Westfälische Wilhelms-Universität Münster

Fachbereich 10 Mathematik und Informatik

Skript Höhere Algebra I.

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

Jannes Bantje

2. Dezember 2015

Aktuelle Version verfügbar bei

GitHub

`https://github.com/JaMeZ-B/latex-wwu`

GitHub ist eine Internetplattform, auf der viele OpenSource-Projekte gehostet werden. Diese Plattform nutzen wir zur Zusammenarbeit, also findet man hier neben den PDFs auch die TEX-Dateien. Außerdem ist über diese Plattform auch direktes Mitarbeiten möglich, siehe nächste Seite.

sciebo die Campuscloud

`https://uni-muenster.sciebo.de/public.php?service=files&t=965ae79080a473eb5b6d927d7d8b0462`

Sciebo ist ein Dropbox-Ersatz der Hochschulen in NRW, der von der Uni Münster in leitender Position auf Basis der OpenSource-Software Owncloud aufgebaut wurde. Wenn man auf den Link klickt, kann man die Freigabe zum eigenen Speicher hinzufügen und hat dann immer automatisch die aktuellste Version.

Bittorrent Sync

`B6WH2DISQ5QVYIRYIEZSF4ZR2IDVKPN3I`

BTSync ist ein peer-to-peer Dateisynchronisations-Tool. Dabei werden die Dateien nur auf den Computern der Teilnehmer an einer Freigabe gespeichert. Ein RasPi ist permanent online, sodass stets die aktuellste Version verfügbar ist. `Clients` gibt es für jedes Betriebssystem. Zugang ist über das obige „Secret“ bzw. den QR-Code möglich.

Vorlesungshomepage

`http://wwwmath.uni-muenster.de/u/franziska.jahnke/ha/`

Hier ist ein Link zur offiziellen Vorlesungshomepage.

Vorwort — Mitarbeit am Skript

Dieses Dokument ist eine Mitschrift aus der Vorlesung „Höhere Algebra I., SoSe 2014“, gelesen von Prof. Dr. Dr. Katrin Tent. Der Inhalt entspricht weitestgehend dem Tafelanschrieb. Für die Korrektheit des Inhalts übernehme ich keinerlei Garantie! Für Bemerkungen und Korrekturen – und seien es nur Rechtschreibfehler – bin ich sehr dankbar. Korrekturen lassen sich prinzipiell auf drei Wegen einreichen:

- Persönliches Ansprechen in der Uni, Mails an `j.bantje@wwu.de` (gerne auch mit annotieren PDFs) oder Kommentare auf `https://github.com/JaMeZ-B/latex-wwu`.
- *Direktes* Mitarbeiten am Skript: Den Quellcode poste ich auf GitHub (siehe oben), also stehen vielfältige Möglichkeiten der Zusammenarbeit zur Verfügung: Zum Beispiel durch Kommentare am Code über die Website und die Kombination Fork + Pull Request. Wer sich verdient macht oder ein Skript zu einer Vorlesung, die ich nicht besuche, beisteuern will, dem gewähre ich gerne auch Schreibzugriff.

  Beachten sollte man dabei, dass dazu ein Account bei `github.com` notwendig ist, der allerdings ohne Angabe von persönlichen Daten angelegt werden kann. Wer bei GitHub (bzw. dem zugrunde liegenden Open-Source-Programm „`git`“) – verständlicherweise – Hilfe beim Einstieg braucht, dem helfe ich gerne weiter. Es gibt aber auch zahlreiche empfehlenswerte Tutorials im Internet.[1]
- *Indirektes* Mitarbeiten: TeX-Dateien per Mail verschicken.

  Dies ist nur dann sinnvoll, wenn man einen ganzen Abschnitt ändern möchte (zB. einen alternativen Beweis geben), da ich die Änderungen dann per Hand einbauen muss! Ich freue mich aber auch über solche Beiträge!

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] zB. `https://try.github.io/levels/1/challenges/1`, ist auf Englisch, aber dafür interaktives LearningBy-Doing

Inhaltsverzeichnis

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 $\varphi : G \to \operatorname{Sym}(X)$. $\ker\varphi$ heißt ***Kern der Wirkung***. Wir schreiben auch kurz $g(x)$ für $\varphi(g)(x)$.
- Für $x \in X$ heißt $G_x = \{g \in G \mid g(x) = x\} \leqslant G$ 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 $\ker\varphi = \{1_G\}$.

Für eine alternative Definition siehe Anhang A.1 auf Seite 51.

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

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 $\operatorname{Im}\varphi \simeq {}^{G}/_{\ker\varphi}$. (Homomorphiesatz)

2. Isomorphiesatz: Ist $H \leqslant G, N \trianglelefteq G$, dann ist ${}^{H}/_{(H\cap N)} \simeq {}^{HN}/_{N}$. ("Erweitern mit N")

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

3. Isomorphiesatz: Sind $N, K \trianglelefteq G, N \leqslant K$, 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***.

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

Gruppenhomomorphismus[2]: $\rho_{gh}(x) = x \cdot g \cdot h = \rho_h \circ \rho_g(x)$.

(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. $\kappa : G \to \operatorname{Aut}(G) \leqslant \operatorname{Sym}(G)$, $g \mapsto \kappa_g$, wobei $\kappa_g(x) = g^{-1} \cdot x \cdot g$

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

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 $\varphi : G \to \operatorname{Sym}(X)$.

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

[2] Beachte: Die Addition in $\operatorname{Sym}(X)$ ist die *linksseitige* Komposition von Abbildungen! Wir wollen also, dass $g \cdot h$ folgendermaßen wirkt: Zuerst g wirken lassen und dann h.

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

1.4. Bahnengleichung Es gilt: $X = \dot{\bigcup}\{G(x) \mid x \in X\}$, denn für jedes $x \in X$ ist $x \in G(x)$. 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 $K_G = \{G(x) \mid x \in G\}$ die Menge der Konjugationsklassen. Sei $K_G^* = \{G(x) \mid x \in G \backslash Z(G)\} = \{G(x) \mid |G(x)| \geqslant 2\}$. Für jede endliche Gruppe G gilt dann nach 1.4

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

1.6. Korollar G endlich, $|G| = p^m$, p prim, $m \geqslant 1 \Rightarrow Z(G) \neq 1$. Also haben p-Gruppen ein nicht-triviales Zentrum.

Beweis: Nach Lagrange[3] gilt für jedes $x \in G$, dass $|Z_G(x)| = p^k$ für ein $k \leqslant m$, also ist $[G : Z_G(x)] = p^{m-k}$. Für $x \notin Z(G)$ gilt dabei insbesondere $k < m$, denn aus $k = m$ würde $x \in Z(G)$ folgen. Wegen $p \mid |G|$ und $|Z(G)| \geqslant 1$ 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 $H \leqslant G$ 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 $S := \{X \subset G \mid |X| = p^a\}$. G operiert auf S durch Rechtsmultiplikation. Es ist

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

Behauptung: $p \nmid |S|$. Betrachte dazu $k_i := \frac{p^a \cdot m - i}{i}$, für $1 \leqslant i < p^a$. 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. nach vollständigem Kürzen von k_i ist dessen Zähler nicht durch p teilbar. Damit ist $p \nmid m \cdot k_1 \cdots k_{p^a - 1} = |S|$.
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

siehe Bahnengleichung 1.4

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

Daher gilt $p \nmid |{}^{G}/_{P}|$, also $p^a \mid |P|$. Andererseits ist $|P| \leqslant p^a$, 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.

[3] Ordnung einer Untergruppe teilt die Gruppenordnung. Die Umkehrung gilt nicht!

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 $i \leqslant a$. 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 $P \cdot P_1 \leqslant G$. Wegen[4] $|P \cdot P_1| = \frac{|P| \cdot |P_1|}{|P \cap P_1|}$ ist $P \cdot P_1$ eine p-Untergruppe von G. Wegen $P \leqslant P \cdot P_1$ 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 $P_2 \leqslant G$ 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 $H \leqslant G$ 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. $H \leqslant P'$.

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 $P \leqslant G$ besitzt, dann ist $P \trianglelefteq G$.

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

Beweis: Sei $g \in G$. Dann ist $P^g \leqslant H^g = H$ 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 $H_1, H_2 \leqslant G$, $H_2 \leqslant N_G(H_1)$, dann ist $H_1 \cdot H_2 = H_2 \cdot H_1 \leqslant G$.

Beweis: Für alle $h_1 \in H_1$ und $h_2 \in H_2$ gilt:

$$h_1 \cdot h_2 = h_2 \cdot \underbrace{h_2^{-1} \cdot h_1 \cdot h_2}_{\in H_1} \quad \text{und} \quad h_2 \cdot h_1 = \underbrace{h_2 \cdot h_1 \cdot h_2^{-1}}_{\in H_1} \cdot h_2. \qquad \square$$

1.10. Bemerkung Offensichtlich gilt für eine endliche Gruppe G, $P \leqslant G$ 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. Es ist $({}^{G}/_{N})/({}^{PN}/_{N}) \overset{\text{3. Iso}}{\simeq} {}^{G}/_{PN}$, und $[G : PN] \mid [G : P]$ teilerfremd zu p. Wegen $[PN : N] = [P : (P \cap N)]$ ist ${}^{PN}/_{N}$ eine p-Gruppe. $\square$

1.11. Definition Eine Folge von Untergruppen $(H_i)_{0 \leqslant i \leqslant n}$ 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[5] für alle $i < n$, dann heißt die Folge ***Kompositionsreihe***. Zwei Normalreihen $(H_i)_{i \leqslant n}$, $(K_j)_{j \leqslant m}$ heißen ***äquivalent***, falls $n = m$ und die auftretenden Quotienten $({}^{H_i}/_{H_{i+1}})_{i \leqslant n-1}$ nach geeigneter Permutation isomorph sind zu den Quotienten $({}^{K_j}/_{K_{j+1}})_{j \leqslant n-1}$.

[4] $P \cdot P_1$ ist Untergruppe, da P P_1 normalisiert

[5] Eine Gruppe G heißt einfach, wenn sie G und $\{1_G\}$ als einzige Normalteiler hat.

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. hat $\mathbb{Z}$ *keine* Kompositionsreihe.

(ii) Eine Normalreihe ist genau dann eine 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 $(H_i)_{i\leqslant n}$ und $(K_j)_{j\leqslant m}$. Dann sind die Reihen äquivalent.

Für den Beweis brauchen wir

1.14. Schmetterlings-Lemma (Zassenhaus) Sei G eine Gruppe, $H, K \leqslant G$ 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.

$$\begin{tikzcd}[column sep=small]
 & H \arrow[d, dash] & & K \arrow[d, dash] & \\
 & H'(H\cap K) \arrow[dr, dash] \arrow[dd, dash] & & K'(H\cap K) \arrow[dl, dash] \arrow[dd, dash] & \\
 & & H\cap K \arrow[dd, dash] & & \\
 & H'(H\cap K') \arrow[dl, dash] \arrow[dr, dash] & & K'(H'\cap K) \arrow[dl, dash] \arrow[dr, dash] & \\
H' \arrow[dr, dash] & & (H\cap K')(H'\cap K) \arrow[dl, dash] \arrow[dr, dash] & & K' \arrow[dl, dash] \\
 & H'\cap K & & H\cap K' &
\end{tikzcd}$$

Beweis: Setze $N := H\cap K$ und $M := H'(H\cap K')$. Dann gilt $N \leqslant N_G(M)$ wegen $H' \trianglelefteq H, K' \trianglelefteq K$ und daher $M \trianglelefteq N\cdot M = H'(H\cap K)$.
Behauptung: Es ist $N\cap M = (H\cap K)\cap \big(H'(H\cap K')\big) = (H'\cap K)(H\cap K')$.

"$\subseteq$": 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 $(H_i)_{i\leqslant n}$, $(K_j)_{j\leqslant m}$ 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 $(H_i)_{i\leqslant n}$ gibt mit $H_i \trianglelefteq G$ und $H_i/H_{i+1} \leqslant Z(G/H_{i+1})$.

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, $H \leqslant G$, 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

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

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 $G_i \leqslant G_{i+1}\cap(G_iN)$, 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:

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

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

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

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

Ist $N \trianglelefteq G$, dann ist $({}^{G_iN}/_{N})$ Zentralreihe 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 $G_i \leqslant G_{i+1}\cap(G_iN)$, 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.) □

1.22. 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

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

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 $H, K \leqslant G$ setze $[K,H] := \big\langle [k,h] | k \in K, h \in H \big\rangle$. Ist $K \leqslant N_G(H)$, dann ist $[K,H] \leqslant H$, denn $k^{-1}\cdot h^{-1}\cdot k\cdot h = \big(h^{-1}\big)^k \cdot h \in H$. 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 $G' \leqslant \ker \varphi$.

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. $G' \leqslant \ker \varphi$. □

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 $\varphi : G \to G/N$, $G' \leqslant \ker \varphi = N$

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 $k \geqslant 0$.

Beweis:

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

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

Bemerkung: Damit ist $(G^{(i)})_{i \leqslant k}$ 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 $G^{[i]}/G^{[i+1]} \leqslant Z(G/G^{[i+1]})$ nach Definition.

