Algebra II

Sommersemester 2010

W. Ebeling

©Wolfgang Ebeling
Institut für Algebraische Geometrie
Leibniz Universität Hannover
Postfach 6009
30060 Hannover
E-mail: ebeling@math.uni-hannover.de

Kapitel 1

Körper

1.1 Normale und separable Körpererweiterungen

Es sollen nun andere Bedingungen dafür angegeben werden, wann eine Körpererweiterung eine Galois-Erweiterung ist.

Definition Eine Körpererweiterung E eines Körpers K heißt *normal*, wenn gilt:

(a) Die Körpererweiterung E von K ist algebraisch.

(b) Jedes *irreduzible* Polynom $f(x) \in K[x]$, das in E eine Nullstelle hat, zerfällt über E in Linearfaktoren.

Bemerkung 1.1.1 Eine Körpererweiterung E eines Körpers K ist offensichtlich genau dann normal, wenn sie algebraisch ist und für jedes $a \in E$ gilt: Das Minimalpolynom von a über K zerfällt über E in Linearfaktoren.

Satz 1.1.1 *Für eine* endliche *Körpererweiterung E eines Körpers K sind folgende Aussagen äquivalent:*

(i) *Die Körpererweiterung E von K ist normal.*

(ii) *Der Körper E ist der Zerfällungskörper eines Polynoms $f(x) \in K[x]$.*

(iii) *Ist E' eine Körpererweiterung von E und $\varphi : E \to E'$ ein Homomorphismus mit $\varphi|_K = \mathrm{id}_K$, so gilt $\varphi(E) \subset E$.*

Beweis.

(i) $\Rightarrow$ (ii): Da E eine endliche Körpererweiterung von K ist, gibt es nach Satz I.5.4.4 über K algebraische Elemente $a_1, \ldots, a_n \in E$ mit $E = K(a_1, \ldots, a_n)$. Da die Körpererweiterung E von K normal ist, zerfällt für jedes $i = 1, \ldots, n$ das Minimalpolynom $f_i(x)$ von a_i über K über E in Linearfaktoren. Also ist $E = K(a_1, \ldots, a_n)$ der Zerfällungskörper des Polynoms

$$f(x) := f_1(x) \cdots f_n(x) \in K[x].$$

(ii) $\Rightarrow$ (iii): Nach Korollar I.5.6.2 gibt es $a_1, \ldots, a_n, b \in E$ mit

$$f(x) = b(x - a_1) \cdots (x - a_n)$$

und $E = K(a_1, \ldots, a_n)$. Ist E' und $\varphi : E \to E'$ wie in (iii), so gilt

$$f(\varphi(a_i)) = \varphi(f(a_i)) = \varphi(0) = 0 \text{ für jedes } i = 1, \ldots, n.$$

Damit folgt

$$\varphi(\{a_1, \ldots, a_n\}) \subset \{a_1, \ldots, a_n\},$$

also nach Satz I.5.2.8 auch

$$\varphi(K(a_1, \ldots, a_n)) \subset K(a_1, \ldots, a_n) = E.$$

(iii) $\Rightarrow$ (i): Da die Körpererweiterung E von K endlich ist, ist sie nach Satz I.5.4.4 algebraisch. Also ist die Bedingung (a) in der Definition einer normalen Körpererweiterung erfüllt. Wir müssen nun die Bedingung (b) nachprüfen. Dazu sei $f(x) \in K[x]$ ein irreduzibles Polynom, das eine Nullstelle a in E hat. Wir können dann $a_1, \ldots, a_n \in E$ so wählen, dass $E = K(a, a_1, \ldots, a_n)$ gilt. Ist $f_i(x) \in K[x]$ das Minimalpolynom von a_i über K, $i = 1, \ldots, n$, und

$$g(x) := f(x)f_1(x) \cdots f_n(x),$$

so ist E ein Zwischenkörper des Zerfällungskörpers E' von $g(x)$ über K. Das Polynom $f(x)$ zerfällt natürlich auch über E' in Linearfaktoren. Ist $a' \in E'$ eine Nullstelle von $f(x)$ in E', so gibt es nach Satz I.5.6.2 einen Automorphismus $\psi : E' \to E'$ mit $\psi(a) = a'$ und $\psi|_K = \mathrm{id}_K$. Wegen $E \subset E'$ ist $\varphi = \psi|_E : E \to E'$ ein Homomorphismus, auf den wir die Bedingung (iii) anwenden können. Wegen $a \in E$ und $\varphi(E) \subset E$ folgt $a' = \varphi(a) \in E$. Also zerfällt $f(x)$ schon über E in Linearfaktoren. □

Definition Es sei K ein Körper, E der Zerfällungskörper eines nicht konstanten Polynoms $f(x) \in K[x]$ und $\alpha \in E$. Die natürliche Zahl

$$\nu(f(x), \alpha) := \max\{n \in \mathbb{N} \mid (x - \alpha)^n \text{ teilt } f(x) \text{ in } E[x]\}$$

heißt *Vielfachheit* von $f(x)$ in α.

Gilt $\nu(f(x), \alpha) = 1$, so nennt man α eine *einfache Nullstelle* von $f(x)$. Im Fall $\nu(f(x), \alpha) \geq 2$ heißt α eine *mehrfache Nullstelle* von $f(x)$.

Definition Es sei K ein Körper.

(a) Ein irreduzibles Polynom $f(x) \in K[x]$ heißt *separabel*, wenn $f(x)$ keine mehrfachen Nullstellen in seinem Zerfällungskörper besitzt. Ein nicht konstantes Polynom $f(x) \in K[x]$ heißt *separabel*, wenn alle seine irreduziblen Faktoren es sind. Andernfalls heißt es *inseparabel*.

(b) Es sei E eine Körpererweiterung von K. Ein Element $\alpha \in E$ heißt *separabel* über K, wenn α Nullstelle eines separablen Polynoms $f(x) \in K[x]$ ist.

(c) Eine Körpererweiterung E von K heißt *separabel*, wenn jedes $\alpha \in E$ separabel über K ist.

(d) Ein Körper K heißt *vollkommen*, wenn jedes nicht konstante Polynom aus $K[x]$ separabel ist.

Bemerkung 1.1.2 Ist E eine Körpererweiterung eines Körpers K und $\alpha \in E$ algebraisch über K, so ist α genau dann separabel über K, wenn sein Minimalpolynom über K separabel ist.

Lemma 1.1.1 *Es sei K ein Körper, $f(x) \in K[x]$ ein nicht konstantes Polynom und E der Zerfällungskörper von $f(x)$. Dann hat $f(x)$ in E genau dann mehrfache Nullstellen, wenn $f(x)$ und $f'(x)$ in $K[x]$ einen nicht konstanten gemeinsamen Teiler haben.*

Beweis.

"$\Rightarrow$": Es sei $\alpha \in E$ eine mehrfache Nullstelle von $f(x)$ und $g(x)$ das Minimalpolynom von α über K. Nach Lemma I.5.7.1 gilt dann $f(\alpha) = f'(\alpha) = 0$. Da $g(x)$ jedes Polynom aus $K[x]$, das α als Nullstelle hat, teilt, ist $g(x)$ ein gemeinsamer Teiler von $f(x)$ und $f'(x)$.

"$\Leftarrow$": Es sei $g(x)$ ein gemeinsamer Teiler von $f(x)$ und $f'(x)$ mit $\operatorname{grad} g(x) \geq 1$ und $\alpha \in E$ eine Nullstelle von $g(x)$. Dann gilt auch $f(\alpha) = f'(\alpha) = 0$. Nach Lemma I.5.7.1 ist also α eine mehrfache Nullstelle von $f(x)$. □

Satz 1.1.2 *Es sei K ein Körper. Ein* irreduzibles *Polynom $f(x) \in K[x]$ ist genau dann separabel, wenn $f'(x) \neq 0$ gilt.*

Beweis. Es sei E der Zerfällungskörper von $f(x)$.

Es sei zunächst $f'(x) = 0$. Dann ist nach Lemma I.5.7.1 jede Nullstelle von $f(x)$ in E eine mehrfache Nullstelle. Also ist $f(x)$ nicht separabel.

Nun sei $f'(x) \neq 0$. Angenommen, $f(x)$ ist nicht separabel. Nach Lemma 1.1.1 haben dann $f(x)$ und $f'(x)$ in $K[x]$ einen nicht konstanten gemeinsamen Teiler $g(x) \in K[x]$. Da $f(x)$ irreduzibel in $K[x]$ ist, folgt $\operatorname{grad} g(x) = \operatorname{grad} f(x) > \operatorname{grad} f'(x)$, ein Widerspruch. □

Korollar 1.1.1 *Jeder Körper der Charakteristik Null ist vollkommen.*

Beweis. Es sei K ein Körper mit $\operatorname{char}(K) = 0$ und $f(x) \in K[x]$. Dann ist $f(x)$ genau dann konstant, wenn $f'(x) = 0$ gilt. Damit folgt die Behauptung aus Satz 1.1.2. □

Lemma 1.1.2 *Es sei K ein Körper der Charakteristik $p > 0$ und $f(x) \in K[x]$. Dann gilt $f'(x) = 0$ genau dann, wenn es ein $g(x) \in K[x]$ gibt mit*

$$f(x) = g(x^p).$$

Beweis. Die Bedingung $f'(x) = 0$ ist äquivalent dazu, dass $f(x)$ von der Form

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{mp} x^{mp}$$

ist. □

Satz 1.1.3 *Ein Körper K der Charakteristik $p > 0$ ist genau dann vollkommen, wenn sein Frobenius-Homomorphismus surjektiv ist.*

Beweis.

"$\Rightarrow$": Es sei K vollkommen. Dann ist für jedes $a \in K$ das Polynom $f(x) := x^p - a \in K[x]$ separabel. Es sei $g(x) \in K[x]$ ein irreduzibler Faktor von $f(x)$, E sein Zerfällungskörper und $b \in E$ eine Nullstelle von $g(x)$. Dann gilt

$$g(b) = 0 \Rightarrow b^p = a \Rightarrow f(x) = x^p - b^p = (x - b)^p \text{ in } E[x].$$

Da $f(x)$ separabel ist, ist auch $g(x)$ separabel, hat also nur einfache Nullstellen in E. Also folgt $g(x) = x - b$ und damit $b \in K$. Zu jedem $a \in K$ gibt es also ein $b \in K$ mit $b^p = a$. Also ist der Frobenius-Homomorphismus surjektiv.

"$\Leftarrow$": Der Frobenius-Homomorphismus sei nun surjektiv und $f(x) \in K[x]$ irreduzibel. Angenommen, $f(x)$ ist nicht separabel. Dann gibt es nach Lemma 1.1.2 ein $g(x) \in K[x]$ mit $f(x) = g(x^p)$. Das bedeutet, dass $f(x)$ von der Form

$$f(x) = a_0 + a_1 x^p + \cdots + a_n (x^p)^n, \quad a_0, \ldots, a_n \in K,$$

ist. Da der Frobenius-Homomorphismus surjektiv ist, gibt es zu jedem $i = 0, \ldots, n$ ein $b_i \in K$ mit $b_i^p = a_i$. Also gilt

$$\begin{aligned} f(x) &= b_0^p + b_1^p x^p + \cdots + b_n^p (x^n)^p \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^p. \end{aligned}$$

Also wäre $f(x)$ nicht irreduzibel. □

Korollar 1.1.2 *Jeder endliche Körper ist vollkommen.*

Unser Ziel ist es nun, den folgenden Satz zu beweisen:

Satz 1.1.4 (Charakterisierung einer Galois-Erweiterung) *Für eine Körpererweiterung E eines Körpers K sind folgende Aussagen äquivalent:*

(i) *E ist eine Galois-Erweiterung von K.*

(ii) *Die Körpererweiterung ist endlich, normal und separabel.*

(iii) *E ist der Zerfällungskörper eines separablen Polynoms aus $K[x]$.*

Für den Beweis dieses Satzes benötigen wir noch zwei Hilfssätze.

Lemma 1.1.3 *Es sei E eine Körpererweiterung eines Körpers K und $\alpha_1, \ldots, \alpha_n$ seien paarweise verschiedene Elemente von E. Im Polynomring $E[x]$ gelte*

$$(x - \alpha_1) \cdots (x - \alpha_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

Dann gilt für jeden Monomorphismus $\varphi : E \to E$ mit $\varphi(\{\alpha_1, \ldots, \alpha_n\}) = \{\alpha_1, \ldots, \alpha_n\}$:

$$\varphi(s_i) = s_i \text{ für } i = 1, \ldots, n.$$

Beweis. Es sei

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

und $\varphi : E \to E$ ein Monomorphismus mit der angegebenen Eigenschaft. Wir betrachten die Fortsetzung $\Phi : E[x] \to E[x]$ auf den Polynomring. Dann gilt

$$\Phi(f(x)) = (x - \varphi(\alpha_1)) \cdots (x - \varphi(\alpha_n)) = f(x).$$

Daraus folgt $\varphi(s_i) = s_i$ für $i = 1, \ldots, n$. □

Lemma 1.1.4 *Es sei E eine Galois-Erweiterung eines Körpers K und $\alpha \in E$. Es gelte*

$$\{\varphi(\alpha) \mid \varphi \in \mathrm{Aut}(E;K)\} = \{\alpha_1, \ldots, \alpha_n\},$$

wobei $\alpha_1, \ldots, \alpha_n \in E$ paarweise verschieden sind.

Dann ist $f(x) := (x-\alpha_1)\cdots(x-\alpha_n)$ das Minimalpolynom von α über K.

Beweis. Es gilt $\varphi(\{\alpha_1, \ldots, \alpha_n\}) = \{\alpha_1, \ldots, \alpha_n\}$ für jedes $\varphi \in \mathrm{Aut}(E;K)$. Nach Lemma 1.1.3 liegen daher die Koeffizienten von $f(x)$ in $\mathrm{Fix}(E;\mathrm{Aut}(E;K))$. Da E eine Galois-Erweiterung von K ist, gilt $\mathrm{Fix}(E;\mathrm{Aut}(E;K)) = K$. Da $f(x)$ normiert ist und $f(\alpha) = 0$ gilt, ist nur noch zu zeigen: $f(x)$ ist irreduzibel in $K[x]$. Dazu sei $f(x) = g(x)h(x)$ mit $g(x), h(x) \in K[x]$. Es sei $g(\alpha) = 0$. Zu jedem $i = 1, \ldots, n$ gibt es aber ein $\varphi \in \mathrm{Aut}(E;K)$ mit $\alpha_i = \varphi(\alpha)$. Daraus folgt

$$g(\alpha_i) = g(\varphi(\alpha)) = \varphi(g(\alpha)) = 0 \text{ für } i = 1, \ldots, n.$$

Da die Elemente $\alpha_1, \ldots, \alpha_n$ paarweise verschieden sind, folgt $f(x)|g(x)$. Also ist $h(x)$ eine Einheit in $K[x]$. □

Beweis von Satz 1.1.4.

(i) ⇒ (ii): Nach Lemma I.5.10.4 und der Definition einer Galois-Erweiterung ist die Körpererweiterung E von K endlich. Nach Lemma 1.1.4 ist das Minimalpolynom jedes Elements $\alpha \in E$ über K endliches Produkt von paarweise verschiedenen Linearfaktoren, also separabel. Also ist die Körpererweiterung E von K auch normal und separabel.

(ii) ⇒ (iii): Die Körpererweiterung E von K sei endlich, normal und separabel. Nach Satz 1.1.1 ist E der Zerfällungskörper eines Polynoms $f(x) \in K[x]$. Wir zeigen, dass $f(x)$ separabel ist. Dazu sei $g(x)$ ein irreduzibler Faktor von $f(x)$ und $\alpha \in E$ eine Nullstelle von $g(x)$. Dann ist $g(x)$ bis auf einen konstanten Faktor gleich dem Minimalpolynom von α über K. Da α separabel über K ist, ist nach Bemerkung 1.1.2 das Polynom $g(x)$ separabel.

(iii) ⇒ (i): Es sei E der Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$ und $G := \mathrm{Aut}(E;K)$. Dann ist $[E:K]$ und damit auch $[E : \mathrm{Fix}(E;G)]$ endlich. Aus Lemma I.5.10.2 folgt

$$|G| \leq [E : \mathrm{Fix}(E;G)] < \infty.$$

Wir zeigen $\mathrm{Fix}(E;G) = K$. Dies zeigen wir durch Induktion über die Anzahl n der Nullstellen von $f(x)$ in $E \setminus K$.

Induktionsanfang: Für $n = 0$ gilt $E = K$ und daher $\mathrm{Fix}(E;G) = K$.

Induktionsschritt: Es sei nun $n \geq 1$ und $\alpha \in E \setminus K$ eine Nullstelle von $f(x)$. Wir ersetzen nun den Grundkörper K durch $K' := K(\alpha)$. Dann ist E der Zerfällungskörper des separablen Polynoms $f(x) \in K'[x]$, das höchstens $n-1$ Nullstellen in $E \setminus K'$ hat. Nach Induktionssannahme gibt es eine endliche Untergruppe G' von $\mathrm{Aut}(E)$ mit

$$\mathrm{Fix}(E; G') = K' \text{ und } G' = \mathrm{Aut}(E; K') \subset G.$$

Es sei nun $\beta \in \mathrm{Fix}(E; G) \subset \mathrm{Fix}(E; G') = K(\alpha)$. Wir müssen zeigen, dass $\beta \in K$ gilt. Dazu sei $g(x)$ das Minimalpolynom von α über K und $r := \operatorname{grad} g(x)$. Das Polynom $g(x)$ ist ein Teiler von $f(x)$ in $K[x]$, also auch separabel. Nach Satz I.5.4.3 gibt es Elemente $c_0, \ldots, c_{r-1} \in K$ mit

$$\beta = c_0 + c_1\alpha + \cdots + c_{r-1}\alpha^{r-1}.$$

Es seien $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ die Nullstellen von $g(x)$ in E. Nach Satz I.5.6.2 gibt es zu jedem $i = 1, \ldots, r$ ein $\varphi_i \in G$ mit $\varphi_i(\alpha) = \alpha_i$. Wegen $\beta \in \mathrm{Fix}(E; G)$ erhält man

$$\beta = \varphi_i(\beta) = c_0 + c_1\alpha_i + \cdots + c_{r-1}\alpha_i^{r-1} \text{ für } i = 1, \ldots, r.$$

Das Polynom

$$h(x) := (c_0 - \beta) + c_1 x + \cdots + c_{n-1}x^{n-1} \in E[x]$$

hat daher die r Nullstellen $\alpha_1, \ldots, \alpha_r$. Wegen $\operatorname{grad} h(x) \leq r-1$ folgt $h(x) = 0$, also $\beta = c_0 \in K$. □

Mit Hilfe von Korollar 1.1.1 folgt aus Satz 1.1.4 sofort:

Korollar 1.1.3 *Ist K ein Körper der Charakteristik 0, so ist eine Körpererweiterung E von K genau dann eine Galois-Erweiterung, wenn sie Zerfällungskörper eines Polynoms aus $K[x]$ ist.*

1.2 Der Satz vom primitiven Element

Nach Satz I.5.4.4 gilt für eine endliche Körpererweiterung E von K, dass sie algebraisch ist und und dass es Elemente $\alpha_1, \ldots, \alpha_n \in E$ gibt mit $E = K(\alpha_1, \ldots, \alpha_n)$. Wir stellen nun die Frage, wann sich eine endliche Körpererweiterung schon durch Adjunktion eines einzigen Elements erhalten lässt. Eine Antwort darauf gibt der folgende Satz.

Satz 1.2.1 (Satz vom primitiven Element) *Es sei K ein unendlicher Körper, $K \subset E$ eine endliche separable Körpererweiterung. Dann gibt es ein $\alpha \in E$ mit $E = K(\alpha)$. Ferner gilt: Wird E über K von $a_1, \ldots, a_n$ erzeugt, dann ist $\alpha = \sum_{i=1}^{n} \lambda_i a_i$, $\lambda_i \in K$.*

Beweis. Da E eine endliche Körpererweiterung von K ist, gibt es Elemente $a_1, \ldots, a_n \in E$ mit $E = K(a_1, \ldots, a_n)$. Da E separabel ist, sind die Elemente $a_1, \ldots, a_n$ separabel über K. Es sei nun $f_i(x) \in K[x]$ das Minimalpolynom von a_i über K, $i = 1, \ldots, n$. Dann ist das Polynom

$$f(x) := f_1(x) \cdots f_n(x) \in K[x]$$

separabel. Es sei L der Zerfällungskörper von $f(x)$ über K. Es gilt $K \subset E \subset L$ und nach Satz 1.1.4 ist L ist eine endliche Galoiserweiterung von K. Aus dem Hauptsatz der Galoistheorie folgt, dass es nur endliche viele echte Zwischenkörper $L_1, \ldots, L_m$ von $K \subset L$ gibt. Also gibt es auch nur endlich viele echte Zwischenkörper $L_1, \ldots, L_r$ von $K \subset E$.

Die Zwischenkörper $L_1, \ldots, L_r$ können nun als K-Unterräume des K-Vektorraums E aufgefasst werden. Da K unendlich viele Elemente hat, gibt es ein $\alpha \in E$, dass nicht in der Vereinigung $L_1 \cup \cdots \cup L_r$ liegt. Für dieses α gilt

$$K(\alpha) \subset E, \qquad K(\alpha) \neq L_i, \quad i = 1, \ldots, r.$$

Also folgt $E = K(\alpha)$.

Der Zusatz ist klar. □

1.3 Auflösung von Gleichungen

Wir betrachten eine Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_j \in \mathbb{C}),$$

wobei x eine Unbekannte ist. Der Fundamentalsatz der Algebra besagt, dass eine solche Gleichung vom Grad n ($a_n \neq 0$) immer eine Lösung in $\mathbb{C}$ besitzt und es mit Vielfachheit gezählt genau n Lösungen in $\mathbb{C}$ gibt.

Es ist nun ein altes Problem, Formeln aufzustellen, mit deren Hilfe man die Lösungen aus den Koeffizienten $a_0, \ldots, a_n$ der gegebenen Gleichung ausrechnen. Eine solche Formel kennen Sie schon aus der Schule für quadratische Gleichungen. Bei einer quadratischen Gleichung

$$a_2 x^2 + a_1 x + a_0 = 0 \quad (a_2 \neq 0)$$

kann man zunächst durch a_2 teilen und erhält eine Gleichung der Form

$$x^2 + px + q = 0.$$

Für diese Gleichung hat man die bekannte Lösungsformel

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Auch für Gleichungen dritten Grades gibt es solche Formeln. Dies sind die so genannten *Formeln von Cardano*. Bei einer Gleichung dritten Grades

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \quad (a_3 \neq 0)$$

kann man zunächst wieder durch a_3 dividieren, also annehmen, dass $a_3 = 1$ ist. Mit Hilfe einer Substitution

$$x \mapsto x - \frac{a_2}{3},$$

einer so genannten *Tschirnhaus-Transformation*, kann man den quadratischen Term eliminieren. Es genügt daher, Gleichungen der Form

$$x^3 + px + q = 0 \quad (p, q \in \mathbb{C})$$

zu betrachten. Für eine solche Gleichung definiert man die *Diskriminante* D der Gleichung durch

$$D := -(4p^3 + 27q^2).$$

Ferner setzt man

$$\begin{aligned} A &:= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \\ B &:= \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}, \end{aligned}$$

wobei die komplexen dritten Wurzeln so bestimmt sein sollen, dass $AB = -3p$ gilt. Außerdem betrachten wir die dritten Einheitswurzeln

$$\begin{aligned} \rho &:= e^{\frac{2\pi i}{3}} = \frac{1}{2}(-1 + i\sqrt{3}), \\ \overline{\rho} &:= e^{\frac{4\pi i}{3}} = \frac{1}{2}(-1 - i\sqrt{3}). \end{aligned}$$

Dann hat die obige Gleichung die drei Lösungen

$$\begin{aligned} x_1 &= \frac{1}{3}(A+B), \\ x_2 &= \frac{1}{3}(\rho^2 A + \rho B) = \frac{1}{3}(\overline{\rho} A + \rho B), \\ x_3 &= \frac{1}{3}(\rho A + \rho^2 B) = \frac{1}{3}(\rho A + \overline{\rho} B). \end{aligned}$$

Auch für Gleichungen vierten Grades kennt man noch solche Formeln. Als weitere Anwendung der Galoistheorie werden wir zeigen, dass es für Gleichungen höheren Grades keine solchen Formeln mehr gibt.

1.4 Auflösbare Gruppen

Wir benötigen nun noch weitere Resultate aus der Gruppentheorie.

Definition Es sei G eine Gruppe.

(a) Für $a, b \in G$ heißt

$$[a,b] := aba^{-1}b^{-1}$$

der *Kommutator* von a und b.

(b) Die Menge

$$K(G) := \{[a_1,b_1]\cdots[a_k,b_k] \mid k \in \mathbb{N}\setminus\{0\},\ a_1,\ldots,a_k,b_1,\ldots,b_k \in G\},$$

die aus allen endlichen Produkten von Kommutatoren besteht, ist eine Untergruppe von G und heißt die *Kommutatorgruppe* von G.

Lemma 1.4.1 *Es sei G eine Gruppe und e ihr neutrales Element. Dann gilt:*

(i) *G abelsch $\Leftrightarrow$ $K(G) = \{e\}$.*

(ii) *Die Kommutatorgruppe $K(G)$ von G ist ein Normalteiler von G.*

Beweis.
(i) ist klar.
(ii) Es sei $g \in G$ und $c \in K(G)$ gegeben. Dann gibt es ein $k \in \mathbb{N}\setminus\{0\}$ und $a_1,\ldots,a_k,b_1,\ldots,b_k \in G$ mit

$$c = [a_1,b_1]\cdots[a_k,b_k].$$

Dann folgt

$$\begin{aligned} gcg^{-1} &= g[a_1, b_1]g^{-1} \cdots g[a_k, b_k]g^{-1} \\ &= [ga_1g^{-1}, gb_1g^{-1}] \cdots [ga_kg^{-1}, gb_kg^{-1}] \in K(G). \end{aligned}$$

□

Lemma 1.4.2 *Es sei G eine Gruppe und N ein Normalteiler von G. Dann gilt:*

$$G/N \text{ abelsch } \Leftrightarrow K(G) \subset N.$$

Beweis.

"⇒": Es sei $\pi : G \to G/N$ der kanonische Epimorphismus. Da G/N abelsch ist, gilt für alle $a, b \in G$:

$$\pi([a, b]) = \pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} = N.$$

Daraus folgt $[a, b] \in \operatorname{Ker} \pi = N$, und damit $K(G) \subset N$.

"⇐": Wegen $K(G) \subset N$ gilt für alle $a, b \in G$:

$$(aN)(bN) = (ab)N = (ab[b^{-1}, a^{-1}])N = (ba)N = (bN)(aN).$$

□

Beispiel 1.4.1 Es sei S_n die symmetrische Gruppe und A_n die alternierende Gruppe von n Elementen. Dann gilt

(1) $K(S_n) = A_n$ falls $n \geq 2$.

(2) $K(A_n) = A_n$ falls $n \geq 5$.

(1) Wegen $|S_n/A_n| = 2$ ist die Gruppe S_n/A_n abelsch. Nach Lemma 1.4.2 folgt $K(S_n) \subset A_n$.

Die Inklusion $A_2 \subset K(S_2)$ ist klar. In den Übungen wurde gezeigt, dass für $n \geq 3$ jede gerade Permutation aus S_n ein Produkt von Dreierzyklen ist. Für paarweise verschiedene $i, j, k \in \{1, \ldots, n\}$ gilt aber

$$\langle i, j, k\rangle = \langle i, k\rangle \circ \langle j, k\rangle \circ \langle i, k\rangle^{-1} \circ \langle j, k\rangle^{-1} \in K(A_n).$$

(2) Im Fall $n \geq 5$ kann man zeigen, dass jeder Dreierzyklus ein Kommutator von Dreierzyklen ist:

$$\langle i, j, k\rangle = \langle i, j, \ell\rangle \circ \langle i, k, m\rangle \circ \langle i, j, \ell\rangle^{-1} \circ \langle i, k, m\rangle^{-1} \in K(A_n),$$

wobei i, j, k, ℓ, m paarweise verschieden sind.

Definition Es sei G eine Gruppe und e ihr neutrales Element. Die Gruppe G heißt *auflösbar*, wenn es eine Kette

$$G = N_0 \supset N_1 \supset \cdots \supset N_\ell = \{e\}$$

von Untergruppen $N_i \subset G$ $(i = 0, \ldots, \ell)$ gibt, so dass gilt: Für $i = 0, \ldots, \ell-1$ ist N_{i+1} Normalteiler von N_i und N_i/N_{i+1} abelsch.

Notation Die Kommutatorbildung kann man iterieren. Für eine Gruppe G definieren wir induktiv:

$$K^0(G) := G \text{ und } K^m(G) := K(K^{m-1}(G)) \text{ für } m \in \mathbb{N} \setminus \{0\}.$$

Satz 1.4.1 *Eine Gruppe G ist genau dann auflösbar, wenn es ein $\ell \in \mathbb{N}$ gibt mit $K^\ell(G) = \{e\}$.*

Beweis.
"$\Rightarrow$": Dies folgt durch Induktion über i aus Lemma 1.4.2.
"$\Leftarrow$": Die Kette

$$G = K^0(G) \supset K^1(G) = K(G) \supset \cdots \supset K^\ell(G) = \{e\}$$

ist nach Lemma 1.4.1 und Lemma 1.4.2 eine Kette von Untergruppen von G mit den gewünschten Eigenschaften. □

Beispiel 1.4.2 (1) Jede abelsche Gruppe ist auflösbar.

(2) Die Gruppen S_n und A_n sind für $n \geq 5$ nicht auflösbar, da für alle $m \in \mathbb{N} \setminus \{0\}$ nach Beispiel 1.4.1 gilt:

$$K^m(A_n) = K^m(S_n) = A_n.$$

Satz 1.4.2 *Ist G eine endliche auflösbare Gruppe, so gibt es eine Kette*

$$G = N_0 \supset N_1 \supset \cdots \supset N_\ell = \{e\}$$

von Untergruppen $N_i \subset G$ $(i = 0, \ldots, \ell)$, so dass gilt: Für $i = 0, \ldots, \ell - 1$ ist N_{i+1} Normalteiler von N_i und N_i/N_{i+1} eine zyklische Gruppe von Primzahlordnung.

Beweis. Da G auflösbar ist, gibt es eine Kette

$$G = N_0 \supset N_1 \supset \cdots \supset N_\ell = \{e\}$$

von Untergruppen $N_i \subset G$ $(i = 0, \ldots, \ell)$ gibt, so dass gilt: Für $i = 0, \ldots, \ell-1$ ist N_{i+1} Normalteiler von N_i und N_i/N_{i+1} abelsch. Wir können dabei annehmen, dass $N_i \neq N_{i+1}$ für $i = 0, \ldots, \ell - 1$ gilt. Wir verfeinern nun diese Kette,

indem wir zwischen N_{i+1} und N_i so lange geeignete Untergruppen von N_i einschieben, bis die Quotientengruppen zyklisch werden.

Es sei $a \in N_i/N_{i+1}$, $a \neq N_{i+1}$, ein Element von Primzahlordnung. Ein solches Element existiert, da G endlich ist. Es sei $\langle a \rangle$ die von a erzeugte zyklische Untergruppe von N_i/N_{i+1}, $\pi : N_i \to N_i/N_{i+1}$ der kanonische Epimorphismus und $U := \pi^{-1}(\langle a \rangle)$. Da N_i/N_{i+1} abelsch ist, ist U ein Normalteiler von N_i. Da der Homomorphismus $\pi_U : U \to N_i/N_{i+1}$ den Kern N_{i+1} und das Bild $\langle a \rangle$ hat, folgt nach dem Homomorphiesatz

$$U/N_{i+1} \cong \langle a \rangle.$$

Die Gruppe U/N_{i+1} ist also eine zyklische Gruppe von Primzahlordnung. Die Gruppe N_i/U ist abelsch, denn die Zuordnung $bN_{i+1} \mapsto bU$ liefert einen Epimorphismus $\rho : N_i/N_{i+1} \to N_i/U$. Wenn $U = N_i$ ist, sind wir fertig. Ansonsten wiederholen wir die Konstruktion mit U anstelle von N_{i+1}. □

Lemma 1.4.3 *Ist $f : G \to G'$ ein Gruppenhomomorphismus, so gilt für alle $m \in \mathbb{N}$*

$$f(K^m(G)) = K^m(f(G)) \subset K^m(G').$$

Beweis. Es gilt für alle $a, b \in G$

$$f([a,b]) = f(aba^{-1}b^{-1}) = f(a)f(b)f(a)^{-1}f(b)^{-1} = [f(a), f(b)].$$

Die Inklusion $K^m(f(G)) \subset K^m(G')$ ist klar, da $f(G)$ eine Untergruppe von G' ist. Die Gleichung

$$f(K^m(G)) = K^m(f(G))$$

beweisen wir durch Induktion nach m.

