ALGEBRA II

Autoren:
David Arnold, Roman Bergmann, Sophie Burzlaff, Thomas Drögemüller, Sören Hermann, Hannes Hirt, Nils Höfer, Aaron Kamp, Caroline Lassueur, Benjamin Leßmann, Max Möhnle, Hendrik Peters, Ben Schiemann, Lukas Schulze, Cagla Sengül, Michel Strohschän, Enrique Vizcarra Carrazco, Luke Wenderoth, Fabiola Werner, Lena Winkler, Jule Wolterink ...

kollaboratives Skript zur Vorlesung
SoSe 2025
@ Leibniz Universität Hannover
(Vorlesung: 4SWS // Übung: 2SWS)

Version: 13. Juli 2025

Inhaltsverzeichnis

Konventionen iii

Teil I. Modultheorie 8

Kapitel 1. Moduln – Grundbegriffe 8
1 Definitionen und Beispiele . . . 8
2 Untermoduln . . . 12
3 Morphismen . . . 14
3.1 Kern und Bild . . . 17
3.2 Rechtsmultiplikation . . . 18
4 Faktormoduln . . . 19
4.1 Die Isomorphisätze . . . 21
4.2 Annulatoren . . . 22
5 Einfache Moduln . . . 23
6 Exakte Sequenzen . . . 24
6.1 Grundlegende Eigenschaften . . . 24
6.2 Diagramm-Lemmata* . . . 28
7 Projektive and Injektive Moduln . . . 30
8 Freie Moduln . . . 34

Kapitel 2. Endlichkeitsbedingungen 43
9 Kompositionsreihen . . . 43
10 Noethersche Moduln . . . 46
11 Artinsche Moduln . . . 50
12 (Un)zerlegbare Moduln . . . 52
13 Das Jacobson-Radikal . . . 56
14 Halbeinfache Moduln . . . 59
14.1 Halbeinfache Ringe . . . 61
14.2 J-Halbeinfachheit . . . 63
14.3 Der Artin–Wedderburn-Struktursatz . . . 64

Kapitel 3. Moduln über Hauptidealringe **66**
15 Primelemente und Torsion . . . 66
16 Freie und torsionsfreie Moduln . . . 68
17 Torsionsmoduln . . . 70
18 Der Hauptsatz . . . 75

Kapitel 4. Tensorprodukte **79**
19 Tensorprodukte von Moduln . . . 79
20 Modulstruktur . . . 82
21 Tensorprodukte und Direkte Summen . . . 85

Teil II. Einführung in die Kategorientheorie **88**

Kapitel 5. Kategorientheorie **88**
22 Kategorien . . . 88
23 Funktoren . . . 92
24 Äquivalenzen von Kategorien . . . 97
25 Morita Theorie . . . 101

Teil III. Gruppentheorie und Körpertheorie **106**

Kapitel 6. Gruppentheorie und Galoistheorie **106**
26 Auflösbare Gruppen . . . 107
26.1 Definitionen und Beispiele . . . 107
26.2 Der $p^a q^b$-Satz und der Satz von Feit und Thompson . . . 112
26.3 Höhere Kommutatorgruppen . . . 113
27 Auflösbarkeit durch Radikale . . . 115
27.1 Lösbarkeit von Polynomgleichungen. . . . 116
27.2 Metazyklische Erweiterungen . . . 119

Anhang **122**
A Mengenlehre: Zorns Lemma . . . 122

Konventionen

Im Folgenden bezeichnet $(R, +, \cdot)$ (oder einfach R) stets einen Ring.

Wir setzen voraus, dass alle Ringe **assoziativ mit** 1 sind.

Wie üblich schreiben wir:

- 0_R oder einfach 0 für das neutrale Element bezüglich $+$ (der Addition);
- 1_R oder einfach 1 für das neutrale Element bezüglich $\cdot$ (der Multiplikation);
- rs statt $r \cdot s$.

Außerdem bezeichnet $(K, +, \cdot)$ (oder einfach K) stets einen Körper.

Teil I.
Modultheorie

Motivation und Grundidee: In der Linearen Algebra I/II studiert man K-Vektorräume: Es sind abelsche Gruppen $(V,+)$ mit einer äußeren Miltiplikation $* : K \times V \longrightarrow V$, $(\lambda, v) \mapsto \lambda * v$, wobei K ein Köper ist. In der Modultheorie ersetzen wir den Körper K durch einen Ring R. (Dieser muss nicht unbedingt kommutativ sein). Wir sprechen dann nicht mehr von ***Vektorräumen*** sondern von ***Moduln***.
Wir definieren dies zunächst und werden im Lauf der Vorlesung sehen, welche Vektorraumeigenschaften verlorengehen und was sich verallgemeinern lässt.

1 Definitionen und Beispiele

Zunächst erinnern wir einmal an die Definition eines K-Vektorraums.

Definition: Sei K ein Körper. Ein **Vektorraum über** K (kurz: K-Vektorraum) ist eine Menge V zusammen mit 2 Operationen

$$+ : V \times V \longrightarrow V, (v,w) \mapsto v + w \quad (\text{die „Addition in } V\text{“}),$$
$$\cdot : K \times V \longrightarrow V, (\lambda, v) \mapsto \lambda \cdot v \quad (\text{die Skalarmultiplikation}),$$

sodass für alle $v, w \in V$ und alle $\lambda, \mu \in K$ gelten:

(V1) $(V,+)$ ist eine abelsche Gruppe (mit neutralem Element : 0_V);
(V2) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$;
(V3) $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$;
(V4) $\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v$;
(V5) $1_K \cdot v = v$.

Wir ersetzen also den Körper durch einen Ring und erhalten die folgende Definition.

Definition 1.1 (*Linksmodul*)

Sei R ein Ring. Ein **Linksmodul** über R (kurz: R-**Linksmodul** oder einfach R-**Modul**) ist eine Menge M zusammen mit 2 Operationen

$$+ : M \times M \longrightarrow M, (m,n) \mapsto m + n \quad (\text{die „Addition in } M\text{“}), \text{ und}$$
$$\cdot : R \times M \longrightarrow M, (r,m) \mapsto r \cdot m \quad (\text{die „äußere Multiplikation“}),$$

sodass für alle $m, n \in M$ und alle $r, s \in R$ gelten:

(M1) $(M, +)$ ist eine abelsche Gruppe (mit neutralem Element 0_M);

(M2) $(r + s) \cdot m = r \cdot m + s \cdot m$;

(M3) $r \cdot (m + n) = r \cdot m + r \cdot n$;

(M4) $r \cdot (s \cdot m) = (rs) \cdot m$;

(M5) $1_R \cdot m = m$.

Beachten Sie: Anders als z.B. in der Studienordnung heißt es in der Mathematik **der** Modul und die Modul**n** im Plural.

Analog definieren wir Rechtsmoduln.

Definition 1.2 (*Rechtsmodul*)

Sei R ein Ring. Ein **Rechtsmodul** über R (kurz: R-**Rechtsmodul**) ist eine Menge M zusammen mit 2 Operationen

$$+ : M \times M \longrightarrow M, (m, n) \mapsto m + n \quad (\text{die „Addition in } M\text{“}), \text{ und}$$
$$\cdot : M \times R \longrightarrow M, (m, r) \mapsto m \cdot r \quad (\text{die „äußere Multiplikation“}),$$

sodass für alle $m, n \in M$ und alle $r, s \in R$ gelten:

(RM1) $(M, +)$ ist eine abelsche Gruppe (mit neutralem Element 0_M);

(RM2) $m \cdot (r + s) = m \cdot r + m \cdot s$;

(RM3) $(m + n) \cdot r = m \cdot r + n \cdot r$;

(RM4) $(m \cdot r) \cdot s = m \cdot (rs)$;

(RM5) $m \cdot 1_R = m$.

Ist der Ring R nicht kommutativ, so sind R-Linksmoduln und R-Rechtsmoduln im Allgemeinen nicht „dasselbe“. Wir dürfen auch Moduln betrachten die gleichzeitig Linksmoduln und Rechtsmoduln für verschiedene Ringe sind.

Definition 1.3 (*Bimoduln*)

Seien R und S zwei Ringe. Ein (R, S)-**Bimodul** ist eine abelsche Gruppe $(M, +)$ mit einer R-Linksmodulstruktur und mit einer S-Rechtsmodulstruktur, sodass

$$(r \cdot m) \cdot s = r \cdot (m \cdot s) \qquad \forall\, m \in M, \forall\, r \in R, \forall\, s \in S$$

gilt.

Schreibweise 1.4

(1) **Konvention**: Wenn nicht anders gesagt, so betrachten wir nur R-Linksmoduln und wir schreiben einfach „R-Modul“ statt „R-Linksmoduln“.

(2) Ist $(M, +, \cdot)$ ein R-Modul, so schreiben wir wie üblich:

- 0_M oder einfach 0 für das neutrale Element bezüglich $+$;
- rm statt $r \cdot m$ (für $r \in R$ und $m \in M$).

Aufgabe 1.5 (*Aufgabe 1(a), Blatt 1*)

Die Definition eines R-Linksmoduls ist äquivalent zur folgenden Definition.

Ein R-Linksmodul ist ein 3-Tupel $(M, +, \cdot)$, so dass die folgenden Axiome gelten:

(MH1) $(M, +)$ ist eine abelsche Gruppe; und

(MH2) $\cdot : R \times M \longrightarrow M, (r, m) \mapsto r \cdot m$ ist eine äußere Multiplikation und erfüllt die Bedingung, dass

$$\begin{array}{rccl} \lambda\colon & R & \longrightarrow & \mathrm{End}(M) \\ & r & \mapsto & \lambda(r) := \lambda_r : M \longrightarrow M, m \mapsto r \cdot m \end{array}$$

ein Ringhomomorphismus ist. (Hier bezeichnet $\mathrm{End}(M)$ die Menge aller Gruppen-Endomorphismen von M.)

Aufgabe 1.6 (*Aufgabe 1, Präsenzblatt 0*)

Sei $(M, +, \cdot)$ ein R-Modul. Zeigen Sie, dass die folgenden Rechenregeln gelten:

(1) $r \cdot 0_M = 0_M \quad \forall\, r \in R$;

(2) $0_R \cdot m = 0_M \quad \forall\, m \in M$;

(3) $(-r) \cdot m = -(r \cdot m) = r \cdot (-m) \quad \forall\, r \in R, \forall\, m \in M$.

Beispiel 1

(0) Der **Nullmodul** $0 := \{0\}$ mit äußren Multiplikation $\cdot : R \times 0 \longrightarrow 0, (r, 0) \mapsto r \cdot 0 = 0$. (Dieser existiert für jeden Ring).

(1) Ist $R := K$ ein Körper, so sind die K-Moduln genau die K-Vektorräume.

(2) Ist $R := \mathbb{Z}$, so sind die $\mathbb{Z}$-Moduln genau die abelschen Gruppen.

- Jeder $\mathbb{Z}$-Modul ist eine abelsche Gruppe nach Definition (nach Axiom (M1).)
- Umgekehrt: Ist $(M, +)$ eine abelsche Gruppe, so ist $(M, +, \cdot)$ ein $\mathbb{Z}$-Modul für die äußere

Multiplikation

$$\cdot : \mathbb{Z} \times M \longrightarrow M$$
$$(z, m) \mapsto z \cdot m := \begin{cases} m + \cdots m \quad (z\text{-mal}) & \text{falls } z > 0 \\ 0_M & \text{falls } z = 0 \\ -|z| \cdot m & \text{falls } z < 0 \end{cases}$$

(3) Der Ring $(R, +, \cdot)$ selbst kann als R-Modul betrachtet werden:

- die Addition bleibt gleich;
- äußere Multiplikation := innere Multiplikation.

Schreibweise: Wir schreiben R^{reg} statt R, um die Modulstruktur zu betonen.
Terminologie: R^{reg} ist der **reguläre R-Modul**.

(4) Das kartesische Produkt $R^n = R \times \cdots \times R$ (n-mal) mit $n \in \mathbb{N}$ ist ein R-Modul für die Addition

$$+ : R^n \times R^n \longrightarrow R^n$$
$$\big((v_1, \ldots, v_n), (w_1, \ldots, w_n)\big) \mapsto (v_1, \ldots, v_n) + (w_1, \ldots, w_n) = (v_1 + w_1, \ldots, v_n + w_n)$$

und äußere Multiplikation

$$\cdot : R \times R^n \longrightarrow R^n$$
$$\big(r, (v_1, \ldots, v_n)\big) \mapsto r \cdot (v_1, \ldots, v_n) = (rv_1, \ldots, rv_n)\,.$$

(5) $\left.\begin{array}{l} \text{Sei } K \text{ ein Körper }, n \in \mathbb{N} \\ R := M_n(K) = K^{n \times n} \end{array}\right\} \Longrightarrow M := K^n \text{ ist ein } R\text{-Modul}$

$+$ ist die übliche Vektor-Addition
$\cdot$ ist die übliche Matrix-Vektor-Multiplikation

(6) Ist $(R, +, \cdot)$ ein Ring, so schreiben wir R^{op} für den Ring mit derselben Addition $+$ und mit der Multiplikation $\tilde{\cdot}$ definiert durch

$$\tilde{\cdot} : R \times R,\ (r, s) \mapsto r \,\tilde{\cdot}\, s := s \cdot r\,.$$

Der Ring R^{op} heißt der **entgegengesetzte Ring**.

Aufgabe auf dem Präsenzblatt am Mi. 16.4.2025. Zeigen Sie:

(a) Jeder R-Linksmodul $(M, +, \cdot)$ wird zu einem R^{op}-Rechtsmodul, indem man die äußere Multiplikation wie folgt definiert:

$$m \cdot r := r \cdot m \qquad \forall\, r \in R,\ \forall\, m \in M\,.$$

Umgekehrt geht dies analog.

(b) Ist R ein kommutativer Ring, so ist jeder R-Linksmodul auch ein R-Rechtsmodul, und umgekehrt. Dies gilt insbesondere für alle K-Vektorräume.

Aufgabe 1.7 (*Aufgabe 1(b)-(d), Blatt 1*)

Zeigen Sie:

(a) Ist $(M,+,\cdot)$ ein R-Modul und $\varphi : S \longrightarrow R$ ein Ringhomomorphismus, so wird $(M,+)$ zu einem S-Modul durch die äußere Multiplikation

$$* : S \times M \longrightarrow M, (s,m) \mapsto s * m := \varphi(s) \cdot m\,.$$

(b) Ist S ein Teilring von R, so ist jeder R-Modul auch ein S-Modul.

(c) Ist I ein Ideal von S, so ist jeder S/I-Modul auch ein S-Modul.

2 Untermoduln

Als Nächstes untersuchen wir die Unterstrukturen.

Definition 2.1 (*Untermodul*)

Sei $(M,+,\cdot)$ ein R-Modul. Dann heißt $U \subseteq M$ R-**Untermodul** von M, geschrieben $U \leqslant M$, wenn gelten:

(UM1) $(U,+)$ ist eine Untergruppe von $(M,+)$;

(UM2) $r \cdot u \in U \quad \forall\, r \in R$ und $\forall\, u \in U$.

Äquivalente Charakterisierungen 2.2

Für eine Teilmenge $U \subseteq M$ mit $U \neq \varnothing$ sind folgende Aussagen äquivalent:

(1) $U \leqslant M$;

(2) $r \cdot u + v \in U \quad \forall\, r \in R, \forall\, u, v \in U$;

(3) mit der eingeschränkten Addition und mit der eingeschränkten Multiplikation von M ist U selbst ein R-Modul.

Beweis: Der Beweis ist hier wie bei Vektorräumen! Als Beispiel beweisen wir:

$$U \leqslant M \iff \underbrace{\underbrace{r \cdot u + v \in U}_{(*)} \quad \forall\, r \in R, \forall\, u, v \in U}\,.$$

„$\Longrightarrow$“: Seien $r \in R$ und $u, v \in U$. Dann ist nach (UM2) $r \cdot u \in U \Rightarrow \underbrace{r \cdot u}_{\in U} + \underbrace{v}_{\in U} \in U$ nach (UM1).

„$\Longleftarrow$“: Nehme $r := -1_R \in R$, $u \in U$ beliebig (existiert, da $U \neq \varnothing$), und $v := u$

$\overset{(*)}{\Longrightarrow} U \ni r \cdot u + v = -1_R \cdot u + u = 0_M$. Also ist U nicht-leer.

Wähle $r := 1_R \in R$.

$\overset{(*)}{\Longrightarrow} U \ni r \cdot u + v = 1_R \cdot U + v = u + v \ \forall u, v \in U$. Somit ist $(U, +)$ eine Untergruppe von $(M, +)$ und (UM1) gilt.

Um (UM2) zu zeigen, nehme $v := 0_M \in U$. (Dies ist nach dem ersten Teil des Beweises möglich). Dann folgt erneut aus der Annahme $*$: $\forall r \in R$, $\forall u \in U$ gilt $r \cdot u = r \cdot u + 0_M \in U$. Das heißt (UM2) gilt auch.

■

Beispiel 2

(0) Ist M ein R-Modul, so sind $\{0_M\}$ und M stets R-Untermoduln von M.

(1) Die R-Untermoduln von R^{reg} sind die Linksideale von R.

(2) Für $R = K$ ein Körper: Die K-Untermoduln eines K-Vektorraums sind genau die K-Unterräume.

(3) Für $R = \mathbb{Z}$: Die $\mathbb{Z}$-Untermoduln einer abelschen Gruppe sind genau die Untergruppen.

Es gibt auch hier viele Konstruktionen (z.B. $\bigcap, \sum, \langle - \rangle, \oplus, \dots$) aus der Welt der Vektorräume, die wir verallgemeinern können, ohne Änderungen bei den Beweisen. Aus diesem Grund geben wir diese Ergebnisse hier ohne Beweise an.

Lemma-Definition 2.3 (*Der von S erzeugte Untermodul*)

Sei M ein R-Modul. Für jede Teilmenge $S \subseteq M$ ist der Durchschnitt

$$\langle S \rangle_R := \bigcap \{U \leqslant M \mid S \subseteq U\}$$

ein R-Untermodul von M; der von S **erzeugte R-Untermodul** von M. Es ist

$$\langle S \rangle_R = \left\{ \sum_{i=1}^{n} r_i \cdot x_i \;\middle|\; n \in \mathbb{Z}_{\geqslant 0}, r_1, \dots, r_n \in R, x_1, \dots, x_n \in S \right\}.$$

Beweis: Wie in der linearen Algebra! Übung. ■

Der Begriff einer zyklischen Gruppe bzw. Untergruppe lässt sich auch verallgemeinern.

Beispiel 3

Folgerung aus Lemma-Definition 2.3:
Ist M ein R-Modul, so ist für jedes $x \in M$ die Teilmenge

$$Rx = \{r \cdot x \mid r \in R\} = \langle \{x\} \rangle =: \langle x \rangle_R$$

ein R-Untermodul von M. Diese Untermoduln heißen **zyklische** R-Untermoduln.

- Für R kommutativ gilt: Die Hauptideale sind genau die zyklischen R-Untermoduln von R^{reg}.
- Für $R = \mathbb{Z}$ gilt: Eine abelsche Gruppe ist genau dann als Gruppe zyklisch, wenn sie als $\mathbb{Z}$-Modul zyklisch ist.

Dies erlaubt es uns Durchnitte, direkte Produkte und innere bzw. äussere direkte Summen von R-Moduln zu definieren.

Lemma-Definition 2.4 (*Schnitt und (innere) Summe von Untermoduln*)

Sei M ein R-Modul und sei $\{N_i\}_{i\in I}$ eine Familie von R-Untermodulen von M. Dann gelten:

(1) $\bigcap_{i\in I} N_i$ ist ein R-Untermodul von M;

(2) $\sum_{i\in I} N_i := \langle \bigcup_{i\in I} N_i \rangle_R = \{x_1 + \cdots + x_n \mid n \in \mathbb{N}, x_1, \ldots, x_n \in \bigcup_{i\in I} N_i\}$ ist ein R-Untermodul von M; die sogenannte **(innere) Summe** der N_i ($i \in I$).

Beweis: Wie in der linearen Algebra! Übung. ■

Lemma-Definition 2.5 (*Produkt und (äußere) direkte Summe von Untermoduln*)

Sei $\{M_i\}_{i\in I}$ eine Familie von R-Moduln. Dann ist das kartesische Produkt $\prod_{i\in I} M_i$ mit der komponentenweisen Addition und mit der komponentenweisen äußeren Multiplikation ein R-Modul, das sogenannte **direkte Produkt** der Moduln M_i ($i \in I$).
Die **(äußere) direkte Summe**

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \in \prod_{i\in I} M_i \mid m_i = 0 \text{ für fast alle } i \in I\}$$

ist ein R-Untermodul von $\prod_{i\in I} M_i$.

Beweis: Wie in der linearen Algebra! Übung. ■

3 Morphismen

Als Drittes untersuchen wir die Morphismen zwischen den R-Moduln.

Definition 3.1 (*Morphismen*)

Seien M, N zwei R-Moduln.

(1) Eine Abbildung $f : M \longrightarrow N$ heißt R-**Homomorphismus** oder R-**linear**, falls $\forall\, x, y \in M$, $\forall\, r \in R$ gilt

$$f(r \cdot x + y) = r \cdot f(x) + f(y)\,.$$

(2) Dazu heißt f:

- R-**Endomorphismus**, falls $M = N$;
- R-**Isomorphismus**, falls f bijektiv ist;
- R-**Automorphismus**, falls $M = N$ und f bijektiv ist.

Warnung: Mit den Begriffen „Monomorphismen“ und „Epimorphismen“ arbeiten wir vorerst nicht und verweisen auf den späteren Teil der Kategorientheorie.

Äquivalente Charakterisierungen 3.2

Für eine Abbildung $f : M \longrightarrow N$ zwischen zwei R-Moduln M, N sind folgende Charakterisierungen äquivalent:

(1) f ist ein R-Homomorphismus;

(2) (a) $f(r \cdot x) = r \cdot f(x) \quad \forall\, r \in R, \forall\, x \in M$, und
(b) $f(x + y) = f(x) + f(y) \quad \forall x, y \in M$;

(3) $f(r \cdot x + s \cdot y) = r \cdot f(x) + s \cdot f(y) \quad \forall\, r, s \in R$ und $\forall\, x, y \in M$.

Beweis: Wie in der linearen Algebra! Übung. ■

Schreibweise 3.3

Seinen M und N zwei R-Moduln. Wir schreiben:

- $\mathrm{Hom}_R(M, N) := \{f : M \longrightarrow N \mid f\ R\text{-Homomorphismus}\}$;
- $\mathrm{End}_R(M) := \{f : M \longrightarrow N \mid f\ R\text{-Endomorphismus}\}$;
- $\mathrm{Aut}_R(M) := \{f : M \longrightarrow N \mid f\ R\text{-Automorphismus}\}$;
- $M \cong N$ (oder $M \cong_R N$), falls es einen R-Isomorphismus zwischen M und N gibt, und wir sagen, dass M und N **isomorph** oder **R-isomorph** sind.

Beispiel 4

(0) Die **Nullabbildung** $0 : M \longrightarrow N$, $m \mapsto 0_N$ ist ein R-Homomorphismus, da $\forall\, x, y \in M$ und $\forall\, r \in R$ gelten
$$\begin{cases} 0(r \cdot x + y) = 0_N, & \text{und} \\ r \cdot 0(x) + 0(y) = r \cdot 0_N + 0_N = 0_N. \end{cases}$$

(1) Die **Identitätsabbildung** $\mathrm{Id}_M : M \longrightarrow M$, $m \mapsto m$ ist ein R-Homomorphismus und auch bijektiv.
Somit ist Id_M ein R-Endomorphismus von M, der ein R-Isomorphismus ist, d.h. ein R-Automorphismus von M.

Aufgabe 3.4 (*Aufgabe 2, Blatt 1*)

Sei R ein Ring und seien M und N zwei R-Moduln. Zeigen Sie:

(a) Ist R kommutativ, so ist $\mathrm{Hom}_R(M, N)$ ein R-Linksmodul für die punktweise Addition der Abbildungen

$$\begin{array}{rccc} +: & \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(M,N) \\ & (f, g) & \mapsto & f + g : M \longrightarrow N, m \mapsto f(m) + g(m) \end{array}$$

und für die äußere Multiplikation

$$\begin{array}{rccl} \cdot : & R \times \mathrm{Hom}_R(M,N) & \longrightarrow & \mathrm{Hom}_R(M,N) \\ & (r,f) & \mapsto & r \cdot f : M \longrightarrow N, m \mapsto (r \cdot f)(m) := rf(m)\,. \end{array}$$

(b) Die Menge $\mathrm{End}_R(M)$ mit der punktweisen Addition der Abbildungen und mit der üblichen Komposition der Abbildungen ist ein Ring.

Anmerkung 3.5

Für R-Moduln M und N gelten nach Aufgabe 3.4:

- $\mathrm{Hom}_R(M,N)$ ist immer eine abelsche Gruppe und sogar ein R-Linksmodul, wenn R kommutativ ist;
- $\mathrm{End}_R(M)$ ist immer ein Ring;
- $\mathrm{Aut}_R(M) = \mathrm{End}_R(M)^\times$ ist die Einheitensgruppe von $\mathrm{End}_R(M)$.

Beispiel 5

(3) Ist $U \leqslant M$ ein R-Untermodul, so ist die **kanonische Inklusion**

$$\begin{array}{rcl} \iota_U : U & \hookrightarrow & M \\ u & \mapsto & u \end{array}$$

ein injektiver R-Homomorphismus. Es gilt: $\iota_U = \mathrm{id}_M|_U$.

(4) Die Komposition von R-Homomorphismen (soweit sie möglich ist) ist wieder ein R-Homomorphismus.

(5) Ist $f : M \longrightarrow N$ ein bijektiver R-Homomorphismus, so ist auch die Umkehrabbildung $f^{-1} : N \longrightarrow M$ ein R-Homomorphismus, denn

$$f^{-1}(r \cdot n) = f^{-1}(r \cdot \underbrace{f(f^{-1}(n))}_{=\mathrm{id}_N}) = \underbrace{f^{-1}(f(}_{=\mathrm{id}_M} r \cdot f^{-1}(n))) = r \cdot f^{-1}(n) \qquad \forall r \in R, \forall n \in N\,.$$

(6) Für K-Vektorräume $X := K^n, Y := K^m (m, n \in \mathbb{Z}_{>0})$ gelten:

- $\mathrm{Hom}_K(X,Y) \cong M_{m,n}(K)$ (als K-Vektorräume);
- $\mathrm{End}_K(X) \cong M_n(K)$ (als Ringe);
- $\mathrm{Aut}_K(X) \cong \mathrm{GL}_n(K)$ (als Gruppen).

(7) Ist $\{M_i\}_{i \in I}$ eine Familie von R-Moduln, so sind die kanonischen **Projektionen**

$$\begin{array}{rcl} \pi_j : \prod_{i \in I} M_i & \twoheadrightarrow & M_j \\ (m_i)_{i \in I} & \mapsto & m_j \end{array}$$

surjektive R-Homomorphismen ($j \in J$), und die kanonischen **Injektionen**

$$\iota_j : M_j \hookrightarrow \bigoplus_{i \in I} M_i$$

$$m \mapsto (m_i)_{i \in I} \qquad \text{mit} \begin{cases} m_i := m & \text{für } i = j \\ m_i := 0_{M_i} & \text{für } i \neq j \end{cases}$$

injektive R-Homomorphismen ($j \in J$).

Lemma-Definition 3.6 (*(Innere) direkte Summe*)

Sei M ein R-Modul. Sei $\{N_i\}_{i \in I}$ eine Familie von R-Untermoduln von M. Die Abbildung

$$\bigoplus_{i \in I} N_i \longrightarrow \sum_{i \in I} N_i,$$

$$(n_i)_{i \in I} \mapsto \sum_{i \in I} n_i$$

ist genau dann ein R-Isomorphismus, wenn

$$N_i \bigcap \sum_{\substack{j \in I \\ i \neq j}} N_j = \{0\} \qquad \forall i \in I.$$

Die Summe heißt dann **(innere) direkte Summe der** N_i und wir schreiben auch $\bigoplus_{i \in I} N_i$.

Beweis: Ohne. Wie in der linearen Algebra. ■

3.1 Kern und Bild

Der Kern und das Bild eines R-Homomorphismus definiert man wie bei allen anderen algebraischen Strukturen.

Lemma 3.7 (*Kern und Bild*)

Seien M, N R-Moduln, $f \in \mathrm{Hom}_R(M, N)$.

(a) Für jeden R-Untermodul $U \leqslant M$ gilt $f(U) \leqslant N$. Insbesondere ist $\mathrm{Bild}(f) := f(M)$ ein R-Untermodul von N.

(b) Für jeden R-Untermodul $V \leqslant N$ gilt $f^{-1}(V) \leqslant M$. Insbesondere ist $\mathrm{Ker}(f) := f^{-1}(\{0_N\})$ ein R-Untermodul von M.

Beweis:

(1.) Axiom (UM1) ist für abelsche Gruppen bereits aus der Algebra I bekannt und gilt in (a) und (b).

(2.) Es ist nur notwendig Axiom (UM2) zu zeigen.

(a) Seien $r \in inR$ und $n \in f(U)$. Zu zeigen: $r \cdot n \in f(U)$. Nun gilt:

$$\begin{aligned} n \in f(U) &\implies \exists m \in U \text{ mit } n = f(m) \\ &\implies r \cdot n = r \cdot f(m) \overset{f-\text{Hm}}{=} f(r \cdot m) \in f(U) \end{aligned}$$

(b) Seien $r \in R, m \in f^{-1}(V)$. Zu zeigen ist: $r \cdot m \in f^{-1}(V)$.
Mit $m \in f^{-1}(V)$ folgt, dass $f(m) \in V$. Somit ist

$$f(r \cdot m) \overset{f-\text{Hm}}{=} r \cdot f(m) \in V\,,$$

da $V \leqslant N$. Daher gilt $r \cdot m \in f^{-1}(V)$. ■

3.2 Rechtsmultiplikation

Lemma 3.8

Sei M ein R-Modul.

(a) Ist $x \in M$, so ist $r_x : R \longrightarrow M, r \mapsto r \cdot x$ ein R-Homomorphismus mit $\text{Bild}(r_x) = \langle x \rangle_r$.

(b) Es gilt $\text{Hom}_R(R, M) = \{r_x | x \in M\}$.

(c) Die Abbildung $\varepsilon : \text{Hom}_R(R, M) \longrightarrow M, f \mapsto f(1)$ ist ein Isomorphismus von abelschen Gruppen.

(d) Ist R kommutativ, so ist ε ist ein R-Isomorphismus.

(e) Ist $M := R$, so ist $\varepsilon : \text{End}_R(R) \longrightarrow R^{\text{op}}$ ein Ringisomorphismus.

Beweis:

(a) Seien $r \in R, y_1, y_2 \in R$. Es gilt:

$$\begin{aligned} r_x(r \cdot y_1 + y_2) &= (r \cdot y_1 + r \cdot y_2) \cdot x \\ &= (r \cdot y_1) \cdot x + y_2 \cdot x && \text{nach (M2) für } M \\ &= r \cdot (y_1 \cdot x) + y_2 \cdot x && \text{nach (M4) für } M \\ &= r \cdot r_x(y_1) + r_x(y_2) \end{aligned}$$

Somit ist r_x ein $R-$Homomorphismus.

(b) "$\subseteq$" Klar nach (a).
"$\supseteq$" Sei nun $f \in \text{Hom}_R(R, M)$ und $a \in R$. Es gilt $f(a) = f(a \cdot 1) = a \cdot f(1)$, da f ein R-Homomorphismus ist. Somit ist $f = r_{f(1_R)}$ (Rechtsmultiplikation mit $f(1_R) \in M$).

(c)
- ε ist ein Gruppenhomomorphismus:

$$\varepsilon(f + g) = (f + g)(1) = f(1) + g(1) = \varepsilon(f) + \varepsilon(g) \qquad \forall f, g \in \text{Hom}_R(R, M)$$

- Für die Abbildung $f : M \longrightarrow \text{Hom}_R(R, M), x \mapsto r_x$ gilt $r \circ \varepsilon = \text{id}$ und $\varepsilon \circ r = \text{id}$. Damit ist r die Umkehrabbildung und ε is bijektiv. Somit ist ε ein Gruppenhomomorphismus.

(d)
- Nach (c) ist ε:
  (1) Gruppenhomomorphismus

(2) bijektiv

- Ferner gilt, dass $\forall\, r \in R$, $\forall\, f \in \mathrm{Hom}_R(R, M)$:

$$\varepsilon(rf) = (rf)(1) = f(r) = rf(1) = r\varepsilon(f)\,.$$

(e)
- Nach (c) ist ε: $\varepsilon : (\mathrm{End}_R(R), +) \longrightarrow (R^{\mathrm{op}}, +)$ ist ein Gruppenisomorphismus.
- Nun für $f, g \in \mathrm{End}_R(R)$ gilt:

$$\varepsilon(f \circ g) = (f \circ g)(1) = f(g(1)) = f(g(1) \cdot 1) = g(1) \cdot f(1) = \varepsilon(g) \cdot \varepsilon(f) = \varepsilon(g) \mathbin{\tilde{\cdot}} \varepsilon(f)$$

Damit folgt, dass ε ein Ringisomorphismus $\mathrm{End}_R(R) \longrightarrow R^{\mathrm{op}}$ ist. ∎

4 Faktormoduln

Erneut sind Faktormoduln das Analogon der Begriffe Faktorraum/Faktorgruppe/Faktorring/...und liefern die Isomorphiesätze als Werkzeug für die Konstruktion von R-Isomorphismen.

Lemma-Definition 4.1 (*Faktormodul*)

Seien M ein R-Modul und $U \leqslant M$ ein R-Untermodul. Dann wird die Faktorgruppe M/U mit der äußeren Multiplikation

$$R \times M/U \longrightarrow M/U, (r, m + U) \mapsto r \cdot (m + U) := r \cdot m + U$$

zu einem R-Modul; der **Faktormodul von M nach U**.
Die Abbildung $\pi_U : M \twoheadrightarrow M/U, m \mapsto m + U$ ist ein surjektiver R-Homomorphismus.

Beweis:

(1) Die äußere Multiplikation ist wohldefiniert:
Seien $r \in R$ und $m_1, m_2 \in M$ mit $m_1 + U = m_2 + U$. Somit ist $m_1 - m_2 \in U$ und

$$rm_1 - rm_2 = r(m_1 - m_2) \in U \implies \impliedby rm_1 + U = rm_2 + U$$

und

$$r \cdot (m_1 + U) = rm_1 + U = rm_2 + U = r \cdot (m_2 + U) \in U \implies \impliedby rm_1 + U = rm_2 + U\,.$$

(2) Die R-Modul-Axiome gelten:
(M1) $(M/U, +)$ ist nach Algebra I eine abelsche Gruppe.
(M2) Seien $r, s \in R$ und $m \in M$. Dann gilt:

$$\begin{aligned}(r + s) \cdot (m + U) &\overset{\text{Def.}}{=} (r + s) \cdot m + U \\ &= (r \cdot m + s \cdot m) + U \qquad \text{nach (M2) für } M \\ &= (r \cdot m + U) + (s \cdot m + U) \\ &\overset{\text{Def.}}{=} r \cdot (m + U) + s \cdot (m + U)\,.\end{aligned}$$

(M3)—(M5) Analog und gelten nach (M3) — (M5) für M.

(3) Die Abbildung π_U ist ein surjektiver R-Homomorphismus:

- π_U ist ein surjektiver R-Homomorphismus nach Algebra I; und
- ferner gilt $\forall r \in R, \forall m \in M$:

$$\pi_U(r \cdot m) = (r \cdot m) + U = r \cdot (m + U) = r \cdot \pi_U(m)\,.$$

■

Aufgabe 4.2 (*Aufgabe 1(a), Blatt 2*)

Sei R ein beliebiges Ring, sei I ein zweiseitiges Ideal von R und sei M ein R-Modul. Zeigen Sie:

(i) $IM := \{\sum_{i=1}^{n} a_i x_i \in M \mid n \in \mathbb{N}, a_1, \ldots, x_n \in I \text{ und } x_1, \ldots, x_n \in M\}$ ist ein R-Untermodul von M; und

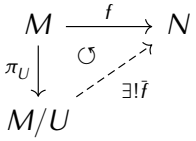
(ii) mit der Operation

$$R/I \times M/IM \longrightarrow M/IM,\ \big(r + I, m + IM\big) \mapsto rm + IM$$

ist die Faktorgruppe M/IM ein R/I-Modul.

Satz 4.3 (*Universelle Eigenschaft des Faktormoduls*)

Seien M, N zwei R-Moduln und $f \in \mathrm{Hom}_R(M, N)$. Ist $U \leqslant M$ mit $U \leqslant \mathrm{Ker}(f)$, dann $\exists!\, \bar{f} \in \mathrm{Hom}_R(M/U, N)$ mit $\bar{f} \circ \pi_U = f$:



Konkret ist $\bar{f}(m + U) := f(m) \quad \forall m + U \in M/U$. Ferner gelten:

- f surjektiv $\implies$ $\bar{f}$ surjektiv;
- $U = \mathrm{Ker}(f) \implies \bar{f}$ injektiv.

Beweis:

- Aus Algebra I bereits bekannt für die Gruppenstrukturen.
- Es ist übrig zu zeigen: $\bar{f}$ ist ein R-Homomorphismus.

  Seien $r \in R, m \in M$. Dann gilt:

$$\begin{aligned}\bar{f}(r \cdot (m + U)) &= \bar{f}(r \cdot m + U) = f \circ \pi_U(r \cdot m)\\ &= f(r \cdot m) = r \cdot f(m)\\ &= r \cdot (\bar{f} \circ \pi_U(m)) = r \cdot \bar{f}(m + U)\,.\end{aligned}$$

■

4.1 Die Isomorphisätze

Satz 4.4 (*1. Isomorphisatz/Homomorphiesatz*)

Seien M, N zwei R-Moduln und $f \in \mathrm{Hom}_R(M, N)$. Dann ist die Abbildung

$$\begin{aligned} M/\operatorname{Ker}(f) &\longrightarrow \operatorname{Bild}(f), \\ m + \operatorname{Ker}(f) &\mapsto f(m) \end{aligned}$$

ein R-Isomorphismus.

Beweis: Direkte Folgerung der universellen Eigenschaft des Faktormoduls. ∎

Satz 4.5 (*2. Isomorphisatz*)

Sei M ein R-Modul und seien $U, V \leqslant M$ R-Untermoduln. Dass ist die Abbildung

$$\begin{aligned} U/(U \cap V) &\longrightarrow (U + V)/V \\ u + U \cap V &\mapsto u + V \end{aligned}$$

ein R-Isomorphismus.

Satz 4.6 (*3. Isomorphisatz*)

Sei M ein R-Modul und seien $U, V \leqslant M$ R-Untermoduln. Ist $U \subseteq V$, so ist die Abbildung

$$\begin{aligned} (M/U)/(V/U) &\longrightarrow M/V \\ (m + U) + V/U &\mapsto m + V \end{aligned}$$

ein R-Isomorphismus.

Beweis vom 2. und 3. Isomorphisatz:

- Beide Aussagen gelten für die Gruppenstrukturen nach der Algebra I. Es sind Folgerungen aus dem 1. Isomorphiesatz für Gruppen.
- Nun gilt auch der 1. Isomorphisatz für die R-Modulstruktur. Das impliziert, dass beide Aussagen auch für die R-Modulstruktur gelten. ∎

Satz 4.7 (*Korrespondenzsatz*)

Ist $U \leqslant_R M$ ein R-Untermodul eines R-Moduls M, so induziert $\pi_U : M \longrightarrow M/U$ eine Bijektion

$$\begin{aligned} \{X \leqslant_R M \mid U \subseteq X\} &\xleftrightarrow{\sim} \{R\text{-Untermoduln von } M/U\} \\ X &\longmapsto X/U \\ \pi_U^{-1}(Z) &\longmapsfrom Z\,. \end{aligned}$$

Daher:
Ist $Z \leqslant M/U$, so existiert $X \leqslant M$ mit $U \leqslant X$ und $Z = X/U$.

Beweis: Erneut ist die Aussage für die Gruppenstrukturen bereits aus Algebra I bekannt.
Ferner sind X/U und $\pi_U^{-1}(Z)$ R-Untermoduln nach den obigen Ergebnissen. Demnach folgt die Aussage für die R-Modulstruktur. ■

4.2 Annulatoren

Definition 4.8 (*Annulatoren*)

Sei M ein R-Modul.

(a) Der **Annulator (in R)** eines Elements $x \in M$ ist

$$\mathrm{Ann}_R(x) := \{r \in R \mid r \cdot x = 0_M\}\,.$$

(b) Der **Annulator (in R)** einer Teilmenge $\varnothing \neq U \subseteq M$ ist

$$\mathrm{Ann}_R(U) := \bigcap_{x \in U} \mathrm{Ann}_R(x) = \{r \in R \mid r \cdot x = 0_M \ \forall\, x \in U\}\,.$$

Klar ist: $\mathrm{Ann}_R(x) = \mathrm{Ann}_R(\{x\})$.

Lemma 4.9

Ist M ein R-Modul, so gelten:

(a) $\mathrm{Ann}_R(U)$ ist ein Linksideal von R $\forall \varnothing \neq U \subseteq M$;

(b) $U \leqslant M \Longrightarrow \mathrm{Ann}_R(U)$ ist ein (zweiseitiges) Ideal von R;

(c) $\forall x \in M$ gilt $\mathrm{Ann}_R(x) = \mathrm{Ker}(r_x)$ und

$$R^{\mathrm{reg}}/\mathrm{Ann}_R(x) \cong_R Rx\,.$$

Beweis: (a) Zunächst zeigen wir, dass $\mathrm{Ann}_R(x)$ ein Linksideal von R ist $\forall x \in U$.
$\mathrm{Ann}_R(x) \neq \varnothing$, da $0_R x = 0_M \Longrightarrow 0_R \in \mathrm{Ann}_R(x)$. Zudem gilt für $r_1, r_2 \in \mathrm{Ann}_R(x)$, dass

$$(r_2 - r_1) \cdot x = r_1 \cdot x - r_2 \cdot x = 0_M - 0_M = 0_M\,.$$

Also $r_2 - r_1 \in \mathrm{Ann}_R(x)$. Somit ist $\mathrm{Ann}_R(x)$ eine Untergruppe von $(R, +)$
Füer $s \in R$ und $r \in \mathrm{Ann}_R(x)$ ist dann $(s \cdot r) \cdot x = s \cdot (r \cdot x) = s \cdot 0_M = 0_M$, also $s \in \mathrm{Ann}_R(x)$. Somit ist $\mathrm{Ann}_R(x)$ ein Linksideal.
Als Schnitt von Linksidealen von R ist $\mathrm{Ann}_R(U)$ dann auch ein Linksideal von R.

