Algebra Vorlesungsmitschrift

nach der 2023S Vorlesung von Michael Pinsker

Ian Hornik, Daniel Mayr, Alexander Zach

Stand vom 31. Mai 2023

Wir bedanken uns bei allen Mitstudierenden, die uns ihre Mitschriften zur Vervollständigung dieses Skriptums zur Verfügung gestellt haben.

Bei Fehlern, Fragen oder Feedback wird um eine Mail an `ian.hornik@tuwien.ac.at`, `daniel.mayr@tuwien.ac.at` oder `alexander.zach@tuwien.ac.at` gebeten.

Wir bemühen uns das Skriptum stets auf dem aktuellsten Stand zu halten und etwaige Fehler auszubessern. Die neueste Version ist stets auf `eps0.link/algebra` zu finden.

Ian Hornik, Daniel Mayr, Alexander Zach

Inhaltsverzeichnis

Kapitel 1

Allgemeine Algebren

Dieses Kapitel behandelt die Inhalte der Vorlesung, welche auch in Goldstern et al.: *Algebra – Eine grundlagenorientierte Einführunsvorlesung* in den Kapiteln *2. Grundbegriffe* und *4.1. Freie Algebren und der Satz von Birkhoff* gefunden werden können.

1.1 Einführung

01.03.2023

Zu Beginn wird der Begriff einer allgemeinen (oder auch universellen) Algebra definiert und es werden weiter einige spezielle Algebren vorgestellt.

Definition 1.1.1. Seien A eine beliebige Menge, $\tau = (n_i)_{i\in I}$ eine Familie aus $\mathbb{N}_0$ über einer beliebigen Indexmenge I und $(f_i)_{i\in I}$ eine Familie von Funktionen, wobei $f_i : A^{n_i} \to A$ ist. Das Tupel $\mathfrak{A} = (A, (f_i)_{i\in I})$ heißt dann *(allgemeine) Algebra* vom *Typ* τ. Die einzelnen Funktionen f_i nennt man *fundamentale Operationen* und haben *Stelligkeit* oder auch *Arität* n_i.

Bemerkung 1.1.2. Für eine endliche Indexmenge $I = \{1, \dots, m\}$ wird der Typ auch als m-Tupel $\tau = (n_1, \dots, n_m)$ geschrieben und die Algebra als $\mathfrak{A} = (A, f_1, \dots, f_m)$.

Bemerkung 1.1.3. Eine nullstellige Operation f_i bildet von der Menge $A^0 := \{\emptyset\}$ auf A ab. Es ist also f_i konstant mit $f(\emptyset) = a \in A$. Im Folgenden wird bei $n_i = 0$ nicht zwischen der Operation f_i und dem Element a, auf das abgebildet wird, unterschieden.

Definition 1.1.4. Eine Algebra $\mathfrak{A} = (A, +)$ vom Typ $\tau = (2)$ heißt *Halbgruppe*, wenn

- $\forall x, y, z \in A : (x + y) + z = x + (y + z)$ (*Assoziativität* von $+$)

gilt.

Beispiel 1.1.5. $(\mathbb{R}, +), (\mathbb{R}, \cdot), (\mathbb{R}^{2\times 2}, \cdot), (\mathbb{N}, +)$ sind Halbgruppen.

Definition 1.1.6. Eine Algebra $\mathfrak{A} = (A, +, e)$ vom Typ $\tau = (2, 0)$ heißt *Monoid*, wenn

- $(A, +)$ eine Halbgruppe ist und
- $\forall x \in A : e + x = x + e = x$ (e ist *neutrales Element* bezüglich $+$)

gilt.

Beispiel 1.1.7. $(\mathbb{R}, +, 0), (\mathbb{R}, \cdot, 1), (\mathbb{R}^{2\times 2}, \cdot, E_2), (\mathbb{N}, \cdot, 1)$ sind Monoide.

Definition 1.1.8. Eine Algebra $\mathfrak{A} = (A, +, e, -)$ vom Typ $\tau = (2, 0, 1)$ heißt *Gruppe*, wenn

- $(A, +, e)$ ein Monoid ist und
- $\forall x \in A : x + (-x) = (-x) + x = e$ ($-$ bildet ab auf *inverse Elemente*)

gilt.

Beispiel 1.1.9. $(\mathbb{R}, +, 0, -), (\mathbb{Z}, +, 0, -)$ sind Gruppen.

Bemerkung 1.1.10. Manchmal werden Gruppen auch als Algebra $\mathfrak{A} = (A, +)$ vom Typ $\tau = (2)$ definiert, für die

- $\forall x, y, z \in A : (x + y) + z = x + (y + z)$,
- $\exists e \in A \forall x \in A : e + x = x + e = x$ und
- $\forall x \in A \exists (-x) \in A : x + (-x) = (-x) + x = e$

gilt. Bei der Definition von Unterstrukturen macht es allerdings einen Unterschied, welche der Definitionen verwendet wird, weshalb im Folgenden Gruppen im Sinne von Definition 2.2.1 zu verstehen sind.

Definition 1.1.11. Eine Halbgruppe / Monoid / Gruppe $\mathfrak{A} = (A, +, \cdots)$ heißt *kommutativ* oder *abelsch*, wenn für die zweistellige Operation $+$

- $\forall x, y \in A : x + y = y + x$

gilt.

Definition 1.1.12. Eine Algebra $\mathfrak{A} = (A, +, 0, \cdot)$ vom Typ $\tau = (2, 0, 2)$ heißt *Halbring*, wenn

- $(A, +, 0)$ ein kommutatives Monoid,
- $(A, \cdot)$ eine Halbgruppe ist und
- $\forall x, y, z \in A : (x + y) \cdot z = x \cdot z + y \cdot z$ ($\cdot$ ist *rechtsdistributiv* über $+$)
  $\wedge\, z \cdot (x + y) = z \cdot x + z \cdot y$ ($\cdot$ ist *linksdistributiv* über $+$)

gilt.

Beispiel 1.1.13. $(\mathbb{N}, +, \cdot, 0), (\mathbb{R}^{2\times 2}, +, \cdot, 0^1)$ sind Halbringe.

Definition 1.1.14. Eine Algebra $\mathfrak{A} = (A, +, 0, -, \cdot)$ vom Typ $\tau = (2, 0, 1, 2)$ heißt *Ring*, wenn

- $(A, +, -, 0)$ eine kommutative Gruppe,
- $(A, \cdot)$ eine Halbgruppe und
- $\cdot$ links- und rechtsdistributiv über $+$ ist.

Gibt es eine weitere nullstellige Operation 1, sodass $(A, \cdot, 1)$ ein (kommutatives) Monoid ist, so spricht man von einem *(kommutativen) Ring mit 1*.

Beispiel 1.1.15. $(\mathbb{Z}, +, 0, -.\cdot), (\mathbb{R}[x], +, 0, -, \cdot)$ sind Ringe.

[1] 0 steht hier für $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Definition 1.1.16. Ist $\mathfrak{A} = (A, +, 0, -, 1, \cdot)$ ein kommutativer Ring mit 1, so heißt $\mathfrak{A}$ *Körper*, wenn

- $\forall x \in A \backslash \{0\} \exists y \in A : x \cdot y = 1$

Ist $\cdot$ nicht kommutativ, so nennen wir $\mathfrak{A}$ *Schiefkörper* oder *Divisionsring*.

Bemerkung 1.1.17. Im Vergleich zu allen anderen bis jetzt definierten speziellen Algebren ist ein Körper nicht durch Allaussagen für alle Elemente (Gesetze) und Operationen definiert.

Definition 1.1.18. Seien $\mathfrak{R} = (R, +, 0, -, \cdot)$ ein Ring, $\mathfrak{G} = (G, \widetilde{+}, \widetilde{0}, \widetilde{-})$ eine abelsche Gruppe und $\odot : R \times G \to G, (a, v) \mapsto a \odot v$ und gelte

- $\forall a, b \in R \forall u \in G : (a \cdot b) \odot u = a \odot (b \odot u)$,
- $\forall a, b \in R \forall u \in G : (a + b) \cdot u = (a \cdot u) \mathbin{\widetilde{+}} (b \cdot u)$,
- $\forall a \in R \forall u, v \in G : a \odot (u \mathbin{\widetilde{+}} v) = (a \odot u) \mathbin{\widetilde{+}} (a \odot v)$,

so heißt $\mathfrak{G}$ mit $\odot$ *Modul über* $\mathfrak{R}$ oder $\mathfrak{R}$*-Modul*.

Ein $\mathfrak{R}$-Modul kann auch als allgemeine Algebra nach Definition 1.1.1 definiert werden, nämlich als $\mathfrak{G}^{\mathfrak{R}} := (G, \widetilde{+}, \widetilde{0}, \widetilde{-}, (m_r)_{r \in \mathfrak{R}})$, wobei $m_r : G \to G, g \mapsto r \odot g$ unäre Operationen sind.

Bemerkung 1.1.19. Ein $\mathfrak{R}$-Modul ist ein Vektorraum (über $\mathfrak{R}$), wenn $\mathfrak{R}$ ein Körper ist.

Beispiel 1.1.20. $(\mathbb{Z}_9, +, 0, -), (\mathbb{Z}_9^{2\times 2}, +, 0, -)$ sind Moduln über $(\mathbb{Z}_9, +, 0, -, \cdot)$.

Definition 1.1.21. Eine Algebra $\mathfrak{A} = (A, \wedge)$ vom Typ $\tau = (2)$ heißt *Halbverband*, wenn

- $\mathfrak{A}$ eine kommutative Halbgruppe ist und
- $\forall x \in A : x \wedge x = x$. ($\wedge$ ist *idempotent*)

gilt.

Bemerkung 1.1.22. $(\mathbb{Z}, \min), (\mathbb{Z}, \max)$ sind Halbverbände.

Definition 1.1.23. Eine Algebra $\mathfrak{A} = (A, \wedge, \vee)$ vom Typ $\tau = (2, 2)$ heißt *Verband (im algebraischen Sinn)*, wenn

- $(A, \wedge)$, $(A, \vee)$ Halbverbände sind,
- $\forall a, b \in A : a \wedge (a \vee b) = a$ und
- $\forall a, b \in A : a \vee (a \wedge b) = a$

gilt, wobei die letzten zwei Gesetze *Verschmelzungsgesetze* genannt werden.

01.03.2023
02.03.2023

Ein Verband heißt *distributiv*, wenn $\wedge$ distributiv[2] über $\vee$ und $\vee$ distributiv über $\wedge$ ist.

Eine Algebra $\mathfrak{A} = (A, \wedge, \vee, 0, 1)$ vom Typ $\tau = (2, 2, 0, 0)$ heißt *beschränkter Verband*, wenn

- $(A, \wedge, \vee)$ ein Verband ist,
- $\forall a \in A : a \wedge 0 = 0$ und
- $\forall a \in A : a \vee 1 = 1$

[2] Es ist ausreichend Rechts- bzw. Linksdistributivität zu fordern, da die jeweilig andere Distributivität aus der Kommutativität folgt.

gilt.

Beispiel 1.1.24. Mit einer beliebigen Menge M, einem $\mathfrak{K}$-Vektorraum $\mathfrak{V}$ und einer linearen Ordnung[3] $(L, \leq)$ sind $(\mathcal{P}(M), \cap, \cup)$, $(\mathrm{Sub}(\mathfrak{V}), \cap, \langle U_1 \cup U_2 \rangle)$, $(L, \min, \max)$ Verbände.

$(\mathcal{P}(M), \cap, \cup)$ ist sogar ein distributiver Verband.

Betrachtet man die Abbildung rechts und definiert eine Ordnungsrelation, wobei die höher stehenden Elemente größer als die niedrigeren sind, und sei $\wedge, \vee$ das Supremum bzw. Infimum zweier Elemente, so ist $(\{0, 1, 2, 3, 4\}, \wedge, \vee)$ ein nicht distributiver Verband, da

$$1 \wedge (2 \vee 3) = 1 \wedge 4 = 1 \neq 0 = (1 \wedge 2) \vee (1 \wedge 3).$$

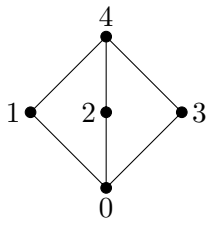

Abbildung 1.1: Hasse-Diagramm einer Ordnungsrelation

$(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ ist ein beschränkter Verband. $(\mathbb{Q}, \min, \max)$ kann hingegen nicht zu einem beschränkten Verband gemacht werden.

Lemma 1.1.25. *Jeder Verband $\mathfrak{V} = (V, \wedge, \vee)$ mit endlicher Trägermenge $V = \{v_1, \ldots, v_n\}$ kann zu einem beschränkten Verband gemacht werden.*

Beweis. Sei $1 := v_1 \vee \ldots \vee v_n$, dann gilt für beliebiges $j \in \{1, \ldots, n\}$, dass

$$v_j \vee 1 = v_j \vee v_1 \vee \ldots \vee v_n = v_1 \vee \ldots \vee v_j \vee v_j \vee \ldots \vee v_n = v_1 \vee \ldots \vee v_n = 1.$$

Analoges gilt für $0 := v_1 \wedge \ldots \wedge v_n$. Damit ist $(V, \wedge, \vee, 0, 1)$ ein beschränkter Verband. □

Definition 1.1.26. Eine Algebra $\mathfrak{A} = (A, \wedge, \vee, 0, 1, ')$ vom Typ $\tau = (2, 2, 0, 0, 1)$ heißt *Boole'sche Algebra*, wenn

- $(A, \wedge, \vee, 0, 1)$ ein beschränkter distributiver Verband ist,
- $\forall x \in A : x \wedge x' = 0$ und
- $\forall x \in A : x \vee x' = 1$

gilt.

Beispiel 1.1.27. Für eine Menge M ist $(\mathcal{P}(M), \cap, \cup, \emptyset, M, ')$ mit $'(X) := M \setminus X$ eine Boole'sche Algebra.

Bemerkung 1.1.28. Alle Boole'schen Algebren werden durch den Darstellungssatz von Stone bis auf Isomorphie beschrieben.

Definition 1.1.29. Seien $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i \in I}), \mathfrak{B} = (B, (f_i^{\mathfrak{B}})_{i \in I})$ zwei Algebren vom selben Typ $\tau = (n_i)_{i \in I}$. Eine Abbildung $\varphi : A \to B$ heißt *Homomorphismus*, wenn

$$\forall i \in I \forall a_1, \ldots, a_{n_i} \in A : \varphi(f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})) = f_i^{\mathfrak{B}}(\varphi(a_1), \ldots, \varphi(a_{n_i})).$$

Wir schreiben dann auch $\varphi : \mathfrak{A} \to \mathfrak{B}$.

Wenn φ bijektiv ist, dann heißt die Funktion *Isomorphismus*. Ist $\mathfrak{A} = \mathfrak{B}$, dann heißt φ *Endomorphismus*. Ein bijektiver Endomorphismus heißt *Automorphismus*.

[3] Eine lineare Ordnung nennt man auch *Totalordnung*.

Definition 1.1.30. Zwei Algebren $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I}), \mathfrak{B} = (B, (f_i^{\mathfrak{B}})_{i\in I})$ von selben Typ nennen wir *isomorph*, wenn es einen Isomorphismus $\varphi : \mathfrak{A} \to \mathfrak{B}$ gibt. Wir schreiben auch $\mathfrak{A} \cong \mathfrak{B}$.

Beispiel 1.1.31. Sei $\mathfrak{A}$ eine Algebra. Wir definieren die Mengen

$$\begin{aligned}\mathrm{End}(\mathfrak{A}) &:= \{f : A \to A \mid f \text{ ist Endomorphismus}\} \text{ und}\\ \mathrm{Aut}(\mathfrak{A}) &:= \{f : A \to A \mid f \text{ ist Automorphismus}\}.\end{aligned}$$

$(\mathrm{End}(\mathfrak{A}), \circ, \mathrm{id}_A)$ ist dann ein Monoid, das *Endomorphismenmonoid von* $\mathfrak{A}$. Jedes Monoid ist isomorph zu einem Endomorphismenmonoid.

$(\mathrm{Aut}(\mathfrak{A}), \circ, \mathrm{id}_A, ^{-1})$ ist eine Gruppe, die *Automorphismengruppe von* $\mathfrak{A}$. Nach dem Satz von Cayley ist jede endliche Gruppe isomorph zu einer Automorphismengruppe.

1.2 Terme und Termalgebra

Definition 1.2.1. Sei X eine beliebige Menge und seien $(f_i)_{i\in I}$ Funktionssymbole mit Aritäten $(n_i)_{i\in I}$. Die Menge $T(X) := T$ ist rekursiv definiert durch

$$T_0 := X, \quad T_{k+1} := T_k \cup \{f_i(t_1, \dots t_{n_i}) \mid i \in I \wedge t_1, \dots, t_{n_i} \in T_k\}, \quad T := \bigcup_{i\geq 0} T_i.$$

Ein Element $t \in T$ heißt *Term*, die Elemente aus X *Variablen*, $(f_i)_{i\in I}$ *Sprache* und die Menge T beschreibt alle *Terme über* $(X, (f_i)_{i\in I})$. Für einen Term $t \in T$ heißt $\mathrm{lvl}(t) := \min\{k \mid t \in T_k\}$ die *Stufe von* t.

Weiter werden die *Variablen eines Terms* rekursiv definiert. Für $x \in X$ ist $\mathrm{var}(x) := \{x\}$ und für $t = f_i(t_1, \dots, t_{n_i})$ ist $\mathrm{var}(t) := \bigcup_{j\in\{1,\dots,n_i\}} \mathrm{var}(t_j)$.

Beispiel 1.2.2. Seien $X = \{x, y, z\}$ und $(f_1, f_2, f_3) = (+, \cdot, -)$ mit Aritäten $(2, 2, 1)$. Damit erhält man x, y, z als Terme 0-ter Stufe, $-x, x + x, x \cdot z, z + x, \dots$ als Terme 1-ter Stufe, $(-x) + y, (x \cdot z) - y, \dots$ als Terme 2-ter Stufe etc.

Definition 1.2.3. Sei T die Menge aller Terme über $(X, (f_i)_{i\in I})$. Es ist dann $\mathfrak{T}(X, (f_i)_{i\in I}) := (T, (f_i^{\mathfrak{T}}))$, die *(erzeugte) Termalgebra*, eine Algebra vom Typ $\tau = (n_i)_{i\in I}$, wobei $f_i^{\mathfrak{T}} : T^{n_i} \to T, (t_1, \dots, t_{n_i}) \mapsto f_i(t_1, \dots, t_{n_i})$.

Satz 1.2.4. *Seien X eine Variablenmenge, $(f_i)_{i\in I}$ Funktionssymbole mit Aritäten $\tau = (n_i)_{i\in I}$, $\mathfrak{T} := \mathfrak{T}(X, (f_i)_{i\in I})$ die induzierte Termalgebra und $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine beliebige Algebra vom Typ τ. Dann kann jede Abbildung $\varphi : X \to A$ eindeutig zu einem Homomorphismus $\overline{\varphi} : T \to A$ fortgesetzt werden. $\overline{\varphi}$ ist also ein Homomorphismus von $\mathfrak{T}$ nach $\mathfrak{A}$ mit $\overline{\varphi}|_X = \varphi$.*

Beweis. Sei $\varphi : X \to A$ beliebig. Es wird dazu $\overline{\varphi} : T \to A$ rekursiv nach der Stufe von Termen definiert. Für $t \in X$ wird $\overline{\varphi}(t) := \varphi(t)$ gewählt und für $t = f_i(t_1, \dots, t_{n_i}) \in T$ definiere $\overline{\varphi}(t) := f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i}))$. Diese Definition ergibt Sinn, da für einen Term t, der als $t = f_i(t_1, \dots, t_{n_i})$ geschrieben werden kann, die Terme $t_1, \dots, t_{n_i}$ von niedrigerer Stufe als t sind.

Aus dieser Definition ist klar, dass $\overline{\varphi}|_X = \varphi$. Für $i \in I$ und $t_1, \dots, t_{n_i} \in T$ gilt $\overline{\varphi}(f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})) = \overline{\varphi}(f_i(t_1, \dots, f_{n_i})) \overset{\text{Def.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i}))$, also $\overline{\varphi} : \mathfrak{T} \to \mathfrak{A}$.

Es bleibt noch die Eindeutigkeit zu zeigen. Sei $\widetilde{\varphi} : T \to A$ ein beliebiger Homomorphismus mit $\widetilde{\varphi}|_X = \varphi$, so zeigen wir vermöge vollständiger Induktion nach Termstufe m, dass $\widetilde{\varphi} = \overline{\varphi}$:

Induktionsanfang ($m = 0$): Für $t \in T_0 = X$ gilt klarerweise $\widetilde{\varphi}(t) = \varphi(t) = \overline{\varphi}(t)$.
Induktionsschritt ($m \to m+1$): Sei nun $t = f_i(t_1, \ldots, t_{n_i}) \in T_{m+1}$ mit $t_1, \ldots, t_{n_i} \in T_m$, dann gilt $\widetilde{\varphi}(t) = \widetilde{\varphi}(f_i(t_1, \ldots, t_{n_i})) = \widetilde{\varphi}(f_i^{\mathfrak{T}}(t_1, \ldots, t_{n_i})) = f_i^{\mathfrak{A}}(\widetilde{\varphi}(t_1), \ldots, \widetilde{\varphi}(t_{n_i})) \overset{\text{I.V.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \ldots, \overline{\varphi}(t_{n_i})) = \overline{\varphi}(t)$. □

02.03.2023
08.03.2023

Definition 1.2.5. Seien $X^{(k)} = \{x_1, \ldots, x_k\} \subseteq X$ eine Teilmenge der Variablenmenge, $\mathfrak{T}^{(k)} = \mathfrak{T}(X^{(k)}, (f_i)_{i\in I}) = (T^{(k)}, (f_i^{\mathfrak{T}})_{i\in I})$ die erzeugte Termalgebra und $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra vom selben Typ. Für $a_1, \ldots, a_k \in A$ heißt $\alpha_{a_1,\ldots,a_k} : X^{(k)} \to A, x_j \mapsto a_j$ eine *Variablenbelegung*. Nach Satz 1.2.4 kann diese nun zum *Einsetzungshomomorphismus* $\overline{\alpha}_{a_1,\ldots,a_k} : T^{(k)} \to A$ fortgesetzt werden.

Für einen beliebigen Term $t \in T^{(k)}$ ist die *durch t in $\mathfrak{A}$ induzierte Termoperation* als $t^{\mathfrak{A}} : A^k \to A, (a_1, \ldots, a_k) \mapsto \overline{\alpha}_{a_1,\ldots a_k}(t)$ definiert. Damit wird aus einem abstrakten Term eine Funktion auf A.

Beispiel 1.2.6. Sei $+$ ein binäres Funktionssymbol und $X = \{x_1, x_2, \ldots\}$. Damit erhält man u. a. die abstrakten Terme $t = x_1 + (x_2 + x_3), s = (x_1 + x_2) + x_3 \in T$.

Betrachtet man die Algebra $\mathfrak{R} = (\mathbb{R}, +_{\mathbb{R}})$, so erhält man die induzierten Termfunktionen

$$t^{\mathfrak{R}} : \mathbb{R}^3 \to \mathbb{R}, (a_1, a_2, a_3) \mapsto a_1 + (a_2 + a_3) \quad \text{und} \quad s^{\mathfrak{R}} : \mathbb{R}^3 \to \mathbb{R}, (a_1, a_2, a_3) \mapsto (a_1 + a_2) + a_3.$$

Da $+_{\mathbb{R}}$ assoziativ ist, gilt $t^{\mathfrak{R}} = s^{\mathfrak{R}}$, obwohl $t \neq s$.

Beispiel 1.2.7. Sei $\mathfrak{V} = (V, +, 0, -, (m_k)_{k\in\mathfrak{K}})$ ein Vektorraum über einem Körper $\mathfrak{K}$. Betrachtet man Terme über der Sprache $(+, -, (m_k)_{k\in\mathfrak{K}})$, also z. B. $x_1 + x_2, m_2(x_1 + x_2), x_1 + m_4(x_2)$, so stellen die davon induzierten Termfunktionen Linearkombinationen dar.

Definition 1.2.8. Seien $s, t \in T$ Terme über einer Sprache $(f_i)_{i\in I}$, dann heißt $s \approx t$ *Gesetz*. Ein Gesetz kann auch als Paar (s, t) von zwei Termen gesehen werden.

Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra über derselben Sprache, dann *erfüllt* $\mathfrak{A}$ *das Gesetz* $s \approx t$ oder kurz $\mathfrak{A} \models s \approx t$, wenn

$$\forall(\alpha : \operatorname{var}(s) \cup \operatorname{var}(t) \to A) : \overline{\alpha}(s) = \overline{\alpha}(t),$$

oder anders formuliert, wenn die Termfunktionen $s^{\mathfrak{A}}$ und $t^{\mathfrak{A}}$ übereinstimmen.

1.3 Varietäten und Klone

In diesem Kapitel werden die Begriffe *Varietät* und *Klon* definiert und es werden Beispiel dazu gegeben. Aussagen darüber folgen in den nächsten Kapiteln.