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

Beweis:

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

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

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

1.29. Einschub über direkte und semidirekte Produkte

a) Sei G eine Gruppe, $H \leqslant G$, $N \trianglelefteq G$ 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 Moduln

Erinnerung: In Algebra I wurden hauptsächlich kommutative Ringe betrachtet:

a) Körper, Polynomringe, $\mathbb{Z}$

b) nicht kommutative Ringe: R Ring, Matrizenring $M_n(R) = R^{n\times n}$.
Sei A eine 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 die 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. (mittels $\varphi(z)(x) = x^z$, für $z \in \mathbb{Z}$)

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

$\{0\}$, 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 oder A.2)

(ii) Ist $N \leqslant M$ ein R-Untermodul, dann ist auch ${}^{M}/_{N}$ ein R-Modul durch

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

φ ist R-linear

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

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

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 $(\varphi \cdot \psi)(m) = \varphi\big(\psi(m)\big)$ 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

Vgl. Kapitel 1 Seite 1

$$^{(A+B)}/_{B} \simeq {}^{A}/_{A\cap B}$$

(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:

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

Die Wohldefiniertheit sowie (ii) und (iii) sind einfache Übungsaufgaben. □

2.10. Definition (Sprechweise) Eine Folge von R-Moduln $(M_i)_i$ und Homomorphismen $f_i : M_{i-1} \to M_i$ heißt ***exakt in*** M_i, falls $\operatorname{Im} f_i = \ker f_{i+1}$. 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***[6], wenn es keine unendliche echt aufsteigende Kette von Untermoduln gibt. M heißt (links-)***artinsch***[7], 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.

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. □

[6] nach Emmy Noether, 1882-1935, siehe `http://de.wikipedia.org/wiki/Emmy_Noether`
[7] nach Emil Artin, 1898-1962, siehe `http://de.wikipedia.org/wiki/Emil_Artin`

Bemerkung: Offensichtlich gilt: Ist ein R-Modul M noethersch (bzw. artinsch) und $N \subseteq M$ ein 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. $(f$ injektiv, $M'' \simeq {}^{M}/_{M'})$

"$\Leftarrow$": (artinsch) Sei $P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \dots$ 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 Vorraussetzung existiert $k \in \mathbb{N}$ mit $P_k \cap M' = P_l \cap M'$ für $l \geqslant k$ und $(P_k+M')/_{M'} = (P_l+M')/_{M'}$ für $l \geqslant k$. Wegen

Isomorphiesätze

$$(P_l+M')/_{M'} \simeq P_l/(P_l \cap M')$$

folgt $P_l = P_k$ für $l \geqslant k$. Entsprechend für aufsteigende Ketten. □

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. □

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 $M \simeq {}^{R}/_{J}$ (siehe 2.6) und ${}^{R}/_{J}$ noethersch (bzw. artinsch) nach Satz 2.13. Sei nun

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

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 $k \cdot \mathbb{Z}$ gilt immer $k \cdot \mathbb{Z} \cap m \cdot \mathbb{Z} \ni k \cdot m \neq 0$.

(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 $M_1 := \sum N_\alpha$.

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 $N \subseteq P$ $\lightning$ 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. 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 "(ii) ⇒ (i)" 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 $P \leqslant N$ 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 $Q' \oplus P \supsetneq P$, also gilt 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 $M = \sum_{m \in M} Rm$ 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 "(ii)⇒(i)"). Daher ist

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

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 ist.

Beweis:

"$\Leftarrow$": klar, weil S_i zyklisch.

"$\Rightarrow$": Ist $M = \langle x_1, \ldots, x_r \rangle$, dann existiert für jedes $j = 1, \ldots, r$ endlich viele $S_{j1}, \ldots, S_{jk}$ mit $x_j \in \bigoplus_{i=1}^{k} S_{ji}$, also ist M die Summe von endlich vielen S_i, d.h. $|I|$ endlich. □

Das heißt wenn R halbeinfach als R-Modul ist, dann ist R noethersch und artinsch (nach 2.14).

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 und $\overline{I} := \{x_{11} \,|\, (x_{ij}) \in I\}$ 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 $E(s,t) \in M_k(R)$ 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 aufgrund der Tatsache $E(1,s)XE(t,1) = x_{s,t}E(1,1)$, 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. $I = M_k(\overline{I})$. □

$\boxed{\Longrightarrow \text{Matrizenringe über Körpern und Schiefkörpern sind einfache Ringe.}}$

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 $M = \bigoplus_{i\leqslant k} M_i$, $\varphi \in \mathrm{End}_R(M)$, dann existieren $\varphi_{i,j} \in \mathrm{Hom}(M_i, M_j)$ für $1 \leqslant i,j \leqslant k$, 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 $\varphi \in \mathrm{End}_R(M)$

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

wobei $\varphi_{i,j} := \pi_i \circ \varphi \circ e_j \in \mathrm{Hom}(M_j, M_i)$. 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^{op}-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

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

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

2.29. Satz (Wedderburn, 1. Struktursatz) Sei $R \neq 0$ 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 $k \geqslant 1$.

Darüber hinaus sind k und D eindeutig bestimmt und der einfache R-Modul ist isomorph zu D^k.

Beweis:

"(i)⇒(ii)": Sei $0 \neq I \subseteq R$ ein minimales Linksideal (existiert, da R links-artinsch 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 $M \simeq Rc_i \simeq Rc$. Die direkte Summe ist endlich, da R artinsch ist nach Bemerkung 2.24. *siehe 2.6*

"(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 $\mathrm{End}_R(L_i) \simeq D'$ 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 nach Satz 2.25 einfach, da D ein Schiefkörper ist. Die Eindeutigkeit von k und D folgt aus Korollar 2.23 (Krull-Remak-Schmidt) und Schurs Lemma (2.26). □ *artinsch, noethersch, da Dimension endlich*

Bemerkung: $(R, +)$ ist also auch noethersch (rechts und links). Achtung: Es gibt Ringe, die links-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 $D_1, \ldots, D_l$, die paarweise nicht isomorph sind 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

$$R^{\mathrm{op}} \simeq \mathrm{End}_R(R, +) \overset{2.30}{\simeq} \mathrm{End}_R(L_1^{k_1}) \oplus \ldots \oplus \mathrm{End}_R(L_l^{k_l}) \simeq M_{k_1}(\tilde{D}_1) \oplus \ldots \oplus M_{k_l}(\tilde{D}_l)$$

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 $x_1, \dots, x_n \in M$ heißen ***R-linear unabhängig***, wenn gilt:

$$\alpha_1, \dots, \alpha_n \in R \ : \ \sum \alpha_i \cdot x_i = 0 \quad \Longrightarrow \quad \forall i : \alpha_i = 0$$

äquivalent dazu: minimale erzeugende Menge

Sonst heißen $x_1, \dots, x_n$ linear abhängig. Eine Menge $X \subseteq M$ heißt linear unabhängig, wenn jede endliche Teilmenge linear abhängig ist. Eine linear unabhängige Erzeuger-Menge 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!

Beispiele:

(i) Wenn $R = K$ für einen Körper K, dann sind alle R-Moduln frei.

(ii) R als R-Modul ist frei mit der Basis $\{1_R\}$.

(iii) R^n für beliebiges $n \in \mathbb{N}$ 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: $(u_i)_{i \in I}$ und $(v_i)_{i \in I}$ induzieren einen Isomorphismus durch

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

Achtung: Die 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

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & M'' \arrow[r] \arrow[l, bend left, dashed, "\sigma"] & 0 \end{tikzcd}$$

eine kurze exakte Sequenz und 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 $M \cong M' \oplus M''$. σ heißt dann ein ***Schnitt***.

Bemerkung: M'' heißt ***projektiv*** genau dann, wenn jede kurze Sequenz mit M'' an dritter Stelle spaltet. Also bedeutet dieses Korollar: 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 $\sigma : M'' \to M$ (nach 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 eines freien R-Moduls, also $M \simeq \mathcal{F}/G$ für einen Untermodul $G \leqslant \mathcal{F}$.

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!
Nur über Körpern sind alle Moduln 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)⇒(ii)": Klar.

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

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

mit $\mathcal{F} \simeq R/I$ eine exakte Sequenz mit $\mathcal{F}$ zyklisch und daher frei nach Vorraussetzung. Da I ein maximales Ideal 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. (Vektorräume haben eine Basis)

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. Genaueres in Aufgabe 1.b) von Blatt 5.

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

BEMERKUNG:

- Körper haben IBL, $\mathrm{End}_R(V)$ nicht immer, 0 nie!
- Man kann zeigen: R hat IBL genau dann, wenn jeder freie R-Modul eindeutige Basislänge hat.

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 mit $R^m \simeq R^n$ 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 mittels Inklusion.

Beweis:

(i) Angenommen $A \in R^{m\times n}$, $B \in R^{n\times m}$ mit $AB = \mathbb{1}_{m\times m}, BA = \mathbb{1}_{n\times n}$ und o.B.d.A. $m < n$. Dann ist

$$\underbrace{\left(\begin{array}{c|c} B & \begin{matrix}0\\0\end{matrix} \end{array}\right)}_{\tilde{B}} \cdot \underbrace{\left(\begin{array}{c} A \\ \hline 0 \quad 0 \end{array}\right)}_{\tilde{A}} = \mathbb{1}$$

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

$$\tilde{A}\cdot\tilde{B} = \left(\begin{array}{c} A \\ \hline 0 \quad 0 \end{array}\right) \cdot \left(\begin{array}{c|c} B & \begin{matrix}0\\0\end{matrix} \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & 0 \end{array}\right)$$

Also $\det(\tilde{A}\cdot\tilde{B}) = 0$ ↯

(ii) Ist $R^m \simeq R^{m+k}$ mit $k \geqslant 1$, 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). ↯

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)[8] , falls R kommutativ und nullteilerfrei ist und jedes Ideal ein Hauptideal ist, das heißt von einem Element erzeugt ist. In Hauptidealringen hat man eine eindeutige Primfaktorzerlegung (bis auf Einheiten).

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

Beweis: Durch Induktion über $m \geqslant 0$. 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

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

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

[8] englisch: PID, prime ideal domain

Fall 2: $\pi(L) \neq 0$, dann ist $\pi(L) \subseteq D$ ein 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 $\ker \pi\big|_L \simeq D^n$, $n \leqslant m$, und $\pi(L) \simeq D$, daher ist $L \simeq D \oplus D^n$. □

Ist D ein Hauptidealring, M endlich erzeugt über D, also $M = Dm_1 + \ldots + Dm_s$. 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 $t \leqslant s$ und $M \simeq {}^{D^s}/_{\ker \varphi}$. Um M zu beschreiben, müssen wir untersuchen, *wie* $\ker \varphi$ in D^s liegt.

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 es gilt $d_i = 1$ für alle i.

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:

- Zeilen von A vertauschen
- Spalten von A vertauschen
- Zeilen/Spalten mit Einheiten multiplizieren
- siehe LA I. 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 $k \geqslant 2$, vertausche 2-te und k-te Spalte. Dann gilt $a_{11} \nmid a_{12}$. Sei $d \in$ $x, y \in D$ $\mathrm{ggT}(a_{11}, a_{12})$, dann $l(d) < l(a_{11})$. Schreibe $d = a_{11} \cdot x + a_{12} \cdot y$ 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

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

das heißt $\left(\begin{smallmatrix} x & e \\ y & f \end{smallmatrix}\right)$ ist invertierbar. Es gilt

$a_{11} \cdot e + a_{12} \cdot f = -d \cdot f \cdot e + d \cdot e \cdot f = 0$

$$\begin{pmatrix} a_{11} & a_{12} & * \\ a_{21} & a_{22} & \\ \multicolumn{2}{c}{*} & * \end{pmatrix} \cdot \begin{pmatrix} \begin{matrix} x & e \\ y & f \end{matrix} & & 0 & \\ & 1 & & \\ 0 & & \ddots & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} d & a_{11}e + a_{12}f & a_{13} \cdots \\ * & * & * \\ * & * & * \end{pmatrix} = \begin{pmatrix} d & 0 & a_{13} \cdots \\ * & * & * \\ * & * & * \end{pmatrix}$$

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

$$\tilde{A} = \begin{pmatrix} \tilde{a_{11}} & \tilde{a_{12}} & \cdots \\ * & * & * \end{pmatrix}$$

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 eine Matrix der Form

$$\begin{pmatrix} \tilde{a}_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$$

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

$$\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_n & \\ & & & 0 \end{pmatrix}$$

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

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

mit $d_i x + d_{i+1} y = d_i' \in \operatorname{ggT}(d_i, d_{i+1})$. Wie eben erhalten wir $\left(\begin{smallmatrix} d_i' & 0 \\ 0 & d_{i+1}f \end{smallmatrix}\right) \rightsquigarrow \ldots$ fertig. □

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

2.44. Definition Ist $A \in D^{m \times n}$ und $i \leqslant m, n$, 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, $A \in D^{m \times n}$ und 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 $d_1 = \delta_1$, $d_i = \prod_{j \leqslant i} \delta_j$.

Beweis: Ist k der Rang von A, dann existiert für alle $i \leqslant k$ ein i-Minor $\neq 0$ in A (Laplace-Entwicklung der Determinante). Insbesondere ist $\delta_1, \ldots, \delta_k \neq 0$, also $d_i \neq 0$ für $i = 1, \ldots, k$.

Für $P \in D^{m \times m}$ sind die Zeilen von $P \cdot A$ Linearkombinationen der Zeilen von A, also sind die j-Minoren von $P \cdot A$ Linearkombinationen der j-Minoren von A. Entsprechendes gilt für die Spalten von $Q \in D^{n \times n}$ 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 nach Satz 2.43

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

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

Die Matrix heißt die ***Smith-Normalform*** von A.

2.46. Beispiel Sei $D = \mathbb{Z}$ und $A = \left(\begin{smallmatrix} 3 & 1 \\ 0 & 4 \end{smallmatrix}\right)$. Die 1-Minoren sind $1, 3, 4$, also ist $\delta_1 = 1 = d_1$. Der 2-Minor ist 12, also gilt $\delta_2 = 12 = d_2$. Damit ist $A \sim_{\mathbb{Z}} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 12 \end{smallmatrix}\right)$.