(b) Aus (a) ist bekannt, dass $\mathrm{Ann}_R(U)$ ein Linksideal ist von R. Es bleibt also zu zeigen, dass

$$r \cdot s \in \mathrm{Ann}_R(U) \quad \forall\, s \in R,\ \forall\, r \in \mathrm{Ann}_R(U)\,.$$

Sei $x \in U, s \in R$ und $r \in \mathrm{Ann}_R(U)$. Dann gilt: $(r \cdot s) \cdot x = r \cdot (s \cdot x) = 0_M$, da $s \cdot x \in U$ (wegen $U \leqslant M$) und $r \in \mathrm{Ann}_R(U)$. Somit ist $r \cdot s \in \mathrm{Ann}_R(x)$. Weil dies $\forall x \in U$ gilt, erhalten wir

$$r \cdot s \in \bigcap_{x \in U} \mathrm{Ann}_R(x) = \mathrm{Ann}_R(U)\,.$$

(c) Wir haben bereits gesehen, dass $r_x : R^{\mathrm{Reg}} \twoheadrightarrow Rx = \langle x \rangle_R, r \mapsto r \cdot x$ ein surjektiver R-Ringhomomorphismus ist. Zudem ist $\mathrm{Ker}(r_x) = \{r \in R | r \cdot x = 0_M\} = \mathrm{Ann}_R(x)$. Der Homomorphiesatz liefert also

$$R^{\mathrm{Reg}}/\mathrm{Ann}_R(x) = R^{\mathrm{Reg}}/\mathrm{Ker}(r_x) \cong \mathrm{Bild}(r_x) = Rx\,.$$

■

Aufgabe 4.10 (*Aufgabe 1(b), Blatt 2*)

Sei R ein Integritätsring. Zeigen Sie:

(i) Die Menge $T(M) := \{x \in M \mid \mathrm{Ann}_R(x) \neq 0\}$ ist ein R-Untermodul von M (der **Torsionsmodul** von M); und

(ii) der Faktormodul $\overline{M} := M/T(M)$ ist **torsionsfrei**, d.h. $T\left(\overline{M}\right) = 0$.

5 Einfache Moduln

Definition 5.1 (*einfacher Modul*)

Ein R-Modul M heißt einfach, wenn die folgenden Bedingungen erfüllt sind:

(1) $M \neq 0$; und

(2) M und $\{0_M\}$ sind die einzigen R-Untermoduln von M.

Diese Definition passt zur Definition einfacher Gruppen in der Gruppentheorie.

Beispiel 6

(1) Der K-Vektorraum $V := K$ ist einfach. Denn $\dim_K(K) = 1$, also sind K und $\{0\}$ die einzigen Unterräume.

(2) Achtung! $\mathbb{Z}$ ist nicht einfach als $\mathbb{Z}$-Modul!
Es ist $2\mathbb{Z}$ ein $\mathbb{Z}$-Untermodul von $\mathbb{Z}$, aber $\{0\} \neq 2\mathbb{Z} \neq \mathbb{Z}$

Anmerkung 5.2

Die einfachen $\mathbb{Z}$-Moduln sind genau $\{\mathbb{Z}/p\mathbb{Z} \mid p \in \mathbb{Z}_{>0}$ Primzahl$\}$.

Für eine abelsche Gruppe A gilt:
A ist einfach als $\mathbb{Z}$-Modul $\iff$ A ist einfach als Gruppe.

Lemma 5.3

Jeder einfache R-Modul M ist R-isomorph zu einem Faktormodul von R^{reg}, denn es gilt

$$M \cong_R R^{\mathrm{reg}}/\mathrm{Ann}_R(x) \quad \forall\, x \in M \backslash \{0\}\,.$$

Beweis: Nach dem vorherigen Lemma gilt $\forall x \in M\backslash\{0\}$: $R^{\text{reg}}/\text{Ann}_R(x) \cong_R Rx$. Weil M einfach ist, gilt $Rx \in \{0, M\}$ und $x \neq 0$ liefert $Rx = M$. ■

Satz 5.4 (Schurs Lemma)

Seien M und N zwei einfache R-Moduln.

(a) Ist $M \ncong N$, so gilt $\text{Hom}_R(M, N) = \{0\}$.

(b) Ist $M = N$, so ist $\text{End}_R(M)$ ein Schiefkörper.

Zur Erinnerung: Ein Ring R ist ein **Schiefkörper**, wenn

(1) $1_R \neq 0_R$; und

(2) $R^\times = R\backslash\{0_R\}$.

Kommutativität wird nicht gefordert.

Beweis: Sei $f \in \text{Hom}_R(M, N)\backslash\{0\}$. Dann:
M einfach $\Longrightarrow \text{Ker}(f) \in \{0, M\} \Longrightarrow \text{Ker}(f) = 0$, da $f \neq 0$ ist; und
N einfach $\Longrightarrow \text{Bild}(f) \in \{0, N\} \Longrightarrow \text{Bild}(f) = N$, da $f \neq 0$ ist.
Gemeinsam mit dem Homomorphiesatz folgt: $M \cong M/\text{Ker}(f) \cong \text{Bild}(f) = N$. $(*)$

(a) $M \ncong N$ und $(*) \Longrightarrow \text{Hom}_R(M, N) = 0$

(b) (1) $(\text{End}_R(M), +, \circ)$ ist ein Ring nach Aufgabe 3.4;
(2) $1_{\text{End}_R(M)} = \text{id}_M \neq 0 = 0_{\text{End}_R(M)}$;
(3) nach (1) und (2) gilt $\text{End}_R(M)\backslash\{0\} = \text{End}_R(M)^\times$.
(1),(2),(3) $\Longrightarrow \text{End}_R(M)$ ist ein Schiefkörper. ■

6 Exakte Sequenzen

6.1 Grundlegende Eigenschaften

Definition 6.1 (*exakte Sequenz*)

(1) Eine Sequenz $\cdots \xrightarrow{\varphi_{i-1}} M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \xrightarrow{\varphi_{i+2}} \cdots$ von R-Moduln und R-Homomorphismen heißt **exakt an der Stelle** M_i, wenn $\text{Ker}(\varphi_{i+1}) = \text{Bild}(\varphi_i)$. Sie heißt **exakt**, falls sie an allen Stellen exakt ist.

(2) Eine **kurze exakte Sequenz** (kurz: k.e.S.) ist eine exakte Sequenz der Form

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0\,.$$

Anmerkung 6.2

$\text{Ker}(\varphi_{i+1}) = \text{Bild}(\varphi_i) \longrightarrow \varphi_{i+1} \circ \varphi_i : M_{i-1} \longrightarrow M_{i+1}$ ist die Nullabbildung.

Anmerkung 6.3

Für R-Moduln und R-Homomorphismen gelten:

(a) $L \xrightarrow{\varphi} M$ injektiv $\iff$ $0 \to L \xrightarrow{\varphi} M$ exakt;

(b) $M \xrightarrow{\psi} N$ surjektiv $\iff$ $M \xrightarrow{\psi} N \to 0$ exakt;

(c) Übung: $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ ist genau dann eine kurze exakte Sequenz, wenn

(1) φ ist injektiv;

(2) ψ ist surjektiv; und

(3) ψ induziert einen R-Isomorphismus $\overline{\psi} : M/\mathrm{Bild}(\varphi) \longrightarrow N$.

Beispiel 7

(1) Ist $\psi \in \mathrm{Hom}_R(M, N)$ surjektiv, so existiert eine k.e.S.

$$0 \to \mathrm{Ker}(\psi) \xrightarrow{i} M \xrightarrow{\psi} N \to 0\,,$$

wobei $i : \mathrm{Ker}(\psi) \longrightarrow M$ die kanonische Inklusion ist.

(2) Ist $\varphi \in \mathrm{Hom}_R(L, M)$ injektiv, so existiert eine k.e.S.

$$0 \to L \xrightarrow{\varphi} M \xrightarrow{\pi} \mathrm{Coker}(\varphi) \to 0\,,$$

wobei $\mathrm{Coker}(\varphi) := M/\mathrm{Bild}(\varphi)$ und $\pi : M \twoheadrightarrow M/\mathrm{Bild}(\varphi)$ die kanonische Abbildung ist.

(3) Die Sequenzen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & [a] & \mapsto & ([a],[0]) & & & & \\ & & & & ([a],[b]) & \mapsto & [b] & & \end{array}$$

und

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & [1] & \mapsto & [2] & & & & \\ & & & & [1] & \mapsto & [1] & & \end{array}$$

sind kurze exakte Sequenzen von $\mathbb{Z}$-Moduln.

Definition 6.4

Eine kurze exakte Sequenz $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ von R-Moduln **zerfällt** (oder ist zerfallend), wenn $\exists\, \sigma \in \mathrm{Hom}_R(M, N)$ mit $\psi \circ \sigma = \mathrm{id}_N$. (Die Abbildung σ heißt **Sektion** für ψ.)

Schreibweise: $0 \longrightarrow L \xrightarrow{\varphi} M \underset{\sigma}{\overset{\psi}{\rightleftarrows}} N \longrightarrow 0\,.$

Beispiel 8

(3) Zurück zum letzten Beispiel:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & [a] & \mapsto & ([a],[0]) & & & & \\ & & & & ([a],[b]) & \mapsto & [b] & & \end{array}$$

zerfällt, denn die Abbildung

$$\sigma : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, [b] \mapsto ([0],[b])$$

erfüllt
$\sigma \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$ und $\psi \circ \sigma([b]) = \psi(([0],[b])) = [b]$, d.h. $\psi \circ \sigma = \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$.

Lemma 6.5

Für eine k.e.S. $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ von R-Moduln sind äquivalent:

(1) die Sequenz zerfällt;

(2) $\exists\, \rho \in \mathrm{Hom}_R(M, L)$, so dass $\rho \circ \varphi = \mathrm{id}_L$ gilt (ρ heißt **Retraktion** für φ); und

(3) $\exists\, M' \leqslant M$ mit $M = \mathrm{Bild}(\varphi) \oplus M'$.

In diesem Fall heißt M' **direkter Summand** von M.

Beweis: von ($(1) \iff (3)$**)**:
$((1) \implies (3))$: Nach (1) $\exists \sigma \in \mathrm{Hom}_R(M, N)$ mit $\psi \circ \sigma = \mathrm{id}_N$. Setze $M' := \sigma(N)$.
Behauptung: $M = M' \oplus \mathrm{Bild}(\varphi) (= M' \oplus \mathrm{Ker}(\psi))$.
Sei $x \in M' \implies \exists n \in N$ mit $x = \sigma(n) \implies n = \psi \circ \sigma(n) = \psi(x) = 0$, da $x \in \mathrm{Ker}(\psi) \implies x = \sigma(n) = \sigma(0) = 0 \implies \mathrm{Ker}(\psi) \cap M' = 0$.
Sei $x \in M$. Schreibe $x = x + 0 = x - \sigma(\psi(x)) + \sigma(\psi(x))$. Es ist $x - \sigma(\psi(x)) \in \mathrm{Ker}(\psi)$ und $\sigma(\psi(x)) \in \sigma(N) = M' \implies \mathrm{Ker}(\psi) + M' = M$.

$((3) \implies (1))$: Sei $M' \neq M$ mit $M = M' \oplus \mathrm{Bild}(\varphi) \implies \psi|_{M'} : M' \longrightarrow N$ ist ein R-Isomorphismus $\implies \sigma := i \circ (\psi|_{M'}) : N \longrightarrow M$ erfüllt $\psi \circ \sigma = \mathrm{id}_N$.

($(1) \iff (2)$**)**: Aufgabe 2(a), Blatt 2.

■

Beispiel 9

Noch einmal zurück zum letzten Beispiel! Die Sequenz

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & [1] & \mapsto & [2] & & & & \\ & & & & [1] & \mapsto & [1] & & \end{array}$$

ist keine zerfallende k.e.S. von $\mathbb{Z}$-Moduln, weil $\mathbb{Z}/4\mathbb{Z} \not\cong_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 6.6 (*Aufgabe 2(b), Blatt 2*)

Seien $m, n \in \mathbb{Z}_{\geqslant 2}$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(1) m und n sind Teilerfremd;

(2) die kurze exakte Sequenz $0 \longrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$ zerfällt, wobei die Abbildung $\cdot n$ (bzw. die Abbildung π) die Multiplikation mit n (bzw. die kanonische Abbildung) ist;

(3) $\mathbb{Z}/mn\mathbb{Z} \cong_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

Aufgabe 6.7 (*Aufgabe 3, Blatt 2*)

Betrachten Sie das folgende kommutative Diagramm von R-Moduln und R-Homomorphismen mit exakten Zeilen:

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5 \end{array}$$

Zeigen Sie die folgenden Aussagen.

(a) Angenommen α_1 ist surjektiv und α_2 und α_4 sind injektiv, so ist α_3 injektiv.

(b) Angenommen α_2 und α_4 sind surjektiv und α_5 ist injektiv, so ist α_3 surjektiv.

(c) Angenommen α_1 ist surjektiv, α_5 ist injektiv und α_2, α_4 sind R-Isomorphismen, so ist α_3 ein R-Isomorphismus.

(d) Sind $A_1 = A_5 = B_1 = B_5 = 0$ und $\alpha_1 = \alpha_5 = 0$, so gilt: α_3 ist ein R-Isomorphismus, wenn α_2 und α_4 R-Isomorphismen sind.
Gilt die Umkehrung?

Konvention: Wenn nicht anders gesagt, bedeuten „K.e.S. "und „K.e.S. von R-Moduln"stets „K.e.S. von R-Moduln und R-Homomorphismen", wobei R der im Kontext betrachtete Ring ist.

Schreibweise 6.8

Sei Q ein R-Modul.

(1) Ist $\varphi : L \to M$ ein R-Homomorphismus, so setzen wir

$$\begin{aligned} \varphi_* := \mathrm{Hom}_R(Q, \varphi) : \mathrm{Hom}_R(Q, L) &\longrightarrow \mathrm{Hom}_R(Q, M) \\ \alpha &\longmapsto \varphi_*(\alpha) := \varphi \circ \alpha \,. \end{aligned}$$

(2) Ist $\varphi : L \to M$ ein R-Homomorphismus, so setzen wir

$$\begin{aligned} \varphi^* := \mathrm{Hom}_R(\varphi, Q) : \mathrm{Hom}_R(M, Q) &\longrightarrow \mathrm{Hom}_R(L, Q) \\ \beta &\longmapsto \varphi^*(\beta) := \beta \circ \varphi \,. \end{aligned}$$

Bemerkung 6.9

(1) Ist $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ eine k.e.S. von R-Moduln, so ist die induzierte Sequenz

$$0 \to \mathrm{Hom}_R(Q, L) \xrightarrow{\varphi_*} \mathrm{Hom}_R(Q, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(Q, N)$$

eine exakte Sequenz von abelschen Gruppen.

(2) Ist $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ eine K.e.S. von R-Moduln, so ist die induzierte Sequenz

$$0 \to \mathrm{Hom}_R(N, Q) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_R(L, Q)$$

eine exakte Sequenz von abelschen Gruppen.

Beweis:

(1) **Exaktheit in $\mathrm{Hom}_R(Q, L)$.** Z.z.: φ_* ist injektiv, d.h. $\mathrm{Ker}(\varphi_*) = 0$.
Sei also $\alpha \in \mathrm{Hom}_R(Q, L)$ mit $\varphi_*(\alpha) = 0$. Daraus folgt:

$$0 = \varphi_*(\alpha)(x) = \varphi \circ \alpha(x) \forall\, x \in Q \quad \Longrightarrow \quad \alpha(x) = 0,$$

denn φ ist injektiv nach Voraussetzung, d.h. $\alpha = 0$.

Exaktheit in $\mathrm{Hom}_R(Q, M)$. Z.z.: $\mathrm{Ker}(\psi_*) = \mathrm{Bild}(\varphi_*)$.

„$\subseteq$“: Sei $\alpha \in \mathrm{Ker}(\psi_*)$.
$\Longrightarrow 0 = \psi_*(\alpha) = \psi \circ \alpha$
$\Longrightarrow \forall\, x \in Q$ gilt $\psi(\alpha(x)) = 0$, d.h. $\alpha(x) \in \mathrm{Ker}(\psi) = \mathrm{Bild}(\varphi)$ (nach Vorraussetzung)
$\Longrightarrow \forall\, x \in Q, \exists y_x \in L$ mit $\varphi(y_x) = \alpha(x)$ und y_x ist eindeutig bestimmt, weil φ ingektiv ist.
Somit ist die Abbildung

$$\begin{aligned} \beta : Q &\mapsto L \\ x &\mapsto y_x \end{aligned}$$

wohldefiniert. Wegen $\beta = \left(\varphi^{-1}|_{\mathrm{Bild}(\varphi)}\right) \circ \alpha$ gelten:

$$\begin{cases} 1. & \beta \text{ ist-}R\text{-linear, und} \\ 2. & \varphi_*(\beta) = \varphi \circ \beta = \alpha, \end{cases}$$

d.h $\alpha \in \mathrm{Bild}(\varphi_*)$.

„$\supseteq$“: Sei nun $\alpha \in \mathrm{Bild}(\varphi_*)$.
$\Longrightarrow \exists \beta \in \mathrm{Hom}_R(Q, L)$ mit $\varphi_*(\beta) = \alpha$
$\Longrightarrow \psi_*(\alpha) = \psi_*(\varphi_*(\beta)) = \underbrace{(\psi \circ \varphi)}_{=0}(\beta) = 0 \implies \alpha \in \mathrm{Ker}(\varphi_*)$

(2) Analog! (Übung) ∎

6.2 Diagramm-Lemmata*

In der Literatur gibt es eine ganze Reihe von Diagramm-Lemmata: Es sind Aussagen, die kommutative Diagramme von R-Moduln und R-Homomorphismen mit exakten Sequenzen voraussetzen und die Existenz/Eindeutigkeit, Surjektivität, Injektivität, Bijektivität, ... von anderen R-Homomorphismen feststellen. In diesem Abschnitt geben wir drei Beispiele an.

Beispiel 10 (*Das Fünferlemma (Aufgabe 3, Blatt 2)*)

Ist

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5 \end{array}$$

ein kommutatives Diagramm von R-Moduln und R-Homomorphismen mit exakten Zeilen, so gilt:

(a) α_1 surjektiv und α_2, α_4 injektiv $\implies$ α_3 injektiv.

(b) α_2, α_4 surjektiv und α_5 injektiv $\implies$ α_3 surjektiv.

Wir verwenden oft die „kurze“ Version; das sogenannte **„2-von-3-Lemma“**: Ist

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_2} & \circlearrowleft & \downarrow{\scriptstyle \alpha_3} & \circlearrowleft & \downarrow{\scriptstyle \alpha_4} & & \\ 0 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von R-Moduln und R-Homomorphismen mit exakten Zeilen, so gilt: Sind zwei Morphismen aus $\{\alpha_1, \alpha_2, \alpha_3\}$ R-Isomorphismen, so ist auch der dritte Morphismus ein R-Isomorphismus.

Beispiel 11 (*Das Schlangenlemma*)

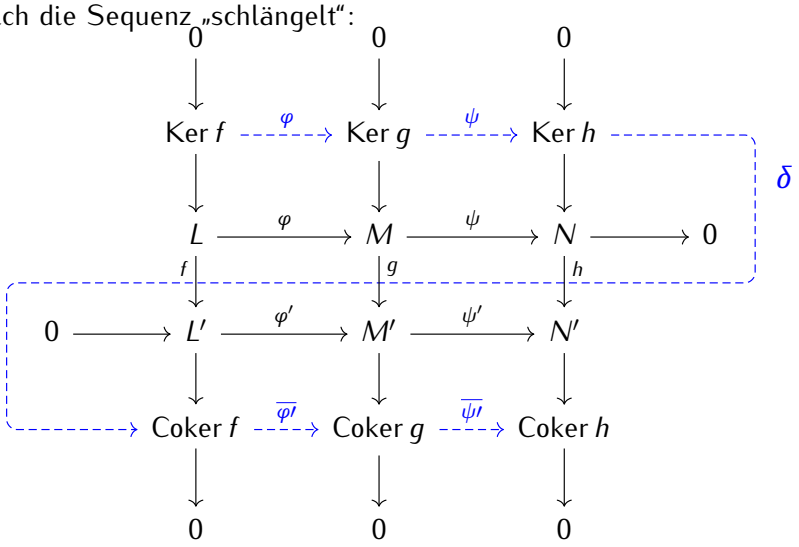
Ist

$$\begin{array}{ccccccccc} & & L & \xrightarrow{\varphi} & M & \xrightarrow{\psi} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \xrightarrow{\varphi'} & M' & \xrightarrow{\psi'} & N' & & \end{array}$$

ein kommutatives Diagramm von R-Moduln und R-Homomorphismen mit exakten Zeilen, so existiert eine exakte Sequenz

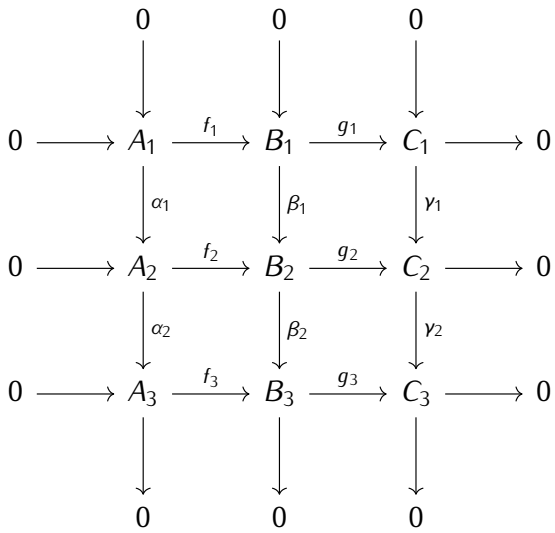
$$\operatorname{Ker} f \xrightarrow{\varphi} \operatorname{Ker} g \xrightarrow{\psi} \operatorname{Ker} h \xrightarrow{\delta} \operatorname{Coker} f \xrightarrow{\overline{\varphi'}} \operatorname{Coker} g \xrightarrow{\overline{\psi'}} \operatorname{Coker} h$$

von R-Moduln und R-Homomorphismen. Erweitert man das Diagramm um Kerne und Cokerne, so sieht man, wie sich die Sequenz „schlängelt“:



Beispiel 12 (*Das* 3×3*-Lemma*)

Ist



ein kommutatives Diagramm von R-Moduln und R-Homomorphismen mit exakten Spalten, so gelten:

(a) 2. und 3. Zeilen exakt $\implies$ die 1. Zeile ist exakt; und

(b) 1. und 2. Zeilen exakt $\implies$ die 3. Zeile ist exakt.

Alle Beweise per „Diagram chasing"!

7 Projektive and Injektive Moduln

Wir führen nun drei wichtige Klassen von Moduln ein.

1. Die **projektiven** Moduln: Diese Moduln haben die Eigenschaft, dass die Sequenz von abelschen Gruppen aus Bemerkung 6.9(1) wieder eine **k.e.S.** ist. D.h. die Sequenz

$$0 \to \mathrm{Hom}_R(Q, L) \xrightarrow{\varphi_*} \mathrm{Hom}_R(Q, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(Q, N) \to 0$$

   ist exakt.

2. Die **injektiven** Moduln: Diese Moduln haben die Eigenschaft, dass die Sequenz von abelschen Gruppen aus Bemerkung 6.9(2) wieder eine **k.e.S.** ist. D.h. die Sequenz

$$0 \to \mathrm{Hom}_R(N, Q) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, Q) \xrightarrow{\varphi^*} \mathrm{Hom}_R(L, Q) \to 0$$

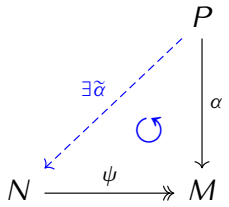
   ist exakt.

3. Die **freien** Moduln: Diese Moduln besitzen eine Basis.

Lemma-Definition 7.1 (*Projektiver Modul*)

Ein R-Modul P heißt **projektiv**, wenn die folgenden äquivalenten Bedingungen erfüllt sind.

(1) $\forall$ R-Moduln $M, N, \forall\, \alpha \in \mathrm{Hom}_R(P, N)$ und $\forall\, \psi \in \mathrm{Hom}_R(M, N)$ surjektiv: $\exists\, \widetilde{\alpha} \in \mathrm{Hom}_R(P, M)$ mit $\psi \circ \widetilde{\alpha} = \alpha$:



(2) Für jede K.e.S. $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ von R-Moduln ist die induzierte Sequenz

$$0 \to \mathrm{Hom}_R(P, L) \xrightarrow{\varphi_*} \mathrm{Hom}_R(P, M) \xrightarrow{\psi_*} \mathrm{Hom}_R(P, N) \longrightarrow 0$$

exakt.

Beweis: Zunächst beobachten wir, dass nach der Bemerkung gilt:

($\circledast$) Bedingung (2) $\iff$ ψ_* ist surjektiv

(1) $\Longrightarrow$ (2): Sei $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ ein k.e.S. von R-Moduln und sei $\alpha \in \mathrm{Hom}_R(P, N)$. Nach (1) existiert $\widetilde{\alpha} \in \mathrm{Hom}_R(P, M)$, sodass

$$\alpha = \psi \circ \widetilde{\alpha} = \psi_*(\widetilde{\alpha})\,.$$

Somit ist ψ_* surjektiv und Bedingung (2) gilt nach $\circledast$.

(2) $\Longrightarrow$ (1): Seien M, N R-Moduln, sei $\psi \in \mathrm{Hom}_R(M, N)$ surjektiv und sei $\alpha \in \mathrm{Hom}_R(P, N)$. Betrachte dann die K.e.S.

$$0 \longrightarrow \mathrm{Ker}(\psi) \xhookrightarrow[\text{Inklusion}]{\text{kan.}} M \xrightarrow{\psi} N \longrightarrow 0$$

Nach $\circledast$ ist Ψ_* sunjektiv. Daher existiert $\widetilde{\alpha} \in \mathrm{Hom}_R(P, M)$ mit

$$\alpha = \psi_*(\widetilde{\alpha}) = \psi \circ \widetilde{\alpha}\,,$$

wie verlangt! ■

Beispiel 13

(1) Der K-Vektorraum K (der Dimension 1) ist projektiv.
Klar: In diesem Fall ist die Sequenz

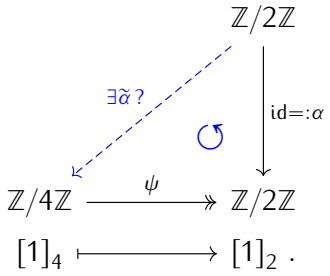
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_K(K, L) & \xrightarrow{\varphi_*} & \mathrm{Hom}_K(K, M) & \xrightarrow{\psi_*} & \mathrm{Hom}_K(K, N) & \longrightarrow & 0 \\ & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\ & & L & & M & & N & & \end{array}$$

aus der Definition stets exakt aus „Dimensionsgründen“!
Weil die Sequenz $0 \to L \to M \to N \to 0$ exakt ist, liefert der Rangsatz

$$\dim_k M = \dim_k L + \dim_K N$$

und somit muss ψ_* surjektiv sein.

(2) Die abelsche Gruppe $\mathbb{Z}/2\mathbb{Z}$ betrachtet als $\mathbb{Z}$-Modul ist **nicht** projektiv:
Betrachte das Diagramm



$$\text{Hier: } \nexists\, \widetilde{\alpha} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}) \quad \text{mit } \alpha = \psi \circ \widetilde{\alpha},$$

denn die einzige Möglichkeit wäre

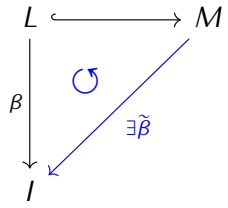
$$\widetilde{\alpha} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$$
$$[1]_2 \mapsto [2]_4$$

und somit wäre $\psi \circ \widetilde{\alpha}\,([1]_2) = [0]_2 \neq [1]_2 = \mathrm{id}\,([1]_2)$.

Lemma-Definition 7.2 (*Injektiver Modul*)

Ein R-Modul I heißt **injektiv**, wenn die folgenden äquivalenten Bedingungen erfüllt sind.

(1) $\forall$ R-Moduln $L, M, \forall\, \varphi \in \mathrm{Hom}_R(L, M)$ injektiv und $\forall\, \beta \in \mathrm{Hom}_R(L, I)$, $\exists\, \widetilde{\beta} \in \mathrm{Hom}_R(M, I)$ mit $\widetilde{\beta} \circ \varphi = \beta$:



(2) Für jede K.e.S. $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ von R-Moduln ist die induzierte Sequenz

$$0 \to \mathrm{Hom}_R(N, I) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, I) \xrightarrow{\varphi^*} \mathrm{Hom}_R(L, I) \longrightarrow 0$$

exakt.

Beweis: Analog zum Beweis der Projektivität! (Übung!) ■

Beispiel 14

(1) Der K-Vektorraum K ist injektiv.
Analog zur Projektivität: Aus Dimensionsgründen!

(2) Siehe auch das Blatt 3.

Aufgabe 7.3 (*Aufgabe 1, Blatt 3*)

(a) Sei I ein R-Modul. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

(i) I ist injektiv;

(ii) jede k.e.S. $0 \longrightarrow I \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ von R-Moduln zerfällt.

(b) Sei P ein R-Modul. Zeigen Sie mithilfe der Definition der Projektivität, dass die folgenden Aussagen äquivalent sind:

(i) P ist projektiv;

(ii) jede k.e.S. $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} P \longrightarrow 0$ von R-Moduln zerfällt.

Aufgabe 7.4 (*Aufgabe 3, Blatt 3*)

Zeigen Sie:

(a) Ist $e \in R$ ein Idempotent (d.h. $e^2 = e$), so sind Re und $R(1-e)$ projektive R-Moduln.

(b) Sind P und Q zwei projektive R-Moduln, so existiert ein freier R-Modul F mit $F \oplus P \cong F \oplus Q$.

(c) Sind P und Q zwei projektive R-Moduln und

$$0 \longrightarrow M \xrightarrow{\varphi} P \xrightarrow{\psi} A \longrightarrow 0 \quad \text{und} \quad 0 \longrightarrow N \xrightarrow{\varphi'} Q \xrightarrow{\psi'} A \longrightarrow 0$$

zwei k.e.S. von R-Moduln, so gilt $M \oplus Q \cong N \oplus P$.

[Hinweis: Betrachen Sie $X := \{(p,q) \in P \oplus Q \mid \psi(p) = \psi'(q)\}$.]

Aufgabe 7.5 (*Aufgabe 1, Blatt 4*)

Sei E ein R-Modul mit der folgenden Eigenschaft: Für jedes Ideal I von R und für jeden R-Homomorphismus $f : I \longrightarrow E$ existiert ein R-Homomorphismus $g : R \longrightarrow E$ mit $g|_I = g \circ i_I = f$, wobei $i_I : I \longrightarrow R$ die kanonische Inklusion bezeichnet.

(a) Sei B ein R-Modul, sei $A \leqslant_R B$ ein R-Untermodul, bezeichne mit $i_A : A \longrightarrow B$ die kanonische Inklusion von A in B und sei $f : A \longrightarrow E$ ein R-Homomorphismus. Sei X die Menge aller Paare (A', g'), so dass $A \leqslant_R A' \leqslant_R B$ ein R-Untermodul ist, und $g' : A' \longrightarrow E$ ist ein R-Homomorphismus mit $g'|_A = f$. Zudem sind $(A', g'), (A'', g'') \in X$, so definieren wir

$$(A', g') \leqslant (A'', g'') \iff (A' \leqslant_R A'' \text{ und } g''|_{A'} = g') .$$

(i) Zeigen Sie, dass die Relation $\leqslant$ eine Halbordnung auf X ist.

(ii) Zeigen Sie, dass $(X, \leqslant)$ die Voraussetzungen von dem Zornschen Lemma erfüllt.

(b) Zeigen Sie, dass E injektiv ist, indem Sie zeigen, dass es ein R-Homomorphismus $\widetilde{f} : B \longrightarrow E$ mit $\widetilde{f} \circ i_A = f$ gibt.

[Hinweise: Betrachten Sie ein maximales Element (A_0, g_0) in X und zeigen Sie, dass $A_0 = B$. Sonst: Ist $A_0 \neq B$, so existiert $b \in B \backslash A_0$ und $I := \{r \in R \mid rb \in A_0\}$ ist ein Ideal von R. Finden Sie einen Widerspruch zur Maximalität von (A_0, g_0).]

8 Freie Moduln

Wir führen nun endlich die freien Moduln ein, als Moduln, die eine Basis besitzen. Damit ist der Begriff des freien Moduls die beste Verallgemeinerung der Begriffe Vektorraum oder freie abelsche Gruppe.

Definition 8.1 (*R-linear (Un)abhängigkeit, Erzeugendensystem*)

Sei M ein R-Modul. Sei $X \subseteq M$ eine Teilmenge. Dann heißt X:

- **(R)-linear unabhängig** (oder **R-frei**), wenn sich 0_M nur trivial als R-Lineankombination von Elementen aus X darstellen lässt, d.h.

$$\left(0_M = \sum_{i=1}^{m} r_i \cdot m_i \quad \text{mit } m \in \mathbb{N},\ r_1, \ldots, r_m \in R,\ m_i, \ldots, m_m \in X \implies r_1 = \ldots = r_m = 0_R\right)$$

  und andernfalls heißt X **(R)-linear abhängig**;

- ein **Erzeugendensystem** für M, wenn $M = \langle X \rangle_R$ ist.

Anmerkung 8.2

Für $X = \{x_1, \ldots, x_m\}$ mit $m \in \mathbb{N}$, schreiben wir $\langle X \rangle_R = \langle \{x_1, \ldots, x_m\} \rangle_R =: \langle x_1, \ldots, x_m \rangle_R$.

Anmerkung 8.3

(0) Die leere Menge $\varnothing$ ist stets R-linear unabhängig, und $\{0\}$ ist stets R-linear abhängig.

(1) Enthählt X ein **Torsionselement** (d.h. aus $T(M) = \{x \in M \mid \mathrm{Ann}_R(x) \neq 0\}$) (siehe Aufgabe 1, Blalt 2) so ist X R-linear abhängig.

Definition 8.4 (*R-Basis*)

Eine **R-Basis** eines R-Moduls ist eine Teilmenge $X \subseteq M$, sodass gilt:

(i) X ist R-linear unabhängig; und

(ii) X ist ein Erzeugendensystem für M.

Definition 8.5 (*freier Modul, endlich erzeugter Modul*)

Ein R-Modul M heißt:

(1) **(R-)frei**, falls er eine R-Basis besitzt;

(2) **endlich erzeugt**, wenn er ein endliches Erzeugendensystem besitzt.

Beispiel 15

(1) Jeder K-Vektorraum ist K-frei. (Bekannt aus der L.A.)

(2) Die abelsche Gruppe $\mathbb{Z}/2\mathbb{Z}$ ist **kein** freier $\mathbb{Z}$-Modul, da beide $[0]_2$ und $[1]_2$ Torsionselemente sind! Somit existiert keine $\mathbb{Z}$-Basis!

(3) Dagegen ist $\mathbb{Z}/2\mathbb{Z}$ frei als $\mathbb{Z}/2\mathbb{Z}$-Modul, mit $\mathbb{Z}/2\mathbb{Z}$-Basis $X = \{[1]_2\}$.

Aufgabe 8.6

(a) Zeigen Sie: Die Menge $\{2, 3\}$ ist ein minimales Erzeugendensystem des regulären $\mathbb{Z}$-Moduls $\mathbb{Z}$ (d.h., keine echte Teilmenge ist ein Erzeugendensystem), aber nicht $\mathbb{Z}$-frei.

(b) Finden Sie alle $\mathbb{Z}$-linear unabhängige Teilmengen des $\mathbb{Z}$-Moduls $\mathbb{Q}$.

(c) Zeigen Sie: Für den Ring $R := \mathbb{Z}[X_i \mid i \in \mathbb{N}]$ gilt $R^{\text{reg}} = \langle 1 \rangle_R$, aber der R-Untermodul $\sum_{i\in\mathbb{N}} RX_i$ hat kein endliches Erzeugendensystem.

(d) Zeigen Sie: Der regulärer $\mathbb{Z}$-Modul $\mathbb{Z}$ ist $\mathbb{Z}$-frei aber nicht injektiv.

(e) Finden Sie einen R-Modul, der projektiv aber nicht R-frei ist.

Schreibweise 8.7

Ist ein R-Modul $M = M_1 \oplus M_2$ die (innere oder äußere) direkte Summe zweier R-Moduln M_1 und M_2, so heißen M_1 und M_2 **direkte Summanden** von M. Wir schreiben dann auch $M_1 \mid M$ und $M_2 \mid M$. Dies hat nichts mit klassischen „Teilbarkeit“ zu tun.

Beispiel 16

(3′) Der reguläre R-Modul R^{reg} ist R-frei mit Basis $X = \{1_R\}$.

(4) Der Nullmodul 0 ist R-frei mit Basis $X = \varnothing$.

Folgerung 8.8

Die einzige endliche abelsche Gruppe G, die frei als $\mathbb{Z}$-Modul ist, ist die triviale Gruppe 0 (mit $\mathbb{Z}$-Basis $\varnothing$).

Beweis: Nach dem Satz von Lagrange ist klar, dass $T(G) = G$ ist. Damit ist $\varnothing \subseteq G$ die einzige R-linear unabhängige Teilmenge. ∎

Bemerkung 8.9

(a) Ist M ein freier R-Modul mit R-Basis X, dann lässt sich jedes Element $m \in M$ eindeutig als R-Linearkombination von Elementen aus X darstellen, d.h.

$$m = \sum_{x\in X} a_x \cdot x$$

mit $\{a_x\}_{x\in X} \subset R$ und jedes a_x ($x \in X$) ist eindeutig bestimmt. Deshalb ist die Abbildung

$$\begin{aligned} \bigoplus_{x\in X} R^{\text{reg}} &\to M \\ (r_x)_{x\in X} &\mapsto \sum_{x\in X} r_x \cdot x \end{aligned}$$

ein R-Isomorphismus. Also können wir $M = \bigoplus_{x\in X} Rx \cong \bigoplus_{x\in X} R$ schreiben, wobei ersteres die innere und zweiteres die äußere Summe ist.

(b) Jede direkte Summe $\bigoplus_{i\in I} M_i$ von freien R-Moduln M_i $(i \in I)$ mit jeweiligen R-Basen X_i $(i \in I)$ ist wieder ein freier R-Modul mit der R-Basis $\coprod_{i\in I} X_i$.

Insbesondere ist für alle $n \in \mathbb{N}$ der R-Modul $R^n = \bigoplus_{i=1}^{n} R^{(\mathrm{reg})}$ ein freier R-Modul.

Beweis:

(a) Die Eindeutigkeit der Linearkombination beweist sich wie in der Linearen Algebra. Die Abbildung zwischen $\bigoplus_{x\in X}$ und M ist R-linear, injektiv und surjektiv (alles einfach nachprüfbar) und damit ein R-Isomorphismus.

(b) Einfach nachprüfbar. ∎

Wie in der linearen Algebra R-Homomorphismen von freien R-Moduln müssen nur auf einer R-Basis definiert werden und linear fortgesetzt.

Satz 8.10 (*Universelle Eigenschaft der freien Moduln*)

Sei P ein freier R-Modul mit R-Basis X und der kanonischen Inklusion $\iota : X \to P$. Dann gilt:

$$\forall\, R\text{-Modul } M, \forall\, \varphi : X \longrightarrow M,\ \exists!\tilde{\varphi} \in \mathrm{Hom}_R(P, M) \text{ mit } \tilde{\varphi} \circ \iota = \varphi\,.$$

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & M \\ {\scriptstyle\iota}\downarrow & \circlearrowleft & \nearrow {\scriptstyle\exists!\tilde{\varphi}} \\ P & & \end{array}$$

Der R-Homomorphismus $\tilde{\varphi}$ heißt **R-lineare Fortsetzung** von φ.

Beweis: Der Beweis funktioniert im Wesentlichen wie man ihn aus der Linearen Algebra heraus erwartet. Sei X eine R-Basis von P. Dies geht, da P frei ist. Mit Anmerkung 8.9 (1) können wir jedes $y \in P$ eindeutig als Linearkombination $y = \sum_{x\in X} a_x \cdot x$ für gewisse $a_x \in R$, $\forall x \in X$ schreiben. Wir definieren also

$$\tilde{\varphi} : P \to M,\ y = \sum_{x\in X} a_x \cdot x \mapsto \sum_{x\in X} a_x \cdot \varphi(x).$$

Das geht, denn wir benutzen φ nur mit Argumenten in X, wo φ ja definiert ist. Klar: $\tilde{\varphi} \circ \iota = \varphi$. Es bleibt zu zeigen, dass $\tilde{\varphi}$ R-linear ist. Seien also $r \in R$ und $y_1, y_2 \in P$ mit eindeutigen Darstellungen $y_1 = \sum_{x\in X} a_x \cdot x$ und $y_2 = \sum_{x\in X} b_x \cdot x$. Dann gilt

$$\begin{aligned} \tilde{\varphi}(r \cdot y_1 + y_2) &= \tilde{\varphi}\Big(r \cdot \big(\sum_{x\in X} a_x \cdot x\big) + \sum_{x\in X} b_x \cdot x\Big) \\ &\overset{\text{Def.}\tilde{\varphi}}{=} \sum_{x\in X} (r \cdot a_x + b_x) \cdot \varphi(x) = r \cdot \sum_{x\in X} a_x \varphi(x) + \sum_{x\in X} b_x \varphi(x) \\ &\overset{\text{Def.}\tilde{\varphi}}{=} r \cdot \tilde{\varphi}(y_1) + \tilde{\varphi}(y_2). \end{aligned}$$

∎

Bemerkung 8.11

(a) Jeder R-Modul ist zu einem Faktormodul eines freien R-Moduls isomorph.

(b) Jeder endlich erzeugte freie R-Modul besitzt eine endliche R-Basis.

Beweis:

(a) Sei M ein R-Modul. Offensichtlich gilt $M = \langle M \rangle_R$. Das heißt, die Abbildung

$$\begin{aligned} \psi : \bigoplus_{m \in M} R &\twoheadrightarrow M \\ (r_m)_{m \in M} &\mapsto \sum_{m \in M} r_m \cdot m \end{aligned}$$

ist surjektiv und R-linear. Letzteres folgt aus der universellen Eigenschaft der freien Moduln (Satz 8.10), denn ψ ist die R-lineare Fortsetzung der Abbildung $\bigoplus_{m \in M} R \longrightarrow M, e_m \mapsto m$, wobei

$$e_m = (r_n)_{n \in M}, \text{mit } r_n = \begin{cases} 0_R & n \neq m, \\ 1_R & n = m. \end{cases}$$

Nun liefert uns der Homomorphiesatz 4.4

$$\bigoplus_{m \in M} R/\operatorname{Ker}(\psi) \xrightarrow{\cong} \operatorname{Bild}(\psi) = M.$$

Also ist M isomorph zu einem Faktormodul von $\bigoplus_{m \in M} R$, welches frei ist. ✓

(b) Sei M ein endlich erzeugter freier R-Modul. Für $M = 0$ gilt die Aussage, also sei $M \neq 0$. Nach Voraussatzung ist M endlich erzeugt, also existiert ein Erzeugendensystem $\{m_1, \ldots, m_k\}$ mit $k \in \mathbb{N}$. Zudem hat M eine R-Basis X.

Da X eine Basis ist, lässt sich jedes m_i $(1 \leqslant i \leqslant k)$ eindeutig als R-Linearkombination aus X darstellen. Es kommen also nur endlich viele Elemente aus X vor, wenn wir alle m_i $(1 \leqslant i \leqslant k)$ nacheinander auf diese Weise darstellen. Also existiert ein $X_0 \subseteq X$ mit $|X_0| < \infty$ und

$$M = Rm_1 + \cdots + Rm_k \subseteq \bigoplus_{x \in X_0} Rx \subseteq M.$$

Also gilt $M = \bigoplus_{x \in X_0} Rx$ und X_0 ist eine endliche R-Basis von M. ■

Nach diesen Aussagen über freie Moduln, können wir nun ein paar Beziehungen zu den projektiven Moduln sehen.

Satz 8.12

(a) Jeder freie R-Modul ist projektiv.

(b) Ein R-Modul P ist projektiv $\Leftrightarrow$ P ist direkter Summand eines freien R-Moduls.

