

Skript Höhere Algebra I


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

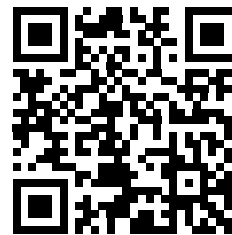
Jannes Bantje

30. Juni 2014

Aktuelle Version verfügbar bei:



 **GitHub** (inklusive Sourcecode)
<https://github.com/JaMeZ-B/latex-www>



 **Bittorrent Sync**
B6WH2DISQ5QVYIRYIEZSF4ZR2IDVKPN3I

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 annotierten PDFs)
- *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 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 Internet¹.

- *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!

Vorlesungshomepage

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

Literatur

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

¹zB. <https://try.github.io/levels/1/challenges/1>, ist auf Englisch, aber dafür interaktives LearningByDoing

Inhaltsverzeichnis

1. Gruppentheorie: Wiederholung, Sylow-Sätze, Kompositionsreihen	1
1.1. Definition: Gruppenwirkung	1
1.2. Bemerkung über eine Abbildung $G/G_x \rightarrow G(x)$	1
1.3. Beispiele für Gruppenwirkungen	1
1.4. Bahnengleichung	2
1.5. Klassengleichung	2
1.6. Korollar: p -Gruppen haben ein nichttriviales Zentrum	2
1.7. Definition: p -Sylowgruppe	2
1.8. Satz (Sylow)	2
1.9. Satz (Frattini-Argument)	3
1.10. Bemerkung zu p -Sylowgruppen in Normalteilern und Faktorgruppen	4
1.11. Definition: Normalreihe und Kompositionsreihe	4
1.12. Beispiel zu Normalreihen	4
1.13. Ziel: Satz von Jordan-Hölder	4
1.14. Schmetterlings-Lemma (Zassenhaus)	4
1.15. Satz von Schreier	5
1.16. Definition: Auflösbare und nilpotente Gruppen	6
1.17. Bemerkung: Nilpotente Gruppen sind auflösbar, Umkehrung gilt nicht	6
1.18. Satz: Auflösbare Untergruppen, Quotienten und Produkten auflösbarer Gruppen	6
1.19. Korollar: Auflösbare ist äquivalent zur Auflösbarkeit von Normalteilern und Quotienten	6
1.20. Korollar: Das Produkt auflösbarer Normalteiler ist auflösbar	6
1.21. Satz: Untergruppen und Quotienten nilpotenter Gruppen	7
1.22. Satz: Endliche p -Gruppen sind nilpotent	7
1.23. Definition: Kommutator	7
1.24. Satz: Eigenschaften der Kommutatorgruppe	7
1.25. Definition: Konstruktion weiterer Kommutatorgruppen	8
1.26. Satz: Auflösbarkeit einer Gruppe G	8
1.27. Definition: Untere Zentralreihe	8
1.28. Satz: Charakterisierung von Nilpotenz über die untere Zentralreihe	8
1.29. Einschub über direkte und semidirekte Produkte	9
2. Moduln: Halbeinfache Moduln, freie Moduln	10
2.1. Satz: Jeder Ring ist isomorph zu einem Endomorphismenring	10
2.2. Definition: Modul	10
2.3. Beispiele für Moduln	10
2.4. Definition: Untermodul, einfache Moduln und Ringe	11
2.5. Definition: erzeugte Untermoduln	11
2.6. Bemerkung zu Modulstrukturen auf Quotienten	11
2.7. Definition: Klasse der R -Moduln, R -Modul-Homomorphismen	11
2.8. Bemerkung zu $\text{Hom}_R(M, N)$	11
2.9. Satz: Homomorphie- und Isomorphiesätze für Moduln	12
2.10. Definition: Exakte Sequenz	12
2.11. Definition: noethersch und artinsch	12
2.12. Proposition: noethersch \iff alle Untermoduln endlich erzeugt	13
2.13. Satz: noethersch (artinsch) innerhalb einer kurzen exakten Sequenz	13
2.14. Korollar: Endliche Summen noetherscher Moduln sind noethersch (artinsch)	13
2.15. Korollar: Moduln über einem noetherschen Ring sind noethersch	13
2.16. Korollar: Endlich erzeugte Moduln über einem Hauptidealring sind noethersch	14
2.17. Definition: Halbeinfacher Modul	14