2.47. Definition Ist $M \in {}_R\mathrm{Mod}$, $m \in M$, dann heißt

$$\mathrm{ann}(m) = \{r \in R \,|\, r \cdot m = 0\}$$

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

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 $M = Dm_1 \oplus \ldots \oplus Dm_k$ mit

$$D \supsetneq \mathrm{ann}(m_1) \supsetneq \mathrm{ann}(m_2) \supsetneq \ldots \supsetneq \mathrm{ann}(m_k)$$

Beweis: Schreibe $M \simeq {}^{D^s}\!/_{L}$ mit $L \simeq D^t$, $t \leqslant s$ (siehe 2.42). Dann ist $L = Dl_1 \oplus \ldots \oplus Dl_t$ mit $l_j = (a_{1j}, \ldots, a_{sj}) \in D^s$. Dann erhalten wir eine Matrix $A = (a_{ij}) \in D^{s \times t}$. Die Smith-Normalform

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

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

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

sowie $f_i = d_i \cdot e_i$ und

$${}^{D^s}\!/_{L} \simeq {}^{D}\!/_{(d_1)} \oplus \ldots \oplus {}^{D}\!/_{(d_k)} \oplus D \oplus \ldots \oplus D$$

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

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

2.50. Definition und Satz Setze $\operatorname{tor}_D(M) := \{m \in M \mid \operatorname{ann}(m) \neq 0\}$. Ist D kommutativ und nullteilerfrei, dann ist $\operatorname{tor}_D(M)$ 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 $d \cdot m \in \operatorname{tor}(M)$ für alle $d \in D$. Sind $m_1, m_2 \in \operatorname{tor}(M)$, 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

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

mit

$$\begin{aligned} \operatorname{ann}(m_i) &\neq 0 \text{ für } i = 1, \ldots, s \\ \operatorname{ann}(m_i) &= 0 \text{ für } i = s+1, \ldots, s+k \end{aligned}$$

Ein Element $d_1 m_1 + \ldots + d_{s+k} m_{s+k} \in M$ ist ein Torsionselement genau dann, wenn $d_{s+1} = \ldots = d_{s+k} = 0$, also wenn es in $Dm_1 \oplus \ldots \oplus Dm_s$ liegt. Damit ist $\operatorname{tor}(M) = Dm_1 \oplus \ldots \oplus Dm_s$. Es ist $M/\operatorname{tor}(M) \simeq D^k$ und k ist nach Satz 2.41 eindeutig bestimmt (M ist halbeinfach). □

2.52. Beispiel

(i) Sei $D = Z$ und $M = \mathbb{R}/\mathbb{Z}$. Dann ist $\operatorname{tor}_{\mathbb{Z}}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$, da $d \cdot r \in \mathbb{Z} \Rightarrow r \in \mathbb{Q}$. Also gilt

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

Anmerkung[9].

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

$$r \cdot p \in \mathbb{Z}\frac{r}{s} \cap \mathbb{Z}\frac{p}{q} \neq 0$$

$\mathbb{Q}$ ist nicht endlich erzeugt als $\mathbb{Z}$-Modul.

Ist A eine endlich erzeugte abelsche Gruppe, dann existiert $k \in \mathbb{Z}$ und eine endliche Gruppe A_0 mit $A \simeq A_0 \oplus \mathbb{Z}^k$. Dabei heißt k der Rang von A. Zusammengefasst ergibt sich:

[9] $\mathbb{R}/\mathbb{Z} \simeq S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ indem man S^1 in Polardarstellung, also nur als Menge der Winkel betrachtet.

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

Jede endliche abelsche Gruppe ist die Summe von zyklischen Gruppen von Primzahlordnung. Diese Ordnung und ihre Vielfachheiten sind eindeutig bestimmt. Zwei endlich erzeugte abelsche Gruppen sind genau dann isomorph, wenn der Rang und diese Ordnungen übereinstimmten.

Bemerkung: Die Zerlegung ist hier anders als in Satz 2.48. Die Zerlegung von $\operatorname{tor}(A)$ folgt aus den Sylow-Sätzen.

3. Tensorprodukte und Algebren

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

$$\begin{tikzcd} U \times V \arrow[r, "\varphi"] \arrow[dr, "f"'] & T \arrow[d, dashed, "f'"] \\ & W \end{tikzcd}$$

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

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

$$\begin{tikzcd} U \times V \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"] \arrow[ddr, "\varphi_1"] \arrow[dddr, "\varphi_2"] & T_1 \arrow[d, dashed, "\varphi_2'"] \arrow[dd, bend left, "\mathrm{id}"] \\ & T_2 \arrow[d, dashed, "\varphi_1'"] \arrow[dd, bend left, "\mathrm{id}"] \\ & T_1 \arrow[d, dashed, "\varphi_2'"] \\ & T_2 \end{tikzcd}$$

also $\varphi_2' \circ \varphi_1' = \mathrm{id}_{T_2}$, $\varphi_1' \circ \varphi_2' = \mathrm{id}_{T_1} \Rightarrow T_1 \simeq T_2$.

Für die Existenz sei $\mathcal{F}_{U \times V}$ 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

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

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

$$\begin{tikzcd} U \times V \arrow[r, hook, "\varphi'"] \arrow[dr, "f"'] & \mathcal{F}_{U \times V} \arrow[d, dashed, "f_1"] \\ & W \end{tikzcd}$$

Nach Definition von B folgt $B \subseteq \ker f_1$, denn es ist zB.

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

da f bilinear ist. Ebenso ist

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

Daher erhalten wir $f' : U \otimes V = \mathcal{F}_{U\times V}/B \to W$ 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 $u,u' \in U, v,v' \in V, \alpha \in R$.

RevChap3

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) $f : U \times V \to V \times U$, $(u,v) \mapsto (v,u)$ ist bilinear. Daher existiert ein Homomorphismus $\alpha : U \otimes V \to V \otimes U$, $u \otimes v \mapsto v \otimes u$, d.h.

$$\alpha\Big(\sum u_i \otimes v_i\Big) = \sum v_i \otimes u_i$$

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

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

$$\tilde{f} : (U\otimes V) \times W \to U \otimes (V \otimes W) \quad , \quad ((u\otimes v),w) \mapsto f_w(u \otimes v) = u \otimes (v \otimes w)$$

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

(iii) Sei $\varphi : U \times (V \oplus W) \to (U \otimes V) \oplus (U \otimes W)$, $(u,v,w) \mapsto (u \otimes v, u \otimes w)$. Ist $f : U \times (V \oplus W) \to Z$ 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.

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

$\square$

3.4. Beispiel

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

Ich bin mir noch unsicher, ob die Rechnung stimmt … bzw verstehe nicht ganz, was sie zeigen soll…

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

(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, $U \in {}_R\mathrm{Mod}$. Dann ist $U \otimes R^n \simeq U^n = U \oplus \ldots \oplus U$.

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 $\theta : R \times U \to U$, $(r,u) \mapsto r \cdot u$. Dann ist θ bilinear. Ist $W \in {}_R\mathrm{Mod}$ und $f : R \times U \to W$ 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. □

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 $\{e_1, \ldots, e_m\}$, $\{f_1, \ldots, f_n\}$ Basen für U bzw. V, dann ist $\{e_i \otimes f_j \,|\, i = 1, \ldots, m, j = 1, \ldots, n\}$ eine Basis für $U \otimes V$.

3.7. Korollar Ist $U \in {}_R\mathrm{Mod}$, 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.

Siehe Beispiel 3.4 (iii)

Sei $V' = \langle v_1, \ldots, v_k \rangle \subseteq V$. 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

$$U \otimes V' \to U \otimes V \qquad \star$$

Achtung: Dieser Homomorphismus muss nicht injektiv sein!

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

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

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*** $C(A) = \{z \in A \,|\, x \cdot z = z \cdot x \;\; \forall x \in A\}$ 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 $nx = x + \ldots + x$, $(-n)x = -(nx)$

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 $x = 1$ ergibt sich $\alpha 1 \cdot y = \alpha \cdot y$. 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 $R \to A$, $\alpha \mapsto \alpha \cdot 1$ ist ein Algebrahomomorphismus in das Zentrum von A, d.h. $R \cdot 1 \subseteq C(A)$.

Umgekehrt gilt: Ist R ein Ring, $f : R \to C(A)$ ein Ringhomomorphismus. Dann wir A zu einer R-Algebra durch $\alpha \cdot x = f(x) \cdot x$ für $x \in A, \alpha \in R$. Mit anderen Worten: Eine R-Algebra ist ein Ring A zusammen mit einem Homomorphismus $f : R \to C(A)$. 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) $U \in {}_R\mathrm{Mod}$, $A = \mathrm{End}_R(U)$. Dann ist A ein R-Modul: Für $f \in A, \alpha \in R$, $x \in U$ ist

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

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

(ii) $B_n(R) =$ Menge der oberen Dreiecksmatrizen ist Unteralgebra von $M_n(R)$.

(iii) Sei $M = \{u_i \,|\, i \in I\}$ 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) $M = \{1, X, X^2, X^3, \ldots\}$, $RM = R[X]$.

(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 $\{u_1, \ldots, u_n\}$, dann ist die Struktur von A eindeutig bestimmt durch die n^3 Strukturkonstanten c_{ijk}, $i, j, k = 1, \ldots, n$ mit $u_i \cdot u_j = \sum_{k=1}^n c_{i,j,k} \cdot u_k$.

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 $U \in {}_R\mathrm{Mod}$, dann sei $T(U) = \bigoplus_{n\in\mathbb{N}} U^{\otimes n}$, mit $U^{\otimes n} = U \otimes \ldots \otimes U$, $U^{\otimes 0} = R$. 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 $A \to \mathrm{End}_R(U)$ für einen R-Modul U. Für jede Algebra A bezeichnet man mit ρ die rechts-reguläre Darstellung A auf sich selbst, d.h.

vgl. $G \to \mathrm{Sym}(X)$ in Def. 1.1

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

Diese Darstellung ist treu, d.h. $\ker \rho = 0$. Ist A endlich dimensionale Algebra über einem Körper K mit Basis $\{u_1, \ldots, u_n\}$, dann ist $\mathrm{End}_K(A) \simeq M_n(K)$. 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 Unteralgebra von $M_n(K)$.

Beweis: $A \simeq \mathrm{Im}\,\rho \subseteq \mathrm{End}_K(A) \simeq M_n(K)$. □

3.13. Satz Ist R ein kommutativer Ring, dann ist für R-Algebren A, B auch $A \otimes B$ eine R-Algebra mit $\mu(A \otimes B) \times (A \otimes B) \to A \otimes B$, $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ 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. □

3.14. Beispiel

(i) 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.

(ii) Sei $A = M_n(R)$. Dann hat A eine R-Basis $\{e_{ij} \mid i, j \leqslant n\}$ mit Multiplikation $e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}$ und $\sum e_{ii} = 1$. Ist B eine R-Algebra, dann ist $A \otimes B$ ein freier B-(Rechts-)Modul mit derselben Basis als B-Modul. d.h. $M_n(R) \otimes B \simeq M_n(B)$. Für $B = M_k(R)$ ist also $M_n(R) \otimes M_k(R) \simeq M_{n \cdot k}(R)$.

Im Folgenden untersuchen wir endlich dimensionale Algebren über einem kommutativen Körper K.

3.15. Definition Eine K-Algebra A heißt ***zentral***, wenn $C(A) = K \cdot 1_A$. Ist A eine endlich dimensionale einfache K-Algebra, dann ist nach Wedderburn (2.29) $A \simeq M_n(D)$ für einen Schiefkörper D, der endliche Dimension über K hat. Weiter ist

$$C(A) \simeq C(D) =: E \supseteq K.$$

Dann ist E ein kommutativer Körper und wir können A als E-Algebra auffassen. Also solche ist A dann eine zentral einfache endlich dimensionale E-Algebra.

Bemerkung: Sind A, B K-Algebren, dann enthält $A \otimes B$ Unteralgebren $1 \otimes B \simeq B$ und $A \otimes 1 \simeq A$. Wir geben eine interne Charakterisierung von Tensorprodukten an (vgl. 1.29).

3.16. Definition Sei C eine K-Algebra, $U, V \subseteq C$ K-Untervektorräume. Dann heißen U und V ***linear disjunkt*** über K, wenn für linear unabhängige $u_i \in U$, $v_j \in V$ die Elemente $u_i v_j \in C$ linear unabhängig sind. Mit anderen Worten ist die natürliche Abbildung $U \otimes V \to C$, $u \otimes v \mapsto uv$ injektiv.

3.17. Proposition Sei C eine K-Algebra, $A, B \subseteq C$ Unteralgebren, dann ist $C \simeq A \otimes B$, falls gilt

(i) A und B sind linear disjunkt über K

(ii) $AB = C$

(iii) $ab = ba$ für alle $a \in A, b \in B$. $(a \otimes 1)(1 \otimes b) = (1 \otimes b)(a \otimes 1) = a \otimes b$

Beweis: Die Abbildung $A \times B \to C$, $(x, y) \mapsto xy$ ist bilinear und induziert daher eine Abbildung $A \otimes B \to C$. Diese Abbildung ist injektiv nach (i), surjektiv nach (ii) und ein Homomorphismus nach (iii). □

3.18. Definition Für eine K-Algebra A heißt $A^e = A \otimes_K A^{\mathrm{op}}$ die ***einhüllende Algebra*** von A. Sei $A \subseteq B$ eine Unteralgebra. Dann wird B in natürlicher Weise zu einem A^e-Modul, nämlich durch

$$\left(\sum a_i \otimes b_i\right) y = \sum a_i \cdot y \cdot b_i$$

für $a_i \in A, b_i \in A^{\mathrm{op}}, y \in B$. Aus der universellen Eigenschaft des Tensorprodukts folgt, dass dies eine wohldefinierte Modulwirkung beschreibt. Insbesondere wird A selber zum A^e-Modul. Die A^e-Untermoduln von A sind genau die beidseitigen Ideale von A. Nach Lemma 2.25 ist $\mathrm{End}_R(R, +) \simeq R^{\mathrm{op}}$, d.h. R-lineare Endomorphismen von $R \in {}_R\mathrm{Mod}$ sind genau die Rechtsmultiplikationen ρ_r für $r \in R$. Daher ist $\mathrm{End}_{A^e}(A)$ die Menge der Abbildungen, die sowohl Rechtsals auch Links-Multiplikation sind, d.h. Abbildungen $x \mapsto c \cdot x = x \cdot d$. Für $x = 1$ erhält man $c = d$, d.h. $c \in C(A)$. Damit folgt $\mathrm{End}_{A^e}(A) \simeq C(A)$.

