KOMMUTATIVE ALGEBRA, SS 2012. NOTIZEN ZUR VORLESUNG.

ULRICH GÖRTZ

Einführung

Die *Kommutative Algebra* behandelt die Theorie der kommutativen Ringe und von Moduln über solchen Ringen. Der Begriff des Moduls über einem Ring ist die natürliche Verallgemeinerung des Begriffs des Vektorraums über einem Körper. Zwei wichtige Beispielklassen kommutativer Ringe sind

Polynomringe über einem (algebraisch abgeschlossenen Körper) und ihre Quotienten nach Idealen. Ist k ein (algebraisch abgeschlossener) Körper und $I = (f_1, \dots, f_m) \subseteq R = k[X_1, \dots, X_n]$ ein Ideal, so reflektiert der Ring R/I viele geometrische Eigenschaften der gemeinsamen Nullstellenmenge

$$V(I) = \{(x_1, \dots, x_n) \in k^n; \forall i : \ f_i(x_1, \dots, x_n) = 0\} \subseteq k^n$$

der Polynome f_i (siehe Korollar 3.24, Korollar 3.25). Wegen der Möglichkeit, geometrische Eigenschaften in algebraische Eigenschaften eines Rings zu übersetzen, ist die Kommutative Algebra ein essenzielles Hilfsmittel der modernen algebraischen Geometrie.

Ganzheitsringe algebraische Zahlkörper. Sei $K/\mathbb{Q}$ eine endliche Körpererweiterung, und sei

$$\mathcal{O}_K = \{x \in K; \ \mathrm{minpol}_{\mathbb{Q}}(x) \in \mathbb{Z}[X]\}.$$

Der Ring $\mathcal{O}_K$ heißt der *Ring der ganzen Zahlen* von K. Er reflektiert wesentliche zahlentheoretische Eigenschaften des Körpers K. Siehe Kapitel 5.

Im Sinne der Übersetzung von algebraischen zu geometrischen Fragen (und umgekehrt), werden wir für jeden Ring R die Menge $\operatorname{Spec} R$ aller Primideale von R zu einem "geometrischen Objekt" zu machen (einem topologischen Raum), siehe Abschnitt 1.1. In der algebraischen Geometrie wird diese Sichtweise dann noch wesentlich ausgebaut. Die so verfügbare geometrische Intuition kann dann auch auf Situationen angewendet werden, die von zahlentheoretischen Fragen herkommen, etwa von Ringen der Form $\mathcal{O}_K$.

Literatur zur Kommutativen Algebra. Es gibt eine Reihe von sehr guten Büchern zur Kommutativen Algebra:

Atiyah, Macdonald [AM]. Einer der "Klassiker", der praktisch alle Ergebnisse der Vorlesung, und einiges darüberhinaus enthält. Ein großer Teil der Vorlesung lässt sich in diesem Buch direkt "wiederfinden". Im Abschnitt über Dedekindringe gehen wir allerdings etwas anders vor.

Matsumura [M2]. Ein sehr umfangreiches Buch, das über den Stoff von [AM] deutlich herausgeht. Insgesamt knapper geschrieben als [AM]. Von Matsumura gibt es auch noch das ältere Buch [M1], das zwar einen großen Durchschnitt mit dem neueren Buch hat, aber auch einige Themen abhandelt, die sich in letzterem nicht finden.

Bourbaki [B]. Die "Enzyklopädie" zur Kommutativen Algebra. Sehr umfangreich und ausführlich geschrieben, wegen der vielen Rückverweise ist es aber vielleicht nicht ganz leicht, sich dort auf Anhieb zurecht zu finden.

Eisenbud [E]. Ein relativ neues Buch zur kommutativen Algebra, das an vielen Stellen an die algebraische Geometrie anknüpft.

Zariski, Samuel [ZS]. Ein weiterer Klassiker, der aber insgesamt ein bisschen in die Jahre gekommen ist.

1. Ringe und Moduln

1.1. **Ringe und Ideale.** [AM] Ch. 1, [M2] §1

Definition 1.1. Eine Menge R zusammen mit Verknüpfungen $+\colon R \times R \to R$ (Addition) und $\cdot\colon R \times R \to R$ (Multiplikation) heißt kommutativer Ring mit 1, falls gilt:

(1) $(R, +)$ ist eine abelsche Gruppe. (Wir bezeichnen das neutrale Element bezüglich $+$ stets mit 0.)
(2) Die Multiplikation $\cdot$ ist assoziativ, besitzt ein neutrales Element (das wir stets mit 1 bezeichnen), verhält sich distributiv bezüglich $+$ und ist kommutativ.

Sofern nicht ausdrücklich etwas Anderes gesagt wird, verstehen wir in diesem gesamten Skript unter einem Ring stets einen kommutativen Ring mit 1.

Wir verwenden die üblichen Bezeichnungen: Der Multiplikationspunkt wird üblicherweise ausgelassen. Das Inverse von $a \in R$ bezüglich der Addition wird mit $-a$ bezeichnet, wir schreiben $a - b$ statt $a + (-b)$.

Beispiel 1.2. Die Menge $R = \{0\}$ mit $0 + 0 = 0$, $0 \cdot 0 = 0$, ist ein Ring, der sogenannte *Nullring*. Dies ist der einzige Ring, in dem $1 = 0$ gilt. Wir schreiben einfach $R = 0$.

Definition 1.3. Sei R ein Ring.

(1) Ein Element $a \in R$ heißt *Einheit*, falls ein Element $b \in R$ existiert mit $ab = 1$. Die Menge $R^\times$ aller Einheiten in R bildet eine Gruppe bezüglich der Multiplikation, die sogenannte *Einheitengruppe*.
(2) Ein Element $a \in R$ heißt *Nullteiler*, falls ein Element $b \in R$, $b \neq 0$, existiert mit $ab = 0$. Ist $R \neq 0$ und hat R keine Nullteiler außer 0, so heißt R *Integritätsring*.

Definition 1.4. Seien R, R' Ringe. Eine Abbildung $f\colon R \to R'$ heißt *Ringhomomorphismus*, wenn gilt:

(1) $f(x + y) = f(x) + f(y)$ für alle $x, y \in R$,

(2) $f(xy) = f(x)f(y)$ für alle $x, y \in R$,
(3) $f(1) = 1$.

Definition 1.5. Eine Teilmenge $S \subseteq R$ eines Ringes R heißt *Unterring*, falls $0, 1 \in S$ und S abgeschlossen bezüglich $+$, $-$ und $\cdot$ ist.

Definition 1.6. Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt *Ideal*, wenn I eine Untergruppe bezüglich der Addition ist, und wenn für alle $x \in R$, $y \in I$ gilt, dass $xy \in I$.

Bemerkung 1.7.
(1) In jedem Ring R sind $\{0\}$ (das *Nullideal*) und R (das *Einsideal*) Ideale.
(2) Der Durchschnitt von Idealen ist ein Ideal.
(3) Sind R ein Ring und ist $X \subseteq R$ eine Teilmenge, so ist

$$(X) := \bigcap_{I \subseteq R \text{ Ideal}, X \subseteq I} I = \left\{ \sum_{i=1}^{n} a_i x_i;\ n \geq 0, a_i \in R, x_i \in X \right\}$$

das kleinste Ideal von R, das X enthält. Wir nennen (X) das von X erzeugte Ideal. Ist $X = \{x_1, \dots, x_n\}$, so schreiben wir $(x_1, \dots, x_n) := (X)$. Beispiel: $(0) = \{0\}$, $(1) = R$. Ein Ideal I heißt *endlich erzeugt*, wenn endlich viele Elemente $x_1, \dots, x_n \in I$ existieren mit $I = (x_1, \dots, x_n)$. Ein Ideal I heißt *Hauptideal*, wenn ein Element $x \in I$ existiert mit $I = (x)$. Ein Integritätsring, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*.
(4) Sei R ein Ring. Sind $I_\nu \subseteq R$ Ideale, so heißt das von $\bigcup_\nu I_\nu$ erzeugte Ideal die *Summe* der Ideale I_ν, in Zeichen $\sum_\nu I_\nu$. Es gilt

$$\sum_\nu I_\nu = \left\{ \sum_\nu x_\nu;\ x_\nu \in I_\nu, \text{nur endlich viele } x_\nu \text{ ungleich} 0 \right\}.$$

Definition 1.8. Seien R ein Ring und $\mathfrak{a}$, $\mathfrak{b}$ Ideale von R. Dann heißt

$$\mathfrak{ab} = (ab;\ a \in \mathfrak{a}, b \in \mathfrak{b}) = \left\{ \sum_i a_i b_i;\ a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

das *Produkt* der Ideale $\mathfrak{a}$ und $\mathfrak{b}$.

Lemma 1.9. *Sei $f\colon R \to R'$ ein Ringhomomorphismus. Dann ist der* Kern $\operatorname{Ker} f := f^{-1}(0)$ *von f ein Ideal von R und das* Bild $\operatorname{Im} f = f(R)$ *von f ein Unterring von R'.*

Quotient nach einem Ideal. Sei R ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal. Die Relation

$$x \sim y \quad \iff \quad x - y \in \mathfrak{a}$$

definiert eine Äquivalenzrelation auf R, deren Äquivalenzklassen wir als die Nebenklassen von $\mathfrak{a}$ in R bezeichnen. Die Äquivalenzklasse von $x \in R$ ist

$$\overline{x} := x + \mathfrak{a} := \{x + a;\ a \in \mathfrak{a}\}.$$

Die Menge $R/\mathfrak{a}$ der Äquivalenzklassen wird durch die (wohldefinierten!) Verknüpfungen

$$\overline{x} + \overline{y} := \overline{x+y}, \qquad \text{und } \overline{x} \cdot \overline{y} := \overline{xy}$$

zu einem kommutativen Ring, und die Abbildung $\pi\colon R \to R/\mathfrak{a}$, $x \mapsto \overline{x}$, die als die *kanonische Projektion* bezeichnet wird, ist ein surjektiver Ringhomomorphismus.

Satz 1.10 (Homomorphiesatz/Universelle Eigenschaft des Quotienten)**.** *Seien R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Sei $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Ein Ringhomomorphismus $\varphi\colon R \to R'$ faktorisiert genau dann über π (d.h. es existiert $\psi\colon R/\mathfrak{a} \to R'$ mit $\psi \circ \pi = \varphi$), wenn $\mathfrak{a} \subseteq \operatorname{Ker}\varphi$. In diesem Fall gilt $\operatorname{Im}\varphi = \operatorname{Im}\psi$, und ψ ist genau dann injektiv, wenn $\mathfrak{a} = \operatorname{Ker}\varphi$.*

Satz 1.11 (Ideale des Quotienten)**.** *Seien R ein Ring und $\mathfrak{a} \subseteq R$ ein Ideal. Sei $\pi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Dann sind die Abbildungen*

$$\mathfrak{b} \mapsto \pi(\mathfrak{b}) \qquad \textit{und } \mathfrak{c} \mapsto \pi^{-1}(\mathfrak{c})$$

zueinander inverse, inklusionserhaltende Bijektionen zwischen der Menge aller Ideale von R, die $\mathfrak{a}$ enthalten, und der Menge aller Ideale von $R/\mathfrak{a}$.

Primideale und maximale Ideale.

Definition 1.12. Sei R ein Ring.

(1) Ein Ideal $\mathfrak{p} \subset R$ heißt *Primideal*, falls $\mathfrak{p} \neq R$ und für alle $x, y \in R$ mit $xy \in \mathfrak{p}$ gilt: $x \in \mathfrak{p}$ oder $y \in \mathfrak{p}$.
(2) Ein Ideal $\mathfrak{m} \subset R$ heißt *maximales Ideal*, falls $\mathfrak{m} \neq R$, und für alle Ideale $\mathfrak{m}' \neq R$ mit $\mathfrak{m} \subseteq \mathfrak{m}'$ gilt: $\mathfrak{m} = \mathfrak{m}'$.