Definition 1.3.1. Sei Σ eine Menge von Gesetzen über eine Sprache $(f_i)_{i\in I}$, dann heißt die Klasse

$$\mathcal{V}(\Sigma) := \{\mathfrak{A} \mid \mathfrak{A} \text{ ist Algebra über der Sprache } (f_i)_{i\in I} \wedge \forall s \approx t \in \Sigma : A \models s \approx t\}$$

Varietät. Es handelt sich dabei also um eine durch Gesetze definierte Klasse von Algebren.

Beispiel 1.3.2. Betrachtet man die Sprache $(+, 0, -)$ mit Stelligkeiten $(2, 0, 1)$ und definiert die Gesetzesmenge (mit Variablenmenge $X = \{x, y, z\}$) $\Sigma = \{$

$(x + y) + z \approx x + (y + z)$,

$0 + x \approx x$, $x + 0 \approx x$,

$x + (-x) \approx 0$, $(-x) + x \approx 0$

$\}$, so ist die Varietät $\mathcal{V}(\Sigma)$ die Klasse aller Gruppen.

Betrachtet man hingegen Gruppen über der Sprache $(+)$ wie in Bemerkung 1.1.10, so kann man die Gruppenaxiome nicht über Gesetze definieren.

Definition 1.3.3. Sei M eine beliebige Menge. Für $1 \leq i \leq n$ ist die *n-dimensionale Projektion auf die i-te Komponente* definiert als

$$\pi_i^{(n)} : M^n \to M, (x_1, \ldots, x_n) \to x_i.$$

Definition 1.3.4. Sei M eine beliebige Menge. Eine Teilmenge von Funktionen $\mathcal{C} \subseteq \bigcup_{n\geq 1}\{f : M^n \to M\}$ heißt *Klon*, wenn

- $\mathcal{C}$ alle Projektionen enthält und
- $\mathcal{C}$ unter Komposition abgeschlossen ist.

Die Komposition von $f : M^n \to M$ und $g_1, \ldots, g_n : M^k \to M$ definieren wir hier als

$$f \circ (g_1, \ldots, g_n) : M^k \to M, (x_1, \ldots, x_k) \mapsto f(g_1(x_1, \ldots, x_k), \ldots, g_n(x_1, \ldots, x_k)).$$

Definition 1.3.5. Sei $\mathfrak{A} = (A, (f_i)_{i\in I})$ eine Algebra und sei die Menge $\mathcal{T}^{(n)}(\mathfrak{A}) := \{f : A^n \to A \mid f \text{ ist Termfunktion von } \mathfrak{A}\}$. Dann ist $\mathcal{T}(\mathfrak{A}) := \bigcup_{n\geq 1} \mathcal{T}^{(n)}(\mathfrak{A})$ ein Klon und wird *Termklon von* $\mathfrak{A}$ genannt.

1.4 Konstruktion neuer Algebren

In diesem Kapitel werden drei verschiedene Konstruktionen vorgestellt um aus bereits gegebenen Algebren neue zu gewinnen.

1.4.1 Unteralgebren

Definition 1.4.1. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und $S \subseteq A$. Dann heißt das Tupel $\mathfrak{S} = (S, (f_i^{\mathfrak{A}}|_{S^{n_i}})_{i\in I})$[4] *Subalgebra* oder *Unteralgebra* von $\mathfrak{A}$, wenn

- $\forall i \in I \forall a_1, \ldots, a_{n_i} \in S : f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i}) \in S$. *($S$ ist abgeschlossen gegenüber allen f_i)*

Wir schreiben in diesem Fall $\mathfrak{S} \leq \mathfrak{A}$.

Beispiel 1.4.2. Sei $\mathfrak{V} = (V, +, 0, -, (m_k)_{k\in\mathfrak{K}})$ ein Vektorraum über einem Körper $\mathfrak{K}$. Dann gilt für jeden Untervektorraum U von V: $\mathfrak{U} = (U, +, 0, -, (m_k)_{k\in\mathfrak{K}}) \leq \mathfrak{V}$.

Weitere Beispiele für Unteralgebren sind $(\mathbb{N}, +) \leq (\mathbb{Z}, +)$ und $(\mathrm{Sl}_n(K), \cdot) \leq (\mathrm{Gl}_n(K), \cdot)$.

[4] Zwecks besserer Lesbarkeit werden wir dafür meist $\mathfrak{S} = (S, (f_i^{\mathfrak{S}})_{i\in I})$ schreiben.

Proposition 1.4.3. *Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra, $s \approx t$ ein Gesetz und gelte $\mathfrak{A} \models s \approx t$. Dann gilt für jede Unteralgebra $\mathfrak{S}$ von $\mathfrak{A}$ auch $\mathfrak{S} \models s \approx t$.*

Beweis. Laut Definition gilt für alle Variablenbelegungen $\varphi : \mathrm{var}(s) \cup \mathrm{var}(t) \to A : \bar{\varphi}(s) = \bar{\varphi}(t)$. Wegen $S \subseteq A$ ist diese Bedingung insbesondere für alle $\varphi : \mathrm{var}(s) \cup \mathrm{var}(t) \to S$ erfüllt, also gilt $\mathfrak{S} \models s \approx t$. □

Bemerkung 1.4.4. Sei $\mathfrak{V} = (V, +, 0, -, (m_k)_{k\in\mathfrak{K}})$ ein Vektorraum über einem Körper $\mathfrak{K}$. Dann ist $x \approx 0$ ein Gesetz, welches in $(\{0\}, +, 0, -)$ erfüllt ist, jedoch nicht in $\mathfrak{V}$. Wir sehen also, dass die Umkehrung von Proposition 1.4.3 nicht gilt.

Korollar 1.4.5. *Varietäten sind abgeschlossen unter der Bildung von Unteralgebren.*

Bemerkung 1.4.6. Eine Folgerung ist unmittelbar, dass die Klasse der Körper keine Varietät bildet, denn $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist eine Unteralgebra von $(\mathbb{Q}, +, 0, -, \cdot, 1)$, aber die ganzen Zahlen stellen keinen Körper dar.

Bemerkung 1.4.7. An dieser Stelle können wir den Unterschied der gegebenen Definitionen einer Gruppe feststellen, denn $(\mathbb{N}, +)$ ist eine Unteralgebra von $(\mathbb{Z}, +)$, jedoch keine Gruppe im Sinne von Bemerkung 1.1.10. Das bedeutet, dass in der Sprache $+$ die Klasse der Gruppen keine Varietät bildet.

08.03.2023
09.03.2023

Proposition 1.4.8. *Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und $(\mathfrak{S}_j = (S_j, (f_i^{\mathfrak{S}_j})_{i\in I}))_{j\in J}$ eine Familie von Unteralgebren von $\mathfrak{A}$. Dann ist auch $\mathfrak{S} = \bigcap_{j\in J} \mathfrak{S}_j := (\bigcap_{j\in J} S_j, (f_i^{\mathfrak{A}}|_{\bigcap_{j\in J} S_j})_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$.*

Beweis. Für $S := \bigcap_{j\in J} S_j$ gilt offensichtlich $S \subseteq A$, also bleibt lediglich die Abgeschlossenheit bezüglich der Funktionen $f_i^{\mathfrak{S}}$ zu zeigen. Seien $a_1, \ldots, a_{n_i} \in S$ beliebig. Dann gilt für alle $j \in J$: $a_1, \ldots, a_{n_i} \in S_j$ und da $\mathfrak{S}_j$ eine Unteralgebra von $\mathfrak{A}$ ist auch $f_i^{\mathfrak{S}_j}(a_1, \ldots, a_{n_i}) \in S_j$. Das ist genau die Definition von $f^{\mathfrak{S}}(a_1, \ldots, a_{n_i}) \in \bigcap_{j\in J} S_j = S$, also ist $\mathfrak{S} = (S, (f_i^{\mathfrak{S}})_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$. □

Korollar 1.4.9. *Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und $S \subseteq A$. Dann ist die von S* erzeugte Unteralgebra *von $\mathfrak{A}$ definiert durch $\langle S\rangle := \bigcap\{\mathfrak{U} \mid S \subseteq U \wedge \mathfrak{U} = (U, (f_i^{\mathfrak{A}})_{i\in I}) \leq \mathfrak{A}\}$ die kleinste S enthaltende Unteralgebra von $\mathfrak{A}$.*

Definition 1.4.10. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und $S \subseteq A$. Die Menge S_∞ ist rekursiv definiert durch

$$S_0 := S, \quad S_{k+1} := S_k \cup \{f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i} \mid i \in I \wedge a_1, \ldots a_{n_i} \in S_k)\}, \quad S_\infty := \bigcup_{k\geq 0} S_k.$$

Beispiel 1.4.11. Diese Skizze zeigt die anschauliche Motiviation der vorhergehenden Definition.

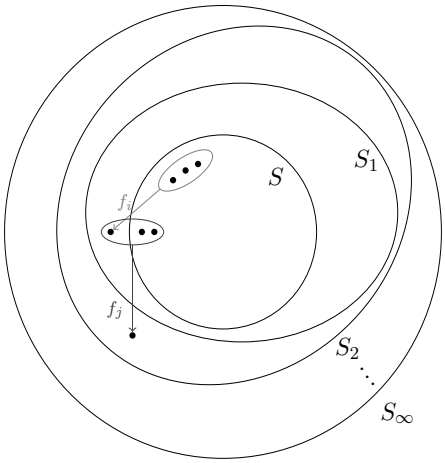

Abbildung 1.2: Subalgebra von unten

Proposition 1.4.12. *Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra, $S \subseteq A$ und X eine Menge mit $|X| \geq \min\{|S|, \aleph_0\}$. Dann gelten die beiden Identitäten:*

1. $\langle S\rangle = S_\infty$
2. $\langle S\rangle = \{t^{\mathfrak{A}}(a_1, \ldots, a_n) \mid n \in \mathbb{N}, a_1, \ldots, a_n \in S, t \in T(X)\}$

Beweis. In beiden Behauptungen wird die gegenseitige Inklusion von zwei Mengen gezeigt.

1. Da S_∞[5] eine S enthaltende Unteralgebra von A ist, folgt aus der Definition der erzeugten Unteralgebra, dass $\langle S\rangle \subseteq S_\infty$ gilt. Für die andere Inklusion wird mittels Induktion gezeigt, dass für alle $k \in \mathbb{N} : S_k \subseteq \langle S\rangle$ gilt, woraus schließlich auch $S_\infty = \bigcup_{k\in\mathbb{N}} S_k \subseteq \langle S\rangle$ folgt.

   Induktionsanfang ($k = 0$): Per Definitionem der erzeugten Algebra gilt $S_0 = S \subseteq \langle S\rangle$.
   Induktionsschritt ($k \to k + 1$): Sei nun $a \in S_{k+1}$ beliebig. Falls $a \in S_k$ ist, so folgt aus der Induktionsvoraussetzung dass $a \in \langle S\rangle$ gilt. Andernfalls existieren ein $i \in I$ und $a_1, \ldots, a_{n_i} \in S_k$, sodass $a = f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})$. Auch hier kann die Induktionsvoraussetzung angewandt werden, weshalb $a_1, \ldots, a_{n_i} \in \langle S\rangle$ ist. Da $(\langle S\rangle, (f_i^{\mathfrak{A}})_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$ ist, gilt auch $a = f_i^{\mathfrak{A}}(a_1 \ldots, a_{n_i}) \in \langle S\rangle$. Daraus folgt die gewünschte Mengeninklusion $S_{k+1} \subseteq \langle S\rangle$.

2. Definiere $M := \{t^{\mathfrak{A}}(a_1, \ldots, a_n) | a_1, \ldots, a_n \in S \wedge t \in T(X)\}$. Es gilt $S \subseteq M$, da die Projektionen $\pi_j^{(n)} : A^n \to A, (a_1, \ldots, a_n) \mapsto a_j$ Termfunktionen sind. Außerdem kann gezeigt werden, dass $(M, (f_i)_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$ ist. Sei $i \in I$ beliebig und seien $b_1, \ldots, b_{n_i} \in M$, dann können diese Elemente als $b_j = t_j^{\mathfrak{A}}(a_1^{(j)}, \ldots, a_{m_j}^{(j)})$ mit $a_1^{(j)}, \ldots, a_{m_j}^{(j)} \in S$ für $j \in \{1, \ldots, n_i\}$ dargestellt werden. Definiert man nun $a := f_i^{\mathfrak{A}}(b_1, \ldots, b_{n_i})$ und den Term $t := f_i^{\mathfrak{T}}(t_1(x_1^{(1)}, \ldots, x_{m_1}^{(1)}), \ldots, t_{n_i}(x_1^{(n_i)}, \ldots, x_{m_{n_i}}^{(n_i)}))$, so erhält man eine passende Termfunktion, das heißt es gilt $t^{\mathfrak{A}}(a_1^{(1)}, \ldots, a_{m_1}^{(1)}, \ldots, a_1^{(n_i)}, \ldots, a_{m_{n_i}}^{(n_i)}) = a$, also insbesondere $a \in M$. Für die andere Mengeninklusion ist erneut eine Induktion nötig. Sei $a = t^{\mathfrak{A}}(a_1, \ldots, a_n) \in M$ beliebig. Zu zeigen ist, dass $a \in \langle S\rangle$ gilt, wobei dies mittels Induktion nach der Stufe von t gezeigt wird.

   Induktionsanfang ($k = 0$): Dann ist der Term t eine Variable x_j und die Termfunktion $t^{\mathfrak{A}}$ ist eine Projektion $a = t^{\mathfrak{A}}(a_1, \ldots, a_n) = \pi_j^n(a_1, \ldots, a_n) = a_j \in S \subseteq \langle S\rangle$.
   Induktionsschritt ($m < k \to k$): Dann ist $t = f_i^{\mathfrak{T}}(t_1, \ldots, t_{n_i})$ und $a = t^{\mathfrak{A}}(a_1, \ldots, a_{n_i}) = f_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}(a_1, \ldots, a_n), \ldots, t_{n_i}^{\mathfrak{A}}(a_1, \ldots, a_n)) \in \langle S\rangle$, da die Terme $t_j^{\mathfrak{A}}$ für $j \in \{1, \ldots, n_i\}$ kleinere

[5] Hier wird die Algebra für bessere Lesbarkeit mit der Trägermenge identifiziert

Stufe als k haben. Daher sind die Argumente nach Induktionsvoraussetzung in $\langle S\rangle$ und damit auch der Funktionswert.

□

Korollar 1.4.13. *Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra, $S = \{s_1, \dots, s_n\} \subseteq A$ und X eine beliebige Menge mit mindestens n-Elementen. Dann gilt für die von S erzeugte Unteralgebra*

$$\langle S\rangle = \{t^{\mathfrak{A}}(s_1, \dots, s_n) \mid t(x_1, \dots, x_n) \in T(X)\}.$$

Beweis. Es gilt klarerweise $\langle S\rangle \supseteq \{t^{\mathfrak{A}}(s_1, \dots, s_n) \mid t(x_1, \dots, x_n) \in T(X)\}$. Sei $a \in \langle S\rangle$ beliebig. Dann existiert ein Term t und es existieren $a_1, \dots, a_\ell \in S$, sodass $a = t^{\mathfrak{A}}(a_1, \dots, a_\ell)$. Mit dem Term $\tilde{t}(x_1, \dots, x_n) := t(y_1, \dots, y_\ell)$, wobei $y_i := x_j \leftrightarrow a_i = s_j$ erhält man $\tilde{t}^{\mathfrak{A}}(s_1, \dots, s_n) = t^{\mathfrak{A}}(a_1, \dots, a_\ell) = a \in \{t^{\mathfrak{A}}(s_1, \dots, s_n) \mid t(x_1, \dots, x_n) \in T(X)\}$. □

Bemerkung 1.4.14. Für eine beliebige Algebra ist mit $\mathrm{Sub}(\mathfrak{A}) := \{\mathfrak{U} \mid \mathfrak{U} \leq \mathfrak{A}\}$ durch $(\mathrm{Sub}(\mathfrak{A}), \subseteq)$ eine Halbordnung gegeben. Weiter ist $(\mathrm{Sub}(\mathfrak{A}, \wedge, \vee))$, wobei $U_1 \wedge U_2 := U_1 \cap U_2$ und $U_1 \vee U_2 := \langle U_1 \cup U_2\rangle$, ein Verband.

1.4.2 Produktalgebren

Bemerkung 1.4.15. Das kartesische Produkt von Mengen $(M_i)_{i\in I}$ ist definiert als

$$\prod_{i\in I} M_i := \left\{ f : I \to \bigcup_{i\in I} M_i \mid \forall i \in I : f(i) \in M_i \right\}.$$

Genau genommen sind die Elemente von Produktmengen also Funktionen. Im Folgenden werden statt Funktionsnotation oft Familien (welche nur eine andere Notation für Funktionen sind) und bei endlicher Indexmenge I auch Tupel geschrieben.

Definition 1.4.16. Sei $\tau = (n_i)_{i\in I}$ ein Typ und sei $(\mathfrak{A}_j)_{j\in J}$ eine Familie von Algebren dieses Typs. Dann heißt $\mathfrak{A} := \prod_{j\in J} \mathfrak{A}_j := (\prod_{j\in J} A_j, (f_i^{\mathfrak{A}})_{i\in I})$ *Produktalgebra*, wobei die Operationen durch $f_i^{\mathfrak{A}} : \mathfrak{A}^{n_i} \to \mathfrak{A}, ((a_j^{(1)})_{j\in J}, \dots (a_j^{(n_i)})_{j\in J}) \mapsto (f_i^{\mathfrak{A}_j}(a_j^{(1)}, \dots, a_j^{(n_i)}))_{j\in J}$ definiert werden.

Beispiel 1.4.17. Abbildung 1.3 visualisiert die Bildung einer Produktalgebra.

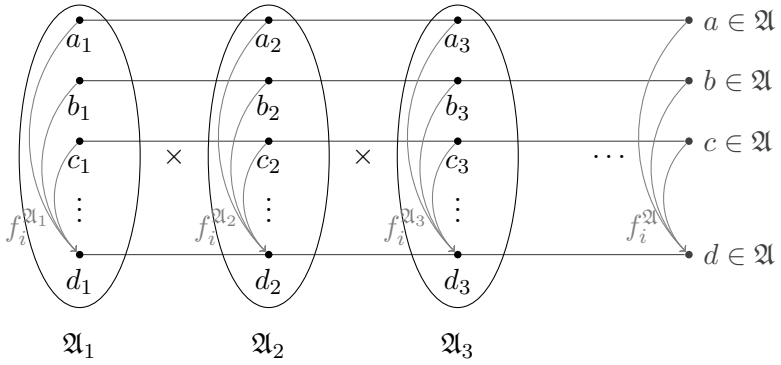

Abbildung 1.3: Visualisierung von Produktalgebren

Bemerkung 1.4.18. Ist $\mathfrak{A} = \prod_{j\in J} \mathfrak{A}_j$ eine Produktalgebra und $j \in J$, so ist durch die Projektionsabbildung $\pi_j : \mathfrak{A} \to \mathfrak{A}_j, (a_j)_{j\in J} \mapsto a_j$ ein surjektiver Homomorphismus gegeben.

Proposition 1.4.19. *Seien $(f_i)_{i\in I}$ eine Signatur, $s \approx t$ ein Gesetz in dieser Sprache, $(\mathfrak{A}_j)_{j\in J}$ eine Familie von Algebren in der Signatur und es gelte für alle $j \in J : \mathfrak{A}_j \models s \approx t$. Dann gilt auch $\mathfrak{A} := \prod_{j\in J} \mathfrak{A}_j \models s \approx t$.*

Beweis. Es ist hinreichend zu zeigen, dass $s^{\mathfrak{A}} = t^{\mathfrak{A}}$ gilt. Seien $\mathbf{a}^{(1)} = (a_j^{(1)})_{j\in J}, \ldots, \mathbf{a}^{(n)} \in A$ beliebig. Dann gilt laut Voraussetzung für alle $j \in J : s^{\mathfrak{A}_j}(a_j^{(1)}, \ldots, a_j^{(n)})) = t^{\mathfrak{A}_j}(a_j^{(1)}, \ldots, a_j^{(n)}))$. Daher folgt $s^{\mathfrak{A}}(\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n)})_j = s^{\mathfrak{A}_j}(a_j^{(1)}, \ldots, a_j^{(n)})) = t^{\mathfrak{A}_j}(a_j^{(1)}, \ldots, a_j^{(n)})) = t^{\mathfrak{A}}(\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n)})_j$ für alle $j \in J$, also insbesondere $s^{\mathfrak{A}}(\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n)}) = t^{\mathfrak{A}}(\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n)})$ und damit $s^{\mathfrak{A}} = t^{\mathfrak{A}}$. □

Korollar 1.4.20. *Varietäten sind abgeschlossen unter der Bildung von Produkten.*

Bemerkung 1.4.21. Auch an dieser Stelle wird deutlich, dass die Klasse der Körper keine Varietät ist. Für einen Körper $\mathfrak{K}$ und den Produktraum $\mathfrak{K} \times \mathfrak{K}$ gilt $(1, 0) \cdot (0, 1) = (0, 0)$. Da Körper immer nullteilerfrei sind, kann dieser Produktraum folglich kein Körper sein.

09.03.2023
15.03.2023

1.4.3 Faktoralgebren

Definition 1.4.22. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra, $m \in \mathbb{N}$ und $R \subseteq A^m$ eine m-stellige Relation auf A. Dann heißt R *invariant unter* $\mathfrak{A}$, wenn

- $\forall i \in I : \forall r^{(1)}, \ldots, r^{(n_i)} \in R : (f_i(r_1^{(1)}, \ldots, r_1^{(n_i)}), \ldots, f_i(r_m^{(1)}, \ldots, r_m^{(n_i)})) \in R$.

Definition 1.4.23. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und $\sim \subseteq A^2$ eine Äquivalenzrelation. Wenn $\sim$ invariant unter $\mathfrak{A}$ ist, dann heißt $\sim$ *Kongruenzrelation*. Außerdem wird damit die Menge $\mathrm{Con}(\mathfrak{A}) := \{\sim \subseteq A^2 \mid \sim \text{ ist Kongruenzrelation auf } \mathfrak{A}\}$ definiert.

Beispiel 1.4.24. Sei X eine Menge, $(f_i)_{i\in I}$ eine Signatur und $\mathfrak{T} = (T, (f_i^{\mathfrak{T}})_{i\in I})$ die Termalgebra über X. Sei außerdem $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra in derselben Signatur. Dann ist durch $t \sim s :\leftrightarrow t^{\mathfrak{A}} = s^{\mathfrak{A}}$ auf $\mathfrak{T}$ eine Kongruenzrelation gegeben.

Beispiel 1.4.25. Für jede beliebige Algebra $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ sind durch die beiden Relationen $\sim_1 = A^2$ und $\sim_2 = \{(a, a) \mid a \in A\}$ Kongruenzrelationen auf $\mathfrak{A}$ gegeben. Diese nennt man daher auch *triviale Kongruenzrelationen*.

Bemerkung 1.4.26. Für eine beliebige Algebra $\mathfrak{A}$ ist durch $(\mathrm{Con}(A), \subseteq)$ eine Halbordnung gegeben. Da es zu zwei Kongruenzrelationen bezüglich der Mengeninklusion immer ein Supremum und Infimum gibt, entsteht sogar ein Verband.

Definition 1.4.27. Eine Algebra $\mathfrak{A}$ heißt *einfach*, wenn es keine nicht-trivialen Kongruenzrelationen gibt.

Definition 1.4.28. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra und sei $\sim \subseteq A^2$ eine Kongruenzrelation. Dann heißt $\mathfrak{A}/_\sim := (A/_\sim, (f_i^{\mathfrak{A}/_\sim})_{i\in I})$ *Faktoralgebra* von $\mathfrak{A}$, wobei $A/_\sim = \{[a]_\sim \mid a \in A\}$ die Menge der Äquivalenzklassen[6] ist und die Funktionen definiert[7] sind durch $f^{\mathfrak{A}/_\sim}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) := [f_i(a_1, \ldots, a_{n_i})]_\sim$.

Beispiel 1.4.29. Betrachten wir die Algebra $(\mathbb{Z}, +, \cdot)$ und definieren darauf die Kongruenzrelation $a \sim b :\leftrightarrow \exists k \in \mathbb{Z}(a - b = k \cdot m)$, so stellt $(\mathbb{Z}_m, +, \cdot) = (\mathbb{Z}, +, \cdot)/_\sim$ eine Faktoralgebra dar. Man bemerke außerdem, dass in $(\mathbb{Z}_m, +, \cdot)$ beispielsweise das Gesetz $\forall x(\overbrace{x + \ldots + x}^{m+1 \text{ mal}} = x)$ gilt, während dieses in $(\mathbb{Z}, +, \cdot)$ nicht gilt. Es können also in einer Faktoralgebra mehr Gesetze erfüllt sein, als in der ursprünglichen Algebra.

Bemerkung 1.4.30. Sei $\mathfrak{A}$ eine beliebige Algebra und $\sim$ eine Kongruenzrelation. Dann ist die *kanonische Faktorabbildung* oder *kanonische Projektion* $\varphi : A \to A/_\sim, a \mapsto [a]_\sim$ ein surjektiver Homomorphismus, das heißt Faktoralgebren sind homomorphe Bilder von Algebren. Der folgende Satz liefert in einem gewissen Sinn die Umkehrung.