2.18. Beispiele zu halbeinfachen Moduln	14
2.19. Satz: Äquivalenzen zu halbeinfach durch Summen aus einfachen Untermoduln	14
2.20. Lemma: Jeder halbeinfache Modul hat einen einfachen Untermodul	15
2.21. Satz: Alle R -Moduln halbeinfach $\Leftrightarrow (R, +)$ halbeinfach	15
2.22. Korollar: M direkte Summe einfacher Untermoduln $\Rightarrow P \leq M$ isomorph zu Teilsumme	15
2.23. Korollar (Krull-Remak-Schmidt)	16
2.24. Bemerkung: M endlich erzeugt $\Leftrightarrow M$ endliche direkte Summe einfacher Untermoduln	16
2.25. Satz über die Ideale eines Ringes R und die Ideale in $M_k(R)$	16
2.26. Satz (Schurs Lemma)	17
2.27. Lemma: Darstellung von $\varphi \in \text{End}_R(M)$ als Matrix	17
2.28. Definition: Entgegengesetzter Ring $R^{\text{op}} \simeq \text{End}_R(R, +)$	17
2.29. Satz (Wedderburn, 1. Struktursatz)	17
2.30. Bemerkung: Einfache, nicht-isomorphe R -Moduln	18
2.31. Satz (2. Struktursatz von Wedderburn)	18
2.32. Definition: linear unabhängig und Basen	19
2.33. Definition: Freier Modul	19
2.34. Definition: Freier R -Modul mit Basis der Mächtigkeit $ I $	19
2.35. Satz: Universelle Eigenschaft der freien R -Moduln	19
2.36. Korollar: Über das Spalten einer kurzen Sequenz von R -Moduln	20
2.37. Satz: Jeder R -Modul ist Quotient eines freien R -Moduls	20
2.38. Satz: Äquivalenzen zu: M ist R -Modul über einem Schiefkörper R	20
2.39. Definition: Invariante Basislänge (IBL)	21
2.40. Lemma: Charakterisierung von IBL mit Matrizen	21
2.41. Satz: Kommutative, noethersche Ringe und Urbilder von Ringhomomorphismen haben IBL	22
2.42. Satz: Für R HIR sind Untermoduln freier R -Moduln frei	22
2.43. Satz: (Smith-Normalform) Invariante Faktoren einer Matrix über einem Hauptidealring	23
2.44. Definition: i -Minoren und Rang	24
2.45. Satz (Elementarteilersatz)	24
2.46. Beispiel: Elementarteilersatz	24
2.47. Definition: Annulatorideal und Torsionselement	25
2.48. Satz: Struktursatz für endlich erzeugte Moduln über HIR	25
2.49. Korollar: Struktursatz für endlich erzeugte abelsche Gruppen	25
2.50. Definition und Satz: Torsionsmodul	25
2.51. Satz: Zerlegung eines endlich erzeugten Moduls in Torsionsmodul und freien Modul	26
2.52. Beispiele für Zerlegungen mit dem Torsionsmodul	26
2.53. Satz: Umformulierung des Struktursatzes für endl. erzeugte abelsche Gruppen	26
3. Tensorprodukte und Algebren	27
3.1. Satz: Universelle Eigenschaft des Tensorproduktes	27
3.2. Bemerkung: Elemente des Tensorprodukts, Modulstruktur des Tensorprodukts	28
3.3. Proposition: Das Tensorprodukt als Operation auf ${}_R \text{Mod}$	28
3.4. Beispiele zu Tensorprodukten	29
3.5. Satz: Tensorprodukt eines R -Moduls und R^n	29
3.6. Korollar: Tensorprodukt von freien Moduln	29
3.7. Korollar: Darstellung der Elemente eines Tensorprodukts mit freiem Modul	29
3.8. Definition: Algebra	30
3.9. Beispiele für Algebren, Zentrum einer Algebra	30
3.10. Weitere Beispiele für Algebren	30
3.11. Definition: Darstellung einer R -Algebra	31
3.12. Korollar: Jede n -dimensionale K -Algebra ist isomorph zu Unteralgebra von $M_n(K)$	31
3.13. Satz: Tensorprodukt von Algebren ist eine Algebra	32

3.14. Beispiel: Erweiterung der Skalare	32
3.15. Definition: Zentrale Algebra	32
3.16. Definition: Linear disjunkt	32
3.17. Proposition: Isomorphie einer K -Algebra zum Tensorprodukt von Unteralgebren	32
3.18. Definition: Einhüllende Algebra	33
3.19. Satz (Dichtheitssatz für halbeinfache Moduln)	33
3.20. Lemma	33
3.21. Satz: Modulisomorphie der einhüllenden Algebra zum Matrizenmodul	34
3.22. Satz	34
3.23. Korollar	34
3.24. Korollar	35
3.25. Korollar	35
3.26. Definition: Zerfällungskörper über zerfallende zentral einfache K -Algebra	35
3.27. Bemerkung	35
3.28. Proposition	35
3.29. Korollar	36
3.30. Satz	36
3.31. Korollar	36
3.32. Korollar	37
3.33. Satz (Skolem-Noether)	37
3.34. Korollar	37
3.35. Korollar	37
3.36. Satz (Brauer)	37
3.37. Korollar	38
3.38. Korollar	38
3.39. Lemma	39
3.40. Satz (Wedderburn): Endliche Schiefkörper sind kommutativ	39
3.41. Definition und Satz: Die Brauergruppe	39
4. Darstellungstheorie endlicher Gruppen	41
4.1. Definition: Darstellung einer Gruppe	41
4.2. Beispiel	41
4.3. Definition: Äquivalenz von Darstellungen	42
4.4. Definition: Spurabbildung	42
4.5. Bemerkung	42
4.6. Satz (Maschke)	42
4.7. Satz (Clifford)	43
4.8. Korollar	43
4.9. Definition: Doppelzentralisatoreigenschaft	43
4.10. Satz	44
4.11. Satz	44
4.12. Satz	44
A. Anhang	45
A.1. Alternative Definition von Gruppenwirkungen	45
Index	A
Abbildungsverzeichnis	B
Todo list	B

1. Gruppentheorie: Wiederholung, Sylow-Sätze, Kompositionsreihen

1.1. Definition: Gruppenwirkung

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

Für eine alternative Definition siehe Anhang A.1 auf Seite 45.

