



Skript Höhere Algebra I

Mitschrift der Vorlesung „Höhere Algebra I“ von Prof. Dr. Dr. Katrin Tent

Jannes Bantje

31. Mai 2014

Erstellt mit \LaTeX

Inhaltsverzeichnis

1 Gruppentheorie: Wiederholung, Sylow-Sätze, Kompositionsreihen	2
1.1 Definition: Gruppenwirkung	2
1.2 Bemerkung über eine Abbildung $G/G_x \rightarrow G(x)$	2
1.3 Beispiele für Gruppenwirkungen	2
1.4 Bahnengleichung	3
1.5 Klassengleichung	3
1.6 Korollar: p -Gruppen haben ein nichttriviales Zentrum	3
1.7 Definition: p -Sylowgruppe	3
1.8 Satz (Sylow)	3
1.9 Satz (Frattini-Argument)	4
1.10 Bemerkung zu p -Sylowgruppen in Normalteilern und Faktorgruppen	4
1.11 Definition: Normalreihe und Kompositionsreihe	5
1.12 Beispiel zu Normalreihen	5
1.13 Ziel: Satz von Jordan-Hölder	5
1.14 Schmetterlings-Lemma (Zassenhaus)	5
1.15 Satz von Schreier	6
1.16 Definition: Auflösbare und nilpotente Gruppen	6
1.17 Bemerkung: Nilpotente Gruppen sind auflösbar, Umkehrung gilt nicht	6
1.18 Satz: Auflösbare Untergruppen, Quotienten und Produkten auflösbarer Gruppen	6
1.19 Korollar: Auflösbare ist äquivalent zur Auflösbare von Normalteilern und Quotienten	7
1.20 Korollar: Das Produkt auflösbarer Normalteiler ist auflösbar	7
1.21 Satz: Untergruppen und Quotienten nilpotenter Gruppen	7
1.22 Satz: Endliche p -Gruppen sind nilpotent	7
1.23 Definition: Kommutator	8
1.24 Satz: Eigenschaften der Kommutatorgruppe	8
1.25 Definition: Konstruktion weiterer Kommutatorgruppen	8
1.26 Satz: Auflösbare einer Gruppe G	8
1.27 Definition: Untere Zentralreihe	8
1.28 Satz: Charakterisierung von Nilpotenz über die untere Zentralreihe	9

1.29	Einschub über direkte und semidirekte Produkte	9
2	Moduln: Halbeinfache Moduln, freie Moduln	10
2.1	Satz: Jeder Ring ist isomorph zu einem Endomorphismenring	10
2.2	Definition: Modul	10
2.3	Beispiele für Moduln	10
2.4	Definition: Untermodul, einfache Moduln und Ringe	11
2.5	Definition: erzeugte Untermoduln	11
2.6	Bemerkung zu Modulstrukturen auf Quotienten	11
2.7	Definition: Klasse der R -Moduln, R -Modul-Homomorphismen	11
2.8	Bemerkung zu $\text{Hom}_R(M, N)$	11
2.9	Satz (Isomorphiesätze)	12
2.10	Definition: Exakte Sequenz	12
2.11	Definition: noethersch und artinsch	12
2.12	Proposition: noethersch \iff alle Untermoduln endlich erzeugt	13
2.13	Satz: noethersch (artinsch) innerhalb einer kurzen exakten Sequenz	13
2.14	Korollar: Endliche Summen noetherscher Moduln sind noethersch (artinsch)	13
2.15	Korollar: Moduln über einen noetherschen Ring sind noethersch	13
2.16	Korollar: Endlich erzeugte Moduln über einem Hauptidealring	14
2.17	Definition: Halbeinfacher Modul	14
2.18	Beispiele halbeinfacher Moduln	14
2.19	Satz: Äquivalenzen zu halbeinfach durch Summen aus einfachen Untermoduln	14
2.20	Lemma: Jeder halbeinfache Modul hat einen einfachen Untermodul	15
2.21	Satz: Äquivalenzen zu halbeinfachen R -Moduln	15
2.22	Korollar: M direkte Summe einfacher Untermoduln \Rightarrow Untermodul isomorph zu Teilsumme	15
2.23	Korollar (Krull-Remak-Schmidt)	16
2.24	Bemerkung: M endlich erzeugt $\Leftrightarrow M$ endliche direkte Summe einfacher Untermoduln	16
2.25	Satz über Ideale eines Ringes R und Ideale in $M_k(R)$	16
2.26	Satz (Schurs Lemma)	17
2.27	Lemma: Darstellung von $\varphi \in \text{End}_R(M)$ als Matrix	17
2.28	Definition: Entgegengesetzter Ring R^{op}	17
2.29	Satz (Wedderburn, 1. Struktursatz)	17
2.30	Bemerkung: Einfache, nicht-isomorphe R -Moduln	18
2.31	Satz (2. Struktursatz von Wedderburn)	18
2.32	Definition: linear unabhängig und Basen	19
2.33	Definition: Freier Modul	19
2.34	Definition: Freier R -Modul mit Basis der Mächtigkeit $ I $	19
2.35	Satz: Universelle Eigenschaft der freien R -Moduln	19
2.36	Korollar: Über das Spalten einer kurzen Sequenz von R -Moduln	20
2.37	Satz: Jeder R -Modul ist Quotient eines freien R -Moduls	20
2.38	Satz: Äquivalenzen zu: M ist R -Moduln über einem Schiefkörper R	20
2.39	Definition: Invariante Basislänge (IBL)	21
2.40	Lemma: Charakterisierung von IBL mit Matrizen	21
2.41	Satz: Kommutative, noethersche Ringe und Urbilder von Ringhomomorphismen haben IBL	22
2.42	Satz: Für R HIR sind Untermoduln freier R -Moduln frei	22
2.43	Satz: (Smith-Normalform) Invariante Faktoren einer Matrix über einem Hauptidealring	23
2.44	Definition: i -Minoren und Rang	24
2.45	Satz (Elementarteilersatz)	24
2.46	Beispiel: Elementarteilersatz	24
2.47	Definition: Annulatorideal und Torsionselement	25
2.48	Satz: Struktursatz für endlich erzeugte Moduln über HIR	25
2.49	Korollar: Struktursatz für endlich erzeugte abelsche Gruppen	25

2.50 Definition und Satz: Torsionsmodul	25
2.51 Satz: Zerlegung eines endlich erzeugten Moduls in Torsionsmodul und freien Modul . . .	26
2.52 Beispiele für Zerlegungen mit dem Torsionsmodul	26
2.53 Satz: Umformulierung des Struktursatzes für endl. erzeugte abelsche Gruppen	26
3 Tensorprodukte und Algebren	27
3.1 Satz: Universelle Eigenschaft des Tensorproduktes	27
3.2 Bemerkung: Elemente des Tensorproduktes	28
3.3 Proposition: Operationen auf ${}_R\text{Mod}$ durch das Tensorprodukt	28
3.4 Beispiele zu Tensorprodukten	29
3.5 Satz: Tensorprodukt eines R -Moduls und R^n	29
3.6 Korollar: Tensorprodukt von freien Moduln	29
3.7 Korollar: Darstellung der Elemente eines Tensorproduktes mit freiem Modul	29
3.8 Definition: Algebra	30
3.9 Beispiele für Algebren	30
3.10 Weitere Beispiele für Algebren	30
3.11 Definition: Darstellung einer R -Algebra	31
3.12 Korollar: Jede n -dimensionale K -Algebra ist isomorph zu Unter algebra von $M_n(K)$. . .	31
3.13 Satz: Tensorprodukt von Algebren ist eine Algebra	32
3.14 Beispiel: Erweiterung der Skalare	32
4 Darstellungstheorie endlicher Gruppen	33
Index	A
Abbildungsverzeichnis	B

Literatur:

- P.M. Cohn: Basic Algebra, (Further Algebra) Springer
- N. Jacobsen: Basic Algebra I + II
- S. Lang : Algebra, Wiley
- F. Lorenz: Algebra III, Springer

1 Gruppentheorie: Wiederholung, Sylow-Sätze, Kompositionsreihen

1.1 Definition: Gruppenwirkung

- Sei G eine Gruppe, $X \neq \emptyset$ Menge. Eine **Gruppenwirkung** von G auf X ist (gegeben durch) einen Gruppenhomomorphismus $\varphi : G \rightarrow \text{Sym}(X)$. $\ker \varphi$ heißt **Kern der Wirkung**.
- Für $x \in X$ heißt $G_x = \{g \in G \mid g(x) = x\} \leq G$ der **Stabilisator** von x .
- Die **Bahn** von $x \in X$ unter G ist $G(x) = \{g(x) \mid g \in G\} \subseteq X$.
- Eine Gruppenwirkung heißt **transitiv**, wenn $G(x) = X$ für ein $x \in X$.
- Eine Gruppenwirkung heißt **treu**, falls $\ker \varphi = \{1_G\}$.

1.2 Bemerkung

Für jedes $x \in X$ ist die Abbildung $G/G_x \rightarrow G(x)$, $gG_x \mapsto g(x)$ eine Bijektion.

Beweis

Es ist $g(x) = h(x) \iff (h^{-1}g)(x) = (h^{-1}h)(x) = x \iff h^{-1}g \in G_x \iff gG_x = hG_x$. Daher ist die Abbildung wohldefiniert und injektiv. Surjektiv ist klar. \square

Wiederholung Isomorphiesätze¹

- 1. Isomorphiesatz:** Ist $\varphi : G \rightarrow H$ surjektiv, dann ist $H \simeq G/\ker \varphi$. Allgemein ist für jeden Homomorphismus $\varphi : G \rightarrow H$ dann $\text{Im } \varphi \simeq G/\ker \varphi$. (Homomorphiesatz)
- 2. Isomorphiesatz:** Ist $H \leq G, N \trianglelefteq G$, dann ist $H/(H \cap N) \simeq HN/N$. ("erweitern mit N ")
- 3. Isomorphiesatz:** Sind $N, K \trianglelefteq G, N \leq K$, dann ist $G/N/K/N \simeq G/K$. ("kürzen mit N ")

Die letzten beiden Sätze lassen sich mit dem ersten beweisen!

1.3 Beispiel

- (i) (a) G wirkt durch Rechtsmultiplikation auf sich selbst ($X = G$). Dann ist $G_x = \{1\}$ für alle $x \in X$, d.h. die Wirkung ist treu und transitiv. Solche Wirkungen heißen **regulär**.

$$\varphi : G \rightarrow \text{Sym}(G), \quad g \mapsto \rho_g \quad \text{mit} \quad \rho_g(x) = x \cdot g$$

Gruppenhomomorphismus: $\rho_{gh}(x) = x \cdot g \cdot h = \rho_h \circ \rho_g(x)$.

- (b) G wirkt durch Linksmultiplikation auf sich selbst (regulär) $\lambda_g(x) = g^{-1} \cdot x$.

- (ii) G operiert durch Konjugation auf sich selbst, d.h. $\kappa : G \rightarrow \text{Aut}(G) \leq \text{Sym}(G)$, $g \mapsto \kappa_g$, wobei $\kappa_g(x) = g^{-1} \cdot x \cdot g$

$$g \cdot h \mapsto \kappa_{g \cdot h} \quad \kappa_{g \cdot h}(x) = h^{-1} \cdot g^{-1} \cdot x \cdot g \cdot h$$

Dann ist $G_x = \{g \in G \mid g^{-1} \cdot x \cdot g = x\} = Z_G(x)$ der **Zentralisator** von x in G . Der Kern der Wirkung ist das **Zentrum** von G $Z(G) = \{g \in G \mid x \cdot g = g \cdot x \text{ für alle } x \in G\}$.

Bemerkung: $\ker \varphi = \bigcap_{x \in X} G_x$ gilt für alle Gruppenwirkungen $\varphi : G \rightarrow \text{Sym}(X)$.

- (iii) $G = \text{Gl}_n(K)$, K Körper, operiert auf K^n durch lineare Abbildungen.

¹siehe auch <http://de.wikipedia.org/wiki/Isomorphiesatz> \square

1.4 Bahnengleichung

Setze $G(X) = \{G(x) \mid x \in X\}$. Dann ist $X = \dot{\bigcup} \{G(x) \mid G(x) \in G(X)\}$. Falls X endlich ist gilt also

$$|X| = \sum |G(x)| = \sum |G/G_x| = \sum [G : G_x]$$

Insbesondere ist $|G(x)| = |G/G_x| = [G : G_x] = \frac{|G|}{|G_x|}$ falls G endlich ist. (Bijektion aus 1.2)

Spezialfall: Wirkung von G durch Konjugation auf sich selbst. $\kappa_g(x) = g^{-1} \cdot x \cdot g$.

1.5 Klassengleichung

Sei $K_G = \{G(x) \mid x \in G\}$ = Menge der Konjugationsklassen. Sei $K_G^* = \{G(x) \mid x \in G \setminus Z(G)\} = \{G(x) \mid |G(x)| \geq 2\}$. Für jede endliche Gruppe G gilt dann nach 1.4

$$|G| = \sum_{K_G} [G : Z_G(x)] = |Z(G)| + \sum_{K_G^*} [G : Z_G(x)] \quad \square$$

1.6 Korollar

G endlich, $|G| = p^m$, p prim, $m \geq 1 \Rightarrow Z(G) \neq 1$.

Beweis

Nach Lagrange² ist für jedes $x \in G$ $|Z_G(x)| = p^k$ für ein $k \leq m$, also ist $[G : Z_G(x)] = p^{m-k}$. Wegen $p \mid |G|$ und $|Z(G)| \geq 1$ folgt $p \mid |Z(G)|$. \square

1.7 Definition

Sei G eine endliche Gruppe, $|G| = p^a \cdot m$ mit $(m, p) = 1$ und p prim. Dann heißt eine Untergruppe $H \leq G$ mit $|H| = p^a$ eine **p -Sylowgruppe** von G .

1.8 Satz (Sylow)

Sei G eine endliche Gruppe, p prim, $|G| = p^a \cdot m$ mit $(p, m) = 1$. Dann gilt

- (i) Jede p -Untergruppe von G ist in einer p -Sylowgruppe enthalten. Insbesondere existieren p -Sylowgruppen immer.
- (ii) Ist $n_p = \#$ p -Sylowgruppen von G , dann gilt: $n_p \mid m$ und $n_p \equiv 1 \pmod{p}$.
- (iii) Alle p -Sylowgruppen sind konjugiert.

