

Algebra II

Sommersemester 2021

Prof. Dr. Alexander Schmidt

Teil 1 – Kommutative Algebra

1 Ringe und Ideale

Sei A ein kommutativer Ring (wie immer mit 1) und $\mathfrak{a} \subset A$ ein Ideal. Die Projektion $\phi : A \rightarrow A/\mathfrak{a}$ ist ein surjektiver Ringhomomorphismus. Wir erinnern an den folgenden Satz:

Satz 1.1 (Algebra I, Satz 2.5). *Die Zuordnung $\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b})$ induziert eine inklusionserhaltende Bijektion zwischen der Menge der Ideale in A/\mathfrak{a} und der Menge der Ideale in A , die \mathfrak{a} umfassen.*

Beweisskizze. Man prüft nacheinander folgendes nach:

- $\phi^{-1}(\mathfrak{b})$ ist ein Ideal in A .
- $\phi^{-1}(\mathfrak{b}) \supset \phi^{-1}(0) = \mathfrak{a}$.
- $\phi^{-1}(\mathfrak{b}_1) = \phi^{-1}(\mathfrak{b}_2) \Rightarrow \mathfrak{b}_1 = \mathfrak{b}_2$ (da ϕ surjektiv).
- Ist $\mathfrak{c} \subset A$ ein Ideal mit $\mathfrak{c} \supset \mathfrak{a}$, so gilt $\phi^{-1}(\phi(\mathfrak{c})) = \mathfrak{c}$. □

Erinnerung 1.2. • $x \equiv y \pmod{\mathfrak{a}}$ bedeutet $x - y \in \mathfrak{a}$.

- $x \in A$ heißt **Nullteiler**, wenn ein $y \in A$, $y \neq 0$, mit $xy = 0$ existiert.
- A heißt **nullteilerfrei**, wenn A nicht der Nullring und $0 \in A$ der einzige Nullteiler ist.
- $x \in A$ heißt **Einheit**, wenn ein $y \in A$ mit $xy = 1$ existiert. Die Menge A^\times der Einheiten von A ist eine Gruppe unter Multiplikation.

Beispiel 1.3. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Die Vielfachen ax eines Elements $x \in A$ bilden ein **Hauptideal**. Bezeichnung (x) oder auch Ax . Das **Nullideal** (0) wird auch einfach mit 0 bezeichnet. Es gilt $(1) = A$ und $(x) = A \Leftrightarrow x \in A^\times$.

Erinnerung 1.4. • $\mathfrak{p} \subset A$ heißt **Primideal**, wenn $\mathfrak{p} \neq (1)$ und es gilt $xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \text{ oder } y \in \mathfrak{p})$.

• $\mathfrak{p} \subset A$ ist Primideal $\iff A/\mathfrak{p}$ ist nullteilerfrei.

• $\mathfrak{m} \subset A$ heißt **Maximalideal** wenn $\mathfrak{m} \neq (1)$ und es kein Ideal \mathfrak{a} mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$ gibt.

• $\mathfrak{m} \subset A$ ist Maximalideal $\iff A/\mathfrak{m}$ ist Körper.

• Jedes Maximalideal ist ein Primideal.

• $f : A \rightarrow B$ Ringhomomorphismus, $\mathfrak{q} \subset B$ Primideal $\Rightarrow f^{-1}(\mathfrak{q}) \subset A$ ist ein Primideal.

Satz 1.5. Jeder Ring $A \neq 0$ besitzt ein Maximalideal.

Beweis. Sei Σ die Menge der Ideale $\neq (1)$ in A . Wegen $A \neq 0$ gilt $(0) \subsetneq (1)$ und damit $\Sigma \neq \emptyset$. Wir ordnen Σ durch die Inklusion, d.h. $\mathfrak{a} \leq \mathfrak{b} \Leftrightarrow \mathfrak{a} \subset \mathfrak{b}$.

Sei nun (\mathfrak{a}_α) eine Kette in Σ . Für α, β haben wir $\mathfrak{a}_\alpha \subset \mathfrak{a}_\beta$ oder $\mathfrak{a}_\beta \subset \mathfrak{a}_\alpha$. Setze $\mathfrak{a} = \bigcup_{\alpha} \mathfrak{a}_\alpha$. Dann ist \mathfrak{a} ein Ideal: $a \in A, x \in \mathfrak{a} \Rightarrow ax \in \mathfrak{a}$ weil $x \in \mathfrak{a}_\alpha$ für ein α und deshalb $ax \in \mathfrak{a}_\alpha \subset \mathfrak{a}$. Es sei nun $x \in \mathfrak{a}_\alpha, y \in \mathfrak{a}_\beta$. Gilt $\mathfrak{a}_\alpha \subset \mathfrak{a}_\beta$ so folgt $x + y \in \mathfrak{a}_\beta \subset \mathfrak{a}$, ansonsten gilt $\mathfrak{a}_\beta \subset \mathfrak{a}_\alpha$ und $x + y \in \mathfrak{a}_\alpha \subset \mathfrak{a}$.

Es gilt $\mathfrak{a} \in \Sigma$ wegen $1 \notin \mathfrak{a} = \bigcup \mathfrak{a}_\alpha$ und \mathfrak{a} ist obere Schranke für die Kette (\mathfrak{a}_α) . Zorn's Lemma $\Rightarrow \Sigma$ besitzt (mindestens) ein maximales Element. \square

Korollar 1.6. Jedes Ideal $\mathfrak{a} \subsetneq A$ ist in einem Maximalideal enthalten.

Beweis. Nach Satz 1.5 besitzt $0 \neq A/\mathfrak{a}$ mindestens ein Maximalideal. Nach Satz 1.1 erhalten wir ein Maximalideal in A welches \mathfrak{a} umfasst. \square

Korollar 1.7. Jede Nichteinheit ist in einem Maximalideal enthalten.

Beweis. Ist x Nichteinheit, so gilt $Ax \subsetneq A$. Nach Korollar 1.6 ist Ax und somit auch x in einem Maximalideal enthalten. \square

Definition 1.8. A heißt **lokal**, wenn es genau ein Maximalideal $\mathfrak{m} \subset A$ gibt. Der Körper $k = A/\mathfrak{m}$ heißt der **Restklassenkörper** von A .

Satz 1.9. Es sei $\mathfrak{m} \subset A$ ein Maximalideal.

(i) $(A \setminus \mathfrak{m}) \subset A^\times \Rightarrow A$ ist lokal.

(ii) $1 + \mathfrak{m} \subset A^\times \Rightarrow A$ ist lokal.

Beweis. (i) Sei $\mathfrak{a} \subsetneq A$ ein Ideal. Dann gilt $\mathfrak{a} \cap A^\times = \emptyset$, also $\mathfrak{a} \cap (A \setminus \mathfrak{m}) = \emptyset$, d.h. $\mathfrak{a} \subset \mathfrak{m}$. Daher ist \mathfrak{m} das einzige Maximalideal. (ii) Für $x \in A$ ist $Ax + \mathfrak{m}$ ein Ideal. Aus $x \notin \mathfrak{m}$ folgt $Ax + \mathfrak{m} \supsetneq \mathfrak{m}$, also $Ax + \mathfrak{m} = (1)$. Daher existieren $a \in A, y \in \mathfrak{m}$ mit $ax + y = 1$, also $ax = 1 - y \in 1 + \mathfrak{m} \subset A^\times$. Aus $ax \in A^\times$ folgt $x \in A^\times$. Wir erhalten $(A \setminus \mathfrak{m}) \subset A^\times$, also A lokal nach (i). \square

Definition 1.10. Sei A ein kommutativer Ring. $x \in A$ heißt **nilpotent**, wenn $x^n = 0$ für ein $n \in \mathbb{N}$ gilt.

Nilpotente Elemente sind Nullteiler, die Umkehrung ist i.A. falsch.

Satz 1.11. Die Menge $\mathfrak{N} = \mathfrak{N}(A)$ aller nilpotenten Elemente in A ist ein Ideal. Der Faktorring A/\mathfrak{N} hat keine nilpotenten Elemente $\neq 0$.