Beweis:

(a) Sei F ein freier R-Modul mit R-Basis X. Wir wollen zeigen, dass Bedingung (1) der Definition von Projektivität (Definition 7.1) gilt. Gegeben seien also R-Moduln M und N, $\alpha \in \operatorname{Hom}_R(F, N)$ und $\psi \in \operatorname{Hom}_R(M, N)$, wobei ψ surjektiv ist:

$$\begin{array}{ccc} & & F \\ & & \downarrow \alpha \\ M & \xrightarrow{\psi} & N \end{array}$$

Weil ψ surjektiv ist, gibt es für jedes $x \in X$ (mindestens) ein Urbild y_x von $\alpha(x)$ unter ψ, d.h. $\psi(y_x) = \alpha(x)$. Wir definieren

$$\begin{aligned} \alpha' : X &\longrightarrow M, \\ x &\mapsto y_x. \end{aligned}$$

Nach der Universellen Eigenschaft des freien Moduls (Satz 8.10) existiert genau ein $\tilde{\alpha} \in \mathrm{Hom}_R(F, M)$, sodass $\tilde{\alpha} \circ \iota = \alpha'$ ist (wobei ι die kanonische Inklusion ist):

$$\begin{array}{ccc} X & \xrightarrow{\alpha'} & M \\ {\scriptstyle\iota}\big\downarrow & \circlearrowleft & \nearrow {\scriptstyle \exists! \tilde{\alpha}} \\ F & & \end{array}$$

Die Behauptung ist nun, dass $\psi \circ \tilde{\alpha} = \alpha$ ist, was die Aussage zeigen würde. Sei $z \in F$ mit eindeutiger R-Linear-Darstellung $z = \sum_{x \in X} a_x \cdot x$. Jetzt haben wir

$$\begin{aligned} \psi \circ \tilde{\alpha}(z) = \psi \circ \tilde{\alpha}\Big(\sum_{x \in X} a_x \cdot x \Big) &\overset{\tilde{\alpha}\, R\text{-lin.}}{=} \psi\Big(\sum_{x \in X} a_x \cdot \tilde{\alpha}(\underbrace{x}_{=\iota(x), x \in F}) \Big) \\ &= \psi\Big(\sum_{x \in X} a_x \cdot \underbrace{\tilde{\alpha} \circ \iota}_{=\alpha'}(x) \Big) = \psi\Big(\sum_{x \in X} a_x \cdot \alpha'(x) \Big) \\ &\overset{\text{Def.}\alpha'}{=} \psi\Big(\sum_{x \in X} a_x \cdot y_x \Big) \overset{\psi\, R\text{-lin.}}{=} \sum_{x \in X} a_x \cdot \psi(y_x) \\ &\overset{\text{Def.}y_x}{=} \sum_{x \in X} a_x \cdot \alpha(x) \overset{\alpha\, R\text{-lin.}}{=} \alpha\Big(\sum_{x \in X} a_x \cdot x \Big) \\ &= \alpha(z). \end{aligned}$$

Also $\psi \circ \tilde{\alpha} = \alpha$. ✓

(b) „⇒“: Wir nehmen an, dass P als R-Modul projektiv ist. Dann existiert nach Teil (1) von Bemerkung 8.11 ein F freies R-Modul und ein Untermodul $N \leqslant F$ mit $P \cong F/N$. Also gibt es eine kurze exakte Sequenz

$$0 \longrightarrow N \overset{\iota}{\hookrightarrow} F \overset{\pi_N}{\twoheadrightarrow} F/N \cong P \longrightarrow 0$$

von R-Moduln, die nach Aufgabe 7.3(a) zerfällt. Also gibt es $\sigma \in \mathrm{Hom}_R(P, F)$ mit $\psi \circ \sigma = \mathrm{id}_P$ und es ist $F \cong \mathrm{Bild}(\iota) \oplus \underbrace{\sigma(P)}_{\cong P, \text{ da } \sigma \text{ inj.}}$, also $P \mid F$. ✓

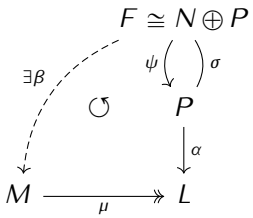
„⇐“: Wir nehmen an, dass ein freies R-Modul F existiert, sodass $P \mid F$. Also gibt es ein R-Modul N mit $F \cong N \oplus P$. Wir beobachten, dass es die folgende kurze exakte Sequenz von R-Moduln gibt

$$\begin{aligned} 0 \longrightarrow N &\xhookrightarrow{\iota} N \oplus P \xrightarrow{\psi} P \longrightarrow 0 \\ n &\longmapsto (n, 0) \\ (n, p) &\longmapsto p, \end{aligned}$$

die mit der Sektion $\sigma : P \longrightarrow N \oplus P, p \mapsto (0, p)$ zerfällt. Wir zeigen nun, dass Bedingung (1) aus der Definition der Projektivität gilt. Seien also M, L R-Moduln und $\alpha \in \mathrm{Hom}_R(P, L)$ und $\mu \in \mathrm{Hom}_R(M, L)$, mit μ surjektiv:

$$\begin{array}{ccc} & & P \\ & & \big\downarrow {\scriptstyle \alpha} \\ M & \xrightarrow{\mu} & L \end{array}$$

Wir zeigen nun die Existenz von β in dem folgenden Diagramm:



Nach (a) gilt, dass F projektiv ist. Also gibt es ein eindeutig bestimmtes $\beta \in \mathrm{Hom}_R(F, N)$ mit $\mu \circ \beta = \alpha \circ \psi$. Setze $\tilde{\alpha} = \beta \circ \sigma$. Dies ist als Verkettung von R-Homomorphismen wieder ein R-Homomorphismus. Somit gilt

$$\alpha = \alpha \circ \mathrm{id}_P = \underbrace{\alpha \circ (\psi \circ \sigma)}_{=\mu\circ\beta} = \mu \circ \underbrace{\beta \circ \sigma}_{=\tilde{\alpha}} = \mu \circ \tilde{\alpha}\,.$$

■

Anmerkung 8.13

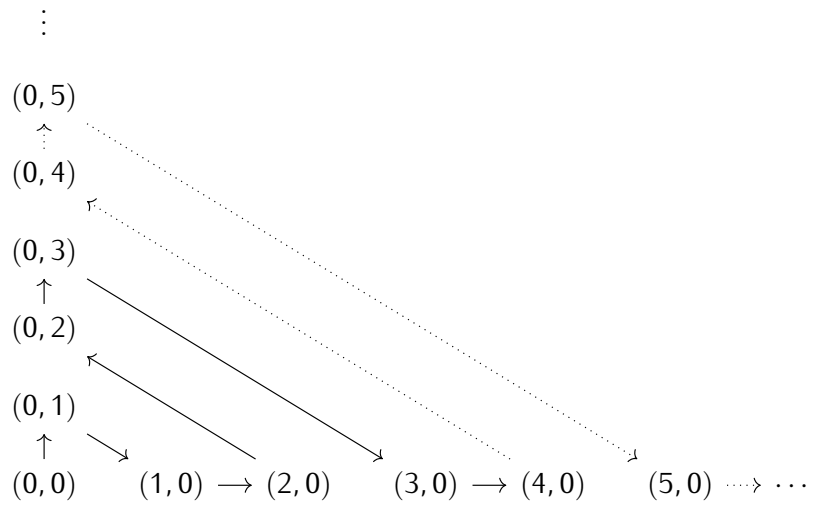
Das Argument aus Teil (2) des Beweises von Bemerkung 8.11 zeigt: **Zwei R-Basen eines freien R-Moduls sind entweder beide endlich oder beide unendlich.** Allerdings können zwei endliche Basen eines freien R-Moduls unterschiedliche Mächtigkeiten haben, wie das nächste Beispiel zeigt! (Anders als bei Vektorräumen.)

Beispiel 17

Betrachte den K-Vektorraum $V \coloneqq \bigoplus_{\mathbb{Z}_{\geqslant 0}} K$. Die Behauptung ist nun, dass für den Ring $R \coloneqq \mathrm{End}_K(V)$ gilt $R \cong_R R \oplus R$. Somit hat R^{reg} die R-Basen $B \coloneqq \{1_R\}$ und $C \coloneqq \{(1,0),(0,1)\}$ mit

$$|B| = 1 \neq 2 = |C|\,.$$

Beweis: (1) Wiederholung aus der Mengenlehre:
Es existiert Bijektion $\varphi : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \times \{0\} \cup \mathbb{Z}_{\geqslant 0} \times \{0\}$, zum Beispiel durch Kantors Diagonalargument:



Schreibe für die zwei kanonischen Projektionen:

$$\pi_1 : \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0} \longrightarrow \mathbb{Z}_{\geqslant 0}, (x, y) \mapsto x$$
$$\pi_2 : \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0} \longrightarrow \mathbb{Z}_{\geqslant 0}, (x, y) \mapsto y\,.$$

② Sei nun $B \coloneqq \{e_n\}_{n\in\mathbb{Z}_{>0}}$ eine K-Basis von V und setze $e_0 \coloneqq 0$. Dann ist die Abbildung

$$f : B \longrightarrow B \times \{0\} \sqcup \{0\} \times B$$
$$e_n \mapsto (e_{\pi_1\circ\varphi(n)}, e_{\pi_2\circ\varphi(n)})$$

offenbar eine Bijektion zwischen der K-Basis B von V und der K-Basis $B \times \{0\} \sqcup \{0\} \times B$ von $V \oplus V$. Die universelle Eigenschaft der freien Moduln liefert also einen K-Isomorphismus

$$\widetilde{f} : V \to V \oplus V$$

wobei $\widetilde{f}$ die K-lineare Fortsetzung der Komposition von f mit der Inklusion von $B \times \{0\} \sqcup \{0\} \times B$ in $V \oplus V$ ist.

③ Wir zeigen nun, dass $R \cong R \oplus R$. Es gilt:

$$\begin{aligned} R = \mathrm{End}_K(V) &= \mathrm{Hom}_K(V, V) \\ &\overset{②}{\cong} \mathrm{Hom}_K(V, V \oplus V) \\ &\overset{\text{L.A.}}{\cong} \mathrm{Hom}_K(V, V) \oplus \mathrm{Hom}_K(V, V) \\ &= \mathrm{End}_K(V) \oplus \mathrm{End}_K(V) \\ &= R \oplus R\,. \end{aligned}$$

Hier beobachten wir noch, dass dies ein R-Isomorphismus nach Definition der R-Modul-Struktur auf $R = \mathrm{End}_K(V)$.

Definition 8.14 (*Rang*)

Haben alle R-Basen eines freien R-Moduls M dieselbe Anzahl von Elementen, so heißt diese Anzahl der R-**Rang** von M, geschrieben $\mathrm{rg}_R(M)$. Sind alle Basen unendlich, so schreiben wir $\mathrm{rg}_R(M) = \infty$.

Das vorherige Beispiel zeigt: Nicht jeder freie R-Modul besitzt einen Rang!

Definition 8.15 (*Eigenschaft des eindeutigen Rangs* (E.e.R.))

Hat der Ring R die Eigenschaft, dass jeder freie R-Modul einen R-Rang besitzt, so sagen wir, dass R die **Eigenschaft des eindeutigen Rangs** (kurz: **E.e.R.**) hat.

Beispiel 18

(1) Körper haben die E.e.R. (Lineare Algebra).

(2) Der Ring $R = \mathrm{End}_K(V)$ aus dem vorherigen Beispiel hat die E.e.R. nicht!

Als nächstes wollen wir die kommutativen Ringe untersuchen, die die E.e.R. auch haben. Zunächst beobachten wir, dass das Argument aus dem Beweis des Satzes De Hammel (siehe Anmerkung–A.3(3)), das zeigt, dass jeder K-Vektorraum eine K-Basis besitzt, funktioniert für R-Moduln mit R kommutativ nicht, da die Invertierbarkeit im Körper verwendet wird. Dafür brauchen wir das folgende Ergebnis von Krull.

Satz 8.16 (Satz von Krull)

Jeder Ring R mit $1_R \neq 0_R$ besitzt ein **maximales** Ideal.

Beweis: Wir betrachten die Menge $X \coloneqq \{I \subsetneq R | \text{ I Ideal von } R\}$ aller echten Ideale von R. Die Inklusion $\subseteq$ bildet eine Halbordnung auf X. Zudem ist klar, dass $X \neq \varnothing$, weil das Nullideal 0 in X liegt. Sei nun $C \subseteq X$ eine Kette bzgl. $\subseteq$ und setze $J \coloneqq \bigcup_{I \in C} I$.

Behauptung: J ist eine obere Schranke für C in X.

(1) Es ist klar nach Definition von J, dass $I \subseteq J \; \forall \, I \in C$ gilt.

(2) Seien nun $x, y \in J$ und $r \in R$. Somit existieren $X, Y \in C$ mit $x \in X$, $y \in Y$ und $X \subseteq Y$ und daraus folgt
$$x - y, rx, xr \in Y \subseteq J\,.$$
Zudem ist $0 \in Y \subseteq J$, so dass $J \neq \varnothing$ Daher ist J ein (zweiseitiges) Ideal von R.
Wegen $1_R \notin I \; \forall \, I \in C$ gilt $1_R \notin J$ und somit ist $J \neq R$ und $J \in X$.

Die Voraussetzungen von dem Lemma von Zorn (siehe Lemma A.2) sind erfüllt und wir erhalten damit, dass X ein maximales Element besitzt, was nach Definition ein maximales Ideal von R ist. ■

Anmerkung 8.17

(1) Der **Satz von Krull** ist äquivalent zum **Zornschen Lemma**.

(2) Mit dem Satz von Krull lässt sich auch beweisen, dass jeder Körper einen algebraischen Abschluss besitzt. (Siehe Algebra I.)

Um das gewünschte Ergebnis für kommutative Ringe zu erahlten, müssen wir nun sowohl den Satz von Krull als auch den Satz von De Hammel verwenden. Insbesondere wird hier das Auswahlaxiom verwendet!

Satz 8.18

Ist R ein kommutativer Ring, so hat R die E.e.R..

Beweis: Die Aussage ist für den Nullring trivial. Wir können also annehmen, dass $R \neq \{0\}$ ist. Sei M ein freier R-Modul. Zu zeigen: Alle Basen von M haben dieselbe Anzahl von Elementen.

Schritt 1: Nach dem Satz von Krull existiert ein maximales Ideal $J \subsetneq R$. Daher ist $R/J =: K$ ein Körper. (Die kommutativität von R wird hier verwendet.)
Nach Aufgabe 1 auf Blatt 2 ist dann $\overline{M} \coloneqq M/JM$ ein R/J-Modul, d.h. ein K-Vektorraum, vermöge
$$(r + J) \cdot (m + JM) \coloneqq rm + JM \; \forall \, r \in R, \forall \, m \in M\,.$$

Schritt 2: Sei nun B ein R-Basis von M. Dann ist $\Rightarrow \overline{B} \coloneqq \{b + JM \in \overline{M} \mid b \in B\}$ ein Erzeugendensystem für $\overline{M}$, weil B ein Erzeugendensystem für M ist. Wir zeigen nun, dass $\overline{B}$ auch K-linear unabhängig ist. Seien also $B' \subseteq B$ mit $|B'| < \infty$ und Elemente $r_b \in R \backslash J \; \forall \, b \in B'$ mit $\sum_{b \in B'} r_b b \in JM$.
Weil B ein Erzeugendensystem für M ist, existiert $\{s_b\}_{b \in B} \subseteq J$ mit fast allen $s_b = 0$ und
$$\sum_{b \in B'} r_b b = \sum_{b \in B} s_b b\,.$$
Aber dann zeigt die R-linear Unabhänghigkeit von B, dass $r_b = s_b \; \forall \, b \in B'$ und somit haben wir einen Widerspruch $\lightning$.
Dieselbe Gleichung zeigt auch, dass die Elemente aus $\{b + JM\}_{b \in B}$ paarweise verschieden sind! Zusammengefasst: $\overline{B}$ ist eine K-Basis von $\overline{M}$ mit $|\overline{B}| = |B|$.

Schritt 3: Ist nun C eine zweite R-Basis von M, so erhalten wir analog, dass $\overline{C}$ eine K-Basis von $\overline{M}$ mit $|\overline{C}| = |C|$ ist.
Schlussfolgerung: $|B| = |B'| = |\overline{C}| = |C|$ unter Verwendung des Satzes von De Hamel (Anmerkung A.3(3)). ■

Folgerung 8.19

Sei R ein kommutativer Ring. Gilt $R^m \cong R^n$ mit $n, m \in \mathbb{N}$, so ist $m = n$.

In der linearen Algebra beweist man Sätze für endlich-dimensionale Vektorräume mithilfe von Basen. Im der Modultheorie gibt es im Allgemeinen leider keine Basen und die endlich erzeugten Moduln verhalten sich weniger anständig! Deshalb führen wir in diesem Kapitel eine Reihe von stärkeren „Endlichkeitsbedingungen“ ein und definieren dadurch vier wichitge Klassen von Moduln:

(1) Moduln mit einer *Kompositionsreihe* (Abschnitt 9);

(2) die *noetherschen* Moduln (Abschnitt 10);

(3) die *artinschen* Moduln (Abschnitt 11);

(4) die *halbeinfachen* Moduln (Abschnitt 14.1).

9 Kompositionsreihen

Definition 9.1 (*Reihe, Länge & Faktoren*)

Sei M ein R-Modul. Eine **Reihe** von M ist eine *endliche* Kette

$$0 = M_t \leqslant M_{t-1} \leqslant \cdots \leqslant M_1 \leqslant M_0 = M$$

von R-Untermoduln von M. Dabei ist die Zahl $t \in \mathbb{Z}_{\geqslant 0}$ die **Länge** der Reihe und wir nennen die Faktormoduln M_i/M_{i-1} (mit $0 \leqslant i \leqslant t-1$) die **Faktoren** der Reihe.

Wir können i.A. weitere Untermoduln in eine Reihe einschieben und sie „verfeinern“.

Definition 9.2 (*Verfeinerung*)

Eine **Verfeinerung** einer Reihe

$$0 = M_t \leqslant M_{t-1} \leqslant \cdots \leqslant M_1 \leqslant M_0 = M \quad (t \in \mathbb{Z}_{\geqslant 0})$$

eines R-Moduls M ist eine Reihe

$$0 = N_s \leqslant N_{s-1} \leqslant \cdots \leqslant N_1 \leqslant N_0 = M \quad (s \in \mathbb{Z}_{\geqslant 0})$$

von M, sodass es eine injektive Abbildung $\iota : \{1, \dots, t-1\} \to \{1, \dots, s-1\}$ mit $M_i = N_{\iota(i)}$ für alle $i = 1, \dots, t-1$ gibt. Sind alle „$\leqslant$“ in der verfeinerten Reihe echte Inklusionen, so heißt die Verfeinerung eine **echte** Verfeinerung.

Wir wollen Zeigen, dass die Faktoren der „feinsten“ Reihen eindeutig bestimmt sind! Dafür brauchen wir einen weiteren Isomorphiesatz von Zassenhaus und den „Verfeinerungssatz“ von Schreier:

Satz 9.3 (Aufgabe 2, Blatt 4)

Seien $U_0 \leqslant U$, $V_0 \leqslant V$ vier R-Untermoduln eines R-Moduls M. Dann gelten:

(a) $U \cap (U_0 + V) = U_0 + (U \cap V)$ (Dedekind-Identität)

(b) $\frac{U_0+(U\cap V)}{U_0+(U\cap V_0)} \cong_R \frac{V_0+(U\cap V)}{V_0+(U_0\cap V)} \cong_R \frac{U\cap V}{(U_0\cap V)+(U\cap V_0)}$ (4. Isomorphiesatz, Zassenhaus)

Definition 9.4 (*Äquivalente Reihen*)

Zwei Reihen eines R-Moduls heißen **äquivalent**, wenn sie *dieselbe Länge* und bis auf Umordnung und bis auf R-Isomorphie *dieselben Faktoren* haben.

Satz 9.5 (Schreiers Verfeinerungssatz)

Je zwei Reihen eines R-Moduls M haben äquivalente Verfeinerungen.

Beweis: Seien

$$0 = M_t \leqslant M_{t-1} \leqslant \cdots \leqslant M_1 \leqslant M_0 = M$$

und

$$0 = N_t \leqslant N_{s-1} \leqslant \cdots \leqslant N_1 \leqslant N_0 = M$$

mit $t, s \in \mathbb{Z}_{\geqslant 0}$ zwei Reihen von M.

- Sei $0 < i \leqslant t$. Wir definieren neue R-Moduln $M_{ij} := M_i + \left(M_{i-1} \cap N_j\right)$ für alle $0 \leqslant j \leqslant s$ und fügen diese zwischen M_i und M_{i-1} ein:

$$M_i = M_{ij} \leqslant M_{i(s-1)} \leqslant \cdots \leqslant M_{i1} \leqslant M_{i0} = M_{i-1}$$

- Analog setzen wir für $0 < j \leqslant s$ fest $N_{ij} := N_j + M_{j-1} \cap M_i$ für alle $0 \leqslant i \leqslant t$ und erhalten eine Unterkette:

$$N_j = N_{tj} \leqslant N_{(t-1)j} \leqslant \cdots \leqslant N_{1j} \leqslant N_{0j} = N_{j-1}$$

- Nach Definition der M_{ij} und N_{ij} ist die Länge der beiden Verfeinerungen gleich.
- Nach dem 4. Isomorphiesatz von Zassenhaus (siehe Satz 9.3) gibt es für alle i, j einen R-Isomorphismus:

$$M_{i(j-1)}/M_{ij} = \frac{M_i + \left(M_{i-1} \cap N_{j-1}\right)}{M_i + \left(M_{i-1} \cap N_j\right)} \cong_R \frac{N_j + \left(M_{i-1} \cap N_{j-1}\right)}{N_j + \left(M_i \cap N_{j-1}\right)} = N_{(i-1)j}/N_{ij}$$

Daher sind die Faktoren der beiden Verfeinerungen auch „gleich“ bis auf R-Isomorphie und Umordnung. ∎

Definition 9.6 (Kompositionsreihe)

Eine **Kompositionsreihe** eines R-Moduls M ist eine Reihe von M, sodass alle Faktoren der Reihe *einfach* sind.

Satz 9.7 (Jordan-Hölder)

Je zwei Kompositionsreihen eines R-Moduls sind äquivalent.

Achtung: Der Satz besagt nicht, dass alle R-Moduln Kompositionsreihen haben!!

Beweis:

- Nach dem Satz von Schreier besitzen je zwei Kompositionsreihen von M äquivalente Verfeinerungen.
- Wir können annehmen, dass es in diesen Verfeinerungen keine Wiederholungen gibt: O.B.d.A. handelt es sich um echte Verfeinerungen.
- Aber: Nach dem Korrespondenzsatz besitzen Kompositionsreihen keine echten Verfeinerungen, weil die Faktoren einfach sind.

  Somit sind Beide Kompositionsreihen selbst äquivalent. ∎

Definition 9.8 (*Länge, Kompositionsfaktoren*)

Sei M ein R-Modul, der eine Kompositionsreihe besitzt.

(1) Die **Länge** von M, geschrieben $l(M)$, ist die Länge einer (beliebigen) Kompositionsreihe von M.

(2) Die **Kompositionsfaktoren** von M sind die Faktoren einer (beliebigen) Kompositionsreihe von M.

Nach dem Satz von Jordan-Hölder ist die Länge wohldefiniert und die Kompositionsfaktoren sind bis auf R-Isomorphie und Umordnung eindeutig bestimmt.

Beispiel 19

(1) (Gegenbeispiel) Der $\mathbb{Z}$-Modul $\mathbb{Z}$ hat *keine* Kompositionsreihe.

Grund: Jede Reihe

$$0 \leqslant n_{t-1}\mathbb{Z} \leqslant \cdots \leqslant n_1\mathbb{Z} < \mathbb{Z} \quad (t \in \mathbb{Z}_{>0})$$

lässt sich zu der Reihe

$$0 \leqslant 2n_{t-1}\mathbb{Z} \leqslant n_{t-1}\mathbb{Z} \leqslant \cdots \leqslant n_1\mathbb{Z} < \mathbb{Z}$$

verfeinern, ohne dass dieses Verfahren endet!

(2) Jeder endlich-dimensionaler K-Vektorraum V hat eine Kompositionsreihe. Ferner gilt:

- $l(V) = \dim_K V$; und
- *alle* Kompositionsfaktoren von V sind isomorph zu K.

Beweis: 1. Fall $V = 0$: Es ist nichts zu tun!

2. Fall $V \neq 0$: Wir wählen eine K-Basis $\{v_1, ..., v_n\}$ von V. Daraus folgern wir die Kompositionsreihe

$$0 = \langle\varnothing\rangle_K < \langle v_1\rangle_K < \langle v_1, v_2\rangle_K < \cdots < \langle v_1, ..., v_n\rangle_K = V$$

mit den Faktoren

$$\langle v_1, ..., v_i\rangle / \langle v_1, ..., v_{i-1}\rangle \cong K \quad (\forall\ 1 \leqslant i \leqslant n)\,.$$

(3) Für vorgegebene einfache R-Moduln $S_1, ..., S_n$ ($n \in \mathbb{N}$) existiert stets ein R-Modul mit Kompositionsfaktoren isomorph zu $S_1, ..., S_n$, nämlich die äußere direkte Summe

$$M := S_1 \oplus \cdots \oplus S_n \,.$$

Achtung: In der Regel gibt es aber viele *nicht*-isomorphe R-Moduln mit den gleichen Kompositionsfaktoren.

(4) Sei $\triangle$ ein Schiefkörper. In diesem Fall kann man die Sätze von Schreier (siehe Satz 9.5) und Jordan-Hölder (siehe Satz 9.7) verwenden, um die Existenz von Basen festzulegen.

(a) Jeder endlich erzeugte $\triangle$-Modul besitzt eine endliche $\triangle$-Basis; und

(b) $\triangle$ hat die E.e.R..

Siehe Aufgabe 1, Blatt 5.

(5) (Gegenbeispiel) Der reguläre $K[X]$-Modul hat auch *keine* Kompositionsreihe!

Grund: $K[X]$ besitzt eine *echt unendliche* Untermodulkette:

$$0 < ... \lneq \langle X^n \rangle \lneq \langle X^{n-1} \rangle \lneq \cdots \lneq \langle X^1 \rangle \lneq K[X]$$

Um dieses Argument richtig zu verstehen müssen wir die „noetherschen“ (Abschnitt 10) und „artinschen“ (Abschnitt 11) Moduln einführen!! Siehe Satz 11.7.

10 Noethersche Moduln

Satz-Definition 10.1 (*Aufsteigende Kettenbedingung, noetherscher Modul*)

Ist M ein R-Modul, so sind die folgenden Bedingungen äquivalent.

(1) Jede *aufsteigende* Kette

$$M_1 \leqslant M_2 \leqslant \cdots \leqslant M_t \leqslant M_{t+1} \leqslant \cdots$$

von R-Untermoduln wird *stationär*, also gibt es ein $a \in \mathbb{N}$, so dass für alle $i \in \mathbb{N}$ gilt: $M_{a+i} = M_a$

(2) Jede nichtleere Menge von R-Untermoduln von M hat ein *maximales Element* bezüglich der Inklusion.

(3) Jeder R-Untermodul von M ist endlich erzeugt.

Gegebenenfalls nennt man M **noethersch**.

Anmerkung 10.2

Insbesondere liefert Bedingung (3): Jeder noethersche R-Modul ist endlich erzeugt.
Aber die Umkehrung gilt nicht! Siehe Aufgabe 2, Blatt 5.

Beweis : (1) $\Rightarrow$ (2): Sei $\mathcal{N} \neq \varnothing$ eine Menge von R-Untermoduln von M.

- Da $\mathcal{N}$ nicht leer ist, gibt es ein R-Untermodul $N_1 \in \mathcal{N}$.
- Ist N_1 maximal, so sind wir fertig!
- Anderenfalls gibt es ein $N_2 \in \mathcal{N}$ mit $N_1 \subsetneq N_2$.
- Ist N_2 maximal, so sind wir fertig!
- Sonst gibt es ein N_3 mit $N_1 \subsetneq N_2 \subsetneq N_3$.
- ...

Nach (1) endet dieses Verfahren nach endlich vielen Schritten mit einem maximalem Element von N.

(2) $\Rightarrow$ (3): Sei U ein R-Untermodul von M. Sei X die Menge aller endlich erzeugten R-Untermoduln von U. Uns ist klar, dass X nicht leer ist, weil $0 \in X$. Nach (2) hat X ein maximales Element, etwa U_0.

- Ist $U_0 = U$, so sind wir fertig!
- Ist $U_0 \neq U$, so existiert ein $x \in U \backslash U_0$ und $U_1 := U_0 + Rx \in X$ ist endlich erzeugt. Zudem liegt U_1 in X und es gilt $U_0 \subsetneq U_1$. Dies ist allerdings ein Widerspruch zu der Maximalität von U_0.

Somit ist $U = U_0$ endlich erzeugt.

(3) $\Rightarrow$ (1): Sei $M_1 \leqslant M_2 \leqslant \cdots \leqslant M_t \leqslant M_{t+1} \text{v} \leqslant \cdots$ eine absteigende Kette von R-Untermoduln von M. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass es ein $a \in \mathbb{N}$ mit $M_a \neq 0$ gibt, weil wir sonst nichts zu tun haben. Dann betrachten wir den R-Untermodul $U := \bigcup_{i \in \mathbb{N}} M_i \text{v} M$. Nach (3) ist U endlich erzeugt. Sei also $B := \{b_1, ..., b_n\}$ mit $n \in \mathbb{N}$ ein Erzeugendensystem von U. Da $|B| < \infty$, gibt es ein $i_0 \in \mathbb{N}$ mit $B \subseteq M_{i_0}$ und nach Definition von U gilt

$$U = \langle B \rangle_R \leqslant M_{i_0} \leqslant U\,.$$

Somit ist $U = M_{i_0}$ und für alle $k \in \mathbb{N}$ gilt $M_{i_0+k} = M_{i_0}$. ∎

Beispiel 20

(1) *Endlich-dimensionale* K-Vektorräume sind noethersche K-Moduln. (Alle K-Unterräume sind sind endlich erzeugt als K-Moduln.)

(2) Alle *endlichen* R-Moduln sind noethersch.

(3) (Gegenbeispiel) Der $\mathbb{Z}$-Modul $\mathbb{Z}[X_i | i \in \mathbb{N}]$ ist *nicht* noethersch!
Grund: Er enthält die unendliche Kette

$$0 \subsetneq \langle X_1 \rangle_{\mathbb{Z}} \subsetneq \langle X_1, X_2 \rangle_{\mathbb{Z}} \subsetneq \langle X_1, X_2, X_3 \rangle_{\mathbb{Z}} \subsetneq \cdots\,.$$

Definition 10.3 (*Noetherscher Ring*)

Der Ring R heißt:

(a) **linksnoethersch**, wenn der reguläre R-Linksmodul R^{reg} noethersch ist;

(b) **rechtsnoethersch**, wenn der reguläre R-Rechtsmodul R^{reg} noethersch ist; und

(c) **noethersch**, wenn er links- und rechtsnoethersch ist.

Beispiel 21

(1) Jeder Körper K ist noethersch.

Klar: $\{0_K\}$ und K sind die einzigen K-Untermoduln von K^{reg}. Somit kann es keine unendliche Kette von Untermoduln geben!

(2) Hauptidealringe sind noethersch.

(3) **Achtung:** Es gibt Ringe, die linksnoethersch sind, aber nicht rechtsnoethersch und umgekehrt:

$\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix} := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Q}) \;\middle|\; c \in \mathbb{Z} \right\}$ ist linksnoethersch, aber nicht rechtsnoethersch und

$\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Q}) \;\middle|\; a \in \mathbb{Z} \right\}$ ist linksnoethersch, aber nicht rechtsnoethersch.

Aufgabe 10.4 (*Aufgabe 2, Blatt 5*)

(a) Zeigen Sie, dass jeder Hauptidealring noethersch ist.

(b) Der reguläre $\mathbb{Z}[X_i \mid i \in \mathbb{N}]$-Modul $\mathbb{Z}[X_i \mid i \in \mathbb{N}]^{\text{reg}}$ ist endlich erzeugt, aber nicht noethersch.

Bemerkung 10.5 (Sandwich-Prinzip)

Sei $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ eine k.e.S. von R-Moduln. Dann gilt:

$$M \text{ ist noethersch} \Leftrightarrow L \text{ und } N \text{ sind noethersch.}$$

Beweis: Aufgabe 2, Blatt 5, Teil (d). ∎

Folgerung 10.6

Sei M ein R-Modul und seien $N, N' \leqslant M$ zwei R-Untermoduln. Dann gelten:

(a) M ist genau dann noethersch, wenn N und M/N noethersch sind;

(b) sind N und N' noethersch, so ist auch $N + N'$ noethersch.

Beweis:

(a) Folgt aus dem Sandwich-Prinzip angewendet mit der k.e.S.

$$0 \longrightarrow N \xrightarrow[\text{Inkl.}]{kan.} M \xrightarrow{\pi_N} M/N \longrightarrow 0\,.$$

(b) Es gilt:

$$\left.\begin{array}{l} N' \text{ noethersch} \\ N \cap N' \leqslant_R N' \end{array}\right\} \overset{\text{(a)}}{\Longrightarrow} N'/N \cap N' \text{ ist noethersch.}$$

Nach dem 2. Isomorphiesatz gilt

$$N'/N \cap N' \cong (N + N')/N'$$

und somit ist auch $N + N'$ noethersch nach (a). ∎

Folgerung 10.7

Ist R linksnoethersch, so ist jeder endlich erzeugte R-Modul noethersch.

Beweis: Sei M ein R-Modul, der endlich erzeugt ist. Ist $M = 0$, so ist M noethersch, da er endlich ist. Wir können also annehmen, dass $M \neq \{0\}$.
Sei $\{b_1, ..., b_n\}$ $(n \in \mathbb{N})$ ein Erzeugendensystem für M. Dann gilt $M = \sum_{i=1}^{n} Rb_i$ und die Abbildungen

$$\begin{aligned} R^{\text{reg}} &\longrightarrow Rb_i \\ r &\mapsto rb_i \end{aligned}$$

sind surjektive R-Homomorphismen $\forall\, 1 \leqslant i \leqslant n$.
Nun gilt:

$$\begin{aligned} R \text{ noethersch} &\overset{\text{Def.}}{\Longrightarrow} && R^{\text{reg}} \text{ ist noethersch} \\ &\overset{\substack{\text{Sandwich-}\\ \text{Prinzip}}}{\Longrightarrow} && Rb_i \text{ ist noethersch } \forall\, 1 \leqslant i \leqslant n \\ &\overset{\substack{\text{Teil (b)}\\ \text{Folgerung 10.6}}}{\Longrightarrow} && \sum_{i=1}^{n} Rb_i \text{ ist noethersch.} \end{aligned}$$

■

Satz 10.8 (Hilberts Basissatz, 1888)

Ist R kommutativ und noethersch, so ist auch der Polynomring $R[X]$ noethersch.

Beweis: Wir nehmen an, dass $R[X]$ nicht noethersch ist.
Nach (3) der Definition 10.1 existiert ein Ideal $I \subseteq R[X]$, das nicht endlich erzeugt ist.
Klar: $I \neq 0$.
Wir definieren nun induktiv eine Folge $(f_i)_{i \in \mathbb{N}}$ von Polynomen in (i).

- Wähle $f_1 \in I \backslash \{0\}$ von minimalem Grad.
- Sind $f_1, ..., f_k$ $(k \in \mathbb{N})$ schon gewählt, dann wähle $f_{k+1} \in I \backslash \langle f_1, ..., f_k \rangle$ von minimalem Grad. (Dies ist möglich, da I nicht endlich erzeugt ist.)

Dann $\forall i \in \mathbb{N}$:

- setze $d_i \coloneqq \deg f_i$; und
- schreibe a_i für den Leitkoeffizient von f_i.

Da R noethersch ist, wird die aufsteigende Kette

$$\langle a_1 \rangle_R \leqslant \langle a_1, a_2 \rangle_R \leqslant \langle a_1, a_2, a_3 \rangle_R \leqslant ...$$

stationär. D.h., $\exists\, m \in \mathbb{N}$ mit $\langle a_1, ..., a_m \rangle_R = \langle a_1, .., a_{m+k} \rangle_R \quad \forall k \in \mathbb{N}$ und somit existieren $r_1, \ldots, r_m \in R$ mit

$$a_{m+1} = \sum_{i=1}^{m} r_i a_i \,.$$

Nach Konstruktion gilt $d_1 \leqslant d_2 \leqslant d_3 \leqslant ... \leqslant d_{m+1}$. Wir können also

$$f \coloneqq f_{m+1} - \sum_{i=1}^{m} r_i \cdot X^{d_{m+1} - d_i} f_i$$

definieren und es gilt Dann ist $f \in I \backslash (f_1, ..., f_m)$ und $\deg(f) < \deg(f_{m+1})$. Dies Widerspricht der Wahl von f_{m+1}. Also muss $R[X]$ noethersch sein. ■

Beispiel 22

(1) Ist R kommutativ und noethersch, so ist $R[X_1, ..., X_n]$ noethersch $\forall\, n \in \mathbb{N}$ nach Hilberts Basissatz.

(2) Nach (1) ist $\mathbb{Z}[X_1, ..., X_n]$ noethersch $\forall n \in \mathbb{N}$.

(3) Dagegen ist $\mathbb{Z}[X_i \mid i \in \mathbb{N}]$ nicht noethersch. (Übung, siehe Blatt 5.)

(4) Der Ring $\mathbb{Z}[X]$ ist ein noetherscher Ring, der kein Hauptidealring ist.

11 Artinsche Moduln

Auch die zur aufsteigenden Kettenbedingung duale Bedingung spielt in der Algebra eine wichtige Rolle:

Satz-Definition 11.1 (*Absteigende Kettenbedingung, artinscher Modul*)

Ist M ein R-Modul, so sind die folgenden Bedingungen äquivalent.

(1) Jede absteigende Kette $M_1 \geqslant M_2 \geqslant ... \geqslant M_t \geqslant M_{t+1} ...$ von R-Untermoduln wird stationär, d.h. $\exists a \in \mathbb{N}$ mit $M_{a+i} = M_a \quad \forall\, i \in \mathbb{N}$.

(2) Jede nichtleere Menge von R-Untermoduln von M hat ein minimales Element bzgl. Inklusion.

Gegebenenfalls nennt man M artinsch.

Beweis:
(1) $\Rightarrow$ (2): Sei $\mathcal{N} \neq \varnothing$ eine Menge von R-Untermoduln von M sei $N_1 \in \mathcal{N}$.

- Ist N_1 minimal, so sind wir fertig.
  Sonst: $\exists N_2 \in \mathcal{N}$ mit $N_1 \gneqq N_2$.
- Ist N_2 minimal, so sind wir fertig.
  Sonst: $\exists N_3 \in \mathcal{N}$ mit $N_1 \gneqq N_2 \gneqq N_3$.

Iterativ erhalten wir eine absteigende Kette

$$N_1 \geqslant N_2 \geqslant N_3 \geqslant N_4 \geqslant ...$$

von R-Untermoduln von M. Diese wird stationär nach (1). D.h. $\exists a \in \mathbb{N}$ mit $N_a = N_{a+i}\ \forall i \in \mathbb{N}$. Der Modul N_a ist das gesuchte minimale Element von $\mathcal{N}$.

(2) $\Rightarrow$ (1): Sei $N_1 \geqslant N_2 \geqslant N_3 \geqslant ...$ eine absteigende Kette von R-Untermoduln von M. Nach (2) besitzt die Menge $\mathcal{N} := \{N_i \mid i \in \mathbb{N}\}$ ein minimales Element, etwa N_a. Somit gilt $N_{a+i} = N_a \quad \forall i \in \mathbb{N}$. ■

Definition 11.2 (*artinscher Ring*)

Der Ring R heißt:

(a) **linksartinsch**, wenn der reguläre R-Linksmodul R^{reg} artinsch ist;

(b) **rechtsartinsch**, wenn der reguläre R-Linksmodul R^{reg} artinsch ist; und

(c) **artinsch**, wenn er links- und rechtsartinsch ist.

Bemerkung 11.3 (Sandwich-Prinzip)

Sei $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\psi} N \longrightarrow 0$ eine k.e.S. von R-Moduln. Dann gilt:

$$M \text{ ist artinsch} \iff L \text{ und } N \text{ sind artinsch.}$$

Beweis: Aufgabe 2(d), Blatt 5. ■

Folgerung 11.4

Sei M ein R-Modul und seinen $N, N' \leqslant M$ zwei R-Untermoduln. Dann gelten:

(a) M ist genau dann artinsch, wenn N und M/N artinsch sind;

(b) $N + N'$ ist artinsch, wenn N und N' artinsch sind.

Folgerung 11.5

Ist R linksartinsch, so ist jeder endlich erzeugte R-Modul artinsch.

Beweis: Komplett analog zu *"noethersch"* mithilfe des Sandwich-Prinzips!! ■

Beispiel 23

(1) Jeder endlich-dimensionale K-Vektorraum V ist artinsch.
Grund: Jede Kette $V_1 \geqslant V_2 \geqslant V_3 \geqslant \ldots$ von K-Unterräumen wird stationär, weil

$$\infty > \dim_k V_1 \geqslant \dim_k V_2 \geqslant \dim_k V_3 \geqslant \ldots \geqslant 0$$

ist.

(2) $\mathbb{Z}$ ist nicht artinsch:

$$\mathbb{Z} \gneqq 2\mathbb{Z} \gneqq 2^2\mathbb{Z} \gneqq 2^3\mathbb{Z} \gneqq \ldots \gneqq 2^n\mathbb{Z} \gneqq 2^{n+1}\mathbb{Z} \gneqq \ldots$$

ist eine unendliche absteigende Kette von $\mathbb{Z}$-Untermoduln.

Aufgabe 11.6

Beweisen Sie oder widerlegen Sie:

(i) Polynomringe sind artinsch.

(ii) Der Matrizenring $M_n(K)$ ist artinsch und noethersch für alle $n \in \mathbb{N}$.

Satz 11.7

Sei M ein R-Modul. Dann gilt:

$$M \text{ hat eine Kompositionsreihe} \iff M \text{ ist artinsch und } M \text{ ist noethersch.}$$

Beweis:

"$\Rightarrow$": Sei $0 = M_0 \leqslant M_1 \leqslant \ldots \leqslant M_l = M$ eine Kompositionsreihe von M. Wir zeigen per Induktion nach l, dass M artinsch und noethersch ist.

- $l = 0 \implies M = 0$. Somit ist M artinsch und noethersch. (Da endlich!)
- $l > 0$: Wir boebachten, dass $0 = M_0 \leqslant \ldots \leqslant M_{l-1}$ eine Kompositionsreihe von M_{l-1} ist. Somit impliziert die Induktionsvoraussetzung, dass M artinsch und noethersch ist.
  Zudem ist M/M_{l-1} einfach. Daher ist M/M_{l-1} ebenfalls artinsch und noethersch, weil die Länge von echten Ketten höchstens 1 ist.
  Teil (a) aus Folgerung 11.4 liefert, dass M artinsch und noethersch ist.

"$\Leftarrow$": Wir nehmen an, dass M artinsch und noethersch ist. Sei dann $\mathcal{M}$ die Menge aller R-Untermoduln von M, die eine Kompositionsreihe besitzen. Wegen $0 \in \mathcal{M}$ ist $\mathcal{M} \neq \varnothing$. Da M noethersch ist, besitzt $\mathcal{M}$ ein maximales Element, etwa $N \leqslant M$.

Behauptung: $N = M$.

