

Algebra I SoSe 2005 Uni HH

1 Einführung Gruppentheorie

- Definitionen: Gruppen, Untergruppen, Normalteiler
Beispiele: Quaternionengruppe \mathbb{Q} , $\mathbb{Z}/m\mathbb{Z}$
- Definitionen: Gruppenhomomorphismus, Kern $\ker(\varphi)$
Beispiel: $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$
- Definitionen: Automorphismus, innerer Automorphismus, $\text{Aut}(G)$, „konjugiert“ als Äquivalenzrelation, Zentrum $Z(G)$
- Untergruppenkriterium, erzeugte Untergruppe $\langle g \rangle$, konjugierte Untergruppen
Beispiele: $G = \mathbb{Z} : \langle 1 \rangle = \mathbb{Z}, \langle 2, 3 \rangle = \mathbb{Z}$
- zyklische Gruppen und deren Eigenschaften, Ordnung eines Elements, Eigenschaften, kleiner Fermat
zyklische Gruppen als homomorphe Bilder von \mathbb{Z}
- Definitionen: Links-/Rechtsnebenklassen, Nebenklassen, Index $|G : U|$
- **Satz von Lagrange:** $U < G \Rightarrow |G| = |U||G : U|$
Folgerungen, Beispiel \mathbb{Z}_n^*
- Homomorphiesatz, 1. Isomorphiesatz, 2. Isomorphiesatz
kanonischer Homomorphismus $\pi : G \rightarrow G/N$
Beispiel: orthogonale Gruppe, $\text{SO}(n) \trianglelefteq \text{O}(n), \text{O}(n)/\text{SO}(n) = \{\pm 1\}$
Anwendung in Vektorräumen

- Definitionen: Äußeres direktes Produkt $\prod_{i=1}^n G_j$, inneres direktes Produkt, deren Zusammenhang, Sätze
- Anwendungen in der Elementaren Zahlentheorie:
 - $\text{ggT}(m, n) = 1 \Rightarrow \mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$
 - $m = \prod p_i^{k_i}$ Primfaktorzerlegung: $\mathbb{Z}/m\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{k_i}\mathbb{Z}$
 - Chinesischer Restsatz
- Gruppenstruktur auf direktem Produkt, kanonischer Projektor
- in der Übung bearbeitet:
 - Normalteiler, $|G| = n \in \mathbb{N}_{>0} \Rightarrow |\text{Aut}(G)| \mid (n-1)!$
 - $\text{Aut}(G)$ bestimmen für $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_7$
 - $\ker(\varphi), \text{im}(\varphi)$ für nichttriviale $\varphi : \text{GL}_n(\mathbb{C}) \rightarrow \mathbb{C}^*$
 - Homomorphismus $\mathbb{Z}_{14} \rightarrow \mathbb{Z}_9$

2 Abzählende Gruppentheorie

- Operation einer Gruppe auf einer Menge
- Definitionen: Bahn/Orbit eines Elements, Fixgruppe/Stabilisator
- Bahnengleichung
- Beispiele zur Anwendung der Bahnengleichung:
 - Diedergruppe, Berechnung $|D_n| = 2n$
 - Abzählung am regelmäßigen Sechseck, Bahnen unter D_6
 - Anzahl von unnummerierten Graphen auf einer Menge $\{1, \dots, p\}$
 - Sätze für $|G| = \text{Primzahlpotenz}$
- in der Übung bearbeitet:
 - Operation der Kleinschen 4er-Gruppe, Bahnen/ Stabilisator/ Vertretersystem/ Fixpunkte bestimmen

- Automorphismengruppe reguläres Fünfeck/Tetraeder/Würfel
 - Operation $SL_2(\mathbb{R})$ auf \mathcal{H} ; Transitivität, Stabilisator von i
 - Operation $SU(1, 1)$ auf \mathcal{D} ; Transitivität, Stabilisator von 0
 - Operation $SL_2(\mathbb{Z})$ auf \mathcal{H} ; Bahn von i , Fundamentalbereich Γ
- aufsteigende Zentralreihe, Ausschöpfung, Einfachheit von Gruppen
 - absteigende Zentralreihe