3.19. Satz (Dichtheitssatz für halbeinfache Moduln) Sei R ein Ring, $M \in {}_R\mathrm{Mod}$ halbeinfach, $R' = \mathrm{End}_R(M) = C_{\mathrm{End}(M,+)}(\Lambda_R)$ mit $\Lambda_R = \{\lambda_r \mid r \in R\}$, $R'' = \mathrm{End}_{R'}(M)$ (für M aufgefasst als R'-Modul). Sei $\{x_1, \ldots, x_n\} \subseteq M$, $a'' \in R''$, dann existiert $a \in R$ mit $ax_i = a''x_i$ für $i = 1, \ldots, n$. vertauschen

Beweis: Zuerst überlegen wir, dass jeder R-Untermodul $N \subseteq M$ auch ein R''-Untermodul ist. Schreibe $M = N \oplus P$ und $\pi : M = P \oplus N \to N$. Dann ist $\pi \in R'$ und $N = \pi(M)$. Daher ist für $\varphi \in R''$ also

$$\varphi(N) = \varphi\pi(M) = \pi\varphi(M) \subseteq N.$$

D.h. N ist R''-Untermodul von M. Ist nun $n = 1$, dann ist $N = Rx_i$ ein R-Untermoduln und daher auch R''-Untermodul. Wegen $x_1 \in N$ ist für $a'' \in R''$ auch $a''x_1 \in N = Rx_1$. Also existiert $a \in R$ mit $a''x_1 = ax_1$. Für $n \geqslant 1$ benutzen wir folgenden Trick:

3.20. Lemma Sei $M \in {}_R\mathrm{Mod}$, $R' = \mathrm{End}_R(M)$, $R'' = \mathrm{End}_{R'}(M)$. Dann ist für $\alpha \in R''$ die Abbildung $\varphi_\alpha : M^n \to M^n$, $(u_1, \ldots, u_n) \mapsto (\alpha(u_1), \ldots, \alpha(n_n))$ ein Endomorphismus von M^n, ist also $\mathrm{End}_R(M^n)$-Modul.

Beweis: Nach Lemma 2.27 ist $\mathrm{End}_R(M^n) \simeq M_n(R')$. Offensichtlich ist M^n auch $\mathrm{End}_R(M^n)$-Modul. Für die Behauptung ist also nur zu zeigen, dass für jedes $\alpha \in R''$ die Abbildung φ_α mit jedem R-Endomorphismus von M^n vertauscht. Dies ist der Fall, da α gerade mit jedem R-Endomorphismus von M vertauscht. □

Beweis von 3.19: Mit M ist auch M^n halbeinfach. Nach Lemma 3.20 ist für $\alpha'' \in R''$ und $\varphi_{\alpha''}$ wie eben auch $\varphi_{\alpha''} \in \mathrm{End}_{\mathrm{End}_R(M^n)}(M^n)$. Nun wenden wir den Fall $n = 1$ auf den R-Modul M^n und $\varphi_{\alpha''}$. Damit finden wir für $(x_1, \ldots, x_n) \in M^n$ ein $\alpha \in R$ mit

$$\varphi_{\alpha''}(x_1, \ldots, x_n) = \big(\alpha''(x_1), \ldots, \alpha''(x_n)\big) = \alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n).$$

3.21. Satz Ist A eine endlich dimensionale zentral einfache K-Algebra, dann ist $A^e = A \otimes A^{\mathrm{op}} \simeq M_n(K)$ mit $n = \dim A$.

Beweis: Betrachte A als A^e-Modul. Dann ist A einfach und $\mathrm{End}_{A^e}(A) \simeq K$. Da A endlich dimensional über K ist, folgt aus dem Dichtheitssatz (3.19), dass $A^e \to \mathrm{End}_K(A)$ surjektiv ist. Da

$$\dim_K A^e = \dim_K \mathrm{End}_K(A) = n^2$$

folgt $A^e \simeq \mathrm{End}_K(A)$ und wegen $\mathrm{End}_K(A) \simeq M_n(K)$ folgt die Behauptung. □

3.22. Satz Sei B eine K-Algebra. A eine endlich dimensionale zentral einfache Unteralgebra. Dann gilt $B \simeq A \otimes_K C$, wobei $C = C_B(A)$ der Zentralisator von A in B ist, d.h. $C = \{x \in B \mid xa = ax \ \forall a \in A\}$.

Die Abbildung $I \mapsto A \otimes I$ ist Verbandsisomorphismus zwischen den Idealen von B und den Idealen von C und es ist $C(B) = C(C)$

Beweis: Betrachte B als A^e-Modul. Da A^e nach Satz 3.21 einfach ist, $A^e = M_n(K)$, ist nach Wedderburn (2.31) $B = \bigoplus A^e x_i$ direkte Summe von einfachen A^e-Moduln, die alle isomorph zu A sind. Als A^e-Modul wird A von 1_A erzeugt und es ist

$$(a \otimes 1)1 = a \cdot 1 = 1 \cdot a = (1 \otimes a)1$$

und falls $(a \otimes 1)1 = 0$, dann ist $a = 0$. Da alle $A^e x_i \simeq A$ als A^e-Moduln, existiert ein $c_i \in A^e x_i$ mit $(a \otimes 1)c_i = (1 \otimes a)c_i$ und $(a \otimes 1)c_i = 0 \Rightarrow a = 0$. Daher ist $B = \bigoplus A c_i$ mit $ac_i = c_i a$ für alle $a \in A$ und $ac_i = 0 \Rightarrow a = 0$. Daher sind alle $c_i \in C = C_B(A)$ und jedes Element in B hat *eindeutige* Darstellung der Form $\sum a_i c_i$ mit $a_i \in A$.

Ist $c \in C$, $c = \sum a_i c_i$, dann folgt wegen $ac = ca$ für alle $a \in A$ auch $aa_i = a_i a$ für alle $a \in A$, d.h. $a_i \in C(A) \simeq K$. Daher ist $C = \sum K c_i$, d.h. $\{c_i \mid i \in I\}$ ist Basis für C. Nach Proposition 3.17 ist $B = A \otimes_K C$.

Für den zweiten Teil sei $I \trianglelefteq C$ ein Ideal. Dann ist $A \otimes I$ ein Ideal in $B = A \otimes C$ und es ist $(A \otimes I) \cap (1 \otimes C) = I$. Ist $(x_1 = 1, x_2, \dots, x_n)$ Basis für A, dann hat jedes $b \in B$ eine *eindeutige* Darstellung der Form $b = \sum c_i \otimes x_i = \sum c_i x_i$ mit $c_i \in C$. Die Elemente von $A \otimes I$ sind von der Form $\sum d_i x_i$ mit $d_i \in I$. Daher folgt aus $b = \sum d_i x_i \in C$ schon $b = c_1 x_1$ mit $c_1 \in C$, d.h. $C \cap AI = \{d_1 x_1 = d_1 \in I\} = I$. Daher ist $I \mapsto A \otimes I$ injektiv. Ist I' ein Ideal in B, dann ist I' ein A^e-Untermodul von B, d.h. für $I = I' \cap C$ ist dann $I' = \sum A d_j$ mit $d_j \in I$. Daher ist $I' = A \cdot I_i$, d.h. die Abbildung $I \mapsto A \otimes I$ ist surjektiv.

Noch zu zeigen: $C(B) = C(C)$. "$\subseteq$" ist klar. Ist $c \in C(C)$, dann vertauscht c mit allen $a \in A$ und mit allen $d \in C$, also $c \in C(B)$. □

3.23. Korollar Ist A eine endlich dimensionale zentral einfache K-Algebra, C eine beliebige K-Algebra, dann ist die Abbildung $I \mapsto A \otimes I$ ein Verbandsisomorphismus zwischen Idealen von $B = A \otimes C$ und den Idealen von C und es ist $C(B) = C(C)$.

Beweis: Identifiziere A, C mit $A \otimes I$ bzw. $1 \otimes C$ in $B = A \otimes C$. Behauptung: $C = C_B(A)$. Klar "$\subseteq$". "$\supseteq$" wie eben. Daher folgt die Behauptung aus 3.22. □

3.24. Korollar Ist A eine endlich dimensionale zentral einfache K-Algebra, C eine beliebige K-Algebra, dann ist $A \otimes C$ einfach genau dann, wenn C einfach ist und $A \otimes C$ ist zentral genau dann, wenn C zentral ist. Insbesondere gilt: Ist A endlich dimensionale zentral einfache K-Algebra, $E \supseteq K$ eine Körpererweiterung, dann ist $A_E = A \otimes E$ endlich dimensionale zentral einfache E-Algebra.

3.25. Korollar Sind $A_1, \dots, A_n$ endlich dimensionale zentral einfache K-Algebren, dann ist auch $A_1 \otimes \ldots \otimes A_n$ zentral einfach und endlich dimensional.

3.26. Definition $M_n(K)$ heißt zerfallende zentral einfache K-Algebra. Ist A endlich dimensionale zentral einfache K-Algebra, dann heißt eine Körpererweiterung $E \supseteq K$ ein ***Zerfällungskörper*** für A, falls $A_E = A \otimes_K E \simeq M_n(E)$ für ein $n \in \mathbb{N}$. Man sagt A zerfällt über E.

3.27. Bemerkung

(i) Ist E Zerfällungskörper für A, dann auch jedes $E' \supseteq E$. Insbesondere ist jedes $E \supseteq K$ Zerfällungskörper für $M_n(K)$.

(ii) Sind A, B zentral einfach und E Zerfällungskörper für A, B, dann auch für $A \otimes B$: Es ist

$$(A \otimes B)_E = (A \otimes B) \otimes E \simeq (A \otimes_k B) \otimes_K E \simeq (A \otimes E) \otimes (B \otimes E).$$

$M_{nk}(E) \simeq M_n(E) \otimes M_k(E)$.

(iii) Ist E Zerfällungskörper für A ,dann auch für A^{op}:

$$A \otimes E \otimes E \otimes A^{\mathrm{op}} = M_n(E) = M_r(E) \otimes (E \otimes A^{\mathrm{op}}) = M_r(E \otimes A^{\mathrm{op}})$$

Daher ist $E \otimes A^{\mathrm{op}} \simeq M_s(E)$ mit $r \cdot s = n$.

(iv) Ist $A \simeq M_r(B)$, B zentral einfach über K, dann ist $E \supseteq K$ Zerfällungskörper von A genau dann, wenn E Zerfällungskörper von B ist. Es ist

$$A \otimes E \simeq M_r(B) \otimes E \simeq M_r(K) \otimes B \otimes E \simeq M_r(B_E).$$

3.28. Proposition Sei K algebraisch abgeschlossen, A eine endlich dimensionale K-Algebra. Ist A nullteilerfrei, dann ist $A = K$. Insbesondere existieren keine echten endlich dimensionalen Schiefkörper über einem algebraisch abgeschlossenen Körper K.

Beweis: Sei $a \in A$. Da A endliche K-Dimension hat, sind die Potenzen von a linear abhängig über K. Sei etwa $f(a) = a^n c_1 + a^{n-1} c_2 + \ldots + c_n = 0$ mit $c_i \in K$ und n minimal. Da K algebraisch abgeschlossen ist, hat $f(X) \in K[X]$ eine Nullstelle $\lambda \in K$. Daher ist $f(X) = (X - \lambda) \cdot g(X)$ mit $\deg(g) = n - 1$. Nach Vorraussetzung ist aber $g(a) \neq 0$, wegen n minimal. Weil A nullteilerfrei ist, folgt $a = \lambda \in K$. $\square$

3.29. Korollar Sei K algebraisch abgeschlossen, A zentral einfache, endlich dimensionale Algebra über K. Dann ist $A \simeq M_n(K)$ für ein $n \in \mathbb{N}$.

Beweis: $A \simeq M_n(D)$ für einen endlich dimensionalen Schiefkörper über K. Dann ist $D = K$ nach 3.28. $\square$

Bemerkung: Insbesondere zerfällt jede zentral einfache, endlich dimensionale K-Algebra über dem algebraischen Abschluss von K. Ziel: Zeige Existenz endlicher Körpererweiterungen als Zerfällungskörper. Zeige: Jeder maximale kommutative Teilkörper von D ist Zerfällungskörper für $A \simeq M_N(D)$.

3.30. Satz Ist D ein Schiefkörper endlicher Dimension über K. Dann ist eine endliche Körpererweiterung E/K ein Zerfällungskörper für D genau dann, wenn E Teilkörper einer Algebra $A = M_r(D)$ mit $C_A(E) = E$ ist.