Induktionsanfang: Für $m = 0$ ist sie klar, für $m = 1$ folgt sie aus der obigen Gleichung.

Induktionsschritt: Es gilt

$$\begin{aligned} f(K^{m+1}(G)) &= f(K(K^m(G))) = K(f(K^m(G))) \text{ (nach obiger Gleichung)} \\ &= K(K^m(f(G))) \text{ (nach Induktionsannahme)} \\ &= K^{m+1}(f(G)). \end{aligned}$$

□

Satz 1.4.3 (i) *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

(ii) *Ist $N \subset G$ ein Normalteiler, so gilt:*

$$G \text{ auflösbar} \Leftrightarrow N \text{ und } G/N \text{ auflösbar.}$$

Beweis. (i) Ist $H \subset G$ eine Untergruppe und $\iota : H \to G$ die Inklusionsabbildung, so folgt aus Lemma 1.4.3 für alle $m \in \mathbb{N}$

$$\iota(K^m(H)) = K^m(\iota(H)) \subset K^m(G).$$

Ist G auflösbar, so folgt aus Satz 1.4.1 dass $K^\ell(G) = \{e\}$ für ein $\ell \in \mathbb{N}$. Damit gilt auch $K^\ell(H) = \{e\}$.

(ii) " $\Rightarrow$": Nach (i) ist N auflösbar. Es sei $\pi : G \to G/N$ der kanonische Homomorphismus. Dann folgt aus Lemma 1.4.3

$$K^m(G/N) = \pi(K^m(G)).$$

Daher ist mit G auch G/N auflösbar.

"$\Leftarrow$" Nach Satz 1.4.1 können wir ein $\ell \in \mathbb{N}$ wählen mit $K^\ell(N) = \{e\}$ und $K^\ell(G/N) = \{\bar{e}\}$, wobei $\bar{e} = N$ das neutrale Element in G/N ist. Nach Lemma 1.4.3 gilt wieder

$$\pi(K^\ell(G)) = K^\ell(G/N) = \{\bar{e}\},$$

also $K^\ell(G) \subset N$. Daraus folgt

$$K^{2\ell}(G) = K^\ell(K^\ell(G)) \subset K^\ell(N) = \{e\}.$$

□

Satz 1.4.4 *Ist p eine Primzahl und $n \in \mathbb{N}$, so ist jede Gruppe G der Ordnung p^n auflösbar.*

Beweis. Wir beweisen den Satz durch Induktion über n.

Induktionsanfang: Für $n = 0$ ist der Satz trivial.

Induktionsschritt: Es sei $n \geq 1$. Dann betrachten wir das Zentrum Z von G. Nach I.2.4 ist dies ein Normalteiler von G. Es gilt $|Z| = p^m$ mit $m \leq n$. Das Korollar I.2.4.1 zur Klassenformel besagt

$$|G| = \sum_{h \in R} [G : C_G(h)],$$

wobei R ein Repräsentantensystem der Konjugationsklassen von G ist. Das Zentrum besteht nun gerade aus den Fixpunkten der Operation durch Konjugation von G auf sich selbst, also den Elementen $g \in G$, für die Bahnen dieser Operation, die Konjugationsklassen, einelementig sind. Damit können wir die Klassenformel so umschreiben

$$|G| = |Z| + \sum_{i=1}^{k} [G : C_G(h_i)],$$

wobei $h_1, \ldots, h_k$ Repräsentanten der mehrelementigen Konjugationsklassen sind. Da alle Summanden dieser Formel Potenzen von p sind, folgt hieraus $m > 0$, also

$$|G/Z| = p^{n-m} < p^n.$$

Nach Induktionsannahme ist G/Z auflösbar. Da Z abelsch und damit ebenfalls auflösbar ist, folgt die Behauptung aus Satz 1.4.3. □

1.5 Radikalerweiterungen

Wir wollen nun die Galoistheorie auf die Frage der Auflösbarkeit von Gleichungen durch Radikale anwenden. Dazu dienen die folgenden Vorbereitungen. Es sei μ_n die Gruppe der n-ten Einheitswurzeln in K (vgl. I.5.7).

Definition Es sei K ein Körper. Ein Polynom

$$x^n - a \quad (n \in \mathbb{N} \setminus \{0\},\ a \in K)$$

wird *reines Polynom* über K genannt.

Satz 1.5.1 *Es sei $n \in \mathbb{N} \setminus \{0\}$ und K ein Körper, dessen Charakteristik kein Teiler von n ist. Es gelte $\mu_n \subset K$. Dann gilt:*

(i) *Die Galoisgruppe des Polynoms $f(x) = x^n - a$ ($a \in K^*$) ist zyklisch.*

(ii) *Zu jeder Galois-Erweiterung E von K vom Grad n mit zyklischer Galoisgruppe $\mathrm{Aut}(E;K)$ gibt es ein $\alpha \in E$ mit $E = K(\alpha)$ und $\alpha^n \in K$. Insbesondere ist dann E Zerfällungskörper des reinen Polynoms $x^n - \alpha^n \in K[x]$.*

Beweis.

(i) Da $\mathrm{char}\, K$ kein Teiler von n ist, ist das Polynom $f(x)$ separabel. Es sei E der Zerfällungskörper von $f(x)$ und $\zeta \in K$ eine primitive n-te Einheitswurzel. Wenn $\alpha \in E$ eine Nullstelle von $f(x)$ ist, dann ist

$$\{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$$

die Menge aller Nullstellen von $f(x)$. Also gilt $E = K(\alpha)$.

Jedes $\sigma \in \mathrm{Aut}(E;K)$ ist durch $\sigma(\alpha) = \zeta^m\alpha$ schon eindeutig bestimmt. Wie im Beweis von Satz I.5.11.1 zeigt man, dass man einen Monomorphismus

$$\begin{array}{rccc} \rho: & \mathrm{Aut}(E;K) & \longrightarrow & \mathbb{Z}_n \\ & \sigma & \longmapsto & m + n\mathbb{Z} \end{array}$$

erhält. Als Untergruppe der zyklischen Gruppe $\mathbb{Z}_n$ ist das Bild von ρ und damit $\mathrm{Aut}(E;K)$ selbst zyklisch.

(ii) Es sei σ ein erzeugendes Element von $\mathrm{Aut}(E;K)$ und $\zeta \in K$ eine primitive n-te Einheitswurzel. Nach dem Hauptsatz der Galoistheorie gilt $|\mathrm{Aut}(E;K)| = n$ und nach Satz I.5.10.3 sind die Automorphismen $1, \sigma, \ldots, \sigma^{n-1}$ linear unabhängig über K. Es gibt daher ein $x \in E$, so dass die *Lagrangesche Resolvente*

$$(\zeta, x) := x + \zeta\sigma(x) + \zeta^2\sigma^2(x) + \cdots + \zeta^{n-1}\sigma^{n-1}(x)$$

nicht verschwindet. Es folgt

$$\sigma((\zeta, x)) = \sigma(x) + \zeta\sigma^2(x) + \cdots + \zeta^{n-2}\sigma^{n-1}(x) + \zeta^{n-1}x = \zeta^{-1}(\zeta, x),$$

also

$$\sigma((\zeta, x)^n) = (\sigma((\zeta, x))^n = (\zeta, x)^n,$$

und damit $(\zeta, x)^n \in \mathrm{Fix}(E; \mathrm{Aut}(E;K)) = K$.

Setze $\alpha := (\zeta, x)$. Wir müssen noch $E = K(\alpha)$ zeigen. Wegen $\sigma^m(\alpha) = \zeta^{-m}\alpha$ für alle $m \in \mathbb{N}$ sind die Beschränkungen der Automorphismen $1, \sigma, \ldots, \sigma^{n-1}$ auf $K(\alpha)$ paarweise verschieden. Aus Lemma I.5.10.2 folgt

$$[K(\alpha) : K] \geq n.$$

Wegen $[E : K] = n$ folgt hieraus $E = K(\alpha)$. □

Definition Eine Körpererweiterung E eines Körpers K heißt *Radikalerweiterung*, wenn es eine Kette

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = E$$

von Zwischenkörpern von $K \subset E$ gibt, so dass für jedes $i = 0, \ldots, m-1$ gilt: $L_{i+1} = L_i(\alpha_i)$, wobei α_i Nullstelle eines reinen Polynoms über L_i ist.

Definition Es sei K ein Körper und $f(x) \in K[x]$. Die Gleichung $f(x) = 0$ heißt über K *durch Radikale auflösbar*, wenn es eine Radikalerweiterung E von K gibt, so dass $f(x)$ über E in Linearfaktoren zerfällt.

Eins der Hauptresultate der Galoistheorie ist der folgende Satz:

Satz 1.5.2 *Es sei K ein Körper der Charakteristik 0 und $f(x) \in K[x]$ nicht konstant. Dann ist die Gleichung $f(x) = 0$ genau dann über K durch Radikale auflösbar, wenn die Galoisgruppe von $f(x)$ über K auflösbar ist.*

Zum Beweis dieses Satzes benötigen wir noch einige Hilfssätze.

Lemma 1.5.1 *Ist K ein Körper der Charakteristik 0 und E eine Radikalerweiterung von K, so gibt es eine Körpererweiterung E' von E, so dass E' eine Radikalerweiterung und Galois-Erweiterung von K ist.*

Beweis. Wir beweisen das Lemma durch Induktion über den Grad $[E : K]$.

Induktionsanfang: Für $[E : K] = 1$ kann man $E' = E$ nehmen.

Induktionsschritt. Es sei nun $[E : K] \geq 2$. Da E eine Radikalerweiterung von K vom Grad ≥ 2 ist, gibt es einen Zwischenkörper L von $K \subset E$ mit $L \neq E$, ein $n \in \mathbb{N} \setminus \{0\}$ und ein $\alpha \in E$, so dass L eine Radikalerweiterung von K ist, $\alpha^n \in L$ ist und $E = L(\alpha)$ gilt. Wegen $[L : K] < [E : K]$ gibt es nach Induktionsannahme einen Erweiterungskörper L' von L, so dass L' eine Radikalerweiterung und eine Galois-Erweiterung von K ist. Dann ist L' Zerfällungskörper eines Polynoms $f(x) \in K[x]$. Setze $G' := \mathrm{Aut}(L'; K)$ und

$$g(x) := \prod_{\varphi \in G'} (x^n - \varphi(\alpha^n)).$$

Es sei

$$E' := \text{ Zerfällungskörper von } g(x) \in L'[x].$$

Nach Konstruktion sind die Koeffizienten von $g(x)$ invariant unter G'. Wegen $\mathrm{Fix}(L'; G') = K$ gilt also $g(x) \in K[x]$. Also ist E' Zerfällungskörper des Polynoms $f(x)g(x) \in K[x]$ und damit eine Galoiserweiterung von K. Da α eine Nullstelle von $g(x)$ ist, folgt $E = L(\alpha) \subset E'$. Da jede Nullstelle von $g(x)$ eine n-te Wurzel aus einem Element von L' ist, ist E' eine Radikalerweiterung von L' und damit auch von K, da L' eine Radikalerweiterung von K ist. □

Lemma 1.5.2 *Es sei K ein Körper der Charakteristik 0, $n \in \mathbb{N}\setminus\{0\}$, $\zeta \in \mu_n$ eine primitive n-te Einheitswurzel und E eine Galois-Erweiterung von K. Dann ist $E(\zeta)$ eine Galois-Erweiterung von K und von $K(\zeta)$.*

Beweis. Da E eine Galois-Erweiterung von K ist, ist E nach Korollar 1.1.3 Zerfällungskörper eines Polynoms $f(x) \in K[x]$. Dann ist $E(\zeta)$ Zerfällungskörper des Polynoms

$$g(x) := (x^n - 1)f(x),$$

also auch eine Galois-Erweiterung von K. Nach dem Hauptsatz der Galoistheorie ist $E(\zeta)$ dann auch eine Galois-Erweiterung von $K(\zeta)$. □

Lemma 1.5.3 *Es sei K ein Körper der Charakteristik 0, $n \in \mathbb{N} \setminus \{0\}$ und $\zeta \in \mu_n$ eine primitive n-te Einheitswurzel. Gilt $n = m\ell$ für $m, \ell \in \mathbb{N}$, so ist ζ^ℓ eine primitive m-te Einheitswurzel in μ_m.*

Beweis. Nach Voraussetzung sind die Elemente

$$1, \zeta^\ell, (\zeta^\ell)^2, \ldots, (\zeta^\ell)^{m-1}$$

paarweise verschieden. □

Beweis von Satz 1.5.2.

"⇒": Es sei $K \subset L \subset E$ eine Körperkette, wobei E eine Radikalerweiterung von K und L der Zerfällungskörper von $f(x)$ über K ist. Nach Lemma 1.5.1 können wir annehmen, dass E eine Galois-Erweiterung von K ist. Es sei nun

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = E$$

eine Kette von Zwischenkörpern von $K \subset E$, so dass für jedes $i = 0, \ldots, m-1$ gilt: $L_{i+1} = L_i(\alpha_i)$, wobei α_i Nullstelle eines reinen Polynoms vom Grad n_i über L_i ist. Wir wollen nun auf die Körpererweiterung L_{i+1} von L_i Satz 1.5.1(i) anwenden. In der Voraussetzung dieses Satzes wird aber verlangt, dass $\mu_{n_i}(L_i) \subset L_i$. Diese Voraussetzung ist aber im Allgemeinen nicht erfüllt. Deshalb machen wir die folgende Konstruktion: Es sei $n = n_0 \cdots n_{m-1}$ und ζ eine primitive n-te Einheitswurzel in μ_n. Wir setzen

$$L_i' := L_i(\zeta), \quad i = 0, \ldots, m, \quad K' = K(\zeta),\ E' = E(\zeta).$$

Damit erhalten wir eine Kette

$$K \subset K' = L_0' \subset L_1' \subset \cdots \subset L_m' = E'$$

von Zwischenkörpern von $K \subset E'$. Nach Lemma 1.5.2 ist E' eine Galois-Erweiterung von K. Auf die Körpererweiterungen L_{i+1}' von L_i' können wir nun Satz 1.5.1(i) anwenden. Nach Lemma 1.5.2 ist L_{i+1}' eine Galois-Erweiterung von L_i'. Nach dem Hauptsatz der Galoistheorie folgt dann, dass

$$\mathrm{Aut}(E'; K) \supset \mathrm{Aut}(E'; K') \supset \mathrm{Aut}(E'; L_1') \supset \cdots \supset \mathrm{Aut}(E'; L_m') = \{\mathrm{id}_{E'}\}$$

eine Kette von Normalteilern ist. Aus dem Isomorphismus

$$\mathrm{Aut}(E'; L_{i-1}')/\mathrm{Aut}(E'; L_i') \cong \mathrm{Aut}(L_i'; L_{i-1}')$$

folgt, dass diese Faktorgruppe zyklisch ist. Die Faktorgruppe

$$\mathrm{Aut}(E'; K)/\mathrm{Aut}(E'; K') \cong \mathrm{Aut}(K'; K)$$

ist abelsch, da $K' = K(\zeta)$. Also ist die Gruppe $\mathrm{Aut}(E'; K')$ auflösbar. Da L als Zerfällungskörper von $f(x)$ galoisch ist, folgt

$$\mathrm{Aut}(L; K) \cong \mathrm{Aut}(E'; K)/\mathrm{Aut}(E'; L).$$

Aus Satz 1.4.3 folgt damit, dass auch $\mathrm{Aut}(L;K)$ auflösbar ist.

"$\Leftarrow$": Es sei G die Galoisgruppe von $f(x)$ über K. Nach Satz 1.4.2 gibt es in G eine Kette

$$G = N_0 \supset N_1 \supset \cdots \supset N_m = \{e\}$$

von Normalteilern mit zyklischen Quotienten. Es sei E der Zerfällungskörper von $f(x)$ und $L_i := \mathrm{Fix}(E;N_i)$, $i = 0,\ldots,m$. Nach dem Hauptsatz der Galoistheorie ist

$$K = L_0 \subset L_1 \subset \cdots \subset L_m = E$$

eine Kette von Zwischenkörpern von $K \subset E$ mit folgenden Eigenschaften: Für jedes $i = 0,\ldots,m-1$ ist L_{i+1} eine Galois-Erweiterung von L_i und es gilt:

$$N_i/N_{i+1} \cong \mathrm{Aut}(L_{i+1};L_i).$$

Die Gruppe $\mathrm{Aut}(L_{i+1};L_i)$ ist also für jedes $i = 0,\ldots,m-1$ eine zyklische Gruppe der Ordnung n_i. Wir wollen nun Satz 1.5.1(ii) anwenden. Wieder ist die Voraussetzung $\mu_{n_i}(L_i) \subset L_i$ im Allgemeinen nicht erfüllt. Es sei $n := |G|$ und ζ eine primitive Einheitswurzel über E. Wir setzen

$$L_i' := L_i(\zeta), \quad i = 0,\ldots,m, \quad K' = K(\zeta),\ E' = E(\zeta).$$

Damit erhalten wir eine Kette

$$K \subset K' = L_0' \subset L_1' \subset \cdots \subset L_m' = E'$$

von Zwischenkörpern von $K \subset E'$. Wir zeigen, dass nun für jedes $i = 0,\ldots,m-1$ die Körpererweiterung L_{i+1}' von L_i' die Voraussetzungen von Satz 1.5.1(ii) erfüllt. Nach Lemma 1.5.2 ist L_{i+1}' eine Galois-Erweiterung von L_i' für $i = 0,\ldots,m-1$. Man hat Homomorphismen

$$\mathrm{Aut}(L_{i+1}';L_i') \hookrightarrow \mathrm{Aut}(L_{i+1}';L_i) \to \mathrm{Aut}(L_{i+1};L_i),$$

deren Hintereinanderschaltung injektiv ist, wie man leicht zeigen kann. Da $\mathrm{Aut}(L_{i+1};L_i)$ eine zyklische Gruppe der Ordnung n_i mit $n_i|n$ ist, ist auch $\mathrm{Aut}(L_{i+1}';L_i')$ eine zyklische Gruppe der Ordnung n_i' mit $n_i'|n$. Nach Lemma 1.5.3 gilt schließlich $\mu_{n_i'}(L_i') \subset L_i'$.

Aus Satz 1.5.1(ii) folgt dann, dass E' und damit auch E eine Radikalerweiterung von K ist. □

1.6 Symmetrische Funktionen

Wir wollen nun die wichtigste Anwendung von Satz 1.5.2 geben. Dazu brauchen wir noch einige Vorbereitungen.

Definition Es sei K ein Körper und $K(u_1, \ldots, u_n)$ der Körper der rationalen Funktionen in den Unbestimmten $u_1, \ldots, u_n$ über dem Körper K. Dann heißt das Polynom

$$x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n \in K(u_1, \ldots, u_n)[x]$$

das *allgemeine Polynom n-ten Grades* über K.

Das allgemeine Polynom n-ten Grades habe über dem Zerfällungskörper die Nullstellen $r_1, \ldots, r_n$, d.h. es gelte

$$x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n = (x - r_1) \cdots (x - r_n).$$

Die Vietaschen Wurzelsätze besagen nun, dass gilt:

$$\begin{aligned} u_1 &= r_1 + \cdots + r_n \\ u_2 &= r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n \\ &\vdots \quad \vdots \quad \vdots \\ u_n &= r_1 r_2 \cdots r_n \end{aligned}$$

Allgemein gilt für $\nu = 1, \ldots, n$

$$u_\nu = \sum_{1 \le i_1 < \ldots < i_\nu \le n} r_{i_1} \cdots r_{i_\nu}.$$

Definition Für $\nu = 1, \ldots, n$ heißt die Funktion

$$s_\nu(x_1, \ldots, x_n) := \sum_{1 \le i_1 < \ldots < i_\nu \le n} x_{i_1} \cdots x_{i_\nu}$$

in den Unbestimmten $x_1, \ldots, x_n$ die *ν-te elementarsymmetrische Funktion* in den Unbestimmten $x_1, \ldots, x_n$.

Nun betrachten wir eine Gleichung, deren *Wurzeln* Unbestimmte $x_1, \ldots, x_n$ sind und deren Koeffizienten daher die elementarsymmetrischen Funktionen dieser Unbestimmten sind:

$$(x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n, \quad s_\nu = s_\nu(x_1, \ldots, x_n).$$

Definition Ein Polynom (oder eine rationale Funktion) $f(x_1, \ldots, x_n)$ in den Unbestimmten $x_1, \ldots, x_n$ heißt *symmetrisch*, falls

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n) \text{ für alle } \sigma \in S_n$$

gilt.

Satz 1.6.1 (Hauptsatz über symmetrische Funktionen) *Jede symmetrische rationale Funktion (bzw. jedes symmetrische Polynom) ist eine rationale Funktion (bzw. ein Polynom) in den elementarsymmetrischen Funktionen.*

Beweis. (a) Wir beweisen zunächst die Aussage des Satzes für symmetrische rationale Funktionen. Es sei L der Körper der symmetrischen rationalen Funktionen in den Unbestimmten $x_1, \ldots, x_n$ und $L' := K(s_1, \ldots, s_n)$. Dann ist zu zeigen: $L = L'$.

Zunächst gilt

$$L = \mathrm{Fix}(K(x_1, \ldots, x_n); S_n).$$

Also ist $K(x_1, \ldots, x_n)$ eine Galois-Erweiterung von L mit Galoisgruppe S_n und es gilt nach Lemma I.5.10.4

$$[K(x_1, \ldots, x_n) : L] = |S_n| = n!.$$

Wir wollen nun den Grad der Körpererweiterung $K(x_1, \ldots, x_n)$ von L' abschätzen. Dazu betrachten wir die folgende Kette von Zwischenkörpern von $L' \subset K(x_1, \ldots, x_n)$

$$L' \subset L'(x_n) \subset L'(x_{n-1}, x_n) \subset \cdots \subset L'(x_1, \ldots, x_n) = K(x_1, \ldots, x_n)$$

und das Polynom

$$f(x) := (x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \in L'[x].$$

Dann gilt $[L'(x_n) : L'] \leq n$, da x_n Nullstelle von $f(x)$ ist. Es gibt ein Polynom $f_{n-1}(x) \in L'(x_n)[x]$ mit $f(x) = f_{n-1}(x)(x - x_n)$. Da x_{n-1} Nullstelle von $f_{n-1}(x)$ ist, folgt

$$[L'(x_{n-1}, x_n) : L'(x_n)] \leq \operatorname{grad} f_{n-1}(x) = n - 1.$$

Auf diese Weise sieht man induktiv: Zu jedem $i = 1, \ldots, n-1$ gibt es ein

$$f_i(x) \in L'(x_{i+1}, \ldots, x_n)[x] \text{ mit } f(x) = f_i(x)(x - x_{i+1}) \cdots (x - x_n).$$

Da x_i Nullstelle von $f_i(x)$ ist, erhält man

$$[L'(x_i, \ldots, x_n) : L'(x_{i+1}, \ldots, x_n)] \leq \operatorname{grad}(f_i) = i.$$

Also folgt

$$[K(x_1, \ldots, x_n) : L'] = \prod_{i=1}^{n} [L'(x_i, \ldots, x_n) : L'(x_{i+1}, \ldots, x_n)] \leq n!.$$

Wegen $L' \subset L$ folgt daraus $L = L'$.

(b) Nun beweisen wir die Aussage des Satzes für symmetrische Polynome. Ein Polynom in den Unbestimmten $x_1, \ldots, x_n$ ist ein Ausdruck

$$f(x_1, \ldots, x_n) = \sum_{\alpha_1=0}^{m_1} \cdots \sum_{\alpha_n=0}^{m_n} a_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

mit $a_{\alpha_1,\ldots,\alpha_n} \in K$ und $m_1, \ldots, m_n \in \mathbb{N}$. Einen Term $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ bezeichnen wir als *Monom* des Polynoms. Nun führen wir eine Ordnung auf den Monomen eines Polynoms ein. Wir ordnen die Monome "lexikographisch", d.h. wir definieren

$$\begin{aligned} x_1^{\alpha_1} \cdots x_n^{\alpha_n} &< x_1^{\beta_1} \cdots x_n^{\beta_n} \\ &:\Leftrightarrow \quad \exists s, 0 \leq s < n, \alpha_1 = \beta_1, \ldots, \alpha_s = \beta_s, \alpha_{s+1} < \beta_{s+1}. \end{aligned}$$

Gilt $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x_1^{\beta_1} \cdots x_n^{\beta_n}$ oder $x_1^{\alpha_1} \cdots x_n^{\alpha_n} < x_1^{\beta_1} \cdots x_n^{\beta_n}$, so schreiben wir $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\beta_1} \cdots x_n^{\beta_n}$.

Es sei nun $f(x_1, \ldots, x_n)$ ein symmetrisches Polynom und $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ das größte in $f(x_1, \ldots, x_n)$ vorkommende Monom. Da $f(x_1, \ldots, x_n)$ symmetrisch ist, kommen mit diesem Monom auch alle Monome vor, deren Exponenten durch eine Permutation von $\alpha_1, \ldots, \alpha_n$ hervorgehen. Deswegen gilt

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n.$$

Nun bilden wir ein Produkt von elementarsymmetrischen Funktionen, das ausmultipliziert und lexikographisch geordnet dasselbe größte Monom hat. Dazu überlegt man sich, dass das größte Monom in der elementarsymmetrischen Funktion s_i das Monom $x_1 \cdots x_i$ ist. Demnach ist in $s_1^{\beta_1} \cdots s_n^{\beta_n}$ das größte vorkommende Monom

$$x_1^{\beta_1+\cdots+\beta_n} x_2^{\beta_2+\cdots+\beta_n} \cdots x_n^{\beta_n}.$$

Also besitzen $f(x_1, \ldots, x_n)$ und das Produkt

$$s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$$

die gleichen größten Monome. Es sei $ax_1^{\alpha_1} \cdots x_n^{\alpha_n}$ das lexikographische Anfangsglied von $f(x_1, \ldots, x_n)$. Dann ist das größte in

$$g = f - as_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$$

vorkommende Monom kleiner als das größte in $f(x_1, \ldots, x_n)$ vorkommende Monom. Diesen Schritt wiederholen wir solange, bis wir das Nullpolynom erhalten. Auf diese Weise können wir dann $f(x_1, \ldots, x_n)$ als Linearkombination von Monomen in den elementarsymmetrischen Funktionen darstellen. □

Beispiel 1.6.1 Eine wichtige symmetrische Funktion ist

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)^2.$$

Ihr Ausdruck als Polynom in $s_1, \ldots, s_n$, $\Delta(s_1, \ldots, s_n)$, heißt die *Diskriminante* des Polynoms

$$f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

Das Verschwinden von Δ für gewisse Werte von $s_1, \ldots, s_n$ gibt an, dass $f(x)$ eine mehrfache Nullstelle hat. Zum Beispiel ist für $f(x) = x^2 + px + q$ die Diskriminante $\Delta(p, q) = p^2 - 4q$.

Satz 1.6.2 *Ist $f(x) \in K(u_1, \ldots, u_n)[x]$ das allgemeine Polynom n-ten Grades über einem Körper K, so ist seine Galoisgruppe über $K(u_1, \ldots, u_n)$ isomorph zur symmetrischen Gruppe S_n.*

Beweis. Wir betrachten zunächst das Polynom mit allgemeinen Nullstellen

$$f(x) := (x - x_1) \cdots (x - x_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n,$$

wobei $s_\nu = s_v(x_1, \ldots, x_n)$ die ν-te elementarsymmetrische Funktion ist, $\nu = 1, \ldots, n$. Es gilt $f(x) \in K(s_1, \ldots, s_n)[x]$. Dann ist der Zerfällungskörper von $f(x)$ über $K(s_1, \ldots, s_n)$ der Körper $E := K(x_1, \ldots, x_n)$. Der Beweis von Satz 1.6.1 zeigt, dass E eine Galois-Erweiterung von $K(s_1, \ldots, s_n)$ mit Galoisgruppe S_n ist.

Nun betrachten wir das allgemeine Polynom n-ten Grades

$$g(x) := x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n = (x - r_1) \cdots (x - r_n).$$

Dann ist $E' = K(r_1, \ldots, r_n)$ der Zerfällungskörper von $g(x)$ über $K(u_1, \ldots, u_n)$.

Wir konstruieren nun einen Isomorphismus

$$\varphi : K[u_1, \ldots, u_n] \to K[s_1, \ldots, s_n],$$

der einen Isomorphismus

$$\varphi' : K(u_1, \ldots, u_n) \to K(s_1, \ldots, s_n)$$

und einen Isomorphismus

$$\Phi : E' \to E$$

induziert. Dazu betrachten wir die Fortsetzung der durch $\varphi(u_i) = s_i$ für $i = 1, \ldots, n$ gegebenen Abbildung zu einem Homomorphismus

$$\varphi : K[u_1, \ldots, u_n] \to K[s_1, \ldots, s_n].$$

Dieser Homomorphismus ist offensichtlich surjektiv. Wir zeigen, dass er auch injektiv ist. Dazu betrachten wir den Homomorphismus

$$\psi' : K[x_1, \ldots, x_n] \to K[r_1, \ldots, r_n] \text{ mit } \psi'(x_i) = r_i, i = 1, \ldots, n.$$

Wegen

$$\psi'(s_i(x_1, \ldots, x_n)) = s_i(r_1, \ldots, r_n) = u_i, \quad i = 1, \ldots, n,$$

induziert ψ' einen Homomorphismus

$$\psi : K[s_1, \ldots, s_n] \to K[u_1, \ldots, u_n].$$

Offensichtlich ist $\psi \circ \varphi$ die Identität. Also ist φ ein Isomorphismus.

Der Isomorphismus φ induziert einen Isomorphismus

$$\varphi' : K(u_1, \ldots, u_n) \to K(s_1, \ldots, s_n)$$

der Quotientenkörper. Da φ' die Koeffizienten von $g(x)$ auf die Koeffizienten von $f(x)$ abbildet, lässt sich nach Satz I.5.6.2 der Isomorphismus φ' zu einem Isomorphismus

$$\Phi : E' \to E$$

der Zerfällungskörper fortsetzen. Damit gibt es ein kommutatives Diagramm

$$\begin{array}{ccc} E' = K(r_1, \ldots, r_n) & \xrightarrow{\Phi} & E = K(x_1, \ldots, x_n) \\ \cup & & \cup \\ K(u_1, \ldots, u_n) & \xrightarrow{\varphi'} & K(s_1, \ldots, s_n) \end{array}$$

Daraus folgt, dass die Abbildung

$$\mathrm{Aut}(E'; K(u_1, \ldots, u_n)) \to \mathrm{Aut}(E; K(s_1, \ldots, s_n)), \quad \sigma \mapsto \Phi \circ \sigma \circ \Phi^{-1},$$

ein Isomorphismus ist. Also ist die Galoisgruppe von $g(x)$ isomorph zu der Galoisgruppe von $f(x)$, also zu S_n. □

Aus diesem Satz, Satz 1.5.2 und Beispiel 1.4.2 folgt damit:

Korollar 1.6.1 (Abel) *Für $n \geq 5$ ist die allgemeine Gleichung n-ten Grades über einem Körper der Charakteristik 0 nicht durch Radikale auflösbar.*

1.7 Konstruierbarkeit regulärer n-Ecke

Zum Abschluss formulieren wir das Ergebnis von Gauß zur Konstruierbarkeit regulärer n-Ecke.