Satz 1.13. *Sei R ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal.*

(1) *Das Ideal $\mathfrak{a}$ ist genau dann ein Primideal, wenn $R/\mathfrak{a}$ ein Integritätsring ist.*
(2) *Das Ideal $\mathfrak{a}$ ist genau dann ein maximales Ideal, wenn $R/\mathfrak{a}$ ein Körper ist.*

Insbesondere gilt: Jedes maximale Ideal ist ein Primideal.

Satz 1.14. *Sei R ein Ring, $\mathfrak{a}$ ein Ideal von R, $\mathfrak{a} \neq R$. Dann besitzt R ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Insbesondere besitzt jeder Ring $R \neq 0$ ein maximales Ideal.*

Satz 1.15. *Die Bijektionen in Satz 1.11 erhalten die Eigenschaften* Primideal *und* maximales Ideal.

Das Primspektrum eines Rings. Sei R ein Ring. Wir bezeichnen mit $\operatorname{Spec} R$ die Menge der Primideale in R und nennen $\operatorname{Spec} R$ das *Spektrum* oder *Primspektrum* von R. Wir bezeichnen mit $\operatorname{Spm} R$ die Menge aller maximalen Ideale von R und nennen $\operatorname{Spm} R$ das *Maximalspektrum* von R. Offenbar ist $\operatorname{Spm} R \subseteq \operatorname{Spec} R$.

Ist $\mathfrak{a} \subseteq R$ ein Ideal, so setzen wir

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} R;\ \mathfrak{a} \subseteq \mathfrak{p}\}.$$

Lemma 1.16. *Sei R ein Ring.*

1. $V((0)) = \operatorname{Spec} R$, $V((1)) = \emptyset$.
2. *Sind $\mathfrak{a}_i$, $i \in I$, Ideale von R, so gilt*
$$\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i).$$
3. *Sind $\mathfrak{a}$, $\mathfrak{b}$ Ideale von R, so gilt*
$$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}).$$

Satz 1.17. *Die Mengen $V(\mathfrak{a})$ für alle Ideale $\mathfrak{a} \subseteq R$ bilden die abgeschlossenen Mengen einer Topologie auf* $\operatorname{Spec} R$, *der sogenannten* Zariski-Topologie.

Satz 1.18. *Sei $\varphi\colon R \to R'$ ein Ringhomomorphismus. Dann ist*
$$\varphi^a\colon \operatorname{Spec} R' \to \operatorname{Spec} R, \qquad \mathfrak{p}' \mapsto \varphi^{-1}(\mathfrak{p}'),$$
eine stetige Abbildung.

Bemerkung 1.19. Die offenen Teilmengen der Form $D(f) := \operatorname{Spec} R \setminus V(f)$ heißen *ausgezeichnete offene Teilmengen.* Sie bilden eine Basis der Topologie, d.h. dass jede offene Teilmenge von $\operatorname{Spec} R$ eine Vereinigung von Teilmengen dieser Form ist. Außerdem sind endliche Durchschnitte von ausgezeichneten offenen Teilmengen wieder ausgezeichnete offene Teilmengen sind. Es gilt nämlich
$$\operatorname{Spec} R \setminus V(\mathfrak{a}) = \bigcup_{f\in\mathfrak{a}} D(f) \qquad \text{und} \quad D(f) \cap D(g) = D(fg).$$

1.2. **Lokale Ringe, Lokalisierung.** [AM] Ch. 3, [M2] §4

Definition 1.20. Ein Ring R heißt *lokaler Ring*, wenn R genau ein maximales Ideal $\mathfrak{m}$ besitzt. Wir bezeichnen dann den Körper $R/\mathfrak{m}$ als den Restklassenkörper von R. Wir schreiben: *Sei $(R, \mathfrak{m})$ ein lokaler Ring.* als Kurzform für: *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$.* Wir schreiben: *Sei $(R, \mathfrak{m}, k)$ ein lokaler Ring.* als Kurzform für: *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und Restklassenkörper k.*

Satz 1.21. *Sei R ein Ring, $\mathfrak{m} \subsetneq R$ ein Ideal. Dann sind äquivalent:*

1. *Der Ring R ist lokal mit maximalem Ideal $\mathfrak{m}$.*
2. *Es gilt $R \setminus \mathfrak{m} \subseteq R^\times$.*
3. *Das Ideal $\mathfrak{m}$ ist maximal und für alle $x \in \mathfrak{m}$ ist $1 + x \in R^\times$.*

Beispiele für lokale Ringe sind Körper und die Ringe
$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b};\ a, b \in \mathbb{Z},\ p \nmid b\right\}, \qquad p \ \text{Primzahl.}$$
Allgemeiner werden wir unten zu jedem Ring R und Primideal $\mathfrak{p} \subset R$ einen lokalen Ring $R_\mathfrak{p}$ konstruieren.

Definition 1.22. Sei R ein Ring. Eine Teilmenge $S \subseteq R$ heißt *multiplikative Teilmenge* (oder *multiplikatives System*), falls $1 \in S$ und für $s, s' \in S$ stets $ss' \in S$ gilt.

Sei R ein Ring und $S \subseteq R$ eine multiplikative Teilmenge. Die auf der Menge $R \times S$ durch

$$(r,s) \sim (r',s') \iff \exists t \in S\colon t(rs' - r's) = 0$$

definierte Relation ist eine Äquivalenzrelation. Wir bezeichnen die Äquivalenzklasse von (r,s) mit $\frac{r}{s}$, und die Menge der Äquivalenzklassen mit $S^{-1}R$.

Mit den (wohldefinierten!) Verknüpfungen

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'} \qquad \text{und } \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}$$

wird $S^{-1}R$ zu einem kommutativen Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$. Die Abbildung $\tau\colon R \to S^{-1}R$, $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus, und es gilt $\tau(S) \subseteq (S^{-1}R)^\times$. *Achtung: Im allgemeinen ist die Abbildung τ nicht injektiv!*

Der Ring $S^{-1}R$ zusammen mit dem Homomorphismus τ heißt die *Lokalisierung von R nach S*.

Satz 1.23 (Universelle Eigenschaft der Lokalisierung)**.** *Mit den obigen Notationen gilt: Ist $\varphi\colon R \to R'$ ein Ringhomomorphismus mit $\varphi(S) \subseteq (R')^\times$, so faktorisiert φ in eindeutiger Weise über $\tau\colon R \to S^{-1}R$.*

Ist R ein Integritätsring, $S \subseteq R$ eine multiplikative Teilmenge, so gilt $\frac{r}{s} = \frac{r'}{s'}$ genau dann, wenn $rs' = r's$. Für einen Integritätsring R erhält man für $S = R \setminus \{0\}$ als Lokalisierung $S^{-1}R$ einen Körper, den sogenannten *Quotientenkörper* $\operatorname{Quot}(R)$ von R.

Ist R ein Ring, $f \in R$, so ist $S := \{1, f, f^2, \dots\}$ eine multiplikative Teilmenge; in diesem Fall schreibt man $R_f := S^{-1}R$. Ist R ein Ring und $\mathfrak{p} \subset R$ ein Primideal, so ist $S := R \setminus p$ eine multiplikative Teilmenge; in diesem Fall schreibt man $R_\mathfrak{p} := S^{-1}R$.

Bemerkung 1.24. Sei R ein Ring, S eine multiplikative Teilmenge. Genau dann gilt $R = 0$, wenn $0 \in S$.

Satz 1.25. *Sei R ein Ring, $S \subseteq R$ eine multiplikative Teilmenge. Dann besteht eine Bijektion*

$$\operatorname{Spec} S^{-1}R \to \{\mathfrak{p} \in \operatorname{Spec} R;\ \mathfrak{p} \cap S = \emptyset\}, \quad \mathfrak{q} \mapsto \tau^{-1}(\mathfrak{q}).$$

Die Umkehrabbildung bildet $\mathfrak{p}$ ab auf das von $\tau(\mathfrak{p})$ in $S^{-1}R$ erzeugte Ideal (das wir mit $\mathfrak{p}S^{-1}R$ bezeichnen).

Definition 1.26. Sei R ein Ring, $\mathfrak{p} \in \operatorname{Spec} R$. Dann heißt

$$\kappa(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = \operatorname{Quot}(R/\mathfrak{p})$$

der *Restklassenkörper* von R in $\mathfrak{p}$.

Zu jedem $f \in R$, $\mathfrak{p} \in \operatorname{Spec} R$, bezeichnen wir mit $f(\mathfrak{p})$ das Bild von f in $\kappa(\mathfrak{p})$. In dieser Weise kann man die Elemente von f als Funktionen auf $\operatorname{Spec} R$ auffassen.

1.3. **Radikale.** [AM] Ch. 1, [M2] §1

Definition 1.27. Sei R ein Ring. Das Ideal

$$\mathrm{Jac}(R) := \bigcap_{\mathfrak{m}\in \mathrm{Spm}\, R} \mathfrak{m}$$

heißt das *Jacobson-Radikal von R.*

Beispiel 1.28. (1) $\mathrm{Jac}(\mathbb{Z}) = 0$.
(2) Ist k ein Körper, so ist $\mathrm{Jac}(k[X]) = 0$.

Lemma 1.29. *Sei R ein Ring. Dann gilt*

$$\mathrm{Jac}(R) = \{x \in R;\ \forall y \in R : 1 + xy \in R^\times\}.$$

Definition 1.30. Sei R ein Ring. Das Ideal

$$\mathrm{Rad}(R) := \bigcap_{\mathfrak{p}\in \mathrm{Spec}\, R} \mathfrak{p}$$

heißt das *(Nil-)Radikal von R.*

Definition 1.31. Sei R ein Ring. Ein Element $x \in R$ heißt *nilpotent*, wenn $n \geq 0$ existiert mit $x^n = 0$. Der Ring R heißt *reduziert*, wenn R keine nilpotenten Elemente $\neq 0$ enthält.

Satz 1.32. *Sei R ein Ring. Dann gilt*

$$\mathrm{Rad}(R) = \{x \in R;\ x \ \ \textit{nilpotent}\}.$$

Satz 1.33. *Sei R ein Ring und $\mathfrak{a}$ ein Ideal. Dann ist*

$$\bigcap_{\mathfrak{p}\in V(\mathfrak{a})} \mathfrak{p} = \{x \in R;\ \exists n \geq 0 : x^n \in \mathfrak{a}\},$$

und dieses Ideal heißt das Radikal von $\mathfrak{a}$ *und wird mit* $\sqrt{\mathfrak{a}}$ *bezeichnet. Gilt* $\mathfrak{a} = \sqrt{\mathfrak{a}}$*, so nennt man* $\mathfrak{a}$ *auch* Radikalideal.

Ist R ein Ring, und $\mathfrak{a} \subseteq R$ ein Ideal, so gilt $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.

Lemma 1.34. *Sei R ein Ring, $\mathfrak{a}$ ein Ideal von R, und seien $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in$ $\mathrm{Spec}\, R$ mit*

$$\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Dann existiert ein i mit $\mathfrak{a} \subseteq \mathfrak{p}_i$.

Lemma 1.35. *Sei R ein Ring, seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ Ideale, und sei $\mathfrak{p} \in$ $\mathrm{Spec}\, R$. Wenn*

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq p,$$

so gibt es ein i mit $\mathfrak{a}_i \subseteq p$. Gilt in der Voraussetzung sogar Gleichheit, so gilt sogar $\mathfrak{a}_i = p$.

1.4. **Moduln.** [AM] Ch. 2, 3, [M2] §2

Definition 1.36. Sei R ein Ring. Eine Menge M zusammen mit Verknüpfungen $+\colon M \times M \to M$, $\cdot\colon R \times M \times M$ heißt R-Modul, wenn gilt:

(1) $(M, +)$ ist eine abelsche Gruppe,
(2) für alle $r, s \in R$, $m \in M$ gilt: $(rs) \cdot m = r \cdot (s \cdot m)$,
(3) für alle $r, s \in R$, $m, n \in M$ gilt: $(r + s)m = rm + sm$, $r(m + n) = rm + rn$,
(4) für alle $m \in M$ gilt: $1 \cdot m = m$.

Definition 1.37. Sei R ein Ring. Eine Abbildung $f\colon M \to N$ zwischen R-Moduln M und N heißt *R-Modul-Homomorphismus*, falls gilt:

$$f(m + m') = f(m) + f(m'), \quad f(rm) = rf(m) \quad \text{für alle} \quad m, m' \in M, r \in R.$$

Ein Isomorphismus zwischen R-Moduln ist ein Homomorphismus, der einen Umkehrhomomorphismus besitzt.