Ist $N \neq M$, so ist M/N artinsch und die Menge $\mathcal{N}$ aller nicht-trivialen R-Untermoduln von M/N besitzt ein minimales Element, etwa L/N mit $N \lneq L \leqslant M$. Die Minimalität von L/N bedeutet, dass L/N einfach ist und somit hat L eine Kompositionsreihe. Dies ist ein Widerspruch zur Wahl von N. Somit ist $M = N$ und M hat eine Kompositionsreihe. ∎

Wir erwähnen noch ohne Beweis:

Satz 11.8 (Satz von Hopkins, 1939)

Ist R linksartinsch, so ist R auch linksnoethersch.

Dies ist eher überraschend, weil:

- Gesehen: Die Umkehrung gilt nicht!
  Z.B. ist $\mathbb{Z}$ noethersch, aber nicht artinsch als $\mathbb{Z}$-Modul.
- Es existieren R-Moduln, die artinsch, aber nicht noethersch sind!

12 (Un)zerlegbare Moduln

Wir möchten nun R-Moduln in direkte Summen Zerlegen können, und wir untersuchen, unter welchen Vorausetzungen solche Zerlegungen eindeutig bestimmt sind, d.h. bis auf Isomorphismus und bis auf Reihenfolge der Summanden!

Definition 12.1 (*(un)zerlegbarer Modul*)

Ein R-Modul $M \neq 0$ heißt **unzerlegbar**, wenn gilt:

$$M = M_1 \oplus M_2 \text{ mit } M_1, M_2 \leqslant_R M \quad \implies \quad M_1 = 0 \text{ oder } M_2 = 0.$$

Anderenfalls heißt er **zerlegbar**.

Beispiel 24

(1) Einfache R-Moduln sind unzerlegbar! Klar: $M_1 \leqslant_R M$ einfach $\implies M_1 = 0$.

(2) Die Kleinsche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ist offenbar zerlegbar als $\mathbb{Z}$-Modul und als $\mathbb{Z}/2\mathbb{Z}$-Modul.

(3) Die zyklische Gruppe $\mathbb{Z}/4\mathbb{Z}$ ist unzerlegbar als $\mathbb{Z}$-Modul, da die einzige Untergruppe U mit $1 \neq |U| \neq 4$ die Gruppe $\mathbb{Z}/2\mathbb{Z}$ ist, aber $\mathbb{Z}/4\mathbb{Z} \not\cong_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 12.2 (*Aufgabe 3(b), Blatt 6*)

Für den Ring $R := T_n(K)$ der oberen Dreiecksmatrizen in $M_n(K)$ ist der R-Modul $M := K^n$ (mit der natürlichen Linksmultiplikation mit den Matrizen in $T_n(K)$) unzerlegbar, aber für $n > 1$ nicht einfach.

Definition 12.3 (*endliche Zerlegung in eine direkte Summe unzerlegbarer Summanden*)

Sei M ein R-Modul. Ist

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n \qquad (\text{bzw. } M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_n)$$

mit $n \in \mathbb{Z}_{\geqslant 0}$ und $M_1, \ldots, M_n \leqslant_R M$ unzerlegbar, so nennt man $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ eine bfendliche Zerlegung von M in eine direkte Summe unzerlegbarer Summanden.

Satz 12.4

Sei M ein R-Modul. Ist M noethersch (bzw. artinsch), so besitzt M eine (endliche) Zerlegung in eine direkte Summe unzerlegbarer Summanden.

Beobachtung: Falls M eine Zerlegung in eine direkte Summe unzerlegbarer Summanden $M = \bigoplus_{i \in I} M_i$ besitzt, so muss diese Summe endlich sein. Sonst gibt es unendliche absteigende und aufsteigende Ketten in M, was widerspricht der Voraussetzung, dass M artinsch bzw. noethersch ist.

Beweis: O.B.d.A. können wir annehmen, dass $M \neq 0$, denn $0 = \bigoplus_{i \in \varnothing} M_i$ ist.
Wir nehmen dann an, dass M keine Zerlegung in eine direkte Summe unzerlegbarer Summanden besitzt. Insbesondere muss M zerlegbar sein. (Wäre M unzerlegbar, so hätten wir eine endliche Zerlegung der Länge 1.)
Daher existieren $M_1, W_1 \leqslant_R M$ mit $M = M_1 \oplus W_1$. und wir können annehmen, dass W_1 auch keine endliche Zerlegung in eine direkte Summe unzerlegbarer Summanden besitzt. Daher existieren $M_2, W_2 \leqslant_R W_1$ mit $W_1 = M_2 \oplus W_2$.
...
Iterativ erhalten wir zwei unendliche Untermodulketten:

(1) $W_1 \gneqq W_2 \gneqq W_3 \gneqq \ldots$; und

(2) $M_1 \lneq M_1 \oplus M_2 \lneq M_1 \oplus M_2 \oplus M_3 \lneq \ldots$

Dann liefert (1) einen Widerspruch zur Voraussetzung, dass M artinsch ist und (2) liefert einen Widerspruch zur Voraussetzung, dass M noethersch ist. ∎

Lemma 12.5

Ist $M \neq 0$ ein R-Modul, so sind die folgenden Bedingungen äquivalent:

(1) M ist unzerlegbar;

(2) id_M und 0 sind die einzigen Idempotenten in $\mathrm{End}_R(M)$.

Erinnerung: Ein Element s eines Ringes S heißt idempotent, wenn $s^2 = s$.
Klar: $\mathrm{id}_M^2 = \mathrm{id}_M$, $0^2 = 0$.

Beweis:

(2) $\Rightarrow$ (1): Wir nehmen an, dass $M = M_1 \oplus M_2$ mit $M_1, M_2 \leqslant_R M$. Z.z: $M_1 = 0$ oder $M_2 = 0$. Schreibe $p_1 : M_1 \oplus M_2 \longrightarrow M_1 \oplus M_2$, $(m_1, m_2) \mapsto (m_1, 0)$ für die 1. Projektion. Offenbar ist $p_1 \in \mathrm{End}_R(M)$ ein Idempotent: $p_1^2 = p_1 \circ p_1 = p_1$. Nach (2) gilt $p_1 \in \{0, \mathrm{id}_M\}$. Ist $p_1 = 0$, so ist $M_1 = 0$ und $M_2 = M$. Ist $p_1 = \mathrm{id}_M$, so ist $M_1 = M$ und $M_2 = 0$.

(1) $\Rightarrow$ (2): Sei $f \in \mathrm{End}_R(M)$ mit $f^2 = f$. Z.z.: $f \in \{0, \mathrm{id}_M\}$. Setze $M_1 := \ker(f)$ und $M_2 := \mathrm{Bild}(f)$.

Behauptung. Es gilt $M = M_1 \oplus M_2$.

- $M = M_1 + M_2$: Sei $x \in M$. Dann ist $x = (x - f(x)) + f(x)$ mit $x - f(x) \in \ker(f) = M_1$, da

$$f(x - f(x)) = f(x) - f^2(x) = f(x) - f(x) = 0$$

  ist, und $f(x) \in \mathrm{Bild}(f) = M_2$.

- $M_1 \cap M_2 = \{0\}$: Sei $x \in M_1 \cap M_2$. Dann ist $f(x) = 0$ und $\exists y \in M$ mit $x = f(y)$. Somit gilt

$$0 = f(x) = f(f(y)) = f^2(y) = f(y) = x\,.$$

Aber M ist unzerlegbar nach (1). Somit gilt $M_1 = 0$, $M_2 = M$ oder $M_1 = M$, $M_2 = 0$.

· Im ersten Fall ist f bijektiv mit $f = f^2 \circ f^{-1} = f \circ f^{-1} = \mathrm{id}_M$.

· Im zweiten Fall ist $f = 0$.

■

Lemma 12.6 (Fittings Lemma)

Sei M ein R-Modul, der eine Kompositionsreihe besitzt. Ist $f \in \mathrm{End}_R(M)$, so existiert $n \in \mathbb{N}$ mit

$$M = \ker(f^n) \oplus \mathrm{Bild}(f^n).$$

Beweis: Siehe:

Aufgabe 12.7 (*Aufgabe 3, Blatt 5.*)

(a) Sei M ein R-Modul und sei $f \in \mathrm{End}_R(M)$. Zeigen Sie:

(i) Ist M noethersch, so gibt es ein $n \in \mathbb{N}$ mit $\mathrm{Bild}(f^m) \cap \ker(f^m) = 0$ für alle $m \geqslant n$. Außerdem ist f genau dann bijektiv, wenn f surjektiv ist.

(ii) Ist M artinsch, so gibt es ein $n \in \mathbb{N}$ mit $M = \mathrm{Bild}(f^m) + \ker(f^m)$ für alle $m \geqslant n$. Außerdem ist f genau dann bijektiv, wenn f injektiv ist.

(iii) Hat M eine Kompositionsreihe, so gibt es ein $n \in \mathbb{N}$ mit $M = \mathrm{Bild}(f^m) \oplus \ker(f^m)$ für alle $m \geqslant n$.

(b) Zeigen Sie: Jeder Linksnoethersche Ring hat die **E.e.R.**.

■

Folgerung 12.8

Sei M ein unzerlegbarer R-Modul, der eine Kompositionsreihe besitzt und seien $f, g \in \mathrm{End}_R(M)$. Dann gilt: Ist $f + g$ ein R-Isomorphismus, so ist f oder g ein R-Isomorphismus.

Beweis: Weil M eine Kompositionsreihe hat, liefert Satz 11.7, dass M artinsch und noethersch ist. Nun ist $f+g$ ein R-Isomorphismus, so ist $f+g$ bijektiv. Daher ist die Umkehrabbildung $(f+g)^{-1}$ definiert und diese ist auch ein R-Isomorphismus. Definiere also

$$\widetilde{f} := (f+g)^{-1} \circ f \quad \text{und} \quad \widetilde{g} := (f+g)^{-1} \circ g\,.$$

Dann gilt

$$\widetilde{f} + \widetilde{g} = (f+g)^{-1} \circ f + (f+g)^{-1} \circ g = (f+g)^{-1} \circ (f+g) = \mathrm{id}_M\,,$$

weil $f+g$ bijektiv ist.
Wir nehmen nun an, dass f nicht bijektiv ist. Wir müssen also zeigen, dass g bijektiv ist. Nach Fittings Lemma existiert $n \in \mathbb{N}$ mit

$$M = \ker(f^n) \oplus \mathrm{Bild}(f^n)\,.$$

Weil f nicht bijektiv ist, liefert Aufgabe 12.7(a)(i), dass f^n nicht surjektiv ist. (Sonst wäre f auch surjektiv.) Somit ist $\mathrm{Bild}(f^n) \neq M$ und wir erhalten $M = \ker(f^n)$ und $\mathrm{Bild}(f^n) = 0$, weil M unzerlegbar ist. Daher ist $f^n = 0$ und es gilt

$$\mathrm{id}_M = (\mathrm{id}_M - \widetilde{f}) \circ (\mathrm{id}_M + \widetilde{f} + \widetilde{f}^2 + \cdots + \widetilde{f}^{n-1})\,.$$

Daher ist $\widetilde{g} = \mathrm{id}_M - \widetilde{f}$ surjektiv, was bedeutet, dass g injektiv ist. Schließlich muss g bijektiv nach Aufgabe 12.7(a)(ii) sein. ∎

Satz 12.9 (Satz von Krull-Schmidt)

Jeder R-Modul, der eine Kompositionsreihe besitzt, hat eine endliche Zerlegung

$$M = M_1 \oplus \cdots \oplus M_r \quad (n \in \mathbb{Z}_{\geqslant 0})$$

in eine direkte Summe unzerlegbarer Summanden, die bis auf Reihenfolge und Isomorphie eindeutig bestimmt sind.

Beweis:

Existenz: gilt nach Satz 12.4.

Eindeutigkeit: Zunächst können wir annehmen, dass $M \neq 0$. Seien dann

$$M_1 \oplus \cdots \oplus M_n = M = N_1 \oplus \cdots \oplus N_l \qquad (n, l \in \mathbb{N})$$

zwei Zerlegungen von M in direkte Summen unzerlegbarer Summanden. Wir führen eine Induktion nach n durch.
Für $n = 1$: gilt $M_1 = M = N_1$ und M ist unzerlegbar. Nichts zu tun!

Sei also $n \geqslant 2$. Dann $\forall\, 1 \leqslant i \leqslant n$ schreibe

$$\pi_i : M_1 \oplus \cdots \oplus M_n \longrightarrow M_1 \oplus \cdots \oplus M_n, (m_1, \ldots, m_n) \mapsto (0, \ldots, 0, m_i, 0, \ldots, 0)$$

für die i-te Projektion der 1. Zerlegung und schreibe

$$p : N_1 \oplus \cdots \oplus N_l \longrightarrow N_1, (n_1, \ldots, n_l) \mapsto n_1$$

für die 1. Projektion der 2. Zerlegung. Dann ist $p|_{N_1} = \mathrm{id}_{N_1}$ bijektiv, d.h.

$$p|_{N_1} = p \circ (\pi_1 + \cdots + \pi_n)|_{N_1} = (p \circ \pi_1)|_{N_1} + \cdots + (p \circ \pi_1)|_{N_1}$$

ist bijektiv. Nach Folgerung 12.8 können wir annehmen, dass $(p \circ \pi_1)|_{N_1}$ bijektiv ist. (Bis auf Umordnung!) Daher ist $\pi_1|_{N_1}$ injektiv und $p|_{M_1}$ surjektiv. Nun setze

$$\sigma := \pi_1|_{N_1} \circ (p \circ \pi_1)|_{N_1}^{-1} \circ p|_{M_1} \in \mathrm{End}_R(M_1)\,.$$

Es gilt

$$\sigma^2 = \pi_1|_{N_1} \circ (p \circ \pi_1)|_{N_1}^{-1} \circ p|_{M_1} \circ \pi_1|_{N_1} \circ (p \circ \pi_1)|_{N_1}^{-1} \circ p|_{M_1} = \pi_1|_{N_1} \circ \mathrm{id}_{N_1} \circ (p \circ \pi_1)|_{N_1}^{-1} \circ p|_{M_1} = \sigma$$

und $\sigma \neq 0$. Es folgt also aus Lemma 12.5, dass $\sigma = \mathrm{id}_{M_1}$ ist, weil M_1 unzerlegbar ist. Daher ist $\pi_1|_{N_1}$ injektiv und $\pi_1|_{N_1} : N_1 \longrightarrow M_1$ ist ein R-Isomorphismus.

Behauptung: $M = N_1 \oplus (M_2 \oplus \cdots \oplus M_n)$.

(1.) Für $x \in N_1 \cap (M_2 \oplus \cdots \oplus M_n)$ gilt $\pi_1(x) = 0$, weil $x \in M_2 \oplus \cdots \oplus M_n$ ist. Somit ist $x = 0$, weil $\pi_1|_{N_1}$ injektiv ist.

(2.) Ist $x \in M_1$, so existiert $y \in N_1$ mit $\pi_1(x) = x = \pi_1(y)$, weil $\pi_1|_{N_1}$ ein Isomorphismus ist. D.h.

$$x - y \in \ker(\pi_1) = M_2 \oplus \cdots \oplus M_n\,.$$

Somit gilt $M = N_1 \oplus (M_2 \oplus \cdots \oplus M_n)$. Der 1. Isomorphiesatz liefert dann

$$M/N_1 \cong M_2 \oplus \cdots \oplus M_n \cong N_2 \oplus \cdots \oplus N_l\,.$$

Daher ist $n = l$ und die Behauptung folgt aus der Induktionsvoraussetzung. ■

13 Das Jacobson-Radikal

Schreibweise 13.1

Wir schreiben $\mathrm{Irr}(R)$ für die Menge aller einfachen R-Moduln betrachtet bis auf Isomorphie.

Definition 13.2 (*Jakobson-Radikal*)

Das **Jacobson-Radikal** von R ist das zweiseitige Ideal

$$J(R) := \bigcap_{V \in \mathrm{Irr}(M)} \mathrm{Ann}_R(V).$$

Wir haben die folgenden äquivalenten Charakterisierungen:

Lemma 13.3

Es gilt

$$J(R) = \bigcap_{\substack{I \text{ max.} \\ \text{Linksideal} \\ \text{von } R}} I \quad = \{x \in R | 1_R - axb \in R^\times, \forall a, b \in R\}.$$

Beweis: Aufgabe 1, Blatt 6. ■

Das Radikal $J(R)$ von Jacobson ist sehr hilfreich in der Untersuchung der einfachen R-Moduln, da R und $R/J(R)$ *die gleichen* einfachen Moduln haben. Genauer:

Lemma 13.4

Es existiert eine Bijektion

$$\mathrm{Irr}(R) \xleftrightarrow{\sim} \mathrm{Irr}(R/J(R)),$$

die die Gruppenstruktur unverändert lässt.

Beweis: Wir konstruieren zwei Abbildungen:

- $f\colon \mathrm{Irr}(R) \longrightarrow \mathrm{Irr}(R/J(R)), (S,+,\cdot) \mapsto f(S,+,\cdot) := (S,+,*)$ mit

$$*\colon R/J(R) \times S \longrightarrow S, (r+J(R),s) \mapsto (r+J(R)) * s := r \cdot s\,;$$

- $g\colon \mathrm{Irr}(R/J(R)) \longrightarrow \mathrm{Irr}(R), (S,+,*) \mapsto g(S,+,*) := (S,+,\cdot)$ mit

$$\cdot\colon R \times S \longrightarrow S, (r,s) \mapsto r \cdot s := (r+J(R)) * s\,.$$

Es sind somit folgende Beobachtungen klar:

(1) $f(S,+,\cdot)$ ist ein $R/J(R)$-Modul nach Aufgabe 1(a), Blatt 2, weil $J(R)S = 0$ nach der Definition von $J(R) = \bigcap_{V\in\mathrm{Irr}(R)} \mathrm{Ann}_R(V)$;

(2) $g(S,+,*)$ ist ein R-Modul nach Aufgabe 1(d), Blatt 1;

(3) $(S,+,\cdot)$ einfach $\Rightarrow f(S,+,\cdot)$ einfach und $(S,+,*)$ einfach $\Rightarrow g(S,+,*)$ einfach (schließlich ist die äußere Multiplikation "die gleiche" und nicht triviale Untermoduln des einen Modul wären sofort nicht triviale Untermoduln des anderen);

(4) $f \circ g = \mathrm{id}$ und $g \circ f = \mathrm{id}$ nach der Definition von "$\cdot$" und "$*$". ■

Lemma 13.5 (Nakayamas Lemma - Version 1)

Ist M ein endlich erzeugter R-Modul mit $J(R)M = M$, so gilt $M = 0$.

Beweis: Im Fall, dass $M = 0$ haben wir die Aussage bereits gezeigt. Angenommen deshalb $M \neq 0$. Sei $\{b_1,\dots,b_n\}$, $n \in \mathbb{N}$ ein Erzeugendensystem für M. Wir können annehmen, dass B minimal ist, d.h. ($B' \subseteq B$, $|B'| < |B| \Rightarrow \langle B'\rangle_R \neq M$. Nach Voraussetzung ist $J(R)M = M$. Daher existieren $r_1,\dots r_n \in J(R)$ mit $b_1 = \sum_{i=1}^n r_i \cdot b_i$. Es folgt:

$$(1-r_1)b_1 - \sum_{i=2}^{n} r_i b_i$$

Wegen $r_1 \in J(R)$ ist $1 - r_1 = 1 - 1 \cdot r_1 \cdot 1 \in R^\times$ nach Lemma 13.3, Setze $u := (1-r_1)^{-1}$. Somit gilt

$$b_1 = 1 \cdot b_1 = u(1-r_1) \cdot b_1 = \sum_{i=2}^{n} u r_i \cdot b_i\,.$$

Es folgt

$$b_1 \in \langle b_2,\dots,b_n\rangle_R\,.$$

Dies liefert einen Widerspruch zur Minimalität von B. Daher muss M bereits 0 sein. ■

Weiterhin gibt es eine weitere Version des Lemma von Nakayama .

Lemma 13.6 (Nakayamas Lemma - Version 2)

Ist M ein endlich erzeugter R-Modul mit einem R-Untermodul U, sodass $U + J(R)M = M$, so gilt $U = M$.

Beweis: Aufgabe 2, Blatt 6. Ein direkter Beweis ist möglich, man kann aber auch die Version 1 verwenden. ■

Schliesslich möchten wir zeigen, dass das Jacobson-Radikal auch die Unzerlegbarkeit von Moduln erkannen kann! Dafür brauchen wir die folgende Definition.

Definition 13.7 (Lokale Ringe)

Ein Ring R heißt **lokal**, wenn $R\backslash R^\times$ ein zweiseitiges Ideal von R ist.

Außerdem haben wir die folgenden äquivalenten Charakterisierungen.

Aufgabe 13.8 (*Aufgabe 2(b), Blatt 6*)

Zeigen Sie, dass die folgenden Ringe lokal sind:

(a) $R := \{\frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z} \text{ und } b \in \mathbb{Z}\backslash p\mathbb{Z}\}$, wobei $p \in \mathbb{Z}$ eine Primzahl ist;

(b) $R := \left\{A \in M_n(K) \mid A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & a_1 & \dots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_1 \end{pmatrix}\right\}$.

Aufgabe 13.9 (*Aufgabe 2(a), Blatt 6*)

Die folgenden Aussagen sind äquivalent:

(1) R ist lokal;

(2) $R\backslash R^\times = J(R)$ (d.h. $J(R)$ ist das einzige maximale Linksideal von R);

(3) $R/J(R)$ ist ein Schiefkörper.

Mit diesen Ergebnissen erhalten wir eine Charakterisierung der Unzerlegbarkeit.

Satz 13.10

Sei $M \neq 0$ ein R-Modul, der eine Kompositionsreihe besitzt. Dann gilt:

$$M \text{ ist unzerlegbar} \iff \mathrm{End}_R(M) \text{ ist lokal.}$$

Beweis:

"$\Leftarrow$" Wir nehmen an, dass der Endomorphismenring $\mathrm{End}_R(M)$ lokal ist. Es ist zu zeigen, dass M unzerlegbar ist. Hierfür nutzen wir die Charakterisierung der Unzerlegbarkeit von Moduln aus Lemma 12.5, dass die Abbildungen $\mathrm{id}_M, 0 \in \mathrm{End}_R(M)$ die einzigen Idempotente sind. Sei hierfür $f \in \mathrm{End}_R(M)$ mit $f^2 = f$.

Weil $f + (\mathrm{id}_M - f) = \mathrm{id}_M \in \mathrm{End}_R(M)$ invertierbar ist, muss einer der beiden Summanden bereits invertierbar sein, d.h. $f \in \mathrm{End}_R(M)$ oder $\mathrm{id}_M - f \in \mathrm{End}_R(M)$, da nach Voraussetzung $\mathrm{End}_R(M)$ lokal und somit $\mathrm{End}_R(M)\backslash \mathrm{End}_R(M)^\times$ ein Ideal ist. Wären also beide Summanden nicht invertierbar, müsste auch die Summe nicht invertierbar sein.

Weiterhin gilt:

$$(*) \qquad 0 = f - f = f - f^2 = f \circ (\mathrm{id}_M - f)$$

Wir müssen nun also zwei Fälle unterscheiden, je nachdem welcher Summand invertierbar ist:

1. Sei $f \in \mathrm{End}_R(M)^\times$ invertierbar. Dann folgt aus der obigen Gleichung:
$$(*) \iff \underbrace{f^{-1} \circ 0}_{=0} = \underbrace{f^{-1} \circ f}_{\mathrm{id}_M} \circ (\mathrm{id}_M - f) = \mathrm{id}_M - f$$
Es folgt also, dass $f = \mathrm{id}_M$
2. Sei $\mathrm{id}_M - f \in \mathrm{End}_R(M)^\times$ invertierbar. Dann folgt aus der obigen Gleichung:
$$(*) \iff \underbrace{0 \circ (\mathrm{id}_M - f)^{-1}}_{=0} = f \circ \underbrace{(\mathrm{id}_M - f) \circ (\mathrm{id} - f)^{-1}}_{=\mathrm{id}_M} = f$$
Es folgt also, dass $f = 0$

Somit sind die einzigen Idempotenten im Endomorphismenring die Null und die Identität und M ist unzerlegbar.

„$\Rightarrow$“ Wir nehmen nun an, dass M unzerlegbar ist. Wir haben zu zeigen, dass $\mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times$ ein zweiseitiges Ideal ist. Sei hierfür $\varphi \in \mathrm{End}_R(M)$. Weil M eine Kompositionsreihe hat, existiert nach dem Lemma von Fitting $n \in \mathbb{N}$ mit

$$M = \ker(\varphi^n) \oplus \mathrm{Bild}(\varphi^n)\,.$$

Weil M unzerlegbar gibt es nur zwei Möglichkeiten:

(1) $\ker(\varphi^n) = M$ und $\mathrm{Bild}(\varphi^n) = 0$; oder
(2) $\ker(\varphi^n) =$ und $\mathrm{Bild}(\varphi^n) = M$.

Im ersten Fall ist φ^n bijektiv, sodass φ nach Aufgabe 12.7 auch bijektiv ist. D.h. φ ist invertierbar. Im zweiten Fall ist $\varphi^n = 0$, d.h. φ ist nilpotent. Daher gilt

$$\mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^\times = \{\varphi \in \mathrm{End}_R(M) \mid \varphi \text{ ist nilpotent}\} =: N\,.$$

Wir müssen also nur noch zeigen, dass N ein zweiseitiges Ideal von $\mathrm{End}_R(M)$ ist.

- Wegen $0 \in N$ gilt $N \neq \varnothing$. Ist $\varphi \in N$, d.h. nilpotent, so existiert $n \in \mathbb{N}$ mit $\varphi^n = 0$. Somit ist $(-\varphi^n) = \pm\varphi^n = 0$ und $-\varphi \in N$. Sind nun $\varphi, \rho \in N$, so ist auch $\varphi + \rho \in N$ nach Folgerung 12.8. (Sonst wäre $\varphi + \rho$ invertierbar und somit wäre auch φ oder ρ invertierbar.)
- Sei $\varphi \in N$, sei $\rho \in \mathrm{End}_R(M)$, und sei $m \in \mathbb{N}$ minimal mit $\varphi^m = 0$ (d.h. $\varphi^i \neq 0\ \forall\, 1 \leqslant i \leqslant m-1$). Dann gilt
$$\varphi^{m-1}(\varphi\rho) = \varphi^m\rho = 0\rho = 0 = \rho 0 = \rho\varphi^m = (\rho\varphi)\varphi^{m-1}$$
und daraus folgt, dass $\varphi\rho, \rho\varphi \in N$ sind, weil $\varphi^{m-1} \neq 0$ ist.

■

14 Halbeinfache Moduln

Zum Schluss untersuchen wir noch die klasse der *halbeinfachen* Moduln, die als direkte Summen von einfachen Moduln definiert sind. Die einfachen Moduln können gewissermaßen als „Grundbausteine“der Modultheorie gedacht werden. Die *halbeinfachen Moduln* bilden dann die nächstkompliziertere Klasse von Monduln.

Satz-Definition 14.1 (*Halbeinfacher Modul*)

Ist M ein R-Modul, so sind die folgenden Bedingungen äquivalent:

(1) $M = \bigoplus_{i\in I} S_i$, wobei $\{S_i\}_{i\in I}$ eine Familie von einfachen R-Untermoduln von M ist;

(2) $M = \sum_{i\in I} S_i$, wobei $\{S_i\}_{i\in I}$ eine Familie von einfachen R-Untermoduln von M ist;

(3) für jeden R-Untermodul $M_1 \leqslant_R M$ existiert $M_2 \leqslant_R M$ mit $M = M_1 \oplus M_2$.

Gegebenenfalls nennt man M **halbeinfach**.

Anmerkung 14.2

Gilt Bedingung (3) für ein R-Modul M, so gilt sie auch für jeden R-Untermodul $U \leqslant_R M$. Denn ist $U_1 \leqslant_R U$, so ist $U_1 \leqslant_R M$ und $\exists\, M_2 \leqslant_R M$ mit $M = U_1 \oplus M_2$. Es folgt nun us der Dedekind-Identität (Satz 9.3(a)), dass

$$\begin{aligned} U = U \cap M = U \cap (U_1 \oplus M_2) &= U \cap (U_1 + M_2) \\ &= U_1 + (U \cap M_2) = U_1 \oplus \underbrace{(U \cap M_2)}_{\leqslant_R U} \end{aligned}$$

ist. Das bedeutet, dass jeder R-Untermodul eines halbeinfachen R-Moduls ist selbst halbeinfach. Es folgt auch aus Bedingung (3), dass jeder Faktormodul eines halbeinfachen R-Moduls halbeinfach ist: Ist $U \leqslant_R M$, so existiert $V \leqslant_R M$ mit $M = U \oplus V$. Dabei ist V auch halbeinfach nach dem obigen Argument und so ist auch $M/U \cong V$.

Beweis:

(1) $\Rightarrow$ (2) In dieser Richtung ist nichts zu tun. (Direkte Summen sind Summen!)

(2) $\Rightarrow$ (3) Schreibe $M = \sum_{i\in I} S_i$ mit $S_i \leqslant_R M$ einfach $\forall i \in I$ und sei $M_1 \leqslant_R M$. Sei X die Familie aller $J \subseteq I$ mit:

(i) $\sum_{i\in J} S_i$ ist eine direkte Summe;
(ii) $M_1 \cap \sum_{i\in J} S_i = \{0\}$.

Es ist klar, dass $X \neq \varnothing$, da $\varnothing \in X$. Des Weiteren können wir für jede Kette $C \subseteq X$ eine obere Schranke angeben, nämlich $\hat{C} := \bigcup_{J\in C} J$. Es sind somit die Voraussetzungen für das Lemma von Zorn gegeben und es existiert ein maximales Element $J_0 \in X$. Wir setzen nun

$$M' := M_1 + \sum_{i\in J_0} S_i \overset{(i)+(ii)}{=} M_1 \oplus \sum_{i\in J_0} S_i\,.$$

Wir müssen nur noch zeigen, dass dieses M' bereits ganz M ist, also $S_i \subseteq M', \forall i \in I$. Angenommen also es gäbe ein $j \in I$ sodass $S_j \nsubseteq M'$, dann gilt $S_j \cap M' = \{0\}$. Schließlich ist $S_j \cap M' \leqslant_R S_j$ und S_j ist einfach und keine Teilmenge von M'. Somit folgt, dass

$$S_j + M' = M_1 \oplus \sum_{i\in J_0} S_i \oplus S_j$$

ist. Dies ist jedoch ein Widerspruch zur Maximalität von J_0. Es folgt, dass $M = M' = M_1 \oplus (\sum_{i\in J_0} S_i)$ ist. Wir setzen also $M_2 := \sum_{i\in J_0} S_i$.

(2) $\Rightarrow$ (1) Mit dem selben Argument und der Wahl $M_1 = \{0\}$ erhält man diese Implikation.

(3) $\Rightarrow$ (1) Sei M_1 die Summe aller einfachen R-Untermoduln von M. Nach (3) gibt es $M_2 \leqslant_R M$ mit $M = M_1 \oplus M_2$. Ist $M_2 = 0$ so sind wir fertig. Wir zeigen, dass der Fall $M_2 \neq 0$ nicht eintreten

kann. Es reicht zu zeigen, dass M_2 einen einfachen R-Untermodul von M enthält: Widerspruch zur Definition von M_1.
Sei also $m \in M_2 \backslash \{0\}$. Nach Anmerkung 14.2 reicht es, den Fall $M_2 = Rm$ zu betrachten.
Nun: Zorns Lemma $\Rightarrow \exists\, N \leqslant_R M_2$ maximal bzgl. $m \notin N$. Nehme dann ein R-Untermodul N' mit $M_2 = N \oplus N'$. (Klar: $N' \neq 0$, weil $M_2 \ni m \notin N$.)

Behauptung: N' ist einfach.

Grund: Ist $0 \neq N'' \leqslant N'$, so gilt $m \in N \oplus N''$ wegen der Maximalität von N und somit ist $M_2 = N \oplus N''$ und $N' = N''$. ■

Beispiel 25

(0) Der Nullmodul 0 ist halbeinfach, aber nicht einfach!
Klar: $0 = \bigoplus_{i \in \varnothing} S_i$ mit $\{S_i\}_{i \in \varnothing}$ leerer Familie von R-Untermoduln.

(1) K-Vektorräume sind halbeinfach.

(2) $S_1, \ldots, S_n$ einfache R-Moduln $\Longrightarrow S_1 \oplus \ldots \oplus S_n$ ist halbeinfach

Aufgabe 14.3 (*Aufgabe 3(a), Blatt 6*)

(a) $\{\binom{x}{0} \in V \mid x \in K\}$ ist ein einfacher R-Untermodul von V; aber

(b) V ist nicht halbeinfach.

14.1 Halbeinfache Ringe

Erneut übertragen wir die *Halbeinfachheit* für Moduln auf Ringe und untersuchen Abhängigkeiten zwischen allen Begriffen, die wir in diesem Kapitel eingeführt haben.

Satz-Definition 14.4

Für einen Ring R sind die folgenden Bedingungen äquivalent:

(1) alle k.e.S. von R-Moduln zerfallen;

(2) alle R-Moduln sind halbeinfach;

(3) alle endlich erzeugten R-Moduln sind halbeinfach;

(4) R^{reg} ist halbeinfach (genauer: R^{reg} ist eine endliche direkte Summe von minimalen Linksidealen).

Gegebenenfalls nennt man R **halbeinfach**.

Beweis:

(1) $\Rightarrow$ (2) Sei M ein R-Modul und sei $U \leqslant_R M$. Betrachte dann die k.e.S..

$$0 \longrightarrow U \xrightarrow[Inkl.]{kan.} M \twoheadrightarrow M/U \longrightarrow 0.$$

Diese Sequenz zerfällt nach (1). Somit ist $M \cong U \oplus M/U$ und Bedingung (3) der Def. eines halbeinfachen Moduls (Definition 26.13) ist erfüllt.

(2) $\Rightarrow$ (1) Klar nach der Charakterisierung der zerfallenden k.e.S.

(2) $\Rightarrow$ (3) Nichts zu tun!

(3) $\Rightarrow$ (4) Nach (3) ist klar, dass R^{reg} halbeinfach ist, da $R^{\text{reg}} = \langle 1 \rangle_R$ endlich erzeugt ist.

2. Behauptung: Schreibe $R^{\text{reg}} = \bigoplus_{i \in I} L_i$ mit $\{L_i\}_{i \in I}$ Familie von minimalen Linksidealen (= einfache R-Untermoduln) von R. Nach Def. der direkten Summe existieren $n \in \mathbb{N}$ und $i_1, ..., i_n \in I$ mit

$$1_R = x_{i_1} + ... + x_{i_n},$$

wobei $x_{i_j} \in L_{i_j}$ für alle $1 \leqslant j \leqslant n$. Daher gilt

$$a = a \cdot 1_R = a x_{i_1} + ... + a x_{i_n}$$

für alle $a \in R$ und es folgt, dass

$$R^{\text{reg}} = L_{i_1} + ... + L_{i_n} = L_{i_1} \oplus ... \oplus L_{i_n}$$

ist.

(4) $\Rightarrow$ (2) Sei M ein R-Modul. Schreibe $M = \sum_{m \in M} \langle m \rangle_R$. Dann gilt für alle $m \in M$:

- Der zyklische Modul $\langle m \rangle_R = Rm$ ist isomorph zu einem Faktormodul von R^{reg} und somit auch zu einem R-Untermodul von R^{reg} nach Anmerkung 14.2.
- Weil R^{reg} halbeinfach ist, ist auch $\langle m \rangle_R$ halbeinfach erneut nach Anmerkung 14.2.

Somit ist M halbeinfach als Summe von halbeinfachen R-Untermoduln. ∎

Folgerung 14.5

Ist R ein halbeinfacher Ring, so gilt:

(a) R^{reg} besitzt eine Kompositionsreihe;

(b) R ist linksartinsch und linksnoethersch.

Beweis: Teil (a) folgt aus Bedingung (4) von Satz-Definition 14.4. Aus (a) und Satz 11.7 folgt dann, dass R^{reg} artinsch und noethersch (als R-Modul) ist. Somit ist der Ring R linksartinsch und linksnoethersch nach Definition 11.2 und Definition 10.3. ∎

Folgerung 14.6

Ist R ein halbeinfacher Ring, so gilt $|\operatorname{Irr}(R)| < \infty$.

Folgt z.B. aus der folgenden Anmerkung.

Anmerkung 14.7

Sei $R \neq 0$ ein halbeinfacher Ring. Gesehen in Kapitel 1:

$$\forall\, S \in \operatorname{Irr}(R) \;\text{ gilt }\; S \cong_R R^{\text{reg}}/\operatorname{Ann}_R(x) \quad \forall\, x \in S \backslash \{0\}\,.$$

Nach Satz-Definition 14.4 ist R^{reg} halbeinfach und die k.e.S.

$$0 \longrightarrow \operatorname{Ann}_R(x) \hookrightarrow R^{\text{reg}} \twoheadrightarrow R^{\text{reg}}/\operatorname{Ann}_R(x) \longrightarrow 0$$

zerfällt für alle $x \in S\backslash\{0\}$. Somit ist $S \cong R^{\text{reg}}/\text{Ann}_x(R) \mid R^{\text{reg}}$, d.h.: S ist isomorph zu einem minimalen Linksideal von R. Der Satz von Jordan-Hölder liefert also

$$R^{\text{reg}} \cong \bigoplus_{S \in \text{Irr}(R)} \bigoplus_{i=1}^{n_s} S\,,$$

wobei die Vielfachheiten $n_s \in \mathbb{Z}_{>0}$ eindeutig bestimmt sind.

14.2 *J*-Halbeinfachheit

Wir führen noch die sogenannte *J-Halbeinfachheit*, die i.A. schwacher als die *Halbeinfachheit* ist.

Definition 14.8 (*J-halbeinfacher Ring*)

Ein Ring R heißt **J-halbeinfach**, falls $J(R) = 0$ ist.

Beispiel 26

$\mathbb{Z}$ ist J-halbeinfach, aber nicht halbeinfach!

Klar: Es gilt

$$J(\mathbb{Z}) = \bigcap_{\substack{I \text{ max.} \\ \text{Linksideal} \\ \text{von } \mathbb{Z}}} I = \bigcap_{p \in \mathbb{P}} p\mathbb{Z} = \{0\}\,.$$

Nichtsdestotrotz:

Lemma 14.9

Ist R ein halbeinfacher Ring, so ist R auch J-halbeinfach.

Und beide Begriffe sind für linksartinsche Ringe äquivalent.

Satz 14.10

Ist R linksartinsch, dann gilt:

$$R \text{ ist halbeinfach} \iff R \text{ ist } J\text{-halbeinfach.}$$

Beweis:

„$\Rightarrow$“: (Es ist die Aussage von Lemma 14.9.)
Weil R halbeinfach ist, zerfällt die k.e.S.

$$0 \longrightarrow J(R) \xrightarrow[Inkl.]{kan.} R^{\text{reg}} \xrightarrow{\pi_{J(R)}} R/J(R) \longrightarrow 0$$

nach Satz-Definition 14.4 und daher ist $R^{\text{reg}} \cong_R J(R) \oplus R/J(R)$. Nun:
Einerseits ist $J(R) \cdot R^{\text{reg}} = J(R)$ und andererseits ist

$$J(R) \cdot (J(R) \oplus R/J(R)) = J(R)J(R) \oplus J(R)/J(R) = J(R)J(R)\,.$$

Nach Nakayamas Lemma gilt also $J(R) = 0$.

„⇐“: Wir müssen nun annehmen, dass R linksartinsch ist. Wir können auch annehmen, dass $R \neq 0$ ist, sonst gibt es nichts zu tun! Zudem nehmen wir an, dass R J-halbeinfach ist, aber nicht halbeinfach. Wähle dann ein minimales Linksideal $I_0 \subseteq R$ (z.B. ein minimales Element der Familie aller Hauptideale $\neq 0$). Dann gilt $0 \neq I_0 \neq R$, weil I_0 einfach ist.

Behauptung: $I_0 \mid R^{\mathrm{reg}}$

Bew: Wegen $I_0 \neq 0 = J(R) = \bigcap_{\substack{I \text{ max.} \\ \text{Linksideal} \\ \text{von } R}} I$ existiert ein maximales Linksideal $\mathfrak{m}_0 \subsetneq R$ mit $I_0 \nsubseteq \mathfrak{m}_0$. Weil $I_0 \cap \mathfrak{m}_0 = 0$ (I_0 einfach!), gilt

$$R^{\mathrm{reg}} = I_0 \oplus \mathfrak{m}_0 \,,$$

da $R^{\mathrm{reg}}/\mathfrak{m}_0$ einfach ist, wie gewünscht.
Dabei muss $\mathfrak{m}_0 \neq 0$ sein und somit existiert ein minimales Linksideal I_1 in $\mathfrak{m}_0$. Es gilt $0 \neq I_1 \neq \mathfrak{m}_0$, sonst wäre $R^{\mathrm{reg}} = I_0 \oplus I_1$ halbeinfach. Die Behauptung angewandt auf I_1 liefert $I_1 \mid R^{\mathrm{reg}}$ und somit auch $I_1 \mid \mathfrak{m}_0$. Es existiert also ein Linksideal $0 \neq \mathfrak{m}_1$ von R mit $\mathfrak{m}_0 = I_1 \oplus \mathfrak{m}_1$.
Iterativ erhalten wir eine unendliche absteigende Kette $\mathfrak{m}_0 \supsetneq \mathfrak{m}_1 \supsetneq \ldots$ von Linksidealen von R.
↯ Dies widerspricht die Voraussetzung, dass R linksartinsch ist! ■

Auch wenn der Ring R selbst nicht J-halbeinfach ist, hat man dennoch:

Satz 14.11

Der Faktorring $R/J(R)$ ist J-halbeinfach.

Beweis: Aufgabe 1(b), Blatt 6. ■

14.3 Der Artin–Wedderburn-Struktursatz

Wir wollen zeigen, dass jeder halbeinfache Ring als endliches Produkt von Matrixringen über geeigneten Schiefkörpern geschrieben werden kann (Artin-Wedderburn-Strukturs̈atze). Als Vorbereitung benötigen wir folgende Erkenntnis.

Lemma 14.12 (*Aufgabe 2, Blatt 7*)

Sei $n \in \mathbb{N}$ und seien $M, M_1, \ldots, M_n$ R-Moduln. Dann gibt es Ringisomorphismen:

(a) $\mathrm{End}_R(M^n) \cong M_n(\mathrm{End}_R(M))$; und

(b) $\mathrm{End}_R(M_1 \oplus \ldots \oplus M_n) \cong \mathrm{End}_R(M_1) \times \ldots \times \mathrm{End}_R(M_n)$, falls $\mathrm{Hom}_R(M_i, M_j) = 0$ für alle $1 \leqslant i \neq j \leqslant n$ gilt.

Nun sind wir bereit für den angekündigten Struktursatz.

Satz 14.13 (Artin–Wedderburn)

Ist R ein halbeinfacher Ring, so existiert ein Ringisomorphismus

$$R \cong \prod_{S \in \mathrm{Irr}(R)} M_n(D_s),$$

wobei $D_s := \mathrm{End}_R(S)^{\mathrm{op}}$ ein Schiefkörper für alle $S \in \mathrm{Irr}(R)$ ist.