Lemma 1.4.31. *Seien $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ und $\mathfrak{B} = (B, (f_i^{\mathfrak{B}})_{i\in I})$ Algebren vom selben Typ und sei $h : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. Dann ist $\ker h := \{(a, b) \in A^2 \mid h(a) = h(b)\}$ eine Kongruenzrelation auf $\mathfrak{A}$.*

Beweis. Es sei $i \in I$ beliebig und $a_1 \ldots, a_{n_i}, b_1 \ldots, b_{n_i} \in A$ mit $(a_j, b_j) \in \ker h$ für alle $j \in \{1, \ldots, n_i\}$. Laut Definition gilt also $h(a_j) = h(b_j)$ für alle $j \in \{1, \ldots, n_i\}$ und daher auch $h(f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})) = f_i^{\mathfrak{B}}(h(a_1), \ldots, h(a_{n_i})) = f_i^{\mathfrak{B}}(h(b_1), \ldots, h(b_{n_i})) = h(f_i^{\mathfrak{A}}(b_1, \ldots, b_{n_i}))$, also ist $(f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i}), f_i^{\mathfrak{A}}(b_1, \ldots, b_{n_i})) \in \ker h$. Damit ist $\ker h$ invariant unter $\mathfrak{A}$ und da es sich offensichtlich um eine Äquivalenzrelation handelt, ist $\ker h$ eine Kongruenzrelation auf $\mathfrak{A}$. □

Satz 1.4.32 (Homomorphiesatz)**.** *Seien $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ und $\mathfrak{B} = (B, (f_i^{\mathfrak{B}})_{i\in I})$ zwei Algebren in derselben Signatur, $h : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus und sei $\varphi : \mathfrak{A} \to \mathfrak{A}/_{\ker h}$ die kanonische Faktorabbildung. Dann existiert genau ein Homomorphismus $\tilde{h} : \mathfrak{A}/_{\ker h} \to \mathfrak{B}$ mit $h = \tilde{h} \circ \varphi$. Dieser Homomorphismus ist injektiv und, falls h surjektiv ist, auch surjektiv.*

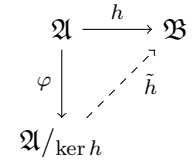

Abbildung 1.4: Visualisierung der Aussage des Homomorphiesatzes

Beweis. Für die Surjektivität von $\tilde{h}$ ist nichts zu zeigen. Der übrige Beweis ist in vier Schritte gegliedert.

Eindeutigkeit: Seien $\tilde{h}$ und $\hat{h}$ zwei Homomorphismen von $\mathfrak{A}/_{\ker h}$ nach $\mathfrak{B}$ mit den geforderten Eigenschaften. Dann gilt für $a \in A$ beliebig $\hat{h}([a]) = h(a) = \tilde{h}([a])$, also $\hat{h} = \tilde{h}$.

Existenz: Sei $[a] \in A/_{\ker h}$ beliebig und definiere $\tilde{h}([a]) := h(a)$. Diese Abbildung ist wohldefiniert, da aus $[a] = [b]$ laut Definition $h(a) = h(b)$ folgt, das heißt die Definition ist unabhängig von der Wahl des Repräsentanten.

[6] Für die Äquivalenzklassen einer Äquivalenzrelation wird häufig $[a]$ statt $[a]_\sim$ geschrieben.

[7] Dass diese Funktionen tatsächlich wohldefiniert sind, folgt direkt aus der Definition der Invaranz einer Kongruenzrelation unter der Algebra.

Homomorphismus: Sei $i \in I$ und seien $[a_1], \ldots, [a_{n_i}] \in A/_{\ker h}$ beliebig. Dann gilt laut Definition $\tilde{h}(f_i^{\mathfrak{A}/_{\ker h}}([a_1], \ldots, [a_{n_i}])) = \tilde{h}([f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})]) = h(f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})) = f_i^{\mathfrak{B}}(h(a_1), \ldots, h(a_{n_i})) = f_i^{\mathfrak{B}}(\tilde{h}([a_1]), \ldots, \tilde{h}([a_{n_i}]))$, also ist $\tilde{h}$ ein Homomorphismus.

Injektivität: Seien $[a], [b] \in A/_{\ker h}$ beliebig mit $\tilde{h}([a]) = \tilde{h}([b])$. Dann folgt laut Definition $h(a) = h(b)$, also $(a, b) \in \ker h$ und damit $[a] = [b]$. □

Proposition 1.4.33. *Seien $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i \in I})$ eine Algebra, $s \approx t$ ein Gesetz und gelte $\mathfrak{A} \models s \approx t$. Dann gilt für jede Faktoralgebra $\mathfrak{A}/_\sim \models s \approx t$.*

Beweis. Seien $x_1, \ldots, x_n$ Variablen mit $\operatorname{var}(s) \cup \operatorname{var}(t) \subseteq \{x_1, \ldots, x_n\}$ und seien $[a_1], \ldots, [a_n] \in A/_\sim$. Laut Voraussetzung gilt $s^{\mathfrak{A}}(a_1, \ldots, a_n) = t^{\mathfrak{A}}(a_1, \ldots, a_n)$, woraus $s^{\mathfrak{A}/_\sim}([a_1], \ldots, [a_n]) = [s^{\mathfrak{A}}(a_1, \ldots, a_n)] = [t^{\mathfrak{A}}(a,1 \ldots, a_n)] = t^{\mathfrak{A}/_\sim}([a_1], \ldots, [a_n])$ folgt. Inbesondere ist also $\mathfrak{A}/_\sim \models s \approx t$ erfüllt. □

Korollar 1.4.34. *Varietäten sind abgeschlossen unter der Bildung von Faktoralgebren.*

15.03.2023
16.03.2023

1.4.4 Der Satz von Birkhoff

Definition 1.4.35. Sei $\mathcal{K}$ eine Klasse von Algebren. Dann definieren wir:

- H$\mathcal{K}$ als die Klasse aller Algebren $\mathfrak{A}/_\sim$, wobei $\mathfrak{A} \in \mathcal{K}$ und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$ sind.
- S$\mathcal{K}$ als die Klasse aller Algebren $\mathfrak{A}'$, zu der es eine Algebra $\mathfrak{A} \in \mathcal{K}$ mit $\mathfrak{A}' \leq \mathfrak{A}$ gibt.
- P$\mathcal{K}$ als die Klasse aller Algebren $\prod_{j \in J} \mathfrak{A}_j$, wobei J eine beliebige Indexmenge und $\mathfrak{A}_j \in \mathcal{K}$ sind.

Wir sagen, dass $\mathcal{K}$ unter HSP abgeschlossen ist, wenn $\mathrm{H}\mathcal{K} = \mathcal{K}, \mathrm{S}\mathcal{K} = \mathcal{K}$ und $\mathrm{P}\mathcal{K} = \mathcal{K}$ gilt.

Satz 1.4.36 (Birkhoff)**.** *Sei $\tau = (f_i)_{i \in I}$ eine Signatur und $\mathcal{K}$ eine Klasse von τ-Algebren. Dann gilt:*

$$\mathcal{K} \textit{ ist abgeschlossen unter } \mathrm{HSP} \quad \Leftrightarrow \quad \mathcal{K} \textit{ ist eine Varietät}$$

Definition 1.4.37. Für eine Klasse $\mathcal{K}$ von Algebren sei die *Menge aller Gesetze von $\mathcal{K}$* definiert als

$$\Sigma(\mathcal{K}) := \{s \approx t \mid \forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx t\}.$$

Für eine einzelne Algebra $\mathfrak{A}$ sei die *Menge aller Gesetze von* $\mathfrak{A}$ definiert als

$$\Sigma(\mathfrak{A}) := \Sigma(\{\mathfrak{A}\}).$$

Beweis des Satzes von Birkhoff. Ist $\mathcal{K}$ eine Varietät, so ist $\mathcal{K}$ laut 1.4.5, 1.4.20 und 1.4.34 unter HSP abgeschlossen. Es bleibt die andere Implikation zu zeigen. Sei also $\mathcal{K}$ unter HSP abgeschlossen und definiere $\Sigma := \Sigma(\mathcal{K})$ und $\mathcal{V} := \mathcal{V}(\Sigma)$, womit $\mathcal{V} = \mathcal{K}$ zu zeigen ist. Trivialerweise ist $\mathcal{V} \supseteq \mathcal{K}$ erfüllt. Für die andere Inklusion sei $\mathfrak{A} \in \mathcal{V}$ beliebig, das heißt es gilt $\mathfrak{A} \in \mathcal{K}$ zu zeigen.

Für jedes Gesetz $s \approx t$, welches nicht in Σ liegt, wähle eine Algebra $\mathfrak{A}_{s \approx t} \in \mathcal{K}$ mit $\mathfrak{A}_{s \approx t} \not\models s \approx t$. Es sei $\mathfrak{B} := \prod_{s \approx t \notin \Sigma} \mathfrak{A}_{s \approx t}$. Da $\mathcal{K}$ unter Produktbildung abgeschlossen ist, gilt $\mathfrak{B} \in \mathcal{K}$. Da

eine Produktalgebra ein Gesetz genau dann erfüllt, wenn es komponentenweise erfüllt ist, folgt $\Sigma(\mathfrak{B}) = \Sigma \subseteq \Sigma(\mathfrak{A})$. Zu zeigen ist nun, dass $\mathfrak{A} \in \mathrm{HSP}\mathfrak{B}$.

Bilde die Produktalgebra $\mathfrak{B}^{B^A} = \prod_{i \in B^A} \mathfrak{B}$ und betrachte für alle $a \in A$ die Funktion $\pi_a : B^A \to B, \alpha \mapsto \alpha(a)$ sowie die erzeugte Unteralgebra $\mathfrak{S} := \langle \{\pi_a \mid a \in A\} \rangle \leq \mathfrak{B}^{B^A}$. Dann kann ein surjektiver Homomorphismus $\varphi : S \to A$ mit $\varphi(\pi_a) = a$ folgendermaßen definiert werden. Jedes Element aus S besitzt eine Darstellung der Form $t^{\mathfrak{S}}(\pi_{a_1}, \ldots, \pi_{a_n})$ mit $a_1 \ldots, a_n \in A$. Daher wird $\varphi(t^{\mathfrak{S}}(\pi_{a_1}, \ldots, \pi_{a_n})) := t^{\mathfrak{A}}(a_1, \ldots, a_n)$ definiert.

Wohldefiniertheit: Es ist zu zeigen, dass die Definition von φ unabhängig von der Wahl der Darstellung ist. Das heißt, wenn u, v beliebige Terme und $a_1, \ldots, a_n, a'_1, \ldots, a'_m \in A$ sind, sodass $u^{\mathfrak{S}}(\pi_{a_1}, \ldots, \pi_{a_n}) = v^{\mathfrak{S}}(\pi_{a'_1}, \ldots, \pi_{a'_m})$ gilt, dann soll auch $u^{\mathfrak{A}}(a_1, \ldots, a_n) = v^{\mathfrak{A}}(a'_1, \ldots, a'_m)$ gelten. Dafür werden $x_i := a_i$ und $x'_i := a_i$ als Variablen eingeführt. Es ist nun hinreichend zu zeigen, dass $\mathfrak{B} \models u(x_1, \ldots, x_n) \approx v(x'_1, \ldots, x'_m)$ gilt, da dieses Gesetz wegen $\Sigma(\mathfrak{B}) \subseteq \Sigma(\mathfrak{A})$ dann auch in $\mathfrak{A}$ gilt, was insbesondere $u^{\mathfrak{A}}(a_1, \ldots, a_n) = v^{\mathfrak{A}}(a'_1, \ldots, a'_m)$ bedingen würde. Sind $b_i, b'_i \in B$ beliebige Werte für die Variablen x_i respektive x'_i, so muss $u^{\mathfrak{B}}(b_1, \ldots, b_n) = v^{\mathfrak{B}}(b'_1, \ldots, b'_m)$ gezeigt werden. Nun kann $\alpha \in B^A$ mit $\alpha(a_i) = b_i$ und $\alpha(a'_i) = b'_i$ gewählt werden, da aus $x_i = a_i = a_j = x_j$ folgen würde, dass $b_i = b_j$ gelten muss. Das analoge Argument gilt auch in den Fällen $a_i = a'_j$ und $a'_i = a'_j$. Da voraussetzungsgemäß $u^{\mathfrak{S}}(\pi_{a_1}, \ldots, \pi_{a_n}) = v^{\mathfrak{S}}(\pi_{a'_1}, \ldots, \pi_{a'_m})$ erfüllt ist, gilt diese Gleichheit insbesondere wenn α als Argument eingesetzt wird. Dies liefert $u^{\mathfrak{B}}(b_1, \ldots, b_n) = u^{\mathfrak{S}}(\pi_{a_1}, \ldots, \pi_{a_n})(\alpha) = v^{\mathfrak{S}}(\pi_{a'_1}, \ldots, \pi_{a'_m})(\alpha) = v^{\mathfrak{B}}(b'_1, \ldots, b'_m)$, also was zu zeigen war.

Surjektivität: φ ist trivialerweise surjektiv, da für $a \in A$ stets $\pi_a \in S$ gilt und $\varphi(\pi_a) = a$ ist.

Homomorphismus: Es bleibt noch zu zeigen, dass φ ein Homomorphismus ist. Sei $i \in I$ beliebig und seien $g_1, \ldots, g_{n_i} \in S$ beliebig. Zu zeigen ist $\varphi(f_i^{\mathfrak{S}}(g_1, \ldots, g_{n_i})) = f_i^{\mathfrak{A}}(\varphi(g_1), \ldots, \varphi(g_{n_i}))$. Für jedes $j \in 1, \ldots, n$ können ein Term t_j sowie $a_1^{(j)}, \ldots, a_{m_j}^{(j)} \in A$ gewählt werden, sodass $g_j = t_j^{\mathfrak{S}}(\pi_{a_1^{(j)}}, \ldots, \pi_{a_{m_j}^{(j)}})$ gilt. Nun wird $t := f_i^{\mathfrak{T}}(t_1, \ldots, t_{n_i})$ als neuer Term definiert und es folgt

$$\begin{aligned}
\varphi(f_i^{\mathfrak{S}}(g_1, \ldots, g_{n_i})) &= \varphi(f_i^{\mathfrak{S}}(t_1^{\mathfrak{S}}(\pi_{a_1^{(1)}}, \ldots, \pi_{a_{m_1}^{(1)}}), \ldots, t_{n_i}^{\mathfrak{S}}(\pi_{a_1^{(n_i)}}, \ldots, \pi_{a_{m_{n_i}}^{(n_i)}}))) = \\
&= \varphi(t^{\mathfrak{S}}(\pi_{a_1^{(1)}}, \ldots, \pi_{a_{m_{n_i}}^{(n_i)}})) \overset{(*)}{=} t^{\mathfrak{A}}(a_1^{(1)}, \ldots, a_{m_{n_i}}^{(n_i)}) = \\
&= f_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}(a_1^{(1)}, \ldots, a_{m_1}^{(1)}), \ldots, t^{\mathfrak{A}}(a_1^{n_i}, \ldots, a_{m_{n_i}}^{(n_i)})) \overset{(*)}{=} f_i^{\mathfrak{A}}(\varphi(g_1), \ldots, \varphi(g_{n_i})).
\end{aligned}$$

An den Stellen die mit $(*)$ markiert sind, wurde die Definition von φ verwendet.

Mit dem Homomorphiesatz erhalten wir damit einen Isomorphismus $\tilde{\varphi} : \mathfrak{S}/_{\ker \varphi} \to \mathfrak{A}$. Damit ist $\mathfrak{A}$ isomorph zu einer Faktoralgebra, welche durch HSP aus $\mathfrak{B}$ hervorgeht, was zu zeigen war. □

Korollar 1.4.38. *Sei $\mathcal{K}$ eine Klasse von Algebren und $\mathcal{V}(\Sigma(\mathcal{K}))$ die erzeugte Varietät. Dann gilt für alle Algebren $\mathfrak{A}$*

$$\mathfrak{A} \in \mathcal{V}(\Sigma(\mathcal{K})) \quad \Leftrightarrow \quad \mathfrak{A} \in \mathrm{HSP}\mathcal{K}.$$

Beweis. Die Implikation von rechts nach links ist trivialerweise erfüllt. Die Implikation von links nach rechts folgt aus der Tatsache, dass man, wie im Beweis des Satzes von Birkhoff, $\mathfrak{B} \in P(\mathcal{K})$ mit $\Sigma(\mathfrak{A}) \supseteq \Sigma(\mathfrak{B})$ finden kann und auf $\mathfrak{A} \in \mathrm{HSP}\mathfrak{B} \subseteq \mathrm{HSP}\mathcal{K}$ schließt. □

1.5 Freie Algebren

Definition 1.5.1. Sei $\tau = (n_i)_{i\in I}$, $\mathcal{K}$ eine Klasse von τ-Algebren, $\mathfrak{F} \in K$ und $X \subseteq F$. Dann heißt $\mathfrak{F}$ *frei über X in $\mathcal{K}$*, wenn es für alle $\mathfrak{A} \in \mathcal{K}$ und alle $\varphi : X \to A$ genau einen Homomorphismus $\overline{\varphi} : \mathfrak{F} \to \mathfrak{A}$ mit $\overline{\varphi}|_X = \varphi$ gibt.

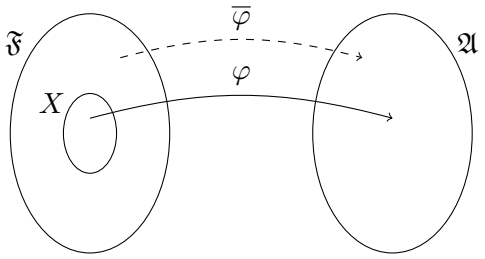

Abbildung 1.5: $\mathfrak{F}$ frei über X

Beispiel 1.5.2. Sei $\mathcal{K}$ die Klasse der Vektorräume über dem Körper $\mathbb{C}$, $\mathfrak{V} \in \mathcal{K}$ beliebig und $X \subseteq V$ eine Basis von $\mathfrak{V}$. Dann ist $\mathfrak{V}$ frei über X in $\mathcal{K}$.

Mit einer Variablenmenge X ist die Termalgebra $\mathfrak{T}(X, (f_i)_{i\in I})$ frei über X in der Klasse aller τ-Algebren.

Beispiel 1.5.3. Sei $\mathcal{K}$ eine Varietät definiert durch Gesetze Σ, also $\mathcal{K} = \{\mathfrak{A} \mid \mathfrak{A} \models \Sigma\}$. Sei $\mathfrak{B} \in \mathcal{K}$ so, dass $\Sigma(\mathfrak{B}) = \Sigma$ – nach dem Beweis des Satzes von Birkhoff wissen wir, dass ein solches $\mathfrak{B}$ existiert! Sei

$$\mathfrak{S} \leq \mathfrak{B}^{B^X}, \quad S := \langle \{\pi_x \mid x \in X\} \rangle,$$

so ist $\mathfrak{S}$ frei über $\{\pi_x \mid x \in X\}$ in $\mathcal{K}$.

Proposition 1.5.4. *Sei $\mathcal{K}$ eine Varietät, $\mathfrak{F}_1, \mathfrak{F}_2 \in \mathcal{K}$ frei über X in $\mathcal{K}$, dann ist $\mathfrak{F}_1 \cong \mathfrak{F}_2$.*

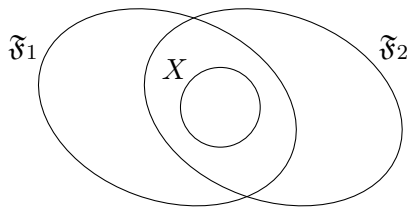

Abbildung 1.6: $\mathfrak{F}_1, \mathfrak{F}_2$ frei über X

Beweis. Betrachten wir $\mathrm{id}_X : X \to X$, so gibt es eindeutige Homomorphismen $\varphi : \mathfrak{F}_1 \to \mathfrak{F}_2, \psi : \mathfrak{F}_2 \to \mathfrak{F}_1$ mit $\varphi|_X = \mathrm{id}_X, \psi|_X = \mathrm{id}_X$. Es ist dann $\psi \circ \varphi : \mathfrak{F}_1 \to \mathfrak{F}_1$ ein Homomorphismus mit $(\psi \circ \varphi)|_X = \mathrm{id}_X$. Da $\mathfrak{F}_1$ frei über X ist gilt $\psi \circ \varphi = \mathrm{id}_{F_1}$, womit ψ surjektiv und φ injektiv ist. Analog folgt, dass ψ injektiv und φ surjektiv ist, womit φ, ψ Isomorphismen mit $\varphi = \psi^{-1}$ sind. □

16.03.2023
22.03.2023

Proposition 1.5.5. *Sei $\mathcal{K}$ eine Klasse von Algebren mit Typ $(n_i)_{i\in I} =: \tau$. Sei*

$$\mathcal{S}(\mathcal{K}) := \{\mathfrak{A} \mid \exists \mathfrak{B} \in \mathcal{K} : \mathfrak{A} \leq \mathfrak{B}\} \subseteq \mathcal{K},$$

was insbesondere der Fall ist, falls $\mathcal{K}$ eine Varietät ist. Sei $\mathfrak{F}$ in $\mathcal{K}$ frei über $X \subseteq F$, so ist $\mathfrak{F} = \langle X \rangle$.

Beweis. Zunächst gilt $\langle X\rangle \leq \mathfrak{F} \in \mathcal{K}$, und damit auch $\langle X\rangle \in \mathcal{K}$.

Nun ist $\langle X\rangle$ frei über X in $\mathcal{K}$. Um dies einzusehen, seien $\mathfrak{A} \in \mathcal{K}, \varphi : X \to A$ beliebig. Zu zeigen ist, dass es einen eindeutigen, φ fortsetzenden Homomorphismus $\overline{\varphi} : \langle X\rangle \to \mathfrak{A}$ gibt mit $\overline{\varphi}|_X = \varphi$. Wir wissen es gibt einen eindeutigen Homomorphismus $\overline{\overline{\varphi}} : F \to A$ mit $\overline{\overline{\varphi}}|_X = \varphi$. Definiere $\overline{\varphi} := \overline{\overline{\varphi}}|_{\langle X\rangle}$, so erfüllt dieser Homomorphismus die geforderte Eigenschaft. Die Eindeutigkeit folgt aus Bemerkung 1.5.6.

Betrachte $\mathrm{id}_X : (X \subseteq \langle X\rangle) \to (X \subseteq F)$, so gibt es eindeutige Fortsetzungen

$$\varphi : \langle X\rangle \to \mathfrak{F}, \quad \varphi|_X = \mathrm{id}_X, \qquad \psi : \mathfrak{F} \to \langle X\rangle, \quad \psi|_X = \mathrm{id}_X,$$

womit auch $\psi \circ \varphi : \langle X\rangle \to \langle X\rangle$ ein Homomorphismus mit $(\psi \circ \varphi)|_X = \mathrm{id}_X$ ist. Mit der Eindeutigkeit folgt $\psi \circ \varphi = \mathrm{id}_{\langle X\rangle}$ und analog damit auch $\varphi \circ \psi = \mathrm{id}_F$.

Nun sind φ, ψ bijektiv, also Isomorphismen. Betrachte nochmals $\varphi : \langle X\rangle \to F, \varphi|_X = \mathrm{id}_X$ und sei $c \in \langle X\rangle$ beliebig, so gilt $c = t^{\langle X\rangle}(x_1, ..., x_n)$ mit $x_1, ..., x_n \in X$. Es folgt

$$\varphi(c) = \varphi(t^{\langle X\rangle}(x_1, ..., x_n)) = t^{\langle X\rangle}(\varphi(x_1), ..., \varphi(x_n)) = t^{\langle X\rangle}(x_1, ..., x_n) = c,$$

also $\varphi = \mathrm{id}_{\langle X\rangle}$. Da φ surjektiv ist folgt damit $\langle X\rangle = F$. □

Bemerkung 1.5.6. Allgemein gilt, dass zwei Homomorphismen übereinstimmen, wenn sie das auf einem Erzeuger tun. Sind also $\mathfrak{C}, \mathfrak{D}$ Algebren, $C = \langle S\rangle$ und $\varphi, \psi : \mathfrak{C} \to \mathfrak{D}$ Homomorphismen mit $\varphi|_S = \psi|_S$, so folgt $\varphi = \psi$.

Bemerkung 1.5.7. Wir wollen die freie Algebra als Faktoralgebra der Termalgebra darstellen. Sei dazu $\tau := (n_i)_{i\in I}$ eine Signatur und X eine Menge, so ist

$$\mathfrak{T}^X := \mathfrak{T}(X, (f_i^{\mathfrak{T}})_{i\in I})$$

frei über X in der Klasse der τ-Algebren.

Sei $\mathcal{K}$ eine Varietät von τ-Algebren, so stellt sich die Frage ob $\mathfrak{T}^X$ frei über X in $\mathcal{K}$ ist. Allgemein ist dies nicht der Fall, da $\mathfrak{T}^X$ nicht in $\mathcal{K}$ enthalten sein muss.

Proposition 1.5.8. *Sei $\mathcal{K}$ eine Varietät und definiere*

$$\Sigma_X := \{(s,t) \mid s,t \in T(X), \forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx t\} \subseteq T(X)^2,$$

so ist Σ_X eine Kongruenzrelation auf $T(X)$.