3 Symmetrische / Alternierende Gruppe

- Symmetrische Gruppe S_n :
 - r -Zykel, Transpositionen
 - Beispiel: Kleinsche Vierergruppe als Permutationsgruppe betrachtet
 - injektiver Homomorphismus $\varphi : S_n \rightarrow S_{n+1}$
 - S_{n+1} als disjunkte Vereinigung von Nebenklassen $f_1\varphi(S_n), \dots, f_{n+1}\varphi(S_n)$
 - $|S_n| = n!$
 - jede Permutation ist Produkt von Transpositionen
 - Signatur von Permutationen $\text{sgn}(f)$
 - Beweis Homomorphie $\text{sgn}(f) : S_n \rightarrow \{\pm 1\}$
 - $\text{sgn}(f) = (-1)^{\text{Anzahl Transpositionen in } f}$
 - gerade/ungerade Permutationen
- die alternierende Gruppe A_n :
 - $|A_n| = \frac{n!}{2}$ ($n \geq 2$)
 - ist Normalteiler in S_n ,
 - enthält alle 3-Zykel
 - **Satz:** für $n \geq 5$ ist A_n eine einfache Gruppe

4 Normal- und Kompositionsreihen

- Definitionen absteigende Gruppenkette, normale Gruppenkette, Faktoren der Reihe, Normalreihe, abelsche/zyklische Normalreihe
- Verfeinerung einer Gruppenkette
- Äquivalenz von Normalreihen
- Definition Kompositionsreihe
- Lemma und daraus folgenden **Satz** (Otto/Schreier): Je zwei Normalreihen besitzen äquivalente Verfeinerungen
- jede Normalreihe einer endlichen Gruppe läßt sich zu einer Kompositionsreihe verfeinern
- **Korollar** (Jordan/Hölder): je zwei Kompositionsreihen sind äquivalent
- Definition Kommutator $[a, b]$, Kommutator-Untergruppe $K(G)$
 - **Satz** über Eigenschaften von $K(G)$
 - induktiv: $K^{m+1}(G) = K(K^m(G))$, „auflösbare Reihe“
 - $\varphi \in \text{Aut}(G) : \varphi([a, b]) = [\varphi(a), \varphi(b)], \varphi(K(G)) = K(\varphi(G))$
 - $K(G), K^m(G)$ sind Normalteiler
- Definition auflösbare Gruppe
- **Satz:** Charakterisierung Auflösbarkeit
- Definitionen: Sequenzen von Gruppen, exakte Sequenzen
 - kurze exakte Sequenz
 - splittende Sequenzen

5 Grundbegriffe der Ringtheorie

- Definitionen assoziativer Ring, kommutativer Ring, Ring mit Eins
- Beispiele: $\text{End}_{\mathbb{K}}(V)$, $\text{Abb}(X, R)$, R^{opp} , direktes Produkt von Ringen
- Definition Ringhomomorphismus, Bild und Kern eines Ringhom.
- Definition Unterring, Satz über Kriterium Unterring
- Definitionen Linksideal, Rechtsideal, Ideal
Beispiel: $(\mathbb{Z}, +, \cdot) : m\mathbb{Z}$ sind die Ideale in \mathbb{Z} für $m \in \mathbb{N}_0$
- Bemerkung: triviale Ideale \emptyset, R ; Körper enthalten nur triviale Ideale
- Urbilder von Idealen sind Ideale, Bilder von Idealen unter surjektiven Homomorphismen sind Ideale
- Definition Faktorring bzw. Restklassenring modulo Ideal
- kanonischer Restklassen-Epimorphismus $\pi : R \rightarrow R/I, x \mapsto x + I$
- Homomorphiesatz, 1. und 2. Isomorphiesatz
- Anwendungsbeispiel: $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}, n, m \in \mathbb{Z}, (n, m) = 1$
- der Durchschnitt einer Familie von Idealen ist wieder ein Ideal
- Definition und Charakterisierung erzeugtes Ideal
- Definition Hauptideal
- Adjunktion eines Einselementes
- Produkt und Summe von Idealen
- Definition Einheitengruppe (Menge der invertierbaren Elemente)
- Definition Schiefkörper, Nullteiler, einfacher Ring
- Beispiel $R = \text{End}_{\mathbb{K}}(V)$, Links-/Rechts-Invertierbarkeit

