und $x^+ \in \text{Ord}$ nach Satz 1.2.4.4.

Für $z \in \text{Ord}$ gilt: $z > x \iff x \in z \iff x^+ = x \cup \{x\} \subset z \iff x^+ \leq z$.

3. Sei $x \neq \emptyset$ und $x \cup \{x\} \subset y \cup \{y\}$. Dann ist entweder $x \in y$ oder $x = y$, also $x \leq y$.

4. Sei $y = x^+ = x \cup \{x\}$. Dann ist $x = \max(x^+)$ und daher $y = \max(y)^+$.

5. Nach Definition ist y eine obere Schranke von y . Ist $z \in y$, so folgt $z^+ \in y$, da y eine Limeszahl ist. Ist daher z eine obere Schranke von y , so ist $u < z$ für alle $u \in y$, also $y \subset z$ und daher $y \leq z$. Daher folgt $y = \sup(y)$. \square

Satz 1.2.8 (Peano-Eigenschaften für ω). ω ist eine Ordinalklasse (also insbesondere $\omega = \text{Ord}$ oder $\omega \in \text{Ord}$) und hat die folgenden Eigenschaften:

1. $\emptyset \in \omega$, und für alle $x \in \omega$ ist $x^+ \in \omega$.
2. Für alle $x \in \omega$ ist $x^+ \neq \emptyset$.
3. Sind $x, y \in \omega$ mit $x^+ = y^+$, so folgt $x = y$.
4. Sei $A \subset \omega$, so dass $\emptyset \in A$ und $[x \in A \implies x^+ \in A]$, so folgt $A = \omega$.

BEWEIS. Ist $x \in \omega$ und $y \in x$, so folgt $y \subset x$, daher hat auch jede Teilmenge von y ein Maximum, und es folgt $y \in \omega$. Daher ist ω transitiv und daher eine Ordinalklasse.

1., 2. und 3. sind offensichtlich.

4. Angenommen, es sei $A \subsetneq \omega$. Dann ist $u = \min(\omega \setminus A) \neq \emptyset$ eine Nachfolgerzahl (da sie ein Maximum besitzt), also $u = x^+$. Wegen $x < u$ ist $x \in A$ und es folgt $u = x^+ \in A$, ein Widerspruch. \square

Folgerung. Da ω die Peano-Axiome erfüllt, andererseits aber die natürlichen Zahlen durch die Peano-Axiome (bis auf Isomorphie) eindeutig bestimmt sind, haben wir auf diese Weise ein Modell der natürlichen Zahlen innerhalb der ZF-Mengenlehre konstruiert. Aus den Peano-Axiomen kann man alle bekannten Eigenschaften der natürlichen Zahlen folgern und damit das Zahlssystem aufbauen.

Konvention. Wir arbeiten auch weiterhin mit den (naiven) natürlichen Zahlen $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. Für $n \in \mathbb{N}_0$ definieren wir rekursiv $\underline{n} \in \omega$ durch $\underline{0} = \emptyset$ und $\underline{n+1} = \underline{n}^+ = \underline{n} \cup \{\underline{n}\}$. Dann ist $\underline{n} = \{0, \underline{1}, \dots, \underline{n-1}\}$ für alle $n \in \mathbb{N}_0$, und $\omega = \{\underline{n} \mid n \in \mathbb{N}_0\}$ [denn: Es ist $\underline{\mathbb{N}} = \{\underline{n} \mid n \in \mathbb{N}_0\} \subset \omega$, $\emptyset \in \underline{\mathbb{N}}$, und für alle $x \in \underline{\mathbb{N}}$ ist $x^+ \in \underline{\mathbb{N}}$. Nach Satz 1.2.8.4 folgt $\underline{\mathbb{N}} = \omega$, und offensichtlich ist $\mathbb{N} \cong \omega$, also insbesondere $\mathbb{N} \approx \omega$.

Axiom 9 (Unendlichkeitsaxiom). ω ist eine Menge [äquivalent: Es gibt eine unendliche Menge (siehe Satz 1.2.12)].

Satz 1.2.9. Seien $\alpha \in \text{Ord}$, $m \in \omega$ und $\alpha \approx m$. Dann ist $\alpha = m$. Insbesondere ist α genau dann eine endliche Menge, wenn $\alpha \in \omega$ [d. h., α ist eine endliche Ordinalzahl].

BEWEIS. Wir zeigen zuerst :

A. Ist $m \in \omega$, so gibt es keine injektive Abbildung $m^+ \rightarrow m$.

Beweis von A. Sei $A = \{m \in \omega \mid \text{es gibt eine injektive Abbildung } m^+ \rightarrow m\} \neq \emptyset$ und $m = \min(A)$. Dann ist $m \neq \emptyset$, also $m = n^+$ für ein $n \in \omega$, und es sei $g: m^+ \rightarrow m = n^+$ injektiv. Es ist $m = \max(m^+)$, $n = \max(n^+)$, und es sei $g(m) = k \in m$. Definiert man

$$h: n^+ \rightarrow n^+ \quad \text{durch} \quad h(k) = n, \quad h(n) = k \quad \text{und} \quad h(x) = x \quad \text{für} \quad x \in n^+ \setminus \{k, n\},$$

so ist $h \circ g$ injektiv und $h \circ g(m) = n$, also $h \circ g \upharpoonright m: m = n^+ \rightarrow n$ injektiv, ein Widerspruch zur Minimalwahl von m .

Wir nehmen nun an, der Satz sei falsch, es sei $m \in \omega$ minimal mit $T = \{\alpha \in \text{Ord} \mid \alpha \approx m, \alpha \neq m\} \neq \emptyset$ und $\beta = \min(T)$. Dann ist $\beta \approx m$, $\beta > m$ und daher $m^+ \leq \beta$, also $m^+ \subset \beta$. Ist nun $g: \beta \rightarrow m$ bijektiv, so ist $g \upharpoonright m^+: m^+ \rightarrow m$, injektiv, ein Widerspruch. \square

Definition 1.2.10. $(X, <)$ und $(X', <')$ seien totalgeordnete Mengen. Eine Abbildung $f: X \rightarrow X'$ heißt

- *ordnungstreu*, wenn $\forall x, y \in X [x < y \implies f(x) <' f(y)]$
[dann ist f injektiv, und $f^{-1}: f[X] \rightarrow X$ ist ebenfalls ordnungstreu];
- *Ordnungsisomorphie*, wenn f ordnungstreu und bijektiv ist [dann ist auch $f^{-1}: X' \rightarrow X$ eine Ordnungsisomorphie].

$(X, <)$ und $(X', <')$ heißen *ordnungsisomorph*, $X \cong X'$, wenn es eine Ordnungsisomorphie $f: X \rightarrow X'$ gibt.

Satz 1.2.11 (Vergleichssatz). $(X, <)$ sei eine wohlgeordnete Menge.

1. Ist $C \subset X$ ein Anfangsstück und $f: C \rightarrow X$ ordnungstreu, so folgt $\forall x \in C [f(x) \geq x]$.
2. Ist $C \subset X$ ein Anfangsstück von X und $C \cong X$, so folgt $C = X$.
3. Es gibt genau ein $\alpha \in \text{Ord}$ mit $X \cong \alpha$. Ist $\beta \in \text{Ord}$ und $X \subset \beta$, so folgt $\alpha \leq \beta$.

BEWEIS. 1. Angenommen, $Z = \{x \in C \mid f(x) < x\} \neq \emptyset$ und $z = \min(Z)$. Dann ist $f(z) < z$, also $f(z) \in C$ und $f(f(z)) < f(z)$, ein Widerspruch zur Minimalität von z .

2. Sei $f: X \rightarrow C$ eine Ordnungsisomorphie. Dann ist $f: X \rightarrow C \hookrightarrow X$ ordnungstreu. Für alle $u \in X$ ist $f(u) \geq u$ nach 1. und $f(u) \in C$, also auch $u \in C$. Daher ist $C = X$.

3. Sei $f = \{(x, u) \mid x \in X, u \in \text{Ord}, X(x) \cong u\}$.

f ist eine Funktion: Seien $(x, u), (x, u') \in f$. Dann ist $u \cong u'$ und daher $u = u'$ nach 2.

f ist ordnungstreu, $\mathcal{D}(f) \subset X$ und $\mathcal{W}(f) \subset \text{Ord}$ sind Anfangsstücke: Sei $x \in \mathcal{D}(f)$, $y \in X(x)$, $u = f(x)$ und $v < u$. Dann gibt es eine Ordnungsisomorphie $g: X(x) \rightarrow u$, und daher sind auch $g \upharpoonright X(y): X(y) = X(x)(y) \rightarrow u(g(y)) = g(y)$ und $g \upharpoonright X(g^{-1}(v)) \rightarrow v$ Ordnungsisomorphismen, also $y \in \mathcal{D}(f)$, $f(y) = g(y) < u = f(x)$ und $v \in \mathcal{W}(f)$.

Nach dem Ersetzungsaxiom ist $\mathcal{W}(f)$ eine Menge, also $\mathcal{W}(f) = \alpha \in \text{Ord}$. Wäre $\mathcal{D}(f) \subsetneq X$ und $a = \min(X \setminus \mathcal{D}(f))$, so folgte $\mathcal{D}(f) = X(a) \cong \alpha$ und daher $(a, \alpha) \in f$ ein Widerspruch. Die Eindeutigkeit von α folgt nach 2.

Sei nun $\beta \in \text{Ord}$, $X \subset \beta$ und $f: \alpha \rightarrow X \subset \beta$ ordnungstreu. Nach 1. ist $x \leq f(x) < \beta$ für alle $x \in \alpha$, also $\alpha \subset \beta$ und daher $\alpha \leq \beta$. \square

Satz 1.2.12 (Wohlordnungssatz). *Sei a eine Menge. Dann gibt es ein $\alpha \in \text{Ord}$ mit $a \approx \alpha$, und es gibt eine Wohlordnung auf a . Ist a unendlich, so gibt es eine injektive Abbildung $f: \omega \rightarrow a$, und $f[\omega] \subset a$ ist eine abzählbare Teilmenge.*

BEWEIS. Nach dem Auswahlaxiom gibt es eine Abbildung $c: \mathbb{P}a \setminus \{\emptyset\} \rightarrow a$, so dass $c(x) \in x$ für alle $x \in \mathbb{P}a \setminus \{\emptyset\}$. Sei Ω die Klasse aller Funktionen f mit $\mathcal{D}(f) \in \text{Ord}$, $\mathcal{W}(f) \subset a$, so dass

$$f[\alpha] \neq a \quad \text{und} \quad f(\alpha) = c(a \setminus f[\alpha]) \quad \text{für alle } \alpha \in \mathcal{D}(f) \quad [\implies f \text{ injektiv}].$$

A. Für alle $f, g \in \Omega$ ist $f \subset g$ oder $g \subset f$

Beweis von A. Seien $f, g \in \Omega$ und o.B.d.A. $\mathcal{D}(f) \subset \mathcal{D}(g)$. Wir zeigen: $\forall x \in \mathcal{D}(f) [f(x) = g(x)]$ [dann ist $f \subset g$]. Angenommen, $Z = \{x \in \mathcal{D}(f) \mid f(x) \neq g(x)\} \neq \emptyset$ und $z = \min(Z)$. Dann ist $f \upharpoonright z = g \upharpoonright z$, also $f[z] = g[z]$ und daher $f(z) = g(z)$, ein Widerspruch.

Nach **A.** ist $F = \bigcup \Omega$ eine injektive Funktion, $\mathcal{D}(F) = \bigcup \{\mathcal{D}(f) \mid f \in \Omega\} \subset \text{Ord}$ ist ein Anfangsstück, und $\mathcal{W}(F) \subset a$. Aufgrund des Ersetzungsaxioms ist $\mathcal{D}(F) = F^{-1}[\mathcal{W}(F)]$ eine Menge, also $\mathcal{D}(F) \in \text{Ord}$, und wir zeigen $\mathcal{W}(F) = a$. Angenommen, $\mathcal{W}(F) \subsetneq a$. Dann definieren wir $\tilde{F}: \mathcal{D}(F)^+ \rightarrow a$ durch $\tilde{F} \upharpoonright \mathcal{D}(F) = F$ und $\tilde{F}(\mathcal{D}(F)) = c(a \setminus \mathcal{W}(F))$. Dann folgt $\tilde{F} \in \Omega$ und $F \subsetneq \tilde{F}$, ein Widerspruch.

Ist a unendlich, so ist $\alpha \geq \omega$ und $F \upharpoonright \omega: \omega \rightarrow a$ eine injektive Abbildung. \square

Definition und Satz 1.2.13. *Sei (X, \leq) eine teilgeordnete Menge.*

1. (Hausdorff'sches Maximalprinzip) *Die Menge \mathcal{S} aller Ketten in X besitzt (bezüglich \subset) maximale Elemente.*
2. (Zorn'sches Lemma) *Habe jede Kette in X eine obere Schranke. Dann gibt es zu jedem $a \in X$ ein in X maximales Element a^* mit $a^* \geq a$.*

(X, \leq) heißt *induktiv geordnet*, wenn $X \neq \emptyset$ und jede Kette in X eine obere Schranke besitzt.

Jede induktive geordnete Menge besitzt maximale Elemente.

BEWEIS. 1. Angenommen, \mathcal{S} habe keine maximalen Elemente. Dann gibt nach Satz 1.1.10 eine Abbildung $c: \mathcal{S} \rightarrow \mathcal{S}$, so dass $c(S) \supsetneq S$ für alle $S \in \mathcal{S}$. Sei Ω die Klasse aller Funktionen f mit $\mathcal{D}(f) \in \text{Ord}$ und $\mathcal{W}(f) \subset \mathcal{S}$, so dass für alle $\alpha \in \mathcal{D}(f)$ gilt:

$$\forall x, y \in \alpha [x < y \implies f(x) \subsetneq f(y)] \quad \text{(dann ist } \bigcup f[\alpha] \in \mathcal{S}\text{),} \quad \text{und} \quad f(\alpha) = c\left(\bigcup f[\alpha]\right).$$

Dann ist $f(x) \subsetneq f(\alpha)$ für alle $x \in \alpha$ und daher f injektiv.

A. Für alle $f, g \in \Omega$ ist $f \subset g$ oder $g \subset f$

Beweis von A. Seien $f, g \in \Omega$ und o.B.d.A. $\mathcal{D}(f) \subset \mathcal{D}(g)$. Wir zeigen: $\forall x \in \mathcal{D}(f) [f(x) = g(x)]$ [dann ist $f \subset g$]. Angenommen, $Z = \{x \in \mathcal{D}(f) \mid f(x) \neq g(x)\} \neq \emptyset$ und $z = \min(Z)$. Dann ist $f \upharpoonright z = g \upharpoonright z$, also $f[z] = g[z]$ und daher $f(z) = g(z)$, ein Widerspruch.

Nach **A.** ist $F = \bigcup \Omega$ eine injektive Funktion, $\mathcal{D}(F) = \bigcup \{\mathcal{D}(f) \mid f \in \Omega\} \subset \text{Ord}$ ist ein Anfangsstück, $\mathcal{W}(F) \subset \mathcal{S}$, für alle $a, b \in \mathcal{W}(F)$ ist $a \subset b$ oder $b \subset a$, und daher folgt $\bigcup \mathcal{W}(F) \in \mathcal{S}$. Aufgrund des Ersetzungsaxioms ist $\mathcal{D}(F) = F^{-1}[\mathcal{W}(F)]$ eine Menge, und daher ist $\mathcal{D}(F) \in \text{Ord}$. Definiert man nun $\tilde{F}: \mathcal{D}(F)^+ \rightarrow \mathcal{S}$ durch $\tilde{F} \upharpoonright \mathcal{D}(F) = F$ und $\tilde{F}(\mathcal{D}(F)) = c(\bigcup \mathcal{W}(F))$, so ist $\tilde{F} \in \Omega$ und $F \subsetneq \tilde{F}$, ein Widerspruch!

2. Nach 1. existiert eine maximale Kette in X , und diese hat nach Voraussetzung eine obere Schranke. Diese ist ein maximales Element von X . \square

1.3. Kardinalzahlen

Definition 1.3.1. Eine Ordinalzahl $\alpha \in \text{Ord}$ heißt *Kardinalzahl*, wenn $\alpha = \min\{x \in \text{Ord} \mid \alpha \approx x\}$. Card bezeichne die Klasse aller Kardinalzahlen.

Definition und Satz 1.3.2. Zu jeder Menge a gibt es genau eine Kardinalzahl κ mit $a \approx \kappa$.

$\kappa = |a|$ heißt *Kardinalität* oder *Mächtigkeit* von a . Wir definieren $|a| = \infty \iff |a| \geq \omega$, und $|a| < \infty \iff |a| < \omega$.

BEWEIS. Nach Satz 1.2.12. \square

Nach Satz 1.2.9 ist $\omega \subset \text{Card}$, $\omega \in \text{Card}$, und für Mengen a, b gilt: $|a| = |b| \iff a \approx b$.

Im Folgenden benutzen wir die Bezeichnung ω für die abzählbare Kardinalzahl und \mathbb{N}_0 für die (naiven) natürlichen Zahlen. Es ist $|\mathbb{N}_0| = |\mathbb{N}| = \omega$.

Definition 1.3.3. Seien $\alpha, \beta \in \text{Card}$ und b eine Menge mit $|b| = \beta$ und $b \cap \alpha = \emptyset$ (siehe Satz 1.1.7.3). Dann definieren wir

$$\alpha + \beta = |\alpha \cup b| \quad (\text{unabhängig von der Wahl von } b), \quad \alpha\beta = |\alpha \times \beta| \quad \text{und} \quad \alpha^\beta = |\text{Abb}(\beta, \alpha)|.$$

Für endliche Mengen verallgemeinern diese Definitionen den naiven Anzahlbegriff. Ist $n \in \mathbb{N}_0$ und a eine Menge mit n Elementen (im naiven Sinne), so ist $|a| = \underline{n}$ (wir schreiben dann wieder wie üblich $|a| = n$). Ferner gilt für alle $m, n \in \mathbb{N}_0$: $\underline{m+n} = \underline{m} + \underline{n}$, $\underline{mn} = \underline{m} \underline{n}$ und $\underline{m}^{\underline{n}} = \underline{m}^n$.

Für $\alpha \in \text{Card}$ und $n \in \mathbb{N}_0$ sei α^n rekursiv definiert durch $\alpha^0 = \underline{1}$ und $\alpha^{n+1} = \alpha^n \alpha$. Dann ist $\alpha^n = \alpha^n$ für alle $n \in \mathbb{N}_0$.

Satz 1.3.4. Seien a, b, a', b' Mengen.

1. Es sind äquivalent:

(a) $|a| \leq |b|$.

(b) Es gibt eine injektive Abbildung $f: a \rightarrow b$.

(c) Ist $a \neq \emptyset$, so gibt es eine surjektive Abbildung $g: b \rightarrow a$.

2. Sei $|a| \leq |a'|$ und $|b| \leq |b'|$. Dann folgt $|a| + |b| \leq |a'| + |b'|$, $|a||b| \leq |a'||b'|$ und $|a|^{|b|} \leq |a'|^{|b'|}$.

3. $|a \times b| = |a||b|$, $|\text{Abb}(a, b)| = |b|^{|a|}$, $|a \cup b| + |a \cap b| = |a| + |b|$. Insbesondere: $|a \cup b| \leq |a| + |b|$, mit Gleichheit, falls $a \cap b = \emptyset$.

4. Für alle $\alpha, \beta, \gamma \in \text{Card}$ gilt: $\alpha + \beta = \beta + \alpha$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, $\alpha\beta = \beta\alpha$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$, $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ und $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$.

BEWEIS. 1. (a) \Leftrightarrow (b) Seien $\varphi: a \rightarrow |a|$ und $\psi: b \rightarrow |b|$ bijektiv. Ist $|a| \leq |b|$, so ist $|a| \subset |b|$ und daher $\psi^{-1} \circ \varphi: a \rightarrow b$ injektiv.

Sei nun $f: a \rightarrow b$ injektiv. Dann ist auch $\psi \circ f \circ \varphi^{-1}: |a| \rightarrow |b|$ injektiv, also $X = \mathcal{W}(\psi \circ f \circ \varphi^{-1}) \subset |b|$ und $|a| = |X| \leq |b|$ nach Satz 1.2.11.3.

(b) \Rightarrow (c) Sei $f: a \rightarrow b$ injektiv und $x \in a$. Dann ist $g = f^{-1} \cup ((b \setminus f[a]) \times \{x\}): b \rightarrow a$ surjektiv.

(c) \Rightarrow (b) Ist $a = \emptyset$, so ist $\emptyset: a \rightarrow b$ eine injektive Abbildung. Sei also $a \neq \emptyset$. Ist $g: b \rightarrow a$ eine surjektive Abbildung, so ist g^{-1} eine Relation mit $\mathcal{D}(g^{-1}) = a$. Nach Satz 1.1.10.2 gibt es eine Funktion f mit $f \subset g^{-1}$ und $\mathcal{D}(f) = a$. Wegen $f^{-1} \subset (g^{-1})^{-1} = g$ ist f eine injektive Funktion, und $\mathcal{W}(f) \subset \mathcal{W}(g^{-1}) = b$.

2., 3. und 4. Übung. □

Satz 1.3.5 (Cantor). *Für jede Menge a ist $2^{|a|} = |\mathbb{P}(a)| > |a|$.*

BEWEIS. Für $X \subset a$ sei $1_X: a \rightarrow \{0, 1\}$ die charakteristische Funktion von X . Dann ist $X \mapsto 1_X$ eine bijektive Abbildung $\mathbb{P}(a) \rightarrow \text{Abb}(a, \{0, 1\})$, und daher $|\mathbb{P}(a)| = |\text{Abb}(a, \{0, 1\})| = 2^{|a|}$.

Angenommen, es sei $|a| \geq |\mathbb{P}(a)|$. Dann gibt es eine surjektive Abbildung $g: a \rightarrow \mathbb{P}(a)$, und es ist $c = \{x \in a \mid x \notin g(x)\} \subset a$. Sei $z \in a$ mit $g(z) = c$. Ist nun $z \in c = g(z)$, so folgt $z \notin g(z)$, und ist $z \notin c = g(z)$, so folgt $z \in g(z)$, ein Widerspruch. □

Satz 1.3.6.

1. Seien $\alpha, \beta \in \text{Card}$, $\beta \leq \alpha$ und $\alpha \geq \omega$. Dann ist $\alpha + \beta = \alpha\beta = \alpha$. Insbesondere ist $\alpha^n = \alpha$ für alle $n \in \mathbb{N}$.
2. Sei a eine unendliche Menge, $b \subset a$ und $|b| < |a|$. Dann ist $|a \setminus b| = |a|$.

BEWEIS. 1. Wir führen den Beweis in mehreren Schritten.

A. Für jede abzählbare Menge X ist $|X| = |X \times \{1, 2\}| = |X| + |X| = |X \times X|$.

Beweis von A. Es genügt, die Behauptung für $X = \mathbb{N}$ zu zeigen. Die Abbildung $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, definiert durch $f(m, n) = 2^{m-1}(2n - 1)$, ist bijektiv. Daher folgt

$$|\mathbb{N}| = |\mathbb{N} \times \{1\}| \leq |\mathbb{N} \times \{1, 2\}| = |\mathbb{N} \times \{1\}| + |\mathbb{N} \times \{2\}| = |\mathbb{N}| + |\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$

B. Für jede unendliche Menge a und jede höchstens abzählbare Menge F ist $|a \cup F| = |a|$.

Beweis von B. Nach Satz 1.2.12 besitzt a eine abzählbare Teilmenge Z , und es folgt

$$|a| \leq |a \cup F| \leq |Z \cup F| + |a \setminus Z| \leq |Z| + |F| + |a \setminus Z| \leq |Z| + |Z| + |a \setminus Z| = |Z| + |a \setminus Z| = |a|.$$

C. $\alpha + \beta = \alpha$.

Beweis von C. Es genügt, $\alpha + \alpha = \alpha$ zu zeigen [denn dann folgt $\alpha \leq \alpha + \beta \leq \alpha + \alpha = \alpha$]. Wegen $|\alpha \times \{0, 1\}| = |\alpha \times \{0\}| + |\alpha \times \{1\}| = \alpha + \alpha$ genügt es, die Existenz einer bijektiven Abbildung $F: \alpha \times \{0, 1\} \rightarrow \alpha$ zu zeigen. Sei Ω die Menge aller bijektiven Abbildungen $f: X \times \{0, 1\} \rightarrow X$ mit einer unendlichen Teilmenge $X \subset \alpha$. Wegen $\omega \subset \alpha$ und **A.** ist $\Omega \neq \emptyset$. Ist $\mathcal{S} \subset \Omega$ eine Kette, so folgt $\bigcup \mathcal{S} \in \Omega$. Daher besitzt Ω nach dem Zorn'schen Lemma ein maximales Element $F: C \times \{0, 1\} \rightarrow C$ mit einer unendlichen Teilmenge $C \subset \alpha$. Ist $\alpha \setminus C$ endlich, so folgt mit **B.**

$$|\alpha \times \{0, 1\}| = |C \times \{0, 1\}| + |(\alpha \setminus C) \times \{0, 1\}| = |C \times \{0, 1\}| = |C| = |C| + |\alpha \setminus C| = |\alpha|.$$

Ist $\alpha \setminus C$ unendlich, so gibt es eine abzählbare Menge $B \subset \alpha \setminus C$, und nach **A.** gibt es eine bijektive Abbildung $g: B \times \{0, 1\} \rightarrow B$. Definiert man $F^*: (B \cup C) \times \{0, 1\} \rightarrow B \cup C$ durch $F^* \upharpoonright C \times \{0, 1\} = F$ und $F^* \upharpoonright B \times \{0, 1\} = g$, so ist $F^* \in \Omega$ und $F \subsetneq F^*$, ein Widerspruch.

D. $\alpha\beta = \alpha$.

Beweis von D. Es genügt, $\alpha^2 = \alpha$ zu zeigen [denn dann folgt $\alpha \leq \alpha\beta \leq \alpha^2 = \alpha$]. Sei Ω die Menge aller bijektiven Abbildungen $f: X \times X \rightarrow X$ mit einer unendlichen Teilmenge $X \subset \alpha$. Wegen $\omega \subset \alpha$ und **A.** ist $\Omega \neq \emptyset$. Ist $\mathcal{S} \subset \Omega$ eine Kette, so folgt $\bigcup \mathcal{S} \in \Omega$. Daher besitzt Ω nach dem Zorn'schen Lemma ein maximales Element $F: C \times C \rightarrow C$ mit einer unendlichen Teilmenge $C \subset \alpha$.

Wir nehmen nun zuerst an, es sei $|\alpha \setminus C| > |C|$. Dann gibt es eine Teilmenge $B \subset \alpha \setminus C$ mit $|B| = |C|$. Es folgt $(B \cup C) \times (B \cup C) = (C \times C) \cup D$ mit $D = (B \times B) \cup (B \times C) \cup (C \times B)$, es ist $(C \times C) \cap D = \emptyset$ und $|B \times B| = |B \times C| = |C \times B| = |B|$. Nach **C.** ist $|D| = |B|$, und daher gibt es eine bijektive Abbildung $g: D \rightarrow B$. Definiert man $F^*: (B \cup C) \times (B \cup C) \rightarrow B \cup C$ durch $F^* \upharpoonright C \times C = F$ und $F^* \upharpoonright D = g$, so ist $F^* \in \Omega$ und $F \subsetneq F^*$, ein Widerspruch.

Daher ist $|\alpha \setminus C| \leq |C|$, es folgt $\alpha = |\alpha \setminus C| + |C| = |C|$ und daher $\alpha^2 = |\alpha \times \alpha| = \alpha$. Mittels Induktion folgt $\alpha^n = \alpha$ für alle $n \in \mathbb{N}$.

2. Es ist entweder $a \setminus b$ oder b unendlich, und daher folgt $|a| = |a \setminus b| + |b| = \max\{|a \setminus b|, |b|\} = |a \setminus b|$, da $|b| < |a|$. \square

Satz 1.3.7. Sei $(a_i)_{i \in I}$ eine Familie von Mengen und $\alpha \in \text{Card}$.

1. Ist $|a_i| \leq \alpha$ für alle $i \in I$, so folgt $|\bigcup\{a_i \mid i \in I\}| \leq |I|\alpha$.
2. Sei $|a_i| \geq \alpha$ und $a_i \cap a_j = \emptyset$ für alle $i, j \in I$ mit $i \neq j$. Dann folgt $|\bigcup\{a_i \mid i \in I\}| \geq |I|\alpha$.

BEWEIS. 1. Sei o. E. $a_i \neq \emptyset$ für alle $i \in I$. Dann gibt es surjektive Abbildungen $g_i: \alpha \rightarrow a_i$, und die Abbildung $g: I \times \alpha \rightarrow \bigcup\{a_i \mid i \in I\}$, definiert durch $g(i, x) = g_i(x)$, ist ebenfalls surjektiv. Daher folgt $|\bigcup\{a_i \mid i \in I\}| \leq |I \times \alpha| = |I|\alpha$.

2. Für $i \in I$ sei $f_i: \alpha \rightarrow a_i$ eine injektive Abbildung. Dann ist $f: I \times \alpha \rightarrow \bigcup\{a_i \mid i \in I\}$, definiert durch $f(i, x) = f_i(x)$, ebenfalls eine injektive Abbildung. \square

Satz 1.3.8. Sei a eine Menge, $\mathcal{F}(a) = \bigcup\{a^n \mid n \in \mathbb{N}_0\}$ die Menge aller endlichen Folgen in a und $\mathcal{P}(a)$ die Menge aller endlichen Teilmengen von a . Dann ist $|a| \leq |\mathcal{P}(a)| \leq |\mathcal{F}(a)| \leq \max\{|a|, \omega\}$.

BEWEIS. Die Abbildung, die jeder endlichen Folge ihre Gliedermenge zuordnet, ist eine surjektive Abbildung $\mathcal{F}(a) \rightarrow \mathcal{P}(a)$, und daher folgt $|a| \leq |\mathcal{P}(a)| \leq |\mathcal{F}(a)|$. Nach Satz 1.3.6 folgt (mit Induktion) $|a^n| \leq \max\{|a|, \omega\}$ für alle $n \in \mathbb{N}$, und nach Satz 1.3.7 ist $|\mathcal{F}(a)| \leq \omega \max\{|a|, \omega\} = \max\{|a|, \omega\}$. \square

1.4. Kategorien und Funktoren

Definition 1.4.1. Eine *Kategorie* \mathcal{C} besteht aus

- einer Klasse $\text{Ob } \mathcal{C}$ (deren Elemente heißen *Objekte* von \mathcal{C} , man schreibt meist kurz $\mathcal{C} = \text{Ob } \mathcal{C}$);
- einer Klasse paarweise disjunkter Mengen $\{\text{Mor}_{\mathcal{C}}(A, B) \mid (A, B) \in \mathcal{C} \times \mathcal{C}\}$ (die Elemente von $\text{Mor}(A, B) = \text{Mor}_{\mathcal{C}}(A, B)$ heißen *Morphismen* oder *Pfeile* von A nach B [Schreibweise: $f: A \rightarrow B$ oder $A \xrightarrow{f} B$]; die Klasse $\text{Mor}(\mathcal{C}) = \bigcup\{\text{Mor}_{\mathcal{C}}(A, B) \mid (A, B) \in \mathcal{C} \times \mathcal{C}\}$ heißt *Klasse der Morphismen* von \mathcal{C});
- einer Klasse ausgezeichneter Elemente $\{\text{id}_A \in \text{Mor}_{\mathcal{C}}(A, A) \mid A \in \mathcal{C}\}$ (id_A heißt *Identität auf* A);
- einer Klasse von Abbildungen $\{\circ: \text{Mor}_{\mathcal{C}}(A, B) \times \text{Mor}_{\mathcal{C}}(B, C) \rightarrow \text{Mor}_{\mathcal{C}}(A, C) \mid (A, B, C) \in \mathcal{C}^3\}$, geschrieben in der Form $(f, g) \mapsto g \circ f$ (genannt *Verknüpfungen* oder *Verkettungen*),

so dass gilt:

- (C1) Für alle $A, B, C, D \in \mathcal{C}$ und alle $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ ist $h \circ (g \circ f) = (h \circ g) \circ f$.
- (C2) Für alle $A, B \in \mathcal{C}$ und alle $f: A \rightarrow B$ ist $\text{id}_B \circ f = f \circ \text{id}_A = f$.

Ein Morphismus $f \in \text{Mor}_{\mathcal{C}}(A, B)$ heißt *Isomorphismus*, wenn es einen Morphismus $g \in \text{Mor}_{\mathcal{C}}(B, A)$ gibt mit $g \circ f = \text{id}_A$ und $f \circ g = \text{id}_B$ [dann ist g eindeutig bestimmt und heißt der zu f *inverse Isomorphismus*, $g = f^{-1}$]. Zwei Objekte $A, B \in \mathcal{C}$ heißen *isomorph*, $A \cong B$, wenn es einen Isomorphismus $f: A \rightarrow B$ gibt. Isomorphie ist eine Äquivalenzrelation auf \mathcal{C} [denn: Die Identitäten sind Isomorphismen, und die Verknüpfung zweier Isomorphismen ist wieder ein Isomorphismus].

Ist $A \in \mathcal{C}$, so nennt man die Elemente von $\text{End}_{\mathcal{C}}(A) = \text{Mor}_{\mathcal{C}}(A, A)$ *Endomorphismen* von A . $(\text{End}_{\mathcal{C}}(A), \circ)$ ist ein Monoid mit neutralem Element id_A .

Ein Objekt $E \in \mathcal{C}$ heißt

- *initial*, wenn $|\text{Mor}_{\mathcal{C}}(E, A)| = 1$ für alle $A \in \mathcal{C}$;
- *final*, wenn $|\text{Mor}_{\mathcal{C}}(A, E)| = 1$ für alle $A \in \mathcal{C}$;

Satz 1.4.2. *Sei \mathcal{C} eine Kategorie und seien E, E' initiale [finale] Objekte von \mathcal{C} . Dann gibt es genau einen Isomorphismus $E \rightarrow E'$.*

BEWEIS. Seien $E, E' \in \mathcal{C}$ initial. Dann ist $\text{Mor}_{\mathcal{C}}(E, E) = \{\text{id}_E\}$, $\text{Mor}_{\mathcal{C}}(E', E') = \{\text{id}_{E'}\}$, $\text{Mor}_{\mathcal{C}}(E, E') = \{f\}$, $\text{Mor}_{\mathcal{C}}(E', E) = \{f'\}$ und daher notwendig $f' \circ f = \text{id}_E$ und $f \circ f' = \text{id}_{E'}$. \square

Beispiele 1.4.3.

1. **Mg**, die Kategorie der Mengen. Objekte sind Mengen, Morphismen sind Abbildungen, Isomorphismen sind bijektive Abbildungen. Zwei Mengen A, B sind isomorph in **Mg**, wenn $|A| = |B|$. \emptyset ist das einzige initiale Objekt in **Mg**, alle Einermengen sind finale Objekte in **Mg**.

2. **WO**, die Kategorie der wohlgeordneten Mengen. Objekte sind wohlgeordnete Mengen, Morphismen sind ordnungstreue Abbildungen, Isomorphismen sind Ordnungsisomorphismen. \emptyset ist ein initiales Objekt in **WO**, und **WO** hat keine finalen Objekte.

3. **Grp**, die Kategorie der Gruppen. Objekte sind Gruppen, Morphismen sind Gruppenhomomorphismen, Isomorphismen sind Gruppenisomorphismen. Jede triviale Gruppe (bestehend aus einem Element) ist initiales und finales Element in **Grp**. **Ab** bezeichne die Kategorie der abelschen Gruppen, und für einen Körper k bezeichne **Vek_k** die Kategorie der k -Vektorräume.

Ist $\mathcal{C} = \mathbf{Ab}$ oder $\mathcal{C} = \mathbf{Vek}_k$, so hat für alle $A, B \in \mathcal{C}$ die Menge $\text{Mor}_{\mathcal{C}}(A, B)$ die Struktur einer abelschen Gruppe (bei wertweiser Addition der Homomorphismen), die Verknüpfung von Morphismen ist bilinear, und $\text{End}_{\mathcal{C}}(A) = (\text{End}_{\mathcal{C}}(A), +, \circ)$ ist ein Ring, der *Endomorphismenring* von A .

4. **Rg**, die Kategorie der (unitären) Ringe. Objekte sind Ringe, Morphismen sind (unitäre) Ringhomomorphismen. \mathbb{Z} ist ein initiales Objekt und jeder Nullring ist ein finales Objekt in **Rg**.

5. Sei $(X, <)$ eine teilgeordnete Menge. Dann definiert man die Kategorie $\mathcal{C}(X, <)$ wie folgt: Objekte sind die Elemente $a \in X$, für $a, b \in X$ sei

$$\text{Mor}_{\mathcal{C}(X, <)}(a, b) = \begin{cases} \{(a, b)\}, & \text{falls } a \leq b, \\ \emptyset & \text{sonst.} \end{cases}$$

Dann gibt es nur eine mögliche Verknüpfung von Morphismen, und für $a \in X$ ist $\text{id}_a = (a, a)$.

6. Sei \mathcal{C} eine Kategorie und $A \in \mathcal{C}$. Dann definiert man die Kategorie \mathcal{C}_A wie folgt: Objekte sind Morphismen $f: X \rightarrow A$ in \mathcal{C} . Sind $f: X \rightarrow A$ und $g: Y \rightarrow A$ Objekte in \mathcal{C}_A , so definiert man $\text{Mor}_{\mathcal{C}_A} = \{h \in \text{Mor}_{\mathcal{C}}(X, Y) \mid g \circ h = f\}$.

$$\begin{array}{ccc} X & \xrightarrow{h} & Y \\ & \searrow f & \swarrow g \\ & & A \end{array}$$

Definition 1.4.4. Sei \mathcal{C} eine Kategorie und $\mathbf{A} = (A_i)_{i \in I}$ eine Familie in \mathcal{C} . Dann seien die Kategorien $\mathcal{C}_{\mathbf{A}}$ und $\mathcal{C}^{\mathbf{A}}$ wie folgt definiert:

Objekte von $\mathcal{C}_{\mathbf{A}}$ sind Familien von Morphismen $\varphi = (\varphi_i: X \rightarrow A_i)_{i \in I}$ in \mathcal{C} . Sind $\varphi = (\varphi_i: X \rightarrow A_i)_{i \in I}$, $\psi = (\psi_i: Y \rightarrow A_i)_{i \in I} \in \mathcal{C}_{\mathbf{A}}$, so besteht $\text{Mor}_{\mathcal{C}_{\mathbf{A}}}(\varphi, \psi)$ aus allen Morphismen $f: X \rightarrow Y$ in \mathcal{C} , so dass $\forall i \in I [\psi_i \circ f = \varphi_i]$. Ein *Produkt* der Familie \mathbf{A} ist ein finales Objekt in der Kategorie $\mathcal{C}_{\mathbf{A}}$.

Explizit: Eine Familie von Morphismen $\mathbf{p} = (p_i: P \rightarrow A_i)_{i \in I}$ ist ein Produkt von $(A_i)_{i \in I}$, wenn es zu jeder Familie $\varphi = (\varphi_i: X \rightarrow A_i)_{i \in I}$ genau einen Morphismus $\varphi: X \rightarrow P$ gibt, so dass $p_i \circ \varphi = \varphi_i$ für alle $i \in I$. Man nennt dann auch P das Produkt der Familie $(A_i)_{i \in I}$ und $(p_i)_{i \in I}$ die Familie der kanonischen Projektionen.

Objekte von $\mathcal{C}^{\mathbf{A}}$ sind Familien von Morphismen $\varphi = (\varphi_i: A_i \rightarrow X)_{i \in I}$ in \mathcal{C} . Sind $\varphi = (\varphi_i: A_i \rightarrow X)_{i \in I}$, $\psi = (\psi_i: A_i \rightarrow Y)_{i \in I} \in \mathcal{C}^{\mathbf{A}}$, so besteht $\text{Mor}_{\mathcal{C}^{\mathbf{A}}}(\varphi, \psi)$ aus allen Morphismen $f: X \rightarrow Y$ in \mathcal{C} , so dass $\forall i \in I [f \circ \varphi_i = \psi_i]$. Ein *Koprodukt* der Familie \mathbf{A} ist ein initiales Objekt in der Kategorie $\mathcal{C}^{\mathbf{A}}$.

Explizit: Eine Familie von Morphismen $\varepsilon = (\varepsilon_i: A_i \rightarrow C)_{i \in I}$ ist ein Koprodukt von $(A_i)_{i \in I}$, wenn es zu jeder Familie $\varphi = (\varphi_i: A_i \rightarrow X)_{i \in I}$ genau einen Morphismus $\varphi: C \rightarrow X$ gibt, so dass $\varphi \circ \varepsilon_i = \varphi_i$ für alle $i \in I$. Man nennt dann auch C das Koprodukt der Familie $(A_i)_{i \in I}$ und $(\varepsilon_i)_{i \in I}$ die Familie der kanonischen Einlagerungen.

Nach Satz 1.4.2 sind Produkt und Koprodukt einer Familie von Objekten bis auf (eindeutige) Isomorphie eindeutig bestimmt.

Beispiele 1.4.5.

1. Sei $\mathbf{A} = (A_i)_{i \in I}$ eine Familie von Mengen, $P = \prod_{i \in I} A_i$ und $(p_i: P \rightarrow A_i)_{i \in I}$ die Familie der kanonischen Projektionen. Dann ist $(p_i)_{i \in I}$ ein Produkt von \mathbf{A} in \mathbf{Mg} .

Sei $C = \bigcup_{i \in I} (A_i \times \{i\})$ eine *disjunkte Vereinigung* von \mathbf{A} . Für $i \in I$ sei $\varepsilon_i: A_i \rightarrow C$ definiert durch $\varepsilon_i(x) = (x, i)$. Dann ist $(\varepsilon_i)_{i \in I}$ ein Koprodukt von \mathbf{A} in \mathbf{Mg} .

2. Sei $\mathbf{A} = (A_i)_{i \in I}$ eine Familie von (additiven) abelschen Gruppen,

$$P = \prod_{i \in I} A_i \quad \text{und} \quad C = \prod_{i \in I} A_i = \bigoplus_{i \in I} A_i = \{(a_i)_{i \in I} \mid a_i = 0 \text{ für fast alle } i \in I\}$$

(mit komponentenweiser Addition; hier ist die Bezeichnung nicht einheitlich).

Sei $(p_i: P \rightarrow A_i)_{i \in I}$ die Familie der kanonischen Projektionen und $(\varepsilon_i: A_i \rightarrow C)_{i \in I}$ die Familie der kanonischen Einlagerungen, definiert durch $\varepsilon_i(a_i) = (\dots, 0, a_i, 0, \dots)$. Dann ist $(p_i)_{i \in I}$ ein Produkt und $(\varepsilon_i)_{i \in I}$ ein Koprodukt von \mathbf{A} in \mathbf{Ab} [der Nachweis ist "straightforward"]. Ferner gilt

$$p_i \circ \varepsilon_j = \begin{cases} 0, & \text{falls } i \neq j, \\ \text{id}_{A_i}, & \text{falls } i = j, \end{cases} \quad \text{und} \quad c = \sum_{i \in I} \varepsilon_i \circ p_i(c) \quad \text{für alle } c \in C.$$

Definition 1.4.6. Sei \mathcal{C} eine Kategorie. Dann definiert man die *Gegenkategorie* \mathcal{C}^{op} wie folgt:

- $\text{Ob } \mathcal{C}^{\text{op}} = \text{Ob } \mathcal{C}$; für $A, B \in \mathcal{C}$ sei $\text{Mor}_{\mathcal{C}^{\text{op}}}(A, B) = \text{Mor}_{\mathcal{C}}(B, A)$;
- für $A, B, C \in \mathcal{C}$, $f \in \text{Mor}_{\mathcal{C}}(A, B) = \text{Mor}_{\mathcal{C}^{\text{op}}}(B, A)$, $g \in \text{Mor}_{\mathcal{C}}(B, C) = \text{Mor}_{\mathcal{C}^{\text{op}}}(C, B)$ definiert man $f \circ_{\text{op}} g = g \circ f \in \text{Mor}_{\mathcal{C}}(A, C) = \text{Mor}_{\mathcal{C}^{\text{op}}}(C, A)$.

Bemerkungen 1.4.7. Sei \mathcal{C} eine Kategorie. Dann ist $(\mathcal{C}^{\text{op}})^{\text{op}} = \mathcal{C}$, initiale Objekte von \mathcal{C} sind finale Objekte von \mathcal{C}^{op} , und Produkte in \mathcal{C} sind Koprodukte in \mathcal{C}^{op} .

Definition 1.4.8. \mathcal{C} und \mathcal{D} seien Kategorien.

Ein (*kovarianter*) *Funktor* $T: \mathcal{C} \rightarrow \mathcal{D}$ besteht aus

- einer Abbildung $T: \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{D}$, $A \mapsto T(A) = TA$;

• Für alle $(A, B) \in \mathcal{C} \times \mathcal{C}$ einer Abbildung $T = T_{A,B}: \text{Mor}_{\mathcal{C}}(A, B) \rightarrow \text{Mor}_{\mathcal{D}}(TA, TB)$, $f \mapsto Tf$, so dass gilt:

F1. Für alle $A, B, C \in \mathcal{C}$ und $f: A \rightarrow B$, $g: B \rightarrow C$ ist $T(g \circ f) = Tg \circ Tf$.

F2. Für alle $A \in \mathcal{C}$ ist $T(\text{id}_A) = \text{id}_{TA}$.

Ein *kontravarianter Funktor* $T: \mathcal{C} \rightarrow \mathcal{D}$ ist eine Funktor $T: \mathcal{C}^{\text{op}} \rightarrow \mathcal{D}$.

Explizit: Ist T ein kontravarianter Funktor und $f \in \text{Mor}_{\mathcal{C}}(A, B)$, so ist $Tf \in \text{Mor}_{\mathcal{D}}(TB, TA)$, und für $g \in \text{Mor}_{\mathcal{C}}(B, C)$ ist $T(g \circ f) = Tf \circ Tg$.

Beispiele 1.4.9.

1. Sei \mathcal{C} eine Kategorie. Der identische Funktor $\text{Id}: \mathcal{C} \rightarrow \mathcal{C}$ ist definiert als identische Abbildung auf Objekten und Morphismen.

2. Seien \mathcal{C}, \mathcal{D} Kategorien und $D \in \mathcal{D}$. Der konstante Funktor $T_D: \mathcal{C} \rightarrow \mathcal{D}$ ist definiert durch $T_D(A) = D$ für alle $A \in \mathcal{C}$ und $Tf = \text{id}_D$ für alle Morphismen in \mathcal{C} .

3. *Vergiss-Funktoren.* Wirken identisch auf Objekten und Morphismen, vergessen aber einen Teil der Struktur. Beispiele: **Grp** \rightarrow **Mg** (ordnet jeder Gruppe die zugrunde liegende Menge und jedem Homomorphismus die zugrunde liegende Abbildung zu); $k\text{-Vek}$ \rightarrow **Ab** (ordnet jedem k -Vektorraum seine Additionsgruppe zu).

4. Einheitsgruppen. Für einen Ring R sei R^\times seine Einheitsgruppe. Für jeden Ringhomomorphismus $f: R \rightarrow S$ ist $f(R^\times) \subset S^\times$, und $f|_{R^\times}: R^\times \rightarrow S^\times$ ist ein Gruppenhomomorphismus. Daher ist $U: \mathbf{Rg} \rightarrow \mathbf{Grp}$ ein Funktor (definiert durch $U(R) = R^\times$ für jeden Ring R und $U(f) = f|_{R^\times}$ für jeden Ringhomomorphismus $f: R \rightarrow S$).

5. Potenzmengen. Für eine Abbildung $f: A \rightarrow B$ sei $f^*: \mathbb{P}(B) \rightarrow \mathbb{P}(A)$ definiert durch $f^*(Y) = f^{-1}(Y)$. Damit wird $\mathbb{P}: \mathbf{Mg} \rightarrow \mathbf{Mg}$ zum kontravarianten Funktor (definiert durch $\mathbb{P}f = f^*$ für jede Abbildung f).

6. Die Morphismenfunktoren. Sei \mathcal{C} eine Kategorie und $A \in \mathcal{C}$. Für $X \in \mathcal{C}$ definiert man

$$h_A(X) = \text{Mor}_{\mathcal{C}}(A, X) \quad \text{und} \quad h'_A(X) = \text{Mor}_{\mathcal{C}}(X, A),$$

und für einen Morphismus $f \in \text{Mor}_{\mathcal{C}}(X, Y)$ definiert man

$$h_A(f): \text{Mor}_{\mathcal{C}}(A, X) \rightarrow \text{Mor}_{\mathcal{C}}(A, Y) \quad \text{durch} \quad h_A(f)(\varphi) = f \circ \varphi$$

und

$$h'_A(f): \text{Mor}_{\mathcal{C}}(Y, A) \rightarrow \text{Mor}_{\mathcal{C}}(X, A) \quad \text{durch} \quad h'_A(f)(\psi) = \psi \circ f.$$

Damit ist $h_A: \mathcal{C} \rightarrow \mathbf{Mg}$ ein (kovarianter) Funktor und $h'_A: \mathcal{C} \rightarrow \mathbf{Mg}$ ein kontravarianter Funktor.

Bemerkung 1.4.10. Seien $T: \mathcal{C} \rightarrow \mathcal{D}$ und $U: \mathcal{D} \rightarrow \mathcal{E}$ Funktoren. Dann ist $U \circ T: \mathcal{C} \rightarrow \mathcal{E}$ ein Funktor. Damit entsteht der Wunsch, Kategorien als Objekte einer "Superkategorie" mit den Funktoren als Morphismen aufzufassen. Dem stehen mengentheoretische Schwierigkeiten entgegen, da Kategorien Klassen sind und als solche nicht wieder zu Klassen zusammengefasst werden können. Diese Schwierigkeiten können auf zwei Arten umgangen werden.

1. Eine Kategorie \mathcal{C} heißt *klein*, wenn $\text{Ob } \mathcal{C}$ eine Menge ist (dann ist auch

$$\text{Mor}(\mathcal{C}) = \bigcup_{(A,B) \in \mathcal{C} \times \mathcal{C}} \text{Mor}_{\mathcal{C}}(A, B)$$

eine Menge). Damit wird die Klasse der kleinen Kategorien mit den Funktoren als Morphismen zur Kategorie.

2. Grothendieck'sche Universen. Wir legen die ZF-Mengenlehre zugrunde. Eine Menge U heißt (*Grothendieck'sches*) *Universum*, wenn sie die folgenden Bedingungen erfüllt:

U1. $a \in U \implies a \subset U$ und $\mathbb{P}a \in U$.

U2. $a, b \in U \implies \{a, b\} \in U$.

U3. Ist $F \subset U \times U$ eine Abbildung und $J \subset U$, so ist auch $\bigcup F[J] \in U$.

Dann ist jedes nicht-leere Universum ein Modell von ZF [das heißt, die ZF-Axiome gelten, wenn man die Quantoren über die Elemente von U laufen lässt] (der Beweis ist einfach, aber länglich).

Grothendieck'sches Universenaxiom. Jede Menge ist Element eines Universums.

In ZF mit dem Grothendieck'schen Universenaxiom kann man nun mathematische Theorien wie folgt aufbauen. Man wählt ein Universum U und formuliert die klassische Mathematik innerhalb U (Mengen sind dann Elemente von U , genannt U -Mengen, und Klassen sind Teilmengen von U , genannt U -Klassen). Dann ist eine U -Kategorie eine U -Klasse, so dass . . .

Wählt man nun ein Universum U_1 , so dass $U \in U_1$, so wird jede U -Klasse zur U_1 -Menge, und man kann die U_1 -Kategorie aller U -Kategorien bilden.

Dieses Verfahren kann iteriert werden. Mengentheoretische Schwierigkeiten werden dadurch umgangen, dass man (stillschweigend) in höhere Universen aufsteigt.

Definitionen und Bemerkungen 1.4.11. $S, T: \mathcal{C} \rightarrow \mathcal{D}$ seien Funktoren. Eine *natürliche Transformation* oder ein *Morphismus* $\alpha: S \rightarrow T$ ist eine Familie von Morphismen $(\alpha(C): SC \rightarrow TC)_{C \in \mathcal{C}}$ in \mathcal{D} , so dass für jeden Morphismus $f: C \rightarrow C'$ in \mathcal{C} das folgende Diagramm kommutiert:

$$\begin{array}{ccc} SC & \xrightarrow{\alpha(C)} & TC \\ sf \downarrow & & \downarrow Tf \\ SC' & \xrightarrow{\alpha(C')} & TC' \end{array}$$

Man sagt dann auch, $(\alpha(C))_{C \in \mathcal{C}}$ ist eine *Familie funktorieller Homomorphismen* oder $\alpha(C)$ ist ein (in C) natürlicher oder funktorieller Homomorphismus.