Satz 1.7.1 (Gauß) *Es sei $n > 2$ eine natürliche Zahl. Dann sind folgende Aussagen äquivalent:*

(i) *Das reguläre n-Eck ist mit Zirkel und Lineal konstruierbar.*

(ii) *Die Zahl $\varphi(n)$ ist eine Potenz von 2.*

(iii) *Es gibt $m, r \in \mathbb{N}$ und paarweise verschiedene Fermatsche Primzahlen $p_1, \ldots, p_r$ mit*

$$n = 2^m p_1 \cdots p_r.$$

Beweis.
(i) $\Rightarrow$ (ii): Dies ist Satz I.5.7.4.
(ii) $\Rightarrow$ (i): Es sei ζ eine primitive n-te Einheitswurzel. Aus

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = 2^m \text{ für ein } m \in \mathbb{N}$$

folgt, dass für $G := \mathrm{Aut}(\mathbb{Q}(\zeta); \mathbb{Q})$ gilt

$$|G| = 2^m.$$

Aus Satz 1.4.4 folgt, dass die Gruppe G auflösbar ist. Nach Satz 1.4.2 gibt es eine Kette von Normalteilern

$$G = N_0 \supset N_1 \supset \cdots \supset N_m = \{e\}$$

mit zyklischen Quotienten der Ordnung 2. Nach dem Hauptsatz der Galoistheorie gehört dazu eine Kette

$$\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_m = \mathbb{Q}(\zeta)$$

von Zwischenkörpern mit $[L_{i+1} : L_i] = 2$ für $i = 0, \ldots, m-1$. Aus Satz I.5.5.1 folgt, dass $\zeta \in \mathcal{K}(\{0, 1\})$. Nach I.5.5 ist demnach das reguläre n-Eck mit Zirkel und Lineal konstruierbar.

(ii) $\Leftrightarrow$ (iii): (vgl. I.5.7) Es sei

$$n = p_1^{\ell_1} \cdots p_r^{\ell_r}$$

die Primfaktorzerlegung von n. Nach Korollar I.1.4.3 gilt

$$\varphi(n) = p_1^{\ell_1 - 1} \cdots p_r^{\ell_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Also ist $\varphi(n)$ genau dann eine Potenz von 2, wenn für jedes $p_j \neq 2$ ($j = 1, \ldots, r$) gilt: $\ell_j = 1$ und $p_j - 1$ ist eine Potenz von 2. Aus Lemma I.1.3.1 folgt dann die Behauptung. $\square$

Kapitel 2

Moduln

2.1 Moduln und Modulhomomorphismen

Im Folgenden sei R immer ein Ring mit 1, der nicht notwendig kommutativ ist.

Definition Ein *R-Linksmodul* ist eine Menge $(M, +, \cdot)$ mit zwei Verknüpfungen $+ : M \times M \to M, (x, y) \mapsto x + y$, $\cdot : R \times M \to M, (a, x) \mapsto ax$, für die die folgenden Axiome erfüllt sind

(M1) $(M, +)$ ist eine abelsche Gruppe.

(M2) Für alle $a, b \in R$ und $x, y \in M$ gilt:

- (a) $a(x + y) = ax + ay$.
- (b) $(a + b)x = ax + bx$.
- (c) $a(bx) = (ab)x$.
- (d) $1x = x$.

Beispiel 2.1.1 Ist $R = K$ ein Körper, so ist ein K-Linksmodul das gleiche wie ein K-Vektorraum.

Definition Ein *R-Rechtsmodul* ist eine Menge $(M, +, \cdot)$ mit zwei Verknüpfungen $+ : M \times M \to M, (x, y) \mapsto x + y$, $\cdot : M \times R \to M, (x, a) \mapsto xa$, für die die folgenden Axiome erfüllt sind

(RM1) $(M, +)$ ist eine abelsche Gruppe.

(RM2) Für alle $a, b \in R$ und $x, y \in M$ gilt:

(a) $(x+y)a = xa + ya$.

(b) $x(a+b) = xa + xb$.

(c) $x(ab) = (xa)b$.

(d) $x1 = x$.

Definition Für jeden Ring R bezeichne R^{op} den *entgegengesetzten Ring* von R, d.h. den Ring, der als additive Gruppe gleich R ist, mit der Multiplikation $\cdot : R \times R \to R$, $(a, b) \mapsto ba$.

Bemerkung 2.1.1 Ist M ein R-Rechtsmodul, so wird M durch die skalare Multiplikation $ax := xa$ zu einem R^{op}-Linksmodul. Umgekehrt wird jeder R^{op}-Linksmodul zu einem R-Rechtsmodul durch $xa := ax$.

Vereinbarung Im Folgenden betrachten wir fast immer Linksmoduln. Wir schreiben kurz R-Modul für R-Linksmodul.

Beispiele 2.1.1 (1) $R = \mathbb{Z}$: Es sei M eine abelsche Gruppe. Dann definieren wir auf ihr eine skalare Multiplikation mit $r \in \mathbb{Z}$ wie folgt:

$$rx := \begin{cases} \underbrace{x + \cdots + x}_{r} & \text{für } r > 0, \\ 0 & \text{für } r = 0, \\ -\underbrace{(x + \cdots + x)}_{|r|} & \text{für } r < 0. \end{cases}$$

Damit wird M zu einem $\mathbb{Z}$-Modul. Man kann leicht zeigen (Übungsaufgabe!), dass dies die einzige $\mathbb{Z}$-Modulstruktur auf M ist, so dass die gegebene Addition mit der Moduladdition übereinstimmt. Auf diese Weise entsprechen sich $\mathbb{Z}$-Moduln und abelsche Gruppen.

(2) Ist $I \subset R$ ein Ideal, so ist I ein R-Modul bezüglich der Ringmultiplikation $ax := a \cdot x$ für $a \in R$ und $x \in I$. Insbesondere ist der Ring R ein R-Modul.

Definition Es seien M, N R-Moduln. Eine Abbildung $f : M \to N$ heißt *R-Modulhomomorphismus* oder *R-linear*, wenn für alle $a \in R$ und $x, y \in M$ gilt:

$$\begin{aligned} f(x+y) &= f(x) + f(y), \\ f(ax) &= af(x). \end{aligned}$$

Ein surjektiver R-Modulhomomorphismus heißt *R-Modulepimorphismus*. Ein injektiver R-Modulhomomorphismus heißt *R-Modulmonomorphismus*. Ein

bijektiver R-Modulhomomorphismus heißt *R-Modulisomorphismus*. Zwei R-Moduln M und N heißen *isomorph*, wenn es einen R-Modulisomorphismus $M \to N$ gibt.

Die Zusammensetzung von R-Modulhomomorphismen ist wieder R-linear.

Definition Für R-Moduln M, N definieren wir

$$\mathrm{Hom}_R(M,N) := \{f : M \to N \mid f \ R\text{-Modulhomomorphismus}\}.$$

Insbesondere setzen wir

$$\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M).$$

Die Elemente von $\mathrm{End}_R(M)$ nennen wir auch *Endomorphismen* von M. Schließlich setzen wir

$$M^* := \mathrm{Hom}_R(M,R).$$

Lemma 2.1.1 *Es sei R kommutativ. Mit den Verknüpfungen ($f, g \in \mathrm{Hom}_R(M,N)$, $a \in R$, $x \in M$)*

$$\begin{aligned}(f+g)(x) &:= f(x)+g(x),\\ (af)(x) &:= af(x)\end{aligned}$$

wird $\mathrm{Hom}_R(M,N)$ zu einem R-Modul.

Beweis. Übungsaufgabe. □

Definition Ist $u : M' \to M$ ein R-Modulhomomorphismus, so definieren wir

$$\begin{array}{rccc} u^t: & \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(M',N)\\ & f & \longmapsto & f\circ u \end{array}.$$

Ist $v : N \to N'$ ein R-Modulhomomorphismus, so definieren wir

$$\begin{array}{rccc} v': & \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(M,N')\\ & f & \longmapsto & v\circ f \end{array}.$$

Bemerkung 2.1.2 Betrachten wir R als Modul über sich selbst, so haben wir für jeden R-Modul M einen Isomorphismus abelscher Gruppen

$$\mathrm{Hom}_R(R,M) \to M, \quad f \mapsto f(1).$$

Ist R kommutativ, so ist dies ein Isomorphismus von R-Moduln.

2.2 Untermoduln und Faktormoduln

Definition Eine Teilmenge $N \subset M$ eines R-Moduls M heißt *Untermodul* von M, wenn gilt:

(U0) $N \neq \emptyset$.

(U1) $x, y \in N \Rightarrow x + y \in N$.

(U2) $x \in N, a \in R \Rightarrow ax \in N$.

Lemma 2.2.1 *Ein Untermodul N eines R-Moduls M ist unter der Einschränkung der Addition und skalaren Multiplikation von M auf N selbst wieder ein R-Modul. Die Inklusion von N in M ist dann ein R-Modulhomomorphismus.*

Beweis. wie in Lineare Algebra I, Übungsaufgabe. □

Ist $N \subset M$ ein Untermodul eines R-Moduls, so ist nach Algebra I die Quotientengruppe (oder Faktorgruppe)

$$M/N = \{x + N \mid x \in M\}$$

definiert. Wir definieren auf dieser Faktorgruppe eine skalare Multiplikation durch

$$a(x + N) := ax + N \quad \text{für } a \in R \text{ und } x \in M.$$

(Übungsaufgabe: Zeige, dass dies wohldefiniert ist.) Damit wird M/N zu einem R-Modul.

Definition Der R-Modul M/N heißt der *Faktormodul* (oder *Quotientenmodul*) von M nach N.

Beispiel 2.2.1 Es sei $f : M \to N$ ein R-Modulhomomorphismus. Dann ist

$$\operatorname{Ker} f := \{x \in M \mid f(x) = 0\}$$

ein Untermodul von M und

$$\operatorname{Im} f := f(M)$$

ein Untermodul von N.

Definition Es sei $f : M \to N$ ein R-Modulhomomorphismus. Der *Kokern* von F ist definiert als

$$\operatorname{Kokern} f := N/\operatorname{Im} f.$$

Satz 2.2.1 (Kern-Bild-Satz) *Es sei $f : M \to N$ ein R-Modulhomomorphismus. Dann gilt*

$$M/\mathrm{Ker}\, f \cong \mathrm{Im}\, f.$$

Beweis. Man kann leicht zeigen, dass

$$\begin{array}{rccc} \bar{f}: & M/\mathrm{Ker}\, f & \longrightarrow & \mathrm{Im}\, f \\ & x + \mathrm{Ker}\, f & \longmapsto & f(x) \end{array}$$

ein R-Modulhomomorphismus ist. □

Sind N_1, N_2 Untermoduln eines R-Moduls M, so sind

$$N_1 \cap N_2, \quad N_1 + N_2 := \{x_1 + x_2 \,|\, x_1 \in N_1, x_2 \in N_2\}$$

Untermoduln von M.

Satz 2.2.2 (Isomorphiesätze) *Es sei M ein R-Modul.*

(i) *Es seien $N \subset M \subset L$ R-Moduln. Dann gilt*

$$(L/N)/(M/N) \cong L/M.$$

(ii) *Es seien N_1, N_2 Untermoduln von M. Dann gilt*

$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

Beweis. (i) Betrachte

$$\begin{array}{rccc} \varphi: & L/N & \longrightarrow & L/M \\ & x + N & \longmapsto & x + M \end{array}.$$

Man zeigt:

(a) φ ist wohldefiniert.

(b) φ ist R-Modulhomomorphismus.

(c) φ ist surjektiv.

(d) $\mathrm{Ker}\, \varphi = M/N$.

Zu (d):

$$x + N \in \mathrm{Ker}\, \varphi \Rightarrow \varphi(x + N) = M \Rightarrow x + N \subset M.$$

(ii) Betrachte

$$\begin{array}{rccccc} \psi & : & N_2 & \to & N_1 + N_2 & \to & (N_1 + N_2)/N_1 \\ & & x_2 & \mapsto & 0 + x_2 & \mapsto & x_2 + N_1 \end{array}.$$

Man zeigt:

(a) ψ ist R-Modulhomomorphismus.

(b) ψ ist surjektiv.

(c) $\operatorname{Ker}\psi = N_1 \cap N_2$.

□

2.3 Direkte Summen und Produkte

Es sei $(M_i)_{i\in I}$ eine Familie von R-Moduln mit einer beliebigen Indexmenge I.

Definition Das *kartesische Produkt* $\prod_{i\in I} M_i$ ist die Menge aller Familien $(x_i)_{i\in I}$ mit $x_i \in M_i$.

Wir machen $\prod_{i\in I} M_i$ zu einem R-Modul, indem wir die Addition und skalare Multiplikation komponentenweise einführen:

$$\begin{aligned}(x_i)_{i\in I} + (y_i)_{i\in I} &:= (x_i + y_i)_{i\in I},\\ a(x_i)_{i\in I} &:= (ax_i)_{i\in I} \quad (a \in R).\end{aligned}$$

Definition Die Menge $\prod_{i\in I} M_i$ mit dieser R-Modulstruktur heißt das *direkte Produkt* aller M_i.

Definition In dem direkten Produkt $\prod_{i\in I} M_i$ bildet die Menge aller Familien $(x_i)_{i\in I}$ mit $x_i = 0$ für fast alle i (d.h. für alle bis auf endlich viele i) einen Untermodul, den wir die *direkte Summe* der M_i nennen und mit $\bigoplus_{i\in I} M_i$ bezeichnen.

Für das direkte Produkt $\prod_{i\in I} M_i$ nennen wir die Abbildung (für jedes $j \in I$)

$$\begin{array}{rccc} p_j: & \prod_{i\in I} M_i & \longrightarrow & M_j \\ & (x_i)_{i\in I} & \longmapsto & x_j \end{array}$$

die *Projektion* auf den Faktor M_j. Diese Projektionen sind R-Modulhomomorphismen.

Für die direkte Summe $\bigoplus_{i\in I} M_i$ nennen wir die Abbildung (für jedes $j \in I$)

$$\begin{array}{rccc} q_j: & M_j & \longrightarrow & \bigoplus_{i\in I} M_i \\ & x & \longmapsto & (x_i)_{i\in I} \text{ mit } x_j = x \text{ und } x_i = 0 \text{ für } i \neq j \end{array}$$

die *Einbettung* des Faktors M_j. Sie ist ebenfalls ein R-Modulhomomorphismus.

Ist I endlich, so gilt $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$. Ist $I = \{1, 2, \ldots, r\}$, so gilt

$$\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i =: M_1 \oplus \cdots \oplus M_r.$$

Es sei nun $(M_i)_{i\in I}$ eine Familie von Untermoduln eines R-Moduls M. Dann sind auch

$$\begin{aligned} \bigcap_{i\in I} M_i &:= \{x \in M \mid x \in M_i \text{ für alle } i \in I\} \text{ und} \\ \sum_{i\in I} M_i &:= \left\{ \sum_{i\in I} x_i \;\middle|\; x_i \in M_i, x_i = 0 \text{ für fast alle } i \in I \right\} \end{aligned}$$

Untermoduln von M. Es sei nun $\psi_i : M_i \to M$ $(i \in I)$ die Inklusion. Es gibt dann eine R-lineare Abbildung

$$\begin{array}{rccc} \psi: & \bigoplus_{i\in I} M_i & \longrightarrow & M \\ & (x_i)_{i\in I} & \longmapsto & \sum_{i\in I} x_i \end{array}.$$

Das Bild von ψ ist gerade $\sum_{i\in I} M_i$. Ist ψ injektiv, so sagen wir, dass die Summe der M_i *direkt* ist und schreiben

$$\sum_{i\in I} M_i = \bigoplus_{i\in I} M_i.$$

Ist $I = \{1, 2, \ldots, r\}$, so schreibt man in diesem Fall

$$M_1 + \cdots + M_r = M_1 \oplus \cdots \oplus M_r.$$

Wie in Lineare Algebra II zeigt man leicht:

$$M_1 + M_2 = M_1 \oplus M_2 \Leftrightarrow M_1 \cap M_2 = \{0\}.$$

Notation Es sei M ein R-Modul und I eine Indexmenge. Für die Familie $(M_i)_{i\in I}$ mit $M_i = M$ für alle i schreiben wir

$$M^I := \prod_{i\in I} M_i \quad \text{und} \quad M^{(I)} := \bigoplus_{i\in I} M_i.$$

Für $I = \{1, 2, \ldots, r\}$ schreibt man

$$M^r = M^I = M^{(I)}.$$

2.4 Erzeugendensysteme und Basen

Es sei nun wieder M ein R-Modul.

Definition Es seien $N, P \subset M$ Untermoduln. Wir definieren

$$(N : P) := \{a \in R \,|\, aP \subset N\} \subset R.$$

Dies ist ein Ideal in R (Übungsaufgabe). Die Menge

$$\mathrm{Ann}_R(M) := (0 : M) = \{a \in R \,|\, aM = 0\}$$

wird der *Annullator* von M genannt.

Lemma 2.4.1 *Es sei $I \subset \mathrm{Ann}_R(M)$ ein Ideal. Dann ist M ein R/I-Modul.*

Beweis. Für $\bar{a} \in R/I$ und $x \in M$ definieren wir $\bar{a}x := ax$. Man zeigt leicht, dass diese skalare Multiplikation wohldefiniert ist. □

Definition (a) Eine Familie $(x_i)_{i\in I}$ von Elementen in M heißt *Erzeugendensystem* von M (über R), wenn es für jedes $x \in M$ eine Familie von Elementen $(a_i)_{i\in I}$ mit $a_i = 0$ für fast alle $i \in I$ gibt, so dass

$$x = \sum_{i\in I} a_i x_i \quad \text{(endliche Linearkombination)}.$$

(b) Eine Familie $(x_i)_{i\in I}$ von Elementen in M heißt *linear unabhängig* (über R), wenn für jede Familie von Elementen $(a_i)_{i\in I}$ mit $a_i = 0$ für fast alle $i \in I$ gilt:

$$\sum_{i\in I} a_i x_i = 0 \Rightarrow a_i = 0 \text{ für alle } i \in I.$$

(c) Eine Familie $(x_i)_{i\in I}$ von Elementen in M heißt *Basis* von M (über R), wenn $(x_i)_{i\in I}$ linear unabhängig und ein Erzeugendensystem von M (über R) ist.

(d) Der R-Modul M heißt *endlich erzeugt* (über R), wenn M ein endliches Erzeugendensystem (über R) hat.

(e) Der R-Modul M heißt *frei* (über R), wenn M eine Basis (über R) besitzt.

Bemerkung 2.4.1 Aus der Linearen Algebra weiß man, dass alle (endlich dimensionalen) Vektorräume (= Moduln über einem Körper) frei sind. (Man kann zeigen, dass dies auch für unendlich dimensionale Vektorräume gilt, siehe unten.) Dies ist über beliebigen Ringen nicht der Fall: $\mathbb{Z}_n$ für $n \geq 2$ ist eine abelsche Gruppe, also ein $\mathbb{Z}$-Modul, besitzt aber keine Basis über $\mathbb{Z}$.

Zwei Basen eines endlich dimensionalen Vektorraums haben stets gleich viele Elemente. Man kann zeigen, dass dies für Basen freier Moduln über beliebigen Ringen nicht mehr gilt. Im Folgenden soll gezeigt werden, dass dies aber auch für freie Moduln über nichttrivialen kommutativen Ringen gilt.

Dazu benötigen wir das sogenannte *Lemma von Zorn*. Dies ist eine Aussage, die wir nicht beweisen können, sondern als Axiom voraussetzen müssen.

Definition Es sei X eine Menge. Eine *Halbordnung* $\leq$ ist eine Relation mit folgenden Eigenschaften (für alle $x, y, z \in X$):

(R) $x \leq x$ ($\leq$ ist *reflexiv*),

(A) $x \leq y$ und $y \leq x \Rightarrow x = y$ ($\leq$ ist *antisymmetrisch*),

(T) $x \leq y$ und $y \leq z \Rightarrow x \leq z$ ($\leq$ ist *transitiv*).

Definition Es sei X eine Menge mit einer Halbordnung $\leq$. Eine Teilmenge $Z \subset X$ heißt eine *Kette* (oder *total geordnet*), wenn für alle $x, y \in Z$ gilt: $x \leq y$ oder $y \leq x$.

Man sagt, eine Kette Z in X hat eine *obere Schranke* in X, falls es ein $s \in X$ gibt mit $z \leq s$ für alle $z \in Z$.

Ein *maximales Element* von X ist ein Element $m \in X$, so dass aus $m \leq x$ für $x \in X$ folgt, dass $x = m$ ist.

Axiom (Lemma von Zorn) *Es sei X eine nichtleere Menge mit einer Halbordnung. Hat jede Kette Z in X eine obere Schranke, so besitzt X ein maximales Element.*

Mit Hilfe des Lemmas von Zorn kann man nun beweisen:

Satz 2.4.1 *Jeder Vektorraum $V \neq \{0\}$ über einem Körper K besitzt eine Basis.*

Beweis. Es sei X die Menge aller linear unabhängigen Teilmengen von V. Die Inklusion definiert eine Halbordnung auf X. Diese Menge ist nicht leer, da V ein Element $v \neq 0$ besitzt und $\{v\}$ linear unabhängig ist. Es sei Z eine Kette

in X. Wir behaupten, dass $\bigcup_{S\in Z} S$ eine obere Schranke von Z ist. Dazu ist zu zeigen, dass

$$\bigcup_{S\in Z} S \in X.$$

Dazu sei

$$\sum_{i=1}^{n} \lambda_i x_i = 0, \quad \lambda_i \in K, \quad x_i \in \bigcup_{S\in Z} S.$$

Dann gilt $x_i \in S_i \in Z$, $i = 1, \ldots, n$. Da Z eine Kette ist, können wir o.B.d.A. annehmen, dass

$$S_i \subset S_1 \quad \text{für } i = 1, \ldots, n.$$

Also folgt

$$x_i \in S_1 \quad \text{für } i = 1, \ldots, n.$$

Da die Vektoren aus S_1 linear unabhängig sind, folgt $\lambda_i = 0$ für $i = 1, \ldots, n$. Also ist $\bigcup_{S\in Z} S$ linear unabhängig.

Nach dem Lemma von Zorn besitzt die Menge X ein maximales Element M. Da $M \in X$ ist, ist M linear unabhängig. Wir zeigen, dass M ein Erzeugendensystem von V ist. Dazu sei $v \in V$ ein beliebiger Vektor. Wir können annehmen, dass $v \notin M$. Da M maximal ist, ist die Menge $M \cup \{v\}$ linear abhängig. Also gibt es $\lambda \in K$, $\lambda_1, \ldots, \lambda_k \in K$, nicht alle gleich Null, und $x_1, \ldots, x_k \in M$ mit

$$\lambda v + \lambda_1 x_1 + \cdots + \lambda_k x_k = 0.$$

Hier ist $\lambda \neq 0$, denn aus $\lambda = 0$ würde $\lambda_i = 0$ für $i = 1, \ldots, k$ folgen. Also gilt

$$v = -\frac{1}{\lambda}(\lambda_1 x_1 + \cdots + \lambda_k x_k).$$

Also ist M ein Erzeugendensystem von V und damit eine Basis von V. □

Satz 2.4.2 *Jeder nichttriviale kommutative Ring R besitzt mindestens ein maximales Ideal.*

Beweis. Es sei X die Menge aller Ideale $I \neq R$ mit der Inklusion als Halbordnung. Diese Menge ist nicht leer, da $(0) \in X$. Es sei Z eine Kette in X. Bilde $I_0 := \bigcup_{I\in Z} I$. Wir behaupten, dass I_0 eine obere Schranke von Z ist. Dazu ist zu zeigen, dass $I_0 \in X$. Für alle $x, y \in I_0$ existiert nun ein Ideal $I \in Z$ mit $x, y \in I$. Da I ein Ideal ist, ist $x - y \in I$ und $ax \in I$ für alle $a \in R$. Also ist I_0 ein Ideal in R. Es gilt $1 \notin I_0$, da $1 \notin I$ für alle $I \in Z$. Also gilt $I_0 \in Z$. Nach dem Lemma von Zorn besitzt X ein maximales Element. Dies ist ein maximales Ideal in R. □

Es sei R wieder ein beliebiger Ring (mit 1). In Algebra I hatten wir definiert, was ein Ideal ist. Da wir auch nicht kommutative Ringe betrachten, wollen wir nun auch zwischen Linksidealen und Rechtsidealen unterscheiden.

Definition Es sei R ein Ring. Eine Teilmenge $I \subset R$ heißt *Linksideal* (bzw. *Rechtsideal*) von R, wenn gilt:

(I0) $I \neq \emptyset$.

(I1) Für alle $x, y \in I$ gilt $x - y \in I$.

(I2) Für alle $x \in I$ und $r \in R$ gilt $r \cdot x \in I$ (bzw. $x \cdot r \in I$).

Ein Ideal ist also eine Teilmenge von R, die gleichzeitig ein Links- und ein Rechtsideal ist.

Notation Ist I ein Linksideal in R und M ein R-Modul, so definieren wir

$$IM = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; n \in \mathbb{N}, a_i \in I, x_i \in M \text{ für alle } i = 1, \ldots, n \right\}.$$

Die Menge IM ist ein Untermodul von M.

Lemma 2.4.2 *Ist I ein (zweiseitiges) Ideal in R, so ist der Faktormodul M/IM ein R/I-Modul.*

Beweis. Definiere die skalare Multiplikation durch

$$(a + I)(x + IM) := ax + IM.$$

□

Lemma 2.4.3 *Es sei I ein Ideal von R und M ein R-Modul. Ist $v_1, v_2, \ldots, v_n$ eine Basis von M über R, so ist $v_1 + IM, v_2 + IM, \ldots, v_n + IM$ eine Basis von M/IM über R/I.*

Beweis. Übungsaufgabe. □

Satz 2.4.3 *Es sei R ein nichttrivialer kommutativer Ring und M ein endlich erzeugter freier R-Modul. Dann haben je zwei Basen von M über R die gleiche Anzahl von Elementen.*

Definition Unter den Voraussetzungen von Satz 2.4.3 heißt die Anzahl von Elementen einer Basis der *Rang* des freien R-Moduls.

Beweis von Satz 2.4.3. Es seien $v_1, v_2, \ldots, v_n$ und $w_1, w_2, \ldots, w_m$ zwei Basen von M. Nach Satz 2.4.2 gibt es ein maximales Ideal I in R. Nach Algebra I ist R/I ein Körper. Nach Lemma 2.4.3 sind dann sowohl $v_1 + IM, v_2 + IM, \ldots, v_n + IM$ als auch $w_1 + IM, w_2 + IM, \ldots, w_m + IM$ Basen des Vektorraums M/IM über R/I. Also gilt $n = m$. □

Wir leiten nun einen nützlichen Satz ab, der für die folgenden Betrachtungen wichtig ist. Zunächst zeigen, dass der in Lineare Algebra II betrachtete Satz von Cayley-Hamilton auch für Matrizen mit Einträgen in einem kommutativen Ring gilt.

Satz 2.4.4 (Cayley-Hamilton) *Es sei R ein kommutativer Ring, $A = (a_{ij})$ eine $n \times n$-Matrix mit Einträgen in R. Betrachte das Polynom $P_A(x) = \det(xE_n - A) \in R[x]$. Dann gilt*

$$P_A(A) = 0.$$

Beweis. Wir verwenden die gleiche Beweismethode wie in Lineare Algebra II.

Es sei $\varphi : R^n \to R^n$ der R-Modulendomorphismus des freien R-Moduls R^n, der der Matrix A entspricht, d.h.

$$\varphi\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Es sei $\mathrm{Mat}(n, n; R)$ der Ring aller $n \times n$-Matrizen über R und $R[\varphi] \subset \mathrm{Mat}(n, n; R)$ der Unterring von $\mathrm{Mat}(n, n; R)$, der durch die skalaren Vielfachen von E_n und A erzeugt wird. Wir können dann R^n auch als $R[\varphi]$-Modul betrachten, indem wir die skalare Multiplikation mit einer Matrix $B \in \mathrm{Mat}(n, n; R)$ wie oben durch die Multiplikation mit der Matrix B erklären.

Bezeichnet $e_1, \ldots, e_n$ die kanonische Basis von R^n, d.h.

$$e_1 = (1, 0, \ldots, 0, 0)^t, \ldots, e_n = (0, 0, \ldots, 0, 1)^t,$$

so erhalten wir das Gleichungssystem

$$\varphi e_i = \sum_{j=1}^{n} a_{ij} e_j, \quad i = 1, \ldots, n.$$

Dieses Gleichungssystem ist äquivalent zu

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij}) e_j = 0, \quad i = 1, \ldots, n. \tag{2.1}$$

Nun setzen wir

$$B := (\delta_{ij}\varphi - a_{ij})_{ij}.$$

Dies ist eine $n \times n$-Matrix mit Einträgen in $R[\varphi]$.

Es reicht nun zu zeigen, dass $\det B = 0$ in $R[\varphi]$. Denn da $P_A(x) = \det(xE_n - A) \in R[x]$ und der Einsetzungshomomorphismus $R[x] \to R[\varphi]$ R-linear ist (also mit den algebraischen Operationen, die notwendig sind, um die Determinante zu berechnen, kommutiert), folgt, dass

$$P_A(x) \mapsto P_A(A) = \det B.$$

Es sei B^* die adjungierte Matrix zu B. Nach Lineare Algebra I gilt

$$B^*B = \det B \cdot E_n.$$

Wenden wir nun diese Gleichung auf $e_1, \ldots, e_n$ an, so folgt aus (2.1)

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = B^*B \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} \det Be_1 \\ \vdots \\ \det Be_n \end{pmatrix}.$$

Also ist $\det B = 0$. □

Das folgende Resultat wird auf die gleiche Weise wie der Satz von Cayley-Hamilton bewiesen.

Satz 2.4.5 (Determinantentrick) *Es sei R ein kommutativer Ring, M ein endlich erzeugter R-Modul, $I \subset R$ ein Ideal, $\varphi : M \to M$ ein R-Modulendomorphismus mit $\varphi(M) \subset IM$. Dann genügt φ einer Gleichung*

$$\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 = 0$$

mit $a_i \in I$.

Beweis. Es sei $v_1, \ldots, v_n$ ein Erzeugendensystem von M. Wegen $\varphi(M) \subset IM$ gilt

$$\varphi(v_i) = \sum_{j=1}^{n} a_{ij}v_j, \quad i = 1, \ldots, n; \quad a_{ij} \in I.$$

Dieses Gleichungssystem ist äquivalent zu

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})v_j = 0, \quad i = 1, \ldots, n.$$

Setzen wir

$$B := (\delta_{ij}\varphi - a_{ij})_{ij}, \quad v := \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

so ist dieses Gleichungssystem äquivalent zu

$$Bv = 0.$$

Setze nun

$$\Delta := \det B \in I[\varphi].$$

Es sei B^* die adjungierte Matrix zu B. Nach Lineare Algebra I gilt

$$B^*B = \Delta \cdot E_n.$$

Also folgt aus $Bv = 0$

$$\Delta v = B^*Bv = 0,$$

also

$$\Delta v_i = 0 \text{ für } i = 1, \ldots, n.$$

Da $v_1, \ldots, v_n$ den R-Modul M erzeugen, folgt

$$\Delta = \det B = 0.$$

Entwicklung der Determinante Δ liefert

$$\Delta = \varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_0 = 0.$$

□

Korollar 2.4.1 *Es sei R ein kommutativer Ring, M ein endlich erzeugter R-Modul, $I \subset R$ ein Ideal mit $IM = M$. Dann existiert ein $x \in R$ mit $x \equiv 1 \bmod I$, so dass $xM = 0$.*

Beweis. Setze in Satz 2.4.5 $\varphi = \mathrm{id}$. Dann folgt aus diesem Satz, dass

$$x = 1 + a_{n-1} + \cdots + a_0$$

die gewünschten Eigenschaften hat. □

Definition Ein kommutativer Ring R heißt *lokal*, wenn R genau ein maximales Ideal $\mathfrak{m}$ enthält.