Beweis: Für $R = 0$ ist nichts zu tun! Sei daher $R \neq 0$. Es ist R halbeinfach. Nach Anmerkung 14.7 ist

$$R^{\mathrm{reg}} \cong \bigoplus_{S \in \mathrm{Irr}(R)} \bigoplus_{i=1}^{n_s} S\,,$$

wobei die Zahlen $n_s \in \mathbb{Z}_{>0}$ eindeutig bestimmt sind. Somit ist

$$\begin{aligned}
R^{\mathrm{op}} &\cong \mathrm{End}_R(R^{\mathrm{reg}}) && \text{(nach Lemma 3.8(e))}\\
&\cong \mathrm{End}_R\Big(\bigoplus_{S \in \mathrm{Irr}(R)} \bigoplus_{i=1}^{n_s} S\Big)\\
&\cong \prod_{S \in \mathrm{Irr}(R)} \mathrm{End}_R\Big(\bigoplus_{i=1}^{n_s} S\Big) && \text{(nach Lemma 14.12(b), anwendbar wegen Schurs Lemma)}\\
&\cong \prod_{S \in \mathrm{Irr}(R)} M_{n_s}(\mathrm{End}_R(S)) && \text{(nach Lemma 14.12(a))}\,.
\end{aligned}$$

Nun setzen wir $\widetilde{D}_S := \mathrm{End}_R(S)$ für alle $S \in \mathrm{Irr}(R)$. Wegen Schurs Lemma (Lemma 5.4) sind die Ringe $\widetilde{D}_s$ Schiefkörper. Dann ist aber auch $D_S := \widetilde{D}_s^{\mathrm{op}}$ ein Schiefkörper für alle $S \in \mathrm{Irr}(R)$. Somit ist

$$\begin{aligned}
R \cong (R^{\mathrm{op}})^{\mathrm{op}} &\cong \Big[\prod_{S \in \mathrm{Irr}(R)} M_{n_s}(\widetilde{D}_S)\Big]^{\mathrm{op}}\\
&\cong \prod_{S \in \mathrm{Irr}(R)} M_{n_s}(\widetilde{D}_S)^{\mathrm{op}} && \text{(wegen der komponentenweisen Multiplikation)}\\
&\cong \prod_{S \in \mathrm{Irr}(R)} M_{n_s}(\widetilde{D}_S^{\mathrm{op}})\\
&\cong \prod_{S \in \mathrm{Irr}(R)} M_{n_s}(D_S)\,,
\end{aligned}$$

wie gewünscht. ∎

Aufgabe 14.14 (*Aufgabe 3, Blatt 7*)

Für zwei Ideale I, J von R schreiben wir $IJ := \{\sum_{i=1}^{n} x_i y_j \in R \mid n \in \mathbb{N}, x_1, \ldots x_n \in I, y_1, \ldots y_n \in J\}$. Wir definieren $I^0 := R$ und induktiv $I^{n+1} := II^n$ für jedes $n \in \mathbb{N}$. Existiert ein $n \in \mathbb{N}$ mit $I^n = 0$, so nennt man I nilpotent.

Wir nehmen an, dass R ein artinscher Ring ist. Zeigen Sie:

(a) $J(R)$ ist nilpotent; und

(b) jedes nilpotente Ideal von R liegt in $J(R)$.

[Hinweise: (a) Betrachten Sie die Kette $J(R) \supseteq J(R)^2 \supseteq J(R)^3 \supseteq \ldots$ und verwenden Sie die Charakterisierung der artinschen Ringen durch minimale Elemente bzw. das Lemma von Zorn. (b) Verwenden Sie die Artin-Wedderburn-Zerlegung von $R/J(R)$.]

Notation. In diesem Kapitel ist R **stets ein Hauptidealring** (kurz: HIR) und daher ein Integritätsring und $R \neq 0$.

Ziel. Wir wollen eine Klassifikation für endlich erzeugte R-Moduln finden und explizit beschreiben.

Zur Erinnerung wissen wir aus der Algebra I, dass gilt:

{Körper} $\subseteq$ {Euklidische Ringe} $\subseteq$ {Hauptidealringe} $\subseteq$ {faktorielle Ringe} $\subseteq$ {Integritätsringe} $\subseteq$ {kommutative Ringe}
(D.h. bis auf Isomorphie.) Insbesondere dürfen wir die Existenz und Eindeutigkeit von Primfaktorzerlegungen ausnutzen!

15 Primelemente und Torsion

Zunächst erinnern wir ein paar Definitionen und Ergebnisse aus der Vorlesung Algebra I.

Definition 15.1 (*irreduzibles Element, Primelement*)

Sei S ein beliebiger Ring. Ein Element $p \in S \backslash (S^x \cup \{0\})$ heißt:

- **irreduzibel**, falls für alle $a, b \in S$ gilt: $p = a \cdot b \Longrightarrow a \in S^x$ oder $b \in S^x$;
- **Primelement** (oder **prim**), falls für alle $a, b \in S$ gilt: $p | (a \cdot b) \Longrightarrow p | a$ oder $p | b$.

Dabei sei erwähnt, dass Primelemente irreduzibel sind.

Satz 15.2

Ist R ein Hauptidealring und $p \in R \backslash (R^x \cup \{0\})$, so sind die folgenden Aussagen äquivalent:

(a) p ist Primelement;

(b) p ist irreduzibel;

(c) $\langle p \rangle$ ist maximales Ideal;

(d) $\langle p \rangle$ ist Primideal.

Schreibweise 15.3

Wir bezeichnen mit $\mathbb{P}(R)$ die Menge aller Primelemente in R, und mit $\overline{\mathbb{P}}(R)$ ein Repräsentantensystem für die Klassen assoziierten Primelemente in R.
Weil R ein HIR ist, ist R faktoriell. Ist $x \in R\backslash\{0\}$, so schreiben wir:

$$x = u \cdot \prod_{p \in \overline{\mathbb{P}}(R)} p^{e(p)} = \tilde{u} \cdot \prod_{i=1}^{n} p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$$

mit $u, \tilde{u} \in \mathbb{R}^x$, $n \in \mathbb{Z}_{\geqslant 0}$, $p_1, \ldots, p_n \in \overline{\mathbb{P}}(R)$ paarweise verschieden und $e_1,\ldots,e_n \in \mathbb{N}$ für die Primfaktorzerlegung von x.

Als Nächstes erinnern wir auch ein Begriff, der wir in Aufgabe 4.10 schon eingeführt hatten.

Lemma-Definition 15.4 (*Torsionselement, Torsionsuntermodul*)

Sei M ein R-Modul.

(a) Ein Element $x \in M$ heißt **Torsionselement (bzgl. R)**, wenn $\mathrm{Ann}_R(x) \neq \{0_R\}$ (d.h. $\exists\, r \in R\backslash\{0_r\}$ mit $r \cdot x = 0_M$).

(b) Die Menge $T(M) := \{x \in M \mid \mathrm{Ann}_R(x) \neq \{0_R\}\}$ aller Torsionselemente von M ist ein R-Untermodul von M; der sogenannte **Torsionsteil** oder **Torsionsuntermodul** von M.

(c) Es gilt $T(M/T(M)) = 0$.

Definition 15.5 (*Torsionsmodul, torsionsfrei*)

Ein R-Modul M heißt:

(a) **Torsionsmodul** (oder **R-Torsionsmodul**), falls $T(M) = M$; und

(b) **torsionsfrei**, falls $T(M) = 0$.

Beispiel 27

(a) Ist $R = \mathbb{Z}$ und $M := \mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{Z}_{\geqslant 2}$, so gilt:

$$m \cdot (x + m\mathbb{Z}) = mx + m\mathbb{Z} = 0 + m\mathbb{Z} \qquad \forall\, x \in \mathbb{Z}\,.$$

Somit ist $T(M) = M$ und M ist ein Torsionsmodul.

(b) Ist $R = \mathbb{Z}$ und $(G, +)$ eine abelsche Gruppe (d.h. ein $\mathbb{Z}$-Modul), so gilt

$$\begin{aligned} T(G) &= \{x \in G \mid \exists\, m \in \mathbb{Z}\backslash\{0\} \text{ mit } mx = 0\} \\ &= \{x \in G \mid o(x) < \infty\}. \end{aligned}$$

(Schreibweise: $o(x)$ bezeichnet hier die Ordnung des Elements x.)

16 Freie und torsionsfreie Moduln

Wir untersuchen nun als Erstes die freie und Torsionsfreie endlich erzeugte Moduln über HIRe. Wir zeigen, dass in diesem Fall beide Begriffe übereinstimmen.

Satz 16.1

Sei R ein HIR. Dann gelten:

(a) Jeder R-Untermodul U eines freien R-Moduls M von Rang $m \in \mathbb{N}$ ist frei mit $\mathrm{rg}_R(U) \leqslant \mathrm{rg}_R(M)$.

(b) Jeder R-Untermodul eines endlich erzeugten R-Moduls ist endlich erzeugt.

Beweis: (a) Per Induktion nach $m = \mathrm{rg}_R(M)$.

- Fall $m = 1$: Es ist $M \cong R$ und U is isomorph zu einem Linksideal von R. Dieses Linksideal ist ein Hauptideal, da R ein HIR ist. Damit wird U von einem Element $y \in U$ erzeugt und U ist frei mit
$$\mathrm{rg}_R(U) = \begin{cases} 0, & y = 0\,, \\ 1, & \text{sonst,} \end{cases}$$
und es gilt $\mathrm{rg}_R(U) \leqslant 1 = \mathrm{rg}_R(M)$.
- Fall $m > 1$. Sei die Aussage für $\mathrm{rg}_R \leqslant m-1$ bereits bewiesen (IV). Sei dann $X = \{x_1, \ldots, x_m\}$ eine R-Basis von M. Für alle $x \in M$ gibt es $r_1(x), \ldots, r_m(x) \in R$, so dass
$$s = \sum_{i=1}^{m} r_i(x) x_i\,.$$
Setze $A := \{r_1(x) \mid x \in U\}$. Dies ist ein Linksideal von R. (Einfach nachrechnen!) Da R ein HIR ist, gibt es ein Element $d_1 \in R$ mit $\langle d_1 \rangle = A$. Außerdem gibt es ein Element $y_1 \in U$ mit $y_1 = d_1 x_1$. Setze
$$M_1 := \bigoplus_{i=2}^{m} R x_i\,.$$
Dann ist M_1 frei und $y_1 + M_1 = d_1 x_1 + M_1$ in M/M_1.
  - Fall $d_1 = 0$. Dann ist $U \leqslant M_1$ und wegen $\mathrm{rg}_R(M_1) = m-1$ gilt die Behauptung nach der (IV).
  - Fall $d_1 \neq 0$. Sei dann $y \in U$. Es gibt $s_1, \ldots, s_m \in R$, so dass
$$y = \sum_{i=1}^{m} s_i x_i$$
und $s_1 \in A$, d.h. es gibt ein Element $c_1 \in R$ mit $s_1 = c_1 d_1$. Dann ist
$$y - c_1 y_1 = c_1 d_1 x_1 + \sum_{i=1}^{m} s_i x_i - c_1 d_1 x_1 = \sum_{i=1}^{m} s_i x_i \in (M_1 \cap U) \leqslant_R M_1.$$
Somit ist nach (IV) der R-Untermodul $M_1 \cap U$ frei mit $\mathrm{rg}_R(M_1 \cap U) \leqslant M_1 = m-1$. Sei also $\{\widetilde{y}_1, \ldots, \widetilde{y}_r\}$ mit $r \leqslant m-1$ eine R-Basis von $M_1 \cap U$. Dann ist $\{y_1, \widetilde{y}_1, \ldots, \widetilde{y}_r\}$ ein Erzeugendensystem von U. Da X eine R-Basis ist, folgt mit der Definition von M_1, dass dieses Erzeugendensystem bereits frei ist. Somit besitzt U eine R-Basis und $\mathrm{rg}_R(U) \leqslant m = \mathrm{rg}_R(M)$.

(b) Aufgabe 1(a), Blatt 7.

■

Aufgabe 16.2 (*Aufgabe 1(a), Blatt 7*)

Die **Erzeugendenzahl** eines endlich erzeugten R-Moduls M ist

$$\operatorname{erz}_R(M) := \min\{|A| \mid A \subseteq M \text{ und } M = \langle A\rangle_R\} \in \mathbb{Z}_{\geqslant 0}\,.$$

Zeigen Sie:

(i) Es gilt $\operatorname{erz}_R(R^{\text{reg}}) = 1$ und M ist genau dann zyklisch, wenn $\operatorname{erz}_R(M) \leqslant 1$.

(ii) Ist R ein Hauptidealring und U ein R-Untermodul eines endlich erzeugten R-Moduls M, so ist U endlich erzeugt mit

$$\operatorname{erz}_R(U) \leqslant \operatorname{erz}_R(M)\,.$$

Anmerkung 16.3

Teil (a) gilt auch bei unendlichem Rang! Dies kann mit Hilfe des Lemmas von Zorn gezeigt werden. Uns reicht aber die Aussage für endlichen Rang.

Folgerung 16.4

Sei R ein HIR und M ein endlich erzeugter R-Modul. Dann gilt:

$$M \text{ ist torsionsfrei} \iff M \text{ ist frei.}$$

Beweis:

„$\Leftarrow$“: Falls M frei ist, so ist M auch torsionsfrei.

„$\Rightarrow$“: Für $M = 0$ ist M sowohl frei, als auch torsionsfrei. Seien daher $M \neq 0$, $X = \{x_1, \ldots, x_n\}$ mit $n \in \mathbb{N}$ ein Erzeugendensystem von M. Bis auf Umordnung können wir annehmen, dass $\{x_1, \ldots, x_m\}$ ein maximales freies Teilsystem ist. Für alle $m+1 \leqslant j \leqslant n$ wähle ein $r_j \in R\backslash\{0\}$. Dann existieren $r_1(j), \ldots, r_m(j)$ mit

$$r_j x_j = \sum_{i=1}^{m} r_i(j) x_i\,.$$

Setze $r := \prod_{j=m+1}^{n} r_j$. Es ist $r \in R\backslash\{0\}$, weil R ein Integritätsring ist. Die Abbildung

$$\varphi\colon M \longrightarrow \bigoplus_{i=1}^{m} Rx_i,\ x \mapsto r \cdot x$$

ist dann wohldefiniert und R-linear und nach Definition von $T(M)$ ist

$$\ker(\varphi) := \{x \in M \mid r \cdot x = 0\} \leqslant T(M) = 0,$$

weil M torsionsfrei ist. Damit ist φ injektiv und daher $M \cong \varphi(M) \leqslant \bigoplus_{i=1}^{m} Rx_i$. Da $\bigoplus_{i=1}^{m} Rx_i$ frei ist, lässt sich Satz 16.1 anwenden und M ist frei. ∎

Als Konsequenz erhalten wir, dass man die Torsionsmoduln und die Torsionsfreien Moduln über HIRe getrennt untersuchen kann.

Satz 16.5

Sei R ein HIR und M ein endlich erzeugter R-Modul. Dann existiert ein freier R-Untermodul F von M mit

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

Beweis: Betrachte die k.e.S.

$$0 \to T(M) \xrightarrow{i} M \xrightarrow{\pi} M/T(M) \to 0\,,$$

wobei i die kanonische Inklusion und π die kanonische Projektion sind. Der Faktormodul $M/T(M)$ ist torsionsfrei nach Aufgabe4.10(ii), also frei nach Satz 16.4, also projektiv nach Satz 8.12. Dies heißt nach Aufgabe 7.3 dass die k.e.S. zerfällt. Also gibt es ein $\sigma \in \mathrm{Hom}_R(M/T(M), M)$ mit $\pi \circ \sigma = \mathrm{id}$ und es gilt

$$M = T(M) \oplus \sigma(M/T(M))\,.$$

Wir definieren $F := \sigma(M/T(M)) \cong M/T(M)$, da σ injektiv ist. Da $M/T(M)$ frei ist, ist auch F frei. ■

Anmerkung 16.6

Beachte, dass der R-Untermodul F im allgemeinen nicht eindeutig bestimmt ist! (D.h. als Teilmenge von M.) Es ist i.A. möglich zwei R-Untermoduln F, F' zu finden mit $F \neq F'$, aber $M = T(M) \oplus F$ und $M = T(M) \oplus F'$.

Als Folge von Satz 16.5 können wir also $T(M)$ und F getrennt untersuchen!

(1) Wegen der Kommutativität von R gilt $F \cong R^{\mathrm{rg}_R(F)}$, wobei die ganze Zahl $\mathrm{rg}_R(F) \in \mathbb{Z}_{\geqslant 0}$ eindeutig bestimmt ist. Siehe Kapitel 1.

(2) Andererseits müssen wir $T(M)$ in eine direkte Summe von „elementaren Teilen“ zerlegen!

Modell: Zerlegung einer endlichen abelschen Gruppe als direkte Summe von zyklischen Gruppen der Form $\mathbb{Z}/p^a\mathbb{Z}$ mit p^a Primzahlpotenz.

Beispiel 28

Es gilt

$$\mathbb{Z}/7000\mathbb{Z} \cong_{\mathbb{Z}} \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/5^3\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z}$$

und

$$\mathbb{Z}/7000\mathbb{Z} \oplus \mathbb{Z}/7^2\mathbb{Z} \cong_{\mathbb{Z}} \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7^2\mathbb{Z} \oplus \mathbb{Z}/5^3\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z}\,.$$

17 Torsionsmoduln

Wir untersuchen nun den „Torsionsteil“ von endlich erzeugten Moduln.

Konvention: In diesem Abschnitt sind alle R-Moduln endlich erzeugt (kurz: e.e.).

Definition 17.1 (*p-primäres Element, p-primärer Modul*)

Sei $p \in \mathbb{P}(R)$ und sei M ein R-Torsinonsmodul. Dann:

(a) $x \in M$ heißt **p-primär**, wenn $e \in \mathbb{N}$ mit $p^e \cdot x = 0_M$ existiert;

(b) $M_p := \{x \in M \mid x\text{ist } p\text{-primär}\}$ ist der **R-Untermodul der p-primären Elementen** von M;

(c) M heißt **p-primär**, wenn $M = M_p$.

Beobachtung: $p_1, p_2 \in \mathbb{P}(R), u \in R^\times$ mit $p_1 = up_2 \implies M_{p_1} = M_{p_2}$.

Aufgabe 17.2 (*Blatt 7, Aufgabe 1(b)*)

Zeigen Sie, dass die Menge M_p aus Definition 17.1 ein R-Untermodul von M ist.

Beispiel 29

(1) Als $\mathbb{Z}$-Modul ist $(\mathbb{Z}/25\mathbb{Z})_5 = \mathbb{Z}/25\mathbb{Z}$.
Klar: Ordnungen der Elemente sind $1, 5$ oder $5^2 \implies 5^2 \cdot x = 0\ \forall x \in \mathbb{Z}/5\mathbb{Z}$

(2) Der $\mathbb{Z}$-Modul $\mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ ist 5-primär.

(3) $(\mathbb{Z}/25\mathbb{Z})_7 = 0$ (als $\mathbb{Z}$-Modul)
$= (\mathbb{Z}/25\mathbb{Z})_p\ \forall\, p \in \mathbb{P}(\mathbb{Z})\backslash\{\pm 5\}$

Satz 17.3

Ist M ein R-Tosionsmodul, so gilt

$$M = \bigoplus_{p \in \overline{\mathbb{P}}(R)} M_p\,.$$

Beweis:

(1) Zunächst zeigen wir, dass

$$M \leqslant_R \sum_{p \in \overline{\mathbb{P}}(R)} M_p$$

ist. Sei also $x \in M$. Weil R ein HIR ist, existiert $a \in R$ mit $\mathrm{Ann}_R(x) = \langle a \rangle$. Schreibe

$$a = u \cdot \prod_{i=1}^{n} p_i^{e_i}$$

für die Primfaktorzerlegung von a. O.B.d.A $u = 1$, denn es gilt $\langle a \rangle = \langle u^{-1} a \rangle$. Schreibe dann $a = p_i^{e_i} \cdot a_i$ mit

$$a_i := \prod_{\substack{j=1 \\ j \neq i}}^{n} p_j^{e_j}$$

$\forall\, 1 \leqslant i \leqslant n$. Somit ist $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ und nach dem Satz von Bézout existieren $b_1, \ldots, b_n \in R$ mit $\sum_{i=1}^{n} b_i a_i = 1$. Nun $\forall\, 1 \leqslant i \leqslant n$ setze $x_i := b_i a_i \cdot x$. Dann gilt $p_i^{e_i} \cdot x_i = \underbrace{p_i^{e_i} a_i} b_i x = b_i \underbrace{a x}_{=0} = 0$.
$\qquad\quad =a$

Somit $x_i \in M_{p_i}$ $\forall\, 1 \leqslant i \leqslant n$ und wir erhalten

$$x = 1 \cdot x = (\sum_{i=1}^{n} b_i a_i) \cdot x = \sum_{i=1}^{n} \underbrace{b_i a_i x}_{=x_i} = \sum_{i=1}^{n} x_i \text{ d.h. } x \in \sum_{i=1}^{n} M_{p_i} \leqslant_R \sum_{p \in \overline{\mathbb{P}}(R)} M_p \,.$$

(2) Weil alle M_p Untermoduln von M sind, folgt es aus (1), dass

$$M = \sum_{p \in \overline{\mathbb{P}}(R)} M_p$$

ist.

(3) Wir müssen noch zeigen, dass die Summe direkt ist. Wir nehmen also an, dass $\sum_{i=1}^{n} x_i = 0$ gilt, wobei $x_i \in M_{p_i}$ $\forall\, 1 \leqslant i \leqslant n$. Nach Definition von M_{p_i} $(1 \leqslant i \leqslant n)$ existiert $e_i \in \mathbb{N}$ mit $p_i^{e_i} x_i = 0$ $(\star)$. Setze also

$$a := \prod_{j=1}^{n} p_j^{e_j} = p_i^{e_i} \cdot a_i$$

mit $a_1, \ldots, a_n$ wie in Teil (1). Dann gilt $\mathrm{ggT}(p_i^{e_i}, a_i) = 1 \;\; \forall\, 1 \leqslant i \leqslant n$ und nach dem Satz von Bézout existieren $c_i, d_i \in R$ mit

$$c_i p_i^{e_i} + d_i a_i = 1 \,,$$

sodass

$$x_i = 1 \cdot x_i = (c_i p_i^{e_i} + d_i a_i) x_i = c_i \cdot \underbrace{p_i^{e_i} x_i}_{\substack{=0 \\ \text{nach } (\star)}} + d_i a_i x_i = d_i a_i x_i \quad (\star\star).$$

Somit gilt $\forall\, 1 \leqslant j \leqslant n$:

$$\begin{aligned} 0 &= d_j a_j \cdot (\sum_{i=1}^{n} x_i) \quad (\text{weil } 0 = \sum_{i=1}^{n} x_i) \\ &= \sum_{i=1}^{n} \underbrace{d_j a_j}_{\substack{=0 \,\forall\, i \neq j, \text{ weil} \\ a_j \in \mathrm{Ann}_R(x_j)}} x_i = d_j a_j x_j \overset{(\star\star)}{=} x_j \end{aligned}$$

und daher ist die Summe direkt. ∎

Lemma 17.4

Sei M ein R-Torsionsmodul. Dann gelten:

(a) $\mathrm{Ann}_R(M) =: \langle a \rangle$ mit $a \in R \backslash \{0\}$ und $\exists\, y \in M$ mit $\mathrm{Ann}_R(y) = \langle a \rangle$.

(b) Ist $a = u \cdot \prod_{i=1}^{n} p_i^{e_i}$ die Primfaktorzerlegung von a, so gilt

$$M = \bigoplus_{i=1}^{n} M_{p_i} \,,$$

wobei $\mathrm{Ann}_R(M_{p_i}) = \langle p_i^{e_i} \rangle$ für alle $1 \leqslant i \leqslant n$ ist.

Beweis:

(a) Sei $X := \{x_1, \dots, x_m\}$ ($m \in \mathbb{N}$) ein Erzeugendensystem für M. Dann $\forall\, 1 \leqslant i \leqslant n, \exists\, a_i \in R\backslash\{0\}$ mit $\mathrm{Ann}_R(x_i) = \langle a_i \rangle$, denn R ist ein HIR. Aus demselben Grund existiert $a \in R$ mit

$$\bigcap_{i=1}^{m} \mathrm{Ann}_R(x_i) = \langle a \rangle.$$

Z.z: $\mathrm{Ann}_R(M) = \langle a \rangle$.
„$\subseteq$“: Zunächst gilt $\langle a \rangle \overset{\text{Def.}}{=} \bigcap_{i=1}^{m} \mathrm{Ann}(x_i) \supseteq \bigcap_{x \in M} \mathrm{Ann}_R(x) = \mathrm{Ann}_R(M)$.
„$\supseteq$“: Sei $b \in \langle a \rangle$ und sei $x \in M$. Dann existieren $r_1, \dots, r_m \in R$ mit $x = \sum_{i=1}^{m} r_i x_i$. Daraus folgt

$$b \cdot x = \sum_{i=1}^{m} b r_i x_i = \sum_{i=1}^{m} r_i \underbrace{b x_i}_{=0} = 0\,.$$

Somit ist $b \in \mathrm{Ann}_R(M)$ und $\langle a \rangle \subseteq \mathrm{Ann}_R(M)$.
Rest von (a) beweisen wir nach Teil (b)!!

(b) Nach dem Beweis von Satz 17.3 gilt

$$M = \bigoplus_{i=1}^{n} M_{p_i}.$$

Außerdem gilt $\forall\, 1 \leqslant i \leqslant n$:

$$\mathrm{Ann}_R(M_{p_i}) \overset{\text{(Def.)}}{=} \bigcap_{x \in M_{p_i}} \mathrm{Ann}_R(x) \overset{(1)}{=} \langle p_i^{f_i} \rangle$$

mit $f_i \in \mathbb{N}$ und $f_i \leqslant e_i$.

Wir zeigen (1): Sei $1 \leqslant i \leqslant n$ fest. Dann $\forall\, x \in M_{p_i}, \exists\, e_i(x)$ mit $p_i^{e_i(x)} x = 0$ nach Definition von M_{p_i}.
Somit ist $p_i^{e_i(x)} \in \mathrm{Ann}_R(x) = \langle z_i \rangle$ mit $z_i \in R$. Daher gilt $p_i^{e_i(x)} \mid z_i$.
Andererseits wegen $\langle a \rangle = \mathrm{Ann}_R(M) = \mathrm{Ann}_R(\bigoplus_{i=1}^{n} M_{p_i}) \subseteq \mathrm{Ann}_R(x) = \langle z_i \rangle$ gilt $p_i^{e_i} x = 0$, wobei $p_i^{e_i} \neq 0$ ist, so dass $z_i \mid p_i^{e_i}$, was (1) zeigt.
Wie in (a) erhalten wir dann

$$\underbrace{\bigcap_{i=1}^{n} \langle p_i^{f_i} \rangle}_{= \langle \prod_{i=1}^{n} p_i^{f_i} \rangle} = \mathrm{Ann}_R(M) = \langle a \rangle.$$

Die Eindeutigkeit der Primfaktorzerlegung von a liefert $f_i = e_i$ $\forall\, 1 \leqslant i \leqslant n$ und $\exists\, y_i \in M_{p_i}$ mit $\mathrm{Ann}_R(y_i) = \langle p_i^{e_i} \rangle$ (sonst $\mathrm{Ann}_R(y_i) = \langle p_i^{f_i} \rangle$ mit $f_i < e_i$ $\lightning$ für ein i).

Zurück zu (a): Wegen $a_i \neq 0$ $\forall\, 1 \leqslant i \leqslant m$ ist auch $a \neq 0$ (R ist ein Integritätsring). Setze $y := \sum_{i=1}^{n} y_i$ (mit y_i wie in (b)). Dann existiert $b \in R$ mit

$$\mathrm{Ann}_R(y) = \langle b \rangle$$

und dauraus folgt, dass

$$0 = b \cdot y = \sum_{i=1}^{r} b \cdot y_i \in \bigoplus_{i=1}^{m} M_{p_i}.$$

Daher gilt $b y_i = 0$ $\forall\, 1 \leqslant i \leqslant n$ (weil die Summe direkt ist und $b y_i \in M_{p_i}$). Es folgt:

$$b \in \mathrm{Ann}_R(y_i) = \langle p_i^{e_i} \rangle \;\forall\, 1 \leqslant i \leqslant n \text{ und } b \in \bigcap_{i=1}^{n} \langle p_i^{e_i} \rangle = \langle a \rangle \text{ nach Teil (b)}\,.$$

Somit gilt $a|b$, aber $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(y) = \langle b \rangle$, sodass $b|a$. Schließlich $a|b$ und $b|a$ implizieren, dass $\langle a \rangle = \langle b \rangle$, wie gewünscht. ■

Satz 17.5

Sei $p \in \mathbb{P}(R)$. Ist $M \neq 0$ ein p-primärer R-Torsionsmodul, dann existieren $t \in \mathbb{N}$, $x_1, \ldots, x_t \in M$, $e_1, \ldots, e_t \in \mathbb{N}$ mit

$$M = \bigoplus_{i=1}^{t} Rx_i \,.$$

Dabei gilt:

(1) $\mathrm{Ann}_R(x_i) = \langle p^{e_i} \rangle$; und

(2) $e_1 \leqslant e_2 \leqslant \cdots \leqslant e_t$ sind durch M eindeutig bestimmt.

Beweis: (Beweisidee)
Weil M p-primär ist, gilt $M = M_p$. Dann nach Lemma 17.4 existiert ein $x \in M$ mit

$$\mathrm{Ann}_R(M) = \mathrm{Ann}_R(x) = \langle p^e \rangle$$

für ein $e \in \mathbb{Z}_{\geqslant 0}$. Setze also $\overline{M} := M/Rx$.

Schritt 1: Wir zeigen, dass

$$\overline{M} = \bigoplus_{i=1}^{m} R\overline{x_i}$$

für gewisse $\overline{x_i} \in \overline{M}$ $(1 \leqslant i \leqslant m)$. Dann existieren $x_i \in M$ $(1 \leqslant i \leqslant m)$ mit $\overline{x_i} = x_i + Rx$ und

$$\mathrm{Ann}_R(x_i) = \mathrm{Ann}_R(\overline{x_i}) \,,$$

sodass

$$M = Rx \oplus \bigoplus_{i=1}^{m} Rx_i \,.$$

Setze nun $M_{(p)} := \{z \in M \mid pz = 0\}$. Dann ist klar, dass $M_{(p)}$ ein $R/\langle p \rangle$-Modul ist. Zudem setze $K := R/\langle p \rangle$. Dann ist K ein Körper und $M_{(p)}$ ist ein K-Vektorraum. Da $M_{(p)}$ endlich erzeugt ist, folgt

$$\dim_K M_{(p)} < \infty.$$

Schritt 2: Setze

$$\overline{M}_{(p)} := M_{(p)}/\big(M_{(p)} \cap Rx\big).$$

Dann gilt

$$\dim_K \overline{M}_{(p)} < \dim_K M_{(p)}.$$

Klar: Sei $\{\overline{y}_1, \ldots, \overline{y}_m\}$ eine K-Basis von $\overline{M}_{(p)}$.

$$\text{Dann } \{\overline{y}_1, \ldots, \overline{y}_m\} \xrightarrow{\text{Schritt 1}} \text{es existieren } y_i \in M_{(p)} \text{ mit } \overline{y}_i = y_i + (M_{(p)} \cap Rx),$$

und $\mathrm{Ann}_R(y_i) = \langle p \rangle$, wobei $y_1, \ldots, y_m$ R-linear unabhängig sind. Dann folgt: $y_1, \ldots, y_m$ sind auch K-linear unabhängig in $M_{(p)}$.
Außerdem: Aus $\mathrm{Ann}_R(x) = \langle p^e \rangle$ folgt für $y := p^{e-1}x$,

$$\mathrm{Ann}_R(y) = \langle p \rangle \quad \text{und} \quad \overline{y} = 0 \text{ in } \overline{M}_{(p)}.$$

Daher ist $\{y, y_1, \ldots, y_m\}$ K-linear unabhängig in $M_{(p)}$.
Schritt 3: Wir zeigen, dass

$$M = \bigoplus_{i=1}^{t} Rx_i \quad \text{mit} \quad \operatorname{Ann}_R(x_i) = \langle p^{e_i} \rangle.$$

Dies folgt durch Induktion über $\dim_K M_{(p)}$ mit Hilfe der Zerlegung aus Schritt 1.

Schritt 4: Die e_i sind paarweise verschieden. ∎

Folgerung 17.6

Mit den Voraussetzungen von Satz 17.5 gilt

$$M \cong \bigoplus_{i=1}^{t} R/\langle p^{e_i} \rangle .$$

18 Der Hauptsatz

Aus Satz 16.1, Satz 17.3, Lemma 17.4 und Satz 17.5 folgt nun die gewünschte Klassifikation der endlich erzeugten Moduln über Hauptidealringe:

Satz 18.1 (Hauptsatz: Klassifikation der e.e. Moduln über HIR)

Sei R ein HIR und sei M ein endlich erzeugter R-Modul. Dann ist M der Form

$$M = \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} Rx_{ij} \oplus F$$

mit $s \in \mathbb{Z}_{\geqslant 0}$, $t_i \in \mathbb{N}\ \forall\, 1 \leqslant i \leqslant s$. Außerdem gelten:

- F ist ein freier R-Untermodul von M;
- $x_{ij} \in M\ \forall\, 1 \leqslant i \leqslant s, \forall\, 1 \leqslant j \leqslant t_i$ mit $\operatorname{Ann}_R(x_{ij}) = \langle p_i^{e_{ij}} \rangle$ und $p_i \in \overline{\mathbb{P}}(R)$ paarweise verschieden, $e_{i1} \leqslant e_{i2} \leqslant \cdots \leqslant e_{it_i}$ eindeutig bestimmt.

Aufgabe 18.2 (*Aufgabe 1(b), Blatt 8*)

Sei M ein endlich erzeugter R-Modul. Dann existieren $d_1, \ldots, d_s \in R\backslash\{0\}$ mit $1 \neq d_1 \mid d_2 \mid \cdots \mid d_s$ und $t \in \mathbb{Z}_{\geqslant 0}$, so dass

$$M \cong R/Rd_1 \oplus \ldots \oplus R/Rd_s \oplus R^t .$$

Sowohl die Ideale $\langle d_1 \rangle \supseteq \ldots \supseteq \langle d_s \rangle$ von R als auch die Zahl t sind eindeutig durch M bestimmt.

Im Folgenden wollen wir un ein paar Anwendungen des Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen betrachten.

Als erstes erhalten wir eine Verallgemeinerung des chinesischen Restsatzes.

Satz 18.3 (*Hauptsatz über simultane Kongruenzen*)

Sei R ein Hauptidealring, $a \in R\backslash(R^\times \cup \{0\})$ mit Primfaktorzerlegung $a = u \cdot \prod_{i=1}^{n} p_i^{e_i}$ wie in Schreibweise 15.3. Dann gilt

$$R/\langle a\rangle \cong \bigoplus_{i=1}^{n} R/\langle p_i^{e_i}\rangle .$$

Beweis: Wie in der Algebra I (klassischer chinesischer Restsatz), oder als direkte Folgerung aus dem Hauptsatz über endlich erzeugte Moduln (siehe Aufgabe 1, Blatt 8). ■

Als nächste Anwendung betrachten wir die Klassifikation der endlich erzeugten abelschen Gruppen.

Satz 18.4 (*Hauptsatz über endlich erzeugte abelsche Gruppen*)

Sei A eine endlich erzeugte abelsche Gruppe. Dann existieren $s, r, t_i, e_{i_j} \in \mathbb{Z}_{\geqslant 0}$ und $p_i \in \overline{\mathbb{P}}(\mathbb{Z})$ $(1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant t_i)$, so dass

$$A \cong \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} \mathbb{Z}/p_i^{e_{i_j}}\mathbb{Z} \ \oplus \ \bigoplus_{i=1}^{r} \mathbb{Z}\,.$$

Dabei sind alle Parameter eindeutig durch M bestimmt.

Beweis: Hauptsatz für endlich erzeugte Moduln mit $R = \mathbb{Z}$ zusammen mit Folgerung 17.6. ■

Schließlich wollen wir den Hauptsatz noch mit der Jordanschen Normalform in Verbindung bringen.

Satz 18.5 (*Jordansche Normalform*)

Sei $A \in \mathrm{M}_n(K)$ mit $n \in \mathbb{N}$. Dann existiert $J \in \mathrm{GL}_n(K)$, sodass JAJ^{-1} in Jordanscher Normalform ist.

Jordansche Normalform.
Wir erarbeiten zunächst die allgemeine Jordansche Normalform über einem Körper K.
Sei $K[X] := R$ ein Hauptidealring, sei V ein K-Vektorraum mit $\dim_K(V) < \infty$ und sei $\Phi \in \mathrm{End}_K(V)$ ein K-linearer Endomorphismus von V.

Nach Aufgabe 3 auf Blatt 0 ist V ein R-Modul mit äußerer Multiplikation

$$\cdot : R \times V \to V, \quad (f, v) \mapsto f \cdot v := f(\Phi)(v).$$

Sei $g_\Phi \in R$ das Minimalpolynom von Φ. Dann gilt

$$0 = g_\Phi \cdot v = g_\Phi(\Phi)(v) \qquad \forall\, v \in V$$

und daher ist $g_\Phi \in \mathrm{Ann}_R(V)$. Tatsächlich gilt sogar $\mathrm{Ann}_R(V) = \langle g_\Phi\rangle_R$, da g_Φ minimal ist. Somit ist V, als R-Modul gesehen, ein R-Torsionsmodul mit

$$\mathrm{Ann}_R(V) = \langle g_\Phi\rangle_R\,.$$

Sei also

$$g_\Phi = u \cdot \prod_{i=1}^{s} p_i(X)^{e_i}$$

die Primfaktorzerlegung von g_Φ (d.h. mit $u \in K\backslash\{0\}$ und $p_1(X), \dots, p_n(X) \in R$ irreduzibel und paarweise teilerfremd. Dann ergibt sich die Primärzerlegung von V als R-Modul zu

$$V = \bigoplus_{i=1}^{s} V_{p_i(X)},$$

wobei

$$\mathrm{Ann}_R\big(V_{p_i(X)}\big) = \langle p_i(X)^{e_i}\rangle_R \quad \text{für alle } 1 \leqslant i \leqslant s.$$

Jeder $p_i(X)$-primäre Modul ist von der Form

$$V_{p_i(X)} = \bigoplus_{j=1}^{t_i} Rv_{ij}, \quad \text{mit } \mathrm{Ann}_R(v_{ij}) = \langle p_i(X)^{e_{ij}}\rangle,$$

wobei gilt $e_{i1} \leqslant e_{i2} \leqslant \cdots \leqslant e_{it_i} = e_i$, und diese Exponentenfolge ist durch V eindeutig bestimmt. Setze $f_i := \deg(p_i(X))$ und schreibe

$$p_i(X) = \sum_{k=1}^{f_i} a_k X^k.$$

Dann ist die Menge

$$B_{ij} := \big\{v_{ij}, \Phi(v_{ij}), \dots, \Phi^{f_i-1}(v_{ij}),\ p_i(\Phi)(v_{ij}), \Phi(p_i(\Phi)(v_{ij})), \dots, \Phi^{f_i-1}(p_i(\Phi)(v_{ij})),\ \dots,$$

$$p_i(\Phi)^{e_{ij}-1}(v_{ij}), \dots, \Phi^{f_i-1}(p_i(\Phi)^{e_{ij}-1}(v_{ij}))\big\}$$

eine Basis von Rv_{ij}. Die Matrixdarstellung $D_{B_{ij}}(\Phi)$ von $\Phi|_{Rv_{ij}}$ bezüglich dieser Basis ist ein *verallgemeiner Jordanblock*, dessen Blockstruktur wie folgt aussieht:

$$\begin{bmatrix}
0 & 0 & \cdots & 0 & -a_{i0} & & & & \\
1 & 0 & \cdots & 0 & -a_{i1} & & & 0 & \\
0 & 1 & \cdots & 0 & -a_{i2} & & & & \\
\vdots & \vdots & \ddots & \vdots & \vdots & & & & \\
0 & 0 & \cdots & 1 & -a_{i,f_i-1} & & & & \\
 & & & & \mathbf{1} & 0 & 0 \cdots & -a_{i0} & \\
 & & & & & 1 & 0 \cdots & -a_{i1} & \\
 & & & & & 0 & 1 \cdots & -a_{i2} & \\
 & & & & & \vdots & \vdots \ddots & \vdots & \\
 & & & & & 0 & 0 \cdots & -a_{i,f_i-1} & \\
 & & 0 & & & & & \mathbf{1} & \\
 & & & & & & & & \ddots
\end{bmatrix}$$

Weil

$$V = \bigoplus_{i,j} Rv_{ij}$$

ist, nehmen wir dann

$$B = \bigcup_{i,j} B_{ij}.$$

Somit ist die Matrix von Φ bzgl. B der Form

$$D_B(\Phi) = \begin{bmatrix} J_{11} & & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & J_{st_s} \end{bmatrix},$$

wobei $J_{ij} := D_{B_{ij}}(\Phi)$. Wir nennen die Matrix $D_B(\Phi)$ die **verallgemeinerte Jordan-Normalform** von Φ.

Damit kehren wir zum eigentlichen Beweis zurück.

Beweis: Setze $V := K^n$. Dann kann A als Matrix eines K-Endomorphismus $\Phi \in \mathrm{End}_K(V)$ bezüglich der Standardbasis E von V betrachtet werden. Sei B die oben konstruierte Basis von V. Somit ist die Matrix von Φ bezüglich B in Jordanscher Normalform. Die Basiswechselmatrix von E nach B sei J. Dann gilt

$$JAJ^{-1} = D_B(\Phi),$$

wobei $D_B(\Phi)$ die Jordan-Normalform von Φ ist. Somit existiert eine invertierbare Matrix $J \in \mathrm{GL}_n(K)$ mit JAJ^{-1} = Jordanscher Normalform von A. ∎

In diesem Kapitel untersuchen wir Tensorprodukte von Moduln. Es handelt sich um eine Konstruktion die neuen Moduln aus alten Moduln produziert!

Konventionen: In diesem Kapitel ist R wieder ein beliebiger Ring. Außerdem sind $M, M', M_1, M_2, \ldots, M_i$ $(i \in I)$ stets als R-Rechtsmoduln und $N, N', N_1, N_2, \ldots, N_j$ $(j \in J)$ stets als R-Linksmoduln zu verstehen. Ferner bezeichnet A stets eine abelsche Gruppe, also ein $\mathbb{Z}$-Modul.

19 Tensorprodukte von Moduln

Definition 19.1 (*Tensorprodukt*)

Sei M ein R-Rechtsmodul und sei N ein R-Linksmodul. Sei F der freier $\mathbb{Z}$-Modul mit $\mathbb{Z}$-Basis $M \times N$ (hier als Menge gesehen) und betrachte die Teilmenge

$$\begin{aligned} X := &\{(m_1 + m_2, n) - (m_1, n) - (m_2, n) \in F \mid m_1, m_2 \in M, N \in N\} \\ &\cup \{(m, n_1 + n_2) - (m, n_1) - (m, n_2) \in F \mid m \in M, n_1, n_2 \in N\} \\ &\cup \{(mr, n) - (m, rn) \in F \mid m \in M, n \in N, r \in R\} \end{aligned}$$

von F. Das **Tensorprodukt** von M und N (**ausgeglichen**) **über** R ist die Faktorgruppe

$$M \otimes_R N := F/\langle X \rangle_{\mathbb{Z}}\,.$$

Die Elemente $m \otimes n := (m, n) + \langle X \rangle_{\mathbb{Z}}$ von $M \otimes_R N$ heißen **Elementartensoren**.

Die folgenden Eigenschaften folgen direkt aus Definition 19.1.