Sei $U: \mathcal{C} \rightarrow \mathcal{D}$ ein weiterer Funktor, und seien $\alpha: S \rightarrow T$ und $\beta: T \rightarrow U$ Morphismen. Wir definieren $\beta \circ \alpha: S \rightarrow U$ durch $(\beta \circ \alpha)(C) = \beta(C) \circ \alpha(C): SC \rightarrow UC$. Dann ist auch $\beta \circ \alpha$ ein Morphismus. Damit wird die Klasse der Funktoren $\mathcal{C} \rightarrow \mathcal{D}$ zur Kategorie $\text{Fun}(\mathcal{C}, \mathcal{D})$ (mit den natürlichen Transformationen als Morphismen). Für jeden Funktor $S: \mathcal{C} \rightarrow \mathcal{D}$ ist $\text{id}_S = (\text{id}_{S(C)})_{C \in \mathcal{C}}$ die Identität auf S . Eine natürliche Transformation $\alpha: S \rightarrow T$ ist genau dann ein Isomorphismus, wenn $\alpha(C): SC \rightarrow TC$ für alle $C \in \mathcal{C}$ ein Isomorphismus in \mathcal{D} ist (dann ist $\alpha^{-1} = (\alpha(C)^{-1})_{C \in \mathcal{C}}$).

Beispiel 1.4.12. Sei k ein Körper. Für einen k -Vektorraum $V \in k\text{-Vek}$ sei $V^* = \text{Hom}_k(V, k)$ der Dualraum, und für einen k -Vektorraum-Homomorphismus $f: V \rightarrow W$ sei $f^*: W^* \rightarrow V^*$ definiert durch $f^*(\varphi) = \varphi \circ f$. Damit ist $D: k\text{-Vek} \rightarrow k\text{-Vek}$, definiert durch $DV = V^*$ und $Df = f^*$, ein kontravarianter Funktor und $D \circ D: k\text{-Vek} \rightarrow k\text{-Vek}$ ein (kovarianter) Funktor (der Bidualfunctor). Die Abbildung $\alpha(V): V \rightarrow V^{**}$, definiert durch $\alpha(V)(v)(\varphi) = \varphi(v)$ für alle $v \in V$ und $\varphi \in V^*$, ist ein in V funktorieller k -Vektorraumhomomorphismus: Für einen k -Vektorraum-Homomorphismus $f: V \rightarrow W$ ist

$$\begin{array}{ccc} V & \xrightarrow{\alpha(V)} & V^{**} \\ f \downarrow & & \downarrow f^{**} \\ W & \xrightarrow{\alpha(W)} & W^{**} \end{array}$$

ein kommutatives Diagramm, denn für $v \in V$ und $\psi \in W^*$ ist

$$[f^{**} \circ \alpha(V)](v)(\psi) = [\alpha(V)(v) \circ f^*](\psi) = \alpha(V)(v)[f^*(\psi)] = \alpha(V)(v)(\psi \circ f) = \psi \circ f(v) = [\alpha(W) \circ f](v)(\psi).$$

Daher ist $\alpha = (\alpha(V))_{V \in k\text{-Vek}}: \text{Id} \rightarrow D \circ D$ ein Morphismus von Funktoren.

Modultheorie

Sei $R \neq \mathbf{0}$ ein (unitärer) Ring.

2.1. Definitionen und elementare Eigenschaften

Definition 2.1.1. Sei M eine additive abelsche Gruppe. Eine R -(Links-)Modulstruktur auf M ist eine Abbildung

$$\sigma: R \times M \rightarrow M, \quad (\lambda, x) \mapsto \lambda x \quad (\text{genannt Skalarmultiplikation}),$$

so dass für alle $\lambda, \mu \in R$ und alle $x, y \in M$ gilt (wir folgen der Konvention Punkt- vor Strichrechnung):

M1. $(\lambda + \mu)x = \lambda x + \mu x$.

M2. $\lambda(x + y) = \lambda x + \lambda y$.

M3. $(\lambda\mu)x = \lambda(\mu x)$.

M4. $1x = x$.

Ein R -(Links-)Modul $M = (M, \sigma)$ ist eine additive abelsche Gruppe M mit einer R -(Links-)Modulstruktur auf M . Schreibweise: $M = {}_R M$. Wir bezeichnen mit $R\text{-Mod}$ die Klasse aller R -(Links-)Moduln. Analog definiert man den Begriff der R -Rechtsmodulstruktur $\sigma_*: M \times R \rightarrow M, (x, \lambda) \mapsto x\lambda$ und den Begriff des R -Rechtsmoduls. Ist M ein R -Rechtsmodul, so schreibt man $M = M_R$.

Bemerkung 2.1.2. Sei M ein R -Modul. Dann gilt für alle $x \in M$ und $\lambda \in R$

$$0_R x = 0_M, \quad \lambda 0_M = 0_M \quad \text{und} \quad (-\lambda)x = -\lambda x, \quad \text{insbesondere} \quad -x = (-1)x.$$

Beweis: Aus $0_R x + 0_R x = (0_R + 0_R)x = 0_R x$ folgt $0_R x = 0_M$, aus $\lambda 0_M + \lambda 0_M = \lambda(0_M + 0_M) = \lambda 0_M$ folgt $\lambda 0_M = 0_M$, und aus $(-1)x + x = (-1)x + 1x = [(-1) + 1]x = 0_M$ folgt $(-1)x = -x$. \square

Bemerkung 2.1.3. Sei M eine abelsche Gruppe und $\text{End}(M) = \text{Hom}(M, M)$ der Endomorphismenring von M .

Sei $\sigma: R \times M \rightarrow M$ eine R -Linksmodulstruktur auf M . Für $\lambda \in R$ ist $(x \mapsto \lambda x) \in \text{End}(M)$, und $\widehat{\sigma}: R \rightarrow \text{End}(M)$, definiert durch $\widehat{\sigma}(\lambda)(x) = \lambda x$ für alle $\lambda \in R$ und $x \in M$, ist ein Ringhomomorphismus. Ist umgekehrt $\tau: R \rightarrow \text{End}(M)$ ein Ringhomomorphismus und definiert man $\sigma_\tau: R \times M \rightarrow M$ durch $\sigma_\tau(\lambda, x) = \tau(\lambda)(x)$, so ist σ_τ eine R -Linksmodulstruktur auf M , und $\widehat{\sigma_\tau} = \tau$.

Ist $\sigma_*: M \times R \rightarrow M$ eine R -Rechtsmodulstruktur auf M und definiert man $\widehat{\sigma_*}: R \rightarrow \text{End}(M)$ durch $\widehat{\sigma_*}(\lambda)(x) = x\lambda$ für alle $\lambda \in R$ und $x \in M$, so ist $\widehat{\sigma_*}$ kein Ringhomomorphismus, denn für alle $\lambda, \mu \in R$ ist $\widehat{\sigma_*}(\lambda\mu) = \widehat{\sigma_*}(\mu) \circ \widehat{\sigma_*}(\lambda)$. Der Gegenring R^{op} von R sei definiert als Ring mit derselben Additionsgruppe wie R und der Multiplikation $x \cdot^{\text{op}} y = yx$. Dann ist $\widehat{\sigma_*}: R^{\text{op}} \rightarrow \text{End}(M)$ ein Ringhomomorphismus.

Ist umgekehrt $\tau: R^{\text{op}} \rightarrow \text{End}(M)$ ein Ringhomomorphismus und definiert man $\sigma_{\tau_*}: M \times R \rightarrow M$ durch $\sigma_{\tau_*}(x, \lambda) = \tau(\lambda)(x)$, so ist σ_{τ_*} eine R -Rechtsmodulstruktur auf M , und $\widehat{\sigma_{\tau_*}} = \tau$.

Daher ist ein R -Rechtsmodul dasselbe wie ein R^{op} -(Links-)Modul. Ist R kommutativ, so ist $R^{\text{op}} = R$ und daher ist jeder R -(Links-)Modul auch ein R -Rechtsmodul.

Definition 2.1.4. Sei M ein R -Modul und $N \subset M$.

1. Sei M ein R -Modul. Eine Teilmenge $N \subset M$ heißt *(R-)Unterm modul*, wenn $0 \in N$, $N + N \subset N$ und $RN \subset N$ [explizit: $0 \in N$, und für alle $x, y \in N$ und $\lambda \in R$ ist $x + y \in N$ und $\lambda x \in N$].
Ist $N \subset M$ ein R -Unterm modul, so ist N , versehen mit der eingeschränkten Skalarmultiplikation, wieder ein R -Modul.
2. Auf der Faktorgruppe $M/N = \{x + N \mid x \in M\}$ sei eine R -Modulstruktur definiert durch

$$\lambda(x + N) = \lambda x + N \quad \text{für alle } \lambda \in R \text{ und } x \in M.$$

[Nachrechnen: 1) Die Definition ist unabhängig von der Wahl der Repräsentanten; 2) die Bedingungen von Definition 2.1.1 sind erfüllt].

Versehen mit dieser R -Modulstruktur, nennt man M/N den *Faktormodul* oder *Restklassenmodul* und die Abbildung $\pi: M \rightarrow M/N$, definiert durch $\pi(x) = x + N$, die *Restklassenabbildung*.

Beispiele 2.1.5.

1. Sei R ein Körper. Dann sind R -Moduln dasselbe wie R -Vektorräume, Unterm oduln sind Unterräume und Faktormoduln sind Faktorräume. Allgemeiner: Ist R ein Divisionsring [d. h., $R^\times = R \setminus \mathbf{0}$], so nennt man einen R -Modul auch einen R (-Links-)Vektorraum.

2. Sei M eine additive abelsche Gruppe. Dann ist die Vielfachenbildung $\mathbb{Z} \times M \rightarrow M$, $(n, x) \rightarrow nx$ die einzige \mathbb{Z} -Modulstruktur auf M . Daher ist ein \mathbb{Z} -Modul dasselbe wie eine additive abelsche Gruppe, \mathbb{Z} -Unterm oduln sind Untergruppen, und \mathbb{Z} -Faktormoduln sind Faktorgruppen.

3. Sei $n \in \mathbb{N}$. Dann wird R^n zum R -Modul vermöge $\lambda(c_1, \dots, c_n) = (\lambda c_1, \dots, \lambda c_n)$. Insbesondere ist R ein R -Modul (in diesem Falle stimmen Ringmultiplikation und Skalarmultiplikation überein). Die R -Unterm oduln von R sind genau die Linksideale von R .

4. Auf der trivialen additiven abelschen Gruppe $\mathbf{0}$ gibt es genau eine R -Modulstruktur. Man nennt $\mathbf{0}$ den *Nullmodul*.

Sei M ein R -Modul. Dann sind $\mathbf{0} = \{0\}$ und M R -Unterm oduln von M . Ist Ω eine Menge von R -Unterm oduln von M , so ist auch $\bigcap \Omega$ ein R -Unterm oduln von M . Ist Ω eine Kette (bzgl. \subset), so ist auch $\bigcup \Omega$ ein R -Unterm oduln von M .

5. Ist $R = \mathbf{0}$ der Nullring, so kann man den Begriff des R -Moduls wie eben definieren, aber dann ist $\mathbf{0}$ der einzige R -Modul.

Definition 2.1.6. M und N seien R -Moduln.

1. Eine Abbildung $f: M \rightarrow N$ heißt *R-linear* oder ein *R-(Modul)-Homomorphismus*, wenn für alle $x, y \in M$ und $\lambda \in R$ gilt:
 - $f(x + y) = f(x) + f(y)$ (d. h., f ist ein Homomorphismus abelscher Gruppen);
 - $f(\lambda x) = \lambda f(x)$.

$\text{Hom}_R(M, N)$ bezeichne die Menge aller R -Homomorphismen.

2. Sei $f: M \rightarrow N$ ein R -Homomorphismus. f heißt ein *(R-)Monomorphismus* [(*R*-)Epimorphismus, (*R*-)Isomorphismus], wenn f injektiv [surjektiv, bijektiv] ist.

$\text{Bi}(f) = f(M)$ heißt *Bild* von f , und $\text{Ker}(f) = f^{-1}(\mathbf{0})$ heißt *Kern* von f .

3. M und N heißen *(R-)isomorph*, wenn es einen R -Isomorphismus $f: M \rightarrow N$ gibt; Schreibweisen: $f: M \xrightarrow{\sim} N$, $M \cong_R N$.

Bemerkungen 2.1.7.

1. Ist R ein Körper, so sind R -Modulhomomorphismen dasselbe wie R -Vektorraum-Homomorphismen. \mathbb{Z} -Modulhomomorphismen sind Gruppenhomomorphismen.

2. Sei $N \subset M$ ein R -Untermodul. Dann ist die Einlagerung $i = (N \hookrightarrow M)$ ein R -Monomorphismus und die natürliche Restklassenabbildung $\pi: M \rightarrow M/N$ ein R -Epimorphismus. Insbesondere ist id_M ein R -Isomorphismus.

3. Sind $f: M \rightarrow N$ und $g: N \rightarrow P$ R -Homomorphismen [R -Monomorphismen, R -Epimorphismen, R -Isomorphismen], so auch $g \circ f: M \rightarrow P$. Insbesondere ist $R\text{-Mod}$ eine Kategorie mit den R -Homomorphismen als Morphismen. Wir bezeichnen mit $\mathbf{Mod}\text{-}R = R^{\text{op}}\text{-Mod}$ die Kategorie der R -Rechtsmoduln.

4. Ist M ein R -Modul, so ist $M/M = \mathbf{0}$, und der Restklassenhomomorphismus $\pi: M \rightarrow M/\mathbf{0}$ ist ein Isomorphismus. Wir identifizieren $M = M/\mathbf{0}$ (vermöge $x = x + \mathbf{0}$).

5. Ein R -Homomorphismus $f: M \rightarrow N$ ist genau dann ein R -Isomorphismus, wenn es einen R -Homomorphismus $g: N \rightarrow M$ gibt mit $g \circ f = \text{id}_M$ und $f \circ g = \text{id}_N$ [und dann ist $g = f^{-1}$]. Insbesondere ist ein R -Isomorphismus im Sinne von Definition 2.1.6.2 dasselbe wie ein Isomorphismus in $R\text{-Mod}$.

6. Sei $f: M \rightarrow N$ ein R -Homomorphismus, und seien $M' \subset M$ und $N' \subset N$ R -Untermoduln. Dann sind auch $f(M') \subset N$ und $f^{-1}(N') \subset M$ R -Untermoduln. Insbesondere sind $\text{Ker}(f) \subset M$ und $\text{Bi}(f) \subset N$ R -Untermoduln, und f ist genau dann ein R -Monomorphismus, wenn $\text{Ker}(f) = \mathbf{0}$.

Ist $f(M') \subset N'$, so ist auch $f|_{M'}: M' \rightarrow N'$ ein R -Homomorphismus. Insbesondere ist $f: M \rightarrow f(M)$ ein R -Epimorphismus.

7. M und N seien R -Moduln, $0: M \rightarrow N$ bezeichne die konstante Abbildung mit Wert $0 \in N$; sie ist ein R -Homomorphismus, genannt *Nullhomomorphismus*. Es ist $\text{Hom}_R(\mathbf{0}, N) = \mathbf{0}$ und $\text{Hom}_R(M, \mathbf{0}) = \mathbf{0}$. Insbesondere ist $\mathbf{0}$ initial und final in $R\text{-Mod}$.

8. *Homomorphiesatz*. Sei $f: M \rightarrow N$ ein R -Homomorphismus, $M' \subset \text{Ker}(f)$ ein R -Untermodul und $\pi: M \rightarrow M/M'$ der Restklassenhomomorphismus. Dann gibt es genau einen R -Homomorphismus $\tilde{f}: M/M' \rightarrow N$ mit $f = \tilde{f} \circ \pi$. Dieser ist gegeben durch $\tilde{f}(x + M') = f(x)$ für alle $x \in M$, es ist $\text{Ker}(\tilde{f}) = \text{Ker}(f)/M'$ und $\text{Bi}(\tilde{f}) = \text{Bi}(f)$.

Insbesondere gibt es genau einen Isomorphismus $f^*: M/\text{Ker}(f) \xrightarrow{\sim} \text{Bi}(f)$, der das folgende Diagramm kommutativ macht:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \pi \downarrow & & \uparrow i \\ M/\text{Ker}(f) & \xrightarrow{f^*} & \text{Bi}(f) \end{array}$$

9. *Erster Isomorphiesatz*. Seien $N \subset M$ und $P \subset M$ R -Untermoduln. Dann sind auch $N + P$ und $N \cap P$ R -Untermoduln von M , und es gibt einen R -Isomorphismus

$$\phi: N/N \cap P \xrightarrow{\sim} (N + P)/P \quad \text{mit} \quad \phi(x + N \cap P) = x + P.$$

10. *Zweiter Isomorphiesatz*. Seien $P \subset N \subset M$ R -Untermoduln. Dann ist auch $N/P \subset M/P$ ein R -Untermodul, und es gibt einen R -Isomorphismus

$$\phi: (M/P)/(N/P) \xrightarrow{\sim} M/N \quad \text{mit} \quad \phi((x + P) + N/P) = x + N.$$

11. Sei $N \subset M$ ein R -Untermodul und $\pi: M \rightarrow M/N$ der Restklassenepimorphismus. Dann definiert die Zuordnung $P \mapsto P/N$ eine bijektive Abbildung von der Menge aller R -Untermoduln $P \subset M$ mit $N \subset P$ auf die Menge aller R -Untermoduln von M/N . Die Umkehrabbildung ist gegeben durch $P^* \mapsto \pi^{-1}(P^*)$.

12. Seien $f, g: M \rightarrow N$ R -Homomorphismen. Dann ist auch $f + g: M \rightarrow N$ ein R -Homomorphismus, und bezüglich dieser Addition ist $\text{Hom}_R(M, N)$ eine abelsche Gruppe. Sind $\varphi: L \rightarrow M$ und $\psi: N \rightarrow P$ weitere R -Homomorphismen, so folgt $(f + g) \circ \varphi = f \circ \varphi + g \circ \varphi$ und $\psi \circ (f + g) = \psi \circ f + \psi \circ g$.

$\text{Hom}_R(M, -): R\text{-Mod} \rightarrow \mathbf{Ab}$ ist ein (kovarianter) und $\text{Hom}_R(-, N): R\text{-Mod} \rightarrow \mathbf{Ab}$ ist ein kontravarianter Funktor.

[Ist $f \in \text{Hom}_R(X, Y)$, so ist

$$\text{Hom}_R(M, f): \text{Hom}_R(M, X) \rightarrow \text{Hom}_R(M, Y) \text{ gegeben durch } \text{Hom}_R(M, f)(\varphi) = f \circ \varphi,$$

und das ist ein Gruppenhomomorphismus.

$$\text{Hom}_R(f, N): \text{Hom}_R(Y, N) \rightarrow \text{Hom}_R(X, N) \text{ ist gegeben durch } \text{Hom}_R(f, N)(\psi) = \psi \circ f,$$

und das ist ebenfalls ein Gruppenhomomorphismus].

13. Sei R kommutativ, $f: M \rightarrow N$ ein R -Homomorphismus und $\lambda \in R$. Dann ist auch λf ein R -Homomorphismus. Damit wird $\text{Hom}_R(M, N)$ zum R -Modul. Die Abbildung

$$\varepsilon: \text{Hom}_R(R, M) \rightarrow M, \text{ definiert durch } \varepsilon(f) = f(1),$$

ist ein in M funktorieller R -Isomorphismus [also ein Iso von Funktoren $\text{Hom}_R(R, -) \xrightarrow{\sim} \text{Id}_{R\text{-Mod}}$].

[Beweis: Man hat die folgenden (trivialen) Fakten nachzuweisen: **1)** ε ist ein R -Homomorphismus; **2)** Für jedes $x \in M$ ist $\eta_x = (\lambda \mapsto \lambda x) \in \text{Hom}_R(R, M)$; **3)** $\eta: M \rightarrow \text{Hom}_R(R, M)$, definiert durch $\eta(x) = \eta_x$, ist ein R -Homomorphismus; **4)** $\eta \circ \varepsilon = \text{id}_{\text{Hom}_R(R, M)}$ und $\varepsilon \circ \eta = \text{id}_M$; **5)** Jeder R -Homomorphismus $f: M \rightarrow M'$ induziert ein kommutatives Diagramm

$$\begin{array}{ccc} \text{Hom}_R(R, M) & \xrightarrow{\varepsilon} & M \\ \text{Hom}_R(R, f) \downarrow & & \downarrow f \\ \text{Hom}_R(R, M') & \xrightarrow{\varepsilon'} & M' \end{array} .$$

14. Sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus und N ein S -Modul. Dann wird N zum R -Modul vermöge $\lambda x = \varphi(\lambda)x$ für alle $\lambda \in R$ und $x \in N$.

Ist N' ein weiterer S -Modul, so folgt $\text{Hom}_S(N, N') \subset \text{Hom}_R(N, N')$, mit Gleichheit, falls φ surjektiv ist. Damit erhalten wir einen Funktor $S\text{-Mod} \rightarrow R\text{-Mod}$. Insbesondere ist S ein R -Modul. Wichtiger Spezialfall: $R \subset S$ ist ein Teilring und $f = (R \hookrightarrow S)$.

15. Seien $f: A \rightarrow B$ und $g: B \rightarrow C$ R -Homomorphismen. Man sagt, $A \xrightarrow{f} B \xrightarrow{g} C$ ist eine *exakte Sequenz*, wenn $\text{Ker}(g) = \text{Bi}(f)$.

Insbesondere gilt: $\mathbf{0} \rightarrow A \xrightarrow{f} B$ ist genau dann exakt, wenn f ein Monomorphismus ist, und $A \xrightarrow{f} B \rightarrow \mathbf{0}$ ist genau dann exakt, wenn f ein Epimorphismus ist.

Eine (endliche oder unendliche) Folge von R -Modulhomomorphismen

$$\dots \rightarrow A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} \dots$$

heißt *exakt*, wenn jede 3-gliedrige Teilsequenz exakt ist.

Eine exakte Sequenz der Form $\mathbf{0} \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \mathbf{0}$ heißt *kurze exakte Sequenz*.

Ist $N \subset M$ ein R -Untermodul, so ist $\mathbf{0} \rightarrow N \hookrightarrow M \rightarrow M/N \rightarrow \mathbf{0}$ eine kurze exakte Sequenz.

Ist $\mathbf{0} \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \mathbf{0}$ eine kurze exakte Sequenz, so ist $f: A \xrightarrow{\sim} \text{Ker}(g) = \text{Bi}(f)$ ein Isomorphismus, g induziert einen Isomorphismus $g^*: B/\text{Bi}(f) = B/\text{Ker}(g) \xrightarrow{\sim} C$, und wir erhalten das kommutative

Diagramm

$$\begin{array}{ccccccc}
 \mathbf{0} & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & \mathbf{0} \\
 & & f \downarrow & & \downarrow \text{id}_B & & \uparrow g^* & & \\
 \mathbf{0} & \longrightarrow & \text{Bi}(f) & \longrightarrow & B & \xrightarrow{\pi} & B/\text{Bi}(f) & \longrightarrow & \mathbf{0}
 \end{array}$$

Definition 2.1.8. Sei M ein R -Modul.

1. Sei $(M_i)_{i \in I}$ eine Familie von R -Untermoduln. Dann nennt man

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in I} m_i \mid m_i \in M_i, m_i = 0 \text{ f\"ur fast alle } i \in I \right\}$$

die *Summe* der Familie $(M_i)_{i \in I}$.

2. Sei $E \subset M$. Dann nennt man

$${}_R\langle E \rangle = \bigcap \{ N \mid N \subset M \text{ ist ein } R\text{-Untermodul mit } E \subset N \}$$

den von E erzeugten R -Untermodul von M . Ist ${}_R\langle E \rangle = M$, so nennt man E ein *Erzeugendensystem* von M . Man nennt M *endlich erzeugt*, wenn M ein endliches Erzeugendensystem besitzt.

F\"ur eine Familie $(u_i)_{i \in I}$ in M sei ${}_R\langle u_i \mid i \in I \rangle = {}_R\langle \{u_i \mid i \in I\} \rangle$, und man nennt $(u_i)_{i \in I}$ ein *Erzeugendensystem* von M , wenn $\{u_i \mid i \in I\}$ ein Erzeugendensystem von M ist. F\"ur $a_1, \dots, a_n \in M$ schreibt man ${}_R\langle a_1, \dots, a_n \rangle = {}_R\langle \{a_1, \dots, a_n\} \rangle$.

3. M hei\u00dft *zyklisch*, wenn $M = {}_R\langle a \rangle$ f\"ur ein $a \in M$. [Im Falle $R = \mathbb{Z}$ ist das die Definition der zyklischen Gruppe].
4. M hei\u00dft *einfach*, wenn $M \neq \mathbf{0}$, und $\mathbf{0}$ und M sind die einzigen R -Untermoduln von M .
5. Sei $E \subset M$. Dann nennt man $\text{Ann}_R(E) = \{ \lambda \in R \mid \lambda x = 0 \text{ f\"ur alle } x \in E \} \subset R$ den *Annulator* von E [$\text{Ann}_R(E)$ ist ein Linksideal von R].
6. M hei\u00dft *torsionsfrei*, wenn $\text{Ann}_R(x) = \mathbf{0}$ f\"ur alle $x \in M \setminus \mathbf{0}$.

Satz 2.1.9. Sei M ein R -Modul.

1. Ist $E \subset M$, so ist

$${}_R\langle E \rangle = \sum_{x \in E} Rx = \left\{ \sum_{\nu=1}^n \lambda_\nu x_\nu \mid n \in \mathbb{N}, \lambda_\nu \in R, x_\nu \in E \right\},$$

${}_R\langle E \rangle$ ist der kleinste E enthaltende R -Untermodul von M . Ist $f: M \rightarrow N$ ein R -Homomorphismus, so ist ${}_R\langle f(E) \rangle = f({}_R\langle E \rangle)$, und f\"ur zwei R -Homomorphismen $f, g: {}_R\langle E \rangle \rightarrow N$ gilt: Aus $f|_E = g|_E$ folgt $f = g$. Ist R kommutativ, so folgt $\text{Ann}_R(E) = \text{Ann}_R({}_R\langle E \rangle)$.

2. Ist $(E_i)_{i \in I}$ eine Familie von Teilmengen von M , so folgt

$${}_R\left\langle \bigcup_{i \in I} E_i \right\rangle = \sum_{i \in I} {}_R\langle E_i \rangle.$$

3. F\"ur $a \in M$ ist ${}_R\langle a \rangle = Ra$, und $\phi: R/\text{Ann}_R(a) \rightarrow Ra$, definiert durch $\phi(\lambda + \text{Ann}_R(a)) = \lambda a$, ist ein R -Modulisomorphismus.
4. M ist genau dann zyklisch, wenn $M \cong R/L$ mit einem Linksideal $L \subset R$, und M ist genau dann einfach, wenn $M \cong R/L$ mit einem maximalen Linksideal $L \subset R$.

BEWEIS. 1. Nach Definition ist ${}_R\langle E \rangle \subset M$ ein R -Untermodul, und für jeden R -Untermodul $N \subset M$ mit $E \subset N$ ist ${}_R\langle E \rangle \subset N$. Daher ist ${}_R\langle E \rangle$ der kleinste E enthaltende R -Untermodul von M . Nach Definition ist

$$\sum_{x \in E} Rx = \left\{ \sum_{x \in E} \lambda_x x \mid \lambda_x \in R, \lambda_x = 0 \text{ für fast alle } x \in E \right\} = \left\{ \sum_{\nu=1}^n \lambda_\nu x_\nu \mid n \in \mathbb{N}, \lambda_\nu \in R, x_\nu \in E \right\},$$

und das ist ebenfalls der kleinste R -Untermodul von M , der E enthält, stimmt also mit ${}_R\langle E \rangle$ überein. Sei $f: M \rightarrow N$ ein R -Homomorphismus und $y \in N$. Genau dann ist $y \in {}_R\langle f(E) \rangle$, wenn

$$y = \sum_{\nu=1}^n \lambda_\nu f(x_\nu) = f\left(\sum_{\nu=1}^n \lambda_\nu x_\nu\right) \quad \text{mit } \lambda_\nu \in R \text{ und } x_\nu \in E,$$

und das ist genau dann der Fall, wenn $y \in f({}_R\langle E \rangle)$.

Seien $f, g: {}_R\langle E \rangle \rightarrow N$ R -Homomorphismen mit $f|_E = g|_E$. Ist $x \in {}_R\langle E \rangle$, so folgt $x = \lambda_1 x_1 + \dots + \lambda_n x_n$ mit $\lambda_\nu \in R$ und $x_\nu \in E$, und es folgt

$$f(x) = \sum_{\nu=1}^n \lambda_\nu f(x_\nu) = \sum_{\nu=1}^n \lambda_\nu g(x_\nu) = g(x).$$

2. Beide Seiten stellen den kleinsten R -Untermodul von M dar, der alle E_i enthält, und daher gilt Gleichheit.

3. Nach 1. ist ${}_R\langle a \rangle = Ra$, und die Abbildung $\varphi: R \rightarrow Ra$, definiert durch $\varphi(\lambda) = \lambda a$ ist ein R -Epimorphismus mit $\text{Ker}(\varphi) = \text{Ann}_R(a)$. Nach dem Homomorphiesatz induziert φ einen Isomorphismus $\phi: R/\text{Ann}_R(a) \rightarrow Ra$ wie behauptet.

4. Ist $L \subset R$ ein Linksideal, so ist $R/L = \{\lambda + L \mid \lambda \in R\} = \{\lambda(1 + L) \mid \lambda \in R\} = {}_R\langle 1 + L \rangle$ zyklisch, und nach 3. ist jeder zyklische R -Modul von dieser Form. Ist M einfach, so ist M zyklisch und daher $M = R/L$ mit einem Linksideal $L \subsetneq R$. Die Untermoduln von M sind von der Form J/L mit Linksidealen $J \subset R$, so dass $L \subset J$. Daher ist M genau dann einfach, wenn L ein maximales Linksideal ist. Ist umgekehrt $L \subset R$ ein maximales Linksideal, so ist R/L einfach. \square

Definition und Satz 2.1.10. Sei $(M_i)_{i \in I}$ eine Familie von R -Moduln,

$$P = \prod_{i \in I} M_i \quad \text{und} \quad C = \bigoplus_{i \in I} M_i = \{(a_i)_{i \in I} \mid a_i = 0 \text{ für fast alle } i \in I\},$$

$(p_i: P \rightarrow M_i)_{i \in I}$ die Familie der kanonischen Projektionen und $(\varepsilon_i: M_i \rightarrow C)_{i \in I}$ die Familie der Einlagerungen (siehe Beispiel 1.1.5.2). Für $\lambda \in R$ und $a = (a_i)_{i \in I} \in P$ definiert man $\lambda a = (\lambda a_i)_{i \in I}$.

Damit wird P zum R -Modul, $C \subset P$ ist ein R -Untermodul, $(p_i: P \rightarrow M_i)_{i \in I}$ ist ein Produkt und $(\varepsilon_i: M_i \rightarrow C)_{i \in I}$ ist ein Koproduct in der Kategorie $R\text{-Mod}$.

Man nennt P das direkte Produkt und C die (äußere) direkte Summe der Familie $(M_i)_{i \in I}$. Ist $M_i = M$ für alle $i \in I$, so schreibt man $P = M^I$ und $C = M^{(I)}$. Ist I endlich, so ist $P = C$, und im Falle $I = \emptyset$ ist $P = C = \mathbf{0}$. Ist $I = [1, n]$ mit $n \in \mathbb{N}$, so schreibt man $P = C = M_1 \times \dots \times M_n = M_1 \oplus \dots \oplus M_n$ und $M^I = M^{(I)} = M^n$.

Für jeden R -Modul N ist die Abbildung

$$\Phi: \text{Hom}_R\left(\bigoplus_{i \in I} M_i, N\right) \rightarrow \prod_{i \in I} \text{Hom}_R(M_i, N), \quad \text{definiert durch } \Phi(f) = (f \circ \varepsilon_i)_{i \in I},$$

ein Isomorphismus abelscher Gruppen.

Ist $(N_i \subset M_i)_{i \in I}$ eine Familie von R -Untermoduln, so ist

$$\bigoplus_{i \in I} N_i \subset \bigoplus_{i \in I} M_i; \quad \text{und} \quad \bigoplus_{i \in I} M_i / \bigoplus_{i \in I} N_i \rightarrow \bigoplus_{i \in I} M_i / N_i, \quad (m_i)_{i \in I} + \bigoplus_{i \in I} N_i \mapsto (m_i + N_i)_{i \in I}$$

ist ein R -Isomorphismus.

Im Falle $I = \{1, 2\}$ ist $P = C = M_1 \oplus M_2$, und es bestehen die exakten Sequenzen

$$\mathbf{0} \rightarrow M_1 \xrightarrow{\varepsilon_1} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \rightarrow \mathbf{0} \quad \text{und} \quad \mathbf{0} \rightarrow M_2 \xrightarrow{\varepsilon_2} M_1 \oplus M_2 \xrightarrow{p_1} M_1 \rightarrow \mathbf{0}.$$

BEWEIS. Offensichtlich ist $(p_i: P \rightarrow M_i)_{i \in I}$ ein Produkt und $(\varepsilon_i: M_i \rightarrow C)_{i \in I}$ ein Koprodukt in der Kategorie $R\text{-Mod}$. Wegen

$$\Phi(f + g) = ((f + g) \circ \varepsilon_i)_{i \in I} = (f \circ \varepsilon_i + g \circ \varepsilon_i)_{i \in I} = (f \circ \varepsilon_i)_{i \in I} + (g \circ \varepsilon_i)_{i \in I} = \Phi(f) + \Phi(g)$$

ist Φ ein Homomorphismus. Zu jeder Familie $\psi = (\psi_i \in \text{Hom}_R(M_i, N))_{i \in I}$ gibt es nach Definition des Koproduktes genau ein $f \in \text{Hom}_R(C, N)$ mit $f \circ \varepsilon_i = \psi_i$ für alle $i \in I$, also $\Phi(f) = \psi$. Daher ist Φ ein Isomorphismus.

Ist $(N_i \subset M_i)_{i \in I}$ eine Familie von R -Untermoduln, so ist

$$\bigoplus_{i \in I} M_i \rightarrow \bigoplus_{i \in I} M_i/N_i, \quad (m_i)_{i \in I} \mapsto (m_i + N_i)_{i \in I}, \quad \text{ein } R\text{-Epimorphismus mit Kern } \bigoplus_{i \in I} N_i,$$

und nach dem Homomorphiesatz folgt der behauptete Isomorphismus. Die Exaktheit der Sequenzen ist offensichtlich. \square

Definition 2.1.11. Sei M ein R -Modul und $L \subset R$ ein Linksideal.

1. Man definiert

$$LM = \sum_{x \in M} Lx = \left\{ \sum_{\nu=1}^n \lambda_\nu x_\nu \mid n \in \mathbb{N}, \lambda_\nu \in L, x_\nu \in M \right\}$$

[$LM \subset M$ ist ein R -Untermodul, $L \subset \text{Ann}_R(M/LM)$, und $L \subset \text{Ann}_R(M) \iff LM = \mathbf{0}$.]

2. Ist $\mathfrak{a} \triangleleft R$ und $\mathfrak{a} \subset \text{Ann}_R(M)$, so wird M zum R/\mathfrak{a} -Modul vermöge $(\lambda + \mathfrak{a})x = \lambda x$ für alle $\lambda \in R$ und $x \in M$ [Nachrechnen!].

Bemerkung 2.1.12. Sei $\mathfrak{a} \triangleleft R$, und seien M, N R -Moduln. Dann ist

$$\text{Hom}_R(M/\mathfrak{a}M, N/\mathfrak{a}N) = \text{Hom}_{R/\mathfrak{a}}(M/\mathfrak{a}M, N/\mathfrak{a}N) \quad (\text{siehe Bemerkung 2.1.7.14}).$$

Zu jedem $f \in \text{Hom}_R(M, N)$ gibt es genau ein $f^* \in \text{Hom}_{R/\mathfrak{a}}(M/\mathfrak{a}M, N/\mathfrak{a}N)$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \pi_M \downarrow & & \downarrow \pi_N \\ M/\mathfrak{a}M & \xrightarrow{f^*} & N/\mathfrak{a}N. \end{array}$$

Damit ist $M \mapsto M/\mathfrak{a}M$, $f \mapsto f^*$ ein Funktor $R\text{-Mod} \rightarrow R/\mathfrak{a}\text{-Mod}$.

2.2. Innere direkte Summen und freie Moduln

Definition und Satz 2.2.1. Sei M ein R -Modul, $(M_i)_{i \in I}$ eine Familie von R -Untermoduln von M ,

$$M' = \sum_{i \in I} M_i \quad \text{und} \quad \psi: \bigoplus_{i \in I} M_i \rightarrow M' \quad \text{definiert durch} \quad \psi((x_i)_{i \in I}) = \sum_{i \in I} x_i.$$

Dann ist ψ ein R -Homomorphismus, und die folgenden Aussagen sind äquivalent:

(a) ψ ist ein R -Isomorphismus.

(b) Für alle $j \in I$ ist

$$M_j \cap \sum_{i \in I \setminus \{j\}} M_i = \mathbf{0}.$$

(c) Jedes $x \in M'$ hat eine eindeutige Darstellung in der Form

$$x = \sum_{i \in I} x_i \quad \text{mit } x_i \in M_i \text{ und } x_i = 0 \text{ für fast alle } i \in I.$$

Sind diese Bedingungen erfüllt, so sagt man, die Summe der Familie $(M_i)_{i \in I}$ ist *direkt*, nennt man M' die (*innere*) *direkte Summe* der Familie $(M_i)_{i \in I}$ und schreibt

$$M' = \sum_{i \in I} M_i \quad (\text{dir})$$

BEWEIS. Offensichtlich ist ψ ein R -Homomorphismus.

(a) \Rightarrow (b) Sei $j \in I$ und $x_j \in M_j \cap \sum_{i \in I \setminus \{j\}} M_i$. Dann ist $-x_j = \sum_{i \in I \setminus \{j\}} x_i$ mit $x_i \in M_i$, also $\psi((x_i)_{i \in I}) = 0$ und daher $x_i = 0$ für alle $i \in I$.

(b) \Rightarrow (c) Sei $x \in M'$. Wegen $M' = \sum_{i \in I} M_i$ ist $x = \sum_{i \in I} x_i$ mit $x_i \in M_i$ und $x_i = 0$ für fast alle $i \in I$. Sei nun auch $x = \sum_{i \in I} x'_i$ mit $x'_i \in M_i$ und $x'_i = 0$ für fast alle $i \in I$. Für alle $j \in I$ ist dann

$$x_j - x'_j = \sum_{i \in I \setminus \{j\}} (x'_i - x_i) \in M_j \cap \sum_{i \in I \setminus \{j\}} M_i = \mathbf{0}, \quad \text{also } x_j = x'_j.$$

(c) \Rightarrow (a) Nach (c) gibt es zu jedem $x \in M'$ genau ein $(x_i)_{i \in I} \in \bigoplus_{i \in I} M_i$ mit $\psi((x_i)_{i \in I}) = x$. \square

Bemerkungen 2.2.2. Sei M ein R -Modul.

1. Sei $(M_i)_{i \in I}$ eine Familie von R -Untermoduln von M und $J \subset I$, so dass $M_j = \mathbf{0}$ für alle $j \in I \setminus J$. Dann ist

$$\sum_{i \in I} M_i = \sum_{i \in J} M_i,$$

und die Summe der Familie $(M_i)_{i \in I}$ ist genau dann direkt, wenn die Summe der Familie $(M_i)_{i \in J}$ direkt ist.

2. Seien $A, B \subset M$ R -Untermoduln. Dann sind äquivalent:

(a) $M = A + B$ (dir);

(b) $M = A + B$ und $A \cap B = \mathbf{0}$.

(c) Jedes $x \in M$ hat eine eindeutige Darstellung $x = a + b$ mit $a \in A$ und $b \in B$.

Definition 2.2.3. Sei M ein R -Modul.

1. Eine Familie $(u_i)_{i \in I}$ in M heißt *linear unabhängig* über R , wenn für jede Familie $(\lambda_i)_{i \in I}$ in R gilt:

$$\text{Ist } \lambda_i = 0 \text{ für fast alle } i \in I \text{ und } \sum_{i \in I} \lambda_i u_i = 0, \text{ so folgt } \lambda_i = 0 \text{ für alle } i \in I$$

[äquivalent: Der R -Homomorphismus

$$\psi: R^{(I)} \rightarrow M, \quad \text{definiert durch } \psi((\lambda_i)_{i \in I}) = \sum_{i \in I} \lambda_i u_i, \quad \text{ist injektiv].}$$

2. Eine Familie $(u_i)_{i \in I}$ in M heißt (R -) *Basis* von M , wenn $(u_i)_{i \in I}$ ein linear unabhängiges Erzeugendensystem von M ist [äquivalent: Der R -Homomorphismus $\psi: R^{(I)} \rightarrow M$ aus 1. ist ein Isomorphismus].

3. Eine Teilmenge $B \subset M$ heißt *linear unabhängig* bzw. eine *R-Basis* von M , wenn die Familie $(b)_{b \in B}$ das ist.
4. M heißt *(R-)frei*, wenn M eine *R-Basis* besitzt. Ist $(u_i)_{i \in I}$ eine *R-Basis* von M , so sagt man, M ist frei vom *Rang* $|I|$ und schreibt $\text{rg}_R(M) = |I|$.

Korollar 2.2.4. *Sei M ein R -Modul.*

1. *Für eine Familie $(u_i)_{i \in I}$ in M sind die folgenden Aussagen äquivalent:*

- (a) *$(u_i)_{i \in I}$ ist eine R -Basis von M .*
- (b) *Jedes $x \in M$ hat eine eindeutige Darstellung*

$$x = \sum_{i \in I} \lambda_i u_i \quad \text{mit} \quad \lambda_i \in R, \lambda_i = 0 \text{ für fast alle } i \in I.$$

- (c) *Die Summe der Familie $(Ru_i)_{i \in I}$ ist direkt, und für alle $i \in I$ ist $\text{Ann}_R(u_i) = \mathbf{0}$.*
2. *Sei $(M_i)_{i \in I}$ eine Familie von R -Untermoduln von M , und sei M die direkte Summe der Familie $(M_i)_{i \in I}$. Für jedes $i \in I$ sei B_i eine R -Basis von M_i . Dann ist $B = \bigcup \{B_i \mid i \in I\}$ eine R -Basis von M .*

BEWEIS. Nach Satz 2.2.1. □

Bemerkungen 2.2.5.

1. Ist R ein Körper, so sind die Begriffe von 2.2.1 mit denen der linearen Algebra konsistent. Der Nullmodul $\mathbf{0}$ ist frei mit Basis \emptyset .
2. Der R -Modul $R^{(I)}$ ist R -frei mit Basis $(e_i)_{i \in I}$, wobei $e_i = (\dots, 0, 1_i, 0, \dots)$. Insbesondere ist R ein R -freier R -Modul mit Basis (1).
3. Der Polynomring $R[X]$ ist R -frei mit Basis $(X^i)_{i \in \mathbb{N}_0}$.
4. Sei R kommutativ und $\mathfrak{a} \triangleleft R$. Für alle $a, b \in \mathfrak{a}$ ist (a, b) linear abhängig über R [denn: Ist $a = 0$ oder $b = 0$, so ist nichts zu zeigen; ist $a \neq 0$ und $b \neq 0$, so folgt die lineare Abhängigkeit aus $ba + (-a)b = 0$]. Also folgt: Ein Ideal $\mathfrak{a} \triangleleft R$ ist genau dann R -frei, wenn $\mathfrak{a} = Ra$, wobei $a \in R$ kein Nullteiler ist].
5. Sei M ein R -Modul und $(u_i)_{i \in I}$ eine Familie in M . Genau dann ist $(u_i)_{i \in I}$ linear unabhängig über R , wenn die Menge $\{u_i \mid i \in I\}$ linear unabhängig ist und $u_i \neq u_j$ für alle $i, j \in I$ mit $i \neq j$.

Satz 2.2.6. *Sei B eine Menge.*

1. *Es gibt einen R -Modul M mit $B \subset M$, so dass B eine Basis von M ist.*
2. *Sei M ein freier R -Modul mit Basis B , N ein weiterer R -Modul und $f_0: B \rightarrow N$ eine Abbildung. Dann gibt es genau einen R -Homomorphismus $f: M \rightarrow N$ mit $f|_B = f_0$. Insbesondere ist $\text{Hom}_R(M, -) \rightarrow \text{Abb}(B, -)$ ein Isomorphismus von Funktoren $R\text{-Mod} \rightarrow \mathbf{Mg}$.*
3. *Sind M und M' freie R -Moduln mit Basis B , so gibt es genau einen Isomorphismus $f: M \rightarrow M'$ mit $f|_B = \text{id}_B$.*

BEWEIS. 1. Es genügt, einen freien R -Modul M' mit einer Basis B' und einer bijektiven Abbildung $\varphi: B \rightarrow B'$ zu konstruieren. Dann folgt nach dem Austauschprinzip die Existenz eines R -Moduls $M \supset B$ und eines R -Isomorphismus $\Phi: M \rightarrow M'$ mit $\Phi|_B = \varphi$, und dieser ist R -frei mit Basis B .

Explizit: Nach Satz 1.1.7.3 gibt es eine Menge C mit $C \cap B = \emptyset$ und eine Bijektion $\psi: C \rightarrow M' \setminus B'$. Sei dann $M = B \cup C$, $\Phi: M \rightarrow M'$ definiert durch $\Phi|_B = \varphi$ und $\Phi|_C = \psi$. Dann ist Φ bijektiv, und auf M gibt es genau eine R -Modulstruktur, so dass Φ ein R -Isomorphismus ist.

Nach Bemerkung 2.2.5.2 ist $M' = R^{(B')}$ frei mit Basis $B' = \{e_b \mid b \in B\}$.

2. Die Eindeutigkeit von f folgt aus Satz 2.1.9.1. Ist $x \in M$, so besitzt x eine eindeutige Darstellung

$$x = \sum_{b \in B} \lambda_b b \quad \text{mit } \lambda_b \in R, \lambda_b = 0 \text{ f\u00fcr fast alle } b \in B, \text{ und wir setzen } f(x) = \sum_{b \in B} \lambda_b f_0(b).$$

Dann ist f ein Homomorphismus mit $f|_B = f_0$. Daher ist $\rho(N): \text{Hom}_R(M, N) \rightarrow \text{Abb}(B, N)$, definiert durch $\rho(N)(\varphi) = \varphi|_B$, eine Bijektion, und wir m\u00fcssen zeigen, dass $(\rho(N))_{N \in R\text{-Mod}}$ ein Morphismus von Funktoren ist, also f\u00fcr jeden R -Homomorphismus $\varphi: N \rightarrow N'$ folgende Diagramm kommutativ macht.

$$\begin{array}{ccc} \text{Hom}_R(M, N) & \xrightarrow{\rho(N)} & \text{Abb}(B, N) \\ \text{Hom}_R(M, \varphi) \downarrow & & \downarrow \text{Abb}(B, \varphi) \\ \text{Hom}_R(M, N') & \xrightarrow{\rho(N')} & \text{Abb}(B, N') \end{array}$$

Ist $f \in \text{Hom}_R(M, N)$, so folgt

$$\text{Abb}(B, \varphi) \circ \rho(N)(f) = \varphi \circ \rho(N)(f) = \varphi \circ (f|_B) = (\varphi \circ f)|_B = \rho(N') \circ \text{Hom}_R(M, \varphi)(f).$$

3. Sei \mathcal{C} die folgende Kategorie. Objekte sind Abbildungen $j: B \rightarrow N$ mit $N \in R\text{-Mod}$. F\u00fcr Objekte $j: B \rightarrow N$ und $j': B \rightarrow N'$ in \mathcal{C} definiert man $\text{Mor}_{\mathcal{C}}(j, j') = \{f \in \text{Hom}_R(N, N') \mid f \circ j = j'\}$. Dann ist $(B \hookrightarrow M)$ und $(B \hookrightarrow M')$ initiale Objekte in \mathcal{C} , also isomorph. \square

Satz 2.2.7. Sei M ein R -Modul.

1. Sei E ein Erzeugendensystem von M . Dann gibt es einen R -Epimorphismus $f: R^{(E)} \rightarrow M$. Insbesondere ist jeder (endlich erzeugte) R -Modul epimorphes Bild eines (endlich erzeugten) freien R -Moduls.
2. Sei $g: M \rightarrow F$ ein R -Epimorphismus auf einen freien R -Modul F . Dann gibt es einen R -Monomorphismus $\psi: F \rightarrow M$ mit $g \circ \psi = \text{id}_F$, und f\u00fcr jedes solche ψ ist $M = \text{Ker}(g) + \text{Bi}(\psi)$ (dir).

BEWEIS. 1. Definiere $f: R^{(E)} \rightarrow M$ durch

$$f((\lambda_e)_{e \in E}) = \sum_{e \in E} \lambda_e e.$$

2. Sei $(u_i)_{i \in I}$ eine R -Basis von F . F\u00fcr $i \in I$ sei $x_i \in M$ mit $g(x_i) = u_i$. Nach Satz 2.2.6.2 gibt es genau einen R -Homomorphismus $\psi: F \rightarrow M$ mit $\psi(u_i) = x_i$ f\u00fcr alle $i \in I$. Dann ist $g \circ \psi: F \rightarrow F$ ein R -Homomorphismus mit $g \circ \psi(u_i) = u_i = \text{id}_F(u_i)$ f\u00fcr alle $i \in I$. Daher ist $g \circ \psi = \text{id}_F$, und ψ ist ein Monomorphismus.

Sei nun $\psi: F \rightarrow M$ ein R -Homomorphismus mit $g \circ \psi = \text{id}_F$. Nach Satz 2.2.1 ist zu zeigen: $M = \text{Ker}(g) + \text{Bi}(\psi)$ und $\text{Ker}(g) \cap \text{Bi}(\psi) = \mathbf{0}$. F\u00fcr $x \in M$ ist $g(x - \psi \circ g(x)) = g(x) - g \circ \psi \circ g(x) = 0$ und daher $x = [x - \psi \circ g(x)] + \psi(g(x)) \in \text{Ker}(g) + \text{Bi}(\psi)$. Ist $x \in \text{Ker}(g) \cap \text{Bi}(\psi)$, so ist $x = \psi(y)$ mit $y \in F$, und es gibt ein $u \in M$ mit $y = g(u)$. Daher folgt $0 = g(x) = g \circ \psi \circ g(u) = g(u) = y$ und daher $x = 0$. \square

Definitionen und Bemerkungen 2.2.8.

1. Sei R ein kommutativer Ring. Eine (assoziative unit\u00e4re) R -Algebra ist ein R -Modul A , gemeinsam mit einer Multiplikation $A \times A \rightarrow A$, $(a, b) \mapsto a \cdot b = ab$, so dass gilt:

A1. $(A, +, \cdot)$ ist ein Ring.

A2. F\u00fcr alle $\lambda \in R$ und $a, b \in A$ ist $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Ist A eine R -Algebra, so ist $\varepsilon: R \rightarrow A$, definiert durch $\varepsilon(\lambda) = \lambda 1_A$, ein Ringhomomorphismus, und f\u00fcr alle $\lambda \in R$ und $a \in A$ ist $\varepsilon(\lambda)a = a\varepsilon(\lambda)$ [denn: F\u00fcr alle $\lambda, \mu \in R$ und $a \in A$ ist

$$\varepsilon(\lambda\mu) = (\lambda\mu)1_A = \lambda(\mu 1_A) = \lambda[1_A(\mu 1_A)] = (\lambda 1_A)(\mu 1_A) = \varepsilon(\lambda)\varepsilon(\mu)$$

und

$$\varepsilon(\lambda)a = (\lambda 1_A)a = \lambda(1_A a) = \lambda(a 1_A) = a(\lambda 1_A) = a\varepsilon(\lambda).$$

Sei umgekehrt A ein Ring und $\varepsilon: R \rightarrow A$ ein Ringhomomorphismus, so dass $\varepsilon(\lambda)a = a\varepsilon(\lambda)$ für alle $\lambda \in R$ und $a \in A$. Dann ist A ein R -Modul und eine R -Algebra [nachrechnen!]. Man nennt ε den *Strukturhomomorphismus* der R -Algebra A und sagt auch, $\varepsilon: R \rightarrow A$ ist eine R -Algebra. Insbesondere ist jeder kommutative Oberring von R und jedes epimorphe Bild von R eine R -Algebra.

Seien $\varepsilon_1: R \rightarrow A_1$ und $\varepsilon_2: R \rightarrow A_2$ R -Algebren. Ein R -Algebrenhomomorphismus $f: A_1 \rightarrow A_2$ ist ein Ringhomomorphismus mit $f \circ \varepsilon_1 = \varepsilon_2$ [äquivalent: f ist ein Ringhomomorphismus und ein R -Modulhomomorphismus]. $\text{Hom}_{R\text{-Alg}}(A_1, A_2)$ bezeichne die Menge der R -Algebrenhomomorphismen $A_1 \rightarrow A_2$. Damit wird $R\text{-Alg}$ zur Kategorie.