Satz 2.4.6 (Lemma von Nakayama) *Es sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Ist M ein endlich erzeugter R-Modul mit $M = \mathfrak{m}M$, so gilt $M = 0$.*

Beweis. Aus Korollar 2.4.1 folgt, dass es ein $x \in R$ mit $x \equiv 1 \bmod \mathfrak{m}$ gibt, so dass $xM = 0$. Daraus folgt, dass $x \in \mathrm{Ann}_R(M)$. Angenommen, $\mathrm{Ann}_R(M) \neq R$. Dann folgt $\mathrm{Ann}_R(M) \subset \mathfrak{m}$, also $x \in \mathfrak{m}$ und damit $1 \in \mathfrak{m}$, ein Widerspruch. Also gilt $\mathrm{Ann}_R(M) = R$, also $RM = 0$ und damit $\mathfrak{m}M = 0$. Aus der Voraussetzung $M = \mathfrak{m}M$ folgt dann aber $M = 0$. □

Korollar 2.4.2 *Es sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, M ein endlich erzeugter R-Modul, $N \subset M$ ein Untermodul. Gilt $M = N + \mathfrak{m}M$, so folgt $M = N$.*

Beweis. Wende Satz 2.4.6 auf M/N an. (Beachte $\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N$.) □

Es sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$. Dann ist $K = R/\mathfrak{m}$ ein Körper. Es sei M ein endlich erzeugter R-Modul. Dann gilt

$$\mathfrak{m} \subset \mathrm{Ann}_R(M/\mathfrak{m}M).$$

Also ist $M/\mathfrak{m}M$ ein $R/\mathfrak{m}$-Modul, d.h. ein K-Vektorraum, und nach Voraussetzung endlich dimensional.

Satz 2.4.7 *Es sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, M ein endlich erzeugter R-Modul. Sind $x_1, \ldots, x_n$ Elemente von M, deren Bilder in $M/\mathfrak{m}M$ eine Basis dieses K-Vektorraums bilden, so erzeugen $x_1, \ldots, x_n$ den R-Modul M.*

Beweis. Es sei $N \subset M$ der Untermodul, der von $x_1, \ldots, x_n$ erzeugt wird. Die Zusammensetzung der Abbildungen

$$\begin{array}{ccccc} N & \to & M & \to & M/\mathfrak{m}M \\ x_i & \mapsto & x_i & \mapsto & \overline{x}_i \end{array}$$

ist surjektiv. Daraus folgt $N + \mathfrak{m}M = M$. Aus Korollar 2.4.2 folgt $N = M$. □

2.5 Exakte Sequenzen

Wir erinnern an den Begriff exakte Sequenz, den wir schon in Lineare Algebra II eingeführt hatten, und den wir jetzt auf R-Moduln erweitern. Es sei R wieder ein beliebiger Ring.

Definition Es sei

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

eine (endliche oder unendliche) Sequenz von R-Moduln und R-linearen Abbildungen. Die Sequenz heißt *exakt*, wenn für jedes i gilt:

$$\operatorname{Ker} f_i = \operatorname{Im} f_{i-1}.$$

Unter einer *kurzen exakten Sequenz* versteht man eine exakte Sequenz der Gestalt

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0. \tag{2.2}$$

Es sei

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

eine kurze exakte Sequenz von R-Moduln. Dann gilt

$$\begin{aligned} \text{Exaktheit an der Stelle } M' &\Leftrightarrow f \text{ injektiv}, \\ \text{Exaktheit an der Stelle } M &\Leftrightarrow \operatorname{Im} f = \operatorname{Ker} g, \\ \text{Exaktheit an der Stelle } M'' &\Leftrightarrow g \text{ surjektiv}. \end{aligned}$$

Ist $f : M \to N$ ein R-Modulhomomorphismus zwischen R-Moduln M und N, so hat man immer eine kurze exakte Sequenz

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow M \xrightarrow{f} \operatorname{Im} f \longrightarrow 0,$$

wobei $\operatorname{Ker} f \longrightarrow M$ die Inklusionsabbildung ist.

Ist zum Beispiel N ein Untermodul eines R-Moduls M und bezeichnen $\iota : N \to M$ die Inklusion und $\pi : M \to M/N$ die kanonische Abbildung, so ist

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

eine kurze exakte Sequenz.

Jede kurze exakte Sequenz ist im Wesentlichen von dieser Form: Setzen wir in (2.2) $N = \operatorname{Ker} g$, so induziert g nach dem Kern-Bild-Satz einen Isomorphismus $\overline{g} : M/N \to M''$ und f ist ein Isomorphismus $M' \to N$.

Satz 2.5.1 *Es sei*

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

eine kurze exakte Sequenz von R-Moduln. Dann sind äquivalent:

(i) *Es gibt einen Untermodul $N \subset M$ mit $M = \operatorname{Ker} g \oplus N$.*

(ii) *Es gibt eine R-lineare Abbildung $s : M'' \to M$ mit $g \circ s = \mathrm{Id}_{M''}$.*

(iii) *Es gibt eine R-lineare Abbildung $t : M \to M'$ mit $t \circ f = \mathrm{Id}_{M'}$.*

Definition Wenn eine der äquivalenten Bedingungen von Satz 2.5.1 erfüllt ist, so sagt man, dass die kurze exakte Sequenz

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

spaltet.

Beweis von Satz 2.5.1. (i) $\Leftrightarrow$ (ii): Es sei N ein Untermodul mit $M = \operatorname{Ker} g \oplus N$. Dann ist $g|_N : N \to M''$ ein Isomorphismus und $s := \iota \circ (g|_N)^{-1} : M'' \to M$ ($\iota : N \to M$ die Inklusion) erfüllt die Bedingung von (ii). Es sei umgekehrt $s : M'' \to M$ eine R-lineare Abbildung mit $g \circ s = \mathrm{Id}_{M''}$. Setze $N := s(M'')$. Wir behaupten, dass $M = \operatorname{Ker} g \oplus N$ gilt. Dazu sei $x \in M$. Wir schreiben

$$x = x - s(g(x)) + s(g(x)).$$

Dann ist $s(g(x)) \in N$ und $x - s(g(x)) \in \operatorname{Ker} g$, da

$$g(x - s(g(x))) = g(x) - (g \circ s)(g(x)) = g(x) - g(x) = 0.$$

Es sei nun $x \in \operatorname{Ker} g \cap N$. Dann ist $x = s(y)$ für ein $y \in M''$. Wegen $g(s(y)) = y$ ist $s(y) \in \operatorname{Ker} g$ genau dann, wenn $y = 0$ gilt. Also folgt $\operatorname{Ker} g \cap N = \{0\}$.

(i) $\Leftrightarrow$ (iii): Es sei N ein Untermodul mit $M = \operatorname{Ker} g \oplus N$. Wegen $\operatorname{Ker} g = f(M')$ gilt dann auch $M = f(M') \oplus N$. Es sei $p : M \to f(M')$ die Projektion auf den ersten Summanden und $h : f(M') \to M$ die Umkehrabbildung von $f : M' \xrightarrow{\sim} f(M')$. Dann erfüllt $t := h \circ p : M \to M'$ die Bedingung von (iii). Es sei umgekehrt $t : M \to M'$ eine R-lineare Abbildung mit $t \circ f = \mathrm{Id}_{M'}$. Setze $N := \operatorname{Ker} t$. Wir behaupten, dass $M = f(M') \oplus N$ gilt. Dazu sei $x \in M$. Wir schreiben

$$x = f(t(x)) + x - f(t(x)).$$

Dann ist $f(t(x)) \in f(M')$ und $x - f(t(x)) \in N$, da

$$t(x - f(t(x))) = t(x) - (t \circ f)(t(x)) = t(x) - t(x) = 0.$$

Außerdem gilt für alle $y \in M'$, dass $t(f(y)) = y$ ist. Also ist $f(y) \in \operatorname{Ker} t$ genau dann, wenn $y = 0$ ist. Also folgt $f(M') \cap \operatorname{Ker} t = \{0\}$. □

Satz 2.5.2 *Es sei*

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

eine kurze exakte Sequenz von R-Moduln. Ist M'' ein freier Modul, so spaltet diese Sequenz und es ist $M \cong M' \oplus M''$.

Beweis. Es sei $(v_i)_{i\in I}$ eine Basis von M'' über R. Da g surjektiv ist, gibt es für alle $i \in I$ ein $x_i \in M$ mit $g(x_i) = v_i$. Es gibt genau eine R-lineare Abbildung $s : M'' \to M$ mit der Eigenschaft, dass $s(v_i) = x_i$ für alle $i \in I$. Diese Abbildung erfüllt $g \circ s = \mathrm{Id}_{M''}$ nach Konstruktion. Also spaltet die Sequenz. Nach Satz 2.5.1 folgt $M = \operatorname{Ker} g \oplus s(M'') \cong M' \oplus M''$. □

Korollar 2.5.1 *Es sei*

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

eine kurze exakte Sequenz von R-Moduln. Sind M' und M'' frei, so auch M.

Beweis. Nach Satz 2.5.2 ist dann M eine direkte Summe von zwei freien Moduln und damit auch frei. □

Eine direkte Folgerung ist:

Korollar 2.5.2 *Es sei R ein kommutativer Ring und*

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

eine kurze exakte Sequenz von R-Moduln. Sind M' und M'' endlich erzeugt und frei, so ist auch M endlich erzeugt und frei und es gilt

$$\operatorname{Rang} M = \operatorname{Rang} M' + \operatorname{Rang} M''.$$

Satz 2.5.3 *Es sei*

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

eine kurze exakte Sequenz von R-Moduln.

(i) *Ist M endlich erzeugt, so auch M''.*

(ii) *Sind M' und M'' endlich erzeugt, so auch M.*

Beweis. (i) Ist $v_1, \ldots, v_n$ ein Erzeugendensystem von M, so ist $g(v_1), \ldots, g(v_n)$ ein Erzeugendensystem von M'' (Beweis: Übungsaufgabe).

(ii) Ist $u_1, \ldots, u_r$ ein Erzeugendensystem von M' und $v_1, \ldots, v_s$ ein Erzeugendensystem von M'', so wähle $w_i \in M$ mit $g(w_i) = v_i$ $(i = 1, \ldots, s)$. Dann ist $f(u_1), \ldots, f(u_r), w_1, \ldots, w_s$ ein Erzeugendensystem von M (Beweis: Übungsaufgabe). □

Korollar 2.5.3 *Der R-Modul M sei die direkte Summe endlich vieler Untermoduln, $M = \bigoplus_{i=1}^{r} M_i$. Dann ist M genau dann endlich erzeugt, wenn alle M_i endlich erzeugt sind.*

Beweis. Dies folgt aus Satz 2.5.3 durch Induktion über r: Setze

$$M' := \bigoplus_{i=1}^{r-1} M_i.$$

Dann erhält man eine kurze exakte Sequenz

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M_r \longrightarrow 0.$$

□

2.6 Noethersche Moduln und Ringe

Satz 2.6.1 *Es sei M ein R-Modul. Dann sind die folgenden Aussagen äquivalent:*

(i) *Jeder Untermodul von M ist endlich erzeugt.*

(ii) *Jede aufsteigende Kette von Untermoduln von M*

$$M_1 \subset M_2 \subset M_3 \subset \ldots$$

wird stationär, d.h. es gibt ein $n \in \mathbb{N}$ mit $M_j = M_n$ für alle $j \geq n$. (Man sagt, M erfüllt die aufsteigende Kettenbedingung.*)*

(iii) *Jede nicht leere Menge Σ von Untermoduln von M hat ein maximales Element (d.h. es gibt einen Untermodul $M_0 \in \Sigma$, so dass für jedes Element N von Σ mit $M_0 \subset N$ gilt: $M_0 = N$.)*

Definition Ein R-Modul M, für den eine dieser Eigenschaften erfüllt ist, heißt *noethersch.*

Beweis von Satz 2.6.1. "(i) ⇒ (ii)": Es sei

$$M_1 \subset M_2 \subset \ldots$$

eine aufsteigende Kette von Untermoduln vom M. Setze

$$N := \bigcup_{j=1}^{\infty} M_j.$$

Nach Voraussetzung ist N endlich erzeugt. Es sei $x_1, \ldots, x_r$ ein Erzeugendensystem von N. Es sei

$$x_i \in M_{n_i},\ i = 1, \ldots, r, \quad n := \max_{i=1,\ldots,r} n_i.$$

Dann gilt

$$x_1, \ldots, x_n \in M_n \subset N.$$

Also folgt

$$M_n = M_{n+1} = \cdots = N.$$

"(ii) $\Rightarrow$ (iii)": Es sei N_0 ein Element aus Σ.

$$\begin{array}{rcl} N_0 \text{ nicht maximal} & \Rightarrow & N_0 \subsetneq N_1 \in \Sigma \\ N_1 \text{ nicht maximal} & \Rightarrow & N_1 \subsetneq N_2 \in \Sigma \\ \vdots & \vdots & \vdots \end{array}$$

Auf diese Weise könnten wir eine unendliche nicht stationäre Kette von Untermoduln von M erzeugen.

"(iii) $\Rightarrow$ (i)": Es sei N ein Untermodul von M und Σ die Menge aller endlich erzeugten Untermoduln von N. Die Menge Σ ist nicht leer, da der triviale Modul 0 in Σ liegt. Nach Voraussetzung hat Σ ein maximales Element N_0. Wir behaupten, dass $N_0 = N$ gilt. Angenommen, es gelte $N_0 \neq N$. Dann gibt es ein $x \in N$ mit $x \notin N_0$. Dann folgt

$$N_0 \subsetneq N_0 + Rx.$$

Aber $N_0 + Rx$ ist endlich erzeugt. Dies ist ein Widerspruch zur Maximalität von N_0. Also gilt $N = N_0$ und damit ist N endlich erzeugt. □

Beispiele 2.6.1 (1) Nach Lemma I.3.8.2 ist jeder Hauptidealring noethersch.

(2) Es sei

$$C[0,1] := \{f : [0,1] \to \mathbb{R} \mid f \text{ stetig}\}$$

der Ring aller reellwertigen stetigen Funktionen auf dem Intervall $[0,1]$. Es sei

$$A_0 \supset A_1 \supset \ldots$$

eine Intervallschachtelung des Intervalls $[0,1]$ mit

$$\bigcap_{i=0}^{\infty} A_i = \{\text{Pkt.}\}.$$

Zu einem Intervall A_j definieren wir das Ideal

$$I_j := \{f \in C[0,1] \mid f(A_j) = 0\} \subset C[0,1].$$

Dann ist

$$I_0 \subset I_1 \subset \ldots$$

eine Kette von Idealen von $C[0,1]$, die nicht stationär wird. Also ist der Ring $C[0,1]$ nicht noethersch.

Satz 2.6.2 *Es sei M ein noetherscher R-Modul. Dann ist jeder Untermodul und jeder Quotientenmodul von M noethersch.*

Beweis. Dass jeder Untermodul von M noethersch ist, folgt aus Satz 2.6.1(i).

Es sei $N \subset M$ ein Untermodul und $\pi : M \to M/N$ der kanonische Epimorphismus. Es sei

$$\overline{M}_0 \subset \overline{M}_1 \subset \dots$$

eine aufsteigende Kette von Untermoduln von M/N. Setze

$$M_i := \pi^{-1}(\overline{M}_i), \quad i = 0, 1, \dots.$$

Dann ist

$$M_0 \subset M_1 \subset \dots$$

eine aufsteigende Kette von Untermoduln von M. Nach Voraussetzung wird diese Kette bei M_n stationär, d.h. es gilt

$$M_j = M_n \text{ für } j \geq n.$$

Aus $\pi(M_i) = \overline{M}_i$ folgt die Behauptung. □

Satz 2.6.3 *Es sei*

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

eine kurze exakte Sequenz von R-Moduln. Dann ist M genau dann noethersch, wenn M' und M'' noethersch sind.

Beweis. "⇒": Es sei N' ein Untermodul von M'. Dann ist $N' \cong f(N') \subset M$ und damit ist N endlich erzeugt. Daher ist M' noethersch. Es sei N'' ein Untermodul von M'' und $N := g^{-1}(N'')$. Dann ist mit N auch N'' endlich erzeugt. Also ist M'' noethersch.

"⇐": Es sei N ein Untermodul von M. Dann haben wir eine kurze exakte Sequenz

$$0 \longrightarrow f^{-1}(N) \longrightarrow N \longrightarrow g(N) \longrightarrow 0,$$

in der die Abbildungen die Einschränkungen von f und g auf die jeweiligen Untermoduln sind. Sind nun M' und M'' noethersch, so sind $f^{-1}(N)$ und $g(N)$ endlich erzeugt. Aus Satz 2.5.3(ii) folgt dann, dass auch N endlich erzeugt ist. Damit ist M noethersch. □

Korollar 2.6.1 *Es sei M ein R-Modul und $N \subset M$ ein Untermodul. Falls N und M/N noethersch sind, so ist auch M noethersch.*

Beweis. Wende Satz 2.6.3 auf die kurze exakte Sequenz

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

an. □

Korollar 2.6.2 *Der R-Modul M sei die direkte Summe endlich vieler Untermoduln, $M = \bigoplus_{i=1}^{r} M_i$. Dann ist M genau dann noethersch, wenn alle M_i noethersch sind.*

Beweis. Vergleiche den Beweis von Korollar 2.5.3. □

Definition Ein Ring R heißt *linksnoethersch*, wenn er als Linksmodul über sich selbst noethersch ist. Ein Ring R heißt *rechtsnoethersch*, wenn er als Rechtsmodul über sich selbst noethersch ist. (Das ist äquivalent dazu, dass R^{op} linksnoethersch ist.) Ein Ring heißt *noethersch*, wenn er sowohl limks- als auch rechtsnoethersch ist.

Bemerkung 2.6.1 Für kommutative Ringe fallen alle drei Begriffe zusammen und wir erhalten die Definition aus Lemma I.3.8.2.

Satz 2.6.4 *Es sei R ein linksnoetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist M noethersch.*

Beweis. Es seien $x_1, \ldots, x_n$ Erzeugende von M. Wir betrachten den R-Modulhomomorphismus

$$\begin{array}{rccl} \varphi: & \underbrace{R \oplus \cdots \oplus R}_{n} & \longrightarrow & M \\ & (a_1, \ldots, a_n) & \longmapsto & a_1 x_1 + \cdots + a_n x_n \end{array}.$$

Da $\{x_1, \ldots, x_n\}$ ein Erzeugendensystem von M ist, ist φ surjektiv. Nach dem Kern-Bild-Satz gilt

$$(R \oplus \cdots \oplus R)/\operatorname{Ker}\varphi \cong M.$$

Damit folgt die Behauptung aus Korollar 2.6.2 und Satz 2.6.2. □

Satz 2.6.5 *Es sei R ein linksnoetherscher Ring und I ein Ideal in R. Dann ist auch R/I linksnoethersch.*

Beweis. Die R/I-Untermoduln des R/I-Moduls R/I sind auch die R-Untermoduln von R/I, aufgefasst als R-Modul. Ein solcher Untermodul ist genau dann endlich erzeugt über R/I, wenn er endlich erzeugt über R ist. Aus Satz 2.6.4 folgt, dass R/I ein noetherscher R-Modul ist. Also ist R/I linksnoethersch. □

Lemma 2.6.1 *Es seien M und N R-Moduln. Gilt $M \cong M \oplus N$ und $N \neq 0$, so ist M nicht noethersch.*

Beweis. Wir betrachten die Menge Σ aller Untermoduln $N' \subset M$, für die es einen Untermodul $M' \subset M$ gibt, so dass $M = M' \oplus N'$ und $M \cong M'$. Diese Menge ist nicht leer, da sie $N' = 0$ enthält.

Angenommen, Σ besitzt ein maximales Element N'. Dann gibt es $M' \subset M$ mit $M = M' \oplus N'$ und $M' \cong M$. Nach Voraussetzung ist $M \cong M \oplus N$. Also gibt es einen Isomorphismus

$$\varphi : M \oplus N \xrightarrow{\sim} M' \text{ und es gilt } M' = \varphi(M) \oplus \varphi(N).$$

Also folgt

$$M = \underbrace{\varphi(M)}_{=:M''} \oplus \underbrace{\varphi(N) \oplus N'}_{=:N''}.$$

Da φ injektiv ist, gilt $M'' \cong M$ und $\varphi(N) \neq 0$, also $N'' \in \Sigma$ und $N' \subsetneq N''$. Dies ist ein Widerspruch zur Maximalität von N'. Also enthält Σ kein maximales Element und M ist daher nicht noethersch. □

Satz 2.6.6 *Es sei $R \neq 0$ ein linksnoetherscher Ring. Sind $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ Basen eines R-Moduls M, so gilt $n = m$.*

Beweis. O.B.d.A. $n \geq m$. Da $v_1, \ldots, v_n$ eine Basis von M ist, folgt $M \cong R^n$, und da $w_1, \ldots, w_m$ eine Basis von M ist, folgt $M \cong R^m$. Also folgt

$$R^m \cong R^n \cong R^m \oplus R^{n-m}.$$

Da R^m ein noetherscher Modul ist, folgt aus Lemma 2.6.1, dass $R^{n-m} = 0$, also $n = m$, da $R \neq 0$. □

Es sei nun R ein kommutativer Ring.

Theorem 2.6.1 (Hilbertscher Basissatz) *Wenn der kommutative Ring R noethersch ist, so ist auch der Polynomring $R[x]$ noethersch.*

Beweis. Es sei $\mathfrak{a} \subset R[x]$ ein Ideal. Es ist zu zeigen, dass $\mathfrak{a}$ endlich erzeugt ist. Dazu betrachten wir die Menge I aller Leitkoeffizienten von Polynomen in $\mathfrak{a}$. Dann ist I ein Ideal in R. Da R noethersch ist, ist I endlich erzeugt. Es sei $a_1, \ldots, a_n$ ein Erzeugendensystem von I. Es sei $f_i(x) \in \mathfrak{a}$ ein Polynom mit Leitkoeffizient a_i, d.h.

$$f_i(x) = a_i x^{r_i} + \text{ Terme vom Grad } < r_i, \quad i = 1, \ldots, n.$$

Es sei $\mathfrak{a}' \subset \mathfrak{a}$ das von $f_1(x), \ldots, f_n(x)$ erzeugte Ideal in $R[x]$, $r := \max\{r_i \mid i = 1, \ldots, n\}$. Es sei

$$f(x) = ax^m + \text{ Terme niedrigeren Grades} \in \mathfrak{a}.$$

Dann ist $a \in I$, also $a = \sum_{i=1}^n u_i a_i$, $u_i \in R$. Angenommen, $m \geq r$. Dann folgt

$$f(x) - \sum_{i=1}^n u_i f_i(x) x^{m-r_i} \in \mathfrak{a}, \quad \operatorname{grad}\left(f(x) - \sum_{i=1}^n u_i f_i(x) x^{m-r_i}\right) < m.$$

Durch Iteration dieses Schrittes folgt, dass es ein $h(x) \in \mathfrak{a}'$ gibt mit

$$f(x) - h(x) = g(x) \in \mathfrak{a}, \quad \operatorname{grad} g(x) < r.$$

(Wenn $m < r$ gilt, setze $h(x) = 0$.) Es sei M der von den Polynomen $1, x, \ldots, x^{r-1}$ erzeugte R-Modul. Wir haben gezeigt:

$$\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'.$$

Nun ist M ein endlich erzeugter R-Modul. Aus Satz 2.6.4 folgt, dass M noethersch ist. Aus Satz 2.6.2 folgt, dass $\mathfrak{a} \cap M$ als R-Modul noethersch ist. Also ist $\mathfrak{a} \cap M$ als R-Modul endlich erzeugt. Es sei $g_1(x), \ldots, g_m(x) \in \mathfrak{a}$ ein Erzeugendensystem von $\mathfrak{a} \cap M$. Also ist

$$g_1(x), \ldots, g_m(x), f_1(x), \ldots, f_n(x)$$

ein Erzeugendensystem von $\mathfrak{a}$. Also ist $\mathfrak{a}$ endlich erzeugt. □

Korollar 2.6.3 *Wenn der kommutative Ring R noethersch ist, so ist auch $R[x_1, \ldots, x_n]$ noethersch.*

Beweis. Dies folgt durch Induktion nach n aus Theorem 2.6.1. □

2.7 Unzerlegbare Moduln

Definition Ein R-Modul M heißt *unzerlegbar*, wenn $M \neq 0$ und wenn für alle Untermoduln M_1, M_2 von M mit $M = M_1 \oplus M_2$ gilt, dass $M_1 = 0$ oder $M_2 = 0$.

Beispiele 2.7.1 (1) Ist K ein Körper, so ist ein K-Vektorraum genau dann unzerlegbar, wenn er die Dimension 1 hat.

(2) Es sei R ein Integritätsbereich. Dann ist jedes nicht triviale Ideal $I \subset R$ unzerlegbar als R-Modul: Angenommen, $I = I_1 \oplus I_2$ für zwei Ideale $I_1, I_2 \neq 0$. Wähle $a_1 \in I_1$, $a_1 \neq 0$, und $a_2 \in I_2$, $a_2 \neq 0$. Dann folgt

$$0 \neq a_1 a_2 \in I_1 \cap I_2 = 0,$$

ein Widerspruch.

(3) Es $R := \mathrm{Mat}(2, 2; K)$ der Ring der 2×2-Matrizen über einem Körper K. Dann ist R als Modul über sich selbst zerlegbar: Es gilt $R = M_1 \oplus M_2$ mit

$$M_1 := \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \,\middle|\, a, c \in K \right\}, \quad M_2 := \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \,\middle|\, b, d \in K \right\}.$$

Definition Ein Element $e \in R$ heißt *idempotent*, wenn $e^2 = e$ gilt.

Bemerkung 2.7.1 Es sei $e \in R$ ein idempotentes Element. Dann gilt

$$e(1-e) = e - e^2 = e - e = 0 \text{ und entsprechend } (1-e)e = 0.$$

Wegen $(1-e)^2 = 1 - e$ ist mit e auch $1 - e$ idempotent.

Lemma 2.7.1 *Es sei M ein R-Modul und $e \in \mathrm{End}_R(M)$ ein idempotentes Element. Dann sind $e(M)$ und $(1-e)(M)$ Untermoduln von M und es gilt*

$$M = e(M) \oplus (1-e)(M).$$

Beweis. Dass $e(M)$ und $(1-e)(M)$ Untermoduln von M sind, ist klar.

Für $x \in M$ gilt $x = e(x) + (1-e)(x)$. Also gilt $M \subset e(M) + (1-e)(M)$. Es sei $x \in e(M) \cap (1-e)(M)$. Dann gibt es $y, z \in M$ mit $x = e(y) = (1-e)(z)$. Dann folgt

$$e(x) = e^2(y) = e(y) = x \text{ und } e(x) = e(1-e)(z) = 0.$$

Also folgt $x = 0$. □

Lemma 2.7.2 *Ein R-Modul $M \neq 0$ ist genau dann unzerlegbar, wenn 0 und 1 die einzigen idempotenten Elemente in $\mathrm{End}_R(M)$ sind.*

Beweis. "⇒": Nach Lemma 2.7.1 liefert jedes idempotente Element in $\mathrm{End}_R(M)$ eine Zerlegung

$$M = e(M) \oplus (1-e)(M).$$

Ist $e \neq 0, 1$ so sind beide Summanden vom Nullmodul verschieden, da $M \neq 0$. Also ist M zerlegbar.

"$\Leftarrow$": Angenommen, $M = M_1 \oplus M_2$ mit Untermoduln M_1, M_2 von M. Betrachte die Projektion $p_1 : M \to M_1$ und die Inklusion $q_1 : M_1 \to M$. Dies sind Homomorphismen von R-Moduln. Setze

$$e := q_1 \circ p_1 \in \mathrm{End}_R(M).$$

Dann gilt

$$e^2(x_1 + x_2) = e(x_1) = x_1 = e(x_1 + x_2) \text{ für alle } x_i \in M_i, i = 1, 2.$$

Also ist e idempotent und $M_1 = e(M)$, $M_2 = (1 - e)(M)$. □

Ein endlich dimensionaler Vektorraum über einem Körper K ist die direkte Summe von eindimensionalen Vektorräumen, also von unzerlegbaren K-Moduln. Allgemeiner gilt:

Satz 2.7.1 *Es sei M ein noetherscher R-Modul. Dann gibt es unzerlegbare Untermoduln $M_1, \ldots, M_r$ von M, so dass*

$$M = M_1 \oplus \cdots \oplus M_r.$$

Beweis. Der Satz gilt auch für $M = 0$, weil man die leere Summe ($r = 0$) als den Nullmodul interpretiert.

Nun sei $M \neq 0$. Es sei Σ die Menge aller Untermoduln von M, die *nicht* endliche direkte Summe von unzerlegbaren Untermoduln sind. Wir müssen zeigen, dass $\Sigma = \emptyset$. Angenommen, die Menge Σ ist nicht leer und $M \in \Sigma$.

Es sei nun $\mathcal{X}$ die Menge aller Untermoduln $N \subset M$, $N \neq M$, so dass ein $M' \in \Sigma$ existiert mit $M = N \oplus M'$. Nach der Annahme $M \in \Sigma$ ist diese Menge nicht leer, denn $0 \in \mathcal{X}$ ($M = 0 \oplus M$).

Da M noethersch ist, gibt es ein maximales Element $N \in \mathcal{X}$. Dann existiert $M' \in \Sigma$ mit $M = N + M'$. Wegen $N \neq M$ ist $M' \neq 0$. Dann ist M' zerlegbar, da es sonst eine Summe mit einem unzerlegbaren Summanden wäre. Also gilt $M' = M_1 \oplus M_2$ mit $M_1 \neq 0$, $M_2 \neq 0$. Dann gilt $M_1 \in \Sigma$ oder $M_2 \in \Sigma$, denn andernfalls wären M_1 und M_2 endliche direkte Summen unzerlegbarer Untermoduln und damit auch $M' = M_1 \oplus M_2$. O.B.d.A. $M_2 \in \Sigma$. Also gilt

$$M = \underbrace{N \oplus M_1}_{=:N'} \oplus M_2 = N' \oplus M_2, \quad M_2 \in \Sigma.$$

Da $M_2 \neq 0$, gilt $N' \neq M$. Also gilt $N' \in \mathcal{X}$. Wegen $M_1 \neq 0$ gilt $N \subsetneq N'$. Dies ist aber ein Widerspruch zur Maximalität von N. Also ist die Menge Σ leer. □

2.8 Moduln über Hauptidealringen

Wir setzen in diesem Abschnitt voraus, dass R ein nullteilerfreier Hauptidealring ist. Das bedeutet insbesondere, dass R kommutativ und noethersch ist. Außerdem ist R ein Integritätsbereich und damit nach Definition nichttrivial, also $R \neq 0$.

Es sei M ein endlich erzeugter freier R-Modul. Dann haben nach Satz 2.4.3 je zwei Basen von M über R die gleiche Anzahl von Elementen und diese Anzahl heißt der Rang von M.

Satz 2.8.1 *Ist M ein freier R-Modul vom Rang $n \in \mathbb{N}$, so ist jeder Untermodul N von M frei vom Rang $\leq n$.*

Beweis. Für $N = 0$ ist die Aussage trivial. Sei also $N \neq 0$. Es sei $(v_1, \ldots, v_n)$ eine Basis von M. Es sei

$$N_r := N \cap (Rv_1 + \cdots + Rv_r), \quad r = 1, \ldots n.$$

Wir zeigen durch Induktion nach r:

Behauptung N_r ist frei vom Rang $\leq r$.

Induktionsanfang $r = 1$: $N_1 = N \cap Rv_1$ ist ein Untermodul von Rv_1, also vom Typ Ra_1v_1 für ein $a_1 \in R$. Also ist N_1 entweder trivial oder frei vom Rang 1.

Induktionsschritt $r \to r + 1$: Angenommen, N_r ist frei vom Rang $\leq r$. Es sei I die Menge aller Elemente $a \in R$ mit der Eigenschaft, dass ein Element $x \in N$ existiert mit

$$x = b_1v_1 + \cdots + b_rv_r + av_{r+1}, \quad b_i \in R.$$

Dann ist I offensichtlich ein Ideal von R, also ein Hauptideal und wird von einem Element $a_{r+1} \in R$ erzeugt. Ist $a_{r+1} = 0$, so gilt $N_{r+1} = N_r$ und die Behauptung ist bewiesen. Ist $a_{r+1} \neq 0$, so sei $w \in N_{r+1}$ ein Element, dessen Koeffizient bezüglich v_{r+1} gerade a_{r+1} ist. Ist nun $x \in N_{r+1}$ beliebig, so ist der Koeffizient von x bezüglich v_{r+1} durch a_{r+1} teilbar. Also existiert ein $c \in R$ mit

$$x - cw \in N_r.$$

Also gilt

$$N_{r+1} = N_r + Rw.$$

Andererseits gilt offensichtlich $N_r \cap Rw = \{0\}$. Also folgt

$$N_{r+1} = N_r \oplus Rw,$$

und damit unsere Behauptung.