Beweis:

"$\Leftarrow$": Sei $E \subseteq M_r(D) = A$ mit $C_A(E) = E$. Dann ist $A = \operatorname{End}(V)$, wobei V ein r-dimensionaler D^{op}-Vektorraum ist. Dann ist V auch $D^{\mathrm{op}} \otimes_K E$-Modul, da

$$(d \otimes e)x = d \cdot e \cdot x = e \cdot d \cdot x$$

treu, da Kern sonst Unteralgebra

für $d \in D^{\mathrm{op}}$, $e \in E \subseteq A$, $x \in V$. Da $D^{\mathrm{op}} \otimes E$ einfach ist, ist die Darstellung von $D^{\mathrm{op}} \otimes E$ auf V treu, d.h. wir können $D^{\mathrm{op}} \otimes E$ mit dem entsprechenden Endomorphismenring identifizieren. Da $D^{\mathrm{op}} \otimes E$ endlich dimensional und einfach über K ist, ist nach den Sätzen von Wedderburn V als $D^{\mathrm{op}} \otimes E$ als Modul halbeinfach und daher ist der Dichtheitssatz anwendbar:

zusätzlich auch mit E vertauschen

Es ist $A = \operatorname{End}_{D^{\mathrm{op}}}(V)$, also ist $\operatorname{End}_{D^{\mathrm{op}} \otimes E}(V) = C_A(E) = E$. Also können wir V auch als endlich dimensionalen E-Vektorraum betrachten. Nach dem Dichtheitssatz ist $D^{\mathrm{op}} \otimes E = \operatorname{End}_E(V) \simeq M_n(E)$ für $n = \dim_E V$. Daher ist E Zerfällungskörper von D^{op} und damit von D.

"$\Rightarrow$": Ist umgekehrt $D \otimes E \simeq M_n(E)$, dann auch $D^{\mathrm{op}} \otimes E \simeq M_n(E)$. Ist V ein irreduzibler $D^{\mathrm{op}} \otimes E$-Modul, dann auch ein $M_n(E)$-Modul, d.h. V ist n-dimensionaler E-Vektorraum und $\operatorname{End}_E(V) = D^{\mathrm{op}} \otimes E$. Aber V ist auch ein endlich dimensionaler D^{op}-Vektorraum also etwa $r = \dim_{D^{\mathrm{op}}} V$. Dann ist $E \subseteq \operatorname{End}_{D^{\mathrm{op}}}(V)$. Daher ist

$$E \subseteq C_{\operatorname{End}_{D^{\mathrm{op}}}(V)}(E) \subseteq C_{\operatorname{End}_E(V)}(D^{\mathrm{op}} \otimes E) = E.$$

Daher ist $E = C_{M_r(D)}(E)$. □

3.31. Korollar Ist A eine zentral einfache K-Algebra mit $A \simeq M_r(D)$, D Schiefkörper. Dann ist jeder maximale kommutative Teilkörper E von D Zerfällungskörper für A.

Beweis: Klar: Es existiert ein maximaler kommutativer Teilkörper E, denn $\dim_K D$ ist endlich. Es reicht zu zeigen: E ist Zerfällungskörper für D. (Wende Satz 3.30 an mit $A = D$). Sei $E' = C_D(E) \supseteq E$. Ist $E \subsetneq E'$, wähle $c \in E' \setminus E$. Dann ist der von E und c erzeugte Unterkörper von D auch kommutativ. $\lightning$ Maximalität von E. Also gilt $C_D(E) = E$ und die Behauptung folgt aus 3.30. □

Beispiel: $\mathbb{H}$ reelle Quaternionen.

3.32. Korollar Ist A zentral einfache K-Algebra endlicher Dimension, dann ist $\dim_K A = n^2$ für ein $n \in \mathbb{N}$ der ***Grad*** von A.

Beweis: Es ist $A \otimes E \simeq M_n(E)$ für einen Zerfällungskörper E und $\dim_K A = \dim_E\big(M_n(E)\big) = n^2$. □

3.33. Satz (Skolem-Noether) Ist B eine endlich dimensionale, zentral einfache K-Algebra, $A \subseteq B$ einfache Unteralgebra, dann lässt sich jeder Monomorphismus $f : A \to B$ zu einem inneren Automorphismus[10] fortsetzen, d.h. es existiert ein $b \in B$ mit $f(a) = b^{-1} \cdot a \cdot b$.

[10] Automormphismus durch Konjugation

Beweis: $E = A \otimes_K B^{\mathrm{op}}$ ist einfach und endlich dimensional. Nach Wedderburn ist jeder E-Modul halbeinfach und alle einfachen E-Moduln sind isomorph. Daher sind auch endlich dimensionale E-Moduln derselben Dimension isomorph. Betrachte B als E-Modul auf zwei Weisen:

$$\Big(\sum a_i \otimes b_i\Big)x = \sum a_i \cdot x \cdot b_i \qquad \Big(\sum a_i \otimes b_i\Big)x = \sum f(a_i) \cdot x \cdot b_i$$

Dies definiert eine E-Modulstruktur auf B, weil f ein Homomorphismus ist. Nach Vorüberlegung sind diese beiden E-Moduln isomorph, d.h. es existiert ein E-linearer Isomorphismus $\varphi : B \to B$ mit

$$\varphi\Big(\sum f(a_i) \otimes b_i\Big) = \sum a_i \varphi(x) b_i$$

für $a_i \in A$, $b_i, x \in B$. Insbesondere ist dann $\varphi(xb) = \varphi(x)b$ für alle $x, b \in B$. Daher ist $\varphi(x) = \varphi(1)x = dx$ für ein invertierbares $d \in B$, denn φ ist invertierbar. Wegen $\varphi(f(a)x) = a \cdot \varphi(x)$ für alle $a \in A, x \in B$ folgt $Adx = df(a)x$ und für $x = 1$ folgt $f(a) = d^{-1}ad$, d.h. f lässt sich zum inneren Automorphismus $\kappa_d : x \mapsto d^{-1}xd$ fortsetzen. □

3.34. Korollar Jeder Automorphismus einer endlich dimensionalen, zentral einfachen Algebra ist ein innerer.

Beweis: Setze $A = C(B) = K$ in Satz 3.33. □

3.35. Korollar In einer endlich dimensionalen, zentral einfachen Algebra sind einfache Unteralgebren derselben Dimension konjugiert (und ebenso ihre Zentralisatoren).

Dieses Korollar verlangt noch nach etwas Erläuterung

3.36. Satz (Brauer) Sei A endlich dimensional, zentral einfache K-Algebra, $B \subseteq A$ eine einfache Unteralgebra mit $C(B) = E \supseteq K$. Dann gilt: $B' = C_A(B)$ ist einfach mit Zentrum E und $B'' = C_A(B') = C_A(C_A(B)) = B$. Weiter ist $C_A(E) = B \otimes B'$ und $[A : B'] = [B : K]$. Für $r := [B : K]$ ist

$$A \otimes B^{\mathrm{op}} \simeq B' \otimes M_r(K) \simeq M_r(B')$$

Beweis: Sei $r = \dim_K B$ und betrachte B als $M_r(K)$-Modul. Dann enthält $M_r(K)$ die Unteralgebra $\rho_B = B^{\mathrm{op}}$ und $\lambda_B \simeq B$ als Bilder der rechts- bzw. linksreguläre Darstellung. Dann ist $A \otimes_K M_r(K)$ zentral einfach über K und enthält Unteralgebren

$$B \otimes_K 1 \simeq 1 \otimes \lambda_B \simeq 1 \otimes B \simeq B.$$

Diese Unteralgebren sind einfach und daher nach Skolem-Noether (3.33) in $A \otimes M_r(K)$ konjugiert mit isomorphen Zentralisatoren. Also gilt:

Rechtswirkung und Linkswirkung zentralisieren sich

$$B' \otimes M_r(K) \simeq A \otimes \rho_B \simeq A \otimes B^{\mathrm{op}} \simeq M_r(B')$$

Damit folgt die letzte Behauptung. Die Dimension über B' ergeben

$$r^2 = \dim_{B'} M_r(B') = [A : B'] \cdot [B : K],$$

also $[A : B'] = r$. Nun ist nach 3.24 $A \otimes B^{\mathrm{op}}$ einfach und wieder nach 3.24 ist dann auch B' einfach. Es ist $B \subseteq B''$, $B''' = C_A(B'') = B'$ und wie eben (mit B ersetzt durch B') folgt $[B'' : K] = r$, d.h. $B'' = B$. Sei nun $F = C(B')$, dann ist $F \supseteq E$ und wegen $B'' = B$ folgt $E \supseteq F$, d.h. $E = F$. Daher sind B und B' zentral einfache E-Algebren. $B, B' \subseteq C_A(E)$ und aus Satz 3.22 folgt $C_A(E) = B \otimes B'$. □

beide Teile einfach

Bemerkung: Falls $C(B) \supsetneq K$, dann ist $C_A(E) \subsetneq A$, denn A ist zentral einfach.

3.37. Korollar Ist A zentral einfach mit endlicher Dimension über K, $E \subseteq A$ ein Teilkörper mit $K \subseteq E$ und $B \subseteq C_A(E)$. Dann ist

$$A \otimes E \simeq B \otimes M_r(K)$$

mit $r = \dim_K E$. Ist $n = \dim_K A$, dann ist $r^2 \mid n$ und $A \otimes B^{\mathrm{op}} \simeq M_{n/r}(E)$.

Beweis: Setze $B = E$ im Satz 3.36, dann ist $[C_A(E) : A] = \frac{n}{r^2} = [B : K]$. Mit $n = [A : K] = r^2 \cdot [B : K]$ gilt $C_A(E) \simeq E \otimes B$. Folglich ist $[C_A(E) : E] = [B : K]$. □

3.38. Korollar A endlich dimensionale, zentral einfache K-Algebra, $E \subseteq A$ Teilkörper mit $K \subseteq E$. Dann sind äquivalent:

(i) $E' = C_A(E) = E$

(ii) E ist ein maximaler kommutativer Unterring von A.

(iii) $[A : K] = [E : K]^2$

(iv) $[A : K] = [A : E]^2$

Insbesondere gilt für maximale Unterkörper in einem Schiefkörper D also $[D : K] = [E : K]^2 = [D : E]^2$

Beweis:

(i)⇔(ii): Klar.

(iii)+(iv)⇔(i) Es ist $E' \supseteq E$ und

$$[A : K] = [A : E] \cdot [E : K] = [E : K] = [E : K] \cdot [E' : K].$$

Also ist $[A : E]^2 \geqslant [A : K] \geqslant [E : K]^2$ und Gleichheit gilt genau dann, wenn $E = E'$, d.h. (iii)+(iv) sind äquivalent zu (i).

Bemerkung: Unterkörper $E \subseteq A$ mit $\dim_K A = (\dim_E A)^2$ muss es nicht geben. Z.B. $M_r(K)$, K algebraisch abgeschlossen, $r \geqslant 2$. Zum Satz von Wedderburn über Nicht-Existenz von endlichen Schiefkörpern:

3.39. Lemma Sei G eine endliche Gruppe, $H \lneq G$. Dann ist G *nicht* die Vereinigung der Konjugierten von H.

Beweis: Sei $|G| = |H| \cdot n$, also wenn $h = |H|$, dann ist $G/H = \{a_1 H, \dots, a_n H\}$. Dann ist für $b \in G$

$$bHb^{-1} = \underbrace{bH}_{a_i H}\underbrace{H^{-1}b^{-1}}_{H^{-1}a_i^{-1}} = a_i \underbrace{HH^{-1}}_{=H} a_i^{-1} = a_i H a_i^{-1}$$

Daher existieren höchstens n viele Konjugierte von H, die alle 1_G enthalten. Damit ist

$$\left| \bigcup_{i=1}^{n} a_i H a_i^{-1} \right| \leqslant n \cdot (h-1) + 1 < n \cdot h = |G|$$ □

3.40. Satz (Wedderburn) Jeder endliche Schiefkörper ist kommutativ.

Beweis: Sei D ein endlicher Schiefkörper, $K = C(D)$, d.h. D ist zentral einfach, endlich dimensional über K. Sei $E \subseteq D$ ein maximaler kommutativer Teilkörper. Nach Korollar 3.38 (ii) haben alle maximalen Unterkörper denselben Grad r über K, die maximalen Teilkörper sind nach Korollar 3.35 alle konjugiert. Da jedes Element von $a \in D$ über K einen kommutativen Teilkörper erzeugt, liegt jedes $a \in D$ in einem Konjugierten von E. nach Lemma 3.39 (angewandt auf die multiplikative Gruppe von D) folgt also $E = D = K$. □

3.41. Definition und Satz Zwei zentral einfache, endlich dimensionale K-Algebren A und B heißen ***ähnlich*** (oder Brauer-äquivalent, $A \sim B$), falls $A \simeq M_n(D)$, $B \simeq M_k(D)$ für einen Schiefkörper D über K, $n, k \in \mathbb{N}$. Dabei sind D, n, k nach Satz 2.29 eindeutig bestimmt. Insbesondere gibt es zu jeder zentral einfachen Algebra A einen Schiefkörper D über K mit $A \sim D$. Offensichtlich ist $\sim$ eine Äquivalenzrelation.

Für jeden Körper K bildet die Menge der Äquivalenzklassen bezüglich des Tensorprodukts eine Gruppe, die ***Brauergruppe*** $\mathrm{Br}(K)$ von K. Dabei ist $[K]$ das Neutralelement (denn $K \sim M_n(K)$) und $A \otimes K \simeq A$ und für $[A] \in \mathrm{Br}(K)$ ist $A \otimes A^{\mathrm{op}} \simeq M_n(K)$, d.h. $[A^{\mathrm{op}}] = [A]^{-1}$.

Beweis: Wir hatten bereits gesehen, dass das Tensorprodukt kommutativ und assoziativ ist, daher ist nur zu zeigen, dass $[A][B] = [A \otimes B]$ wohldefiniert ist, d.h. sind

$$M_n(D) \otimes M_k(D') \sim M_m(D) \otimes M_l(D') \sim D \otimes D'$$

Beispiel:

(i) Ist K algebraisch abgeschlossen oder endlich, dann ist $\mathrm{Br}(K) = 1$.

(ii) Ist $K = \mathbb{R}$, dann folgt aus $[\mathbb{C} : \mathbb{R}] = 2$ und $\mathbb{C}$ algebraisch abgeschlossen nach Korollar 3.40 , dass ein Schiefkörper über $\mathbb{R}$ Grad 2 (also Dimension 4) hat. Das heißt ist D endlicher Schiefkörper über $\mathbb{R}$, dann ist $\dim_{\mathbb{R}} D = \{1, 4\}$. Jeder echte Schiefkörper über $\mathbb{R}$ ist isomorph zu den Quaternionen.