Sind $A_1 \supset R$ und $A_2 \supset R$ kommutative Oberringe, so ist ein Ringhomomorphismus $f: A_1 \rightarrow A_2$ genau dann ein R -Algebrenhomomorphismus, wenn $f|_R = \text{id}_R$ [denn: Ist f ein R -Algebrenhomomorphismus und $c \in R$, so folgt $f(c) = f(c1) = cf(1) = c1 = c$. Ist $f|_R = \text{id}_R$, $c \in R$ und $x \in A_1$, so folgt $f(cx) = f(c)f(x) = cf(x)$].

Ist R ein Ring, so gibt es genau einen Ringhomomorphismus $\varepsilon: \mathbb{Z} \rightarrow R$ (gegeben durch $\varepsilon(m) = m1_R$ für alle $m \in \mathbb{Z}$). Damit wird R zur \mathbb{Z} -Algebra, und es ist $\mathbb{Z}\text{-Alg} = \mathbf{Rg}$.

2. Sei R ein kommutativer Ring, B ein (multiplikatives) Monoid und A ein freier R -Modul mit Basis B . Dann gibt es genau eine Verknüpfung $\cdot: A \times A \rightarrow A$, die A zur R -Algebra macht, so dass $B \subset A$ ein Teilmonoid ist. Diese ist gegeben durch

$$\left(\sum_{b \in B} \lambda_b b \right) \left(\sum_{b \in B} \lambda'_b b \right) = \sum_{b \in B} \left(\sum_{\substack{b_1, b_2 \in B \\ b_1 b_2 = b}} \lambda_{b_1} \lambda'_{b_2} \right) b.$$

Man nennt $A = R[B]$ die *Monoidalgebra*, den *Monoidring* oder *Halbgruppenring* von B über R . Es ist $1_B = 1_A$, $R1_B \subset A$ ist ein Teilring, und wegen $\text{Ann}_R(1_B) = \mathbf{0}$ ist $\varepsilon: R \xrightarrow{\sim} R1_B$, $\lambda \mapsto \lambda 1_B$, ein Ringisomorphismus. Identifiziert man R mit $R1_B$ vermöge ε (wofür man natürlich $R \cap (A \setminus R1_B) = \emptyset$ voraussetzen muss), so ist $R \subset A$ ein Teilring, und man sagt, R ist in A eingebettet.

3. Ein multiplikatives [additives] abelsches Monoid F heißt *frei abelsch* mit Basis P , wenn jedes $b \in F$ eine eindeutige Darstellung in der Form

$$b = \prod_{p \in P} p^{n_p} \quad \left[b = \sum_{p \in P} n_p p \right] \quad \text{mit } n_p \in \mathbb{N}_0, \quad n_p = 0 \text{ für fast alle } p \in P \text{ besitzt.}$$

\mathbb{N} ist ein multiplikatives freies abelsches Monoid mit Basis \mathbb{P} . Bezüglich komponentenweiser Addition ist $\mathbb{N}_0^{(P)} = \{(n_p)_{p \in P} \mid n_p \in \mathbb{N}_0, n_p = 0 \text{ für fast alle } p \in P\}$ ein freies abelsches Monoid mit Basis $\{e_p \mid p \in P\}$. Wie im Beweis von Satz 2.2.6 folgt nun, dass es zu jeder Menge B ein (bis auf kanonische Isomorphie) eindeutig bestimmtes freies abelsches Monoid mit Basis B gibt.

Sei $\mathbf{X} = (X_i)_{i \in I}$ eine Familie paarweise verschiedener Objekte, $[\mathbf{X}]$ das freie abelsche Monoid mit Basis $\{X_i \mid i \in I\}$, $R[\mathbf{X}] = R[(X_i)_{i \in I}]$ die Monoidalgebra von $[\mathbf{X}]$ über R , und sei R in $R[\mathbf{X}]$ eingebettet. Dann nennt man $R[\mathbf{X}]$ einen *Polynomring* in den Unbestimmten $(X_i)_{i \in I}$ und die Elemente von $[\mathbf{X}]$ *Monome* in \mathbf{X} . Für jedes $f \in R[\mathbf{X}]$ gibt es $i_1, \dots, i_k \in I$ mit $f \in R[X_{i_1}, \dots, X_{i_k}]$ [dabei ist $R[X_{i_1}, \dots, X_{i_k}]$ ein gewöhnlicher Polynomring in $(X_{i_1}, \dots, X_{i_k})$]. Ist R ein Bereich, so ist auch $R[\mathbf{X}]$ ein Bereich [denn: Sind $f, g \in R[\mathbf{X}]$, so gibt es $i_1, \dots, i_n \in I$ mit $f, g \in R[X_{i_1}, \dots, X_{i_n}]$, und aus $fg = 0$ folgt $f = 0$ oder $g = 0$].

Ist A eine kommutative R -Algebra und $(x_i)_{i \in I}$ eine Familie in A , so gibt es genau einen R -Algebrenhomomorphismus $\phi_{\mathbf{x}}: R[\mathbf{X}] \rightarrow A$ mit $\phi_{\mathbf{x}}(X_i) = x_i$ für alle $i \in I$. Diesen erhält man wie folgt:

Für $\mathbf{n} = (n_i)_{i \in I} \in \mathbb{N}_0^{(I)}$ sein $\mathbf{X}^{\mathbf{n}} = \prod_{i \in I} X_i^{n_i}$ und $\mathbf{x}^{\mathbf{n}} = \prod_{i \in I} x_i^{n_i}$. Dann hat jedes $f \in R[\mathbf{X}]$ eine eindeutige Darstellung

$$f = \sum_{\mathbf{n} \in \mathbb{N}_0^{(I)}} c_{\mathbf{n}} \mathbf{X}^{\mathbf{n}} \quad \text{mit } c_{\mathbf{n}} \in R, c_{\mathbf{n}} = 0 \text{ für fast alle } \mathbf{n} \in \mathbb{N}_0^{(I)}, \text{ und dann ist } \phi_{\mathbf{x}}(f) = f(\mathbf{x}) = \sum_{\mathbf{n} \in \mathbb{N}_0^{(I)}} c_{\mathbf{n}} \mathbf{x}^{\mathbf{n}}.$$

Man nennt $\phi_{\mathbf{x}}$ den *Einsetzungshomomorphismus*. Insbesondere ist jeder kommutative Ring epimorphes Bild eines Polynomringes $\mathbb{Z}[\mathbf{X}]$ für eine geeignete Familie $\mathbf{X} = (X_i)_{i \in I}$ von Unbestimmten.

Sei \mathcal{A} die folgende Kategorie: Objekte von \mathcal{A} sind Abbildungen $j: I \rightarrow A$ der Menge I in eine kommutative R -Algebra A . Für zwei Objekte $j_1: I \rightarrow A_1$ und $j_2: I \rightarrow A_2$ in \mathcal{A} sei

$$\text{Mor}_{\mathcal{A}}(j_1, j_2) = \{\phi \in \text{Hom}_{R\text{-Alg}}(A_1, A_2) \mid \phi \circ j_1 = j_2\}.$$

Dann ist $j: I \rightarrow R[\mathbf{X}]$, definiert durch $j(i) = X_i$ für alle $i \in I$, ein initiales Objekt in \mathcal{A} .

Definition und Satz 2.2.9. Sei M ein R -Modul und $M^* = \text{Hom}_R(M, R)$. Für $\varphi \in M^*$ und $\lambda \in R$ sei $\varphi\lambda: M \rightarrow R$ definiert durch $(\varphi\lambda)(x) = \varphi(x)\lambda$ für alle $x \in M$. Für $y \in M$ sei $y^{**}: M^* \rightarrow R$ definiert durch $y^{**}(\varphi) = \varphi(y)$ für alle $\varphi \in M^*$.

1. $M^* \times R \rightarrow M^*$, $(\varphi, \lambda) \mapsto \varphi\lambda$, ist eine R -Rechtsmodulstruktur auf M^* .

Der R -Rechtsmodul M^* heißt *Dualmodul* von M , und der R -(Links)-Modul $M^{**} = (M^*)^*$ heißt *Bidualmodul* von M .

2. Für jedes $y \in M$ ist $y^{**} \in M^{**}$, und die Abbildung $\beta: M \rightarrow M^{**}$, definiert durch $\beta(y) = y^{**}$, ist ein R -Homomorphismus.
3. Sei M R -frei und $(u_i)_{i \in I}$ eine R -Basis von M . Für $i \in I$ sei $u_i^* \in M^*$ der (nach Satz 2.2.6.2 eindeutig bestimmte R -Homomorphismus mit $u_i^*(u_j) = \delta_{i,j}$ für alle $j \in I$. Dann ist $(u_i^*)_{i \in I}$ linear unabhängig, $\beta: M \rightarrow M^{**}$ ist ein R -Monomorphismus, und für alle $f \in M^*$ gilt: Ist $\{i \in I \mid f(u_i) \neq 0\}$ endlich, so folgt

$$f = \sum_{i \in I} u_i^* f(u_i).$$

Ist insbesondere I endlich, so ist $(u_i^*)_{i \in I}$ eine R -Basis von M^* und β ist ein Isomorphismus. In diesem Falle heißt $(u_i^*)_{i \in I}$ die zu $(u_i)_{i \in I}$ duale Basis.

BEWEIS. 1. Wir müssen zeigen:

- a. Für alle $\varphi \in M^*$ und $\lambda \in R$ ist auch $\varphi\lambda \in M^*$, d. h., für alle $x, y \in M$ und $\alpha \in R$ gilt: **1)** $(\varphi\lambda)(x + y) = (\varphi\lambda)(x) + (\varphi\lambda)(y)$; **2)** $(\varphi\lambda)(\alpha x) = \alpha(\varphi\lambda)(x)$. Die Beweise sind einfach. Man beachte: Die Abbildung $\lambda\varphi: M \rightarrow R$, definiert durch $(\lambda\varphi)(x) = \lambda\varphi(x)$, ist im Allgemeinen kein R -Homomorphismus.
- b. Für alle $\varphi, \psi \in M^*$ und $\lambda, \mu \in R$ gilt: **1)** $\varphi(\lambda + \mu) = \varphi\lambda + \varphi\mu$; **2)** $(\varphi + \psi)\lambda = \varphi\lambda + \psi\lambda$; **3)** $\varphi(\lambda\mu) = (\varphi\lambda)\mu$; **4)** $\varphi 1 = \varphi$. Der Nachweis erfolgt wertweise für alle $x \in M$.

2. Wir müssen zeigen:

- a. Für alle $y \in M$ ist $y^{**} \in M^{**}$, d. h., für alle $\varphi, \psi \in M^*$ und $\alpha \in R$ gilt: **1)** $y^{**}(\varphi + \psi) = y^{**}(\varphi) + y^{**}(\psi)$; **2)** $y^{**}(\varphi\alpha) = y^{**}(\varphi)\alpha$. Das ist einfach nachzurechnen.
- b. β ist ein R -Homomorphismus, d. h., für alle $x, y \in M$ und $\alpha \in R$ gilt: **1)** $(x + y)^{**} = x^{**} + y^{**}$; **2)** $(\alpha y)^{**} = \alpha y^{**}$. Der Nachweis erfolgt wertweise für alle $\varphi \in M^*$. Man beachte: M^* ist ein R -Rechtsmodul, und daher ist $(\alpha y)^{**}(\varphi) = \alpha y^{**}(\varphi)$ für alle $\varphi \in M^*$.

3. Sei $(\lambda_i)_{i \in I}$ eine Familie in R und $\lambda_i = 0$ für fast alle $i \in I$. Aus

$$\sum_{i \in I} u_i^* \lambda_i = 0 \in M^* \quad \text{folgt} \quad 0 = \left(\sum_{i \in I} u_i^* \lambda_i \right) (u_j) = \lambda_j \quad \text{für alle } j \in I.$$

Daher ist $(u_i^*)_{i \in I}$ linear unabhängig. Ist

$$x = \sum_{i \in I} \lambda_i u_i \in \text{Ker}(\beta), \quad \text{so folgt} \quad 0 = x^{**}(u_j^*) = u_j^* \left(\sum_{i \in I} \lambda_i u_i \right) = \lambda_j \quad \text{für alle } j \in I, \text{ also } x = 0.$$

Sei nun $f \in M^*$ und $f(u_i) = 0$ für fast alle $i \in I$. Für alle $j \in I$ ist dann

$$\left(\sum_{i \in I} u_i^* f(u_i) \right) (u_j) = f(u_j) \quad \text{und daher} \quad \sum_{i \in I} u_i^* f(u_i) = f.$$

Sei nun I endlich. Dann ist $M^* = {}_R \langle \{u_i^* \mid i \in I\} \rangle$ und daher $(u_i^*)_{i \in I}$ eine Basis von M^* . Für alle $i, j \in I$ ist $u_i^{**}(u_j^*) = u_j^*(u_i) = \delta_{i,j}$. Daher ist $(u_i^{**})_{i \in I}$ die duale Basis von $(u_i^*)_{i \in I}$ und β ein Isomorphismus. \square

Bemerkung und Definition 2.2.10. Sei $g: M \rightarrow N$ ein R -Homomorphismus und $g^\dagger: N^* \rightarrow M^*$ definiert durch $g^\dagger(\varphi) = \varphi \circ g$. Man nennt g^\dagger die *Transponierte* von g . g^\dagger ist ein R -Rechtsmodulhomomorphismus, und für jeden R -Homomorphismus $h: N \rightarrow P$ ist $(h \circ g)^\dagger = g^\dagger \circ h^\dagger: P^* \rightarrow M^*$ (alles nachrechnen!). Damit wird $M \mapsto M^*, g \mapsto g^\dagger$ zu einem kontravarianten Funktor $R\text{-Mod} \rightarrow \text{Mod-}R$.

2.3. Existenz und Mächtigkeit von Basen

Satz 2.3.1. Sei R ein Divisionsring und X ein R -Vektorraum.

1. Sei W ein R -Erzeugendensystem von X und $B \subset W$. Dann sind äquivalent:
 - (a) B ist eine R -Basis von X .
 - (b) B ist eine maximale R -linear unabhängige Teilmenge von W .
 - (c) B ist ein minimales R -Erzeugendensystem von X .
2. Sei W ein R -Erzeugendensystem von X und $B \subset W$ eine R -linear unabhängige Teilmenge. Dann gibt es eine R -Basis B^* von X mit $B \subset B^* \subset W$.
3. X besitzt eine R -Basis, und je zwei R -Basen sind gleichmächtig. Genauer gilt: Ist B eine R -Basis von X , $B_0 \subset X$ R -linear unabhängig und B_1 ein R -Erzeugendensystem von X , so folgt $|B_0| \leq |B| \leq |B_1|$.

Satz 2.3.1 folgt mit dem untenstehenden allgemeinen Basissatz für Hüllenoperationen (Satz 2.3.5).

Definition 2.3.2. Sei X eine Menge. Eine Abbildung $h: \mathbb{P}(X) \rightarrow \mathbb{P}(X)$ heißt *Hüllenoperation*, wenn für alle $Z, Z' \subset X$ und alle $u, v \in X$ gilt:

- H1.** $Z \subset h(Z)$.
- H2.** Aus $Z \subset h(Z')$ folgt $h(Z) \subset h(Z')$.
- H3.** $h(Z) = \bigcup \{h(E) \mid E \subset Z \text{ endlich}\}$.
- H4.** Ist $v \in h(Z \cup \{u\}) \setminus h(Z)$, so folgt $u \in h(Z \cup \{v\})$.

Sei $h: \mathbb{P}(X) \rightarrow \mathbb{P}(X)$ eine Hüllenoperation. Eine Teilmenge $Z \subset X$ heißt

- *h-unabhängig*, wenn $h(Z') \subsetneq h(Z)$ für alle $Z' \subsetneq Z$;
- ein *h-Erzeugendensystem*, wenn $X = h(Z)$;
- eine *h-Basis* (von X), wenn Z ein h -unabhängiges h -Erzeugendensystem ist.

Bemerkung 2.3.3. Sei R ein Divisionsring und X ein R -Vektorraum. Dann ist $h: \mathbb{P}(X) \rightarrow \mathbb{P}(X)$, definiert durch $h(Z) = {}_R \langle Z \rangle$, eine Hüllenoperation, und für $Z \subset X$ gilt:

- Z ist h -unabhängig $\iff Z$ ist R -linear unabhängig.
- Z ist ein h -Erzeugendensystem $\iff X = {}_R \langle Z \rangle$.

- Z ist eine h -Basis $\iff Z$ ist eine R -Basis von X .

Die Beweise sind offensichtlich. Wir zeigen exemplarisch **H4**. Ist $v \in h(Z \cup \{u\}) \setminus h(Z)$, so folgt

$$v = \sum_{z \in Z} \lambda_z z + \lambda u \quad \text{mit} \quad \lambda_z, \lambda \in R, \lambda_z = 0 \text{ f\u00fcr fast alle } z \in Z, \lambda \neq 0,$$

und daher

$$u = \sum_{z \in Z} (-\lambda^{-1} \lambda_z) z + \lambda^{-1} v \in h(Z \cup \{v\}).$$

Lemma 2.3.4. *Sei X eine Menge und $h: \mathbb{P}(X) \rightarrow \mathbb{P}(X)$ eine H\u00fcllenoperation.*

1. Ist $Z \subset Z' \subset X$, so ist $h(Z) \subset h(Z')$, $h(h(Z)) = h(Z)$, und aus $Z \subset h(Z' \setminus Z)$ folgt $h(Z') = h(Z' \setminus Z)$.
2. $Z \subset X$ ist genau dann h -unabh\u00e4ngig, wenn $u \notin h(Z \setminus \{u\})$ f\u00fcr alle $u \in Z$.
3. Ist $Z \subset Z' \subset X$ und ist Z' h -unabh\u00e4ngig, so ist auch Z h -unabh\u00e4ngig.
4. Ist $\mathcal{S} \subset \mathbb{P}(X)$ eine Kette (bezuglich \subset), so ist $h(\bigcup \mathcal{S}) = \bigcup \{h(B) \mid B \in \mathcal{S}\}$, und es gilt: Ist jedes $B \in \mathcal{S}$ h -unabh\u00e4ngig, so ist auch $\bigcup \mathcal{S}$ h -unabh\u00e4ngig.
5. (Austauschsatz) Sei $E \subset X$ endlich und h -unabh\u00e4ngig, $F \subset X$ und $E \subset h(F)$. Dann gibt es eine Teilmenge $F_0 \subset F$ mit $|F_0| = |E|$ und $h(E \cup F \setminus F_0) = h(F)$. Insbesondere folgt $|E| \leq |F|$.

BEWEIS. 1. Ist $Z \subset Z' \subset X$, so folgt $Z \subset Z' \subset h(Z')$ nach **H1** und daher $h(Z) \subset h(Z')$ nach **H2**. Aus $h(Z) \subset h(Z)$ folgt $h(h(Z)) \subset h(Z)$ nach **H2**, und nach **H1** gilt Gleichheit. Ist $Z \subset h(Z' \setminus Z)$, so ist $Z' = (Z' \setminus Z) \cup Z \subset h(Z' \setminus Z)$ und daher $h(Z') \subset h(Z' \setminus Z) \subset h(Z')$.

2. Ist $u \in Z$ und $u \in h(Z \setminus \{u\})$, so folgt $h(Z) = h(Z \setminus \{u\})$, und daher ist Z nicht h -unabh\u00e4ngig. Ist Z nicht h -unabh\u00e4ngig, so gibt es eine Teilmenge $Z' \subsetneq Z$ mit $h(Z') = h(Z)$, und f\u00fcr $u \in Z \setminus Z'$ folgt $u \in h(Z) = h(Z') \subset h(Z \setminus \{u\})$.

3. Ist $Z \subset Z' \subset X$ und Z nicht h -unabh\u00e4ngig, so gibt es ein $u \in Z$ mit $u \in h(Z \setminus \{u\}) \subset h(Z' \setminus \{u\})$. Daher ist auch Z' nicht h -unabh\u00e4ngig.

4. Ist $x \in h(\bigcup \mathcal{S})$, so gibt es nach **H3** eine endliche Teilmenge $E \subset \bigcup \mathcal{S}$ mit $x \in h(E)$, und da \mathcal{S} eine Kette ist, gibt es ein $B \in \mathcal{S}$ mit $E \subset B$ und folglich $x \in h(B)$.

Sei nun jedes $B \in \mathcal{S}$ h -unabh\u00e4ngig und $u \in \bigcup \mathcal{S}$. Sei $B_1 \in \mathcal{S}$ mit $u \in B_1$. Dann ist $u \notin h(B_1 \setminus \{u\})$. Ist $B \in \mathcal{S}$ beliebig, so ist $B \subset B_1$ oder $B_1 \subset B$. Im ersten Fall ist $u \notin h(B \setminus \{u\})$, im zweiten Fall ist $u \in B$ und daher ebenfalls $u \notin h(B \setminus \{u\})$. Daher folgt $u \notin \bigcup \{h(B \setminus \{u\}) \mid B \in \mathcal{S}\} = h(\bigcup \mathcal{S} \setminus \{u\})$.

5. Induktion nach $|E|$. Im Falle $E = \emptyset$ ist nichts zu zeigen. Sei also $v \in E$ und $E' = E \setminus \{v\}$. Dann gibt es nach Induktionsvoraussetzung eine Teilmenge $F'_0 \subset F$ mit $|F'_0| = |E'|$ und $h(E' \cup F \setminus F'_0) = h(F)$. Daher ist $v \in h(E' \cup F \setminus F'_0)$, es gibt eine endliche Teilmenge $G \subset E' \cup F \setminus F'_0$ mit $v \in h(G)$, und es sei G minimal mit dieser Eigenschaft. Dann ist $G \not\subset E'$ und daher $G \cap (F \setminus F'_0) \neq \emptyset$. Sei nun $u \in G \cap (F \setminus F'_0)$, $G_0 = G \setminus \{u\}$ und $F_0 = F'_0 \cup \{u\}$. Dann ist $|F_0| = |E|$, und wegen $v \in h(G_0 \cup \{u\}) \setminus h(G_0)$ folgt nach **H4** $u \in h(G_0 \cup \{v\}) \subset h(E \cup F \setminus F_0)$, denn $G_0 \cup \{v\} \subset [E' \cup F \setminus (F'_0 \cup \{u\})] \cup \{v\} = E \cup F \setminus F_0$. Folglich ist $h(F) = h(E' \cup F \setminus F'_0) \subset h(E \cup F \setminus F_0) = h(E \cup F \cup \{u\} \setminus F_0) = h(E \cup F \setminus F_0)$. \square

Satz 2.3.5. *Sei X eine Menge und $h: \mathbb{P}(X) \rightarrow \mathbb{P}(X)$ eine H\u00fcllenoperation.*

1. Sei W ein h -Erzeugendensystem von X und $B \subset W$. Dann sind \u00e4quivalent:
 - (a) B ist eine h -Basis.
 - (b) B ist eine maximale h -unabh\u00e4ngige Teilmenge von W .
 - (c) B ist ein minimales h -Erzeugendensystem von X .
2. Sei W ein h -Erzeugendensystem von X und $B \subset W$ eine h -unabh\u00e4ngige Teilmenge. Dann gibt es eine h -Basis B^* mit $B \subset B^* \subset W$.

3. X besitzt eine h -Basis, und je zwei h -Basen sind gleichmächtig.

Genauer gilt: Ist B eine h -Basis, $B_0 \subset X$ h -unabhängig und B_1 ein h -Erzeugendensystem von X , so folgt $|B_0| \leq |B| \leq |B_1|$.

BEWEIS. 1. (a) \Rightarrow (b) Als h -Basis ist B h -unabhängig. Ist $B' \supsetneq B$, so folgt $X = h(B) \subset h(B') \subset X$, also $h(B) = h(B')$ und daher ist B' nicht h -unabhängig.

(b) \Rightarrow (c) Wir zeigen $W \subset h(B)$. Dann folgt $X = h(W) \subset h(B)$, also $X = h(B)$, und für jede echte Teilmenge $B' \subsetneq B$ ist $h(B') \subsetneq h(B)$. Angenommen, es gibt ein $z \in W \setminus h(B)$. Dann ist $z \notin B$, also $B \cup \{z\}$ nicht h -unabhängig, und daher gibt es ein $u \in B \cup \{z\}$ mit $u \in h(B \cup \{z\} \setminus \{u\})$. Wegen $z \notin h(B)$ ist $u \neq z$, also $u \in B$. Daher ist $u \in h(B \cup \{z\} \setminus \{u\}) \setminus h(B \setminus \{u\})$, und es folgt $z \in h(B \setminus \{u\} \cup \{u\}) = h(B)$.

(c) \Rightarrow (a) Ist B nicht h -unabhängig, so gibt es eine echte Teilmenge $B' \subsetneq B$ mit $h(B') = h(B) = X$ im Widerspruch zur Minimalität von B .

2. Die Menge $\Omega = \{B' \subset W \mid B' \text{ ist } h\text{-unabhängig, und } B \subset B'\}$ ist induktiv geordnet nach Lemma 2.3.4.4 und besitzt nach dem Zorn'schen Lemma ein maximales Element B^* . Dieses ist nach 1. ein h -Basis von X .

3. Die Existenz einer h -Basis folgt aus 2. mit $B = \emptyset$ und $W = X$. Als Nächstes zeigen wir:

A. Ist B eine h -Basis, $B_0 \subset X$ h -unabhängig, und ist entweder B oder B_0 endlich, so folgt $|B_0| \leq |B|$.

B. Sind B und B' h -Basen, so folgt $|B| = |B'|$.

Seien **A** und **B** gezeigt. Sei B eine h -Basis, $B_0 \subset X$ eine h -unabhängige Menge und B_1 ein h -Erzeugendensystem. Nach 2. gibt es h -Basen B'_0 und B'_1 von X mit $B_0 \subset B'_0$ und $B'_1 \subset B_1$, und nach **B.** ist $|B_0| \leq |B'_0| = |B| = |B'_1| \leq |B_1|$.

Beweis von A. Ist B_0 endlich, so folgt $|B_0| \leq |B|$ aus Lemma 2.3.4.5 wegen $B_0 \subset X = h(B)$. Ist B endlich, so folgt $|B_1| \leq |B|$ für jede endliche Teilmenge $B_1 \subset B_0$, und daher auch $|B_0| \leq |B|$.

Beweis von B. Es genügt, $|B| \leq |B'|$ zu zeigen. Ist B' endlich, so folgt die Behauptung aus **A.** Seien also B' unendlich. Für $b \in B'$ sei $B_b \subset B$ endlich mit $b \in h(B_b)$ und $B^* = \bigcup \{B_b \mid b \in B'\} \subset B$. Für $b \in B'$ ist dann $b \in h(B_b) \subset h(B^*)$ und daher folgt $X = h(B') \subset h(B^*)$, also $h(B^*) = X$. Nach 1. ist B ein minimales h -Erzeugendensystem von X und daher $B = B^*$. Daher folgt $|B| = |B^*| \leq |B'| \omega = |B'|$ nach Satz 1.3.7. \square

Satz 2.3.6. Sei M ein R -Modul und $E \subset M$ mit $M = {}_R\langle E \rangle$.

1. Sei $(M_i \neq \mathbf{0})_{i \in I}$ eine unendliche Familie von R -Modulen, so dass

$$M = \bigoplus_{i \in I} M_i = \langle E \rangle. \quad \text{Dann ist } |E| \geq |I|.$$

2. Seien B, B' R -Basen von M . Ist B unendlich, so folgt $|B| = |B'| \leq |E|$.

3. Sei B eine R -Basis von M . Dann ist $|M| = |R|^{|B|}$, falls B endlich ist, und $|M| = \max\{|R|, |B|\}$ sonst.

4. Sei $(u_i)_{i \in I}$ eine R -Basis von M und $\mathfrak{a} \triangleleft R$. Dann hat jedes $x \in \mathfrak{a}M$ eine eindeutige Darstellung

$$x = \sum_{i \in I} c_i u_i \quad \text{mit } c_i \in \mathfrak{a}, c_i = 0 \text{ für fast alle } i \in I,$$

und $M/\mathfrak{a}M$ ist ein freier R/\mathfrak{a} -Modul mit Basis $(u_i + \mathfrak{a}M)_{i \in I}$.

5. Sei R kommutativ, und seien B und B' R -Basen von M . Dann ist $|B| = |B'|$.

BEWEIS. 1. Für $x = (x_i)_{i \in I} \in M$ sei $\text{supp}(x) = \{i \in I \mid x_i \neq 0\} \subset I$, und diese Mengen sind endlich. Dann ist $I = \bigcup \{\text{supp}(x) \mid x \in E\}$, I ist unendlich, und daher ist auch E unendlich. Aus Satz 1.3.7 folgt $|I| \leq |E| \omega = |E|$.

2. Wegen $M \cong R^{(B)}$ können wir $M = R^{(B)}$ annehmen. Dann folgt $|E| \geq |B|$ aus 1. Insbesondere ist $|B'| \leq |B|$ und $|B| \leq |B'|$, also $|B| = |B'|$.

3. Wir können wieder $M = R^{(B)}$ annehmen. Ist B endlich, so ist $M = R^{(B)} = R^B$ und $|M| = |R|^{|B|}$. Sei nun B unendlich. Dann ist auch M unendlich und daher $|M| = |M \setminus \mathbf{0}|$. Sei \mathcal{P}^* die Menge aller endlichen nicht-leeren Teilmengen von B . Nach Satz 1.3.8 ist $|B| = |\mathcal{P}^* \cup \{\emptyset\}| = |\mathcal{P}^*| + 1 = |\mathcal{P}^*|$. Für $J \in \mathcal{P}^*$ sei

$$M_J = \{(x_b)_{b \in B} \in M \mid x_b \neq 0 \iff b \in J\}, \quad \text{also } |M_J| = |R^{\bullet}|^J \quad \text{und} \quad M \setminus \mathbf{0} = \bigcup \{M_J \mid J \in \mathcal{P}^*\}.$$

$(M_J)_{J \in \mathcal{P}^*}$ ist eine Familie paarweise disjunkter nicht-leerer Mengen. Ist R endlich, so folgt $1 \leq |M_J| \leq \omega$ für alle $J \in \mathcal{P}^*$. Nach Satz 1.3.7 ist $|B| = |\mathcal{P}^*| \leq |M \setminus \mathbf{0}| \leq |\mathcal{P}^*| \omega = |B|$, also $|M| = |M \setminus \mathbf{0}| = |B|$. Ist R unendlich, so ist $|M_J| = |R^{\bullet}| = |R|$ für alle $J \in \mathcal{P}^*$ und daher

$$|M| = |M \setminus \mathbf{0}| = |R| |\mathcal{P}^*| = |R| |B| = \max\{|R|, |B|\}.$$

4. Die Eindeutigkeit der Darstellung folgt aus Korollar 2.2.4. Sei $x \in \mathfrak{a}M$. Dann ist

$$x = \sum_{\nu=1}^n \lambda_{\nu} a_{\nu} \quad \text{mit } n \in \mathbb{N}, \lambda_{\nu} \in \mathfrak{a} \quad \text{und} \quad a_{\nu} \in M.$$

Jedes a_{ν} hat eine Darstellung

$$a_{\nu} = \sum_{i \in I} \lambda_{i,\nu} u_i \quad \text{mit } \lambda_{i,\nu} \in R, \quad \lambda_{i,\nu} = 0 \quad \text{für fast alle } i \in I,$$

es folgt

$$x = \sum_{i \in I} \left(\sum_{\nu=1}^n \lambda_{\nu} \lambda_{i,\nu} \right) u_i, \quad \text{und es ist } \sum_{\nu=1}^n \lambda_{\nu} \lambda_{i,\nu} \in \mathfrak{a} \quad \text{für alle } i \in I.$$

Die Abbildung $M \rightarrow M/\mathfrak{a}M$, $x \mapsto x + \mathfrak{a}M$, ist ein R -Epimorphismus, und daher ist $(u_i + \mathfrak{a}M)_{i \in I}$ ein R -Erzeugendensystem von $M/\mathfrak{a}M$. Sei nun

$$\sum_{i \in I} \bar{\lambda}_i (u_i + \mathfrak{a}M) = 0 \in M/\mathfrak{a}M \quad \text{mit } \bar{\lambda}_i \in R/\mathfrak{a}, \bar{\lambda}_i = 0 \quad \text{für fast alle } i \in I.$$

Dann ist $\bar{\lambda}_i = \lambda_i + \mathfrak{a}$ mit $\lambda_i \in R$ und $\lambda_i = 0$ für fast alle $i \in I$, und es folgt

$$0 = \sum_{i \in I} \bar{\lambda}_i (u_i + \mathfrak{a}M) = \sum_{i \in I} \lambda_i u_i + \mathfrak{a}M, \quad \text{also } \sum_{i \in I} \lambda_i u_i \in \mathfrak{a}M,$$

und (nach 1.) $\lambda_i \in \mathfrak{a}$, also $\bar{\lambda}_i = 0$ für alle $i \in I$. Daher ist $(u_i + \mathfrak{a}M)_{i \in I}$ eine R/\mathfrak{a} -Basis von $M/\mathfrak{a}M$.

5. Ist R kommutativ, so gibt es nach dem Krull'schen Existenzsatz (siehe den nachfolgenden Satz 2.3.7) ein maximales Ideal $\mathfrak{m} \triangleleft R$. Ist $\pi: M \rightarrow M/\mathfrak{m}M$ der kanonische Epimorphismus, so sind nach 4. die Familien $(\pi(b))_{b \in B}$ und $(\pi(b))_{b \in B'}$ R/\mathfrak{m} -Basen von $M/\mathfrak{m}M$. Aber R/\mathfrak{m} ist ein Körper, und daher folgt $|B| = |B'|$ nach Satz 2.3.1. \square

Satz 2.3.7 (Krull'scher Existenzsatz für Primideale). *Sei R kommutativ, $\mathfrak{a} \triangleleft R$, $\emptyset \neq T \subset R$ eine multiplikativ abgeschlossene Teilmenge mit $T \cap \mathfrak{a} = \emptyset$ und $\Omega = \{\mathfrak{b} \triangleleft R \mid \mathfrak{a} \subset \mathfrak{b}, \mathfrak{b} \cap T = \emptyset\}$.*

Dann besitzt Ω (bezüglich \subset) maximale Elemente, und jedes maximale Element von Ω ist ein Primideal. Insbesondere besitzt R maximale Ideale, und jedes Ideal $\mathfrak{a} \neq R$ ist in einem maximalen Ideal von R enthalten.

BEWEIS. (Ω, \subset) ist induktiv geordnet und besitzt daher nach dem Zorn'schen Lemma maximale Elemente. Sei $\mathfrak{p} \in \Omega$ maximal, also $\mathfrak{p} \triangleleft R$, $\mathfrak{a} \subset \mathfrak{p}$ und $\mathfrak{p} \cap T = \emptyset$. Sind dann $a, b \in R \setminus \mathfrak{p}$, so ist $\mathfrak{p} + aR \notin \Omega$ und $\mathfrak{p} + bR \notin \Omega$. Daher existieren $p, q \in \mathfrak{p}$ und $x, y \in R$ mit $p + ax \in T$ und $q + by \in T$. Dann folgt $(p + ax)(q + by) = (pq + pby + axq) + xy \in T$, und wegen $pq + pby + axq \in \mathfrak{p}$ ist $xy \notin \mathfrak{p}$. Daher \mathfrak{p} ein Primideal.

Mit $\mathfrak{a} = \mathbf{0}$ und $T = R^\times$ folgt die Existenz maximaler Ideale. Ist $\mathfrak{a} \neq R$ ein Ideal von R , so folgt die Existenz eines \mathfrak{a} umfassenden maximalen Ideals mit $T = R^\times$. \square

2.4. Matrizenrechnung

Definitionen und Bemerkungen 2.4.1. Seien $m, n \in \mathbb{N}$. Für eine Menge C sei $\mathbf{M}_{m,n}(C)$ die Menge der (m, n) -Matrizen über C und $\mathbf{M}_m(C) = \mathbf{M}_{m,m}(C)$. Ist $A = (a_{\mu,\nu})_{\mu \in [1,m], \nu \in [1,n]} \in \mathbf{M}_{m,n}(C)$, so schreiben wir auch $A_{\mu,\nu} = a_{\mu,\nu}$ und definieren die zu A *transponierte* Matrix $A^t \in \mathbf{M}_{n,m}(C)$ durch $(A^t)_{\nu,\mu} = A_{\mu,\nu}$ für alle $(\nu, \mu) \in [1, n] \times [1, m]$.

Ist C eine additive abelsche Gruppe, so ist $\mathbf{M}_{m,n}(C)$ bezüglich der komponentenweisen Addition eine zu C^{mn} isomorphe abelsche Gruppe, es sei $\mathbf{0}_{m,n} \in \mathbf{M}_{m,n}(C)$ die (m, n) -Nullmatrix. $\mathbf{M}_{m,n}(R)$ mit komponentenweiser Skalarmultiplikation ist ein freier R -Modul vom Rang mn , und es sei $I_n \in \mathbf{M}_n(R)$ die n -reihige Einheitsmatrix.

Sei E ein R -Rechtsmodul. Für $m, n, q \in \mathbb{N}$, $A \in \mathbf{M}_{m,n}(E)$ und $X \in \mathbf{M}_{n,q}(R)$ definiert man $AX \in \mathbf{M}_{m,q}(E)$ durch

$$(AX)_{\mu,\rho} = \sum_{\nu=1}^n A_{\mu,\nu} X_{\nu,\rho} \quad \text{für alle } \mu \in [1, m] \text{ und } \rho \in [1, q].$$

Für diese Matrizenmultiplikation gelten die Assoziativ- und Distributivgesetze. Insbesondere ist $\mathbf{M}_n(R)$ ein Ring mit Eins I_n , und die Abbildung $A \mapsto A^t$ definiert einen Isomorphismus $\mathbf{M}_n(R)^{\text{op}} \xrightarrow{\sim} \mathbf{M}_n(R^{\text{op}})$. Es sei $\text{GL}_n(R) = \mathbf{M}_n(R)^\times$. Ist $A \in \text{GL}_n(R)$, so ist auch $A^t \in \text{GL}_n(R)$, und $(A^t)^{-1} = (A^{-1})^t$. Ist R kommutativ, so ist $\mathbf{M}_n(R)$ eine R -Algebra.

Ist $f: R \rightarrow R'$ ein Ringhomomorphismus, so ist $\mathbf{M}_n(f): \mathbf{M}_n(R) \rightarrow \mathbf{M}_n(R')$ ein Ringhomomorphismus, und damit wird $\mathbf{M}_n: \mathbf{Rg} \rightarrow \mathbf{Rg}$ zum Funktor.

Satz 2.4.2. Sei $n \in \mathbb{N}$, E ein freier R -Rechtsmodul und $\mathbf{u} = (u_1, \dots, u_n) \in \mathbf{M}_{1,n}(E)$ eine R -Basis von E .

1. Ist $m \in \mathbb{N}$ und $\mathbf{v} = (v_1, \dots, v_m) \in \mathbf{M}_{1,m}(E)$, so gibt es genau eine Matrix $A \in \mathbf{M}_{n,m}(R)$ mit $\mathbf{v} = \mathbf{u}A$.
2. Ist $A \in \mathbf{M}_n(R)$ und $\mathbf{v} = \mathbf{u}A \in \mathbf{M}_{1,n}(E)$, so ist \mathbf{v} genau dann eine R -Basis von E , wenn $A \in \text{GL}_n(R)$.

BEWEIS. 1. Nach Korollar 2.2.4 gibt es zu jedem $\mu \in [1, m]$ eindeutig bestimmte $A_{1,\mu}, \dots, A_{n,\mu} \in R$ mit

$$v_\mu = \sum_{\nu=1}^m u_\nu A_{\nu,\mu}, \quad \text{und } A = (A_{\nu,\mu})_{\nu \in [1,n], \mu \in [1,m]} \text{ ist die eindeutig bestimmte Matrix mit } \mathbf{v} = \mathbf{u}A.$$

2. Sei \mathbf{v} eine R -Basis von E . Nach 1. gibt es eine Matrix $A' \in \mathbf{M}_n(R)$ mit $\mathbf{u} = \mathbf{v}A'$. Damit folgt $\mathbf{u} = \mathbf{u}AA'$ und $\mathbf{v} = \mathbf{v}A'A$, und wegen der Eindeutigkeit in 1. ist $AA' = A'A = I_n$, also $A \in \text{GL}_n(R)$.

Sei nun $A \in \text{GL}_n(R)$. Dann ist $\mathbf{u} = \mathbf{v}A^{-1}$, also $\{u_1, \dots, u_n\} \subset {}_R\langle v_1, \dots, v_n \rangle$ und daher \mathbf{v} ein Erzeugendensystem von R . Seien nun $\lambda_1, \dots, \lambda_n \in R$ mit $0 = v_1\lambda_1 + \dots + v_n\lambda_n$, und sei $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n)^t$. Dann folgt $0 = \mathbf{v}\boldsymbol{\lambda} = \mathbf{u}(A\boldsymbol{\lambda})$, also $A\boldsymbol{\lambda} = \mathbf{0}_{n,1}$ und daher $\boldsymbol{\lambda} = A^{-1}\mathbf{0}_{n,1} = \mathbf{0}_{n,1}$. \square

Definitionen und Bemerkungen 2.4.3. Sei E ein freier R -Rechtsmodul mit Basis $\mathbf{u} = (u_1, \dots, u_n)$, F ein freier R -Rechtsmodul mit Basis $\mathbf{v} = (v_1, \dots, v_m)$, $f \in \text{Hom}_R(E, F)$ und $f(\mathbf{u}) = (f(u_1), \dots, f(u_n))$. Nach Satz 2.4.2 gibt es genau eine Matrix $\mathcal{M}_{\mathbf{u},\mathbf{v}}(f) \in \mathbf{M}_{m,n}(R)$ mit $f(\mathbf{u}) = \mathbf{v}\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)$. Man nennt $\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)$ die *Matrix von f bezüglich des Basispaares (\mathbf{u}, \mathbf{v})* . Die Abbildung

$$\mathcal{M}_{\mathbf{u},\mathbf{v}}: \text{Hom}_R(E, F) \rightarrow \mathbf{M}_{m,n}(R)$$

ist ein Isomorphismus abelscher Gruppen [denn: Offensichtlich ist $\mathcal{M}_{\mathbf{u},\mathbf{v}}$ ein Homomorphismus, und zu jedem $A \in \mathbf{M}_{m,n}(R)$ gibt es nach Satz 2.2.6.2 genau einen R -Homomorphismus $f: E \rightarrow F$ mit $f(\mathbf{u}) = \mathbf{v}A$]. Ist R kommutativ, so ist $\mathcal{M}_{\mathbf{u},\mathbf{v}}$ ein R -Isomorphismus.

Sei \mathbf{u}' eine weitere R -Basis von E und \mathbf{v}' eine weitere R -Basis von F . Dann gibt es nach Satz 2.4.2 Matrizen $S \in \mathbf{GL}_n(R)$ und $T \in \mathbf{GL}_m(R)$ mit $\mathbf{u}' = \mathbf{u}S$ und $\mathbf{v}' = \mathbf{v}T$, und es folgt

$$f(\mathbf{u}') = f(\mathbf{u})S = \mathbf{v}\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)S = \mathbf{v}'T^{-1}\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)S \quad \text{und daher} \quad \mathcal{M}_{\mathbf{u}',\mathbf{v}'}(f) = T^{-1}\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)S.$$

Zwei Matrizen $A, B \in \mathbf{M}_{m,n}(R)$ heißen *äquivalent*, $A \sim B$, wenn es Matrizen $U \in \mathbf{GL}_m(R)$ und $V \in \mathbf{GL}_n(R)$ gibt mit $B = UAV$. \sim ist eine Äquivalenzrelation auf $\mathbf{M}_{m,n}(R)$, und die Äquivalenzklasse von $\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)$ ist durch f eindeutig bestimmt.

Sei $q \in \mathbb{N}$, G ein freier R -Rechtsmodul mit Basis $\mathbf{w} = (w_1, \dots, w_q)$ und $g \in \text{Hom}_R(F, G)$. Dann folgt $(g \circ f)(\mathbf{u}) = g(\mathbf{v}\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)) = g(\mathbf{v})\mathcal{M}_{\mathbf{u},\mathbf{v}}(f) = \mathbf{w}\mathcal{M}_{\mathbf{v},\mathbf{w}}(g)\mathcal{M}_{\mathbf{u},\mathbf{v}}(f)$ und daher

$$\mathcal{M}_{\mathbf{u},\mathbf{w}}(g \circ f) = \mathcal{M}_{\mathbf{v},\mathbf{w}}(g)\mathcal{M}_{\mathbf{u},\mathbf{v}}(f).$$

Ist $f \in \text{End}_R(E)$, so ist $\mathcal{M}_{\mathbf{u}}(f) = \mathcal{M}_{\mathbf{u},\mathbf{u}}(f) \in \mathbf{M}_n(R)$ und $\mathcal{M}_{\mathbf{u}'}(f) = S^{-1}\mathcal{M}_{\mathbf{u}}(f)S$. Die Abbildung $\mathcal{M}_{\mathbf{u}}: \text{End}_R(E) \rightarrow \mathbf{M}_n(R)$ ist ein Ringisomorphismus (und sogar ein R -Algebrenisomorphismus, falls R kommutativ ist).

Man beachte: Ist E ein R -Linksmodul, so ist E ein R^{op} -Rechtsmodul und $\mathcal{M}_{\mathbf{u}}: \text{End}_R(E) \xrightarrow{\sim} \mathbf{M}_n(R^{\text{op}})$.

Zwei Matrizen $A, B \in \mathbf{M}_n(R)$ heißen *ähnlich*, $A \simeq B$, wenn es eine Matrix $U \in \mathbf{GL}_n(R)$ gibt mit $B = U^{-1}AU$. \simeq ist eine Äquivalenzrelation auf $\mathbf{M}_n(R)$. Ist $f \in \text{End}_R(E)$, so ist die Ähnlichkeitsklasse von $\mathcal{M}_{\mathbf{u}}(f)$ durch f eindeutig bestimmt.

Definitionen und Bemerkungen 2.4.4. Sei R kommutativ und $n \in \mathbb{N}$. Für $A \in \mathbf{M}_n(R)$ definiert man die Determinante durch

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}.$$

Dann gelten alle aus der Linearen Algebra über Körpern bekannten Rechenregeln für Determinanten (für die man nicht dividieren muss) [Beweisskizze: Ist R ein Integritätsbereich, so bette man R in seinen Quotientenkörper K ein und rechne in K . Ist R beliebig, so gibt es nach Bemerkung 2.2.8.3 einen Bereich $D = \mathbb{Z}[\mathbf{X}]$ und einen Ringepimorphismus $f: D \rightarrow R$. Dieser induziert einen Ringepimorphismus $\mathbf{M}_n(f): \mathbf{M}_n(D) \rightarrow \mathbf{M}_n(R)$, und für alle $C \in \mathbf{M}_n(D)$ ist $\det(\mathbf{M}_n(f)(C)) = f(\det(C))$, und mittels f übertragen sich alle Determinantenrechenregeln von D auf R].

Für eine Matrix $A \in \mathbf{M}_n(R)$ und $i, j \in [1, n]$ bezeichne $A^{j,i} \in \mathbf{M}_{n-1}(R)$ die Matrix, welche aus A durch Streichen der j -ten Zeile und der i -ten Spalte entsteht. Definiert man die *adjungierte Matrix* $A^\#$ von A durch

$$(A^\#)_{i,j} = (-1)^{i+j} \det(A^{j,i}), \quad \text{so folgt} \quad AA^\# = A^\#A = \det(A)I_n.$$

Für $A, B \in \mathbf{M}_n(R)$ ist $\det(AB) = \det(A)\det(B)$, und genau dann ist $A \in \mathbf{GL}_n(R)$, wenn $\det(A) \in R^\times$ (dann ist $\det(A)^{-1} = \det(A^{-1})$). [Beweis: Ist $A \in \mathbf{GL}_n(R)$, so folgt $1 = \det(I_n) = \det(A)\det(A^{-1})$. Ist $\det(A) \in R^\times$ und $A' = \det(A)^{-1}A^\#$, so folgt $AA' = A'A = I_n$].

Lemma 2.4.5. Sei R kommutativ, $n \in \mathbb{N}$, seien $\mathbf{b}_1, \dots, \mathbf{b}_n, \mathbf{b} \in \mathbf{M}_{n,1}(R)$ und $\alpha_1, \dots, \alpha_n \in R$. Dann ist

$$\det(\mathbf{b}_1 + \alpha_1\mathbf{b}, \dots, \mathbf{b}_n + \alpha_n\mathbf{b}) = \det(\mathbf{b}_1, \dots, \mathbf{b}_n) + \sum_{i=1}^n \alpha_i \det(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_n).$$

BEWEIS. Wir zeigen durch Induktion für alle $j \in [0, n]$

$$\det(\mathbf{b}_1 + \alpha_1 \mathbf{b}, \dots, \mathbf{b}_j + \alpha_j \mathbf{b}, \mathbf{b}_{j+1}, \dots, \mathbf{b}_n) = \det(\mathbf{b}_1, \dots, \mathbf{b}_n) + \sum_{i=1}^j \alpha_i \det(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_n).$$

Für $j = 0$ ist nichts zu zeigen.

$j \in [0, n-1]$, $j \rightarrow j+1$: Wegen der Linearität der Determinante in den Spalten und unter Benutzung der Induktionsvoraussetzung ist

$$\begin{aligned} & \det(\mathbf{b}_1 + \alpha_1 \mathbf{b}, \dots, \mathbf{b}_{j+1} + \alpha_{j+1} \mathbf{b}, \mathbf{b}_{j+2}, \dots, \mathbf{b}_n) \\ &= \det(\mathbf{b}_1 + \alpha_1 \mathbf{b}, \dots, \mathbf{b}_j + \alpha_j \mathbf{b}, \mathbf{b}_{j+1}, \dots, \mathbf{b}_n) + \alpha_{j+1} \det(\mathbf{b}_1 + \alpha_1 \mathbf{b}, \dots, \mathbf{b}_j + \alpha_j \mathbf{b}, \mathbf{b}, \mathbf{b}_{j+2}, \dots, \mathbf{b}_n) \\ &= \det(\mathbf{b}_1, \dots, \mathbf{b}_n) + \sum_{i=1}^j \alpha_i \det(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_n) \\ &\quad + \alpha_{j+1} \left[\det(\mathbf{b}_1, \dots, \mathbf{b}_j, \mathbf{b}, \mathbf{b}_{j+2}, \dots, \mathbf{b}_n) + \sum_{i=1}^j \alpha_i \det(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_j, \mathbf{b}, \mathbf{b}_{j+2}, \dots, \mathbf{b}_n) \right] \\ &= \det(\mathbf{b}_1, \dots, \mathbf{b}_n) + \sum_{i=1}^{j+1} \alpha_i \det(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}, \mathbf{b}, \mathbf{b}_{i+1}, \dots, \mathbf{b}_n) \end{aligned}$$

(denn die Determinante einer Matrix mit zwei gleichen Spalten verschwindet). \square

Definition 2.4.6. Sei R kommutativ, $M = {}_R\langle x_1, \dots, x_n \rangle$ ein endlich erzeugter R -Modul und $k \in \mathbb{N}$. Sei $m \in \mathbb{N}$. Eine (m, n) -Matrix $\Lambda = (\lambda_{\mu, \nu})_{\mu \in [1, m], \nu \in [1, n]} \in \mathbf{M}_{m, n}(R)$ heißt *Relationenmatrix* von (x_1, \dots, x_n) , wenn $\lambda_{\mu, 1}x_1 + \dots + \lambda_{\mu, n}x_n = 0$ für alle $\mu \in [1, m]$.

Ein Element $\delta \in R$ heißt *Relationendeterminante der Ordnung k* von (x_1, \dots, x_n) , wenn δ die Determinante einer k -reihigen Untermatrix einer Relationenmatrix von (x_1, \dots, x_n) ist. $\mathcal{F}_k(x_1, \dots, x_n)$ bezeichne die Menge aller Relationendeterminanten von (x_1, \dots, x_n) . Offensichtlich ist jedes $\delta \in \mathcal{F}_k(x_1, \dots, x_n)$ eine k -reihige Unterdeterminante einer Relationenmatrix $\Lambda \in \mathbf{M}_{k, n}(R)$.

Für $k \in [0, n-1]$ sei $\mathbf{F}_k(M) = {}_R\langle \mathcal{F}_{n-k}(x_1, \dots, x_n) \rangle$, und für $k \geq n$ sei $\mathbf{F}_k(M) = R$ [die Ideale $\mathbf{F}_k(M)$ hängen nur von M und nicht vom Erzeugendensystem (x_1, \dots, x_n) ab, siehe Satz 2.4.7]. Das Ideal \mathbf{F}_k heißt *k -tes Fittingideal* von M .