Beweis. Σ_X ist Äquivalenzrelation:

- reflexiv: Ist $t \in T(X)$ beliebig, so gilt $\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models t \approx t$.
- symmetrisch: Sind $s, t \in T(X), (s,t) \in \Sigma_X$, so gilt

  $$\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx t \quad \Longrightarrow \quad \forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models t \approx s,$$

  also $(t,s) \in \Sigma_X$.
- transitiv: Sind $s, t, u \in T(X), (s,t), (t,u) \in \Sigma_X$, so gilt

  $$(\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx t \quad \wedge \quad \forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models t \approx u) \quad \Longrightarrow \quad \forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx u,$$

  also $(s,u) \in \Sigma_X$.

Um zu sehen, dass Σ_X auch eine Kongruenzrelation ist, seien $i \in I, (s_1, t_1), ..., (s_{n_i}, t_{n_i}) \in \Sigma_X$. Zu zeigen ist $(f_i(s_1, ..., s_{n_i}), f_i(t_1, ..., t_{n_i})) \in \Sigma_X$. Es gilt

$$\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s_1 \approx t_1 \wedge ... \wedge s_{n_i} \approx t_{n_i},$$

insbesondere folgt also

$$\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models f_i(s_1, ..., s_{n_i}) \approx f_i(t_1, ..., t_{n_i})$$

und damit $(f_i(s_1, ..., s_{n_i}), f_i(t_1, ..., t_{n_i})) \in \Sigma_X$. □

Definition 1.5.9. Wir definieren $\mathfrak{T}^{X,\Sigma_X} := \mathfrak{T}^X/_{\Sigma_X}$.

Satz 1.5.10. *$\mathfrak{T}^{X,\Sigma_X}$ ist frei über X in $\mathcal{K}$.*

Beweis. Sei $\mathfrak{B} \in \mathcal{K}$ mit $\Sigma(\mathfrak{B}) = \Sigma(\mathcal{K})$, wobei wir die Existenz aus dem Beweis des Satzes von Birkhoff wissen.

Sei $\langle \{\pi_x \mid x \in X\} \rangle =: \mathfrak{S} \leq \mathfrak{B}^{B^X}$, wobei $\pi_x : B^X \to B, \alpha \mapsto \alpha(x)$ (wie im Beweis des Satzes von Birkhoff), so wissen wir, dass $\mathfrak{S}$ frei über $\{\pi_x \mid x \in X\}$ in $\mathcal{K}$ ist.

Betrachte

$$\varphi : \mathfrak{S} \to \mathfrak{T}^{X,\Sigma_X}, t^{\mathfrak{S}}(\pi_{x_1}, ..., \pi_{x_n}) \mapsto [t(x_1, ..., x_n)]_{\Sigma_X}.$$

Zunächst ist φ wohldefiniert: Seien dazu $u, v \in T(X)$ mit $u^{\mathfrak{S}}(\pi_{x_1}, ..., \pi_{x_n}) = v^{\mathfrak{S}}(\pi_{x'_1}, ..., \pi_{x'_m})$, so gilt für alle $\mathfrak{A} \in \mathcal{K}$, dass $\mathfrak{A} \models u(x_1, ..., x_n) \approx v(x'_1, ..., x'_m)$, womit $(u(x_1, ..., x_n), v(x'_1, ..., x'_m)) \in \Sigma_X$ und damit $[u(x_1, ..., x_n)]_{\Sigma_X} = [v(x'_1, ..., x'_m)]_{\Sigma_X}$ folgt.

Weiters ist φ surjektiv, da mit beliebigem $[t(x_1, ..., x_n)]_{\Sigma_X} \in \mathfrak{T}^{X,\Sigma_X}$ sofort
$t^{\mathfrak{S}}(\pi_{x_1}, ..., \pi_{x_n}) \overset{\varphi}{\mapsto} [t(x_1, ..., x_n)]_{\Sigma_X}$ gilt.

Um einzusehen, dass φ injektiv ist seien $u, v \in T(X)$ mit $[u(x_1, ..., x_n)]_{\Sigma_X} = [v(x'_1, ..., x'_m)]_{\Sigma_X}$ beliebig, so gilt für alle $\mathfrak{A} \in \mathcal{K}$, dass $\mathfrak{A} \models u(x_1, ..., x_n) \approx v(x'_1, ..., x'_m)$. Inbesondere gilt $\mathfrak{S} \models u(x_1, ..., x_n) \approx v(x'_1, ..., x'_m)$ und damit $u^{\mathfrak{S}}(\pi_{x_1}, ..., \pi_{x_n}) = v^{\mathfrak{S}}(\pi_{x'_1}, ..., \pi_{x'_m})$.

Dass φ ein Homomorphismus ist verifiziert man unmittelbar in Analogie zum Beweis des Satzes von Birkhoff. Damit ist φ insgesamt also ein Isomorphismus, $\mathfrak{S} \cong \mathfrak{T}^{X,\Sigma_X}$, womit $\mathfrak{T}^{X,\Sigma_X}$ frei über $\{[x]_{\Sigma_X} \mid x \in X\}$ ist. □

22.03.2023
23.03.2023

Definition 1.5.11. Sei $(H, \cdot)$ eine Halbgruppe und $a \in H$. Dann wird für $n \in \mathbb{N}$ rekursiv definiert:

$$a^1 := a, \quad a^{n+1} := a \cdot a^n.$$

Falls[8] es ein neutrales Element e gibt, so wird $a^0 := e$ definiert und im Fall, dass a ein inverses Element a^* besitzt wird rekursiv definiert:

$$a^{-1} := a^*, \quad a^{-(n+1)} := a^* \cdot a^{-n}.$$

[8] Insbesondere sind diese Notationen für Monoide und Gruppen definiert.

Beispiel 1.5.12. Bezeichne $(\cdot, e, ^{-1})$ vom Typ $\tau = (2, 0, 1)$ die Sprache der Gruppen. Sei $X = \{x_1, x_2, ...\}$ eine Variablenmenge so sind

$$\left.\begin{array}{c} x_1, x_2, x_3, ... \\ e, x_1 \cdot x_2, x_2 \cdot x_1, x_1^{-1}, ... \\ e \cdot x_1, x_1 \cdot e, (x_1 \cdot x_2) \cdot x_3, x_1 \cdot (x_2 \cdot x_3), ... \\ \vdots \end{array}\right\} \quad \begin{array}{c}(T(X), .^{\mathfrak{T}}, e^{\mathfrak{T}}, {}^{-1^{\mathfrak{T}}}) \text{ ist frei über} \\ X \text{ in der Klasse aller } \tau\text{-Algebren.}\end{array}$$

Beispiele für Terme respektiver 1., 2. und 3. Stufe. Bezeichne nun

$$\Sigma_X = \{(e \cdot x_1, x_1), ((x_1 \cdot x_2) \cdot x_3, x_1 \cdot (x_2 \cdot x_3)), (e, x_1 \cdot x_1^{-1}), ...\}$$

die Menge aller Gesetze welche in allen Gruppen gelten. Faktorisieren wir nun nach Termäquivalenz, so erhalten wir

$$T(X)/_{\Sigma_X} = \{[e], [x_1], [x_2], ..., [x_1 \cdot x_2], [x_2 \cdot x_1], ...\}.$$

Jedes Element t von $T(X)/_{\Sigma_X}$ (außer $[e]$) hat also einen Repräsentanten der Form $a_1 \cdot a_2 \cdot ... \cdot a_n$, wobei $a_i = x_j$ oder $a_i = x_j^{-1}$ für ein j, aber nie x_j und x_j^{-1} aufeinanderfolgen oder umgekehrt. Mit Hilfe von Definition 1.5.11 können diese Repräsentanten auch als $x_{j_1}^{n_1} \cdots x_{j_m}^{n_m}$ mit $n_1, \ldots, n_m \in \mathbb{Z}$ und $x_{j_i} \neq x_{j_{i+1}}$ für $i \in \{1, \ldots, m-1\}$ geschrieben werden.

Bemerkung 1.5.13. Ist $(G, \cdot, e, ^{-1})$ eine Gruppe so gilt $\forall m, n \in \mathbb{Z} \forall a \in G : a^m \cdot a^n = a^{m+n}$ und $(a^m)^n = a^{m \cdot n}$. Falls $\cdot$ kommutativ ist, gilt weiters $\forall a, b \in G \forall m \in \mathbb{Z} : (a \cdot b)^m = a^m \cdot b^m$.

Beispiel 1.5.14. Es sei $(\cdot, e, ^{-1})$ die Sprache der Gruppen und $X = \{x_1, x_2, \ldots\}$ eine Variablenmenge. Ausgehend von Beispiel 1.5.12 kann analog die freie kommutative Gruppe über X in der Klasse aller kommutativen Gruppen konstruiert werden. Jedes Element der Termalgebra besitzt dann einen Repräsentanten der Form $x_{i_1}^{m_1}, \ldots, x_{i_k}^{m_k}$ mit $m_1, \ldots, m_k \in \mathbb{Z}$ und $\forall j, \ell \in \{1, \ldots, k\} : j < \ell \Rightarrow i_j < i_\ell$.

Beispiel 1.5.15. Betrachten wir die freie Gruppe über der einelementigen Menge $X = \{x\}$, so können alle Elemente durch x^n für $n \in \mathbb{N}$ repräsentiert werden. Außerdem gilt für $m, n \in \mathbb{Z}$: $x^m \cdot x^n = x^{m+n}$. Das bedeutet, dass diese freie Gruppe isomorph zu $(\mathbb{Z}, +, 0, -)$ ist, vermöge dem Isomorphismus $\varphi : \{x^n \mid n \in \mathbb{Z}\} \to \mathbb{Z}, x^n \mapsto n$.

Beispiel 1.5.16. In Analogie zum letzten Beispiel kann auch die freie kommutative Gruppe über der Menge $X = \{x, y\}$ klassifiziert werden. Ihre Elemente besitzen eindeutige Repräsentanten der Form $x^{n_1} \cdot y^{n_2}$ mit $n_1, \ldots, n_2 \in \mathbb{Z}$. Die Identität $(x^{n_1} \cdot y^{n_2}) \cdot (x^{m_1} \cdot x^{m_2}) = (x^{n_1+m_1} \cdot y^{n_2+m_2})$ begründet die Isomorphie zur Gruppe $(\mathbb{Z}, +, 0, -)^2$ vermöge der Abbildung $\varphi : \{x^{n_1} \cdot y^{n_2} \mid (n_1, n_2) \in \mathbb{Z}^2\} \to \mathbb{Z}^2, x^{n_1} \cdot y^{n_2} \mapsto (n_1, n_2)$.

Beispiel 1.5.17. Es sei $\mathfrak{K}$ ein Körper und $(+, 0, -, (m_r)_{r \in \mathfrak{K}})$ die Sprache der Vektorräume und $\tau = (2, 0, 1,)$. Sei $X = \{x_1, x_2, \ldots\}$ eine Variablenmenge so sind

$$\left.\begin{array}{c} x_1, x_2, x_3, ... \\ 0, x_1 + x_2, x_2 + x_1, r \odot x_1, -x_1, ... \\ 0 + x_1, r \odot (x_1 + x_2), (r \odot x_1) + (r \odot x_2), ... \\ \vdots \end{array}\right\} \quad \begin{array}{c}(T(X), +^{\mathfrak{T}}, 0^{\mathfrak{T}}, -^{\mathfrak{T}}, (m_r^{\mathfrak{T}})_{r \in \mathfrak{K}}) \text{ ist frei über} \\ X \text{ in der Klasse aller } \tau\text{-Algebren.}\end{array}$$

Beispiele für Terme respektiver 1., 2. und 3. Stufe. Bezeichne nun

$$\Sigma_X = \{(0 + x_1, x_1), (r \odot (x_1 + x_2), (r \odot x_1) + (r \odot x_2)), ((r \cdot s) \odot x_1, r \odot (s \odot x_1)), ...\}$$

die Menge aller Gesetze welche in allen Vektorräumen gelten. Faktorisieren wir nun nach Termäquivalenz, so erhalten wir

$$T(X)/_{\Sigma_X} = \{[x_1], [x_2], ..., [c_1 \odot x_1 + c_2 \odot x_2], ...\}.$$

Jedes Element t von $T(X)/_{\Sigma_X}$ hat also einen Repräsentanten der Form $c_1 \odot x_{i_1} + \ldots + c_n \odot x_{i_n}$ mit $\forall j, k \in \{1, \ldots, n\} : i < j \Rightarrow i_j < i_k$. Man kann daher $[x_1], [x_2], \ldots$ als Basis des freien Vektorraumes über die Menge X[9] sehen.

[9] Hier bezieht sich das "über die Menge X" auf die Freiheit und nicht auf den zugrundeliegenden Körper. Der Vektorraum ist weiterhin ein Vektorraum über den Körper $\mathfrak{K}$.

Kapitel 2

Elementare Strukturentheorie

Dieses Kapitel behandelt die Inhalte der Vorlesung, welche auch in Goldstern et al.: *Algebra – Eine grundlagenorientierte Einführunsvorlesung* in dem Kapitel *3. Elementare Strukturtheorien* gefunden werden können.

2.1 Halbgruppen und Monoide

Dieses Kapitel beschäftigt sich mit elementaren Aussagen zu Halbgruppen und Monoiden. Wesentliche Resultate davon sind der Darstellungssatz von Cayley für Monoide 2.1.10, der Fundamentalsatz der Arithmetik 2.1.11 und Satz 2.1.18.

Zu Beginn wollen wir auf die Definitionen 1.1.4, 1.1.6 und 2.2.1 hinweisen, die die im Folgenden verwendeten Begriffe *Halbgruppe*, *Monoid*, *neutrales Element* und *inverses Element* definieren.

Beispiel 2.1.1. Für eine beliebige Menge M ist die Menge aller Funktionen von M nach M mit der Verkettung eine Halbgruppe $\mathfrak{H} = (M^M, \circ)$.

Definition 2.1.2. Sei $\mathfrak{M} = (M, \cdot, e)$ ein Monoid und $a, a' \in M$, dann heißt

- a' *linksinvers* zu a, wenn $a' \cdot a = e$ und
- a' *rechtsinvers* zu a, wenn $a \cdot a' = e$ gilt.

Ist a' links- und rechtsinvers zu a so nennt man a' *invers* zu a und a heißt *Einheit*.

Lemma 2.1.3. *Neutrale und inverse Elemente auf Halbgruppen sind eindeutig.*

Beweis. Beginnen wir mit der Eindeutigkeit von neutralen Elementen. Sei $\mathfrak{H} = (H, \cdot)$ eine Halbgruppe und seien $e, e' \in H$ neutrale Elemente. Dann gilt $e = e \cdot e' = e'$.

Es bleibt noch die Eindeutigkeit von inversen Elementen zu zeigen. Sei $\mathfrak{M} = (M, \cdot, e)$ ein Monoid und seien $a, a', a'' \in M$, wobei a' sowie a'' invers zu a. Wir erhalten dann $a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''$. □

Bemerkung 2.1.4. Da in einem Monoid $\mathfrak{M} = (M, \cdot, e)$ immer $e \cdot e = e$ gilt, also e zu sich selbst invers ist, ist e immer eine Einheit. Seien $G := \{a \in M \mid a \text{ ist Einheit von } \mathfrak{M}\}$ und $^{-1} : G \to G$ die Abbildung, die jedem Element sein inverses Element zuordnet, dann ist $\mathfrak{G} = (G, \cdot, e, ^{-1})$ eine Gruppe.

Beispiel 2.1.5. $\mathfrak{H} = (\mathbb{R}^{2\times 2}, \cdot)$ ist eine Halbgruppe. Die Einheitsmatrix $I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist ein neutrales Element, womit $(\mathbb{R}^{2\times 2}, \cdot, I_2)$ ein Monoid ist. Die Menge der invertierbaren reellen 2×2 Matrizen ist die Menge aller Einheiten von $\mathfrak{H}$.

Proposition 2.1.6. *Sei $(H, \cdot)$ eine Halbgruppe und $e \notin H$. Wir definieren $H' := H \cup \{e\}$ und*

$$\bar{\cdot} : (H')^2 \to H', (h_1, h_2) \mapsto \begin{cases} h_1 \cdot h_2, & \text{wenn } h_1, h_2 \in H, \\ h_1, & \text{wenn } h_1 = e, \\ h_2, & \text{sonst.} \end{cases}$$

Dann ist $(H', \bar{\cdot}, e)$ ein Monoid und es gilt $\bar{\cdot}|_{H^2} = \cdot$.

Bemerkung 2.1.7. Die einfach nachzurechnende Proposition 2.1.6 liefert eine einfache Möglichkeit eine Halbgruppe zu einem Monoid zu ergänzen. Sie ist der Grund, warum sich die Theorien von Halbgruppen und Monoiden sehr ähnlich sind.

Bemerkung 2.1.8. Betrachten wir das freie Monoid über $X^{(1)} = \{x_1\}$. Wir erhalten damit x_1 als einzigen Term 0-ter Stufe, $e, x_1 \cdot x_1$ als Terme 1-ter Stufe, $e \cdot x_1, (x_1 \cdot x_1), \ldots$ als Terme 2-ter Stufe etc. Nach Faktorisieren wie in Satz 1.5.10 erhalten wir die Repräsentanten $e, x_1, x_1^2, x_1^3, \ldots$, womit klarerweise das hier erhaltene freie Monoid kommutativ ist. Da Monoide i. A. aber nicht kommutativ sind, erhalten wir, dass freie Algebren mehr Gesetze erfüllen können, als in der gesamten Varietät gelten.

Betrachten wir allerdings das freie Monoid über $X^{(2)} = \{x_1, x_2\}$, so ist dieses nicht mehr kommutativ, also "freier" als das über $X^{(1)}$.

Ist der Generator (die Variablenmenge) X mindestens abzählbar unendlich, so ist das erzeugte Monoid *total frei* über X, also es gelten genau die Gesetze, die in der Varietät gelten.

Bemerkung 2.1.9. Aus der vorherigen Bemerkung erhalten wir die folgende Beobachtung:

Ist $\mathcal{K}$ eine Varietät, $\mathfrak{F}$ frei über X in $\mathcal{K}$, dann gilt

$$\forall s, t \in T(X) : \mathfrak{F} \models s \approx t \Leftrightarrow (\forall \mathfrak{A} \in \mathcal{K} : \mathfrak{A} \models s \approx t) .$$

Ist allerdings $Y \supsetneq X$ und sind $s, t \in T(Y)$, so erhalten wir keine ähnliche Aussage über $\mathfrak{F} \models s \approx t$.

Satz 2.1.10 (Darstellungssatz von Cayley für Monoide)**.** *Sei $\mathfrak{M} = (M, \cdot, e)$ ein Monoid, so existiert ein injektiver Homomorphismus $\varphi : \mathfrak{M} \to (M^M, \circ, \mathrm{id}_M)$.*

Beweis. Wähle für $a \in M$ die Funktion $f_a : M \to M, b \mapsto a \cdot b$ und sei $\varphi : M \to M^M, a \mapsto f_a$. Zeigen wir nun, dass φ ein injektiver Homomorphismus von $\mathfrak{M}$ nach $(M^M, \circ, \mathrm{id}_M)$ ist. Seien $a_1, a_2 \in M$, so gilt

$$\varphi(a_1 \cdot a_2) = f_{a_1 \cdot a_2} = (M \to M, b \mapsto a_1 \cdot a_2 \cdot b) = f_{a_1} \circ f_{a_2} = \varphi(a_1) \circ \varphi(a_2)$$

und es ist $\varphi(e) = f_e = \mathrm{id}_M$. Damit ist φ mit den Operationen verträglich, also ein Homomorphismus. Bleibt noch die Injektivität zu zeigen. Sei angenommen $\varphi(a_1) = \varphi(a_2)$, dann folgt daraus $a_1 = a_1 \cdot e = f_{a_1}(e) = f_{a_2}(e) = a_2 \cdot e = a_2$, womit φ injektiv ist. □

Satz 2.1.11 (Fundamentalsatz der Arithmetik)**.** *Sei $\mathfrak{S} = (S, +^{\mathfrak{S}}, 0^{\mathfrak{S}}) \leq \prod_{p \in \mathbb{P}} (\mathbb{N}, +, 0)$ definiert durch*

$$S = \{(s_p)_{p \in \mathbb{P}} \in \prod_{p \in \mathbb{P}} \mathbb{N} \mid s_p = 0 \text{ für fast alle } p \in \mathbb{P}\},$$

dann ist $\mathfrak{S} \cong (\mathbb{N} \setminus \{0\}, \cdot, 1)$.

Beweis. Definieren wir $\varphi : S \to \mathbb{N}, (s_p)_{p \in \mathbb{P}} \mapsto \prod_{p \in \mathbb{P}} p^{s_p}$ und zeigen, dass dieses φ ein Isomorphismus ist.

– φ ist wohldefiniert, da für fast alle $p \in \mathbb{P} : s_p = 0$ ist und φ damit nur auf endliche Produkte abbildet.

– Homomorphismus: Seien $(s_p)_{p\in\mathbb{P}}, (t_p)_{p\in\mathbb{P}} \in S$. Dann erhalten wir $\varphi((s_p)_{p\in\mathbb{P}} +^{\mathfrak{S}} (t_p)_{p\in\mathbb{P}}) = \prod_{p\in\mathbb{P}} p^{s_p+t_p} = \prod_{p\in\mathbb{P}} p^{s_p} \cdot \prod_{p\in\mathbb{P}} p^{t_p}$.

– Surjektivität: Zeigen wir mittel Induktion nach n die Existenz eines Elements $\mathbf{s}$ aus S, sodass $\varphi(\mathbf{s}) = n$.

Induktionsanfang ($n = 1$): Es ist $n = \varphi(0^{\mathfrak{S}})$.

Induktionsschritt ($k < n \implies n$): Ist $n \in \mathbb{P}$, so kann $\mathbf{s} = (\delta_{n,p})_{p\in\mathbb{P}}$ gewählt werden und damit ist $\varphi(\mathbf{s}) = p$. Betrachten wir nun noch den Fall $p \notin \mathbb{P}$. Wir wissen, dass es $i, j \leq n$ gibt, sodass $i \cdot j = n$. Nach der Induktionsvoraussetzung existieren $\mathbf{s}^{(i)}, \mathbf{s}^{(j)} \in S$ mit $\varphi(\mathbf{s}^{(i)}) = i$ und $\varphi(\mathbf{s}^{(j)}) = j$. Sei $\mathbf{s} := \mathbf{s}^{(i)} + \mathbf{s}^{(j)}$, dann gilt $\varphi(\mathbf{s}) = \varphi(\mathbf{s}^{(i)} + \mathbf{s}^{(j)}) = \varphi(\mathbf{s}^{(i)}) \cdot \varphi(\mathbf{s}^{(j)}) = i \cdot j = n$, weil φ ein Homomorphismus ist.

23.03.2023
29.03.2023

– Injektivität: Zu zeigen ist, dass es für alle $n \in \mathbb{N}\backslash\{0\}$ höchstens eine Primfaktorenzerlegung gibt. Wir wenden Induktion nach n an:

Induktionsanfang ($n = 1$): Klarerweise hat 1 nur die "triviale" Primfaktorenzerlegung, nämlich $0 \in S$, da jedes andere Produkt echt größer als 1 ist.

Induktionsschritt ($k < n \implies n$): Sei indirekt angenommen n hätte zwei Zerlegungen $n = p_1 \cdot ... \cdot p_e = q_1 \cdot ... \cdot q_m$, wobei $p_i, q_i \in \mathbb{P}$. Gibt es nun i, j mit $p_i = q_j$, so betrachten wir

$$\frac{n}{p_i} = p_1 \cdot ... \cdot p_{i-1} \cdot p_{i+1} \cdot ... \cdot p_\ell = q_1 \cdot ... \cdot q_{j-1} \cdot q_{j+1} \cdot ... \cdot q_m,$$

womit folgt, dass die Zerlegungen bereits gleich sind (bis auf Reihenfolge). Damit können wir von nun an annehmen, dass $p_i \neq q_j$ für alle i, j gilt – o. B. d. A. sei $p_1 < q_1$. Wir betrachten

$$n' := q_1 \cdot ... \cdot q_m - p_1 \cdot q_2 \cdot ... \cdot q_m < n,$$

so gilt insbesondere

$$n' = p_1 \cdot ... \cdot p_\ell - p_1 \cdot q_2 \cdot ... \cdot q_m$$

und damit $p_1 \mid n'$. Jedoch gilt $p_1 \nmid q_1 - p_1$, da $q_1 \in \mathbb{P}$. Zerlegen wir nun

$$q_1 - p_1 = r_1 \cdot ... \cdot r_s$$

in Primfaktoren, so erhalten wir

$$n' = (q_1 - p_1) \cdot q_2 \cdot ... \cdot q_m = r_1 \cdot ... \cdot r_s \cdot q_2 \cdot ... \cdot q_m$$

eine Primfaktorenzerlegung von n', wobei für alle i $r_i \neq p_1, q_i \neq p_1$. Damit haben wir zwei verschiedene Primfaktorenzerlegungen von $n' < n$, im Widerspruch zu unserer Induktionsvoraussetzung.

□

Bemerkung 2.1.12. Betrachte nochmals den obigen Isomorphismus φ. Es ist $(\mathbb{N}, \leq)$ eine Totalordnung, also eine Halbordnung in der für alle x, y entweder $x \leq y$ oder $y \leq x$ gilt.