Beweis. $x \in \mathfrak{N}$, $a \in A \Rightarrow ax \in \mathfrak{N}$ (klar). Seien $x, y \in \mathfrak{N}$, $x^n = 0 = y^m$. Dann gilt $(x+y)^{n+m-1} = 0$ (binomische Formel) also $x+y \in \mathfrak{N}$. Daher ist \mathfrak{N} ein Ideal. Sei nun $x \in A$ und $\bar{x} \in A/\mathfrak{N}$ nilpotent. Dann gilt $\bar{x}^n = 0$ in A/\mathfrak{N} für ein $n \in \mathbb{N}$, also $x^n \in \mathfrak{N}$, und somit $x^{nm} = 0$ für geeignetes $m \in \mathbb{N}$. \square

Definition 1.12. Das Ideal \mathfrak{N} aller nilpotenten Elemente heißt das **Nilradikal**.

Satz 1.13. Das Nilradikal von A ist der Durchschnitt aller Primideale.

Beweis. Sei \mathfrak{N}' der Durchschnitt aller Primideale. Sei $x \in \mathfrak{N}$, also $x^n = 0$ für ein n . Dann gilt für jedes Primideal \mathfrak{p} : $x^n \in \mathfrak{p}$, also $x \in \mathfrak{p}$. Dies zeigt $\mathfrak{N} \subset \mathfrak{N}'$. Angenommen es gäbe ein $x \in \mathfrak{N}' \setminus \mathfrak{N}$. Sei Σ die Menge aller Ideale $\mathfrak{a} \subset A$ mit

$$x^n \notin \mathfrak{a} \quad \text{für alle } n \in \mathbb{N}.$$

Wegen $0 \in \Sigma$ ist Σ nichtleer. Wir ordnen Σ durch Inklusion. Nach Zorns Lemma existiert ein maximales Element $\mathfrak{p} \in \Sigma$.

Behauptung: \mathfrak{p} ist Primideal.

Beweis der Behauptung. Seien $s, t \notin \mathfrak{p}$. Dann gilt $\mathfrak{p} \subsetneq As + \mathfrak{p}$ und $\mathfrak{p} \subsetneq At + \mathfrak{p}$, also $As + \mathfrak{p}$, $At + \mathfrak{p} \notin \Sigma$. Nach Definition von Σ existieren $n, m \in \mathbb{N}$ mit $x^n \in As + \mathfrak{p}$, $x^m \in At + \mathfrak{p}$. Dies impliziert $x^{n+m} \in Ast + \mathfrak{p}$, also $Ast + \mathfrak{p} \notin \Sigma$. Aus $st \in \mathfrak{p}$ würde $\mathfrak{p} = Ast + \mathfrak{p} \in \Sigma$ folgen, also $st \notin \mathfrak{p}$, d.h. \mathfrak{p} ist Primideal. Dies zeigt die Behauptung.

Wegen $\mathfrak{p} \in \Sigma$ gilt $x \notin \mathfrak{p}$. Also $x \notin \mathfrak{N}'$. Widerspruch. \square

Operationen auf Idealen

Sei $(\mathfrak{a}_i)_{i \in I}$ eine nicht notwendig endliche Familie von Idealen. Dann sind

$$\bigcap_{i \in I} \mathfrak{a}_i \quad \text{und} \quad \sum_{i \in I} \mathfrak{a}_i := \left\{ \sum_{i \in I} \alpha_i \mid \alpha_i \in \mathfrak{a}_i \text{ und } \alpha_i = 0 \text{ f.f.a. } i \right\}$$

Ideale in A . Ist $I = \{1, \dots, n\}$ endlich, haben wir das Produkt

$$\prod_{i=1}^n \mathfrak{a}_i = \left\{ \sum_{\text{endl.}} x_1 x_2 \cdots x_n \mid x_i \in \mathfrak{a}_i \right\}$$

Bemerkung 1.14. Durchschnitt, Summe und Produkt sind assoziativ und kommutativ. Desweiteren gilt $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

Notation: $\mathfrak{a}^n = \mathfrak{a} \cdots \mathfrak{a}$ (n Faktoren).

Lemma 1.15. (i) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ falls $\mathfrak{a} \supset \mathfrak{b}$ oder $\mathfrak{a} \supset \mathfrak{c}$.

(ii) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.

Beweis. (i) OE sei $\mathfrak{b} \subset \mathfrak{a}$. Für ein Element $b + c \in \mathfrak{a}$, $b \in \mathfrak{b}$, $c \in \mathfrak{c}$ gilt $b \in \mathfrak{a} \cap \mathfrak{b}$ und daher $c \in \mathfrak{a} \cap \mathfrak{c}$. Gilt umgekehrt $b \in \mathfrak{b}$, $c \in \mathfrak{a} \cap \mathfrak{c}$, so gilt $b + c \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$.

(ii) folgt durch Einsetzen der Definitionen. \square

Zwei Ideale $\mathfrak{a}, \mathfrak{b} \subset A$ heißen **relativ prim**, wenn $\mathfrak{a} + \mathfrak{b} = (1)$. Für relativ prime Ideale $\mathfrak{a}, \mathfrak{b}$ gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ nach Lemma 1.15(ii).

Nun seien A_1, \dots, A_n Ringe. Ihr Produkt $A = \prod_{i=1}^n A_i$ mit komponentenweiser Addition und Multiplikation ist ein Ring mit Einselement $(1, \dots, 1)$. Die Projektionen $A \rightarrow A_i$, $x = (x_1, \dots, x_n) \mapsto x_i$ sind Ringhomomorphismen.

Warnung: Die Inklusionen $A_i \hookrightarrow A$, $x_i \mapsto (0, \dots, x_i, \dots, 0)$ sind keine Ringhomomorphismen!

Nun sei A ein Ring und $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale in A . Wir betrachten den Homomorphismus

$$\begin{aligned} \phi : A &\longrightarrow \prod_{i=1}^n A/\mathfrak{a}_i, \\ x &\longmapsto (x + \mathfrak{a}_1, \dots, x + \mathfrak{a}_n). \end{aligned}$$

Lemma 1.16 (Verallgemeinerter Chinesischer Restsatz). (i) Sind für $i \neq j$ die Ideale \mathfrak{a}_i und \mathfrak{a}_j relativ prim, so gilt

$$\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i.$$

(ii) ϕ surjektiv $\iff \mathfrak{a}_i$ und \mathfrak{a}_j sind relativ prim für alle $i \neq j$.

(iii) ϕ injektiv $\iff \bigcap_{i=1}^n \mathfrak{a}_i = 0$.

Beweis. (i) $n = 2$ schon bekannt nach Lemma 1.15(ii). $n \geq 3$ per Induktion.

Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ paarweise relativ prime Ideale und $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. Wegen $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ für $i = 1, \dots, n-1$, finden wir Elemente $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_n$ mit $x_i + y_i = 1$. Es gilt $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}$. Daher gilt $\mathfrak{b} + \mathfrak{a}_n = (1)$ und

$$\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^n \mathfrak{a}_i.$$

(ii): \Rightarrow . Wir zeigen $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ falls $i \neq j$. Ohne Einschränkung sei $i = 1, j = 2$. Es existiert ein $x \in A$ mit $\phi(x) = (1, 0, \dots, 0)$, also $x \equiv 1 \pmod{\mathfrak{a}_1}$, $x \equiv 0 \pmod{\mathfrak{a}_2}$, so dass

$$1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$$

(ii): \Leftarrow . Es genügt zu zeigen, dass für alle i das Element $(0, \dots, 0, 1, 0, \dots, 0)$ (1 an i -ter Stelle) in $\text{im}(\phi)$ liegt. Ohne Einschränkung sei $i = 1$. Wegen $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ für $i \geq 2$ haben wir Elemente $u_i \in \mathfrak{a}_1$, $v_i \in \mathfrak{a}_i$ mit $u_i + v_i = 1$. Setze $x = \prod_{i=2}^n v_i$.

