WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

BTsync:

Skript Höhere Algebra I

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

Jannes Bantje

18. Mai 2014
Erstellt mit XƎLaTeX

Inhaltsverzeichnis

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 $\varphi : G \to \mathrm{Sym}(X)$. $\ker \varphi$ 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 $\ker \varphi = \{1\}$.

1.2 Bemerkung

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

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

Wiederholung Isomorphiesätze[1]

1. **Isomorphiesatz:** Ist $\varphi : G \to H$ surjektiv, dann ist $H \simeq G/\ker\varphi$. Allgemein ist für jeden Homomorphismus $\varphi : G \to H$ dann $\mathrm{Im}\,\varphi \simeq G/\ker\varphi$. (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 $G/N \big/ K/N \simeq G/K$. (”kürzen mit N”)

$HN = \{hn \mid h \in H, n \in N\}$ ist Untergruppe, da $HN = NH$ für N normal

Die letzten beiden Sätze lassen 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**.

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

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. $\kappa : G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, $g \mapsto \kappa_g$, 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 $G_x = \left\{g \in G \,\middle|\, g^{-1} \cdot x \cdot g = x\right\} = Z_G(x)$ 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 $\varphi : G \to \mathrm{Sym}(X)$.

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

[1] siehe auch http://de.wikipedia.org/wiki/Isomorphiesatz

1.4 Bahnengleichung

Setze $G(X) = \{G(x)\,|\,x \in X\}$. Dann ist $X = \dot{\bigcup}\{G(x)\,|\,G(x) \in G(X)\}$. 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 $K_G = \{G(x)\,|\,x \in G\}$ = Menge der Konjugationsklassen. Sei $K_G^* = \{G(x)\,|\,x \in G \backslash Z(G)\} = \{G(x)\,|\,|G(x)| \geq 2\}$. Für jede endliche Gruppe G gilt dann nach 1.4

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

1.6 Korollar

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

Beweis
Nach Lagrange[2] 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 $p \mid |Z(G)|$. □

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 $n_p \equiv 1 \mod p$.

(iii) Alle p-Sylowgruppen sind konjugiert.

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

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

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 $p \nmid m \cdot k_1 \cdots k_{p^a - 1} = |S|$.

[2] Ordnung 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 $P \cdot P_1 \leq G$. Wegen[3] $|P \cdot P_1| = \frac{|P| \cdot |P_1|}{|P \cap P_1|}$ 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 $|T| = 1 \mod p$.

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 $P_2 = P_2 \cdot P' = P' \in T$ $\lightning$. Daher hat P_2 auf T keinen Fixpunkt. Dann folgt aber $p \mid |T|$ $\lightning$ Damit sind alle p-Sylowgruppen in T enthalten, d.h. $|T| = n_p = 1 \mod p$.

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

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

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 $N_G(P) = \left\{ g \in G \,\middle|\, P^g = g^{-1} \cdot P \cdot g = P \right\}$.

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

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

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 $|N : P \cap N| \overset{\text{2. Iso}}{=} |PN : P|$ 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 $\left({}^{H_i}/_{H_{i+1}}\right)_{i\leq n-1}$ nach geeigneter Permutation isomorph sind zu dem Quotienten $\left({}^{K_j}/_{K_{j+1}}\right)_{j\leq n-1}$.

1.12 Beispiel

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

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.

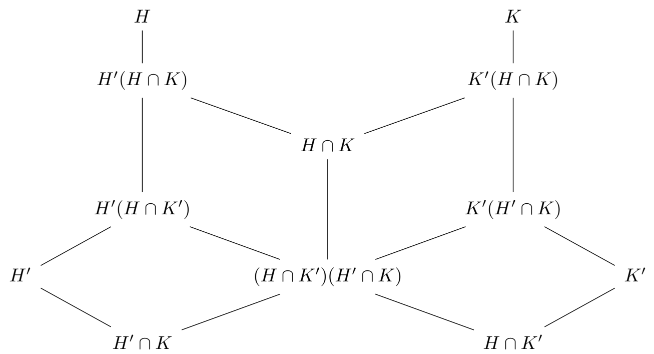
Für den Beweis brauchen wir

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 $M \trianglelefteq N \cdot M = H'(H \cap K)$.

<u>Behauptung:</u> Es ist $N \cap M = (H \cap K) \cap \big(H'(H \cap K')\big) = (H' \cap K)(H \cap K')$.