Nummerierung prüfen

4. Darstellungstheorie endlicher Gruppen

4.1. Definition Eine ***Darstellung*** einer Gruppe ist (gegeben durch) einen Homomorphismus $\rho : G \to GL(V)$ für einen (endlich dimensionalen) K-Vektorraum. Der ***Grad*** der Darstellung ist $\dim V$. Ist $B = \{u_1, \dots, u_n\}$ eine K-Basis für V, dann ergibt jede Darstellung $\rho : G \to \mathrm{GL}(V)$ eine Matrix-Darstellung von G, indem $\rho(g) \in \mathrm{GL}(V)$ durch die zugehörigen Matrix bezüglich B beschrieben wird.
Ist $h : G \to \mathrm{Sym}(n)$ ein Homomorphismus, dann erhält man die zugehörige ***Permutationsdarstellung*** durch $\rho(g)u_i = u_{h(g)(i)}$. Dies hat man insbesondere für $|G| = n$ und

$$h : G \to \mathrm{Sym}(G) \quad , \quad g \mapsto \lambda_g = [x \mapsto gx].$$

4.2. Beispiel

(i) Ist $G = \langle g \rangle$ zyklisch, $|G| = n$, dann erhält man für $g = (1, \dots, n) \in \mathrm{Sym}(n)$ also $\rho(g)u_i = u_{i+1}$, $\rho(g)u_n = u_1$ mit zugehöriger Matrixdarstellung

$$\rho : g \longmapsto \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & 0 & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}$$

Ziel ist es, die Struktur aller Darstellungen zu verstehen. Jede Darstellung $\rho : G \to \mathrm{GL}(V)$ hat eine eindeutige Fortsetzung auf die Gruppenalgebra:

$$\tilde{\rho} : K[G] \to \mathrm{End}(V) \simeq M_n(K)$$

Erinnerung: $K[G]$ ist die K-Algebra mit Basis $G = \{g_1, \dots, g_n\}$ mit Multiplikation

$$\left(\sum_{g \in G} \alpha_g g\right)\left(\sum_{h \in G} \beta_h h\right) = \sum_{g,h} \alpha_g \beta_h (g \cdot h) \qquad , \quad \alpha_g, \beta_h \in K$$

Umgekehrt induziert jede Darstellung der Gruppenalgebra $K[G] \to \mathrm{End}(V)$ eine Darstellung der Gruppe $G \to \mathrm{GL}(V)$. Durch eine Darstellung $\rho : K[G] \to \mathrm{End}_K(V)$ wird V zu einem $K[G]$-Modul durch

$$\left(\sum_{g \in G} \alpha_g g\right) \cdot v = \rho\left(\sum_g \alpha_g g\right)(v).$$

Das heißt endlich dimensionale Darstellungen einer Gruppe G sind „das gleiche" wie $K[G]$-Moduln, die als K-Vektorräume endlich dimensional sind.

Übersetzung der Begriffe: Ist $\rho : G \to \mathrm{GL}\, V$ eine Darstellung, dann ist $U \leqslant V$ ein $K[G]$-Modul von V genau dann, wenn U ein $\rho(G)$-invarianter Untervektorraum von V ist, d.h. wenn $\rho(g)U \subseteq U$ für alle $g \in G$. Ist U ein $K[G]$-Untermodul, dann erhalten wir induzierte Darstellungen, nämlich $\rho\big|_U : G \to \mathrm{GL}(U)$ und die Quotientendarstellung

$$\rho_{V/U} : G \to \mathrm{GL}\, V/U \quad , \quad p_{V/U}(g) = [x + U \mapsto \rho(g)(x) + U]$$

Eine Darstellung $\rho : G \to \mathrm{GL}(V)$ heißt irreduzibel (bzw. vollständig reduzibel oder halbeinfach), falls V als $K[G]$-Modul irreduzibel (oder einfach) bzw. vollständig reduzibel (oder auch halbeinfach) ist. [11]

Erinnerung: M ist halbeinfacher R-Modul $\iff M = \bigoplus M_i$, M_i einfacher R-Modul $\iff$ jeder R-Untermodul $U \subseteq M$ hat Komplement $U^\perp$ in M, d.h. $M = U \oplus U^\perp$.

4.3. Definition Zwei Darstellungen $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$ heißen ***äquivalent***, falls ein Vektorraumisomorphismus $\varphi : V_1 \to V_2$ existiert mit $\rho_2 = \varphi\rho_1\varphi^{-1}$. Dann sind offensichtlich V_1 und V_2 als $K[G]$-Moduln isomorph.

4.4. Definition Sei G eine endliche Gruppe, V ein $K[G]$-Modul (oder G-Modul). Die ***Spurabbildung*** ist definiert durch

$$\mathrm{Tr}_G : V \to V^G = \{v \in V \mid gv = v \;\; \forall g \in G\} \quad , \qquad x \mapsto \sum_{g \in G} gx.$$

Ist $f : V \to W$ ein K-Homomorphismus von $K[G]$-Moduln, dann setze $\mathrm{Tr}_G(f) : x \mapsto \sum_{g\in G} gfg^{-1}x$. Dann ist $\mathrm{Tr}_G(f) : V \to W$ ein Homomorphismus von $K[G]$-Moduln[12].

4.5. Bemerkung Ist $f : V \to W$ bereits ein Homomorphismus von G-Moduln, dann ist $\mathrm{Tr}_G(f) = |G| \cdot f$.

4.6. Satz (Maschke) Sei G eine endliche Gruppe, K ein Körper. Dann ist $K[G]$ genau dann halbeinfach, wenn

$$\mathrm{char}(K) \nmid |G|.$$

Beweis:

"$\Leftarrow$": Sie $n = |G|$, $\mathrm{char}(K) \nmid |G|$. Dann existiert $\frac{1}{n} \in K$. Sei V ein $K[G]$-Modul, $U \subseteq V$ ein $K[G]$-Untermodul. Wir müssen zeigen, dass U ein G-invariantes Komplement hat. Sei U' ein beliebiges Vektorraum-Komplement von U in V, d.h. $V = U \oplus U'$ als Vektorraum (aber U' ist vielleicht nicht G-invariant). Betrachte nun die Vektorraum-Projektion $\pi_U : V \to U$ auf U. Definiere $\varphi : V \to U$ durch

$$\varphi = \frac{1}{n}\,\mathrm{Tr}_G(\pi).$$

Wegen $\pi|_U = \mathrm{id}_U$, gilt $\varphi|_U = \frac{1}{n}\,\mathrm{Tr}(\mathrm{id}_U) = \mathrm{id}_U$ nach Lemma 4.5. Nun ist φ ein $K[G]$-Modulhomomorphismus, d.h. $\ker\varphi = U^\perp$ ist ein $K[G]$-Untermodul von V und daher gilt

$$V = U \oplus U^\perp$$

als $K[G]$-Modul.

"$\Rightarrow$": Sei nun $\mathrm{char}\, K \mid |G|$, $|G| = n$. Betrachte die reguläre Darstellung von G auf $K[G] = V$. Dann ist $v = \sum_{g \in G} g \in V^G$ und $V^G \leqslant V$ ist ein G-invarianter Untervektorraum von V, also $K[G]$-Untermodul von V, $0 \lneq V^G \lneq V$. Ist nun $\pi : V \to V^G$ ein beliebiger $K[G]$-Homomorphismus, betrachte $v = \sum g \in V^G$

$$\pi(v) = \sum_g \pi(g) = \sum_g g\pi(1) = n\pi(1) = 0$$

[11] $p \in \mathrm{End}_k(V)$ zentral G, d.h. $\forall v \in V, g \in G : \varphi(gv) = g(\varphi(v)) \iff \varphi \in \mathrm{End}_{K[G]}(V)$
[12] $\varphi : V \to W$ ist $K[G]$-Homomorphismus: $\varphi(g \cdot v) = g \cdot \varphi(v)$

Daher kann es keine $K[G]$-lineare Projektion von V auf V^G geben und daher hat V^G kein Komplement in V als $K[G]$-Modul. □

Ist nun G eine Gruppe, $\rho : G \to \mathrm{GL}(V)$ halbeinfache Darstellung von G auf einem K-Vektorraum V (d.h. V ist als $K[G]$-Modul halbeinfach), dann zerfällt V in die direkte Summe von einfachen $K[G]$-Moduln als

$$V = V_1^{(1)} \oplus \ldots \oplus V_1^{(m_1)} \oplus V_2^{(1)} \oplus \ldots \oplus V_2^{(m_2)} \oplus \ldots \oplus V_r^{(1)} \oplus \ldots \oplus V_r^{(m_r)}$$

mit $V_i^k \simeq V_j^l$ als $K[G]$-Moduln genau dann, wenn $i = j$. Mit $\rho_i = \rho\big|_{V_i}$ schreibt man auch

$$\rho \sim m_1\rho_1 \oplus m_2\rho_2 \oplus \ldots \oplus m_r\rho_r.$$

Dabei heißen die m_i die Vielfachheiten der irreduziblen Komponenten ρ_i.

$$W_i = \bigoplus_{j=1}^{m_i} V_i^{(r)}$$

heißt homogenene Komponente von V. Ist G eine Gruppe, $H \trianglelefteq G$ ein Normalteiler, $\sigma : H \to \mathrm{GL}(V)$ eine Darstellung, dann ist für $g \in G$ die Abbildung $\sigma^g : H \to \mathrm{GL}(V)$, $h \mapsto [v \mapsto \sigma(ghg^{-1})v]$ wieder eine Darstellung von H auf V ($ghg^{-1} \in H$), die zu σ konjugiert ist. Es ist σ irreduzibel genau dann wenn σ^g irreduzibel ist.

4.7. Satz (Clifford) Sei G eine endliche Gruppe, $H \trianglelefteq G$ ein Normalteiler, $\rho : G \to \mathrm{GL}(V)$ eine irreduzible Darstellung von G auf V. Dann ist $\rho_H : H \to \mathrm{GL}(V)$ halbeinfach und alle homogenen irreduziblen Komponenten von V als $K[H]$-Modul sind konjugiert und haben die gleiche Multiplizität.

Beweis: Sei U ein irreduzibler $K[H]$-Untermodul von V und betrachte $\sum_{g\in G} \rho(g)U$. Dieser Raum ist G-invariant, weil V als $K[G]$-Modul irreduzibel ist, also $= V$. Seien nun $g \in G$, $h \in H$, $y \in U$. Dann folgt

$$\rho(h)\underbrace{(\rho(g)y)}_{\in\rho(g)U} = \rho(hg)y = \rho(gh^g)y = \rho(g)\underbrace{\rho(h^g)y}_{\in U} \in \rho(g)U$$

Daher ist $\rho(g)U$ ebenfalls $K[H]$-Untermodul. Behauptung: Für alle $g \in G$ ist $\rho(g)U$ irreduzibel $K[H]$-Modul. U ist als H-Modul irreduzibel und die Wirkung von H auf $\rho(g)U$ ist gegeben durch die Konjugationswirkung von H auf einem zu U isomorphen Vektorraum. Nach der Vorbemerkung sind also alle $\rho(g)U$ irreduzible H-Moduln, d.h. ist als H-Modul halbeinfach. Da die irreduziblen Komponenten von der Form $\rho(g)U$ für ein $g \in G$ sind, haben alle dieselbe Dimension und sind konjugiert. Die G-Wirkung bildet isomorphe H-Untermoduln wieder auf solche ab. Daher permutiert G die H-homogenen Komponenten transitiv und alle homogenen Komponenten haben dieselbe Multiplizität. □

4.8. Korollar Ist G eine endliche Gruppe, $H \trianglelefteq G$, $\rho : G \to \mathrm{GL}(V)$ halbeinfach, dann ist auch $\rho\big|_H$ halbeinfach.

Beweis: Wende 4.7 auf die irreduziblen Komponenten an. □

4.9. Definition Eine K-Algebra A hat die ***Doppelzentralisatoreigenschaft***, falls für einen A-Modul V und $A' = \operatorname{End}_A V$, $A'' = \operatorname{End}_{A'} V$ gilt $A = A''$.

4.10. Satz Ist $\rho : G \to \mathrm{GL}(V)$ eine halbeinfache Darstellung, dann hat $A = K[G]$ die Doppelzentralisatoreigenschaft.

Beweis: Dichtheitssatz von Jacobson 3.10. □

Sei nun G eine endliche Gruppe, K ein Körper, $\operatorname{char} K \nmid |G|$, $A = K[G]$. Es gibt eine Zerlegung $A = \bigoplus_{i=1}^s A_i$ in einfache Algebren. Nach Wedderburn ist $A_i \simeq M_{n_i}(D_i)$ für einen Schiefkörper D_i über K, $i = 1, \ldots, s$, $d_i = \dim_K(D_i)$.

4.11. Satz Sein G, K, A_i wie eben, dann entsprechen die minimalen Linksideale $J_i \subseteq A_i$ genau den irreduziblen Darstellungen von G. Der Grad der zu J_i gehörigen Darstellung ist $n_i \cdot d_i$. $J_i = M_{n_i}(D_i)e_{kk}$, $A_i = \bigoplus_{k=1}^{n_i} M_{n_i}(D_i)e_{kk}$

Beweis: Für eine halbeinfache Algebra A entsprechen die irreduziblen A-Moduln genau den minimalen Linksidealen der A_i. Ein minimales Linksideal in $M_n(D)$ ist von der Form $M_n(D)e_{ii}$ mit K-Dimension $n \cdot \dim_K D$.