Dann gilt $x \equiv 0 \pmod{\mathfrak{a}_i}$ für $i \geq 2$ und $x = \prod_{i=2}^n (1 - u_i) \equiv 1 \pmod{\mathfrak{a}_1}$. Daher gilt $\phi(x) = (1, 0, \dots, 0)$.

(iii) Dies ist klar wegen $\ker(\phi) = \bigcap_{i=1}^n \mathfrak{a}_i$. □

Die Vereinigung $\mathfrak{a} \cup \mathfrak{b}$ zweier Ideale ist i.A. kein Ideal.

Satz 1.17 (Primvermeidung). (i) Es seien $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ Primideale und \mathfrak{a} ein Ideal mit $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$. Dann gilt bereits $\mathfrak{a} \subset \mathfrak{p}_i$ für ein i .

(ii) Es seien $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ Ideale und \mathfrak{p} ein Primideal mit $\mathfrak{p} \supset \bigcap_{i=1}^n \mathfrak{a}_i$. Dann gilt $\mathfrak{p} \supset \mathfrak{a}_i$ für ein i . Aus $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$ folgt $\mathfrak{p} = \mathfrak{a}_i$ für ein i .

Bemerkung 1.18. Eine Umformulierung von (i) ist: Ist \mathfrak{a} in keinem der Primideale \mathfrak{p}_i enthalten, so existiert ein $a \in \mathfrak{a}$ mit $a \notin \mathfrak{p}_i$ für alle i . Daher kommt der Name „Primvermeidung“.

Beweis von Satz 1.17. Wir zeigen (i) per Induktion nach n in der Form

$$\mathfrak{a} \not\subset \mathfrak{p}_i \quad \text{für } i = 1, \dots, n \implies \mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$$

Die Aussage ist trivial für $n = 1$. Sei $n > 1$ und die Aussage richtig für $n - 1$. Dann existiert für jedes $i = 1, \dots, n$ ein $x_i \in \mathfrak{a}$ mit $x_i \notin \mathfrak{p}_j$ für alle $j \neq i$. Gilt $x_i \notin \mathfrak{p}_i$ für ein i , so sind wir fertig. Im anderen Fall gilt $x_i \in \mathfrak{p}_i$ für alle i . Für

$$y = \sum_{i=1}^n x_1 \dots x_{i-1} x_{i+1} x_{i+2} \dots x_n$$

gilt dann $y \in \mathfrak{a}$ und $y \notin \mathfrak{p}_i$ für $i = 1, \dots, n$, also $\mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$.

(ii) Wir nehmen an, dass $\mathfrak{p} \not\subset \mathfrak{a}_i$ für alle i . Dann existieren Elemente $x_i \in \mathfrak{a}_i$, $x_i \notin \mathfrak{p}$ und wir erhalten

$$x_1 \cdots x_n \in \prod_{i=1}^n \mathfrak{a}_i \subset \bigcap_{i=1}^n \mathfrak{a}_i$$

aber $x_1 \cdots x_n \notin \mathfrak{p}$, da \mathfrak{p} prim. Also folgt $\mathfrak{p} \not\subset \bigcap_{i=1}^n \mathfrak{a}_i$.

Gilt schließlich $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, so haben wir gerade gesehen: $\mathfrak{p} \supset \mathfrak{a}_{i_0}$ für ein i_0 . Aus

$$\mathfrak{a}_{i_0} \subset \mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{a}_{i_0} \text{ folgt } \mathfrak{p} = \mathfrak{a}_{i_0}.$$

□

Definition 1.19. Für Ideale $\mathfrak{a}, \mathfrak{b} \subset A$ setzt man

$$\mathfrak{a} : \mathfrak{b} = \{x \in A, x\mathfrak{b} \subset \mathfrak{a}\}.$$

Dies ist ein Ideal in A . Das Ideal

$$\text{Ann}(\mathfrak{b}) \stackrel{\text{df}}{=} 0 : \mathfrak{b} = \{x \in A \mid x\mathfrak{b} = 0\}$$

heißt der **Annulator** von \mathfrak{b} . Für $x \in A$ schreiben wir $\text{Ann}(x) = \text{Ann}((x))$. Für die Menge D der Nullteiler von A gilt nach Definition:

$$D = \bigcup_{x \neq 0} \text{Ann}(x).$$

Beispiel 1.20. Sei $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$. Dann ist $\mathfrak{a} : \mathfrak{b}$ das durch $\frac{m}{\text{ggT}(m,n)}$ erzeugte Hauptideal.

Lemma 1.21. Es gilt

- (i) $\mathfrak{a} \subset \mathfrak{a} : \mathfrak{b}$.
- (ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$.
- (iii) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$.
- (iv) $(\bigcap_i \mathfrak{a}_i) : \mathfrak{b} = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.
- (v) $\mathfrak{a} : (\sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Beweis. Übungsaufgabe. □

Definition 1.22. Das **Radikal** $r(\mathfrak{a})$ eines Ideals \mathfrak{a} ist definiert durch

$$r(\mathfrak{a}) := \{x \in A \mid x^n \in \mathfrak{a} \text{ für ein } n \in \mathbb{N}\}.$$

Ist $\phi : A \rightarrow A/\mathfrak{a}$ die natürliche Projektion, so gilt

$$r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}(A/\mathfrak{a})).$$

Daher ist $r(\mathfrak{a})$ ein Ideal.

Lemma 1.23. *Es gilt*

- (i) $r(\mathfrak{a}) \supset \mathfrak{a}$.
- (ii) $r(r(\mathfrak{a})) = r(\mathfrak{a})$.
- (iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
- (iv) $r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$.
- (v) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
- (vi) Für ein Primideal \mathfrak{p} gilt $r(\mathfrak{p}^n) = \mathfrak{p}$ für alle $n \in \mathbb{N}$.

Beweis. Übungsaufgabe. □

Satz 1.24. Das **Radikal** $r(\mathfrak{a})$ ist der Durchschnitt aller \mathfrak{a} umfassenden Primideale.

Beweis. Sei $\phi : A \rightarrow A/\mathfrak{a}$ die kanonische Projektion. Dann gilt

$$r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}(A/\mathfrak{a})) = \phi^{-1}\left(\bigcap_{\mathfrak{p} \subset A/\mathfrak{a}} \mathfrak{p}\right) = \bigcap_{\substack{\mathfrak{p} \subset A \\ \mathfrak{a} \subset \mathfrak{p}}} \mathfrak{p}. \quad \square$$

Satz 1.25. Für die Menge D der Nullteiler von A gilt

$$D = \bigcup_{x \neq 0} r(\text{Ann}(x)).$$

Beweis. Für eine Teilmenge(!) $E \subset A$ definieren wir $r(E)$ wie für Ideale. Dann ist $r(E)$ wieder eine Teilmenge und man sieht leicht $r(\bigcup_i E_i) = \bigcup_i r(E_i)$. Für ein Element $x \in r(D)$ existiert ein $n \in \mathbb{N}$, so dass x^n Nullteiler ist. Dann ist aber auch schon x Nullteiler. Wir erhalten:

$$\begin{aligned} D = r(D) &= r\left(\bigcup_{x \neq 0} (\text{Ann}(x))\right) \\ &= \bigcup_{x \neq 0} r(\text{Ann}(x)). \end{aligned}$$

□

Beispiel 1.26. Sei $A = \mathbb{Z}$, $\mathfrak{a} = (m)$ und p_1, \dots, p_n seien die (verschiedenen) Primteiler von m . Dann gilt $r(\mathfrak{a}) = (p_1 \cdots p_n)$.

Satz 1.27. $r(\mathfrak{a}) + r(\mathfrak{b}) = (1) \implies \mathfrak{a} + \mathfrak{b} = (1)$.

Beweis. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r((1)) = (1)$, also $\mathfrak{a} + \mathfrak{b} = (1)$. □

Erweiterung und Kontraktion

Sei $f : A \rightarrow B$ ein Ringhomomorphismus.