1.2. Bemerkung

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

Beweis

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

Wiederholung Isomorphiesätze²

1. Isomorphiesatz: Ist $\varphi : G \rightarrow H$ surjektiv, dann ist $H \simeq G/\ker \varphi$. Allgemein ist für jeden Homomorphismus $\varphi : G \rightarrow H$ dann $\text{Im } \varphi \simeq G/\ker \varphi$. (Homomorphiesatz)

2. Isomorphiesatz: Ist $H \leq G$, $N \trianglelefteq G$, dann ist $H/(H \cap N) \simeq HN/N$. ("Erweitern mit N ")

3. Isomorphiesatz: Sind $N, K \trianglelefteq G$, $N \leq K$, dann ist $G/N/K/N \simeq G/K$. ("Kürzen mit N ")

Die letzten beiden Sätze lassen sich mit dem ersten beweisen!


1.3. Beispiel

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

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

$$\text{Gruppenhomomorphismus}^3: \rho_{gh}(x) = x \cdot g \cdot h = \rho_h \circ \rho_g(x).$$

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

²siehe auch <http://de.wikipedia.org/wiki/Isomorphiesatz> 

³Beachte: Die Addition in $\text{Sym}(X)$ ist die *linksseitige* Komposition von Abbildungen! Wir wollen also, dass $g \cdot h$ folgendermaßen wirkt: Zuerst g wirken lassen und dann h .

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

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

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

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

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

1.4. Bahnengleichung

Es gilt: $X = \bigcup \{G(x) \mid x \in X\}$, 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 $K_G^* = \{G(x) \mid x \in G \setminus Z(G)\} = \{G(x) \mid |G(x)| \geq 2\}$. Für jede endliche Gruppe G gilt dann nach 1.4

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

1.6. Korollar

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

Beweis

Nach Lagrange⁴ gilt für jedes $x \in G$, dass $|Z_G(x)| = p^k$ für ein $k \leq m$, 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 $|Z(G)| \geq 1$ folgt $p \mid |Z(G)|$. \square

1.7. Definition

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

1.8. Satz (Sylow)

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

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

⁴Ordnung einer Untergruppe teilt die Gruppenordnung. Die Umkehrung gilt nicht!

Beweis

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

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

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

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

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

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

Sei nun $T \subseteq S$ die Menge aller Konjugierten von P unter der Konjugationswirkung. Dann operiert auch P durch Konjugation auf T . Nach der Bahnengleichung (1.4) hat jede Bahn die Länge p^i für ein $i \leq a$. Offensichtlich ist P ein Fixpunkt dieser Wirkung. Ist $P_1 \in T$ ein weiterer Fixpunkt, dann ist $P \subseteq N_G(P_1)$, daher ist $P \cdot P_1 \leq G$. Wegen⁵ $|P \cdot P_1| = \frac{|P| \cdot |P_1|}{|P \cap P_1|}$ ist $P \cdot P_1$ eine p -Untergruppe von G . Wegen $P \leq P \cdot P_1$ und $p \nmid m$ folgt $P = P \cdot P_1 = P_1$. Daher ist $|T| = 1 \pmod p$.

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

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

Weil G durch Konjugation transitiv auf T operiert, folgt

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

Bemerkung

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

1.9. Satz (Frattini-Argument)

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

Beweis

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

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

Bemerkung

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

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

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

⁵ $P \cdot P_1$ ist Untergruppe, da $P \trianglelefteq P_1$ normalisiert

1.10. Bemerkung

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

(i) $P \cap N$ ist p -Sylowgruppe von N

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

Beweis

Es ist $[N : P \cap N] \stackrel{2. \text{ Iso}}{=} [PN : P]$ teilerfremd zu p , und $P \cap N$ ist p -Untergruppe von N . Es ist $(G/N)/(P \cdot N / N) \stackrel{3. \text{ Iso}}{\simeq} G/PN$, 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 $(H_i)_{0 \leq i \leq n}$ mit $H_0 = G$, $H_n = \{1_G\}$, $H_{i+1} \trianglelefteq H_i$ heißt **Normalreihe** in G . Ist H_i/H_{i+1} einfach⁶ für alle $i < n$, dann heißt die Folge **Kompositionsreihe**. Zwei Normalreihen $(H_i)_{i \leq n}$, $(K_j)_{j \leq m}$ heißen **äquivalent**, falls $n = m$ und die auftretenden Quotienten $(H_i/H_{i+1})_{i \leq n-1}$ nach geeigneter Permutation isomorph sind zu den Quotienten $(K_j/K_{j+1})_{j \leq n-1}$.

1.12. Beispiel

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

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 $(H_i)_{i \leq n}$ und $(K_j)_{j \leq m}$. Dann sind die Reihen äquivalent.

Für den Beweis brauchen wir

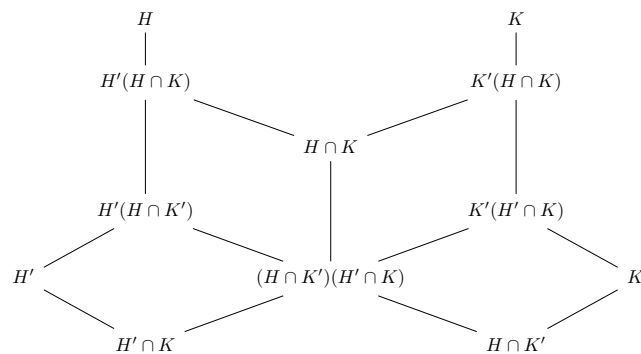
1.14. Schmetterlings-Lemma (Zassenhaus)

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

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

⁶ Eine Gruppe G heißt einfach, wenn sie G und $\{1_G\}$ als einzige Normalteiler hat.

und die Quotienten sind isomorph.