6 Maximale und Prim-Ideale

- Definitionen maximales Ideal, lokaler Ring, Prim-Ideal, Integritätsring, Hauptidealring
- Beispiel \mathbb{Z} als Hauptidealring, maximale und prime Ideale in \mathbb{Z}
- Beispiel $\mathbb{Z}_{(p)}$ als Hauptidealring, lokaler Ring
- Zur Mengentheorie:
 - Definitionen Halbordnung, vollständige Ordnung, obere Schranke, maximales Element, induktiv geordnete Menge
 - Beispiele: (\mathbb{R}, \leq) , (\mathbb{R}, \geq) , Potenzmenge $\mathfrak{P}(M)$ mit Mengen-Inklusion: Vereinigung als obere Schranke, Durchschnitt als untere Schranke
 - Beispiel: \mathbb{C} mit lexikographischer Ordnung, sowie Ordnung auf Geraden durch Nullpunkt
 - Lemma von Zorn: starke und schwache Version, Beweis ihrer Gleichwertigkeit
 - Erwähnung Auswahlaxiom als weitere Version
- Anwendung des Zornschen Lemmas: Ringe mit 1 besitzen maximale Ideale
- für ein Ideal I in R ist äquivalent: I ist maximal $\Leftrightarrow R/I$ ist ein Körper
- Jedes Ideal $I \subsetneq R$ liegt in einem maximalen Ideal
- Sei R kommutativ mit Eins:
 - R ist lokal $\Leftrightarrow R/R^*$ ist ein Ideal
 - $I \neq R$ sei Ideal; es ist äquivalent:
 - * I ist Primideal
 - * $R \setminus I$ ist multiplikativ abgeschlossen
 - * R/I ist ein Integritätsring

- Lokalisierung:
 - Voraussetzungen: R kommutativer Ring, $H \subset R$ multiplikativ abgeschlossene Teilmenge, ohne Nullteiler in R
 - Definition der Äquivalenzrelation \sim auf $R \times H$, Äq.klassen $r//h$
 - Definition der Addition auf $R \times H$ (Wohldefiniertheit, Nachweis, daß $(R \times H, +)$ abelsche Gruppe)
 - Definition der Multiplikation auf $R \times H$ (Wohldefiniertheit, Assoziativität, Kommutativität, Einselement)
 - Nachweis Distributivgesetz
 - $R \times H / \sim$ ist kommutativer Ring mit Eins: Schreibweise RH^{-1}
 - $\alpha : R \rightarrow RH^{-1}$, $x \mapsto xu//u$ ist unabhängig von u und injektiver Ringhomomorphismus
 - $\alpha(h)$ mit $h \in H$ ist invertierbar in RH^{-1} , Inverses: $h//h^2$
 - $\varphi : R \rightarrow S$ Ringhomomorphismus, $\varphi(h)$ mit $h \in H$ sei invertierbar in S . Dann $\exists! \psi : RH^{-1} \rightarrow S$ Ringhomomorphismus mit $\psi(\alpha(r)) = \varphi(r) \forall r \in R$.
 - Beispiele:
 - Konstruktion von $\mathbb{Q} := \mathbb{Z}(\mathbb{Z}^*)^{-1}$ als Lokalisierung von \mathbb{Z} bzgl. $\mathbb{Z} \setminus \{0\}$
 - $\mathbb{Z}_{(p)}$ als Lokalisierung an Primideal $p\mathbb{Z}$
 - $Q(R) := RH^{-1}$ als Quotientenring (H Menge aller Nichtnullteiler)
wenn R Integritätsring, dann $H = R \setminus \{0\}$, $Q(R)$ ist Quotientenkörper
Enthält K den Integritätsring R (im Sinne injektiver Einbettung), dann auch den Quotientenkörper $Q(R)$.
 - Bemerkungen:
 - Verallgemeinerung der Lokalisierung unter Zulassung von Nullteilern
 - Universelle Eigenschaft, Folgerung: (RH^{-1}, α) ist eindeutig festgelegt

7 Aufbau des Zahlensystems

(I) \mathbb{N} als bekannt vorausgesetzt (Axiome!)