Definition 1.28. (i) Für ein Ideal $\mathfrak{a} \subset A$ nennt man

$$\mathfrak{a}^e := Bf(\mathfrak{a}) = \left\{ \sum_{\text{endl.}} b_i f(a_i) \mid b_i \in B, a_i \in \mathfrak{a} \right\}$$

die **Erweiterung** von \mathfrak{a} auf B .

(ii) Für ein Ideal $\mathfrak{b} \subset B$ heißt

$$\mathfrak{b}^c := f^{-1}(\mathfrak{b})$$

die **Kontraktion** von \mathfrak{b} auf A .

Bemerkungen 1.29. • Wir können f in der Form

$$A \xrightarrow{p} f(A) \xhookrightarrow{i} B$$

faktorisieren. Die Situation für p ist einfach nach Satz 1.1, i ist kompliziert.

- Ist $\mathfrak{q} \subset B$ ein Primideal, so auch $\mathfrak{q}^c \subset A$.
- Ist $\mathfrak{p} \subset A$ ein Primideal, so muss $\mathfrak{p}^e \subset B$ nicht unbedingt ein Primideal sein.

Beispiel 1.30. Wir betrachten $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$.

Frage: Welche Primideale aus \mathbb{Z} „bleiben“ Primideale in $\mathbb{Z}[i]$? Da \mathbb{Z} und $\mathbb{Z}[i]$ euklidisch, also faktoriell sind (siehe Algebra I), stellt sich die Frage: Welche Primzahlen bleiben als Elemente in $\mathbb{Z}[i]$ irreduzibel? Wir brauchen die folgende zahlentheoretische Aussage.

Satz von Lagrange: Eine Primzahl p ist genau dann als Summe zweier Quadratzahlen darstellbar, wenn $p \not\equiv 3 \pmod{4}$.

Sei $p \in \mathbb{Z}$ eine Primzahl. Aus $p = (x+iy) \cdot (x'+iy')$ folgt $p^2 = N(x+iy) \cdot N(x'+iy')$. Sind beides keine Einheiten, so folgt

$$p = N(x+iy) = (x+iy)(x-iy) = x^2 + y^2.$$

Also: $p \equiv 3 \pmod{4} \Rightarrow p$ irreduzibel in $\mathbb{Z}[i]$.

Für $p = 2$ gilt $2 = (1+i)(1-i) = -i(1+i)^2$. In Idealen: $(2)^e = (1+i)^2$.

Sei nun $p \equiv 1 \pmod{4}$ und $x, y \in \mathbb{N}$ mit $p = x^2 + y^2$. Dann gilt

$$p = (x+iy)(x-iy).$$

In Idealen $(p)^e = (x+iy) \cdot (x-iy)$. Wegen $N(x+iy) = p$ ist $x+iy$ irreduzibel. Jetzt kann man noch nachrechnen, dass $(x+iy) \not\sim (x-iy)$ und erhält:

Zerlegungsgesetz in $\mathbb{Z}[i]$

$$(p)^e = \begin{cases} \text{Primideal, wenn} & p \equiv 3 \pmod{4}, \\ \text{Produkt zweier verschiedener PI, wenn} & p \equiv 1 \pmod{4}, \\ \text{Quadrat eines Primideals, wenn} & p = 2. \end{cases}$$

Im Allgemeinen haben wir die folgenden Aussagen. Es sei $f : A \rightarrow B$ ein Ringhomomorphismus und $\mathfrak{a} \subset A$, $\mathfrak{b} \subset B$ Ideale.

Satz 1.31. (i) $\mathfrak{a} \subset \mathfrak{a}^{ec}$, $\mathfrak{b} \supset \mathfrak{b}^{ce}$.

(ii) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$

(iii) Sei C die Menge der Ideale in A die Kontraktionen von Idealen aus B sind und E die Menge der Ideale in B die Erweiterungen von Idealen in A sind. Dann gilt

$$\begin{aligned} C &= \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}, \\ E &= \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}. \end{aligned}$$

Wir haben Bijektionen

$$C \begin{array}{c} \xrightarrow{\mathfrak{a} \mapsto \mathfrak{a}^e} \\ \xleftarrow{\mathfrak{b}^c \mapsto \mathfrak{b}} \end{array} E.$$

Beweis. (i) folgt durch Einsetzen der Definitionen.

(ii): Nach (i) erhalten wir

$$\begin{aligned} \mathfrak{b}^c &\subset (\mathfrak{b}^c)^{ec} = \mathfrak{b}^{cec} \quad \text{und} \\ \mathfrak{b}^c &\supset (\mathfrak{b}^{ce})^c = \mathfrak{b}^{cec}. \end{aligned}$$

Die andere Aussage zeigt man analog.

(iii): Für $\mathfrak{a} \in C$ gilt $\mathfrak{a} = \mathfrak{b}^c$ für ein \mathfrak{b} . Also $\mathfrak{a}^{ec} = \mathfrak{b}^{cec} = \mathfrak{b}^c = \mathfrak{a}$.

Analog: $\mathfrak{b} \in E$, $\mathfrak{b} = \mathfrak{a}^e$ für $\mathfrak{a} \subset A$ und $\mathfrak{b}^{ce} = \mathfrak{a}^{ece} = \mathfrak{a}^e = \mathfrak{b}$.

Die Bijektion folgt. □

Lemma 1.32. Es seien $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$, $\mathfrak{b}_1, \mathfrak{b}_2 \subset B$. Dann gilt

$$\begin{aligned} (\mathfrak{a}_1 + \mathfrak{a}_2)^e &= \mathfrak{a}_1^e + \mathfrak{a}_2^e, (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 \cap \mathfrak{a}_2)^e &\subset \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 \mathfrak{a}_2)^e &= \mathfrak{a}_1^e \mathfrak{a}_2^e, (\mathfrak{b}_1 \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c \mathfrak{b}_2^c, \\ (\mathfrak{a}_1 : \mathfrak{a}_2)^e &\subset (\mathfrak{a}_1^e : \mathfrak{a}_2^e), (\mathfrak{b}_1 : \mathfrak{b}_2)^c \subset (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\ r(\mathfrak{a})^e &\subset r(\mathfrak{a}^e), r(\mathfrak{b})^c = r(\mathfrak{b}^c). \end{aligned}$$

Beweis. Übungsaufgabe. □

2 Moduln

Sei R ein Ring, unitär aber hier noch nicht notwendig kommutativ und seien M und N R -(Links-)Moduln. Die Menge der R -Modulhomomorphismen von M nach N wird mit $\text{Hom}_R(M, N)$ bezeichnet und wird zur abelschen Gruppe durch

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m).$$

Ist $R = A$ kommutativ, so wird $\text{Hom}_A(M, N)$ zum A -Modul durch

$$(a\varphi)(m) = a(\varphi(m)).$$

Lemma 2.1. Die natürliche Abbildung

$$\mathrm{Hom}_R(R, M) \rightarrow M, \varphi \mapsto \varphi(1),$$

ist ein Isomorphismus abelscher Gruppen. Ist $R = A$ kommutativ, so ist sie ein Isomorphismus von A -Moduln.

Beweis. Injektivität. $\varphi(1) = 0 \Rightarrow \varphi(r) = r\varphi(1) = 0$ für alle $r \in R$.

Surjektivität: Sei $m \in M$ beliebig. Definiere $\varphi : R \rightarrow M$ durch $\varphi(r) = rm$. Dann bildet sich φ auf m ab. \square

Operationen auf Untermoduln.

Sei M ein R -Modul und $(M_i)_{i \in I}$ eine Familie von Untermoduln. Dann ist $\bigcap_{i \in I} M_i$ ein Untermodul, sowie

$$\sum_{i \in I} M_i = \left\{ \sum_i m_i \mid m_i \in M_i, m_i = 0 \text{ für fast alle } i \right\}.$$

Dies ist der kleinste Untermodul in M , der alle M_i enthält.