Beweis

Sei $S := \{X \subset G \mid |X| = p^a\}$. G operiert auf S durch Rechtsmultiplikation. Es ist

$$|S| = \binom{p^a \cdot m}{p^a} = \frac{p^a \cdot m \cdot (p^a \cdot m - 1) \cdot \dots \cdot (p^a \cdot m - (p^a - 1))}{1 \cdot 2 \cdot \dots \cdot p^a - 1 \cdot p^a}$$

Behauptung: $p \nmid |S|$. Betrachte dazu $k_i := \frac{p^a \cdot m - i}{i}$, für $1 \leq i < p^a$. Wenn $p^j \mid p^a \cdot m - i$, dann ist $j < a$ und $p^j \mid i$. Daher sind $p^a \cdot m - i$ und i durch dieselbe Potenz von p teilbar, d.h. $p \nmid k_i$. Damit ist $p \nmid m \cdot k_1 \cdot \dots \cdot k_{p^a-1} = |S|$.

²Ordnung einer Untergruppe teilt die Gruppenordnung. Die Umkehrung gilt nicht!

siehe
Bahnengleichung
1.4

Daher existiert eine G -Bahn $S_1 \subseteq S$ mit $p \nmid |S_1|$. Wähle $X \in S_1$, d.h. $|X| = p^a$. Setze $P := G_X$. Dann ist

$$|S_1| = [G : G_X] = [G : P]$$

Daher gilt $p \nmid |G/P|$, also $p^a \mid |P|$. Andererseits ist $|P| \leq p^a$, denn für $x \in X, g \in P$ ist $x \cdot g \in X$ und die $x \cdot g$ für $g \in P$ sind paarweise verschieden. Daher ist $|P| = p^a$ und P eine p -Sylowgruppe.

Sei nun $T \subseteq S$ die Menge aller Konjugierten von P unter der Konjugationswirkung. Dann operiert auch P durch Konjugation auf T . Nach der Bahnengleichung (1.4) hat jede Bahn die Länge p^i für ein $i \leq a$. Offensichtlich ist P ein Fixpunkt dieser Wirkung. Ist $P_1 \in T$ ein weiterer Fixpunkt, dann ist $P \subseteq N_G(P_1)$, daher ist $P \cdot P_1 \leq G$. Wegen³ $|P \cdot P_1| = \frac{|P| \cdot |P_1|}{|P \cap P_1|}$ ist $P \cdot P_1$ eine p -Untergruppe von G . Wegen $P \leq P \cdot P_1$ und $p \nmid m$ folgt $P = P \cdot P_1 = P_1$. Daher ist $|T| \equiv 1 \pmod{p}$.

Noch zu zeigen: T enthält alle Sylowgruppen und jede p -Gruppe ist in einer p -Sylowgruppe enthalten. Sei $P_2 \leq G$ eine p -Sylowgruppe mit $P_2 \notin T$. Dann operiert auch P_2 durch Konjugation auf T . Wenn P_2 auf T einen Fixpunkt $P' \in T$ hat, dann ist wie eben $P_2 \cdot P'$ eine p -Untergruppe und dann $P_2 = P_2 \cdot P' = P' \in T$ ∇ . Daher hat P_2 auf T keinen Fixpunkt. Dann folgt aber $p \mid |T|$ ∇ . Damit sind alle p -Sylowgruppen in T enthalten, d.h. $|T| \equiv 1 \pmod{p}$.

Ist $H \leq G$ eine p -Untergruppe, dann operiert auch H durch Konjugation auf T . Wegen $p \nmid |T|$ muss H einen Fixpunkt $P' \in T$ besitzen, dann folgt $H \cdot P' = P'$, d.h. $H \leq P'$.

Weil G durch Konjugation transitiv auf T operiert, folgt

$$n_p = |T| = [G : N_G(P)] \mid [G : P] = m. \quad \square$$

Bemerkung

Wenn G nur eine p -Sylowgruppe $P \leq G$ besitzt, dann ist $P \trianglelefteq G$.

1.9 Satz (Frattini-Argument)

Ist G eine beliebige Gruppe, $H \trianglelefteq G$ endlich und $P \leq H$ eine p -Sylowgruppe von H . Dann ist $G = N_G(P) \cdot H$, wobei $N_G(P) = \{g \in G \mid P^g = g^{-1} \cdot P \cdot g = P\}$.

Beweis

Sei $g \in G$. Dann ist $P^g \leq H^g = H$ eine p -Sylowgruppe von H . Daher existiert ein $h \in H$ mit $P^g = P^h$. Dann ist $P = P^{g \cdot h^{-1}}$, d.h. $g \cdot h^{-1} \in N_G(P)$. Damit ist

$$g = \underbrace{g \cdot h^{-1}}_{\in N_G(P)} \cdot \underbrace{h}_{\in H} \quad \square$$

Bemerkung

Sind $H_1, H_2 \leq G$, $H_2 \leq N_G(H_1)$, dann ist $H_1 \cdot H_2 = H_2 \cdot H_1 \leq G$.

1.10 Bemerkung

Offensichtlich gilt für eine endliche Gruppe G , $P \leq G$ p -Sylowgruppe, $N \trianglelefteq G$

- (i) $P \cap N$ ist p -Sylowgruppe von N (ii) $P \cdot N / N$ ist p -Sylowgruppe von G/N .

Beweis

Es ist $|N : P \cap N| \stackrel{2, \text{Iso}}{=} |PN : P|$ teilerfremd zu p und $P \cap N$ ist p -Untergruppe von N . Wegen $G/N / PN/N \simeq G/PN$ ist $|G : PN| \mid |G : P|$ teilerfremd zu p . Wegen $|PN : N| = |P : (P \cap N)|$ ist PN/N eine p -Gruppe. \square

³ $P \cdot P_1$ ist Untergruppe, da P, P_1 normalisiert

1.11 Definition

Eine Folge von Untergruppen $(H_i)_{0 \leq i \leq n}$ mit $H_0 = G$, $H_n = \{1_G\}$, $H_{i+1} \trianglelefteq H_i$ heißt **Normalreihe** in G . Ist H_i/H_{i+1} einfach für alle $i < n$, dann heißt die Folge **Kompositionsreihe**. Zwei Normalreihen $(H_i)_{i \leq n}$, $(K_j)_{j \leq m}$ heißen **äquivalent**, falls $n = m$ und die auftretenden Quotienten $(H_i/H_{i+1})_{i \leq n-1}$ nach geeigneter Permutation isomorph sind zu dem Quotienten $(K_j/K_{j+1})_{j \leq n-1}$.

1.12 Beispiel

$$\begin{aligned} \mathbb{Z}_6 &\simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \triangleright \mathbb{Z}_3 \triangleright \{1\} \\ &\triangleright \mathbb{Z}_2 \triangleright \{1\} \end{aligned}$$

Bemerkung

- (i) Nicht jede Gruppe besitzt eine Kompositionsreihe, zB. \mathbb{Z} hat *keine* Kompositionsreihe.
- (ii) Eine Normalreihe ist genau dann Kompositionsreihe, wenn es keine echte Verfeinerung gibt. Insbesondere hat also jede endliche Gruppe eine Kompositionsreihe.

1.13 Ziel: Satz von Jordan-Hölder

Sei G eine Gruppe mit Kompositionsreihen $(H_i)_{i \leq n}$ und $(K_j)_{j \leq m}$. Dann sind die Reihen äquivalent.

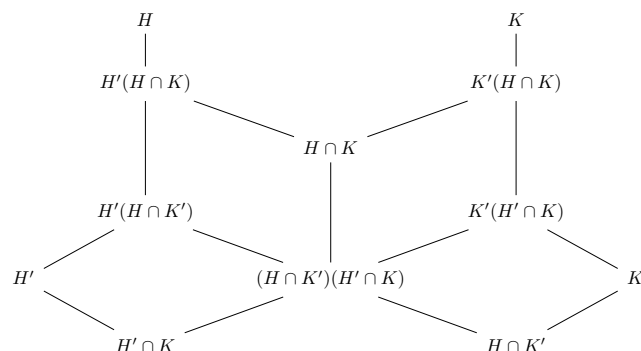
Für den Beweis brauchen wir

1.14 Schmetterlings-Lemma (Zassenhaus)

Sei G eine Gruppe, $H, K \leq G$ und $H' \trianglelefteq H, K' \trianglelefteq K$. Dann ist

$$H'(H \cap K') \trianglelefteq H'(H \cap K) \quad \text{und} \quad K'(K \cap H') \trianglelefteq K'(K \cap H)$$

und die Quotienten sind isomorph.



Beweis

Setze $N := H \cap K$ und $M := H'(H \cap K')$. Dann gilt $N \leq N_G(M)$ wegen $H' \trianglelefteq H, K' \trianglelefteq K$ und daher $M \trianglelefteq N \cdot M = H'(H \cap K)$.

Behauptung: Es ist $N \cap M = (H \cap K) \cap (H'(H \cap K')) = (H' \cap K)(H \cap K')$.

" \subseteq ": Sei $h' \cdot k \in H \cap K$ mit $h' \in H'$ und $k \in H \cap K' \Rightarrow h' \cdot k \in (H' \cap K)(H \cap K')$

" \supseteq ": $h' \cdot k$ mit $h' \in H' \cap K$ und $k \in H \cap K'$, dann ist $h' \cdot k \in H \cap K$.

Daher ist

$$NM/M = H'(H \cap K')(H \cap K)/H'(H \cap K) \cong N/N \cap M \cong (H \cap K)/(H' \cap K)(H \cap K')$$

(so steht es in den Notizen). Besser finde ich:

$$NM/M \stackrel{2. \text{ Iso}}{\cong} N/N \cap M = (H \cap K)/(H' \cap K)(H \cap K')$$

Die rechte Seite ist symmetrisch in H und K . Daher sind beide Quotienten im Lemma isomorph zu $N/N \cap M$ und das Lemma ist bewiesen. \square

Damit zeigen wir
nun folgenden Satz:

1.15 Satz von Schreier

Sind $(H_i)_{i \leq n}, (K_j)_{j \leq m}$ Normalreihen in G , dann existieren äquivalente Verfeinerungen.

Beweis

Für $j = 1, \dots, m-1, i = 0, \dots, n-1$ setze

$$H'_{im+j} := H_{i+1}(H_i \cap K_j)$$

und für $i = 0, \dots, n$ sei

$$H'_{im} := H_i = H_{i+1}(H_i \cap K_0) = H_i(H_{i-1} \cap K_m).$$

Für $i = 1, \dots, n-1, j = 0, \dots, m-1$ setze dementsprechend $K'_{jn+i} := K_{j+1}(K_j \cap H_i)$ und $K'_{jn} := K_j(= K_{j+1}(K_j \cap H_0) = K_j(K_{j-1} \cap H_n))$ für $j = 0, \dots, m$.

Nach dem Zassenhaus-Lemma (1.14) sind dann

$$H'_{im+j}/H'_{im+j+1} \simeq K'_{jn+i}/K'_{jn+i+1}$$

und damit sind diese Verfeinerungen äquivalent. Damit folgt der Satz von Jordan-Hölder: Kompositionsreihen haben keine echten Verfeinerungen, müssen also bereits äquivalent sein! \square

reviewed 22.4.14

1.16 Definition

Eine Gruppe heißt **auflösbar**, wenn sie eine abelsche Normalreihe besitzt, d.h. eine Normalreihe mit abelschen Quotienten. Eine Gruppe heißt **nilpotent**, wenn es eine Normalreihe $(H_i)_{i \leq n}$ gibt mit $H_i \trianglelefteq G$ und $H_i/H_{i+1} \leq Z(G/H_{i+1})$.

1.17 Bemerkung

Jede nilpotente Gruppe ist auflösbar, aber nicht umgekehrt: S_3 ist auflösbar $1 \trianglelefteq \langle (123) \rangle \trianglelefteq S_3$, aber $Z(S_3) = 1$, d.h. S_3 ist *nicht* nilpotent.

1.18 Satz

Untergruppen und Quotienten auflösbarer Gruppen sind auflösbar, direkte Produkte auflösbarer Gruppen sind ebenfalls auflösbar.

Beweis

Ist $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ abelsche Normalreihe, $H \leq G$, dann ist $1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \dots \trianglelefteq G_n \cap H = H$ abelsche Normalreihe in H , denn

$$(G_{i+1} \cap H)/G_i \cap H \simeq G_i(G_{i+1} \cap H)/G_i \leq G_{i+1}/G_i \text{ ist abelsch.}$$

Ist $N \trianglelefteq G$, dann ist $(G_i N/N)$ abelsche Normalreihe für G/N , denn es ist

$$(G_{i+1} N/N)/(G_i N/N) \simeq G_{i+1} N/G_i N \simeq G_{i+1}/G_i \cap (G_i N)$$

ein Quotient von G_{i+1}/G_i und daher abelsch. (Da $G_i \leq G_{i+1} \cap (G_i N)$, ist $G_{i+1}/G_i \rightarrow G_{i+1}/G_{i+1} \cap (G_i N)$ ein Epimorphismus und daher ist die rechte Seite abelsch.) \square

1.19 Korollar

Sei $N \trianglelefteq G$. Dann ist G auflösbar genau dann, wenn N und G/N auflösbar sind.

Beweis

" \Rightarrow ": 1.18

" \Leftarrow ": klar: Wir können die abelschen Normalreihen für N und G/N zusammensetzen:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_k = N, \quad K_0/N = N \trianglelefteq K_1/N \trianglelefteq \dots \trianglelefteq K_m/N = G/N$$

Setze $1 = H_0 \trianglelefteq \dots \trianglelefteq H_k = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_m = G$. Wegen $(K_{i+1}/N)/(K_i/N) \simeq K_{i+1}/K_i$. \square

1.20 Korollar

Sind $M, N \trianglelefteq G$ auflösbar, dann auch MN auflösbar.

Beweis

$MN/N \simeq M/M \cap N$ ist auflösbar. Nach 1.19 ist MN auflösbar. \square

Einschub: Direktes Produkt

Sind G, H Gruppen, dann ist das direkte Produkt $G \times H$ die Gruppe mit Multiplikation

$$(g, h) \cdot (g', h') = (g \cdot g', h \cdot h')$$

1.21 Satz

Untergruppen und Quotienten nilpotenter Gruppen sind wieder nilpotent, die Produkte nilpotenter Gruppen sind nilpotent.