Beweis

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

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

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

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

Daher ist

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

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

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

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

Damit zeigen wir
nun folgenden Satz:

1.15. Satz von Schreier

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

Beweis

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

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

und für $i = 0, \dots, n$ sei

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

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

Nach dem Zassenhaus-Lemma (1.14) sind dann

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

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

reviewed 22.4.14

1.16. Definition

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

1.17. Bemerkung

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

1.18. Satz

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

Beweis

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

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

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

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

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

1.19. Korollar

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

Beweis

" \Rightarrow ": 1.18

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

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

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

1.20. Korollar

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

Beweis

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

Einschub: Direktes Produkt

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

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

1.21. Satz

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

Beweis

Wie Satz 1.18:

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

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

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

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

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

1.22. Satz

Endliche p -Gruppen sind nilpotent.

Beweis

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

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

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

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

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

1.23. Definition

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

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

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

1.24. Satz

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

Beweis

(i) Es ist $g^{-1}[a, b]g = [a^g, b^g]$ nach 1.23 (ii).

(ii) Klar nach 1.23 (i).

(iii) Es ist $\varphi([a, b]) = [\varphi(a), \varphi(b)] = 1$, d.h. $G' \leq \ker \varphi$. □

Bemerkung

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

1.25. Definition

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

1.26. Satz

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

Beweis

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

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

Bemerkung

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

1.27. Definition

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

1.28. Satz

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

Beweis

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

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

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

1.29. Einschub über direkte und semidirekte Produkte

- a) Sei G eine Gruppe, $H \leq G$, $N \trianglelefteq G$ ein Normalteiler mit $H \cap N = \{1\}$ und $N \cdot H = G$. Dann ist die Abbildung $\varphi : N \times H \rightarrow G$, $(n, h) \mapsto n \cdot h$ bijektiv, d.h. für jedes $g \in G$ existiert ein eindeutig bestimmtes $n \in N, h \in H$ mit $n \cdot h = g$. 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 $\varphi(n_1, h_1) \cdot \varphi(n_2, h_2) = \varphi(n_1 \cdot n_2, h_1 \cdot h_2)$

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

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

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

2. Moduln: Halbeinfache Moduln, freie Moduln

Erinnerung

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

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

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

2.1. Satz

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

Beweis

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

2.2. Definition

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

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

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

2.3. Beispiele

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

2.4. Definition

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

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

Bemerkung

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

2.5. Definition

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

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

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

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

2.6. Bemerkung

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

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

2.7. Definition

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

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

2.8. Bemerkung

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

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

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

2.9. Satz (Isomorphiesätze)

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

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

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

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

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

Vgl. Kapitel 1 Seite 1

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

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

Beweis für (i)

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

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

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

2.10. Definition (Sprechweise)

Eine Folge von R -Moduln $(M_i)_i$ und Homomorphismen $f_i : M_{i-1} \rightarrow M_i$ heißt **exakt in M_i** , falls $\text{Im } f_i = \ker f_{i+1}$. Eine **exakte Sequenz** ist eine Folge, die überall exakt ist. Eine exakte Sequenz von der Form

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

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

2.11. Definition

Ein (Links) R -Modul M heißt (links-) **noethersch**⁷, wenn es keine unendliche echt aufsteigende Kette von Untermoduln gibt. M heißt (links-) **artinsch**⁸, 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.

⁷nach Emmy Noether, 1882-1935, siehe http://de.wikipedia.org/wiki/Emmy_Noether

⁸nach Emil Artin, 1898-1962, siehe http://de.wikipedia.org/wiki/Emil_Artin

2.12. Proposition

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

Beweis

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

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

Bemerkung

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

Beweis

" \Rightarrow ": klar nach voriger Bemerkung.

(f injektiv, $M'' \simeq M/M'$)

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

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

in M' und

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

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

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

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

Isomorphiesätze

2.14. Korollar

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

Beweis

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

2.15. Korollar

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

Beweis

Durch Induktion über die Anzahl der Erzeuger. Ist M zyklisch, dann ist $M \simeq R/J$ (siehe 2.6) und R/J noethersch (bzw. artinsch) nach Satz 2.13. Sei nun

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

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

2.16. Korollar

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

2.17. Definition

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

2.18. Beispiele

- (i) \mathbb{Z} (als \mathbb{Z} -Modul) ist *nicht* halbeinfach. $m\mathbb{Z} \subseteq \mathbb{Z}, m \neq 0$ hat kein Komplement, denn für $k \cdot \mathbb{Z}$ 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

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

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

Beweis (mit Lemma 2.20)

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

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

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

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

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

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

Behauptung:

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

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

"(ii) \Rightarrow (iii)": folgt aus dem Beweis "(ii) \Rightarrow (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 $P \leq N$ mit $m \notin P$ (denn 0 ist ein solcher Untermodul). Sei Q ein Komplement von P in N , also $P \oplus Q = N, Q \neq 0$, da $m \notin P$.

Behauptung: Q ist einfach. Beweis: $Q \subseteq N \subseteq M$. Ist $0 \neq Q' \subseteq Q$ ein Untermodul, dann ist $Q' \oplus P \supsetneq P$, 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) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)" Klar.

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

"(iii) \Rightarrow (i)": Sei $M \in {}_R \text{Mod}$, dann ist $M = \sum_{m \in M} Rm$ 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) \Rightarrow (i)"). Daher ist

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

2.23. Korollar (Krull-Remak-Schmidt)

Ist

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

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

Beweis

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

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

Nach Induktionsvoraussetzung folgt die Behauptung. \square

2.24. Bemerkung

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

Beweis

" \Leftarrow ": klar, weil S_i zyklisch.