Ist $\mathfrak{a} \subset R$ ein (Links)Ideal und M ein R -(Links)Modul, so definiert man den Untermodul $\mathfrak{a}M \subset M$ durch

$$\mathfrak{a}M = \left\{ \sum_{\text{endl.}} a_i m_i \mid a_i \in \mathfrak{a}, m_i \in M \right\}.$$

Sind N, P Untermoduln in M , so setzt man

$$(N : P) = \{r \in R \mid rP \subset N\}.$$

$(N : P)$ ist ein (Links)Ideal in R . Gilt $P \subset N$, so ist $(N : P) = R$.

Spezialfall:

Definition 2.2.

$$\mathrm{Ann}(M) = (0 : M) = \{r \in R \mid rm = 0 \quad \forall m \in M\}$$

heißt der **Annulator** von M . Es heißt M **treuer** R -Modul, wenn $\mathrm{Ann}(M) = 0$ gilt.

Bemerkung 2.3. Sei $R = A$ kommutativ. Ist M ein A -Modul und $\mathfrak{a} \subset \mathrm{Ann}(M)$ ein Ideal, so können wir M als A/\mathfrak{a} -Modul auffassen: setze $(a + \mathfrak{a})m = am$. Wegen $\mathfrak{a}M = 0$ ist die Definition repräsentantenunabhängig. Als $A/\mathrm{Ann}(M)$ -Modul ist M treu.

Lemma 2.4. Es seien $N, P \subset M$ Untermoduln. Dann gilt

- (i) $\text{Ann}(N + P) = \text{Ann}(N) \cap \text{Ann}(P)$.
- (ii) $(N : P) = \text{Ann}((N + P)/N)$.

Beweis. Übungsaufgabe. □

Ist M ein freier A -Modul vom Rang n , so gibt es nach Wahl einer Basis einen Isomorphismus $M \cong A^n$ und einen Isomorphismus

$$\text{End}_A(M) \cong \text{Mat}_{n,n}(A).$$

Für eine $n \times n$ -Matrix M über A haben wir die **Adjunkte** M^{ad}

$$M^{ad} = (y_{ij}) \in \text{Mat}_{n,n}(A)$$

mit $y_{ij} = (-1)^{i+j} \det(M_{j,i})$, wobei $M_{j,i}$ aus M durch Streichen der j -ten Zeile und i -ten Spalte entsteht.

Satz 2.5. (Cramersche Regel) Es gilt

$$M^{ad} \cdot M = M \cdot M^{ad} = \text{diag}(\det(M), \dots, \det(M)).$$

Beweis. Siehe LA I, 4.36. □

Satz 2.6. Sei M ein endlich erzeugter A -Modul, $\mathfrak{a} \subset A$ ein Ideal und $\phi \in \text{End}_A(M)$ mit $\phi(M) \subset \mathfrak{a}M$. Dann genügt ϕ einer Gleichung

$$\phi^n + a_{n-1}\phi^{n-1} + \dots + a_0 = 0$$

mit $a_0, \dots, a_{n-1} \in \mathfrak{a}$.

Beweis. Seien x_1, \dots, x_n Erzeuger von M . Für jedes

$$x \in \mathfrak{a}M = \left\{ \sum_{\text{endl.}} \alpha_i y_i \mid \alpha_i \in \mathfrak{a}, y_i \in M \right\}$$

finden wir (stelle y_i als Linearkombination von x_1, \dots, x_n dar) eine Darstellung der Form

$$x = \sum_{i=1}^n a_i x_i, \quad a_i \in \mathfrak{a}.$$

Somit gilt für $i = 1, \dots, n$:

$$\phi(x_i) = \sum_{j=1}^n a_{ij} x_j, \quad \text{mit gewissen } a_{ij} \in \mathfrak{a}.$$

Es folgt $\sum_{j=1}^n (\delta_{ij} \phi - a_{ij})(x_j) = 0$, wobei $\delta_{ij} = \text{Kronecker-}\delta$.

Wir betrachten nun den von ϕ über A in $\text{End}_A(M)$ erzeugten Teilring

$$A[\phi] = \left\{ \sum_{\text{endl.}} a_i \phi^i \right\} \subset \text{End}_A(M),$$

(Konvention: $\phi^0 = \text{id}_M$). Es ist $A[\phi]$ ist kommutativer Ring mit 1 und

$$X := (\delta_{ij}\phi - a_{ij})_{ij}$$

ist eine $n \times n$ -Matrix mit Werten in $A[\phi]$. Nach Satz 2.5 erhalten wir

$$X^{ad} \cdot X = \text{diag}(\det(X)).$$

Durch die Regel $(\sum a_i \phi^i)(x) = \sum a_i \phi^i(x)$ wird M in natürlicher Weise zu einem $A[\phi]$ -Modul. Es gilt

$$X \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0, \quad \text{und daher nach Cramer } \text{diag}(\det(X)) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Weil nun aber die x_i den A -Modul M erzeugen, folgt $\det(X) \cdot x = 0$ für alle $x \in M$, d.h. $\det(X) = 0 \in A[\phi] \subset \text{End}_A(M)$. Nach der Leibniz-Formel entwickelt, gilt nun

$$\det(X) = \det((\delta_{ij}\phi - a_{ij})_{ij}) = \phi^n + \alpha_{n-1}\phi^{n-1} + \cdots + \alpha_0$$

mit gewissen $\alpha_i \in \mathfrak{a}$. □

Korollar 2.7. Sei M ein endlich erzeugter A -Modul und \mathfrak{a} ein Ideal mit $\mathfrak{a}M = M$. Dann existiert ein $a \in A$, $a \equiv 1 \pmod{\mathfrak{a}}$, mit $aM = 0$.

Beweis. Wir benutzen Satz 2.6 mit $\phi = \text{id}_M$ und erhalten $a_0, \dots, a_{n-1} \in \mathfrak{a}$ mit

$$x + a_{n-1}x + \cdots + a_0x = 0 \quad \text{für alle } x \in M.$$

Setze $a = 1 + a_{n-1} + \cdots + a_0$. □

Satz 2.8. (Nakayamas Lemma) Sei (A, \mathfrak{m}) ein lokaler Ring und M ein endlich erzeugter A -Modul. Dann folgt aus $\mathfrak{m}M = M$, dass $M = 0$.

Beweis. Nach Korollar 2.7 existiert ein $a \in A$, $a \equiv 1 \pmod{\mathfrak{m}}$, mit $aM = 0$. Wegen $a - 1 \in \mathfrak{m}$ folgt $a \in A^\times$. Es folgt $M = 1 \cdot M = a^{-1}aM = a^{-1}0 = 0$. □

Korollar 2.9. Es sei (A, \mathfrak{m}) ein lokaler Ring, M ein endlich erzeugter A -Modul und N ein Untermodul von M . Dann folgt aus $M = \mathfrak{m}M + N$, dass $M = N$.

Beweis. Es gilt $\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N$. Nach Voraussetzung gilt $\mathfrak{m}(M/N) = M/N$, also $M/N = 0$ nach Satz 2.8. □

Korollar 2.10. Es sei (A, \mathfrak{m}) ein lokaler Ring, $k = A/\mathfrak{m}$ und M ein endlich erzeugter A -Modul. Für Elemente $x_1, \dots, x_n \in M$ sind äquivalent:

- (i) x_1, \dots, x_n erzeugen M als A -Modul.
- (ii) Die Bilder $\bar{x}_1, \dots, \bar{x}_n$ von x_1, \dots, x_n in $M/\mathfrak{m}M$ erzeugen den k -Vektorraum $M/\mathfrak{m}M$.

Beweis. Sei N der durch x_1, \dots, x_n in M erzeugte Untermodul. Die Komposition $N \hookrightarrow M \rightarrow M/\mathfrak{m}M$ hat das Bild $(N + \mathfrak{m}M)/\mathfrak{m}M$. Daher gilt

$$\bar{x}_1, \dots, \bar{x}_n \text{ erzeugen } M/\mathfrak{m}M \iff N + \mathfrak{m}M = M \xrightarrow{2.9} N = M. \quad \square$$

3 Tensorprodukte

Es sei A ein kommutativer Ring.