Die Aussage des Satzes folgt nun daraus, dass $N = N_r$ für ein r mit $1 \leq r \leq n$. □

Satz 2.8.2 (Elementarteilersatz) *Es sei M ein freier R-Modul vom Rang n und N ein Untermodul von M. Dann gibt es eine Basis $v_1, \ldots, v_n$ von M über R und $a_1, \ldots, a_n \in R$ mit*

$$N = Ra_1v_1 + \cdots + Ra_nv_n \text{ und } a_i | a_{i+1} \text{ für } i = 1, \ldots, n-1.$$

Beweis. Ist $N = 0$, so können wir eine beliebige Basis von M wählen und die Behauptung gilt mit $a_i = 0$ für alle $i = 1, \ldots, n$. Wir nehmen daher $N \neq 0$ an.

(a) Wir geben zunächst einen Beweis in dem Fall, dass R ein euklidischer Ring ist. Es sei $d : R \setminus \{0\} \to \mathbb{N}$ die Abbildung, für die gilt: Für alle $a, b \in R$ mit $b \neq 0$ gibt es Elemente $q, r \in R$ mit $a = qb + r$, wobei entweder $r = 0$ oder $d(r) < d(b)$.

Es sei $(u_1, \ldots, u_n)$ eine Basis von M und $(w_1, \ldots, w_m)$ eine Basis von N. Dann gilt

$$w_i = \sum_{j=1}^{n} a_{ij}u_j, \quad a_{ij} \in R, \quad i = 1, \ldots, m.$$

Es sei A die $m \times n$-Matrix $A = (a_{ij})$. Dann gilt

$$\begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = A \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

Wir wollen nun zeigen, dass wir durch elementare Zeilen- und Spaltentransformationen die Matrix auf die Form

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a_m & 0 & \cdots & 0 \end{pmatrix}$$

bringen können. Den elementaren Zeilen- und Spaltentransformationen entsprechen Transformationen der Basen $(u_1, \ldots, u_n)$ und $(w_1, \ldots, w_m)$. Dabei nehmen wir die folgenden elementaren Transformationen vor:

1. Vertauschungen zweier Zeilen oder Spalten von A.

2. Subtraktion der mit $\lambda \in R$ multiplizierten i-ten Zeile von der j-ten Zeile ($i \neq j$).

3. Subtraktion der mit $\lambda \in R$ multiplizierten i-ten Spalte von der j-ten Spalte ($i \neq j$).

Wegen $N \neq 0$ ist $A \neq 0$. Es sei a_{ij} der von Null verschiedene Eintrag, für den $d(a_{ij})$ minimal ist. Durch Zeilen- und Spaltenvertauschungen können wir annehmen, dass a_{11} dieser Eintrag ist. Es sei nun a_{i1} ein von Null verschiedener Eintrag, $i \neq 1$. Dann liefert Division mit Rest

$$a_{i1} = qa_{11} + r \text{ mit } r = 0 \text{ oder } d(r) < d(a_{11}).$$

Nun subtrahieren wir das q-fache der 1. Zeile von der i-ten Zeile. Damit haben wir a_{i1} durch r ersetzt. Gilt $r \neq 0$, also $d(r) < d(a_{11})$, so vertauschen wir die i-te Zeile und die erste Zeile, so dass r das neue Element a_{11} wird. Auf diese Weise können wir erreichen, dass alle Elemente in der ersten Spalte mit Ausnahme des Eintrags in der ersten Zeile zu Null werden. Entsprechend können wir alle Einträge in der ersten Zeile mit Ausnahme des Eintrags in der ersten Spalte zu Null machen. Damit können wir erreichen, dass die transformierte Matrix die Gestalt

$$\left(\begin{array}{c|ccc} b_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{array}\right) \tag{2.3}$$

hat. Ist nun ein Eintrag b_{ij} der Matrix B' nicht durch b_{11} teilbar, so liefert Division mit Rest wieder

$$b_{ij} = q'b_{11} + r' \text{ mit } r' \neq 0 \text{ und } d(r') < d(b_{11}).$$

Addiert man zuerst die erste Zeile zur i-ten und subtrahiert dann die mit q' multiplizierte erste Spalte von der j-ten, so wird aus b_{ij} der Eintrag r'. Nun kann man das Element r' an die Stelle von b_{11} bringen und dann das obige Verfahren wiederholen. Damit können wir erreichen, dass wir schließlich eine Matrix der Form (2.3) erhalten, bei der alle Einträge von B' durch b_{11} teilbar sind. Die Behauptung folgt dann durch Induktion.

(b) Nun geben wir einen anderen Beweis für den allgemeinen Fall, dass R ein nullteilerfreier Hauptidealring ist.

Betrachte den R-Modul $M^* = \mathrm{Hom}_R(M, R)$. Für alle $\psi \in M^*$ ist $\psi(N)$ ein Untermodul von R. Es sei Σ die Menge aller Untermoduln von R, die von der Form $\psi(N)$ für ein $\psi \in M^*$ sind. Da R noethersch ist, gibt es ein $\varphi_1 \in M^*$,

so dass $\varphi_1(N)$ ein maximales Element von Σ ist. Da R ein Hauptidealring ist, gibt es ein $a_1 \in R$ mit $\varphi_1(N) = Ra_1$. Wegen $N \neq 0$ ist $a_1 \neq 0$. Es sei $x_1 \in N$ mit $\varphi_1(x_1) = a_1$.

Behauptung 2.8.1 Es gilt

$$\psi(x_1) \in Ra_1 \quad \text{für alle } \psi \in M^*.$$

Zum Beweis der Behauptung sei $\psi \in M^*$. Betrachte das von $\psi(x_1)$ und $a_1 = \varphi_1(x_1)$ erzeugte Ideal. Dies ist ein Hauptideal, wird also von einem Element $a \in R$ erzeugt. Dann gibt es $b, b_1 \in R$ mit

$$a = b\psi(x_1) + b_1\varphi_1(x_1) = (b\psi + b_1\varphi_1)(x_1) \in (b\psi + b_1\varphi_1)(N).$$

Es folgt

$$Ra_1 \subset Ra \subset (b\psi + b_1\varphi_1)(N).$$

Wegen der Maximalität von Ra_1 muss $Ra_1 = Ra = (b\psi + b_1\varphi_1)(N)$ gelten. Also folgt $\psi(x_1) \in Ra_1$, was zu zeigen war.

Es sei $w_1, \ldots, w_n$ eine beliebige Basis von M. Dann gilt

$$x_1 = c_1w_1 + \cdots + c_nw_n \text{ für } c_1, \ldots, c_n \in R.$$

Betrachte $\psi_j \in M^*$ mit

$$\begin{array}{rccc} \psi_j : & M & \longrightarrow & R \\ & \lambda_1w_1 + \cdots + \lambda_nw_n & \longmapsto & \lambda_j \end{array}, \quad j = 1, \ldots, n.$$

Dann folgt aus der Behauptung, dass $c_j \in Ra_1$ für $j = 1, \ldots, n$ ist. Also gilt $c_j = a_1c_j'$ für $c_j' \in R$ und für

$$v_1 := c_1'w_1 + \ldots + c_n'w_n$$

gilt $x_1 = a_1v_1$.

Behauptung 2.8.2

$$M = Rv_1 \oplus \operatorname{Ker}\varphi_1.$$

Aus $\varphi_1(x_1) = a_1$ folgt $\varphi_1(v_1) = 1$. Also gilt $Rv_1 \cap \operatorname{Ker}\varphi_1 = \{0\}$. Für $x \in M$ gilt aber $\varphi_1(x - \varphi_1(x)v_1) = 0$, also $x - \varphi_1(x)v_1 \in \operatorname{Ker}\varphi_1$. Daher ist M die Summe der angegebenen Untermoduln und die Summe ist direkt. Damit ist die Behauptung bewiesen.

Setze

$$M' := \operatorname{Ker}\varphi_1, \quad N' := \operatorname{Ker}\varphi_1 \cap N.$$

Dann ist M' als Untermodul des freien Moduls M frei (Satz 2.8.1) und es gilt

$$M = Rv_1 \oplus M'.$$

Wegen Behauptung 2.8.2 ist der Rang von M' gleich $n-1$. Daher folgt der Rest durch Induktion. (Man beachte, dass aus der Maximalität von Ra_1 folgt, dass $a_1|a_2$.) □

Korollar 2.8.1 *Es sei M ein endlich erzeugter R-Modul. Dann gibt es $a_1, a_2, \ldots, a_m \in R$, die keine Einheiten in R sind, so dass*

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$$

und $a_i|a_{i+1}$ für $i = 1, \ldots, m-1$.

Beweis. Da M endlich erzeugt ist, gibt es ein $n \in \mathbb{N}$ und einen Epimorphismus $\varphi : R^n \to M$. Nach Satz 2.8.2 gibt es eine Basis $v_1, \ldots, v_n$ von R^n und $b_1, \ldots, b_n \in R$ mit

$$\operatorname{Ker}\varphi = Rb_1v_1 \oplus \cdots \oplus Rb_nv_n \text{ und } b_i|b_{i+1} \text{ für } i = 1, \ldots, n-1.$$

Nach dem Kern-Bild-Satz folgt wegen $R^n = Rv_1 \oplus \cdots \oplus Rv_n$

$$M \cong R^n/\operatorname{Ker}\varphi \cong (Rv_1/Rb_1v_1) \oplus \cdots \oplus (Rv_n/Rb_nv_n).$$

Für jedes $i = 1, \ldots, n$ haben wir einen Isomorphismus

$$R/(b_i) \xrightarrow{\sim} Rv_i/Rb_iv_i, \quad a \mapsto av_i.$$

Ist b_i eine Einheit in R, so gilt $(b_i) = R$, also $R/(b_i) = 0$. Also können wir den entsprechenden Summanden weglassen.

Ist b_i eine Einheit, so auch alle b_j mit $j < i$, da $b_j|b_i$. Es gibt also ein r, $0 \leq r \leq n$, so dass $b_1, \ldots, b_r$ Einheiten sind, aber nicht $b_{r+1}, \ldots, b_n$. Dann setze $a_i := b_{i+r}$. Dann gilt

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_m).$$

und $a_i|a_{i+1}$ für $i = 1, \ldots, m-1$. □

Definition Ein Modul M über einem Integritätsbereich R' heißt *torsionsfrei*, wenn für alle $a \in R'$ und $x \in M$ gilt:

$$ax = 0 \Rightarrow a = 0 \text{ oder } x = 0.$$

Beispiele 2.8.1 (1) Jeder freie Modul ist torsionsfrei. Jeder Untermodul eines freien Moduls ist ebenfalls torsionsfrei. Der $\mathbb{Z}$-Modul $\mathbb{Q}$ ist torsionsfrei, aber nicht frei.

(2) Der $\mathbb{Z}$-Modul $\mathbb{Z}_n$ ($n \in \mathbb{N}$, $n \geq 1$) ist nicht torsionsfrei: Für $x \in \mathbb{Z}_n$ gilt $nx = 0$.

Definition Es sei M ein Modul über einem Integritätsbereich R'. Ein Element $x \in M$ heißt *Torsionselement*, wenn es ein $a \in R'$, $a \neq 0$, mit $ax = 0$ gibt. Die Menge aller Torsionselemente wird mit $T(M)$ bezeichnet. Die Menge $T(M)$ ist ein Untermodul von M, er wird der *Torsionsuntermodul* von M genannt. Der Modul M heißt *Torsionsmodul*, wenn $M = T(M)$ gilt.

Bemerkung 2.8.1 Offensichtlich ist M genau dann torsionsfrei, wenn $T(M) = 0$ gilt.

Satz 2.8.3 *Es sei M ein endlich erzeugter R-Modul. Dann gibt es einen freien Untermodul $F \subset M$ mit*

$$M = F \oplus T(M).$$

Beweis. Nach Korollar 2.8.1 gibt es eine direkte Summenzerlegung

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_m).$$

Es sei F die direkte Summe aller Summanden $R/(a_i)$ mit $a_i = 0$ und M' die der übrigen Summanden. Dann gilt

$$M = F \oplus M'$$

und F ist frei. Es bleibt zu zeigen, dass $M' = T(M)$.

Es sei i mit $a_i \neq 0$. Dann gilt $a_i((a_i) + a) = 0$ in $R/(a_i)$ für alle $a \in R$. Daher ist $R/(a_i)$ ein Torsionsmodul. Es folgt $M' \subset T(M)$.

Gilt nun $M' \neq T(M)$, so folgt aus $M = F \oplus M'$, dass $T(M) \cap F \neq 0$. Da F frei ist, gilt aber $0 = T(F) = F \cap T(M)$. □

Aus Satz 2.8.3 folgt sofort:

Korollar 2.8.2 *Ein endlich erzeugter R-Modul ist genau dann torsionsfrei, wenn er frei ist.*

Nun wollen wir den Torsionsuntermodul $T(M)$ genauer untersuchen. Dazu brauchen wir eine weitere Verallgemeinerung des chinesischen Restsatzes (Satz I.3.7.4). Nach Satz I.3.8.9 ist R faktoriell.

Lemma 2.8.1 *Es seien $p_1, \ldots, p_m$ paarweise teilerfremde Primelemente in dem Ring R, $r_1, \ldots, r_m$ positive ganze Zahlen. Dann gilt*

(i) *Jedes Element $p_j^{r_j}$ ist teilerfremd zu $\prod_{i \neq j} p_i^{r_i}$.*

(ii) *Es gilt $(p_1^{r_1}) \cap \cdots \cap (p_m^{r_m}) = (p_1^{r_1} \cdots p_m^{r_m})$.*

Beweis. (i) Es sei j fest. Da $p_j^{r_j}$ und $p_i^{r_i}$ für $i \neq j$ teilerfremd sind, gibt es Elemente $a_i, b_i \in R$ mit $a_i p_j^{r_j} + b_i p_i^{r_i} = 1$. Daraus folgt

$$1 = \prod_{i \neq j} (a_i p_j^{r_j} + b_i p_i^{r_i}) = a p_j^{r_j} + b \prod_{i \neq j} p_i^{r_i} \text{ mit } a, b \in R.$$

(ii) Beweis durch Induktion über m:

Induktionsanfang $m = 2$: Es ist zu zeigen: $(p_1^{r_1}) \cap (p_2^{r_2}) = (p_1^{r_1} p_2^{r_2})$. Die Inklusion $(p_1^{r_1} p_2^{r_2}) \subset (p_1^{r_1}) \cap (p_2^{r_2})$ ist klar. Es sei $x \in (p_1^{r_1}) \cap (p_2^{r_2})$. Da $p_1^{r_1}$ und $p_2^{r_2}$ teilerfremd sind, gibt es $a, b \in R$ mit $a p_1^{r_1} + b p_2^{r_2} = 1$. Es gilt

$$x = x \cdot 1 = a x p_1^{r_1} + b x p_2^{r_2} \in (p_1^{r_1} p_2^{r_2}).$$

Induktionsschritt $m \to m + 1$: Es sei $m \geq 2$. Dann gilt nach Induktionsannahme

$$(p_1^{r_1}) \cap \cdots \cap (p_m^{r_m}) = (p_1^{r_1} \cdots p_m^{r_m}).$$

Nach (i) und dem Fall $m = 2$ folgt

$$(p_1^{r_1}) \cap \cdots \cap (p_m^{r_m}) \cap (p_{m+1}^{r_{m+1}}) = (p_1^{r_1} \cdots p_m^{r_m}) \cap (p_{m+1}^{r_{m+1}}) = (p_1^{r_1} \cdots p_m^{r_m} p_{m+1}^{r_{m+1}}).$$

□

Satz 2.8.4 *Es sei $b \in R$ und*

$$b = u p_1^{r_1} \cdots p_m^{r_m}$$

die Primfaktorzerlegung von b. Die Abbildung

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & R/(p_1^{r_1}) \times \cdots \times R/(p_m^{r_m}) \\ & x & \longmapsto & ((p_1^{r_1}) + x, \ldots, (p_m^{r_m}) + x) \end{array}$$

induziert einen Isomorphismus

$$R/(b) = R/(p_1^{r_1} \cdots p_m^{r_m}) \xrightarrow{\sim} R/(p_1^{r_1}) \times \cdots \times R/(p_m^{r_m}).$$

Beweis. Es sei $m \geq 2$. Wir zeigen, dass die Abbildung φ surjektiv ist. Dazu seien $x_1, \ldots, x_m \in R$ gegeben. Für jedes $j = 1, \ldots, m$ sind nach Lemma 2.8.1(i) die Elemente $p_j^{r_j}$ und $q_j := \prod_{i \neq j} p_i^{r_i}$ teilerfremd, also gibt es Elemente $a_j, b_j \in R$ mit $a_j p_j^{r_j} + b_j q_j = 1$. Setze

$$x := b_1 q_1 x_1 + \cdots + b_m q_m x_m.$$

Dann gilt $x \equiv x_j \bmod (p_j^{r_j})$ für alle $j = 1, \ldots, n$.

Der Kern von φ ist gleich $(p_1^{r_1}) \cap \cdots \cap (p_m^{r_m})$, also nach Lemma 2.8.1(ii) auch gleich $(p_1^{r_1} \cdots p_m^{r_m})$. □

Es sei $b \in R$, $b \neq 0$, keine Einheit. Dann gibt es paarweise teilerfremde Primelemente $p_1, \ldots, p_m \in R$, Exponenten $r_1, \ldots, r_m > 0$ und eine Einheit $u \in R$ mit

$$b = u p_1^{r_1} \cdots p_m^{r_m}.$$

Nach Satz 2.8.4 gibt es einen Ringisomorphismus

$$R/(b) = R/(p_1^{r_1} \cdots p_m^{r_m}) \xrightarrow{\sim} R/(p_1^{r_1}) \times \cdots \times R/(p_m^{r_m}),$$

der durch $(b)+x \mapsto ((p_1^{r_1})+x, \ldots, (p_m^{r_m})+x)$ gegeben wird. Diese Abbildung ist offensichtlich auch R-linear, also auch ein Isomomorphismus von R-Moduln.

Satz 2.8.5 *Es sei M ein endlich erzeugter R-Modul. Dann gibt es paarweise teilerfremde Primelemente $p_1, \ldots, p_m \in R$ und nicht negative ganze Zahlen n, r_i mit $r_i > 0$ und $\nu_{i,r}$ für $i = 1, \ldots, m$ und $r = 1, \ldots, r_i$, so dass*

$$M \cong R^n \oplus M_1 \oplus \cdots \oplus M_m, \quad M_i = (R/(p_i))^{\nu_{i,1}} \oplus \cdots \oplus (R/(p_i^{r_i}))^{\nu_{i,r_i}}.$$

Beweis. Dies folgt aus Korollar 2.8.1, indem wir alle Summanden $R/(a_i)$ mit Hilfe der obigen Ringisomorphismen weiter zerlegen und die neuen Summanden entsprechend sammeln. □

Wir wollen nun zeigen, dass in der Zerlegung von Satz 2.8.5 die Primelemente $p_1, \ldots, p_m$ und die Zahlen n, r_i mit $r_i > 0$ und $\nu_{i,r}$ für $i = 1, \ldots, m$ und $r \in \mathbb{N}$, $r > 0$ durch M eindeutig bestimmt sind. Dazu dienen die folgenden Vorbereitungen.

Für jedes Primelement $p \in R$ ist (p) ein maximales Ideal in R, also $R/(p)$ ein Körper. Für jeden R-Modul M ist nach Lemma 2.4.2 M/pM ein $R/(p)$-Modul, also ein Vektorraum über dem Körper $R/(p)$. Wenden wir diese Tatsache auf den Modul $p^k M$ anstelle von M an, so erhalten wir, dass $p^k M/p^{k+1} M$ ein $R/(p)$-Vektorraum ist für jedes $k \in \mathbb{N}$.

Lemma 2.8.2 *Es sei $p \in R$ ein Primelement.*

(i) *Es sei $M = R$. Dann gilt für alle $k \in \mathbb{N}$*

$$\dim_{R/(p)}(p^k M/p^{k+1}M) = 1.$$

(ii) *Es sei $M = R/(p^r)$ mit $r \in \mathbb{N}$. Dann gilt für alle $k \in \mathbb{N}$*

$$\dim_{R/(p)}(p^k M/p^{k+1}M) = \begin{cases} 1 & \text{für } k < r, \\ 0 & \text{für } k \geq r. \end{cases}$$

(iii) *Es sei $q \in R$ ein zu p teilerfremdes Primelement und $M = R/(q^r)$ für ein $r \in \mathbb{N}$. Dann gilt für alle $k \in \mathbb{N}$*

$$\dim_{R/(p)}(p^k M/p^{k+1}M) = 0.$$

Beweis. Es sei $\pi : R \to M$ der kanonische Epimorphismus. (Im Fall (i) ist $\pi = \mathrm{Id} : R \to M$.) Dann gilt für alle $k \in \mathbb{N}$ die Identität $p^k M = Rp^k\pi(1)$. Also wird $p^k M/p^{k+1}M$ als $R/(p)$-Vektorraum von der Klasse von $p^k\pi(1)$ erzeugt. Daher gilt $\dim_{R/(p)}(p^k M/p^{k+1}M) \leq 1$ und

$$\dim_{R/(p)}(p^k M/p^{k+1}M) = 1 \Leftrightarrow p^k M \neq p^{k+1}M.$$

(i) Aus der Eindeutigkeit der Primfaktorzerlegung folgt $Rp^k \neq Rp^{k+1}$ für alle $k \in \mathbb{N}$. Daraus folgt (i).

(ii) Es sei $M = R/(p^r)$ mit $r \in \mathbb{N}$. Für $k \geq r$ gilt $p^k M = 0$. Daraus und aus (i) folgt (ii).

(iii) Da p und q teilerfremd sind, sind auch p^k und q^r für alle $k, r \in \mathbb{N}$ teilerfremd. Also gibt es $a, b \in R$ mit $ap^k + bq^r = 1$. Daraus folgt

$$p^k M = Rp^k/(q^r) = (Rp^k + Rq^r)/(q^r) = R/(q^r) = M \text{ für alle } k \in \mathbb{N},$$

also insbesondere $p^k M = p^{k+1}M$. □

Satz 2.8.6 *In Satz 2.8.5 sind die Primelemente $p_1, \ldots, p_m$ und die Zahlen n, r_i mit $r_i > 0$ und $\nu_{i,r}$ für $i = 1, \ldots, m$ und $r = 1, \ldots, r_i$ durch M eindeutig bestimmt.*

Beweis. Es gilt $M \cong R^n \oplus T(M)$, also

$$R^n \cong M/T(M).$$

Daher ist n als Rang des freien Moduls $M/T(M)$ eindeutig bestimmt.

Es sei $M = N_1 \oplus \cdots \oplus N_s$. Dann gilt $p^k M = \bigoplus_{i=1}^s p^k N_i$ für alle Primelemente $p \in R$ und alle $k \in \mathbb{N}$. Also folgt

$$p^k M/p^{k+1}M \cong \bigoplus_{i=1}^{s} (p^k N_i/p^{k+1}N_i).$$

Aus Lemma 2.8.2 folgt für p_i für $i = 1, \ldots, m$ und alle $k \in \mathbb{N}$

$$\dim_{R/(p_i)}(p_i^k M/p_i^{k+1}M) = n + \sum_{r=k+1}^{\infty} \nu_{i,r}.$$

Daraus lassen sich rekursiv die Zahlen $\nu_{i,r}$ als Differenzen zweier solcher Dimensionen berechnen. Also folgt, dass auch die $\nu_{i,r}$ eindeutig bestimmt sind. □

Da $\mathbb{Z}$-Moduln und endliche abelsche Gruppen im Wesentlichen dasselbe sind, haben wir damit auch bewiesen:

Korollar 2.8.3 *Es sei G eine endlich erzeugte abelsche Gruppe. Dann gibt es paarweise teilerfremde Primzahlen $p_1, \ldots, p_m$ und nicht negative ganze Zahlen n, r_i mit $r_i > 0$ und $\nu_{i,r}$ für $i = 1, \ldots, m$ und $r = 1, \ldots, r_i$, so dass*

$$G \cong \mathbb{Z}^n \oplus M_1 \oplus \cdots \oplus M_m, \quad M_i = (\mathbb{Z}_{p_i})^{\nu_{i,1}} \oplus \cdots \oplus (\mathbb{Z}_{p_i^{r_i}})^{\nu_{i,r_i}}.$$

Definition Für jeden R-Modul M und jedes Primelement $p \in R$ setzen wir

$$T_p(M) := \{x \in M \mid \text{es existiert } k \in \mathbb{N} \text{ mit } p^k x = 0\}.$$

Dies ist offensichtlich ein Untermodul von M.

Satz 2.8.7 *Es sei M ein endlich erzeugter R-Modul. Es seien $p_1, \ldots, p_m \in R$ paarweise teilerfremde Primelemente und r_i mit $r_i > 0$ und $\nu_{i,r}$ für $i = 1, \ldots, m$ und $r = 1, \ldots, r_i$ nicht negative ganze Zahlen, so dass*

$$T(M) \cong M_1 \oplus \cdots \oplus M_m, \quad M_i = (R/(p_i))^{\nu_{i,1}} \oplus \cdots \oplus (R/(p_i^{r_i}))^{\nu_{i,r_i}}.$$

Dann gilt

$$T(M) = \bigoplus_{i=1}^{m} T_{p_i}(M).$$

Beweis. Es sei $p \in R$ ein Primelement. Ist $M = N_1 \oplus \cdots \oplus N_s$, so gilt $T_p(M) = \bigoplus_{i=1}^s T_p(N_i)$. Offensichtlich gilt

$$T_p(R) = 0 \text{ und } T_p(R/(p^r)) = R/(p^r) \text{ für alle } r \in \mathbb{N}, r > 0.$$

Ist $q \in R$ ein zu p teilerfremdes Primelement, so folgt wie im Beweis von Lemma 2.8.2

$$T_p(R/(q^r)) = 0 \text{ für alle } r \in \mathbb{N}, r > 0.$$

Daraus folgt die Behauptung. □

Satz 2.8.8 *In Satz 2.8.2 sind die Hauptideale Ra_i durch M und N eindeutig bestimmt. In Korollar 2.8.1 sind die Hauptideale Ra_i durch M eindeutig bestimmt.*

Beweis. (a) Wir betrachten zunächst Korollar 2.8.1. Es gibt dort ein $\ell \in \mathbb{N}$ mit $0 \leq \ell \leq m$, so dass $a_i \neq 0$ für alle $i \leq \ell$ und $a_i = 0$ für alle $i > \ell$. Dann gilt

$$T(M) \cong \bigoplus_{i=1}^{\ell} R/(a_i), \quad M/T(M) \cong R^{m-\ell}.$$

Nach Voraussetzung gilt $a_i | a_{i+1}$ für $i = 1, \ldots, \ell - 1$. Es seien $p_1, \ldots, p_m \in R$ die paarweise verschiedenen Primteiler von a_ℓ. Für jedes $i \leq \ell$ haben wir eine Zerlegung

$$a_i = u_i p_1^{\rho_{i,1}} \cdots p_m^{\rho_{i,m}},$$

wobei $u_i \in R$ eine Einheit ist und $\rho_{i,j} \in \mathbb{N}$. Ein Vergleich mit der Zerlegung in Satz 2.8.5 zeigt, dass

$$\nu_{j,r} := |\{1 \leq i \leq \ell \,|\, \rho_{i,j} = r\}|.$$

Außerdem gilt

$$\rho_{1,j} \leq \rho_{2,j} \leq \cdots \leq \rho_{\ell,j} \text{ für alle } j = 1, \ldots, m.$$

Nach Satz 2.8.6 sind die $\nu_{j,r}$ durch M eindeutig bestimmt. Daher sind auch die Zahlen $\rho_{i,j}$ eindeutig festgelegt und damit auch die Hauptideale $(a_i) = (\prod_{j=1}^m p_j^{\rho_{i,j}})$. Schließlich ist auch die Zahl ℓ festgelegt: Da a_1 keine Einheit ist, gibt es ein j mit $1 \leq j \leq m$ und $p_j | a_1$. Dann gilt

$$\ell = \sum_{r=1}^{r_j} \nu_{j,r}.$$

(b) Nun betrachten wir Satz 2.8.2. O.B.d.A. können wir annehmen, dass r mit $0 \leq r \leq n$ so gewählt werden kann, dass $a_1, \ldots, a_r$ Einheiten sind, aber nicht $a_{r+1}, \ldots, a_n$. Dann gilt für $1 \leq i \leq r$ die Gleichheit $(a_i) = R$. Es sei $m := n - r$. Dann sind $a_{r+1}, \ldots, a_n$ gerade die Elementarteiler von M/N, also sind $a_{r+1}, \ldots, a_n$ und $r = n - m$ nach (a) durch M und N eindeutig festgelegt. □

Satz 2.8.9 *Es seien M und M' freie R-Moduln von endlichem Rang und $f : M \to M'$ eine R-lineare Abbildung. Dann gibt es eine Basis $v_1, \ldots, v_n$ von M und eine Basis $w_1, \ldots, w_m$ von M', eine natürliche Zahl $k \leq \min\{n, m\}$ und $a_1, \ldots, a_k \in R \setminus \{0\}$ mit $a_i | a_{i+1}$ für $i = 1, \ldots, k-1$, so dass*

$$f(v_i) = \begin{cases} a_i w_i & \text{für } 1 \leq i \leq k, \\ 0 & \text{für } k < i \leq n. \end{cases}$$

Die Zahl k und die Ideale (a_i) sind durch f eindeutig bestimmt.

Beweis. Wir wenden den Elementarteilersatz (Satz 2.8.2) auf den Untermodul $f(M) \subset M'$ an. Nach diesem Satz gibt es eine Basis $w_1, \ldots, w_m$ von M' und $a_1, \ldots, a_m \in R$ mit

$$f(M) = Ra_1 w_1 + \cdots + Ra_m w_m \text{ und } a_i | a_{i+1} \text{ für } 1 \leq i \leq m-1.$$

Es gibt dann ein $k \leq m$ mit

$$a_i = 0 \text{ für alle } i > k \text{ und } a_i \neq 0 \text{ für alle } i \leq k.$$

Dann ist $a_1 w_1, \ldots, a_k w_k$ eine Basis von $f(M)$ über R. Da $f(M)$ frei ist, spaltet die Sequenz

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow M \xrightarrow{f} f(M) \longrightarrow 0.$$

Es gibt also eine R-lineare Abbildung $s : f(M) \to M$ mit $f \circ s = \mathrm{Id}_{f(M)}$ und es gilt $M = \operatorname{Ker} f \oplus \operatorname{Im} s$. Setze

$$v_i := s(a_i w_i) \text{ für alle } i \leq k.$$

Dann folgt $f(v_i) = a_i w_i$ für $i \leq k$. Da $s : f(M) \xrightarrow{\sim} \operatorname{Im} s$ ein Isomorphismus ist, ist $v_1, \ldots, v_k$ eine Basis von $\operatorname{Im} s$. Wähle eine Basis $v_{k+1}, \ldots v_n$ von $\operatorname{Ker} f$. Dann ist $v_1, \ldots, v_n$ eine Basis von M und $f(v_1), \ldots, f(v_n)$ hat die gewünschte Gestalt.

Die Zahl k ist der Rang von $f(M)$. Die Hauptideale (a_i) sind nach Satz 2.8.8 durch f eindeutig festgelegt. □

2.9 Moduln über $K[x]$

Es sei K ein Körper. Wir können die im letzten Abschnitt entwickelte Theorie auf den Polynomring $K[x]$ anwenden, der ja nach Algebra I ein Hauptidealring ist.

Es sei V ein K-Vektorraum und $\varphi : V \to V$ eine lineare Abbildung. Dann wird V durch die skalare Multiplikation

$$(a_0 + a_1 x + \cdots + a_n x^n)(v) := a_0 v + a_1 \varphi(v) + \cdots + a_n \varphi^n(v)$$

zu einem $K[x]$-Modul, den wir mit (V, φ) bezeichnen.

Ist umgekehrt M ein $K[x]$-Modul, so können wir M auch als K-Modul betrachten, wenn wir die skalare Multiplikation $K[x] \times M \to M$, $(p(x), v) \mapsto p(x)v$, auf $K \times M \to M$ einschränken. Die Abbildung

$$\begin{array}{rccc} \psi : & M & \longrightarrow & M \\ & v & \longmapsto & xv \end{array}$$

ist dann eine K-lineare Abbildung. Es folgt, dass M als $K[x]$-Modul isomorph zu (M, ψ) ist.