"$\subseteq$": 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:

$$^{NM}/_{M} \overset{\text{2. Iso}}{\simeq} {^{N}}/_{N\cap M} = {^{(H\cap K)}}/_{(H'\cap K)(H\cap K')}$$

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. □

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

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

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! □

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 $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ abelsche Normalreihe, $H \leq G$, dann ist $1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \ldots \trianglelefteq G_n \cap H = H$ 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 $({^{G_iN}}/_{N})$ abelsche Normalreihe für ${^G}/_N$, denn es ist

$$^{(G_{i+1}N/N)}/_{(G_iN/N)} \simeq {^{G_{i+1}N}}/_{G_iN} \simeq {^{G_{i+1}}}/_{G_{i+1}\cap(G_iN)}$$

ein Quotient von ${^{G_{i+1}}}/_{G_i}$ und daher abelsch. (Da $G_i \leq G_{i+1} \cap (G_iN)$, ist ${^{G_{i+1}}}/_{G_i} \to {^{G_i+1}}/_{G_{i+1}\cap G_iN}$ ein Epimorphismus und daher ist die rechte Seite abelsch.) □

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:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = N, \qquad {}^{K_0}/_{N} = N \trianglelefteq {}^{K_1}/_{N} \trianglelefteq \ldots \trianglelefteq {}^{K_m}/_{N} = {}^{G}/_{N}$$

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

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. □

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

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

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 ${}^{G_{i+1}}/_{G_i} \to {}^{G_i+1}/_{G_{i+1} \cap G_i N}$ ein Epimorphismus und daher ist die rechte Seite abelsch.) □

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

$$H_2 := \pi^{-1}_{Z(G)}\left(Z({}^{G}/_{Z(G)})\right) \quad \text{usw.}$$

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 $\varphi : G \to H$, 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 $[K,H] := \big\langle [k,h] | k \in K, h \in H \big\rangle$. Ist $K \leq N_G(H)$, dann ist $[K,H] \leq H$, denn $k^{-1} \cdot h^{-1} \cdot k \cdot h = \left(h^{-1}\right)^k \cdot h \in H$. Die Gruppe $G' = [G,G] = \big\langle [g,h] | g,h \in G \big\rangle$ heißt **Kommutatorgruppe** von G.

1.24 Satz

(i) $G' \trianglelefteq G$

(ii) G/G' ist abelsch.

(iii) Ist $\varphi : G \to A$ 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 $\varphi : G \to G/N$, $G' \leq \ker \varphi = N$

1.25 Definition

Wir setzen $G^{(0)} = G$, $G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right]$. 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

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

"⇒": 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 $G^{[0]} = G$, $G^{[i]} = \left[G^{[i-1]}, G\right]$. 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 $1 = N_0 \leq N_1 \ldots \leq N_n = G$ 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 $i = 1, \ldots, n$, 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 $\varphi : N \times H \to G$, $(n, h) \mapsto n \cdot h$ bijektiv, d.h. für jedes $g \in G$ existiert ein eindeutig bestimmtes $n \in N, h \in H$ mit $n \cdot h = g$. Denn 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, $\varphi : H \to \mathrm{Aut}(N)$ ein Homomorphismus, dann definiere eine Verknüpfung auf der Menge $G = N \times H$ durch

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

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 $\varphi : H \to \mathrm{Aut}(N)$, $h \mapsto \kappa_h$ (Konjugation mit h).

2 Moduln: Halbeinfache Moduln, freie, projektive und injektive Moduln, Tensorprodukte

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 $\mathrm{End}(A) = \mathrm{Hom}(A, A)$ ein Ring

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$
$$(\varphi \cdot \psi)(x) = \varphi(\psi(x))$$

$\mathrm{End}(A)$ 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 $R \to \mathrm{End}(A), a \mapsto \lambda_a$ mit $\lambda_a : A \to A, x \mapsto a \cdot x$ 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 $R \times M \to M, (r, m) \mapsto r \cdot m$ 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 $\varphi : R \to \mathrm{End}(M, +)$ 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. $\varphi : R \to \mathrm{End}(R)$, $r \mapsto \lambda_r$.

(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 $\bigcap_{\alpha \in J} N_\alpha$ 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

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

  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

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

(ii) 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 ${}_R\mathrm{Mod}$. Sind $M, N \in {}_R\mathrm{Mod}$ und $\varphi : (M,+) \to (N,+)$ ein Homomorphismus (der additiven Gruppen), dann ist φ ein R-**Modul-Homomorphismus**, falls *φ ist R-linear*

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

2.8 Bemerkung

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

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

und $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$ 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 $f : M \to N$ ein R-Modul-Homomorphismus, $M' \subseteq M$ Untermodul mit $M' \subseteq \ker f$, dann existiert ein eindeutiger R-Modul-Homomorphismus $f' : {}^{M}\!/_{M'} \to N$ mit

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"] & N \\ {}^{M}\!/_{M'} \arrow[ur, dashed, "f'"'] & \end{tikzcd}$$

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 $f' : {}^{M}\!/_{M'} \to N$, $m + M' \mapsto f(m)$ R-linear ist. Das folgt sofort

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

(ii), (iii) Übungsaufgabe. □

2.10 Definition (Sprechweise)

Eine Folge von R-Moduln (M_i) und Homomorphismen $f_i : M_i \to M_{i-1}$ 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

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

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.