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

Das heißt wenn R halbeinfach als R -Modul 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 $\bar{I} := \{x_{11} \mid (x_{ij}) \in I\}$ die Menge aller $(1, 1)$ -Koeffizienten in $X \in I$. Man rechnet leicht nach, dass $\bar{I} \trianglelefteq R$ ein beidseitiges Ideal ist:

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

Sei $E(s, t) \in M_k(R)$ mit

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

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

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

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

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

\Rightarrow Matrizenringe über Körpern und Schiefkörpern sind einfache Ringe.

2.26. Satz (Schurs Lemma)

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

Beweis

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

2.27. Lemma

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

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

Insbesondere ist

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

Beweis

Seien $e_j : M_j \rightarrow M$ die Einbettungen, $\pi_i : M \rightarrow M_i$ die Projektionen. Dann ist für jeden Endomorphismus $\varphi \in \text{End}_R(M)$

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

wobei $\varphi_{i,j} := \pi_i \circ \varphi \circ e_j \in \text{Hom}(M_j, M_i)$. 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. \square

2.28. Definition + Lemma

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

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

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

Beweis

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

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

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

RevChap2

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 $k \geq 1$. Darüber hinaus sind k und D eindeutig bestimmt und der einfache R -Modul ist isomorph zu D^k .

Beweis

"(i) \Rightarrow (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 $Rc \rightarrow Rcr, s \cdot c \mapsto s \cdot c \cdot r$ ein Epimorphismus, also $Rcr = Rc$ wegen der Minimalität von Rc . Daher ist $(R, +)$ Summe von einfachen Untermoduln, also halbeinfach nach Satz 2.19.

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

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

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

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

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

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

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

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

Bemerkung

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

2.30. Bemerkung

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

2.31. Satz (2. Struktursatz von Wedderburn)

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

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

als Ringisomorphismus.

Beweisnach Bemerkung
2.30

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

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

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

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

Freie Moduln**2.32. Definition**

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

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

2.33. Definition

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

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

Beispiel

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

2.34. Definition

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

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

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

Achtung: Umkehrung gilt nicht! (siehe 2.33)

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

2.35. Satz

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

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

Beweis

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

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

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

Bemerkung

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

2.36. Korollar

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

Bemerkung

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

Beweis

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

2.37. Satz

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

Beweis

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

2.38. Satz

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

- (i) Jeder (Links-) R -Modul ist frei.
 - (ii) Jeder zyklischer (Links-) R -Modul ist frei.
 - (iii) R ist einfach als Links- R -Modul.
 - (iv) Jedes $x \in R \setminus \{0\}$ hat ein Linksinverses.
 - (v) R ist ein Schiefkörper.
- (i) - (v) sind auch äquivalent zu (i)_R - (iv)_R für Rechts- R -Moduln.

Beweis

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

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

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

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

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

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

$$bc = 1 = ab.$$

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

"(v)⇒(i)": Lineare Algebra I.

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

Achtung

Auch freie Moduln haben nicht notwendig eine Dimension!

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

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

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

2.39. Definition

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

Bemerkung

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

Beispiel

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

2.40. Lemma

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

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

dann ist $n = m$.

Beweis

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

Folgerung

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

2.41. Satz

Sei $R \neq 0$ ein Ring.

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

Beweis

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

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

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

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

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

weitere Zeichnung

- (ii) Ist $R^m \simeq R^{m+k}$ mit $k \geq 1$, dann ist $R^m \simeq R^{m+k} \simeq R^{m+2k}$ und man erhält eine unendliche, echt aufsteigende (absteigende) Kette in R^m . Mit R ist auch R^m noethersch (bzw. artinsch). \swarrow
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)⁹, falls R kommutativ und nullteilerfrei ist und jedes Ideal ein Hauptideal ist, das heißt von einem Element erzeugt. 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 $n \leq m$, d.h. Untermoduln freier Moduln sind frei.

Beweis

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

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

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

⁹englisch: PID, prime ideal domain

Hier fehlt noch eine Zeichnung mit Blockmatrizen!

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

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

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

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

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

2.43. Satz

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

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

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

Beweis

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

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

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

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

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

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

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

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

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

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

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

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

matrix hier

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

matrix hier

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

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

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

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

2.44. Definition

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

2.45. Satz (Elementarteilersatz)

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

Beweis

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

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

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

2.46. Beispiel

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

2.47. Definition

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

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

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

2.48. Satz: Struktursatz für endlich erzeugte Moduln über HIR

Sei D ein Hauptidealring, M ein endlich erzeugter D -Modul. Dann ist M die Summe von zyklischen Moduln $M = Dm_1 \oplus \dots \oplus Dm_k$ mit

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

Beweis

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

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

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

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

$f_i = d_i e_i$ und

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

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

2.49. Korollar: Struktursatz für endlich erzeugte abelsche Gruppen

Ist A 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, vgl. Bemerkung 2.3 (iv). □

2.50. Definition und Satz

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

Beweis

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

2.51. Satz

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

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

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

Beweis

Nach Satz 2.48 ist

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

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

Nummerierung
überprüfen

2.52. Beispiel

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

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

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

2.53. Satz

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

3. Tensorprodukte und Algebren

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

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

3.1. Satz

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

Beweis

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

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

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

Für die Existenz 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

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

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

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

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

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

da f bilinear ist. Ebenso ist

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

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

3.2. Bemerkung

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

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

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

Achtung

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

3.3. Proposition

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

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

Beweis

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

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

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

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

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

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

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

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

3.4. Beispiel

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

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

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

Beweis

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

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

3.6. Korollar

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

Bemerkung

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

3.7. Korollar

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

Vorsicht

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

Siehe Beispiel 3.4

(iii)

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

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

★

Achtung: Dieser Homomorphismus muss nicht injektiv sein!