Sind $(V, \varphi), (V', \varphi')$ zwei solche $K[x]$-Moduln, so ist eine Abbildung $f : V \to V'$ genau dann $K[x]$-linear, wenn f eine K-lineare Abbildung mit $\varphi' \circ f = f \circ \varphi$ ist. Insbesondere sind $(V, \varphi), (V', \varphi')$ genau dann isomorphe $K[x]$-Moduln, wenn es einen Isomorphismus $f : V \xrightarrow{\sim} V'$ von K-Vektorräumen mit $\varphi' = f \circ \varphi \circ f^{-1}$ gibt.

Es sei nun (V, φ) ein $K[x]$-Modul, wobei $V \neq 0$ ein endlich dimensionaler K-Vektorraum ist. Es sei $n := \dim_K V$. Es sei $K[\varphi]$ der Unterring von $\mathrm{End}_K(V)$, der von φ erzeugt wird (vgl. den Beweis von Satz 2.4.4). Er ist kommutativ, da Potenzen von φ miteinander kommutieren. Der Kern der Abbildung

$$K[x] \to K[\varphi], \quad p(x) \mapsto p(\varphi),$$

ist ein Hauptideal von $K[x]$, das von dem Nullideal verschieden ist, da $K[\varphi]$ nach Satz 2.4.5 endlich dimensional über K ist. Dieses Hauptideal wird von einem eindeutig bestimmten normierten Polynom $\mu_\varphi(x)$ vom Grad > 0 erzeugt. Dies ist gerade das Minimalpolynom von φ.

Definition Es sei R ein beliebiger Ring. Ein R-Modul M heißt *zyklisch*, falls es ein $x \in M$ gibt mit $M = Rx$.

Lemma 2.9.1 *Es sei $V \neq 0$ ein K-Vektorraum der Dimension n und $\varphi : V \to V$ eine lineare Abbildung. Der $K[x]$-Modul (V, φ) ist genau dann zyklisch, wenn es ein $v \in V$ gibt, so dass $v, \varphi(v), \ldots, \varphi^{n-1}(v)$ eine Basis von V ist.*

Beweis. Übungsaufgabe. □

Es sei (V, φ) ein zyklischer $K[x]$-Modul und

$$\mu_\varphi(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

das Minimalpolynom von φ. Nach Lemma 2.9.1 existiert dann ein $v \in V$, so dass $v, \varphi(v), \ldots, \varphi^{n-1}(v)$ eine Basis von V ist. Bezüglich dieser Basis hat φ die folgende Matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Lemma 2.9.2 *Es sei $V \neq 0$ ein K-Vektorraum der Dimension n und $\varphi : V \to V$ eine lineare Abbildung. Der $K[x]$-Modul (V, φ) ist genau dann zyklisch, wenn er isomorph zu einem Modul $K[x]/(f(x))$ für ein normiertes Polynom $f(x) \in K[x]$ ist. Das Polynom $f(x)$ ist dabei eindeutig durch φ bestimmt.*

Beweis. "$\Rightarrow$": Es sei (V, φ) ein zyklischer $K[x]$-Modul und $v \in V$ ein Element mit $V = K[x]v = K[\varphi]v$. Dann gilt

$$a_0 v + a_1 \varphi(v) + \cdots + a_{n-1}\varphi^{n-1}(v) + \varphi^n(v) = 0 \text{ für } a_0, \ldots a_{n-1} \in K.$$

Es sei $f(x) \in K[x]$ das Polynom

$$f(x) := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n.$$

Dann ist die Abbildung $K[x]/(f(x)) \to V$, $p(x) \mapsto p(\varphi)v$, ein Isomorphismus von $K[x]$-Moduln. Das Polynom $f(x)$ hängt nur von φ, nicht aber von der Wahl des erzeugenden Elements $v \in V$ ab.

"$\Leftarrow$": Es sei $F : K[x]/(f(x)) \xrightarrow{\sim} V$ ein Isomorphismus. Der Modul $K[x]/(f(x))$ hat über K die Basis

$$w_1 = 1 + (f(x)), w_2 = x + (f(x)), \ldots, w_n = x^{n-1} + (f(x)).$$

In diesem Modul gilt dann $xw_i = w_{i+1}$ für $1 \leq i < n$. Dann ist $F(w_1), \ldots, F(w_n)$ eine Basis von V. Wegen

$$\varphi(F(w_i)) = xF(w_i) = F(xw_i) = F(w_{i+1})$$

für $1 \leq i < n$ folgt dann, dass $F(w_i) = \varphi^{i-1}(F(w_1))$ für $i = 1, \ldots, n$ ist. Damit folgt die Behauptung aus Lemma 2.9.1. □

Definition Ist (V, φ) ein zyklischer $K[x]$-Modul, so heißt das Polynom $f(x)$ aus Lemma 2.9.2 das *Begleitpolynom* von V.

Satz 2.9.1 *Es sei $V \neq 0$ eine endlich dimensionaler K-Vektorraum und $\varphi : V \to V$ eine lineare Abbildung. Dann lässt sich V als direkte Summe*

$$V = V_1 \oplus \ldots \oplus V_m$$

darstellen, wobei jedes V_i ein zyklischer $K[x]$-Modul mit Begleitpolynom $f_i(x) \neq 0$ ist und so dass

$$f_1(x)|f_2(x)|\cdots|f_m(x)$$

gilt. Die Folge $(f_1(x), f_2(x), \ldots, f_m(x))$ ist durch (V, φ) eindeutig bestimmt und $f_m(x)$ ist das Minimalpolynom von φ.

Beweis. Die erste Behauptung ist eine direkte Übersetzung von Korollar 2.8.1, wobei wir Lemma 2.9.2 benutzen. Es kann $f_i(x) = 0$ nicht vorkommen, da $K[x]/(0) = K[x]$ unendliche Dimension hat.

Die Eindeutigkeitsaussage folgt aus Satz 2.8.8.

Das Polynom $f_m(x)$ ist das Minimalpolynom von φ: Es gilt $f_m(\varphi) = 0$, da $f_i(x)|f_m(x)$ für alle $i = 1, \ldots m$. Kein Polynom von kleinerem Grad kann V annullieren, da ein solches Polynom nicht V_m annulliert. □

Nun sei (V, φ) ein $K[x]$-Modul, so dass das charakteristische Polynom von φ in Linearfaktoren zerfällt. Für $\lambda \in K$ wird dann der $(x-\lambda)$-Torsionsmodul von V durch

$$T_{x-\lambda}(V) = \{v \in V \,|\, \text{es gibt ein } r \in \mathbb{N} \text{ mit } (\varphi - \lambda)^r(v) = 0\}$$

gegeben. Dies ist gerade der Hauptraum $\mathrm{Hau}(\varphi, \lambda)$ von φ zum Eigenwert λ nach Lineare Algebra II. Die Formel von Satz 2.8.7 besagt, dass V die direkte Summe der Haupträume von φ ist. Damit erhalten wir die Hauptraumzerlegung aus Lineare Algebra II. Daraus leiten wir nun erneut die Existenz der Jordanschen Normalform von φ ab.

Lemma 2.9.3 *Es sei $\lambda \in K$ und $n \in \mathbb{N}$, $n > 0$. Der durch (V, φ) gegebene $K[x]$-Modul ist genau dann zu $K[x]/((x-\lambda)^n)$ isomorph, wenn es eine Basis von V gibt, bezüglich der die Matrix von φ gleich*

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} \in \mathrm{Mat}(n, n; K)$$

ist.

Beweis. "⇒": Es sei $f(x) := (x-\lambda)^n$. Der Modul $K[x]/(f(x))$ hat über K die Basis

$$w_1 = (x-\lambda)^{n-1} + (f(x)), \ldots, w_{n-1} = x - \lambda + (f(x)), w_n = 1 + (f(x)).$$

Dann gilt

$$\begin{aligned}
xw_1 &\equiv \lambda w_1 \bmod (f(x)),\\
xw_2 &\equiv x(x-\lambda)^{n-2} \equiv (x-\lambda)^{n-1} + \lambda(x-\lambda)^{n-2} \equiv w_1 + \lambda w_2 \bmod (f(x)),\\
&\vdots \quad \vdots \quad \vdots\\
xw_n &\equiv x \equiv x - \lambda + \lambda \equiv w_{n-1} + \lambda w_n \bmod (f(x)).
\end{aligned}$$

Der Rest des Beweises dieser Richtung geht genau wie der Beweis von Lemma 2.9.2 "⇐".

"⇐": Es sei $v_1, \ldots, v_n$ eine Basis von V, bezüglich der φ die obige Gestalt hat. Dann liefert die K-lineare Abbildung $F : K[x]/((x-\lambda)^n) \to V$ mit $F(w_i) = v_i$ für $i = 1, \ldots, n$ einen Isomorphismus der entsprechenden $K[x]$-Moduln. □

Satz 2.9.2 (Jordansche Normalform) *Es sei V ein endlich dimensionaler K-Vektorraum ist und $\varphi : V \to V$ eine K-lineare Abbildung, deren charakteristisches Polynom in Linearfaktoren zerfällt. Dann gibt es $\lambda_1, \ldots, \lambda_r \in K$, positive ganze Zahlen $m_1, \ldots, m_r$ und eine Basis von V, bezüglich der φ die Form*

$$\begin{pmatrix}
J_{m_1}(\lambda_1) & & & 0\\
& J_{m_2}(\lambda_2) & & \\
& & \ddots & \\
0 & & & J_{m_1}(\lambda_r)
\end{pmatrix}$$

hat. Die Paare (λ_i, m_i) sind durch φ bis auf Reihenfolge eindeutig bestimmt.

Beweis. Dieser Satz folgt aus Satz 2.8.7 und Satz 2.8.6. □

Kapitel 3

Algebren und ganze Ringerweiterungen

3.1 Algebren

Es sei B ein kommutativer Ring. (Weiterhin betrachten wir nur Ringe mit 1.)

Definition Ein Ring A heißt *B-Algebra*, wenn A ein B-Modul ist und die beiden Strukturen verträglich sind, d.h. die Ringmultiplikation $A \times A \to A$ ist B-bilinear:

$$(ba)a' = a(ba') = b(aa') \quad \text{für alle } b \in B, a, a' \in A.$$

Es sei A eine B-Algebra. Erkläre

$$f : B \to A \text{ durch } f(b) = b \cdot 1.$$

Dann ist f ein Ringhomomorphismus. Die Additivität $f(b+b') = f(b)+f(b')$ folgt aus den Modulaxiomen. Außerdem gilt

$$f(bb') = (bb')1 = b(b'1) = b(1(b'1)) = (b1)(b'1) = f(b)f(b').$$

Es gilt $\operatorname{Im} f \subset Z(A)$, wobei $Z(A)$ das Zentrum von A bezeichnet, also

$$Z(A) := \{a \in A \,|\, ax = xa \text{ für alle } x \in A\}.$$

Denn es gilt für alle $b \in B$ und $x \in A$

$$f(b)x = (b1)x = b(1x) = bx = b(x1) = x(b1) = xf(b).$$

Ist umgekehrt ein Ring A und ein Ringhomomorphismus $f : B \to Z(A)$ gegeben, so können wir eine skalare Multiplikation $B \times A \to A$ durch

$$ba := f(b)a, \quad b \in B, a \in A,$$

definieren. Dadurch wird A zu einer B-Algebra.

Eine B-Algebra ist also ein Ring A zusammen mit einem Ringhomomorphismus $f : B \to Z(A)$.

Beispiele 3.1.1 (1) Der Polynomring $R[x_1, \ldots, x_n]$ über einem kommutativen Ring R ist eine kommutative R-Algebra.

(2) Es sei R ein Ring. Für alle $n \in \mathbb{N}$, $n > 0$, bezeichnen wir mit

$$M_n(R) := \mathrm{Mat}(n, n; R)$$

den Ring aller $n \times n$-Matrizen mit Einträgen in R. Ist R kommutativ, so ist $M_n(R)$ eine R-Algebra, die im Allgemeinen nicht kommutativ ist.

Definition Es seien A, A' B-Algebren. Ein *B-Algebrahomomorphismus* ist ein Ringhomomorphismus $h : A \to A'$, der auch ein B-Modulhomomorphismus ist.

Bemerkung 3.1.1 Es seien A, A' B-Algebren, $f : B \to Z(A)$, $g : B \to Z(A')$ die zugehörigen Ringhomomorphismen. Dann gilt: Ein Ringhomomorphismus $h : A \to A'$ ist genau dann ein B-Algebrahomomorphismus, wenn $h \circ f = g$ gilt.

Definition Es sei A ein kommutativer Ring, der eine B-Algebra ist.

(a) A heißt *endlich erzeugt* über B (*endlich erzeugt als B-Algebra*), falls es endlich viele Elemente $a_1, \ldots, a_n \in A$ gibt mit $A = B[a_1, \ldots, a_n]$.

(b) A heißt *endliche B-Algebra*, falls A endlich erzeugt als B-Modul ist, d.h. es gibt endlich viele Elemente $a_1, \ldots, a_n \in A$ mit

$$A = Ba_1 + \cdots + Ba_n.$$

Beispiel 3.1.1 Der Polynomring $R[x_1, \ldots, x_n]$ ist endlich erzeugte, aber keine endliche R-Algebra.

3.2 Ganze Ringerweiterungen

Definition Es seien $B \subset A$ kommutative Ringe.

(a) Ein Element $x \in A$ heißt *ganz* über B, falls x eine Gleichung

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0 \quad \text{mit } b_i \in B \tag{3.1}$$

erfüllt.

(b) A heißt *ganz* über B, falls alle Elemente $x \in A$ ganz über B sind.

Bemerkung 3.2.1 Man beachte: Der Leitkoeffizient in der Gleichung (3.1) ist 1, d.h. das Polynom ist normiert.

Satz 3.2.1 *Es seien $C \subset B \subset A$ kommutative Ringe.*

(i) *Ist B eine endliche C-Algebra und A eine endliche B-Algebra, so ist A eine endliche C-Algebra.*

(ii) *Ist A eine endliche B-Algebra, so ist A ganz über B.*

(iii) *Ist $x \in A$ ganz über B, so ist $B[x]$ eine endliche B-Algebra.*

Beweis. (i) Es sei $b_1, \ldots, b_m$ ein Erzeugendensystem von B als C-Modul, d.h.

$$B = Cb_1 + \cdots + Cb_m.$$

Es sei $a_1, \ldots, a_n$ ein Erzeugendensystem von A als B-Modul, d.h.

$$A = Ba_1 + \cdots + Ba_n.$$

Dann folgt

$$A = Ca_1b_1 + \cdots + Ca_1b_m + \cdots + Ca_nb_1 + \cdots + Ca_nb_m.$$

(ii) Es sei $x \in A$. Wende Satz 2.4.5 auf $I = B$, $\varphi = x \cdot \mathrm{Id}$ an. Die Voraussetzung $xA \subset BA$ ist trivialerweise erfüllt. Aus Satz 2.4.5 folgt dann, dass x ganz über B ist.

(iii) Da $x \in A$ ganz über B ist, genügt x einer Gleichung

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0 \quad \text{mit } b_i \in B.$$

Daraus folgt

$$B[x] = B + Bx + \cdots + Bx^{n-1}.$$

□

Lemma 3.2.1 (Lemma von Nakayama) *Es sei $A \neq 0$ eine endliche B-Algebra. Dann gilt für alle echten Ideale I von B, dass*

$$IA \neq A.$$

Beweis. Angenommen, $IA = A$. Aus Satz 2.4.5 mit $\varphi = \mathrm{Id}$ folgt dann, dass $a_0, \dots a_{n-1} \in I$ existieren mit

$$1 + a_{n-1} + \cdots + a_0 = 0.$$

Daraus folgt $1 \in I$, ein Widerspruch. □

Lemma 3.2.2 *Es sei A ein Körper, $B \subset A$ ein Unterring, so dass A eine endliche B-Algebra ist. Dann ist auch B ein Körper.*

Beweis. Es sei $b \in B$, $b \neq 0$. Da A ein Körper ist, existiert das Inverse $b^{-1} \in A$ von b.

Es ist zu zeigen: $b^{-1} \in B$. Aus Satz 3.2.1(ii) folgt, dass $b_0, \dots, b_{n-1} \in B$ existieren, so dass

$$b^{-n} + b_{n-1}b^{-(n-1)} + \cdots + b_1 b^{-1} + b_0 = 0.$$

Multiplizieren wir diese Gleichung mit b^{n-1}, so folgt

$$b^{-1} = -(b_{n-1} + b_{n-2}b + \cdots + b_1 b^{n-2} + b_0 b^{n-1}) \in B.$$

□

3.3 Noether-Normalisierung

Definition Es sei K ein Körper, A ein endlich erzeugte K-Algebra. Die Elemente $y_1, \dots, y_m \in A$ heißen *algebraisch unabhängig* über K, falls kein vom Nullpolynom verschiedenes Polynom $f(t_1, \dots, t_m) \in K[t_1, \dots, t_m]$ mit $f(y_1, \dots, y_m) = 0$ existiert.

Bemerkung 3.3.1 Die Elemente $y_1, \dots, y_m \in A$ sind genau dann algebraisch unabhängig über K, wenn die Abbildung

$$\begin{array}{ccc} K[t_1, \dots, t_m] & \to & K[y_1, \dots, y_m] \\ t_i & \mapsto & y_i, i = 1, \dots, m \end{array}$$

ein K-Algebraisomorphismus ist.

Theorem 3.3.1 (Noether-Normalisierung) *Es sei K ein unendlicher Körper, $A = K[a_1, \ldots, a_n]$ eine endlich erzeugte K-Algebra. Dann existieren Elemente $y_1, \ldots, y_m \in A$, $m \leq n$, so dass*

(i) *$y_1, \ldots, y_m$ sind algebraisch unabhängig über K.*

(ii) *A ist eine endliche $K[y_1, \ldots, y_m]$-Algebra.*

Theorem 3.3.2 (Schwacher Nullstellensatz) *Es sei K ein unendlicher Körper, A eine endlich erzeugte K-Algebra, die ein Körper ist. Dann ist A algebraisch über K.*

Beweis. Es sei $A = K[a_1, \ldots, a_n]$ ein Körper. Nach Theorem 3.3.1 gibt es ein $m \leq n$ und Elemente $y_1, \ldots y_m \in A$, so dass gilt

(i) $y_1, \ldots, y_m$ sind algebraisch unabhängig über K.

(ii) A ist eine endliche $K[y_1, \ldots, y_m]$-Algebra.

Setze $B := K[y_1, \ldots, y_m] \subset A$. Aus Lemma 3.2.2 folgt, dass B ein Körper ist. Da $y_1, \ldots y_m$ algebraisch unabhängig über K sind, folgt $m = 0$. Also ist A eine endliche K-Algebra, also eine endliche Körpererweiterung von K. Nach Satz I.5.4.4 ist A algebraisch über K. □

Zum Beweis von Theorem 3.3.1 brauchen wir noch ein Lemma.

Lemma 3.3.1 *Es sei K ein unendlicher Körper, $f \in K[x_1, \ldots, x_n]$, $f \neq 0$, $d = \operatorname{Grad} f$. Dann gibt es eine lineare Koordinatentransformation*

$$x_i' = x_i - \alpha_i x_n, \quad \alpha_i \in K, \quad 1 \leq i \leq n-1,$$

so dass das Polynom

$$f(x_1' + \alpha_1 x_n, \ldots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \in K[x_1', \ldots, x_{n-1}', x_n]$$

einen Term der Form cx^d für ein $c \in K$, $c \neq 0$, hat.

Bemerkung 3.3.2 Tatsächlich gilt die Aussage von Lemma 3.3.1 für "fast alle" α_i.

Beweis. Wir können f schreiben als

$$f = F_d + G,$$

wobei F_d homogen vom Grad d und G ein Polynom vom Grad $\leq d-1$ ist. Dann folgt

$$\begin{aligned} & f(x'_1 + \alpha_1 x_n, \ldots, x'_{n-1} + \alpha_{n-1} x_n, x_n) \\ &= F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) x_n^d + \text{ Terme niedrigeren Grades in } x_n. \end{aligned}$$

Dabei ist $F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \in K[\alpha_1, \ldots, \alpha_{n-1}]$ nicht das Nullpolynom. Betrachte

$$V(F_d) := \{(\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1} \mid F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) = 0\}.$$

Da K ein unendlicher Körper ist, ist $V(F_d)$ nicht der ganze K^{n-1}. Also gibt es $\alpha_1, \ldots, \alpha_{n-1} \in K$, so dass

$$F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0.$$

Dann können wir

$$c := F_d(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$$

setzen. □

Beweis von Theorem 3.3.1. Wir beweisen das Theorem durch Induktion nach n. Zunächst betrachten wir den Kern $I \subset K[x_1, \ldots, x_n]$ der Abbildung

$$\begin{array}{ccc} K[x_1, \ldots, x_n] & \to & K[a_1, \ldots, a_n] \\ x_i & \mapsto & a_i \end{array}$$

Gilt $I = 0$, so können wir $m := n$ und $y_i := a_i$ für $i = 1, \ldots, n$ setzen. Wir nehmen also an, dass $I \neq 0$ gilt. Dann gibt es ein $f \in I$, $f \neq 0$. Es sei Grad $f = d$.

Für $n = 1$ folgt $f(a_1) = 0$. In diesem Fall können wir $m := 0$ setzen. Die Behauptung (ii) folgt dann aus Satz 3.2.1(iii).

Es sei nun $n > 1$. Dann existieren nach Lemma 3.3.1 $\alpha_1, \ldots, \alpha_{n-1} \in K$, so dass für

$$a'_i := a_i - \alpha_i a_n. \quad i = 1, \ldots, n-1,$$

das Polynom

$$f(a'_1 + \alpha_1 x_n, \ldots, a'_{n-1} + \alpha_{n-1} x_n, x_n) \in K[a'_1, \ldots, a'_{n-1}, x_n]$$

einen Term der Form cx_n^d mit $c \in K$, $c \neq 0$, hat. Setze

$$\begin{aligned} A' &:= K[a'_1, \ldots, a'_{n-1}] \subset A, \\ F(x_n) &:= \frac{1}{c} f(a'_1 + \alpha_1 x_n, \ldots, a'_{n-1} + \alpha_{n-1} x_n, x_n) \in A'[x_n]. \end{aligned}$$

Dann ist das Polynom $F(x_n)$ normiert und es gilt $F(a_n) = 0$. Dies zeigt, dass a_n ganz über A' ist.

Auf A' können wir die Induktionsannahme anwenden. Danach gibt es Elemente $y_1, \ldots, y_m \in A'$, so dass gilt

(i') $y_1, \ldots, y_m$ sind algebraisch unabhängig über K.

(ii') A' ist eine endliche $K[y_1, \ldots, y_m]$-Algebra.

Da a_n ganz über A' ist, folgt aus Satz 3.2.1(iii), dass $A = A'[a_n]$ eine endliche A'-Algebra ist. Aus (ii') und Satz 3.2.1(i) folgt dann, dass A eine endliche $K[y_1, \ldots, y_m]$-Algebra ist. □

Kapitel 4

Tensorprodukte

4.1 Tensorprodukte von Moduln

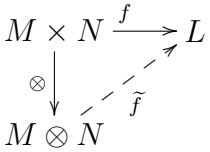
In diesem Kapitel sei A ein *kommutativer* Ring.

Definition Es seien L, M, N A-Moduln. Eine Abbildung $f : M \times N \to L$ heißt *bilinear*, falls gilt

$$\begin{aligned} f(ax + by, u) &= af(x, u) + bf(y, u), \\ f(x, au + bv) &= af(x, u) + bf(x, v) \end{aligned}$$

für alle $x, y \in M$, $u, v \in N$ und $a, b \in A$.

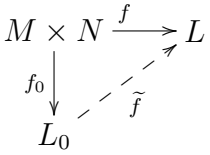
Die Idee des Tensorprodukts besteht darin, einen A-Modul $M \otimes N$ zu konstruieren, so dass *jede* bilineare Abbildung f über das Tensorprodukt faktorisiert:



Dabei ist $\otimes : M \times N \to M \otimes N$ eine feste bilineare Abbildung, Die Abbildung $\widetilde{f}$ ist linear. Es ist also ein Paar $(M \otimes N, \otimes)$ mit dieser "universellen Eigenschaft" zu konstruieren.

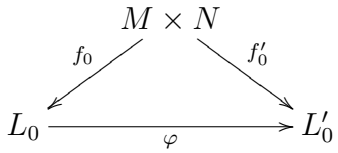
Definition Ein *Tensorprodukt* zweier A-Moduln M und N ist ein A-Modul L_0 mit einer bilinearen Abbildung $f_0 : M \times N \to L_0$, welche die folgende universelle Eigenschaft hat: Für jeden A-Modul L und jede bilineare Abbildung $f : M \times N \to L$ gibt es genau eine lineare Abbildung $\widetilde{f} : L_0 \to L$, so

dass das folgende Diagramm kommutiert:



Wir zeigen zunächst einmal, dass es bis auf Isomorphie höchstens ein Tensorprodukt geben kann:

Satz 4.1.1 *Sind sowohl (L_0, f_0) und (L_0', f_0') Tensorprodukte zweier A-Moduln M und N, so gibt es genau einen Isomorphismus $\varphi : L_0 \xrightarrow{\sim} L_0'$, so dass das folgende Diagramm kommutiert:*



Beweis. Wegen der universellen Eigenschaft von L_0 gibt es genau eine lineare Abbildung $\varphi : L_0 \to L_0'$ mit $\varphi \circ f_0 = f_0'$. Wegen der universellen Eigenschaft von L_0' gibt es genau eine lineare Abbildung $\psi : L_0' \to L_0$ mit $\psi \circ f_0' = f_0$. Es gilt

$$f_0' = \varphi \circ \psi \circ f_0'.$$

Wenden wir die universelle Eigenschaft von L_0' auf die Abbildung $f_0' : M \times N \to L_0'$ an, so folgt, dass es genau eine Abbildung von $\widetilde{f_0'} : L_0' \to L_0'$ mit $\widetilde{f_0'} \circ f_0' = f_0'$ gibt, nämlich die Identität $\mathrm{Id}_{L_0'}$. Also folgt $\varphi \circ \psi = \mathrm{Id}_{L_0'}$. Entsprechend folgt aus $f_0 = \psi \circ \varphi \circ f_0$, dass $\psi \circ \varphi = \mathrm{Id}_{L_0}$. Also ist φ ein Isomorphismus. □

Satz 4.1.2 *Für je zwei A-Moduln M und N existiert ein Tensorprodukt von M und N.*

Zum Beweis dieses Satzes brauchen wir einige Vorbereitungen. Es sei X eine beliebige Menge. Wir setzen

$$F(X) := \{f : X \to A \,|\, f(x) \neq 0 \text{ für nur endlich viele } x \in X\}.$$

Dies ist ein Modul über dem Ring A. Wir bezeichnen diesen A-Modul als den *freien A-Modul* über der Menge X. Wir erhalten eine *Basis* von $F(X)$ über A durch die Elemente f_x, $x \in X$, mit

$$\begin{array}{rccl} f_x : & X & \longrightarrow & A \\ & y & \longmapsto & \begin{cases} 1 & \text{falls } y = x, \\ 0 & \text{falls } y \neq x. \end{cases} \end{array}$$

Jedes Element $f \in F(X)$ besitzt dann eine eindeutige Darstellung als endliche Linearkombination

$$f = \lambda_1 f_{x_1} + \cdots + \lambda_n f_{x_n}, \quad x_1, \ldots, x_n \in X, \quad \lambda_1, \ldots, \lambda_n \in A.$$

Mittels der Inklusion $X \to F(X)$, $x \mapsto f_x$, kann man X als Teilmenge von $F(X)$ auffassen. Identifiziert man x mit f_x mittels dieser Inklusion, so kann $f \in F(X)$ auch in der folgenden Form schreiben:

$$f = \lambda_1 x_1 + \cdots + \lambda_n x_n, \quad x_1, \ldots, x_n \in X, \quad \lambda_1, \ldots, \lambda_n \in A.$$

Wir benötigen auch das folgende Lemma.

Lemma 4.1.1 *Es seien M und M' A-Moduln, $\varphi : M \to M'$ eine A-lineare Abbildung und N ein Untermodul von M mit $N \subset \operatorname{Ker} \varphi$. Dann gibt es genau eine A-lineare Abbildung $\overline{\varphi} : M/N \to M'$, so dass das folgende Diagramm kommutiert:*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ M/N & & \end{array}$$

Dabei ist π der kanonische Epimorphismus.

Beweis. Falls das Diagramm kommutiert, muss gelten

$$\overline{\varphi}(x + N) = \varphi(x) \text{ für alle } x \in M. \tag{4.1}$$

Dies ergibt die Eindeutigkeit. Wir definieren deshalb $\overline{\varphi}$ durch Gleichung (4.1). Es ist zu zeigen:

(i) $\overline{\varphi}$ ist wohldefiniert.

(ii) $\overline{\varphi}$ ist A-linear.

Dies zeigt man auf bekannte Weise (vgl. den Kern-Bild-Satz). □

Beweis von Satz 4.1.2. Wir betrachten den freien A-Modul $F(M \times N)$ über $M \times N$. Darin betrachten wir den Untermodul Z, der von den folgenden Elementen erzeugt wird:

$$\begin{aligned} &(ax + by, u) - a(x, u) - b(y, u), \quad x, y \in M, u \in N, a, b \in A, \\ &(x, au + bv) - a(x, u) - b(x, v), \quad x \in M, u, v \in N, a, b \in A. \end{aligned}$$

Wir setzen

$$L_0 := F(M \times N)/Z.$$

Es sei $\pi : F(M \times N) \to L_0$ der kanonische Epimorphismus. Wir definieren

$$\begin{array}{rccl} f_0: & M \times N & \longrightarrow & L_0 \\ & (x,u) & \longmapsto & \pi((x,u)) = (x,u) + Z \end{array}$$

Behauptung (L_0, f_0) ist ein Tensorprodukt von M und N.

(i) f_0 ist bilinear: Es gilt

$$f_0(ax + by, u) = af_0(x,u) + bf_0(y,u),$$

da

$$(ax + by, u) - a(x,u) - b(y,u) \in Z.$$

Analog zeigt man die Linearität im zweiten Argument.

(ii) Es sei L ein A-Modul und $f : M \times N \to L$ eine bilineare Abbildung. Wir definieren

$$\widehat{f} : F(M \times N) \to L \text{ durch } \widehat{f}(x,u) = f(x,u) \text{ für alle } (x,u) \in M \times N.$$

Damit ist $\widehat{f}$ also auf der Basis festgelegt und kann auf eindeutige Weise zu einer A-linearen Abbildung $\widehat{f} : F(M \times N) \to L$ fortgesetzt werden. Um Lemma 4.1.1 anwenden zu können, müssen wir $Z \subset \operatorname{Ker} \widehat{f}$ zeigen. Dies folgt, da

$$\begin{aligned} &\widehat{f}((ax + by, u) - a(x,u) - b(y,u)) \\ &= f((ax + by, u) - a(x,u) - b(y,u)) = 0, \end{aligned}$$

wobei benutzt wurde, dass f bilinear ist. Analog folgt dies für das zweite Argument.

Aus Lemma 4.1.1 folgt, dass es eine eindeutig bestimmte Abbildung $\overline{f} : F(M \times N)/Z \to L$ gibt, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} F(M \times N) & \xrightarrow{\widehat{f}} & L \\ {\scriptstyle \pi}\downarrow & \nearrow_{\overline{f}} & \\ F(M \times N)/Z & & \end{array}$$

Es ist zu zeigen, dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & L \\ {\scriptstyle f_0}\downarrow & \nearrow_{\overline{f}} & \\ L_0 & & \end{array}$$

Dies folgt wegen

$$(\overline{f} \circ f_0)(x,u) = \overline{f}(\pi(x,u)) = \widehat{f}(x,u) = f(x,u).$$

Schließlich folgt die Eindeutigkeit von $\overline{f}$ aus der Tatsache, dass $F(M \times N)/Z$ als A-Modul von den Restklassen $(x,u) + Z$ erzeugt wird. □

Notation Wir führen nun die folgende Notation für das Tensorprodukt (L_0, f_0) zweier A-Moduln M und N ein. Wir setzen

$$M \otimes N := L_0, \qquad x \otimes u := f_0(x,u) \quad \text{für } x \in M, u \in N.$$

Wenn zweifelhaft sein könnte, welches der zugrunde liegende Ring ist, schreiben wir auch

$$M \otimes_A N \text{ statt } M \otimes N.$$

Die Bilinearität von f_0 drückt sich nun wie folgt in Formeln aus. Für alle $a, b \in A$, $x, y \in M$, $u, v \in N$ gilt:

$$(ax + by) \otimes u = a(x \otimes u) + b(y \otimes u) \tag{4.2}$$
$$x \otimes (au + bv) = a(x \otimes u) + b(x \otimes v) \tag{4.3}$$

Aus dem Beweis von Satz 4.1.2 folgt, dass sich jedes Element von $M \otimes N$ in der Form

$$\sum_{i=1}^{r} x_i \otimes u_i \quad \text{mit } r \in \mathbb{N}, x_i \in M, u_i \in N$$

schreiben lässt. (Man beachte, dass zwar die Elemente $x \otimes u$ für $x \in M$ und $u \in N$ den A-Modul $M \otimes N$ erzeugen, dass aber nicht jedes Element von dieser Form ist!)