Beweis

Wie Satz 1.18:

Ist $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$ Zentralreihe, $H \leq G$, dann ist $1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \dots \trianglelefteq G_n \cap H = H$ Zentralreihe in H , denn

$$(G_{i+1} \cap H)/(G_i \cap H) \stackrel{2. \text{ Iso}}{\simeq} G_i(G_{i+1} \cap H)/G_i \leq G_{i+1}/G_i \text{ ist abelsch.}$$

Ist $N \trianglelefteq G$, dann ist $(G_i N/N)$ Zentralreihe für G/N , denn es ist

$$(G_{i+1} N/N)/(G_i N/N) \simeq G_{i+1} N/G_i N \simeq G_{i+1}/G_{i+1} \cap (G_i N)$$

ein Quotient von G_{i+1}/G_i und daher abelsch. (Da $G_i \leq G_{i+1} \cap (G_i N)$, ist $G_{i+1}/G_i \rightarrow G_{i+1}/G_{i+1} \cap (G_i N)$ ein Epimorphismus und daher ist die rechte Seite abelsch.) \square

1.22 Satz

Endliche p -Gruppen sind nilpotent.

Beweis

Nach Satz 1.6 ist $H_1 := Z(G) \neq 1$. Da $G/Z(G)$ wieder p -Gruppe ist, ist $Z(G/Z(G)) \neq 1$. Setze

$$H_2 := \pi_{Z(G)}^{-1}(Z(G/Z(G))) \text{ usw.}$$

Nach endlich vielen Schritten ist $H_k = G$. Es gilt dann

$$H_{i+1}/H_i = Z(G/H_i)$$

d.h. die H_i bilden die **obere Zentralreihe**.

1.23 Definition

Für $a, b \in G$ heißt $[a, b] = a^{-1} \cdot b^{-1} \cdot a \cdot b$ der **Kommutator** von a und b .

- (i) Es ist $a \cdot b = b \cdot a \cdot [a, b]$ und $[a, b] = 1$, genau dann wenn $a \cdot b = b \cdot a$.
- (ii) Ist $\varphi : G \rightarrow H$, dann ist $\varphi([a, b]) = [\varphi(a), \varphi(b)]$.
- (iii) Produkte von Kommutatoren sind nicht unbedingt selber wieder ein Kommutator!

Für Untergruppen $H, K \leq G$ setze $[K, H] := \langle [k, h] \mid k \in K, h \in H \rangle$. Ist $K \leq N_G(H)$, dann ist $[K, H] \leq H$, denn $k^{-1} \cdot h^{-1} \cdot k \cdot h = (h^{-1})^k \cdot h \in H$. Die Gruppe $G' = [G, G] = \langle [g, h] \mid g, h \in G \rangle$ heißt **Kommutatorgruppe** von G .

1.24 Satz

- (i) $G' \trianglelefteq G$
- (ii) G/G' ist abelsch.
- (iii) Ist $\varphi : G \rightarrow A$ ein Gruppenhomomorphismus und A abelsch, dann ist $G' \leq \ker \varphi$.

Beweis

- (i) Es ist $g^{-1}[a, b]g = [a^g, b^g]$ nach 1.23 (ii).
- (ii) Klar nach 1.23 (i).
- (iii) Es ist $\varphi([a, b]) = [\varphi(a), \varphi(b)] = 1$, d.h. $G' \leq \ker \varphi$. □

Bemerkung

Mit anderen Worten: G' ist der kleinste Normalteiler von G mit G/G' abelsch, denn ist G/N abelsch, dann ist nach (iii) mit $\varphi : G \rightarrow G/N$, $G' \leq \ker \varphi = N$.

1.25 Definition

Wir setzen $G^{(0)} = G$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Dann ist $G^{(1)} = G'$ und $G^{(i+1)} \trianglelefteq G^{(i)}$, $G^{(i)}/G^{(i+1)}$ abelsch.

1.26 Satz

G ist auflösbar genau dann, wenn $G^{(k)} = 1_G$ für ein $k \geq 0$.

Beweis

" \Leftarrow ": Die $G^{(i)}$ bilden eine abelsche Normalreihe.

" \Rightarrow ": Ist $(N_i)_{i \leq n}$, $N_0 = G$, $N_n = \{1\}$, dann ist mit Induktion $G^{(i)} \leq N_i$ nach voriger Bemerkung, also $G^{(n)} \leq \{1\} = N_n$.

Bemerkung

Damit ist $(G^{(i)})_{i \leq k}$ die am schnellsten absteigende untere Normalreihe für G . k heißt **auflösbare Länge** von G .

1.27 Definition

Die **untere Zentralreihe** einer nilpotenten Gruppe G ist definiert durch $G^{[0]} = G$, $G^{[i]} = [G^{[i-1]}, G]$. Es ist $G^{[i]}/G^{[i+1]} \leq Z(G/G^{[i+1]})$ nach Definition.

1.28 Satz

Eine Gruppe G ist nilpotent genau dann, wenn $G^{[k]} = 1_G$ für ein $k \geq 0$.

Beweis

" \Leftarrow ": Klar nach voriger Bemerkung: $(G^{[i]})_{i \leq k}$ bilden Zentralreihe.

" \Rightarrow ": Ist $1 = N_0 \leq N_1 \leq \dots \leq N_n = G$ eine Zentralreihe, dann ist $G^{[1]} \leq N_{n-1}$, denn G/N_{n-1} ist abelsch. Zeige $G^{[i]} \leq N_{n-i}$ für $i = 1, \dots, n$, denn dann folgt $G^{[n]} = 1$. Weil $N_{n-i}/N_{n-(i+1)} \leq Z(G/N_{n-(i+1)})$ folgt $[N_{n-i}, G] \leq N_{n-(i+1)}$. Nach Induktion ist wegen $G^{[i]} \leq N_{n-i}$ dann

$$G^{[i+1]} = [G^{[i]}, G] \leq [N_{n-i}, G] \leq N_{n-(i+1)}$$

1.29 Einschub über direkte und semidirekte Produkte

- a) Sei G eine Gruppe, $H \leq G$, $N \trianglelefteq G$ ein Normalteiler mit $H \cap N = \{1\}$ und $N \cdot H = G$. Dann ist die Abbildung $\varphi : N \times H \rightarrow G$, $(n, h) \mapsto n \cdot h$ bijektiv, d.h. für jedes $g \in G$ existiert ein eindeutig bestimmtes $n \in N$, $h \in H$ mit $n \cdot h = g$. Dann ist

$$n_1 \cdot h_1 = n_2 \cdot h_2 \iff \underbrace{n_2^{-1}n_1}_{\in N} = \underbrace{h_2 \cdot h_1^{-1}}_{\in H} \in N \cap H = 1$$

Aber: Im Allgemeinen ist φ kein Gruppenhomomorphismus, denn es ist

$$(n_1, h_1)(n_2, h_2) = (n_1, \underbrace{h_1 n_2 h_1^{-1}}_{\in N})(\underbrace{h_1 h_2}_{\in H}) = (n_1 n_2)(n_2^{-1} h_1 n_2 h_2)$$

Daher ist φ ein Gruppenhomomorphismus genau dann, wenn H die Elemente aus N zentralisiert ($n \cdot h = h \cdot n$), d.h. wenn $H \trianglelefteq G$. In dem Fall ist dann $G \simeq N \times H$.

Ist $H \trianglelefteq G$, dann gilt $\varphi(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot n_2, h_1 \cdot h_2)$

- b) Sind H, N, G , $\varphi : H \rightarrow \text{Aut}(N)$ ein Homomorphismus, dann definiere eine Verknüpfung auf der Menge $G = N \rtimes H$ durch

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2), h_1 \cdot h_2)$$

Mit dieser Verknüpfung wird G zu einer Gruppe mit Untergruppen $\{1\} \times H \simeq H$, $N \times \{1\} \simeq N$. Man schreibt $G = N \rtimes H = N \rtimes_{\varphi} H$ für das **semidirekte Produkt**. Mit $\{1\} \times H$ und $N \times \{1\}$ können wir G wie in a) beschreiben. Dabei ist $\varphi : H \rightarrow \text{Aut}(N)$, $h \mapsto \kappa_h$ (Konjugation mit h).

2 Moduln: Halbeinfache Moduln, freie Moduln

Erinnerung

Ringe in Algebra I kommutativ:

- a) Körper, Polynomringe, \mathbb{Z}
- b) nicht kommutative Ringe: R Ring, Matrizenring $M_n(R) = R^{n \times n}$.
Sei A abelsche Gruppe, dann ist $\text{End}(A) = \text{Hom}(A, A)$ ein Ring

$$\begin{aligned}(\varphi + \psi)(x) &= \varphi(x) + \psi(x) \\ (\varphi \cdot \psi)(x) &= \varphi(\psi(x))\end{aligned}$$

$\text{End}(A)$ heißt der **Endomorphismenring** von A . Dies ist das allgemeinste Beispiel, denn es gilt:

2.1 Satz

Jeder Ring R ist isomorph zu einem Ring von Endomorphismen einer abelschen Gruppe.

Beweis

Ist $(R, +, \cdot)$ gegeben, dann ist $A = (R, +)$ eine abelsche Gruppe. Die Abbildung $R \rightarrow \text{End}(A)$, $a \mapsto \lambda_a$ mit $\lambda_a : A \rightarrow A, x \mapsto a \cdot x$ ist ein injektiver Ringhomomorphismus, eingeschränkt auf das Bild also ein Isomorphismus.

2.2 Definition

Sei R ein Ring, $(M, +)$ eine abelsche Gruppe. Eine R -(Links-) **Modulstruktur** auf M ist eine Verknüpfung $R \times M \rightarrow M, (r, m) \mapsto r \cdot m$ mit

- (i) $r(x + y) = r \cdot x + r \cdot y$
- (ii) $(r + s) \cdot x = r \cdot x + s \cdot x$
- (iii) $(r \cdot s)x = r \cdot (s \cdot x)$
- (iv) $1_R \cdot x = x$

für alle $r, s \in R, x, y \in M$. Ist R ein Körper, dann sind R -Moduln genau die R -Vektorräume. Mit anderen Worten: Eine R -Modulstruktur auf M ist (gegeben durch) einen Ringhomomorphismus $\varphi : R \rightarrow \text{End}(M, +)$ mit $r \cdot x = \varphi(r)(x)$.

2.3 Beispiele

- (i) Ist R ein Körper, dann ist ein R -Modul ein R -Vektorraum.
- (ii) $(R, +)$ ist R -Modul durch Produktwirkung, d.h. $\varphi : R \rightarrow \text{End}(R), r \mapsto \lambda_r$.
- (iii) Ist $I \trianglelefteq R$ ein **Ideal** (d.h. für alle $i, j \in I, r \in R$ ist $i + j, i \cdot r, r \cdot i \in I$), dann ist auch $(I, +)$ ein R -Modul, ein R -Untermodul von $(R, +)$.
- (iv) Jede abelsche Gruppe ist ein \mathbb{Z} -Modul.

2.4 Definition

Ist M ein R -Modul, $N \leq M$ Untergruppe mit $r \cdot x \in N$ für alle $x \in N, r \in R$, dann heißt N ein **R -Untermodul** von M .

Beispiel

$\{0\}, M$ sind immer Untermoduln. Ein Modul $M \neq \{0\}$ heißt **einfach** (oder **irreduzibel**), wenn $0, M$ die einzigen Untermoduln sind. Ein Ring R heißt (links-) **einfach**, wenn er als (Links-) R -Modul einfach ist.

Bemerkung

Einfache kommutative Ringe sind genau die Körper. Jedes Ideal in R ist Untermodul, aber nicht jedes Untermodul ist ein Ideal.

2.5 Definition

- Ist $\{N_\alpha\}_{\alpha \in I}$ Menge von Untermoduln von M , dann ist $\bigcap_{\alpha \in I} N_\alpha$ ein Untermodul.
- Ist $\emptyset \neq S \subseteq M$, dann ist $\langle S \rangle = \bigcap_{N \supseteq S} N$ der von S **erzeugte Untermodul**. Der von einer Summe erzeugte Modul ist gegeben durch

$$\sum_{\alpha \in I} N_\alpha = \langle n_{\alpha_1} + \dots + n_{\alpha_k} : \alpha_i \in I, n_{\alpha_i} \in N_{\alpha_i} \rangle$$

Ist S endlich, dann heißt $\langle S \rangle$ **endlich erzeugt**. Ist $|S| = 1$, dann heißt $\langle S \rangle = M$ **zyklisch**.

- Ein einfacher Modul ist zyklisch, aber nicht umgekehrt (zB. \mathbb{Z}).

2.6 Bemerkung

- Ist M ein zyklischer R -Modul, dann ist $M \simeq R/I$ für ein Ideal $I \trianglelefteq R$. (siehe Blatt 3)
- Ist $N \leq M$ ein R -Untermodul, dann ist auch M/N ein R -Modul durch

$$r(m + N) = r \cdot m + N$$

2.7 Definition

Die Klasse aller R -Links-Moduln bezeichnen wir mit ${}_R \text{Mod}$. Sind $M, N \in {}_R \text{Mod}$ und $\varphi : (M, +) \rightarrow (N, +)$ ein Homomorphismus (der additiven Gruppen), dann ist φ ein **R -Modul-Homomorphismus**, falls φ ist R -linear

$$\varphi(r \cdot m) = r \cdot \varphi(m) \quad \varphi(\lambda_r(m)) = \lambda_r(\varphi(m)).$$

2.8 Bemerkung

Kerne und Bilder von R -Modul-Homomorphismen sind R -Untermoduln. Die Menge $\text{Hom}_R(M, N) := \{\varphi : M \rightarrow N \mid \varphi \text{ ist } R\text{-Modul-Homomorphismus}\}$ ist eine abelsche Gruppe mit

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

und $\text{End}_R(M) := \text{Hom}_R(M, M)$ ist mit $(\varphi \cdot \psi)(m) = \varphi(\psi(m))$ der Endomorphismenring von M . Die Homomorphie- und Isomorphiesätze für Gruppen gelten auch für Moduln:

2.9 Satz (Isomorphiesätze)

- (i) Ist $f : M \rightarrow N$ ein R -Modul-Homomorphismus, $M' \subseteq M$ Untermodul mit $M' \subseteq \ker f$, dann existiert ein eindeutiger R -Modul-Homomorphismus $f' : M/M' \rightarrow N$ mit

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow \pi & \nearrow f' & \\ M/M' & & \end{array}$$

und f' ist injektiv genau dann, wenn $M' = \ker f$.