Definition 3.1. Seien M, N, P A -Moduln. Eine Abbildung $f: M \times N \rightarrow P$ heißt **(A-)bilinear**, wenn

- (1) für jedes $m \in M$ ist die Abbildung $N \rightarrow P, n \mapsto f(m, n)$ A -linear.
- (2) für jedes $n \in N$ ist die Abbildung $M \rightarrow P, m \mapsto f(m, n)$ A -linear.

Satz 3.2. Seien A -Moduln M, N gegeben. Es gibt ein Paar (T, g) bestehend aus einem A -Modul T und einer bilinearen Abbildung $g: M \times N \rightarrow T$ mit folgender **Universaleigenschaft**:

Zu jedem A -Modul P und jeder bilinearen Abbildung $f: M \times N \rightarrow P$ existiert ein eindeutig bestimmter A -Modulhomomorphismus $h: T \rightarrow P$, so daß $f = h \circ g$ gilt.

(T, g) ist eindeutig bis auf kanonische Isomorphie.

Beweis. Eindeutigkeit: Diese folgt in der üblichen Weise durch Ausnutzung der Universaleigenschaft.

Existenz: Sei $C = A^{(M \times N)} = \bigoplus_{M \times N} A$. Elemente von C sind formale endliche A -Linearkombinationen von Elementen aus $M \times N$. (Man identifiziere ein Element $i \in M \times N$ mit dem Element in C , dessen i -te Komponente gleich 1 und alle anderen Komponenten gleich 0 sind). Wir betrachten den Untermodul D von C der durch alle Elemente der Form

$$\begin{aligned} (x + x', y) &= (x, y) + (x', y) \\ (x, y + y') &= (x, y) + (x, y') \\ a(x, y) &= (ax, y) \\ a(x, y) &= (x, ay) \end{aligned}$$

erzeugt wird und setzen $T = C/D$. Wir bezeichnen das Bild von $1 \cdot (x, y) \in C$ in T mit $x \otimes y$. Dann ist T durch Elemente der Form $x \otimes y$ erzeugt, und diese erfüllen:

$$\begin{aligned}(x + x') \otimes y &= x \otimes y + x' \otimes y, \\ x \otimes (y + y') &= x \otimes y + x \otimes y', \\ (ax) \otimes y &= x \otimes (ay) = a(x \otimes y).\end{aligned}$$

M.a.W.: Die Abbildung $g: M \times N \rightarrow T$, $(x, y) \mapsto x \otimes y$ ist bilinear.

Ist nun $f: M \times N \rightarrow P$ eine bilineare Abbildung, so erhalten wir wegen der universellen Eigenschaft der direkten Summe einen natürlichen Homomorphismus

$$\bar{f}: A^{(M \times N)} = C \rightarrow P$$

mit $\sum_{\text{endl.}} a_i(x_i, y_i) \rightarrow \sum_{\text{endl.}} a_i f(x_i, y_i)$. \bar{f} verschwindet auf den Erzeugern von D und daher auf ganz D . Daher induziert \bar{f} einen wohldefinierten Homomorphismus $h: C/D = T \rightarrow P$ mit

$$h(x \otimes y) = \bar{f}((x, y)) = f(x, y).$$

Der Homomorphismus h ist durch die Eigenschaft eindeutig auf einfachen Tensoren und damit insgesamt eindeutig bestimmt. \square

Bemerkungen 3.3. 1) T heißt das **Tensorprodukt** von M und N . Schreibweise: $T = M \otimes_A N$ oder auch $T = M \otimes N$.

Gewöhnungsbedürftig: Die Elemente von $M \otimes N$ sind endliche Summen $\sum_{\text{endl.}} x_i \otimes y_i$, die man nicht immer vereinfachen kann.

2) Für $x \in M$ gilt $x \otimes 0 = 0$ in $M \otimes N$ wegen $x \otimes 0 = x \otimes (0 + 0) = x \otimes 0 + x \otimes 0$. Also $x \otimes 0 = 0$.

3) Wir werden die Konstruktion des Tensorprodukts nicht mehr brauchen, nur die universelle Eigenschaft und, dass das Tensorprodukt von den einfachen Tensoren $x \otimes y$ erzeugt wird, sowie die Rechenregeln.

4) Ist (x_1, \dots, x_m) ein Erzeugendensystem von M und (y_1, \dots, y_n) ein Erzeugendensystem von N , so ist

$$(x_i \otimes y_j)_{\substack{i=1, \dots, m \\ j=1, \dots, n}}$$

ein Erzeugendensystem von $M \otimes N$. Insbesondere ist das Tensorprodukt endlich erzeugter A -Moduln wieder endlich erzeugt.

Bemerkung 3.4. Ist R ein nicht-kommutativer Ring, so kann man das Tensorprodukt $M \otimes_R N$ zwischen einem R -Rechtsmodul M und einem R -Linksmodul N definieren. Dieses ist (nur noch) eine abelsche Gruppe.

Multitensorprodukt: Sind M_1, \dots, M_n und P A -Moduln, so nennen wir eine Abbildung

$$f: M_1 \times \dots \times M_n \longrightarrow P$$

multilinear, wenn f in jedem Argument linear ist. Ganz analog zeigt man die Existenz des Multi-Tensorprodukts $M_1 \otimes \cdots \otimes M_n$, das universell bezüglich multilinearer Abbildungen ist. Es wird durch Multitensoren $x_1 \otimes \cdots \otimes x_n$, $x_i \in M_i$, $i = 1, \dots, n$, erzeugt.

Lemma 3.5. *Seien M, N, P A -Moduln. Dann gibt es eindeutig bestimmte A -Modulisomorphismen*

- (i) $M \otimes N \xrightarrow{\sim} N \otimes M$,
- (ii) $(M \otimes N) \otimes P \xrightarrow{\sim} M \otimes (N \otimes P)$,
- (iii) $(M \oplus N) \otimes P \xrightarrow{\sim} M \otimes P \oplus N \otimes P$,
- (iv) $A \otimes M \xrightarrow{\sim} M$,

so dass entsprechend gilt

- (a) $x \otimes y \mapsto y \otimes x$,
- (b) $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$,
- (c) $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$,
- (d) $a \otimes x \mapsto ax$.

Beweis. Die Eindeutigkeit folgt dadurch, dass die Abbildungen auf den einfachen Tensoren vorgegeben sind, und diese das Tensorprodukt erzeugen.

(i) Betrachte die Komposition $\bar{\phi} : M \times N \xrightarrow{\text{Vert}} N \times M \xrightarrow{\text{kan}} N \otimes M$, also die Abbildung $\bar{\phi} : M \times N \rightarrow N \otimes M$, $(x, y) \mapsto y \otimes x$. Es ist $\bar{\phi}$ bilinear. Z.B.

$$\bar{\phi}(x_1 + x_2, y) = y \otimes (x_1 + x_2) = y \otimes x_1 + y \otimes x_2 = \bar{\phi}(x_1, y) + \bar{\phi}(x_2, y).$$

Dies zeigt die Existenz einer eindeutig bestimmten Abbildung $\phi : M \otimes N \rightarrow N \otimes M$ mit $\phi(m \otimes n) = n \otimes m$. Umgekehrt erhalten wir $\psi : N \otimes M \rightarrow M \otimes N$ mit $\psi(n \otimes m) = m \otimes n$. Schließlich gilt $\psi \circ \phi = \text{id}_{M \otimes N}$, $\phi \circ \psi = \text{id}_{N \otimes M}$ (weil diese Gleichheiten auf einfachen Tensoren stimmen.)

(ii) Betrachte die Abbildung

$$\bar{\phi} : M \times N \times P \longrightarrow (M \otimes N) \otimes P, \quad (x, y, z) \longmapsto (x \otimes y) \otimes z.$$

Diese Abbildung ist trilinear und induziert so eine Abbildung

$$\phi : M \otimes N \otimes P \rightarrow (M \otimes N) \otimes P$$

mit $x \otimes y \otimes z \mapsto (x \otimes y) \otimes z$. Nun fixieren wir ein Element $z \in P$. Die Abbildung

$$\bar{f}_z : M \times N \longrightarrow M \otimes N \otimes P, \quad (x, y) \longmapsto x \otimes y \otimes z$$

ist bilinear und induziert eine Abbildung

$$f_z : M \otimes N \longrightarrow M \otimes N \otimes P$$

mit $f_z(x \otimes y) = x \otimes y \otimes z$.