Die universelle Eigenschaft besagt, dass es zu jeder bilinearen Abbildung $f : M \times N \to L$ eine lineare Abbildung $\widetilde{f} : M \otimes N \to L$ gibt mit $\widetilde{f}(x \otimes u) = f(x,u)$ für alle $x \in M$ und $u \in N$.

Bemerkung 4.1.1 Es gilt $0 \otimes u = x \otimes 0 = 0$ für alle $x \in M$ und $u \in N$.

Beweis. $0 \otimes u = (0+0) \otimes u = 0 \otimes u + 0 \otimes u$, also $0 \otimes u = 0$. Analog zeigt man $x \otimes 0 = 0$.

Beispiele 4.1.1 (1) Es seien m und n teilerfremde ganze Zahlen mit $m, n > 1$. Dann ist das Tensorprodukt der $\mathbb{Z}$-Moduln $\mathbb{Z}_n$ und $\mathbb{Z}_m$

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0.$$

Denn für alle $x \in \mathbb{Z}_n$ und $u \in \mathbb{Z}_m$ gilt

$$n(x \otimes u) = (nx) \otimes u = 0 \otimes u = 0 \text{ und } m(x \otimes u) = x \otimes mu = x \otimes 0 = 0.$$

Also ist $x \otimes u = 0$ für alle $x \in \mathbb{Z}_n$ und $u \in \mathbb{Z}_m$. Da $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m$ von Elementen dieses Typs erzeugt wird, folgt $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$.

(2) Für jeden A-Modul M gibt es Isomorphismen

$$\varphi : M \otimes A \xrightarrow{\sim} M \quad \text{und} \quad \psi : A \otimes M \xrightarrow{\sim} M$$

mit $\varphi(x \otimes a) = ax$ und $\psi(a \otimes x) = ax$ für alle $a \in A$ und $x \in M$.

Beweis. Die Existenz der linearen Abbildungen φ und ψ folgt aus der universellen Eigenschaft der Tensorprodukte, angewendet auf die bilinearen Abbildungen

$$M \times A \to M, (x, a) \mapsto ax, \text{ und } A \times M \to M, (a, x) \mapsto ax.$$

Aus (4.2) und (4.3) folgt, dass die Abbildungen

$$\varphi' : \begin{array}{ccc} M & \longrightarrow & M \otimes A \\ x & \longmapsto & x \otimes 1 \end{array} \quad \text{und} \quad \psi' : \begin{array}{ccc} M & \longrightarrow & A \otimes M \\ x & \longmapsto & 1 \otimes x \end{array}$$

linear sind. Aus

$$x \otimes a = a(x \otimes 1) = ax \otimes 1 \quad \text{und} \quad a \otimes x = a(1 \otimes x) = 1 \otimes ax$$

folgt, dass φ' invers zu φ und ψ' invers zu ψ ist.

4.2 Eigenschaften des Tensorprodukts

Satz 4.2.1 *Für je zwei A-Moduln M und N gibt es einen Isomorphismus*

$$\varphi : M \otimes N \xrightarrow{\sim} N \otimes M$$

mit $\varphi(x \otimes u) = u \otimes x$ für alle $x \in M$ und $u \in N$.

Beweis. Die Abbildung $M \times N \to N \otimes M$, $(x, u) \mapsto u \otimes x$, ist bilinear. Nach der universellen Eigenschaft des Tensorprodukts gibt es eine lineare Abbildung φ wie behauptet. Aus Symmetriegründen gibt es eine lineare Abbildung $\psi : N \otimes M \to M \otimes N$ mit $\psi(u \otimes x) = x \otimes u$ für alle $x \in M$ und $u \in N$. Man sieht leicht, dass φ und ψ invers zu einander sind. □

Satz 4.2.2 *Für alle A-Moduln L, M, N gibt es einen Isomorphismus*

$$\varphi : L \otimes (M \otimes N) \xrightarrow{\sim} (L \otimes M) \otimes N$$

mit $\varphi(s \otimes (x \otimes u)) = (s \otimes x) \otimes u$ für alle $s \in L$, $x \in M$, $u \in N$.

Beweis. Es sei $s \in L$. Die Abbildung

$$\begin{array}{rccc} f_s : & M \times N & \longrightarrow & (L \otimes M) \otimes N \\ & (x, u) & \longmapsto & (s \otimes x) \otimes u \end{array}$$

ist nach (4.2) und (4.3) bilinear. Nach der universellen Eigenschaft des Tensorprodukts gibt es genau eine lineare Abbildung

$$\widetilde{f_s} : M \otimes N \to (L \otimes M) \otimes N$$

mit $\widetilde{f_s}(x \otimes u) = (s \otimes x) \otimes u$ für alle $x \in M$, $u \in N$. Die Abbildung

$$\begin{array}{rcl} L \times (M \otimes N) & \to & (L \otimes M) \otimes N \\ (s, x \otimes u) & \mapsto & \widetilde{f_s}(x \otimes u) \end{array}$$

ist bilinear und liefert eine lineare Abbildung φ mit den gewünschten Eigenschaften. □

Satz 4.2.3 *Es seien $f : M \to M'$ und $g : N \to N'$ lineare Abbildungen von A-Moduln. Dann gibt es genau eine lineare Abbildung*

$$f \otimes g : M \otimes N \to M' \otimes N'$$

mit $(f \otimes h)(x \otimes u) = f(x) \otimes g(u)$ für alle $x \in M$, $u \in N$.

Beweis. Wir betrachten die Abbildung

$$\begin{array}{rcl} M \times N & \to & M' \otimes N' \\ (x, u) & \mapsto & f(x) \otimes g(u) \end{array}$$

Da f und g linear sind, ist diese Abbildung bilinear. Die universelle Eigenschaft des Tensorprodukts liefert dann die gewünschte lineare Abbildung $f \otimes g$. □

Bemerkung 4.2.1 Man kann leicht zeigen, dass die Konstruktion von $f \otimes g$ die folgenden Eigenschaften hat:

(i) $\mathrm{Id}_M \otimes \mathrm{Id}_N = \mathrm{Id}_{M \otimes N}$.

(ii) Sind $f' : M' \to M''$ und $g' : N' \to N''$ weitere lineare Abbildungen von A-Moduln, so gilt

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g).$$

Lemma 4.2.1 *Es sei M ein A-Modul und $(N_i)_{i\in I}$ eine Familie von A-Moduln. Dann gibt es einen Isomophismus*

$$\varphi : M \otimes \left(\bigoplus_{i\in I} N_i \right) \xrightarrow{\sim} \bigoplus_{i\in I} (M \otimes N_i)$$

mit $\varphi(x \otimes (u_i)_{i\in I}) = (x \otimes u_i)_{i\in I}$ für alle $x \in M$ und $u_i \in N_i$.

Beweis. Es sei $j \in I$ fest. Anwendung von Satz 4.2.3 auf $f = \mathrm{Id}_M$ und g die Projektion $\bigoplus_{i\in I} N_i \to N_j$ liefert eine lineare Abbildung

$$\begin{array}{rccc} \varphi_j : & M \otimes \left(\bigoplus_{i\in I} N_i\right) & \longrightarrow & M \otimes N_j \\ & x \otimes (u_i)_{i\in I} & \longmapsto & x \otimes u_j \end{array}$$

Diese Abbildungen setzen sich zusammen zu einer linearen Abbildung

$$\begin{array}{rccc} \varphi : & M \otimes \left(\bigoplus_{i\in I} N_i\right) & \longrightarrow & \prod_{i\in I} (M \otimes N_i) \\ & x \otimes (u_i)_{i\in I} & \longmapsto & (x \otimes u_i)_{i\in I} \end{array}$$

Behauptung Diese Abbildung nimmt Werte in

$$\bigoplus_{i\in I} (M \otimes N_i) \subset \prod_{i\in I} (M \otimes N_i)$$

an.

Denn jedes Element in $M \otimes \left(\bigoplus_{i\in I} N_i\right)$ ist von der Form

$$\sum_{j=1}^{r} x_j \otimes \left(\sum_{k=1}^{s_j} u_{j_k} \right) = \sum_{j=1}^{r} \sum_{k=1}^{s_j} x_j \otimes u_{j_k}.$$

Die Abbildung φ bildet solche Elemente nach $\bigoplus_{i\in I} (M \otimes N_i)$ ab.

Die Umkehrabbildung zu φ erhält man wie folgt. Es sei $j \in I$ wieder fest. Wir wenden Satz 4.2.3 auf $f = \mathrm{Id}_M$ und g die Inklusion $N_j \to \bigoplus_{i\in I} N_i$ an und erhalten eine lineare Abbildung

$$\psi_j : M \otimes N_j \to M \otimes \left(\bigoplus_{i\in I} N_i \right)$$

mit $\psi_j(x \otimes u_j) = x \otimes (v_i)_{i \in I}$, wobei

$$v_i := \begin{cases} u_j & \text{für } i = j, \\ 0 & \text{für } i \neq j. \end{cases}$$

Daraus erhalten wir eine Abbildung

$$\psi : \bigoplus_{i \in I} (M \otimes N_i) \to M \otimes \left(\bigoplus_{i \in I} N_i \right)$$

mit $\psi|_{M \otimes N_j} = \psi_j$. Mit rechnet leicht nach, dass ψ invers zu φ ist. □

Lemma 4.2.2 *Es sei N ein A-Modul und $(M_i)_{i \in I}$ eine Familie von A-Moduln. Dann gibt es einen Isomophismus*

$$\varphi : \left(\bigoplus_{i \in I} M_i \right) \otimes N \xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes N)$$

mit $\varphi((x_i)_{i \in I} \otimes u) = (x_i \otimes u)_{i \in I}$ für alle $x_i \in M_i$ und $u \in N$.

Beweis. Der Beweis verläuft entweder analog zu dem Beweis von Lemma 4.2.1 und man benutzt Satz 4.2.1. □

Lemma 4.2.3 *Es sei M ein A-Modul und N ein freier A-Modul mit Basis $(u_j)_{j \in J}$. Dann hat jedes Element von $M \otimes N$ eine eindeutige Darstellung der Form*

$$\sum_{j \in J} x_j \otimes u_j$$

mit $x_j \in M$, $x_j = 0$ für fast alle $j \in J$.

Beweis. Es sei zunächst $|J| = 1$, also $\{u_0\}$ eine Basis von N. Dann kann jedes Element von $M \otimes N$ in der Form

$$\sum_{j=1}^{r} x_j \otimes a_j u_0 = \left(\sum_{j=1}^{r} a_j x_j \right) \otimes u_0$$

mit $x_j \in M$, $a_j \in A$ geschrieben werden. Also ist jedes Element von $M \otimes N$ von der Form $x \otimes u_0$ für ein $x \in M$.

Nun kann man wie bei Beispiel 4.1.1(2) zeigen, dass es einen Isomorphismus

$$\varphi : M \otimes N \xrightarrow{\sim} M$$

mit $\varphi(x \otimes a u_0) = ax$ gibt. Daraus folgt die Eindeutigkeit der Darstellung.

Im allgemeinen Fall gilt

$$N = \bigoplus_{j \in J} Au_j.$$

Die Behauptung folgt dann aus Lemma 4.2.1. □

Satz 4.2.4 *Sind M und N freie A-Moduln, so ist auch $M \otimes N$ frei. Ist $(x_i)_{i \in I}$ eine Basis von M und $(u_j)_{j \in J}$ eine Basis von N, so ist*

$$(x_i \otimes u_j)_{(i,j) \in I \times J}$$

eine Basis von $M \otimes N$.

Beweis. Dies folgt direkt aus Lemma 4.2.3. □

Korollar 4.2.1 *Ist M ein freier A-Modul vom Rang m und N ein freier A-Modul vom Rang n, so ist $M \otimes N$ eine freier A-Modul vom Rang mn.*

Beispiel 4.2.1 Ist $M = A^m$ und $N = A^n$ mit Standardbasen $e_1, \dots e_m$ und $e'_1, \dots, e'_n$, so besitzt jedes Element von $M \otimes N$ eine eindeutige Darstellung der Form

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} e_i \otimes e'_j, \quad \text{mit } a_{ij} \in A.$$

Es sei M ein A-Modul. Wir erinnern an den Begriff des dualen Moduls

$$M^* = \mathrm{Hom}_A(M, A).$$

Satz 4.2.5 *Für alle A-Moduln M und N gibt es einen Homomorphismus von A-Moduln*

$$\mu : M^* \otimes N \longrightarrow \mathrm{Hom}_A(M, N)$$

mit $\mu(f \otimes u)(x) = f(x)u$ für alle $f \in M^*$, $u \in N$ und $x \in M$. Ist M frei von endlichem Rang, so ist μ ein Isomorphismus.

Beweis. Die Abbildung

$$\varphi : M^* \times N \to \mathrm{Hom}_A(M, N)$$

mit $\varphi(f, u)(x) = f(x)u$ für alle $f \in M^*$, $u \in N$ und $x \in M$ ist bilinear. Nach der universellen Eigenschaft des Tensorprodukts existiert ein Homomorphismus μ mit der angegebenen Eigenschaft.

Es sei $x_1, \ldots, x_m$ eine Basis von M und $x_1^*, \ldots, x_m^*$ die duale Basis. (Sie ist charakterisiert durch

$$x_i^*(x_j) = \delta_{ij} \text{ für } i, j \in \{1, \ldots, m\}.)$$

Wir definieren eine Abbildung

$$\mu' : \mathrm{Hom}_A(M, N) \to M^* \otimes N$$

durch

$$F \mapsto \sum_{i=1}^{m} x_i^* \otimes F(x_i).$$

Es ist klar, dass diese Abbildung A-linear ist. Wegen

$$\begin{aligned} (\mu' \circ \mu)(x_j^* \otimes u) &= \sum_{i=1}^{m} x_i^* \otimes x_j^*(x_i)u = \sum_{i=1}^{m} x_i^* \otimes \delta_{ji} u = x_j^* \otimes u, \\ (\mu \circ \mu')(F)(x_j) &= \sum_{i=1}^{m} x_i^*(x_j) F(x_i) = \sum_{i=1}^{m} \delta_{ij} F(x_i) = F(x_j) \end{aligned}$$

für $j = 1, \ldots, m$ folgt, dass μ' invers zu μ ist. □

Satz 4.2.6 *Es sei*

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

eine kurze exakte Sequenz von A-Moduln. Dann ist für jeden A-Modul N die Sequenz

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

mit $f' = f \otimes \mathrm{Id}_N$ und $g' = g \otimes \mathrm{Id}_N$ exakt.

Beweis. (a) g' ist surjektiv: Es sei $x'' \in M''$ und $u \in N$. Da g surjektiv ist, gibt es $x \in M$ mit $g(x) = x''$. Dann folgt $g'(x \otimes u) = x'' \otimes u$. Da die Elemente $x'' \otimes u$ den Modul $M'' \otimes N$ erzeugen, folgt die Surjektivität von g'.

(b) $\mathrm{Im}\, f' \subset \mathrm{Ker}\, g'$: Aus $g \circ f = 0$ folgt $g' \circ f' = (g \circ f) \otimes (\mathrm{Id}_N \circ \mathrm{Id}_N) = 0$, also $\mathrm{Im}\, f' \subset \mathrm{Ker}\, g'$.

(c) $\mathrm{Ker}\, g' \subset \mathrm{Im}\, f'$: Es sei $L := \mathrm{Im}\, f'$. Nach Lemma 4.1.1 haben wir eine kanonische Abbildung

$$\overline{g}' : (M \otimes N)/L \to M'' \otimes N.$$

Wir definieren eine lineare Abbildung

$$\widetilde{h} : M'' \otimes N \to (M \otimes N)/L,$$

so dass $\widetilde{h} \circ \overline{g}' = \mathrm{Id}$. Daraus folgt, dass $\overline{g}'$ injektiv ist, also die Inklusion $\mathrm{Ker}\, g' \subset \mathrm{Im}\, f'$.

Es sei $x'' \in M$ und $u \in N$. Es sei $x \in M$ mit $g(x) = x''$. Wir definieren eine Abbildung

$$\begin{array}{rccc} h: & M'' \times N & \longrightarrow & (M \otimes N)/L \\ & (x'', u) & \longmapsto & x \otimes u + L \end{array}$$

Diese Abbildung ist wohl definiert: Sind $x_1, x_2 \in M$ mit $g(x_1) = g(x_2) = x''$, so folgt $x_1 - x_2 \in \mathrm{Ker}\, g$, also $x_1 - x_2 \in \mathrm{Im}\, f$. Also gibt es ein $x' \in M'$ mit $f(x') = x_1 - x_2$. Dann gilt

$$x_1 \otimes u - x_2 \otimes u = (x_1 - x_2) \otimes u = f(x') \otimes u.$$

Daraus folgt

$$x_1 \otimes u \equiv x_2 \otimes u \bmod L.$$

Deshalb ist die Abbildung h wohl definiert. Sie ist bilinear. Aus der universellen Eigenschaft des Tensorprodukts folgt die Existenz der Abbildung $\widetilde{h}$. Es gilt

$$(\widetilde{h} \circ \overline{g}')(x \otimes u + L) = \widetilde{h}(g(x) \otimes u) = x \otimes u + L.$$

Also ist die Einschränkung von $\widetilde{h} \circ \overline{g}'$ auf Restklassen von Elementen der Form $x \otimes u$ die Identität. Da diese Elemente den Modul $M \otimes N$ erzeugen, folgt $\widetilde{h} \circ \overline{g}' = \mathrm{Id}$, was zu zeigen war. □

Warnung Es ist nicht immer wahr, dass die Sequenz

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

exakt ist, siehe Beispiel 4.2.2. Sie ist aber exakt, wenn die Sequenz

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

spaltet. Denn wenn $\sigma : M \to M'$ mit $\sigma \circ f = \mathrm{Id}_{M'}$ existiert, so gilt

$$(\sigma \otimes \mathrm{Id}_N) \circ (f \otimes \mathrm{Id}_N) = (\sigma \circ f) \otimes (\mathrm{Id}_N \circ \mathrm{Id}_N) = \mathrm{Id}_{M'} \otimes \mathrm{Id}_N = \mathrm{Id}_{M' \otimes N}\,.$$

Also ist $f' = f \otimes \mathrm{Id}_N$ injektiv.

Beispiel 4.2.2 Wir betrachten die kurze exakte Sequenz von $\mathbb{Z}$-Moduln

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

wobei $f : \mathbb{Z} \to \mathbb{Z}$ die Abbildung mit $f(x) = 2x$ und $g : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ die kanonische Abbildung ist. Dann ist die Abbildung $f' : \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ die Nullabbildung, also nicht injektiv, denn es gilt

$$f'(x \otimes [1]) = (2x) \otimes [1] = x \otimes 2[1] = x \otimes 0 = 0$$

für alle $x \in \mathbb{Z}$, wobei $[1]$ die Restklasse von 1 in $\mathbb{Z}/2\mathbb{Z}$ ist, während

$$\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \neq 0.$$

Satz 4.2.7 *Ist I ein Ideal von A, so haben wir für jeden A-Modul M einen Isomorphismus*

$$(A/I) \otimes M \xrightarrow{\sim} M/IM$$

mit $(a + I) \otimes x \mapsto ax + IM$.

Beweis. Wir wenden Satz 4.2.6 auf die kurze exakte Sequenz

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

mit der Inklusion und der kanonischen Abbildung an und erhalten eine exakte Sequenz

$$I \otimes M \xrightarrow{\varphi} A \otimes M \longrightarrow (A/I) \otimes M \longrightarrow 0.$$

Nach Beispiel 4.1.1(2) haben wir einen Isomorphismus

$$\psi : A \otimes M \xrightarrow{\sim} M$$

mit $a \otimes x \mapsto ax$. Dann folgt

$$(A/I) \otimes M \cong A \otimes M/\varphi(I \otimes M) \cong M/(\psi \circ \varphi)(I \otimes M)$$

und $(\psi \circ \varphi)(I \otimes M) = IM$. □

Beispiel 4.2.3 Für alle $n \in \mathbb{Z}$ und alle $\mathbb{Z}$-Moduln M folgt aus Satz 4.2.7:

$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} M \cong M/nM.$$

4.3 Erweiterung des Grundrings

Es sei nun B ein kommutativer Ring, der A als Unterring enthält. Es sei M ein A-Modul.

Für alle $b \in B$ ist die Multiplikation mit b eine A-lineare Abbildung

$$\begin{array}{rccc} \ell_b : & B & \longrightarrow & B \\ & c & \longmapsto & bc \end{array}$$

Nach Satz 4.2.3 erhalten wir eine lineare Abbildung

$$\mathrm{Id}_M \otimes \ell_b : M \otimes_A B \to M \otimes_A B.$$

Wir können nun $M \otimes_A B$ zu einem B-Modul machen, wenn wir

$$b(x \otimes c) = (\mathrm{Id}_M \otimes \ell_b)(x \otimes c) = x \otimes bc \text{ für alle } b, c \in B, x \in M$$

setzen.

Beispiel 4.3.1 Im Spezialfall $M = A$ ist der Isomorphismus $A \otimes_A B \xrightarrow{\sim} B$ mit $a \otimes c \mapsto ac$ nach Beispiel 4.1.1(2) nun ein Isomorphismus von B-Moduln.

Satz 4.3.1 *Es sei M ein freier A-Modul mit Basis $(v_i)_{i \in I}$. Dann ist $M \otimes_A B$ ein freier B-Modul mit Basis $(v_i \otimes 1)_{i \in I}$.*

Beweis. Nach Voraussetzung ist $M = \bigoplus_{i \in I} Av_i$. Für jedes $i \in I$ ist die Abbildung $A \xrightarrow{\sim} Av_i$, $a \mapsto av_i$, ein Isomorphismus von A-Moduln. Nach Lemma 4.2.2 erhalten wir einen Isomorphismus von A-Moduln

$$M \otimes_A B \xrightarrow{\sim} \bigoplus_{i \in I} Av_i \otimes_A B.$$

Dies ist auch ein Isomorphismus von B-Moduln. Außerdem ist für jedes $i \in I$ die Abbildung

$$B \xrightarrow{\sim} A \otimes_A B \xrightarrow{\sim} Av_i \otimes_A B, \quad b \mapsto 1 \otimes b \mapsto v_i \otimes b = b(v_i \otimes 1)$$

ein Isomorphismus von B-Moduln. □

4.4 Tensorprodukte von Algebren

Es sei A ein kommutativer Ring. Wir können das Tensorprodukt auch auf zwei A-Algebren R und S anwenden. Das Tensorprodukt ist dann in natürlicher Weise wieder eine A-Algebra.

Satz 4.4.1 *Es seien R, S zwei A-Algebren. Dann gibt es auf $R \otimes_A S$ genau eine Multiplikation, die $R \otimes_A S$ zu einer A-Algebra macht und so dass*

$$(x \otimes u)(y \otimes v) = xy \otimes uv \tag{4.4}$$

für alle $x, y \in R$ und $u, v \in S$ gilt.

Beweis. Für alle $y \in R$ und $v \in S$ ist die Abbildung

$$r_y : \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & xy \end{array} \quad \text{bzw.} \quad r_v : \begin{array}{ccc} S & \longrightarrow & S \\ u & \longmapsto & uv \end{array}$$

A-linear. Nach Satz 4.2.3 gibt es deshalb eine A-lineare Abbildung

$$r_{(y,v)} : R \otimes_A S \to R \otimes_A S \text{ mit } x \otimes u \mapsto xy \otimes uv$$

für alle $x \in R$ und $u \in S$. Nun betrachtet man für ein festes $t \in R \otimes_A S$ die Abbildung

$$\ell'_t : R \times S \to R \otimes_A S \text{ mit } (y, v) \mapsto r_{(y,v)}(t).$$

Man rechnet leicht nach, dass diese Abbildung bilinear ist. Nach der universellen Eigenschaft des Tensorprodukts gibt es also eine lineare Abbildung

$$\ell_t : R \otimes_A S \to R \otimes_A S \text{ mit } y \otimes v \mapsto r_{(y,v)}(t).$$

Man definiert nun die Multiplikation auf $R \otimes_A S$ durch

$$t \cdot t' := \ell_{t'}(t).$$

Dann gilt nach Konstruktion (4.4). Es ist leicht nachzuprüfen, dass $R \otimes_A S$ mit dieser Multiplikation eine A-Algebra wird. □

Bemerkung 4.4.1 Man nennt $R \otimes_A S$ mit der Algebrastruktur (4.4) das *Tensorprodukt der A-Algebren R und S*. Dieses Objekt hat die folgende universelle Eigenschaft: Für jede A-Algebra T und für alle Homomorphismen $f : R \to T$ und $g : S \to T$ von A-Algebren mit $f(x)g(u) = g(u)f(x)$ für alle $x \in R$ und $u \in S$ gibt es genau einen Homomorphismus $\varphi : R \otimes_A S \to T$ von A-Algebren mit $\varphi(x \otimes u) = f(x)g(u)$ für alle $x \in R$, $u \in S$.

Beispiel 4.4.1 Es sei R ein beliebiger Ring. Es sei $M_n(R)$ der Ring aller $n \times n$-Matrizen mit Einträgen in R. Es sei $E_{ij} \in M_n(R)$ $(1 \leq i, j \leq n)$ die Matrix mit 1 an der Stelle (i, j) und 0 sonst. Dann ist $M_n(R)$ ein freier R-Modul vom Rang n^2 mit Basis $(E_{ij})_{1 \leq i,j \leq n}$. Es gilt

$$E_{ij}E_{kl} = \delta_{jk}E_{il} \text{ für alle } i, j, k, l \text{ mit } 1 \leq i, j, k, l \leq n.$$

Für einen kommutativen Ring A ist $M_n(A)$ eine A-Algebra.

Wir haben nun für alle A-Algebren R und alle n einen Isomorphismus

$$R \otimes_A M_n(A) \xrightarrow{\sim} M_n(R). \tag{4.5}$$

Beweis. Nach Lemma 4.2.3 lässt sich jedes Element von $R \otimes_A M_n(A)$ eindeutig in der Form

$$\sum_{i,j} x_{ij} \otimes E_{ij} \text{ mit } x_{ij} \in R$$

schreiben. Wir definieren nun eine Abbildung (4.5) wie folgt:

$$\sum_{i,j} x_{ij} \otimes E_{ij} \mapsto \sum_{i,j} x_{ij} E_{ij},$$

wobei E_{ij} nun als Matrix aufgefasst wird. Man kann leicht zeigen, dass diese Abbildung ein Isomorphismus von A-Moduln ist, der mit der Multiplikation verträglich ist.

4.5 Mehrfache Tensorprodukte

Es sei A ein kommutativer Ring und $M_1, \ldots, M_p$ und N A-Moduln.

Definition Eine Abbildung

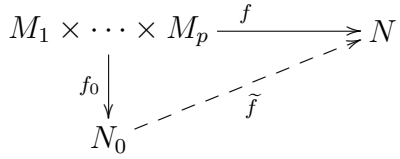
$$f : M_1 \times \cdots \times M_p \to N$$

heißt *p-(multi)linear*, falls für jedes $i = 1, \ldots, p$ gilt

$$\begin{aligned} & f(x_1, \ldots, x_{i-1}, ax_i + bx_i', x_{i+1}, \ldots, x_p) \\ &= af(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_p) + bf(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_p) \end{aligned}$$

für $x_i, x_i' \in M_i$, $a, b \in A$.

Definition Ein *Tensorprodukt* der A-Moduln $M_1, \ldots, M_p$ ist ein A-Modul N_0 mit einer p-linearen Abbildung $f_0 : M_1 \times \cdots \times M_p \to N_0$, welche die folgende universelle Eigenschaft hat: Für jeden A-Modul N und jede p-lineare Abbildung $f : M_1 \times \cdots \times M_p \to N$ gibt es genau eine lineare Abbildung $\widetilde{f} : N_0 \to N$, so dass das folgende Diagramm kommutiert:



Wie im Fall $p = 2$ zeigt man:

Satz 4.5.1 *Es gibt bis auf Isomorphie genau ein Tensorprodukt von $M_1, \ldots, M_p$.*

Notation Wir setzen

$$\begin{aligned} M_1 \otimes \cdots \otimes M_p &:= N_0, \\ x_1 \otimes \cdots \otimes x_p &:= f_0(x_1, \ldots, x_p) \text{ für } x_i \in M_i, i = 1, \ldots, p. \end{aligned}$$

Wie Satz 4.2.2 beweist man:

Satz 4.5.2 *Es seien $p, q \in \mathbb{N}$, $p, q > 0$ und $M_1, \ldots, M_{p+q}$ A-Moduln. Dann gibt es einen kanonischen Isomorphismus*

$$\varphi : (M_1 \otimes \cdots \otimes M_p) \otimes (M_{p+1} \otimes \cdots \otimes M_{p+q}) \xrightarrow{\sim} M_1 \otimes \cdots \otimes M_{p+q}$$

mit

$$\varphi((x_1 \otimes \cdots \otimes x_p) \otimes (x_{p+1} \otimes \cdots \otimes x_{p+q})) = x_1 \otimes \cdots \otimes x_{p+q}$$

für $x_i \in M_i$, $i = 1, \ldots, p+q$.

Es sei K ein Körper. In Lineare Algebra II hatten wir für K-Vektorräume $V_1, \ldots, V_p$ und W den Vektorraum

$$\mathrm{Hom}(V_1, \ldots, V_p; W)$$

aller p-linearen Abbildungen $f : V_1 \times \ldots, \times V_p \to W$ eingeführt. Es gilt nun

$$\mathrm{Hom}(V_1, \ldots, V_p; W) \cong \mathrm{Hom}_K(V_1 \otimes \ldots \otimes V_p; W),$$

d.h. jeder p-linearen Abbildung $f : V_1, \ldots, V_p \to W$ entspricht eine lineare Abbildung $\widetilde{f} : V_1 \otimes \ldots \otimes V_p \to W$ des Tensorprodukts. Insbesondere gilt für einen K-Vektorraum V

$$T^p(V) = \mathrm{Hom}(\underbrace{V, \ldots, V}_{p}; K) \cong \mathrm{Hom}(\underbrace{V \otimes \cdots \otimes V}_{p}; K).$$

Satz 12.2 aus Lineare Algebra I können wir jetzt so interpretieren:

$$T^p(V) \cong \underbrace{V^* \otimes \cdots \otimes V^*}_{p}.$$

4.6 Tensoralgebra

Notation Es sei M ein A-Modul. Für $p \geq 2$ setzen wir

$$\otimes^p M := \underbrace{M \otimes \cdots \otimes M}_{p}.$$

Ferner sei

$$\otimes^0 M := A, \quad \otimes^1 M := M.$$

Definition (a) Die Elemente von $\otimes^p M$ heißen *Tensoren der Stufe p.*

(b) Ein Tensor $x \in \otimes^p M$ heißt *zerlegbar*, falls es eine Darstellung

$$x = x_1 \otimes \cdots \otimes x_p$$

gibt.

Warnung Man beachte, dass nicht alle Elemente von $\otimes^p M$ von der Form $x = x_1 \otimes \cdots \otimes x_p$, also zerlegbar sind, sondern $\otimes^p M$ wird nur von solchen Elementen erzeugt!

Aus Satz 4.2.4 folgt:

Satz 4.6.1 *Es sei M ein freier A-Modul mit Basis $v_1, \ldots, v_n$. Dann bilden die Elemente*

$$v_{i_1} \otimes \cdots \otimes v_{i_p}, \quad 1 \leq i_1, \ldots, i_p \leq n,$$

eine Basis von $\otimes^p M$. Insbesondere hat $\otimes^p M$ den Rang n^p.