- (ii) Sind $A, B \subseteq M$ Untermoduln, dann gilt

$$(A+B)/B \simeq A/A \cap B$$

- (iii) Ist $M' \subseteq M$ ein Untermodul, dann existiert ein **Verbandsisomorphismus** zwischen den Untermoduln von M , die M' enthalten und den Untermoduln von M/M' , nämlich $N \mapsto N/M'$ und es gilt (vgl. 1.2)

$$(M/M')/(N/M') \simeq M/N$$

Beweis für (i)

Es ist nur nachzurechnen, dass der (einzige mögliche) Gruppenhomomorphismus $f' : M/M' \rightarrow N$, $m + M' \mapsto f(m)$ R -linear ist. Das folgt sofort

$$f'(r(m + M')) = f'(r \cdot m + M') = f(r \cdot m) = r \cdot f(m) = r \cdot f'(m + M')$$

(ii), (iii) Übungsaufgabe. □

2.10 Definition (Sprechweise)

Eine Folge von R -Moduln (M_i) und Homomorphismen $f_i : M_i \rightarrow M_{i+1}$ heißt **exakt in M_i** , falls $\ker f_i = \operatorname{Im} f_{i-1}$.

Eine **exakte Sequenz** ist eine Folge, die überall exakt ist. Eine exakte Sequenz von der Form

$$0 \rightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \rightarrow 0$$

heißt **kurze exakte Sequenz**. Dieses bedeutet f_1 injektiv, f_2 surjektiv und daher ist dann $M_3 \simeq M_2/M_1$.

2.11 Definition

Ein (Links) R -Modul M heißt (links-) **noethersch**⁴, wenn es keine unendliche echt aufsteigende Kette von Untermoduln gibt. M heißt (links-) **artinsch**⁵, wenn es keine unendliche echt absteigende Kette von Untermoduln gibt.

Ein Ring R heißt **noethersch** (bzw. **artinsch**), wenn er als R -Modul noethersch (bzw. artinsch) ist.

Beispiel

\mathbb{Z} ist noethersch aber nicht artinsch. Allgemein gilt: HIR sind noethersch. Körper sind artinsch und noethersch.

⁴nach Emmy Noether, 1882-1935, siehe http://de.wikipedia.org/wiki/Emmy_Noether

⁵nach Emil Artin, 1898-1962, siehe http://de.wikipedia.org/wiki/Emil_Artin

2.12 Proposition

Ein R -Modul M ist noethersch genau dann, wenn alle Untermoduln endlich erzeugt sind.

Beweis

" \Rightarrow ": Sei $N \subseteq M$, wähle induktiv $x_1, x_2, \dots \in N$ mit $x_i \notin \langle x_1, \dots, x_{i-1} \rangle =: N_{i-1}$. Dann ist (N_i) eine echt aufsteigende Kette und muss — da M noethersch ist — nach endlich vielen Schritten mit $\langle x_1, \dots, x_k \rangle = N$ enden. Das heißt N ist endlich erzeugt.

" \Leftarrow ": Sei $N_0 \subseteq N_1 \subseteq \dots$ eine echt aufsteigende Kette von Untermoduln in M und $N := \sum N_i$. Da N endlich erzeugt ist, existieren $x_1, \dots, x_r \in N$ mit $N = \langle x_1, \dots, x_r \rangle$. Dann existiert ein k mit $x_1, \dots, x_r \in N_k$; d.h. $N = N_k$ und die Kette ist endlich. \square

Bemerkung

Offensichtlich gilt: Ist M noethersch (bzw. artinsch) R -Modul, $N \subseteq M$ Untermodul. Dann sind auch N und M/N noethersch (bzw. artinsch). Dies gilt nach den Isomorphiesätzen.

2.13 Satz

Ist $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ eine kurze exakte Sequenz von R -Moduln, dann gilt: M noethersch (bzw. artinsch) genau dann, wenn M' und M'' noethersch (bzw. artinsch).

Beweis

" \Rightarrow ": klar nach voriger Bemerkung.

" \Leftarrow ": (artinsch) Sei $P_0 \supseteq P_1 \supseteq P_2 \supseteq \dots$ eine echt absteigende Kette in M . Dann betrachte

$$P_0 \cap M' \supseteq P_1 \cap M' \supseteq \dots$$

in M' und

$$(P_0 + M')/M' \supseteq (P_1 + M')/M' \supseteq \dots$$

in M/M' . Nach Voraussetzung existiert $k \in \mathbb{N}$ mit $P_k \cap M' = P_l \cap M'$ für $l \geq k$ und $(P_k + M')/M' = (P_l + M')/M'$ für $l \geq k$. Wegen

$$(P_l + M')/M' \simeq P_l / (P_l \cap M')$$

folgt $P_l = P_k$ für $l \geq k$. Entsprechend für aufsteigende Ketten. \square

2.14 Korollar

Endliche Summen von noetherschen (bzw. artinschen) Moduln sind wieder noethersch (bzw. artinsch).

Beweis

Ist $M = N + P$ und N, P noethersch, dann betrachte $0 \rightarrow N \hookrightarrow M \twoheadrightarrow M/N \rightarrow 0$. Wegen $M/N = (N+P)/N \simeq P/(N \cap P)$ ist M/N noethersch, also ist nach Satz 2.13 auch M noethersch. Entsprechend für artinsch. \square

2.15 Korollar

Ist R ein noetherscher (bzw. artinscher) Ring, dann ist jeder endlich erzeugte R -Modul noethersch (bzw. artinsch).

Beweis

Durch Induktion über die Anzahl der Erzeuger. Ist M zyklisch, dann ist $M \simeq R/J$ und R/J noethersch (bzw. artinsch) nach Satz 2.13. Sei nun

$$M = \langle x_1, \dots, x_n \rangle, \quad M' = \langle x_1, \dots, x_{n-1} \rangle$$

Nach Induktionsvoraussetzung ist M' noethersch (artinsch) und M/M' ist zyklisch, daher auch noethersch (artinsch), nach 2.13 ist M noethersch (artinsch). \square

2.16 Korollar

Ist R ein Hauptidealring, dann ist jeder endlich erzeugte R -Modul noethersch.

2.17 Definition

Ein R -Modul M heißt **halbeinfach** (oder vollständig zerlegbar), wenn jeder Untermodul N ein Komplement hat, d.h. wenn $N' \subseteq M$ existiert mit $M = N \oplus N'$, d.h. $N \cap N' = \{0\}, N + N' = M$.

2.18 Beispiele

- (i) \mathbb{Z} (als \mathbb{Z} -Modul) ist *nicht* halbeinfach. $m\mathbb{Z} \subseteq \mathbb{Z}, m \neq 0$ hat kein Komplement, denn für $k \cdot \mathbb{Z}$ ist $k \cdot \mathbb{Z} \cap m \cdot \mathbb{Z} \ni k \cdot m \neq 0$.
- (ii) Ist R ein Körper, dann sind alle R -Vektorräume halbeinfach nach dem Basisergänzungssatz.
- (iii) Untermoduln und Quotienten halbeinfacher Moduln sind halbeinfach.
- (iv) Einfache Moduln sind halbeinfach.
- (v) $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$ ist halbeinfach, weil $\mathbb{Z}_2, \mathbb{Z}_3$ die einzigen nicht-trivialen Untermoduln sind.

Ein Ring R heißt (links-)halbeinfach, wenn er als R -Modul halbeinfach ist.

2.19 Satz

Für einen R -Modul M sind äquivalent:

- (i) M ist halbeinfach.
- (ii) M ist Summe von einfachen Moduln, d.h. es existiert Familie $(N_\alpha)_{\alpha \in I}$ von einfachen Untermoduln, die M erzeugen, also $M = \sum_{\alpha \in I} N_\alpha$.
- (iii) M ist direkte Summe von einfachen Untermoduln, d.h. es existiert eine Familie $(N'_\alpha)_{\alpha \in I'}$ von einfachen Untermoduln mit

$$M = \bigoplus_{\alpha \in I'} N'_\alpha$$

$$\text{d.h. } N'_\alpha \cap \sum_{\beta \neq \alpha} N'_\beta = 0$$

Beweis (mit Lemma 2.20)

"(i) \Rightarrow (ii)": Sei $\{N_\alpha\}_{\alpha \in I}$ die Menge *aller* einfachen Untermoduln von M . Diese ist nach Lemma 2.20 nicht leer. Setze $M_1 := \sum N_\alpha$.

Behauptung: $M_1 = M$. Sonst existiert ein Komplement $P \subseteq M$ mit $P \neq 0, P \oplus M_1 = M$. Dann ist P halbeinfach und enthält daher einen einfachen Untermodul $N \subseteq P$ zu $N \in \{N_\alpha\}_{\alpha \in I}$.

"(iii) \Rightarrow (ii)": Klar.

"(ii) \Rightarrow (i)": Sei $P \subseteq M$ Untermodul. Betrachte die Menge aller $J \subseteq I$ mit

- (a) $N_i \cap \sum_{j \neq i, j \in J} N_j = 0$ für alle $i \in J$
- (b) $P \cap \sum_j N_j = 0$

Weil $J = \emptyset$ die Bedingungen (a) und (b) erfüllt, können wir Zorns Lemma anwenden und finden eine maximale Teilmenge $J \subseteq I$ mit (a) und (b).

Behauptung:

$$M_1 := P \oplus \sum_{j \in J} N_j = P \oplus \bigoplus_{j \in J} N_j = M$$

Für $\alpha \in I$ ist $N_\alpha \cap M_1 \in \{0, N_\alpha\}$, da N_α einfach. Ist $N_\alpha \cap M_1 = 0$, dann erfüllt $J \cup \{\alpha\}$ die Bedingungen (a) und (b). \nexists Maximalität von J . Daher ist $N_\alpha \subseteq M_1$, also $M_1 = M$.

"(ii) \Rightarrow (iii)": folgt aus dem Beweis "(i) \Rightarrow (ii)" mit $P = 0$. □

2.20 Lemma

Ist $M \neq 0$ halbeinfach, dann hat M einen einfachen Untermodul.

Beweis

Sei $m \in M, m \neq 0$. Betrachte $N := \langle m \rangle \subseteq M$. Nach Zorns Lemma existiert ein maximaler Untermodul $P \leq N$ mit $m \notin P$ (denn 0 ist ein solcher Untermodul). Sei Q ein Komplement von P in N , also $P \oplus Q = N, Q \neq 0$, da $m \notin P$.

Behauptung: Q ist einfach. Beweis: $Q \subseteq N \subseteq M$. Ist $0 \neq Q' \subseteq Q$ ein Untermodul, dann ist ja $Q' \oplus P \supsetneq P$, also wegen der Maximalität von P : $m \in Q' \oplus P$, also $Q' \oplus P = N$ und daher $Q = Q'$. □

2.21 Satz

Für einen Ring R sind äquivalent:

- (i) Alle R -Moduln sind halbeinfach.
- (ii) Alle endlich erzeugten R -Moduln sind halbeinfach.
- (iii) Alle zyklischen R -Moduln sind halbeinfach.
- (iv) $(R, +)$ ist als R -Modul halbeinfach.

Beweis

"(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)" Klar.

"(iv) \Rightarrow (iii)": Jeder zyklische R -Modul ist von der Form R/I und Quotienten halbeinfacher Moduln sind halbeinfach. siehe 2.6 bzw. Blatt 3

"(iii) \Rightarrow (i)": Sei $M \in {}_R \text{Mod}$, dann ist $M = \sum_{m \in M} R \cdot m$ Summe zyklischer Moduln. Da jeder zyklische R -Modul halbeinfach ist und Summen halbeinfacher Moduln wieder halbeinfach sind, folgt die Behauptung. □

2.22 Korollar

Sei $M = \bigoplus_{\alpha \in I} N_\alpha$ mit N_α einfach. Ist $P \subseteq M$ Untermodul, dann existiert $J \subseteq I$ mit

$$P \simeq \bigoplus_{\alpha \in J} N_\alpha.$$

Ist P einfach, dann ist $P \simeq N_\alpha$ für ein $\alpha \in I$.

Beweis

Nach Satz 2.19 existiert $J' \subseteq J$ mit $P \oplus \bigoplus_{j \in J'} N_j = M$ (Beweis "(i) \Rightarrow (ii)"). Daher ist

$$P \simeq M / \bigoplus_{j \in J'} N_j \simeq \bigoplus_{j \in J \setminus J'} N_j$$

aber nicht
unbedingt gleich
 N_α

□

2.23 Korollar (Krull-Remak-Schmidt)

Ist

$$M = \bigoplus_{i \in I} N_i = \bigoplus_{k \in K} L_k,$$

mit N_i, L_k einfach und I endlich. Dann ist $|I| = |K|$ und es existiert ein $\pi \in \text{Sym}(K)$ mit $L_k \simeq N_{\pi(k)}$.

Beweis

Durch Induktion über $n = |I|$. Für $n = 1$ folgt $k = 1$, weil M einfach. Im Allgemeinen existiert ein $j \in I$ mit $L_i \simeq N_j$ (nach Korollar 2.22). Dann ist

$$\bigoplus_{j \neq i} L_j \simeq M/L_i \simeq M/N_j \simeq \bigoplus_{i \neq j} N_i$$

Nach Induktionsvoraussetzung folgt die Behauptung. \square

2.24 Bemerkung

Sei $M = \bigoplus_{i \in I} S_i$ mit S_i einfach. Dann ist M endlich erzeugt genau dann, wenn $|I|$ endlich.

Beweis

" \Leftarrow ": klar, weil S_i zyklisch.

" \Rightarrow ": Ist $M = \langle x_1, \dots, x_r \rangle$, dann existiert für jedes $j = 1, \dots, r$ endlich viele S_{j_1}, \dots, S_{j_k} mit $x_j \in \bigoplus_{i=1}^k S_{j_i}$, also ist M die Summe von endlich vielen S_i , d.h. $|I|$ endlich. \square

Das heißt wenn R halbeinfach als R -Modul, dann noethersch und artinsch.

2.25 Satz

Sei R ein Ring. Die Ideale in $M_k(R)$ sind genau von der Form $M_k(I)$ für ein Ideal $I \trianglelefteq R$. Insbesondere ist $M_k(R)$ einfach genau dann, wenn R einfach ist.