Nun betrachten wir $\bar{f}: (M \otimes N) \times P \rightarrow M \otimes N \otimes P$ mit $\bar{f}(t, z) = f_z(t)$ ein Homomorphismus. Desweiteren gilt für festes $t = \sum_{i=1}^n x_i \otimes y_i \in M \otimes N$ dass:

$$\begin{aligned}\bar{f}(t, z_1 + z_2) &= \\ f_{z_1+z_2}(\sum x_i \otimes y_i) &= \sum x_i \otimes y_i \otimes (z_1 + z_2) \\ &= \sum x_i \otimes y_i \otimes z_1 + \sum x_i \otimes y_i \otimes z_2 \\ &= f_{z_1}(\sum x_i \otimes y_i) + f_{z_2}(\sum x_i \otimes y_i) \\ &= \bar{f}(t, z_1) + \bar{f}(t, z_2).\end{aligned}$$

Analog zeigt man $\bar{f}(t, az) = a\bar{f}(t, z)$. Daher ist \bar{f} bilinear und induziert einen eindeutig bestimmten Homomorphismus $f: (M \otimes N) \otimes P \rightarrow M \otimes N \otimes P$ mit $(x \otimes y) \otimes z \mapsto x \otimes y \otimes z$. Wir erhalten $f \circ \phi = \text{id}_{M \otimes N \otimes P}$ und $\phi \circ f = \text{id}_{(M \otimes N) \otimes P}$, d.h. ϕ ist ein Isomorphismus $M \otimes N \otimes P \xrightarrow{\sim} (M \otimes N) \otimes P$. Analog konstruiert man einen Isomorphismus

$$\psi: M \otimes N \otimes P \xrightarrow{\sim} M \otimes (N \otimes P)$$

mit $\psi(x \otimes y \otimes z) = x \otimes (y \otimes z)$ und die Komposition

$$\psi \circ \phi^{-1}: (M \otimes N) \otimes P \xrightarrow{\sim} M \otimes (N \otimes P)$$

ist ein Isomorphismus der $(x \otimes y) \otimes z$ auf $x \otimes (y \otimes z)$ abbildet.

(iii) Die Kompositionen

$$(M \oplus N) \times P \xrightarrow{((x,y),z) \mapsto (x,z)} M \times P \xrightarrow{\text{kan}} M \otimes P$$

$$(M \oplus N) \times P \xrightarrow{((x,y),z) \mapsto (y,z)} N \times P \xrightarrow{\text{kan}} N \otimes P$$

setzen sich zu einer Abbildung

$$\bar{\phi}: (M \oplus N) \times P \rightarrow (M \otimes P) \oplus (N \otimes P)$$

mit $((x, y), z) \mapsto x \otimes z + y \otimes z$ zusammen. Diese Abbildung ist linear in $M \oplus N$ und in P : Z.B. $\bar{\phi}((x_1, y_1) + (x_2, y_2), z) = (x_1 + x_2) \otimes z + (y_1 + y_2) \otimes z$
 $= x_1 \otimes z + x_2 \otimes z + y_1 \otimes z + y_2 \otimes z = (x_1 \otimes z + y_1 \otimes z) + (x_2 \otimes z + y_2 \otimes z)$
 $= \bar{\phi}((x_1, y_1), z) + \bar{\phi}((x_2, y_2), z)$

und wir erhalten einen Homomorphismus

$$\phi: (M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$$

mit $\phi((x, y) \otimes z) = x \otimes z + y \otimes z$.

Umgekehrt betrachten wir $\bar{\psi}_1: M \times P \rightarrow (M \oplus N) \otimes P$ mit $\bar{\psi}_1(x, z) = (x, 0) \otimes z$ und erhalten $\psi_1: M \otimes P \rightarrow (M \oplus N) \otimes P$. Analog $\psi_2: N \otimes P \rightarrow (M \oplus N) \otimes P$.

Diese setzen sich zusammen zu einem Homomorphismus $\psi : (M \otimes P) \oplus (N \otimes P) \rightarrow (M \oplus N) \otimes P$ und wieder ist $\phi \circ \psi = \text{id}$, $\psi \circ \phi = \text{id}$.

(iv) $\bar{\phi} : A \times M \rightarrow M$, $\bar{\phi}(a, x) = ax$ induziert $\phi : A \otimes M \rightarrow M$ wie gewünscht. Betrachten wir umgekehrt die zusammengesetzte Abbildung $\psi : M \rightarrow A \times M \mapsto A \otimes M$, $x \mapsto (1, x) \mapsto 1 \otimes x$, so gilt $\phi \circ \psi = \text{id}$ und auch $\psi \circ \phi = \text{id}$ wegen $a \otimes x \mapsto ax \mapsto 1 \otimes ax = a \otimes x$. \square

Korollar 3.6. Es gilt

$$A^m \otimes A^n \cong A^{mn}$$

Beweis.

$$\begin{aligned} A^m \otimes A^n &= \underbrace{(A \oplus \dots \oplus A)}_{m\text{-mal}} \otimes \underbrace{(A \oplus \dots \oplus A)}_{n\text{-mal}} \\ &= \underbrace{(A \otimes A) \oplus \dots \oplus (A \otimes A)}_{mn\text{-mal}} \\ &= A^{mn}. \end{aligned}$$

\square

Das Tensorprodukt vertauscht nicht nur mit endlichen, sondern auch mit beliebigen direkten Summen

Lemma 3.7. Sei $(M_i)_{i \in I}$ eine Familie von A -Moduln und N ein weiterer A -Modul. Dann gibt es einen natürlichen Isomorphismus

$$\left(\bigoplus_{i \in I} M_i \right) \otimes N \cong \bigoplus_{i \in I} M_i \otimes N.$$

Beweis. Den Beweis lassen wir als Übungsaufgabe. \square

Korollar 3.8. Ist M ein A -Modul und I eine Indexmenge, so gilt

$$(A^{(I)}) \otimes M \cong M^{(I)}.$$

Beweis. Nach 3.5(iv) gilt $A \otimes M \cong M$. Nach 3.7 folgt

$$(A^{(I)}) \otimes M = \left(\bigoplus_{i \in I} A \right) \otimes M \cong \bigoplus_{i \in I} A \otimes M \cong \bigoplus_{i \in I} M = M^{(I)}. \quad \square$$

Satz 3.9. Sei $\mathfrak{a} \subset A$ ein Ideal und M ein A -Modul. Dann gibt es einen natürlichen Isomorphismus

$$\phi : A/\mathfrak{a} \otimes M \xrightarrow{\sim} M/\mathfrak{a}M$$

mit $(r + \mathfrak{a}) \otimes m \mapsto rm + \mathfrak{a}M$.

Beweis. Wir zeigen zunächst:

Behauptung: jedes Element in $A/\mathfrak{a} \otimes M$ ist von der Form $(1 + \mathfrak{a}) \otimes m$ für ein $m \in M$.

Beweis der Behauptung: Es gilt

$$\sum (a_i + \mathfrak{a}) \otimes m_i = \sum a_i ((1 + \mathfrak{a}) \otimes m_i) = (1 + \mathfrak{a}) \otimes \left(\sum a_i m_i \right).$$

Nun betrachten wir die Abbildung $\bar{\phi} : A/\mathfrak{a} \times M \rightarrow M/\mathfrak{a}M$, $(a + \mathfrak{a}, m) \mapsto am + \mathfrak{a}M$. Diese ist bilinear und induziert die gesuchte Abbildung $\phi : A/\mathfrak{a} \otimes M \xrightarrow{\sim} M/\mathfrak{a}M$. Es bleibt zu zeigen, dass ϕ ein Isomorphismus ist.