Definition einer Relation auf $\mathbb{N} \times \mathbb{N}$: $(a, b) \sim (c, d) :\Leftrightarrow a + d = b + c$

$\mathbb{N} \times \mathbb{N} / \sim$ ist abelsche Gruppe

neutrales Element: $a//a$ (unabhängig von a)

inverses Element zu $a//b$ ist $b//a$

$\mathbb{N} \times \mathbb{N} / \sim$ enthält \mathbb{N} über die injektive Abbildung $a \mapsto (a + 1)//1$

(II) Definition einer Multiplikation auf $\mathbb{N} \times \mathbb{N} / \sim$

$$(a//b)(c//d) := (ac + bd)//(ad + bc)$$

prüfen: Wohldefiniertheit, Ringeigenschaften

Multiplikation aus \mathbb{N} auf eindeutige Weise fortgesetzt

Wir erhalten den Ring \mathbb{Z} .

(III) Konstruktion von \mathbb{Q} :

$$\mathbb{Q} := Q(\mathbb{Z}) = \mathbb{Z} \times \mathbb{Z}^* / \sim$$

(IV) Konstruktion von \mathbb{R} :

über Cauchy-Folgen, das Ideal der Nullfolgen ausfaktoriert

bis zur Definition der Norm, Ordnung, Vollständigkeit (Beweis übergegangen)

total geordnet, archimedisch.

(V) Übergang zu \mathbb{C} :

Nachweis: $(X^2 + 1)$ ist maximales Ideal in $\mathbb{R}[X]$, betrachten den Körper

$$\mathbb{R}[X]/(X^2 + 1) = \{\alpha + \beta\bar{x} \mid \alpha, \beta \in \mathbb{R}\}$$

8 Teilbarkeit in Integritätsringen

- Schreibweise $a \mid b \Leftrightarrow \exists c \in R : b = ac$
- elementare Teilbarkeitsregeln, \dots , $a \mid b \Leftrightarrow (a) \supset b$
- Definition assoziiert: $a \sim b \Leftrightarrow \exists u \in R^* : a = bu$
- Definitionen: $p \notin R^* \cup \{0\} : p$ heißt
 - prim: $p \mid ab \Rightarrow p \mid a \vee p \mid b$
 - unzerlegbar: $p = ab \Rightarrow a \in R^* \vee b \in R^*$
- **Satz:** wenn $p \notin R^* \cup \{0\}$, dann
 - (1) p prim $\Leftrightarrow (p)$ Primideal
 - (2) p unzerlegbar $\Leftrightarrow (p)$ maximal unter allen Hauptidealen
 - (3) p prim $\Rightarrow p$ unzerlegbar
- Def. Hauptidealring: ist Integritätsring, und jedes Ideal ist Hauptideal
- Korollar: in HIR ist p prim $\Leftrightarrow p$ unzerlegbar. Ist $a \neq 0$, dann ist (a) Primideal $\Leftrightarrow (a)$ maximales Ideal
- Definition gemeinsamer Teiler, größter gemeinsamer Teiler
- **Satz:** in HIR existiert ggT, d ist ggT(a_1, \dots, a_n) $\Leftrightarrow (d) = (a_1, \dots, a_n)$
- Korollar: in HIR $\exists r_1, \dots, r_n \in R : d = r_1 a_1 + \dots + r_n a_n$
- **Satz** über die bis auf Reihenfolge bzw. Assoziiertheit eindeutige Zerlegung in Primelemente in Hauptidealringen
- Definition faktorieller Ring
- **Satz** über Äquivalenz von faktoriell und Zerlegbarkeit in prime bzw. unzerlegbare Elemente
- **Satz:** jeder Hauptidealring ist faktoriell
- Definition euklidischer Ring
- **Satz:** jeder euklidische Ring ist Hauptidealring
- R ist euklidisch $\Rightarrow R$ ist HIR $\Rightarrow R$ ist faktoriell $\Rightarrow R$ ist IR
Umkehrung ist im Allgemeinen nicht richtig.