Wir definieren nun eine Halbordnung auf S durch

$$f \leq g :\Leftrightarrow \forall p \in \mathbb{P} : f(p) \leq g(p).$$

Mit

$$f \vee g := (p \mapsto \max(f(p), g(p))),$$
$$f \wedge g := (p \mapsto \min(f(p), g(p)))$$

wird S also zu einem Verband $(S, \vee, \wedge)$.

Bemerkung 2.1.13. Wir betrachten $(\mathbb{N} \setminus \{0\}, |)$, wobei

$$n \mid k :\Leftrightarrow \exists s \in \mathbb{N} : n \cdot s = k,$$

was eine Halbordnung bildet. Wir beobachten nun, dass für alle $f, g \in S$ gilt, dass $f \leq g \Leftrightarrow \varphi(f) \mid \varphi(g)$. Damit ist φ ein *Ordnungsisomorphismus.*

Korollar 2.1.14. $(\mathbb{N}, |)$ *ist ein Verband.*

Beweis. Seien $n, m \in \mathbb{N} \setminus \{0\}$ und definiere

$$n \vee m := \varphi(\varphi^{-1}(n) \vee \varphi^{-1}(m)) = \mathrm{kgV}(n, m)$$
$$n \wedge m := \varphi(\varphi^{-1}(n) \wedge \varphi^{-1}(m)) = \mathrm{ggT}(n, m).$$

□

Definition 2.1.15. Sei H ein Monoid und $a \in H$. Gilt für alle $b, b' \in H$

- $a \cdot b = a \cdot b' \implies b = b'$, so heißt a *linkskürzbar.*
- $b \cdot a = b' \cdot a \implies b = b'$, so heißt a *rechtskürzbar.*

Bemerkung 2.1.16. Es stellt sich die Frage ob es möglich ist ein Monoid $(H, \cdot, e)$ in eine Gruppe einzubetten. Wir beobachten, dass in einer Gruppe für alle Elemente sowohl links-, als auch rechtskürzbar sind. Notwendig für Einbettbarkeit von einem Monoid $\mathfrak{H} = (H, \cdot, e)$ in eine Gruppe ist also jedenfalls, dass für alle $a \in H$ a sowohl links- als auch rechtskürzbar ist.

Hinreichend hingegen ist die obige Kürzbarkeit mit der zusätzlichen Forderung das $\mathfrak{H}$ kommutativ ist. Es sei angemerkt, dass, obwohl dies hinreichend ist, die Kommutativität im Allgemeinen nicht notwenig ist.

Beispiel 2.1.17.

1. Betrachte $\mathrm{Gl}_2(\mathbb{R})$ und das (nicht kommutative) Untermonoid $\mathfrak{H} := \mathrm{Gl}_2(\mathbb{R}) \cap \mathbb{Z}^{2\times 2}$.
2. Betrachte die freie Gruppe über $\{x, y\}$, so erhalten wir Wörter wie $x^{n_1}y^{m_1} \cdot ... \cdot x^{n_l}y^{m_l}$ $(n_i, m_i \geq 0)$.

Satz 2.1.18. *Sei $\mathfrak{H} = (H, \cdot, e)$ ein kommutatives Monoid und jedes $a \in H$ kürzbar[1]. Dann gilt*

1. $\sim \subseteq (H^2)^2$
$$(a, b) \sim (c, d) :\Leftrightarrow a \cdot d = b \cdot c$$
ist eine Kongruenzrelation auf $\mathfrak{H}^2$.
2. $\mathfrak{H}^2/_\sim$ *ist eine Gruppe.*

[1] Aufgrund der Kommutativität reicht es sogar lediglich Links- oder Rechtskürzbarkeit zu fordern.

3. *Die Abbildung*
$$\varphi : \mathfrak{H} \to \mathfrak{H}^2/_\sim,\ a \mapsto [(a,e)]_\sim$$
ist eine Einbettung*, also ein injektiver Homomorphismus.*

4. *Sei* $\mathfrak{G}$ *eine Gruppe, so gibt es für alle* $\psi : \mathfrak{H} \to \mathfrak{G}$ *einen injektiven Homomorphismus* $\overline{\psi} : \mathfrak{H}^2/_\sim \to \mathfrak{G}$ *mit* $\overline{\psi} \circ \varphi = \psi$.

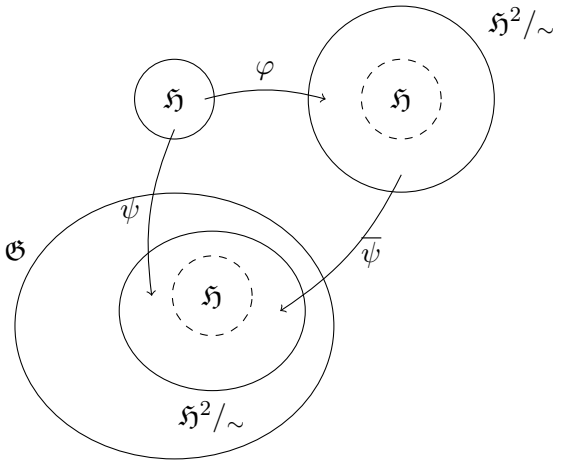

Abbildung 2.1: Visualisierung der Einbettung von $\mathfrak{H}$ in die Gruppen $\mathfrak{G}, \mathfrak{H}^2/_\sim$

Beweis.

1. Prüfen wir zunächst, dass $\sim$ eine Äquivalenzrelation ist.
   a) reflexiv: Es gilt $(a,b) \sim (a,b)$, da $ab = ab$.
   b) symmterisch: Es gilt
   $$(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow bc = ad \Leftrightarrow (c,d) \sim (a,b).$$
   c) transitiv: Seien $(a,b) \sim (c,d) \sim (u,v)$, es gilt also $ad = bc$ und $cv = du$. Dann folgt
   $$(av)(cd) = addu = bcdu = (bu)(cd)$$
   und damit $av = bu$ und $(a,b) \sim (a,v)$ aus der Kürzbarkeit.

   Seien $(a_1,b_1) \sim (c_1,d_1), (a_2,b_2) \sim (c_2,d_2)$, also $a_1d_1 = c_1b_1$ und $a_2d_2 = c_2b_2$ und damit $a_1a_2d_1d_2 = c_1c_2b_1b_2$, also $(a_1a_2, b_1b_2) \sim (c_1c_2, d_1d_2)$, womit $\sim$ auch eine Kongruenzrelation ist.

2. Wir bemerken, dass $(a,b) \sim (e,e) \Leftrightarrow ae = be \Leftrightarrow a = b$, also ist $[(e,e)]_\sim = \{(a,a) \mid a \in H\}$ unser neutrales Element in $\mathfrak{H}^2/_\sim$.

   Wegen
   $$[(a,b)]_\sim \cdot [(b,a)]_\sim = [(ab,ab)]_\sim = [(e,e)]_\sim$$
   ist $[(b,a)]_\sim$ invers zu $[(a,b)]_\sim$, womit $\mathfrak{H}^2/_\sim$ eine Gruppe ist.

3. Es gilt
   $$\varphi(e) = [(e,e)]_\sim \quad \text{neutral in } \mathfrak{H}^2/_\sim,$$
   sowie für $a, b \in H$
   $$\varphi(ab) = [(ab,e)]_\sim = [(a,e)]_\sim \cdot [(b,e)]_\sim = \varphi(a) \cdot \varphi(b),$$

womit φ eine Homomorphismus ist.

Seien nun $a, b \in H$ mit $\varphi(a) = \varphi(b)$, also $[(a,e)]_\sim = [(b,e)]_\sim$, so folgt $a = ae = eb = b$, womit φ injektiv ist.

4. Sei o. B. d. A. $\psi = \mathrm{id}_H$ und definiere $\overline{\psi} : \mathfrak{H}^2/_\sim \to \mathfrak{G},\ [(a,b)]_\sim \mapsto a \cdot b^{-1}$.

   Seien $a, b, c, d \in H$ beliebig mit $ab^{-1} = cd^{-1}$, so folgt $ad = bc$, also $[(a,b)]_\sim = [(c,d)]_\sim$, womit $\overline{\psi}$ injektiv ist.

   Weiters ist

$$\begin{aligned}\overline{\psi}([(a,b)]_\sim \cdot [(c,d)]_\sim) &= \overline{\psi}([(ac,bd)]_\sim) = ac(bd)^{-1} = ab^{-1} \cdot cd^{-1} \\ &= \overline{\psi}([(a,b)]_\sim) \cdot \overline{\psi}([(c,d)]_\sim),\end{aligned}$$

   womit $\overline{\psi}$ ein Homomorphismus ist.

□

2.2 Gruppen

Definition 2.2.1. Sei $\mathfrak{G} = (G, \cdot, e, ^{-1})$ eine Gruppe.

- Wir nennen $|G|$ die *Ordnung* der Gruppe.
- Sei $g \in G$, so erzeugt dieses Element eine Untergruppe

$$\langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

  Wir nennen $|\langle \{g\} \rangle|$ die *Ordnung* von g und schreiben auch $\mathrm{ord}(g)$. Ist $\mathrm{ord}(g)$ endlich, so heißt g *Torsionselement*.

- $\mathfrak{G}$ heißt *zyklisch*, falls es ein $g \in G$ mit $G = \langle \{g\} \rangle$ gibt.

Bemerkung 2.2.2. Im Folgenden werden wir Gruppen durch ihre Trägermengen identifizieren. Für die Gruppe $\mathfrak{G} = (G, \cdot, e, ^{-1})$ wird oft nur G geschrieben.

Beispiel 2.2.3.

1. Betrachte $\mathbb{Z} \times \mathbb{Z}_m$, so ist $\mathrm{ord}(1,0) = \infty$ und $\mathrm{ord}(0,1) = m$.
2. Betrachte $\mathbb{Z}_6$, so ist $\mathrm{ord}(1) = 6$, $\mathrm{ord}(2) = 3$ und $\mathrm{ord}(3) = 2$.

Beispiel 2.2.4.

1. Die Gruppen $(\mathbb{Z}, +, 0, -) = \langle \{1\} \rangle, (\mathbb{Z}_m, +, 0, -) = \langle \{1\} \rangle$ sind zyklisch.
2. Die Gruppe $(\mathrm{Gl}_2(\mathbb{Q}), \cdot, E_2, ^{-1})$ ist *nicht* zyklisch, da – wie wir noch sehen werden – zyklische Gruppen abelsch sind.

29.03.2023
30.03.2023

2.2.1 Nebenklassen und Normalteiler

Definition 2.2.5. Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $g \in G$. Wir definieren

- die *Linksnebenklasse von g nach U* $gU := \{gu \mid u \in U\}$ und
- die *Rechtsnebenklasse von g nach U* $Ug := \{ug \mid u \in U\}$.

Lemma 2.2.6. *Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $g, g', x, y \in G$. Dann gilt:*

1. *Die Menge $\{gU \mid g \in G\}$ aller Linksnebenklassen von g nach U bildet eine Partition von G.*
2. *Es gilt $gU = g'U$ genau dann, wenn $g^{-1}g' \in U$.*
3. *Die Partition induziert eine Äquivalenzrelation $\sim$ auf G, wobei $x \sim y \Leftrightarrow \exists \tilde{g} \in G : x, y \in \tilde{g}U$.*
4. *Es gilt für diese Äquivalenzrelation $x \sim y \Leftrightarrow x^{-1}y \in U$.*
5. *Es ist $U = [e]_\sim$.*

Beweis.

1. Es gilt $G = \bigcup_{g \in G} gU$, denn für $h \in G$ ist $h \in hU$, weil $e \in U$ und $h = h \cdot e$ ist.

   Es bleibt noch zu zeigen, dass die Nebenklassen disjunkt sind. Dafür zeigen wir, dass nicht disjunkte Linksnebenklassen gleich sind. Seien also $g, g' \in G$ beliebig mit $gU \cap g'U \neq \emptyset$. Es existieren dann $u, u' \in U$, sodass $gu = g'u'$. Sei $a = gu_a \in gU$ beliebig. Es ist dann

   $$a = gu_a = guu^{-1}u_a = g' \underbrace{u'u^{-1}u_a}_{\in U} \in g'U,$$

   also $gU \subseteq g'U$. Analog erhält man die andere Mengeninklusion, womit $gU = g'U$ gilt.

2. Es ist

   $$gU = g'U \Leftrightarrow \exists u, u' \in U : gu = g'u' \Leftrightarrow \exists u, u' \in U : u\left(u'\right)^{-1} = g^{-1}g' \Leftrightarrow g^{-1}g' \in U.$$

3. Klarerweise wird durch eine Partition eine Äquivalenzrelation induziert. $\exists \tilde{g} \in G : x, y \in \tilde{g}U$ ist äquivalent dazu, dass $xU = yU$, was wiederum äquivalent dazu ist, dass x, y die gleiche Äquivalenzklasse haben.

4. "$\Rightarrow$": Es gibt $u, u' \in U$, sodass $x = gu$ und $y = gu'$. Es ist also $x^{-1}y = u^{-1}g^{-1} \cdot gu' = u^{-1}u' \in U$.

   "$\Leftarrow$": Es gilt $x^{-1} \cdot y = u$, also $y = x \cdot u$. Es ist nun $x \in xU$ und auch $y \in xU$, also $x \sim y$.

5. Es ist $a \in [x]_\sim \Leftrightarrow e \sim x \Leftrightarrow e^{-1}a = a \in U$.

□

Bemerkung 2.2.7. Lemma 2.2.6 gilt analog für Rechtsnebenklassen. Im Allgemeinen erhält man dabei allerdings eine andere Äquivalenzrelation.

Lemma 2.2.8. *Seien G eine Gruppe, $U \leq G$ eine Untergruppe und $g \in G$. Es gilt*

$$|gU| = |U| = |Ug|.$$

Beweis. Definieren wir die Funktion $\varphi : U \to gU, u \mapsto g \cdot u$ und zeigen, dass sie bijektiv ist. Die Surjektivität ist klar, da gU genau als das Bild von φ definiert ist. Die Injektivität erhalten wir wegen $gu = gu' \Rightarrow u = u'$. Damit ist $|U| = |gU|$. Die zweite Gleichheit wird analog gezeigt. □

Bemerkung 2.2.9. Ist G eine endliche Gruppe, dann gilt $|G| = |\{gU \mid g \in G\}| \cdot |U|$, da alle Links-/Rechtsnebenklassen gleich mächtig sind. Durch umformen zu $|\{gU \mid g \in G\}| = \frac{|G|}{|U|}$ erhalten wir, dass es gleich viele Linksnebenklassen wie Rechtsnebenklassen gibt.

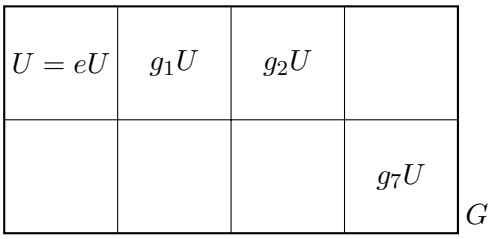

Abbildung 2.2: Nebenklassenzerlegung einer endlichen Gruppe

Bemerkung 2.2.10. Es gilt auch für Gruppen mit unendlicher Trägermenge, dass es gleich viele Linksnebenklassen wie Rechtsnebenklassen gibt. Es kann dafür die Funktion $\varphi : gU \mapsto Ug^{-1}$ definiert werden und gezeigt werden, dass diese wohldefiniert und bijektiv ist.

Satz 2.2.11 (Lagrange)**.** *Sei G eine endliche Gruppe, $U \leq G$ eine Untergruppe und $g \in G$. Dann gilt*

- *$|U|$ teilt $|G|$ und*
- *$\mathrm{ord}(g)$ teilt $|G|$.*

Beweis. Die erste Behauptung folgt aus Bemerkung 2.2.9, für die zweite wählen wir $U := \langle g \rangle$. □

Beispiel 2.2.12. Betrachten wir $(\mathbb{Z}_6, +, 0, -)$ mit Ordnung 6. Es sind dann $\mathrm{ord}(0) = 1, \mathrm{ord}(1) = \mathrm{ord}(5) = 6, \mathrm{ord}(2) = \mathrm{ord}(4) = 3, \mathrm{ord}(3) = 2$, welche alle Teiler von 6 sind.

Sei G eine Gruppe mit $|G| = p \in \mathbb{P}$. Für $g \in G \setminus \{e\}$ gilt nun $\mathrm{ord}(g) = p \Rightarrow \langle g \rangle = G$, womit G zyklisch ist. Gruppen mit Primzahlordnung sind also zyklisch.

Definition 2.2.13. Sei G eine Gruppe und $U \leq G$ eine Untergruppe. Der *Index von U in G* ist definiert als $[G : U] := |\{gU \mid g \in G\}| = |\{Ug \mid g \in G\}|$.

Bemerkung 2.2.14. Ist G endlich, dann haben wir in Bemerkung 2.2.9 $[G : U] = \frac{|G|}{|U|}$ gezeigt.

Satz 2.2.15 (Indexsatz)**.** *Sei G eine Gruppe und seien $U \leq V \leq G$ Untergruppen, dann ist*

$$[G : V] = [G : U] \cdot [U : V].$$

Beweis. Wurde in der Übung bewiesen. □

Im Allgemeinen ist die durch Links-/Rechtsnebengruppen induzierte Äquivalenzrelation keine Kongruenzrelation. Der folgende Satz 2.2.17 liefert Bedingungen, wann dies erfüllt ist.

Definition 2.2.16. Sei G eine Gruppe, dann heißt eine Teilmenge $N \subseteq G$ *Normalteiler*, wenn eine der Bedingungen aus Satz 2.2.17 erfüllt ist. Man schreibt $N \lhd G$.

Satz 2.2.17. *Sei G eine Gruppe, $N \subseteq G$, dann sind äquivalent:*

(1) Es gibt genau eine Kongruenzrelation $\sim$ auf G mit $N = [e]_\sim$, nämlich $x \sim y :\Leftrightarrow x^{-1}y \in N$.

(1') Es gibt eine Kongruenzrelation $\sim$ auf G mit $N = [e]_\sim$.

(2) Es gibt eine Gruppe H und einen surjektiven Homomorphismus $\varphi : G \to H$ mit $N = \varphi^{-1}(\{e_H\})$.

(2') Es gibt eine Gruppe H und einen Homomorphismus $\varphi : G \to H$ mit $N = \varphi^{-1}(\{e_H\})$.

(3) Es ist $N \leq G$ mit $\forall x \in G : xNx^{-1} = N$.

(3') Es ist $N \leq G$ mit $\forall x \in G : xNx^{-1} \subseteq N$.

(4) Es ist $N \leq G$ mit $\forall x \in G : xN = Nx$.

(4') Es ist $N \leq G$ mit $\forall x \in G : xN \subseteq Nx$.

Beweis.

(1) $\Rightarrow$ (1'): Trivial.

(1') $\Rightarrow$ (2): Wählen wir $H = G/_\sim$ und sei $\varphi : G \to H, g \mapsto [g]_\sim$ die kanonische Einbettung. Es ist dann klarerweise φ surjektiv und $\varphi^{-1}(\{e_H\}) = [e]_\sim = N$.

(2) $\Rightarrow$ (2'): Trivial.

(2') $\Rightarrow$ (3'): Zeigen wir zuerst, dass N eine Untergruppe ist. Seien dazu $n, n' \in N = \varphi^{-1}(\{e_H\})$. Dann ist $\varphi(nn') = \varphi(n)\varphi(n') = e_H e_H = e_H$, womit $nn' \in \varphi^{-1}(\{e_H\}) = N$ ist und damit $N \leq G$.

Zeigen wir nun noch für $x \in G, n \in N$, dass $y = xnx^{-1} \in N$ ist. Wir erhalten

$$\varphi(y) = \varphi(x)\underbrace{\varphi(n)}_{=e_H}\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = e_H \;\Rightarrow\; y \in \varphi^{-1}(\{e_H\}) = N.$$

(3') $\Rightarrow$ (3): Wir wissen bereits, dass $\forall x \in G : xNx^{-1} \subseteq N$ gilt und wollen zeigen, dass für $y \in G$ die umgekehrte Inklusion gilt. Es ist $y^{-1} \in G$, womit $y^{-1}N(y^{-1})^{-1} = y^{-1}Ny \subseteq N$ ist. Wir erhalten damit nun

$$N \overset{(*)}{=} yy^{-1}Nyy^{-1} = y(y^{-1}Ny)y^{-1} \subseteq yNy^{-1},$$

wobei $(*)$ einfach nachzurechnen ist.

(3) $\Rightarrow$ (4): Zeigen wir für $x \in G$, dass $xN \subseteq Nx$ ist. Für ein $y \in xN$ gibt es ein $n \in N$, sodass $y = xn$. Wählen wir $n' = yx^{-1} = xnx^{-1} \in xNx^{-1} = N$, so ist $y = n'x$ und damit $y \in Nx$. Die andere Mengeninklusion zeigt man analog.

(4) $\Rightarrow$ (4'): Trivial.

(4') $\Rightarrow$ (1): Zeigen wir zuerst die Eindeutigkeit: Sei angenommen es gibt eine Kongruenzrelation $\sim$ auf G mit $N = [e]_\sim$. Für $x, y \in G$ gilt dann

- $x \sim y \;\Rightarrow\; x^{-1}x \sim x^{-1}y \;\Leftrightarrow\; e \sim x^{-1}y \;\Leftrightarrow\; x^{-1}y \in [e]_\sim = N$ und
- $x^{-1}y \in N = [e]_\sim \;\Leftrightarrow\; e \sim x^{-1}y \;\Leftrightarrow\; x = xe \sim x(x^{-1}y) = y$.

Es ist dann also $x \sim y \Leftrightarrow x^{-1}y \in N$.

Zeigen wir nun noch, dass dieses $\sim$ eine Kongruenzrelation auf G ist. Nach Lemma 2.2.6 ist $\sim$ eine Äquivalenzrelation, bleibt also noch die Invarianz unter G zu zeigen.

- Zeigen wir für $x, x', y, y' \in G$ mit $x \sim y, x' \sim y'$, dass $xx' \sim yy'$. Es gilt

$$xx' \sim yy' \;\Leftrightarrow\; x'^{-1} \underbrace{x^{-1}y}_{=:n \in N}\, y' = \underbrace{x'^{-1}n}_{\in x'^{-1}N \subseteq Nx'^{-1}}\, y' \overset{(*)}{=} n' \underbrace{x'^{-1}y'}_{\in N} \in N,$$

  wobei wir bei $(*)$ verwenden, dass nach (4') ein $n' \in N$ existiert, sodass $x'-1n = n'x'-1$.

- Zeigen wir für $x, y \in G$ mit $x \sim y$, dass $x^{-1} \sim y^{-1}$. Es gilt

$$x \sim y \;\Leftrightarrow\; x^{-1}x \sim x^{-1}y \;\Leftrightarrow\; e \sim x^{-1}y \;\Leftrightarrow\; ey^{-1} \sim x^{-1}yy^{-1} \;\Leftrightarrow\; y^{-1} \sim x^{-1}.$$

- Klarerweise ist $e \sim e$, also ist $\sim$ invariant unter der 0-stelligen Operation e.

□

Bemerkung 2.2.18. Satz 2.2.17 beschreibt einige Eigenschaften von Normalteilern.

- (1), (1') liefern den bijektiven Zusammenhang von Normalteilern und Kongruenzrelation. Betrachtet man die Verbände von Normalteilern bzw. Kongruenzrelationen, so stellt diese Bijektion einen Verbandsisomorphismus dar.
- (2), (2') beschreiben die Darstellung des Normalteilers über den Kern eines Homomorphismus $\varphi : G \to H$. Es ist $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\}) = N$.
- (3), (3') liefern direkt, dass Normalteiler unter Abbildungen $\pi_x : G \to G, g \mapsto xgx^{-1}$ abgeschlossen sind. So eine Abbildung nennt man *inneren Automorphismus*.
- (4), (4') besagen, dass die Links- und Rechtsnebenklassen genau dann gleich sind, wenn die Untergruppe ein Normalteiler ist.

Inbesondere sind alle Äquivalenzklassen einer Kongruenzrelation gleich groß, da sie lediglich "Verschiebungen" der Äquivalenzklasse des neutralen Elements sind.

Korollar 2.2.19. *In einer abelschen Gruppe G ist $N \subseteq G$ genau dann ein Normalteiler, wenn N eine Untergruppe von G ist.*

Beweis. In einer abelschen Gruppe ist immer $xN = Nx$. Satz 2.2.17 (4) liefert dann damit die Behauptung. □

30.03.2023
19.04.2023

Bemerkung 2.2.20. Seien G, H Gruppen, $h : G \to H$ ein Homomorphismus. Es sei erinnert, dass h injektiv ist, wenn

$$\{(x, y) \mid h(x) = h(y)\} = \{(x, x) \mid x \in G\}.$$

Erstere Menge definiert eine Kongruenzrelation $\sim$ auf G. Also ist h genau dann injektiv, wenn $\sim$ die triviale Gleichheitsrelation ist, also $[e]_\sim = \{e\}$, also gerade $\ker h = \{e\}$. Man vergleiche diese Eigenschaft mit der Injektivität von Vektorraum-Homomorphismen aus der Linearen Algebra.