Anmerkung 19.2

(a) Es ist $M \otimes_R N = \langle\, m \otimes n \mid m \in M,\ n \in N \,\rangle_{\mathbb{Z}}$.

(b) Es gilt $\forall\, m, m_1, m_2 \in M,\ n, n_1, n_2 \in N,\ r \in R$:

(i) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$;

(ii) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$; und

(iii) $(mr) \otimes n = m \otimes (rn)$.

Aufgabe 19.3 (*Aufgabe 2(a)(i), Blatt 8*)

Für jeden $m \in M$ und für jeden $n \in N$ gelten:

(i) $m \otimes 0 = 0 = 0 \otimes n$; und

(ii) $m \otimes (-n) = -(m \otimes n) = (-m) \otimes n$.

Definition 19.4 (*ausgeglichene Abbildung*)

Eine Abbildung $f : M \times N \longrightarrow A$ heißt **ausgeglichen**, falls $\forall\, m, m_1, m_2 \in M$, $\forall\, n_1, n_2 \in N$ und $\forall\, r \in R$ folgende Bedingungen gelten:

(1) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$;

(2) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$;

(3) $f(mr, n) = f(m, rn)$.

Anmerkung: Bedingungen (1) und (2) besagen, dass f $\mathbb{Z}$-bilinear ist.

Lemma 19.5

Die kanonische Abbildung $t : M \times N \longrightarrow M \otimes_R N$, $(m, n) \mapsto m \otimes n$ ist ausgeglichen.

Beweis: Dies folgt direkt aus der Definition von $M \otimes_R N$. Wir beweisen beispielhaft Bedingung (1). Nach Anmerkung 19.2(b)(ii) $\forall\, m_1, m_2 \in M$, $\forall\, n \in N$ gilt

$$t(m_1 + m_2, n) = (m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n = t(m_1, n) + t(m_2, n).$$

Analog werden Bedingungen (2) und (3) bewiesen. ∎

Satz 19.6 (*Universelle Eigenschaft des Tensorproduktes*)

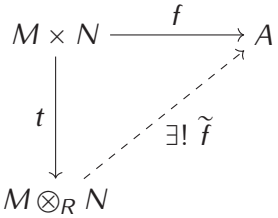
Sei M ein R-Rechtsmodul und sei N ein R-Linksmodul. Dann existiert für jeden $\mathbb{Z}$-Modul A und jede ausgeglichene Abbildung

$$f : M \times N \longrightarrow A$$

genau ein $\mathbb{Z}$-Homomorphismus

$$\widetilde{f} : M \otimes_R N \longrightarrow A,$$

so dass folgendes Diagramm kommutiert:

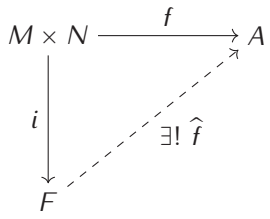


Beweis: Wir verwenden in diesem Beweis die Schreibweise aus der Definition von $M \otimes_R N$.

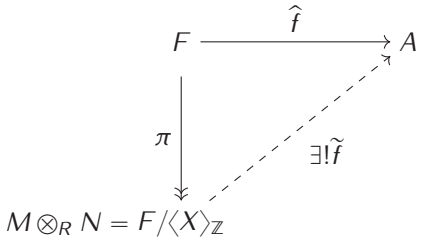
Schreibe $i : M \times N \hookrightarrow F$ für die kanonische Abbildung und $\pi : F \twoheadrightarrow F/\langle X \rangle_{\mathbb{Z}} = M \otimes_R N$ für die

Faktorabbildung. Außerdem sei $t : M \times N \longrightarrow M \otimes_R N$ die kanonische Abbildung aus Lemma 19.5. Nach Definition von t gilt dann $t = \pi \circ i$.

(1) Zunächst liefert die universelle Eigenschaft der freien $\mathbb{Z}$-Moduln einen eindeutig bestimmten $\mathbb{Z}$-Homomorphismus $\widehat{f} : F \longrightarrow A$ mit $\widehat{f} \circ i = f$.



(2) Weil f ausgeglichen ist, gilt $\langle X \rangle_{\mathbb{Z}} \subseteq \ker(\widehat{f})$ (nach Definition von X). Somit liefert die universelle Eigenschaft des Faktormoduls



den eindeutig bestimmten $\mathbb{Z}$-Homomorphismus

$$\widetilde{f} : M \otimes_R N \longrightarrow A$$

mit

$$\widetilde{f} \circ \pi = \widehat{f}.$$

Aus (1) und (2) folgt nun, dass

$$\widetilde{f} \circ t = \widetilde{f} \circ \pi \circ i = \widehat{f} \circ i = f\,.$$

■

Anmerkung 19.7

Das Tensorprodukt von M und N über R sollte eigentlich als Paar $(M \otimes_R N, t)$ gedacht werden, wobei t die kanonische Abbildung ist.

Aufgabe 19.8 (*Aufgabe 2(a)(iii), Blatt 8*)

Zeigen Sie: Das Paar $(M \otimes_R N, t)$ ist eindeutig durch seine universelle Eigenschaft bestimmt. D.h.: Erfüllt das Paar (T, t') auch die universelle Eigenschaft des Tensorprodukts, so gilt:

$$\exists!\, \alpha \in \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, T) \quad \text{mit} \quad t' = \alpha \circ t\,.$$

Aufgabe 19.9 (*Aufgabe 2(a)(ii), Blatt 8*)

Sei M ein R-Rechtsmodul und sei N ein R-Linksmodul. Zeigen Sie, dass es Isomorphismen von abelschen Gruppen $R \otimes_R N \cong N$ und $M \otimes_R R \cong M$ gibt.

Lemma 19.10 (*Tensorprodukt von Homomorphismen*)

Ist $f : M \longrightarrow M'$ ein Homomorphismus von R-Rechtsmoduln und $g : N \longrightarrow N'$ ein Homomorphismus von R-Linksmoduln, so ist die Abbildung

$$\begin{aligned} f \otimes g : M \otimes_R N &\longrightarrow M' \otimes_R N' \\ m \otimes n &\mapsto f(m) \otimes g(n) \end{aligned}$$

ein $\mathbb{Z}$-Homomorphismus. Wir nennen diese Abbildung **Tensorprodukt** von f und g.

Beweis : Die Abbildung

$$\begin{array}{ccccc} M \times N & \xrightarrow{(f,g)} & M' \times N' & \xrightarrow{t_{M' \otimes_R N'}} & M' \otimes_R N' \\ (m,n) & \longmapsto & (f(m), g(n)) & \longmapsto & f(m) \otimes g(n) \end{array}$$

ist ausgeglichen über R, denn f und g sind R-Homomorphismen und $t_{M' \otimes_R N'}$ ist ausgeglichen über R nach Lemma 19.10. Nach der universellen Eigenschaft des Tensorproduktes (19.6) gibt es genau einen $\mathbb{Z}$-Homomorphismus $f \otimes g := t_{M' \otimes_R N'} \circ (f, g)$, so dass das Diagramm

$$\begin{array}{ccc} M \times N & \xrightarrow{(f,g)} & M' \times N' \\ {\scriptstyle t_{M \otimes_R N}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle t_{M' \otimes_R N'}} \\ M \otimes_R N & \xrightarrow[f \otimes g]{} & M' \otimes_R N' \end{array}$$

kommutativ ist. Dann gilt

$$\begin{aligned} (f \otimes g)(m \otimes n) &= (f \otimes g) \circ t_{M \otimes_R N}(m, n) \\ &= t_{M' \otimes_r N'} \circ (f, g)(m, n) \\ &= t_{M' \otimes_r N'}(f(m), g(n)) \\ &= f(m) \otimes g(n) \end{aligned}$$

für alle $m \in M$ und für alle $n \in N$ nach Konstruktion. ∎

Anmerkung 19.11

Die folgenden elementaren Eigenschaften folgen direkt aus Lemma 26.13:

(i) $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$; und

(ii) für Verkettungen $M \xrightarrow{f} M' \xrightarrow{f'} M''$ und $N \xrightarrow{g} N' \xrightarrow{g'} N''$ von Homomorphismen von R-Rechtsmoduln bzw. R-Linksmoduln gilt

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)\,.$$

20 Modulstruktur

Wir betonen, dass das Tensorprodukt $M \otimes_R N$ zweier Moduln nach Definition ein $\mathbb{Z}$-Modul ist, d.h. eine abelsche Gruppe, Unter bestimmten Voraussetzungen trägt es jedoch die Struktur eines Moduls (oder Bimoduls), wie die folgenden Aufgaben zeigen.

Aufgabe 20.1 (*Aufgabe 2(b), Blatt 8*)

Seien Q, R und S Ringe. Zeigen Sie:

(a) Ist M ein (Q,R)-Bimodul und N ein R-Linksmodul, so ist $M \otimes_R N$ ein Q-Linksmodul mit äußerer Multiplikation

$$\begin{aligned} Q \times (M \otimes_R N) &\longrightarrow M \otimes_R N \\ (q, m \otimes n) &\mapsto q \cdot (m \otimes n) := (q \cdot m) \otimes n\,. \end{aligned}$$

(b) Ist M ein R-Rechtsmodul und N ein (R,S)-Bimodul, so ist $M \otimes_R N$ ein S-Rechtsmodul mit äußerer Multiplikation

$$\begin{aligned} (M \otimes_R N) \times S &\longrightarrow M \otimes_R N \\ (m \otimes n, s) &\mapsto (m \otimes n) \cdot s := m \otimes (n \cdot s)\,. \end{aligned}$$

Beispiel 30

(a) Mit der üblichen Schreibweise gelten:

$$\begin{aligned} M \otimes_R R &\cong M \quad \text{(als } R\text{-Rechtsmodul), und)} \\ R \otimes_R N &\cong N \quad \text{(als } R\text{-Linksmodul).} \end{aligned}$$

Z.B. ist die Abbildung

$$\begin{aligned} \alpha : M \times R &\longrightarrow M \\ (m, r) &\mapsto mr \end{aligned}$$

ausgeglichen über R, so dass die universelle Eigenschaft des Tensorprodukts einen Isomorphismus $\widetilde{\alpha}$ mit $\widetilde{\alpha} m \otimes r = mr$ für jedes $m \in M$ und jedes $r \in R$ liefert.

(b) Ist $I \subseteq R$ ein Ideal eines kommutativen Ringes, so gibt es einen Isomorphismus von R-Linksmoduln

$$R/I \otimes_R N \cong N/IN$$

für jeden R-Linksmodul. Zunächst liefert die universelle Eigenschaft des Tensorprodukts einen $\mathbb{Z}$-Homomorphismus

$$\widetilde{\alpha} : R/I \otimes_R N \longrightarrow N/IN\,,$$

der R-linear ist, und die universelle Eigenschaft des Faktormoduls liefert einen R-Homomorphismus

$$\widetilde{\beta} : N/IN \longrightarrow R/I \otimes_R N/IN\,.$$

Man zeigt leicht, dass $\widetilde{\alpha}$ und $\widetilde{\beta}$ inverse Abbildungen sind. Siehe Aufgabe 3(a), Blatt 8.

Lemma 20.2 (*Assoziativität des Tensorprodukts*)

Seien R und S zwei Ringe. Sei M ein R-Rechtsmodul, sei N ein (R,S)-Bimodul und sei P ein S-Linksmodul. Dann gilt

$$M \otimes_R (N \otimes_S P) \cong_{\mathbb{Z}} (M \otimes_R N) \otimes_S P.$$

Beweis: Für jedes Element $x \in M$ definiere

$$\begin{aligned} \alpha_x : N \times P &\longrightarrow (M \otimes_R N) \otimes_S P \\ (n,p) &\mapsto (x \otimes n) \otimes p \end{aligned}$$

Diese Abbildung ist offensichtlich ausgeglichen über S. Die universelle Eigenschaft des Tensorprodukts liefert also die Existenz eines $\mathbb{Z}$-Homomorphismus

$$\widetilde{\alpha}_x : N \otimes_S P \longrightarrow (M \otimes_R N) \otimes_S P \quad \text{mit } \widetilde{\alpha}_x \circ t = \alpha_x,$$

d.h. $\widetilde{\alpha}_x(n \otimes p) = (x \otimes n) \otimes p$ für alle $n \in N$ und für alle $p \in P$. Definiere nun

$$\begin{aligned} \beta : \ M \times (N \otimes_S P) &\longrightarrow (M \otimes_R N) \otimes_S P \\ (m,w) &\mapsto \widetilde{\alpha}_m(w) \end{aligned}$$

Diese Abbildung ist offensichtlich ausgeglichen über R. Die universelle Eigenschaft des Tensorprodukts liefert also die Existenz eines $\mathbb{Z}$-Homomorphismus

$$\widetilde{\beta} : \ M \otimes_R (N \otimes_S P) \longrightarrow (M \otimes_R N) \otimes_S P$$

mit $\widetilde{\beta} \circ t = \beta$, d.h. $\widetilde{\beta}(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$ für alle $m \in M$, für alle $n \in N$ und für alle $p \in P$. Analog erhält man einen eindeutig bestimmten $\mathbb{Z}$-Homomorphismus

$$\widetilde{\gamma} : \quad (M \otimes_R N) \otimes_S P \longrightarrow M \otimes_R (N \otimes_S P)$$

mit $\widetilde{\gamma}((m \otimes n) \otimes p) = m \otimes (n \otimes p)$, für alle $m \in M$, für alle $n \in N$ für alle $p \in P$. Somit gilt

$$\widetilde{\beta} \circ \widetilde{\gamma} = \mathrm{id}, \widetilde{\gamma} \circ \widetilde{\beta} = \mathrm{id} \Rightarrow \widetilde{\beta}$$

und $\widetilde{\gamma}$ sind Isomorphismen. ■

Wiederholung: Ist R ein kommutativ er Ring, so wissen wir aus Kapitel 1: Ist M ein R-Rechtsmodul (bzw. N ein R-Linksmodul), so wird M auf natürliche Weise zu einem R-Linksmodul (bzw. zu einem R-Rechtsmodul). D.h.: In diesem FAll können alle R-Moduln als (R,R)-Bimoduln verstanden werden!

Anmerkung 20.3

Sei R ein kommutativer Ring. In der universellen Eigenschaft des Tensorprodukts (siehe 19.6) gilt: Ist A ein R-Modul und die Abbildung $f : M \times N \longrightarrow A$ R-bilinear (also ausgeglichen), so ist der $\mathbb{Z}$-Homomorphismus $\widetilde{f}$ eigentlich ein R-Homomorphismus.

Lemma 20.4 (*Kommutativität des Tensorprodukts*)

Sei R ein kommutativer Ring. Seien M und N zwei R-Moduln (verstanden als (R,R)-Bimoduln). Dann gilt

$$M \otimes_R N \cong_R N \otimes_R M.$$

Beweis: Die Abbildung

$$\alpha : M \times N \longrightarrow N \otimes_R M$$
$$(m, n) \mapsto n \otimes m$$

ist offensichtlich R-bilinear. Die universelle Eigenschaft des Tensorprodukts und Anmerkung 20.5 liefern also: Es gibt einen eindeutig bestimmten R-Homomorphismus

$$\widetilde{\alpha} : M \otimes_R N \longrightarrow N \otimes_R M,$$

so dass $\widetilde{\alpha}(m \otimes n) = n \otimes m$ für alle $m \in M$ und für alle $n \in N$.
Analog: Es existiert genau ein R-Homomorphismus $\widetilde{\beta} : N \otimes_R M \longrightarrow M \otimes_R N$ mit $\widetilde{\beta}(n \otimes m) = m \otimes n$ für alle $m \in M$ und für alle $n \in N$. Außerdem gilt $\widetilde{\alpha} \circ \widetilde{\beta} = \mathrm{id}$ und $\widetilde{\beta} \circ \widetilde{\alpha} = \mathrm{id}$. Somit sind $\widetilde{\alpha}$ und $\widetilde{\beta}$ R-Isomorphismen. ■

21 Tensorprodukte und Direkte Summen

Lemma 21.1 (*Distributivität des Tensorprodukts*)

Sei $\{M_i\}_{i \in I}$ eine Familie von R-Rechtsmoduln und sei $\{N_j\}_{j \in J}$ eine Familie von R-Linksmoduln. Dann gilt

$$(\bigoplus_{i \in I} M_i) \otimes_R (\bigoplus_{j \in J} N_j) \cong_{\mathbb{Z}} \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j).$$

Beweisskizze: Die Abbildung

$$\alpha : (\bigoplus_{i \in I} M_i) \times (\bigoplus_{j \in J} N_j) \longrightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j)$$
$$(\sum_i m_i, \sum_j n_j) \mapsto \sum_{(i,j)} m_i \otimes n_j$$

ist ausgeglichen über R.

- Die universelle Eigenschaft des Tensorprodukts liefert also die Existenz eines $\mathbb{Z}$-Homomorphismus

$$\widetilde{\alpha} : (\bigoplus_{i \in I} M_i) \otimes_R (\bigoplus_{j \in J} N_j) \longrightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j),$$

  sodass $\widetilde{\alpha}((\sum_i m_i) \otimes (\sum_j n_j)) \mapsto \sum (i,j) m_i \otimes n_j$.

- Definiere dann

$$\widetilde{\beta} : \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R N_j) \longrightarrow (\bigoplus_{i \in I} M_i) \otimes_R (\bigoplus_{j \in J} N_j)$$
$$\sum_{(i,j)} m_i \otimes n_j \mapsto \sum \eta_i(m_i) \otimes \eta_j(n_j)$$

Es gilt $\widetilde{\alpha} \circ \widetilde{\beta}$ id und $\widetilde{\beta} \circ \widetilde{\alpha} = \mathrm{id}$, so dass $\widetilde{\alpha}$ und $\widetilde{\beta}$ Isomorphismen sind. ■

Folgerung 21.2

Ist M ein R-Rechtsmodul und F ein freier R-Linksmodul mit R-Basis X, so gilt

$$M \otimes_R F \cong_{\mathbb{Z}} \bigoplus_{x \in X} M .$$

Beweis: Schreibe $F \cong \bigoplus_{x \in X} R$. Dann gilt

$$\begin{aligned} M \otimes_R F &\cong M \otimes_R (\bigoplus_{x \in X} R) \\ &\cong \bigoplus_{x \in X} (M \otimes_R R) \\ &\cong \bigoplus_{x \in X} M . \end{aligned}$$

■

Folgerung 21.3

Sei R kommutativ und seien F und F' freie R-Moduln mit R-Basen $\{x_i\}_{i \in I}$ bzw. $\{y_j\}_{j \in J}$. Dann ist $F \otimes_R F'$ ein freier R-Modul mit R-Basis $\{x_i \otimes y_j\}_{(i,j) \in I \times J}$ und es gilt

$$\operatorname{rg}_R(F \otimes_R F') = \operatorname{rg}_R(F) \cdot \operatorname{rg}_R(F') .$$

Beweis: Schreibe $F = \bigoplus_{i \in I} x_i R$ und $F' = \bigoplus_{j \in J} R y_j$. Dann gilt

$$\begin{aligned} F \otimes_R F' &= (\bigoplus_{i \in I} x_i R) \otimes_R (\bigoplus_{j \in J} R y_j) \\ &= \bigoplus_{(i,j) \in I \times J} \underbrace{x_i R \otimes_R R y_j}_{\cong R(x_i \otimes y_j)} \end{aligned}$$

■

Beispiel 31

Das Tensorprodukt $V \otimes_K W$ zweier K-Vektorräume V und W ist wieder ein K-Vektorraum mit

$$\dim_K(V \otimes_K W) = \dim_K V \cdot \dim_K W .$$

Teil II.
Kategorientheorie

Hintergrund-Mengenlehre.

- Arbeitet man mit den Axiomen zur Mengenlehre von Zermelo-Fraenken (+ Auswahlaxiom), so ist es bekannt, dass die „Ansammlung aller Mengen" keine Menge ist.
- Aus diesem Grund arbeitet man in der Kategorientheorie mit den Axiomen von Neumann-Bernays-Gödel (NBG). Hiermit sind solche Ansammlungen erlaubt: Es sind „Klassen".

  Wir verwenden den Begriff „Klasse" nur informell, um Ansammlungen zu beschreiben!!

22 Kategorien

Definition 22.1 (*Kategorie*/*Objekt*/*Morphismus*/*Komposition*)

Eine **Kategorie** $\mathcal{C}$ besteht aus:

- eine Klasse $\mathcal{O}\mathrm{b}(\mathcal{C})$ von **Objekten**;
- Klassen $\mathrm{Hom}_{\mathcal{C}}(A,B)$ von **Morphismen** zu allen $A,B \in \mathcal{O}\mathrm{b}(\mathcal{C})$; und
- **Kompositionen**:
$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(A,B)\times\mathrm{Hom}_{\mathcal{C}}(B,C) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,C)\\ (f,g) &\longmapsto g\circ f\end{aligned}$$
zu allen $A,B,C \in \mathcal{O}\mathrm{b}(\mathcal{C})$.

Dabei wird verlangt, das folgende Axiome erfüllt sind:

(K1) $\mathrm{Hom}_{\mathcal{C}}(A,B)\cap\mathrm{Hom}_{\mathcal{C}}(C,D)=\varnothing \quad \forall\, A,B,C,D\in\mathcal{O}\mathrm{b}(\mathcal{C})$ mit $(A,B)\neq(C,D)$;

(K2) $h\circ(g\circ f)=(h\circ g)\circ f \qquad \forall\, A,B,C,D\in\mathcal{O}\mathrm{b}(\mathcal{C}),\ f\in\mathrm{Hom}_{\mathcal{C}}(A,B),\ g\in\mathrm{Hom}_{\mathcal{C}}(B,C),$ und $h\in\mathrm{Hom}_{\mathcal{C}}(C,D)$;

(K3) $\forall\, A\in\mathcal{O}\mathrm{b}(\mathcal{C}),\exists\ \mathrm{id}_A\in\mathrm{Hom}_{\mathcal{C}}(A,A)$ mit

$$g\circ\mathrm{id}_A=g \quad \text{und} \quad \mathrm{id}_A\circ f=f$$

$\forall\, B\in\mathcal{O}\mathrm{b}(\mathcal{C}), g\in\mathrm{Hom}_{\mathcal{C}}(A,B), f\in\mathrm{Hom}_{\mathcal{C}}(B,A)$.

Anmerkung 22.2

(1) Man schreibt Morphismen in der Form $f : A \longrightarrow B$ oder $A \xrightarrow{f} B$. Es bedeutet aber nicht, dass Morphismen Abbildungen sind!!

(2) Der Morphismus id_A ist die **Identität** von A in $\mathcal{C}$.

(3) Oft spricht man einfach von einem Objekt A in $\mathcal{C}$ und von einem Morphismus $f : A \longrightarrow B$ in $\mathcal{C}$.

(4) Sind $\mathcal{O}\mathrm{b}(\mathcal{C})$ und alle $\mathrm{Hom}_{\mathcal{C}}(A, B)$ Mengen, so nennt man $\mathcal{C}$ eine **kleine** Kategorie.

(5) Sind alle $\mathrm{Hom}_{\mathcal{C}}(A, B)$ Mengen, so nennt man $\mathcal{C}$ **lokal klein**.

(6) Wir schreiben $\mathrm{Mor}(\mathcal{C}) := \bigcup_{A,B \in \mathcal{O}\mathrm{b}(\mathcal{C})} \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Beispiel 32

(1) Algebraische/ Topologische Strukturen Zunächst gibt es viele natürliche Beispiele aus der Algebra und aus der Topologie, für die die Morphismen einfach Abbildungen sind.

Schreibweise	$\mathcal{O}\mathrm{b}(\mathcal{C})$	$\mathrm{Mor}(\mathcal{C})$	Komposition
$\mathcal{S}$et	Alle Mengen	Alle Abbildungen zwischen Mengen	Übliche Kompositionen der Abbildungen
$\mathcal{G}$rp	Alle Gruppen	Alle Homomorphismen von Gruppen	– " –
$\mathcal{A}$b	Alle abelschen Gruppen	Alle Homomorphismen von abelschen Gruppen	– " –
$\mathcal{R}$ng	Alle (assoziative) Ringe (mit 1)	Alle Homomorphismen von Ringen	– " –
K-Vek	Alle K-Vektorräume	Alle K-Homomorphismen	– " –
R-Mod	Alle R-Linksmoduln	Alle R-Homomorphismen	– " –
Mod-R	Alle R-Rechtsmoduln	– " –	– " –
R-Mod-S	Alle (R, S)-Bimoduln	Alle (R, S)-Homomorphismen	– " –
...			
$\mathcal{T}$op	Alle topologischen Räume	Alle stetigen Abbildungen	– " –
$\mathcal{T}\mathrm{op}_*$	Alle topologischen Räume mit Basispunkt	Alle $*$-stetigen Abbildungen	– " –

Dies bedeutet aber nicht, dass die Morphismen Abbildungen sein müssen!! Die Kompositionen müssen auch keine Kompositionen von Abbildungen sein!

(2) Exotischere Beispiele Die folgenden Beispiele zeigen, dass ein

(a) Sei $(G, \cdot)$ eine Gruppe. Definiere die Kategorie $\underline{\mathcal{G}}$ mit:

- $\mathcal{O}\mathrm{b}(\mathcal{G}) =: \{\star\}$
- $\mathrm{Hom}_{\mathcal{G}}(\star, \star) =: G$
- Komposition
$$\cdot : \mathrm{Hom}_{\mathcal{G}}(\star, \star) \times \mathrm{Hom}_{\mathcal{G}}(\star, \star) \longrightarrow \mathrm{Hom}_{\mathcal{G}}(\star, \star)$$
$$(x, y) \longmapsto x \circ y\,.$$

(b) Die Kategorie $\underline{2}$ mit:

- $\mathcal{O}\mathrm{b}(\underline{2}) \coloneqq \{0, 1\}$
- $\mathrm{Hom}_{\underline{2}}(0,0) = \{\mathrm{id}_0\}$
$\mathrm{Hom}_{\underline{2}}(0,1) = \{\delta\}$
$\mathrm{Hom}_{\underline{2}}(1,0) = \varnothing$
$\mathrm{Hom}_{\underline{2}}(1,1) = \{\mathrm{id}_1\}$
- Kompositionen:
$$\delta \circ \mathrm{id}_0 = \delta$$
$$\mathrm{id}_1 \circ \delta = \delta$$
$$0 \xrightarrow{\ \delta\ } 1$$
id_0 id_1

(Und die trivialen Kompositionen $\mathrm{id}_0 \circ \mathrm{id}_0 = \mathrm{id}_0$ und $\mathrm{id}_1 \circ \mathrm{id}_1 = \mathrm{id}_1$, aber diese folgen aus Axiom (K3).)

(c) Sei R ein kommutativer Ring. Definiere eine Kategorie $\mathcal{C} \coloneqq \underline{\mathrm{Mat}_R}$ durch:

- $\mathcal{O}\mathrm{b}(\mathcal{C}) \coloneqq \mathbb{N}$
- $\mathrm{Hom}_{\mathcal{C}}(a, b) = \mathrm{M}_{a \times b}(R) \quad \forall\, a, b \in \mathbb{N}$
- Komposition: Matrizenmultiplikation

Konstruktionen 22.3 (*Duale Kategorie, Produktkategorie*)

(a) Die duale Kategorie: Zu jeder Kategorie $\mathcal{C}$ gibt es eine **duale Kategorie** $\mathcal{C}^{op}$:

- $\mathcal{O}\mathrm{b}(\mathcal{C}^{op}) \coloneqq \mathcal{O}\mathrm{b}(\mathcal{C})$;
- $\mathrm{Hom}_{\mathcal{C}^{op}}(A, B) \coloneqq \mathrm{Hom}_{\mathcal{C}}(B, A) \qquad \forall\, A, B \in \mathcal{O}\mathrm{b}(\mathcal{C}^{op})$; und
- $f \circ_{\mathcal{C}^{op}} g \coloneqq g \circ f$ in $\mathcal{C}$.

(b) Produkte von Kategorien: Für Kategorien $\mathcal{C}$ und $\mathcal{D}$ definiert man die **Produktkategorie** $\mathcal{C} \times \mathcal{D}$ durch:

- $\mathcal{O}\mathrm{b}(\mathcal{C} \times \mathcal{D}) \coloneqq \mathcal{O}\mathrm{b}(\mathcal{C}) \times \mathcal{O}\mathrm{b}(\mathcal{D})$;
- $\mathrm{Hom}_{\mathcal{C}\times\mathcal{D}}(A, B), (C, D)) \coloneqq \mathrm{Hom}_{\mathcal{C}}(A, C) \times \mathrm{Hom}_{\mathcal{C}}(B, D)$;
- $(g, g') \circ (f, f') \coloneqq (g \circ f, g' \circ f')$.

Außerdem gilt $\mathrm{id}_{(A,B)} = (\mathrm{id}_A, \mathrm{id}_B)$.

Wir untersuchen nun Eigenschaften der Morphismen, die die Surjektivität und Injektivität der Abbildungen verallgemeinern.

Definition 22.4 (*Monomorphismus/Epimorphismus/Isomorphismus*)

Ein Morphismus $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ einer Kategorie $\mathcal{C}$ heißt:

(1) **Monomorphismus**, falls $\forall\, C \in \mathcal{O}\mathrm{b}(\mathcal{C}), \forall\, g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(C, A)$ gilt:

$$f \circ g_1 = f \circ g_2 \Longrightarrow g_1 = g_2\,;$$

(2) **Epimorphismus**, falls $\forall\, C \in \mathcal{O}\mathrm{b}(\mathcal{C}), \forall\, g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ gilt:

$$g_1 \circ f = g_2 \circ f \Longrightarrow g_1 = g_2\,;$$

(3) **Isomorphismus**, falls ein Morphismus $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ mit $f \circ g = \mathrm{id}_B$ und $g \circ f = \mathrm{id}_A$ existiert. Gegebenenfalls schreibt man $A \cong_{\mathcal{C}} B$ und $g =: f^{-1}$ ..

Anmerkung 22.5

Wenn dies Sinn ergibt, d.h. die Morphismen sind Abbildungen zwischen Mengen, gelten:

- injektive Morphismen sind Monomorphismen; und
- surjektive Morphismen sind Epimorphismen.

Dies gilt z.B. in $\underline{\mathcal{S}\mathrm{et}}$, $\underline{\mathcal{G}\mathrm{rp}}$, $R\text{–}\underline{\mathrm{Mod}}$, $\underline{\mathcal{R}\mathrm{ng}}$, ...

Aber (!) i.A. ersetzen die Begriffe "Monomorphismusünd Ëpimorphismus"nicht die Injektivität und Surjektivität. Es ist subtiler!

Aufgabe 22.6 (*Aufgabe 2(b)+(d)*)

Zeigen Sie:

(a) Die kanonische Inklusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ ist ein Epimorphismus in $\underline{\mathcal{R}\mathrm{ng}}$, der nicht surjektiv ist. (!)

(b) Dagegen sind alle Monomorphismen in $\underline{\mathcal{R}\mathrm{ng}}$ injektiv.

Aufgabe 22.7 (*Aufgabe 1(b) + Aufgabe 2(a), Blatt 9*)

(a) Zeigen Sie, dass jeder Isomorphismus einer Kategorie $\mathcal{C}$ ein Monomorphismus und auch ein Epimorphismus ist.

(b) Für $\mathcal{C} \in \{\underline{\mathcal{G}}, \underline{2}\}$ (aus Beispiel 32) geben Sie an:

(i) die Objekte, die Morphismen und die Kompositionen in $\mathcal{C}^{\mathrm{op}}$;

(ii) alle Monomorphismen, alle Epimorphismen und alle Isomorphismen.

(c) Geben Sie ein Beispiel an, von einem Morphismus, der ein Epimorphismus und ein Monomorphismus ist, aber kein Isomorphismus.

Lemma 22.8

In der Kategorie R-Mod der R-Linksmoduln gelten:

(a) Jeder Epimorphismus ist surjektiv; und

(b) jeder Monomorphismus ist injektiv.

Beweis:

(a) Sei $f : A \longrightarrow B$ ein Monomorphismus in R-Mod. Betrachte die Morphismen:

$$\begin{array}{ccccc} \mathrm{Ker}(f) & & & & \\ & \searrow^{\iota} & & & \\ \mathrm{Ker}(f) & \xrightarrow{0} & A & \xrightarrow{f} & B \end{array} \qquad \text{(mit } \iota \coloneqq \text{kanonische Inklusion)}$$

Offensichtlich gilt $f \circ \iota = f \circ 0$. Daraus folgt, dass $\iota = 0$, denn f ist ein Monomorphismus. Somit gilt $\ker(f) = 0$, d.h. f ist injektiv.

(b) Sei $f : A \longrightarrow B$ ein Epimorphismus in R-Mod. Betrachte die Morphismen

$$\begin{array}{ccccc} & & & & B/f(A) \\ & & & \nearrow^{\pi} & \\ A & \xrightarrow{f} & B & \xrightarrow[0]{} & B/f(A) \end{array} \qquad \text{(mit } \pi = \text{Faktorabbildung).}$$

Offensichtlich gilt $\pi \circ f = 0 \circ f$. Daher ist $\pi = 0$, denn f ist ein Epimorphismus. Somit ist $B/f(A) = 0$, d.h. $B = f(A)$ und f ist surjektiv. ∎

Aufgabe 22.9

(a) Gilt der Beweis von Lemma 22.8(a) auch in der Kategorie $\mathcal{G}$rp der Gruppen? Begründen Sie Ihre Antwort.

(b) Erklären Sie, warum der Beweis von Lemma 22.8(b) für die Kategorie $\mathcal{R}$ng nicht funktioniert.

Aufgabe 22.10

Zeigen Sie, dass in der Kategorie $\mathcal{S}$et gelten:

(a) Jeder Epimorphismus ist surjektiv.

(b) Jeder Monomorphismus ist injektiv.

23 Funktoren

Um Kategorien zu vergleichen, verwenden wir eine Art von Abbildungen zwischen diesen Kategorien, die *Funktoren* heißen. Diese kommen in zwei Variationen vor.

Definition 23.1 (*kovarianter Funktor*)

Seien $\mathcal{C}$ und $\mathcal{D}$ zwei Kategorien. Ein **kovarianter Funktor** von $\mathcal{C}$ nach $\mathcal{D}$ besteht aus:

(1) einer Abbildung $\Phi : \mathcal{O}\mathrm{b}(\mathcal{C}) \longrightarrow \mathcal{O}\mathrm{b}(\mathcal{D})$; und

(2) für alle $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$ einer Abbildung

$$\Phi_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$$

mit den folgenden Eigenschaften:

(F1) $\Phi_{A,A}(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)}$;

(F2) $\Phi_{A,C}(g \circ f) = \Phi_{B,C}(g) \circ \Phi_{A,B}(f)$.

Definition 23.2 (*kontravarianter Funktor*)

Seien $\mathcal{C}$ und $\mathcal{D}$ zwei Kategorien. Ein **kontravarianter Funktor** von $\mathcal{C}$ nach $\mathcal{D}$ besteht aus:

(1) einer Abbildung $\Phi : \mathcal{O}\mathrm{b}(\mathcal{C}) \longrightarrow \mathcal{O}\mathrm{b}(\mathcal{D})$;
und

(2) für alle $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$ einer Abbildung

$$\Phi_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$$

mit den folgenden Eigenschaften:

(F1) $\Phi_{A,A}(\mathrm{id}_A) = \mathrm{id}_{\Phi(A)}$;

(F2) $\Phi_{A,C}(g \circ f) = \Phi_{B,C}(f) \circ \Phi_{A,B}(g)$.

Anmerkung 23.3

(1) Mathematiker sind sehr informell mit den Funktoren: Oft schreibt man Funktoren einfach als

$$\Phi : \mathcal{C} \longrightarrow \mathcal{D}\,.$$

Es wird auch einfach von "Funktoren"gesprochen, ohne dass es gesagt wird, ob diese kovariant oder kontravariant sind. Noch schlimmer: Funktoren werden oft einfach auf den Objekten definiert und der Leser soll raten, wie sie auf den Morphismen definiert sind.

(2) Man nennt Φ:

- **voll**, wenn $\Phi_{A,B}$ surjektiv $\forall\, A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$ ist;
- **treu**, wenn $\Phi_{A,B}$ injektiv $\forall\, A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$ ist.

Beispiel 33

Die folgenden Abbildungen definieren Funktoren:

(1) $\pi_1 : \underline{\mathcal{T}\mathrm{op}}_* \longrightarrow \underline{\mathcal{G}\mathrm{rp}}$ mit $(X,*) \in \mathcal{O}\mathrm{b}(\underline{\mathcal{T}\mathrm{op}}_*) \mapsto \pi_1(X,*)$ (die Fundamentalgruppe).

(2) $(-)^{**} : K\text{-}\underline{\mathrm{Vek}} \longrightarrow K\text{-}\underline{\mathrm{Vek}}$ mit $V \in \mathcal{O}\mathrm{b}(\underline{\mathcal{S}\mathrm{et}}) \mapsto V^{**}$ (der Bidualraum)

(3) $\mathrm{Fr} : \underline{\mathcal{S}\mathrm{et}} \longrightarrow R\text{-}\underline{\mathrm{Mod}}$ mit

$$X \in \mathcal{O}\mathrm{b}(\mathcal{S}\mathrm{et}) \mapsto \mathrm{Fr}(X) \coloneqq \text{freier } R\text{-Modul mit } R\text{-Basis } X$$

$$\big(X \longrightarrow X\big) \mapsto \big(\mathrm{Fr}(X) \longrightarrow \mathrm{Fr}(Y)\big)$$

eindeutig bestimmtes R-Homomorphismus, der mit der unviversellen Eigenschaft der freien Moduln konstruiert wird.

(4) Für $\mathcal{C} = \underline{\mathcal{G}\mathrm{rp}}$, $K\text{-}\underline{\mathrm{Vek}}$, $\underline{\mathcal{R}\mathrm{ng}}$, $R\text{-}\underline{\mathrm{Mod}}$,... gibt es einen „**Vergißfunktor**" $\mathcal{C} \longrightarrow \underline{\mathcal{S}\mathrm{et}}$, der ein $X \in \mathcal{O}\mathrm{b}(\mathcal{C})$ die zugrundeliegende Menge zuordnet (und Morphismen die zugrunde liegende Abbildung (von Mengen)).
Analog ist z.B.

$$R\text{-}\underline{\mathrm{Mod}} \longrightarrow \mathbb{Z}\text{-}\underline{\mathrm{Mod}}$$
$$(A,+,*) \mapsto (A,+)$$

ein Vergißfunktor.

(5) Sei X ein (R,S)-Bimodul. Dann ist $X \otimes_S - : S\text{-}\underline{\mathrm{Mod}} \longrightarrow R\text{-}\underline{\mathrm{Mod}}$ mit

$$A \in \mathcal{O}\mathrm{b}(S\text{-Mod}) \mapsto X \otimes_S A$$

und

$$\big(A \xrightarrow{f} B\big) \mapsto \big(X \otimes_S f \coloneqq \mathrm{id}_X \otimes f : X \otimes_S A \longrightarrow X \otimes_S B\big)$$

ein kovarianter Funktor.

(6) Sei X ein R-Linksmodul. Dann:

(i) $\mathrm{Hom}_R(X,-) : R\text{-}\underline{\mathrm{Mod}} \longrightarrow \mathbb{Z}\text{-}\underline{\mathrm{Mod}}$ mit

$$A \in \mathcal{O}\mathrm{b}(R\text{-}\underline{\mathrm{Mod}}) \mapsto \mathrm{Hom}_R(X,A)$$

und

$$\big(A \xrightarrow{f} B\big) \mapsto \big(\mathrm{Hom}_R(X,f) : \mathrm{Hom}_R(X,A) \longrightarrow \mathrm{Hom}_R(X,B), g \mapsto f_*(g) = f \circ g\big)$$

ist ein kovarianter Funktor; und

(ii) $\mathrm{Hom}_R(-,X) : R\text{-}\underline{\mathrm{Mod}} \longrightarrow \mathbb{Z}\text{-}\underline{\mathrm{Mod}}$ mit

$$A \in \mathcal{O}\mathrm{b}(R\text{-}\underline{\mathrm{Mod}}) \mapsto \mathrm{Hom}_R(A,X)$$

und

$$\big(A \xrightarrow{f} B\big) \mapsto \big(\mathrm{Hom}_R(f,X) : \mathrm{Hom}_R(B,X) \longrightarrow \mathrm{Hom}_R(A,X), g \mapsto f^*(g) = g \circ f\big)$$

ist ein kontravarienter Funktor.

Anmerkung 23.4

(1) Die Abbildung $\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathcal{C}$ mit $\mathrm{Id}_{\mathcal{C}}(A) := A$ und $\mathrm{Id}_{\mathcal{C}}(f) := f$ für jedes Objekt $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ und für jeden Morphismus $f \in \mathrm{Mor}(\mathcal{C})$ ist der **Identitätsfunktor** auf $\mathcal{C}$.

(2) Sind $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ und $\Psi : \mathcal{D} \longrightarrow \mathcal{E}$ zwei Funktoren (beide kovariant oder beide kontravariant), so definiert man in offensichtlicher Weise einen Funktor

$$\Psi \circ \Phi : \mathcal{C} \xrightarrow{\Phi} \mathcal{D} \xrightarrow{\Psi} \mathcal{E}$$

von $\mathcal{C}$ nach $\mathcal{E}$. Diese Komposition ist assoziativ und $\Phi \circ \mathrm{Id}_{\mathcal{C}} = \Phi$, $\mathrm{Id}_{\mathcal{D}} \circ \Psi = \Psi$.

(3) Somit kann man die Kategorie aller **kleinen** Kategorien konstruieren, wobei die Morphismen die Funktoren sind.

(4) (!) Es existiert keine Kategorie aller Kategorien! Dies würde zu einem Paradoxon führen! Aber: Die Ansammlung aller Kategorien ist eine sogenannte 2-**Kategorie**.

Aufgabe 23.5

(1) Sei $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ ein kovarianter Funktor. Zeigen Sie: Sind $A, B \in \mathrm{Ob}(\mathcal{C})$ Objekte mit $A \cong_{\mathcal{C}} B$, so gilt $\Phi(A) \cong_{\mathcal{D}} \Phi(B)$.

(2) Ein Funktor $\Phi : R\text{-Mod} \longrightarrow S\text{-Mod}$ heißt **additiv**, falls $\Phi(f + g) = \Phi(f) + \Phi(g)$ für alle $M, N \in R\text{-Mod}$, und alle $f, g \in \mathrm{Hom}_R(M, N)$ gilt. Zeigen Sie:

(i) Additive Funktoren bilden die Nullabbildung auf der Nullabbildung ab.

(ii) Ist $\Phi : R\text{-Mod} \longrightarrow S\text{-Mod}$ ein additiver Funktor, so gilt $\Phi(0) = 0$. (Hier bezeichnet 0 den Nullmodul in R-Mod bzw. in S-Mod.)

(iii) Ist X ein R-Linksmodul, so ist $\mathrm{Hom}_R(X, -)$ ein additiver Funktor.

Definition 23.6 (*exakter/linksexakter/rechtsexakter Funktor*)

Seien $\mathcal{C}$ und $\mathcal{D}$ zwei Kategorien von Moduln und sei $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ eine k.e.S. in $\mathcal{C}$.

(a) Ein kovarianter Funktor $F : \mathcal{C} \longrightarrow \mathcal{D}$ heißt:

(1) **exakt**, falls $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ eine k.e.S. ist;

(2) **linksexakt**, falls $0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ exakt ist;

(3) **rechtsexakt**, falls $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$ exakt ist.