9 Einige Beispiele

- Quadratische Zahlkörper $\mathbb{Q}(\sqrt{n})$, $\mathbb{Z} \ni n \neq 0, 1$ quadratfrei
- Definition Normabbildung

$$\begin{aligned} N : \mathbb{Q}(\sqrt{n}) &\rightarrow \mathbb{Q} \\ x + y\sqrt{n} &\mapsto x^2 - ny^2 \end{aligned}$$

Eigenschaften

- $\mathbb{Z}[\sqrt{n}]$, Einheiten darin
- **Satz:** $\mathbb{Z}[\sqrt{n}]$ ist euklidisch für $n = -1, -2, 2, 3$
- **Korollar:** Der Ring der ganzen gaußschen Zahlen $\mathbb{Z}[i]$ ist euklidisch
- Einheiten, Primelemente in $\mathbb{Z}[i]$
- **Satz von Fermat** über die Zerlegung einer Primzahl in zwei quadratische Summanden
- $\mathbb{Z}[\sqrt{-5}]$ als Beispiel für einen Integritätsring, der nicht faktoriell ist

10 Polynomringe

- Definition Ring der formalen Potenzreihen $R[[X]]$
(kommutativer Ring mit Eins)
Ringeigenschaften, Schreibweise als Funktionen sowie als formale Reihe
- Definition Ring der Polynome $R[X]$
- Definitionen Gradfunktion, Leitkoeffizient, Begriffe normiert und irreduzibel
- Eigenschaften der Gradfunktion
- Division mit Rest in $R[X]$

- Korollar: für kommutativen Ring R mit Eins ist äquivalent:
 R ist Körper $\Leftrightarrow R[X]$ ist euklidisch $\Leftrightarrow R[X]$ ist HIR
- Korollar: für Körper K
 - $K[X]$ ist faktoriell, jedes $f \neq 0$ läßt sich bis auf Reihenfolge eindeutig als $f = cp_1 \dots p_k$, $c \in K, p_i$ normiert und irreduzibel, schreiben
 - wenn $f \in K[X]$ irreduzibel ist, dann ist $K[X]/(f)$ ein Körper
- **Satz:** R sei \mathbb{R} , $f \in R[X]$, $\deg f = n$. Dann hat f höchstens n verschiedene Nullstellen. Für jede Nullstelle $\alpha \in R$ ist $x - \alpha$ ein Teiler von f in $R[X]$.
- Definition Inhalt $I(f) = \text{ggT}(a_0, \dots, a_n)$
- **Satz von Gauß:** R faktoriell, $f, g \in R[X] \setminus \{0\}$: $I(fg) = I(f)I(g)$
- Universelle Eigenschaft des Polynomrings

11 Das Gaußsche Lemma

- **Lemma:** R sei kommutativer Ring mit Eins und P Primideal von R
 $\Rightarrow P[X]$ ist Primideal in $R[X]$
- **Satz:** Sei R faktoriell, K der Quotientenkörper von R , $f \in R[X] \setminus \{0\}$. Sei $f = gh$ eine Zerlegung mit $g, h \in K[X]$. Dann existieren $\alpha, \beta \in K, c \in R$ mit
 - $\alpha g =: g_1, \beta h =: h_1, g_1, h_1 \in R[X]$,
 - $f = cg_1h_1, g_1, h_1$ primitiv
- Korollar: $f \in R[X]$ unzerlegbar $\Rightarrow f$ in $K[X]$ irreduzibel
- Korollar: $f \in R[X], f \notin R^* \cup \{0\}$ primitiv. f sei in $K[X]$ irreduzibel
 $\Rightarrow f$ in $R[X]$ prim, insbesondere unzerlegbar
- **Satz:** R faktoriell $\Rightarrow R[X_1, \dots, X_n]$ faktoriell
- Irreduzibilitätskriterium von Eisenstein, Beispiele $X^n - b, \sum_{i=0}^{p-1} X^i$