Ist R ein Körper, so ist ein R-Modul nichts anderes als ein R-Vektorraum, und ein R-Modul-Homomorphismus nichts anderes als ein R-Vektorraum-Homomorphismus.

Wie im Vektorraumfall überprüft man leicht, dass jeder bijektive Homomorphismus ein Isomorphismus ist.

Definition 1.38. Sei R ein Ring. Eine *R-Algebra* A ist ein Ring, der auch eine R-Modulstruktur trägt, so dass die Ringaddition und die Moduladdition übereinstimmen, und die Ringmultiplikation und die Skalarmultiplikation verträglich sind: $r(xy) = (rx)y = x(ry)$ für alle $r \in R$, $x, y \in A$. In diesem Fall definiert die Zuordnung $r \mapsto r\cdot 1$ einen Ringhomomorphismus $\varphi\colon R \to A$.

Ist andersherum $\varphi\colon R \to A$ ein Ringhomomorphismus, so definiert die Skalarmultiplikation $r \cdot x := \varphi(r)x$ eine Algebrenstruktur auf A.

Genauer sollte man die hier definierten Algebren als *assoziative kommutative Algebren mit Eins* bezeichnen. Andere Algebren kommen aber in diesem Skript nicht vor.

Definition 1.39. Seien R ein Ring und M ein R-Modul. Eine Teilmenge $N \subseteq M$ heißt *Untermodul*, falls $0 \in N$ und N abgeschlossen ist unter Addition und unter Skalarmultiplikation mit Elementen aus R.

Bemerkung 1.40. Weil $(-1)n = -n$ ist ein Untermodul stets abgeschlossen unter Bildung des additiven Inversen. Daher ist eine Teilmenge eines R-Moduls genau dann ein Untermodul, wenn sie mit den Einschränkungen von $+$ und $\cdot$ selbst ein R-Modul ist.

Ist R ein Ring, so ist R selbst in offensichtlicher Weise ein R-Modul. Die R-Untermoduln von R sind genau die Ideale von R. Ein $\mathbb{Z}$-Modul ist “dasselbe” wie eine abelsche Gruppe; unter dieser Entsprechung entsprechen sich die Begriffe von Modulhomomorphismus und Gruppenhomomorphismus, und die Begriffe von Untermodul und Untergruppe.

Definition 1.41. Sei R ein Ring. Ein R-Modul M heißt *frei*, wenn er eine Basis besitzt, d.h. wenn eine Familie $(b_i)_i$ von Elementen aus M existiert, so dass sich jedes $m \in M$ in eindeutiger Weise als Linearkombination der b_i mit Koeffizienten in R schreiben lässt.

Über einen Körper sind alle Moduln frei: Das ist gerade der Satz, dass jeder Vektorraum eine Basis besitzt. Andererseits ist zum Beispiel der $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$ nicht frei.

Bemerkung 1.42. Sei R ein Ring.

(1) Die triviale abelsche Gruppe $\{0\}$ kann in eindeutiger Weise zu einem R-Modul gemacht werden, den wir auch mit 0 bezeichen. Dieser Modul heißt der Nullmodul. Der Ring R selbst ist in offensichtlicher Weise ein (freier) R-Modul.
(2) Sei M ein R-Modul. Der Durchschnitt von Untermodul von M ist ein Untermodul.
(3) Sind R ein Ring, M ein R-Modul und ist $X \subseteq M$ eine Teilmenge, so ist

$$\langle X\rangle_R := \bigcap_{N\subseteq M \quad \text{Untermodul}, X\subseteq N} N = \left\{\sum_{i=1}^{n} a_i x_i;\ n \geq 0, a_i \in R, x_i \in X\right\}$$

der kleinste Untermodul von M, der X enthält. Wir nennen $\langle X\rangle_R$ den von X erzeugten Untermodul. Ist $X = \{x_1, \dots, x_n\}$, so schreiben wir $\langle x_1, \dots, x_n\rangle_R := \langle X\rangle_R$. Ein Untermodul N heißt *endlich erzeugt*, wenn endlich viele Elemente $x_1, \dots, x_n \in N$ existieren mit $N = \langle x_1, \dots, x_n\rangle$.
(4) Sind $N_\nu \subseteq M$ Untermoduln, so heißt der von $\bigcup_\nu N_\nu$ erzeugte Untermodul die *Summe* der Untermoduln N_ν, in Zeichen $\sum_\nu N_\nu$.

Definition 1.43. Sei R ein Ring, $f\colon M \to N$ ein Homomorphismus von R-Moduln. Dann sind der *Kern* $\operatorname{Ker} f := f^{-1}(0)$ und das *Bild* $\operatorname{Im} f := f(M)$ von f Untermoduln von M bzw. von N.

Definition 1.44. Sei R ein Ring. Sind M, N zwei R-Moduln, so ist die Menge $\operatorname{Hom}_R(M, N)$ aller R-Modul-Homomorphismen von M nach N in natürlicher Weise ein R-Modul.

Definition 1.45. Sei R ein Ring, und sei $(M_i)_{i\in I}$ eine Familie von R-Moduln.

(1) Das kartesische Produkt $\prod_i M_i$ ist mit komponentenweiser Addition und Skalarmultiplikation ein R-Modul, das *(direkte) Produkt* der M_i.
(2) Die Teilmenge

$$\bigoplus_{i\in I} M_i := \{(m_i)_i \in \prod_i M_i;\ m_i = 0 \text{ für alle bis auf endlich viele } i\}$$

ist ein Untermodul von $\prod_i M_i$ und heißt die *direkte Summe* der M_i.

(3) Ist speziell $M_i = M$ für alle i, so schreiben wir auch $M^I := \prod_i M$, $M^{(I)} := \bigoplus_i M$.

Ist die Indexmenge I in der Definition endlich, so stimmen direktes Produkt und direkte Summe überein.

Lemma 1.46. *Sei R ein Ring, M ein R-Modul. Der R-Modul M ist genau dann frei, wenn eine Menge I existiert, so dass $M \cong R^{(I)}$.*

Direktes Produkt und direkte Summe lassen sich durch universelle Eigenschaften charakterisieren, es handelt sich gerade um das Produkt und das Koprodukt in der Kategorie der R-Moduln, siehe 2.3.

Lokalisierung von Moduln. Ist R ein Ring, M ein R-Modul und $S \subseteq R$ eine multiplikative Teilmenge, so kann man analog zur Lokalisierung von Ringen einen $S^{-1}R$-Modul $S^{-1}M$ aller Brüche $\frac{m}{s}$, $m \in M$, $s \in S$, konstruieren. Wie im Fall von Ringen gilt

$$\frac{m}{s} = \frac{m'}{s'} \quad \Longleftrightarrow \quad \exists t \in S\colon t(ms' - m's) = 0.$$

In Analogie zu den Schreibweisen $R_{\mathfrak{p}}$, R_f schreiben wir auch $M_{\mathfrak{p}}$, M_f.

Quotient eines Moduls nach einem Untermodul. Ist R ein Ring, M ein R-Modul und $N \subseteq M$ ein Untermodul, so ist die abelsche Gruppe M/N in natürlicher Weise ein R-Modul (mit $r(m+N) := (rm) + N$ als Skalarmultiplikation), und es gilt die offensichtliche Version des Homomorphiesatzes.

Lemma 1.47. *Ein R-Modul M ist genau dann endlich erzeugt, wenn $n \geq 0$ und ein Untermodul $N \subseteq R^n$ existieren mit $M \cong R^n/N$.*

Das Lemma von Nakayama.

Definition 1.48. Sind R ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal und M ein R-Modul, so sei

$$\mathfrak{a} \cdot M := \langle am;\ a \in \mathfrak{a}, m \in M \rangle_R.$$

Satz 1.49 (Lemma von Nakayama)**.** *Sei R ein Ring, $\mathfrak{a} \subseteq \mathrm{Jac}(R)$ ein Ideal von R und sei M ein endlich erzeugter R-Modul mit $\mathfrak{a}M = M$. Dann gilt $M = 0$.*

Korollar 1.50. *Sei R ein Ring, $\mathfrak{a} \subseteq \mathrm{Jac}(R)$ ein Ideal von R und sei M ein endlich erzeugter R-Modul. Ist $N \subseteq M$ ein Untermodul mit $N + \mathfrak{a}M = M$, so gilt $N = M$.*

Korollar 1.51. *Sei $(R, \mathfrak{m}, k)$ ein lokaler Ring und M ein endlich erzeugter R-Modul. Dann ist $M/\mathfrak{m}M$ in natürlicher Weise ein (endlich erzeugter) Vektorraum über dem Restklassenkörper k von R. Sind $x_1, \dots, x_n \in M$ Elemente, deren Restklassen in $M/\mathfrak{m}M$ ein Erzeugendensystem dieses k-Vektorraums bilden, so ist $x_1, \dots, x_n$ ein Erzeugendensystem von M.*

Definition 1.52. Sei R ein Ring, M ein R-Modul, $\mathfrak{p} \in \operatorname{Spec} R$. Dann heißt

$$M(\mathfrak{p}) := M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$$

die *Faser von M über $\mathfrak{p}$*.

Bemerkung 1.53. Sei M ein endlich erzeugter R-Modul, und seien $\mathfrak{p} \subseteq \mathfrak{p}'$ Primideale von R. Dann gilt $\dim_{\kappa(\mathfrak{p})} M(\mathfrak{p}) \leq \dim_{\kappa(\mathfrak{p}')} M(\mathfrak{p}')$.

Satz 1.54. *Sei R ein Ring, M ein R-Modul. Betrachte die Eigenschaften*

(1) $M = 0$.
(2) *Für alle* $\mathfrak{p} \in \operatorname{Spec} R$ *gilt* $M_{\mathfrak{p}} = 0$.
(3) *Für alle* $\mathfrak{m} \in \operatorname{Spm} R$ *gilt* $M_{\mathfrak{m}} = 0$.
(4) *Für alle* $\mathfrak{m} \in \operatorname{Spm} R$ *gilt* $M(\mathfrak{m}) = 0$.

Dann sind (1), (2), (3) äquivalent und implizieren (4). Ist M endlich erzeugt über R, so sind alle vier Eigenschaften äquivalent.

1.5. **Tensorprodukte.** [AM] Ch. 2, [M2] App. A

Sei R ein Ring.

Definition 1.55. Seien M, N zwei R-Moduln. Ein R-Modul T zusammen mit einer bilinearen Abbildung $\varphi\colon M \times N \to T$ heißt *Tensorprodukt von M und N über R*, falls für jeden R-Modul P und jede bilineare Abbildung $f\colon M \times N \to P$ genau ein R-Modulhomomorphismus $\psi\colon T \to P$ existiert, so dass $\psi \circ \varphi = f$.

Satz 1.56. *Seien M, N zwei R-Moduln. Dann existiert ein Tensorprodukt von M und N über R, und es ist eindeutig bestimmt bis auf eindeutigen Isomorphismus.*

Wir bezeichnen das Tensorprodukt von M und N über R mit $M \otimes_R N$, und das Bild von $(x, y) \in M \times N$ in $M \otimes_R N$ mit $x \otimes y$.

Beispiel 1.57. Ist K ein Körper und sind V, W zwei K-Vektorräume, so haben wir Identifizierungen

$$\operatorname{Hom}(V \otimes_K W, K) = \operatorname{Bil}(V \times W, K) = \operatorname{Hom}(V, W^\vee),$$

also ist $V \otimes_K W = \operatorname{Hom}_K(V, W^\vee)^\vee$.

Speziell können wir $K^m \otimes_K K^n$ mit $\operatorname{Mat}_{m\times n}(K)$ identifizieren.

Bemerkung 1.58. Seien R ein Ring und seien M, N zwei R-Moduln.