Beispiel

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

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

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

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

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

3.8. Definition

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

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

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

3.9. Beispiel

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

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

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

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

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

Bemerkung

Für $y = 1$ in Definition 3.8 ergibt sich $x \cdot \alpha 1 = \alpha x$ und für $x = 1$ 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 $R \rightarrow A, \alpha \mapsto \alpha \cdot 1$ ist ein Algebrehomomorphismus in das Zentrum von A , d.h. $R \cdot 1 \subseteq C(A)$.

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

3.10. Beispiel

Sei R ein kommutativer Ring.

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

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

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

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

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

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

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

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

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

3.11. Definition

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

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

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

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

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

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

3.12. Korollar

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

Beweis

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

3.13. Satz

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

Beweis

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

3.14. Beispiel

- (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 $\{e_{ij} \mid i, j \leq n\}$ 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 $U \otimes V \rightarrow C$, $u \otimes v \mapsto uv$ 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 $A \times B \rightarrow C, (x, y) \mapsto xy$ ist bilinear und induziert daher eine Abbildung $A \otimes B \rightarrow C$. Diese Abbildung ist injektiv nach (i), surjektiv nach (ii) und ein Homomorphismus nach (iii). \square

3.18. Definition

Für eine K -Algebra A heißt $A^e = A \otimes_K A^{\text{op}}$ die **einshüllende Algebra** von A . Sei $A \subseteq B$ eine Unter- algebra. 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 $a_i \in A, b_i \in A^{\text{op}}, y \in B$. 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 $\text{End}_R(R, +) \simeq R^{\text{op}}$, d.h. R -lineare Endomorphismen von $R \in {}_R \text{Mod}$ sind genau die Rechtsmultiplikationen ρ_r für $r \in R$. Daher ist $\text{End}_{A^e}(A)$ die Menge der Abbildungen, die sowohl Rechts- als 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 $\text{End}_{A^e}(A) \simeq C(A)$.

3.19. Satz (Dichtheitssatz für halbeinfache Moduln)

vertauschen

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

Beweis

Zuerst überlegen wir, dass jeder R -Untermodul $N \subseteq M$ auch ein R'' -Untermodul ist. Schreibe $M = N \oplus P$ und $\pi : M = P \oplus N \rightarrow N$. 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 -Untermodul 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 $n \geq 1$ benutzen wir folgenden Trick:

3.20. Lemma

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

Beweis

Nach Lemma 2.27 ist $\text{End}_R(M^n) \simeq M_n(R')$. Offensichtlich ist M^n auch $\text{End}_R(M^n)$ -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. \square

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 $\varphi_{\alpha''} \in \text{End}_{\text{End}_R(M^n)}(M^n)$. Nun wenden wir den Fall $n = 1$ auf den R -Modul M^n und $\varphi_{\alpha''}$. Damit finden wir für $(x_1, \dots, x_n) \in M^n$ ein $\alpha \in R$ mit

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

3.21. Satz

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

Beweis

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

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

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

3.22. Satz

Sei B eine K -Algebra. A eine endlich dimensionale zentral einfache Unter algebra. 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 $a c_i = c_i a$ für alle $a \in A$ und $a c_i = 0 \Rightarrow a = 0$. 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. $C \cap A I = \{d_1 x_1 = d_1 \in I\} = I$. Daher ist $I \mapsto A \otimes I$ injektiv. Ist I' ein Ideal in B , dann ist I' ein A^e -Unterm modul von B , d.h. für $I = I' \cap C$ ist dann $I' = \sum A d_j$ mit $d_j \in I$. Daher ist $I' = A \cdot I$, 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 $c \in C(B)$. \square

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 oben. Daher folgt die Behauptung aus 3.22. \square

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 $A_1 \otimes \dots \otimes A_n$ 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} :

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

Daher ist $E \otimes A^{\text{op}} \simeq M_s(E)$ 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 $f(a) = a^n c_1 + a^{n-1} c_2 + \dots + c_n = 0$ 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 Voraussetzung 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 $A = \text{End}(V)$, wobei V ein r -dimensionaler D^{op} -Vektorraum ist. Dann ist V auch $D^{\text{op}} \otimes_K E$ -Modul, da

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

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

treu, da Kern sonst Unteralgebra

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

zusätzlich auch mit E vertauschen

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

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

Daher ist $E = C_{M_r(D)}(E)$. \square

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. \nmid Maximalität von E . Also gilt $C_D(E) = E$ und die Behauptung folgt aus 3.30. \square

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 $\dim_K A = \dim_E(M_n(E)) = n^2$. \square

3.33. Satz (Skolem-Noether)

Ist B eine endlich dimensionale, zentral einfache K -Algebra, $A \subseteq B$ einfache Unteralgebra, dann lässt sich jeder Monomorphismus $f : A \rightarrow B$ zu einem inneren Automorphismus¹⁰ fortsetzen, d.h. es existiert ein $b \in B$ mit $f(a) = b^{-1} \cdot a \cdot b$.