12 Moduln

- Definition (unitärer) R -Modul
- Beispiele: abelsche Gruppe als \mathbb{Z} -Modul, ${}_R R$, Vektorraum, ${}_K G V$
- Definitionen R -Untermodule, zyklischer Modul, Faktormodul, Modulhomomorphismus
- Analog zu Gruppen: Kern und Bild unter Modulhomomorphismen sind Untermodule, Homomorphie- und Isomorphiesätze gelten analog
- Definition Torsionselement, torsionsfreie Moduln
- **Satz:** R Integritätsring $\Rightarrow \text{Tor}({}_R M)$ ist R -Untermodule von ${}_R M$
- Definition einer Darstellung $\varphi : R \rightarrow \text{End}(M)$, M abelsch, R Ring, unitäre Darstellung
- **Satz:**

(1) M sei (unitärer) R -Modul. Dann definiert die Abbildung

$$\begin{aligned}\varphi : R &\rightarrow \text{End}(M) \\ \varphi(r)(m) &:= rm \quad \forall r \in R, m \in M\end{aligned}$$

eine (unitäre) Darstellung.

(2) M sei abelsche Gruppe, $\varphi : R \rightarrow \text{End}(M)$ eine (unitäre) Darstellung. Dann definiert

$$\begin{aligned}R \times M &\rightarrow M \\ (r, m) &\mapsto \varphi(r)(m) \quad \forall r \in R, m \in M\end{aligned}$$

eine (unitäre) Modulstruktur.

- **Satz:** $\prod_{i \in I} {}_R M_i$ ist R -Modul, $\coprod_{i \in I} {}_R M_i$ ist R -Untermodule, es gelten universelle Eigenschaften
- Definitionen freie endliche Familie (m_i) (R -linear unabhängig), beliebige freie Familie, R -Basis, freier R -Modul
- Freie Moduln über Integritätsring sind torsionsfrei
- Torsionsfreie Moduln sind nicht notwendig frei. Beispiel: \mathbb{Q} ist torsionsfreier \mathbb{Z} -Modul, doch je zwei Elemente aus \mathbb{Q} sind \mathbb{Z} -abhängig

- äquivalente Charakterisierungen für: ${}_R M$ ist frei mit Basis S
- hat ${}_R M$ endliche Basis S , dann ${}_R M \cong \coprod_{s \in S} R s$
- Beispiel für freien R -Modul mit Basen verschiedener Mächtigkeit
- **Satz:** R sei kommutativ mit Eins, ${}_R M$ ein freier unitärer R -Modul. Dann haben alle Basen gleiche Länge.
- Definition Rang von ${}_R M$ als Mächtigkeit einer R -Basis (R kommutativ mit Eins, ${}_R M$ unitär und R -frei)
- **Satz:** ${}_R N$ sei Untermodul von ${}_R M$, (R beliebig mit Eins), ${}_R M / {}_R N$ sei freier R -Modul. Dann existiert ein R -Untermodul ${}_R N'$ von ${}_R M$ mit ${}_R M = {}_R N \oplus {}_R N'$.
- **Satz:** Jeder unitäre R -Modul ist homomorphes Bild eines freien R -Moduls.

13 Tensorprodukte

- Definition Rechtsmoduln, Bimoduln, Schreibweisen für die Kategorien
- Definition balancierte Abbildung
- Definition Tensorprodukt (T, t) als Quotient F/H , Schreibweise $T = M \otimes_R N$
- Universelle Eigenschaft
- Rechenregeln:

$$\begin{aligned} (m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2 \\ mr \otimes n &= m \otimes rn \end{aligned}$$
 speziell: $m \otimes 0 = 0 \otimes 0 = 0 \otimes n \quad \forall m \in N, n \in N$
- **Satz** über die eindeutige Bestimmtheit des Tensorprodukts
- **Satz:** $M \in {}_S \text{Mod}_R, N \in {}_R \text{Mod} \Rightarrow M \otimes_R N \in {}_S \text{Mod}$ mit $s(m \otimes n) = (sm) \otimes n$