Beweis

Klar ist: Wenn $I \trianglelefteq R$, dann $M_k(I) \trianglelefteq M_k(R)$. Sei nun $I \trianglelefteq M_k(R)$ ein Ideal, $\bar{I} := \{x_{11} \mid (x_{ij}) \in I\}$ die Menge aller $(1,1)$ -Koeffizienten in $X \in I$. Man rechnet leicht nach, dass $\bar{I} \trianglelefteq R$ ein beidseitiges Ideal ist:

$$\underbrace{\begin{pmatrix} j & * \\ * & * \end{pmatrix}}_{\in I} \cdot \underbrace{\begin{pmatrix} r & \\ & 0 \end{pmatrix}}_{\in M_k(R)} = \underbrace{\begin{pmatrix} j \cdot r & \\ & 0 \end{pmatrix}}_{\in I}$$

Sei $E(s, t)_{\mu, \nu} \in M_k(R)$ mit

$$E(s, t)_{\mu, \nu} = \begin{cases} 1, & \text{falls } s = \mu, t = \nu \\ 0, & \text{sonst} \end{cases}$$

eine Elementarmatrix. Dann ist $E(s, t)XE(u, v) = x_{t,u}E(s, v)$. Für $X \in I$ folgt wegen $E(1, s)XE(t, 1) = x_{s,t}E(1, 1)$, also $x_{s,t} \in \bar{I}$. Daher ist $I \subseteq M_k(\bar{I})$.

Noch zu zeigen: $M_k(\bar{I}) \subseteq I$. Sei also $Y \in M_k(\bar{I})$. Dann existiert für s, t ein $X \in I$ mit $y_{s,t} = x_{1,1}$. Das heißt $y_{s,t}E(s, t) = x_{1,1}E(s, t) = E(s, 1)XE(1, t) \in I$. Daher ist

$$Y = \sum y_{s,t}E(s, t) \in I$$

d.h. $I = M_k(\bar{I})$. \square

Matrizenringe über Körpern und Schiefkörpern sind einfache Ringe.

2.26 Satz (Schurs Lemma)

Ist $M \in {}_R \text{Mod}$ einfach, dann ist $\text{End}_R(M)$ ein Schiefkörper.

Beweis

Wegen $M \neq 0$ ist $\text{End}_R(M) \neq 0$. Ist $\varphi \in \text{End}_R(M) \setminus \{0\}$, dann ist $\varphi(M) \neq 0$, also $\varphi(M) = M$, da M einfach. Ebenso $\ker \varphi \neq M$, daher $\ker \varphi = 0$. Daher ist φ ein Isomorphismus und hat ein Inverses in $\text{End}_R(M)$. \square

2.27 Lemma

Ist $M = \bigoplus_{i \leq k} M_i$, $\varphi \in \text{End}_R(M)$, dann existieren $\varphi_{i,j} \in \text{Hom}(M_i, M_j)$ $1 \leq i, j \leq k$, so dass für alle $x = (x_1, \dots, x_k) \in M_1 \oplus \dots \oplus M_k$ gilt

$$\varphi(x) = \begin{pmatrix} \varphi_{1,1} & \cdots & \varphi_{1,k} \\ \vdots & & \vdots \\ \varphi_{k,1} & \cdots & \varphi_{k,k} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$$

Insbesondere ist

$$\text{End}_R(M^k) \simeq M_k(\text{End}_R(M))$$

Beweis

Seien $e_j : M_j \rightarrow M$ die Einbettungen, $\pi_i : M \rightarrow M_i$ die Projektionen. Dann ist für jeden Endomorphismus $\varphi \in \text{End}_R(M)$ mit $\varphi_{i,j} := \pi_i \circ \varphi \circ e_j \in \text{Hom}(M_j, M_i)$ und es gilt

$$\varphi = \sum e_i \circ \varphi_{i,j} \circ \pi_j$$

Es ist leicht nachzurechnen, dass die Verknüpfung von Endomorphismen der Multiplikation von Matrizen entspricht, d.h. $\varphi\psi = \sum \varphi_{i,j} \psi_{j,k}$. Damit folgt die Behauptung. \square

2.28 Definition + Lemma

Ist $(R, +, \cdot, 1)$ ein Ring, dann ist $R^{\text{op}} := R(+, *, 1)$ ein Ring mit $r * s = s \cdot r$, der **entgegengesetzte Ring**.

Klar: Ist R kommutativ, dann ist $R^{\text{op}} \simeq R$. Jeder Links- R -Modul lässt sich als Rechts- R -Modul auffassen. Es gilt

$$\text{End}_R(R, +) \simeq R^{\text{op}}$$

Beweis

Setze $\rho : R^{\text{op}} \rightarrow \text{End}_R(R, +)$, $\rho(r) = \rho_r : x \mapsto x \cdot r$. Homomorphie: $\rho_{r*s} : x \mapsto x \cdot s \cdot r$. Dann ist ρ ein Ringhomomorphismus mit $\ker \rho = 0$, also injektiv. Ist $\varphi \in \text{End}_R(R, +)$, so betrachte $\varphi(1) = r \in R$. Dann ist

$$\varphi(r)(x) = x \cdot r = x \cdot \varphi(1) = \varphi(x \cdot 1) = x \cdot r$$

d.h. $\varphi = \rho_r$. Daher ist ρ ein Isomorphismus. \square

2.29 Satz (Wedderburn, 1. Struktursatz)

Sei R ein Ring. Dann sind äquivalent:

- (i) R ist einfach als Ring und links-artinsch als R -Modul.
- (ii) Alle einfachen R -Moduln sind isomorph und R ist halbeinfach als Modul.

- (iii) $R \simeq M_k(D)$ für einen Schiefkörper D und ein $k \geq 1$. Darüber hinaus sind k und D eindeutig bestimmt und der einfache R -Modul ist $\simeq D^k$

Beweis

"(i) \Rightarrow (ii)": Sei $0 \neq I \subseteq R$ ein minimales Linksideal (existiert, da R linksartinsch als Modul). Das heißt $I = Rc \neq 0$ für ein $c \in R$ (zyklisch!). Dann ist

$$\sum_{r \in R} Rc \cdot r = J$$

ein beidseitiges Ideal im Ring R , also $R = \sum_{r \in R} Rc \cdot r$, da R einfach. Ist $Rcr \neq 0$, dann ist $Rc \rightarrow Rcr, s \cdot c \mapsto s \cdot c \cdot r$ ein Epimorphismus, also $Rcr = Rc$ wegen der Minimalität von Rc . Daher ist $(R, +)$ Summe von einfachen Untermoduln, also halbeinfach nach Satz 2.19.

Noch zu zeigen: Alle einfachen R -Moduln sind isomorph.

Ist M ein einfacher R -Modul, dann ist $M = R \cdot m$ zyklisch und also $M \simeq R/I$ für ein maximales Linksideal I in $(R, +)$. Weil R halbeinfach ist, ist M isomorph zu einem minimalen Linksideal in $(R, +)$ und wegen $R = \bigoplus_{i=1}^k Rc_i$ nach Satz 2.19 ist dann $M \simeq Rc_i =: Rc$. Die direkte Summe ist endlich, da R artinsch ist nach Bemerkung 2.24.

"(ii) \Rightarrow (iii)": $(R, +)$ ist als Links- R -Modul endlich erzeugt (sogar zyklisch, $R = R \cdot 1$). Daher ist nach Voraussetzung

$$(R, +) \simeq \bigoplus_{i=1}^k L_i$$

mit L_i minimale Linksideale in R , $L_1 \simeq \dots \simeq L_k$ und nach Schurs Lemma (2.26) ist $\text{End}_R(L_1) \simeq D'$ ein Schiefkörper. Daher ist

$$R^{\text{op}} \simeq \text{End}_R(R, +) \simeq M_k(D')$$

nach 2.27 und damit $R \simeq M_k(D)$ mit $D = (D')^{\text{op}}$ (Da $M_k(R)^{\text{op}} = M_k(R^{\text{op}})$).

"(iii) \Rightarrow (i)": $M_k(D)$ ist ein k^2 -dimensionaler D -Vektorraum. Linksideale sind D -Untervektorräume, also ist $M_k(D)$ noethersch und artinsch und einfach nach Satz 2.25. Die Eindeutigkeit von k und D folgt aus Korollar 2.23 (Krull-Remak-Schmidt) und Schurs Lemma (2.26). \square

Bemerkung

$(R, +)$ ist also auch noethersch (rechts und links). Achtung: Es gibt Ringe, die link-noethersch aber nicht rechts-noethersch sind!

2.30 Bemerkung

Sind M, N einfache, nicht-isomorphe R -Moduln, dann ist $\text{Hom}_R(M, N) = 0$. (Klar!)

2.31 Satz (2. Struktursatz von Wedderburn)

Sei $R \neq 0$ ein Ring, halbeinfach als R -Modul. Dann existieren Schiefkörper D_1, \dots, D_l paarweise nicht isomorph und $k_1, \dots, k_l \in \mathbb{N}$, so dass

$$R \simeq M_{k_1}(D_1) \oplus \dots \oplus M_{k_l}(D_l).$$

als Ringisomorphismus.

Beweis

$(R, +) \simeq L_1^{k_1} \oplus \dots \oplus L_l^{k_l}$ mit $L_i \subseteq R$ minimale Linksideale, L_i paarweise nicht isomorph. Dann ist

$$R^{\text{op}} \simeq \text{End}_R(R, +) \simeq \text{End}_R(L_1^{k_1}) \oplus \dots \oplus \text{End}_R(L_l^{k_l}) \simeq M_{k_1}(\tilde{D}_1) \oplus \dots \oplus M_{k_l}(\tilde{D}_l)$$

mit $\tilde{D}_i = \text{End}_R(L_i)$. Setze $D_i := \tilde{D}_i^{\text{op}}$. Damit ist dann

$$R \simeq M_{k_1} \oplus \dots \oplus M_{k_l}(D_l)$$

nach Bemerkung
2.30

Freie Moduln**2.32 Definition**

Sei M ein Links- R -Modul. Elemente $x_1, \dots, x_n \in M$ heißen **R -linear unabhängig**, wenn gilt: Sind $\alpha_1, \dots, \alpha_n \in R$ mit $\sum \alpha_i \cdot x_i = 0$, dann ist $\alpha_i = 0$ für $i = 1, \dots, n$.

Sonst heißen x_1, \dots, x_n linear abhängig. Eine (beliebige Menge) $X \subseteq M$ heißt linear unabhängig, wenn jede endliche Teilmenge linear unabhängig ist. Eine linear unabhängige Menge von Erzeugern heißt **Basis** für M .

2.33 Definition

Sei R ein Ring. Ein R -Modul heißt **frei**, wenn er eine Basis hat.

Achtung: Die Mächtigkeit einer Basis ist *nicht* notwendig eindeutig bestimmt!

Beispiel

- (i) Wenn $R = K$ Körper, dann sind alle R -Moduln frei.
- (ii) R als R -Modul ist frei mit der Basis 1.
- (iii) R^n für beliebiges n ist frei.

2.34 Definition

Für eine beliebige Menge I heißt der (Links-) R -Modul $\mathcal{F}_I = \bigoplus_I R$ der freie R -Modul mit Basis der Mächtigkeit $|I|$.

Elemente von \mathcal{F}_I sind von der Form $(a_i)_{i \in I}$ mit $a_i = 0$ für fast alle $i \in I$, d.h. $a_i = 0$ für alle bis auf endlich viele $i \in I$. Jeder andere freie R -Modul mit Basis der Mächtigkeit $|I|$ ist isomorph zu \mathcal{F}_I via Bijektion der Basen: $(u_i)_{i \in I}, (v_i)_{i \in I}$ induziert einen Isomorphismus durch

$$\sum_{i \in I} \alpha_i \cdot u_i \mapsto \sum_{i \in I} \alpha_i \cdot v_i$$

Achtung: Umkehrung gilt nicht! (siehe 2.33)

Freie Moduln können durch ihre **universelle Eigenschaft** charakterisiert werden:

2.35 Satz

Sei R ein Ring. Dann existiert für jede Menge I ein R -Modul \mathcal{F}_I und eine Abbildung $\varphi : I \rightarrow \mathcal{F}_I$, die universell ist für R -Moduln. D.h. für jede Abbildung $f : I \rightarrow M$ in einen R -Modul M existiert ein eindeutiger Homomorphismus $f' : \mathcal{F}_I \rightarrow M$ mit $f = f' \circ \varphi$. Also

$$\begin{array}{ccc} I & \xrightarrow{\varphi} & \mathcal{F}_I \\ & \searrow f & \downarrow f' \\ & & M \end{array}$$

Beweis

Sei $\mathcal{F}_I = \bigoplus_I R$ mit Basis $(u_i)_{i \in I}$ und $\varphi(i) = u_i$. Ist $f : I \rightarrow M$ eine Abbildung, dann gilt für $f' : \mathcal{F}_I \rightarrow M$ mit $f' = f' \circ \varphi$ offensichtlich $f'(u_i) = f(i)$. Also muss gelten

$$f'\left(\sum \alpha_i u_i\right) = \sum \alpha_i f(i) \quad (\star)$$

Daher folgt die Existenz von f' und die Eindeutigkeit ebenfalls. \square

Bemerkung

Aus der universellen Eigenschaft folgt, dass der freie R -Modul mit Basis der Mächtigkeit $|I|$ bis auf Isomorphie eindeutig bestimmt ist.

2.36 Korollar

Ist $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$ eine kurze exakte Sequenz, M'' ein freier R -Modul, dann **spaltet** die Sequenz, d.h. es existiert ein R -Modulhomomorphismus $\sigma : M'' \rightarrow M$ mit $\beta \circ \sigma = \text{id}_{M''}$. Dann ist $M \cong M' \oplus M''$.

Bemerkung

M'' heißt **projektiv** genau dann, wenn jede kurze Sequenz mit M'' an dritter Stelle spaltet. Das heißt, dass dieses Korollar bedeutet: Freie R -Moduln sind projektiv.

Beweis

Sei I Basis für M'' . Da β surjektiv ist, existiert für jedes $i \in I$ ein $u_i \in M$ mit $\beta(u_i) = i$. Die Abbildung $f : I \rightarrow M, i \mapsto u_i$ lässt sich fortsetzen zu $\sigma : M'' \rightarrow M$ (2.35) und dann gilt $\beta \circ \sigma = \text{id}_{M''}$. Damit ist $M = \text{Im } \alpha \oplus \text{Im } \sigma \simeq M' \oplus M''$. \square

2.37 Satz

Jeder R -Modul ist Quotient (also homom Bild) eines freien R -Moduls.