Beweis

$E = A \otimes_K B^{\text{op}}$ 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:

$$\left(\sum a_i \otimes b_i\right)x = \sum a_i \cdot x \cdot b_i \quad \left(\sum a_i \otimes b_i\right)x = \sum f(a_i) \cdot x \cdot b_i$$

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 $\varphi : B \rightarrow B$ mit

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

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 $Adx = d f(a)x$ 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. \square

3.34. Korollar

Jeder Automorphismus einer endlich dimensional, zentral einfachen Algebra ist ein innerer.

Beweis

Setze $A = C(B) = K$ in Satz 3.33. \square

3.35. Korollar

In einer endlich dimensional, 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

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

¹⁰Automorphismus durch Konjugation

Beweis

Sei $r = \dim_K B$ und betrachte B als $M_r(K)$ -Modul. Dann enthält $M_r(K)$ die Unter algebra $\rho_B = B^{\text{op}}$ 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 Unter algebren

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

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

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

Rechtswirkung und
Linkswirkung
zentralisieren sich

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 $A \otimes B^{\text{op}}$ 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 $C_A(E) = B \otimes B'$. \square

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 $A \otimes B^{\text{op}} \simeq M_{n/r}(E)$.

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 $[C_A(E) : E] = [B : K]$. \square

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) \Leftrightarrow (ii): Klar.

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

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

Also ist $[A : E]^2 \geq [A : K] \geq [E : K]^2$ 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, $r \geq 2$. Zum Satz von Wedderburn über Nicht-Existenz von endlichen Schiefkörpern:

3.39. Lemma

Sei G eine endliche Gruppe, $H \leq G$. Dann ist G nicht die Vereinigung der Konjugierten von H .

Beweis

Sei $|G| = |H| \cdot n$, also wenn $h = |H|$, dann ist $G/H = \{a_1H, \dots, a_nH\}$. Dann ist für $b \in G$

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

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

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

□

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** $\text{Br}(K)$ von K . Dabei ist $[K]$ das Neutralelement (denn $K \sim M_n(K)$) und $A \otimes K \simeq A$ und für $[A] \in \text{Br}(K)$ ist $A \otimes A^{\text{op}} \simeq M_n(K)$, d.h. $[A^{\text{op}}] = [A]^{-1}$.

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 $\text{Br}(K) = 1$.

Nummerierung
prüfen

(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.

4. Darstellungstheorie endlicher Gruppen

4.1. Definition

Eine **Darstellung** einer Gruppe ist (gegeben durch) einen Homomorphismus $\rho : G \rightarrow GL(V)$ 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 $\rho : G \rightarrow GL(V)$ eine Matrix-Darstellung von G , indem $\rho(g) \in GL(V)$ durch die zugehörigen Matrix bezüglich B beschrieben wird.

Ist $h : G \rightarrow \text{Sym}(n)$ 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

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

4.2. Beispiel

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

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

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

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

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

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

wobei $\alpha_g, \beta_h \in K$. Umgekehrt induziert jede Darstellung der Gruppenalgebra $K[G] \rightarrow \text{End}(V)$ eine Darstellung der Gruppe $G \rightarrow GL(V)$. Durch eine Darstellung $\rho : K[G] \rightarrow \text{End}_K(V)$ wird V zu einem $K[G]$ -Modul durch

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

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 $\rho : G \rightarrow GL(V)$ eine Darstellung, dann ist $U \leq V$ 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 $K[G]$ -Untermodule, dann erhalten wir induzierte Darstellungen, nämlich $\rho|_U : G \rightarrow GL(U)$ und die Quotientendarstellung

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

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

¹¹ $p \in \text{End}_K(V)$ zentral G , d.h. $\forall v \in V, g \in G : \varphi(gv) = g(\varphi(v)) \iff \varphi \in \text{End}_{K[G]}(V)$

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 $\rho_i : G \rightarrow \text{GL}(V_i)$, $i = 1, 2$ heißen **äquivalent**, falls ein Vektorraumisomorphismus $\varphi : V_1 \rightarrow V_2$ 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

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

Ist $f : V \rightarrow W$ ein K -Homomorphismus von $K[G]$ -Moduln, dann setze $\text{Tr}_G(f) : x \mapsto \sum_{g \in G} gfg^{-1}x$. Dann ist $\text{Tr}_G(f) : V \rightarrow W$ ein Homomorphismus von $K[G]$ -Moduln¹².

4.5. Bemerkung

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

4.6. Satz (Maschke)

Sei G eine endliche Gruppe, K ein Körper. Dann ist $K[G]$ genau dann halbeinfach, wenn wenn

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

Beweis

" \Leftarrow ": Sei $n = |G|$, $\text{char}(K) \nmid |G|$. 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 $\pi_U : V \rightarrow U$ auf U . Definiere $\varphi : V \rightarrow U$ durch

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

Wegen $\pi|_U = \text{id}_U$, gilt $\varphi|_U = \frac{1}{n} \text{Tr}(\text{id}_U) = \text{id}_U$ 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 $\text{char } K \mid |G|$, $|G| = n$. Betrachte die reguläre Darstellung von G auf $K[G] = V$. Dann ist $v = \sum_{g \in G} g \in V^G$ und $V^G \leq V$ ist ein G -invarianter Untervektorraum von V , also $K[G]$ -Untermodul von V , $0 \subsetneq V^G \subsetneq V$. Ist nun $\pi : V \rightarrow V^G$ ein beliebiger $K[G]$ -Homomorphismus, betrachte $v = \sum_{g \in G} g \in V^G$

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

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. \square

¹² $\varphi : V \rightarrow W$ ist $K[G]$ -Homomorphismus: $\varphi(g \cdot v) = g \cdot \varphi(v)$

Ist nun G eine Gruppe, $\rho : G \rightarrow \text{GL}(V)$ 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

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

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

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

Dabei heißen die m_i die Vielfachheiten der irreduziblen Komponenten ρ_i .