Ist ρ_i die zu $J_i = A_i$ gehörige irreduzible Darstellung, dann ist für eine beliebige Darstellung $\rho : G \to \mathrm{GL}(V)$ (für $\operatorname{char} K \nmid |G|$) also V ein halbeinfacher $A(= K[G])$-Modul und zerfällt in einfache Komponenten $V = \bigoplus V_j$, V_j G-invariant. Für jedes j existiert ein i mit $\rho|_{V_j} = \rho_i$ und wir können schreiben

$$\rho \sim m_1\rho_1 \oplus \ldots \oplus m_s\rho_s$$

□

4.12. Satz Ist $\rho : G \to K[G]$ die reguläre Darstellung, dann ist die Vielfachheit von ρ_i in ρ genau n_i in der Notation von vorher, also

$$\rho \sim n_1\rho_1 \oplus \ldots \oplus n_s\rho_s$$

Beweis: Die reguläre Darstellung ist die Linkswirkung von G auf $A = K[G]$, d.h. $K[G]$ betrachtet als $K[G]$-Modul. Es ist $A = \bigoplus_{i=1}^s A_i$,

$$A_i = M_{n_i}(D_i) = \bigoplus_{k=1}^{n_i} M_{n_i}(D_i)e_{kk}$$

Daraus folgt die Behauptung. □

4.13. Satz Sei G eine endliche Gruppe, $G = C_1 \cup \ldots \cup C_r$ die Zerlegung in die Konjugiertenklassen. Wir setzen $c_i = \sum_{h \in C_i} h \in A$, $i \leqslant r$. Dann bilden $c_1, \ldots, c_r$ eine Basis für $Z(A)$. $Z(A) = \bigoplus_{i=1}^s Z(A_i)$

1. Behauptung: $c_i \in Z(A)$**:** Für $g \in G$ gilt

$$g^{-1}c_i g = \sum_{h \in c_i} g^{-1}hg = \sum h = c_i \in Z(A)$$

2. Behauptung: $\{c_1, \ldots, r_r\}$ **linear unabhängig:** Klar.

3. Behauptung: $\langle\{c_1,\dots,c_r\}\rangle = Z(A)$: Sei nun $c \in Z(A)$ beliebig, etwa $c = \sum_{g\in G}\gamma_g g$, $\gamma_g \in K$, $g \in G$. Sei $h \in G$, also

$$h^{-1}ch = \sum_g \gamma_g h^{-1}gh = \sum_g \gamma_{hgh^{-1}}g = \sum_g \gamma_g g = c$$

Ein Koeffizientenvergleich ergibt $\gamma_g = \gamma_{hgh^{-1}}$ für alle $g,h \in G$, d.h. es existiert $\gamma_i \in K$, so dass für alle $g \in C_i$ gilt $\gamma_g = \gamma_i$. Daraus folgt die Behauptung. □

4.14. Bemerkung Daher gilt $s \leqslant \dim Z(A) = r$. Es gilt also $\dim Z(A) = \sum_{i=1}^s [K_i : K] = r$ und daher $r = s$ genau dann, wenn A_i zentral einfach für alle $i = 1,\dots,s$. Ist K algebraisch abgeschlossen, dann ist immer $r = s$.

4.15. Satz Sei G eine endliche Gruppe, K algebraisch abgeschlossen, $\operatorname{char} K \nmid |G|$, $s =$ #Konjugiertenklassen von G. Dann ist die Anzahl der irreduziblen Darstellungen von G (bis auf Äquivalenz) genau s und falls die $\rho_1,\dots\rho_s$ wie eben sind mit $\deg\rho_i = n_i$, dann folgt

$$|G| = \sum_{i=1}^s n_i^2.$$

Beweis: Die erste Aussage ist genau die Vorbemerkung 4.14. Ist K algebraisch abgeschlossen, dann ist $A = K[G] = \bigoplus_{i=1}^s M_{n_i}(K)$, daher gilt $|G| = \dim A = \sum_{i=1}^s n_i^2$. □

4.16. Korollar Ist G abelsch, dann ist über algebraisch abgeschlossenen Körpern K mit $\operatorname{char} K \nmid |G|$ jede irreduzible Darstellung 1-dimensional, d.h. jede Darstellung $G \to \mathrm{GL}(V)$, für V K-Vektorraum, ist diagonalisierbar.

Beweis: Es ist $s = |G|$, also $n_i = 1$ für $i = 1,\dots,s$. □

4.17. Beispiel Sei $n \in \mathbb{N}$, $G = C_n$ zyklisch der Ordnung n, $A = \mathbb{C}[G]$. Da G abelsch ist, gibt es genau n irreduzible Darstellungen, jeweils von Grad 1. Die entsprechenden Darstellungen sind:

$$g \mapsto \left(e^{\frac{2\pi i r}{n}}\right) \qquad , \qquad r = 1,\dots,n, \ \langle g\rangle = C_n$$

Erinnerung: Ist V ein K-Vektorraum, $L \supseteq K$ eine Körpererweiterung, dann ist $V_L = V \otimes_K L$ ein L-Vektorraum mit $\dim_L V_L = \dim_K V$. Jede K-lineare Abbildung von V lässt sich kanonisch zu einer L-linearen Abbildung von V_L fortsetzen. Ds gilt insbesondere für Darstellungen $\rho : G \to \mathrm{GL}(V)$ und entsprechend $\rho_L : G \to \mathrm{GL}(V_L)$.

4.18. Satz Sei G eine Gruppe, K ein Körper, $L \supseteq K$ eine Körpererweiterung, V ein K-Vektorraum. Dann gilt

$$\operatorname{End}_{L[G]} V_L = L \cdot \operatorname{End}_K[G]V \simeq \big(\operatorname{End}_{K[G]} V\big)_L$$

Beweis: Es ist

$$\operatorname{End}_{L[G]} V_L = \operatorname{End}_{L[G]}(V \otimes_K L) = \operatorname{End}_{K[G]} V \otimes_K L = \big(\operatorname{End}_{K[G]} V\big)_L$$

Klar ist auch $L \cdot \operatorname{End}_{K[G]} V \subseteq \operatorname{End}_{L[G]} V_L$. Für die andere Inklusion wähle eine Basis $\{\lambda_i \mid i \in I\}$ für L über K. Jedes $\alpha \in \operatorname{End}_L V_L$ lässt sich eindeutig schreiben als $\alpha = \sum_{i\in I} \lambda_i l_i$ mit $l_i \in \operatorname{End}_K V$. Es ist $\alpha \in \operatorname{End}_{L[G]} V_L$ genau dann, wenn α mit der G-Wirkung vertauscht, genau dann wenn jedes l_i mit der G-Wirkung vertauscht, d.h. wenn $l_i \in \operatorname{End}_{K[G]} V$. □

Ist $U \subseteq V$ ein G-invariante Unterraum, dann ist auch $U \otimes L \subseteq V_L$ G-invariant. Daher ist falls ρ_L irreduzibel ist, ach ρ irreduzibel. Aber die Umkehrung gilt *nicht*:

Beispiel: Sie $G = C_4 = \langle g \rangle$, $K = \mathbb{R}$, $V = \mathbb{R}^2$, $\rho : G \to \mathrm{GL}_2(\mathbb{R})$, $\rho(g) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, Drehung um 90°. In V gibt es keine G-invarianten Unterräume, d.h. ρ ist irreduzibel. Aber über $\mathbb{C}$ hat eine abelsche Gruppe keine irreduzible Darstellung in Dimension > 1. Bei geeigneter Wahl einer Basis für $V_\mathbb{C}$ wird $\rho_\mathbb{C}(G)$ als Diagonalmatrix dargestellt.

Bemerkung: $\rho : G \to \mathrm{GL}_n(K)$ irreduzibel, $L \supseteq K \not\Rightarrow \rho_L : G \to \mathrm{GL}_n(L)$ irreduzibel. $\Leftarrow$ gilt aber!

4.19. Definition Eine Darstellung $\rho : G \to \mathrm{GL}(V)$ für einen K-Vektorraum V heißt ***absolut irreduzibel***, falls ρ_L irreduzibel ist für jeden Körper $L \supseteq K$.

Hier stimmt die Nummerierung noch nicht!

4.20. Satz Sei G eine endliche Gruppe, $\rho : G \to \mathrm{GL}(V)$ eine Darstellung über K mit $\operatorname{char} K \nmid |G|$. Setze $A := K[G]$ und $A' = \operatorname{End}_A(V) = C_{\operatorname{End}_K(V)}(A)$. Dann ist ρ irreduzibel genau dann, wenn A' ein Schiefkörper ist und absolut irreduzibel, wenn $A' = K$ gilt.

Beweis: Der erste Teil der Behauptung ist Schurs Lemma (2.26): Wenn ρ irreduzibel ist, dann ist A' ein Schiefkörper. Ist umgekehrt ρ nicht irreduzibel, dann ist $V = B \oplus C$ für $K[G]$-Untermoduln B und C. Die Projektion $\pi_B : V \to B$ ist $K[G]$-linear, d.h. $\pi_B \in A'$, aber $\pi_B \neq 0$ und π_B ist nicht invertierbar, d.h. A' ist kein Schiefkörper.

Ist nun ρ absolut irreduzibel und $K \subsetneq A'$, dann sei $c \in A' \setminus K$. f sei das Minimalpolynom von c über K, d.h. $\deg f > 1$ und f ist irreduzibel, weil A' ein Schiefkörper ist. Setze

$$L = {}^{K[X]}/_{(f)}$$

und betrachte A'_L. Dann hat f eine Nullstelle in L, d.h. A'_L ist kein Schiefkörper, weil A'_L Nullteiler enthält $\lightning$ ρ absolut irreduzibel. Ist umgekehrt $A' = K$, dann ist für jeden Körper $L \supseteq K$ natürlich $A'_L = K \otimes L = L$ ein Körper, also ρ absolut irreduzibel. □

4.21. Definition Sei G eine endliche Gruppe, K ein Körper. Dann heißt K ***Zerfällungskörper*** für G, wenn jede Darstellung von G über K absolut irreduzibel ist.

4.22. Satz Sei G eine endliche Gruppe, K ein Körper mit $\operatorname{char} K \nmid |G|$. Dann ist K Zerfällungskörper für G genau dann, wenn $K[G]$ die direkte Summe von Matrizengruppen $M_n(K)$ ist.

Beweis: Zerlege $A = K[G] = \bigoplus A_i$, wobei A_i einfach ist. Sei $J_i \subseteq A_i$ ein minimales Linksideal in A_i. Die irreduziblen Darstellungen von G über K entsprechen genau den Darstellungen ρ_i von G auf J_i. Also ist K genau dann Zerfällungskörper, wenn alle ρ_i absolut irreduzibel sind. Nach Satz 4.21 ist dies genau dann der Fall, wenn

$$D'_i = \operatorname{End}_A J_i = K \quad \text{für alle } i.$$

Wegen der Irreduzibilität von J_i ist D_i' ein Schiefkörper und wegen der Doppelzentralisatoreigenschaft (Satz 4.10) gilt

$$\operatorname{End}_{D_i'} J_i = \rho_i(A) \simeq M_{n_i}(D_i)$$

für $D_i = (D_i')^{\mathrm{op}}$ und $n_i = \dim_{D_i'} J_i$. Da die A_i einfach sind, ist $\rho_i(A) = A_i$, d.h. $A_i \simeq M_{n_i}(D_i)$. Wenn K ein Zerfällungskörper ist, dann sind die ρ_i absolut irreduzibel, d.h. $D_i' = K$ und $A_i \simeq M_{n_i}(K)$.

Ist $A_i \simeq M_{n_i}(K) = M_{n_i}(D_i)$, dann folgt $K = D_i$, insbesondere $D_i' = K$ und nach Satz 4.20 sind die ρ_i absolut irreduzibel, d.h. K ist Zerfällungskörper. □

4.23. Definition Eine 1-dimensionale Darstellung $G \to \mathrm{GL}_1(K) = K^*$ heißt ***linearer Charakter***. Ist $\rho : G \to \mathrm{GL}(V)$ eine Darstellung, dann heißt $\chi_\rho : G \to K$, $\chi_\rho(g) = \mathrm{Tr}\big(\rho(g)\big)$ der zu ρ gehörige ***Charakter***, d.h. ist$p(x) = (\rho_{ij}(x))$ so ist

$$\mathrm{Tr}\big(p(x)\big) = \sum_{i=1}^{\dim V} \rho_{ii}(x)$$

Bemerkung: χ_ρ ist wohldefiniert, weil Tr nicht von der Basiswahl abhängt. Jede 1-dimensionale Darstellung ist ihre eigener Charakter. Für abelsche Gruppen über algebraisch abgeschlossenen Körpern sind die Charaktere genau die irreduziblen Darstellungen.

4.24. Proposition

(i) Äquivalente Darstellungen haben denselben Charakter.

(ii) Jeder Charakter ist eine Klassenfunktion, d.h. konstant auf Konjugationsklassen von G.

(iii) Ist $\operatorname{char} K = 0$, dann $\chi_\rho(1) = \dim V$.

(iv) Sind ρ_1, ρ_2 Darstellungen mit Charakteren χ_i und χ_2, dann sind $\rho_1 \oplus \rho_2$, $\rho_1 \otimes \rho_2$ Darstellungen mit Charakter $\chi_1 + \chi_2$ bzw. $\chi_1 \cdot \chi_2$

(v) Ist $K = \mathbb{C}$, $x \in G$ mit $x^n = 1_G$, dann ist $\chi(x)$ Summe von n-ten Einheitswurzeln in $\mathbb{C}$.

Beweis:

(i) Klar: Sind ρ_1, ρ_2 äquivalent via dem Vektorraumisomorphismus φ, dann ist auch $\rho_2(g) = \varphi\rho_1(g)\varphi^{-1}$, also $\mathrm{Tr}\,\rho_2(g) = \mathrm{Tr}\,\rho_1(g)$.