(1) Jedes Element von $M \otimes_R N$ ist eine endliche Summe von Elementen der Form $x \otimes y$, $x \in M$, $y \in N$.
(2) Seien $(x_i)_i$ ein Erzeugendensystem von M und $(y_i)_i$ ein Erzeugendensystem von N. Dann ist $(x_i \otimes y_i)_i$ ein Erzeugendensystem von $M \otimes_R N$.
(3) Wir haben kanonische Isomorphismen $R \otimes_R M \xrightarrow{\sim} M$, $r \otimes m \mapsto rm$ und $M \otimes N \xrightarrow{\sim} N \otimes M$, $m \otimes n \mapsto n \otimes n$.

(4) Das Tensorprodukt ist "funktoriell" im folgenden Sinne: Sind $\varphi\colon M \to M'$ und $\psi\colon N \to N'$ zwei R-Modulhomomorphismen, so erhalten wir einen R-Modul-Homomorphismus

$$\varphi \otimes \psi\colon M \otimes_R N \to M' \otimes_R N', \quad m \otimes n \mapsto m' \otimes n'.$$

Diese Konstruktion ist verträglich mit der Verkettung von Abbildungen.

Satz 1.59. *Seien M und N zwei R-Moduln, seien $x_i \in M$, $y_i \in N$ mit*

$$\sum_i x_i \otimes y_i = 0 \quad \text{in} \quad M \otimes_R N.$$

Dann existieren endlich erzeugte Untermoduln $M_0 \subseteq M$, $N_0 \subseteq N$, so dass $x_i \in M_0$, $y_i \in N_0$ für alle i und so dass

$$\sum_i x_i \otimes y_i = 0 \quad \text{in} \quad M_0 \otimes_R N_0.$$

Bemerkung 1.60. Analog zum obigen Fall kann man für multilineare (anstelle von bilinearen) Abbildungen vorgehen. Man erhält dann Tensorprodukte $M_1 \otimes_R M_2 \otimes \cdots \otimes_R M_n$. Man hat natürliche Identifikationen

$$M \otimes N \otimes P = (M \otimes N) \otimes P = M \otimes (N \otimes P),$$

und entsprechend für mehr als 3 Faktoren.

Bemerkung 1.61. Seien A, B Ringe, sei M ein A-Modul, P ein B-Modul, und sei N ein (A,B)-Bimodul, d.h. es sei N ein A-Modul und gleichzeitig ein B-Modul, so dass $(ax)b = a(xb)$ für alle $a \in A$, $b \in B$, $x \in N$. Wir schreiben hier die Skalarmultiplikation mit Elementen von B als Multiplikation von rechts.

Dann ist $M \otimes_A N$ ein B-Modul ("von rechts"), und $N \otimes_B P$ ein A-Modul ("von links"), und

$$(M \otimes_A N) \otimes_B P = M \otimes_A (N \otimes_B P), \quad m \otimes n \otimes p \mapsto m \otimes n \otimes p$$

ist ein Isomorphismus von (A,B)-Bimoduln, mit dem wir stets die beiden Seiten identifizieren.

Basiswechsel. Sei $\varphi\colon A \to B$ ein Ringhomomorphismus und M ein A-Modul. Dann wird der A-Modul $B \otimes_A M$ durch die (wohldefinierte!) Skalarmultiplikation

$$B \times (B \otimes_A M) \to B \otimes_A M, \quad (b, b' \otimes m) \mapsto (bb') \otimes m$$

zu einem B-Modul. Wir sagen, der B-Modul $B \otimes_A M$ entstehe aus M durch *Basiswechsel mit φ.*

Beispiel 1.62. (1) Sei R ein Ring, $S \subseteq R$ eine multiplikative Teilmenge, $\varphi\colon R \to S^{-1}$ der natürliche Homomorphismus und M ein R-Modul. Dann ist

$$S^{-1}R \otimes_R M \to S^{-1}M, \quad \frac{x}{s} \otimes m \mapsto \frac{xm}{s}$$

ein Isomorphismus von $S^{-1}R$-Moduln (mit Umkehrabbildung $\frac{m}{s} \mapsto \frac{1}{s} \otimes m$).

(2) Sei R ein Ring und $\mathfrak{a}$ ein Ideal. Sei $\varphi\colon R \to R/\mathfrak{a}$ die kanonische Projektion. Dann ist

$$R/\mathfrak{a} \otimes_R M \to M/\mathfrak{a}M, \quad \overline{x} \otimes m \mapsto \overline{xm}$$

ein Isomorphismus von $R/\mathfrak{a}$-Moduln (mit Umkehrabbildung $\overline{m} \mapsto 1 \otimes m$).

(3) Sei R ein Ring und $\mathfrak{p} \in \operatorname{Spec} R$ ein Primideal. Sei M ein R-Modul. Dann gilt

$$M(\mathfrak{p}) = M \otimes_R \kappa(\mathfrak{p}).$$

Bemerkung 1.63. Ist andererseits $\varphi\colon A \to B$ ein Ringhomomorphismus und N ein B-Modul, so kann man M als A-Modul auffassen durch die Skalarmultiplikation $a \cdot m := \varphi(a)m$. Wir bezeichnen den so erhaltenen A-Modul in der Regel wieder mit M.

Tensorprodukt von Algebren. Seien R ein Ring und A, B zwei R-Algebren. Dann wird $A \otimes_R B$ mit der (wohldefinierten!) Multiplikation

$$(a \otimes b)(a' \otimes b') := aa' \otimes bb'$$

zu einem Ring, und vermöge des Ringhomomorphismus $R \to A \otimes_R B$, $x \mapsto x \otimes 1 (= 1 \otimes x)$ zu einer R-Algebra. Mit den Ringhomomorphismen $\alpha : A \to A \otimes_R B$, $a \mapsto a \otimes 1$ bzw. $\beta : B \to A \otimes_R B$, $b \mapsto 1 \otimes b$ können wir $A \otimes_R B$ auch als A-Algebra bzw. als B-Algebra auffassen.

Satz 1.64 (Universelle Eigenschaft des Tensorprodukts von Algebren)**.** *Seien R ein Ring und seien A, B zwei R-Algebren.*

Es existiert ein kommutatives Diagramm

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\psi"] & A \arrow[d, "\alpha"] \\ B \arrow[r, "\beta"] & A \otimes_R B \end{tikzcd}$$

von Ringhomomorphismen, und für jeden Ring T zusammen mit Ringhomomorphismen $f : A \to T$, $g : B \to T$ mit $f \circ \varphi = g \circ \psi$ existiert ein eindeutig bestimmter Ringhomomorphismus $h : A \otimes_R B \to T$, so dass $f = h \circ \alpha$, $g = h \circ \beta$.

Mit den obigen Notationen ist $h(a \otimes b) = f(a) \cdot g(b)$.

Bemerkung 1.65 (Umformulierung des universellen Eigenschaft). Seien A, B zwei R-Algebren. Dann sind die Abbildungen $\alpha\colon A \to A \otimes_R B$, $a \mapsto a \otimes 1$, und $\beta\colon B \to A \otimes_R B$, $b \mapsto 1 \otimes b$, Homomorphismen von R-Algebren.

Für jede R-Algebra C und R-Algebren-Homomorphismen $f\colon A \to C$, $g\colon B \to C$ existiert ein eindeutig bestimmter Homomorphismus $h\colon A \otimes_R B \to C$ von R-Algebren, so dass $h \circ \alpha = f$, $h \circ \beta = g$.

Mit anderen Worten: Das Tensorprodukt $A \otimes_R B$ (zusammen mit den Abbildungen α β) erfüllt die universelle Eigenschaft des Koprodukts in der Kategorie der R-Algebren, siehe Definition 2.3.

Bemerkung 1.66.
(1) Ist B eine A-Algebra und ist $\mathfrak{a} \subseteq A$ ein Ideal, so gilt $A/\mathfrak{a} \otimes_A B = B/\mathfrak{a}B$.
(2) Ist B eine A-Algebra und ist $S \subseteq A$ eine multiplikative Teilmenge, so gilt $S^{-1}A \otimes_A B = S^{-1}B$.
(3) Ist B eine A-Algebra, so gilt $A[X] \otimes_A B = B[X]$.

2. Funktoren und exakte Sequenzen

2.1. **Kategorien und Funktoren.** [GW] App. A

Definition 2.1. Eine *Kategorie* $\mathscr{C}$ ist gegeben durch

(1) eine Klasse $\mathrm{Ob}(\mathscr{C})$ von *Objekten*
(2) für je zwei Objekte $X, Y \in \mathrm{Ob}(\mathscr{C})$ eine Klasse $\mathrm{Hom}_{\mathscr{C}}(X, Y)$ von *Morphismen* von X nach Y
(3) für je drei Objekte $X, Y, Z \in \mathrm{Ob}(\mathscr{C})$ eine Abbildung (*Verkettung von Morphismen*)

$$\mathrm{Hom}_{\mathscr{C}}(X, Y) \times \mathrm{Hom}_{\mathscr{C}}(Y, Z) \to \mathrm{Hom}_{\mathscr{C}}(X, Z), (f, g) \mapsto g \circ f,$$

(4) für jedes Objekt $X \in \mathrm{Ob}(\mathscr{C})$ ein Element $\mathrm{id}_X \in \mathrm{Hom}_{\mathscr{C}}(X, X)$ (*Identitätsmorphismus*),

so dass

(1) $f \circ \mathrm{id}_X = f$, $\mathrm{id}_X \circ g = g$ für alle f, g, für die die Verkettung existiert,
(2) $(f \circ g) \circ h = f \circ (g \circ h)$, für alle f, g, h, für die diese Verkettungen existieren.

Beispiel 2.2.
(1) Die Kategorie der Mengen: Objekte sind Mengen, Morphismen sind Abbildungen zwischen Mengen.
(2) Die Kategorie der Gruppen: Objekte sind Gruppen, Morphismen sind Gruppenhomomorphismen. Entsprechend: Die Kategorie der abelschen Gruppen.
(3) Sei R ein Ring. Die Kategorie $(R-\mathrm{Mod})$ der R-Moduln hat als Objekte die R-Moduln, als Morphismen die R-Modul-Homomorphismen. Die Kategorie $(R-\mathrm{Alg})$ der R-Algebren hat als Objekte die R-Algebren, als Morphismen die R-Algebra-Homomorphismen.
(4) Die Kategorie der topologischen Räume: Objekte sind topologische Räume, Morphismen sind stetige Abbildungen.
(5) Sei G ein Gruppe. Wir können eine Kategorie $\mathscr{C}$ definieren, die ein einziges Objekt X hat, und so dass $\mathrm{Hom}_{\mathscr{C}}(X, X) = G$. Die Verkettung von Morphismen sei durch die Multiplikation in G gegeben, id_X sei das neutrale Element von G.

(6) Als letztes Beispiel betrachte die Kategorie $\mathscr{C}$, deren Objekte alle Mengen sind, und so dass für Mengen X, Y die Menge der Morphismen definiert sei als

$$\mathrm{Hom}_{\mathscr{C}}(X,Y) = \{\Gamma \subseteq X \otimes Y \quad \text{Teilmenge}\}.$$

Die Verknüpfung sei folgendermaßen gegeben: Für $f \in \mathrm{Hom}(X,Y)$, $g \in \mathrm{Hom}(Y,Z)$ setze

$$g \circ f = \{(x,y) \in X \times Z;\ \exists y \in Y : (x,y) \in f, (y,z) \in g\} \in \mathrm{Hom}(X,Z).$$

Definition 2.3 (Kategorielle Sprechweisen)**.** Sei $\mathscr{C}$ eine Kategorie, $X, Y, \dots \in \mathrm{Ob}\,\mathscr{C}$.