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

heißt homogene Komponente von V . Ist G eine Gruppe, $H \trianglelefteq G$ ein Normalteiler, $\sigma : H \rightarrow \text{GL}(V)$ eine Darstellung, dann ist für $g \in G$ die Abbildung $\sigma^g : H \rightarrow \text{GL}(V)$, $h \mapsto [v \mapsto \sigma(ghg^{-1})v]$ 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, $\rho : G \rightarrow \text{GL}(V)$ eine irreduzible Darstellung von G auf V . Dann ist $\rho_H : H \rightarrow \text{GL}(V)$ halbeinfach und alle homogenen irreduziblen Komponenten von V als $K[H]$ -Modul sind konjugiert und haben die gleiche Multiplizität.

Beweis

Sei U ein irreduzibler $K[H]$ -Untermodule 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 $K[H]$ -Untermodule. Behauptung: Für alle $g \in G$ ist $\rho(g)U$ irreduzibler $K[H]$ -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 -Untermodule wieder auf solche ab. Daher permutiert G die H -homogenen Komponenten transitiv und alle homogenen Komponenten haben dieselbe Multiplizität. \square

4.8. Korollar

Ist G eine endliche Gruppe, $H \trianglelefteq G$, $\rho : G \rightarrow \text{GL}(V)$ halbeinfach, dann ist auch $\rho|_H$ halbeinfach.

Beweis

Wende 4.7 auf die irreduziblen Komponenten an. \square

4.9. Definition

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

4.10. Satz

Ist $\rho : G \rightarrow \text{GL}(V)$ 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, $\text{char } K \nmid |G|$, $A = K[G]$. 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 , $i = 1, \dots, s$, $d_i = \dim_K(D_i)$.

4.11. Satz

Seien G, K, A_i wie oben, 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 $n_i \cdot d_i$.

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 $\rho : G \rightarrow \text{GL}(V)$ (für $\text{char } K \nmid |G|$) 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

$$p \sim m_1 \rho_1 \oplus \dots \oplus m_s \rho_s$$

4.12. Satz

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

A. Anhang

A.1. Alternative Definition von Gruppenwirkungen

Eine **Gruppenwirkung** von G auf X ist (gegeben durch) eine Abbildung $G \times X \rightarrow X$, $(g, x) \mapsto g \cdot x$, 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 $X \times G \rightarrow X$, $(x, g) \mapsto x \cdot g$, 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 $\varphi : G \rightarrow \text{Sym}(X)^{\text{op}}$ beschrieben werden, wobei $\text{Sym}(X)^{\text{op}} := (\text{Sym}(X), *)$ mit $f * g := g \circ f$ ist. (vgl. Definition 2.28).

Index

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

R -Modul-Homomorphismus, 11

Algebra

zentral, 32

Annulatorideal, 25

artinsch, 12

auflösbar, 6

auflösbare Länge, 8

Bahn, 1

Basis (Modul), 19

Brauergruppe, 39

Darstellung, 31, 41

einhängende Algebra, 33

endlich erzeugt, 11

Endomorphismenring, 10

entgegengesetzte Ring, 17

erzeugte Untermodul, 11

exakte Folge, 12

exakte Sequenz, 12

frei, 19

Grad, 37, 41

Gruppenalgebra, 31

Gruppenwirkung, 1, 43

linksseitige, 43

rechtsseitige, 43

reguläre, 1

transitive, 1

treue, 1

Hauptidealring, 22

Ideal, 10

invariante Basislänge, 21

invarianten Faktoren, 24

Kern der Wirkung, 1

Kommutator, 7

Kommutatorgruppe, 7

Kompositionsreihe, 4

kurze exakte Sequenz, 12

linear disjunkt, 32

linear unabhängig in Moduln, 19

Minor, 24

Modul

einfach, 11

halbeinfach, 14

irreduzibel, 11

Modulstruktur, 10

nilpotent, 6

noethersch, 12

Normalreihe, 4

obere Zentralreihe, 7

p -Sylowgruppe, 2

Permutationsdarstellung, 41

projektiv, 20

Rang, 24

Ring

artinsch, 12

einfach, 11

noethersch, 12

semidirektes Produkt, 9

spaltet, 20

Spurabbildung, 42

Stabilisator, 1

Tensoralgebra, 31

Torsionselement, 25

Torsionsmodul, 25

unital, 30

universelle Eigenschaft, 19

Unteralgebra, 30

untere Zentralreihe, 8

Untermodul, 11

Verbandsisomorphismus, 12

Zentralisator, 2

Zentrum, 2, 30

Zerfallungskörper, 35

zyklisch, 11

ähnlich, 39

äquivalent, 4, 42

Abbildungsverzeichnis

Todo's und andere Baustellen

RevChap2	17
Hier fehlt noch eine Zeichnung mit Blockmatrizen!	22
Matrizen hinzufügen	24
Nummerierung überprüfen	26
Dieses Korollar verlangt noch nach etwas Erläuterung	37
Nummerierung prüfen	40