[4] nach Emmy Noether, 1882-1935, siehe `http://de.wikipedia.org/wiki/Emmy_Noether`
[5] nach 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 $x_1, x_2, \ldots \in N$ mit $x_i \notin \langle x_1, \ldots, x_{i-1} \rangle =: N_{i-1}$. Dann ist (N_i) eine echt aufsteigende Kette und muss — da M noethersch ist — nach endlich vielen Schritten mit $\langle x_1, \ldots, x_k \rangle = N$ enden. Das heißt N ist endlich erzeugt.

"$\Leftarrow$": Sei $N_0 \subseteq N_1 \subseteq \ldots$ eine echt aufsteigende Kette von Untermoduln in M und $N := \sum N_i$. Da N endlich erzeugt ist, existieren $x_1, \ldots, x_r \in N$ mit $N = \langle x_1, \ldots, x_r \rangle$. Dann existiert ein k mit $x_1, \ldots, x_r \in N_k$; 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 $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ 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 $P_0 \supseteq P_1 \supseteq P_2 \supseteq \ldots$ eine echt absteigende Kette in M. Dann betrachte

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

in M' und

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

in M/M'. Nach Vorraussetzung 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 $0 \to N \hookrightarrow M \twoheadrightarrow M/N \to 0$. 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. artinschen) 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

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

Nach Induktionsvorraussetzung ist M' noethersch (artinsch) und M/M' ist zyklisch, daher auch noethersch (artinsch), nach 2.13 ist M noethersch (artinsch). □

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
$$M = \bigoplus_{\alpha \in I'} N'_\alpha$$
d.h. $N'_\alpha \cap \sum_{\beta \neq \alpha} N'_\beta = 0$

Beweis (mit Lemma 2.20)

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

<u>Behauptung:</u> $M_1 = M$. 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 $N \subseteq P$ $\lightning$ zu $N \in \{N_\alpha\}_{\alpha \in I}$.

"(iii)⇒(ii)": Klar.

"(ii)⇒(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). $\lightning$ Maximalität von J. Daher ist $N_\alpha \subseteq M_1$, also $M_1 = M$.

"(ii)⇒(iii)": folgt aus dem Beweis "(i) ⇒ (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)⇒(ii)⇒(iii)⇒(iv)" Klar.

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

"(iii)⇒(i)": Sei $M \in {}_R\mathrm{Mod}$, 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 $\alpha \in I$. *aber nicht unbedingt gleich N_α*

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

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

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 $\pi \in \mathrm{Sym}(K)$ 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 Induktionsvorraussetzung folgt die Behauptung. □

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 $S_{j1}, \dots, S_{jk}$ mit $x_j \in \bigoplus_{i=1}^k S_{ji}$, also ist M die Summe von endlich vielen S_i, d.h. $|J|$ endlich. □

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, $\overline{I} := \{x_{11} \mid (x_{ij}) \in I\}$ die Menge aller $(1,1)$-Koeffizienten in $X \in I$. Man rechnet leicht nach, dass $\overline{I} \trianglelefteq R$ 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 $x_{s,t} \in \overline{I}$. Daher ist $I \subseteq M_k(\overline{I})$.

Noch zu zeigen: $M_k(\overline{I}) \subseteq I$. Sei also $Y \in M_k(\overline{I})$. 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. $I = M_k(\overline{I})$. □
Matrizenringe über Körpern und Schiefkörpern sind einfache Ringe.

2.26 Satz (Schurs Lemma)

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

Beweis
Wegen $M \neq 0$ ist $\mathrm{End}_R(M) \neq 0$. Ist $\varphi \in \mathrm{End}_R(M) \setminus \{0\}$, 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 $\mathrm{End}_R(M)$. □

2.27 Lemma

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

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

Insbesondere ist

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

Beweis
Seien $e_j : M_j \to M$ die Einbettungen, $\pi_i : M \to M_i$ die Projektionen. Dann ist für jeden Endomorphismus $\varphi \in \mathrm{End}_R(M)$ mit $\varphi_{i,j} := \pi_i \circ \varphi \circ e_j \in \mathrm{Hom}(M_j, M_i)$ 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. □

2.28 Definition + Lemma

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

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

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

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

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)⇒(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 $Rc \to Rcr$, $s \cdot c \mapsto s \cdot c \cdot r$ 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)⇒(iii)": $(R, +)$ ist als Links-R-Modul endlich erzeugt (sogar zyklisch, $R = R \cdot 1$). Daher ist nach Vorraussetzung

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

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

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

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

"(iii)⇒(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). □

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 $\mathrm{Hom}_R(M, N) = 0$. (Klar!)