(1) Die Elemente von $\mathrm{Hom}_{\mathscr{C}}(X,X)$ heißen *Endomorphismen* von X. Man schreibt auch $\mathrm{End}_{\mathscr{C}}(X) := \mathrm{Hom}_{\mathscr{C}}(X,X)$.
(2) Ein Element $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$ heißt *Isomorphismus*, falls ein Morphismus $g \in \mathrm{Hom}_{\mathscr{C}}(Y,X)$ existiert mit $g \circ f = \mathrm{id}_X$, $f \circ g = \mathrm{id}_Y$. Dann ist g eindeutig bestimmt, und heißt der Umkehrmorphismus zu f.
(3) Ein Element $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$ heißt *Monomorphismus*, falls für alle Z und alle $g, g' \in \mathrm{Hom}(Z,X)$ mit $f \circ g = f \circ g'$ gilt: $g = g'$.
(4) Ein Element $f \in \mathrm{Hom}_{\mathscr{C}}(X,Y)$ heißt *Epimorphismus*, falls für alle Z und alle $g, g' \in \mathrm{Hom}(Y,Z)$ mit $g \circ f = g' \circ f$ gilt: $g = g'$.
(5) Ein Objekt P von $\mathscr{C}$ zusammen mit Abbildungen $p\colon P \to X$, $q\colon P \to Y$ heißt *Produkt von X und Y in $\mathscr{C}$*, falls für alle Objekte T zusammen mit Abbildungen $p'\colon T \to X$, $q'\colon T \to Y$ ein eindeutig bestimmter Morphismus $f\colon T \to P$ in $\mathscr{C}$ existiert, so dass $p' = p \circ f$, $q' = q \circ g$. Das Produkt ist, sofern es existiert, eindeutig bestimmt bis auf eindeutigen Isomorphismus. Wir bezeichnen es mit $X \times Y$, und bezeichnen die Abbildungen p, q als die Projektionen auf X bzw. Y. Entsprechend kann man das Produkt $\prod_{i\in I} X_i$ definieren.
(6) Ein Objekt K von $\mathscr{C}$ zusammen mit Abbildungen $p\colon X \to K$, $q\colon Y \to K$ heißt *Koprodukt von X und Y in $\mathscr{C}$*, falls für alle Objekte T zusammen mit Abbildungen $p'\colon X \to T$, $q'\colon Y \to T$ ein eindeutig bestimmter Morphismus $f\colon K \to T$ in $\mathscr{C}$ existiert, so dass $p' = f \circ p$, $q' = g \circ q$. Das Koprodukt ist, sofern es existiert, eindeutig bestimmt bis auf eindeutigen Isomorphismus. Wir bezeichnen es mit $X \coprod Y$. Entsprechend kann man das Koprodukt $\coprod_{i\in I} X_i$ definieren.

Jeder Isomorphismus ist ein Monomorphismus und ein Epimorphismus.

Der Begriff des Koprodukts entsteht aus dem des Produkts durch "Umkehren alle Pfeile".

Beispiel 2.4. (1) Sei $\mathscr{C}$ die Kategorie der Mengen, der abelschen Gruppen oder allgemeiner der Moduln über einem Ring R. Dann ist eine Abbildung genau dann ein Isomorphismus, wenn sie bijektiv ist; genau dann ein Monomorphismus, wenn sie injektiv ist; genau dann ein Epimorphismus, wenn sie surjektiv ist.

(2) Punkt (1) ist auch richtig für die Kategorie der Gruppen, es ist aber nicht so leicht zu zeigen, dass jeder Epimorphismus surjektiv ist.
(3) Der Ringhomomorphismus $\mathbb{Z} \to \mathbb{Q}$ ist ein Epimorphismus, der nicht surjektiv ist. Zugleich ist er ein Monomorphismus, aber kein Isomorphismus.
(4) In der Kategorie der topologischen Räume gibt es Morphismen, die keine Isomorphismen, aber bijektive Abbildungen sind.

Beispiel 2.5. (1) In der Kategorie der Mengen existieren Produkte und Koprodukte für beliebige Indexmengen. Das Produkt in der Kategorie der Mengen ist das übliche kartesische Produkt. Das Koprodukt in der Kategorie der Mengen ist die disjunkte Vereinigung.
(2) Sei R ein Ring. In der Kategorie der R-Moduln existieren Produkte und Koprodukte für beliebige Indexmengen; siehe Definition 1.45.
(3) Sei $\mathscr{C}$ die Kategorie der Körper. Seien k, k' Körper unterschiedlicher Charakteristik. Dann existieren weder das Produkt von k und k' noch das Koprodukt von k und k' in $\mathscr{C}$ (denn es gibt keinen Körper, der Homomorphismen sowohl nach k als auch nach k' zulässt, und keinen Körper der Homomorphismen sowohl von k als auch von k' zulässt).
(4) Sei K ein Körper. In der Kategorie der endlich-dimensionalen K-Vektorräume existieren Produkte für endliche Indexmengen, jedoch (außer in trivialen Fällen) nicht für unendliche Indexmengen.

Funktoren.

Definition 2.6. Seien $\mathscr{C}$, $\mathscr{D}$ Kategorien. Ein (kovarianter) Funktor $F\colon \mathscr{C} \to \mathscr{D}$ ist gegeben durch

(1) für jedes $X \in \operatorname{Ob} \mathscr{C}$ ein Objekt $F(X) \in \operatorname{Ob} \mathscr{D}$,
(2) für jedes $f \in \operatorname{Hom}_{\mathscr{C}}(X, Y)$ ein $F(f) \in \operatorname{Hom}_{\mathscr{D}}(F(X), F(Y))$,

so dass

(1) $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ für alle $X \in \operatorname{Ob} \mathscr{C}$,
(2) $F(f \circ g) = F(f) \circ F(g)$ für alle f, g, so dass die Verkettung $f \circ g$ existiert.

Ein kontravarianter Funktor $F\colon \mathscr{C} \to \mathscr{D}$ ist gegeben durch

(1) für jedes $X \in \operatorname{Ob} \mathscr{C}$ ein Objekt $F(X) \in \operatorname{Ob} \mathscr{D}$,
(2) für jedes $f \in \operatorname{Hom}_{\mathscr{C}}(X, Y)$ ein $F(f) \in \operatorname{Hom}_{\mathscr{D}}(F(Y), F(X))$,

so dass

(1) $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ für alle $X \in \operatorname{Ob} \mathscr{C}$,
(2) $F(f \circ g) = F(g) \circ F(f)$ für alle f, g, so dass die Verkettung $f \circ g$ existiert.

Bemerkung 2.7. Funktoren bilden Isomorphismen auf Isomorphismen ab: Ist F ein Funktor und $X \cong Y$, so gilt $F(X) \cong F(Y)$.

Beispiel 2.8.
1. (Vergissfunktoren) Wir haben offensichtliche Funktoren von der Kategorie der Moduln über einem Ring R in die Kategorie der abelschen Gruppen; von der Kategorie der abelschen Gruppen in die Kategorie der Mengen; von der Kategorie der topologischen Räume in die Kategorie der Mengen usw., die durch Vergessen eines Teils der Struktur (der Skalarmultiplikation; der Addition; der Topologie usw.) gegeben sind. Funktoren dieser Art heißen Vergissfunktoren.
2. Sei K ein Körper. Der Funktor, der jeden K-Vektorraum auf seinen Dualraum und jede lineare Abbildung auf ihre duale Abbildung abbildet, ist ein kontravarianter Funktor von der Kategorie der K-Vektorräume in sich selbst.

Definition 2.9. Sei $\mathscr{C}$ eine Kategorie, und sei X ein Objekt von $\mathscr{C}$.

1. Der Hom-Funktor $\mathrm{Hom}(X, \cdot)$ ist der kovariante Funktor von $\mathscr{C}$ in die Kategorie der Mengen, der auf Objekten durch
$$Y \mapsto \mathrm{Hom}(X, Y)$$
und auf Morphismen durch
$$(f\colon Y \to Z) \mapsto (\mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z),\ g \mapsto f \circ g)$$
definiert ist.
2. Der Hom-Funktor $\mathrm{Hom}(\cdot, X)$ ist der kontravariante Funktor von $\mathscr{C}$ in die Kategorie der Mengen, der auf Objekten durch
$$Y \mapsto \mathrm{Hom}(Y, X)$$
und auf Morphismen durch
$$(f\colon Y \to Z) \mapsto (\mathrm{Hom}(Y, X) \to \mathrm{Hom}(Z, X),\ g \mapsto g \circ f)$$
definiert ist.
3. Ist $\mathscr{C}$ die Kategorie der Moduln über einem Ring R, so erhält man auf diese Weise Funktoren von $\mathscr{C}$ in die Kategorie der R-Moduln.

Lokalisierung ist ein Funktor. Seien R ein Ring, $S \subseteq R$ eine multiplikative Teilmenge. Wir definieren einen Funktor
$$F\colon (R - \mathrm{Mod}) \to (S^{-1}R - \mathrm{Mod})$$
durch $F(M) := S^{-1}M$, und indem wir einen Homomorphismus $f\colon M \to N$ auf
$$F(f)\colon S^{-1}M \to S^{-1}N, \quad \frac{m}{s} \mapsto \frac{f(m)}{s}$$
abbilden. Wir schreiben auch $S^{-1}f$ für $F(f)$.

Basiswechsel ist ein Funktor. Sei $R \to R'$ ein Ringhomomorphismus. Wir definieren den *Basiswechselfunktor*

$$(R - \text{Mod}) \to (R' - \text{Mod})$$

auf Objekten durch $M \mapsto R' \otimes_R M$ und auf Morphismen durch $(f\colon M \to N) \mapsto \mathrm{id}_{R'} \otimes f$, mit

$$\mathrm{id}_{R'} \otimes f\colon R' \otimes_R M \to R' \otimes_R N, \quad x \otimes m \mapsto x \otimes f(m)$$

Der Lokalisierungsfunktor ist der Spezialfall dieses Funktors für den Ringhomomorphismus $R \to S^{-1}R$.

2.2. **Exakte Sequenzen.** [AM] Ch. 2

Sei R ein Ring. Eine *Sequenz* von R-Moduln ist eine Familie M_i, $i \in \mathbb{Z}$, zusammen mit R-Modul-Homomorphismen

$$\cdots \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots$$

(analog für "Intervalle" in $\mathbb{Z}$ als Indexmengen).

Eine Sequenz heißt *Komplex*, falls $f_{i+1} \circ f_i = 0$ für alle i.

Eine Sequenz heißt *exakt an der Stelle i* (oder *bei M_i*), falls $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$. Sie heißt *exakt*, wenn sie an allen Stellen exakt ist.

Beispiel 2.10.

(1) Eine Sequenz

$$0 \longrightarrow M' \xrightarrow{f} M$$

ist genau dann exakt (bei M'), wenn f injektiv ist.

(2) Eine Sequenz

$$M \xrightarrow{f} M'' \longrightarrow 0$$

ist genau dann exakt (bei M''), wenn f surjektiv ist.

Definition 2.11. Eine exakte Sequenz der Form

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

heißt *kurze exakte Sequenz*. Die Exaktheit ist dazu äquivalent, dass f injektiv, g surjektiv, und dass $\operatorname{Ker} g = \operatorname{Im} f$ ist.

In der Situation der Definition induziert g einen Isomorphismus $M'' \cong M/M'$ (wobei wir M' vermöge der Injektion f als Untermodul von M auffassen). Ist andererseits $N \subseteq M$ ein Untermodul, so geben die Einbettung von N nach M und die kanonische Projektion auf den Quotienten Anlass zu einer kurzen exakten Sequenz

$$0 \to N \to M \to M/N \to 0.$$

Satz 2.12.

(1) *Sei*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

eine Sequenz von R-Moduln. Dann gilt: Die Sequenz ist genau dann exakt, wenn für alle R-Moduln N die Sequenz

$$0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N)$$

(vergleiche Definition 2.9) exakt ist.

(2) *Sei*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

eine Sequenz von R-Moduln. Dann gilt: Die Sequenz ist genau dann exakt, wenn für alle R-Moduln N die Sequenz

$$0 \to \mathrm{Hom}(N, M') \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N, M'')$$

(vergleiche Definition 2.9) exakt ist.

Satz 2.13 (Schlangenlemma)**.** *Sei R ein Ring und*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u} & N & \xrightarrow{v} & N'' & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von R-Moduln, in dem die Zeilen exakte Sequenzen sind. Dann existiert eine exakte Sequenz

$$0 \longrightarrow \mathrm{Ker}\, f' \xrightarrow{\overline{u}} \mathrm{Ker}\, f \xrightarrow{\overline{v}} \mathrm{Ker}\, f'' \xrightarrow{d}$$

$$N'/\,\mathrm{Im}\, f' \xrightarrow{\overline{u'}} N/\,\mathrm{Im}\, f \xrightarrow{\overline{v'}} N''/\,\mathrm{Im}\, f'' \longrightarrow 0,$$

wobei $\overline{u}$, $\overline{v}$, $\overline{u'}$, $\overline{v'}$ die von u, v, u', v' induzierten Abbildungen sind.