Bemerkung 2.2.21. Es sei an Definition 1.4.27 einer einfachen Algebra erinnert. Wir bemerken, dass eine Gruppe genau dann einfach ist, wenn sie nur ihre Trägermenge und $\{e\}$ als Normalteiler hat.

Definition 2.2.22. Sei G eine Gruppe, $N \lhd G$ ein Normalteiler und $\sim$ die entsprechende Kongruenzrelation. Wir definieren die *Faktorgruppe*

$$G/_N := G/_\sim = \{aN \mid a \in G\}.$$

Dabei ist

$$aN \cdot bN := (a \cdot b)N.$$

Man überzeugt sich leicht davon, dass dies gerade dann wohldefiniert ist wenn eben N ein Normalteiler ist.

Beispiel 2.2.23. Betrachte die Gruppe $(\mathbb{Z}, +, 0, -)$, so ist für jedes $m \in \mathbb{N}$ die Menge $m\mathbb{Z}$ eine Untergruppe, und da sie kommutativ ist nach Korollar 2.2.19 auch ein Normalteiler.

Sei $\sim$ die entsprechende Kongruenzrelation und betrachten wir $(\mathbb{Z}, +, 0, -)/_\sim$, so enthält diese Faktorgruppe

$$0 + m\mathbb{Z}, \quad 1 + m\mathbb{Z}, \quad \ldots, \quad (m-1) + m\mathbb{Z}.$$

In dieser Gruppe rechnet man

$$(i + m\mathbb{Z}) + (j + m\mathbb{Z}) = (i + j) + m\mathbb{Z},$$

wobei man auch $(i + j \pmod m)$ für einen "schöneren" Repräsentanten betrachten kann.

Im Falle $n = 4$ ist beispielsweise

$$(1 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 4 + 4\mathbb{Z} = 0 + 4\mathbb{Z}.$$

Beispiel 2.2.24. Betrachte die Gruppe $(\mathrm{Gl}_2(\mathbb{R}), \cdot, E_2, {}^{-1})$ und

$$N := \{A \in \mathrm{Gl}_2(\mathbb{R}) \mid \det A = 1\}.$$

Für ein beliebiges $A \in \mathrm{Gl}_2(\mathbb{R})$ gilt $ANA^{-1} \subseteq N$, da mit $C \in N$

$$\det(ACA^{-1}) = \det A \det C \det A^{-1} = \det C = 1.$$

Also ist N ein Normalteiler. Sei $\sim$ die entsprechende Äquivalenzrelation, wir wollen die Struktur von $\mathrm{Gl}_2(\mathbb{R})/_\sim$ analysieren. Es gilt

$$A \sim B \Leftrightarrow A \cdot B^{-1} \in N \Leftrightarrow \det(A \cdot B^{-1}) = 1 \Leftrightarrow \det A = \det B,$$

die Äquivalenzklassen hängen also nur von der Determinante und ansonsten nicht von der unterliegenden Matrixstruktur ab. Also ist $\mathrm{Gl}_2(\mathbb{R})/_\sim \cong (\mathbb{R} \setminus \{0\}, \cdot, 1, {}^{-1})$.

Bemerkung 2.2.25. Sei G eine Gruppe, $\sim$ eine Kongruenzrelation. Wir fragen uns, wann $G/_\sim$ kommutativ ist. Dazu bemerken wir

$$G/_\sim \text{ kommutativ} \quad \Leftrightarrow \quad \forall a, b \in G : (ab)N = (aN)(bN) = (bN)(aN) = (ba)N.$$

Letzteres können wir umschreiben als $a^{-1}b^{-1}abN = N$, was genau dann der Fall ist, wenn für beliebiges a, b gilt

$$[a, b] := a^{-1}b^{-1}ab \in N.$$

Wir nennen $[a, b]$ den *Kommutator* von (a, b).

Definition 2.2.26. Definiere

$$G' := \langle \{[a,b] \mid a,b \in G\} \rangle \leq G.$$

Wir nennen G' die *Ableitung* oder auch die *Kommutatorgruppe* von G.

Proposition 2.2.27. *Sei G eine Gruppe. Ist G abelsch, so ist $G' = \{e\}$.*

Beweis. Ist G abelsch so ist

$$G' = \langle \{a^{-1}b^{-1}ab \mid a,b \in G\} \rangle = \langle \{a^{-1}b^{-1}ba \mid a,b \in G\} \rangle = \langle \{e\} \rangle = \{e\}.$$

□

Satz 2.2.28. *Sei G eine Gruppe. Dann gilt:*

1. *$G' \lhd G$*
2. *$G/_{G'}$ ist abelsch.*
3. *$\forall N \lhd G : (G/_N \text{ abelsch} \Leftrightarrow N \supseteq G')$*

Beweis. (2) ist ein Spezialfall von (3).

Um (3) einzusehen sei $N \lhd G$, so folgt mit obiger Bemerkung sofort

$$\begin{aligned} G/_N \text{ abelsch} &\Leftrightarrow \forall a,b : (aN)(bN) = (bN)(aN) \Leftrightarrow \\ &\Leftrightarrow \forall a,b a^{-1}b^{-1}ab \in N \Leftrightarrow \forall a,b : [a,b] \in N \Leftrightarrow N \subseteq G'. \end{aligned}$$

Zeigen wir nun (1). Sei $h : G \to G$ ein beliebiger Endomorphismus, dann gilt für alle $a,b \in G$, dass $h([a,b]) = [h(a),h(b)]$, also $h(G') \subseteq G'$. Für beliebiges $x \in G$ definieren wir

$$h_x : G \to G, g \mapsto xgx^{-1},$$

so ist h_x ein Automorphismus[2]. Also ist

$$xG'x^{-1} = h_x(G') \subseteq G',$$

womit $G' \lhd G$ folgt. □

2.2.2 Innere direkte Produkte

Definition 2.2.29. Sei G eine Gruppe, $U_1, U_2 \subseteq G, x \in G$, so definieren wir das *Komplexprodukt*

$$U_1 \cdot U_2 = \{u_1 \cdot u_2 \mid u_1 \in U_1, u_2 \in U_2\}.$$

Definition 2.2.30. Sei G eine Gruppe, $U_1, \ldots, U_n \leq G$. Wir nennen G ein *inneres direktes Produkt* von $(U_1, \ldots, U_n)$, wenn die Abbildung

$$\varphi : U_1 \times \ldots \times U_n \to G, (u_1, \ldots u_n) \mapsto u_1 \cdot \ldots \cdot u_n$$

ein Isomorphismus ist. In diesem Fall schreiben wir $G = U_1 \odot \ldots \odot U_n$.

[2] h_x ist wie früher schon bemerkt ein *innerer Automorphismus*.

Bemerkung 2.2.31. Wir sammeln nun notwendige Bedingungen dafür, dass G ein inneres direktes Produkt ist.

Für $i \in \{1, \dots, n\}$ definiere $V_i := U_1 \cdot \ldots \cdot U_{i-1} \cdot U_{i+1} \cdot \ldots \cdot U_n$, so muss gelten

$$U_i \cap V_i = \{e\}.$$

Sonst gäbe es $(u_j)_{j=1}^n \in (U_j)_{j=1}^n, u_i \neq e$ mit

$$\varphi(e, \dots, e, \overbrace{u_i}^{i\text{-te Stelle}}, e, \dots, e) = u_i \overset{!}{=} u_1 \cdot \ldots \cdot u_{i-1} \cdot u_{i+1} \cdot \ldots \cdot u_n = \varphi(u_1, \dots, u_{i-1}, e, u_{i+1}, \dots, u_n),$$

womit φ nicht injektiv wäre.

Weiters muss $U_i \lhd G$ sein. Um dies einzusehen, betrachte die Abbildung

$$\psi_i : U_1 \times ... \times U_n \to U_1 \times ... \times U_{i-1} \times U_{i+1} \times ... \times U_n, (u_i)_{i=1}^n \mapsto (u_i, \dots, u_{i-1}, u_{i+1}, \dots, u_n).$$

Diese ist ein Homomorphismus, womit

$$\ker \psi_i = \{e\} \times ... \times \{e\} \times U_i \times \{e\} \times ... \times \{e\} \lhd U_1 \times ... \times U_n.$$

Damit ist $U_i = \varphi(\ker \psi_i) \lhd G$.

Zuletzt gilt in einem direkten inneren Produkt für $i \neq j, x \in U_i, y \in U_j$, dass $xy = yx$. Um dies einzusehen sei o. B. d. A. $i < j$, so gilt

$$\begin{aligned} xy &= \varphi(e, \dots, e, \overbrace{x}^{i\text{-te Stelle}}, e, \dots, e) \cdot \varphi(e, \dots, e, \overbrace{y}^{j\text{-te Stelle}}, e, \dots, e) = \\ &= \varphi(e, \dots, e, \overbrace{x}^{i\text{-te Stelle}}, e, \dots, e, \overbrace{y}^{j\text{-te Stelle}}, e, \dots, e) = \\ &= \varphi(e, \dots, e, \overbrace{y}^{i\text{-te Stelle}}, e, \dots, e) \cdot \varphi(e, \dots, e, \overbrace{x}^{j\text{-te Stelle}}, e, \dots, e) = yx. \end{aligned}$$

Lemma 2.2.32. *Sei G eine Gruppe, $U, V \lhd G$, $U \cap V = \{e\}$, dann gilt für alle $u \in U$ und $v \in V$, dass $uv = vu$.*

Beweis. Es gilt

$$uv = vu \Leftrightarrow u^{-1}v^{-1}uv = e.$$

Nun ist $u^{-1}v^{-1}u \in V$, damit $u^{-1}v^{-1}uv \in V$. Andererseits gilt $v^{-1}uv \in U$, damit $u^{-1}v^{-1}uv \in U$. Also folgt $u^{-1}v^{-1}uv = e$ und damit $uv = vu$. □

Proposition 2.2.33. *Sei G eine Gruppe und $U_1, \dots, U_n \leq G$. Gelte $G = U_1 \cdot \ldots \cdot U_n$, beziehungsweise äquivalent die Surjektivität von φ wie in Definition 2.2.30. Gelte weiters für $i \in \{1, \dots, n\}$, dass $U_i \lhd G$ und $U_i \cap V_i = \{e\}$, wobei V_i wie in Bemerkung 2.2.31 definiert ist. Dann ist $G = U_1 \odot \ldots \odot U_n$.*

Beweis. Definiere φ wie in Definition 2.2.30, so ist φ nach Voraussetzung surjektiv.

Zeigen wir, dass φ ein Homomorphismus ist. Mit Lemma 2.2.32 gilt

$$\begin{aligned} \varphi((u_1, \dots, u_n) \cdot (v_1, \dots, v_n)) &= \varphi(u_1 v_1, \dots, u_n v_n) = u_1 v_1 \dots u_n v_n = \\ &= u_1 \dots u_n v_1 \dots v_n = \varphi(u_1, \dots, u_n)\varphi(v_1, \dots, v_n). \end{aligned}$$

Bleibt die Injektivität zu zeigen. Dazu reicht es nach Bemerkung 2.2.20 zu zeigen, dass der Kern trivial ist. Sei also $\varphi(u_1, \ldots, u_n) = e$, so ist $(u_1, \ldots, u_n) = (e, \ldots, e)$ zu zeigen. Sei dazu indirekt angenommen es wäre nicht der Fall und sei i minimal mit $u_i \neq e$, also

$$e = \varphi(u_1, \ldots, u_n) = e \ldots e u_i \ldots u_n = u_i \ldots u_n,$$

womit $u_i^{-1} = u_{i+1} ... u_n \in V_i$ folgt. Da jedoch auch $u_i^{-1} \in U_i$ und $U_i \cap V_i = \{e\}$ folgt damit $u_i = e$, im Widerspruch.

Insgesamt ist φ also ein Isomorphismus, was zu zeigen war. □

Bemerkung 2.2.34. Sei $(U_i)_{i \in I}$ eine Familie von Untergruppen einer Gruppe G, wobei $(I, <)$ totalgeordnet ist. Wir definieren das *schwache Produkt*

$$\prod_{i \in I}^{w} U_i := \{f : I \to \bigcup_{i \in I} U_i \mid \forall i \in I : f(i) \in U_i \wedge f(i) = e \text{ für fast alle } i \in I\}.$$

Definiere weiters

$$\varphi : \prod_{i \in I}^{w} U_i \to G, f \mapsto f(i_1) \cdot \ldots \cdot f(i_k),$$

wobei $i_1 < \ldots < i_k$ genau jene Indizes sind, für die $f(i_j) \neq e$ ist.

Falls φ ein Isomorphismus ist, so nennen wir G *inneres direktes Produkt* von $(U_i)_{i \in I}$.

Ohne Beweis sei angemerkt dass Proposition 2.2.33 entsprechend auch für solche inneren direkten Produkte gilt.

19.04.2023
20.04.2023

2.2.3 Zyklische Gruppen

Es sei an die Definition einer zyklischen Gruppe in Definition 2.2.1 erinnert.

Beispiel 2.2.35. $\mathbb{Z} = \langle\{1\}\rangle$ und $\mathbb{Z}_m = \langle\{1\}\rangle$ sind zyklische Gruppen.

Proposition 2.2.36. *Für eine Gruppe G gilt:*

1. *G zyklisch $\Leftrightarrow \exists h : \mathbb{Z} \to G$ surjektiver Homomorphisus*
2. *G zyklisch $\Rightarrow G$ abelsch*
3. *G zyklisch $\Rightarrow \forall F \in H(\{G\}) : F$ zyklisch*
4. *G zyklisch $\Rightarrow \forall F \in S(\{G\}) : F$ zyklisch*

Beweis.

1. $\Leftarrow$: Es gilt $\mathbb{Z} = \langle\{1\}\rangle$ und damit folgt $G = \langle\{h(1)\}\rangle$.

   $\Rightarrow$: Sei $g \in G$ so, dass $G = \{g^n \mid g \in \mathbb{Z}\}$. Definiere die Abbildung $h : \mathbb{Z} \to G, n \mapsto g^n$. Dafür gilt $h(0) = e_g$, $h(n)^{-1} = (g^n)^{-1} = g^{-n} = h(-n)$ und $h(m+n) = g^{m+n} = g^m g^n = h(m)h(n)$, womit h ein Homomorphismus ist. Aufgrund der Wahl von g ist h nun surjektiv.

2. Diese Aussage folgt direkt aus 1., da abelsche Gruppen eine Varietät bilden. Es ist $\mathbb{Z}$ abelsch, also auch dessen homomorphe Bilder, insbesondere G.

3. Sei $F \in \mathrm{H}(\{G\})$ beliebig, es gibt also einen surjektiven Homomorphismus $\varphi : G \to F$. Aus 1. erhalten wir außerdem, da G zyklisch ist, die Existenz eines surjektiven Homomorphismus $h : \mathbb{Z} \to G$. Die Verkettung $\varphi \circ h : \mathbb{Z} \to F$ ist nun erneut ein surjektiver Homomorphismus, weshalb wir erneut aus 1. erhalten, dass F zyklisch ist.

4. Sei $F \in \mathrm{S}(\{G\})$ beliebig, also $F \leq G$. Weiter sei $h : \mathbb{Z} \to G$ ein nach 1. existierender surjektiver Homomorphismus. Wir wählen nun $U := h^{-1}(F) \leq \mathbb{Z}$ und $m := \min\{n > 0 \mid n \in U\}$ bzw. 0, falls die Menge leer ist.

   Wir behaupten nun, dass $U = m\mathbb{Z}$. Sei zuerst $mk \in m\mathbb{Z}$, dann folgt, da $m \in U$ und U als Untergruppe unter Addition und Inversenbildung abgeschlossen ist, induktiv auch $mk \in U$. Es gilt also $U \subseteq m\mathbb{Z}$. Sei nun $n \in U$ und o. B. d. A. $n > 0$. Es gibt dann $k \in \mathbb{N}$ und $r \in \{0, \dots, m-1\}$, sodass $n = mk + r$. Durch Umformen erhalten wir $r = n - mk \in U$. Aufgrund der Wahl von m folgt nun, dass $r = 0$, da es sonst ein kleineres positives Element als m in G gäbe, im Widerspruch zur Minimalität von m. Es ist also $n = mk \in m\mathbb{Z}$, womit $U = m\mathbb{Z}$ folgt.

   Betrachten wir nun den surjektiven Homomorphismus $h|_{m\mathbb{Z}} : m\mathbb{Z} \to F$. Da $m\mathbb{Z} = \langle\{m\}\rangle$ und $m\mathbb{Z}$ damit zyklisch ist, folgt aus 1., dass F zyklisch ist.

□

Bemerkung 2.2.37. Es ist leicht einzusehen, dass $\mathbb{Z}_2 \times \mathbb{Z}_2$ nicht zyklisch ist, obwohl $\mathbb{Z}_2$ es ist. Die zyklischen Gruppen sind also nicht unter P abgeschlossen und daher keine Varietät.

Proposition 2.2.38. *Sei G eine zyklische Gruppe. Dann ist $G \cong \mathbb{Z}$ oder $G \cong \mathbb{Z}_m$.*

Beweis. Aus Proposition 2.2.36 folgt die Existenz eines surjektiven Homomorphismus $h : \mathbb{Z} \to G$. Der Homomorphiesatz (1.4.32) liefert, dass $G \cong \mathbb{Z}/_{\ker h}$. Ist $\ker h = \{0\}$, so ist $G \cong \mathbb{Z}$. Ist $\ker h$ nicht trivial, so gibt es ein $m \in \mathbb{N}$, sodass $\ker h = m\mathbb{Z}$, da der Kern immer eine Untergruppe ist und im Beweis von Proposition 2.2.36 gezeigt wurde, dass alle Untergruppen von $\mathbb{Z}$ diese Form haben. Es folgt also $G \cong \mathbb{Z}/_{m\mathbb{Z}} \cong \mathbb{Z}_m$. □

Definition 2.2.39. Für $m \in \mathbb{N} \setminus \{0\}$ bezeichne mit ${C_m}^3$ die Gruppe $(\{0, \dots, m-1\}, +, 0, -)$ wobei

$$a + b := \min\{n \geq 0 \mid a + b \equiv n \bmod(m)\}.$$

2.2.4 Symmetrische und Permutationsgruppen

Definition 2.2.40. Für eine Menge A sei

$$S_A = \{f : A \to A \mid f \text{ bijektiv}\}$$

definiert. Wir nennen $(S_A, \circ, \mathrm{id}_A, {}^{-1})$ die *symmetrische Gruppe von A*.

Jede Untergruppe $U \leq S_A$ einer symmetrischen Gruppe heißt *Permutationsgruppe*.

Satz 2.2.41 (Darstellungssatz von Cayley für Gruppen)**.** *Sei G eine Gruppe, dann existiert eine Permutationsgruppe U, sodass $G \cong U$.*

[3] Man verifiziert sofort, dass $C_m \cong \mathbb{Z}_m$ gilt, vermöge dem Isomorphismus $\varphi : C_m \to \mathbb{Z}_m, x \mapsto \{x + km \mid k \in \mathbb{Z}\}$.

Beweis. Definieren wir die Abbildungen

$$f_g : G \to G, h \mapsto gh \quad \text{und} \quad \varphi : G \to G^G, g \mapsto f_g.$$

Im Beweis von Satz 2.1.10 wurde bereits gezeigt, dass φ ein Monoid-Homomorphismus bezüglich $\cdot/\circ$ ist. Sei nun $g \in G$ beliebig, dann gilt

$$\mathrm{id}_G = f_e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g) \circ \varphi(g^{-1}) = f_g \circ f_{g^{-1}}$$

und analog $f_{g^{-1}} \circ f_g = \mathrm{id}_G$, also sind diese invers zueinander und somit Bijektionen. Wir erhalten daraus nun, dass $\varphi(g)^{-1} = \varphi(g^{-1})$ gilt, also φ ein Gruppenhomomorphismus ist und, dass $\varphi(G) \leq S_G$. □

Definition 2.2.42. Sei A eine Menge und G eine Gruppe. Ein Homomorphismus $h : G \to S_A$ heißt *(Gruppen)Aktion von G auf A*. Man schreibt auch $G \overset{h}{\curvearrowright} A$.

Bemerkung 2.2.43. Eine andere Gruppenaktionen von G nach G als die Linkstranslation φ. Eine weitere ist die aus dem Beweis von Satz 2.2.41 bekannte Abbildung

$$\Psi : G \to G^G, g \mapsto [\psi_g : G \to G, h \mapsto ghg^{-1}]. \qquad \text{(Konjugation)}$$

Ist G abelsch, so ist $\Psi(G) = \{\mathrm{id}_G\}$. Außerdem ist

$$\ker \Psi = \{g \in G \mid \psi_g = \mathrm{id}_G\} = \{g \in G \mid \forall h \in G : ghg^{-1} = h\} = \{g \in G \mid \forall h \in G : gh = hg\}.$$

Wir definieren das *Zentrum von G* als

$$Z(G) := \{g \in G \mid \forall h \in G : gh = hg\}.$$

Definition 2.2.44. Eine *Permutation* ist eine bijektive Abbildung $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$. Eine Darstellung von Permutationen ist die sogenannte *Zyklenschreibweise*. Es wird die Permutation dabei dargestellt als

$$(a_1\ \pi(a_1)\ \pi^2(a_1)\ \dots\ \pi^{\ell_{a_1}-1}(a_1))(a_2\ \pi(a_2)\ \dots\ \pi^{\ell_{a_2}-1}(a_2)) \dots (a_n\ \pi(a_n)\ \dots\ \pi^{\ell_{a_n}-1}(a_n)),$$

wobei die einzelnen Klammern *Zyklus (von a_i)* genannt werden und ℓ_{a_i} die kleinste natürliche Zahl ist, sodass $\pi^{\ell_{a_i}}(a_i) = a_i$ gilt. Zyklen mit $\ell_{a_i} = 1$ (Fixpunkte) können in der Zyklenschreibweise weggelassen werden. Die Gruppe aller Permutationen für bestimmtes $n \in \mathbb{N}$ ist die *symmetrische Gruppe* und wir schreiben auch $S_n := S_{\{1,\dots,n\}}$.

Eine *Transposition* ist eine Permutation der Form $(i\ j)$.

Proposition 2.2.45. *Für $n \in \mathbb{N}_{\geq 2}$ gilt*

1. $|S_n| = n!$,
2. $\forall \pi \in S_n : \pi$ *ist das Produkt von Transpositionen und*
3. $\forall \pi \in S_n : \#$ *der Transpositionen modulo 2 ist unabhängig von der Darstellung.*

Beweis.

1. Wir beweisen mittels vollständiger Induktion, dass es $n!$ Bijektionen zwischen zwei n-elementigen Mengen $X_n = \{x_1, \dots, x_n\}, Y_n = \{y_1, \dots, y_n$ gibt.

   Induktionsanfang ($n = 1$): Es gibt genau eine (bijektive) Abbildung $f : \{x_1\} \to \{y_1\}$.
   Induktionsschritt ($n \to n + 1$): Für $i \in \{1, \dots, n + 1\}$ gibt es wegen der Induktionsvoraussetzung genau $n!$ Bijektionen von X_n nach $\{y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_{n+1}\}$ gibt, also gibt es $n!$ Bijektionen zwischen X_{n+1} und Y_{n+1} mit $f(x_{n+1}) = y_i$. Da nun i aus $n + 1$ Zahlen gewählt werden kann, gibt es $(n + 1)n! = (n + 1)!$ Bijektionen zwischen X_{n+1} und Y_{n+1}.

   Mit $X_n = Y_n = \{1, \dots, n\}$ folgt die Behauptung.

2. Wir zeigen die Aussage mittels vollständiger Induktion:

   Induktionsanfang ($n = 2$): Es ist $S_n = \{\mathrm{id}_{\{1,2\}}, (1\ 2)\}$, wobei $\mathrm{id}_{\{1,2\}} = (1\ 2) \circ (1\ 2)$.
   Induktionsschritt ($n \to n + 1$): Sei $\pi \in S_{n+1}$. Falls $\pi(n + 1) \neq n + 1$ wählen wir die (selbstinverse) Transposition $\tau = (\pi(n + 1)\ n + 1)$. Wählen wir nun $\tilde{\pi} := \tau \circ \pi$ oder $\tilde{\pi} = \pi$ falls $\pi(n+1) = n+1$. Es ist dann $\tilde{\pi}|_{\{1,\dots,n\}} \in S_n$, womit es nach der Induktionsvoraussetzung eine Darstellung als Produkt von Transpositionen gibt. Da $\pi = \tilde{\pi}$ oder $\pi = \tau\tilde{\pi}$ gibt es nun also auch für π eine solche Darstellung.