2.31 Satz (2. Struktursatz von Wedderburn)

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

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

als Ringisomorphismus.

Beweis
$(R,+) \simeq L_1^{k_1} \oplus \ldots \oplus L_l^{k_l}$ mit $L_i \subseteq R$ minimale Linksideale, L_i paarweise nicht isomorph. Dann ist *nach Bemerkung 2.30*

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

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

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

Freie Moduln

2.32 Definition

Sei M ein Links-R-Modul. Elemente $x_1, \ldots, x_n \in M$ heißen R-**linear unabhängig**, wenn gilt: Sind $\alpha_1, \ldots, \alpha_n \in R$ mit $\sum \alpha_i \cdot x_i$, dann ist $\alpha_i = 0$ für $i = 1, \ldots, n$.
Sonst heißen $x_1, \ldots, x_n$ linear abhängig. Eine (beliebige Menge) $X \subseteq M$ heißt linear unabhängig, wenn jede endliche Teilmenge linear abhängig ist. Eine linear unabhängige Menge von Erzeugern heißt **Basis** für M. (äquivalent dazu: minimale erzeugende Menge)

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

$$\begin{tikzcd} I \arrow[r, "\varphi"] \arrow[dr, "f"'] & \mathcal{F}_I \arrow[d, dashed, "f'"] \\ & M \end{tikzcd}$$

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

$$f'\Big(\sum \alpha_i u_i\Big) = \sum \alpha_i f(i) \tag{$\star$}$$

Daher folgt die Existenz von f' und die Eindeutigkeit ebenfalls. □

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 $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ eine kurze exakte Sequenz, M'' ein freier R-Modul, dann **spaltet** die Sequenz, d.h. es existiert ein R-Modulhomomorphismus $\sigma : M'' \to M$ mit $\beta \circ \sigma = \mathrm{id}_{M''}$. 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 $f : I \to M$, $i \mapsto u_i$ lässt sich fortsetzen zu $\sigma : M'' \to M$ (2.35) und dann gilt $\beta \circ \sigma = \mathrm{id}_{M''}$. Damit ist $M = \operatorname{Im}\alpha \oplus \operatorname{Im}\sigma \simeq M' \oplus M''$. □

2.37 Satz

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

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

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

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

mit $\mathcal{F} \simeq {}^R/_I$ eine exakte Sequenz mit $\mathcal{F}$ zyklisch und daher frei nach Vorraussetzung. 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)⇒(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)⇒(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)⇒(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)$_R$. □

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

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

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, $\mathrm{End}_R(V)$ 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. □

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 $\varphi : S \to R$ 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

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

Hier fehlt noch eine Zeichnung mit Blockmatrizen!

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

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

Es gilt $\det(\tilde{B}\tilde{A}) = \det \ = 1$ 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). $\lightning$

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 $n \geq m$, 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 $\varphi : D \to Da$, $s \mapsto s \cdot a$ (Isomorphismus, da D nullteilerfrei).

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

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

[6] englisch: PID, prime ideal domain

Fall 1: $\pi(L) = 0$, dann ist $L \subseteq \ker \pi = 0 \oplus D^m \simeq D^m$ und nach Induktionsvorraussetzung 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

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

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

Ist D ein Hauptidealring, M endlich erzeugt über D, $M = Dm_1 + \ldots + Dm_s$. Betrachte $\varphi : D^s \to M$ mit $(d_1, \ldots, d_s) \mapsto \sum d_i m_i$. 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

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

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 $a = p_1 \cdot \ldots \cdot p_s$ 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
- Spalten von A vertauschen
- Zeilen/Spalten mit Einheiten multiplizieren
- 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 üben 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 $a_1 1 \nmid a_{12}$. Sei $d \in \mathrm{ggT}(a_{11}, a_{12})$, 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 $e \cdot y - fx\cdot = 1$. 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 $\left(\begin{smallmatrix} x & e \\ y & f \end{smallmatrix}\right)$ ist invertierbar. Es gilt

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

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

Hier fehlen noch ein paar Matrizen

$$matrixhier$$

und $l(\tilde{a_1}1) \leq l(b_{ij})$ 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 $d_i x + d_{i+1} y = d_i' \in \mathrm{ggT}(d_i, d_{i+1})$. Wie eben erhalten wir $\begin{pmatrix} d_i' & 0 \\ 0 & d_{i+1}f \end{pmatrix} \rightsquigarrow \dots$ fertig. □

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 $P \in D^{m \times m}$ sin 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

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

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

3 Algebren: Einfache Algebren, Tensorprodukte, äußere Algebra

4 Darstellungstheorie endlicher Gruppen

Index

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

Abbildungsverzeichnis