Korollar 2.14. *Wenn in der Situation des Schlangenlemmas zwei der drei Homomorphismen f', f, f'' Isomorphismen sind, so auch der dritte.*

2.3. **Exakte Funktoren.** [AM] Ch. 2, 3

Seien R und R' Ringe. Für R-Moduln M, N trägt die Menge $\mathrm{Hom}_R(M, N)$ durch die Gruppenstruktur auf N die Struktur einer abelschen Gruppe (und sogar, induziert durch die R-Modulstruktur auf N die Struktur eines R-Moduls).

Definition 2.15. Ein (kovarianter) Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *additiv*, falls für alle R-Moduln M, N die durch F gegebene Abbildung

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{R'}(F(M), F(N))$$

ein Homomorphismus abelscher Gruppen ist.

Ein kontravarianter Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *additiv*, falls für alle R-Moduln M, N die durch F gegebene Abbildung

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{R'}(F(N), F(M))$$

ein Homomorphismus abelscher Gruppen ist.

Bemerkung 2.16. Ist F ein additiver Funktor, so gilt $F(0) = 0$.

Definition 2.17.

(1) Ein kovarianter Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *linksexakt*, falls F additiv ist und falls für jede kurze exakte Sequenz
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
die Sequenz
$$0 \to F(M_1) \to F(M_2) \to F(M_3)$$
exakt ist.

(2) Ein kontravarianter Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *linksexakt*, falls F additiv ist und falls für jede kurze exakte Sequenz
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
die Sequenz
$$0 \to F(M_3) \to F(M_2) \to F(M_1)$$
exakt ist.

(3) Ein kovarianter Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *rechtsexakt*, falls F additiv ist und falls für jede kurze exakte Sequenz
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
die Sequenz
$$F(M_1) \to F(M_2) \to F(M_3) \to 0$$
exakt ist. Analog: rechtsexakte kontravariante Funktoren.

(4) Ein kovarianter Funktor $F\colon (R-\mathrm{Mod}) \to (R'-\mathrm{Mod})$ heißt *exakt*, falls F additiv ist und falls für jede kurze exakte Sequenz
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
die Sequenz
$$0 \to F(M_1) \to F(M_2) \to F(M_3) \to 0$$
exakt ist, d. h. wenn F linksexakt und rechtsexakt ist. Analog: exakte kontravariante Funktoren.

Bemerkung 2.18.

(1) Sei F ein linksexakter kovarianter Funktor und sei $0 \to M_1 \to M_2 \to M_3$ exakt. Dann ist $0 \to F(M_1) \to F(M_2) \to F(M_3)$ exakt. Analog für kontravariante Funktoren.

(2) Sei F ein rechtsexakter kovarianter Funktor und sei $M_1 \to M_2 \to M_3 \to 0$ exakt. Dann ist $F(M_1) \to F(M_2) \to F(M_3) \to 0$ exakt. Analog für kontravariante Funktoren.

(3) Sei F ein exakter kovarianter Funktor und sei $M_1 \to M_2 \to M_3$ exakt. Dann ist $F(M_1) \to F(M_2) \to F(M_3)$ exakt. Analog für kontravariante Funktoren.

Der Hom-*Funktor ist linksexakt.*

Satz 2.19. *Seien R ein Ring und N ein R-Modul. Dann sind die Funktoren* $\mathrm{Hom}_R(\cdot, N)$ *und* $\mathrm{Hom}(N, \cdot)$ *linksexakt. (Vergleiche Definition 2.9 und Satz 2.12).*

Tensorprodukt ist rechtsexakt.

Satz 2.20. *Seien R ein Ring und N ein R-Modul. Dann ist der Funktor $M \mapsto M \otimes_R N$ rechtsexakt.*

Flache Moduln.

Definition 2.21. Sei R ein Ring. Ein R-Modul M heißt *flach*, wenn der Funktor $N \mapsto M \otimes_R N$ exakt ist.

Weil Tensorieren stets rechtsexakt ist, ist ein R-Modul M genau dann flach, wenn für jeden injektiven Homomorphismus $\varphi : N' \to N$ von R-Moduln auch der Homomorphismus $\mathrm{id}_M \otimes \varphi : M \otimes_R N' \to M \otimes_R N$ injektiv ist.

Beispiel 2.22. Sei $n \in \mathbb{Z}_{>0}$. Dann ist der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ nicht flach.

Satz 2.23. *Ist R ein Ring und M ein freier R-Modul, so ist M flach.*

Insbesondere folgt aus dem Satz: Ist K ein Körper, so ist jeder K-Vektorraum flach.

Eine R-Algebra A heißt flach, wenn A als R-Modul flach ist.

Beispiel 2.24. Sei k ein Körper, $R = k[T]$.

(1) Die R-Algebren $R[X]/(X - T)$ und $R[X]/(X^2 - T)$ sind flach (sie sind sogar freie R-Moduln).
(2) Die R-Algebra $R[X]/(XT - 1)$ ist flach (aber kein freier R-Modul).
(3) Die R-Algebra $R[X]/(XT)$ ist nicht flach.

2.3.1. *Lokalisierung ist exakt.*

Satz 2.25. *Seien R ein Ring und $S \subseteq R$ eine multiplikative Teilmenge. Dann ist der Funktor $M \mapsto S^{-1}M$ exakt.*

Korollar 2.26. *Sei R ein Ring, und sei $S \subseteq R$ eine multiplikative Teilmenge. Ist $N \subseteq M$ eine Inklusion von R-Moduln, so ist $S^{-1}N \subseteq S^{-1}M$ und $S^{-1}M/S^{-1}N \cong S^{-1}(M/N)$.*

Satz 2.27. *Sei R ein Ring, $f\colon M \to N$ ein R-Modul-Homomorphismus. Dann sind äquivalent:*

(1) $f = 0$
(2) *Für alle $\mathfrak{p} \in \operatorname{Spec} R$ ist $f \otimes \mathrm{id}_{R_\mathfrak{p}}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ die Nullabbildung.*
(3) *Für alle $\mathfrak{m} \in \operatorname{Spm} R$ ist $f \otimes \mathrm{id}_{R_\mathfrak{m}}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ die Nullabbildung.*

Satz 2.28. *Sei R ein Ring, und sei*

$$M' \to M \to M''$$

eine Sequenz von R-Moduln. Dann sind äquivalent:

(1) *Die Sequenz* $M' \to M \to M''$ *ist exakt.*
(2) *Für alle* $\mathfrak{p} \in \operatorname{Spec} R$ *ist die Sequenz* $(M')_\mathfrak{p} \to M_\mathfrak{p} \to (M'')_\mathfrak{p}$ *exakt.*
(3) *Für alle* $\mathfrak{m} \in \operatorname{Spm} R$ *ist die Sequenz* $(M')_\mathfrak{m} \to M_\mathfrak{m} \to (M'')_\mathfrak{m}$ *exakt.*

Satz 2.29. *Sei* R *ein Ring und sei* M *ein* R*-Modul. Dann sind äquivalent:*
(1) *Der* R*-Modul* M *ist flach.*
(2) *Für alle* $\mathfrak{p} \in \operatorname{Spec} R$ *ist der* $R_\mathfrak{p}$*-Modul* $M_\mathfrak{p}$ *flach.*
(3) *Für alle* $\mathfrak{m} \in \operatorname{Spm} R$ *ist der* $R_\mathfrak{m}$*-Modul* $M_\mathfrak{m}$ *flach.*

3. Ganze und endliche Ringhomomorphismen

3.1. **Definitionen, einfache Eigenschaften.** [AM] Ch. 5, [M2] §9

Definition 3.1. Sei $\varphi\colon A \to B$ ein Ringhomomorphismus.
(1) Ein Element $b \in B$ heißt *ganz über* A *(bezüglich* φ*)*, wenn ein normiertes Polynom $f \in R[X]$ existiert mit $f(b) = 0$.
(2) Der Homomorphismus φ heißt *ganz*, falls jedes Element $b \in B$ ganz über A ist.
(3) Der Homomorphismus φ heißt *endlich*, falls B als A-Modul endlich erzeugt ist.

Definition 3.2. Sei B eine A-Algebra. Dann heißt B eine *endlich erzeugte* A*-Algebra*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:
(1) Es existieren endlich viele Elemente $b_1, \dots, b_n \in B$, so dass B die kleinste A-Unteralgebra von B ist, die alle b_i enthält.
(2) Es existiert $n \geq 0$ und ein surjektiver A-Algebren-Homomorphismus $A[X_1, \dots, X_n] \to B$.

Im folgenden Satz benutzen wir die Determinante von quadratischen Matrizen mit Einträgen in einem beliebigen kommutativen Ring. Wir definierten die Determinante durch die Leibniz-Formel. Insbesondere können wir dann zu jeder Matrix $m \in \operatorname{Mat}_{n\times n}(R)$ die Komplementärmatrix von m im Sinne der Cramerschen Regel bilden.

Satz 3.3. (1) *(Cramersche Regel) Sei* R *ein Ring,* $m \in \operatorname{Mat}_{n\times n}(R)$*. Sei* $\tilde{m}$ *die Komplementärmatrix von* m *im Sinne der Cramerschen Regel. Dann gilt*
$$m\tilde{m} = \tilde{m}m = \det(m)E_n.$$
(2) *("Cayley-Hamilton") Sei* M *ein endlich erzeugter* R*-Modul,* $\mathfrak{a} \subseteq R$ *ein Ideal, und* $\varphi\colon M \to M$ *ein* R*-Endomorphismus von* M *mit* $\varphi(M) \subseteq \mathfrak{a}M$*. Dann existieren Elemente* $a_i \in \mathfrak{a}$ *mit*
$$\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 \operatorname{id}_M = 0 \qquad in \operatorname{End}(M).$$

Satz 3.4. *Sei* $\varphi\colon A \to B$ *ein Ringhomomorphismus, und sei* $b \in B$*. Dann sind äquivalent:*
(1) *Das Element* b *ist ganz über* A*.*
(2) *Die von* b *erzeugte* A*-Algebra* $A[b]$ *ist als* A*-Modul endlich erzeugt, d.h.* $A \to A[b]$ *ist ein endlicher Ringhomomorphismus.*

(3) *Es existiert ein Unterring $C \subseteq B$ mit $b \in C$, so dass $A \to C$ ein endlicher Ringhomomorphismus ist.*

Korollar 3.5. *Sei $\varphi\colon A \to B$ ein Ringhomomorphismus. Dann sind äquivalent:*

(1) *φ ist ganz und B ist als A-Algebra endlich erzeugt.*
(2) *φ ist endlich.*

Korollar 3.6. *Seien $\varphi\colon A \to B$, $\psi\colon B \to C$ Ringhomomorphismen.*

(1) *Wenn φ und ψ endlich sind, so ist auch $\psi \circ \varphi$ endlich.*
(2) *Wenn φ und ψ ganz sind, so ist auch $\psi \circ \varphi$ ganz.*

Definition 3.7. Sei $\varphi\colon A \to B$ ein Ringhomomorphismus. Dann ist die Teilmenge

$$C := \{b \in B;\ b \text{ ist ganz über } A\}$$

ein Unterring von B, der als der *ganze Abschluss von A in B* bezeichnet wird.

Definition 3.8. Sei $\varphi A \to B$ ein injektiver Ringhomomorphismus. Dann heißt A *ganzabgeschlossen in B*, wenn A mit dem ganzen Abschluss von A in B übereinstimmt, mit anderen Worten: wenn die einzigen Elemente von B, die ganz über A sind, die Elemente von A sind.

Ein Integritätsring heißt *ganzabgeschlossen*, wenn er ganzabgeschlossen in seinem Quotientenkörper ist.

Bemerkung 3.9. Seien $\varphi\colon A \to B$ ein Ringhomomorphismus und $C \subseteq B$ der ganze Abschluss von A in B. Dann ist C ganzabgeschlossen in B.