Beweis

Ist $M \in {}_R \text{Mod}$, setze $\mathcal{F}_M = \bigoplus_{m \in M} R$. Dann lässt sich die Abbildung $f : M \rightarrow M$ fortsetzen zu einem Epimorphismus $f' : \mathcal{F}_M \rightarrow M$, d.h. $M \simeq \mathcal{F}_M / \ker f'$. Daher sind Quotienten von freien Moduln im Allgemeinen *nicht* frei! \square

2.38 Satz

Sei R ein nicht-trivialer Ring. Dann sind äquivalent:

- (i) Jeder (Links-) R -Modul ist frei.
- (ii) Jeder zyklischer (Links-) R -Modul ist frei.
- (iii) R ist einfach als Links- R -Modul.
- (iv) Jedes $x \in R \setminus \{0\}$ hat ein Linksinverses.
- (v) R ist ein Schiefkörper.

(i) - (v) sind auch äquivalent zu (i)_R - (iv)_R für Rechts- R -Moduln.

Beweis

"(i) \Rightarrow (ii)": Klar.

"(ii) \Rightarrow (iii)": Sei I ein maximales Links-Ideal in $(R, +)$. Dann ist

$$0 \rightarrow I \rightarrow R \rightarrow \mathcal{F} \rightarrow 0$$

mit $\mathcal{F} \simeq R/I$ eine exakte Sequenz mit \mathcal{F} zyklisch und daher frei nach Voraussetzung. Da I ein maximales war, ist \mathcal{F} einfach. R ist auch zyklisch und daher frei, d.h. $R \simeq \mathcal{F}$ und daher auch R einfach als R -Modul.

"(iii) \Rightarrow (iv)": Sei $c \in R \setminus \{0\}$. Dann ist $Rc = R$, also existiert $b \in R$ mit $bc = 1$, d.h. c hat ein Linksinverses.

"(iv) \Rightarrow (v)": Sei $c \in R \setminus \{0\}$ mit Linksinversem b und a Linksinverses von b , also

$$bc = 1 = ab.$$

Dann ist also $a = a(bc) = (ab)c = c$. Dann folgt $a = c$ und $bc = cb = 1$. Damit ist R ein Schiefkörper.

"(v) \Rightarrow (i)": Lineare Algebra I.

Die Äquivalenz von (i) $_R$ - (v) $_R$ folgt entsprechend. Wegen (v) $=$ (v) $_R$ (weil (v) symmetrisch ist), sind also (i)- (v) auch äquivalent zu (i) $_R$ - (iv) $_R$. \square

Achtung

Auch freie Moduln haben nicht notwendig eine Dimension!

Beispiel: Sei V ein unendlich dimensionaler K -Vektorraum, dann ist $V \simeq V \oplus V$, also ist

$$R = \text{End}_K(V) \simeq \text{End}_K(V^2) \simeq M_2(R) \simeq R^4$$

Das heißt R als freier R -Modul hat eine Basis der Mächtigkeit 1, aber auch Basen jeder anderen Mächtigkeit.

2.39 Definition

Ein Ring hat **invariante Basislänge** (IBL), wenn aus $R^m \simeq R^n$ (als Links-Moduln) schon $m = n$ folgt.

Bemerkung

Man kann zeigen: R hat IBL genau dann, wenn jeder freie R -Modul eindeutige Basislänge hat.

Beispiel

Körper haben IBL, $\text{End}_R(V)$ nicht immer, 0 nie!

2.40 Lemma

Ein Ring R hat in IBL, wenn für alle $m, n \in \mathbb{N}$ gilt: Ist $A \in R^{m \times n}$, $B \in R^{n \times m}$ mit

$$AB = \mathbb{1}_{m \times m} \quad , \quad BA = \mathbb{1}_{n \times n}$$

dann ist $n = m$.

Beweis

Dies ist die Matrizenformulierung der Definition von IBL mit Lemma 2.27. \square

Folgerung

R hat IBL für Links- R -Moduln genau dann, wenn R IBL für Rechts- R -Moduln hat.

2.41 Satz

Sei $R \neq 0$ ein Ring.

- (i) Ist R kommutativ, dann hat R IBL.
- (ii) Ist R noethersch (bzw. artinsch), dann hat R IBL. Insbesondere haben halbeinfache Ringe IBL.
- (iii) Ist $\varphi : S \rightarrow R$ ein Ringhomomorphismus ($\varphi(1_S) = 1_R$) und R hat IBL, dann auch S . Insbesondere vererbt sich IBL auf Unterringe.

Beweis

- (i) Angenommen $A \in R^{m \times n}$, $B \in R^{n \times m}$ mit

$$AB = \mathbb{1}_{m \times m} \quad , \quad BA = \mathbb{1}_{n \times n}$$

und o.B.d.A. $m < n$. Dann ist

$$\tilde{B} \cdot \tilde{A} = \mathbb{1}$$

Es gilt $\det(\tilde{B}\tilde{A}) = \det \mathbb{1} = 1$ und $\det(\tilde{A}\tilde{B}) = \det(\tilde{B}\tilde{A})$, aber

weitereZeichnung

- (ii) Ist $R^m \simeq R^{m+k}$ mit $k \geq 1$, dann ist $R^m \simeq R^{m+k} \simeq R^{m+2k}$ und man erhält eine unendliche, echt aufsteigende (absteigende) Kette in R^m . Mit R ist auch R^m noethersch (bzw. artinsch). \downarrow
Halbeinfacher Ring \Rightarrow noethersch und artinsch.

- (iii) Seien $A \in S^{m \times n}$, $B \in S^{n \times m}$ mit $AB = \mathbb{1}$, $BA = \mathbb{1}$. Dann gilt

$$\varphi(A)\varphi(B) = 1 \quad , \quad \varphi(B)\varphi(A) = 1$$

das heißt es gilt $n = m$.

Erinnerung

R ist ein **Hauptidealring** (HIR)⁶, falls R kommutativ und nullteilerfrei ist und jedes Ideal ein Hauptideal ist, das heißt von einem Element erzeugt. In Hauptidealringen hat man eindeutige Primfaktorzerlegung (bis auf Einheiten).

2.42 Satz

Sei D ein Hauptidealring, $L \subseteq D^m$ ein Untermodul, dann $L \simeq D^n$ für ein $n \leq m$, d.h. Untermoduln freier Moduln sind frei.

Beweis

Durch Induktion über $m \geq 0$. Für $m = 0$ ist die Aussage klar. Für $m = 1$ ist $L \subseteq D$ ein Linksideal und da D kommutativ ist, ist $L \trianglelefteq D$. Weil D Hauptidealring ist, folgt $L = Da$ für ein $a \in D$, d.h. L ist frei. Weiter ist $D \simeq Da$ via $\varphi : D \rightarrow Da$, $s \mapsto s \cdot a$ (Isomorphismus, da D nullteilerfrei).

Induktionsschritt: Sei $L \subseteq D^{m+1} = D \oplus D^m$, $\pi : D \oplus D^m \rightarrow D$ die Projektion auf die erste Komponente. Betrachte die exakte Sequenz

$$0 \rightarrow \ker \pi|_L \rightarrow L \xrightarrow{\pi} \pi(L) \rightarrow 0$$

⁶englisch: PID, prime ideal domain

Fall 1: $\pi(L) = 0$, dann ist $L \subseteq \ker \pi = 0 \oplus D^m \simeq D^m$ und nach Induktionsvoraussetzung ist L frei, $L \simeq D^n$, $n \leq m$.

Fall 2: $\pi(L) \neq 0$, dann ist $\pi(L) \subseteq D$ freier D -Modul. Nach Korollar 2.36 ist

$$L \simeq \ker \pi|_L \oplus \pi(L)$$

Nach Induktionsvoraussetzung ist $\ker \pi|_L \subseteq D^m$ ein freier Modul, also $\ker \pi|_L \simeq D^n$, $n \leq m$, und $\pi(L) \simeq D$, daher ist $L \simeq D \oplus D^n$. \square

Ist D ein Hauptidealring, M endlich erzeugt über D , $M = Dm_1 + \dots + Dm_s$. Betrachte $\varphi : D^s \rightarrow M$ mit $(d_1, \dots, d_s) \mapsto \sum d_i m_i$. Nach Satz 2.42 ist $\ker \varphi \simeq D^t$ für $t \leq s$ und $M \simeq D^s / \ker \varphi$. Um M zu beschreiben, müssen wir untersuchen, wie $\ker \varphi \subseteq D^s$

2.43 Satz

Sei $A = (a_{ij}) \in D^{m \times n}$, D ein Hauptidealring. Dann gibt es invertierbare Matrizen $P \in D^{m \times m}$, $Q \in D^{n \times n}$ mit

$$P \cdot A \cdot Q = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ 0 & & d_k & 0 \\ & & & \ddots \\ & & & & 0 \end{pmatrix} \quad d_1, \dots, d_k \neq 0, d_i \mid d_{i+1}$$

Falls D ein Körper ist, folgt dies aus dem Gauß-Verfahren und $d_i = 1$.

Beweis

Für $a \in D \setminus \{0\}$ sei $l(a) = s$, falls $a = p_1 \cdot \dots \cdot p_s$ mit p_i prim (eindeutig, da D HIR). Ist $a \in D^\times$ Einheit, setze $l(a) = 0$ und $l(0) = \infty$. Für $A = 0$ ist nichts zu zeigen.

Erinnerung: Durch Links- und Rechtsmultiplikation mit geeigneten invertierbaren Matrizen können wir (wie in LA I.)

- Zeilen von A vertauschen
- Zeilen/Spalten mit Einheiten multiplizieren
- Spalten von A vertauschen
- zu einer Zeile/Spalte beliebige Vielfache einer anderen Zeile/Spalte aufaddieren

Wähle a_{ij} in A mit $l(a_{ij})$ minimal. Durch Zeilen- und Spaltenvertauschungen können wir erreichen, dass a_{ij} links oben steht (vertausche i -te und 1. Zeile, dann j -te und 1. Spalte). Wenn $a_{11} \nmid a_{1k}$ für $k \geq 2$, vertausche 2-te und k -te Spalte, also $a_{11} \mid a_{12}$. Sei $d \in \text{ggT}(a_{11}, a_{12})$, dann $l(d) < l(a_{11})$. Schreibe $d = a_{11} \cdot x + a_{12} \cdot y$, $x, y \in D$ und $d \cdot e = a_{12}$ sowie $d \cdot f = -a_{11}$. Dann ist

$$\begin{pmatrix} -f & e \\ y & -x \end{pmatrix} \cdot \begin{pmatrix} x & e \\ y & f \end{pmatrix} = \begin{pmatrix} -f \cdot x + y \cdot e & 0 \\ 0 & e \cdot y - f \cdot x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

denn $d \cdot e \cdot y - d \cdot f \cdot x = a_{12} \cdot y + a_{11} \cdot x = d$, daher $e \cdot y - f \cdot x = 1$. Ebenso

$$\begin{pmatrix} x & e \\ y & f \end{pmatrix} \cdot \begin{pmatrix} -f & e \\ y & -x \end{pmatrix} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

das heißt $\begin{pmatrix} x & e \\ y & f \end{pmatrix}$ ist invertierbar. Es gilt

$$\begin{pmatrix} a_{11} & a_{12} & * \\ a_{21} & a_{22} & * \\ * & * & * \end{pmatrix} \begin{pmatrix} x & e & 0 \\ y & f & 1 \\ 0 & & \ddots \\ & & & 1 \end{pmatrix} = \begin{pmatrix} d & 0a_{13} \dots & * \\ * & * & * \\ * & * & * \end{pmatrix}$$

Damit transformieren wir nach und nach die Matrix A auf die Gestalt

$$\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \dots \\ * & & * \end{pmatrix}$$

mit $\tilde{a}_{11} \mid \tilde{a}_{ik}$ und $\tilde{a}_{11} \mid \tilde{a}_{k1}$. Durch Addieren von geeigneten Vielfachen der 1-ten Zeile/Spalte erhalten wir die Matrix

matrixhier

und $l(\tilde{a}_{11}) \leq l(b_{ij})$ für $B = (b_{ij})$. Induktiv erhalten wir eine Matrix der Form

matrixhier

mit $l(d_i) \leq l(d_{i+1})$. Ist $d_i \nmid d_{i+1}$, dann transformieren wir weiter:

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_{i+1} \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_i & d_{i+1} \\ & d_{i+1} \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_i & d_{i+1} \\ & d_{i+1} \end{pmatrix} \begin{pmatrix} x & e \\ y & f \end{pmatrix} = \begin{pmatrix} d'_i & 0 \\ d_{i+1}y & d_{i+1}f \end{pmatrix}$$

mit $d_i x + d_{i+1} y = d'_i \in \text{ggT}(d_i, d_{i+1})$. Wie eben erhalten wir $\begin{pmatrix} d'_i & 0 \\ 0 & d_{i+1}f \end{pmatrix} \rightsquigarrow \dots$ fertig. \square

Die d_i, \dots, d_k heißen die **invarianten Faktoren** von A . Diese sind eindeutig (bis auf Einheiten).

2.44 Definition

Ist $A \in D^{m \times n}$ und $i \leq m, n$, dann ist die Determinante einer Matrix $A' \in D^{i \times i}$ ein **i -Minor** von A , wenn A' aus A hervorgeht durch Streichen von $m - i$ Zeilen und $n - i$ Spalten. Der **Rang** von A ist das größte i , für das A einen i -Minor $\neq 0$ besitzt.

2.45 Satz (Elementarteilersatz)

Sei D ein Hauptidealring, $A \in D^{m \times n}$, k der Rang von A . Für $j \neq k$ sei $\delta_j = \delta_j(A)$ ein ggT aller j -Minoren von A . Dann sind die invarianten Faktoren eindeutig bestimmt (bis auf Einheiten) und von der Form $d_1 = \delta_1, d_i = \prod_{j \leq i} \delta_j$.

Beweis

Ist k der Rang von A , dann existiert für alle $i \leq k$ ein i -Minor $\neq 0$ in A (Laplace-Entwicklung der Determinante). Insbesondere ist $\delta_1, \dots, \delta_k \neq 0$, also $d_i \neq 0$ für $i = 1, \dots, k$. Für $P \in D^{m \times m}$ sind die Zeilen von $P \cdot A$ Linearkombinationen der Zeilen von A und die j -Minoren von $P \cdot A$ sind Linearkombinationen der j -Minoren von A . Entsprechend für $Q \in D^{n \times n}$ und $A \cdot Q$. Wenn also $P \in D^{m \times m}, Q \in D^{n \times n}$ invertierbare Matrizen sind, dann folgt $\delta_j(P \cdot A \cdot Q) \mid \delta_j(A)$ und $\delta_j(A) \mid \delta_j(P \cdot A \cdot Q)$ ist. Das heißt $\delta_j(P \cdot A \cdot Q) = u \cdot \delta_j(A)$ für eine Einheit $u \in D^\times$. Ist

$$P \cdot A \cdot Q = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k & 0 \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}$$

mit $d_i \mid d_{i+1}$, dann ist $\delta_j(A) = d_i \cdot \dots \cdot d_j$. Dies zeigt, dass die invarianten Faktoren bis auf Einheiten eindeutig sind.