Satz 2.4.7. Sei R kommutativ und M ein endlich erzeugter R -Modul. Dann ist die Folge der Fittingideale $(\mathbf{F}_k(M))_{k \geq 0}$ unabhängig von dem der Definition zugrunde liegenden Erzeugendensystem, und für alle $k \geq 0$ ist $\mathbf{F}_k(M) \subset \mathbf{F}_{k+1}(M)$.

BEWEIS. Sei $M = {}_R\langle x_1, \dots, x_n \rangle$, $k \in [1, n-1]$ und $\delta \in \mathcal{F}_{k+1}(x_1, \dots, x_n)$. Dann ist δ eine $(k+1)$ -reihige Unterdeterminante einer Relationenmatrix von (x_1, \dots, x_n) . Entwickelt man diese nach einer Zeile, so folgt $\delta = \lambda_1 \delta_1 + \dots + \lambda_{k+1} \delta_{k+1}$ mit k -reihigen Unterdeterminanten $\delta_i \in \mathcal{F}_k(x_1, \dots, x_n)$ und $\lambda_i \in R$. Damit erhalten wir

$${}_R\langle \mathcal{F}_{k+1}(x_1, \dots, x_n) \rangle \subset {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$$

und (sobald die Unabhängigkeit vom Erzeugendensystem gezeigt ist), $\mathbf{F}_{n-k-1}(M) \subset \mathbf{F}_{n-k}(M)$, also $\mathbf{F}_0(M) \subset \mathbf{F}_1(M) \subset \dots \subset \mathbf{F}_n(M) = R$.

Es genügt daher, die folgende Behauptung zu zeigen.

- A.** Sei $M = {}_R\langle x_1, \dots, x_n \rangle$ und $x_{n+1} \in M$. Dann ist ${}_R\langle \mathcal{F}_1(x_1, \dots, x_{n+1}) \rangle = R$, und für alle $k \in [1, n]$ ist ${}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle = {}_R\langle \mathcal{F}_{k+1}(x_1, \dots, x_{n+1}) \rangle$.

Beweis von A. Sei $x_{n+1} = \alpha_1 x_1 + \dots + \alpha_n x_n$ mit $\alpha_1, \dots, \alpha_n \in R$. Dann ist $(-\alpha_1, \dots, -\alpha_n, 1) \in M_{1, n+1}(R)$ eine Relationenmatrix von (x_1, \dots, x_{n+1}) und daher $1 \in \mathcal{F}_1(x_1, \dots, x_{n+1})$.

Sei nun $k \in [1, n]$.

1) $\mathcal{F}_k(x_1, \dots, x_n) \subset {}_R\langle \mathcal{F}_{k+1}(x_1, \dots, x_{n+1}) \rangle$: Sei $\delta \in \mathcal{F}_k(x_1, \dots, x_n)$, $\Lambda \in M_{k, n}(R)$ eine Relationenmatrix on (x_1, \dots, x_n) und $\Lambda' \in M_k(R)$ eine k -reihige Untermatrix von Λ mit $\delta = \det(\Lambda')$. Sei

$$\tilde{\Lambda} = \begin{pmatrix} \alpha & 1 \\ \Lambda & \mathbf{0}_{k,1} \end{pmatrix} \in M_{k+1, n+1}(R) \quad \text{mit} \quad \alpha = (-\alpha_1, \dots, -\alpha_n).$$

Dann ist $\tilde{\Lambda}$ eine Relationenmatrix von (x_1, \dots, x_{n+1}) und hat eine $(k+1)$ -reihige Untermatrix der Form

$$\tilde{\Lambda}' = \begin{pmatrix} \alpha' & 1 \\ \Lambda' & \mathbf{0}_{k,1} \end{pmatrix} \quad \text{mit einem } k\text{-gliedrigen Teilvektor } \alpha' \text{ von } \alpha.$$

Daher ist $\delta = \det(\Lambda') = \pm \det(\tilde{\Lambda}') \in {}_R\langle \mathcal{F}_{k+1}(x_1, \dots, x_{n+1}) \rangle$.

2) $\mathcal{F}_{k+1}(x_1, \dots, x_{n+1}) \subset {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$: Sei $\delta \in \mathcal{F}_{k+1}(x_1, \dots, x_{n+1})$ eine $(k+1)$ -reihige Unterdeterminante der Relationenmatrix $\Lambda = (\lambda_{\mu, \nu})_{\mu \in [1, k+1], \nu \in [1, n+1]} \in M_{k+1, n+1}(R)$ von (x_1, \dots, x_{n+1}) . Für $\nu \in [1, n+1]$ sei $\Lambda_\nu = (\lambda_{1, \nu}, \dots, \lambda_{k+1, \nu})^t$ die ν -te Spalte von Λ . Dann ist

$$0 = \sum_{\nu=1}^{n+1} \Lambda_\nu x_\nu = \sum_{\nu=1}^n \Lambda_\nu x_\nu + \Lambda_{n+1} \sum_{\nu=1}^n \alpha_\nu x_\nu = \sum_{\nu=1}^n (\Lambda_\nu + \alpha_\nu \Lambda_{n+1}) x_\nu,$$

und daher ist $(\Lambda_1 + \alpha_1 \Lambda_{n+1}, \dots, \Lambda_n + \alpha_n \Lambda_{n+1}) \in M_{k+1, n}(R)$ eine Relationenmatrix von (x_1, \dots, x_n) .

Wir zeigen nun zunächst:

[*] Für alle $1 \leq i_1 < \dots < i_k \leq n$ ist $\det(\Lambda_{i_1}, \dots, \Lambda_{i_k}, \Lambda_{n+1}) \in {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$.

Durch elementare Spaltenumformungen und Entwicklung nach der letzten Spalte folgt

$$D = \det(\Lambda_{i_1}, \dots, \Lambda_{i_k}, \Lambda_{n+1}) = \det(\Lambda_{i_1} + \alpha_{i_1} \Lambda_{n+1}, \dots, \Lambda_{i_k} + \alpha_{i_k} \Lambda_{n+1}, \Lambda_{n+1}) = \sum_{\rho=1}^{k+1} \lambda_{\rho, n+1} \delta_\rho.$$

Dabei sind $\pm \delta_\rho$ k -reihige Unterdeterminanten der Matrix $(\Lambda_1 + \alpha_1 \Lambda_{n+1}, \dots, \Lambda_n + \alpha_n \Lambda_{n+1})$, also $\pm \delta_\rho \in \mathcal{F}_k(x_1, \dots, x_n)$, und es folgt $D \in \mathcal{F}_k(x_1, \dots, x_n)$, also **[*]**.

Seien nun $1 \leq \nu_1 < \dots < \nu_{k+1} \leq n+1$ mit $\delta = \det(\Lambda_{\nu_1}, \dots, \Lambda_{\nu_{k+1}})$.

FALL 1: $\nu_{k+1} = n+1$. Dann ist $\delta \in {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$ nach **[*]**.

FALL 2: $\nu_{k+1} < n+1$. Dann ist $k < n$ und

$$\Delta = \det(\Lambda_{\nu_1} + \alpha_{\nu_1} \Lambda_{n+1}, \dots, \Lambda_{\nu_{k+1}} + \alpha_{\nu_{k+1}} \Lambda_{n+1}) \in \mathcal{F}_{k+1}(x_1, \dots, x_n) \subset {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle.$$

Nach Lemma 2.4.5 ist

$$\Delta = \det(\Lambda_{\nu_1}, \dots, \Lambda_{\nu_{k+1}}) + \sum_{i=1}^{k+1} \alpha_{\nu_i} \det(\Lambda_{\nu_1}, \dots, \Lambda_{\nu_{i-1}}, \Lambda_{n+1}, \Lambda_{\nu_{i+1}}, \dots, \Lambda_{\nu_{k+1}}) = \delta + \sum_{i=1}^{k+1} \alpha_{\nu_i} \delta_i,$$

und nach **[*]** ist $\delta_i \in {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$ für alle $i \in [1, k+1]$. Daher folgt $\delta \in {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle$. \square

Satz 2.4.8. Sei R kommutativ, $n \in \mathbb{N}$, $M = Rx_1 + \dots + Rx_n$ (dir) ein R -Modul mit $x_1, \dots, x_n \in M$ und $d_1, \dots, d_n \in R$, so dass $d_1 R \supset d_2 R \supset \dots \supset d_n R$ und $\text{Ann}_R(x_i) = d_i R$ für alle $i \in [1, n]$. Für alle $j \in \mathbb{N}_0$ ist dann

$$F_j(M) = d_1 \dots d_{n-j} R, \quad \text{falls } j < n, \quad \text{und} \quad F_j(M) = R, \quad \text{falls } j \geq n.$$

BEWEIS. Nach Definition ist $F_j(M) = R$ für alle $j \geq n$. Sei also $j \in [0, n-1]$, $k = n-j$, $\delta \in \mathcal{F}_k(x_1, \dots, x_n)$, $\Lambda = (\lambda_{\mu, \nu})_{\mu \in [1, m], \nu \in [1, n]} \in M_{m, n}(R)$ eine Relationenmatrix von (x_1, \dots, x_n) und $\delta = \det(\Lambda')$ mit einer k -reihigen Untermatrix Λ' von Λ . Für alle $\mu \in [1, m]$ ist $\lambda_{\mu, 1}x_1 + \dots + \lambda_{\mu, n}x_n = 0$, und daher ist $\lambda_{\mu, i}x_i = 0$, also $\lambda_{\mu, i} \in d_i R$ für alle $i \in [1, n]$. Damit folgt $\delta \in d_{\nu_1} \cdot \dots \cdot d_{\nu_k} R$ mit Indizes $1 \leq \nu_1 < \dots < \nu_k \leq n$, und daher $\delta \in d_1 \cdot \dots \cdot d_k R$. Nun ist aber auch die Diagonalmatrix $\text{diag}(d_1, \dots, d_n)$ eine Relationenmatrix von (x_1, \dots, x_n) , also $d_1 \cdot \dots \cdot d_k \in \mathcal{F}_k(x_1, \dots, x_n)$, und daher folgt $F_j(M) = {}_R\langle \mathcal{F}_k(x_1, \dots, x_n) \rangle = d_1 \cdot \dots \cdot d_k R$. \square

2.5. Noethersche Moduln und Ringe

Definition und Satz 2.5.1. Für einen R -Modul M sind die folgenden Aussagen äquivalent:

- (a) Jede nicht-leere Menge von R -Untermoduln von M hat ein maximales Element.
- (b) Jede aufsteigende Folge von R -Untermoduln von M wird stationär [d. h., für jede Folge $(M_i)_{i \geq 0}$ von R -Untermoduln von M mit $M_0 \subset M_1 \subset M_2 \subset \dots$ gibt es ein $m \in \mathbb{N}$, so dass $M_n = M_m$ für alle $n \geq m$].
- (c) Jeder R -Untermodul von M ist endlich erzeugt.

Erfüllt M obige Bedingungen, so heißt M *noethersch*. Der Ring R heißt *linksnoethersch*, wenn ${}_R R$ ein noetherscher R -Modul ist [äquivalent: Jedes Linksideal von R ist endlich erzeugt]. R heißt *rechtsnoethersch*, wenn R^{op} linksnoethersch ist [äquivalent: Jedes Rechtsideal von R ist endlich erzeugt]. R heißt *noethersch*, wenn R links- und rechtsnoethersch ist.

BEWEIS. (a) \Rightarrow (b) Offensichtlich.

(b) \Rightarrow (c) Durch Widerspruch. Sei $N \subset M$ ein nicht endlich erzeugter Untermodul und $\mathbb{P}_f(N)$ die Menge der endlichen Teilmengen von N . Für jede endliche Teilmenge $E \subset N$ ist dann ${}_R\langle E \rangle \subsetneq N$, und nach Satz 1.1.10 gibt es eine Funktion Φ mit $\mathcal{D}(\Phi) = \mathbb{P}_f(N)$ und $\Phi(E) \in N \setminus {}_R\langle E \rangle$. Sei die Folge $(a_n)_{n \geq 0}$ in N rekursiv definiert durch $a_0 = \Phi(\emptyset)$ und $a_{n+1} = \Phi(\{a_0, \dots, a_n\})$ für alle $n \geq 0$. Dann ist $({}_R\langle a_0, \dots, a_n \rangle)_{n \geq 0}$ eine nicht abbrechende aufsteigende Folge von R -Untermoduln von M .

(c) \Rightarrow (a) Sei Ω eine nicht-leere Menge von R -Untermoduln von M . Nach Satz 1.2.13 genügt es, zu zeigen: Jede Kette in Ω hat eine obere Schranke. Sei $\mathcal{S} \subset \Omega$ eine Kette und $L = \bigcup \mathcal{S}$. Dann ist $L \subset M$ ein R -Untermodul, und wir zeigen $L \in \Omega$. Nach (c) ist $L = {}_R\langle E \rangle$ mit einer endlichen Menge E , und da \mathcal{S} eine Kette ist, gibt es ein $N \in \mathcal{S}$ mit $E \subset N$. Dann ist aber $N \subset L = {}_R\langle E \rangle \subset N$ und daher $L = N \in \mathcal{S} \subset \Omega$. \square

Satz 2.5.2. Sei M ein R -Modul.

1. Sei $M \rightarrow M'$ ein R -Modulepimorphismus und M noethersch. Dann ist auch M' noethersch.
2. Sei $N \subset M$ ein R -Untermodul. Genau dann ist M noethersch, wenn N und M/N beide noethersch sind. Allgemeiner gilt: Ist $\mathbf{0} \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow \mathbf{0}$ eine kurze exakte Sequenz von R -Moduln, so ist M genau dann noethersch, wenn M' und M'' beide noethersch sind.
3. Ist $n \in \mathbb{N}$ und $M = M_1 \oplus \dots \oplus M_n$ mit R -Moduln M_1, \dots, M_n , so ist M genau dann noethersch, wenn alle M_i noethersch sind.

BEWEIS. 1. Sei $(N'_i)_{i \geq 0}$ eine aufsteigende Folge von R -Untermoduln von M' . Dann ist $(f^{-1}(N'_i))_{i \geq 0}$ eine aufsteigende Folge von R -Untermoduln von M , und es gibt ein $m \in \mathbb{N}$, so dass $f^{-1}(N'_i) = f^{-1}(N'_m)$ für alle $i \geq m$. Damit folgt $N'_i = f(f^{-1}(N'_i)) = f(f^{-1}(N'_m)) = N'_m$ für alle $i \geq m$.

2. Ist M noethersch, so ist N noethersch nach Definition und M/N noethersch nach 1. Seien also N und M/N beide noethersch, und sei $(M_i)_{i \geq 0}$ eine aufsteigende Folge von R -Untermoduln von M . Dann ist $(M_i \cap N)_{i \geq 0}$ eine aufsteigende Folge von R -Untermoduln von N und $((M_i + N)/N)_{i \geq 0}$ eine aufsteigende Folge von R -Untermoduln von M/N . Daher gibt es ein $m \in \mathbb{N}$, so dass $M_i \cap N = M_m \cap N$ und $(M_i + N)/N = (M_m + N)/N$ für alle $i \geq m$. Wir zeigen $M_i \subset M_m$ (also $M_i = M_m$) für alle

$i \geq m$. Sei $i \geq m$ und $x \in M_i$. Dann ist $x + N \in (M_i + N)/N = (M_m + N)/N$, und daher gibt es ein $y \in M_m$ mit $x - y \in N$. Dann ist aber $x - y \in M_i \cap N = M_m \cap N$ und daher $x = (x - y) + y \in M_m$.

3. Es genügt, die Behauptung für $n = 2$ zu beweisen (dann folgt der allgemeine Fall durch Induktion). Sei $\pi: M \rightarrow M_2$ die Projektion auf den zweiten Faktor. Dann ist $\text{Ker}(\pi) \cong M_1$ und $M_2 \cong M/\text{Ker}(\pi)$. Nach 2. ist M genau dann noethersch, wenn $\text{Ker}(\pi)$ und $M/\text{Ker}(\pi)$ noethersch sind, wenn also M_1 und M_2 beide noethersch sind. \square

Satz 2.5.3. *Sei R linksnoethersch.*

1. *Jeder endlich erzeugte R -Modul ist noethersch.*
2. *Ist $R \rightarrow S$ ein Ringepimorphismus, so ist auch S linksnoethersch.*

BEWEIS. 1. Sei M ein endlich erzeugter R -Modul. Nach Satz 2.2.7 gibt es ein $n \in \mathbb{N}$ und einen R -Epimorphismus $f: R^n \rightarrow M$. Nach Satz 2.5.2.3 ist R^n noethersch, und nach Satz 2.5.2.1 ist dann auch M noethersch.

2. Sei $f: R \rightarrow S$ ein Ringepimorphismus und $L \subset S$ ein Linksideal. Dann ist $f^{-1}(L) \subset R$ ein Linksideal, also endlich erzeugt, und $f|_{f^{-1}(L)}: f^{-1}(L) \rightarrow L$ ist ein R -Modulepimorphismus. Daher ist L ein endlich erzeugter R -Modul, und jedes R -Erzeugendensystem von L ist ein S -Erzeugendensystem. \square

Satz 2.5.4 (Hilbert'scher Basissatz). *Sei R kommutativ und noethersch. Dann ist für jedes $n \in \mathbb{N}$ auch der Polynomring $R[X_1, \dots, X_n]$ noethersch.*

BEWEIS. Es genügt, den Fall $n = 1$, also den Polynomring $R[X]$, zu betrachten. Wir notieren Polynome $f \in R[X]$ in der Form

$$f = \sum_{n \geq 0} f_n X^n \quad \text{mit} \quad f_n \in R, \quad f_n = 0 \quad \text{für fast alle} \quad n \geq 0.$$

Sei $\mathbf{0} \neq \mathfrak{a} \triangleleft R[X]$. Für $n \in \mathbb{N}_0$ sei $\mathfrak{a}_n = \{f_n \mid f \in \mathfrak{a}, \text{gr}(f) \leq n\}$. Für $f, g \in \mathfrak{a}$ und $\lambda \in R$ ist $f + g \in \mathfrak{a}$, $\lambda f \in \mathfrak{a}$ und $Xf \in \mathfrak{a}$. Für $n \in \mathbb{N}_0$ ist $(f + g)_n = f_n + g_n$, $(\lambda f)_n = \lambda f_n$, und $(Xf)_{n+1} = f_n$. Daher ist $(\mathfrak{a}_n)_{n \geq 0}$ eine aufsteigende Folge von Idealen von R , und es gibt ein $m \in \mathbb{N}$ mit $\mathfrak{a}_n = \mathfrak{a}_m$ für alle $n \geq m$.

Für $j \in [0, m]$ sei $\mathfrak{a}_j = R\langle (f_{j,1})_j, \dots, (f_{j,k_j})_j \rangle$ mit Polynomen $f_{j,i} \in \mathfrak{a}$. Wir zeigen

$$\mathfrak{a} = \mathfrak{a}' \quad \text{mit} \quad \mathfrak{a}' = R[X]\langle \{f_{j,\nu} \mid j \in [0, m], \nu \in [1, k_j]\} \rangle.$$

Offensichtlich ist $\mathfrak{a} \supset \mathfrak{a}'$. Angenommen, es sei $\mathfrak{a} \supsetneq \mathfrak{a}'$, und es sei $f \in \mathfrak{a} \setminus \mathfrak{a}'$ ein Polynom minimalen Grades $j = \text{gr}(f) \in \mathbb{N}_0$.

FALL 1: $j \leq m$. Dann ist $f_j \in \mathfrak{a}_j$ und daher

$$f_j = \sum_{\nu=1}^{k_j} \lambda_\nu (f_{j,\nu})_j \quad \text{mit} \quad \lambda_\nu \in R, \quad f^* = f - \sum_{\nu=1}^{k_j} \lambda_\nu f_{j,\nu} \in \mathfrak{a} \quad \text{und} \quad (f^*)_j = 0, \quad \text{also} \quad \text{gr}(f^*) < j.$$

Daher ist $f^* \in \mathfrak{a}'$, und es folgt $f \in \mathfrak{a}'$, ein Widerspruch.

FALL 2: $j > m$. Dann ist $f_j \in \mathfrak{a}_j = \mathfrak{a}_m$ und daher

$$f_j = \sum_{\nu=1}^{k_m} \lambda_\nu (f_{m,\nu})_m \quad \text{mit} \quad \lambda_\nu \in R, \quad f^* = f - \sum_{\nu=1}^{k_m} \lambda_\nu X^{j-m} f_{m,\nu} \in \mathfrak{a} \quad \text{und} \quad (f^*)_j = 0, \quad \text{also} \quad \text{gr}(f^*) < j.$$

Daher ist $f^* \in \mathfrak{a}'$, und es folgt $f \in \mathfrak{a}'$, ein Widerspruch. \square

2.6. Moduln über Hauptidealbereichen

Satz 2.6.1. *Sei R ein Hauptidealbereich, M ein R -freier R -Modul mit Basis B und $N \subset M$ ein R -Untermodul. Dann ist N R -frei mit einer Basis B' , so dass $|B'| \leq |B|$.*

BEWEIS. Sei Ω die Menge aller Tripel (E, E', φ) , bestehend aus Teilmengen $E' \subset E \subset B$ und einer Abbildung $\varphi: E' \rightarrow N \cap_R \langle E \rangle$, so dass $\varphi(E')$ eine R -Basis von $N \cap_R \langle E \rangle$ ist. Wegen $(\emptyset, \emptyset, \emptyset) \in \Omega$ ist $\Omega \neq \emptyset$. Für $(E, E', \varphi), (F, F', \psi) \in \Omega$ definieren wir

$$(E, E', \varphi) \leq (F, F', \psi) \iff E \subset F, E' \subset F' \text{ und } \psi|_{E'} = \varphi.$$

Wir zeigen:

A. Ω besitzt ein maximales Element.

B. Ist (E, E', φ) ein maximales Element von Ω , so ist $E = B$.

Sind **A** und **B** gezeigt und ist (B, E', φ) ein maximales Element von Ω , so ist $B' = \varphi(E')$ eine R -Basis von $N \cap_R \langle B \rangle = N$, und $|B'| \leq |E'| \leq |B|$.

Beweis von A. Offensichtlich ist (Ω, \leq) eine teilgeordnete Menge. Nach dem Zorn'schen Lemma genügt es, zu zeigen: Jede Kette in Ω besitzt eine obere Schranke. Sei $\mathcal{S} = \{(E_\lambda, E'_\lambda, \varphi_\lambda \mid \lambda \in \Lambda\}$ eine Kette in Ω , $E = \bigcup \{E_\lambda \mid \lambda \in \Lambda\}$, $E' = \bigcup \{E'_\lambda \mid \lambda \in \Lambda\}$ und $\varphi = \bigcup \{\varphi_\lambda \mid \lambda \in \Lambda\}$. Wir zeigen $(E, E', \varphi) \in \Omega$ (dann ist (E, E', φ) eine obere Schranke von \mathcal{S}). Nach Konstruktion ist $E' \subset E \subset B$ und $\varphi: E' \rightarrow \bigcup \{N \cap_R \langle E_\lambda \rangle \mid \lambda \in \Lambda\} \subset N \cap_R \langle \bigcup \{E_\lambda \mid \lambda \in \Lambda\} \rangle = N \cap_R \langle E \rangle$ ist eine Abbildung. Daher genügt es, zu zeigen, dass $\varphi(E')$ eine R -Basis von $N \cap_R \langle E \rangle$ ist. $\{\varphi(E'_\lambda) \mid \lambda \in \Lambda\}$ ist eine Kette linear unabhängiger Mengen, und daher ist auch $\varphi(E') = \bigcup \{\varphi(E'_\lambda) \mid \lambda \in \Lambda\} \subset N \cap_R \langle E \rangle$ linear unabhängig. Ist $x \in N \cap_R \langle E \rangle$, so gibt es ein $\lambda \in \Lambda$ mit $x \in N \cap_R \langle E_\lambda \rangle = {}_R \langle \varphi(E'_\lambda) \rangle \subset {}_R \langle \varphi(E') \rangle$, und daher ist $\varphi(E')$ auch ein R -Erzeugendensystem von $N \cap_R \langle \varphi(E') \rangle$.

Beweis von B. Angenommen, es sei (E, E', φ) ein maximales Element von Ω , $E \subsetneq B$ und $b \in B \setminus E$. Sei $I = \{\lambda \in R \mid (\exists y \in {}_R \langle E \rangle) y + \lambda b \in N\} = \text{Ann}_R(\bar{b}) \triangleleft R$ mit $\bar{b} = b + (N + {}_R \langle E \rangle) \in M/(N + {}_R \langle E \rangle)$. FALL 1: $I = \mathbf{0}$. Ist dann $x \in {}_R \langle E \cup \{b\} \rangle \cap N = ({}_R \langle E \rangle + Rb) \cap N$, so ist $x = y + \lambda b$ mit $y \in {}_R \langle E \rangle$ und $\lambda \in R$, also $\lambda b \in N + {}_R \langle E \rangle$. Daher ist $\lambda = 0$ und $x \in {}_R \langle E \rangle$, und es folgt $N \cap_R \langle E \cup \{b\} \rangle = N \cap_R \langle E \rangle$, also $(E \cup \{b\}, E', \varphi) \in \Omega$, ein Widerspruch zur Maximalität von (E, E', φ) .

FALL 2: $I \neq \mathbf{0}$, $I = \alpha R$ mit $\alpha \in R^\bullet$. Sei $y_0 \in {}_R \langle E \rangle$ mit $y_0 + \alpha b \in N$, $\bar{E} = E \cup \{b\}$, $\bar{E}' = E' \cup \{b\}$, und sei $\bar{\varphi}: \bar{E}' \rightarrow N \cap_R \langle \bar{E} \rangle$ definiert durch $\bar{\varphi}|_E = \varphi$ und $\bar{\varphi}(b) = y_0 + \alpha b \in {}_R \langle E \rangle + Rb = {}_R \langle \bar{E} \rangle$. Dann ist $\bar{E}' \subset \bar{E} \subset B$, und wir zeigen $(\bar{E}, \bar{E}', \bar{\varphi}) \in \Omega$, was wieder der Maximalität von (E, E', φ) widerspricht. Dazu müssen wir zeigen, dass $\bar{\varphi}(\bar{E}') = \varphi(E') \cup \{y_0 + \alpha b\}$ eine R -Basis von $N \cap ({}_R \langle E \rangle + Rb)$ ist.

1) $\varphi(E') \cup \{y_0 + \alpha b\}$ ist linear unabhängig: Sei

$$\sum_{e \in E'} \lambda_e \varphi(e) + \lambda(y_0 + \alpha b) = 0 \quad \text{mit } \lambda, \lambda_e \in R, \lambda_e = 0 \text{ für fast alle } e \in E'.$$

Dann ist $\lambda(y_0 + \alpha b) \in {}_R \langle \varphi(E') \rangle \subset {}_R \langle E \rangle$, und wegen $y_0 \in {}_R \langle E \rangle$ folgt $\lambda \alpha b \in {}_R \langle E \rangle$. Da $E \cup \{b\}$ linear unabhängig ist, folgt $\lambda \alpha = 0$, also $\lambda = 0$, und da $\varphi(E')$ linear unabhängig ist, folgt $\lambda_e = 0$ für alle $e \in E'$.

2) $\varphi(E') \cup \{y_0 + \alpha b\}$ ist ein R -Erzeugendensystem von $N \cap ({}_R \langle E \rangle + Rb)$. Sei $z \in N \cap ({}_R \langle E \rangle + Rb)$. Dann ist $z = y + \lambda b$ mit $y \in {}_R \langle E \rangle$ und $\lambda \in R$, also $\lambda \in I$ und daher $\lambda = \alpha \beta$ mit $\beta \in R$. Nun folgt $z - \beta(y_0 + \alpha b) = y - \beta y_0 \in N \cap {}_R \langle E \rangle = {}_R \langle \varphi(E') \rangle$ und daher $z \in {}_R \langle \varphi(E') \cup \{y_0 + \alpha b\} \rangle$. \square

Korollar 2.6.2. $\mathbb{Z}^{\mathbb{N}}$ ist nicht \mathbb{Z} -frei.

BEWEIS. Angenommen, es sei B eine \mathbb{Z} -Basis von $\mathbb{Z}^{\mathbb{N}}$. Dann ist $|\mathbb{Z}^{\mathbb{N}}| = \max\{|B|, \omega\} \geq 2^\omega > \omega$ und daher $|B| > \omega$. Sei $p \in \mathbb{P}$. Für $x \in \mathbb{Z}$ sei $v_p(x) = \sup\{i \in \mathbb{N}_0 \mid p^i \mid x\} \in \mathbb{N}_0 \cup \{\infty\}$, und

$$x' = \begin{cases} x, & \text{falls } p \nmid x, \\ p^{-1}x, & \text{falls } p \mid x. \end{cases}$$

Dann ist

$$S = \{(x_i)_{i \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \mid \lim_{i \rightarrow \infty} v_p(x_i) = \infty\} \subset \mathbb{Z}^{\mathbb{N}} \quad \text{ein } \mathbb{Z}\text{-Untermodul und daher frei mit einer Basis } (u_i)_{i \in I}.$$

Die Abbildung $\varphi: \mathbb{Z}^{\mathbb{N}} \rightarrow S$, definiert durch $\varphi((x_i)_{i \in \mathbb{N}}) = (p^i x_i)_{i \in \mathbb{N}}$, ist ein Monomorphismus. Daher ist $\mathbb{Z}^{\mathbb{N}} \cong \varphi(\mathbb{Z}^{\mathbb{N}})$, $\varphi(\mathbb{Z}^{\mathbb{N}}) \subset S$ ist ein Untermodul, $\varphi(\mathbb{Z}^{\mathbb{N}})$ ist frei mit Basis $\varphi(B)$, und $\omega < |B| = |\varphi(B)| \leq |I|$. Nach Satz 2.3.6 ist S/pS ein $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ -Vektorraum mit Basis $(u_i + pS)_{i \in I}$. Ist $\mathbf{x} = (x_i)_{i \in \mathbb{N}} \in S$, so ist auch $\mathbf{x}' = (x'_i)_{i \in \mathbb{N}} \in S$, und

$$\mathbf{x} = p\mathbf{x}' + \sum_{\substack{i \in \mathbb{N} \\ p \nmid x_i}} (1-p)x_i \mathbf{e}_i \in pS + \mathbb{Z}\langle \{\mathbf{e}_i \mid i \in \mathbb{N}\} \rangle.$$

Damit folgt $S/pS = \mathbb{F}_p\langle \{\mathbf{e}_i + pS \mid i \in \mathbb{N}\} \rangle$, also $|\{\mathbf{e}_i + pS \mid i \in \mathbb{N}\}| \geq |I| > \omega$ nach Satz 2.3.6, ein Widerspruch. \square

Bemerkung und Definition 2.6.3. Sei R ein Bereich und M ein R -Modul. Dann ist

$$M_{\text{tor}} = \{x \in M \mid \text{Ann}_R(x) \neq \mathbf{0}\} \subset M$$

ein R -Untermodul. [Beweis: Seien $x, y \in M_{\text{tor}}$ und $a, b \in R^\bullet$ mit $ax = by = 0$. Dann ist $ab \in R^\bullet$ und $ab(x+y) = 0$, also $x+y \in M_{\text{tor}}$. Ist $\lambda \in R$, so ist auch $a(\lambda x) = 0$ und daher $\lambda x \in M_{\text{tor}}$].

M_{tor} heißt *Torsionsuntermodul*. M heißt *R -torsionsfrei*, wenn $M_{\text{tor}} = \mathbf{0}$, und ein *R -Torsionsmodul*, wenn $M_{\text{tor}} = M$.

Ist M ein endlich erzeugter R -Torsionsmodul, so ist $\text{Ann}_R(M) \neq \mathbf{0}$ [denn: Ist $M = {}_R\langle x_1, \dots, x_n \rangle$ und $0 \neq a_i \in \text{Ann}_R(x_i)$, so folgt $a_1 \cdot \dots \cdot a_n \in \text{Ann}(M)$].

Jeder R -freie Modul ist R -torsionsfrei. Im Falle $R = \mathbb{Z}$ stimmen obige Begriffe mit den üblichen gruppentheoretischen Begriffen überein.

Im \mathbb{Z} -Modul \mathbb{Q} sind je zwei Elemente linear abhängig über \mathbb{Z} [denn: Seien $a, b \in \mathbb{Q}^\times$ und $m \in \mathbb{N}$ mit $ma, mb \in \mathbb{Z}$. Dann ist $(mb)a + (-ma)b = 0$]. Insbesondere: \mathbb{Q} ist als \mathbb{Z} -Modul zwar torsionsfrei, aber nicht frei.

Definitionen und Bemerkungen 2.6.4. Sei R ein Bereich und $K = \mathfrak{q}(R)$ sein Quotientenkörper.

1. Teilbarkeitslehre in R : Für $a, b \in R$ definiert man (wie üblich)

$$a \mid b \quad (a \text{ teilt } b) \iff bR \subset aR \quad \text{und} \quad a \simeq b \quad (a \text{ und } b \text{ sind assoziiert}) \iff aR = bR.$$

$p \in R^\bullet$ heißt *Primelement*, wenn $pR \in \text{spec}(R)$ [äquivalent: $p \notin R^\times$, und für alle $a, b \in R$ gilt: $p \mid ab \implies p \mid a \vee p \mid b$].

Eindeutigkeit der Primzerlegung: Sind $m, n \in \mathbb{N}_0$ und $p_1, \dots, p_n, p'_1, \dots, p'_m \in R^\bullet$ Primelemente mit $p_1 \cdot \dots \cdot p_n \simeq p'_1 \cdot \dots \cdot p'_m$, so folgt $m = n$, und es gibt eine Permutation $\sigma \in \mathfrak{S}_n$, so dass $p'_{\sigma(i)} \simeq p_i$ für alle $i \in [1, n]$.

Größter gemeinsamer Teiler: Seien $n \in \mathbb{N}$ und $x_1, \dots, x_n \in R$. Ein Element $d \in R$ heißt ggT von x_1, \dots, x_n , wenn dR das kleinste $\{x_1, \dots, x_n\}$ umfassende Hauptideal ist. Besitzen x_1, \dots, x_n einen ggT, so ist dieser bis auf Assoziierte eindeutig bestimmt. x_1, \dots, x_n heißen *teilerfremd*, wenn 1 ein ggT von x_1, \dots, x_n ist.

2. Faktorielle Bereiche: R heißt *faktoriell*, wenn jedes $a \in R^\bullet \setminus R^\times$ Produkt von Primelementen ist. Beispiele: \mathbb{Z} ; jeder Körper; R faktoriell $\implies R[X_1, \dots, X_n]$ faktoriell.

Sei R faktoriell und \mathcal{P} ein *Repräsentantensystem der Primelemente* von R [das heißt, \mathcal{P} ist eine Menge von Primelementen, so dass es zu jedem Primelement $p \in R$ genau ein $p_0 \in \mathcal{P}$ gibt mit $p \simeq p_0$]. Jedes $a \in K^\times$ hat eine eindeutige Darstellung

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{mit} \quad u \in R^\times \quad \text{und} \quad v_p(a) \in \mathbb{Z}, \quad v_p(a) = 0 \quad \text{für fast alle } p \in \mathcal{P};$$

$v_p(a)$ hängt nur von a und pR ab, heißt *p-adischer Wert* von a , und wir setzen $v_p(0) = \infty$. Die Abbildung $v_p: K^\times \rightarrow \mathbb{Z}$ ist ein Gruppenepimorphismus, und obige Produktdarstellung definiert einen Isomorphismus

$$K^\times \xrightarrow{\sim} R^\times \times \mathbb{Z}^{(\mathcal{P})}, \quad a \mapsto (u, (v_p(a))_{p \in \mathcal{P}}), \quad \text{und} \quad R = \{a \in K \mid (\forall p \in \mathcal{P}) v_p(a) \geq 0\}.$$

Für $a, b \in R$ ist genau dann $a \mid b$, wenn $v_p(a) \leq v_p(b)$ für alle $p \in \mathcal{P}$. Sind $a_1, \dots, a_n \in R$, so ist ein Element $d \in R$ genau dann ein ggT von a_1, \dots, a_n , wenn $v_p(d) = \min\{v_p(a_1), \dots, v_p(a_n)\}$ (insbesondere besitzen a_1, \dots, a_n einen ggT in R). Genau dann sind a_1, \dots, a_n teilerfremd, wenn es kein $p \in \mathcal{P}$ gibt, so dass $p \mid a_i$ für alle $i \in [1, n]$.

3. Hauptidealbereiche: Sei R ein Hauptidealbereich. Dann ist R noethersch und faktoriell, und es sei \mathcal{P} ein Repräsentantensystem der Primelemente von R . Dann ist $\max(R) = \{pR \mid p \in \mathcal{P}\}$. Für $a_1, \dots, a_n, d \in R$ ist d genau dann ein ggT von a_1, \dots, a_n , wenn ${}_R\langle a_1, \dots, a_n \rangle = dR$. Insbesondere sind a_1, \dots, a_n genau dann teilerfremd, wenn es $x_1, \dots, x_n \in R$ gibt mit $a_1x_1 + \dots + a_nx_n = 1$.

Seien $p_1, \dots, p_n \in \mathcal{P}$ verschieden, $k_1, \dots, k_n \in \mathbb{N}$ und $q_i = p_i^{k_i}$ für alle $i \in [1, n]$. Dann sind q_1, \dots, q_n paarweise teilerfremd, und nach dem Chinesischen Restsatz gibt es einen Ringepimorphismus

$$\Phi: R \rightarrow \prod_{i=1}^n R/q_iR \quad \text{mit} \quad \Phi(x) = (x + q_1R, \dots, x + q_nR), \quad \text{und} \quad \text{Ker}(\Phi) = \bigcap_{i=1}^n q_iR = \prod_{i=1}^n q_iR.$$

Sei M ein R -Modul und $p \in \mathcal{P}$. Dann ist $M(p) = \{x \in M \mid (\exists r \in \mathbb{N}) p^r x = 0\} \subset M$ ein (nur von pR abhängiger) R -Unterm modul und heißt *p-Komponente* von M , und M heißt *p-primär*, wenn $M = M(p)$. Ist $x \in M(p)$, so nennt man $\text{ord}_p(x) = \min\{r \in \mathbb{N}_0 \mid p^r x = 0\}$ die (*p*-)Ordnung oder (*p*-)Periode von x .

Satz 2.6.5. *Sei R ein Hauptidealbereich, \mathcal{P} ein Repräsentantensystem der Primelemente von R und M ein R -Torsionsmodul. Dann ist*

$$M = \sum_{p \in \mathcal{P}} M(p) \quad (\text{dir}).$$

Ist M endlich erzeugt, so ist $M(p) = \mathbf{0}$ für fast alle $p \in \mathcal{P}$.

BEWEIS. Sei $x \in M$, $\text{Ann}_R(x) = aR$ und $a = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$ mit $r \in \mathbb{N}_0$, verschiedenen $p_1, \dots, p_r \in \mathcal{P}$ und $k_1, \dots, k_r \in \mathbb{N}$. Für $i \in [1, r]$ sei $q_i = p_i^{-k_i} a \in R$. Dann sind q_1, \dots, q_r teilerfremd, und daher gibt es $\alpha_1, \dots, \alpha_r \in R$ mit $1 = q_1\alpha_1 + \dots + q_r\alpha_r$. Es folgt $x = q_1\alpha_1x + \dots + q_r\alpha_rx$, und für alle $i \in [1, r]$ ist $p_i^{k_i} q_i \alpha_i x = a \alpha_i x = 0$, also $q_i \alpha_i x \in M(p_i)$.

Daher ist M die Summe der Familie $(M(p))_{p \in \mathcal{P}}$. Für den Nachweis der Direktheit der Summe zeigen wir:

$$\text{Ist } p \in \mathcal{P} \text{ und } x \in M(p) \cap \sum_{p' \in \mathcal{P} \setminus \{p\}} M(p'), \text{ so folgt } x = 0.$$

Sei also $p \in \mathcal{P}$, seien $p_1, \dots, p_n \in \mathcal{P} \setminus \{p\}$, und sei $x = x_1 + \dots + x_n \in M(p)$ mit $x_i \in M(p_i)$ für alle $i \in [1, n]$. Seien $r, r_1, \dots, r_n \in \mathbb{N}$ mit $p^r x = 0$ und $p_i^{r_i} x_i = 0$ für alle $i \in [1, n]$. Da p^r und $p_1^{r_1} \cdot \dots \cdot p_n^{r_n}$ teilerfremd sind, gibt es $\alpha, \beta \in R$ mit $\alpha p^r + \beta p_1^{r_1} \cdot \dots \cdot p_n^{r_n} = 1$, und es folgt $x = \alpha p^r x + \beta p_1^{r_1} \cdot \dots \cdot p_n^{r_n} x = 0$.

Sei nun $\mathcal{P}_0 = \{p \in \mathcal{P} \mid M(p) \neq \mathbf{0}\}$ unendlich und E ein Erzeugendensystem von M . Nach Satz 2.3.6.1 ist dann $|E| \geq |\mathcal{P}_0|$. Ist insbesondere M endlich erzeugt, so ist \mathcal{P}_0 endlich. \square

Satz 2.6.6 (Struktursatz für Moduln über Hauptidealbereichen). *Sei R ein Hauptidealbereich.*

1. *Sei F ein endlich erzeugter freier R -Modul und $M \subset F$ ein R -Unterm modul. Dann gibt es eine R -Basis (u_1, \dots, u_n) von F , ein $m \in [0, n]$ und $d_1, \dots, d_m \in R^\bullet$ mit $d_1R \supset d_2R \supset \dots \supset d_mR$, so dass (d_1u_1, \dots, d_mu_m) eine R -Basis von M ist. Dabei sind die Ideale d_1R, \dots, d_mR eindeutig bestimmt.*

2. Sei M ein endlich erzeugter R -Torsionsmodul. Dann gibt es ein $m \in \mathbb{N}_0$, $d_1, \dots, d_m \in R^\bullet$ und $x_1, \dots, x_m \in M$, so dass

- $M = Rx_1 + \dots + Rx_m$ (dir), und $\text{Ann}_R(x_i) = d_i R$ für alle $i \in [1, m]$;
- $R \supseteq d_1 R \supset d_2 R \supset \dots \supset d_m R$.

Dabei sind die Ideale $d_1 R, \dots, d_m R$ eindeutig bestimmt.

3. Sei M ein endlich erzeugter R -Modul. Dann gibt es einen R -freien R -Untermodul $U \subset M$, so dass $M = M_{\text{tor}} + U$ (dir), und $U \cong M/M_{\text{tor}}$. Insbesondere gilt: Ist M R -torsionsfrei, so ist M R -frei.

BEWEIS. *Existenzbeweis in 1.* Induktion nach n . Ist $n = 0$ oder $M = \mathbf{0}$, so ist nichts zu zeigen. Sei also $M \neq \mathbf{0}$.

$n \geq 1$, $n - 1 \rightarrow n$: Sei $F^* = \text{Hom}_R(F, R)$. Für jedes $f \in F^*$ ist $f(M) \triangleleft R$, und es seien $f_1 \in F^*$ und $d_1 \in R$, so dass $f_1(M) = d_1 R$ ein maximales Element von $\{f(M) \mid f \in F^*\}$ ist. Sei $x_1 \in M$ mit $f_1(x_1) = d_1$. Wir zeigen nun zunächst:

A. $0 \neq x_1 \in d_1 F$.

Beweis von A. Sei (e_1, \dots, e_n) eine Basis von F und (e_1^*, \dots, e_n^*) die dazu duale Basis von F^* . Ist $x \in M \setminus \mathbf{0}$, so ist $x = \lambda_1 e_1 + \dots + \lambda_n e_n$ mit $\lambda_1, \dots, \lambda_n \in R$, und es gibt ein $j \in [1, n]$ mit $\lambda_j \neq 0$. Dann ist aber $e_j^*(x) = \lambda_j \neq 0$, also $e_j^*(M) \neq \mathbf{0}$ und daher $d_1 R \neq \mathbf{0}$, also auch $x_1 \neq 0$. Sei nun $x_1 = \alpha_1 e_1 + \dots + \alpha_n e_n$. Für $\nu \in [1, n]$ sei $\alpha_\nu R + d_1 R = b_\nu R$ mit $b_\nu \in R$, und es seien $\beta_\nu, \gamma_\nu \in R$ mit $b_\nu = \alpha_\nu \beta_\nu + d_1 \gamma_\nu$. Dann ist $g_\nu = \beta_\nu e_\nu^* + \gamma_\nu f_1 \in F^*$, $g_\nu(x_1) = \beta_\nu \alpha_\nu + \gamma_\nu d_1 = b_\nu$ und daher $f_1(M) = d_1 R \subset b_\nu R \subset g_\nu(M)$. Aus der Maximalität von $f_1(M)$ folgt $\alpha_\nu \in b_\nu R = d_1 R$. Daher ist $x_1 \in d_1 F$ und **A** gezeigt.

Sei $x_1 = d_1 u_1$ mit $u_1 \in F$. Dann ist $f_1(x_1) = d_1 = d_1 f_1(u_1)$ und daher $f_1(u_1) = 1$. Wir setzen $F_1 = \text{Ker}(f_1) \subset F$ und $M_1 = M \cap F_1$. Dann gilt:

B. $F = Ru_1 + F_1$ (dir) und $M = Rd_1 u_1 + M_1$ (dir).

Beweis von B. Ist $x \in F$, so folgt $x - f_1(x)u_1 \in \text{Ker}(f_1) = F_1$ und daher $x \in Ru_1 + F_1$, also $F = Ru_1 + F_1$. Ist $x \in M$, so ist $f_1(x)u_1 \in d_1 Ru_1 = Rx_1 \subset M$, also $x - f_1(x)u_1 \in F_1 \cap M = M_1$ und daher $x \in Rd_1 u_1 + M_1$, also $M = Rd_1 u_1 + M_1$. Wegen $Rd_1 u_1 \cap M_1 \subset Ru_1 \cap F_1$ ist nun nur noch $Ru_1 \cap F_1 = \mathbf{0}$ zu zeigen. Ist $x \in Ru_1 \cap F_1$, so ist $x = \lambda u_1$ mit $\lambda \in R$ und $0 = f_1(x) = \lambda$, also $x = 0$. Damit folgt **B**.

Nach Satz 2.6.1 ist F_1 R -frei und $\text{rg}(F_1) \leq \text{rg}(F)$. Ist $m \in \mathbb{N}$ und (v_2, \dots, v_m) eine R -Basis von F_1 , so ist (u_1, v_2, \dots, v_m) eine Basis von F , also $m = n$ und F_1 R -frei vom Rang $n - 1$. Nach Induktionsvoraussetzung gibt es eine R -Basis (u_2, \dots, u_n) von F_1 , ein $m \in [1, n]$ und $d_2, \dots, d_m \in R^\bullet$ mit $d_2 R \supset \dots \supset d_m R$, so dass $(d_2 u_2, \dots, d_m u_m)$ eine R -Basis von M_1 ist. Dann ist (u_1, \dots, u_n) eine R -Basis von F , $(d_1 u_1, \dots, d_m u_m)$ eine R -Basis von M , und es bleibt $d_1 R \supset d_2 R$ zu zeigen.

Sei ${}_R \langle d_1, d_2 \rangle = dR$ mit $d \in R$, seien $\alpha_1, \alpha_2 \in R$ mit $d = \alpha_1 d_1 + \alpha_2 d_2$, und sei (u_1^*, \dots, u_n^*) die zu (u_1, \dots, u_n) duale Basis von F^* . Dann ist $g = \alpha_1 u_1^* + \alpha_2 u_2^* \in F^*$, $u = d_1 u_1 + d_2 u_2 \in M$ und $g(u) = d$, also $d_1 R \subset dR \subset g(M)$. Aus der Maximalität von $d_1 R$ folgt $d_1 R = dR \supset d_2 R$.

Beweis von 2. und 3. Sei M ein endlich erzeugter R -Modul, F ein endlich erzeugter freier R -Modul minimalen Ranges, der einen R -Epimorphismus $g: F \rightarrow M$ gestattet, $M_1 = \text{Ker}(g)$ und $g^*: F/M_1 \xrightarrow{\sim} M$ der von g induzierte Isomorphismus. Nach 1. gibt es eine R -Basis (u_1, \dots, u_n) von F , ein $m \in [0, n]$ und $d_1, \dots, d_m \in R^\bullet$ mit $d_1 R \supset d_2 R \supset \dots \supset d_m R$, so dass $(d_1 u_1, \dots, d_m u_m)$ eine R -Basis von M_1 ist. Für $i \in [1, n]$ sei $x_i = g(u_i) \in M$. Dann ist $M = {}_R \langle x_1, \dots, x_n \rangle$, und aufgrund der Minimalwahl von F ist $x_i \neq 0$ für alle $i \in [1, n]$. Ist $\varphi: R^n \rightarrow F$ der durch $\varphi(\lambda_1, \dots, \lambda_n) = \lambda_1 u_1 + \dots + \lambda_n u_n$ definierte Isomorphismus, so ist $M_1 = \varphi(d_1 R \oplus \dots \oplus d_n R)$ (mit $d_j = 0$ für alle $j \in [m+1, n]$), und φ induziert einen Isomorphismus $\varphi^*: R/d_1 R \oplus \dots \oplus R/d_n R \rightarrow F/M_1$. Dann ist $\phi = g^* \circ \varphi^*: R/d_1 R \oplus \dots \oplus R/d_n R \rightarrow M$ ein Isomorphismus mit $\phi(\lambda_1 + d_1 R, \dots, \lambda_n + d_n R) = \lambda_1 x_1 + \dots + \lambda_n x_n$. Daher ist $M = Rx_1 + \dots + Rx_n$ (dir), $\text{Ann}_R(x_i) = \text{Ann}_R(1 + d_i R) = d_i R$ für alle $i \in [1, n]$, und wegen $x_1 \neq 0$ ist $R \supseteq d_1 R$. Es folgt $M_{\text{tor}} = Rx_1 + \dots + Rx_m$ (dir), und $U = Rx_{m+1} + \dots + Rx_n$ ist R -frei mit Basis (x_{m+1}, \dots, x_n) . Nach

Satz 2.4.8 ist dann $F_j(M_{\text{tor}}) = d_1 \cdot \dots \cdot d_{m-j}R$, falls $j < m$ und $F_j(M_{\text{tor}}) = R$, falls $j \geq m$, und daher sind die Ideale d_1R, \dots, d_mR eindeutig bestimmt.

Eindeutigkeitsbeweis in 1. Sind $d_1, \dots, d_m \in R^\bullet$ wie in 1., so folgt $(F/M)_{\text{tor}} = Rx_1 + \dots + Rx_m$ mit $x_j = u_j + M$ und $\text{Ann}_R(x_j) = d_jR$ für alle $j \in [1, m]$, und die Eindeutigkeit folgt wie eben aus Satz 2.4.8. \square

Satz 2.6.7 (Satz von der Smith'schen Normalform). *Sei R ein Hauptidealbereich, $m, n \in \mathbb{N}$ und $A \in M_{m,n}(R)$. Dann gibt es eindeutig bestimmte $r \in [1, \min\{m, n\}]$ und $d_1, \dots, d_r \in R^\bullet$, so dass*

$$d_1R \supset d_2R \supset \dots \supset d_rR \quad \text{und} \quad A \sim D = \begin{pmatrix} \text{diag}(d_1, \dots, d_r) & \mathbf{0}_{r, m-r} \\ \mathbf{0}_{n-r, r} & \mathbf{0}_{n-r, m-r} \end{pmatrix}.$$

D heißt *Smith'sche Normalform* von A .

BEWEIS. Sei $e^{(n)}$ die kanonische Basis von R^n , $e^{(m)}$ die kanonische Basis von R^m und $f: R^n \rightarrow R^m$ definiert durch $f(e^{(n)}) = e^{(m)}A$. Dann ist $A = \mathcal{M}_{e^{(n)}, e^{(m)}}(f)$.

EINDEUTIGKEIT: Ist $A \sim D$, so gibt es nach Bemerkung 2.4.3 R -Basen \mathbf{u} von R^n und $\mathbf{v} = (v_1, \dots, v_m)$ von R^m , so dass $\mathcal{M}_{\mathbf{u}, \mathbf{v}}(f) = D$, und dann ist (d_1v_1, \dots, d_rv_r) eine R -Basis von $\text{Bi}(f)$. Nach Satz 2.6.6 sind dadurch d_1R, \dots, d_rR eindeutig bestimmt.