Wegen $m + \mathfrak{a}M = \phi((1 + \mathfrak{a}) \otimes m)$ ist ϕ surjektiv. Bleibt zu zeigen, dass ϕ injektiv ist. Sei $x \in \ker(\phi)$. Z.z: $x = 0 \in A/\mathfrak{a} \otimes M$. Nach der obigen Behauptung können wir ohne Einschränkung annehmen, dass $x = (1 + \mathfrak{a}) \otimes m$ für ein $m \in M$ gilt. Es folgt $0 = \phi(x) = 1m + \mathfrak{a}M$. Hieraus folgt $m \in \mathfrak{a}M$, also $m = \sum a_i m_i$ mit $a_i \in \mathfrak{a}$, $m_i \in M$. Es folgt

$$\begin{aligned} x &= (1 + \mathfrak{a}) \otimes m = (1 + \mathfrak{a}) \otimes \left(\sum_i a_i m_i \right) = \\ &= \sum_i (1 + \mathfrak{a}) \otimes a_i m_i = \sum_i (a_i + \mathfrak{a}) \otimes m_i = \sum_i (0 + \mathfrak{a}) \otimes m_i = \sum_i 0 = 0. \end{aligned}$$

□

Korollar 3.10. Sind $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale, so gilt

$$A/\mathfrak{a} \otimes A/\mathfrak{b} \cong A/(\mathfrak{a} + \mathfrak{b}).$$

Beweis. Man setzt $M = A/\mathfrak{b}$ in 3.9 und erhält

$$A/\mathfrak{a} \otimes A/\mathfrak{b} \cong (A/\mathfrak{b})/\mathfrak{a}(A/\mathfrak{b}).$$

Nun gilt

$$\mathfrak{a}(A/\mathfrak{b}) = \left\{ \sum_{\text{endl.}} a_i (r_i + \mathfrak{b}) \mid a_i \in \mathfrak{a}, r_i \in A \right\} = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b}.$$

Es folgt

$$(A/\mathfrak{b})/\mathfrak{a}(A/\mathfrak{b}) = (A/\mathfrak{b})/((\mathfrak{a} + \mathfrak{b})/\mathfrak{b}) = A/(\mathfrak{a} + \mathfrak{b}).$$

□

Funktoriell Verhalten

Seien $f : M_1 \rightarrow M_2$, $g : N_1 \rightarrow N_2$ A -Modulhomomorphismen. Dann gibt es eine wohldefinierte A -lineare Abbildung

$$f \otimes g : M_1 \otimes N_1 \longrightarrow M_2 \otimes N_2$$

mit $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

Grund: Die bilineare Abbildung $M_2 \times N_2 \rightarrow M_2 \otimes N_2$, $(x, y) \rightarrow x \otimes y$, induziert über f und g eine bilineare Abbildung $M_1 \times N_1 \rightarrow M_2 \otimes N_2$ mit $(x, y) \mapsto f(x) \otimes g(y)$. Nach Universaleigenschaft existiert daher die Abbildung $M_1 \otimes N_1 \rightarrow M_2 \otimes N_2$ wie beschrieben.

Lemma 3.11. Sind f und g surjektiv, so auch $f \otimes g$.

Beweis. Sei $z = x_1 \otimes y_1 + \cdots + x_n \otimes y_n \in M_2 \otimes N_2$ beliebig. Setze

$$\bar{z} = \bar{x}_1 \otimes \bar{y}_1 + \cdots + \bar{x}_n \otimes \bar{y}_n \in M_1 \otimes N_1$$

mit Urbildern $\bar{x}_1, \dots, \bar{x}_n$ von x_1, \dots, x_n unter f und $\bar{y}_1, \dots, \bar{y}_n$ von y_1, \dots, y_n unter g . Dann gilt $(f \otimes g)(\bar{z}) = z$. \square

Warnung: Sind f und g injektiv, so braucht das $f \otimes g$ nicht zu sein.

Beispiel 3.12. Betrachte die injektiven Homomorphismen von \mathbb{Z} -Moduln:

$$f : \mathbb{Z} \rightarrow \mathbb{Z}, \quad x \mapsto 2x, \quad g = \text{id}_{\mathbb{Z}/2\mathbb{Z}} : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}.$$

Dann ist

$$f \otimes g : \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$$

die Nullabbildung wegen

$$(f \otimes g)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$$

für beliebige $x \in \mathbb{Z}$, $y \in \mathbb{Z}/2\mathbb{Z}$.

Nun sei $f : A \rightarrow B$ ein Ringhomomorphismus (man sagt, B ist eine A -Algebra). B wird zum A -Modul durch $ab := f(a)b$. Allgemeiner können wir jeden B -Modul N durch $an := f(a)n$ als A -Modul auffassen.

Definition/Lemma 3.13. Für einen A -Modul M betrachten wir

$$M_B = M \otimes_A B.$$

Für $b \in B$ ist die b -Multiplikationsabbildung $b(m \otimes b') := m \otimes bb'$ wohldefiniert und definiert eine B -Modulstruktur auf M_B . Man nennt M_B den **Basiswechsel von M nach B** .

Beweis. Für festes $b \in B$ ist die Abbildung $M \times B \rightarrow M \otimes_A B$, $(m, b') \mapsto m \otimes bb'$ A -bilinear und induziert somit die b -Multiplikationsabbildung $\cdot b : M \otimes_A B \rightarrow M \otimes_A B$, $b(m \otimes b') := m \otimes bb'$. Dass diese Regel eine B -Modulstruktur auf M_B induziert folgt direkt aus den Rechenregeln für Tensoren. \square

Satz 3.14. *Es sei B eine A -Algebra, M ein A -Modul und N ein B -Modul. Dann gibt es natürliche Isomorphismen von B -Moduln*

- (i) $\text{Hom}_B(M \otimes_A B, N) \cong \text{Hom}_A(M, N)$,
- (ii) $(M \otimes_B B) \otimes_B N \cong M \otimes_A N$.

Hier ist die B -Modulstruktur auf $\text{Hom}_A(M, N)$ durch $(bf)(m) = bf(m)$ gegeben und die B -Modulstruktur auf $M \otimes_A N$ durch $b(m \otimes n) = m \otimes bn$.

Beweis. Zunächst bemerken wir, dass für $b \in B$ die beschriebene b -Wirkung auf $M \otimes_A N$ wohldefiniert ist, weil $M \times N \rightarrow M \otimes_A N$, $(m, n) \mapsto m \otimes bn$ A -bilinear ist.

- (i) Wir betrachten die Abbildung

$$\Phi : \text{Hom}_B(M \otimes_A B, N) \rightarrow \text{Hom}_A(M, N), \quad \Phi(f)(m) := f(m \otimes 1_B).$$

In der anderen Richtung ist für $g \in \text{Hom}_A(M, N)$ die Abbildung $M \times B \rightarrow N$, $(m, b) \mapsto bg(m)$ A -bilinear und induziert damit einen Homomorphismus $M \otimes_A B \rightarrow N$, $m \otimes b \mapsto bg(m)$. Daher ist

$$\Psi : \text{Hom}_A(M, N) \rightarrow \text{Hom}_B(M \otimes_A B, N), \quad \Psi(g)(m \otimes b) = bg(m)$$

wohldefiniert. Man rechnet leicht nach, dass Φ und Ψ zueinander invers sind.

- (ii) Für festes $n \in N$ ist $M \times B \rightarrow M \otimes_A N$, $(m, b) \mapsto m \otimes bn$, A -bilinear und induziert $\phi_n : M \otimes_A B \rightarrow M \otimes_A N$. Wir machen $M \otimes_A N$ zum B -Modul durch Die Zuordnung $(M \otimes_A B) \times N \rightarrow M \otimes_A N$, $(m \otimes b, n) \mapsto \phi_n(m \otimes b) = m \otimes bn$ ist B -bilinear und induziert

$$\Phi : (M \otimes_B B) \otimes_B N \longrightarrow M \otimes_A N.$$

Man rechnet leicht nach, dass Φ und Ψ zueinander invers sind. □