(ii) Für $g, h \in G$ ist

$$\mathrm{Tr}\big(\rho\big(hgh^{-1}\big)\big) = \mathrm{Tr}\big(\rho(h)\rho(g)\rho(h)^{-1}\big) = \mathrm{Tr}\big(\rho(g)\big)$$

(iii) Es ist $\rho(1_G) = \mathrm{id}_V$

(iv) Es ist $\mathrm{Tr}(A \oplus B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ und $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A) \cdot \mathrm{Tr}(B)$

(v) Ist $x^n = 1_G$ für $x \in G$, dann gilt für $A = \rho(x)$ ebenfalls $A^n = \mathrm{id}_V$, d.h. das Minimalpolynom von A teilt das Polynom $X^n - 1$, mit Wurzeln $\omega_1, \ldots, \omega_n \in \mathbb{C}$. Daher ist A eine Diagonalmatrix mit Einträgen aus $\{\omega_1, \ldots, \omega_n\}$. □

4.25. Beispiel

(i) Sei $\rho : G \to \mathrm{GL}_1(V)$ die triviale Darstellung mit $\rho(g) = 1$, dann heißt $\chi_\rho : G \to K^*$, $g \mapsto 1$ ***trivialer Charakter***.

(ii) Sei G endlich, $|G| = n$, $\rho : G \to \mathrm{GL}_n(K)$ die reguläre Darstellung durch Permutationsmatrizen. Dann ist

$$\chi_\rho(g) = \begin{cases} n, & \text{falls } g = 1_G \\ 0, & \text{sonst} \end{cases}$$

4.26. Satz (Orthogonalitätsrelationen für irreduzible Darstellungen) Sei G eine endliche Gruppe, K der Zerfällungskörper für G, $\operatorname{char} K = 0$. Sind ρ, σ irreduzible Darstellungen der Dimension c bzw. d, dann gilt für alle $i, j \leqslant c$ und $p, q \leqslant d$

in der „Praxis“: $K = \mathbb{C}$

$$\sum_{g \in G} \rho_{ij}(g) \cdot \sigma_{pq}(g^{-1}) = \begin{cases} 0, & \text{falls } \rho, \sigma \text{ nicht äquivalent} \\ \frac{|G|}{d} \cdot \delta_{jp} \cdot \delta_{iq}, & \text{falls } \rho = \sigma \end{cases}$$

wobei $\rho(g) = \big(\rho_{ij}(g)\big)_{i,j \leqslant c}$, $\sigma(g) = \big(\sigma_{pq}(g)\big)_{p,q \leqslant d}$.

Beweis: Seien $\rho : G \to \mathrm{GL}(U)$, $\sigma : G \to \mathrm{GL}(V)$, $(u_1, \dots, u_c)$ bzw. $(v_1, \dots, v_d)$ Basen von U bzw. V. Sei weiter

$$\alpha_{jp} : U \to V \quad , \quad u_i \mapsto \delta_{ij} \cdot v_p = \begin{cases} u_j \mapsto v_p, & \text{für } i = j \\ u_i \mapsto 0 & \text{für } i \neq j \end{cases}$$

α_{jp} ist K-linear und $\mathrm{Tr}(\alpha_{jp}) : U \to V$ ist $K[G]$-linear. Sind ρ und σ nicht äquivalent, dann folgt $\mathrm{Tr}(\alpha_{jp}) = 0$ für alle $j \leqslant c$, $p \leqslant d$. (siehe 2. Satz von Wedderburn, 2.31). Sind $\rho \sim \sigma$, also $U \simeq V$ $K[G]$-Moduln, dann ist $\mathrm{Tr}(\alpha_{jp}) = \lambda_{jp} \in K$, denn U ist einfach und $\mathrm{End}_{K[G]} U = K$.

Es ist $(\alpha_{jp})_{iq} = \delta_{ij} \cdot \delta_{pq}$, also

$$\big(\mathrm{Tr}(\alpha_{jp})\big)_{iq} = \sum_{\substack{h \leqslant c, r \leqslant d \\ g \in G}} \rho_{ij}(g) \cdot \delta_{hj} \cdot \delta_{pr} \cdot \sigma_{rq}(g)^{-1} = \sum_{g \in G} \rho_{ij}(g) \cdot \sigma_{pq}(g)^{-1}$$

Falls $\rho \not\sim \sigma$, folgt die Behauptung. Sei nun $\rho = \sigma$. Dann ist

$$\sum_g \rho_{ij}(g) \cdot \rho_{pq}(g)^{-1} = \lambda_{jp} \cdot \delta_{iq}$$

Für $i = q$ ergibt sich als Summe $i = 1, \dots, d = c$

$$d\lambda_{jp} = \sum_i \sum_g \rho_{pi}(g)^{-1} \cdot \rho_{ij}(g) = \sum_g \rho_{pj}(1) = |G| \cdot \delta_{jp}$$

Daher gilt $\lambda_{jp} = \frac{|G|}{d} \delta_{jp}$ und damit

$$\sum_g \rho_{ij}(g) \cdot \sigma_{pq}(g)^{-1} = \frac{|G|}{d} \cdot \delta_{jp} \cdot \delta_{iq}. \qquad \square$$

4.27. Korollar Sei G eine endliche Gruppe, K ein Zerfällungskörper, $\operatorname{char} K \nmid |G|$, $\{\rho_1, \dots, \rho_s\}$ Repräsentanten für die Äquivalenzklassen der irreduziblen Darstellung über K. Für jedes $i = 1, \dots, s$ sei $\rho^{(i)}$ eine Matrixdarstellung für ρ_i. Dann gilt

$$\sum_g \rho_{ij}^{(k)}(g) \cdot \rho_{pq}^{(l)}(g)^{-1} = \begin{cases} 0, & \text{falls } k \neq l \\ \frac{|G|}{\deg \rho_k} \cdot \delta_{jp} \cdot \delta_{iq}, & \text{falls } k = l \end{cases}$$

4.28. Korollar Sind χ_i, $i = 1, \dots, s$ die zu ρ_i gehörigen Charaktere, dann gilt

$$\sum_g \chi_i(g) \cdot \chi_j(g)^{-1} = \begin{cases} 0, & \text{falls } i \neq j \\ |G|, & \text{falls } i = j \end{cases}$$

Ist speziell $K = \mathbb{C}$, dann folgt wegen Proposition 4.24(v)

$$\sum_g \chi_i(g) \cdot \chi_j(g)^{-1} = \sum_g \chi_i(g) \cdot \overline{\chi_j(g)} = \begin{cases} 0, & \text{falls } i \neq j \\ \sum_g \chi_i(g) \cdot \overline{\chi_i(g)} = \sum_g \left|\chi_i(g)^2\right| = |G|, & \text{falls } i = j \end{cases}$$

Betrachte $K[G] = K^G$ als K-Vektorraum aller K-wertigen Funktionen auf G. Definiere inneres Produkt auf $K[G]$ durch

$$\left(\sum_{x \in G} \alpha_x x, \sum_{y \in G} \beta_y y \right) = \frac{1}{|G|} \sum_{x \in G} \alpha_{x^{-1}} \beta_x \in K,$$

falls $\operatorname{char} K \nmid |G|$. Für $K = \mathbb{C}$ erhalten wir eine hermitesche Form durch

$$(\varphi, \psi) = \frac{1}{|G|} \sum_g \overline{\varphi(g)} \psi(g).$$

Dann ist

$$(\varphi, \varphi) = \frac{1}{|G|} \sum_g \overline{\varphi(g)} \varphi(g) = \frac{1}{|G|} \sum_g |\varphi(g)|^2 \geqslant 0$$

und $(\varphi, \varphi) = 0 \iff \varphi = 0$, d.h. $(\_, \_)$ ist positiv definit und regulär. Nach Korollar 4.28 gilt $(\chi_i, \chi_j) = \delta_{ij}$, d.h. die Charaktere der irreduziblen Darstellung $\chi_i, \dots \chi_s$ bilden eine Orthonormalbasis des $\mathbb{C}$-Vektorraumes der Klassenfunktionen.

Ist nun $\rho : G \to \mathrm{GL}(\mathbb{C})$ eine beliebige Darstellung mit Charakter χ, dann ist $\rho \sim m_1 \rho_i \oplus \dots \oplus m_s \rho_s$ und daher

$$\chi = m_i \cdot \chi_i \dots + m_s \cdot \chi_s.$$

Daher ist $(\chi_i, \chi_i) = m_i$, $i = 1, \dots, s$.

4.29. Korollar Komplexe Darstellungen einer endlichen Gruppe sind genau dann äquivalent, wenn sie denselben Charakter haben.

4.30. Beispiel Bestimme alle irreduziblen Charaktere (bzw. Darstellungen) von S_3. Es gilt $|S_3| = 6$. S_3 hat drei Konjugationsklassen mit Vertretern

$$\mathrm{id}, \begin{matrix} (1\ 2) \\ (1\ 3), \\ (2\ 3) \end{matrix} \begin{matrix} (1\ 2\ 3) \\ (2\ 3\ 1) \end{matrix}$$

Es gibt zwei 1-dimensionale Darstellung von S_3 mit Charakter $\chi_i(g) = 1$ und $\chi_2(g) = \operatorname{sgn}(g)$. Wegen $6 = 1^2 + 1^2 + 2^2$ existiert noch eine 2-dimensionale Darstellung, d.h. es gilt $\chi_3(1) = 2$. Nun muss χ_3 auf χ_1 und χ_2 senkrecht sein, d.h.

$$(\chi_1, \chi_3) = \frac{1}{6} \big(2 + 3\chi_3((1\ 2)) + 2\chi_3((1\ 2\ 3))\big) = 0$$
$$(\chi_2, \chi 3) = \frac{1}{6} \big(2 - 3\chi_3((1\ 2)) + 2\chi_3((1\ 2\ 3))\big) = 0$$

$\Rightarrow \chi_3(1\ \ 2) = 0$ und $\chi_3(1\ \ 2\ \ 3) = -1$. Damit ergibt sich die Charaktertafel

Und für größere n die Young-Tableaus.

Dualität für endliche abelsche Gruppen

4.31. Definition Sei G eine abelsche Gruppe, dann heißt $G^* = \operatorname{Hom}(G, \mathbb{C}^*)$ die ***Charaktergruppe*** (oder duale Gruppe) von G unter der Multiplikation: $\varphi, \psi \in G^*$,

$$\varphi \cdot \psi : G \to \mathbb{C}^*, g \mapsto \varphi(g) \cdot \psi(g)$$

Bemerkung: Ist $G = {}^{\mathbb{Z}}/_{n\mathbb{Z}} = C_n$ zyklisch mit $G = \langle s \rangle$, $\chi : G \to \mathbb{C}^*$, dann ist $\chi(s)$ eine n-te Einheitswurzel. Ist $\omega^* \in \mu_n$ eine n-te Einheitswurzel, dann ist $\chi(s^i) = \omega^i$ ein Charakter. Daher ist hier $C_n^* = \mu_n \simeq C_n$ Gruppe der n-ten Einheitswurzeln.

4.32. Satz Jede endliche abelsche Gruppe A ist isomorph zur dualen Gruppe A^*.

Beweis: Nach dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen ist $A \simeq A_1 \oplus \ldots \oplus A_r$ mit A_i zyklisch. Offensichtlich gilt

$$\hom(B \times C, \mathbb{C}^*) \cong \hom(B, \mathbb{C}^*) \times \hom(C, \mathbb{C}^*).$$

Daher ist $(B \times C)^* \cong B^* \times C^*$. Also

$$A^* \simeq A_1^* \times \ldots \times A_r^* \simeq A_1 \times \ldots \times A_r = A. \qquad \square$$

A. Anhang

A.1. Alternative Definition von Gruppenwirkungen Eine ***Gruppenwirkung*** von G auf X ist (gegeben durch) eine Abbildung $G \times X \to X$, $(g, x) \mapsto g \cdot x$, mit folgenden Eigenschaften:

- $e_G \cdot x = x$, und
- $g \cdot (h \cdot x) = (gh) \cdot x$,

für alle $x \in X$ und alle $g, h \in G$.

Rechts-Gruppenwirkung: Die oben angegebenen Definitionen beschreiben eine ***linksseitige Gruppenwirkung***.
Eine ***rechtsseitige Gruppenwirkung*** ist (gegeben durch) eine Abbildung $X \times G \to X$, $(x, g) \mapsto x \cdot g$, wobei für alle $x \in X$ und alle $g, h \in G$ die Bedingungen $x \cdot e = x$ und $(x \cdot g) \cdot h = x \cdot (gh)$ erfüllt sind.
Alternativ kann eine rechtsseitige Gruppenwirkung durch einen Gruppenhomomorphismus $\varphi : G \to \mathrm{Sym}(X)^{\mathrm{op}}$ beschrieben werden, wobei $\mathrm{Sym}(X)^{\mathrm{op}} := (\mathrm{Sym}(X), *)$ mit $f * g := g \circ f$ ist. (vgl. Definition 2.28).

A.2. Beweis für 2.6(a) von Blatt 3 Sei M ein zyklischer R-Modul. Sei $0 \neq x \in M$. Dann gilt $\langle x \rangle = M$. Betrachte den Homomorphismus $\varphi : R \to M$, $r \mapsto r \cdot x$. φ ist surjektiv, da $\langle x \rangle = M$. Dann gilt

$$R/\ker\varphi \simeq M$$

Dann ist $J := \ker\varphi$ ein Ideal in R. Zu zeigen: J ist maximal. Annahme: Es existiert ein echtes Ideal $I \subset R$ mit $J \subsetneq I$. Dann ist I/J ein Ideal in $R/J \simeq M$. Dann ist I/J ein Untermodul von M. Da M zyklisch ist und I/J ein nichtriviales Element enthält, gilt $I/J = M$. Dann folgt aber $I = R$ und wir erhalten einen Widerspruch. $\square$

Index

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

Abbildungsverzeichnis

Todo’s und andere Baustellen