Satz 3.10. *Sei $\varphi\colon A \to B$ ein endlicher (bzw. ganzer) Ringhomomorphismus.*

(1) *Ist $\mathfrak{b} \subseteq B$ ein Ideal, so ist auch der von φ induzierte Homomorphismus $A/\varphi^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$ endlich (bzw. ganz).*
(2) *Ist $S \subseteq A$ eine multiplikative Teilmenge, so ist auch der von φ induzierte Homomorphismus $S^{-1}A \to S^{-1}B$ endlich (bzw. ganz).*
(3) *Ist C eine A-Algebra, so ist auch der von φ induzierte Homomorphismus $C \to B \otimes_A C$ endlich (bzw. ganz).*

3.2. **Going-up.** [AM] Ch. 5, [M2] §9

Satz 3.11. *Seien A und B Integritätsringe und sei $\varphi\colon A \to B$ ein injektiver ganzer Ringhomomorphismus. Dann ist A ein Körper genau dann, wenn B ein Körper ist.*

Satz 3.12. *Sei $\varphi\colon A \to B$ ein ganzer Ringhomomorphismus, $\mathfrak{q} \in \operatorname{Spec} B$, $\mathfrak{p} = \varphi^{-1}(\mathfrak{q}) \in \operatorname{Spec} A$. Dann ist $\mathfrak{q}$ ein maximales Ideal genau dann, wenn $\mathfrak{p}$ ein maximales Ideal ist.*

Satz 3.13. *Sei $\varphi\colon A \to B$ ein ganzer Ringhomomorphismus, seien $\mathfrak{q}$, $\mathfrak{q}'$ Primideale von B mit $\mathfrak{q} \subseteq \mathfrak{q}'$ und $\varphi^{-1}(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q}')$. Dann gilt $\mathfrak{q} = \mathfrak{q}'$.*

Theorem 3.14. *Sei $\varphi\colon A \to B$ ein injektiver ganzer Ringhomomorphismus. Dann ist die von φ induzierte Abbildung* $\operatorname{Spec} B \to \operatorname{Spec} A$ *surjektiv, d.h. für jedes $\mathfrak{p} \in \operatorname{Spec} A$ existiert ein $\mathfrak{q} \in \operatorname{Spec} B$ mit $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$.*

Theorem 3.15 (going-up)**.** *Sei $\varphi\colon A \to B$ ein injektiver ganzer Ringhomomorphismus, sei*

$$\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n \subset A$$

eine Kette von Primidealen, und sei

$$\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m \subset B$$

eine Kette von Primidealen in B mit $m \leq n$ und $\varphi^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$ für $i = 1, \dots, m$.

Dann existieren Primideale $\mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n \subset B$, so dass $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1}$ und so dass $\varphi^{-1}(\mathfrak{q}_i) = \mathfrak{p}$ für alle i.

Theorem 3.16. *Sei $\varphi\colon A \to B$ ein endlicher Ringhomomorphismus. Dann sind die Fasern der Abbildung ${}^a\varphi : \operatorname{Spec} B \to \operatorname{Spec} A$ endliche Mengen, und zwischen den Primidealen in einer Faser bestehen keine echten Inklusionen.*

Satz 3.17. *Sei $\varphi\colon A \to B$ ein Ringhomomorphismus. Sei $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ die von φ induzierte Abbildung, sei $\mathfrak{p} \in \operatorname{Spec} A$ und sei $\kappa(\mathfrak{p})$ der Restklassenkörper von A in $\mathfrak{p}$. Dann induziert die natürliche Abbildung* $\operatorname{Spec}(B \otimes_A \kappa(p)) \to \operatorname{Spec} B$ *eine Bijektion [genauer: sogar einen Homöomorphismus] von* $\operatorname{Spec}(B \otimes_A \kappa(p))$ *auf die Faser $f^{-1}(\mathfrak{p})$ von f über $\mathfrak{p}$.*

Definition 3.18. Ein Ring R heißt *Artin-Ring*, wenn für die Ideale in R die absteigende Kettenbedingung gilt, d.h., falls jede absteigende Kette

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$$

von Idealen in R stationär wird. (Vgl. [AM] Ch. 8.)

Satz 3.19. *Sei A ein Körper und $A \to B$ ein endlicher Ringhomomorphismus. Dann ist B ein Artin-Ring.*

Satz 3.20. *Sei B ein Artin-Ring.*

(1) *Alle Primideale von B sind maximale Ideale.*
(2) *B besitzt nur endlich viele Primideale.*

3.3. **Noether-Normalisierung und der Hilbertsche Nullstellensatz.**

[AM] Ch. 5, [Mu] I.1, [GW] (1.3).

Theorem 3.21 (Noethersches Normalisierungslemma)**.** *Sei k ein Körper und sei $R \neq 0$ eine endlich erzeugte k-Algebra. Dann existieren $n \geq 0$ und ein injektiver endlicher k-Algebren-Homomorphismus $k[X_1, \dots, X_n] \to R$.*

Definition 3.22. Ein Ring A heißt *Jacobsonsch*, wenn für jedes Primideal $\mathfrak{p} \in \operatorname{Spec} A$ gilt

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \in \operatorname{Spm} A, \mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m}.$$

Theorem 3.23 (Hilbertscher Nullstellensatz)**.** *Sei k ein Körper und A eine endlich erzeugte k-Algebra.*

(1) *Der Ring A ist Jacobsonsch.*
(2) *Ist $\mathfrak{m}$ ein maximales Ideal von A, so ist $k \to A/\mathfrak{m}$ eine endliche Körpererweiterung.*

Korollar 3.24. *Sei k ein algebraisch abgeschlossener Körper.*

(1) *Sei A eine endlich erzeugte k-Algebra und sei $\mathfrak{m} \subset A$ ein maximales Ideal. Dann gilt $A/\mathfrak{m} = k$.*
(2) *Sei $\mathfrak{m} \subset k[T_1, \dots, T_n]$ ein maximales Ideal. Dann existieren $t_1, \dots, t_n \in k$ mit $\mathfrak{m} = (T_1 - t_1, \dots, T_n - t_n)$.*

Korollar 3.25. *Sei k ein algebraisch abgeschlossener Körper, und seien $f_1, \dots, f_m \in k[T_1, \dots, T_n]$. Dann haben wir eine Bijektion*

$$\{(t_i)_i \in k^n;\ \forall j : f_j(t_1, \dots, t_n) = 0\} \xrightarrow{\sim} \operatorname{Spm} k[T_1, \dots, T_n]/(f_1, \dots, f_m),$$
$$(t_i)_i \mapsto (T_1 - t_1, \dots, T_n - t_n)$$

Korollar 3.26. *Sei k ein Körper und sei $\varphi\colon A \to B$ ein Homomorphismus von endlich erzeugten k-Algebren. Dann ist für jedes maximale Ideal $\mathfrak{n} \subset B$ das Urbild $\varphi^{-1}(\mathfrak{n})$ ein maximales Ideal von A.*

4. Noethersche Ringe

4.1. **Definition und einfache Eigenschaften.** [AM] Ch. 6, 7, [M2] §3

Definition 4.1. Ein Ring R heißt *noethersch*, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(1) Jede aufsteigende Kette
$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$
von Idealen in R wird stationär, d.h. es existiert $n \geq 0$, so dass $\mathfrak{a}_m = \mathfrak{a}_n$ für alle $m \geq n$.
(2) Jedes Ideal von R ist endlich erzeugt.
(3) Jede nichtleere Menge von Idealen in R besitzt ein maximales Element bezüglich Inklusion.

Beispiel 4.2. (1) Jeder Hauptidealring ist noethersch.
(2) Ist R ein noetherscher Ring und $\mathfrak{a} \subseteq R$ ein Ideal, so ist auch $R/\mathfrak{a}$ noethersch.
(3) Sei $R \neq 0$ ein Ring. Dann ist der Polynomring $R[X_i;\ i \in \mathbb{N}]$ in unendlich vielen Unbestimmten nicht noethersch. Insbesondere sind Unterringe noetherscher Ringe nicht notwendig noethersch.

Satz 4.3. *Sei R ein noetherscher Ring, $S \subseteq A$ eine multiplikative Teilmenge. Dann ist $S^{-1}R$ noethersch.*

Definition 4.4. Sei R ein Ring (nicht notwendig noethersch). Ein R-Modul M heißt noethersch, wenn die folgenden äquivalenten Bedingungen erfüllt sind:

(1) Jede aufsteigende Kette von Untermoduln von M wird stationär.
(2) Jeder Untermodul von M ist endlich erzeugt.
(3) Jede nichtleere Menge von Untermoduln von M besitzt ein maximales Element bezüglich Inklusion.

Mit dieser Definition gilt: Ein Ring R ist genau dann noethersch, wenn der R-Modul R noethersch ist.

Satz 4.5. *Sei R ein Ring.*

(1) *Sei*
$$0 \to M' \to M \to M'' \to 0$$
eine kurze exakte Sequenz von R-Moduln. Dann gilt: M ist genau dann noethersch, wenn M' und M'' noethersch sind.
(2) *Sei R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist M noethersch.*

4.2. **Der Hilbertsche Basissatz.** [AM] Ch. 7, [M2] §3

Theorem 4.6 (Hilbertscher Basissatz)**.** *Sei R ein noetherscher Ring. Dann ist auch der Polynomring $R[X]$ noethersch.*

Korollar 4.7. *Sei R ein noetherscher Ring und A eine endlich erzeugte R-Algebra. Dann ist auch der Ring A noethersch.*

5. Diskrete Bewertungsringe und Dedekindringe

5.1. **Diskrete Bewertungsringe.** [AM] Ch. 9, [M2] §11, [S] Ch. 1.

Definition 5.1. Sei K ein Körper. Eine *diskrete Bewertung auf K* ist eine surjektive Abbildung $v\colon K^\times \to \mathbb{Z}$, für die gilt:

(1) $v(xy) = v(x) + v(y)$ für alle $x, y \in K^\times$,
(2) $v(x+y) \geq \min(v(x), v(y))$ für alle $x, y \in K^\times$.

Bemerkung 5.2. Sei K ein Körper mit einer diskreten Bewertung v. Sei $c \in \mathbb{R}$, $0 < c < 1$. Dann definiert
$$|x| = c^{v(x)} \quad \text{für} \quad x \in K^\times, \qquad |0| = 0,$$
einen Absolutbetrag auf K, d.h. eine Abbildung $|\cdot|\colon K \to \mathbb{R}$ mit

(1) $|x| = 0 \iff x = 0$,
(2) $|xy| = |x| \cdot |y|$,
(3) (Dreiecksungleichung) $|x+y| \leq |x| + |y|$.

Genauer gilt in dieser Situation sogar die *starke Dreiecksungleichung*:
$$|x+y| \leq \max(|x|, |y|).$$
Man spricht in diesem Fall von einem *nicht-archimedischen* Absolutbetrag.

Lemma 5.3. *Sei K ein Körper mit einer diskreten Bewertung v. Dann ist*
$$\{x \in K;\ v(x) \geq 0\} \cup \{0\}$$
ein Unterring von K, der sogenannte Bewertungsring *von (K, v).*

Beispiel 5.4. (1) Sei R ein faktorieller Ring, $K = \mathrm{Quot}(R)$, $p \in R$ ein Primelement. Jedes Element $x \in K^in\times$ lässt sich schreiben als $x = p^n \frac{a}{b}$ mit $n \in \mathbb{Z}$, $a, b \in R$, $p \not| ab$. Dabei ist n eindeutig bestimmt und durch $v(x) := n$ wird eine diskrete Bewertung auf K definiert.

(2) Sei speziell $K = \mathbb{Q}$, $p \in \mathbb{Z}$ eine Primzahl. Die wie in (1) definierte Bewertung v_p heißt die p-adische Bewertung auf $\mathbb{Q}$. Der Bewertungsring von v_p ist der Ring $\mathbb{Z}_{(p)}$, die Lokalisierung von $\mathbb{Z}$ nach dem Primideal (p). Man kann zeigen, dass alle diskreten Bewertungen auf $\mathbb{Q}$ diese Form haben.