2.46 Beispiel

Sei $D = \mathbb{Z}$ und $A = \begin{pmatrix} 3 & 1 \\ 0 & 4 \end{pmatrix}$. Dann ist $\delta_1 = 1, \delta_2 = 12 = d_2$. Damit ist $A \sim_{\mathbb{Z}} \begin{pmatrix} 1 & 0 \\ 0 & 12 \end{pmatrix}$.

2.47 Definition

Ist $M \in {}_R \text{Mod}$, $m \in M$, dann heißt

$$\text{ann}(m) = \{r \in R \mid r \cdot m = 0\}$$

das **Annulatorideal** von m in R . $m \in M$ heißt **Torsionselement**, falls $\text{ann}(m) \neq 0$

2.48 Satz: Struktursatz für endlich erzeugte Moduln über HIR

Sei D ein Hauptidealring, M ein endlich erzeugter D -Modul. Dann ist M die Summe von zyklischen Moduln $M = D_{m_1} \oplus \dots \oplus D_{m_k}$ mit

$$D \supsetneq \text{ann}(m_1) \supsetneq \text{ann}(m_2) \supsetneq \dots \supsetneq \text{ann}(m_k)$$

Beweis

Schreibe $M \simeq D^s/L$ mit $L \simeq D^t$, $t \leq s$. Dann ist $L = Dl_1 \oplus \dots \oplus Dl_t$ mit $l_j = (a_{1j}, \dots, a_{sj}) \in D^s$. Dann erhalten wir eine Matrix $A = (a_{ij}) \in D^{s \times t}$. Die Smith-Normalform

$$P \cdot A \cdot Q = \begin{pmatrix} a_1 & & & & 0 \\ & \ddots & & & \\ & & a_k & & \\ & & & 0 & \\ 0 & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

liefert ein neues Erzeugendensystem für D^s , L nämlich $e_1, \dots, e_s, f_1, \dots, f_t$ mit

$$D^s = \bigoplus_{i=1}^s Dl_i, \quad L = \bigoplus_{j=1}^t Df_j$$

$f_i = d_i e_i$ und

$$D^s/L \simeq D/(d_1) \oplus \dots \oplus D/(d_k) \oplus D \oplus \dots \oplus D$$

Für $d_i \in D^\times$ Einheit ist $D/(d_i) = 0$, also einfach weglassen. □

2.49 Korollar: Struktursatz für endlich erzeugte abelsche Gruppen

Ist A endlich erzeugte abelsche Gruppe, dann ist A direkte Summe von endlich vielen zyklischen Gruppen.

Beweis

Dies folgt unmittelbar aus der Tatsache, dass jede abelsche Gruppe ein \mathbb{Z} -Modul ist, vgl. Bemerkung 2.3 (iv). □

2.50 Definition und Satz

Setze $\text{tor}_D(M) := \{m \in M \mid \text{ann}(m) \neq 0\}$. Ist D kommutativ und nullteilerfrei, dann ist $\text{tor}_D(M)$ ein Untermodul, der **Torsionsmodul** von M .

Beweis

Ist $a \cdot m = 0$, dann ist $d \cdot a \cdot m = a \cdot d \cdot m$ also $d \cdot m \in \text{tor}(M)$ für alle $d \in D$. Sind $m_1, m_2 \in \text{tor}(M)$, also $am_1 = bm_2 = 0$, dann ist $ab(m_1 + m_2) = 0$. □

2.51 Satz

Ist M ein endlich erzeugter Modul über einem Hauptidealring D , dann ist

$$M \simeq \operatorname{tor}_D(M) \oplus D^k$$

und $\operatorname{tor}_D(M)$, k sind eindeutig bestimmt.

Beweis

Nach Satz 2.48 ist

$$M \simeq Dm_1 \oplus \dots \oplus Dm_s \oplus Dm_{s+1} \oplus \dots \oplus Dm_{s+k}$$

mit $\operatorname{ann}(m_i) \neq 0$ für $i = 1, \dots, s$ und $\operatorname{ann}(m_i) = 0$ für $i = s+1, \dots, s+k$. Ein Element $d_1m_1 + \dots + d_{s+k}m_{s+k} \in M$ ist ein Torsionselement genau dann, wenn $d_{s+1} = \dots = d_{s+k} = 0$ genau dann, wenn es in $Dm_1 \oplus \dots \oplus Dm_s$ liegt. Damit ist $\operatorname{tor}(M) = Dm_1 \oplus \dots \oplus Dm_s$. Es ist $M/\operatorname{tor}(M) \simeq D^k$ und k ist nach Satz 2.31 eindeutig bestimmt.

ich bin mir nicht
sicher, ob die
Nummer stimmt

2.52 Beispiel

- (i) Sei $D = \mathbb{Z}$, $M = \mathbb{R}/\mathbb{Z}$. $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$. Dann ist $\operatorname{tor}_{\mathbb{Z}}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, also gilt $(d \cdot r \in \mathbb{Z} \Rightarrow r \in \mathbb{Q})$

$$\mathbb{R}/\mathbb{Z} \simeq \mathbb{Q}/\mathbb{Z} \oplus \bigoplus \mathbb{Q}$$

- (ii) $D = \mathbb{Z}$, $M = \mathbb{Q}$, $\operatorname{tor}_{\mathbb{Z}}(\mathbb{Q}) = 0$, aber $(\mathbb{Q}, +)$ ist *kein* freier \mathbb{Z} -Modul: Seien $\frac{r}{s}, \frac{p}{q} \in \mathbb{Q}$. Dann ist $r \cdot p \in \mathbb{Z} \cdot r/s \cap \mathbb{Z} \cdot \frac{p}{q} \neq 0$.

2.53 Satz

Eine endlich erzeugte abelsche Gruppe ist direkte Summe einer endlichen Gruppe, der Torsionsgruppe, und einer freien abelschen Gruppe $\simeq \mathbb{Z}^k$. Dabei heißt k der Rang der Gruppe. Jede endliche abelsche Gruppe ist direkte Summe von zyklischen Gruppen.

3 Tensorprodukte und Algebren

Zuerst Tensorprodukte für Moduln über kommutativen Ringen R . Sind $U, V, W \in {}_R \text{Mod}$, $f : U \times V \rightarrow W$ bilinear, dann suchen wir ein universelles Objekt T und eine bilineare Abbildung φ so, dass es für jedes bilineare f und jedes W einen eindeutigen R -Modulhomomorphismus f' gibt, sodass das Diagramm kommutiert.

$$\begin{array}{ccc} U \times V & \xrightarrow{\varphi} & T \\ & \searrow f & \downarrow f' \\ & & W \end{array}$$

3.1 Satz

Sei R ein kommutativer Ring, $U, V \in {}_R \text{Mod}$. Dann existiert ein bis auf Isomorphie eindeutiger R -Modul $U \otimes V$ und eine bilineare Abbildung $\varphi : U \times V \rightarrow U \otimes V$, die universell für alle bilinearen Abbildungen $f : U \times V \rightarrow W$ sind.

Beweis

Eindeutigkeit ist klar: Seien T_1, φ_1 und T_2, φ_2 zwei universelle Objekte. Dann betrachte

$$\begin{array}{ccc} U \times V & \xrightarrow{\varphi_1} & T_1 \\ & \searrow \varphi_2 & \downarrow \varphi'_2 \\ & & T_2 \\ & \nearrow \varphi_1 & \downarrow \varphi'_1 \\ & & T_1 \\ & \searrow \varphi_2 & \downarrow \varphi'_2 \\ & & T_2 \end{array} \quad \begin{array}{c} \text{id} \\ \text{id} \end{array}$$

also $\varphi'_2 \circ \varphi'_1 = \text{id}_{T_2}$, $\varphi'_1 \circ \varphi'_2 = \text{id}_{T_1} \Rightarrow T_1 \simeq T_2$.

Für die Existenz sein $\mathcal{F}_{U \times V}$ der freie R -Modul mit Basis (indiziert durch) $U \times V$ und sei $B \subseteq \mathcal{F}_{U \times V}$ der Untermodul, der von allen Elementen der folgenden Form erzeugt wird

$$\begin{aligned} (u + u', v) - (u, v) - (u', v) \\ (u, v + v') - (u, v) - (u, v') \\ (\alpha \cdot u, v) - \alpha(u, v) \\ (u, \alpha \cdot v) - \alpha(u, v) \end{aligned}$$

für alle $u, u' \in U$, $v, v' \in V$, $\alpha \in R$. Sei φ die Hintereinanderausführung

$$0 \rightarrow U \times V \hookrightarrow \mathcal{F}_{U \times V} \rightarrow \mathcal{F}_{U \times V}/B \rightarrow 0$$

Offensichtlich ist φ bilinear: Es ist $\varphi((u, v + v')) = (u, v + v') + B$. Wegen $(u, v + v') = (u, v) + (u, v')$ in $\mathcal{F}_{U \times V}/B$ ist φ bilinear. Setze $U \otimes V := \mathcal{F}_{U \times V}/B$. Noch zu zeigen: $U \otimes V, \varphi$ erfüllen die universelle Eigenschaft: Sie also $f : U \times V \rightarrow W$ bilinear. Dann lässt sich wegen der universellen Eigenschaft des freien Moduls $\mathcal{F}_{U \times V}$ f fortsetzen zu $f_1 : \mathcal{F}_{U \times V} \rightarrow W$ (Satz 2.35)

$$\begin{array}{ccc} U \times V & \xrightarrow{\varphi} & \mathcal{F}_{U \times V} \\ & \searrow f & \downarrow f_1 \\ & & W \end{array}$$

Nach Definition von B folgt $B \subseteq \ker f$, denn es ist zB

$$f_1([(u + u', v) - (u, v) - (u', v)]) = f(u + u', v) - f(u, v) - f(u', v) = 0$$

da f bilinear ist. Ebenso ist

$$f_1([\alpha(u, v) - \alpha(u, v)]) = f(\alpha u, v) - \alpha f(u, v) = 0$$

Daher erhalten wir $f' : U \otimes V = \mathcal{F}_{U \times V} / B \rightarrow W$ und dieses f' ist eindeutig bestimmt, da die Bilder von (u, v) den Modul $U \otimes V$ erzeugen. \square

3.2 Bemerkung

Das Bild von (u, v) in $U \otimes V$ unter φ wird mit $u \otimes v$ bezeichnet. D.h. $U \otimes V$ ist R -Modul mit Erzeugermenge $\{u \otimes v \mid u \in U, v \in V\}$ und definiert Relationen

$$\begin{aligned}(u + u') \otimes v &= u \otimes v + u' \otimes v \\ u \otimes (v + v') &= u \otimes v + u \otimes v' \\ \alpha u \otimes v &= \alpha(u \otimes v) = u \otimes \alpha v\end{aligned}$$

für alle $u, u' \in U, v, v' \in V, \alpha \in R$.

Achtung

Nicht jedes Element in $U \otimes V$ ist von der Form $u \otimes v$, $u \in U, v \in V$! Ein allgemeines Element ist von der Form $\sum_{i=1}^k u_i \otimes v_i$ für $u_i \in U, v_i \in V, k \in \mathbb{N}$.

3.3 Proposition

Sei R ein kommutativer Ring, U, V, W seien R -Moduln. Dann gilt

- (i) $U \otimes V \simeq V \otimes U$
- (ii) $U \otimes (V \otimes W) \simeq (U \otimes V) \otimes W$
- (iii) $U \otimes (V \oplus W) \simeq (U \otimes V) \oplus (U \otimes W)$

Beweis

- (i) $f : U \times V \rightarrow V \times U, (u, v) \mapsto (v, u)$ ist bilinear. Daher existieren Homomorphismen $\alpha : U \otimes V \rightarrow V \otimes U, u \otimes v \mapsto v \otimes u$, d.h.

$$\alpha\left(\sum u_i \otimes v_i\right) = \sum v_i \otimes u_i$$

Ebenso ist $\beta : V \otimes U \rightarrow U \otimes V, v \otimes u \mapsto u \otimes v$ ein R -Modulhomomorphismus. Dann ist $\beta \circ \alpha = \text{id}_{U \otimes V}$ und $\alpha \circ \beta = \text{id}_{V \otimes U}$, d.h. α, β sind Isomorphismen.

- (ii) Betrachte $f : U \times V \times W \rightarrow U \otimes (V \otimes W), (u, v, w) \mapsto u \otimes (v \otimes w)$. Für festes $w \in W$ ist f bilinear in u, v und wir erhalten $f'_w : (U \otimes V) \rightarrow U \otimes (V \otimes W), (u \otimes v) \mapsto u \otimes (v \otimes w)$. Dann ist f'_w R -linear und wir erhalten eine bilineare Abbildung

$$\tilde{f} : (U \otimes V) \times W \rightarrow U \otimes (V \otimes W), ((u \otimes v), w) \mapsto u \otimes (v \otimes w)$$

Daraus erhalten wir $f' : (U \otimes V) \otimes W \rightarrow U \otimes (V \otimes W)$. Entsprechend erhalten wir Inverses $g' : U \otimes (V \otimes W) \rightarrow (U \otimes V) \otimes W$

- (iii) Sei $\varphi : U \times (V \oplus W) \rightarrow (U \otimes V) \oplus (U \otimes W), (u, v, w) \mapsto (u \otimes v, u \otimes w)$. Ist $f : U \times (V \oplus W) \rightarrow Z$ eine bilineare Abbildung in einen R -Modul Z , dann ist $f(u, v, w) = f(u, v) + f(u, w)$ und dies kann auch als Abbildung von $(U \otimes V) \oplus (U \otimes W)$ aufgefasst werden. Daher erfüllt $(U \otimes V) \oplus (U \otimes W)$ die erforderliche universelle Eigenschaft, d.h.

$$U \otimes (V \oplus W) \simeq (U \otimes V) \oplus (U \otimes W) \quad \square$$

3.4 Beispiel

(i) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{R}$ via $q \otimes r \mapsto q \cdot r$.

$$\sum_{i=1}^k \frac{m_i}{n_i} \otimes r_i = \sum \frac{\prod_{i=1}^k m_i}{n_i \prod_{j \neq i} m_j} \otimes r_i = \sum \frac{1}{\prod n_i} \otimes \left(m_i \prod_{j \neq i} n_j \right) = \frac{1}{\prod n_i} \otimes \left(\sum \dots \right)$$

(ii) Seien $r, s \in \mathbb{N}$, $(r, s) = 1$ und $mr + ns = 1$. Dann ist

$$\mathbb{Z}/(r) \otimes_{\mathbb{Z}} \mathbb{Z}/(s) = 0,$$

denn für jeden Erzeuger $a \otimes b$ gilt

$$\begin{aligned} a \otimes b &= (mr + ns)(a \otimes b) = mr(a \otimes b) + ns(a \otimes b) = m(ra \otimes b) + n(a \otimes sb) \\ &= m(0 \otimes b) + n(a \otimes 0) = 0 \end{aligned}$$

(iii) Ist A eine abelsche Torsionsgruppe, dann ist $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. Denn ist $a \in A$ mit $ma = 0$, dann ist

$$a \otimes \frac{p}{q} = a \otimes \frac{p \cdot m}{q \cdot m} = a \cdot m \otimes \frac{p}{q \cdot m} = 0$$

3.5 Satz

Sei R ein kommutativer Ring, $U \in {}_R \text{Mod}$. Dann ist $U \otimes R^n \simeq U^n = U \oplus \dots \oplus U$.