(b) Ein kontravarianter Funktor $F : \mathcal{C} \longrightarrow \mathcal{D}$ heißt:

(1) **exakt**, falls $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A) \longrightarrow 0$ eine k.e.S. ist;

(2) **linksexakt**, falls $0 \longrightarrow F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A) \longrightarrow 0$ exakt ist;

(3) **rechtsexakt**, falls $F(C) \xrightarrow{F(g)} F(B) \xrightarrow{F(f)} F(A) \longrightarrow 0$ exakt ist.

Beispiel 34

Aus Kapitel 1 (siehe Bemerkung 6.9) wissen wir, dass die folgenden Funktoren linksexakt bzw. exakt sind.

(1) Der kovariante Funktor $\mathrm{Hom}_R(Q,-) : R\text{-Mod} \longrightarrow \mathbb{Z}\text{-Mod}$ ist linksexakt für jeden Modul $Q \in \mathcal{O}\mathrm{b}(R\text{-Mod})$, und er ist exakt, falls Q projektiv ist.

(2) Der kontravariante Funktor $\mathrm{Hom}_R(-,Q) : R\text{-Mod} \longrightarrow \mathbb{Z}\text{-Mod}$ ist linksexakt für jeden Modul $Q \in \mathcal{O}\mathrm{b}(R\text{-Mod})$, und er ist **exakt**, falls Q injektiv ist.

Lemma 23.7

Ist X ein R-Rechtsmodul, so ist der kovariante Funktor $X \otimes_R - : R\text{-Mod} \longrightarrow \mathbb{Z}\text{-Mod}$ rechtsexakt.

Beweis: Sei $0 \longrightarrow A \xrightarrow{f} A' \xrightarrow{g} A'' \longrightarrow 0$ eine k.e.S. in R-Mod. Wir müssen zeigen, dass dei Sequenz $X \otimes_R A \xrightarrow{X\otimes_R f} X \otimes A' \xrightarrow{X\otimes_R g} X \otimes_R A'' \longrightarrow 0$ exakte ist.

(1) Exaktheit an der Stelle $X \otimes_R A'$: Aufgabe 1(a), Blatt 10.

(2) Exaktheit an der Stelle $X \otimes_R A''$:
Sei $x \otimes a \in X \otimes A''$ ein Elementartensor. Nach der Surjektivität von g existiert $b \in A'$ mit $g(b) = a$. Somit gilt
$$x \otimes a = \mathrm{id}_X(x) \otimes g(b) = (\mathrm{id}_x \otimes g)(x \otimes b) = (X \otimes_R g)(x \otimes b)$$
und es folgt, dass der Morphismus $X \otimes_R g$ surjektiv ist, weil $X \otimes_R A'' = \langle x \otimes a \mid x \in X, a \in A'' \rangle_{\mathbb{Z}}$. ■

Anmerkung 23.8

Analog: Ist X ein R-Linksmodul, so ist der kovariante Funktor $- \otimes_R X : \mathrm{Mod}\text{-}R \longrightarrow \mathbb{Z}\text{-Mod}$ rechtsexakt.

Definition 23.9 (*flacher Modul*)

(a) Ein R-Rechtsmodul X heißt **flach**, wenn der Funktor $X \otimes_R -$ exakt ist.

(b) Ein R-Linksmodul X heißt **flach**, wenn der Funktor $- \otimes_R X$ exakt ist.

Beispiel 35

Freie und projektive R-Moduln sind flach. (Uebung!)

Aufgabe 23.10

1. Sei $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ ein kovarianter Funktor. Zeigen Sie: Sind $A, B \in \mathrm{Ob}(\mathcal{C})$ Objekte mit $A \cong_{\mathcal{C}} B$, so gilt $\Phi(A) \cong_{\mathcal{D}} \Phi(B)$.
2. Ein (kovarianter) Funktor $\Phi : R\text{-}\underline{\mathrm{Mod}} \longrightarrow S\text{-}\underline{\mathrm{Mod}}$ heißt **additiv**, falls $\Phi(f+g) = \Phi(f) + \Phi(g)$ für alle $M, N \in R\text{-}\underline{\mathrm{Mod}}$, und alle $f, g \in \mathrm{Hom}_R(M,N)$ gilt. Zeigen Sie:
   (i) Additive Funktoren bilden die Nullabbildung auf der Nullabbildung ab.
   (ii) Ist $\Phi : R\text{-}\underline{\mathrm{Mod}} \longrightarrow S\text{-}\underline{\mathrm{Mod}}$ ein additiver Funktor, so gilt $\Phi(0) = 0$. (Hier bezeichnet 0 den Nullmodul in $R\text{-}\underline{\mathrm{Mod}}$ bzw. in $S\text{-}\underline{\mathrm{Mod}}$)
   (iii) Ist X ein R-Linksmodul, so ist $\mathrm{Hom}_R(X,-)$ ein additiver Funktor.

24 Äquivalenzen von Kategorien

Definition 24.1 (*natürliche Transformation*)

Seien $\Phi, \Psi : \mathcal{C} \longrightarrow \mathcal{D}$ kovariante Funktoren. Eine **natürliche Transformation** von Φ nach Ψ, geschrieben $\Phi \overset{\tau}{\Rightarrow} \Psi$ ist eine Abbildung $\tau : \mathcal{O}\mathrm{b}(\mathcal{C}) \longrightarrow \mathrm{Mor}(\mathcal{D})$, so dass

$$\tau_X := \tau(x) \in \mathrm{Hom}_{\mathcal{D}}(\Phi(X), \Psi(X)) \quad \forall\, X \in \mathcal{O}\mathrm{b}(\mathcal{C})$$

und für jeden Morphismus $X \xrightarrow{f} Y \in \mathrm{Mor}(\mathcal{C})$ ist das Diagramm

$$\begin{array}{ccc} \Phi(X) & \xrightarrow{\Phi(f)} & \Phi(Y) \\ {\scriptstyle \tau_X}\downarrow & \circlearrowleft & \downarrow{\scriptstyle \tau_Y} \\ \Psi(X) & \xrightarrow[\Psi(f)]{} & \Psi(Y) \end{array}$$

kommutativ, d.h. $\tau_y \circ \Phi(f) = \Psi(f) \circ \tau_x$.

Beispiel 36

(0) Nehme $\mathcal{D} = \mathcal{C}$ und $\Psi = \Phi$. Dann ist $\mathrm{id}_\Phi : \Phi \Rightarrow \Phi$ mit

$$(\mathrm{id}_\Phi)_A := \mathrm{id}_{\Phi(A)} \quad \forall\, A \in \mathcal{O}\mathrm{b}(\mathcal{C})$$

eine natürliche Transformation.
Die Diagramme aus der Definition sind offensichtlich kommutativ, weil alle Moprphismen Identitäten sind.

(1) Sei K ein Körper und sei $\mathcal{C} = \mathcal{D} := K\text{-Vek}_{<\infty}$ die Kategorie der endlich-dimensionalen K-Vektorräume. Betrachte die Funktoren $\Phi := \mathrm{Id}_{\mathcal{C}}$ und $\Psi : K\text{-Vek}_{<\infty} \longrightarrow K\text{-Vek}_{<\infty}$ mit

$$\Psi(V) := V^{**} \quad \forall\, V \in \mathcal{O}\mathrm{b}(K\text{-Vek}_{<\infty})$$

($V^{**} = (= \mathrm{Hom}_K(\mathrm{Hom}_K(V, K), K))$) und

$$\Psi(V \xrightarrow{f} W) = f^{**}\,(= (f^*)^*) \quad \forall\, V \xrightarrow{f} W \in \ \mathrm{Mor}\ (K\text{-Vek}_{<\infty})$$

wobei $f^* := \mathrm{Hom}_k(V, f)$ ist. Für $V \in \mathcal{O}\mathrm{b}(K\text{-Vek}_{<\infty})$ definiere $\tau_v \in \mathrm{Hom}_K(V, V^{**})$ durch

$$(\tau_V(v))(\lambda) := \lambda(v) \qquad \forall\, v \in V, \forall\, \lambda \in V^*\,.$$

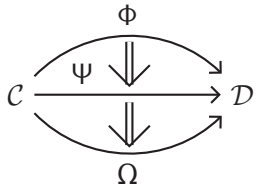
Es folgt aus der Linearen Algebra, dass $\tau = (\tau_V)_{V \in \mathcal{O}\mathrm{b}(K\text{-Vek}_{<\infty})}$ eine natürliche Transformation $\mathrm{Id}_{K\text{-Vek}<\infty} \Rightarrow \Psi$ ist.

Aufgabe 24.2 (*Aufgabe 2(a), Blatt 10*)

Definieren Sie den Begriff der **natürlichen Transformation** zwischen zwei kontravarianten Funktoren.

Anmerkung 24.3

(1) Sind $\Phi, \Psi, \Omega : \mathcal{C} \longrightarrow \mathcal{D}$ kovariante (bzw. Kontravariante) Funktoren und $\Phi \overset{\tau}{\Rightarrow} \Psi, \Psi \overset{\gamma}{\Rightarrow} \Omega$ natürliche Transformationen, dann ist auch $\gamma \circ \tau : \Phi \Rightarrow \Omega$ mit $(\gamma \circ \tau_A) := \gamma_A \circ \tau_A$ eine natürliche Transformation.



(2) Seien $\Phi, \Psi, \Gamma, \Delta$ Funktoren und $\Phi \overset{\tau}{\Rightarrow} \Psi$ eine natürliche Transformation, wie folgt:

$$\mathcal{B} \xrightarrow{\Gamma} \mathcal{C} \underset{\Psi}{\overset{\Phi}{\underset{\tau \Downarrow}{\longrightarrow}}} \mathcal{D} \xrightarrow{\Delta} \mathcal{E}$$

Dann sind auch

$$\tau \circ \Gamma := (\tau_{\Gamma(B)})_{\mathcal{O}b(\mathcal{B})} : \Phi \circ \Gamma \Rightarrow \Psi \circ \Gamma$$

und

$$\Delta \circ \tau := (\Delta(\tau_C))_{C \in \mathcal{O}b(\mathcal{C})} : \Delta \circ \Phi \Rightarrow \Delta \circ \Psi$$

natürliche Transformationen.
Übung: Aufgabe 1(c), Blatt 10.

(3) Auf dieser Weise wird die Klasse aller Funktoren zwischen zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ zu einer Kategorie $\mathcal{C}^{\mathcal{D}}$:

- **Morphismen:** Die natürlichen Transformationen;
- **Komposition:** Komposition der natürlichen Transformationen, wie in (2).

Man nennt $\mathcal{D}^{\mathcal{C}}$ die **Funktorenkategorie** zwischen $\mathcal{C}$ und $\mathcal{D}$.

Definition 24.4 (*natürlicher Isomorphismus*)

Seien $\Phi, \Psi : \mathcal{C} \longrightarrow \mathcal{D}$ zwei kovariante (bzw. kontravariante) Funktoren. Eine natürliche Transformation $\Phi \overset{\tau}{\Rightarrow} \Psi$ nennt man **natürlichen Isomorphismus**, falls τ_A ein Isomorphismus in $\mathcal{D}$ für jedes Objekt $A \in \mathcal{O}b(\mathcal{C})$ ist. Ggf. schreibt man $\Phi \cong \Psi$.

Anmerkung 24.5

Man zeigt leicht, dass $\cong$ eine Äquivalenzrelation ist.

Definition 24.6

Zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$ heißen:

(a) **isomorph**, falls Funktoren $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ und $\Psi : \mathcal{D} \to \mathcal{C}$ mit $\Phi \circ \Psi = \mathrm{Id}_{\mathcal{D}}$ und $\Psi \circ \Phi = \mathrm{Id}_{\mathcal{C}}$;

(b) **äquivalent**, falls Funktoren $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ und $\Psi : \mathcal{D} \to \mathcal{C}$ mit $\Phi \circ \Psi \cong \mathrm{Id}_{\mathcal{D}}$ und $\Psi \circ \Phi \cong \mathrm{Id}_{\mathcal{C}}$.

Anmerkung 24.7

Jeder Isomorphismus von Kategorien ist eine Äquivalenz von Kategorien, aber die Umkehrung ist i.A. falsch.

Beispiel 37

(1) Die natürlichen Transformationen $\mathrm{id}_\Phi : \Phi \Rightarrow \Phi$ und $\mathrm{Id}_{K\text{-Vek}_{<\infty}} \Rightarrow \Psi$ aus dem vorherigen Beispiel sind natürliche Isomorphismen.
Im ersten Fall ist es klar, dass $(\mathrm{Id}_\Phi)_A = \mathrm{id}_{\Phi(A)}$ ein Isomorphismus für jedes Objekt A ist.
Im zweiten Fall ist $\tau_V : V \longrightarrow V^{**}$ ein K-Isomorphismus $\forall\, V \in \mathcal{O}\mathrm{b}(K\text{-Vek}_{<\infty})$, weil die Dimension endlich ist. (Sieh die LA.)

(2) (Aufgabe 1(b), Blatt 10.)
Ist R ein Ring (assoziativ mit 1), so existiert ein natürlicher Isomorphismus $-\otimes_R R \Rightarrow \mathrm{Id}_{R-\mathrm{Mod}}$.

Satz 24.8

Sei $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ ein Funktor. Genau dann ist Φ eine Äquivalenz, wenn die folgenden zwei Bedingungen erfüllt sind:

(1) Φ ist voll und treu; und

(2) für jedes Objekt $D \in \mathcal{O}\mathrm{b}(\mathcal{D})$ existiert ein Objekt $C \in \mathcal{O}\mathrm{b}(\mathcal{C})$ mit $\Phi(C) = D$.

Beweis:

„$\Rightarrow$“: Wir nehmen an, dass Φ eine Äquivalenz ist. Seien noch $\Psi : \mathcal{DC}$ ein Funktor sowie

$$\alpha : \Psi\Phi \Rightarrow \mathrm{Id}_{\mathcal{C}} \quad \text{und} \quad \beta : \Phi\Psi \Rightarrow \mathrm{Id}_{\mathcal{D}} \quad (*)$$

natürliche Isomorphismen.

- Zunächst zeigen wir, dass Φ treu ist. Seien also $f, g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ zwei Morphismen in $\mathcal{C}$ mit

  $$(**) \qquad \Phi(f) = \Phi(g)\,.$$

  Dann gilt

  $$f \overset{(*)}{=} \alpha_B \circ \Psi(\Phi(f)) \circ \alpha_A^{-1} \overset{(**)}{=} \alpha_B \circ \Psi(\Phi(g)) \circ \alpha_A^{-1} \overset{(*)}{=} g\,,$$

  wie verlangt.

  $$\begin{array}{ccc} \Psi\Phi(A) & \xrightarrow{\Psi\Phi(f)} & \Psi\Phi(B) \\ {\scriptstyle\alpha_A}\downarrow{\scriptstyle\cong} & \circlearrowleft & {\scriptstyle\cong}\downarrow{\scriptstyle\alpha_B} \\ A & \xrightarrow[f]{} & B \end{array}$$

- Analog erhält man, dass Ψ treu ist.
- Wir zeigen nun, dass Φ voll ist. Sei also $g \in \mathrm{Hom}_{\mathcal{D}}(\Phi(A), \Phi(B))$. Dann gilt

  $$\Psi(g) \in \mathrm{Hom}_{\mathcal{C}}(\Psi\Phi(A), \Psi\Phi(B)).$$

  Setze also $f := \alpha_B \circ \Psi(g) \circ \alpha_A^{-1} \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

$$\begin{array}{ccc} \Psi\Phi(A) & \xrightarrow{\Psi(g)} & \Psi\Phi(B) \\ {\scriptstyle \alpha_A^{-1}}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \alpha_B} \\ A & \xrightarrow[f]{} & B \end{array}$$

Nach $(*)$ gilt

$$\Psi(g) = \alpha_B^{-1} \circ f \circ \alpha_A = \Psi(\Phi(f))\,.$$

Daher ist $g = \Phi(f)$, weil Ψ treu ist. D.h. Φ ist voll. Somit gilt Bedingung (1).

- Schließlich zeigen wir, dass Bedingung (2) gilt. Sei $D \in \mathcal{O}\mathrm{b}(\mathcal{D})$. und setze $C := \Psi(D) \in \mathcal{O}\mathrm{b}(\mathcal{C})$. Dann ist $\beta_D : \Phi\Psi(D) \longrightarrow D$ ein Isomorphismus nach Voraussetzung $(*)$. Dann gilt

$$\Phi(C) = \Phi(\Psi(D)) = \underbrace{\Phi\Psi(D)}_{=\Phi(C)} \cong D\,,$$

also $\Phi(C) \cong D$. D.h. Bedingung (2) ist erfüllt.

„$\Longleftarrow$“: Wir treffen die folgenden Annahmen:

(a) Der Funktor $\Phi : \mathcal{C} \longrightarrow \mathcal{D}$ ist voll und treu.

(b) Für alle Objekte $D \in \mathcal{O}\mathrm{b}(\mathcal{D})$ existiere ein $C_D \in \mathcal{O}\mathrm{b}(\mathcal{C})$ mit $\Phi(C_D) \cong_{\mathcal{D}} D$.

Wir möchten nun zeigen, dass Φ eine Äquivalenz ist. Hierfür wird ein weiterer Funktor von $\mathcal{D}$ nach $\mathcal{C}$ benötigt.

Schritt 1. Wir konstruieren diesen Funktor $\Psi : \mathcal{D} \longrightarrow \mathcal{C}$ wie folgt.

Objekte: Für beliebige $D \in \mathcal{O}\mathrm{b}(\mathcal{D})$ setze $\Psi(D) := C_D$. Beobachte, dass dann

$$\Phi \circ \Psi(D) = \Phi(C_D) \cong_{\mathcal{D}} D$$

nach Annahme (b) gilt. Wir können also einen Isomorphismus $\beta_D : \Phi\Psi(D) \longrightarrow D$ wählen.

Morphismen: Sei $g \in \mathrm{Hom}_{\mathcal{D}}(D, E)$ in $\mathrm{Mor}(\mathcal{D})$. Wir müssen ein Morphismus $\Psi(g)$ definieren mit den folgenden Eigenschaften:

$$\begin{array}{ccc} \Phi(C_D) \cong D & \xrightarrow{\quad g \quad} & E \cong \Phi(C_E) \\ & {\scriptstyle \Psi}\vdots & \\ \Psi\Phi(C_D) \cong \Psi(D) & \xrightarrow[\Psi(g)]{} & \Psi(E) \cong \Psi\Phi(C_E) \end{array}$$

Setze also $\Psi(g) := \Phi^{-1}(\beta_E^{-1} \circ g \circ \beta_D)$ (Φ^{-1} existiert, da Φ treu!). Es bleibt zu zeigen, dass Funktoreigenschaften (F1) und (F2) gelten.

(F1) Es gilt $\Psi(\mathrm{id}_D) = \Phi^{-1}(\beta_D^{-1} \circ \mathrm{id}_D \circ \beta_D) = \mathrm{id}_{\Psi(D)}$.

(F2) Für jede Komposition $D \xrightarrow{g} E \xrightarrow{h} F$ von Morphismen in $\mathcal{D}$ gilt

$$\begin{aligned} \Psi(h \circ g) &= \Phi^{-1}(\beta_F^{-1} \circ (h \circ g) \circ \beta_D) \\ &= \Phi^{-1}(\beta_F^{-1} \circ h \circ \beta_E \circ \beta_E^{-1} \circ g \circ \beta_D) \\ &= \Phi^{-1}(\beta_F^{-1} \circ h \circ \beta_E) \circ \Phi^{-1}(\beta_E^{-1} \circ g \circ \beta_D) = \Psi(h) \circ \Psi(g)\,. \end{aligned}$$

Schritt 2. Wir zeigen nun die Existenz eines natürlichen Isomorphismus von Φ nach Ψ.

Nach Konstruktion ist $\beta := (\beta_D)_{D \in \mathcal{O}\mathrm{b}(\mathcal{D})}$ ein natürlicher Isomorphismus $\Phi\Psi \Rightarrow \mathrm{Id}_{\mathcal{D}}$.

Es ist Φ voll und treu, weshalb dies auch für Ψ gilt nach Definition. Es folgt daraus:

$$(\Phi\Psi \overset{\cong}{\Longrightarrow} \mathrm{Id}_{\mathcal{D}}) \Rightarrow (\Psi\Phi \overset{\cong}{\Longrightarrow} \mathrm{Id}_{\mathcal{C}})\,.$$

■

Aufgabe 24.9 (*Aufgabe 2(b), Blatt 10*)

Wir bezeichnen mit $\underline{\mathcal{C}\mathrm{Rng}}$ die Kategorie der kommutativen Ringen und mit $\underline{\mathcal{G}rp}$ die Kategorie der Gruppen. Sei $n \in \mathbb{N}$. Zeigen Sie:

(i) $(-)^\times : \underline{\mathcal{C}\mathrm{Rng}} \longrightarrow \underline{\mathcal{G}\mathrm{rp}}$ mit $R^\times = \{r \in R \mid r \text{ ist invertierbar}\}$ für jedes Objekt R in $\underline{\mathcal{C}\mathrm{Rng}}$ und mit $f^\times := \overline{f|_{R^\times}}$ für jeden Morphismus $f \in \mathrm{Hom}_{\underline{\mathcal{C}\mathrm{Rng}}}(R, S)$ ist ein Funktor;

(ii) $\mathrm{GL}_n(-) : \underline{\mathcal{C}\mathrm{Rng}} \longrightarrow \underline{\mathcal{G}\mathrm{rp}}$ mit $\mathrm{GL}_n(R) := M_n(R)^\times$ für jedes Objekt R in $\underline{\mathcal{C}\mathrm{Rng}}$ und mit $\mathrm{GL}_n(f)(\overline{(a_{ij})_{ij}}) := (f(a_{ij}))_{ij}$ für jeden Morphismus $f \in \mathrm{Hom}_{\underline{\mathcal{C}\mathrm{Rng}}}(R, S)$ und jede Matrix $(a_{ij})_{ij} \in \mathrm{GL}_n(R)$ ist ein Funktor; und

(iii) die Determinante der Matrizen induziert eine natürliche Transformation zwischen den Funktoren $\mathrm{GL}_n(-)$ und $(-)^\times$. Ist es ein natürlicher Isomorphismus?

25 Morita Theorie

Ziel ist nun die Charakterisierung von Modulkategorien. Hierfür werden wir den Satz von Morita beweisen, der Kriterien für ihre Äquivalenz gibt. Der Beweis für diesen benötigt den Begriff des Progenerators, den wir im Folgenden definieren werden.

Es sind im Übrigen alle von hier an betrachteten Ringe assoziativ mit 1.

Definition 25.1 (*Erzeuger/Generator*)

Ein R-Modul M ist ein **Erzeuger** (oder **Generator**) der Kategorie R-$\underline{\mathrm{Mod}}$, wenn für jeden R-Modul N eine Indexmenge J un ein Epimorphismus $\bigoplus_J M \twoheadrightarrow N$ existieren.

Definition 25.2 (*Progenerator*)

Ein Erzeuger M der Kategorie R-$\underline{\mathrm{Mod}}$ heißt R-**Progenerator**, falls M endlich erzeugt und projektiv ist.

Beispiel 38

Der reguläre Modul R^{reg} ist ein Erzeuger von R-$\underline{\mathrm{Mod}}$. Klar: Es existiert ein Epimorphismus $\bigoplus_{n\in\mathbb{N}} R \twoheadrightarrow N$, weil N isomorph zu einem Faktormodul eines freien Moduls nach Lemma ?? ist. Außerdem ist R^{reg} projektiv und endlich erzeugt.

Satz 25.3 (Morita, 1958)

Die folgenden Aussagen sind äquivalent.

(1) Die Kategorien R-$\underline{\mathrm{Mod}}$ und S-$\underline{\mathrm{Mod}}$ sind äquivalent.

(2) Es existiert ein S-Progenerator P mit $R \cong \mathrm{End}(P)^{\mathrm{op}}$ (als Ringe).

(3) Es existiert ein (S, R)-Bimodul M, sodass der Funktor $M \otimes_R - : R\text{-}\underline{\mathrm{Mod}} \longrightarrow S\text{-}\underline{\mathrm{Mod}}$ eine Äquivalenz von Kategorien ist.

Anmerkung 25.4

Sind die äquivalenten Bedingungen aus dem Satz von Morita erfüllt, so nennt man die Ringe R und S Morita-äquivalent sind, und wir schreiben $R \sim_M S$.

Beweis: (3) $\Rightarrow$ (1): klar (bereits vorausgesetzt).

(1) $\Rightarrow$ (2): Seien R-Mod $\underset{G}{\overset{F}{\rightleftharpoons}}$ S-Mod Äquivalenzen von Kategorien mit natürlichen Isomorphismen

$$FG \overset{\varepsilon}{\Rightarrow} \mathrm{Id}_{S\text{-Mod}} \quad \text{und} \quad GF \overset{\eta}{\Rightarrow} \mathrm{Id}_{R\text{-Mod}} .$$

Nach Beispiel 38 ist R^{reg} ein Progenerator. Dies impliziert, dass $F(R^{\mathrm{reg}}) =: P$ ein Progenerator von S-Mod ist. (Alle Eigenschaften der Definition bleiben erhalten, da F eine Äquivalenz ist!)

Behauptung: $\mathrm{Hom}_S(F(R), F(R)) \cong \mathrm{Hom}_R(R, R)$.

Gilt die Behauptung, dann ist

$$\mathrm{End}_S(P) = \mathrm{Hom}_S(P, P) = \mathrm{Hom}_S(F(R), F(R)) \cong \mathrm{Hom}_R(R, R) = \mathrm{End}_R(R) \cong R^{\mathrm{op}}$$

wie gewünscht.
Sei also $f' \in \mathrm{Hom}_S(F(R), F(R))$ und betrachte folgendes kommutatives Diagramm

$$\begin{array}{ccc} GF(R) & \xrightarrow{G(f')} & GF(R) \\ {\scriptstyle \eta_R}\uparrow & & \uparrow{\scriptstyle \eta_R} \\ R & \underset{f := \eta_R^{-1} \circ G(f') \circ \eta_R}{\dashrightarrow} & R \end{array}$$

Somit definieren wir eine Abbildung $\varphi : \mathrm{Hom}_S(F(R), F(R)) \longrightarrow \mathrm{Hom}_R(R, R), f' \mapsto f$.
Klar: φ ist injektiv, denn es gilt: $G(f') = G(f'') \Rightarrow FG(f') = FG(f'')$. Außerdem haben wir folgendes kommutatives Diagramm

$$\begin{array}{ccccc} F(R) & \xleftarrow{\varepsilon_{F(R)}} & FGF(R) & \xrightarrow{\varepsilon_{F(R)}} & F(R) \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle FG(f')} & & \downarrow{\scriptstyle f''} \\ F(R) & \xleftarrow[\varepsilon_{F(R)}]{} & FGF(R) & \xrightarrow[\varepsilon_{F(R)}]{} & F(R) \end{array}$$

denn ε ist eine natürliche Transformation. Deshalb gilt $f' = f''$.
Es ist auch klar, dass φ ein Homomorphismus von Ringen ist: Die Operationen $+$ und $\circ$ bleiben erhalten nach Konstruktion. Schließlich für

$$\psi : \mathrm{Hom}_R(R, R) \longrightarrow \mathrm{Hom}_S(F(R), F(R)), f \mapsto F(f)$$

gilt $\varphi\psi(f) = f$ und somit ist $\varphi\psi\varphi(f') = \varphi(f')$ und $\psi\varphi(f') = f'$, da φ injektiv ist, dass heißt $\varphi\psi = \mathrm{id}$, $\psi\varphi = \mathrm{id}$. Daher ist φ ein Isomorphismus von Ringen.

(2) $\Rightarrow$ (3): Sei nun P ein S-Progenerator und sei $f : R \xrightarrow{\cong} \mathrm{End}_S(P)^{\mathrm{op}}$ ein Isomorphismus von Ringen. Zunächst beobachten wir, dass P auch ein R-Rechtsmodul mit äußerer Multiplikation

$$\cdot : P \times R \longrightarrow R, (x, r) \mapsto x \cdot r := f(r)(x)$$

ist. (Dies folgt aus Kapitel 1, da f ein Ringhomomorphismus ist). Außerdem ist diese äußere Multiplikation kompatibel mit der Multiplikation von S, weil gilt

$$s \cdot (x \cdot r) = s \cdot (f(r)(x)) = f(r)(sx) = (sx) \cdot r, \quad \forall\, s \in S, x \in P, r \in R$$

unter Verwendung der S-Linearität bei der zweiten Gleichheit. Damit ist P ein (S,R)-Bimodul.

Behauptung: Die Funktoren $P\otimes_R - : R\text{-}\underline{\mathrm{Mod}} \longrightarrow S\text{-}\underline{\mathrm{Mod}}$ und $\mathrm{Hom}_S(P,-) : S\text{-}\underline{\mathrm{Mod}} \longrightarrow R\text{-}\underline{\mathrm{Mod}}$ liefern eine Äquivalenz von Kategorien.

(1.) Für $A \in \mathcal{O}\mathrm{b}(R\text{-}\underline{\mathrm{Mod}})$ definiere $\eta_A : A \longrightarrow \mathrm{Hom}_S(P, P\otimes_R A), a \mapsto \eta_A(a)$ mit

$$\eta_A(a) : P \longrightarrow P\otimes_R A, p \mapsto p\otimes a\,.$$

Es ist zu zeigen, dass η_A ein R-Isomorphismus, was bedeutet, dass $\eta = (\eta_A)_{A\in\mathcal{O}\mathrm{b}(R\text{-}\underline{\mathrm{Mod}})}$ ein natürlicher Isomorphismus $\mathrm{Id}_{R\text{-}\underline{\mathrm{Mod}}} \Rightarrow \mathrm{Hom}_S(P, P\otimes_R -))$ ist.
Weil R^{reg} ein R-Progenerator ist, existiert ein R-Epimorphismus $\varepsilon_A : \bigoplus_I R \twoheadrightarrow A.$ und es gibt ein kommutatives Diagramm der Form

$$\begin{array}{ccc}
\bigoplus_I R & \xrightarrow{\quad\varepsilon\quad} & A \\
\downarrow\cong & & \\
\bigoplus_I \mathrm{Hom}_S(P,P) & & \\
\downarrow\cong & & \\
\mathrm{Hom}_S(P, \bigoplus_I P) & & \downarrow \eta_A \\
\downarrow\cong & & \\
\mathrm{Hom}_S(P, \bigoplus_I P\otimes_R R) & & \\
\downarrow & & \\
\mathrm{Hom}_S(P, P\otimes_R (\bigoplus_I R)) & \xrightarrow[\varepsilon_{**}]{} & \mathrm{Hom}_S(P, P\otimes_R A)
\end{array}$$

denn ergibt sich für die Elemente:

$$\begin{array}{ccc}
(r_i)_{i\in I} & \longmapsto & \varepsilon_A((r_i)_{i\in I}) \\
\downarrow & & \\
(f(r_i))_{i\in I} & & \\
\downarrow & & \\
x \mapsto (f(r_i)(x))_{i\in I} & & \\
\downarrow & & \\
x \mapsto (x\otimes r_i)_{i\in I} & & \\
\downarrow & & \\
x \mapsto x\otimes (r_i)_{i\in I} & \longmapsto & x \mapsto x\otimes \varepsilon_A((r_i)_{i\in I})
\end{array}$$

Somit erhalten wir ein weiteres kommutatives Diagramm:

$$\begin{array}{ccccccc}
\bigoplus_J R & \xrightarrow{\beta} & \mathrm{Kern}(\varepsilon_A) & \hookrightarrow & \bigoplus_I R & \xrightarrow{\varepsilon_A} & A \\
\downarrow\cong & & & & \downarrow\cong & & \downarrow \eta_A \\
\mathrm{Hom}_S(P, P\otimes_R (\bigoplus_J R)) & \xrightarrow{\mathrm{Hom}_S(P, P\otimes_R \beta)} & & & \mathrm{Hom}_S(P, P\otimes_R (\bigoplus_I R)) & \xrightarrow[\varepsilon_{**}]{} & \mathrm{Hom}_S(P, P\otimes_R A)
\end{array}$$

Wenden wir das 5er-Lemma an, so schließen wir, dass η_A schließlich ein Isomorphismus ist.
(2.) Analog: $P\otimes_R \mathrm{Hom}(P,-) \cong \mathrm{Id}_{S\text{-}\underline{\mathrm{Mod}}}$. Die Behauptung folgt. ■

Wir erwähnen noch eine Folgerung des Satzes von Morita ohne Beweis.

Folgerung 25.5

Sind R und S zwei Ringe mit $R \sim_M S$, so gilt $Z(R) \cong Z(S)$.

Aufgabe 25.6

Seien S, R zwei Ringe und sei $n \in \mathbb{N}$. Zeigen Sie:

(a) Die Ringe $M_n(S)$ und S sind Morita-äquivalent.

(b) Sind R und S isomorph, so sind R und S Morita-äquivalent.

(c) Sind R und S kommutativ, so gilt: R und S sind genau dann Isomorph, wenn R und S Morita-äquivalent sind.

(d) Für jedes Idempotent $e \in R$ mit $ReR = R$ sind die Ringe R und eRe Morita-äquivalent.

Anmerkung 25.7

Morita-Äquivalenzen sind besonders interessant, weil viele Modul-Eigenschaften erhalten bleiben. Genauer: Ist $\Phi : R\text{-}\underline{\text{Mod}} \longrightarrow S\text{-}\underline{\text{Mod}}$ eine Äquivalenzen von Kategorien und M ein R-Modul, so gilt beispielsweise:

$$\begin{array}{lcl}
M \text{ ist einfach} & \Longrightarrow & \Phi(M) \text{ ist einfach;} \\
M \text{ ist projektiv} & \Longrightarrow & \Phi(M) \text{ ist projektiv;} \\
M \text{ ist artinsch} & \Longrightarrow & \Phi(M) \text{ ist artinsch;} \\
M \text{ ist halbeinfach} & \Longrightarrow & \Phi(M) \text{ ist halbeinfach;} \\
M \text{ ist (un)zerlegbar} & \Longrightarrow & \Phi(M) \text{ ist (un)zerlegbar;} \\
M \text{ ist } \ldots & \Longrightarrow & \Phi(M) \text{ ist } \ldots
\end{array}$$

Teil III.
Gruppentheorie und Körpertheorie

Kapitel 6. Gruppentheorie und Galoistheorie

Konventionen in diesem Kapitel:

- $(G, \cdot)$ oder einfach G bezeichnet stets eine Gruppe;
- wenn nicht anders vorausgesetzt, wird die Verknüpfung aller Gruppen als Multiplikation geschrieben;
- C_n (mit $n \in \mathbb{N}$) bezeichnet stets eine zyklische Gruppe der Ordnung n, d.h.

$$C_n = \langle g \mid g^n = 1 \rangle = \{1, g, g^2, ..., g^{n-1}\};$$

- $\mathbb{P}$ bezeichnet stets die Menge aller positiven Primzahlen in $\mathbb{Z}$;
- alle Körper sind Körper der Charakteristik 0;
- $\mathrm{Syl}_p(G)$ bezeichnet die Menge der Sylow-p-Untergruppen der endlichen Gruppe G; und
- $n_p := |\mathrm{Syl}_p(G)|$.

Ziel. Das Ziel dieses Kapitel ist es die Lösbarkeit von Polynomgleichung der Form

$$f(X) = 0 \qquad \text{mit } f \in K[X],$$

wobei $K \subseteq \mathbb{C}$. Wir wollen verstehen, wann man Formeln in den Koeffizienten von f angeben kann, um die Lösungen zu beschreiben. Um dieses Ziel zu erreichen, führen wir zuerst die Klasse der auflösbaren Gruppen ein, die zusammen mit der Galois-Theorie, die in der Algebra I entwickelt wurde, die Antwort liefert.

26 Auflösbare Gruppen

26.1 Definitionen und Beispiele

Definition 26.1 (*auflösbare Gruppe, Normalreihe, Faktoren*)

Eine Gruppe G heißt **auflösbar**, falls es $n \in \mathbb{Z}_{\geqslant 0}$ und Untergruppen

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

existieren, sodass die Faktorgruppe G_i/G_{i-1} für alle $1 \leqslant i \leqslant n$ abelsch ist. Die Reihe

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

heißt **Normalreihe** (**der Länge** n) von G und die Faktorgruppen G_i/G_{i-1} sind die **Faktoren** dieser Normalreihe.

Anmerkung 26.2

Es wird gefordert, dass $G_{i-1} \trianglelefteq G_i$, aber nicht unbedingt $G_i \trianglelefteq G$.

Beispiel 39

(1) Abelsche Gruppen sind auflösbar, da

$$1 = G_0 \trianglelefteq G_1 = G$$

eine Normalreihe ist und die Faktotgruppe $G_1/G_0 \cong G$ ist abelsch.

(2) Die Diedergruppen D_{2n} (mit $n \in \mathbb{Z}_{\geqslant 3}$) sind auflösbar, da gelten:

- $D_{2n} = \langle \sigma, \rho \rangle$ mit $\sigma :=$ Spiegelung, $\rho :=$ Drehung um $\frac{2\pi}{n}$; und
- $1 \trianglelefteq C_n \cong \langle \rho \rangle \trianglelefteq D_{2n}$, weil $|D_{2n}, \langle \rho \rangle| = 2$.

(3) Die zyklischen Gruppen C_p mit $p \in \mathbb{P}$ sind die einzigen **einfachen**, **auflösbaren** Gruppen. (Siehe Aufgabe 1, Blatt 11.)

(4) Die Gruppe $\mathrm{PSL}_2(\mathbb{F}_{11})$ ist NICHT auflösbar, da sie einfach und nicht abelsch ist.

Für endliche Gruppen haben wir weitere äquivalente Charakterisierungen:

Satz 26.3

Sei G eine endliche Gruppe. Dann sind äquivalent:

(a) G ist auflösbar;

(b) es existieren Untergruppen

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

sodass G_i/G_{i-1} für alle $1 \leqslant i \leqslant n$ **zyklisch** ist; und

(c) es existieren Untergruppen wie in (b), sodass G_i/G_{i-1} für alle $1 \leqslant i \leqslant n$ zyklisch von Primzahlordnung ist.

Beweis:

(b) $\Longrightarrow$ (a): klar, weil zyklischen Gruppen abelsch sind.

(c) $\Longrightarrow$ (a): klar, weil zyklischen Gruppen abelsch sind.

(c) $\Longrightarrow$ (b): klar, weil zyklischen Gruppen von Primzahlordnung, zyklisch sind.

(a) $\Longrightarrow$ (b) (bzw. (c)): Wir nehmen an, dass G auflösbar ist. Wir können auch annehmen, dass $G \neq 1$.

Für $G = 1$ ist nichts zu tun.

Schritt 1: Wir zeigen, dass (b) (bzw. (c)) gilt, falls $G \neq 1$ abelschist.

Sei also $p \in \mathbb{P}$ ein Primteiler von $|G|$. Nach dem Satz von Cauchy (ALGEBRA I) existiert $x \in G$ mit Ordnung p. Setze

$$G_0 := 1, \quad G_1 := \langle x \rangle .$$

Dann ist $G_1/G_0 \cong C_p$ zyklisch (von Primzahlordnung). Falls $G = \langle x \rangle$, sind wir fertig. Falls nicht, betrachten wir die Faktorgruppe $G/\langle x \rangle$ (weil G abelsch ist, gilt $\langle x \rangle \trianglelefteq G$.) Per Induktion nach $|G|$ können wir annehmen, dass $G/\langle x \rangle$ Bedingung (b) (bzw. (c)) erfüllt. Sei also

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = G/\langle x \rangle$$

eine Normalreihe von $G/\langle x \rangle$ mit zyklischen Faktoren (von Primzahlordnung). Nach dem Korrespondenzsatz für Gruppen gibt es Untergruppen

$$\langle x \rangle = \widetilde{N}_0 \trianglelefteq \widetilde{N}_1 \trianglelefteq \cdots \trianglelefteq \widetilde{N}_m = G$$

mit $\widetilde{N}_i/\langle x \rangle = N_i$ für alle $0 \leqslant i \leqslant m$. Nach dem 3. Isomorphiesatz ist

$$\widetilde{N}_i/\widetilde{N}_{i-1} \cong (N_i)/\langle x \rangle)/(N_{i-1}/\langle x \rangle) = N_i/N_{i-1}$$

zyklisch (von Primzahlordnung) für alle $1 \leqslant i \leqslant m$. Somit ist

$$1 = G_0 \trianglelefteq G_1 = \langle x \rangle = \widetilde{N}_0 \trianglelefteq \widetilde{N}_1 \trianglelefteq \cdots \trianglelefteq N_m = G$$

eine Normalreihe von G mit zyklischen Faktoren (von Primzahlordnung).

Schritt 2: Wir zeigen nun, dass (b) bzw. (c) für $G \neq 1$ beliebig gelten. Sei

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

eine Normalreihe von G mit abelschen Faktoren. Nach Schritt 1 können wir für alle $1 \leqslant i \leqslant n$ eine Teilreihe

$$G_{i-1} = G_{i-1,0} \trianglelefteq G_{i-1,1} \trianglelefteq \cdots \trianglelefteq G_{i-1,m} = G_i$$

mit zyklischen Faktoren konstruieren. Die Konkatenation von diesen Teilreihen ist eine Normalreihe von G, die Bedingung (b) (bzw. (c)) erfüllt. ■

Anmerkung 26.4

Ist G auflösbar und $G \cong H$ (als Gruppe), so ist auch H auflösbar.
Begründung: Sei $\varphi : G \to H$ ein Isomorphismus von Gruppen.
Ist $1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$ eine Normalreihe von G mit abelschen Faktoren, dann ist auch $1 = \varphi(G_0) \trianglelefteq \cdots \trianglelefteq \varphi(G_n) = \varphi(G) = H$ eine Normalreihe von H mit abelschen Faktoren.

Bemerkung 26.5 (*Sandwich-Prinzip für auflösbare Gruppen*)

Sei $1 \to N \xrightarrow{\varphi} G \xrightarrow{\psi} Q \to 1$ eine k.e.S. von Gruppen. Dann gilt:

$$G \text{ ist auflösbar} \iff N \text{ und } Q \text{ sind auflösbar.}$$

Beweis:

($\Rightarrow$) Sei G eine auflösbare Gruppe und sei $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$ eine Normalreihe von G mit abelschen Faktoren.

(1) Wir Zeigen: Ist $\varphi' : H \hookrightarrow G$ injektiver Homomorphismus von Gruppen, so ist H ist auflösbar.

Es gilt

$$1 = G_0 \cap \varphi'(H) \trianglelefteq G_1 \cap \varphi'(H) \trianglelefteq \cdots \trianglelefteq G_n \cap \varphi'(H) = \varphi'(H)$$

und für alle $1 \leqslant i \leqslant n$ ist

$$(G_i \cap \varphi'(H))/(G_{i-1} \cap \varphi'(H)) \cong (G_i \cap \varphi'(H))/((G_i \cap \varphi'(H) \cap G_{i-1}) \cong (G_i \cap \varphi'(H))G_i/G_{i-1}) \leqslant \underbrace{G_i/G_{i-1}}_{\text{abelsch}}.$$

Somit ist $H \cong \varphi'(H)$ auflösbar nach Anmerkung 26.4.