EXISTENZ: Nach Satz 2.6.1 ist $\text{Bi}(f) \subset R^m$ frei vom Rang $r \in [0, n]$, und nach Satz 2.6.6 gibt es eine Basis $\mathbf{v} = (v_1, \dots, v_m)$ von R^m und $d_1, \dots, d_r \in R^\bullet$ mit $d_1R \supset d_2R \supset \dots \supset d_rR$, so dass (d_1v_1, \dots, d_rv_r) eine R -Basis von $\text{Bi}(f)$ ist. Nach Satz 2.2.7 gibt es einen R -Monomorphismus $\psi: \text{Bi}(f) \rightarrow R^m$ mit $f \circ \psi = \text{id}_{\text{Bi}(f)}$ und $R^n = \text{Bi}(\psi) + \text{Ker}(f)$ (dir). Dann ist $\text{Ker}(f|_{\text{Bi}(\psi)}) = \text{Ker}(f) \cap \text{Bi}(\psi) = \mathbf{0}$ und $\text{Bi}(f) = f(\text{Bi}(\psi))$, also $f|_{\text{Bi}(\psi)}: \text{Bi}(\psi) \xrightarrow{\sim} \text{Bi}(f)$ ein Isomorphismus. Daher gibt es eine R -Basis \mathbf{u}' von $\text{Bi}(\psi)$ mit $f(\mathbf{u}') = (d_1v_1, \dots, d_rv_r)$. Nach Satz 2.6.1 ist auch $\text{Ker}(f)$ R -frei, und es sei \mathbf{u}'' eine R -Basis von $\text{Ker}(f)$. Dann ist $\mathbf{u} = (\mathbf{u}', \mathbf{u}'')$ eine R -Basis von R^n und $f(\mathbf{u}) = (f(\mathbf{u}'), \mathbf{0}_{1, n-r}) = \mathbf{v}D$ mit $D \in M_{m,n}(R)$ wie in der Behauptung, also $D = \mathcal{M}_{\mathbf{u}, \mathbf{v}}(f) \sim A$. \square

Ring- und Körpertheorie

In diesem Kapitel seien alle Ringe kommutativ, unitär und verschieden von $\mathbf{0}$.

3.1. Ganze Ringerweiterungen

Definitionen und Bemerkungen 3.1.1. Für einen Ring R bezeichnen wir mit $R[X]$, $R[T]$, $R[X_1, \dots, X_n]$, $R[\mathbf{X}]$ etc. stets Polynomringe, mit $\text{spec}(R)$ die Menge der Primideale und mit $\text{max}(R)$ die Menge der maximalen Ideale von R .

Sei S ein Ring und $R \subset S$ ein Teilring (dann nennt man $R \subset S$ oder S/R eine *Ringerweiterung*). Für alle $\mathfrak{q} \in \text{spec}(S)$ ist $\mathfrak{q} \cap R \in \text{spec}(R)$. Für $C \subset S$ sei $[C] = \{c_1 \cdot \dots \cdot c_n \mid n \in \mathbb{N}_0, c_1, \dots, c_n \in C\}$ das von C erzeugte multiplikative Teilmonoid von S und $R[C] = {}_R\langle [C] \rangle \subset S$. $R[C]$ ist die Menge aller Linearkombinationen von endlichen Produkten von Elementen aus C mit Koeffizienten in R , und $R[C]$ ist der kleinste $R \cup C$ umfassende Teilring von S (diese Terminologie ist mit der für Polynomringe üblichen Terminologie konsistent). Ist $S = R[C]$ und sind $\varphi_1, \varphi_2: S \rightarrow S'$ Ringhomomorphismen mit $\varphi_1|_{R \cup C} = \varphi_2|_{R \cup C}$, so folgt $\varphi_1 = \varphi_2$.

Sei allgemeiner R ein Ring, A eine kommutative R -Algebra und $\varepsilon: R \rightarrow A$ der Strukturhomomorphismus. Dann ist $\varepsilon(R) \subset A$ eine Ringerweiterung, und für eine Teilmenge $C \subset A$ definieren wir $R[C] = \varepsilon(R)[C]$. Ist $C = \{x_1, \dots, x_n\}$, so nennt man $R[x_1, \dots, x_n] = R[C]$ eine *affine R -Algebra*. Eine kommutative R -Algebra A ist genau dann affin, wenn es ein $n \in \mathbb{N}$ und einen Ringepimorphismus $R[X_1, \dots, X_n] \rightarrow A$ gibt. Ist insbesondere R noethersch, so ist jede affine R -Algebra ebenfalls noethersch.

Definition und Satz 3.1.2. Sei $R \subset S$ eine Ringerweiterung. Für $x \in S$ sind äquivalent:

- Es gibt ein normiertes Polynom $f \in R[X]$ mit $f(x) = 0$ [äquivalent: Es gibt ein $n \in \mathbb{N}$ und $a_0, \dots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$].
- $R[x]$ ist ein endlich erzeugter R -Untermodul von S .
- Es gibt einen Teilring $R' \subset S$, so dass $R[x] \subset R'$ und R' ein endlich erzeugter R -Untermodul von S ist.
- Es gibt einen endlich erzeugten R -Untermodul $M \subset S$ mit $xM \subset M$ und $\text{Ann}_{R[x]}(M) = \mathbf{0}$.

Ist $f \in R[X]$ normiert mit $f(x) = 0$ und $\text{gr}(f) = n \in \mathbb{N}$, so ist $R[x] = {}_R\langle 1, x, \dots, x^{n-1} \rangle$.

Sind diese Bedingungen erfüllt, so heißt x *ganz* über R und $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ eine *ganze Gleichung* von x über R . Eine Teilmenge $C \subset S$ heißt *ganz* über R , wenn jedes Element von C ganz über R ist. Ist insbesondere S ganz über R , so nennt man $R \subset S$ oder S/R eine *ganze Ringerweiterung*.

$\text{Ganz}_S(R) = \{x \in S \mid x \text{ ist ganz über } R\}$ heißt *ganzer Abschluss* von R in S . Ist $\text{Ganz}_S(R) = R$, so heißt R *ganz-abgeschlossen* in S . Ein Bereich R mit Quotientenkörper $\mathfrak{q}(R) = K$ heißt *ganz-abgeschlossen* oder *normal*, wenn R ganz-abgeschlossen in K ist.

Ist $\varepsilon: R \rightarrow A$ eine kommutative R -Algebra, so nennt man A *ganz* über R und ε *ganz*, wenn $\varepsilon(R) \subset A$ ganz ist.

BEWEIS. (a) \Rightarrow (b) Seien $a_0, \dots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. Dann ist $M = {}_R\langle 1, x, \dots, x^{n-1} \rangle \subset S$ ein endlich erzeugter R -Untermodul, und wir zeigen $R[x] = M$. Wegen $R[x] = {}_R\langle \{x^k \mid k \in \mathbb{N}_0\} \rangle$ genügt es, $x^k \in M$ für alle $k \in \mathbb{N}_0$ zu zeigen. Wir tun das mittels Induktion nach k , und für $k \leq n-1$ ist nichts zu zeigen. Sei also $k \geq n$, und sei $\{1, x, \dots, x^{k-1}\} \subset M$. Dann folgt

$$x^k = x^{k-n}x^n = -a_{n-1}x^{k-1} - \dots - a_1x^{k-n+1} - a_0x^{k-n} \in M.$$

(b) \Rightarrow (c) Mit $R' = R[x]$.

(c) \Rightarrow (d) Mit $M = R'$.

(d) \Rightarrow (a) Sei $M = {}_R\langle u_1, \dots, u_m \rangle$ und $xM \subset M$. Dann ist M ein $R[x]$ -Untermodul von S , und es sei

$$xu_j = \sum_{\mu=1}^m a_{j,\mu} u_\mu \quad \text{für alle } j \in [1, m] \text{ mit } a_{j,\mu} \in R, \quad \text{in Matrixschreibweise } x\mathbf{u} = A\mathbf{u}$$

mit $\mathbf{u} = (u_1, \dots, u_m)^t \in \mathbf{M}_{m,1}(M)$ und $A = (a_{j,\mu})_{j,\mu \in [1,m]} \in \mathbf{M}_m(R)$, also $(xI_m - A)\mathbf{u} = \mathbf{0} \in \mathbf{M}_{m,1}(M)$. Multiplikation mit der adjungierten Matrix ergibt

$$\det(xI_m - A)\mathbf{u} = (xI_m - A)^\#(xI_m - A)\mathbf{u} = \mathbf{0}, \quad \text{also } \det(xI_m - A) \in \text{Ann}_{R[x]}(M) = \mathbf{0}$$

und daher $\det(xI_m - A) = 0$, was eine ganze Gleichung für x über R ist. \square

Satz 3.1.3. *Jeder faktorielle Bereich ist ganz-abgeschlossen.*

BEWEIS. Sei R ein faktorieller Bereich, $K = \mathfrak{q}(R)$, und wir nehmen an, es sei $x \in K \setminus R$ ganz über R . Dann ist $x = c^{-1}b$ mit zueinander teilerfremden $b, c \in R$, und es gibt ein Primelement $p \in R$ mit $p \mid c$ und $p \nmid b$. x genügt einer ganzen Gleichung $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_{n-1} \in R$. Multiplikation mit c^n ergibt $b^n + cy = 0$ mit $y = a_{n-1}b^{n-1} + ca_{n-2}b^{n-2} + \dots + a_0c^{n-1} \in R$. Aus $p \mid c$ folgt dann aber $p \mid b^n$, ein Widerspruch zu $p \nmid b$. \square

Satz 3.1.4. *Sei $R \subset S$ eine Ringerweiterung.*

1. Sei $(c_i)_{i \in I}$ eine Familie in S mit $S = {}_R\langle \{c_i \mid i \in I\} \rangle$ und $(e_j)_{j \in J}$ eine Familie in M mit $M = {}_S\langle \{e_j \mid j \in J\} \rangle$, so folgt $M = {}_R\langle \{c_i e_j \mid (i, j) \in I \times J\} \rangle$. Ist $(c_i)_{i \in I}$ eine R -Basis von S und $(e_j)_{j \in J}$ eine S -Basis von M , so ist $(c_i e_j)_{(i,j) \in I \times J}$ eine R -Basis von M .

Insbesondere gilt: Ist S ein endlich erzeugter [freier] R -Modul und M ein endlich erzeugter [freier] S -Modul, so ist M ein endlich erzeugter [freier] R -Modul [mit $\text{rg}_R(M) = \text{rg}_S(M) \text{rg}_R(S)$].

2. Seien $n \in \mathbb{N}_0$ und $x_1, \dots, x_n \in S$. Dann sind äquivalent:

- (a) Für alle $i \in [1, n]$ ist x_i ganz über R .
- (b) $R[x_1, \dots, x_n]$ ist ein endlich erzeugter R -Modul.
- (c) $R[x_1, \dots, x_n]$ ist ganz über R .

Insbesondere folgt: Ist $C \subset S$ und C ganz über R , so ist auch $R[C]$ ganz über R .

3. Ist S ein endlich erzeugter R -Modul, so ist S ganz über R .
4. Sei $T \supset S$ ein Oberring. Ist S ganz über R und $x \in T$ ganz über S , so ist x auch ganz über R .
Insbesondere gilt: T/R ist genau dann eine ganze Ringerweiterung, wenn T/S und S/R ganze Ringerweiterungen sind.
5. $\text{Ganz}_S(R)$ ist ein in S ganz-abgeschlossener Teilring von S .

BEWEIS. 1. Sei $x \in M$. Dann ist

$$x = \sum_{j \in J} b_j e_j, \quad b_j = \sum_{i \in I} \lambda_{i,j} c_i, \quad \text{also } x = \sum_{(i,j) \in I \times J} \lambda_{i,j} c_i e_j$$

(mit $b_j \in S$, $b_j = 0$ für fast alle $j \in J$, und $\lambda_{i,j} \in R$, $\lambda_{i,j} = 0$ für fast alle $(i, j) \in I \times J$). Daher folgt $M = {}_R\langle \{c_i e_j \mid (i, j) \in I \times J\} \rangle$.

Seien nun $(c_i)_{i \in I}$ linear unabhängig über R , $(e_j)_{j \in J}$ linear unabhängig über S , und sei $(\lambda_{i,j})_{(i,j) \in I \times J}$ eine Familie in R mit $\lambda_{i,j} = 0$ für fast alle $(i,j) \in I \times J$. Aus

$$0 = \sum_{(i,j) \in I \times J} \lambda_{i,j} c_i e_j = \sum_{j \in J} \left(\sum_{i \in I} \lambda_{i,j} c_i \right) e_j \quad \text{folgt} \quad \sum_{i \in I} \lambda_{i,j} c_i = 0 \quad \text{für alle } j \in J$$

und daher $\lambda_{i,j} = 0$ für alle $(i,j) \in I \times J$.

2. (a) \Rightarrow (b) Induktion nach n . Für $n = 0$ ist nichts zu zeigen.

$n \geq 1$, $n-1 \rightarrow n$: $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$, und $R[x_1, \dots, x_{n-1}]$ ist ein endlich erzeugter R -Modul nach Induktionsvoraussetzung. x_n ist ganz über R , also auch über $R[x_1, \dots, x_{n-1}]$, und daher ist $R[x_1, \dots, x_n]$ ein endlich erzeugter $R[x_1, \dots, x_{n-1}]$ -Modul nach Satz 3.1.2(b). Nach 1. ist daher $R[x_1, \dots, x_n]$ ein endlich erzeugter R -Modul.

(b) \Rightarrow (c) Nach Satz 3.1.2(c).

(c) \Rightarrow (a) Nach Definition.

Ist $C \subset S$ eine Menge über R ganzer Elemente und $x \in R[C]$, so ist $x \in R[E]$ für eine endliche Teilmenge $E \subset C$ und daher ganz über R .

3. Ist $S = {}_R\langle x_1, \dots, x_n \rangle$, so folgt $S = R[x_1, \dots, x_n]$, und daher ist S ganz über R nach 2.

4. Sei $x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$ mit $n \in \mathbb{N}$ und $b_0, \dots, b_{n-1} \in S$ eine ganze Gleichung von x über S . Dann ist x auch ganz über $R[b_0, \dots, b_{n-1}]$, und daher ist $R[b_0, \dots, b_{n-1}, x] = R[b_0, \dots, b_{n-1}][x]$ ein endlich erzeugter $R[b_0, \dots, b_{n-1}]$ -Modul. Da b_0, \dots, b_{n-1} ganz über R sind, ist $R[b_0, \dots, b_{n-1}]$ ein endlich erzeugter R -Modul nach 2. Nach 1. ist dann auch $R[b_0, \dots, b_{n-1}, x]$ ein endlich erzeugter R -Modul, und nach Satz 3.1.2(c) ist x ganz über R .

5. Sind $x, y \in \text{Ganz}_S(R)$, so ist $\{x - y, xy\} \subset R[x, y] \subset \text{Ganz}_S(R)$ nach 2. und daher $\text{Ganz}_S(R)$ ein Teilring von S . Ist $x \in S$ ganz über $\text{Ganz}_S(R)$, so ist x nach 3. auch ganz über R und daher $x \in \text{Ganz}_S(R)$. Folglich ist $\text{Ganz}_S(R)$ ganz-abgeschlossen in S . \square

Definition 3.1.5. Sei R ein Ring. Dann heißt

$$\dim(R) = \sup\{n \in \mathbb{N}_0 \mid \text{es gibt eine Folge } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n \text{ in } \text{spec}(R)\}$$

die (Krull-)Dimension von R .

Bemerkung 3.1.6. Sei R ein Bereich. Dann ist $\mathbf{0} \in \text{spec}(R)$, und es gilt:

1. Genau dann ist $\dim(R) = 0$, wenn R ein Körper ist.
2. Ist R ein Hauptidealbereich, so ist $\dim(R) \leq 1$.

Satz 3.1.7 (Satz von Cohen-Seidenberg). Sei $R \subset S$ eine ganze Ringerweiterung.

1. Seien $\mathfrak{q} \in \text{spec}(S)$ und $\mathfrak{a} \triangleleft S$ mit $\mathfrak{q} \subset \mathfrak{a}$ und $\mathfrak{q} \cap R = \mathfrak{a} \cap R$. Dann ist $\mathfrak{q} = \mathfrak{a}$.
2. Zu jedem $\mathfrak{p} \in \text{spec}(R)$ und $\mathfrak{a} \triangleleft S$ mit $\mathfrak{a} \cap R \subset \mathfrak{p}$ gibt es ein $\mathfrak{q} \in \text{spec}(S)$ mit $\mathfrak{a} \subset \mathfrak{q}$ und $\mathfrak{q} \cap R = \mathfrak{p}$. Insbesondere ist die Abbildung $\text{spec}(S) \rightarrow \text{spec}(R)$, $\mathfrak{q} \mapsto \mathfrak{q} \cap R$, surjektiv.
3. Seien $\mathfrak{p}_0, \mathfrak{p} \in \text{spec}(R)$ und $\mathfrak{q}_0 \in \text{spec}(S)$ mit $\mathfrak{q}_0 \cap R = \mathfrak{p}_0 \subset \mathfrak{p}$. Dann gibt es ein $\mathfrak{q} \in \text{spec}(S)$ mit $\mathfrak{q}_0 \subset \mathfrak{q}$ und $\mathfrak{q} \cap R = \mathfrak{p}$.
4. $\max(S) = \{\mathfrak{q} \in \text{spec}(S) \mid \mathfrak{q} \cap R \in \max(R)\}$. Insbesondere gibt es zu jedem $\mathfrak{m} \in \max(R)$ ein $\mathfrak{q} \in \max(S)$ mit $\mathfrak{q} \cap R = \mathfrak{m}$.
5. $S^\times \cap R = R^\times$.
6. $\dim(R) = \dim(S)$. Insbesondere: Ist S ein Bereich, so ist S genau dann ein Körper, wenn R ein Körper ist.

BEWEIS. 1. Sei $x \in \mathfrak{a}$ und $n \in \mathbb{N}$ minimal mit folgender Eigenschaft: Es gibt $a_0, \dots, a_{n-1} \in R$ mit $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathfrak{q}$ (aus der Existenz einer ganzen Gleichung für x über R folgt die Existenz eines solchen n). Dann gibt es ein $q \in \mathfrak{q}$ mit

$a_0 = q - x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) \in \mathfrak{a} \cap R = \mathfrak{q} \cap R \subset \mathfrak{q}$, also $x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) \in \mathfrak{q}$, und wegen $x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1 \notin \mathfrak{q}$ folgt $x \in \mathfrak{q}$.

2. Sei $\mathfrak{p} \in \text{spec}(R)$ und $\mathfrak{a} \triangleleft S$ mit $\mathfrak{a} \cap R \subset \mathfrak{p}$. Dann ist $R \setminus \mathfrak{p} \subset S$ eine multiplikativ abgeschlossene Menge und $\mathfrak{a} \cap (R \setminus \mathfrak{p}) = \emptyset$. Nach Satz 2.3.7 hat die Menge $\{\mathfrak{c} \triangleleft S \mid \mathfrak{a} \subset \mathfrak{c} \text{ und } \mathfrak{c} \cap (R \setminus \mathfrak{p}) = \emptyset\}$ ein maximales Element \mathfrak{q} , es ist $\mathfrak{q} \in \text{spec}(S)$, $\mathfrak{a} \subset \mathfrak{q}$ und $\mathfrak{q} \cap R \subset \mathfrak{p}$. Wir nehmen nun an, es sei $\mathfrak{q} \cap R \subsetneq \mathfrak{p}$ und führen das zum Widerspruch. Sei $u \in \mathfrak{p} \setminus \mathfrak{q}$. Wegen der Maximalität von \mathfrak{q} ist dann $(\mathfrak{q} + uS) \cap (R \setminus \mathfrak{p}) \neq \emptyset$, und es sei $q \in \mathfrak{q}$ und $s \in S$, so dass $x = q + us \in R \setminus \mathfrak{p}$. Sei $s^n + a_{n-1}s^{n-1} + \dots + a_1s + a_0 = 0$ eine ganze Gleichung für s über R . Dann folgt $(us)^n + a_{n-1}u(us)^{n-1} + \dots + a_1u^{n-1}(us) + a_0u^n = 0$, und wegen $us \equiv x \pmod{\mathfrak{q}}$ erhalten wir $x^n + a_{n-1}ux^{n-1} + \dots + a_1u^{n-1}x + a_0u^n \in \mathfrak{q} \cap R \subset \mathfrak{p}$. Wegen $u \in \mathfrak{p}$ folgt daraus $x^n \in \mathfrak{p}$ und schließlich $x \in \mathfrak{p}$, ein Widerspruch.

3. Nach 2. mit $\mathfrak{a} = \mathfrak{q}_0$.

4. Sei $\mathfrak{q} \in \text{spec}(S)$. Ist $\mathfrak{q} \notin \text{max}(S)$, so gibt es nach Satz 2.3.7 ein $\mathfrak{m} \in \text{max}(S)$ mit $\mathfrak{q} \subsetneq \mathfrak{m}$. Dann ist aber $\mathfrak{q} \cap R \subsetneq \mathfrak{m} \cap R$ nach 1. und daher auch $\mathfrak{q} \cap R \notin \text{max}(R)$. Ist umgekehrt $\mathfrak{q} \cap R \notin \text{max}(R)$, so gibt es ein $\mathfrak{n} \in \text{max}(R)$ mit $\mathfrak{q} \cap R \subsetneq \mathfrak{n}$, und nach 3. gibt es ein $\mathfrak{m} \in \text{spec}(S)$ mit $\mathfrak{q} \subset \mathfrak{m}$ und $\mathfrak{m} \cap R = \mathfrak{n}$. Daher ist $\mathfrak{q} \subsetneq \mathfrak{m}$ und $\mathfrak{q} \notin \text{max}(S)$.

5. Offensichtlich ist $R^\times \subset R \cap S^\times$. Ist $x \in R \setminus R^\times$, so gibt es ein $\mathfrak{m} \in \text{max}(R)$ mit $x \in \mathfrak{m}$, und nach 2. gibt es ein $\mathfrak{p} \in \text{spec}(S)$ mit $\mathfrak{m} \subset \mathfrak{p}$. Daher ist $x \in \mathfrak{p}$ und $x \notin S^\times$.

6. Sei $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n$ eine Folge in $\text{spec}(R)$. Nach 2. gibt es ein $\mathfrak{q}_0 \in \text{spec}(S)$ mit $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$, und mittels wiederholter Anwendung von 3. folgt die Existenz einer Folge $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_n$ in $\text{spec}(S)$ mit $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ für alle $i \in [1, n]$. Daher ist $\dim(S) \geq \dim(R)$.

Ist umgekehrt $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_n$ eine Folge in $\text{spec}(S)$, so folgt $\mathfrak{q}_0 \cap R \subsetneq \mathfrak{q}_1 \cap R \subsetneq \dots \subsetneq \mathfrak{q}_n \cap R$ nach 1., und daher ist auch $\dim(S) \leq \dim(R)$.

Ist S ein Bereich, so auch R , und wegen $\dim(R) = \dim(S)$ sind beide Körper oder beide nicht. \square

3.2. Quotientenbildung

Definitionen und Bemerkungen 3.2.1. Sei R ein Ring, $T \subset R$ eine multiplikativ abgeschlossene Teilmenge [d. h., $1 \in T$ und $TT = T$], und sei M ein R -Modul.

1. Für $(t, x), (t', x') \in T \times M$ definiert man: $(t, x) \sim (t', x') \iff (\exists s \in T) st'x = stx'$.

Dann ist \sim eine Äquivalenzrelation auf $T \times M$ [Beweis: Nur die Transitivität ist nichttrivial. Sei $(t, x) \sim (t', x')$ und $(t', x') \sim (t'', x'')$. Dann gibt es $s, s' \in T$ mit $st'x = stx'$ und $s't''x' = s't'x''$, und es folgt $s't''st'x = s't''stx' = sts't'x''$, also $(s't'')t''x = (s't'')tx''$ und daher $(t, x) \sim (t'', x'')$.

Wir definieren $T^{-1}M = T \times M / \sim$ und bezeichnen mit $\frac{x}{t} \in T^{-1}M$ die Äquivalenzklasse von (t, x) . Dann folgt:

1) $\frac{x}{t} = \frac{sx}{st}$ für alle $x \in M$ und $s, t \in T$.

2) Für $n \in \mathbb{N}$ und $z_1, \dots, z_n \in T^{-1}M$ gibt es $x_1, \dots, x_n \in M$ und ein $t \in T$, so dass $z_i = \frac{x_i}{t}$ für alle $i \in [1, n]$.

2. Auf $T^{-1}M$ sei eine Addition definiert durch

$$\frac{x}{t} + \frac{x'}{t'} = \frac{t'x + tx'}{tt'}.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten und macht $T^{-1}M$ zur abelschen Gruppe mit Null $\frac{0}{1}$ und Negativem $-\frac{x}{t} = \frac{-x}{t}$.

Die Abbildung

$$j: M \rightarrow T^{-1}M, \quad \text{definiert durch } j(x) = \frac{x}{1},$$

ist ein Gruppenhomomorphismus (genannt *Quotientenhomomorphismus*), und

$$\text{Ker}(j) = \{x \in M \mid (\exists t \in T) xt = 0\} = \{x \in M \mid T \cap \text{Ann}_R(x) \neq \emptyset\}.$$

Ist $0 \in T$, so ist $T^{-1}M = \mathbf{0}$. Ist M torsionsfrei und $0 \notin T$, so ist $j: M \rightarrow T^{-1}M$ ein Monomorphismus.

3. Betrachte nun den Spezialfall $M = R$ und definiere eine Multiplikation auf $T^{-1}R$ durch

$$\frac{a}{t} \frac{a'}{t'} = \frac{aa'}{tt'}.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten. Mit dieser Multiplikation wird $T^{-1}R$ zu einem (kommutativen) Ring mit Eins $\frac{1}{1}$ und $j: R \rightarrow T^{-1}R$ zu einem Ringhomomorphismus (also $T^{-1}R$ zu einer R -Algebra) mit $j(T) = \{\frac{t}{1} \mid t \in T\} \subset (T^{-1}R)^\times$.

Im Spezialfall $T = [x] = \{x^n \mid n \in \mathbb{N}_0\}$ ist $[x]^{-1}R = R[\frac{1}{x}]$ eine affine R -Algebra.

Bezeichne $\mathfrak{n}(R)$ die Menge der Nullteiler von R . Ist dann $T \cap \mathfrak{n}(R) = \emptyset$, so ist $j: R \rightarrow T^{-1}R$ ein Monomorphismus. In diesem Falle fassen wir R als Teilring von $T^{-1}R$ auf und rechnen in der Form $a = \frac{a}{1}$. Ist $T = R \setminus \mathfrak{n}(R)$, so nennt man $T^{-1}R$ den *totalen Quotientenring* von R . Für jede multiplikativ abgeschlossene Teilmenge $T \subset R \setminus \mathfrak{n}(R)$ ist $T^{-1}R$ ein Teilring des totalen Quotientenringes von R . Ist R ein Bereich und $T = R^\bullet$, so ist $T^{-1}R = \mathfrak{q}(R)$ ein Quotientenkörper von R . Ist $T \subset R^\times$, so ist $T^{-1}R = R$, und für jeden R -Modul M ist $T^{-1}M = M$.

4. Sei M ein R -Modul. Definiere eine $T^{-1}R$ -Modulstruktur auf $T^{-1}M$ durch

$$\frac{a}{t} \frac{x}{t'} = \frac{ax}{tt'} \quad \text{für } a \in R, x \in M, t, t' \in T.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten. Damit wird $T^{-1}M$ zum $T^{-1}R$ -Modul, also nach Bemerkung 2.1.7.2 auch zum R -Modul vermöge $a \frac{x}{t} = \frac{ax}{t}$, und dann ist $j: M \rightarrow T^{-1}M$ ein R -Modulhomomorphismus. Ist $N \subset M$ ein R -Untermodul, so ist $T^{-1}N \subset T^{-1}M$ ein $T^{-1}R$ -Untermodul.

5. Sei $f: M \rightarrow M'$ ein R -Modulhomomorphismus. Dann definiert man

$$T^{-1}f: T^{-1}M \rightarrow T^{-1}M' \quad \text{durch} \quad T^{-1}f\left(\frac{x}{t}\right) = \frac{f(x)}{t}.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten, $T^{-1}f$ ist ein $T^{-1}R$ -Modulhomomorphismus. Damit wird $(M \mapsto T^{-1}M, f \mapsto T^{-1}f)$ zum Funktor $R\text{-Mod} \rightarrow T^{-1}R\text{-Mod}$.

Satz 3.2.2. *Sei R ein Ring und $T \subset R$ eine multiplikativ abgeschlossene Menge.*

1. *Seien M, M' R -Moduln und $f: M \rightarrow M'$ ein R -Homomorphismus. Dann ist*

$$\text{Ker}(T^{-1}f) = T^{-1}\text{Ker}(f) \subset T^{-1}M \quad \text{und} \quad \text{Bi}(T^{-1}f) = T^{-1}\text{Bi}(f) \subset T^{-1}M'.$$

2. *Sei M ein R -Modul und $N \subset M$ ein R -Untermodul. Dann ist $T^{-1}N \subset T^{-1}M$ ein $T^{-1}R$ -Untermodul, und es gibt einen $T^{-1}R$ -Isomorphismus*

$$\Phi: T^{-1}M/T^{-1}N \rightarrow T^{-1}(M/N) \quad \text{mit} \quad \Phi\left(\frac{x}{t} + T^{-1}N\right) = \frac{x+N}{t} \quad \text{für alle } x \in M \text{ und } t \in T.$$

3. *Sei M ein R -Modul, $j: M \rightarrow T^{-1}M$ der Quotientenhomomorphismus und E ein R -Erzeugendensystem von M . Dann ist $j(E)$ ein $T^{-1}R$ -Erzeugendensystem von $T^{-1}M$.*

BEWEIS. 1. Sei $\frac{x}{t} \in \text{Ker}(T^{-1}f) \subset T^{-1}M$ mit $x \in M$ und $t \in T$. Dann ist $T^{-1}f\left(\frac{x}{t}\right) = \frac{f(x)}{t} = \frac{0}{t} = \frac{0}{1}$. Daher gibt es ein $s \in T$ mit $0 = sf(x) = f(sx)$, also $sx \in \text{Ker}(f)$ und daher $\frac{x}{t} = \frac{sx}{st} \in T^{-1}\text{Ker}(f)$.

Ist $\frac{x}{t} \in T^{-1}\text{Ker}(f)$ mit $x \in \text{Ker}(f)$ und $t \in T$, so folgt $T^{-1}f\left(\frac{x}{t}\right) = \frac{f(x)}{t} = \frac{0}{t} = \frac{0}{1}$, also $\frac{x}{t} \in \text{Ker}(T^{-1}f)$. Die Aussage über die Bilder folgt unmittelbar aus der Definition.

2. Sei $\pi: M \rightarrow M/N$ der Restklassenhomomorphismus. Dann ist $T^{-1}\pi: T^{-1}M \rightarrow T^{-1}(M/N)$ ein Epimorphismus, $\text{Ker}(T^{-1}\pi) = T^{-1}N$ nach 1., und aus dem Homomorphiesatz folgt die Behauptung.

3. Sei $\frac{x}{t} \in T^{-1}M$ mit $x \in M$ und $t \in T$. Dann ist $x = c_1u_1 + \dots + c_nu_n$ mit $n \in \mathbb{N}$, $c_\nu \in R$ und $u_\nu \in E$ für alle $\nu \in [1, n]$, und es folgt $\frac{x}{t} = \frac{c_1}{t} \frac{u_1}{1} + \dots + \frac{c_n}{t} \frac{u_n}{1} = \frac{c_1}{t} j(u_1) + \dots + \frac{c_n}{t} j(u_n) \in T^{-1}R\langle j(E) \rangle$. \square

Definitionen und Bemerkungen 3.2.3. Sei R ein Ring, $T \subset R$ eine multiplikativ abgeschlossene Menge und A eine R -Algebra. Auf dem $T^{-1}R$ -Modul $T^{-1}A$ sei die Multiplikation definiert durch

$$\frac{a}{t} \frac{a'}{t'} = \frac{aa'}{tt'} \quad \text{für } a, a' \in A \text{ und } t, t' \in T.$$

Diese Definition ist unabhängig von der Wahl der Repräsentanten und macht $T^{-1}A$ zur $T^{-1}R$ -Algebra. Ist $\varepsilon: R \rightarrow A$ der Strukturhomomorphismus von A , so ist $T^{-1}\varepsilon: T^{-1}R \rightarrow T^{-1}A$ der Strukturhomomorphismus von $T^{-1}A$. Ist $j: A \rightarrow T^{-1}A$ der Quotientenhomomorphismus und $C \subset A$ mit $A = R[C]$, so folgt $T^{-1}A = T^{-1}R[j(C)]$ [denn: Ist $[C] = \{c_1 \dots c_n \mid n \in \mathbb{N}, c_\nu \in C\}$, so ist $A = R\langle [C] \rangle$, $j([C]) = [j(C)]$ und daher $T^{-1}A = T^{-1}R\langle [j(C)] \rangle = T^{-1}R[j(C)]$ nach Satz 3.2.2.3].

Ist insbesondere $R \subset A$ eine Ringerweiterung, so ist auch $T^{-1}R \subset T^{-1}A$ eine Ringerweiterung.

Satz 3.2.4. Sei $R \subset S$ eine Ringerweiterung und $T \subset R$ multiplikativ abgeschlossen. Dann ist $T^{-1}\text{Ganz}_S(R) = \text{Ganz}_{T^{-1}S}(T^{-1}R)$. Insbesondere gilt:

1. Ist S ganz über R , so ist auch $T^{-1}S$ ganz über $T^{-1}R$.
2. Ist R ganz-abgeschlossen in S , so ist auch $T^{-1}R$ ganz-abgeschlossen in $T^{-1}S$.

BEWEIS. \subset : Sei $\frac{x}{t} \in T^{-1}\text{Ganz}_S(R)$ mit $x \in \text{Ganz}_S(R)$, $t \in T$ und einer ganzen Gleichung $x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0 = 0$ von x über R . Dann ist

$$\frac{0}{1} = \frac{x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0}{t^d} = \left(\frac{x}{t}\right)^d + \frac{a_{d-1}}{t} \left(\frac{x}{t}\right)^{d-1} + \dots + \frac{a_1}{t^{d-1}} \frac{x}{t} + \frac{a_0}{t^d}$$

eine ganze Gleichung für $\frac{x}{t}$ über $T^{-1}R$, und daher $\frac{x}{t} \in \text{Ganz}_{T^{-1}S}(T^{-1}R)$.

\supset : Sei $\frac{x}{t} \in \text{Ganz}_{T^{-1}S}(T^{-1}R)$ mit $x \in S$, $t \in T$, und sei

$$\left(\frac{x}{t}\right)^d + \frac{a_{d-1}}{w_{d-1}} \left(\frac{x}{t}\right)^{d-1} + \dots + \frac{a_1}{w_1} \frac{x}{t} + \frac{a_0}{w_0} = \frac{0}{1}$$

eine ganze Gleichung von $\frac{x}{t}$ über $T^{-1}R$. Setzt man $s = w_0 \dots w_{d-1}$ und $w = t^d s$, so folgt $s, w \in T$, und die ganze Gleichung hat die Form

$$\frac{sx^d + a'_{d-1}x^{d-1} + \dots + a'_1x + a'_0}{w} = \frac{0}{1}$$

mit $a'_0, \dots, a'_{d-1} \in R$. Daher gibt es ein $s' \in T$ mit $s'(sx^d + a'_{d-1}x^{d-1} + \dots + a'_1x + a'_0) = 0$. Nach Multiplikation mit $(s's)^{d-1}$ erhalten wir eine ganze Gleichung für $s'sx$ über R . Daher ist $s'sx \in \text{Ganz}_S(R)$ und $\frac{x}{t} = \frac{s'sx}{s'st} \in T^{-1}\text{Ganz}_S(R)$. \square

3.3. Algebraische Körpererweiterungen

Definitionen und Bemerkungen 3.3.1. Sei $R \subset S$ eine Ringerweiterung.

1. Für eine Familie $\mathbf{x} = (x_i)_{i \in I}$ in S sei $R[\mathbf{x}] = R[\{x_i \mid i \in I\}]$. Ist $\mathbf{X} = (X_i)_{i \in I}$ und $R[\mathbf{X}]$ der Polynomring in $(X_i)_{i \in I}$, so gibt es nach Bemerkung 2.2.8 genau einen R -Algebrenepimorphismus $\phi_{\mathbf{x}}: R[\mathbf{X}] \rightarrow R[\mathbf{x}]$, und dieser ist gegeben durch $\phi_{\mathbf{x}}(f) = f(\mathbf{x})$ für alle $f \in R[\mathbf{X}]$. Ist \mathbf{x} die leere Familie, so ist $\phi_{\mathbf{x}} = \text{id}_R$.

Eine Familie $\mathbf{x} = (x_i)_{i \in I}$ in S heißt *algebraisch unabhängig* über R , wenn $\phi_{\mathbf{x}}$ injektiv ist, sonst *algebraisch abhängig* über R . Genau dann ist \mathbf{x} algebraisch abhängig über R , wenn $f(\mathbf{x}) = 0$ für ein $f \in R[\mathbf{X}]^\bullet$. Dann gibt es aber Indizes $i_1, \dots, i_n \in I$ mit $f \in R[X_{i_1}, \dots, X_{i_n}]$, und es ist bereits die Teilfamilie $(x_{i_\nu})_{\nu \in [1, n]}$ algebraisch abhängig über R . Ist \mathbf{x} algebraisch unabhängig über R , so ist $x_i \notin R$ für alle $i \in I$ und $x_i \neq x_j$ für alle $i, j \in I$ mit $i \neq j$.

Eine Menge $B \subset S$ heißt *algebraisch (un)abhängig* über R , wenn die Familie $(b)_{b \in B}$ das ist. Genau dann ist B algebraisch abhängig über R , wenn bereits eine endliche Teilmenge von B über R algebraisch abhängig ist. Ist $[B]$ das von B erzeugte multiplikative Teilmonoid von S , so ist B genau dann algebraisch unabhängig über R , wenn $[B]$ linear unabhängig über R ist. Die leere Menge ist definitionsgemäß algebraisch unabhängig über R .

2. Ein Element $x \in S$ heißt *algebraisch* über R , wenn es ein $f \in R[X]^\bullet$ gibt mit $f(x) = 0$ [äquivalent: $\{x\}$ ist algebraisch abhängig über R]. Ist x nicht algebraisch über R , so heißt x *transzendent* oder *frei* über R . Ist R ein Körper, so ist x genau dann algebraisch über R , wenn x ganz über R ist.
3. Seien $K \subset L$ Körper (dann nennt man L/K oder $K \subset L$ eine *Körpererweiterung*). Für $C \subset L$ sei $K(C) = \{a^{-1}b \mid a, b \in K[C], a \neq 0\} \subset L$ ein Quotientenkörper von $K[C]$. Dann ist $K(C)$ der kleinste Teilkörper von L , der $K \cup C$ umfasst. Sind $\varphi_1, \varphi_2: L \rightarrow L'$ Körperhomomorphismen mit $\varphi_1|_{K \cup C} = \varphi_2|_{K \cup C}$, so folgt $\varphi_1|_{K(C)} = \varphi_2|_{K(C)}$.

Die Körpererweiterung L/K heißt *endlich erzeugt*, wenn $L = K(C)$ mit einer endlichen Menge $C \subset L$. Ist $C = \{x_1, \dots, x_n\}$, so sei $K(C) = K(x_1, \dots, x_n)$.

4. Seien $K \subset L$ Körper. Für eine Familie $\mathbf{x} = (x_i)_{i \in I}$ in L sei $K(\mathbf{x}) = K(\{x_i \mid i \in I\})$. Ist $\mathbf{X} = (X_i)_{i \in I}$ und $K[\mathbf{X}]$ der Polynomring in $(X_i)_{i \in I}$, so heißt sein Quotientenkörper $K(\mathbf{X})$ *rationaler Funktionenkörper* in \mathbf{X} . Ist \mathbf{x} algebraisch unabhängig über K , so induziert $\phi_{\mathbf{x}}$ einen Isomorphismus $K(\mathbf{X}) \rightarrow K(\mathbf{x})$. Man nennt dann $K(\mathbf{x})/K$ eine *rein transzendente Körpererweiterung*.
5. Sei L/K eine Körpererweiterung. Eine Teilmenge $C \subset L$ heißt *algebraisch* über K , wenn jedes Element von C über K algebraisch ist [äquivalent: C ist ganz über K]. Ist L algebraisch über K , so nennt man L/K eine *algebraische Körpererweiterung* [äquivalent: L/K ist eine ganze Ringerweiterung]. Ist L/K nicht algebraisch, so nennt man die Körpererweiterung L/K *transzendent* und sagt auch, L ist *transzendent* über K .

Man nennt $[L:K] = \dim_K L$ den *Grad* von L/K und L/K eine *endliche Körpererweiterung*, wenn $[L:K] < \infty$. Man nennt

$$\text{Alg}_L(K) = \text{Ganz}_L(K) = \{z \in L \mid z \text{ ist algebraisch über } K\}$$

den (*relativen*) *algebraischen Abschluss* von K in L . Ist $\text{Alg}_L(K) = K$, so heißt K (*relativ*) *algebraisch abgeschlossen* in L [äquivalent: K ist ganz-abgeschlossen in L].

6. Sei $n \in \mathbb{N}$, und seien K, L, K_1, \dots, K_n Körper, so dass $K \subset K_i \subset L$ für alle $i \in [1, n]$. Dann nennt man

$$\prod_{i=1}^n K_i = K_1 \cdot \dots \cdot K_n = K(K_1 \cup \dots \cup K_n) \subset L$$

das *Kompositum* von K_1, \dots, K_n . Der Körper $K_1 \cdot \dots \cdot K_n$ ist der kleinste Teilkörper von L , der die Körper K_1, \dots, K_n enthält. Es ist $K_1 K_2 = K_1(K_2)$.

7. Sei $\varphi: R \rightarrow R'$ ein Ringhomomorphismus, und seien $R[\mathbf{X}]$ und $R'[\mathbf{X}]$ Polynomringe. Dann bezeichnen wir mit $\varphi_1: R[\mathbf{X}] \rightarrow R'[\mathbf{X}]$ den eindeutig bestimmten Ringhomomorphismus mit $\varphi_1|_R = \varphi$ und $\varphi_1|_{\mathbf{X}} = \text{id}_{\mathbf{X}}$, und wir nennen φ_1 die *Fortsetzung* von φ auf die Polynomringe.

Satz 3.3.2. *Sei L/K eine Körpererweiterung.*

1. *Sei $K \subset M \subset L$ ein Zwischenkörper.*
 - (a) $[L:K] = [L:M][M:K]$. *Insbesondere ist L/K genau dann eine endliche Körpererweiterung, wenn L/M und M/K beide endliche Körpererweiterungen sind.*
 - (b) L/K *genau dann algebraisch, wenn L/M und M/K beide algebraisch sind.*
2. *Ist L/K eine endliche Körpererweiterung, so ist L/K algebraisch.*
3. *Sei $C \subset L$ und C algebraisch über K . Dann ist $K[C] = K(C)$, und $K(C)/K$ ist algebraisch. Ist C endlich, so ist $[K(C):K] < \infty$.*
4. $\text{Alg}_L(K)$ *ist ein über K algebraischer und in L relativ algebraisch abgeschlossener Körper.*
5. *Seien $K \subset M \subset L$ und $K \subset K' \subset L$ Zwischenkörper, und sei M/K algebraisch. Dann ist auch MK'/K' algebraisch.*

BEWEIS. 1. (a) folgt aus Satz 3.1.4.1, und (b) aus Satz 3.1.4.4.

2. Nach Satz 3.1.4.3.

3. Nach Satz 3.1.4.2 ist $K[C]/K$ ganz, also algebraisch. Nach Satz 3.1.7.6 ist $K[C]$ ein Körper und daher $K(C) = K[C]$. Ist C endlich, so ist $[K(C):K] < \infty$ nach Satz 3.1.4.2

4. Nach Satz 3.1.4.5 ist $\text{Alg}_L(K)$ ein in L algebraisch abgeschlossener Körper, und nach Definition ist $\text{Alg}_L(K)$ algebraisch.

5. Ist M algebraisch über K , so ist M auch algebraisch über K' . Daher ist $MK' = K'(M)$ algebraisch über K' nach 3. \square

Definitionen und Bemerkungen 3.3.3. *Sei L/K eine Körpererweiterung.*

1. Sei $x \in L$ algebraisch über K und $\phi_x: K[X] \rightarrow K[x]$ der Einsetzungshomomorphismus (siehe Bemerkung 2.2.8.3). Dann ist $\mathbf{0} \neq \text{Ker}(\phi_x) = fK[X]$ mit einem eindeutig bestimmten normierten Polynom $f \in K[X] \setminus K$, und ϕ_x induziert einen Isomorphismus

$$\phi_x^*: K[X]/fK[X] \xrightarrow{\sim} K[x] = K(x) \subset L \quad \text{mit} \quad \phi_x^*(g + fK[X]) = g(x) \quad \text{für alle} \quad g \in K[X].$$

Daher ist $K[X]/fK[X]$ ein Körper und $fK[X] \triangleleft K[X]$ ein maximales Ideal, also f irreduzibel.

f ist das einzige normierte irreduzible Polynom mit Nullstelle x und heißt *Minimalpolynom* von x über K [denn: Ist $g \in K[X]$ ein normiertes irreduzibles Polynom mit $g(x) = 0$, so ist $g \in fK[X]$, also $f|g$ und daher $f = g$].

Ist $d = \text{gr}(f)$, so ist $(1, x, \dots, x^{d-1})$ eine K -Basis von $K(x)$, also $[K(x):K] = d$ [denn: Nach Satz 3.1.2 ist $(1, x, \dots, x^{d-1})$ ein K -Erzeugendensystem von $K(x)$. Seien $a_0, \dots, a_{d-1} \in K$ mit $a_0 + a_1x + \dots + a_{d-1}x^{d-1} = 0$. Dann ist $g = a_0 + a_1X + \dots + a_{d-1}X^{d-1} \in K[X]$ und $g(x) = 0$, also $g \in \text{Ker}(\phi_x) = fK[X]$ und daher $f|g$. Wegen $\text{gr}(g) < \text{gr}(f)$ folgt $g = 0$].

2. Seien L/K und L'/K' Körpererweiterungen, $\varphi: K \xrightarrow{\sim} K'$ ein Isomorphismus, $\varphi_1: K[X] \xrightarrow{\sim} K'[X]$ seine Fortsetzung auf die Polynomringe, $f \in K[X] \setminus K$ irreduzibel, $x \in L$ mit $f(x) = 0$ und $x' \in L'$ mit $\varphi_1(f)(x') = 0$. Dann gibt es genau einen Isomorphismus $\bar{\varphi}: K(x) \xrightarrow{\sim} K'(x')$ mit $\bar{\varphi}|_K = \varphi$ und $\bar{\varphi}(x) = x'$ [denn: Die Einsetzungshomomorphismen induzieren Isomorphismen

$\phi_x^*: K[X]/fK[X] \xrightarrow{\sim} K(x)$ und $\phi_{x'}^*: K'[X]/\varphi_1(f)K'[X] \rightarrow K'(x')$, und φ_1 induziert einen Isomorphismus $\varphi_1^*: K[X]/fK[X] \xrightarrow{\sim} K'[X]/\varphi_1(f)K'[X]$. Dann ist

$$\bar{\varphi} = \phi_{x'}^* \circ \varphi_1^* \circ (\phi_x^*)^{-1}: K(x) \xrightarrow{\sim} K'(x')$$

der gewünschte Isomorphismus. Die Eindeutigkeit ist offensichtlich].

3. Seien L/K und L'/K Körpererweiterungen. Ein Körperhomomorphismus $\varphi: L \rightarrow L'$ heißt *K-Homomorphismus*, wenn $\varphi|_K = \text{id}_K$. Wir bezeichnen mit $\text{Hom}_K(L, L') = \text{Hom}_{K\text{-Alg}}(L, L')$ die Menge aller K -Homomorphismen $\varphi: L \rightarrow L'$ und mit $\text{Gal}(L/K)$ die Menge aller K -Isomorphismen $\varphi: L \rightarrow L$. $\text{Gal}(L/K) = \text{Hom}_K(L, L)^\times$ ist eine Gruppe und heißt *Galoisgruppe* von L/K . Ist $\varphi \in \text{Hom}_K(L, L')$, $x \in L$ und $f \in K[X]$, so folgt $\varphi(f(x)) = f(\varphi(x))$.
4. Sei L/K eine Körpererweiterung. Zwei Elemente $x, y \in \text{Alg}_L(K)$ heißen *konjugiert* über K , wenn sie dasselbe Minimalpolynom über K haben. Ist $x \in \text{Alg}_L(K)$ und $\varphi \in \text{Hom}_K(L, L)$, so ist auch $\varphi(x) \in \text{Alg}_L(K)$, und x und $\varphi(x)$ sind konjugiert über K .

Ist L/K algebraisch, so ist $\text{Hom}_K(L, L) = \text{Gal}(L/K)$ (jeder K -Homomorphismus $\varphi: L \rightarrow L$ ist ein Isomorphismus). [Beweis: Sei $\varphi \in \text{Hom}_K(L, L)$, $x \in L$, $f \in K[X]$ das Minimalpolynom von x über K und $N = \{z \in L \mid f(z) = 0\}$. Dann ist N endlich, $\varphi(N) \subset N$, und da φ injektiv ist, folgt $\varphi(N) = N$, also $x \in \varphi(N) \subset \varphi(L)$. Daher ist φ surjektiv, also ein Isomorphismus.]

Satz 3.3.4. *Sei K ein Körper.*

1. *Ist L/K eine algebraische Körpererweiterung, so ist $|K| \leq |L| \leq \max\{|K|, \omega\}$.*
2. *Sei $f \in K[X] \setminus K$ und Σ eine Menge mit $K \subset \Sigma$ und $|\Sigma| > \max\{|K|, \omega\}$. Dann gibt es eine Körpererweiterung L/K mit $L \subset \Sigma$ und ein $x \in L$ mit $f(x) = 0$.*

BEWEIS. 1. Für $f \in K[X] \setminus K$ sei $N(f) = \{x \in L \mid f(x) = 0\}$ (diese Menge ist endlich). Dann ist $L = \bigcup \{N(f) \mid f \in K[X] \setminus K\}$, und aus Satz 1.3.7 folgt $|L| \leq \omega |K[X] \setminus K|$. Ist $\mathcal{F}(K)$ die Menge aller endlichen Folgen in K , so ist $g: \mathcal{F}(K) \rightarrow K[X]$, definiert durch $(a_0, \dots, a_n) \mapsto a_0 + a_1X + \dots + a_nX^n$, eine surjektive Abbildung, und mit Satz 1.3.8 folgt $|K[X] \setminus K| \leq |K[X]| \leq |\mathcal{F}(K)| \leq \max\{|K|, \omega\}$.

2. Es genügt, zu zeigen:

- A.** Es gibt einen Körper L_1 , ein Element $x_1 \in L_1$ und einen Körperhomomorphismus $\varepsilon: K \rightarrow L_1$, so dass $\varepsilon_1(f)(x_1) = 0$ (dabei ist $\varepsilon_1: K[X] \xrightarrow{\sim} \varepsilon(K)[X]$ die Fortsetzung von ε auf die Polynomringe).

Sei **A** gezeigt und $L' = \varepsilon(K)(x_1) \subset L_1$. Dann ist $L'/\varepsilon(K)$ algebraisch, und aus 1. folgt

$$|L' \setminus \varepsilon(K)| \leq \max\{|\varepsilon(K)|, \omega\} = \max\{|K|, \omega\} < |\Sigma| = |\Sigma \setminus K|.$$

Daher gibt es eine injektive Abbildung $\varepsilon': L' \setminus \varepsilon(K) \rightarrow \Sigma \setminus K$. Sei $C = \varepsilon'(L' \setminus \varepsilon(K))$, $L = K \cup C$, und sei $\bar{\varepsilon}: L \rightarrow L'$ definiert durch $\bar{\varepsilon}|_C = \varepsilon'^{-1}$ und $\bar{\varepsilon}|_K = \varepsilon$. Dann ist $\bar{\varepsilon}$ bijektiv, und es gibt (genau) eine Körperstruktur auf L , so dass $\bar{\varepsilon}$ ein Körperisomorphismus ist. Dann ist $K \subset L$ ein Teilkörper, und für $x = \bar{\varepsilon}^{-1}(x_1)$ gilt $\bar{\varepsilon}(f(x)) = \bar{\varepsilon}_1(f)(\bar{\varepsilon}(x)) = \varepsilon_1(f)(x_1) = 0$, also auch $f(x) = 0$.

Beweis von A. Sei $f_1 \in K[X] \setminus K$ normiert und irreduzibel mit $f_1 \mid f$. Dann ist $L_1 = K[X]/f_1K[X]$ ein Körper, es sei $\varepsilon^*: K[X] \rightarrow L_1$ der Restklassenhomomorphismus, $x_1 = \varepsilon^*(X)$ und $\varepsilon = \varepsilon^*|_K$. Dann ist $\varepsilon_1(f_1)(x_1) = \varepsilon^*(f_1) = 0$, und wegen $\varepsilon_1(f_1) \mid \varepsilon_1(f)$ ist auch $\varepsilon_1(f)(x_1) = 0$. \square

Satz 3.3.5. *Für einen Körper K sind die folgenden Aussagen äquivalent:*

- (a) *Jedes (normierte) Polynom $f \in K[X] \setminus K$ hat eine Nullstelle in K .*
- (b) *Jedes $f \in K[X] \setminus K$ zerfällt über K in Linearfaktoren, d. h.,*

$$f = c \prod_{i=1}^n (X - x_i) \quad \text{mit } c \in K^\times, n \in \mathbb{N} \text{ und } x_1, \dots, x_n \in K.$$

- (c) *Jedes (normierte) irreduzible Polynom $f \in K[X] \setminus K$ ist linear [d. h., es ist $\text{gr}(f) = 1$.]*

(d) K hat keinen echten algebraischen Erweiterungskörper.