(3) Sei speziell $K = k(T)$ der rationale Funktionenkörper über einem Körper k. Wie in (1) definiert dann jedes irreduzible Polynom $f \in k[T]$ eine Bewertung v_f auf K. Der Bewertungsring von v_f ist der Ring $k[T]_{(f)}$.

(4) Sei $K = k(T)$ wie in 3. Dann ist auch $K = \mathrm{Quot}(k[T^{-1}])$ und wenn wir die Konstruktion in (1) auf das Primelement $T^{-1} \in k[T^{-1}]$ anwenden, erhalten wir eine Bewertung v_∞ auf K, die nicht von der Form v_f wie in (3) ist. Es gilt

$$v_\infty(\frac{f}{g}) = \deg g - \deg f \text{ für } f, g \in k[T], g \neq 0.$$

Der Bewertungsring von v_∞ ist der Ring

$$k[T^{-1}]_{(T^{-1})} = \{\frac{f}{g};\ f, g \in k[T], g \neq 0,\ \deg f \leq \deg g\} \subset K.$$

Man kann zeigen, dass alle Bewertungen auf K die Form v_f, $f \in k[T]$ irreduzibel, oder v_∞ haben.

Definition 5.5. Sei A ein Integritätsring, $K = \mathrm{Quot}(A)$. Der Ring A heißt *diskreter Bewertungsring*, falls eine diskrete Bewertung auf K existiert, deren Bewertungsring A ist.

Bemerkung 5.6. Sei K ein Körper mit diskreter Bewertung v, und sei A der zugehörige Bewertungsring. Es gilt

$$A^\times = \{x \in A;\ v(x) = 0\}.$$

Sei $\pi \in A$ ein Element mit $v(\pi) = 1$. Ein solches Element heißt *uniformisierendes Element*. Dann gilt: Jedes Element $x \in A$ lässt sich schreiben als $x = \pi^{v(x)} u$ mit $u \in A^\times$ (und u ist eindeutig bestimmt).

Jedes Ideal von A außer dem Nullideal hat die Form (π^d), $d \geq 0$. Das Ideal (π) ist das einzige maximale Ideal von A. Insbesondere ist A ein lokaler Hauptidealring.

Lemma 5.7. *Sei A ein Integritätsring. Dann sind äquivalent:*

(1) *Der Ring A ist ein diskreter Bewertungsring.*

(2) *Der Ring A ist noethersch und lokal, und das maximale Ideal von A ist ein Hauptideal.*

Theorem 5.8. *Sei A ein Integritätsring. Dann sind äquivalent:*

(1) *Der Ring A ist ein diskreter Bewertungsring.*
(2) *Der Ring A ist ein lokaler Hauptidealring, aber kein Körper.*
(3) *Der Ring A ist noethersch, ganzabgeschlossen und es gibt genau ein Primideal $\neq 0$ in A.*

5.2. **Dedekindringe.** [AM] Ch. 9, [M2] §11, [S] Ch. 1.

Definition 5.9. Sei A ein Integritätsring. Wir sagen, A habe Dimension 1, in Zeichen: $\dim A = 1$, falls A kein Körper ist, und jedes Primideal $\neq 0$ in A ein maximales Ideal ist.

Theorem 5.10. *Sei A ein Integritätsring. Dann sind äquivalent:*
(1) *A ist ganzabgeschlossen, noethersch und* $\dim A = 1$.
(2) *Für jedes Primideal $\mathfrak{p} \neq 0$ von A ist $A_\mathfrak{p}$ ein diskreter Bewertungsring.*

Theorem 5.11. *Sei A ein Dedekindring, $K = \mathrm{Quot}(A)$, sei L/K eine endliche separable Körpererweiterung, und sei B der ganze Abschluss von A in L. Dann ist auch B ein Dedekindring.*

Bemerkung 5.12. Der Satz ist auch ohne die Voraussetzung, dass die Erweiterung L/K separabel sei, richtig, allerdings dann deutlich schwieriger zu beweisen.

Die Spur einer separablen Körpererweiterung. [N] I §2, [Bo] 4.7.

Sei L/K eine endliche Körpererweiterung. Sei $x \in L$. Dann ist die Abbildung $t_x\colon L \to L$, $z \mapsto xz$, ein Homomorphismus von K-Vektorräumen, und wir setzen $\mathrm{Tr}_{L/K}(x) := \mathrm{Spur}(t_x)$, und erhalten so eine Abbildung $\mathrm{Tr}_{L/K}\colon L \to K$, die sogenannte *Spurabbildung*.

Sei im folgenden stets L/K eine endliche **separable** Körpererweiterung, und sei $\{\sigma_1, \dots, \sigma_n\}$ die Menge aller K-Homomorphismen von L in einen fixierten algebraischen Abschluss von L

Lemma 5.13. *Für alle $x \in L$ gilt* $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$.

Satz 5.14. *Sei L/K eine endliche separable Körpererweiterung. Dann ist die Abbildung*

$$L \times L \to K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(xy),$$

eine nicht-ausgeartete symmetrische Bilinearform auf dem K-Vektorraum L.

Lemma 5.15. *Sei A ein Dedekindring, $K = \mathrm{Quot}(A)$, sei L/K eine endliche separable Körpererweiterung, und sei B der ganze Abschluss von A in L. Dann gilt für alle $b \in B$: $\mathrm{Tr}_{L/K}(b) \in A$.*

Satz 5.16. *Sei A ein Dedekindring, $K = \mathrm{Quot}(A)$, sei L/K eine endliche separable Körpererweiterung, und sei B der ganze Abschluss von A in L. Ist $\alpha_1, \dots, \alpha_n$ eine K-Basis von L mit $\alpha_i \in B$ für alle i, und ist $d = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))$, so gilt*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

5.3. **Zerlegung von Idealen in Primideale in Dedekindringen.** [AM] Ch. 9, [M2] §11, [S] Ch. 1.

Sei A ein Dedekindring mit Quotientenkörper K.

Definition 5.17. Ein *gebrochenes Ideal von A* ist ein von 0 verschiedener endlich erzeugter A-Untermodul $\mathfrak{a} \subset K$.

Jedes Ideal $\neq 0$ von A ist ein gebrochenes Ideal. Ist $x \in A$, $x \neq 0$, so ist $x^{-1}A$ ein gebrochenes Ideal von A.

Sei $\mathfrak{a} \subseteq A$ ein gebrochenes Ideal. Wir setzen

$$\mathfrak{a}^{-1} := \{x \in K; x\mathfrak{a} \subseteq A\}.$$

Dies ist wieder ein gebrochenes Ideal von K.

Für gebrochene Ideale $\mathfrak{a}$, $\mathfrak{b}$ von A definieren wir ihr Produkt durch

$$\mathfrak{a}\mathfrak{b} := \langle ab; a \in \mathfrak{a}, b \in \mathfrak{b}\rangle_A,$$

d.h. als den von allen Produkten von Elementen aus $\mathfrak{a}$ und $\mathfrak{b}$ erzeugten A-Untermodul von K, vergleiche Definition 1.8. Für $n \geq 1$ definieren wir $\mathfrak{a}^n = \mathfrak{a} \cdot \dots \cdot \mathfrak{a}$ (n Faktoren), für $n < 0$ sei $\mathfrak{a}^n := (\mathfrak{a}^{-1})^{-n}$. Wir setzen $\mathfrak{a}^0 := (1)$.

Beispiel 5.18. Sei A ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}$. Dann sind die gebrochenen Ideale von A gerade die Untermoduln $\mathfrak{m}^d$, $d \in \mathbb{Z}$.

Lemma 5.19. *Seien A ein Dedekindring. Seien $\mathfrak{a}$, $\mathfrak{b}$ gebrochene Ideale von A. Dann gilt:*

(1) *Sei $\mathfrak{p} \in \operatorname{Spec} A$. Wie üblich bezeichnen wir für jeden A-Modul $\mathfrak{a}$ mit $\mathfrak{a}_\mathfrak{p}$ die Lokalisierung bezüglich $S = A \setminus \mathfrak{p}$. Dann gilt*
   (a) $(\mathfrak{a} + \mathfrak{b})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} + \mathfrak{b}_\mathfrak{p}$,
   (b) $(\mathfrak{a}\mathfrak{b})_\mathfrak{p} = \mathfrak{a}_\mathfrak{p} \cdot \mathfrak{b}_\mathfrak{p}$,
   (c) $(\mathfrak{a}^{-1})_\mathfrak{p} = (\mathfrak{a}_\mathfrak{p})^{-1}$.

(2) *Es gilt genau dann $\mathfrak{a} = \mathfrak{b}$, wenn für alle $\mathfrak{p} \in \operatorname{Spec} A$ gilt: $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$.*

Satz 5.20. *Sei A ein Dedekindring. Dann ist die Menge der gebrochenen Ideale von A eine Gruppe bezüglich des soeben definierten Produkts. Das neutrale Element ist das Ideal A. Das Inverse eines gebrochenen Ideals $\mathfrak{a}$ ist $\mathfrak{a}^{-1}$. Insbesondere gilt $\mathfrak{a}\mathfrak{a}^{-1} = A$ und $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$ für alle gebrochenen Ideale $\mathfrak{a}$.*

Theorem 5.21. *Sei A ein Dedekindring, und sei $\mathfrak{a} \subseteq A$ ein Ideal $\neq 0$. Dann existieren endlich viele paarweise verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ und natürliche Zahlen $n_i \geq 1$, so dass*

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$

Dabei ist r eindeutig bestimmt, und die $\mathfrak{p}_i$ und n_i sind eindeutig bestimmt bis auf die Reihenfolge.

Für das Einsideal ist die durch das Theorem gegebene Zerlegung das leere Produkt. Mit den Notationen des Theorems gilt: Die Primideale, in denen $\mathfrak{a}$ enthalten ist, sind genau $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Man kann zeigen, dass jeder Integritätsring, der kein Körper ist, und in dem sich jedes Ideal $\neq 0$ als endliches Produkt von Primidealen schreiben lässt, ein Dedekindring ist, siehe [M2] Theorem 11.6.

Beispiel 5.22. Der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$ ist der Ring $A := \mathbb{Z}[\sqrt{-5}]$. Der Ring A ist also ein Dedekindring. Er ist allerdings nicht faktoriell, zum Beispiel sind

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

zwei verschiedene Zerlegungen von 6 in Produkte irreduzibler Elemente. Die Ideale (2), (3), $(1 - \sqrt{-5})$ und $(1 + \sqrt{-5})$ sind keine Primideale. Die Ideale

$$\begin{aligned} \mathfrak{p}_1 &= (2, 1 + \sqrt{-5}), \\ \mathfrak{p}_2 &= (2, 1 - \sqrt{-5}), \\ \mathfrak{p}_3 &= (3, 1 + \sqrt{-5}), \\ \mathfrak{p}_4 &= (3, 1 - \sqrt{-5}) \end{aligned}$$

sind Primideale und es gilt

$$(2) = \mathfrak{p}_1\mathfrak{p}_2, \quad (3) = \mathfrak{p}_3\mathfrak{p}_4, \quad (1 + \sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3, \quad (1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_4,$$

und die obige Zerlegung erklärt sich als

$$(6) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

Literatur

[AM] M. Atiyah, I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley
[Bo] S. Bosch, *Algebra*, Springer
[B] N. Bourbaki, *Algèbre commutative*, oder auf Englisch: *Commutative Algebra*, Ch. 1–10.
[E] D. Eisenbud, *Commutative Algebra with a View towards Algebraic Geometry*, Springer GTM
[GW] U. Görtz, T. Wedhorn, *Algebraic Geometry I*, Vieweg.
[M1] H. Matsumura, *Commutative Algebra*
[M2] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press
[Mu] D. Mumford, *The Red Book on Varieties and Schemes*, Springer LNM 1358.
[N] J. Neukirch, *Algebraische Zahlentheorie*, Springer.
[S] J.-P. Serre, *Corps locaux* (oder auf Englisch: *Local fields*, Springer GTM)
[ZS] O. Zariski, P. Samuel, *Commutative Algebra*, Vol. I, Vol. II, Springer.