3. Sei $\pi \in S_n$ mit zwei Darstellungen $\pi = (i_1\ j_1) \dots (i_k\ j_k) = (a_1\ b_1) \dots (a_\ell\ b_\ell)$. Transposition sind selbstinvers, wir haben also

   $$(a\ell\ b_\ell) \dots (a_1\ b_1)(i_1\ j_1) \dots (i_k\ j_k) = \mathrm{id}_{\{1,\dots,n\}}\,.$$

   Es reicht also zu zeigen, dass die Identität keine ungerade Darstellung besitzt. Dazu bemerken wir, dass S_n auf der Menge $M := \{(i, j) \mid 1 \leq i, j \leq n, i \neq j\}$ als Gruppenaktion agiert, und zwar durch

   $$\pi((i, j)) := (\pi(i), \pi(j)).$$

   Sei $(i, j) \in M, i < j$, dann nennen wir (i, j) einen Fehlstand von π, wenn $\pi(i) > \pi(j)$. Sei $1 \leq a < b \leq n$ und betrachte die Transposition π_{ab} von a und b. Ein Fehlstand muss klarerweise immer a oder b enthalten. Dann hat π_{ab} die Fehlstände (a, b), (a, j), wobei $a < j < b$ und (j, b), wobei $a < j < b$. Insgesamt ist die Anzahl der Fehlstände also ungerade. Da eine ungerade Anzahl an Kompositionen an Transpositionen immer eine ungerade Anzahl an Fehlständen hat, die Identität jedoch eine gerade Anzahl hat (nämlich 0), kann die Identität also nicht aus einer ungeraden Anzahl von Permutationen erzeugt werden.

□

Korollar 2.2.46. *Die Abbildung*

$$\mathrm{sgn} : S_n \to \{-1, 1\}, \pi \mapsto \#\ \textit{Transpositionen in der Darstellung von}\ \pi\ \textit{mod}\ 2$$

ist ein Gruppenhomomorphismus.

Beweis. Zuerst bemerken wir, dass die Abbildung aufgrund von Proposition 2.2.45 wohldefiniert ist. Zeigen wir nun die Verträglichkeit mit den Operationen. Es gilt klarerweise $\mathrm{sgn}(\mathrm{id}) = 1$. Seien nun $\pi, \pi' \in S_n$. Betrachten wir den Fall, dass π und π' Darstellungen durch eine gerade Anzahl an Permutationen haben, dann hat auch $\pi \circ \pi'$ eine Darstellung durch eine gerade Anzahl an Permutationen und es gilt $\mathrm{sgn}(\pi)\,\mathrm{sgn}(\pi') = \mathrm{sgn}(\pi \circ \pi')$. Die anderen drei Fälle sind analog. Zuletzt sei noch $\pi \in G$, dann ist $1 = \mathrm{sgn}(\mathrm{id}) = \mathrm{sgn}(\pi \circ \pi^{-1}) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\pi^{-1})$. Ist nun $\mathrm{sgn}(\pi) = 1$, so folgt $\mathrm{sgn}(\pi^{-1}) = 1 = \mathrm{sgn}(\pi)^{-1}$, der andere Fall ist analog. □

Bemerkung 2.2.47. Es ist die *alternierende Gruppe* $A_n := \ker \operatorname{sgn} \lhd S_n$ ein Normalteiler der symmetrischen Gruppe. Mit dem Homomorphiesatz erhält man, dass $S_n/A_n \cong \operatorname{ran} \operatorname{sgn} = (\{-1, 1\}, \cdot)$.

20.04.2023
26.04.2023

2.2.5 Abelsche Gruppen

Bemerkung 2.2.48. Sei $(G, \cdot, e, ^{-1})$ eine abelsche Gruppe, so ist G auch ein unitärer Modul über dem kommutativen 1-Ring $(\mathbb{Z}, +, 0, -, *, 1)$. Für $n \in \mathbb{Z}, g \in G$ definieren wir dazu $n \odot g := g^n$. Prüfen wir die Anforderungen an ein Modul. Seien $n, m \in \mathbb{Z}, g, h \in G$ beliebig. Dann ist

$$(n * m) \odot g = g^{n*m} = (g^m)^n = n \odot (m \odot g),$$

$$(n + m) \odot g = g^{n+m} = g^n \cdot g^m = (n \odot g) \cdot (m \odot g),$$

$$n \odot (g \cdot h) = (g \cdot h)^n = g^n \cdot h^n = (n \odot g) \cdot (n \odot h),$$

wobei wir bei der letzten Zeile verwenden, dass G abelsch ist.

Es stellt sich die Frage ob G auch ein Modul über einem anderen Ring ist. Sei angenommen es gäbe ein $m \in \mathbb{Z}$, sodass für alle $g \in G$ gilt $g^m = e$. Dann ist G ein unitärer Modul über $(\mathbb{Z}_m, +, 0, -, *, 1)$. Indirekt angenommen es gäbe ein $g \in G$ mit $g^m \neq e$, so wäre $g^0 = e$ ein Widerspruch.

Im Folgenden wollen wir statt $\cdot, *, \odot$ stets nur $\cdot$ schreiben.

Definition 2.2.49. Der *Exponent* einer Gruppe G ist definiert als

$$\exp(G) := \min\{m \in \mathbb{N} \setminus \{0\} \mid \forall g \in G : g^m = e\},$$

wobei wir $\exp(G) = \infty$ setzen, falls die obige Menge leer ist.

Bemerkung 2.2.50. Ist G also eine abelsche Gruppe mit $\exp(G) = m < \infty$, so ist G ein unitärer $\mathbb{Z}_m$-Modul vermöge $k \cdot g := g^k$ für $k \in \mathbb{Z}_m$.

Definition 2.2.51. Sei G eine Gruppe, $g \in G, p \in \mathbb{P}$, so nennen wir g ein *p-Element*, wenn es ein $k \in \mathbb{N}$ mit $\operatorname{ord}(g) = p^k$ gibt. Weiters definieren wir den *p-Anteil* von G als

$$G_p := \{g \in G \mid g \text{ ist } p\text{-Element }\}.$$

Hier sei daran erinnert, dass g *Torsionselement* heißt, wenn es ein $k \in \mathbb{Z} \setminus \{0\}$ mit $g^k = e$ gibt. Wir definieren

$$G_t := \{g \in G \mid g \text{ ist Torsionselement }\}.$$

Lemma 2.2.52. *Sei G eine abelsche Gruppe und seien $a_1, \ldots, a_n \in G_t$, so gelten:*

1. $\operatorname{ord}(a_1 \cdot \ldots \cdot a_n) \mid \operatorname{ord}(a_1) \cdot \ldots \cdot \operatorname{ord}(a_n)$
2. $[\forall i, j \in \{1, \ldots, n\}, i \neq j : \operatorname{ggT}(\operatorname{ord}(a_i), \operatorname{ord}(a_j)) = 1] \Rightarrow \operatorname{ord}(a_1 \cdot \ldots \cdot a_n) = \operatorname{ord}(a_1) \cdot \ldots \cdot \operatorname{ord}(a_n)$
3. $\exists a \in G : \operatorname{ord}(a) = \operatorname{kgV}(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_n))$

Beweis.

1. Wir zeigen die Aussage mittels Induktion nach n. Der Induktionsanfang $n = 1$ ist trivial. Zeigen wir also den Induktionsschritt $n \to n+1$. Setze $a := a_1 \cdot \ldots \cdot a_n$, so ist

$$(a_1 \cdot \ldots \cdot a_n \cdot a_{n+1})^{\mathrm{ord}(a)\cdot\mathrm{ord}(a_{n+1})} = a^{\mathrm{ord}(a)\cdot\mathrm{ord}(a_{n+1})} \cdot a_{n+1}^{\mathrm{ord}(a)\cdot\mathrm{ord}(a_{n+1})} = e,$$

   womit $\mathrm{ord}(a_1 \cdot \ldots \cdot a_{n+1}) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(a_{n+1})$, und nach Induktionsvoraussetzung und der Transitivität von $\mid$ also auch $\mathrm{ord}(a_1 \cdot \ldots \cdot a_{n+1}) \mid \mathrm{ord}(a_1) \cdot \ldots \cdot \mathrm{ord}(a_{n+1})$.

2. Wir zeigen die Aussage wieder mittels Induktion nach n. Der Induktionsanfang $n = 1$ ist trivial. Betrachten wir zunächst $n = 2$. Sei $\mathrm{ggT}(\mathrm{ord}(a_1), \mathrm{ord}(a_2)) = 1, m_1 = \mathrm{ord}(a_1), m_2 = \mathrm{ord}(a_2)$. Definiere $r := \mathrm{ord}(a_1 \cdot a_2)$, so ist

$$a_1^{r\cdot m_2} = a_1^{r\cdot m_2} \cdot a_2^{r\cdot m_2} = (a_1 \cdot a_2)^{r\cdot m_2} = e$$

   und wir schließen $m_1 \mid r \cdot m_2$. Da m_1, m_2 teilerfremd sind folgt damit $m_1 \mid r$. Analog erhalten wir $m_2 \mid r$ und damit $m_1 \cdot m_2 \mid r$. Nach 1 gilt $r \mid m_1 \cdot m_2$, insgesamt folgt also $r = m_1 \cdot m_2$. Der Induktionsschritt $n \to n+1$ folgt nun sofort mit der Induktionsvoraussetzung und dem Fall $n = 2$.

3. Wir zeigen die Aussage wieder mittels Induktion nach n. Der Induktionsanfang $n = 1$ ist trivial. Betrachten wir also wieder zunächst $n = 2$. Setze $m_i := \mathrm{ord}(a_i)$. Wir können nun $\mathrm{kgV}(m_1, m_2) = r_1 \cdot r_2$ schreiben, wobei $\mathrm{ggT}(r_1, r_2) = 1, r_1 \mid m_1, r_2 \mid m_2$. Betrachte nun $b_i := a_i^{m_i/r_i}$, so ist $\mathrm{ord}(b_i) = r_i$. Da r_1, r_2 teilerfremd sind, folgt durch 2 $\mathrm{ord}(b_1 \cdot b_2) = \mathrm{ord}(b_1)\,\mathrm{ord}(b_2) = r_1 \cdot r_2 = \mathrm{kgV}(m_1, m_2)$. Wieder folgt der Induktionsschritt $n \to n+1$ sofort mit der Induktionsvoraussetzung und dem Fall $n = 2$.

□

Korollar 2.2.53. *Sei G eine abelsche Gruppe mit $\exp(G) = m < \infty$. Dann gibt es ein $g \in G$, mit $\mathrm{ord}(g) = m$.*

Beweis. Sei $h \in G$ beliebig, so gilt $h^m = e$ und damit $\mathrm{ord}(h) \mid m$. Damit ist $M := \{\mathrm{ord}(h) \mid h \in G\}$ endlich, wir können also $M = \{\mathrm{ord}(h_1), \ldots, \mathrm{ord}(h_n)\}$, mit $h_i \in G$, schreiben. Nach *Lemma* 2.2.52 gibt es nun ein $g \in G$ mit $\mathrm{ord}(g) = \mathrm{kgV}(\mathrm{ord}(h_1), \ldots, \mathrm{ord}(h_n))$. Es gilt nun $h^{\mathrm{ord}(g)} = e$. Insgesamt folgt damit also

$$m \overset{h^{\mathrm{ord}(g)}=e}{\leq} \mathrm{ord}(g) \overset{\exp(G)=m,\, g\in G}{\leq} m$$

. □

Lemma 2.2.54. *Sei G eine abelsche Gruppe und sei $p \in \mathbb{P}$. Dann gilt:*

1. $G_p \leq G$
2. $G_t \leq G$

Beweis.

1. Seien $a, b \in G_p$, so gibt es $u, v \in \mathbb{N}$ mit $\mathrm{ord}(a) = p^u, \mathrm{ord}(b) = p^v$ und es gilt nach Lemma 2.2.52 $\mathrm{ord}(a \cdot b) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(b) = p^{u+v}$, also folgt $a \cdot b \in G_p$. Wegen $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$ folgt auch $a^{-1} \in G_p$.
2. Seien $a, b \in G_t$ mit $\mathrm{ord}(a) = x, \mathrm{ord}(b) = y$, so gilt $\mathrm{ord}(a \cdot b) \mid x \cdot y$, also $a \cdot b \in G_t$.

□

Lemma 2.2.55. *Sei G eine abelsche Gruppe und seien $p, p_1, \ldots, p_n \in \mathbb{P}$ paarweise verschieden, so ist*

$$G_p \cap (G_{p_1} \cdot \ldots \cdot G_{p_n}) = \{e\}.$$

Beweis. Sei $a \in G_{p_1} \cdot \ldots \cdot G_{p_n}$, es gibt also $a_i \in G_{p_i}$ mit $a = a_1 \cdot \ldots \cdot a_n$. Dann gilt $\operatorname{ord}(a) \mid \operatorname{ord}(a_1) \cdot \ldots \cdot \operatorname{ord}(a_n)$, also $\operatorname{ord}(a) = 1$, womit $a = e$ folgt. □

Lemma 2.2.56. *Sei G eine abelsche Gruppe und sei $a \in G$ mit $\operatorname{ord}(a) = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$, wobei $p_1, \ldots, p_n \in \mathbb{P}$ paarweise verschieden sind. Dann ist $a \in G_{p_1} \cdot \ldots \cdot G_{p_n}$.*

Beweis. Wir definieren

$$t_i := \frac{\operatorname{ord}(a)}{p_i^{e_i}}.$$

Dann ist $\operatorname{ggT}(t_1, \ldots, t_n) = 1$. Es gibt also $x_1, \ldots, x_n \in \mathbb{Z}$ mit $\sum_{i=1}^n x_i t_i = 1$. Um dies einzusehen betrachte

$$M := \left\{ \sum_{i=1}^n x_i t_i \mid x_1, \ldots x_n \in \mathbb{Z} \right\} \subseteq \mathbb{Z},$$

so ist $M \leq (\mathbb{Z}, +, 0, -)$ und $M = \langle \{t_1, \ldots, t_n\} \rangle$. Es gibt nun ein m mit $M = m\mathbb{Z}$. Dann gilt für alle i, dass $t_i \in M$, also $m \mid t_i$, womit $m = 1$ folgt und damit $M = \mathbb{Z}$.

Betrachte nun

$$a = a^1 = a^{\sum_{i=1}^n x_i t_i} = (a^{t_1})^{x_1} \cdot \ldots \cdot (a^{t_n})^{x_n}.$$

Es ist aber $\operatorname{ord}(a^{t_i}) = p_i^{e_i}$, womit wegen $((a^{t_i})^{p_i})^{e_i} = a^{\operatorname{ord}(a)} = e$ dann $a^{t_i} \in G_{p_i}$ folgt. □

26.04.2023
27.04.2023

Satz 2.2.57. *Sei G eine abelsche Torsionsgruppe. Dann ist $G = \bigodot_{p \in \mathbb{P}} G_p$.*

Beweis. Wir müssen lediglich zeigen, dass für alle $p \in \mathbb{P}, G_p \lhd G$ gilt, dann folgt die Aussage aus den Lemmata 2.2.55 und 2.2.56 und Proposition 2.2.33. Seien also $p \in \mathbb{P}, g \in G$ beliebig, wir wollen $gG_pg^{-1} \subseteq G_p$ zeigen. Da der p-Anteil nach Lemma 2.2.54 eine Untergruppe ist und G abelsch ist, ist die Behauptung offensichtlich wahr. □

Lemma 2.2.58. *Sei G eine abelsche p-Gruppe und $a \in G$ mit maximaler Ordnung p^n. Dann gilt:*

1. $\langle a \rangle \neq G \Rightarrow \exists b \in G \setminus \{e\} : \langle b \rangle \cap \langle a \rangle = \{e\}$
2. $\exists U \leq G : G = \langle a \rangle \odot U$

Beweis.

1. Sei $\langle a \rangle \neq G$ angenommen und $c \in G \setminus \langle a \rangle$ beliebig. Wir wissen, dass $c^{(p^n)} = e \in \langle a \rangle$. Sei $j \geq 1$ minimal mit $c^{(p^j)} \in \langle a \rangle$, also ist $c^{(p^j)} = a^\ell$ für ein $\ell \in \mathbb{Z}$. Betrachte $b := c^{(p^{j-1})} \cdot a^{-\ell/p}$. Damit dies wohldefiniert ist müssen wir zunächst $p \mid \ell$ zeigen. Wäre dies nicht so, so wäre $\operatorname{ggT}(\ell, p^n) = 1$, also $\langle a \rangle = \langle a^\ell \rangle \subsetneq \langle c \rangle$, womit $\operatorname{ord}(c) > \operatorname{ord}(a)$ wäre, im Widerspruch dazu, dass a maximale Ordnung hat.

   Nun gilt $b^p = c^{(p^j)} \cdot a^{-\ell} = e$. Da $c^{(p^{j-1})} \neq \langle a \rangle, a^{-\ell/p} \in \langle a \rangle$ folgt also $b \notin \langle a \rangle$, inbesondere ist $b \neq e$. Damit erhalten wir $\operatorname{ord}(b) = p$ und damit $\langle b \rangle \cong \mathbb{Z}_p$. Sei indirekt angenommen es gäbe ein $x \in (\langle a \rangle \cap \langle b \rangle) \setminus \{e\}$, dann wäre $b \in \langle x \rangle$, damit $b \in \langle a \rangle$, im Widerspruch. Also folgt $\langle a \rangle \cap \langle b \rangle = \{e\}$.

2. Sei $U \leq G$ maximal mit $U \cap \langle a \rangle = \{e\}$, vermöge Lemma von Zorn angewandt auf $(\{U \leq G \mid U \cap \langle a \rangle = \{e\}\}, \subseteq)$.

   Zunächst gilt für alle $V \leq G/_U, V \neq \{U\}$, dass $\langle aU \rangle \cap V \neq \{U\}$. Sonst wäre $U' := \{c \in G \mid \exists bU \in V : c \in bU\} \leq G$ eine echte Obermenge von U mit $\langle a \rangle \cap U' = \{e\}$, im Widerspruch zur Maximalität von U. Um Letzteres einzusehen sei $b \in \langle a \rangle \cap U'$, dann ist $bU \in \langle aU \rangle \cap V$ und damit $b \in U$, also $b \in U \cap \langle a \rangle$, also $b = e$.

   Damit gilt für alle $b \in G \setminus U$, dass $\langle bU \rangle \cap \langle aU \rangle \neq \{U\}$. Falls nun die Ordnung von aU maximal in $G/_U$ ist, so folgt mit 1. $\langle aU \rangle = G/_U$. Tatsächlich gilt $\operatorname{ord}(aU) = p^n = \operatorname{ord}(a)$, denn ist $a^k U = (aU)^k = U$, so gilt $a^k \in U$, womit $a^k = e$ folgen würde, also $k = p^n$.

   Nun existiert für alle $bU \in G/_U$ ein n mit $(aU)^n = bU$, also $u_1, u_2 \in U$ mit $a^n u_1 = b u_2$, also $a^n u_1 u_2^{-1} = b$ und damit $G = \langle a \rangle \odot U$.

□

Satz 2.2.59. *Sei G eine endliche, abelsche Gruppe. Dann gibt es $p_1, \ldots, p_n \in \mathbb{P}, e_1, \ldots e_n \in \mathbb{N} \setminus \{0\}$ und $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0\}$, sodass für alle $i < j$ gilt $(p_i, e_i) <_{lex} (p_j, e_j)$, und*

$$G \cong \left(C_{p_1^{e_1}}\right)^{m_1} \times \ldots \times \left(C_{p_n^{e_n}}\right)^{m_n}.$$

Diese Darstellung ist eindeutig.

Beweis. Zuerst wollen wir die Existenz zeigen: Es existieren $p_1, \ldots, p_\ell \in \mathbb{P}$ verschieden, sodass $G \cong G_{p_1} \times \ldots \times G_{p_\ell}$. Wir können also o. B. d. A. annehmen, dass G eine p-Gruppe ist ($p \in \mathbb{P}$).

Sei $a \in G$ mit maximaler Ordnung p^{e_n}, so wissen wir nach Lemma 2.2.58 $G \cong \langle a \rangle \times U$, wobei $\langle a \rangle \cong C_{p^{e_n}}$. Dies wird induktiv mit U wiederholt, wobei wir dies nur endlich oft machen müssen, da G endlich ist.

Zeigen wir nun noch die Eindeutigkeit: Sei

$$G \cong \left(C_{p_1^{e_1}}\right)^{m_1} \times \ldots \times \left(C_{p_n^{e_n}}\right)^{m_n} \cong \left(C_{q_1^{f_1}}\right)^{\ell_1} \times \ldots \times \left(C_{q_s^{f_s}}\right)^{\ell_s}.$$

Definiere $m := \max\{r^v | r \in \mathbb{P}, v \geq 1, \exists a \in G : \operatorname{ord}(a) = r^v\}$. Dann existieren $i \in \{1, \ldots, n\}$ und $j \in \{1, \ldots, s\}$ mit $m = (p_i)^{e_i} = (q_j)^{f_j}$. Damit haben die beiden Darstellungen einen Faktor gemeinsam. Damit ist $G/(C_m)$ eine Gruppe mit weniger Elementen als G, welche isomorph zu den beiden Gruppen

$$\left(C_{p_1^{e_1}}\right)^{m_1} \times \ldots \times \left(C_{p_i^{e_i}}\right)^{m_i - 1} \times \ldots \times \left(C_{p_n^{e_n}}\right)^{m_n} \quad \text{und} \quad \left(C_{q_1^{f_1}}\right)^{\ell_1} \times \ldots \times \left(C_{q_j^{f_j}}\right)^{\ell_j - 1} \times \ldots \times \left(C_{q_s^{f_s}}\right)^{\ell_s}$$

ist. Induktives Verfahren liefert damit die Eindeutigkeit der Darstellung. □

27.04.2023
03.05.2023

2.3 Ringe

Zu Beginn dieses Abschnitts sei an Definition 1.1.14 eines *Rings* erinnert.

Beispiel 2.3.1. Ringe sind unter anderen

- der kommutative Ring mit 1 der ganzen Zahlen $(\mathbb{Z}, +, 0, -, \cdot, 1)$,

- der kommutative Ring mit 1 der reellen Polynomfunktionen $(P, +, 0, -\cdot, 1)$, wobei $P \subseteq \mathbb{R}^{\mathbb{R}}$ die Menge aller Polynomfunktionen ist, $+, \cdot$ punktweise Operationen sind und $0, 1$ konstante Polynome mit entsprechendem Wert,
- der (nicht kommutative) Ring mit 1 der reellen 2×2 Matrizen $(\mathbb{R}^{2\times 2}, +, (0)_{2\times 2}, -, \cdot, E_2)$ und
- der kommutative Ring $(m\mathbb{Z}, +, 0, -, \cdot), m \geq 2$ der kein Einselement enthält.

Bemerkung 2.3.2. Wie auch schon im Abschnitt über Gruppen werden wir im Folgenden für einen Ring $\mathfrak{R} = (R, +, 0, -, \cdot)$ mit Einselement 1, falls dieses existiert nur R schreiben, also den Ring mit der Trägermenge identifizieren.

Definition 2.3.3. Sei R ein Ring, so heißt $\emptyset \neq I \subseteq R$ *Ideal*, oder kurz $I \lhd R$, genau dann wenn

- $(I, +, 0, -)$ eine Untergruppe von R ist und
- $\forall r \in R : rI \subseteq I \wedge Ir \subseteq I$.

Gilt bei letzterer Bedingung nur $rI \subseteq I$, beziehungsweise $Ir \subseteq I$, so heißt I *Linksideal*, beziehungsweise *Rechtsideal*.

Bemerkung 2.3.4. Ein Ideal I eines Rings R ist definitionsgemäß eine Untergruppe der additiven Gruppe $(R, +, 0, -)$.

Weiters ist I sogar ein Unterring von R, da I nach Definition unter $\cdot$ abgeschlossen ist.

Bemerkung 2.3.5. Für ein Ideal I eines Rings R gilt $1 \in I \Leftrightarrow I = R$. Nach der Definition ist $I \subseteq R$, für die andere Richtung bemerken wir, dass für alle $r \in R$ gilt $r \cdot 1 = r \in I$.

Beispiel 2.3.6. Betrachte den Ring $(\mathbb{Q}, +, 0, -, \cdot, 1)$, so ist $\mathbb{Z}$ ein Unterring, jedoch kein Ideal.

Beispiel 2.3.7. Es ist $m\mathbb{Z} \subseteq (\mathbb{Z}, +, 0, -, \cdot, 1)$ ein Ideal. Sei P der Ring der reellen Polynomfunktionen. Dann ist $(x^2 + 1) \cdot P \lhd P$. Dies ist ein allgemeines Prinzip, wie wir später noch sehen werden.

Sei M eine Menge und betrachte den Ring $(\mathcal{P}(M), \triangle, \emptyset, \mathrm{id}_{\mathcal{P}(M)}, \cap, M)$. Sei $A \subseteq M$ beliebig, so ist $\mathcal{P}(A) \lhd \mathcal{P}(M)$. Weiters kann $(\mathcal{P}(A), \triangle, \emptyset, \mathrm{id}_{\mathcal{P}(A)}, \cap, A)$ zu einem Ring mit 1 gemacht werden. Es handelt sich dabei um keinen Widerspruch zu Bemerkung 2.3.5, da hier ein anders Einselement gefunden wird als im ursprünglichen Ring.

Bemerkung 2.3.8. Sei $(R, +, 0, -, \cdot)$ ein Ring und $\sim \subseteq R^2$ eine Kongruenzrelation auf R. Dann ist $\sim$ insbesondere eine Kongruenzrelation auf $(R, +, 0, -)$, womit $\sim$ eindeutig durch $[0]_\sim$ bestimmt ist.

Sind $x, y \in R$ beliebig, $x, y \in [0]_\sim$, so gilt $x + y \in [0]_\sim, (-x) \in [0]_\sim$, vergleiche die Theorie von Normalteilern von Gruppen. Sei $r \in R$ beliebig, so gilt $x \sim 0, r \sim r$, und da $\sim$ Kongruenzrelation ist damit $r \cdot x \sim 0 \cdot r = 0$, also folgt $[0]_\sim \lhd R$.