BEWEIS. (a) \Rightarrow (b) Induktion nach $n = \text{gr}(f)$. Im Falle $n = 1$ ist nichts zu zeigen.

$n \geq 2$, $n - 1 \rightarrow n$: Sei $\text{gr}(f) = n$ und $x_1 \in K$ mit $f(x_1) = 0$. Dann gibt es ein $f_1 \in K[X]$ mit $f = (X - x_1)f_1$, und wegen $\text{gr}(f_1) = n - 1$ folgt die Behauptung aus der Induktionsvoraussetzung.

(b) \Rightarrow (c) Klar.

(c) \Rightarrow (d) Sei L/K eine algebraische Körpererweiterung, $x \in L$ und $f \in K[X]$ das Minimalpolynom von x über K . Dann ist f normiert und irreduzibel, und wegen $\text{gr}(f) = 1$ ist $f = X - x$, also $x \in K$. Damit folgt $L = K$.

(d) \Rightarrow (a) Nach Satz 3.3.4.2 □

Definition 3.3.6. Sei K ein Körper.

1. K heißt *algebraisch abgeschlossen*, wenn K die Bedingungen von Satz 3.3.5 erfüllt.
2. Ein Oberkörper $L \supset K$ heißt *algebraischer Abschluss* oder *algebraische Hülle* von K , wenn L algebraisch abgeschlossen und L/K algebraisch ist.

Satz 3.3.7. Sei K ein Körper.

1. Sei $\varphi: K \rightarrow K'$ ein Körperhomomorphismus. L/K und L'/K' seien Körpererweiterungen, L/K sei algebraisch, und L' sei algebraisch abgeschlossen. Dann gibt es einen Körperhomomorphismus $\bar{\varphi}: L \rightarrow L'$ mit $\bar{\varphi}|_K = \varphi$.
2. K besitzt eine algebraische Hülle.
3. Sei $\varphi: K \rightarrow K'$ ein Körperisomorphismus, \bar{K} eine algebraische Hülle von K und \bar{K}' eine algebraische Hülle von K' . Dann gibt es einen Körperisomorphismus $\bar{\varphi}: \bar{K} \rightarrow \bar{K}'$ mit $\bar{\varphi}|_K = \varphi$. Sind insbesondere \bar{K} und \tilde{K} algebraische Hüllen von K , so gibt es einen K -Isomorphismus $\phi: \bar{K} \rightarrow \tilde{K}$.
4. Ist L/K eine algebraische Körpererweiterung und ist \bar{L} eine algebraische Hülle von L , so ist \bar{L} auch eine algebraische Hülle von K .
5. Sei $L \supset K$ ein algebraisch abgeschlossener Oberkörper von K und $\bar{K} = \text{Alg}_L(K)$. Dann ist \bar{K} eine algebraische Hülle von K .
6. Sei \bar{K} eine algebraische Hülle von K , sei $K \subset L \subset \bar{K}$ ein Zwischenkörper und $\varphi: L \rightarrow \bar{K}$ ein K -Homomorphismus. Dann gibt es ein $\sigma \in \text{Gal}(\bar{K}/K)$ mit $\sigma|_L = \varphi$. Insbesondere gilt: Sind $x, y \in \bar{K}$ konjugiert über K . Dann gibt es ein $\sigma \in \text{Gal}(\bar{K}/K)$ mit $\sigma(x) = y$.

BEWEIS. 1. Sei Ω die Menge aller Paare (L_1, φ_1) , bestehend aus einem Zwischenkörper $K \subset L_1 \subset L$ und einem Körperhomomorphismus $\varphi_1: L_1 \rightarrow L'$ mit $\varphi_1|_K = \varphi$ (dann ist $(K, \varphi) \in \Omega$, also $\Omega \neq \emptyset$). Für $(L_1, \varphi_1), (L_2, \varphi_2) \in \Omega$ definieren wir $(L_1, \varphi_1) \leq (L_2, \varphi_2)$, wenn $L_1 \subset L_2$ und $\varphi_2|_{L_1} = \varphi_1$. Dann ist (Ω, \leq) eine teilgeordnete Menge. Ist $\mathcal{S} = \{(L_\lambda, \varphi_\lambda) \mid \lambda \in \Lambda\}$ eine Kette in Ω , $L^* = \bigcup \{L_\lambda \mid \lambda \in \Lambda\}$ und $\varphi^* = \bigcup \{\varphi_\lambda \mid \lambda \in \Lambda\}$, so ist (L^*, φ^*) eine obere Schranke von \mathcal{S} in Ω . Daher besitzt Ω ein maximales Element (L^*, φ^*) , und es genügt, $L^* = L$ zu zeigen.

Sei $x \in L$. Dann ist x algebraisch über K , also auch über L^* , und es sei $f \in L^*[X]$ das Minimalpolynom von x über L^* . Sei $\varphi_1^*: L^*[X] \xrightarrow{\sim} \varphi^*(L^*)[X]$ die Fortsetzung von φ^* auf die Polynomringe. Dann ist auch $\varphi_1^*(f) \in \varphi^*(L^*)[X]$ irreduzibel, und da L' algebraisch abgeschlossen ist, gibt es ein $x_1 \in L'$ mit $\varphi_1^*(f)(x_1) = 0$. Nach Bemerkung 3.3.3.2 gibt es einen Isomorphismus $\bar{\varphi}^*: L^*(x) \xrightarrow{\sim} \varphi^*(L^*)(x_1) \hookrightarrow L'$ mit $\bar{\varphi}^*|_{L^*} = \varphi^*$ und $\bar{\varphi}^*(x) = x_1$. Dann ist $(L^*(x), \bar{\varphi}^*) \in \Omega$ und $(L^*, \varphi^*) \leq (L^*(x), \bar{\varphi}^*)$, also $L^*(x) = L^*$ und daher $x \in L^*$ wegen der Maximalität von (L^*, φ^*) .

2. Sei Σ eine Menge mit $K \subset \Sigma$ und $|\Sigma| > \max\{|K|, \omega\}$. Sei Ω die Klasse aller über K algebraischen Erweiterungskörper $L \supset K$ mit $L \subset \Sigma$ (Teilmenge). Jedes $L \in \Omega$ ist durch die Abbildung $L \times L \rightarrow L \times L$, $(x, y) \mapsto (x + y, xy)$ eindeutig bestimmt. Jede solche Abbildung ist eine Teilmenge von Σ^4 , und daher ist

$\Omega \subset \mathbb{P}(\Sigma^4)$ eine Menge. Für $L, L' \in \Omega$ sei $L \leq L'$, wenn $L \subset L'$ ein Teilkörper (nicht nur eine Teilmenge!) ist. Ist nun $\mathcal{L} \subset \Omega$ eine Kette, so ist $\bigcup \mathcal{L}$ eine obere Schranke von \mathcal{L} in Ω , und nach dem Zorn'schen Lemma besitzt Ω ein maximales Element L^* . Dann ist L^*/K algebraisch, also $|L^*| \leq \max\{|K|, \omega\} < |\Sigma|$ nach Satz 3.3.4.1, und wir zeigen, dass L^* algebraisch abgeschlossen ist. Sei $f \in L^*[X] \setminus L^*$ normiert. Nach Satz 3.3.4.2 gibt es eine Körpererweiterung L_1^*/L^* mit $L_1^* \subset \Sigma$ und ein $x \in L_1^*$ mit $f(x) = 0$. Dann ist $L^*(x) \in \Omega$ und $L^* \leq L^*(x)$, also $L^* = L^*(x)$ wegen der Maximalität von L^* und daher $x \in L^*$ eine Nullstelle von f .

3. Nach 1. gibt es Körperhomomorphismen $\bar{\varphi}: \bar{K} \rightarrow \bar{K}'$ mit $\bar{\varphi}|_K = \varphi$ und $\bar{\varphi}_1: \bar{K}' \rightarrow \bar{K}$ mit $\bar{\varphi}_1|_{K'} = \varphi^{-1}$. Dann sind $\bar{\varphi}_1 \circ \bar{\varphi} \in \text{Hom}_K(\bar{K}, \bar{K})$ und $\bar{\varphi} \circ \bar{\varphi}_1 \in \text{Hom}_{K'}(\bar{K}', \bar{K}')$ Isomorphismen nach Bemerkung 3.3.3.4, und daher ist auch $\bar{\varphi}$ ein Isomorphismus.

4. \bar{L} ist algebraisch über K nach Satz 3.3.2.1(b) und algebraisch abgeschlossen.

5. Nach Satz 3.3.2 ist \bar{K}/K eine algebraische Körpererweiterung. Sei $f \in \bar{K}[X] \setminus \bar{K}$. Dann gibt es ein $\alpha \in L$ mit $f(\alpha) = 0$, α ist algebraisch über \bar{K} , also auch über K , und daher ist $\alpha \in \bar{K}$. Nach Satz 3.3.5 ist \bar{K} algebraisch abgeschlossen.

6. Nach 1. und Bemerkung 3.3.3.4 gibt es ein $\sigma \in \text{Hom}_K(\bar{K}, \bar{K}) = \text{Gal}(\bar{K}/K)$ mit $\sigma|_L = \varphi$. Sind $x, y \in \bar{K}$ konjugiert über K , so gibt es einen K -Homomorphismus $\varphi: K(x) \xrightarrow{\sim} K(y) \hookrightarrow \bar{K}$ mit $\varphi(x) = y$ (nach Bemerkung 3.3.3.2) und daher ein $\sigma \in \text{Gal}(\bar{K}/K)$ mit $\sigma|_{K(x)} = \varphi$, also $\sigma(x) = y$. \square

Satz 3.3.8. *Sei R ein Bereich, $K = \mathfrak{q}(R)$ und L/K eine Körpererweiterung.*

1. $\text{Alg}_L(K) = R^{\bullet-1} \text{Ganz}_L(R)$ [ein Element $x \in L$ ist genau dann algebraisch über K , wenn es ein $q \in R^\bullet$ gibt, so dass qx ganz über R ist].
2. Sei $R \subset S \subset L$ ein Teilring, $L = \mathfrak{q}(S)$ und S/R eine ganze Ringerweiterung. Dann ist L/K algebraisch.
3. Sei $x \in L$ algebraisch über K , $f \in K[X]$ das Minimalpolynom von x über K und $\bar{R} = \text{Ganz}_K(R)$. Genau dann ist x ganz über R , wenn $f \in \bar{R}[X]$.

BEWEIS. 1. Nach Satz 3.2.4 ist $R^{\bullet-1} \text{Ganz}_L(R) = \text{Ganz}_{R^{\bullet-1}L}(R^{\bullet-1}R) = \text{Ganz}_L(K) = \text{Alg}_L(K)$.

2. S ist ganz über R , also auch algebraisch über K . Daher ist $S \subset \text{Alg}_L(K)$. Da $\text{Alg}_L(K)$ ein Körper ist, folgt $L = \mathfrak{q}(S) \subset \text{Alg}_L(K)$, und daher ist L/K algebraisch.

3. Wir können annehmen, dass L/K algebraisch ist. Sei \bar{L} eine algebraische Hülle von L (also auch von K), und seien $x_2, \dots, x_n \in \bar{L}$ mit $f = (X-x)(X-x_2) \cdots (X-x_n)$. Dann ist $f \in R[x, x_2, \dots, x_n][X]$, und nach Satz 3.3.7.4 gibt es für jedes $i \in [2, n]$ ein $\sigma_i \in \text{Gal}(\bar{L}/K)$ mit $x_i = \sigma_i(x)$. Ist $f \in \bar{R}[X]$, so ist x ganz über \bar{R} und nach Satz 3.1.4.4 auch über R .

Sei nun x ganz über R und $g \in R[X]$ ein normiertes Polynom mit $g(x) = 0$. Für $i \in [2, n]$ ist $0 = \sigma_i(g(x)) = g(x_i)$, also x_i ganz über R . Die Koeffizienten von f liegen in $R[x, x_2, \dots, x_n] \cap K$, sind also ganz über R und liegen daher in \bar{R} . \square

3.4. Transzendente Körpererweiterungen

Lemma 3.4.1.

1. Sei F ein freies abelsches Monoid mit Basis $P \neq \emptyset$. Dann ist $|F| = \max\{|P|, \omega\}$.
2. Sei $R \neq \mathbf{0}$ ein kommutativer Ring und $R[\mathbf{X}]$ der Polynomring in der Familie $\mathbf{X} = (X_i)_{i \in I}$ mit $I \neq \emptyset$. Dann ist $|R[\mathbf{X}]| = \max\{|R|, |I|, \omega\}$.
3. Ist R ein Bereich, so ist $|\mathfrak{q}(R)| = |R|$.

BEWEIS. 1. Wegen $F \cong \mathbb{N}_0^{(P)}$ können wir $F = \mathbb{N}_0^{(P)} \subset \mathbb{Z}^{(P)}$ annehmen. Nach Satz 2.3.6 ist $|\mathbb{Z}^{(P)}| = \max\{|P|, \omega\}$. Die Abbildung $\mathbb{N}_0^{(P)} \times \mathbb{N}_0^{(P)} \rightarrow \mathbb{Z}^{(P)}$, $(x, y) \mapsto x - y$, ist surjektiv, und $|\mathbb{N}_0^{(P)}| \geq \omega$. Daher folgt $|\mathbb{N}_0^{(P)}| \leq |\mathbb{Z}^{(P)}| \leq |\mathbb{N}_0^{(P)} \times \mathbb{N}_0^{(P)}| = |\mathbb{N}_0^{(P)}|$, also $|F| = |\mathbb{N}_0^{(P)}| = \max\{|P|, \omega\}$.

2. Ist $[\mathbf{X}]$ das freie abelsche Monoid mit Basis $\{X_i \mid i \in I\}$, so ist $R[\mathbf{X}]$ ein freier R -Modul mit der unendlichen Basis $[\mathbf{X}]$. Nach Satz 2.3.6 und 1. folgt $|R[\mathbf{X}]| = \max\{|R|, |[X]|\} = \max\{|R|, |I|, \omega\}$.

3. Ist R endlich, so ist $\mathfrak{q}(R) = R$. Ist R unendlich, so ist die Abbildung $R^\bullet \times R \rightarrow \mathfrak{q}(R)$, $(x, y) \mapsto x^{-1}y$, surjektiv, und es folgt $|R| \leq |\mathfrak{q}(R)| \leq |R^\bullet \times R| = |R|$. \square

Definition 3.4.2. Eine Familie $\mathbf{x} = (x_i)_{i \in I}$ in L heißt *Transzendenzbasis* von L/K , wenn \mathbf{x} über K algebraisch unabhängig und $L/K(\mathbf{x})$ algebraisch ist. Ist $(x_i)_{i \in I}$ eine Transzendenzbasis von L/K , so nennt man $\text{tr}(L/K) = |I|$ den *Transzendenzgrad* von L/K (siehe Satz 3.4.4). Eine Menge $B \subset L$ heißt *Transzendenzbasis* von L/K , wenn die Familie $(b)_{b \in B}$ eine Transzendenzbasis ist.

Satz 3.4.3. Sei L/K eine Körpererweiterung. Für eine Teilmenge $Z \subset L$ sei $\mathfrak{h}(Z) = \text{Alg}_L K(Z)$.

1. Für $Z \subset L$ und $u \in L$ sind äquivalent:

(a) $u \in \mathfrak{h}(Z)$.

(b) Es gibt eine endliche Teilmenge $E \subset Z$ und ein Polynom $f \in K[E][X]^\bullet$ mit $f(u) = 0$.

(c) Es gibt ein Polynom $F \in K[X_1, \dots, X_n, X]$ und $z_1, \dots, z_n \in Z$, so dass $F(z_1, \dots, z_n, X) \neq 0$ und $F(z_1, \dots, z_n, u) = 0$.

2. $\mathfrak{h}: \mathbb{P}(L) \rightarrow \mathbb{P}(L)$ ist eine Hüllenoperation.

3. Für eine Teilmenge $B \subset L$ gilt:

(a) B ist genau dann \mathfrak{h} -unabhängig, wenn B algebraisch unabhängig über K ist.

(b) B ist genau dann ein \mathfrak{h} -Erzeugendensystem, wenn $L/K(B)$ algebraisch ist.

BEWEIS. 1. (a) \Rightarrow (b) Sei $f \in K(Z)[X]^\bullet$ mit $f(u) = 0$. Nach Multiplikation mit dem Hauptnenner der Koeffizienten können wir $f \in K[Z][X]^\bullet$ annehmen, und dann gibt es eine endliche Teilmenge $E \subset Z$ mit $f \in K[E][X]^\bullet$.

(b) \Rightarrow (c) Sei $E = \{z_1, \dots, z_n\}$. Dann ist

$$f = \sum_{\nu \geq 0} f_\nu(z_1, \dots, z_n) X^\nu \quad \text{mit} \quad f_\nu \in K[X_1, \dots, X_n], \quad f_\nu = 0 \quad \text{für fast alle } \nu \geq 0, \quad \text{und} \quad F = \sum_{\nu \geq 0} f_\nu X^\nu$$

leistet das Gewünschte.

(c) \Rightarrow (a) Es ist $F(z_1, \dots, z_n, X) \in K(Z)[X]^\bullet$.

2. Seien $Z, Z' \subset L$ und $u, v \in L$.

H1. $Z \subset \mathfrak{h}(Z)$: Offensichtlich.

H2. Aus $Z \subset \mathfrak{h}(Z')$ folgt $\mathfrak{h}(Z) \subset \mathfrak{h}(Z')$: Sei $Z \subset \text{Alg}_L K(Z')$ und $x \in \text{Alg}_L K(Z)$. Dann ist $K(Z) \subset \text{Alg}_L K(Z')$, also x auch algebraisch über $\text{Alg}_L K(Z')$ und daher $x \in \text{Alg}_L K(Z')$.

H3. $\mathfrak{h}(Z) = \bigcup \{\mathfrak{h}(E) \mid E \subset Z \text{ endlich}\}$: Nach 1.(b).

H4. Ist $v \in \mathfrak{h}(Z \cup \{u\}) \setminus \mathfrak{h}(Z)$, so folgt $u \in \mathfrak{h}(Z \cup \{v\})$: Sei $K' = K(Z)$. Dann müssen wir zeigen: Aus $v \in \text{Alg}_L K'(u) \setminus \text{Alg}_L K'$ folgt $u \in \text{Alg}_L K'(v)$. Wegen $v \in \text{Alg}_L K'(u)$ gibt es nach 1. ein Polynom $F \in K'[U, V]$ mit $F(u, V) \neq 0$ und $F(u, v) = 0$, und es ist $F(U, v) \neq 0$ zu zeigen (denn dann ist $u \in \text{Alg}_L K'(v)$). Sei

$$F = \sum_{\nu \geq 0} g_\nu(V) U^\nu \quad \text{mit} \quad g_\nu(V) \in K'[V], \quad g_\nu(V) = 0 \quad \text{für fast alle } \nu \geq 0, \quad \text{und} \quad F(U, v) = \sum_{\nu \geq 0} g_\nu(v) U^\nu = 0.$$

Dann ist $g_\nu(v) = 0$ und daher $g_\nu(V) = 0$ für alle $\nu \geq 0$, da $v \notin \text{Alg}_L K'$. Damit folgt $F = 0$, ein Widerspruch.

3.(a) Sei B algebraisch abhängig über K und $\{b_1, \dots, b_n\} \subset B$ eine minimale über K algebraisch abhängige Teilmenge von B . Sei $F \in K[X_1, \dots, X_n]^\bullet$ mit $F(b_1, \dots, b_n) = 0$. Sei

$$F = \sum_{\nu \geq 0} F_\nu(X_1, \dots, X_{n-1})X_n^\nu \quad \text{mit} \quad F_\nu \in K[X_1, \dots, X_{n-1}], \quad F_\nu = 0 \quad \text{für fast alle } \nu \geq 0.$$

Sei $\nu \geq 0$ mit $F_\nu \neq 0$. Da $\{b_1, \dots, b_{n-1}\}$ über K algebraisch unabhängig ist, folgt $F_\nu(b_1, \dots, b_{n-1}) \neq 0$, also auch $F(b_1, \dots, b_{n-1}, X_n) \neq 0$. Nach 1. ist daher $b_n \in \mathfrak{h}(B \setminus \{b_n\})$, und nach Lemma 2.3.4 ist B nicht \mathfrak{h} -unabhängig.

Sei nun B nicht \mathfrak{h} -unabhängig. Nach Lemma 2.3.4 gibt es ein $b \in B$ mit $b \in \mathfrak{h}(B \setminus \{b\})$, und nach 1. gibt es ein Polynom $F \in K[X_1, \dots, X_n, X]$ und $b_1, \dots, b_n \in B \setminus \{b\}$, so dass $F(b_1, \dots, b_n, X) \neq 0$ und $F(b_1, \dots, b_n, b) = 0$. Insbesondere ist (b_1, \dots, b_n, b) und daher auch B algebraisch abhängig über K .

3.(b) B ist ein \mathfrak{h} -Erzeugendensystem $\iff L = \text{Alg}_L(K(B)) \iff L/K(B)$ ist algebraisch. \square

Satz 3.4.4 (Satz von der Transzendenzbasis). *Sei L/K eine Körpererweiterung.*

1. L/K besitzt eine Transzendenzbasis, und je zwei Transzendenzbasen von L/K sind gleichmächtig. Genauer gilt: Ist $B \subset W \subset L$, so dass B über K algebraisch unabhängig und $L/K(W)$ algebraisch ist, so gibt es eine Transzendenzbasis B^* von L/K mit $B \subset B^* \subset W$. Insbesondere gilt: Ist $L = K(W)$, so gibt es eine Transzendenzbasis B^* von L/K mit $B^* \subset W$.
2. $|L| = \max\{|K|, |\text{tr}(L/K)|, \omega\}$.
3. Sei $K \subset M \subset L$ ein Zwischenkörper, B eine Transzendenzbasis von M/K und C eine Transzendenzbasis von L/M . Dann ist $B \cap C = \emptyset$, und $B \cup C$ ist eine Transzendenzbasis von L/K . Insbesondere folgt $\text{tr}(L/K) = \text{tr}(L/M) + \text{tr}(M/K)$.

BEWEIS. 1. Nach Satz 3.4.3 und Satz 2.3.5.

2. Sei $\mathbf{x} = (x_i)_{i \in I}$ eine Transzendenzbasis von L/K und $K[\mathbf{X}]$ der Polynomring in $\mathbf{X} = (X_i)_{i \in I}$. Nach Bemerkung 3.3.1.4 ist $K(\mathbf{x}) \cong K(\mathbf{X}) = \mathfrak{q}(K[\mathbf{X}])$, und nach Lemma 3.4.1 ist

$$|K(\mathbf{x})| = |K(\mathbf{X})| = |K[\mathbf{X}]| = \max\{|K|, |I|, \omega\} = \max\{|K|, \text{tr}(L/K), \omega\}.$$

$L/K(\mathbf{x})$ ist algebraisch, und nach Satz 3.3.4 folgt $|L| = |K(\mathbf{x})|$.

3. Wir zeigen: **1)** $B \cup C$ ist algebraisch unabhängig über K . **2)** $L/K(B \cup C)$ ist algebraisch.

1) Durch Widerspruch. Sei $B \cup C$ algebraisch abhängig über K . Dann gibt es endliche Teilmengen $B_1 \subset B$ und $C_1 \subset C$, so dass $B_1 \cup C_1$ algebraisch abhängig über K ist. Da B und C beide über K algebraisch unabhängig sind, ist $B_1 \neq \emptyset$ und $C_1 \neq \emptyset$. Sei $B_1 = \{b_1, \dots, b_n\}$ und $C_1 = \{c_1, \dots, c_m\}$ mit $m, n \in \mathbb{N}$, $\mathbf{b} = (b_1, \dots, b_n)$ und $\mathbf{c} = (c_1, \dots, c_m)$. Sei $\mathbf{X} = (X_1, \dots, X_n)$, $\mathbf{Y} = (Y_1, \dots, Y_m)$ und $K[\mathbf{X}, \mathbf{Y}]$ der Polynomring in (\mathbf{X}, \mathbf{Y}) . Dann gibt es ein $F \in K[\mathbf{X}, \mathbf{Y}]^\bullet$ mit $F(\mathbf{b}, \mathbf{c}) = 0$. Wegen $F(\mathbf{b}, \mathbf{Y}) \in M[\mathbf{Y}]$, und da \mathbf{c} algebraisch unabhängig über M ist, folgt $F(\mathbf{b}, \mathbf{Y}) = 0$. Sei nun

$$F = \sum_{\boldsymbol{\mu} \in \mathbb{N}_0^m} c_{\boldsymbol{\mu}}(\mathbf{X})\mathbf{Y}^{\boldsymbol{\mu}} \quad \text{mit} \quad c_{\boldsymbol{\mu}}(\mathbf{X}) \in K[\mathbf{X}], \quad c_{\boldsymbol{\mu}} = 0 \quad \text{für fast alle } \boldsymbol{\mu} \in \mathbb{N}_0^m$$

(wobei $(Y_1, \dots, Y_m)^{(\mu_1, \dots, \mu_m)} = Y_1^{\mu_1} \cdot \dots \cdot Y_m^{\mu_m}$). Dann ist $c_{\boldsymbol{\mu}}(\mathbf{b}) = 0$ für alle $\boldsymbol{\mu} \in \mathbb{N}_0^m$, aber es gibt ein $\boldsymbol{\mu} \in \mathbb{N}_0^m$ mit $c_{\boldsymbol{\mu}} \neq 0$. Daher ist \mathbf{b} algebraisch abhängig über K , ein Widerspruch.

2) Die Körpererweiterungen $L/M(C)$ und $M/K(B)$ sind algebraisch. Nach Satz 3.3.2.5 ist auch $MK(B \cup C)/K(B \cup C)$ algebraisch. Aber $MK(B \cup C) = M(C)$, und nach Satz 3.3.2.1(b) ist auch $L/K(B \cup C)$ algebraisch. \square

3.5. Affine Algebren: Normalisierungssatz und Nullstellensatz

Satz 3.5.1 (Noether'scher Normalisierungssatz). *Sei K ein Körper, $n \in \mathbb{N}_0$, $A = K[x_1, \dots, x_n]$ eine affine K -Algebra, $\mathfrak{a} \triangleleft A$, $\mathfrak{a} \neq A$.*

1. *Es existieren $\delta, d \in \mathbb{N}_0$ mit $\delta \leq d \leq n$ und $t_1, \dots, t_d \in A$, so dass gilt:*
 - 1) *(t_1, \dots, t_d) ist algebraisch unabhängig über K .*
 - 2) *A ist ganz über $K[t_1, \dots, t_d]$.*
 - 3) *$\mathfrak{a} \cap K[t_1, \dots, t_d] = K[t_1, \dots, t_d] \langle t_{d+1}, \dots, t_d \rangle$.*
2. *Sind die Bedingungen in 1. erfüllt, so ist $d = \dim(A)$ und $\delta = \dim(A/\mathfrak{a})$. Insbesondere sind die Zahlen d und δ eindeutig bestimmt. Ist A ein Bereich und $L = \mathfrak{q}(A)$, so ist $d = \text{tr}(L/K)$.*

BEWEIS. 1. I. SPEZIALFALL: (x_1, \dots, x_n) ist algebraisch unabhängig über K . Wir zeigen mittels Induktion nach n :

Es gibt über K algebraisch unabhängige Elemente $t_1, \dots, t_n \in A$ und ein $d \in [0, n]$, so dass $A \supset K[t_1, \dots, t_n]$ ganz ist, und $\mathfrak{a} \cap K[t_1, \dots, t_n] = K[t_1, \dots, t_n] \langle t_{d+1}, \dots, t_n \rangle$.

Wir können annehmen, dass $A = K[X_1, \dots, X_n]$ ein Polynomring ist. Im Falle $n = 0$ ist $A = K$ und nichts zu zeigen. Ist $\mathfrak{a} = \mathbf{0}$, so setzt man $d = n$ und $(t_1, \dots, t_n) = (X_1, \dots, X_n)$. Sei also $\mathfrak{a} \neq \mathbf{0}$.

$n \geq 1$, $n-1 \rightarrow n$: Sei $F \in \mathfrak{a} \setminus K$, und $\mathfrak{a} = {}_A \langle F \rangle$, falls $n = 1$. Sei nun $k \in \mathbb{N}$, so dass

$$F = \sum_{\nu_1, \dots, \nu_n \in [0, k-1]} a_{\nu_1, \dots, \nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \quad \text{mit } a_{\nu_1, \dots, \nu_n} \in K.$$

Für $i \in [1, n-1]$ sei $Y_i = X_i - X_n^{k^i}$. Dann ist $A = K[Y_1, \dots, Y_{n-1}, X_n]$, und es folgt

$$\begin{aligned} F &= \sum_{\nu_1, \dots, \nu_n \in [0, k-1]} a_{\nu_1, \dots, \nu_n} (Y_1 + X_n^k)^{\nu_1} (Y_2 + X_n^{k^2})^{\nu_2} \cdots (Y_{n-1} + X_n^{k^{n-1}})^{\nu_{n-1}} X_n^{\nu_n} \\ &= \sum_{\nu_1, \dots, \nu_n \in [0, k-1]} a_{\nu_1, \dots, \nu_n} (X_n^{\nu_n + \nu_1 k + \nu_2 k^2 + \dots + \nu_{n-1} k^{n-1}} + g_{\nu_1, \dots, \nu_n}(Y_1, \dots, Y_{n-1}, X_n)), \end{aligned}$$

wobei für alle $(\nu_1, \dots, \nu_n) \in [0, k-1]^n$ das Polynom $g_{\nu_1, \dots, \nu_n}(Y_1, \dots, Y_{n-1}, X_n) \in K[Y_1, \dots, Y_{n-1}][X_n]$ in X_n einen Grad $d_n < \nu_n + \nu_1 k + \nu_2 k^2 + \dots + \nu_{n-1} k^{n-1}$ hat. Ist nun

$$m = \max\{\nu_n + \nu_1 k + \nu_2 k^2 + \dots + \nu_{n-1} k^{n-1} \mid (\nu_1, \dots, \nu_n) \in [0, k-1]^n, a_{\nu_1, \dots, \nu_n} \neq 0\},$$

$m = \nu'_n + \nu'_1 k + \nu'_2 k^2 + \dots + \nu'_{n-1} k^{n-1}$ mit $(\nu'_1, \dots, \nu'_n) \in [0, k-1]^n$ und $a = a_{\nu'_1, \dots, \nu'_n} \in K^\times$, so folgt

$$F = aX_n^m + \rho_{m-1}X_n^{m-1} + \dots + \rho_1X_n + \rho_0 \quad \text{mit } \rho_\mu \in K[Y_1, \dots, Y_{n-1}].$$

Daher ist $X_n^m + a^{-1}\rho_{m-1}X_n^{m-1} + \dots + a^{-1}\rho_1X_n + a^{-1}(\rho_0 - F) = 0$ eine ganze Gleichung für X_n über $K[Y_1, \dots, Y_{n-1}, F]$, und daher ist $A = K[Y_1, \dots, Y_{n-1}, X_n]$ ganz über $K[Y_1, \dots, Y_{n-1}, F]$. Nach Satz 3.3.8.2 ist $K(X_1, \dots, X_n)/K(Y_1, \dots, Y_{n-1}, F)$ algebraisch und daher

$$n = \text{tr}(K(X_1, \dots, X_n)/K) = \text{tr}(K(Y_1, \dots, Y_{n-1}, F)/K).$$

Nach Satz 3.4.4.1 ist (Y_1, \dots, Y_{n-1}, F) und daher (Y_1, \dots, Y_{n-1}) algebraisch unabhängig über K , und $\mathfrak{a} \cap K[Y_1, \dots, Y_{n-1}] \triangleleft K[Y_1, \dots, Y_{n-1}]$. Nach Induktionsvoraussetzung existieren ein $d \in [0, n-1]$ und $t_1, \dots, t_{n-1} \in K[Y_1, \dots, Y_{n-1}]$, so dass gilt: (t_1, \dots, t_{n-1}) ist algebraisch unabhängig über K , $K[Y_1, \dots, Y_{n-1}] \supset K[t_1, \dots, t_{n-1}]$ ist ganz, und $\mathfrak{a} \cap K[t_1, \dots, t_{n-1}] = K[t_1, \dots, t_{n-1}] \langle t_{d+1}, \dots, t_{n-1} \rangle$. Daher sind $K[t_1, \dots, t_{n-1}, F] \subset K[Y_1, \dots, Y_{n-1}, F] \subset A$ ganze Ringerweiterungen, und nach Satz 3.1.4 ist auch $A/K[t_1, \dots, t_{n-1}, F]$ ganz. Daher ist $K(X_1, \dots, X_n)/K(Y_1, \dots, Y_{n-1}, F)$ algebraisch und (t_1, \dots, t_{n-1}, F) algebraisch unabhängig über K .

Es ist nun noch $\mathfrak{a} \cap K[t_1, \dots, t_{n-1}, F] = K[t_1, \dots, t_{n-1}, F] \langle t_{d+1}, \dots, t_{n-1}, F \rangle$ zu zeigen (dann setze man $t_n = F$, und es folgt die Behauptung des Spezialfalles). Die Inklusion \supset ist offensichtlich. Sei also

$f \in \mathfrak{a} \cap K[t_1, \dots, t_{n-1}, F]$. Dann ist $f = f_0 + FG$ mit $f_0 \in K[t_1, \dots, t_{n-1}]$ und $G \in K[t_1, \dots, t_{n-1}, F]$. Wegen $F \in \mathfrak{a}$ ist dann

$$f_0 = f - FG \in \mathfrak{a} \cap K[t_1, \dots, t_{n-1}] = K[t_1, \dots, t_{n-1}] \langle t_{d+1}, \dots, t_{n-1} \rangle \subset K[t_1, \dots, t_{n-1}, F] \langle t_{d+1}, \dots, t_{n-1}, F \rangle$$

und daher auch $f \in K[t_1, \dots, t_{n-1}, F] \langle t_{d+1}, \dots, t_{n-1}, F \rangle$.

II. ALLGEMEINER FALL: Sei $K[X_1, \dots, X_n]$ ein Polynomring und $\pi: K[X_1, \dots, X_n] \rightarrow A$ der K -Algebren-Epimorphismus mit $\pi(X_i) = x_i$ für alle $i \in [1, n]$. Sei $\mathfrak{c} = \text{Ker}(\pi) \triangleleft K[X_1, \dots, X_n]$. Nach I. gibt es $Y_1, \dots, Y_n \in K[X_1, \dots, X_n]$ und ein $d \in [0, n]$, so dass gilt:

(Y_1, \dots, Y_n) ist algebraisch unabhängig über K , $K[X_1, \dots, X_n] \supset K[Y_1, \dots, Y_n]$ ist ganz, und $\mathfrak{c} \cap K[Y_1, \dots, Y_n] = K[Y_1, \dots, Y_n] \langle Y_{d+1}, \dots, Y_n \rangle$.

Für $i \in [1, d]$ sei $y_i = \pi(Y_i)$. Dann ist $A = \pi(K[X_1, \dots, X_n]) \supset \pi(K[Y_1, \dots, Y_n]) = K[y_1, \dots, y_d]$ ganz, und $\pi_d = \pi|_{K[Y_1, \dots, Y_d]}: K[Y_1, \dots, Y_d] \xrightarrow{\sim} K[y_1, \dots, y_d]$ ist ein K -Algebrenepimorphismus mit Kern

$$\mathfrak{c} \cap K[Y_1, \dots, Y_d] = K[Y_1, \dots, Y_n] \langle Y_{d+1}, \dots, Y_n \rangle \cap K[Y_1, \dots, Y_d] = \mathbf{0}.$$

Daher ist π_d ein K -Isomorphismus, und (y_1, \dots, y_d) ist algebraisch unabhängig über K . Nach I. gibt es $t_1, \dots, t_d \in K[y_1, \dots, y_d]$ und ein $\delta \in [0, d]$, so dass gilt:

(t_1, \dots, t_d) ist algebraisch unabhängig über K , $K[y_1, \dots, y_d] \supset K[t_1, \dots, t_d]$ ist ganz, und $\mathfrak{a} \cap K[t_1, \dots, t_d] = K[t_1, \dots, t_d] \langle t_{\delta+1}, \dots, t_d \rangle$.

Dann ist aber auch $A \supset K[t_1, \dots, t_d]$ ganz.

2. Sei $\rho: A \rightarrow A/\mathfrak{a}$ der Restklassenhomomorphismus. Dann ist

$$\text{Ker}(\rho|_{K[t_1, \dots, t_d]}) = K[t_1, \dots, t_d] \cap \mathfrak{a} = K[t_1, \dots, t_d] \langle t_{\delta+1}, \dots, t_d \rangle$$

und daher $\rho(K[t_1, \dots, t_d]) \cong K[t_1, \dots, t_d]/K[t_1, \dots, t_d] \langle t_{\delta+1}, \dots, t_d \rangle \cong K[t_1, \dots, t_\delta]$. Da $A \supset K[t_1, \dots, t_d]$ ganz ist, ist auch $A/\mathfrak{a} \supset \rho(K[t_1, \dots, t_d])$ ganz, und nach Satz 3.1.7.7 ist $\dim(A) = \dim(K[t_1, \dots, t_d])$ und $\dim(A/\mathfrak{a}) = \dim(\rho(K[t_1, \dots, t_d])) = \dim(K[t_1, \dots, t_\delta])$.

Ist A ein Bereich und $L = \mathfrak{q}(A)$, so ist $L/K(t_1, \dots, t_d)$ algebraisch, da $A/K[t_1, \dots, t_d]$ ganz ist, und damit folgt $\text{tr}(L/K) = \text{tr}(K(t_1, \dots, t_d)/K) = d$. Daher bleibt zu zeigen:

A. Ist $A = K[t_1, \dots, t_n]$ und ist (t_1, \dots, t_n) algebraisch unabhängig über K , so ist $\dim(A) = n$.

Beweis von A. Induktion nach n . Im Falle $n = 0$ ist $A = K$ und $\dim(A) = 0$. Sei also $n \geq 1$, und gelte die Behauptung für Algebren mit weniger als n algebraisch unabhängigen Erzeugenden. Wir können annehmen, dass $A = K[X_1, \dots, X_n]$ ein Polynomring ist.

Für $i \in [1, n]$ ist $K[X_1, \dots, X_n]/A \langle X_1, \dots, X_i \rangle \cong K[X_{i+1}, \dots, X_n]$, und daher ist

$$\mathbf{0} \subsetneq A \langle X_1 \rangle \subsetneq A \langle X_1, X_2 \rangle \subsetneq \dots \subsetneq A \langle X_1, \dots, X_n \rangle \subsetneq A$$

eine Folge in $\text{spec}(A)$, also $\dim(A) \geq n$. Sei nun $k \in \mathbb{N}$ und $\mathbf{0} \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_k \subsetneq A$ eine Folge in $\text{spec}(A)$. Dann müssen wir $k \leq n$ zeigen. Sei $B = A/\mathfrak{p}_1$, $\pi: A \rightarrow B$ der Restklassenhomomorphismus und $x_i = \pi(X_i)$ für alle $i \in [1, n]$. Dann ist $\pi|_K = \text{id}_K$, $B = K[x_1, \dots, x_n]$ ist eine affine K -Algebra und ein Bereich, und $\mathbf{0} \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_k/\mathfrak{p}_1 \subsetneq B$ ist eine Folge in $\text{spec}(B)$. Daher ist $\dim(B) \geq k-1$.

Nach 1. gibt es $y_1, \dots, y_n \in A$ und ein $d \in [0, n]$, so dass gilt: (y_1, \dots, y_n) ist algebraisch unabhängig über K , $A \supset R = K[y_1, \dots, y_n]$ ist ganz, und $\mathfrak{p}_1 \cap R = {}_R \langle y_{d+1}, \dots, y_n \rangle$. Nach Satz 3.1.7.1 ist $\mathfrak{p}_1 \cap R \neq \mathbf{0}$ und daher $d < n$. Da $A \supset R$ ganz ist, ist auch $B \supset \pi(R)$ ganz, und $\pi(R) \cong R/\mathfrak{p}_1 \cap R \cong K[y_1, \dots, y_d]$. Nach Induktionsvoraussetzung ist $d = \dim(K[y_1, \dots, y_d]) = \dim(\pi(R)) = \dim(B) \geq k-1$ und daher $k \leq d+1 \leq n$. \square

Satz 3.5.2. Sei $R \subset A$ eine Ringerweiterung, R ein Bereich, $n \in \mathbb{N}_0$ und $A = R[x_1, \dots, x_n]$. Dann existieren ein $d \in [0, n]$, $t_1, \dots, t_d \in A$ und $s \in R^\bullet$, so dass gilt: (t_1, \dots, t_d) ist algebraisch unabhängig über R , und ist $B = R[t_1, \dots, t_d] \subset A$, so ist $[s]^{-1}A \supset [s]^{-1}B$ ganz.

BEWEIS. Sei $K = \mathfrak{q}(R) = R^{\bullet-1}R$. Dann ist $R^{\bullet-1}A = K\left[\frac{x_1}{1}, \dots, \frac{x_d}{1}\right]$ eine affine K -Algebra, und nach Satz 3.5.1 gibt es ein $d \in [0, n]$ und über K algebraisch unabhängige Elemente $t'_1, \dots, t'_d \in R^{\bullet-1}A$, so dass $R^{\bullet-1}A \supset K[t'_1, \dots, t'_d]$ ganz ist. Für $i \in [1, d]$ sei $t'_i = \frac{t_i}{w}$ mit $t_i \in A$ und $w \in R^\bullet$, und es sei $B = R[t_1, \dots, t_d] \subset A$. Wir zeigen:

A. Es ist $K[t'_1, \dots, t'_d] = R^{\bullet-1}B$, und (t_1, \dots, t_d) ist algebraisch unabhängig über R .

Beweis von A. $R^{\bullet-1}B$ ist eine K -Algebra und $\{t'_1, \dots, t'_d\} \subset R^{\bullet-1}B$, also $K[t'_1, \dots, t'_d] \subset R^{\bullet-1}B$. Ist $f \in R^{\bullet-1}B$, so ist f von der Form

$$\begin{aligned} f &= \frac{\sum_{\nu_1, \dots, \nu_d \leq N} c_{\nu_1, \dots, \nu_d} t_1^{\nu_1} \cdots t_d^{\nu_d}}{v} = \sum_{\nu_1, \dots, \nu_d \leq N} \frac{c_{\nu_1, \dots, \nu_d}}{v} \left(\frac{t_1}{1}\right)^{\nu_1} \cdots \left(\frac{t_d}{1}\right)^{\nu_d} \\ &= \sum_{\nu_1, \dots, \nu_d \leq N} \frac{c_{\nu_1, \dots, \nu_d} w^{\nu_1 + \dots + \nu_d}}{v} \left(\frac{t_1}{w}\right)^{\nu_1} \cdots \left(\frac{t_d}{w}\right)^{\nu_d} = \sum_{\nu_1, \dots, \nu_d \leq N} \frac{c_{\nu_1, \dots, \nu_d} w^{\nu_1 + \dots + \nu_d}}{v} t_1^{\nu_1} \cdots t_d^{\nu_d} \end{aligned}$$

mit $N \in \mathbb{N}$, $c_{\nu_1, \dots, \nu_d} \in R$ und $v \in R^\bullet$, also $f \in K[t'_1, \dots, t'_d]$. Für den Nachweis der algebraischen Unabhängigkeit von (t_1, \dots, t_d) nehmen wir an, es bestehe in B eine Relation der Form

$$\sum_{\nu_1, \dots, \nu_d \leq N} c_{\nu_1, \dots, \nu_d} t_1^{\nu_1} \cdots t_d^{\nu_d} = 0 \quad \text{mit } c_{\nu_1, \dots, \nu_d} \in R.$$

Dann folgt (in $R^{\bullet-1}B = K[t'_1, \dots, t'_d]$)

$$\frac{0}{1} = \sum_{\nu_1, \dots, \nu_d \leq N} \frac{c_{\nu_1, \dots, \nu_d} w^{\nu_1 + \dots + \nu_d}}{1} \left(\frac{t_1}{w}\right)^{\nu_1} \cdots \left(\frac{t_d}{w}\right)^{\nu_d}, \quad \text{also } \frac{c_{\nu_1, \dots, \nu_d} w^{\nu_1 + \dots + \nu_d}}{1} = \frac{0}{1} \in K$$

und daher $c_{\nu_1, \dots, \nu_d} = 0$ für alle $\nu_1, \dots, \nu_d \leq N$. Damit ist **A** gezeigt.

Nach Satz 3.2.4 ist $R^{\bullet-1}A = \text{Ganz}_{R^{\bullet-1}A}(R^{\bullet-1}B) = R^{\bullet-1}\text{Ganz}_A(B)$ und daher $\frac{x_i}{1} = \frac{y_i}{s'} \in R^{\bullet-1}A$ mit $s' \in R^\bullet$ und $y_i \in \text{Ganz}_A(B)$ für alle $i \in [1, d]$. Dann gibt es ein $s_i \in R^\bullet$ mit $s_i s' x_i = s_i y_i$. Sei nun $s'' = s_1 \cdots s_d$ und $s = s' s''$. Dann folgt $s x_i = s'' y_i$, und daher (in $[s]^{-1}A$) $\frac{x_i}{1} = \frac{s x_i}{s} = \frac{s'' y_i}{s}$. Mit y_i ist auch $s'' y_i$ ganz über B , und daher ist $\frac{x_i}{1}$ ganz über $[s]^{-1}B$. Wegen $[s]^{-1}A = [s]^{-1}R\left[\frac{x_1}{1}, \dots, \frac{x_d}{1}\right]$ ist dann $[s]^{-1}A \supset [s]^{-1}B$ ganz. \square

Satz 3.5.3. *Sei $K \subset L$ eine Körpererweiterung, $R \subset K$ ein Bereich mit $K = \mathfrak{q}(R)$ und L eine affine R -Algebra. Dann ist $[L:K] < \infty$, und es gibt ein $a \in R^\bullet$ mit $K = R[a^{-1}]$.*

BEWEIS. Nach Satz 3.5.2 gibt es ein $a \in R^\bullet$, ein $d \in \mathbb{N}_0$ und über R algebraisch unabhängige Elemente $t_1, \dots, t_d \in L$, so dass $L \supset R[t_1, \dots, t_d, a^{-1}]$ ganz ist. Nach Satz 3.1.7.6 ist $R[t_1, \dots, t_d, a^{-1}]$ ein Körper, und da t_1, \dots, t_d auch über K algebraisch unabhängig sind, folgt $R[t_1, \dots, t_d, a^{-1}] \cong R[a^{-1}][X_1, \dots, X_d]$. Daher ist $d = 0$ und $R[a^{-1}]$ ein Körper, also $R[a^{-1}] = K$. \square

Satz 3.5.4 (Abstrakter Nullstellensatz). *Sei K ein Körper, \bar{K} eine algebraische Hülle von K und $A \neq \mathbf{0}$ eine affine K -Algebra.*

1. Ein Ideal $\mathfrak{a} \triangleleft A$ ist genau dann ein maximales Ideal von A , wenn es einen K -Homomorphismus $f: A \rightarrow \bar{K}$ mit $\text{Ker}(f) = \mathfrak{a}$ gibt. Insbesondere ist $\text{Hom}_K(A, \bar{K}) \neq \emptyset$.
2. Ein Element $x \in A$ ist genau dann nilpotent, wenn $f(x) = 0$ für jeden K -Homomorphismus $f: A \rightarrow \bar{K}$.

BEWEIS. Wegen $A \neq \mathbf{0}$ ist der Strukturhomomorphismus $\varepsilon: K \rightarrow A$ injektiv, und wir können $K \subset A = K[x_1, \dots, x_n]$ annehmen.

1. Sei $f: A \rightarrow \bar{K}$ ein K -Homomorphismus. Dann ist $K \subset f(A) = K[f(x_1), \dots, f(x_n)] \subset \bar{K}$, und nach Satz 3.3.2.3 ist $f(A)$ ein Körper. Daher ist $\mathfrak{a} = \text{Ker}(f) \in \text{max}(A)$.

Sei nun $\mathfrak{a} \in \text{max}(A)$, $\pi: A \rightarrow A/\mathfrak{a}$ der Restklassenhomomorphismus und $K' = \pi(K)$. Wegen $\mathfrak{a} \cap K = \mathbf{0}$ ist $\pi|_K: K \xrightarrow{\sim} K'$ ein Isomorphismus, und $A/\mathfrak{a} = K'[\pi(x_1), \dots, \pi(x_n)]$ ist ein Körper. Nach

Satz 3.5.3 ist $A/\mathfrak{a} \supset K'$ endlich, also algebraisch, und nach Satz 3.3.7.1 gibt es einen Körperhomomorphismus $\varphi: A/\mathfrak{a} \rightarrow \overline{K}$ mit $\varphi|_{K'} = (\pi|_{K'})^{-1}$. Dann ist $f = \varphi \circ \pi: A \rightarrow \overline{K}$ ein K -Homomorphismus mit $\text{Ker}(f) = \mathfrak{a}$.

2. Sei $x \in A$ nilpotent und $f: A \rightarrow \overline{K}$ ein K -Homomorphismus. Ist $n \in \mathbb{N}$ mit $x^n = 0$, so folgt $0 = f(x^n) = f(x)^n$ und daher $f(x) = 0$.

Sei nun $x \in A$ nicht nilpotent, $T = \{x^n \mid n \in \mathbb{N}_0\}$ und $j: A \rightarrow \overline{A} = T^{-1}A$ der Quotientenhomomorphismus. Dann ist

$$\frac{1}{x} \neq \frac{0}{1} \in \overline{A} \quad \text{und} \quad \overline{A} = K\left[\frac{x_1}{1}, \dots, \frac{x_n}{1}, \frac{1}{x}\right].$$

Daher ist $\overline{A} \neq \mathbf{0}$ eine affine K -Algebra und besitzt ein maximales Ideal $\overline{\mathfrak{a}}$. Nach 1. gibt es einen K -Homomorphismus $\overline{f}: \overline{A} \rightarrow \overline{K}$ mit $\text{Ker}(\overline{f}) = \overline{\mathfrak{a}}$. Dann ist $f = \overline{f} \circ j: A \rightarrow \overline{K}$ ein K -Homomorphismus, und $f(x) = \overline{f}\left(\frac{x}{1}\right) \neq 0$, da $\frac{x}{1} \in \overline{A}^\times$ und daher $\frac{x}{1} \notin \overline{\mathfrak{a}}$. \square

Definition 3.5.5. Sei K ein Körper, $n \in \mathbb{N}$, $K[\mathbf{X}]$ mit $\mathbf{X} = (X_1, \dots, X_n)$ ein Polynomring und L/K eine Körpererweiterung. Für eine Teilmenge $\mathfrak{X} \subset K[\mathbf{X}]$ sei

$$\mathbb{V}_L(\mathfrak{X}) = \{z \in L^n \mid (\forall f \in \mathfrak{X}) f(z) = 0\} \subset L^n.$$

Eine Teilmenge $Z \subset L^n$ heißt eine über K definierte *algebraische Menge*, wenn $Z = \mathbb{V}_L(\mathfrak{X})$ für eine Teilmenge $\mathfrak{X} \subset K[\mathbf{X}]$.

Offensichtlich ist $\mathbb{V}_L(\mathfrak{X}) = \mathbb{V}_L(K[\mathbf{X}]\langle \mathfrak{X} \rangle)$ für eine Teilmenge $\mathfrak{X} \subset K[\mathbf{X}]$.

Satz 3.5.6 (Hilbert'scher Nullstellensatz). Sei L/K eine Körpererweiterung, $n \in \mathbb{N}$, $K[\mathbf{X}]$ mit $\mathbf{X} = (X_1, \dots, X_n)$ ein Polynomring, $\mathfrak{a} \subsetneq K[\mathbf{X}]$ ein Ideal, $\pi: K[\mathbf{X}] \rightarrow A = K[\mathbf{X}]/\mathfrak{a}$ der Restklassenhomomorphismus und $x_i = \pi(X_i)$ für alle $i \in [1, n]$.

1. Es gibt eine bijektive Abbildung

$$\Phi: \text{Hom}_K(A, L) \rightarrow \mathbb{V}_L(\mathfrak{a}), \quad \text{gegeben durch} \quad \Phi(\varphi) = (\varphi(x_1), \dots, \varphi(x_n)).$$

Ist insbesondere L eine algebraische Hülle von K , so ist $\mathbb{V}_L(\mathfrak{a}) \neq \emptyset$.

2. Sei L eine algebraische Hülle von K und $P \in K[\mathbf{X}]$. Genau dann ist $P(z) = 0$ für alle $z \in \mathbb{V}_L(\mathfrak{a})$, wenn es ein $m \in \mathbb{N}$ gibt mit $P^m \in \mathfrak{a}$.