Es sei M ein A-Modul. Wir betrachten die direkte Summe

$$\otimes M := \bigoplus_{p \geq 0} \otimes^p M.$$

Dies ist ein A-Modul. Ein Element $x \in \otimes M$ lässt sich schreiben als

$$x = (x_p)_{p \in \mathbb{N}} = \sum_{p \geq 0} x_p, \quad x_p \in \otimes^p M \text{ (fast alle } x_p = 0).$$

Wir führen auf $\otimes M$ eine Multiplikation ein. Nach Satz 4.5.2 gibt es einen Isomorphismus

$$\varphi : (\otimes^p M) \otimes (\otimes^q M) \xrightarrow{\sim} \otimes^{p+q} M$$

mit

$$\varphi((x_1 \otimes \cdots \otimes x_p) \otimes (x_{p+1} \otimes \cdots \otimes x_{p+q})) = x_1 \otimes \cdots \otimes x_{p+q}.$$

Das bedeutet: Sind $x \in \otimes^p M$ und $y \in \otimes^q M$, so kann man $x \otimes y$ als Element von $\otimes^{p+q} M$ auffassen. Es sei

$$x = \sum_{p \geq 0} x_p, y = \sum_{p \geq 0} y_p \in \otimes M.$$

Dann definieren wir das Produkt von x und y wie folgt:

$$x \cdot y := \sum_{p \geq 0} \left(\sum_{r+s=p} (x_r \cdot y_s) \right), \text{ wobei } x_r \cdot y_s := x_r \otimes y_s \in \otimes^{r+s} M.$$

Dann wird $\otimes M$ mit dieser Multiplikation zu einer A-Algebra.

Definition Die A-Algebra $\otimes M$ heißt die *Tensoralgebra* von M.

Diese Algebra ist eine *graduierte Algebra*. Es gilt

$$\otimes M = \bigoplus_{p \geq 0} \otimes^p M$$

und die Multiplikation ist eine Abbildung

$$\begin{array}{rcl} \otimes^p M \times \otimes^q M & \to & \otimes^{p+q} M \\ (x_p, x_q) & \mapsto & x_p \cdot x_q \end{array}.$$

Die Elemente von $\otimes^p M$ heißen *homogen vom Grad p*. Es gilt

$$\otimes^0 = A.$$

Ist V ein K-Vektorraum, so gilt mit den neuen Bezeichnungen für den K-Vektorraum $T^p(V)$ aus Lineare Algebra II:

$$T^p(V) = \otimes^p V^*.$$

Satz 4.6.1 stimmt dann mit Satz 12.2 aus Lineare Algebra II überein. Das in Lineare Algebra II eingeführte Tensorprodukt entspricht der Multiplikation auf der Tensoralgebra $\otimes V^*$.

4.7 Äußere Algebra

Es sei M wieder ein A-Modul.

Definition Es sei $N^p(M) \subset \otimes^p M$ der Untermodul, der von den Elementen

$$x_1 \otimes \cdots \otimes x_p \text{ mit } x_i = x_j \text{ für } 1 \leq i \neq j \leq p$$

erzeugt wird. Wir definieren

$$\bigwedge^p M := (\otimes^p M)/N^p(M).$$

Notation Die Restklasse eines Elements $x_1 \otimes \cdots x_p \in \otimes^p M$ in $\bigwedge^p M$ schreiben wir

$$x_1 \wedge \cdots \wedge x_p \in \bigwedge^p M.$$

Bemerkung 4.7.1 Man kann $\bigwedge^p M$ auch durch eine universelle Eigenschaft in Analogie zum Tensorprodukt definieren: Ist N ein A-Modul und $f : \underbrace{M \times \cdots \times M}_{p} \to N$ eine *alternierende* p-lineare Abbildung, so gibt es genau eine lineare Abbildung $\widetilde{f} : \bigwedge^p M \to N$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} M \times \cdots \times M & \xrightarrow{f} & N \\ {\scriptstyle f_0}\downarrow & \nearrow_{\widetilde{f}} & \\ \bigwedge^p M & & \end{array}$$

Man nennt $\bigwedge^p M$ das p-fache *äußere Produkt* von M.

Es sei

$$\bigwedge M = \bigoplus_{p \geq 0} \bigwedge^p M.$$

Wir werden auf $\bigwedge M$ eine Multiplikation erklären: Dazu sei

$$N(M) = \bigoplus_{p \geq 0} N^p(M).$$

Wir behaupten, dass $N(M)$ ein Ideal der A-Algebra $\otimes M$ ist. Ist $x_1 \otimes \cdots \otimes x_p \in \otimes^p M$ ein Element von $N^p(M)$, so gilt für ein beliebiges Element $y_1 \otimes \cdots \otimes y_q \in \otimes^q M$

$$\begin{aligned} &(x_1 \otimes \cdots \otimes x_p) \cdot (y_1 \otimes \cdots \otimes y_q) \\ &= \quad x_1 \otimes \cdots \otimes x_p \otimes y_1 \otimes \cdots \otimes y_q \in N^{p+q}(M), \end{aligned}$$

da $x_i = x_j$ für ein Paar (i, j) mit $i \neq j$. Also ist $N(M)$ ein Ideal in $\otimes M$. Damit wird

$$\bigwedge M := (\otimes M)/N(M)$$

eine A-Algebra. Die Multiplikation von homogenen Elementen wird gegeben durch die Formel

$$(x_1 \wedge \cdots \wedge x_p) \cdot (y_1 \wedge \cdots \wedge y_q) := x_1 \wedge \cdots \wedge x_p \wedge y_1 \wedge \cdots \wedge y_q.$$

Definition Die A-Algebra $\bigwedge M$ heißt die *äußere Algebra* von M.

Satz 4.7.1 *Es sei M ein freier A-Modul mit Basis $v_1, \ldots, v_n$. Dann gilt $\bigwedge^p M = 0$ für $p > n$. Für $1 \leq p \leq n$ bilden die Elemente*

$$v_{i_1} \wedge \cdots \wedge v_{i_p}, \quad 1 \leq i_1 < \cdots < i_p \leq n,$$

eine Basis von $\bigwedge^p M$. Insbesondere hat $\bigwedge^p M$ den Rang

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}.$$

Wir vergleichen diese Resultate mit den entsprechenden aus Lineare Algebra II. Es sei V ein K-Vektorraum. Dann gilt

$$\bigwedge^p(V) \text{ (nach Lineare Algebra II)} = \bigwedge^p V^* \text{ (hier)} .$$

Satz 4.7.1 entspricht Satz 13.4 aus Lineare Algebra II.

4.8 Symmetrische Algebra

Es sei M wieder ein A-Modul. Mit S_p bezeichnen wir wieder die symmetrische Gruppe in p Symbolen.

Definition Es sei $L^p(M) \subset \otimes^p M$ der Untermodul, der von den Elementen

$$x_1 \otimes \cdots \otimes x_p - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(p)}$$

für alle $x_i \in M$ und $\sigma \in S_p$ erzeugt wird. Wir definieren

$$S^p(M) := (\otimes^p M)/L^p(M).$$

Notation Die Restklasse eines Elements $x_1 \otimes \cdots x_p \in \otimes^p M$ in $S^p(M)$ schreiben wir

$$x_1 \vee \cdots \vee x_p \in S^p(M).$$

Es sei

$$S(M) := \bigoplus_{p \geq 0} S^p(M).$$

Es ist leicht zu sehen, dass

$$L(M) := \bigoplus_{p \geq 0} L^p(M)$$

ein Ideal in $S(M)$ ist. Also ist $S(M)$ wieder eine A-Algebra.

Definition Die Algebra $S(M)$ heißt die *symmetrische Algebra* von M.

Wir vergleichen diese Resultate wieder mit den entsprechenden aus Lineare Algebra II. Es sei V ein K-Vektorraum. Dann gilt

$$S^p(V) \text{ (nach Lineare Algebra II)} = S^p(V^*) \text{ (hier)} .$$

Satz 14.4 aus Lineare Algebra II lässt sich zu dem folgenden Satz verallgemeinern:

Satz 4.8.1 *Es sei K ein Körper und V ein K-Vektorraum der Dimension n mit Basis $v_1, \ldots, v_n$. Fasst man diese Elemente als Elemente von $S^1(V)$ auf, so sind sie algebraisch unabhängig über K. Die K-Algebra $S(V)$ ist isomorph zu der Polynomalgebra $K[x_1, \ldots, x_n]$ in n Variablen über K.*

Beweis. Es sei $K^p[x_1, \ldots, x_n]$ der Vektorraum der homogenen Polynome in den Variablen $x_1, \ldots, x_n$ vom Grad p. Wir definieren

$$\Psi^p : S^p(V) \to K^p[x_1, \ldots, x_n]$$

durch

$$v_{i_1} \vee \cdots \vee v_{i_p} \mapsto x_{i_1} \cdots x_{i_p}, \quad 1 \leq i_1 \leq \ldots \leq i_p \leq n.$$

Da die $v_{i_1} \vee \cdots \vee v_{i_p}$ eine Basis von $S^p(V)$ und die Monome $x_{i_1} \cdots x_{i_p}$ eine Basis von $K^p[x_1, \ldots, x_n]$ bilden, folgt, dass sich Ψ^p zu einem Isomorphismus zwischen $S^p(V)$ und $K^p[x_1, \ldots, x_n]$ erweitern lässt. Der Multiplikation in $S(V)$ entspricht die Multiplikation von Polynomen in $K[x_1, \ldots, x_n]$. Durch die Abbildung $\Psi^p : S^p(V) \to K^p[x_1, \ldots, x_n]$ wird also ein K-Algebrahomomorphismus von $S(E)$ nach $K[x_1, \ldots, x_n]$ induziert. □

Kapitel 5

Halbeinfache Moduln

5.1 Matrizen und lineare Abbildungen über nicht kommutativen Ringen

Im Folgenden sei R stets ein Ring (mit 1).

Definition Ein Ring mit $1 \neq 0$, in dem jedes von Null verschiedene Element ein multiplikatives Inverses besitzt, heißt *Divisionsring* oder *Schiefkörper*.

Satz 5.1.1 *Es sei R ein Divisionsring. Dann ist jeder R-Modul $M \neq 0$ frei. Ist M endlich erzeugt, so haben je zwei Basen gleich viele Elemente.*

Beweis. Der Beweis ist der ersten Aussage ist der gleiche wie bei Satz 2.4.1, da dort die Kommutativität von K nicht benutzt wurde. Da ein Divisionsring R offensichtlich noethersch ist ($\{0\}$ und R sind die einzigen Ideale von R), folgt die zweite Aussage aus Satz 2.6.6. □

Wir haben bereits den Ring $M_n(R)$ der $n \times n$-Matrizen mit Einträgen in R betrachtet. Ist R ein Divisionsring, so können wir linearen Abbildungen von R-Moduln wie im Fall von Vektorräumen Matrizen zuordnen. Wir betrachten aber nun eine etwas allgemeinere Situation.

Es seien

$$M = M_1 \oplus \cdots \oplus M_n, \qquad N = N_1 \oplus \cdots \oplus N_m$$

R-Moduln, die als direkte Summe von Untermoduln dargestellt werden können. Wir möchten R-Modulhomomorphismen von M nach N beschreiben.

Wir betrachten zunächst den Fall $N = N_1$. Es sei

$$\varphi : M_1 \oplus \cdots \oplus M_n \to N$$

ein R-Modulhomomorphismus. Jedes Element $x \in M$ hat eine eindeutige Darstellung

$$x = x_1 + \cdots + x_n, \quad x_j \in M_j, j = 1, \ldots, n.$$

Also können wir x als Spaltenvektor

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

auffassen. Es sei $\varphi_j : M_j \to N$ die Einschränkung von φ auf den Summand M_j. Dann können wir φ den Zeilenvektor

$$\varphi = (\varphi_1, \ldots, \varphi_n), \quad \varphi_j \in \mathrm{Hom}_R(M_j, N)$$

zuordnen und es gilt

$$\varphi(x) = (\varphi_1, \ldots, \varphi_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Nun betrachten wir den allgemeinen Fall. Es sei

$$\varphi : M_1 \oplus \cdots \oplus M_n \to N_1 \oplus \cdots \oplus N_m$$

ein R-Modulhomomorphismus. Es sei $p_i : N_1 \oplus \cdots \oplus N_m \to N_i$ die Projektion auf den i-ten Summanden. Dann können wir die vorangehenden Bemerkungen auf die Abbildungen $p_i \circ \varphi_j$ für jedes $i = 1, \ldots, m$ anwenden. Danach existieren eindeutig bestimmte Elemente $\varphi_{ij} \in \mathrm{Hom}_R(M_j, N_i)$, so dass φ eine Matrixdarstellung

$$M(\varphi) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$$

hat, so dass

$$\varphi(x) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Haben wir umgekehrt eine Matrix (φ_{ij}) mit $\varphi_{ij} \in \mathrm{Hom}_R(M_j, N_i)$ gegeben, so können wir mit Hilfe dieser Matrix ein Element von $\mathrm{Hom}_R(M, N)$ definieren.

Wir haben damit bewiesen:

Satz 5.1.2 *Es sei M ein R-Modul und $A := \mathrm{End}_R(M)$. Dann existiert ein Ringisomorphismus*

$$\mathrm{End}_R(M^n) \xrightarrow{\sim} M_n(A),$$

der jedem $\varphi \in \mathrm{End}_R(M^n)$ die Matrix

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & \ddots & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix}$$

wie oben zuordnet, so dass $M_n(A)$ von links auf M^n operiert, wobei wir die Elemente von M^n als Spaltenvektoren auffassen.

Korollar 5.1.1 *Es sei D ein Divisionsring. Dann haben wir einen Isomorphismus*

$$\mathrm{End}_D(D) \xrightarrow{\sim} D^{\mathrm{op}}.$$

Beweis. Es sei M ein D-Modul vom Rang 1 mit Basis $\{v\}$. Für jedes $a \in D$ existiert eine eindeutig bestimmte D-lineare Abbildung $f_a : M \to M$ mit $f_a(v) = av$. Dann gilt

$$f_a f_b(v) = f_a(bv) = bf_a(v) = bav = f_{ba}(v).$$

Wenden wir dies auf $M = D$ an, so folgt, dass der Isomorphismus von Satz 5.1.2 einen Isomorphismus

$$\mathrm{End}_D(D) \xrightarrow{\sim} M_1(\mathrm{End}_D(D)) \cong D^{\mathrm{op}}$$

induziert. □

5.2 Einfache und halbeinfache Moduln

Es sei R wieder ein Ring.

Definition Ein R-Modul M heißt *einfach*, wenn $M \neq \{0\}$ ist und wenn $\{0\}$ und M die einzigen Untermoduln von M sind.

Beispiele 5.2.1 (1) Ist D ein Divisionsring, so sind $\{0\}$ und D die einzigen Linksideale in D. Also ist D ein einfacher D-Modul. Jeder einfache D-Modul ist zu D isomorph. Insbesondere ist ein Vektorraum über einem Körper K genau dann einfach, wenn er die Dimension 1 hat.

(2) Die einfachen $\mathbb{Z}$-Moduln sind gerade die $\mathbb{Z}$-Moduln $\mathbb{Z}_p$, wobei p eine Primzahl ist.

Satz 5.2.1 (Lemma von Schur) *Es seien M, N einfache R-Moduln. Dann ist jeder nicht triviale R-Modulhomomorphismus $M \to N$ ein Isomorphismus. Der Ring* $\mathrm{End}_R(M)$ *ist ein Divisionsring.*

Beweis. Es sei $f : M \to N$ ein nicht trivialer R-Modulhomomorphismus. Dann sind $\mathrm{Ker}\, f \subset M$ und $\mathrm{Im}\, f \subset N$ Untermoduln. Da f nicht trivial ist, gilt $\mathrm{Ker}\, f \neq M$ und $\mathrm{Im}\, f \neq \{0\}$. Da M und N einfach sind, folgt $\mathrm{Ker}\, f = \{0\}$ und $\mathrm{Im}\, f = N$. Also ist f ein Isomorphismus. Wenn $M = N$ ist, so existiert die inverse Abbildung zu f. □

Definition Ein R-Modul M heißt *halbeinfach*, wenn er die direkte Summe von einfachen Moduln ist.

Beispiel 5.2.1 Es sei D ein Divisionsring. Dann ist jeder endlich erzeugte D-Modul M halbeinfach: Nach Satz 5.1.1 ist M frei, also $M \cong D^n$ für ein $n \in \mathbb{N}$, und D ist einfach nach Beispiel 5.2.1(1). Insbesondere ist jeder endlich dimensionale Vektorraum über einem Körper K halbeinfach.

Satz 5.2.2 *Es sei M ein R-Modul. Dann sind die folgenden Aussagen äquivalent:*

(i) *M ist ein halbeinfacher R-Modul.*

(ii) *M ist eine Summe von einfachen Untermoduln.*

(iii) *Für jeden Untermodul N von M gibt es einen Untermodul N' von M, so dass $M = N \oplus N'$.*

Für den Beweis dieses Satzes brauchen wir ein Lemma:

Lemma 5.2.1 *Es sei M ein R-Modul und $(M_i)_{i\in I}$ eine Familie von einfachen Untermoduln von M, so dass $M = \sum_{i\in I} M_i$. Dann gibt es eine Teilmenge $J \subset I$, so dass*

$$M = \bigoplus_{j\in J} M_j.$$

Beweis. Es sei X die Menge aller Teilmengen $I' \subset I$, so dass die Summe $\sum_{i'\in I'} M_{i'}$ direkt ist. Diese Menge ist nicht leer, da $\emptyset \in X$. Wir zeigen, dass die Voraussetzungen des Lemmas von Zorn erfüllt sind. Dazu betrachten wir eine Kette $Z \subset X$, $Z \neq \emptyset$. Setze

$$I_0 := \bigcup_{I'\in Z} I'.$$

Behauptung Die Summe $\sum_{j\in I_0} M_j$ ist direkt.

Eine Summe $\sum_{j\in J} N_j$ von Untermoduln $N_j \subset M$ ist genau dann direkt, wenn für jede endliche Teilmenge $J' \subset J$ die Summe $\sum_{j'\in J'} N_{j'}$ direkt ist. Daher reicht es zu zeigen, dass für jede endliche Teilmenge $I_1 \subset I_0$ die Summe $\sum_{j\in I_1} M_j$ direkt ist. Es sei sei $I_1 \subset I_0$ eine endliche Teilmenge. Dann ist $I_1 \subset I'$ für ein $I' \in Z$. Wegen $Z \subset X$ ist dann die Summe $\sum_{j\in I'} M_j$ direkt, also auch die kleinere Summe $\sum_{j\in I_1} M_j$.

Aus der Behauptung folgt, dass jede Kette $Z \subset X$ eine obere Schranke besitzt. Nach dem Lemma von Zorn gibt es ein maximales Element $J \in X$.

Behauptung Es gilt $M = \bigoplus_{j\in J} M_j$.

Dazu reicht es zu zeigen, dass $M_i \subset \sum_{j\in J} M_j$ für jedes $i \in I$. Dazu betrachten wir

$$N_i := M_i \cap \sum_{j\in J} M_j.$$

Dann ist N_i ein Untermodul von M_i. Da M_i einfach ist, gilt $N_i = 0$ oder $N_i = M_i$. Ist $N_i = 0$, so ist J nicht maximal, da $J \cup \{i\} \in X$. Also folgt $N_i = M_i$, also $M_i \subset \sum_{j\in J} M_j$. □

Beweis von Satz 5.2.2. "(ii) ⇒ (i)": Dies folgt direkt aus Lemma 5.2.1.

"(i) ⇒ (iii)": Es sei ein Untermodul $N \subset M$ gegeben. Nach Voraussetzung gibt es eine Familie $(M_i)_{i\in I}$ einfacher Untermoduln von M mit $M = \bigoplus_{i\in I} M_i$. Dann folgt $M = N + \sum_{i\in I} M_i$. Es sei $J \subset I$ eine maximale Teilmenge von I, so dass die Summe $N + \sum_{j\in J} M_j$ direkt ist. Dann folgt nach den gleichen Argumenten wie beim Beweis von Lemma 5.2.1, dass diese Summe gleich M ist.

"(iii) ⇒ (ii)": Wir zeigen zunächst:

Behauptung Ist $M \neq 0$ ein R-Modul, für den (iii) gilt, so enthält M einen einfachen Untermodul.

Es sei $M \neq 0$ ein R-Modul und $x \in M$, $x \neq 0$. Dann ist Rx ein zyklischer Untermodul und der Kern der R-linearen Abbildung

$$R \to Rx, \quad a \mapsto ax,$$

ist ein Linksideal $I \subset R$, $I \neq R$. Nach Satz 2.4.2 ist I in einem maximalen Ideal $\mathfrak{m}$ von R enthalten. Dann ist $\mathfrak{m}/I$ ein maximaler Untermodul von R/I (und $\mathfrak{m}/I \neq R/I$), also $\mathfrak{m}x$ ein maximaler Untermodul von Rx ($\mathfrak{m}x \neq Rx$). Unter dem Isomorphismus

$$R/I \xrightarrow{\sim} Rx$$

wird $\mathfrak{m}/I$ auf $\mathfrak{m}x$ abgebildet. Nach Voraussetzung können wir $M = \mathfrak{m}x \oplus N$ für einen Untermodul N von M schreiben. Dann gilt

$$Rx = \mathfrak{m}x \oplus (N \cap Rx).$$

Denn jedes Element $ax \in Rx$ kann eindeutig in der Form $ax = bx + y$ mit $b \in \mathfrak{m}$ und $y \in N$ geschrieben werden. Das Element $y = bx - ax$ liegt aber in Rx. Da $\mathfrak{m}x$ maximaler Untermodul von Rx ist, folgt, dass der Modul $N \cap Rx$ einfach ist.

Es sei nun M' der Untermodul von M, der die Summe aller einfachen Untermoduln von M ist. Gilt $M' \neq M$, dann gibt es nach Voraussetzung einen Untermodul $N \neq 0$ von M, so dass $M = M' \oplus N$. Dann erfüllt auch N die Bedingung (iii). Denn ist N' ein Untermodul von N, so gibt es einen Untermodul M'' von M mit $M = N' \oplus M''$. Dann gilt $N = N' \oplus (M'' \cap N)$. Nach der Behauptung enthält N einen einfachen Untermodul im Widerspruch zur Definition von M'. □

5.3 Ein Satz von Wedderburn

Es sei M ein Modul über einem beliebigen Ring R. Es sei $S = \mathrm{End}_R(M)$. Dann kann man M als S-Modul auffassen, wobei die skalare Multiplikation definiert ist durch

$$\varphi \cdot x = \varphi(x) \text{ für alle } \varphi \in \mathrm{End}_R(M) \text{ und } x \in M.$$

Jedes $a \in R$ definiert eine Abbildung

$$\begin{array}{rccc} \ell_a : & M & \longrightarrow & M \\ & x & \longmapsto & ax \end{array}.$$

Diese Abbildung ist S-linear, denn es gilt

$$\varphi \cdot \ell_a(x) = \varphi(ax) = a\varphi(x) = \ell_a(\varphi \cdot x).$$

Damit erhalten wir einen (kanonischen) Ringhomomorphismus

$$R \longrightarrow \mathrm{End}_S(M), \quad a \mapsto \ell_a.$$

Es stellt sich nun die Frage, wie groß das Bild dieses Ringhomomorphismus ist. Eine Antwort darauf gibt der Dichtesatz von Jacobson.

Satz 5.3.1 (Jacobsons Dichtesatz) *Es sei M ein halbeinfacher R-Modul, $S = \mathrm{End}_R(M)$. Es sei $f \in \mathrm{End}_S(M)$ und $x_1, \ldots, x_r \in M$ gegeben. Dann gibt es ein Element $a \in R$ mit*

$$ax_i = f(x_i), \quad \textit{für } i = 1, \ldots, r.$$

Beweis. Wir betrachten zunächst den Fall $r = 1$. Da M halbeinfach ist, gibt es nach Satz 5.2.2 einen Untermodul $N \subset M$ mit

$$M = Rx_1 \oplus N.$$

Es sei $p : M \to Rx_1$ die Projektion auf Rx_1. Dann kann p als Element von $S = \mathrm{End}_R(M)$ aufgefasst werden. Da f ein S-Modulhomomorphismus ist, gilt

$$f(x_1) = f(p(x_1)) = f(p \cdot x_1) = p \cdot f(x_1) = p(f(x_1)) \in Rx_1,$$

d.h. es gibt ein $a \in R$ mit $f(x_1) = ax_1$.

Es sei nun r beliebig. Setze

$$M' := M^r, \quad S' := \mathrm{End}_R(M').$$

Dann ist auch M' ein halbeinfacher R-Modul. Satz 5.1.2 liefert einen Isomorphismus $S' \cong M_r(S)$. Betrachte die Abbildung

$$\begin{array}{rccc} f' : & M' & \longrightarrow & M' \\ & (y_1, \ldots, y_r) & \longmapsto & (f(y_1), \ldots, f(y_r)) \end{array}.$$

Wir zeigen, dass diese Abbildung S'-linear ist. Es sei $\varphi \in S'$. Nach dem Isomorphismus von Satz 5.1.2 wird φ durch eine Matrix

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1r} \\ \vdots & \ddots & \vdots \\ \varphi_{r1} & \cdots & \varphi_{rr} \end{pmatrix}, \quad \varphi_{ij} \in S = \mathrm{End}_R(M),$$

gegeben, die auf M' von links operiert, wobei wir die Elemente von M' als Spaltenvektoren auffassen. Nun gilt

$$\begin{aligned} f' \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1r} \\ \vdots & \ddots & \vdots \\ \varphi_{r1} & \cdots & \varphi_{rr} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} &= f' \begin{pmatrix} \varphi_{11}(y_1) + \cdots + \varphi_{1r}(y_r) \\ \vdots \\ \varphi_{r1}(y_1) + \cdots + \varphi_{rr}(y_r) \end{pmatrix} \\ &= \begin{pmatrix} f(\varphi_{11}(y_1) + \cdots + \varphi_{1r}(y_r)) \\ \vdots \\ f(\varphi_{r1}(y_1) + \cdots + \varphi_{rr}(y_r)) \end{pmatrix} \\ &= \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1r} \\ \vdots & \ddots & \vdots \\ \varphi_{r1} & \cdots & \varphi_{rr} \end{pmatrix} \begin{pmatrix} f(y_1) \\ \vdots \\ f(y_r) \end{pmatrix}, \end{aligned}$$

da $f \in \mathrm{End}_S(M)$.

Wir wenden nun den Fall $r = 1$ auf M', S', f' und $x' := (x_1, \ldots, x_r)$ an und erhalten ein $a \in R$ mit

$$ax' = (ax_1, \ldots, ax_r) = f'(x') = (f(x_1), f(x_2), \ldots, f(x_r)).$$

Daraus folgt die Behauptung. □

Korollar 5.3.1 *Es sei M ein halbeinfacher R-Modul. Ist M als Modul über $S = \mathrm{End}_R(M)$ endlich erzeugt, so ist der kanonische Homomorphismus $R \to \mathrm{End}_S(M)$ surjektiv.*

Beweis. Es seien $x_1, \ldots, x_r$ Erzeugende von M über S und $f \in \mathrm{End}_S(M)$ gegeben. Dann folgt aus Satz 5.3.1 $f = \ell_a$. □

Definition Ein R-Modul M heißt *treu*, wenn es für alle $a \in R$, $a \neq 0$, ein $x \in M$ mit $ax \neq 0$ gibt.

Korollar 5.3.2 (Satz von Wedderburn) *Es sei M ein einfacher und treuer R-Modul. Ist M als Modul über dem Divisionsring $D = \mathrm{End}_R(M)$ endlich erzeugt, so ist R isomorph zu $\mathrm{End}_D(M)$.*

Beweis. Nach Korollar 5.3.1 ist der kanonische Homomorphismus

$$R \to \mathrm{End}_D(M), \quad a \mapsto \ell_a,$$

surjektiv. Dass M treu ist, bedeutet gerade, dass er auch injektiv ist. □

Bemerkung 5.3.1 Es sei M ein einfacher und treuer R-Modul, der als Modul über dem Divisionsring $D = \mathrm{End}_R(M)$ endlich erzeugt ist. Wegen Satz 5.1.2 können wir Korollar 5.3.2 auch so formulieren: Da über dem Divisionsring D alle Moduln frei sind, gibt es ein $n \in \mathbb{N}$ mit $M \cong D^n$. Dann ist R isomorph zu $M_n(D^{\mathrm{op}})$.

Es sei nun K ein Körper und R eine K-Algebra. Es sei M ein R-Modul. Dann ist M auch ein Vektorraum über K und $S = \mathrm{End}_R(M)$ eine K-Algebra. Es sei nun M als K-Vektorraum endlich dimensional. Dann gilt

$$S = \mathrm{End}_R(M) \subset \mathrm{End}_K(M) \cong M_n(K).$$

Da $M_n(K)$ als K-Vektorraum endlich dimensional ist, ist auch S endlich dimensional.

Ist R endlich dimensional über K, so hat jeder einfache R-Modul M endliche Dimension über K. Denn das Bild eines nicht trivialen R-Modulhomomorphismus $R \to M$ ist ein nicht trivialer Untermodul von M, also gleich M.

Korollar 5.3.3 *Es sei R eine endlich dimensionale K-Algebra über einem Körper K und M ein einfacher R-Modul. Es sei $D = \mathrm{End}_R(M)$. Dann ist der kanonische Homomorphismus $R \to \mathrm{End}_D(M)$ surjektiv.*

Beweis. Nach Korollar 5.3.1 reicht es zu zeigen, dass M als Modul über D endlich erzeugt ist. Dies folgt aber daraus, dass M schon als Modul über

$$K \cong K \,\mathrm{Id}_M \subset D$$

endlich erzeugt ist. □

Definition Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom aus $K[x]$ eine Nullstelle in K besitzt.

Satz 5.3.2 (Lemma von Schur) *Es sei K ein algebraisch abgeschlossener Körper, R ein K-Algebra und M ein einfacher R-Modul. Wenn M endlich dimensional über K ist, so gilt $\mathrm{End}_R(M) = K \,\mathrm{Id}_M \cong K$.*

Beweis. Es sei $\varphi \in \mathrm{End}_R(M) \subset \mathrm{End}_K(M)$. Da K algebraisch abgeschlossen ist, muss das charakteristische Polynom von φ mindestens eine Nullstelle $\lambda \in K$ haben. Dann gilt

$$\mathrm{Ker}(\varphi - \lambda \,\mathrm{Id}_M) \neq 0.$$

Da $\varphi - \lambda \,\mathrm{Id}_M$ ein R-lineare Abbildung ist, ist der Kern ein Untermodul von M. Da M einfach ist, folgt

$$\mathrm{Ker}(\varphi - \lambda \,\mathrm{Id}_M) = M.$$

Das bedeutet aber $\varphi = \lambda \,\mathrm{Id}_M \in K \,\mathrm{Id}_M$. □

Korollar 5.3.4 (Burnside) *Es sei K ein algebraisch abgeschlossener Körper, V ein endlich dimensionaler K-Vektorraum und R eine Unteralgebra von $\mathrm{End}_K(V)$. Wenn V als R-Modul einfach ist, so gilt $R = \mathrm{End}_K(V)$.*

Beweis. Aus Satz 5.3.2 folgt, dass $\mathrm{End}_R(M) = K \,\mathrm{Id}_V \cong K$. Also ist nach Korollar 5.3.3 die Inklusion $R \hookrightarrow \mathrm{End}_K(V)$ surjektiv. □

Literaturverzeichnis

[1] J. C. Jantzen, J. Schwermer: Algebra. Springer-Verlag, 2006. ISBN 3-540-21380-5

[2] S. Lang: Algebra. 3rd Edition. (Graduate Texts in Math. 211) Springer-Verlag, 2002. ISBN 0-387-95385-X.

[3] M. Reid: Undergraduate commutative algebra. (London Math. Society Students texts 23) Cambridge University Press. ISBN 0-521-45889-7.

[4] J. Wolfart: Einführung in die Zahlentheorie und Algebra. Vieweg, 1996. ISBN 978-3-528-07286-5

[5] G. Wüstholz: Algebra. Vieweg, 2004. ISBN 978-3-528-07291-9

Inhaltsverzeichnis