Beweis

Durch Induktion nach n : Wegen Proposition 3.3 (iii) genügt es, die Behauptung für $n = 1$ zu zeigen, also $U \otimes_R R \simeq U \simeq R \otimes_R U$.

Sei $\theta : R \times U \rightarrow U$, $(r, u) \mapsto r \cdot u$. Dann ist θ bilinear. Ist $W \in {}_R \text{Mod}$ und $f : R \times U \rightarrow W$ bilinear, dann ist $f(r, u) = f(1, r \cdot u)$, also ist mit $f' : u \mapsto f(1, u)$ gerade $f = \theta \circ f'$. Offensichtlich ist f' eindeutig bestimmt, d.h. U, θ erfüllen die universelle Eigenschaft aus Satz 3.1, also ist $R \otimes U \simeq U$ wegen der Eindeutigkeit. \square

3.6 Korollar

Sind U, V freie R -Moduln, R kommutativ, $U \simeq R^m, V \simeq R^n$. Dann ist $U \otimes V \simeq R^{n \cdot m}$.

Bemerkung

Für Vektorräume über Körpern gilt daher $\dim_K(U \otimes V) = \dim_K U \cdot \dim_K V$. Daher gilt $\{e_1, \dots, e_m\}, \{f_1, \dots, f_n\}$ Basen für U bzw. V , dann ist $\{e_i \otimes f_j \mid i = 1, \dots, m, j = 1, \dots, n\}$ eine Basis für $U \otimes V$.

3.7 Korollar

Ist $U \in {}_R \text{Mod}$, V ein freier R -Modul, R kommutativ. Dann hat jedes Element von $U \otimes V$ eine eindeutige Darstellung der Form $\sum u_i \otimes e_i$ mit $u_i \in U$, $\{e_i\}_{i \in I}$ Basis für V .

Vorsicht

Ist $\sum u_i \otimes v_i = 0$ in $U \otimes V$ und die v_i sind in V linear unabhängig über R . Dann folgt *nicht*, dass $u_i = 0$ gilt.

Sei $V' = \langle v_1, \dots, v_k \rangle \subseteq V$. Ist $\sum u_i \otimes v_i = 0$ in $U \otimes V'$, dann folgt $u_i = 0$. Die Einbettung $V' \hookrightarrow V$ induziert einen Homomorphismus

$$U \otimes V' \rightarrow U \otimes V$$

★

Achtung: Dieser Homomorphismus muss nicht injektiv sein!

Siehe Beispiel 3.4
(iii)

Beispiel

$2\mathbb{Z} \hookrightarrow \mathbb{Z}$ ist injektiv, aber bleibt *nicht* injektiv in

$$2\mathbb{Z} \otimes \mathbb{Z}/2 \rightarrow \mathbb{Z} \otimes \mathbb{Z}/(2) \simeq \mathbb{Z}/(2)$$

Seien e, f, f' Erzeuger der zyklischen Moduln $\mathbb{Z}/(2), \mathbb{Z}, 2\mathbb{Z}$. $2\mathbb{Z} \hookrightarrow \mathbb{Z}, f' \mapsto 2f$ und dann

$$f' \otimes e \mapsto 2f \otimes e = f \otimes 2e = 0$$

Bemerkung: Ist V' direkter Summand in V , dann bleibt nach Proposition 3.3 (iii) die induzierte Abbildung (\star) aber doch eine Einbettung. Über Körpern ist das immer der Fall.

3.8 Definition

Sei R ein kommutativer Ring. Eine R -Algebra ist ein Ring A , der gleichzeitig ein R -Modul ist, sodass die Multiplikation in A R -bilinear ist, d.h. so dass gilt:

$$\alpha(x \cdot y) = x \cdot \alpha y = (\alpha x) \cdot y \quad \forall x, y \in A, r \in R$$

Eine **Unteralgebra** einer R -Algebra A ist ein Unterring, der gleichzeitig ein R -Untermodul ist.

3.9 Beispiel

- (i) Ist A eine R -Algebra, dann ist das Zentrum $C(A) = \{z \in A \mid x \cdot z = z \cdot x \quad \forall x \in A\}$ eine Unteralgebra. $C(A)$ ist R -Untermodul: $z \in C(A)$, dann ist für $\alpha \in R, x \in A$

$$x \cdot (\alpha z) = (\alpha x) \cdot z = z \cdot (\alpha x) = (\alpha z) \cdot x$$

- (ii) Jeder Ring R ist auch R -Algebra:

- (iii) Jeder Ring wird zu einer \mathbb{Z} -Algebra durch $nx = x + \dots + x, (-n)x = -(nx)$

Ein Homomorphismus von R -Algebren ist ein Ringhomomorphismus, der gleichzeitig R -linear ist.

Bemerkung

Für $y = 1$ in Definition 3.8 ergibt sich $x \cdot \alpha 1 = \alpha x$ und für $x = 1$ $\alpha 1 \cdot y = \alpha \cdot y$. Also gilt $\alpha 1 \cdot x = x \cdot \alpha 1 = \alpha x$ für alle $x \in A, \alpha \in \mathbb{R}$. Für $\alpha = \beta \cdot 1$ erhalten wir

$$\alpha 1 \cdot \beta \cdot 1 = \alpha(\beta 1) = \alpha \beta \cdot 1,$$

d.h. die Abbildung $R \rightarrow A, \alpha \mapsto \alpha \cdot 1$ ist ein Algebrehomomorphismus in das Zentrum von A , d.h. $R \cdot 1 \subseteq C(A)$.

Umgekehrt gilt: Ist R ein Ring, $f : R \rightarrow C(A)$ ein Ringhomomorphismus. Dann wird A zu einer R -Algebra durch $\alpha \cdot x = f(\alpha) \cdot x$ für $x \in A, \alpha \in R$. Mit anderen Worten: Eine R -Algebra ist ein Ring A zusammen mit einem Homomorphismus $f : R \rightarrow C(A)$. Manchmal werden Algebren allgemeiner definiert: Eine R -Algebra ist ein R -Modul A mit einer bilinearen Multiplikation (nicht notwendig assoziativ oder mit Eins). Bei uns sind alle Algebren assoziativ und **unital**, d.h. mit 1.

3.10 Beispiel

Sei R ein kommutativer Ring.

- (i) $U \in {}_R \text{Mod}, A = \text{End}_R(U)$. Dann ist A ein R -Modul: Für $f \in A, \alpha \in R, x \in U$ ist

$$(\alpha f)(x) = f(\alpha x)$$

Damit wird A zu einer R -Algebra. Ist $V \simeq R^n$, dann ist $A \simeq M_n(R)$ und $C(A) \simeq R$, nämlich $\alpha \cdot 1, \alpha \in R$.

- (ii) $B_n(R)$ = Menge der oberen Dreiecksmatrizen ist Unter algebra von $M_n(R)$.
- (iii) Sei $M = \{u_i \mid i \in I\}$ ein Monoid (= Halbgruppe mit 1) und sei $A = \mathcal{F}_M$ der freie Modul über M mit Multiplikation $u_i \cdot u_j = u_k$ wie in M . Durch lineares Fortsetzen erhalten wir eine Multiplikation auf A , die A zu einer R -Algebra macht. Dann ist A assoziativ und unital, weil M diese Eigenschaften hat. Diese Algebra wird mit RM bezeichnet.

Häufig: $M = G$ eine Gruppe, $R = K$ ein Körper: Dann heißt KG die **Gruppenalgebra** von G über K . Spezialfälle:

- (a) $M = \{1, X, X^2, X^3, \dots\}$, $RM = R[X]$.
- (b) $G = Z = \langle X \rangle$. Dann ist $KG = K[X, X^{-1}]$ der Ring der Laurent-Polynome in X .

- (iv) Endlich dimensionale Algebra über einem Körper K : Ist A K -Algebra mit $\{u_1, \dots, u_n\}$, dann ist die Struktur von A eindeutig bestimmt durch die n^3 Strukturkonstanten c_{ijk} , $i, j, k = 1, \dots, n$ mit $u_i \cdot u_j = \sum_{k=1}^n c_{ijk} \cdot u_k$.

Ist $u_1 = 1_A$, dann ist $c_{1ir} = c_{i1r} = \delta_{ir}$ und die Assoziativität von A ist äquivalent zu

$$\sum_i c_{i,j,k} = \sum_{i,l,m} c_{lik} \cdot c_{mji}$$

Die Sätze über einfache Artinsche Ringe (Schur, Wedderburn, ...) gelten insbesondere für endlich dimensionale einfache K -Algebren.

- (v) Ist $U \in {}_R \text{Mod}$, dann sei $T(U) = \bigoplus_{n \in \mathbb{N}} U^{\otimes n}$, mit $U^{\otimes n} = U \otimes \dots \otimes U$, $U^{\otimes 0} = R$. Dann heißt $T(U)$ die **Tensoralgebra** von U .

Ist $U = R$, dann ist $T(U) \simeq R[X]$.

3.11 Definition

Eine **Darstellung** der R -Algebra A ist (gegeben durch) einen R -Algebrenhomomorphismus $A \rightarrow \text{End}_R(U)$ für einen R -Modul U . Für jede Algebra A bezeichnet man mit ρ die rechts-reguläre Darstellung A auf sich selbst, d.h.

vgl. $G \rightarrow \text{Sym}(X)$
in Def. 1.1

$$\rho : A \rightarrow \text{End}_R(A), \quad a \mapsto \rho_a : x \mapsto x \cdot a$$

Diese Darstellung ist treu, d.h. $\ker \rho = 0$. Ist A endlich dimensionale Algebra über einem Körper K mit Basis $\{u_1, \dots, u_n\}$, dann ist $\text{End}_K(A) \simeq M_n(K)$. Für $a = \sum \alpha_i u_i \in A$ wird dann ρ_a beschrieben durch die Matrix $(\rho_a)_{ij}$ mit

$$(\rho_a)_{ij} = \sum_{k=1}^n \alpha_k \cdot c_{ijk}$$

mit c_{ijk} wie in 3.10 (iv).

3.12 Korollar

Jede n -dimensionale K -Algebra ist isomorph zu einer Unter algebra von $M_n(K)$.

Beweis

$A \simeq \text{Im } \rho \subseteq \text{End}_K(A) \simeq M_n(K)$. □

3.13 Satz

Ist R ein kommutativer Ring, dann ist für R -Algebren A, B auch $A \otimes B$ eine R -Algebra mit $\mu(A \otimes B) \times (A \otimes B) \rightarrow A \otimes B$, $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ und linearer Fortsetzung. Die Tensoralgebra $A \otimes B$ ist genau dann kommutativ, assoziativ bzw. unital, wenn A und B kommutativ, assoziativ und unital sind.

Beweis

Es genügt nachzurechnen, dass diese Multiplikation bilinear ist und die Eigenschaften von A, B sich übertragen. \square

3.14 Beispiel

Sei K ein Körper, $E \supseteq K$ eine Körpererweiterung und eine K -Algebra A gegeben. Dann ist $A \otimes E$ eine E -Algebra mit $\dim_E(A \otimes E) = \dim_K(A)$ nach Beispiel 3.9, denn $1 \otimes E \subseteq C(A \otimes_K E)$ und für eine K -Basis $\{u_1, \dots, u_n\}$ von A ist $\{u_1 \otimes 1, \dots, u_n \otimes 1\}$ eine E -Basis für $E =: A_E$. Man sagt: A_E entsteht aus A durch Erweiterung der Skalare.

4 Darstellungstheorie endlicher Gruppen

Index

Die Seitenzahlen sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar 

R -Modul-Homomorphismus, 11

Annulatorideal, 25
artinsch, 12
auflösbar, 6
auflösbare Länge, 8

Bahn, 2
Basis (Modul), 19

Darstellung, 31

einfach, 11
endlich erzeugt, 11
Endomorphismenring, 10
entgegengesetzte Ring, 17
erzeugte Untermodul, 11
exakte Folge, 12
exakte Sequenz, 12

frei, 19

Gruppenalgebra, 31
Gruppenwirkung, 2
 reguläre, 2
 transitive, 2
 treue, 2

halbeinfach, 14
Hauptidealring, 22

Ideal, 10
invariante Basislänge, 21
invarianten Faktoren, 24
irreduzibel, 11

Kern der Wirkung, 2
Kommutator, 8
Kommutatorgruppe, 8
Kompositionsreihe, 5
kurze exakte Sequenz, 12

linear unabhängig in Moduln, 19

Minor, 24
Modulstruktur, 10

nilpotent, 6

noethersch, 12
Normalreihe, 5

obere Zentralreihe, 7

p -Sylowgruppe, 3
projektiv, 20

Rang, 24

semidirektes Produkt, 9
spaltet, 20
Stabilisator, 2

Tensoralgebra, 31
Torsionselement, 25
Torsionsmodul, 25

unital, 30
universelle Eigenschaft, 19
Unteralgebra, 30
untere Zentralreihe, 8
Untermodul, 11

Verbandsisomorphismus, 12

Zentralisator, 2
Zentrum, 2
zyklisch, 11

äquivalent, 5

Abbildungsverzeichnis