3. Sei K algebraisch abgeschlossen. Dann ist

$$\max(K[\mathbf{X}]) = \{K[\mathbf{X}]\langle X_1 - z_1, \dots, X_n - z_n \rangle \mid (z_1, \dots, z_n) \in K^n\}.$$

BEWEIS. 1. Die Abbildung $\Psi: \text{Hom}_K(K[\mathbf{X}], L) \rightarrow L^n$, definiert durch $\Psi(f) = (f(X_1), \dots, f(X_n))$ für alle $f \in \text{Hom}_K(K[\mathbf{X}], L)$, ist bijektiv, und für alle $z \in L^n$ und $P \in K[\mathbf{X}]$ ist $\Psi^{-1}(z)(P) = P(z)$. Genau dann ist $z \in \mathbb{V}_L(\mathfrak{a})$, wenn $\Psi^{-1}(z)|_{\mathfrak{a}} = 0$, und daher ist

$$\mathbb{V}_L(\mathfrak{a}) = \Psi(\{f \in \text{Hom}_K(K[\mathbf{X}], L) \mid f|_{\mathfrak{a}} = 0\}).$$

Nun ist aber auch $\omega: \text{Hom}_K(A, L) \rightarrow \{f \in \text{Hom}_K(K[\mathbf{X}], L) \mid f|_{\mathfrak{a}} = 0\}$, definiert durch $\omega(\varphi) = \varphi \circ \pi$, bijektiv. Daher ist $\Phi = \Psi \circ \omega: \text{Hom}_K(A, L) \rightarrow \mathbb{V}_L(\mathfrak{a})$ bijektiv, und für $\varphi \in \text{Hom}_K(A, L)$ ist

$$\Phi(\varphi) = \Psi(\varphi \circ \pi) = (\varphi \circ \pi(X_1), \dots, \varphi \circ \pi(X_n)) = (\varphi(x_1), \dots, \varphi(x_n)).$$

Ist L eine algebraische Hülle von K , so ist $\text{Hom}_K(A, L) \neq \emptyset$ nach Satz 3.5.4.1 und daher auch $\mathbb{V}_L(\mathfrak{a}) \neq \emptyset$.

2. Ist $m \in \mathbb{N}$ mit $P^m \in \mathfrak{a}$, so ist $P^m(z) = P(z)^m = 0$ und daher $P(z) = 0$ für alle $z \in \mathbb{V}_L(\mathfrak{a})$.

Sei nun $P^m \notin \mathfrak{a}$ für alle $m \in \mathbb{N}$, also $\pi(P) \in A$ nicht nilpotent. Dann gibt es nach Satz 3.5.4.2 ein $\varphi \in \text{Hom}_K(A, L)$ mit $0 \neq \varphi(\pi(P)) = \varphi \circ \pi(P(X_1, \dots, X_n)) = P(\varphi(x_1), \dots, \varphi(x_n))$, aber es ist $(\varphi(x_1), \dots, \varphi(x_n)) \in \mathbb{V}_L(\mathfrak{a})$.

3. Für $\mathbf{z} = (z_1, \dots, z_n) \in K^n$ sei $\mathfrak{m}_{\mathbf{z}} = K[\mathbf{X}] \langle X_1 - z_1, \dots, X_n - z_n \rangle$ und $\varepsilon_{\mathbf{z}} \in \text{Hom}_K(K[\mathbf{X}], K)$ definiert durch $\varepsilon_{\mathbf{z}}(P) = P(\mathbf{z})$ für alle $P \in K[\mathbf{X}]$. Wegen $X_i = (X_i - z_i) + z_i$ für alle $i \in [1, n]$ hat jedes $P \in K[\mathbf{X}]$ eine Darstellung

$$P = c + \sum_{i=1}^n (X_i - z_i) P_i \quad \text{mit} \quad c = P(\mathbf{z}) \quad \text{und} \quad P_1, \dots, P_n \in K[\mathbf{X}],$$

und es folgt $\text{Ker}(\varepsilon_{\mathbf{z}}) = \mathfrak{m}_{\mathbf{z}} \in \max(K[\mathbf{X}])$. Ist umgekehrt $\mathfrak{m} \in \max(K[\mathbf{X}])$, so gibt es nach Satz 3.5.4.1 eine K -Homomorphismus $f: K[\mathbf{X}] \rightarrow K$ mit $\text{Ker}(f) = \mathfrak{m}$. Ist $\mathbf{z} = (f(X_1), \dots, f(X_n)) \in K^n$, so ist $f = \varepsilon_{\mathbf{z}}$ und daher $\mathfrak{m} = \mathfrak{m}_{\mathbf{z}}$. \square

3.6. Separabilität

Bemerkung und Definition 3.6.1. Sei $p \in \mathbb{P}$, K ein Körper mit $\text{char}(K) = p$ und $\overline{K} \supset K$ ein algebraisch abgeschlossener Oberkörper.

1. $\varphi: K \rightarrow K$, definiert durch $\varphi(x) = x^p$, ist ein Körperhomomorphismus und heißt *Frobenius-Homomorphismus*. Für alle $x, y \in K$ und $e \in \mathbb{N}$ ist $(x + y)^{p^e} = x^{p^e} + y^{p^e}$. Insbesondere sind

$$K^{1/p^e} = \{\alpha \in \overline{K} \mid \alpha^{p^e} \in K\}, \quad \text{und} \quad K^{1/p^\infty} = \bigcup \{K^{1/p^e} \mid e \in \mathbb{N}\} \quad \text{Teilkörper von } \overline{K}.$$

2. Sei $a \in K \setminus K^p$ und $n \in \mathbb{N}$. Dann ist $f = X^{p^n} - a \in K[X]$ irreduzibel [Beweis: Sei $\alpha \in \overline{K}$ mit $f(\alpha) = 0$, also $a = \alpha^{p^n} \in K$, $\alpha^{p^m} \notin K$ für alle $m \in [0, n-1]$ und $f = (X - \alpha)^{p^n} \in \overline{K}[X]$. Angenommen, es sei $f = gh$ mit $g, h \in K[X] \setminus K$. Dann folgt $g = (X - \alpha)^k$ mit $k \in [1, p^n - 1]$, also $\pm g(0) = \alpha^k \in K$, und es sei $k = p^m l$ mit $m \in [0, n-1]$ und $l \in \mathbb{N}$, so dass $p \nmid l$. Dann sind l und p^{n-m} teilerfremd, es gibt $u, v \in \mathbb{Z}$ mit $ul + vp^{n-m} = 1$, und es folgt

$$\alpha^{p^m} = \alpha^{p^m(ul+vp^{n-m})} = (\alpha^k)^u (\alpha^{p^n})^v \in K, \quad \text{ein Widerspruch.}]$$

Definition und Satz 3.6.2. Sei K ein Körper, $\overline{K} \supset K$ ein algebraisch abgeschlossener Oberkörper und $f \in K[X] \setminus K$.

1. Die Anzahl $\mathbf{N}(f)$ der Nullstellen von f in \overline{K} hängt nur von f ab.
 f heißt *separabel*, wenn $\mathbf{N}(f) = \text{gr}(f)$ [äquivalent: f hat in keinem Erweiterungskörper von K mehrfache Nullstellen]. Andernfalls heißt f *inseparabel*.
2. Ist f irreduzibel über K , so ist f genau dann inseparabel, wenn $f' = 0$.
3. Genau dann ist $f' = 0$, wenn $\text{char}(K) = p \in \mathbb{P}$, und $f = g(X^p)$ für ein Polynom $g \in K[X]$.
4. Sei f irreduzibel über K und $\mathbf{N}(f) = k \in \mathbb{N}$. Dann gibt es ein $l \in \mathbb{N}$ und ein irreduzibles separables Polynom $g \in K[X]$ mit $f = g(X^l)$. Ist $\text{char}(K) = 0$, so ist $l = 1$. Ist $\text{char}(K) = p \in \mathbb{P}$, so ist l eine p -Potenz. Genau dann ist f separabel, wenn $l = 1$. Ist $c \in K^\times$ der höchste Koeffizient und sind $\alpha_1, \dots, \alpha_k \in \overline{K}$ die Nullstellen von f , so ist

$$g = c \prod_{i=1}^k (X - \alpha_i^l) \quad \text{und} \quad f = c \prod_{i=1}^k (X - \alpha_i)^l, \quad \text{also} \quad \text{gr}(f) = lk.$$

l heißt *Inseparabilitätsgrad* von f .

5. Der Körper K heißt *vollkommen*, wenn jedes irreduzible Polynom $f \in K[X] \setminus K$ separabel ist. Ist $\text{char}(K) = 0$ oder K algebraisch abgeschlossen, so ist K vollkommen. Ist $\text{char}(K) = p \in \mathbb{P}$, so ist K genau dann vollkommen, wenn $K = K^p$ [d. h., jedes Element von K ist eine p -te Potenz, und es ist $K = K^{1/p^\infty}$]. Insbesondere ist jeder endliche Körper vollkommen.

BEWEIS. 1. Sei $K_1 = \text{Alg}_{\overline{K}}(K)$. Nach Satz 3.3.7.5 ist K_1 eine algebraische Hülle von K und alle Nullstellen von f in \overline{K} liegen in K_1 . Daher genügt es, zu zeigen: Sind K_1 und K_2 algebraische Hüllen von K , so hat f in K_1 gleich viele Nullstellen wie in K_2 . Seien also K_1 und K_2 algebraische Hüllen von K . Dann gibt es nach Satz 3.3.7.3 einen K -Isomorphismus $\phi: K_1 \rightarrow K_2$, und dieser induziert eine bijektive Abbildung der Nullstellen von f in K_1 auf die Nullstellen von f in K_2 .

2. Ist $f' = 0$, so ist jede Nullstelle von f in \overline{K} eine mehrfache Nullstelle, also f inseparabel. Sei nun f irreduzibel und inseparabel. Dann hat f in \overline{K} eine mehrfache Nullstelle α . Sei $g \in K[X]$ das Minimalpolynom von α über K . Dann ist $g|f$ und $g|f'$, und da f irreduzibel ist, folgt $f = cg$ mit $c \in K^\times$ und daher $f|f'$. Wegen $\text{gr}(f') < \text{gr}(f)$ ist $f' = 0$.

3. Sei

$$f = \sum_{n \geq 0} a_n X^n \quad \text{mit } a_n \in K, a_n = 0 \text{ für fast alle } n \geq 0, \quad \text{also } f' = \sum_{n \geq 1} n a_n X^{n-1}.$$

Genau dann ist $f' = 0$, wenn $n a_n = 0$ für alle $n \geq 1$. Ist $\text{char}(K) = 0$, so ist das genau dann der Fall, wenn $a_n = 0$ für alle $n \geq 1$, also $f \in K$. Ist $\text{char}(K) = p \in \mathbb{P}$, so ist genau dann $f' = 0$, wenn $a_n = 0$ für alle $n \geq 1$ mit $p \nmid n$, wenn also

$$f = \sum_{j \geq 0} a_{pj} X^{pj} = g(X^p) \quad \text{mit } g = \sum_{j \geq 0} a_{pj} X^j.$$

4. Ist f separabel, so zerfällt f über \overline{K} in verschiedene Linearfaktoren, und es folgt die Behauptung. Sei also f inseparabel. Nach 2. ist $f' = 0$, und nach 3. gibt es ein Polynom $g \in K[X]$ mit $f = g(X^p)$. Sei $e \in \mathbb{N}$ maximal, so dass $f = g(X^{p^e})$ mit einem Polynom $g \in K[X]$. Dann ist g irreduzibel. Wäre g inseparabel, so folgte $g = g_1(X^p)$ mit einem Polynom $g_1 \in K[X]$ nach 2. und 3., im Widerspruch zur Maximalität von e . Daher ist g separabel, also $g = c(X - \beta_1) \cdot \dots \cdot (X - \beta_m) \in \overline{K}[X]$ mit $c \in K^\times$, $m \in \mathbb{N}$ und verschiedenen $\beta_1, \dots, \beta_m \in \overline{K}$. Für $j \in [1, m]$ sei $\beta_j = \gamma_j^{p^e}$ mit $\gamma_j \in \overline{K}$. Dann sind $\gamma_1, \dots, \gamma_m$ verschieden, und es folgt

$$f = g(X^{p^e}) = c \prod_{j=1}^m (X^{p^e} - \gamma_j^{p^e}) = c \prod_{j=1}^m (X - \gamma_j)^{p^e}.$$

Daher ist $m = k$ und $\{\gamma_1, \dots, \gamma_m\} = \{\alpha_1, \dots, \alpha_k\}$.

5. Ist $\text{char}(K) = 0$, so gibt es kein irreduzibles inseparables Polynom. Sei also im Folgenden $\text{char}(K) = p \in \mathbb{P}$.

Ist $a \in K \setminus K^p$, so ist das Polynom $X^p - a$ inseparabel und irreduzibel nach Bemerkung 3.6.1 und daher K nicht vollkommen.

Sei nun $K = K^p$ und $f \in K[X] \setminus K$ mit $f' = 0$. Wir zeigen, dass f reduzibel ist (dann gibt es kein irreduzibles inseparables Polynom in $K[X]$). Nach 3. ist $f = g(X^p)$ mit einem Polynom $g \in K[X]$. Sei

$$g = \sum_{n \geq 0} a_n X^n \quad \text{mit } a_n \in K = K^p, \quad \text{also } a_n = b_n^p. \quad \text{Dann ist } f = \sum_{n \geq 0} b_n^p X^{np} = \left(\sum_{n \geq 0} b_n X^n \right)^p,$$

also f reduzibel. Ist K endlich, so ist die Frobeniusabbildung $x \mapsto x^p$ eine injektive und daher auch surjektive Abbildung $K \rightarrow K$. Daher ist $K = K^p$. \square

Definition 3.6.3. Sei L/K eine Körpererweiterung.

1. Ein Element $\alpha \in L$ heißt *separabel* über K , wenn α über K algebraisch und das Minimalpolynom von α über K ein separables Polynom ist [äquivalent: α ist Nullstelle eines separablen Polynoms $f \in K[X]$]. α heißt *inseparabel* über K , wenn α über K algebraisch und nicht separabel ist.

2. Eine algebraische Körpererweiterung L/K heißt *separabel*, wenn jedes $\alpha \in L$ über K separabel ist, andernfalls *inseparabel* [insbesondere ist über einem vollkommenen Körper jede algebraische Körpererweiterung separabel].
3. Ein Element $\alpha \in L$ heißt *rein inseparabel* über K , wenn $\text{char}(K) = p \in \mathbb{P}$ und $\alpha^{p^n} \in K$ für ein $n \in \mathbb{N}_0$. Eine algebraische Körpererweiterung L/K heißt *rein inseparabel*, wenn jedes $\alpha \in L$ über K rein inseparabel ist

Satz 3.6.4. *Sei L/K eine Körpererweiterung, $\text{char}(K) = p \in \mathbb{P}$ und $\alpha \in L$.*

1. *Genau dann ist α separabel und rein inseparabel über K , wenn $\alpha \in K$. Ist insbesondere L/K algebraisch, so ist L/K genau dann separabel und rein inseparabel, wenn $L = K$.*
2. *Sei $K \subset M \subset L$ ein Zwischenkörper. Ist α separabel über K , so ist α auch separabel über M . Ist insbesondere L/K algebraisch und separabel, so sind auch L/M und M/K separabel.*

BEWEIS. 1. Sei $n \in \mathbb{N}_0$ minimal mit $\alpha^{p^n} = a \in K$. Ist $n = 0$, so ist $\alpha \in K$ und daher α separabel und rein inseparabel über K . Ist $n > 0$, so ist nach Bemerkung 3.6.1 das inseparable Polynom $X^{p^n} - a \in K[X]$ das Minimalpolynom von α über K und daher α inseparabel über K .

2. Sei $f \in K[X]$ das Minimalpolynom von α über K und $g \in M[X]$ das Minimalpolynom von α über M . Dann ist $g \mid f$, und f hat in einer algebraischen Hülle \bar{L} von L keine mehrfachen Nullstellen. Daher hat auch g in \bar{L} keine mehrfachen Nullstellen, und α ist separabel über M . \square

Definition und Satz 3.6.5. *Sei L/K eine endliche Körpererweiterung.*

1. *Für einen Körperhomomorphismus $\varphi: K \rightarrow F$ in einen algebraisch abgeschlossenen Körper F sei $\Omega_{L/K}(\varphi)$ die Menge aller Körperhomomorphismen $\psi: L \rightarrow F$ mit $\psi|_K = \varphi$. Dann hängt $|\Omega_{L/K}(\varphi)|$ nur von der Körpererweiterung L/K ab.
 $[L:K]_s = |\Omega_{L/K}(\varphi)|$ heißt *Separabilitätsgrad* von L/K .*
2. *Sei $L = K(\alpha)$, $f \in K[X]$ das Minimalpolynom von α über K und l der Inseparabilitätsgrad von f (also genau dann $l = 1$, wenn α über K separabel ist, und $l = p^e$ mit $e \in \mathbb{N}$, falls $\text{char}(K) = p$ und α über K inseparabel ist). Dann ist $[K(\alpha):K] = l[K(\alpha):K]_s$, α^l ist separabel über K , und $[K(\alpha):K]_s = [K(\alpha^l):K]$.
Insbesondere ist genau dann $[K(\alpha):K]_s = 1$, wenn entweder $\alpha \in K$ oder $\text{char}(K) = p \in \mathbb{P}$ und α rein inseparabel über K ist.*
3. *Sei $K \subset M \subset L$ ein Zwischenkörper. Dann ist $[L:K]_s = [L:M]_s[M:K]_s$.*
4. *Genau dann ist $[L:K]_s = [L:K]$, wenn L/K separabel ist. Ist $\text{char}(K) = p \in \mathbb{P}$, so gibt es ein $e \in \mathbb{N}_0$ mit $[L:K]_s = p^e [L:K]$.*

Man nennt e den *Inseparabilitätsindex* und p^e den *Inseparabilitätsgrad* von L/K .

5. *Sei $\text{char}(K) = p \in \mathbb{P}$. Genau dann ist L/K rein inseparabel, wenn $[L:K]_s = 1$.*

BEWEIS. 1. Für $i \in \{1, 2\}$ sei $\varphi_i: K \rightarrow F_i$ ein Körperhomomorphismus in einen algebraisch abgeschlossenen Körper F_i . Ist $\psi_i: L \rightarrow F_i$ ein Körperhomomorphismus mit $\psi_i|_K = \varphi_i$, so ist $\psi_i(L)/\varphi_i(K)$ algebraisch, also $\psi_i(L) \subset F'_i = \text{Alg}_{F_i}(\varphi_i(K))$ und $\Omega_{L/K}(\varphi_i) = \Omega_{L/K}(\varphi_i: K \rightarrow F'_i)$. $\varphi_2 \circ \varphi_1^{-1}: \varphi_1(K) \rightarrow \varphi_2(K)$ ist ein Körperisomorphismus, und nach Satz 3.3.7.3 gibt es einen Körperisomorphismus $\phi: F'_1 \rightarrow F'_2$ mit $\phi|_{\varphi_1(K)} = \varphi_2 \circ \varphi_1^{-1}$. Dann ist aber $\phi^*: \Omega_{L/K}(\varphi_1) \rightarrow \Omega_{L/K}(\varphi_2)$, definiert durch $\phi^*(\psi_1) = \phi \circ \psi_1$, eine bijektive Abbildung.

2. Sei F eine algebraische Hülle von L und $\varphi = (K \hookrightarrow F)$. Nach Satz 3.6.2 gibt es ein $k \in \mathbb{N}$ und verschiedene $\alpha_1, \dots, \alpha_k \in F$ mit $\alpha = \alpha_1$, so dass

$$f = \prod_{i=1}^k (X - \alpha_i)^l, \quad \text{und} \quad g = \prod_{i=1}^k (X - \alpha_i^l) \in K[X] \quad \text{ist separabel.}$$

Also ist α^l separabel über K , und genau dann ist $k = 1$, wenn entweder $\alpha \in K$ oder $\text{char}(K) = p \in \mathbb{P}$ und α rein inseparabel über K ist. Ist $\psi \in \Omega_{K(\alpha)/K}(\varphi)$, so folgt $\psi(\alpha) \in \{\alpha_1, \dots, \alpha_k\}$, und die Zuordnung $\psi \mapsto \psi(\alpha)$ definiert eine bijektive Abbildung $\Omega_{K(\alpha)/K}(\varphi) \rightarrow \{\alpha_1, \dots, \alpha_k\}$. Daher ist $[K(\alpha):K]_s = k = [K(\alpha^l):K]$ und $[K(\alpha):K] = kl$.

3. Sei $\varphi: K \rightarrow F$ ein Körperhomomorphismus in einen algebraisch abgeschlossenen Körper F . Dann ist

$$\Omega_{L/K}(\varphi) = \bigoplus_{\psi \in \Omega_{M/K}(\varphi)} \Omega_{L/M}(\psi) \quad \text{und daher} \quad [L:K]_s = [L:M]_s [M:K]_s.$$

4. Induktion nach $[L:K]$. Im Falle $L = K$ ist nichts zu zeigen. Sei also $[L:K] > 1$ und gelte die Behauptung für alle Körpererweiterungen kleineren Grades. Sei $\alpha \in L \setminus K$. Ist L/K inseparabel, so sei α inseparabel über K . Nach 2. ist dann $[K(\alpha):K] = l [K(\alpha):K]_s$ mit $l = 1$, falls α über K separabel ist, und $l = p^d$ mit $d \in \mathbb{N}$, falls $\text{char}(K) = p \in \mathbb{P}$ und α über K inseparabel ist.

Ist L/K separabel, so ist α separabel über K , also $l = 1$ und $[K(\alpha):K] = [K(\alpha):K]_s$. Da auch $L/K(\alpha)$ separabel ist, folgt $[L:K(\alpha)] = [L:K(\alpha)]_s$ nach Induktionsvoraussetzung, und wir erhalten $[L:K] = [L:K(\alpha)] [K(\alpha):K] = [L:K(\alpha)]_s [K(\alpha):K]_s = [L:K]_s$.

Ist L/K inseparabel und $\text{char}(K) = p \in \mathbb{P}$, so ist $[L:K(\alpha)] = p^b [L:K(\alpha)]_s$ mit $b \in \mathbb{N}_0$ nach Induktionsvoraussetzung, und $[L:K] = [L:K(\alpha)] [K(\alpha):K] = p^b [L:K(\alpha)]_s p^d [K(\alpha):K]_s = p^{b+d} [L:K]_s$.

5. Induktion nach $[L:K]$. Im Falle $L = K$ ist nichts zu zeigen. Sei also $[L:K] > 1$ und gelte die Behauptung für alle Körpererweiterungen kleineren Grades. Sei $\alpha \in L \setminus K$, und sei α nicht rein inseparabel, falls die Körpererweiterung L/K nicht rein inseparabel ist.

Ist L/K nicht rein inseparabel, so ist $[K(\alpha):K]_s > 1$ nach 2. und daher $[L:K]_s > 1$. Ist L/K rein inseparabel, so ist auch $L/K(\alpha)$ rein inseparabel, also $[L:K(\alpha)]_s = 1$ nach Induktionsvoraussetzung. Nach 2. ist $[K(\alpha):K]_s = 1$, und damit folgt $[L:K]_s = 1$. \square

Definition und Satz 3.6.6. Sei L/K eine algebraische Körpererweiterung.

1. Sei $C \subset L$, $L = K(C)$, und seien alle $\alpha \in C$ separabel über K . Dann ist L/K separabel.
2. Sei $L_0 = \{\alpha \in L \mid \alpha \text{ ist separabel über } K\}$. Dann ist L_0 der größte über K separable Zwischenkörper von L/K , und die Körpererweiterung L/L_0 ist rein inseparabel. Ist L/K endlich, so ist $[L_0:K] = [L:K]_s$.

L_0 heißt *separabler Abschluss* von K in L . Ist L algebraisch abgeschlossen, so nennt man L_0 eine *separable Hülle* von K .

3. Sei $K \subset M \subset L$ ein Zwischenkörper, und seien L/M und M/K separabel. Dann ist auch L/K separabel.
4. Seien $K \subset K' \subset L$ und $K \subset M \subset L$ Zwischenkörper, und sei M/K separabel. Dann ist auch $K'M/K'$ separabel.

BEWEIS. 1. Sei $\alpha \in L$ und seien $\alpha_1, \dots, \alpha_n \in C$ mit $\alpha \in K(\alpha_1, \dots, \alpha_n)$. Für $i \in [0, n-1]$ ist α_{i+1} separabel über $K_i = K(\alpha_1, \dots, \alpha_i)$, und nach Satz 3.6.5 folgt

$$[K(\alpha_1, \dots, \alpha_n):K] = \prod_{i=0}^{n-1} [K_i(\alpha_{i+1}):K_i] = \prod_{i=0}^{n-1} [K_i(\alpha_{i+1}):K_i]_s = [K(\alpha_1, \dots, \alpha_n):K]_s.$$

Daher ist $K(\alpha_1, \dots, \alpha_n)/K$ separabel, also ist auch α separabel über K .

2. Nach 1. ist $K(L_0)/K$ separabel, also $K(L_0) \subset L_0$, Daher $K(L_0) = L_0$ der größte über K separable Teilkörper von L . Sei nun $\text{char}(K) = p \in \mathbb{P}$ und $\alpha \in L$. Nach Satz 3.6.5.2 gibt es ein $e \in \mathbb{N}_0$, so dass α^{p^e} über K separabel ist. Dann folgt aber $\alpha^{p^e} \in L_0$ und daher ist α über L_0 rein inseparabel. Ist L/K endlich, so ist $[L:L_0]_s = 1$ nach Satz 3.6.5.5 und daher $[L_0:K] = [L_0:K]_s = [L:K]_s$.

3. Sei $\alpha \in L$, $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in M[X]$ das Minimalpolynom von α über M und $M_0 = K(a_0, \dots, a_{n-1}) \subset M$. Dann ist f auch das Minimalpolynom von α über M_0 , also α separabel über M_0 . Da auch M_0/K separabel ist, folgt

$$[M_0(\alpha):K] = [M_0(\alpha):M_0] [M_0:K] = [M_0(\alpha):M_0]_s [M_0:K]_s = [M_0(\alpha):K]_s.$$

Daher ist $M_0(\alpha)/K$ separabel und auch α separabel über K .

4. Es ist $K'M = K'(M)$, und alle $\alpha \in M$ sind separabel über K , also auch über K' . Daher ist $K'M/K'$ separabel nach 1. \square

Satz 3.6.7. Sei L/K eine endliche Körpererweiterung, und sei $\text{char}(K) = p \in \mathbb{P}$. Dann sind äquivalent:

- (a) L/K ist separabel.
- (b) $L = KL^p$.
- (c) Für alle $e \in \mathbb{N}$ ist $L = KL^{p^e}$.
- (d) Für alle $e \in \mathbb{N}$ und jede K -Basis (u_1, \dots, u_n) von L ist auch $(u_1^{p^e}, \dots, u_n^{p^e})$ eine K -Basis von L .

BEWEIS. (a) \Rightarrow (b) Die Körpererweiterung L/KL^p ist separabel und rein inseparabel.

(b) \Rightarrow (c) Induktion nach e . Für $e = 1$ ist nichts zu zeigen.

$e \geq 1$, $e \rightarrow e + 1$: Aus $L = KL^{p^e}$ folgt $L^p = K^p L^{p^{e+1}}$ und $L = KL^p = K K^p L^{p^{e+1}} = KL^{p^{e+1}}$.

(c) \Rightarrow (d) Sei $e \in \mathbb{N}$ und (u_1, \dots, u_n) eine K -Basis von L . Dann ist $L = KL^{p^e} = K \langle u_1^{p^e}, \dots, u_n^{p^e} \rangle$, und wegen $[L:K] = n$ ist $(u_1^{p^e}, \dots, u_n^{p^e})$ linear unabhängig über K .

(d) \Rightarrow (a) Sei (u_1, \dots, u_n) eine K -Basis von L und L_0 der separable Abschluss von K in L . Dann ist L/L_0 rein inseparabel, und daher gibt es ein $e \in \mathbb{N}$, so dass $u_i^{p^e} \in L_0$ für alle $i \in [1, n]$. Damit folgt $L = K \langle u_1^{p^e}, \dots, u_n^{p^e} \rangle \subset L_0$, also $L = L_0$. \square

Definition und Satz 3.6.8. Sei \bar{K}/K eine Körpererweiterung, und seien L und M Zwischenkörper von \bar{K}/K .

1. Sei jede über K linear unabhängige Teilmenge von L auch über M linear unabhängig. Dann ist jede über K linear unabhängige Teilmenge von M auch über L linear unabhängig.

Sind diese Bedingungen erfüllt, so nennt man L und M linear disjunkt über K .

2. Sei $K \subset M' \subset M$ ein Zwischenkörper. Genau dann sind L und M über K linear disjunkt, wenn gilt: L und M' sind linear disjunkt über K , und LM' und M sind linear disjunkt über M' .

BEWEIS. 1. Durch Widerspruch. Sei $B \subset M$ linear unabhängig über K und linear abhängig über L . Dann gibt es $n \in \mathbb{N}$, $r \in [1, n]$, verschiedene $b_1, \dots, b_n \in B$ und $y_1, \dots, y_n \in L^\times$, so dass $b_1 y_1 + \dots + b_n y_n = 0$, (y_1, \dots, y_r) ist linear unabhängig über K und $\{y_{r+1}, \dots, y_n\} \subset_K \langle y_1, \dots, y_r \rangle$. Für $i \in [r+1, n]$ sei

$$y_i = \sum_{\rho=1}^r a_{i,\rho} y_\rho \quad \text{mit } a_{i,\rho} \in K. \quad \text{Dann ist } 0 = \sum_{\rho=1}^r y_\rho b_\rho + \sum_{i=r+1}^n \sum_{\rho=1}^r a_{i,\rho} y_\rho b_i = \sum_{\rho=1}^r \left(b_\rho + \sum_{i=r+1}^n a_{i,\rho} b_i \right) y_\rho.$$

(y_1, \dots, y_r) ist linear unabhängig über M . Daher folgt

$$b_\rho + \sum_{i=r+1}^n a_{i,\rho} b_i = 0 \quad \text{für alle } \rho \in [1, r], \quad \text{im Widerspruch zur linearen Unabhängigkeit von } B \text{ über } K.$$

2. Seien zuerst L und M linear disjunkt über K . Dann ist jede über K linear unabhängige Teilmenge von M (also insbesondere jede über K linear unabhängige Teilmenge von M') linear unabhängig über L . Daher sind auch L und M' linear disjunkt über K . Wir nehmen an, LM' und M seien nicht linear disjunkt über M' . Sei also $B \subset M$ linear unabhängig über M' und linear abhängig über LM' . Dann gibt

es ein $n \in \mathbb{N}$, verschiedene $b_1, \dots, b_n \in B$ und Elemente $y_1, \dots, y_n \in (LM')^\times$, so dass $y_1 b_1 + \dots + y_n b_n = 0$. Sei $(u_i)_{i \in I}$ eine K -Basis von L . Dann ist $(u_i)_{i \in I}$ linear unabhängig über M , also auch über M' , und $M' \cup L \subset M' \langle u_i \mid i \in I \rangle \subset M'[L]$. Für alle $i, j \in I$ ist $u_i u_j \in L$. Daher ist $M' \langle u_i \mid i \in I \rangle$ ein Ring, und es folgt $M' \langle u_i \mid i \in I \rangle = M'[L]$. Da LM' ein Quotientenkörper von $M'[L]$ ist, können wir (nach Hochmultiplizieren der Nenner) $y_\nu \in M'[L]$ für alle $\nu \in [1, n]$ annehmen, und dann ist

$$y_\nu = \sum_{i \in I} a_{\nu,i} u_i \quad \text{mit } a_{\nu,i} \in M', \quad a_{\nu,i} = 0 \text{ für fast alle } i \in I, \quad \text{also} \quad \sum_{i \in I} \left(\sum_{\nu=1}^n a_{\nu,i} b_\nu \right) u_i = 0.$$

Wegen der linearen Unabhängigkeit von $(u_i)_{i \in I}$ über M folgt

$$\sum_{\nu=1}^n a_{\nu,i} b_\nu = 0 \quad \text{für alle } i \in I,$$

also $a_{\nu,i} = 0$ für alle $i \in I$ und $\nu \in [1, n]$ wegen der linearen Unabhängigkeit von (b_1, \dots, b_n) über M' , im Widerspruch zu $y_\nu \neq 0$.

Seien nun L und M' linear disjunkt über K , und seien LM' und M linear disjunkt über M' . Sei $(u_i)_{i \in I}$ eine K -Basis von M' und $(v_j)_{j \in J}$ eine M' -Basis von M . Nach Voraussetzung ist $(u_i)_{i \in I}$ linear unabhängig über L , $(v_j)_{j \in J}$ linear unabhängig über LM' , und nach Satz 3.1.4.1 ist $(u_i v_j)_{(i,j) \in I \times J}$ eine K -Basis von M . Wir nehmen an, L und M seien nicht linear disjunkt über K . Sei $B \subset L$ linear unabhängig über K , aber linear abhängig über M . Dann gibt es ein $n \in \mathbb{N}$, verschiedene $b_1, \dots, b_n \in B$ und $y_1, \dots, y_n \in M^\times$ mit $b_1 y_1 + \dots + b_n y_n = 0$. Für $\nu \in [1, n]$ sei

$$y_\nu = \sum_{(i,j) \in I \times J} a_{\nu,i,j} u_i v_j \quad \text{mit } a_{\nu,i,j} \in K, \quad a_{\nu,i,j} = 0 \text{ für fast alle } (i,j) \in I \times J.$$

Dann folgt

$$\sum_{j \in J} \left(\sum_{i \in I} \sum_{\nu=1}^n b_\nu a_{\nu,i,j} u_i \right) v_j = 0, \quad \text{also} \quad \sum_{i \in I} \sum_{\nu=1}^n b_\nu a_{\nu,i,j} u_i = 0 \quad \text{und} \quad \sum_{\nu=1}^n b_\nu a_{\nu,i,j} = 0 \quad \text{für alle } (i,j) \in I \times J$$

wegen der linearen Unabhängigkeit von $(v_j)_{j \in J}$ über LM' und von $(u_i)_{i \in I}$ über L . Damit erhalten wir einen Widerspruch zur linearen Unabhängigkeit von B über K . \square

Satz 3.6.9. *Sei \bar{K}/K eine Körpererweiterung, und seien L und M Zwischenkörper von \bar{K}/K . Sei M/K algebraisch und L/K rein transzendent. Dann ist auch LM/M rein transzendent, und L und M sind linear disjunkt über K .*

Ist $L = K(C)$ mit einer über K algebraisch unabhängigen Menge C , so ist C auch algebraisch unabhängig über M , und $LM = M(C)$.

BEWEIS. Sei $L = K(C)$ mit einer über K algebraisch unabhängigen Menge C . Dann ist $LM = M(C)$, und wir nehmen an, C sei algebraisch abhängig über M . Dann gibt es ein $n \in \mathbb{N}$ und verschiedene $t_1, \dots, t_n \in C$, so dass (t_1, \dots, t_n) über M algebraisch abhängig ist. Dann ist $M(t_1, \dots, t_n)/K(t_1, \dots, t_n)$ algebraisch, und es folgt

$$\begin{aligned} \text{tr}(M(t_1, \dots, t_n)/K) &= \text{tr}(M(t_1, \dots, t_n)/K(t_1, \dots, t_n)) + \text{tr}(K(t_1, \dots, t_n)/K) = n + 0 \\ &= \text{tr}(M(t_1, \dots, t_n)/M) + \text{tr}(M/K) = \text{tr}(M(t_1, \dots, t_n)/M). \end{aligned}$$

Daher (t_1, \dots, t_n) doch algebraisch unabhängig über M .

Wir müssen noch zeigen, dass L und M über K linear disjunkt sind. Da C auch über M algebraisch unabhängig ist, können wir annehmen, $L = K(\mathbf{X})$ sei ein rationaler Funktionenkörper in einer Familie \mathbf{X} von Unbestimmten. Wir nehmen an, L und M seien nicht linear disjunkt über K , und es sei $B \subset M$ eine über K linear unabhängige Menge, die über L linear abhängig ist. Dann gibt es ein $n \in \mathbb{N}$, verschiedene $b_1, \dots, b_n \in B$ und Elemente $y_1, \dots, y_n \in L^\times$, so dass $b_1 y_1 + \dots + b_n y_n = 0$. Sei (X_1, \dots, X_k) eine endliche Teilfamilie von \mathbf{X} mit $\{y_1, \dots, y_n\} \subset K(X_1, \dots, X_k)$. Nach Multiplikation mit einem

gemeinsamen Nenner können wir $\{y_1, \dots, y_n\} \subset K[X_1, \dots, X_k]$ annehmen. Dann gibt es verschiedene Monome $m_1, \dots, m_N \in [X_1, \dots, X_k]$, so dass für alle $\nu \in [1, n]$

$$y_\nu = \sum_{j=1}^N c_{\nu,j} m_j \quad \text{mit} \quad c_{\nu,j} \in K, \quad \text{also} \quad 0 = \sum_{j=1}^N \left(\sum_{\nu=1}^n c_{\nu,j} b_\nu \right) m_j \quad \text{mit} \quad \sum_{\nu=1}^n c_{\nu,j} b_\nu \in M.$$

Da (X_1, \dots, X_k) über M algebraisch unabhängig ist, ist (m_1, \dots, m_N) über M linear unabhängig. Daher folgt

$$\sum_{\nu=1}^n c_{\nu,j} b_\nu = 0 \quad \text{für alle} \quad j \in [1, N], \quad \text{also} \quad c_{\nu,j} = 0 \quad \text{für alle} \quad \nu \in [1, n] \quad \text{und} \quad j \in [1, N],$$

ein Widerspruch zu $y_1, \dots, y_n \in L^\times$. □

Satz 3.6.10. *Sei K ein Körper, $\text{char}(K) = p \in \mathbb{P}$, L/K eine separabel algebraische Körpererweiterung, $\overline{K} \supset L$ ein algebraisch abgeschlossener Oberkörper und $K^{1/p^\infty} \subset \overline{K}$. Dann sind L und K^{1/p^∞} linear disjunkt über K .*

BEWEIS. Durch Widerspruch. Sei $B \subset L$ linear unabhängig über K und linear abhängig über K^{1/p^∞} . Dann gibt es ein $n \in \mathbb{N}$, verschiedene $b_1, \dots, b_n \in B$ und Elemente $y_1, \dots, y_n \in (K^{1/p^\infty})^\times$ mit $b_1 y_1 + \dots + b_n y_n = 0$. Sei $L' = K(b_1, \dots, b_n)$ und $e \in \mathbb{N}$, so dass $y_\nu^{p^e} \in K$ für alle $\nu \in [1, n]$. Nach Satz 3.3.2.3 ist $n \leq m = [L' : K] < \infty$, und es seien $b_{n+1}, \dots, b_m \in L'$, so dass (b_1, \dots, b_m) eine K -Basis von L' ist. Da L'/K separabel ist, ist $(b_1^{p^e}, \dots, b_m^{p^e})$ eine K -Basis von L' nach Satz 3.6.7. Insbesondere ist $(b_1^{p^e}, \dots, b_n^{p^e})$ linear unabhängig über K , aber $b_1^{p^e} y_1^{p^e} + \dots + b_n^{p^e} y_n^{p^e} = (b_1 y_1 + \dots + b_n y_n)^{p^e} = 0$, ein Widerspruch. □

Definition 3.6.11. Sei L/K eine Körpererweiterung. Eine Transzendenzbasis B von L/K heißt *separierend*, wenn $L/K(B)$ separabel ist. Die Körpererweiterung L/K heißt

- *separabel erzeugt*, wenn sie eine separierende Transzendenzbasis besitzt;
- *separabel*, wenn jeder über K endlich erzeugte Zwischenkörper von L/K über K separabel erzeugt ist.

Satz 3.6.12 (Kriterium von MacLane). *Sei K ein Körper, $\text{char}(K) = p \in \mathbb{P}$, L/K eine Körpererweiterung, $\overline{K} \supset L$ ein algebraisch abgeschlossener Oberkörper und $K^{1/p^\infty} \subset \overline{K}$.*

1. *Ist L/K separabel erzeugt, so sind L und K^{1/p^∞} linear disjunkt über K .*
2. *Die folgenden Aussagen sind äquivalent:*
 - (a) *L und K^{1/p^∞} sind linear disjunkt über K .*
 - (b) *L und $K^{1/p}$ sind linear disjunkt über K .*
 - (c) *Es gibt ein $e \in \mathbb{N}$, so dass L und K^{1/p^e} über K linear disjunkt sind.*
 - (d) *L/K ist separabel.*

Genauer gilt: Ist $K \subset L_0 \subset L$ ein Zwischenkörper und $L_0 = K(C)$ mit einer endlichen Menge C , so gibt es eine separierende Transzendenzbasis B von L_0/K mit $B \subset C$.

Insbesondere ist jede separabel erzeugte Körpererweiterung separabel.

BEWEIS. 1. Sei B eine separierende Transzendenzbasis von L/K . Nach Satz 3.6.9 sind $K(B)$ und K^{1/p^∞} linear disjunkt über K , und nach Satz 3.6.10 sind L und $K(B)^{1/p^\infty}$ linear disjunkt über $K(B)$. Wegen $K^{1/p^\infty}(B) \subset K(B)^{1/p^\infty}$ sind auch L und $K^{1/p^\infty}(B) = K(B)K^{1/p^\infty}$ linear disjunkt über $K(B)$, und nach Satz 3.6.8 sind auch L und K^{1/p^∞} linear disjunkt über K .

2. Für $e \in \mathbb{N}$ ist $K \subset K^{1/p} \subset K^{1/p^e} \subset K^{1/p^\infty}$, und daher folgt (a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (b).

(b) \Rightarrow (d) Wir zeigen die genauere Aussage durch Induktion nach $|C|$. Ist $C = \emptyset$, so ist nichts zu zeigen. Sei also $|C| = n \geq 1$ und gelte die Behauptung für Körpererweiterungen mit weniger als n Erzeugenden. Sei $r = \text{tr}(L_0/K)$, also $r \leq n$. Ist $r = n$, so ist C eine Transzendenzbasis und nichts zu zeigen. Sei also $r < n$ und $C = \{x_1, \dots, x_n\}$, so dass $\text{tr}(K(x_1, \dots, x_{r+1})/K) = r$. Sei $F \in K[X_1, \dots, X_{r+1}]^\bullet$ ein Polynom kleinsten Totalgrades mit $F(x_1, \dots, x_{r+1}) = 0$. Dann ist F irreduzibel, und wir zeigen zunächst:

A. $F \notin K[X_1^p, \dots, X_{r+1}^p]$.

Beweis von **A.** Angenommen, es sei $F \in K[X_1^p, \dots, X_{r+1}^p]$. Dann ist $F = c_1 m_1^p + \dots + c_s m_s^p$ mit $s \in \mathbb{N}$ und verschiedenen Monomen $m_1, \dots, m_s \in K[X_1, \dots, X_{r+1}]$, und es folgt

$$0 = F(x_1, \dots, x_{r+1}) = \left(\sum_{i=1}^s c_i^{1/p} m_i(x_1, \dots, x_{r+1}) \right)^p, \quad \text{also} \quad \sum_{i=1}^s c_i^{1/p} m_i(x_1, \dots, x_{r+1}) = 0.$$

Daher ist $(m_1(x_1, \dots, x_{r+1}), \dots, m_s(x_1, \dots, x_{r+1})) \in L^s$ linear abhängig über $K^{1/p}$, also auch über K , da $K^{1/p}$ und L über K linear disjunkt sind. Daher gibt es $b_1, \dots, b_s \in K$, so dass

$$(b_1 m_1 + \dots + b_s m_s)(x_1, \dots, x_{r+1}) = 0,$$

aber das Polynom $b_1 m_1 + \dots + b_s m_s \in K[X_1, \dots, X_{r+1}]$ hat kleineren Totalgrad als F , ein Widerspruch. Damit ist **A** gezeigt.

Sei (nach geeigneter Umnummerierung) $F \notin K[X_1^p, X_2, \dots, X_{r+1}]$, also

$$F = \sum_{i \geq 0} F_i X_1^i \quad \text{mit} \quad F_i \in K[X_2, \dots, X_{r+1}], \quad F_i = 0 \quad \text{für fast alle} \quad i \geq 0,$$

und $F_j \neq 0$ für ein $j \geq 0$ mit $p \nmid j$. Sei

$$f = F(X_1, x_2, \dots, x_{r+1}) = \sum_{i \geq 0} F_i(x_2, \dots, x_{r+1}) X_1^i \in K[x_2, \dots, x_{r+1}][X_1].$$

Da F_j kleineren Totalgrad als F hat, ist $F_j(x_2, \dots, x_{r+1}) \neq 0$, also $f \notin K[x_2, \dots, x_{r+1}][X_1^p]$. Insbesondere ist $f \notin K(x_2, \dots, x_{r+1})[X_1^p]$ und $f \neq 0$. Wegen $f(x_1) = 0$ ist x_1 algebraisch über $K(x_2, \dots, x_{r+1})$. Daher ist (x_2, \dots, x_{r+1}) algebraisch unabhängig über K . Also ist auch $(X_1, x_2, \dots, x_{r+1})$ algebraisch unabhängig über K , und daher ist der Einsetzungshomomorphismus

$$\phi = \phi_{(X_1, x_2, \dots, x_{r+1})}^{(X_1, X_2, \dots, X_{r+1})}: K[X_1, \dots, X_{r+1}] \rightarrow K[X_1, x_2, \dots, x_{r+1}] = K[x_2, \dots, x_{r+1}][X_1]$$

ein Isomorphismus. Wegen $f = \phi(F)$ ist f irreduzibel in $K[x_2, \dots, x_{r+1}][X_1]$. Da $K[x_2, \dots, x_{r+1}]$ faktoriell ist, ist f auch irreduzibel in $K(x_2, \dots, x_{r+1})[X_1]$, und wegen $f \notin K(x_2, \dots, x_{r+1})[X_1^p]$ ist f separabel. Folglich ist x_1 separabel algebraisch über $K(x_2, \dots, x_{r+1})$ und auch über $K(x_2, \dots, x_n)$. Nach Induktionsvoraussetzung gibt es eine Transzendenzbasis B von $K(x_2, \dots, x_n)$ mit $B \subset \{x_2, \dots, x_n\}$, so dass $K(x_2, \dots, x_n)/K(B)$ separabel algebraisch ist. Dann ist aber auch $K(C)/K(B)$ separabel algebraisch.

(d) \Rightarrow (a) Angenommen, L und K^{1/p^∞} seien nicht linear disjunkt über K . Dann gibt es eine endliche Teilmenge $C \subset L$, die linear unabhängig über K , aber linear abhängig über K^{1/p^∞} ist. Dann ist $K(C)/K$ separabel erzeugt, und nach 1. sind $K(C)$ und K^{1/p^∞} linear disjunkt über K , ein Widerspruch. \square

Korollar 3.6.13. *Ist K ein vollkommener Körper, so ist jede Körpererweiterung L/K separabel.*

BEWEIS. Ist $\text{char}(K) = 0$, so ist nichts zu zeigen. Ist $\text{char}(K) = p$, so ist $K^{1/p^\infty} = K$, und die Behauptung folgt nach Satz 3.6.12. \square

3.7. Derivationen

Definitionen und Bemerkungen 3.7.1. Sei R ein Ring und M ein R -Modul. Eine *Derivation* (von R in M) ist eine Abbildung $D: R \rightarrow M$, so dass für alle $a, b \in R$ gilt:

$$D(a + b) = D(a) + D(b) \quad \text{und} \quad D(ab) = aD(b) + bD(a).$$

1. Sei $D: R \rightarrow M$ eine Derivation und $R_0 \subset R$ ein Teilring. Genau dann ist $D|_{R_0} = 0$, wenn D R_0 -linear ist. [Beweis: Für $\lambda \in R_0$ und $x \in R$ ist $D(\lambda x) = \lambda D(x) + xD(\lambda)$. Ist $D|_{R_0} = 0$, so ist D R_0 -linear. Ist D R_0 -linear, so liefert $x = 1$ die Gleichung $D(\lambda) = \lambda D(1) = \lambda D(1) + D(\lambda)$, also $D|_{R_0} = 0$].
2. Sei $D: R \rightarrow M$ eine Derivation und $R_0 = \{m1_R \mid m \in \mathbb{Z}\} \subset R$ der Primring. Dann ist $D|_{R_0} = 0$. [Beweis: $D(1) = D(1 \cdot 1) = D(1) + D(1)$, also $D(1) = 0$ und daher $D(m1) = mD(1) = 0$ für alle $m \in \mathbb{Z}$].
3. $\text{Der}(R, M)$ bezeichne die Menge aller Derivationen von R in M . Sind $D, D' \in \text{Der}(R, M)$ und $\lambda \in R$, so folgt $D + D' \in \text{Der}(R, M)$ und $\lambda D \in \text{Der}(R, M)$. Damit ist $\text{Der}(R, M)$ ein R -Modul. Für einen Teilring $K \subset R$ sei $\text{Der}_K(R, M) = \{D \in \text{Der}(R, M) \mid D|_K = 0\}$. Die $D \in \text{Der}_K(R, M)$ heißen *K-Derivationen* (von R in M). $\text{Der}_K(R, M) \subset \text{Der}(R, M)$ ist ein R -Untermodul. Wir setzen $\text{Der}(R) = \text{Der}(R, R)$ und $\text{Der}_K(R) = \text{Der}_K(R, R)$.
4. Sei $\varphi: M \rightarrow M'$ ein R -Modulhomomorphismus. Ist $D \in \text{Der}(R, M)$, so ist $\varphi \circ D \in \text{Der}(R, M')$, und $D \mapsto \varphi \circ D$ ist ein R -Modulhomomorphismus $\text{Der}(R, M) \rightarrow \text{Der}(R, M')$. Ist insbesondere $M \subset M'$ ein R -Untermodul, so ist auch $\text{Der}(R, M) \subset \text{Der}(R, M')$ ein R -Untermodul.
5. Sei $D \in \text{Der}(R, M)$. Für $x \in R^\times$ ist $D(x^{-1}) = -x^{-2}D(x)$. [Beweis: $0 = D(1) = D(x^{-1}x) = x^{-1}D(x) + xD(x^{-1})$].
6. Sei $R[\mathbf{X}]$ mit $\mathbf{X} = (X_i)_{i \in I}$ ein Polynomring. Für alle $i \in I$ ist dann die formale partielle Ableitung

$$\frac{\partial}{\partial X_i}: R[\mathbf{X}] \rightarrow R[\mathbf{X}]$$

eine Derivation.

Sei jetzt $R \subset M$ eine Ringerweiterung. Für eine Derivation $D \in \text{Der}(R, M)$ und $f \in R[\mathbf{X}]$ entstehe $f^D \in M[\mathbf{X}]$ durch Anwendung von D auf die Koeffizienten. Explizit:

$$\text{Für } f = \sum_{\nu_1, \dots, \nu_n \geq 0} f_{\nu_1, \dots, \nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \quad \text{sei} \quad f^D = \sum_{\nu_1, \dots, \nu_n \geq 0} D(f_{\nu_1, \dots, \nu_n}) X_1^{\nu_1} \cdots X_n^{\nu_n}.$$

Dann ist $\tilde{D}: R[\mathbf{X}] \rightarrow M[\mathbf{X}]$, definiert durch $\tilde{D}(f) = f^D$, eine Derivation von $R[\mathbf{X}]$ in $M[\mathbf{X}]$ und heißt *triviale Fortsetzung* von D .

Definitionen und Bemerkungen 3.7.2. R sei ein Ring und M ein R -Modul.

Auf $R \oplus M$ sei eine Multiplikation definiert durch

$$(a, u) \cdot (b, v) = (ab, av + bu).$$

Damit wird $R \oplus M$ zur R -Algebra mit Einselement $(1, 0)$ und wird mit $R \ltimes M$ bezeichnet. Der Strukturhomomorphismus $\varepsilon: R \rightarrow R \ltimes M$, definiert durch $\varepsilon(a) = (a, 0)$, ist ein Monomorphismus, die Projektion $\mu: R \ltimes M \rightarrow R$, definiert durch $\mu(a, u) = a$, ist ein R -Algebren-Epimorphismus, und für alle $u \in M$ ist $(0, u)^2 = (0, 0)$. Es ist $(R \ltimes M)^\times = \{(a, u) \in R \ltimes M \mid a \in R^\times\}$ [Beweis: Ist $(a, u) \in (R \ltimes M)^\times$, so ist $a = \mu(a, u) \in R^\times$; ist $a \in R^\times$ und $u \in M$, so folgt $(a, u) \cdot (a^{-1}, -a^{-2}u) = (1, 0)$].