- symmetrische Aussage: $M \in \text{Mod}_R, N \in {}_R\text{Mod}_S \Rightarrow M \otimes_R N \in \text{Mod}_S$ mit $(\sum m_i \otimes n_i)s = \sum m_i \otimes \sum n_i s$

- Weitere Eigenschaften:

– Sei $M \in {}_R\text{Mod}$. Dann ist $M \in \text{Mod}_{R^{\text{opp}}}$.

Speziell: ist R kommutativ, so ist $M \otimes_R N$ ein R -Modul

– Seien $M \in \text{Mod}_R, N \in {}_R\text{Mod}$, dann sind $M \in {}_{R^{\text{opp}}}\text{Mod}, N \in \text{Mod}_{R^{\text{opp}}}$ und es gibt einen Gruppenisomorphismus

$$\begin{aligned} M \otimes_R N &\rightarrow N \otimes_{R^{\text{opp}}} M \\ \sum m_i \otimes n_i &\mapsto \sum n_i \otimes m_i \end{aligned}$$

– Seien $L \in \text{Mod}_R, M \in {}_R\text{Mod}_S, N \in {}_S\text{Mod}$. Dann ist $L \otimes_R M \in \text{Mod}_S, M \otimes_S N \in {}_R\text{Mod}$ und es gibt einen Gruppenisomorphismus

$$(L \otimes_R M) \otimes_S N \xrightarrow{\sim} L \otimes_R (M \otimes_S N)$$

– $R \otimes_R M \cong M$ mittels $r \otimes n \mapsto rn$

- **Satz:**

(1) Seien $M \in \text{Mod}_R, N_i \in {}_R\text{Mod}, i \in I$. Dann gilt

$$M \otimes_R \left(\bigoplus_{i \in I} N_i \right) \cong \bigoplus_{i \in I} M \otimes_R N_i$$

(2) Sei $N \in \text{Mod}_R$, frei mit Basis $(u_i)_{i \in I}$. Dann gilt

$$\begin{aligned} M \otimes_R N &\cong \bigoplus_{i \in I} M \otimes_R Ru_i \\ &\cong \bigoplus_{i \in I} M \end{aligned}$$

(3) Sei $M \in \text{Mod}_R, M'$ ein R -Untermodul von $M, N \in {}_R\text{Mod}$ und N sei frei. Dann ist die Abbildung

$$\begin{aligned} M' \otimes_R N &\hookrightarrow M \otimes_R N \\ m \otimes n &\mapsto m \otimes n \end{aligned}$$

injektiv.

- warnendes Beispiel:

$R = \mathbb{Z}$ und $M = \mathbb{Z}/2\mathbb{Z}, N = \mathbb{Z}/3\mathbb{Z}$ unitäre \mathbb{Z} -Moduln.

$$\begin{aligned} x \in M & : 2x = 0 \\ y \in N & : 3y = 0 \end{aligned}$$

$$\begin{aligned} x \otimes y &= 3(x \otimes y) - 2(x \otimes y) \\ &= x \otimes (3y) - (2x) \otimes y \\ &= 0 \end{aligned}$$

$$\Rightarrow M \otimes_R N = \{0\}$$

- **Satz:** Seien $M, M' \in \text{Mod}_R, N, N' \in {}_R\text{Mod}$, und $f : M \rightarrow M', g : N \rightarrow N'$ seien R -Modulhomomorphismen.

Dann gibt es genau einen Gruppenhomomorphismus

$$f \otimes g : M \otimes_R N \rightarrow M' \otimes_R N'$$

mit

$$f \otimes g \left(\sum m_i \otimes n_i \right) = \sum f(m_i) \otimes g(n_i).$$

Folgerung 1: Sind f, g R -Modulisomorphismen, dann ist $f \otimes g$ ein Gruppenisomorphismus mit Inversem $f^{-1} \otimes g^{-1}$.