(2) Wir zeigen, dass G/N auflösbar ist.
Zunächst ist $1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_nN/N = G/N$ eine Normalreihe von G/N nach dem Korrespondenzsatz. Für alle $1 \leqslant i \leqslant n$ gilt

$$\begin{aligned}
(G_iN/N)/(G_{i-1}N/N) &\underset{\text{3. Iso-Satz}}{\cong} G_iN/G_{i-1}N \\
&= (G_iG_{i-1})N/G_{i-1}N \\
&= G_i(G_{i-1}N)/(G_{i-1}N) \\
&\underset{\text{2. Iso-Satz}}{\cong} G_i/G_i \cap G_{i-1}N \\
&\cong G_i/(G_i \cap N)G_{i-1} \\
&\underset{\text{3. Iso-Satz}}{\cong} \underbrace{\underbrace{(G_i/G_{i-1})}_{\text{abelsch}}/((G_i \cap N)G_{i-1}/G_{i-1})}_{\text{abelsch}}.
\end{aligned}$$

Daher ist G/N auflösbar und es folgt aus Anmerkung 26.4, dass $Q \cong G/N$ auflösbar ist.

($\Leftarrow$) Nach Anmerkung 26.4, können wir annehmen, dass $N \leqslant G$ und $Q = G/N$. Sei also

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$$

eine Normalreihe von N mit abelschen Faktoren. Wie beim vorherigen Beweis hat G/N nach dem Korrespondenzsatz eine Normalreihe der Form

$$1 = G_0/N \trianglelefteq \cdots \trianglelefteq G_s/N = G/N$$

mit $N \trianglelefteq G_0 \trianglelefteq \cdots \trianglelefteq G_s = G$ und abelschen Faktoren. ∎

Folgerung 26.6

Ist G eine auflösbare Gruppe, so sind alle Untergruppen und Faktorgruppen von G auflösbar.

Beweis:

- Untergruppen: Spezialfall im Beweis (1)
- Faktorgruppen: (2) im Beweis

∎

Folgerung 26.7

(a) Endliche p-Gruppen sind auflösbar für alle Primzahlen $p \in \mathbb{P}$.

(b) Endliche Gruppen der Ordnung $p \cdot q$ mit $p, q \in \mathbb{P}$ sind auflösbar.

Beweis:

(a) Sei G eine endliche p-Gruppe. Wir führen eine vollständige Induktion nach $|G|$ durch.

(IA) Ist $|G| = 1$, so its $G = 1$ und G ist auflösbar, da $1 = G_0 = G$ eine Normalreihe mit abelschen Faktoren ist.

Wir nehmen nun an, dass $|G| \geqslant 2$ ist.
(IV) Alle endlichen Gruppen H mit $|H| < |G|$ sind auflösbar.
(IS) Aus Algebra I ist bekannt, dass $1 \neq Z(G) \trianglelefteq G$. Daher ist $|G/Z(G)| = |G|/|Z(G)| < |G|$ und folgende Eigenschaften gelten:

- $Z(G)$ ist auflösbar nach Beispiel 1, weil $Z(G)$ abelsch ist.
- $G/Z(G)$ ist auflösbar nach der (IV).

Wir erhalten also eine k.e.S.

$$1 \longrightarrow \underbrace{Z(G)}_{\text{auflösbar}} \overset{\text{kan. Inkl}}{\hookrightarrow} G \overset{\text{Faktorabb.}}{\twoheadrightarrow} \underbrace{G/Z(G)}_{\text{auflösbar}} \longrightarrow 1\,.$$

Daher ist G auflösbar nach dem Sandwich-Prinzip.

(b) Sei G eine endliche Gruppe der Ordnung $p \cdot q$. Ist $p = q$, so ist G eine p-Gruppe und G ist auflösbar nach Teil (a). O.B.d.A. können wir annehmen, dass $p < q$. Sei $Q \in Syl_q(G)$ eine q-Sylow-Untergruppe. Nach der Sylow-Theorie gelten:

(1) $|G : N_G(Q)| \mid p$; und
(2) $|G : N_G(Q)| \equiv 1 \bmod q$.

Die einzige Möglichkeit, dass (1) und (2) gleichzeitig gelten ist dann $|G : N_G(Q)| = 1$ weil $p < q$ ist. Daher ist $N_G(Q) = G$, d.h. $Q \trianglelefteq G$.
Nun gelten:

- Q ist auflösbar nach der Teil (a), weil Q eine q-Gruppe ist; und
- $G/Q \cong C_p$ ist auflösbar, weil C_p abelsch ist.

Es gibt also eine k.e.S

$$1 \longrightarrow \underbrace{Q}_{\text{auflösbar}} \overset{\text{kan. Inkl.}}{\hookrightarrow} G \overset{\text{Faktorabb.}}{\twoheadrightarrow} \underbrace{G/Q}_{\text{auflösbar}} \longrightarrow 1\,.$$

Daher ist G auflösbar nach dem Sandwich-Prinzip. ∎

Satz 26.8

Alle endlichen Gruppen der Ordnung < 60 sind auflösbar.

Klar für $|G| \in \{p^n, p \cdot q\}$ mit $p, q \in \mathbb{P}, n \in \mathbb{Z}_{\geqslant 0}$ nach Folgerung 26.7. Für die übrigen Ordnungen, d.h.

$$|G| \in \{12, 18, 20, 24, 28, 30, 36, 40, 42, 44, 45, 48, 52, 54\}$$

verwenden wir die Sylow-Theorie! (→ Siehe auch Blatt 11.)

Beweis 26.8: Beispielsweise beweisen wir hier, dass alle Gruppen der Ordnung 30 und 44 auflösbar sind.

(1) $|G| = 44 = 2^2 \cdot 11 \implies G$ ist auflösbar.

Nach der Sylow-Theorie gelten:

(i) $n_{11} \mid 4$;

(ii) $n_{11} \equiv 1 \pmod{11}$.

Nach (i) ist $n_{11} \in \{1, 2, 4\}$ und nach (ii) ist $n_{11} = 1$ die einzige Möglichkeit. Somit ist $\{P_{11}\} := \mathrm{Syl}_{11}(G)$ und die einzige 11-Sylow-Untergruppe muss ein Normalteiler von G sein, weil alle 11-Sylow-Untergruppen G-konjugiert sind, d.h. $P_{11} \trianglelefteq G$. Daher existiert eine k.e.S.

$$1 \to P_{11} \xhookrightarrow[\text{kan. Inkl.}]{\iota} G \xrightarrow[\text{kan. Proj.}]{\pi} G/P_{11} \to 1\,.$$

Dabei gelten nach Folgerung 26.7(a):

- $|P_{11}| = 11 \implies P_{11} \cong C_{11}$ ist ist eine 11-Gruppe, daher auflösbar; und
- $|G/P_{11}| = 4 \implies G/11$ ist eine 2-Gruppe, daher auflösbar.

Insgesamt ist G auflösbar nach dem Sandwich-Prinzip.

(2) $|G| = 30 = 2 \cdot 3 \cdot 5 \cdot 11 \implies G$ ist auflösbar.

Nach der Sylow-Theorie gelten:

(i) $n_5 \mid 2 \cdot 3$ und $n_5 \equiv 1 \pmod{5}$;

(ii) $n_3 \mid 2 \cdot 5$ und $n_3 \equiv 1 \pmod{3}$.

Aus (i) folgt $n_5 \in \{1, 6\}$ und aus (ii) folgt $n_3 \in \{1, 10\}$.

Fall 1: $n_5 = 1$

Wie in (1) ist die einzige 5-Sylow-Untergruppe $\widetilde{P}_5$ ein Normalteiler in G und somit gibt es eine k.e.S.

$$1 \to \widetilde{P}_5 \xhookrightarrow[\text{kan. Inkl.}]{\iota} G \xrightarrow[\text{Faktorabb.}]{\pi} G/\widetilde{P}_5 \to 1$$

wobei $\widetilde{P}_5 \cong C_5$ und $|G/\widetilde{P}_5| = 2 \cdot 3$ sind auflösbar nach Folgerung 26.7. Insgesamt ist G auflösbar nach dem Sandwich-Prinzip.

Fall 2: $n_5 = 6$

Schreibe dann $\mathrm{Syl}_p(G) = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Es gilt $P_i \cong C_5 \,\forall\, 1 \leqslant i \leqslant 6$, weil $|P_5| = 5$ ist, und $P_i \cap P_j = \{1_G\} \,\forall\, 1 \leqslant i \neq j \leqslant 6$, da sonst $P_i = P_j$ gelten müsste. Außerdem besitzt jede Untergruppe vier Elemente der Ordnung 5 und das neutrale Element (der Ordnung 1). Somit haben wir in G:

- genau $6 \cdot 4$ Elemente der Ordnung 5;
- genau ein Element der Ordnung 1; und
- Platz übrig für $30 - 6 \cdot 4 - 1 = 5$ Elemente der Ordnung $o \notin \{1, 5\}$.

Daher ist $n_3 = 10$ nicht möglich, da es sonst genau $10 \cdot 2 = 20$ Elemente der Ordnung 3 geben müsste. Es bleibt $n_3 = 1$ und die einzige 3-Sylow-Untergruppe Q_3 ist ein Normalteiler in G und es existiert eine k.e.S.:

$$1 \to Q_3 \xhookrightarrow[\text{kan. Inkl.}]{\iota} G \xrightarrow[\text{Faktorabb.}]{\pi} G/Q_3 \to 1\,,$$

wobei $|Q_3| = 3$ und $|G/Q_3| = 2 \cdot 5$, sodass Q_3 und G/Q_3 auflösbar nach Folgerung 26.7 sind. Insgesamt ist G auflösbar nach dem Sandwich-Prinzip.

Für alle verbliebenden Ordnungen kann man ein analoges Argument verwenden. ∎

Aufgabe 26.9 (*Augabe 3(a), Blatt 11*)

Zeigen Sie mithilfe der Sylow-Theorie, dass alle Gruppen der Ordnung 12 und 20 auflösbar sind.

Aufgabe 26.10

Zeigen Sie: Die Kleinsche Viergruppe V_4, die alternierenden Gruppen A_2, A_3, A_4 und die symmetrischen Gruppen S_2, S_3 und S_4 sind auflösbar.

26.2 Der $p^a q^b$-Satz und der Satz von Feit und Thompson

Wir erwähnen noch zwei berühmte Sätze zu der Theorie der auflösbaren Gruppen, die sehr einfache Aussagen haben, deren Beweise aber Charaktertheorie erfordern.

Satz 26.11 (*Burnside, 1904*)

Endliche Gruppen der Ordnung $p^a \cdot q^b$ mit $p, q \in \mathbb{P}$ und $a, b \in \mathbb{Z}_{\geqslant 0}$ sind auflösbar.

Zum Beweis:

→ Der Beweis verwendet die Charaktertheorie der endlichen Gruppen!

→ Dieser Satz wird in der Vorlesung „Darstellungstheorie der endlichen Gruppen" bewiesen. (Etwa um die 10. Woche herum!)

→ Die folgende Aufgabe zeigt, wie der letzte Schritt des Beweises funktioniert. ■

Aufgabe 26.12 (*Aufgabe 2(a), Blatt 11*)

Sei G eine endliche Gruppe der Ordnung $p^a q^b$ mit $p, q \in \mathbb{P}$ und $a, b \in \mathbb{Z}_{\geqslant 0}$. Wir nehmen an, dass wir schon zeigen konnten, dass G nicht einfach ist, falls $a + b \geqslant 2$ ist.

(i) Zeigen Sie: Ist $a + b \geqslant 2$, so besitzt G einen Normalteiler $N \lhd G$ mit $|N|, |G/N| < |G|$.

(ii) Zeigen Sie per Induktion nach $a + b$, dass G auflösbar ist.

Der Satz von Feit und Thompson ist einer der berühmtesten Sätze der Theorie der endlichen Gruppen. Einerseits ist die Aussage beeindruckend einfach:

Satz 26.13 (*„The Odd Order Theorem" , Feit-Thompson, 1963*)

Jede endliche Gruppe ungerader Ordnung ist auflösbar.

Andererseits sind (bisher) keine „zugänglichen" Beweise bekannt. Außerdem war dieser Satz eine Vermutung von Burnside aus dem Jahr 1911.

Zum Beweis:

- Originaler Beweis:
  → ca. 250 Seiten;
  → komplette Nr. 3 des *Pacific Journal of Mathematics*. Siehe `https://projecteuclid.org/journals/pacific-journal-of-mathematics/volume-13/issue-3`.

- Vereinfachungen:
  → von Bender-Glaubermann;
  → von Peterfalvi;
  → Hauptstruktur des Beweises bleibt unverändert!
- 2012: Verifikation des Beweise mit **Coq**. ■

26.3 Höhere Kommutatorgruppen

Wir führen eine weitere Charakterisierung der Auflösbarkeit ein, die uns z.B. erlauben wird, alternierende und symmetrische Gruppen zu behandeln.

Wiederholung (Algebra I):

- Sind $x, y \in G$, so ist $[x, y] := xyx^{-1}y^{-1}$ der **Kommutator** des Paares (x, y); und
- $G' := [G, G] := \langle [x, y] \mid x, y \in G \rangle$ ist die **Kommutator-Untergruppe** (oder einfach die **Kommutatorgruppe**) von G.

Definition 26.14 (*i-te Kommutatorgruppe*)

Wir setzen $G^{(0)} := G$ und für jede Zahl $i \in \mathbb{N}$ heißt $G^{(i)} := \left[G^{(i-1)}, G^{(i-1)}\right]$ die ***i*-te Kommutatorgruppe** von G.

Es ist klar, dass $G^{(1)} = [G, G]$ ist.

Wir erhalten folgende weitere Charakterisierung der Auflösbarkeit durch Kommutatorgruppen.

Satz 26.15

Für eine Gruppe G gilt:

$$G \text{ ist auflösbar} \quad \Longleftrightarrow \quad \exists\, j \in \mathbb{N} \text{ mit } G^{(j)} = 1\,.$$

Anmerkung 26.16

Aus der Algebra I ist auch bekannt, dass für eine beliebige Gruppe F gelten:

(1) $[F, F] \,; \trianglelefteq F$

(2) $F/[F, F]$ ist abelsch ; und

(3) F/N ist abelsch $\quad \Longleftrightarrow \quad N \geqslant [F, F]\,.$

Beweis von Satz 26.15 :

„⇐“ : Wir nehmen an, es existiert ein $j \in \mathbb{N}$ mit $G^{(j)} = 1$. Nach (1) und (2) aus der Anmerkung ist es klar, dass

$$1 = G^{(j)} \trianglelefteq G^{(j-1)} \trianglelefteq \ldots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

eine Normalreihe mit abelschen Faktoren ist. Daher ist G auflösbar nach Definition.

„⇒“ : Wir nehmen umgekehrt an, dass G auflösbar ist. Dann existiert ein Normalreihe

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

mit abelschen Faktoren der Länge n.

Behauptung: $G^{(n)} = 1$.
Per Induktion nach n:

(IA): $n = 0 \qquad \Longrightarrow \qquad G^{(0)} = G = G_0 = G_n = 1$.

(IV): Wir können daher annehmen, dass die Behauptung gilt, für alle auflösbaren Gruppen mit Normalreihen der Länge $s \leqslant n-1$ und abelschen Faktoren.

(IS): Da G auflösbar ist, dies impliziert, dass auch ihre Untergruppe G_1 auflösbar ist und dass G_1 eine Normalreihe

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_1$$

mit abelschen Faktoren der Länge $n-1$ hat. Es folgt aus der Indunktionsvorraussetzung, dass $G_1^{(n-1)} = 1$ ist. Nun ist nach (3) aus der Anmerkung $G_1 \geqslant G'$, weil $G/G_1 = G_0/G_1$ abelsch ist. Somit gilt

$$G^{(n)} = G'^{(n-1)} \leqslant G_1^{(n-1)} = 1\,.$$

Folglich ist $G^{(n)} = 1$. ■

Definition 26.17 (*perfekte Gruppe*)

Eine Gruppe G mit $[G, G] = G$ heißt **perfekt**.

Folgerung 26.18

Nichttriviale perfekte Gruppen sind nicht auflösbar.

Beweis : Direkte Folgerung aus Satz 26.15. ■

Beispiel 40

Für die Gruppe $\mathrm{SL}_2(\mathbb{F}_q)$ mit $q \geqslant 5$ gilt

$$\left[\mathrm{SL}_2(\mathbb{F}_q), \mathrm{SL}_2(\mathbb{F}_q)\right] = \mathrm{SL}_2(\mathbb{F}_q),$$

daher ist $\mathrm{SL}_2(\mathbb{F}_q)$ eine perfekte Gruppe und somit nicht auflösbar.

Dieses Argument kann auch verwendet werden, um zu zeigen, dass die Symmetrische Gruppe S_n mit $n \geqslant 5$ nicht auflösbar ist.

Aufgabe 26.19 (*Aufgabe 2(b), Blatt 11*)

Sei $n \in \mathbb{Z}_{\geqslant 5}$.

(i) Zeigen Sie, dass die alternierende Gruppe A_n perfekt ist.
[Hinweise. (1) A_n wird von der Menge aller 3-Zyklen erzeugt. (2) Jeder 3-Zyklus ist der Kommutator von zwei 3-Zyklen.]

(ii) Zeigen Sie, dass A_n und S_n nicht auflösbar sind.

Anmerkung 26.20

Eine Normalreihe $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ mit einfachen Faktoren G_i/G_{i-1} für alle $1 \leqslant i \leqslant n$, nennt man eine **Kompositionsreihe** von G.

Aufgabe 26.21 (*Augabe 3(b), Blatt 11*)

Zeigen Sie, dass jede endliche Gruppe G eine Kompositionsreihe besitzt.
[Hinweis: Induktion nach $|G|$.]

Satz 26.22 (Jordan-Hölder *für Gruppen*)

Je zwei Kompositionsreihen einer Gruppe G sind äquivalent.

Beweis: Analog zu R-Mod. ■

27 Auflösbarkeit durch Radikale

Als Nächstes möchten wir Verbindungen zwischen der Theorie der auflösbaren Gruppen und der Theorie der Körpererweiterungen erstellen.

Wiederholung. (Algebra I)
Zunächst erinnern wir an ein paar Begriffe und Ergebnisse zu den Körpererweiterungen aus der Vorlesung Algebra I.

- Ist L ein körper und $K \subseteq L$ ein Teilkörper, so nennt man L **Körpererweiterung** (oder **Erweiterungskörper**) von K und wir schreiben L/K anstelle von $K \subseteq L$.
- Der **Grad** einer Körpererweiterung L/K ist $[L : K] := \dim_K(L)$.
- Die **Automorphismengruppe** einer Körpererweiterung L/K ist

$$\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}.$$

- Wenn $[L : k] \leqslant \infty$, so heißt die Erweiterung L/K **endlich** und es gilt auch $\mathrm{Aut}(L/K) \leqslant \infty$.
- Eine endliche Körpererweiterung L/K heißt **Galois-Erweiterung**, wenn $|\mathrm{Aut}(L/K)| = [L : K]$ ist. Ggf. schreiben wir $\mathrm{Aut}(L/K) := \mathrm{Aut}(L/K)$.
- Ein Erweiterungskörper L eines Körper K heißt **Zerfällungskörper** eines nicht-konstanten Polynoms $f \in K[X]$, falls gelten:
  (1) $\exists\, m \in \mathbb{N}, \alpha_1, \ldots, \alpha_m \in L, c \in K$ mit $f = c \cdot \prod_{i=1}^{m}(X - \alpha_i)$; und
  (2) $L = K(\alpha_1, \ldots, \alpha_m)$. In diesem Fall gilt: Ist $\mathrm{Char}(K) = 0$, dann ist L/K eine Galois-Erweiterung.

27.1 Lösbarkeit von Polynomgleichungen.

Ziel. Wir möchten nun Körpertheorie und Gruppentheorie gleichzeitig verwenden, um die Losbarkeit von Polynomgleichungen der Form

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X^1 + a_0 = 0$$

mit $n \in \mathbb{N}$, $a_n \in \mathbb{C}^\times$, $a_{n-1}, \ldots, a_0 \in \mathbb{C}$ (bzw. in einem Teilkörper $K \subseteq \mathbb{C}$) zu untersuchen.

Beispiel 41

Ist $n \in \{1, 2, 3, 4\}$, so ist es (seit lang!) bekannt, dass Formeln in den Koeffizienten $a_n, \ldots, a_0$ existieren, um die Nullstellen vom Polynom $f := a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X^1 + a_0$ zu berechnen.

(1) **Fall** $n = 1$: $f = a_1 X + a_0$ hat die Nullstelle $-\frac{a_0}{a_1}$.

(2) **Fall** $n = 2$: $f = a_2 X^2 + a_1 X + a_0$ hat die Nullstellen

$$\frac{-a_1 \pm \sqrt[2]{a_1^2 - 4a_2 a_0}}{2a_2}.$$

(3) **Fall** $n \in \{3, 4\}$: Die Formeln von Cardano liefern die Nullstellen von Polynomen vom Grad 3 und Die Formeln von Lodovico Ferrari liefern die Nullstellen von Polynomen vom Grad 4. Diese Formeln wunden bereits 1545 in einem Buch von Cardano veröffentlicht. Siehe Anhang von C. Bessenrodt in den Vorlesungsfolien!

Definition 27.1 (*Radikalerweiterung*)

Eine Körpererweiterung L/K heißt **Radikalerweiterung**, wenn es Elemente $w_1, \ldots w_n \in L$ ($n \in \mathbb{Z}_{\geqslant 0}$) gibt, sodass gilt: $w_1^{r_1} \in K$ und für $1 < i \leqslant m$ ist $w_i^{r_i} \in K(w_1, \ldots, w_{i-1})$ für geeignete $r_1, \ldots, r_n \in \mathbb{N}$.

Definition 27.2 (*Auflösbarkeit durch Radikale*)

Sei $K \subseteq \mathbb{C}$ ein Körper.Ein nicht-konstantes Polynom $f \in K[X]$ ist **durch Radikale auflösbar**, wenn ein Zerfällungskörper L von f in einer Radikalerweiterung von K liegt.

Äquivalent: f besitzt eine Nullstelle, die in einer Radikalerweiterung liegt.

Anmerkung 27.3

Die Bedeutung von Definition 27.2 ist: Die Lösungen der Gleichung $f(X) = 0$ können durch Elemente aus K, $+$, $-$, $\cdot$, $/$ und das Wurzelziehen ausgedrückt werden.

Unser Ziel ist es, den folgenden Satz von Galois zu verstehen und beweisen.

Satz 27.4 (Galois)

Sei $K \subseteq \mathbb{C}$ ein Körper. Sei $f \in K[X]$ ein nicht-konstantes Polynom und sei L ein Zerfällungskörper von f. Dann gilt:

$$f \text{ ist durch Radikale auflösbar} \iff \mathrm{Aut}(L/K) \text{ ist auflösbar}.$$

Wir fangen mit Folgerungen dieses Satzes und werden erst danach den Beweis angeben.

Die Verbindung mit der Existenz von Lösungsformeln für Polynomgleichungen vom Grad 1/2/3/4 ergibt sich aus der folgenden Folgerung.

Folgerung 27.5

Über einem Körper $K \subseteq \mathbb{C}$ ist jedes nicht-konstantes Polynom $f \in K[X]$ vom Grad höchstens 4 durch Radikale auflösbar.

Beweis: Sei L ein Zerfällungskörper von f. Nach dem Satz von Galois reicht es zu zeigen, dass die Galois-Gruppe $\mathrm{Aut}(L/K)$ auflösbar ist.
Wir wissen aus der Algebra I, dass $\mathrm{Aut}(L/K)$ auf die Menge $\mathcal{M}$ aller Nullstellen von f durch Permutation operiert. Wegen $\deg(f) \leqslant 4$ gilf also $\mathrm{Aut}(L/K) \leqslant S_4$. Nun ist S_4 auflösbar (Aufgabe 1(b), Blatt 11) und somit muss auch $\mathrm{Aut}(L/K)$ auflösbar sein nach Folgerung 26.6. ■

Mit diesem Satz können wir auch beweisen: Es gibt Polynome vom Grad 5, die nicht durch Radikale auflösbar sind!

Folgerung 27.6 (Abel-Ruffini)

Das Polynom $f := X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist nicht durch Radikale auflösbar.

Beweis: Sei L ein Zerfällungskörper von f. Nach dem Satz von Galois reicht es zu zeigen, dass die Galois-Gruppe $\mathrm{Aut}(L/\mathbb{Q})$ NICHT auflösbar ist. Wie im Beweis von Folgerung 27.5 operiert $\mathrm{Aut}(L/\mathbb{Q})$ durch Permutation auf die Menge aller Nullstellen von f. Daher gilt

$$\mathrm{Aut}(L/\mathbb{Q}) \leqslant S_5$$

weil $\deg(f) = 5$ ist. Wir behaupten nun, dass $\mathrm{Aut}(L/\mathbb{Q}) = S_5$ ist.

- Das Polynom f ist irreduzibel über $\mathbb{Z}$ nach dem Eisensteinkriterium (mit $p = 2$), also auch über $\mathbb{Q}$ nach dem Satz von Gauß. Wegen $\deg(f) = 5$ gilt also

$$5 \mid \mathrm{Aut}(L/\mathbb{Q})\,.$$

- Eine übliche Kurven-Analysis zeigt: f hat genau 3 Nullstellen in $\mathbb{R}$. Daher gibt es noch zwei komplex-konjugierten Nullstellen in $\mathbb{C}\backslash\mathbb{R}$ und somit ist die Komplexe-Konjugation eingeschränkt auf L ein Automorphismus in $\mathrm{Aut}(L/\mathbb{Q})$ der Ordnung 2.

Die einzige Untergruppe von S_5, die diese beide Eigenschaften erfüllt sind, ist S_5 selbst. Es folgt also aus Aufgabe 26.19, dass $\mathrm{Aut}(L/\mathbb{Q})$ nicht auflösbar ist. ■

Zurück zum Satz von Galois:
Zunächst untersuchen wir die *reinen Gleichungen*

$$X^n - a = 0 \qquad \text{mit } n \in \mathbb{N} \text{ und } a \in K\,.$$

Ist L ein Zerfällungskörper von $f := X^n - a \in K[X]$, dann ist offenbar L/K eine Radikalerweiterung, da alle Nullstellen b von f die Bedingung $b^n \in K$ erfüllt. (Klar: $b^n = a$.)
Außerdem: Wegen $\mathrm{Char}(K) = 0$ ist $X^n - a$ separabel und wir konnen die Galois-Korrespondenz verwenden.

Ist $z \in \overline{K}$ eine primitive n-te Einheitswurzel, so sind die Nullstellen von $X^n - a$ der Form

$$z^j b \qquad \text{mit } j = 0, 1, \ldots, n-1$$

Also enthält L auch die n-te Einheitswurzeln. Weil die Erweiterungen $K(z)/K$ in der ALGEBRA I bereits untersucht wurden, wenden wir uns jetzt der Erweiterung $L/K(z)$ zu und wir können also von einem Grundkörper ausgehen, der bereits die n-ten Einheitswurzeln enthält.

Satz 27.7

Sei $n \in \mathbb{N}$ und enthälte K die n-ten Einheitswurzeln. Sei $f := X^n - a \in K[X]$ mit $a \neq 0$ und sei L ein Zerfällungskörper von f. Dann gelten:

(a) $\mathrm{Aut}(L/K)$ ist zyklisch;

(b) ist f irreduzibel, so ist $\mathrm{Aut}(L/K) = n$; und

(c) zu jeder zyklischen Erweiterung $\widetilde{L}/K$ mit $[\widetilde{L} : K] = n$ gibt es ein Element $b \in \widetilde{L}$ mit $\widetilde{L} = K(b)$.

Beweis: Sei z eine primitive n-te Einheitswurzel. Nach Voraussetzung ist $z \in K$.

(a) Ist b eine Nullstelle von f in L, dann sind $b, zb, \ldots, z^{n-1}b$ genau die n Nullstellen von f; also ist $L = K(b)$. Daher ist jedes Element $\sigma \in \mathrm{Aut}(L/K)$ durch $\sigma(b)$ eindeutig bestimmt. Ist $\sigma(b) = z^j b$ mit mit $0 \leqslant j \leqslant n-1$, dann ist σ durch $j + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ eindeutig bestimmt. Somit definiert man eine injektive Abbildung

$$\varphi : \mathrm{Aut}(L/K) \longrightarrow \mathbb{Z}/n\mathbb{Z}, \sigma \mapsto j + n\mathbb{Z}\,.$$

Wir zeigen nun, dass σ ein Homomorphismus von Gruppen ist. Seien also $\sigma, \tau \in \mathrm{Aut}(L/K)$ und sein $0 \leqslant j, k \leqslant n-1$ mit $\sigma(b) = z^j b$ und $\tau(b) = z^k b$. Dann ist

$$\tau\sigma(b) = \tau(z^j b) = z^j \tau(b) z^{jk} b = z^{j+k} b =$$

und daraus folgt, dass

$$\varphi(\tau\sigma) = (j+k) + n\mathbb{Z} = (j + n\mathbb{Z}) + (k + n\mathbb{Z}) = \varphi(\sigma) + \varphi(k) = \varphi(k) + \varphi(\sigma).$$

ist, wie verlangt. Somit ist

$$\mathrm{Aut}(L/K) \cong \varphi(\mathrm{Aut}(L/K)) \leqslant \mathbb{Z}/n\mathbb{Z}$$

und muss daher zyklisch sein.

(b) ist klar.

(c) Schreibe $\mathrm{Aut}(\widetilde{L}/K) = \langle\sigma\rangle$. Wegen $[\widetilde{L} : K] = |\mathrm{Aut}(\widetilde{L}/K)| = n$ sind die Automorphismen $\sigma^0, \sigma^1, \ldots, \sigma^{n-1}$ linear unabhängig über K. Insbesondere ist

$$\sum_{i=0}^{n-1} z\sigma^i \neq 0\,.$$

Somit existiert $x \in \widetilde{L}$ mit $b := \sum_{i=0}^{n-1} z\sigma^i(x) \neq 0$ und es ist

$$\sigma(b) = \sum_{i=0}^{n-1} z\sigma^{i+1}(x) = z^{-1} b\,,$$

so dass

$$\sigma(b^n) = z^{-n} b^n = b^n\,.$$

Somit ist $\tau(b^n) = b^n$ für jedes Element $\tau \in \mathrm{Aut}(\widetilde{L}/K)$. Da $\widetilde{L}/K$ eine Galois-Erweiterung ist, folgt also $b^n \in K$. Da $\sigma^r(b) = z^{-r}b$ $(0 \leqslant r \leqslant n-1)$ induzieren die σ^r $(0 \leqslant r \leqslant n-1)$, durch Einschränkung, n verschiedene K-Automorphismen von $K(b)$. Da $[\widetilde{L} : K] = n$ ist und folgt daraus $\widetilde{L} = K(b)$. ■

27.2 Metazyklische Erweiterungen

Definition 27.8 (*(p-)metazyklische Körpererweiterung*)

Sei p eine Primzahl. Eine Körpererweiterung L/K heißt:

(a) **metazyklisch**, wenn eine Kette $K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_r = L$ von Zwischenkörpern $Z_1, \ldots, Z_{r-1}$ $(r \in Z_{\geqslant 0})$ existiert, sodass Z_1/Z_{i-1} $(\forall\ 1 \leqslant i \leqslant r)$ zyklisch ist;

(b) ***p*-metazyklisch**, wenn sie metazyklisch ist, und Z_i/Z_{i-1} ist zyklisch vom Grad p $(\forall\ 1 \leqslant i \leqslant r)$.

Aus Algebra I wissen wir: Eine Galois-Erweiterung L/K ist genau dann zyklisch, wenn $\mathrm{Gal}(L/K)$ eine zyklische Gruppe ist.

Lemma 27.9

Ist L/K eine Galois-Erweiterung, so gelten:

(a) L/K ist metazyklisch $\Leftrightarrow$ $\mathrm{Gal}(L/K)$ ist auflösbar; und

(b) L/K ist p-metazyklisch $\Leftrightarrow$ $\mathrm{Gal}(L/K)$ ist eine p-Gruppe.

Beweisidee: Das Lemma folgt direkt aus der Galois-Korrespondenz!!

z. B. zu (a): „ $\Rightarrow$ “ Wir nehmen an L/K ist metazyklisch, also gibt es eine Kette $K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_r = L$ von Zwischenkörpern $Z_1, \ldots, Z_{r-1}$ $(r \in Z_{\geqslant 0})$, sodass Z_1/Z_{i-1} $(\forall\ 1 \leqslant i \leqslant r)$ zyklisch ist; das heißt $\mathrm{Gal}(Z_i/Z_{i-1})$ ist ebenfalls zyklisch $(\forall\ 1 \leqslant i \leqslant r)$. Die Galois-Korrespondenz besagt, dass man damit eine Normalreihe von $\mathrm{Gal}(L/K)$ hat, wobei alle Faktoren zyklisch sind, also $\mathrm{Gal}(L/K)$ auflösbar ist.

„ $\Leftarrow$ “ Die Rückrichtung funktioniert analog mit einer Normalreihe von $\mathrm{Gal}(L/K)$ mit zyklischen Faktoren und das Bilden des Fixkörper durch die Galois-Korrespondenz.

(b) Analog: mit „zyklisch von Primzahlordnung“ statt „zyklisch“ ■

Wir brauchen noch das folgende Hilfslemma:

Lemma 27.10 (*Verschiebungssatz für Galois-Erweiterungen*)

Sei L/K eine Körpererweiterung. Seien $Z_1 \subseteq Z_2$ und Z drei Zwischenkörper von L/K. Dann gelten:

(a) Z_2/Z_1 ist Galois $\Rightarrow$ ZZ_2/ZZ_1 ist Galois;

(b) $$\begin{array}{rccc} \sum_{1,2} : \mathrm{Gal}(ZZ_2/ZZ_1) & \hookrightarrow & \mathrm{Gal}(Z_2/Z_1) \\ \sigma & \mapsto & \sigma|_{Z_2}. \end{array}$$
ist ein injektiver Homomorphismus von Gruppen.

Beweis: **(a)** Wir nehmen an, Z_2/Z_1 ist Galois. Aus Algebra I wissen wir, dass Z_2 der Zerfällungskörper eines seperablen Polynoms $f \in Z_1[X]$ ist. Somit entsteht ZZ_1 durch Adjunktion der Nullstellen von f an ZZ_1. Also ist ZZ_2/ZZ_1 normal und endlich, sowie seperabel, weil f seperabel über ZZ_1 ist. Das heißt ZZ_2/ZZ_1 ist Galois.

(b)
- $\sum_{1,2}$ ist ein Homomorphismus von Gruppen: Klar, weil es sich nur um die Einschränkung auf Z_2 handelt.
- $\sum_{1,2}$ ist wohldefiniert: $\sigma \in \mathrm{Aut}(ZZ_2)$ mit $\sigma|_{Z_2} = \mathrm{id}|_{Z_1}$
  $\Rightarrow \sigma|_{Z_2} \in \mathrm{Aut}(Z_2)$ und $\left(\sigma|_{Z_2}\right)\big|_{Z_1} = \mathrm{id}|_{Z_1}$
- $\sum_{1,2}$ ist injektiv: klar, weil σ durch die Bilder der Nullstellen von f eindeutig bestimmt ist ■

Satz 27.11

Sei p eine Primzahl. Sei L/K eine Körpererweiterung. Dann gelten:

(a) Sind Z_1, Z_2 Zwischenkörper von L/K mit Z_1/K und Z_2/K metazyklisch (bzw. p-metazyklisch), so ist auch Z_1Z_2/K metazyklisch (bzw. p-metazyklisch).

(b) Ist L/K metazyklisch (bzw. p-metazyklisch) und N die Galois-Hülle von L/K, dann ist $\mathrm{Gal}(N/K)$ auflösbar (bzw. eine p-Gruppe).

Beweis: **(a)** Seien

$$K = K_0^{(i)} \subseteq K_1^{(i)} \subseteq \cdots \subseteq K_{r_i}^{(i)} = Z_i \qquad \text{für } i = 1, 2$$

Körperketten mit zyklischen Teilerweiterungen (bzw. vom Grad p).
Dann ist

$$K = K_0^{(1)} \subseteq K_1^{(1)} \subseteq \cdots \subseteq K_{r_1}^{(1)} = Z_1 \subseteq Z_1K_1^{(2)} \subseteq Z_2K_2^{(2)} \subseteq \cdots \subseteq Z_1K_{r_2}^{(2)} = Z_1Z_2$$

eine Körperkette mit $Z_1K_j^{(2)}/Z_iK_{j-1}^{(2)}$ $(\forall 1 \leqslant j \leqslant r_2)$ zyklisch (bzw. vom Grad p) nach Lemma 27.10.
Das heißt Z_1Z_2/K ist metazyklisch (bzw. p-metazyklisch).

(b) Der Körper N ist nach Definition ein Kompositum von endlich vielen Erweiterungen von K (die alle zu L konjugierte Körper sind) $\left(N = \prod_{i=1}^{t} W_i\right)$, die alle auch metazyklisch (bzw. p-metazyklisch) sind $\Rightarrow N/K$ ist Galois und metazyklisch (bzw. p-metazyklisch).
$\xRightarrow{\text{Lemma 27.9}}$ $\mathrm{Gal}(N/K)$ ist auflösbar (bzw. eine p-Gruppe). ■

Nun kennen wir alle notwendigen Sätze, um endlich zum dem Satz von Galois zurückzukehren.

Satz 27.12 (Galois)

Sei $K \subseteq \mathbb{C}$ ein Körper. Sei $f \in K[X]$ ein nicht-konstantes Polynom und sei L ein Zerfällungskörper von f. Dann gilt:

$$f \text{ ist durch Radikale auflösbar} \quad \Leftrightarrow \quad \mathrm{Gal}(L/K) \text{ ist auflösbar}.$$

Beweis: Wir können annehmen, dass f irreduzibel ist, weil das Ergebnis sonst aus Konkatenation der Körperketten und Normalreihen für die irreduziblen Faktoren folgt.

„⇐“ Wir nehmen an, dass $\mathrm{Gal}(L/K)$ auflösbar ist. Es gibt daher eine Normalreihe

$$\mathrm{Gal}(L/K) = N_0 \trianglerighteqslant N_1 \trianglerighteqslant \cdots \trianglerighteqslant N_t = 1\,,$$

wobei die Faktoren N_{i-1}/N_i zyklisch von Primzahlordnung sind, etwa $|N_{i-1} : N_i| =: p_i \in \mathbb{P}$ $(\forall\ 1 \leqslant i \leqslant t)$. Durch Bildung des Fixkörpers liefert die Galois-Korrespondenz eine Zwischenkörperkette

$$K = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_t = L$$

mit Z_i/Z_{i-1} zyklisch vom Grad p_i $(\forall\ 1 \leqslant i \leqslant t)$. Ist nun $n = [L : K]$ und K' der n-te Kreisteilungskörper über K. Aus der Algebra I wissen wir, dass K' wegen $n = p_1 \cdots p_t$ (und $\mathrm{Char}(K) = 0$) neben den n-ten Einheitswurzeln auch die p_i-ten Einheitswurzeln enthält. Wir können also die Körperkette

$$K' = K'Z_0 \subseteq K'Z_1 \subseteq \cdots \subseteq K'Z_t = K'L$$

betrachten. Nach Lemma 27.10 sind die Erweiterungen $K'Z_i/K'Z_{i-1}$ zyklisch $(\forall\ 1 \leqslant i \leqslant t)$. Nach Satz 27.7 existieren für $i = 1, \ldots, n$ Elemente $b_i \in K'Z_i$ mit $K'Z_{i-1}(b_i) = K'Z_i$ und $b_i^{m_i} \in K'Z_{i-1}$ für geeignete $m_i \in \mathbb{N}$ $(\forall\ 1 \leqslant i \leqslant t)$. Per Definition ist $K'L/K'$ also eine Radikalerweiterung. Da auch K'/K radikal ist, muss auch $K'L/K$ radikal sein, wie gewünscht.

„⇒“ Wir nehmen an, dass f durch Radikale auflösbar ist; also hat f eine Nullstelle (etwa x_0) in einer echter Radikalerweiterung $\tilde{L}/K$. Per Definition gibt es $b_1, \ldots, b_t \in \tilde{L}$, $r_1, \ldots, r_t \in \mathbb{N}$ mit $b_1^{r_1} \in K$ und $b_i^{r_1} \in K(b_1, \ldots, b_{i-1})$ $(\forall\ 2 \leqslant i \leqslant t)$. Wir setzen nun $Z_i = K(b_1, \ldots, b_{i-1})$ $(\forall\ 1 \leqslant i \leqslant t)$ und $Z_0 := K$, damit haben wir die Körperkette:

$$\underbrace{K}_{=:Z_0} \subseteq \underbrace{K(b_1)}_{=:Z_1} \subseteq \cdots \subseteq \underbrace{K(b_1, \ldots, b_i)}_{=:Z_i} \subseteq \cdots \subseteq \underbrace{K(b_1, \ldots, b_t)}_{=:Z_t} = \tilde{L}$$

Weiter sei $n := r_1 \cdots r_t$ und sei K' der n-te Kreisteilungskörper über K. Insbesondere enthällt K_i auch alle r_i-ten Einheitswurzeln $(\forall\ 1 \leqslant i \leqslant t)$. Die Zwischenkörperkette

$$K \subseteq K' \subseteq K'Z_1 \subseteq \cdots \subseteq K'Z_t = K'\tilde{L}$$

erfüllt dann:

- $K'Z_i/K'Z_{i-1}$ ist zyklisch $(\forall\ 1 \leqslant i \leqslant t)$;
- K'/K ist abelsch (Algebra I).

Also ist $K'\tilde{L}/K$ metazyklisch, wonach zusammen mit dem Satz 27.11 $\mathrm{Gal}(N/K)$ auflösbar ist, mit N als Galois-Hülle. Der Zerfällungskörper L von f über K ist ein Zwischenkörper von N/K. Schließlich ist N/K Galois und damit $\mathrm{Gal}(L/K)$ auflösbar, weil dies nach der Galois-Korrespondenz eine Faktorgruppe von $\mathrm{Gal}(N/K)$ ist. ∎

Anhang

In diesem Anhang finden Sie Begriffe und Ergebnisse aus anderen Vorlesungen, die besonders wichtig für die Algebra II sind. Sie sind aber nicht Klausurrelevant.

A Mengenlehre: Zorns Lemma

Definition A.1 (*Halbordnung, Kette, obere Schranke, maximales Element*)

(a) Eine **Halbordnung** (auch Partialordnung, Teilordnung oder partielle Ordnung) auf einer Menge X ist eine Relation „$\leqslant$“, die reflexiv, transitiv und antisymmetrisch ist.

(b) Eine Teilmenge $C \subseteq X$ heißt dann eine **Kette** (bzgl. $\leqslant$), wenn $\forall\, x, y \in C$ eine der Relationen $x \leqslant y$ oder $y \leqslant x$ gilt.

(c) Die Kette C hat eine **obere Schranke** in X, wenn $\exists\, x \in X$ mit $y \leqslant x\ \forall\, y \in C$.

(d) Ein **maximales Element** von X (bzgl. $\leqslant$) ist ein Element $x \in X$, sodass gilt:
$x \in X$ mit $x \leqslant m \quad \Longrightarrow \quad x = m$.

Lemma A.2 (Zorns Lemma)

Sei $X \neq \varnothing$ eine Menge mit einer Halbordnung $\leqslant$. Hat jede Kette $C \subseteq X$ eine obere Schranke in X, so besitzt X ein maximales Element bzgl. $\leqslant$.

Hier: Ohne Beweis! (Dies wird in einer Vorlesung zur Mengenlehre bewiesen.)

Anmerkung A.3

(1) Der Beweis ist nicht konstruktiv!

(2) In der Tat: **Zorns Lemma** ist äquivalent zum **Auswahlaxiom**.

(3) Mithilfe des Zornschen Lemmas lässt sich beispielsweise in der Linearen Algebra einen Beweis führen, dass **jeder K-Vektorraum eine K-Basis besitzt** (Satz von De Hamel).