Für eine Abbildung $F: R \rightarrow M$ sei $F^\times: R \rightarrow R \ltimes M$ definiert durch $F^\times(a) = (a, F(a))$. Es ist $\mu \circ F^\times = \text{id}_R$. Ist $K \subset R$ ein Teilring, so ist F genau dann K -linear, wenn F^\times K -linear ist.

Satz 3.7.3. *Sei R ein Ring und M ein R -Modul.*

1. *Eine Abbildung $D: R \rightarrow M$ ist genau dann eine Derivation, wenn $D^\times: R \rightarrow R \times M$ ein Ringhomomorphismus ist.*
2. *Zu jedem Ringhomomorphismus $G: R \rightarrow R \times M$ mit $\mu \circ G = \text{id}_R$ gibt es genau eine Derivation $D \in \text{Der}(R, M)$ mit $D^\times = G$ (es ist dann $G(a) = (a, D(a))$ für alle $a \in R$).*
3. (Fortsetzung von Derivationen). *Sei $D: R \rightarrow M$ eine Derivation, $\varphi: R \rightarrow A$ eine kommutative R -Algebra, P ein A -Modul, $\phi: M \rightarrow P$ ein R -Modulhomomorphismus und $D': A \rightarrow P$ eine Abbildung. Dann sind äquivalent:*
 - (a) *D' ist eine Derivation mit $D' \circ \varphi = \phi \circ D$.*
 - (b) *$D'^\times: A \rightarrow A \times P$ ist ein Ringhomomorphismus, $\mu \circ D'^\times = \text{id}_A$ und $D'^\times \circ \varphi = (\varphi, \phi) \circ D^\times$ (dabei ist $(\varphi, \phi): R \times M \rightarrow A \times P$ definiert durch $(\varphi, \phi)(a, u) = (\varphi(a), \phi(u))$).*

$$\begin{array}{ccc} R & \xrightarrow{D} & M & & R & \xrightarrow{D^\times} & R \times M \\ \varphi \downarrow & & \downarrow \phi & & \varphi \downarrow & & \downarrow (\varphi, \phi) \\ A & \xrightarrow{D'} & P & & A & \xrightarrow{D'^\times} & A \times P \end{array}$$

BEWEIS. 1. Für all $a, b \in R$ ist $D^\times(a)D^\times(b) = (a, D(a)) \cdot (b, D(b)) = (ab, aD(b) + bD(a))$ und $D^\times(ab) = (ab, D(ab))$. Daher ist D^\times genau dann ein Ringhomomorphismus, wenn D eine Derivation ist.

2. Sei $G: R \rightarrow R \times M$ ein Ringhomomorphismus mit $\mu \circ G = \text{id}_R$. Für eine Abbildung $D: R \rightarrow M$ ist genau dann $D^\times = G$, wenn $G(a) = (a, D(a))$ für alle $a \in R$. Daher gibt es genau eine Abbildung $D: R \rightarrow M$ mit $D^\times = G$, und diese ist nach 1. eine Derivation.

3. Nach 1. genügt es zu zeigen: Genau dann ist $D' \circ \varphi = \phi \circ D$, wenn $D'^\times \circ \varphi = (\varphi, \phi) \circ D^\times$. Für $a \in R$ ist aber $D'^\times \circ \varphi(a) = (\varphi(a), (D' \circ \varphi)(a))$ und $(\varphi, \phi) \circ D^\times(a) = (\varphi, \phi)(a, D(a)) = (\varphi(a), \phi \circ D(a))$, woraus die Behauptung folgt. \square

Satz 3.7.4. *Sei $R \subset A$ eine Ringerweiterung, $n \in \mathbb{N}$, $\mathbf{x} = (x_1, \dots, x_n) \in A^n$ und $A = R[\mathbf{x}]$. Sei $R[\mathbf{X}]$ mit $\mathbf{X} = (X_1, \dots, X_n)$ ein Polynomring, $\phi_{\mathbf{x}}: R[\mathbf{X}] \rightarrow A$ der Einsetzungshomomorphismus und $E \subset R[\mathbf{X}]$ mit $\text{Ker}(\phi_{\mathbf{x}}) = {}_{R[\mathbf{X}]} \langle E \rangle$. Sei M ein A -Modul, $D: R \rightarrow M$ eine Derivation und $(v_1, \dots, v_n) \in M^n$. Dann sind äquivalent:*

- (a) *Es gibt eine Derivation $D': A \rightarrow M$ mit $D'|_R = D$ und $D'(x_i) = v_i$ für alle $i \in [1, n]$.*
- (b) *Für alle $f \in E$ ist*

$$f^D(\mathbf{x}) + \sum_{i=1}^n \frac{\partial f}{\partial X_i}(\mathbf{x})v_i = 0.$$

Sind diese Bedingungen erfüllt, so gibt es genau eine Derivation $D' \in \text{Der}(A, M)$ mit $D'|_R = D$ und $D'(x_i) = v_i$ für alle $i \in [1, n]$. Ist $a \in A$ und $a = F(\mathbf{x})$ mit $F \in R[\mathbf{X}]$, so folgt

$$D'(a) = F^D(\mathbf{x}) + \sum_{i=1}^n \frac{\partial F}{\partial X_i}(\mathbf{x})v_i.$$

Insbesondere gilt: Ist $D' \in \text{Der}_R(A, M)$ und $D'(x_i) = 0$ für alle $i \in [1, n]$, so ist $D' = 0$.

BEWEIS. Nach Satz 3.7.3 gibt es genau dann eine [eindeutig bestimmte] Derivation $D' \in \text{Der}(A, M)$ mit $D'|_R = D$ und $D'(x_i) = v_i$ für alle $i \in [1, n]$, wenn es einen [eindeutig bestimmten] Ringhomomorphismus $G: A \rightarrow A \times M$ gibt, so dass $\mu \circ G = \text{id}_A$, $G|_R = D^\times$ und $G(x_i) = (x_i, v_i)$ für alle $i \in [1, n]$. Dabei kann man auf die Bedingung $\mu \circ G = \text{id}_A$ verzichten, denn aus den übrigen Bedingungen folgt: $\mu_A \circ G: A \rightarrow A$ ist ein Ringhomomorphismus mit $\mu \circ G|_R = \mu \circ D^\times = \text{id}_R$ und $\mu \circ G(x_i) = x_i$ für alle $i \in [1, n]$, also folgt $\mu \circ G = \text{id}_A$.

Genau dann gibt es einen [eindeutig bestimmten] Ringhomomorphismus $G: A \rightarrow A \times M$ mit $G|_R = D^\times$ und $G(x_i) = (x_i, v_i)$ für alle $i \in [1, n]$, wenn es einen [eindeutig bestimmten] Ringhomomorphismus $\tilde{G}: R[\mathbf{X}] \rightarrow A \times M$ gibt, so dass $\tilde{G}(f) = 0$ für alle $f \in E$, $\tilde{G}|_R = D^\times$ und $\tilde{G}(X_i) = (x_i, v_i)$ für alle $i \in [1, n]$. Nun gibt es aber genau einen Ringhomomorphismus $\tilde{G}: R[\mathbf{X}] \rightarrow A \times M$ mit $\tilde{G}|_R = D^\times$ und $\tilde{G}(X_i) = (x_i, v_i)$ für alle $i \in [1, n]$, und dieser ist gegeben durch

$$\tilde{G} \left(\sum_{\nu=(\nu_1, \dots, \nu_n) \in \mathbb{N}_0^n} c_\nu X_1^{\nu_1} \cdot \dots \cdot X_n^{\nu_n} \right) = \sum_{\nu \in \mathbb{N}_0^n} D^\times(c_\nu) \cdot (x_1, v_1)^{\nu_1} \cdot \dots \cdot (x_n, v_n)^{\nu_n}.$$

Für $x \in A$, $v \in M$ und $\nu \in \mathbb{N}_0$ ist

$$\begin{aligned} (x, v)^\nu &= [(x, 0) + (0, v)]^\nu = \sum_{j=0}^{\nu} \binom{\nu}{j} (x^{\nu-j}, 0) \cdot (0, v)^j = (x^\nu, 0) + \nu(x^{\nu-1}, 0) \cdot (0, v) \\ &= (x^\nu, 0) + (0, \nu x^{\nu-1} v). \end{aligned}$$

Daher folgt für $c \in R$ und $(\nu_1, \dots, \nu_n) \in \mathbb{N}_0^n$

$$\begin{aligned} D^\times(c) \cdot (x_1, v_1)^{\nu_1} \cdot \dots \cdot (x_n, v_n)^{\nu_n} &= (c, D(c)) \cdot \prod_{i=1}^n [(x_i^{\nu_i}, 0) + (0, \nu_i x_i^{\nu_i-1} v_i)] \\ &= (c, D(c)) \cdot \left(x_1^{\nu_1} \cdot \dots \cdot x_n^{\nu_n}, \sum_{i=1}^n \nu_i x_1^{\nu_1} \cdot \dots \cdot x_{i-1}^{\nu_{i-1}} x_i^{\nu_i-1} x_{i+1}^{\nu_{i+1}} \cdot \dots \cdot x_n^{\nu_n} v_i \right) \\ &= \left(c x_1^{\nu_1} \cdot \dots \cdot x_n^{\nu_n}, D(c) x_1^{\nu_1} \cdot \dots \cdot x_n^{\nu_n} + \sum_{i=1}^n c \nu_i x_1^{\nu_1} \cdot \dots \cdot x_{i-1}^{\nu_{i-1}} x_i^{\nu_i-1} x_{i+1}^{\nu_{i+1}} \cdot \dots \cdot x_n^{\nu_n} v_i \right), \end{aligned}$$

Folglich gilt für alle $f \in R[\mathbf{X}]$

$$\tilde{G}(f) = \left(f(\mathbf{x}), f^D(\mathbf{x}) + \sum_{i=1}^n \frac{\partial f}{\partial X_i}(\mathbf{x}) v_i \right).$$

Für $f \in E$ ist $f(\mathbf{x}) = 0$ und daher genau dann $\tilde{G}(f) = 0$, wenn

$$f^D(\mathbf{x}) + \sum_{i=1}^n \frac{\partial f}{\partial X_i}(\mathbf{x}) v_i = 0.$$

Ist $a = F(\mathbf{x}) = \phi_{\mathbf{x}}(F) \in A$ mit $F \in R[\mathbf{X}]$, so ist

$$G(a) = \tilde{G}(F) = \left(F(\mathbf{x}), F^D(\mathbf{x}) + \sum_{i=1}^n \frac{\partial F}{\partial X_i}(\mathbf{x}) v_i \right) = (a, D'(a)).$$

□

Satz 3.7.5. Sei R ein kommutativer Ring, M ein R -Modul, $D: R \rightarrow M$ eine Derivation und $T \subset R^\bullet$ eine multiplikativ abgeschlossene Teilmenge. Dann gibt es genau eine Derivation $D': T^{-1}R \rightarrow T^{-1}M$, so dass

$$D' \left(\frac{a}{1} \right) = \frac{D(a)}{1} \quad \text{für alle } a \in R, \quad \text{und für } t \in T \text{ ist dann } D' \left(\frac{a}{t} \right) = \frac{tD(a) - aD(t)}{t^2}.$$

Insbesondere folgt:

1. Ist R ein Bereich, $K = \mathfrak{q}(R)$ und M ein K -Vektorraum, so gibt es genau ein $D' \in \text{Der}(K, M)$ mit $D'|_R = D$.
2. Ist R ein Körper und $R_0 \subset R$ der Primkörper von R , so ist $D|_{R_0} = 0$.

BEWEIS. Der R -Modulisomorphismus $T^{-1}(R \times M) \rightarrow T^{-1}R \times T^{-1}M$ ist ein Ringisomorphismus (nachrechnen!), vermöge dessen wir die beiden Ringe identifizieren. $j: R \rightarrow T^{-1}R$ und $j': M \rightarrow T^{-1}M$ seien die Quotientenhomomorphismen (dann ist auch $(j, j'): R \times M \rightarrow T^{-1}R \times T^{-1}M$ der Quotientenhomomorphismus). Nach Satz 3.7.3.3 gibt es genau dann eine [eindeutig bestimmte] Derivation $D' \in \text{Der}(T^{-1}R, T^{-1}M)$ mit $D' \circ j = j' \circ D$, wenn es einen [eindeutig bestimmten] Ringhomomorphismus $G: T^{-1}R \rightarrow T^{-1}(R \times M)$ gibt mit $\mu \circ G = \text{id}_{T^{-1}R}$ und $G \circ j = (j, j') \circ D^\times$, das heißt, mit

$$(*) \quad G\left(\frac{a}{1}\right) = \left(\frac{a}{1}, \frac{D(a)}{1}\right) \quad \text{für alle } a \in R.$$

Definiert man $G_0: R \rightarrow T^{-1}(R \times M)$ durch $G_0(a) = \left(\frac{a}{1}, \frac{D(a)}{1}\right)$, so ist $G_0(T) \subset (T^{-1}(R \times M))^\times$, und daher gibt es genau einen Ringhomomorphismus $G: T^{-1}R \rightarrow T^{-1}(R \times M)$ mit $G \circ j = G_0$, also (*). Damit folgen Existenz und Eindeutigkeit von D' .

Ist $a \in R$ und $t \in T$, so folgt

$$\left(\frac{t}{1}, \frac{D(t)}{1}\right)^{-1} = \left(\frac{1}{t}, -\frac{D(t)}{t^2}\right),$$

also

$$G\left(\frac{a}{t}\right) = G\left(\left(\frac{t}{1}\right)^{-1} \left(\frac{a}{1}\right)\right) = \left(\frac{1}{t}, -\frac{D(t)}{t^2}\right) \cdot \left(\frac{a}{1}, \frac{D(a)}{1}\right) = \left(\frac{a}{t}, \frac{D(a)t - aD(t)}{t^2}\right)$$

und daher

$$D'\left(\frac{a}{t}\right) = \frac{D(a)t - aD(t)}{t^2}.$$

1. und 2. sind nun offensichtlich. □

Satz 3.7.6. Sei L/K eine Körpererweiterung, $a \in L \setminus K$ mit $L = K(a)$ und $D \in \text{Der}(K)$.

1. Ist a transzendent über K , so gibt es zu jedem $u \in L$ genau eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$ und $D'(a) = u$.
2. Sei a algebraisch über K und $f \in K[X]$ das Minimalpolynom von a über K .
 - (a) Ist a separabel über K , so gibt es genau eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$, und für diese ist

$$D'(a) = -\frac{f^D(a)}{f'(a)}.$$

- (b) Ist a inseparabel über K , so gibt es genau dann eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$, wenn $f^D = 0$. Ist $f^D = 0$, so gibt es zu jedem $u \in L$ genau eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$ und $D'(a) = u$.

BEWEIS. Mit Satz 3.7.4, angewandt auf $(D: K \rightarrow K \hookrightarrow L) \in \text{Der}(K, L)$.

1. Nach Satz 3.7.4 (mit $E = \emptyset$) gibt es zu jedem $u \in L$ genau ein $D_1 \in \text{Der}(K[a], L)$ mit $D_1(a) = u$, und nach Satz 3.7.5 gibt es genau ein $D' \in \text{Der}(L)$ mit $D'|_K[a] = D_1$.

2. Es ist $L = K[a] = K[X]/fK[X]$. Ist $u \in L$, so gibt es nach Satz 3.7.4 genau dann eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$ und $D'(a) = u$, wenn $f^D(a) + f'(a)u = 0$, und dann gibt es nur eine solche. Ist a über K separabel, so ist $f'(a) \neq 0$ und es folgt die Behauptung. Ist a über K inseparabel, so gibt es genau dann eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$ und $D'(a) = u$, wenn $f^D(a) = 0$. Da f normiert ist, ist $\text{gr}(f^D) < \text{gr}(f)$, also genau dann $f^D(a) = 0$, wenn $f^D = 0$. □

Satz 3.7.7. Sei L/K eine endlich erzeugte Körpererweiterung, $n \in \mathbb{N}$, $\mathbf{x} = (x_1, \dots, x_n) \in L^n$ und $L = K(\mathbf{x})$.

1. Die folgenden Aussagen sind äquivalent:
 - (a) L/K ist separabel algebraisch.
 - (b) Zu jeder Derivation $D \in \text{Der}(K)$ gibt es genau eine Derivation $D' \in \text{Der}(L)$ mit $D'|_K = D$.

(c) $\text{Der}_K(L) = \mathbf{0}$.

2. Sei $K[\mathbf{X}]$ mit $\mathbf{X} = (X_1, \dots, X_n)$ ein Polynomring, $\phi_{\mathbf{x}}: K[\mathbf{X}] \rightarrow K[\mathbf{x}]$ der Einsetzungshomomorphismus und $\text{Ker}(\phi_{\mathbf{x}}) = {}_{K[\mathbf{X}]} \langle f_1, \dots, f_m \rangle$ (mit $m \in \mathbb{N}$ und $f_1, \dots, f_m \in K[\mathbf{X}]$). Sei $s = \dim_L \text{Der}_K(L)$. Dann ist

$$s = n - \text{Rang} \left(\frac{\partial f_j}{\partial X_i}(\mathbf{x}) \right)_{i \in [1, n], j \in [1, m]},$$

und $s \in \mathbb{N}_0$ ist die kleinste Zahl mit folgender Eigenschaft:

Es gibt Indizes $1 \leq i_1 < \dots < i_s \leq n$, so dass $L/K(x_{i_1}, \dots, x_{i_s})$ separabel algebraisch ist.

3. Genau dann ist L/K separabel, wenn $\dim_L \text{Der}_K(L) = \text{tr}(L/K)$.

BEWEIS. 1. (a) \Rightarrow (b) Die Behauptung folgt nach Satz 3.7.6 mittels Induktion nach n .

(b) \Rightarrow (c) Sei $D \in \text{Der}_K(L)$, also $D|_K = 0 \in \text{Der}(K)$. Die Derivationen $D \in \text{Der}(L)$ und $0 \in \text{Der}(L)$ sind Fortsetzungen von $0 \in \text{Der}(K)$, und daher ist $D = 0$.

(c) \Rightarrow (a) Angenommen, L/K sei nicht separabel algebraisch. Sei (x_1, \dots, x_r) (mit $r \in \mathbb{N}_0$) eine Transzendenzbasis von L/K .

FALL 1: $L/K(x_1, \dots, x_r)$ ist separabel. Da L/K nicht separabel algebraisch ist, folgt $r > 0$. Nach Satz 3.7.6.1 gibt es eine Derivation $D_1 \in \text{Der}(K(x_1, \dots, x_r))$ mit $D_1|_K(x_1, \dots, x_{r-1}) = 0$ und $D_1(x_r) = 1$. Nach dem in (a) \Rightarrow (b) Gezeigten gibt es eine Derivation $D \in \text{Der}(L)$ mit $D|_K(x_1, \dots, x_r) = D_1$. Dann ist aber $0 \neq D \in \text{Der}_K(L)$.

FALL 2: $L/K(x_1, \dots, x_r)$ ist inseparabel. Sei $\text{char}(K) = p \in \mathbb{P}$ und M der separable Abschluss von $K(x_1, \dots, x_r)$ in L . Dann ist $[L : M] > 1$, L/M ist rein-inseparabel, und es sei $M \subset M_1 \subsetneq L$ ein maximaler Zwischenkörper. Ist $a \in L \setminus M_1$, so folgt $L = M_1(a)$, a ist inseparabel über M_1 , und nach Satz 3.7.6.2 gibt es eine Derivation $D \in \text{Der}(L)$ mit $D|_{M_1} = 0$ und $D(a) = 1$. Dann ist aber $0 \neq D \in \text{Der}_K(L)$.

2. Nach Satz 3.7.5 ist die Abbildung

$$\rho: \text{Der}_K(L) \rightarrow \text{Der}_K(K[\mathbf{x}], L), \quad \text{definiert durch} \quad \rho(D) = D|_{K[\mathbf{x}]},$$

ein L -Vektorraumisomorphismus. Nach Satz 3.7.4 ist die Abbildung

$$\lambda_0: \text{Der}_K(K[\mathbf{x}], L) \rightarrow L^n, \quad \text{definiert durch} \quad \lambda_0(D) = (D(x_1), \dots, D(x_n)),$$

ein L -Vektorraummonomorphismus mit

$$\text{Bi}(\lambda_0) = \left\{ (v_1, \dots, v_n) \in L^n \mid \sum_{i=1}^n \frac{\partial f_j}{\partial X_i}(\mathbf{x}) v_i = 0 \text{ für alle } j \in [1, m] \right\}.$$

Daher ist $\lambda = \lambda_0 \circ \rho: \text{Der}_K(L) \rightarrow L^n$ ein L -Vektorraummonomorphismus, für alle $D \in \text{Der}_K(L)$ ist $\lambda(D) = (D(x_1), \dots, D(x_n))$ und $\text{Bi}(\lambda) = \text{Bi}(\lambda_0)$. Es folgt

$$n - \text{Rang} \left(\frac{\partial f_j}{\partial X_i}(\mathbf{x}) \right)_{i \in [1, n], j \in [1, m]} = \dim_L \text{Bi}(\lambda_0) = \dim_L \text{Der}_K(K[\mathbf{x}], L) = \dim_L \text{Der}_K(L) = s.$$

Sei nun (D_1, \dots, D_s) eine L -Basis von $\text{Der}_K(L)$. Dann ist $(\lambda(D_1), \dots, \lambda(D_s)) \in (L^n)^s$ eine L -Basis von $\text{Bi}(\lambda)$. Daher hat die Matrix $(D_j(x_i))_{j \in [1, s], i \in [1, n]}$ den Rang s , und es sei (nach geeigneter Umnummerierung) $\det((D_j(x_i))_{i, j \in [1, s]}) \neq 0$. Wir setzten $M = K(x_1, \dots, x_s)$ und zeigen, dass L/M separabel algebraisch ist. Nach 1. genügt es, $\text{Der}_M(L) = \mathbf{0}$ zu zeigen. Ist $D \in \text{Der}_M(L) \subset \text{Der}_K(L)$, so gibt es $c_1, \dots, c_s \in L$ mit $D = c_1 D_1 + \dots + c_s D_s$, und für alle $i \in [1, s]$ folgt

$$0 = D(x_i) = \sum_{j=1}^s c_j D_j(x_i) \quad \text{und daher} \quad c_1 = \dots = c_s = 0, \quad \text{also} \quad D = 0.$$

Es bleibt die Minimalität von s zu zeigen. Sei also $t \in [0, n]$ und seien $1 \leq i_1 < \dots < i_t \leq n$, so dass $L/K(x_{i_1}, \dots, x_{i_t})$ separabel algebraisch ist. Dann müssen wir $s \leq t$ zeigen. Sei (nach geeigneter Umnummerierung) $L/K(x_1, \dots, x_t)$ separabel algebraisch. Sei

$$\lambda^*: \text{Der}_K(L) \rightarrow L^t \quad \text{definiert durch} \quad \lambda^*(D) = (D(x_1), \dots, D(x_t)).$$

Dann ist λ^* ein L -Vektorraumhomomorphismus mit

$$\text{Ker}(\lambda^*) = \{D \in \text{Der}_K(L) \mid D(x_1) = \dots = D(x_t) = 0\} = \text{Der}_{K(x_1, \dots, x_t)}(L) = \mathbf{0} \quad (\text{nach 1.})$$

Daher folgt $s = \dim_L \text{Der}_K(L) = \dim_L \text{Bi}(\lambda^*) \leq t$.

3. Nach 2. ist $r = \text{tr}(L/K) \leq s$, und es ist $r < s$, falls L/K nicht separabel ist. Ist L/K separabel, so gibt es eine separierende Transzendenzbasis (x_1, \dots, x_r) von L/K . Daher $s \leq r$ nach 2., also $s = r$. \square

Potenzreste und quadratisches Reziprozitätsgesetz

4.1. Allgemeines über Potenzreste

Definition 4.1.1. Seien $m, n \in \mathbb{N}_{\geq 2}$. Eine ganze Zahl $a \in \mathbb{Z}$ heißt *n-ter Potenzrest modulo m*, wenn es ein $x \in \mathbb{Z}$ gibt mit $a \equiv x^n \pmod{m}$ [äquivalent: $a + m\mathbb{Z}$ ist eine n -te Potenz in $\mathbb{Z}/m\mathbb{Z}$]. Man nennt a im Falle $n = 2$ einen *quadratischen Rest*, im Falle $n = 3$ einen *kubischen Rest* und im Falle $n = 4$ einen *biquadratischen Rest*.

Ist $a \in \mathbb{Z}$ und $\text{ggT}(a, m) = 1$, so bezeichnet $\text{ord}_m(a)$ die Ordnung von $a + m\mathbb{Z}$ in der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 4.1.2. Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$.

1. Sei $m = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ mit $r \in \mathbb{N}$, verschiedenen Primzahlen p_1, \dots, p_r und $e_1, \dots, e_r \in \mathbb{N}$. Genau dann ist a ein n -ter Potenzrest modulo m , wenn für alle $i \in [1, r]$ a ein n -ter Potenzrest modulo $p_i^{e_i}$ ist.
2. Sei $p \in \mathbb{P}$, $e \in \mathbb{N}$ und $a = p^d b$ mit $d \in \mathbb{N}_0$ und $b \in \mathbb{Z} \setminus p\mathbb{Z}$. Genau dann ist a ein n -ter Potenzrest modulo p^e , wenn
 - entweder $d \geq e$
 - oder $d < e$, $d \equiv 0 \pmod{n}$, und b ist n -ter Potenzrest modulo p^{e-d} .

BEWEIS. 1. Chinesischer Restsatz.

2. Im Falle $d \geq e$ ist $a \equiv 0 \equiv 0^n \pmod{p^e}$. Sei also im Folgenden $d < e$.

Sei $a = p^d b$ ein n -ter Potenzrest modulo p^e , $d < e$ und $x \in \mathbb{Z}$ mit $x^n \equiv a \pmod{p^e}$. Dann gibt es ein $u \in \mathbb{Z}$ mit $x^n = p^d b + p^e u = p^d(b + p^{e-d}u)$. Ist nun $x = p^c y$ mit $c \in \mathbb{N}_0$ und $y \in \mathbb{Z} \setminus p\mathbb{Z}$, so folgt $p^{nc} y^n = p^d(b + p^{e-d}u)$, also $d = nc$ und $y^n \equiv b \pmod{p^{e-d}}$.

Ist $d = nc < e$ mit $c \in \mathbb{N}_0$, und ist $y \in \mathbb{Z}$ mit $y^n \equiv b \pmod{p^{e-d}}$, so $(p^c y)^n \equiv a \pmod{p^e}$. □

Bemerkung 4.1.3. Aufgrund von Lemma 4.1.2 genügt es, n -te Potenzreste für prime Restklassen modulo Primzahlpotenzen zu studieren.

Lemma 4.1.4. Sei $k \in \mathbb{N}_0$.

1. Ist $p \in \mathbb{P} \setminus \{2\}$, so folgt $(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$, und $\text{ord}_{p^{k+1}}(1+p) = p^k$.
2. $5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$, und $\text{ord}_{2^{k+2}}(5) = 2^k$.

BEWEIS. 1. Es genügt, die Kongruenz zu zeigen, denn dann ist $(1+p)^{p^k} \equiv 1 \pmod{p^{k+1}}$, und im Falle $k \geq 1$ ist $(1+p)^{p^{k-1}} \equiv 1 + p^k \not\equiv 1 \pmod{p^{k+1}}$. Induktion nach k . Für $k = 0$ ist nichts zu zeigen.

$k \geq 0$, $k \rightarrow k+1$: Nach Induktionsvoraussetzung ist $(1+p)^{p^k} = 1 + p^{k+1} + up^{k+2} = 1 + p^{k+1}(1+pu)$ mit $u \in \mathbb{Z}$ und daher

$$(1+p)^{p^{k+1}} = \sum_{j=0}^p \binom{p}{j} p^{j(k+1)} (1+pu)^j \equiv 1 + p^{1+(k+1)}(1+pu) \equiv 1 + p^{k+2} \pmod{p^{k+3}},$$

denn $v_p(p^{p(k+1)}(1+pu)^p) = p(k+1) \geq k+3$, und für $j \in [2, p-1]$ ist

$$v_p\left(\binom{p}{j} p^{j(k+1)}(1+pu)^j\right) \geq 1 + 2(k+1) \geq k+3.$$

2. Es genügt, die Kongruenz zu zeigen, denn dann ist $5^{2^k} \equiv 1 \pmod{2^{k+2}}$, und im Falle $k \geq 1$ ist $5^{2^{k-1}} \equiv 1 + 2^{k+1} \not\equiv 1 \pmod{2^{k+2}}$. Induktion nach k . Für $k=0$ ist nichts zu zeigen.

$k \geq 0$, $k \rightarrow k+1$: Nach Induktionsvoraussetzung ist $5^{2^k} = 1 + 2^{k+2} + 2^{k+3}u = 1 + 2^{k+2}(1+2u)$ mit $u \in \mathbb{Z}$ und daher $5^{2^{k+1}} = 1 + 2^{k+3}(1+2u) + 2^{2k+4}(1+2u)^2 \equiv 1 + 2^{k+3} \pmod{2^{k+4}}$. \square

Satz 4.1.5 (Struktur der primen Restklassengruppen). *Sei $e \in \mathbb{N}$.*

1. Sei $p \in \mathbb{P} \setminus \{2\}$. Dann ist $(\mathbb{Z}/p^e\mathbb{Z})^\times$ eine zyklische Gruppe der Ordnung $p^{e-1}(p-1)$. Es ist $\text{ord}_{p^e}(1+p) = p^{e-1}$, $\langle (1+p) + p^e\mathbb{Z} \rangle = \{a + p^e\mathbb{Z} \mid a \in \mathbb{Z}, a \equiv 1 \pmod{p}\} \subset (\mathbb{Z}/p^e\mathbb{Z})^\times$, und für $x \in \mathbb{Z}$ ist genau dann $x^{p^{e-1}} \equiv 1 \pmod{p^e}$, wenn $x \equiv 1 \pmod{p}$. Ist $w \in \mathbb{Z}$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times = \langle w + p\mathbb{Z} \rangle$, so folgt $(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle w^{p^{e-1}} + p^e\mathbb{Z}, (1+p) + p^e\mathbb{Z} \rangle = \langle w^{p^{e-1}}(1+p) + p^e\mathbb{Z} \rangle$.
2. $|(\mathbb{Z}/2^e\mathbb{Z})^\times| = 2^{e-1}$. Ist $e \geq 3$, so ist $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle -1 + 2^e\mathbb{Z}, 5 + 2^e\mathbb{Z} \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z}$. Es ist $\text{ord}_{2^e}(5) = 2^{e-2}$, und $\langle 5 + 2^e\mathbb{Z} \rangle = \{a + 2^e\mathbb{Z} \mid a \in \mathbb{Z}, a \equiv 1 \pmod{4}\} \subset (\mathbb{Z}/2^e\mathbb{Z})^\times$.

BEWEIS. Für alle $p \in \mathbb{P}$ ist $(\mathbb{Z}/p^e\mathbb{Z})^\times = \{a + p^e\mathbb{Z} \mid a \in [0, p^e - 1], p \nmid a\}$, und daher folgt $|(\mathbb{Z}/p^e\mathbb{Z})^\times| = p^e - p^{e-1} = p^{e-1}(p-1)$.

1. Nach Lemma 4.1.4.1 ist $\text{ord}_{p^e}(1+p) = p^{e-1}$. Sei $\pi: (\mathbb{Z}/p^e\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ der natürliche Epimorphismus, definiert durch $\pi(a + p^e\mathbb{Z}) = a + p\mathbb{Z}$ für alle $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Dann ist

$$|\text{Ker}(\pi)| = \frac{p^{e-1}(p-1)}{p-1} = p^{e-1} = \text{ord}_{p^e}(1+p),$$

und wegen $\text{Ker}(\pi) = \{a + p^e\mathbb{Z} \mid a \in \mathbb{Z}, a \equiv 1 \pmod{p}\} \subset \langle (1+p) + p^e\mathbb{Z} \rangle$ folgt Gleichheit.

Ist $x \in \mathbb{Z}$ und $x^{p^{e-1}} \equiv 1 \pmod{p^e}$, so folgt $x \equiv x^{p^e} \equiv 1 \pmod{p}$. Ist $x \equiv 1 \pmod{p}$, so ist $x + p^e\mathbb{Z} \in \text{Ker}(\pi)$ und daher $x^{p^{e-1}} \equiv 1 \pmod{p^e}$.

Sei $w \in \mathbb{Z}$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \langle w + p\mathbb{Z} \rangle$. Wegen $w^{p^{e-1}} \equiv w \pmod{p}$ ist $\text{ord}_p(w^{p^{e-1}}) = p-1$, also auch $\text{ord}_{p^e}(w^{p^{e-1}}) = p-1$ und $\text{ord}_{p^e}(w^{p^{e-1}}(1+p)) = p^{e-1}(p-1)$. Damit folgt

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle w^{p^{e-1}}(1+p) + p^e\mathbb{Z} \rangle = \langle w^{p^{e-1}} + p^e\mathbb{Z}, (1+p) + p^e\mathbb{Z} \rangle.$$

2. Es genügt, den Fall $e \geq 3$ zu betrachten. Nach Lemma 4.1.4.2 ist $\text{ord}_{2^e}(5) = 2^{e-2}$. Sei $\pi: (\mathbb{Z}/2^e\mathbb{Z})^\times \rightarrow (\mathbb{Z}/4\mathbb{Z})^\times$ der natürliche Epimorphismus, definiert durch $\pi(a + 2^e\mathbb{Z}) = a + 4\mathbb{Z}$ für alle $a \in \mathbb{Z} \setminus 2\mathbb{Z}$. Wegen $|(\mathbb{Z}/4\mathbb{Z})^\times| = 2$ ist $|\text{Ker}(\pi)| = 2^{e-2} = \text{ord}_{2^e}(5)$, und wegen $5 + 2^e\mathbb{Z} \subset \text{Ker}(\pi)$ folgt Gleichheit. Wegen $-1 + 2^e\mathbb{Z} \notin \text{Ker}(\pi)$ und $\text{ord}_{2^e}(-1) = 2$ folgt $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle -1 + 2^e\mathbb{Z}, 5 + 2^e\mathbb{Z} \rangle$. \square

Lemma 4.1.6. *Sei G eine (multiplikative) endliche abelsche Gruppe mit neutralem Element e und $a \in G$.*

1. Sei $\text{ord}(a) = d \in \mathbb{N}$ und $k \in \mathbb{Z}$. Dann folgt

$$\text{ord}(a^k) = \frac{d}{\text{ggT}(k, d)}.$$

2. Seien $n_1, n_2 \in \mathbb{N}$ mit $\text{ggT}(n_1, n_2) = 1$ und $n = n_1 n_2$. Genau dann ist a eine n -te Potenz in G , wenn a eine n_1 -te und eine n_2 -te Potenz in G ist.

3. Sei G zyklisch, $|G| = N \in \mathbb{N}$ und $n \in \mathbb{N}$. Genau dann ist a eine n -te Potenz in G , wenn $a^{N/\text{ggT}(N, n)} = e$.

BEWEIS. 1. Für $j \in \mathbb{Z}$ gilt: $a^{kj} = e \iff d \mid kj \iff$

$$\iff \frac{d}{\text{ggT}(k, d)} \mid \frac{k}{\text{ggT}(k, d)} j \iff \frac{d}{\text{ggT}(k, d)} \mid j, \quad \text{und daher} \quad \text{ord}(a^k) = \frac{d}{\text{ggT}(k, d)}.$$

2. Ist $a = x^n$ mit $x \in G$, so folgt $a = (x^{n_2})^{n_1} = (x^{n_1})^{n_2}$. Seien nun $x_1, x_2 \in G$ mit $a = x_1^{n_1} = x_2^{n_2}$, und seien $u_1, u_2 \in \mathbb{Z}$ mit $n_1 u_1 + n_2 u_2 = 1$. Dann ist $a = a^{n_1 u_1 + n_2 u_2} = x_2^{n_2 n_1 u_1} x_1^{n_1 n_2 u_2} = (x_1^{u_2} x_2^{u_1})^n$.

3. Ist $a = x^n$ mit $x \in G$, so folgt $a^{N/\text{ggT}(N, n)} = (x^N)^{n/\text{ggT}(N, n)} = e$. Zum Beweis der Umkehrung sei $G = \langle g \rangle$, $a = g^k$ mit $k \in [0, N-1]$, und $e = a^{N/\text{ggT}(N, n)} = g^{kN/\text{ggT}(N, n)}$. Dann folgt $\text{ggT}(N, n) \mid k$, also gibt es $u, v \in \mathbb{Z}$ mit $k = Nu + nv$, und wir erhalten $a = g^k = g^{Nu} g^{nv} = (g^v)^n$. \square

Satz 4.1.7. A. Sei $p \in \mathbb{P} \setminus \{2\}$, $e \in \mathbb{N}$ und $a \in \mathbb{Z} \setminus p\mathbb{Z}$.

1. Ist $n \in \mathbb{N}$ und $p \nmid n$, so sind die folgenden Aussagen äquivalent:

- (a) a ist ein n -ter Potenzrest modulo p^e .
- (b) a ist ein n -ter Potenzrest modulo p .
- (c) $a^{(p-1)/\text{ggT}(p-1, n)} \equiv 1 \pmod{p}$.

2. Sei $d \in \mathbb{N}$. Genau dann ist a ein p^d -ter Potenzrest modulo p^e , wenn $a^{p-1} \equiv 1 \pmod{p^{\min\{e, d+1\}}}$.

B. Seien $d, e \in \mathbb{N}$, $e \geq 3$, $a \in \mathbb{Z}$ und $2 \nmid a$.

- 1. Genau dann ist a ein 2^d -ter Potenzrest modulo 2^e , wenn $a \equiv 1 \pmod{2^{\min\{e, d+2\}}}$.
- 2. Ist $n \in \mathbb{N}$ und $2 \nmid n$, so ist a ein n -ter Potenzrest modulo 2^e .

BEWEIS. **A.** Genau dann ist a ein n -ter Potenzrest modulo p^e , wenn $a + p^e \mathbb{Z}$ eine n -te Potenz in $(\mathbb{Z}/p^e \mathbb{Z})^\times$ ist. Nach Lemma 4.1.6 und Satz 4.1.5 ist das genau dann der Fall, wenn

$$a^B \equiv 1 \pmod{p^e}, \quad \text{wobei} \quad B = \frac{p^{e-1}(p-1)}{\text{ggT}(p^{e-1}(p-1), n)}.$$

1. Ist $p \nmid n$, so ist $\text{ggT}(p^{e-1}(p-1), n) = \text{ggT}(p-1, n)$, und für alle $x \in \mathbb{Z}$ ist genau dann $x^{p^{e-1}} \equiv 1 \pmod{p^e}$, wenn $x \equiv 1 \pmod{p}$ (siehe Satz 4.1.5). Daher folgt

$$a^B \equiv 1 \pmod{p^e} \iff (a^{(p-1)/\text{ggT}(p-1, n)})^{p^{e-1}} \equiv 1 \pmod{p^e} \iff a^{(p-1)/\text{ggT}(p-1, n)} \equiv 1 \pmod{p},$$

und damit die Äquivalenz der drei Bedingungen.

2. Ist $n = p^d$, so folgt $B = (p-1)p^k$ mit $k = e-1 - \min\{d, e-1\}$. Wegen $a^{p-1} \equiv 1 \pmod{p}$ gibt es ein $l \in [0, p^{e-1}-1]$, so dass $a^{p-1} \equiv (1+p)^l \pmod{p^e}$, und dann ist $a^B \equiv (1+p)^{lp^k} \pmod{p^e}$. Daher folgt:

$$\begin{aligned} a^B \equiv 1 \pmod{p^e} &\iff p^{e-1} \mid lp^k \iff p^{\min\{e-1, d\}} \mid l \\ &\iff (1+p)^l \equiv 1 \pmod{p^{\min\{e-1, d\}+1}} \iff a^{p-1} \equiv 1 \pmod{p^{\min\{e, d+1\}}}. \end{aligned}$$

B. 1. Ist a ein 2^d -ter Potenzrest modulo 2^e , so ist $a \equiv 1 \pmod{4}$, und wir nehmen an, es sei $a \equiv 5^l \pmod{2^e}$ mit $l \in [0, 2^{e-2}-1]$. Genau dann ist a ein 2^d -ter Potenzrest modulo 2^e , wenn $a + 2^e \mathbb{Z}$ eine 2^d -te Potenz in $\langle 5 + 2^e \mathbb{Z} \rangle$ ist. Nach Lemma 4.1.6 und Satz 4.1.5 ist das genau dann der Fall, wenn

$$a^B \equiv 1 \pmod{2^e}, \quad \text{wobei} \quad B = \frac{2^{e-2}}{\text{ggT}(2^{e-2}, 2^d)} = 2^k \quad \text{mit} \quad k = e-2 - \min\{e-2, d\}.$$

Wegen $a^B \equiv 5^{2^k l} \pmod{2^e}$ folgt:

$$\begin{aligned} a^B \equiv 1 \pmod{2^e} &\iff 2^{e-2} \mid 2^k l \iff 2^{\min\{e-2, d\}} \mid l \\ &\iff 5^l \equiv 1 \pmod{2^{\min\{e-2, d\}+2}} \iff a \equiv 1 \pmod{2^{\min\{e, d+2\}}}. \end{aligned}$$

2. Klar nach Lemma 4.1.6.3 \square

4.2. Quadratisches Reziprozitätsgesetz

Definition 4.2.1. Sei $p \in \mathbb{P} \setminus \{2\}$. Für $a \in \mathbb{Z} \setminus p\mathbb{Z}$ definieren wir das *Legendre-Symbol* durch

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{sonst.} \end{cases}$$

Folglich ist

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{falls } a + p\mathbb{Z} \in \mathbb{F}_p^{\times 2}, \\ -1, & \text{falls } a + p\mathbb{Z} \notin \mathbb{F}_p^{\times 2}, \end{cases} \quad \text{und wir definieren } \left(\frac{a + p\mathbb{Z}}{p}\right) = \left(\frac{a}{p}\right).$$

Die Abbildung

$$\left(\frac{\cdot}{p}\right): \mathbb{F}_p^\times \rightarrow \{\pm 1\}$$

heißt *quadratischer Charakter modulo* p .

Satz 4.2.2. Sei $p \in \mathbb{P} \setminus \{2\}$.

1. Ist $a \in \mathbb{Z} \setminus p\mathbb{Z}$, so gilt

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}, \quad \text{und} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod{4}, \\ -1, & \text{falls } p \equiv 3 \pmod{4}. \end{cases}$$

2. Für $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$ ist

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \text{und} \quad \left(\frac{\cdot}{p}\right): \mathbb{F}_p^\times \rightarrow \{\pm 1\} \quad \text{ist ein Gruppenhomomorphismus.}$$

BEWEIS. 1. Sei $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Dann ist $a^{(p-1)/2} + p\mathbb{Z}$ eine Nullstelle des Polynoms $X^2 - 1 \in \mathbb{F}_p[X]$ und daher $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Nach Satz 4.1.7.1 folgt

$$\left(\frac{a}{p}\right) = 1 \iff a^{(p-1)/2} \equiv 1 \pmod{p}, \quad \text{und daher} \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Die zweite Aussage folgt, da

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p} \iff \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

2. Nach 1. gilt

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}, \quad \text{und daher} \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Definitionen und Bemerkungen 4.2.3. Für $n \in \mathbb{N}$ sei

$$W_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{2\pi i k/n} \mid k \in [0, n-1]\} = \langle \zeta_n \rangle \quad \text{mit} \quad \zeta_n = e^{2\pi i/n}$$

die Gruppe der n -ten Einheitswurzeln. Für $k \in \mathbb{Z}$ und $\zeta \in W_n$ hängt ζ^k nur von der Restklasse $\kappa = k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ab, und wir definierten $\zeta^\kappa = \zeta^k$. Für $\zeta \in W_n$ ist

$$\sum_{\kappa \in \mathbb{Z}/n\mathbb{Z}} \zeta^\kappa = \begin{cases} n, & \text{falls } \zeta = 1, \\ 0, & \text{falls } \zeta \neq 1. \end{cases}$$

Das ist offensichtlich für $\zeta = 1$. Für $\zeta \neq 1$ ist

$$\sum_{\kappa \in \mathbb{Z}/n\mathbb{Z}} \zeta^\kappa = \sum_{k=0}^{n-1} \zeta^k = \frac{\zeta^n - 1}{\zeta - 1} = 0.$$

Für $p \in \mathbb{P}$ sei $\mathbb{X}_p = \text{Hom}(\mathbb{F}_p^\times, \mathbb{C}^\times)$. Die Elemente von \mathbb{X}_p heißen *Charaktere modulo p* . Sie bilden eine multiplikative Gruppe bei wertweiser Verknüpfung mit Einselement $\mathbf{1}$, definiert durch $\mathbf{1}(t) = 1$ für alle $t \in \mathbb{F}_p^\times$. Für $\chi \in \mathbb{X}_p$ ist $\bar{\chi} = \chi^{-1}$.

Definition 4.2.4. Für $p \in \mathbb{P}$, $\chi \in \mathbb{X}_p$ und $a \in \mathbb{F}_p$ definieren wir die *Gauß'schen Summen* durch

$$\tau_p(a, \chi) = \sum_{t \in \mathbb{F}_p^\times} \chi(t) \zeta_p^{at} \quad \text{und} \quad \tau_p(\chi) = \tau_p(1, \chi).$$

Satz 4.2.5. Sei $p \in \mathbb{P} \setminus \{2\}$, $\chi \in \mathbb{X}_p$ und $a \in \mathbb{F}_p$. Dann ist

$$\tau_p(a, \chi) = \begin{cases} p-1, & \text{falls } a=0 \text{ und } \chi = \mathbf{1}, \\ 0, & \text{falls } a=0 \text{ und } \chi \neq \mathbf{1}, \\ \overline{\chi(a)} \tau_p(\chi), & \text{falls } a \neq 0, \end{cases} \quad |\tau_p(\chi)| = \begin{cases} 1, & \text{falls } \chi = \mathbf{1}, \\ \sqrt{p}, & \text{falls } \chi \neq \mathbf{1}, \end{cases}$$

$$\overline{\tau_p(\chi)} = \chi(-1) \tau_p(\bar{\chi}), \quad \text{und} \quad \tau_p(\chi) \tau_p(\bar{\chi}) = \chi(-1)p, \quad \text{falls } \chi \neq \mathbf{1}.$$

BEWEIS. Nach Bemerkung 4.2.3 ist

$$\tau_p(a, \mathbf{1}) = \sum_{t \in \mathbb{F}_p^\times} \zeta_p^{at} = \sum_{t \in \mathbb{F}_p} \zeta_p^{at} - 1 = \begin{cases} p-1, & \text{falls } a=0, \\ -1, & \text{falls } a \neq 0. \end{cases}$$

Ist $a=0$ und $\chi \neq \mathbf{1}$, so gibt es ein $t_1 \in \mathbb{F}_p^\times$ mit $\chi(t_1) \neq 1$, und es folgt

$$\chi(t_1) \tau_p(0, \chi) = \chi(t_1) \sum_{t \in \mathbb{F}_p^\times} \chi(t) = \sum_{t \in \mathbb{F}_p} \chi(t_1 t) = \tau_p(0, \chi), \quad \text{also} \quad \tau_p(0, \chi) = 0.$$

Ist $a \neq 0$, so ist $\mathbb{F}_p^\times = \{at \mid t \in \mathbb{F}_p^\times\}$, und mit der Substitution $at = s$ folgt wegen $\chi(a^{-1}s) = \overline{\chi(a)} \chi(s)$

$$\tau_p(a, \chi) = \sum_{t \in \mathbb{F}_p^\times} \chi(t) \zeta_p^{at} = \sum_{s \in \mathbb{F}_p^\times} \chi(a^{-1}s) \zeta_p^s = \overline{\chi(a)} \sum_{s \in \mathbb{F}_p^\times} \chi(s) \zeta_p^s = \overline{\chi(a)} \tau_p(\chi).$$

Ist $\chi \neq \mathbf{1}$, so folgt

$$(p-1) |\tau_p(\chi)|^2 = \sum_{a \in \mathbb{F}_p} \tau_p(a, \chi) \overline{\tau_p(a, \chi)} = \sum_{s, t \in \mathbb{F}_p^\times} \chi(t) \overline{\chi(s)} \sum_{a \in \mathbb{F}_p} \zeta_p^{a(t-s)} = \sum_{t \in \mathbb{F}_p^\times} p = p(p-1)$$

und daher $|\tau_p(\chi)| = \sqrt{p}$. Schließlich ist noch

$$\chi(-1) \tau_p(\bar{\chi}) = \tau_p(-1, \bar{\chi}) = \sum_{t \in \mathbb{F}_p^\times} \bar{\chi}(t) \zeta_p^{-t} = \overline{\sum_{t \in \mathbb{F}_p^\times} \chi(t) \zeta_p^t} = \overline{\tau_p(\chi)}$$

und daher $\tau_p(\chi) \tau_p(\bar{\chi}) = \chi(-1) |\tau_p(\chi)|^2 = \chi(-1)p$. □

Satz 4.2.6 (Quadratisches Reziprozitätsgesetz).

1. Seien $p, q \in \mathbb{P} \setminus \{2\}$ und $p \neq q$. Dann ist

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} -1, & \text{falls } p \equiv q \equiv 3 \pmod{4}, \\ 1 & \text{sonst.} \end{cases}$$

2. Sei $p \in \mathbb{P} \setminus \{2\}$. Dann ist

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{falls } p \equiv \pm 3 \pmod{8}. \end{cases}$$

BEWEIS. Sei $\chi: \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ der quadratische Charakter, also

$$\chi(a + p\mathbb{Z}) = \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \quad \text{für alle } a \in \mathbb{Z} \setminus p\mathbb{Z}.$$

Wegen $\chi = \bar{\chi}$ ist $\tau_p(\chi)^2 = (-1)^{(p-1)/2}p$. Wir berechnen die Gauß'sche Summe $\tau_p(\chi) \in \mathbb{Z}[\zeta_p]$ modulo q (das heißt, wir rechnen im \mathbb{F}_q -Vektorraum $\mathbb{Z}[\zeta_p]/q\mathbb{Z}[\zeta_p]$). Es ist

$$\tau_p(\chi)^q = \left(\sum_{t \in \mathbb{F}_p^\times} \chi(t)\zeta_p^t\right)^q \equiv \sum_{t \in \mathbb{F}_p^\times} \chi(t)\zeta_p^{tq} = \tau_p(q + p\mathbb{Z}, \chi) = \left(\frac{q}{p}\right)\tau_p(\chi) \pmod{q}$$

und daher

$$\tau_p(\chi)^{q+1} \equiv \left(\frac{q}{p}\right)(-1)^{(p-1)/2}p \pmod{q}.$$

Andererseits ist aber

$$\begin{aligned} \tau_p(\chi)^{q+1} &= [\tau_p(\chi)^2]^{(q-1)/2}\tau_p(\chi)^2 = [(-1)^{(p-1)/2}p]^{(q-1)/2}(-1)^{(p-1)/2}p \\ &\equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right)(-1)^{(p-1)/2}p \pmod{q}, \end{aligned}$$

und daher

$$\left(\frac{q}{p}\right)(-1)^{(p-1)/2}p \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right)(-1)^{(p-1)/2}p \pmod{q}, \quad \text{also} \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

2. Wir rechnen in $\mathbb{Z}[i]$ modulo p (also im \mathbb{F}_p -Vektorraum $\mathbb{Z}[i]/p\mathbb{Z}[i]$). Es ist

$$(1+i)^{p+1} = [(1+i)^2]^{\frac{p-1}{2}}(1+i)^2 = (2i)^{\frac{p-1}{2}}(2i) \equiv \left(\frac{2}{p}\right)i^{\frac{p-1}{2}}(2i) \pmod{p},$$

aber auch $(1+i)^{p+1} = (1+i)^p(1+i) \equiv (1+i^p)(1+i) \pmod{p}$, und daher

$$\left(\frac{2}{p}\right)i^{\frac{p-1}{2}}(2i) \equiv (1+i^p)(1+i) \pmod{p}.$$

FALL 1: $p \equiv 1 \pmod{4}$. Dann ist $(1+i^p)(1+i) = 2i$ und $i^{(p-1)/2} = (-1)^{(p-1)/4}$. Damit folgt

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod{8}, \\ -1, & \text{falls } p \equiv 5 \pmod{8}. \end{cases}$$

FALL 2: $p \equiv 3 \pmod{4}$. Dann ist $(1+i^p)(1+i) = 2$ und $i^{(p+1)/2} = (-1)^{(p+1)/4}$. Damit folgt

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p+1)/4} = \begin{cases} 1, & \text{falls } p \equiv -1 \pmod{8}, \\ -1, & \text{falls } p \equiv 3 \pmod{8}. \end{cases}$$

Wegen

$$\frac{p^2-1}{8} \equiv \frac{p-1}{4}, \quad \text{falls } p \equiv 1 \pmod{4}, \quad \text{und} \quad \frac{p^2-1}{8} \equiv \frac{p+1}{4} \quad \text{falls } p \equiv 3 \pmod{4}$$

folgt die Behauptung. □