Folgerung 2: ist $f : M \rightarrow M'$ ein R -Modulisomorphismus mit Inversem $f^{-1} : M' \rightarrow M$, dann ist

$$M \otimes N \cong M' \otimes N.$$

14 Moduln über Hauptidealringen

- Sei K ein Körper, $K[X]$ ist Hauptidealring.
Sei V ein Vektorraum, $A \in \text{End}_K(V)$.

Dann wird V ein $K[X]$ -Modul durch

$$f(x) \cdot v = f(A)(v) \quad \forall v \in V.$$

- **Satz:** Sei R ein Hauptidealring, F ein freier endlich erzeugter R -Modul.
Sei $M < F$ ein R -Untermodule.

Dann ist auch M frei mit $\text{Rang}(M) \leq \text{Rang}(F)$.

- **Satz:** Sei R ein Hauptidealring, M ein endlich erzeugter unitärer R -Modul.

Wenn M torsionsfrei ist, dann ist M frei von endlichem Rang.

- **Satz:** Sei R ein Hauptidealring, M ein endlich erzeugter unitärer R -Modul.

(1) $\text{Tor}(M) = \{m \in M \mid \exists r \neq 0 : rm = 0\}$ ist ein endlich erzeugter R -Modul.

(2) $M \cong F \oplus \text{Tor}(M)$, wobei F frei von endlichem Rang ist.

D.h. M wird eindeutig charakterisiert durch $\text{Rang}(F) \in \mathbb{N}$ und $\text{Tor}(M)$.

$\text{Tor}(M)$ ist der Torsionsuntermodul, endlich erzeugter Untermodul.

- **Bezeichnung:** $M_\pi = \{m \in M \mid \exists n(m) : \pi^{n(m)} = 0\}$ für $\pi \in R$

– $M_\pi = \{0\}$ ist möglich

– M_π ist ein Untermodul

Beispiel: $R = \mathbb{C}[X]$, $M = V$ (V ist \mathbb{C} -Vektorraum)

$$A \in \text{End}_{\mathbb{C}}(V) \quad f(x) \cdot m = f(A)m$$

$$\chi(x) \cdot v = 0 \quad \forall v \in V \quad (\chi \text{ ist charakteristisches Polynom})$$

V ist Torsionsmodul.

Primelemente in $\mathbb{C}[X]$: lineare Polynome,

$$\pi_i = X - \alpha_i, \quad \pi_i(v) = (A - \alpha_i \text{Id})(v)$$

$$V_{\pi_i} \neq \{0\} \Leftrightarrow \alpha_i \text{ Eigenwert von } A$$

- **Satz:** Sei R ein Hauptidealring, M ein unitärer endlich erzeugter R -Modul und M sei Torsionsmodul. (d.h. $M = \text{Tor}(M)$)

(1) Es existieren Primelemente $\pi_1, \dots, \pi_n \in R$ mit

$$M = \bigoplus_{i=1}^t M_{\pi_i}$$

Jedes M_{π_i} ist endlich erzeugt. „Primärzerlegung“

(2) Sei $\pi \in R$ ein Primelement mit $M_{\pi} \neq \{0\}$.
Dann existiert ein $i \in \{1, \dots, t\}$, so daß $\pi \sim \pi_i$.

- **Satz:** Sei R ein Hauptidealring, M ein unitärer endlich erzeugter R -Modul, $\pi \in R$ prim, $\pi^n M = 0$.

Dann existieren $s > 0$ und $n_1, \dots, n_s \leq n$, so daß

$$M \cong \bigoplus_{i=1}^s R/(\pi^{n_i}).$$

(entspricht Jordanblöcken)

- **Bemerkung:** (π) sei Primideal. Dann kann man lokalisieren mit $H := R \setminus (\pi)$, bilde Ring RH^{-1} .

Jedes Element von H operiert invertierbar auf M .

Universelle Eigenschaft der Quotientenstruktur: RH^{-1} ist lokaler Ring mit maximalem Ideal (π) .