Umgekehrt sei $I \lhd R$ ein Ideal, wir wollen eine entsprechende Kongruenzrelation $\sim$ definieren. Für $x, y \in R$ definieren wir

$$x \sim y :\Leftrightarrow y - x \in I.$$

Wir wissen, dass $\sim$ eine Kongruenzrelation bezüglich $(R, +, 0, -)$ ist. Sei $a \sim b, c \sim d$, dann folgt

$$(a - b) \cdot d \in I, \quad a \cdot (c - d) \in I \implies (a - b) \cdot d + a \cdot (c - d) \in I.$$

Letzerer Ausdruck ist jedoch gleich

$$ad - bd + ac - ad = -(bd - ac),$$

also folgt $ac \sim bd$ und $\sim$ ist auch eine Kongruenzrelation bezüglich $\cdot$.

Definition 2.3.9. Sei R ein Ring, $I \lhd G$ ein Ideal, dann definieren wir für $a \in R$ die *Nebenklasse von a modulo I* als

$$a + I := \{a + r \mid r \in I\}.$$

Definition 2.3.10. Sei R eine Ring, $I \lhd G$ ein Ideal und $\sim$ die wie in Bemerkung 2.3.8 vom Ideal induzierte Kongruenzrelation. Wir definieren den *Faktorring*

$$R/_I := R/_\sim = \{a + I \mid a \in R\}.$$

Dabei ist

$$(a + I) + (b + I) := (a + b) + I \quad \text{und} \quad (a + I) \cdot (b + I) = (a \cdot b) + I.$$

Definition 2.3.11. Sei R ein Ring, $A \subseteq R$, $a \in R$, so heißen

$$(A) := \bigcap \{I \lhd R \mid A \subseteq I\},$$

$$(a) := \bigcap \{I \lhd R \mid a \in I\}$$

die von A, beziehungsweise a, *erzeugten Ideale*.

Bemerkung 2.3.12. Man beachte dass (A) und (a) tatsächlich Ideale sind, da Ideale unter Schnitten abgeschlossen sind.

Bemerkung 2.3.13. Wir bemerken, dass gilt

$$(A) = \left\{ \sum_i r_i a_i s_i + \sum_j r'_j a'_j + \sum_k a''_k s''_k + \sum_\ell a'''_\ell \mid a_i, a'_j, a''_k \in A, a'''_\ell \in A \cup (-A), r_i, r'_j, s_i, s''_k \in R \right\}.$$

Ist R sogar ein kommutativer Ring mit 1, so gilt

$$(A) = \left\{ \sum_i r_i a_i \mid r_i \in R, a_i \in A \right\}.$$

Definition 2.3.14. Sei R ein Ring. Wir nennen $I \lhd R$ *Hauptideal*, wenn gilt

$$\exists a \in R : I = (a).$$

Weiters nennen wir R einen *Hauptidealring*, wenn gilt

$$\forall I \lhd R : I \text{ ist Hauptideal.}$$

Beispiel 2.3.15. Es ist $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ein Hauptidealring, da alle Unterringe von der Form $m\mathbb{Z} = (m)$ sind.

Definition 2.3.16. Ein Ring R heißt *nullteilerfrei*, wenn

$$\forall a, b \in R : (a \cdot b = 0 \Rightarrow a = 0 \vee b = 0)$$

Ist R ein kommutativer Ring mit 1 und nullteilerfrei, so nennen wir R *Integritätsbereich*.

Beispiel 2.3.17. Ist R ein Körper, so ist R nullteilerfrei, da mit $0 \neq a \in R, b \in R$ gilt

$$ab = 0 \Rightarrow b = a^{-1}ab = a^{-1}0 = 0.$$

Beispiel 2.3.18. Es ist $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ein Integritätsbereich, jedoch kein Körper.

Proposition 2.3.19. *Ist R ein Integritätsbereich und endlich, so ist R ein Körper.*

Beweis. Sei $r \in R \setminus \{0\}$, wir wollen ein multiplikatives Inverses finden. Betrachte die Abbildung

$$\varphi_r : R \to R, x \mapsto r \cdot x.$$

φ_r ist injektiv: Sei $\varphi_r(x) = \varphi_r(y)$, so folgt $rx = ry$, also $r(x - y) = 0$, also $x - y = 0$, also $x = y$. Da R endlich ist, ist damit φ_r auch surjektiv, also gibt es ein $x \in R$ mit $\varphi_r(x) = r \cdot x = 1$. □

Proposition 2.3.20. *Sei R ein kommutativer Ring mit 1, dann ist R ein Körper genau dann, wenn*

$$\forall I \lhd R : (I = \{0\} \vee I = R).$$

Beweis.

- $\Rightarrow$: Sei $I \neq \{0\}, x \in I, x \neq 0$, so ist $1 = x^{-1}x \in I$, also $I = R$.
- $\Leftarrow$: Sei R kein Körper, so gibt es ein $x \in R \setminus \{0\}$ sodass für alle $y \in R$ gilt $xy \neq 1$. Setze $I := (x) \lhd R$, so gilt wegen $x \in I$ dass $I \neq \{0\}$. Wegen $1 \notin I$ ist auch $I \neq R$.

□

Definition 2.3.21. Sei $I \lhd R$. Wir nennen I

- *echt*, wenn $I \subsetneq R$,
- *prim*, wenn I echt ist und $\forall a, b \in R : (ab \in I \Rightarrow a \in I \vee b \in I)$ und
- *maximal*, wenn I echt ist und $\forall J \lhd R : J \supsetneq I \Rightarrow J = R$.

Beispiel 2.3.22. Sei $p \in \mathbb{P}$, so ist $p\mathbb{Z} \lhd \mathbb{Z}$ prim. Ist $m \in \mathbb{N}_{\geq 2} \setminus \mathbb{P}$, so ist $m\mathbb{Z}$ nicht prim.

Proposition 2.3.23. *Sei R ein kommutativer Ring mit 1 und $I \lhd R$. Dann gilt:*

- *$R/_I$ ist Körper $\Leftrightarrow$ I ist maximal*
- *$R/_I$ ist prim $\Leftrightarrow$ I ist prim*
- *I ist maximal $\Rightarrow$ I ist prim*
- *I ist echt $\Rightarrow \exists J \supseteq I : J \lhd R$ ist maximal*

Beweis.

1. $\Rightarrow$: Angenommen I wäre nicht maximal, es gibt also ein $R \neq J \supsetneq I, J \lhd R$. Sei $J' := \{a + I \mid a \in J\}$. Dann ist $J' \lhd R/I, J' \neq R/I$ und $J \neq \{I\}$. Also hat R/I ein echtes Ideal, im Widerspruch dazu, dass R/I ein Körper ist.

   $\Leftarrow$: Sei I maximal. Wir behaupten, dass R/I keine echten Ideale außer dem trivialen hat. Wäre dies nicht so, so sei $J \lhd R/I$ echt, $J \neq \{I\}$ und sei $J' := \bigcup_{M \in J} M$. Dann ist $J' \supsetneq I, J' \neq R, J' \lhd R$, im Widerspruch zur Maximalität von I.

2. Es gilt

$$\begin{aligned} R/I \text{ ist Integritätsbereich} &\Leftrightarrow \forall a, b \in R : (a + I)(b + I) = I \Rightarrow a + I = I \vee b + I = I \\ &\Leftrightarrow \forall a, b \in R : ab \in I \Rightarrow a \in I \vee b \in I \\ &\Leftrightarrow I \text{ ist prim.} \end{aligned}$$

3. Folgt direkt aus (1) und (2).

4. Diese Aussage kann leicht mit dem bekannten Lemma von Zorn bewiesen werden. Dazu wird die Menge aller echten Ideale J mit $J \supseteq I$ mittels Mengeninklusion partiell geordnet. Ist nun $\mathcal{K}$ eine Kette von Idealen, so stellt $\bigcup_{J \in \mathcal{K}} J$ wieder ein Ideal dar. Dieses ist tatsächlich echt, denn es gilt für jedes Ideal $J \in \mathcal{K} : 1 \notin J$, also ist $1 \notin \bigcup_{J \in \mathcal{K}} J$. Klarerweise ist die Vereinigung damit eine obere Schranke und aus dem Lemma von Zorn folgt nun die Existenz eines maximalen Elements. Dieses maximale Element ist auch maximal in der Menge aller echten Ideale und ist trivialerweise eine Obermenge von I.

□

03.05.2023
04.05.2023

Beispiel 2.3.24. Betrachte den Ring $\mathbb{Z}$, $p \in \mathbb{P}$ und $p\mathbb{Z} \lhd \mathbb{Z}$, so erhalten wir $\mathbb{Z}/_{p\mathbb{Z}} = \mathbb{Z}_p$. $p\mathbb{Z}$ ist dabei ein Primideal und $\mathbb{Z}_p$ ein Körper.

Für ein $m \in \mathbb{N}$ betrachte $m\mathbb{Z} \lhd \mathbb{Z}$, so ist zwar $\mathbb{Z}/_{m\mathbb{Z}} = \mathbb{Z}_m$, jedoch kein Integritätsbereich, also insbesondere kein Körper.

Beispiel 2.3.25. Sei P die Menge der Polynomfunktionen auf $\mathbb{R}$ und $(x^2 + 1) \cdot P \lhd P$, so ist dies ein Primideal, und $P/_{(x^2+1)\cdot P}$ sogar ein Integritätsbereich. Jedoch ist es kein Körper, da $(x^2 + 1) \cdot P$ nicht maximal ist – betrachte dazu beispielsweise

$$(x^2 + 1) \cdot P \subsetneq (x^2 + 1) \cdot P + x \cdot P \lhd P$$

.

Das Ideal $I := (x^2-1) \cdot P \lhd P$ ist kein Primideal, da $(x-1) \notin I, (x+1) \notin I$, aber $(x-1)(x+1) = x^2 - 1 \in I$.

Definition 2.3.26. Wir definieren die *Charakteristik* eines Rings als

$$\operatorname{char} R := \begin{cases} \min\{n \in \mathbb{N} \mid \sum_{i=1}^{n} 1 = 0\} & \text{falls existent,} \\ 0 & \text{sonst.} \end{cases}$$

Beispiel 2.3.27. Für $m \in \mathbb{N}$ ist $\mathbb{Z}_m$ ein bekanntes Beispiel für einen Ring mit Charakteristik m. $(\mathbb{Z}_m)^{\mathbb{N}}$ ist beispielsweise ein unendlicher Ring mit Charakteristik m.

Proposition 2.3.28. *Sei R ein Ring mit 1,* $\operatorname{char} R = p \in \mathbb{P}$. *Dann ist*

$$\varphi : R \to R, x \mapsto x^{p^k}$$

ein Homomorphismus.

Beweis. Wir zeigen die Aussage mittels Induktion nach k.

Induktionsanfang ($k = 1$): Es gilt

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-1}.$$

Wir beobachten

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-i+1)}{1 \cdot \ldots \cdot i} \equiv 0 \bmod p$$

für $i \neq 0, p$, daher folgt $(a+b)^p \equiv a^p + b^p \bmod p$.

Induktionsschritt ($k \to k+1$): Es gilt unmittelbar

$$(a+b)^{p^{k+1}} = (a^{p^k} + b^{p^k})^p = a^{p^{k+1}} + b^{p^{k+1}}.$$

□

Bemerkung 2.3.29. Sei R ein kommutativer Ring mit 1, wir wollen R in einen Körper einbetten. Es gelte o. B. d. A. $0 \neq 1$ (da sonst für alle x gilt $x = 1 \cdot x = 0 \cdot x = 0$). Wir sammeln nun notwendige Voraussetzungen.

Es muss R ein Integritätsbereich sein, da $rs = 0 \Rightarrow r^{-1}rs = s = 0$ für $r, s \in R$ folgen wird.

Nicht notwendig (da es aus der vorigen Bedingung folgt), aber interessant ist die Tatsache, dass wenn R ein Integritätsbereich ist, jedes Element außer 0 bereits kürzbar ist. Denn für $r, x, y \in R, r \neq 0$ gilt $rx = ry \Rightarrow r(x-y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.

Es ist $R^* := R \setminus \{0\}$ ein kommutatives Monoid mit der Operation $\cdot$. Definiere eine Äquivalenzrelation $\sim \subseteq (R \times R^*)^2, (a,b) \sim (c,d) :\Leftrightarrow ad = bc$. Wie man nachrechnet ist dies sogar eine Kongruenzrelation. Dann ist $((R \times R^*)/_\sim, \cdot, [(1,1)]_\sim) =: M$ ein Monoid, wobei jedes $[(x,y)]_\sim$ mit $x \neq 0$ ein Inverses besitzt.

Dann ist

$$\varphi : R \to M, x \mapsto [(x,1)]_\sim$$

eine homomorphe Einbettung von R in M.

Für jedes multiplikative Monoid N mit einer Einbettung $\psi : R \to N$ und der Eigenschaft

$$\forall x \in R^* \exists y \in N : y\varphi(x) = \varphi(x)y = 1$$

gibt es eine Einbettung $\bar{\psi} : M \to N$ mit $\bar{\psi} \circ \varphi = \psi$.

Auf M definieren wir nun eine Addition

$$(a,b) + (c,d) := (ad + bc, bd), \quad -(a,b) := (-a, b),$$

so ist $(R \times R^*, +, (0,1), -)$ eine Gruppe.

Lemma 2.3.30. *Die in Bemerkung 2.3.29 definierte Äquivalenzrelation $\sim \subset (R \times R^*)^2$ ist eine Kongruenzrelation bezüglich $+$.*

Beweis. Seien $(z_1, n_1), (z_1', n_1'), (z_2, n_2), (z_2', n_2') \in R \times R^*$ mit $(z_1, n_1) \sim (z_1', n_1')$ und $(z_2, n_2) \sim (z_2', n_2')$ gegeben. Dann ist zu zeigen, dass $(z_1 n_2 + z_2 n_1, n_1 n_2) \sim (z_1' n_2' + z_2' n_1', n_1' n_2')$ gilt. Die Behauptung folgt durch Einsetzen in die Definition:

$$(z_1 n_2 + z_2 n_1) n_1' n_2' = \overbrace{z_1 n_1'}^{z_1' n_1} n_2 n_2' + \overbrace{z_2 n_2'}^{z_2' n_2} n_1 n_1' = (z_1' n_2' + z_2' n_1') n_1 n_2$$

□

Satz 2.3.31. *Sei R ein kommutativer Ring mit $1 \neq 0$, der zusätzlich ein Integritätsbereich ist. Sei weiters $\sim \subseteq (R \times R^*)^2$ wie in Bemerkung 2.3.29 definiert. Dann gilt:*

1. *$K := (R \times R^*)/_\sim$ mit $+, \cdot$ aus Bemerkung 2.3.29 ist ein Körper.*
2. *$\varphi : R \to K, x \mapsto [(x, 1)]_\sim$ ist eine Einbettung.*
3. *Für alle Einbettungen $\psi : R \to L$ in einen Körper L gibt es eine Einbettung $\bar{\psi} : K \to L$ mit $\bar{\psi} \circ \varphi = \psi$.*

Beweis. Wir haben bereits gezeigt, dass $\sim$ eine Kongruenzrelation ist, womit K wohldefiniert ist.

Wir wissen $(K, \cdot, [(1,1)]_\sim)$ ist ein kommutatives Monoid.

Weiters ist $(K \setminus \{[(0,1)]_\sim\}, \cdot, [(1,1)]_\sim) = (R^* \times R^*)/_\sim$ eine kommutative Gruppe, genauso auch $(K, +, [(0,1)]_\sim, -)$.

Das Distributivgesetz verifiziert man unmittelbar durch Nachrechnen.

Nach Konstruktion ist φ eine injektive Einbettung bezüglich $\cdot$. Allerdings gilt für $a, b \in R$, dass $\varphi(a+b) = [(a+b, 1)]_\sim = [(1a + 1b, 1 \cdot 1)]_\sim = [(a,1)]_\sim + [(b,1)]_\sim = \varphi(a) + \varphi(b)$. Wegen $\varphi(0) = [(0,1)]_\sim \varphi(0) = 0$ wird auch das neutrale Element von φ erhalten, woraus bereits die Verträglichkeit mit additiven Inversen folgt. Daher ist φ sogar eine Einbettung bezüglich $+$.

Sei $\psi : R \to L$ eine Einbettung in einen Körper L. Nach der Monoidkonstruktion gibt es eine Einbettung $\bar{\psi} : K \to L$ bezüglich $\cdot$ mit $\bar{\psi} \circ \varphi = \psi$. Wir verifizieren nun, dass $\bar{\psi}$ mit der Addition verträglich ist:

$$\begin{aligned}
\bar{\psi}([(z_1, u_1)]_\sim + [(z_2, u_2)]_\sim) &= \bar{\psi}([(z_1 u_2 + z_2 u_1, u_1 u_2)]_\sim) \\
&= \bar{\psi}([(z_1 n_2 + z_2 n_1, 1)]_\sim) \cdot \bar{\psi}([(1, n_1 n_2)]_\sim) \\
&= \overbrace{\bar{\psi} \circ \varphi}^{=\psi}(z_1 n_2 + z_2 n_1) \cdot \bar{\psi}([(1, n_1 n_2)]_\sim) \\
&= \big(\overbrace{\bar{\psi}}^{\bar{\psi} \circ \varphi}(z_1 n_2) + \overbrace{\bar{\psi}}^{\bar{\psi} \circ \varphi}(z_2 n_1)\big) \cdot \bar{\psi}([(1, n_1 n_2)]_\sim) \\
&= \bar{\psi}([(z_1 n_2, 1)]_\sim) \cdot \bar{\psi}([(1, n_1 n_2)]_\sim) + \bar{\psi}([(z_2 n_1, 1)]_\sim) \cdot \bar{\psi}([(1, n_1 n_2)]_\sim) \\
&= \bar{\psi}([(z_1, n_1)]_\sim) + \bar{\psi}([(z_2, n_2)]_\sim)
\end{aligned}$$

□

Proposition 2.3.32. *Sei L ein Körper mit der obigen Eigenschaft (3) aus Satz 2.3.31, so gilt bereits $L \cong K$, wobei K unser konstruierter Körper ist.*

Beweis. Gegeben sind also $\varphi : R \to K$ und $\varphi_0 : R \to L$ jeweils mit Eigenschaft (3). Daher existieren $\bar{\varphi} : L \to K$ mit $\bar{\varphi} \circ \varphi_0 = \varphi$ und $\varphi_0 : K \to L$ mit $\bar{\varphi_0} \circ \varphi = \varphi_0$. Wir zeigen zuerst die folgenden Behauptung. Für jeden injektiven Homomorphismus $\xi : K \to K$ mit $\xi|_{\varphi(R)} = \mathrm{id}_R$ folgt $\xi = \mathrm{id}$. Dies folgt aus der folgenden Rechnung:

$$\xi([(a,b)]_\sim) = \xi([(a,1)]_\sim)\xi([1,b]_\sim) = [(a,1)]_\sim \cdot [(b,1)]_\sim^{-1} = [(a,b)]_\sim.$$

Insbesondere gilt daher $\bar{\varphi} \circ \bar{\varphi_0} = \mathrm{id}_K$, da $(\bar{\varphi} \circ \bar{\varphi_0} \circ \varphi)(a) = (\bar{\varphi} \circ \varphi_0)(a) = \varphi(a)$ gilt. □

Definition 2.3.33. Sei R ein kommutativer Ring mit $1 \neq 0$ und ein Integritätsbereich. Dann wird der Körper $(R \times R^*)/_\sim$ aus Satz 2.3.31 *Quotientenkörper von* R genannt. Für $[(z,n)]_\sim$ schreibt man auch $\frac{z}{n}$.

Bemerkung 2.3.34. Die letzten beiden Theoreme liefern uns folgendes Ergebnis: Zu einem kommutativen Ring mit $1 \neq 0$ der ein Integritätsbereich ist, kann der Quotientenkörper konstruiert werden. Dieser ist (bis auf Isomorphie) eindeutig bestimmt und der kleinste Körper der R enthält.

Definition 2.3.35. Sei R eine Ring mit 1. Wir definieren den *Polynomring über* R

$$R[x] := \left\{ (x_n)_{n\in\mathbb{N}} \in R^{\mathbb{N}} \;\middle|\; |\{x_n \neq 0 \mid n \in \mathbb{N}\}| < \infty \right\}$$

mit den Operationen

$$+ : R[x] \times R[x] \to R[x], ((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \mapsto (x_n + y_n)_{n\in\mathbb{N}}$$
$$\cdot : R[x] \times R[x] \to R[x], ((x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}) \mapsto \left(\sum_{i=0}^{n} x_i y_{n-i} \right)_{n\in\mathbb{N}}$$

Elemente von $R[x]$ bezeichnen wir als *Polynome*.

Weiter definieren wir den Ring der *formalen Potenzreihen*

$$R[[x]] := \left\{ (x_n)_{n\in\mathbb{N}} \in R^{\mathbb{N}} \right\}$$

mit denselben Operation wie oben.

Die Elemente von $R[x]$ wollen wir auch als $p(x) = \sum_{i=0}^{n} a_i x^i$ auffassen, wenn $a_i = 0$ für $i > n$ gilt. Formal ist hier eigentlich die Folge der Koeffizienten ein Element des Ringes. Weiters schreiben wir für die Elemente von $R[[x]]$ auch $p(x) = \sum_{i=0}^{\infty} a_i x^i$.

Bemerkung 2.3.36. Alternativ kann der Polynomring wie folgt definiert werden:

Sei R ein kommutativer Ring mit 1, x eine Variable und definiere

$$R[x] := \{t(x) \mid t \text{ Term über } x \text{ in Sprache } +, \cdot, (r)_{r\in R}\}/_\sim,$$

wobei $\sim$ die von Gesetzen der kommutativen Ringe mit 1 und Gesetzen in R erzeugte Äquivalenzrelation ist. In $R[x]$ gilt also beispielsweise

$$x + x \cdot x = x \cdot x + x, \quad r \cdot (s \cdot x) = (r \cdot s) \cdot x.$$

Vorteil von Definition 2.3.35 ist, dass analog auch die Verallgemeinerung der formalen Potenzreihen definiert werden kann, was mit diesem Ansatz nicht möglich ist.

Proposition 2.3.37. *Sei R ein kommutativer Ring mit* 1*. Dann gilt:*

- *$R[x]$ ist ein kommutativer Ring mit* 1*.*
- *$R[x] \subseteq R[[x]]$*
- *R ist in $R[x]$ eingebettet vermöge $r \mapsto \sum_{i=0}^{0} rx^i$*
- *R ist ein Integritätsbereich $\Leftrightarrow$ $R[x]$ und $R[[x]]$ sind Integritätsbereiche.*

04.05.2023
10.05.2023

Definition 2.3.38. Sei R ein Ring mit $1 \neq 0$ und ein Integritätsbereich. Dann nennen wir den Quotientenkörper von $R[x]$

$$R(x) := \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x), q(x) \in R[x], q(x) \neq 0 \right\} \Big/ _{\sim}$$

mit der üblichen Relation $\frac{p}{q} \sim \frac{r}{s} \Leftrightarrow sp = qr$ den Körper der *gebrochen rationalen Funktionen*.

Bemerkung 2.3.39. Ist R ein Ring mit $1 \neq 0$ und ein Integritätsbereich so kann der Quotientenkörper K und dann von diesem der Polynomring $K[x]$ betrachten werden. Dieser besitzt nun einen Quotientenkörper $K(x)$. Andererseits kann man auch den Quotientenkörper des Polynomrings über R betrachten und erhält durch $R(x)$ einen dazu isomorphen Körper, also $K(x) \cong R(x)$.

Bemerkung 2.3.40. Als Verallgemeinerung des Polynomrings kann man auch den Polynomring in n-Variablen $x_1, \ldots, x_n$ rekursiv definieren durch $R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$. Auch für eine beliebige Variablenmenge X kann eine Verallgemeinerung getroffen werden, indem man mit $R[x]$ die Terme über der Sprache $(+, 0, -, \cdot, 1, (x)_{x \in X}, (m_r)_{r \in R})$ nach den Ringgesetzen und Gleichheiten in R faktorisiert.

Definition 2.3.41. Sei K ein Körper. Dann heißt K *algebraisch abgeschlossen*, wenn

$$\forall p(x) \in K[x] : p \notin {}^4K \Rightarrow \exists a \in K : p(a) = 0$$

gilt.

Satz 2.3.42 (Nullstellensatz von Hilbert, klein)**.** *Sei K ein algebraisch abgeschlossener Körper und $I \lhd K[x_1, \ldots, x_n]$ ein echtes Ideal. Dann gilt $\exists (a_1, \ldots, a_n) \in K^n : \forall p(x_1, \ldots, x_n) \in I : p(a_1, \ldots, a_n) = 0$.*

Bemerkung 2.3.43. Satz 2.3.42 ist nicht Teil dieser Lehrveranstaltung, sondern soll nur einen Ausblick auf die Algebra 2 Vorlesung geben. Die Anforderung an ein echtes Ideal sind dabei sehr natürlich. Ein echtes Ideal kann nämlich keine Konstanten c enthalten, da sonst $c \in I \Rightarrow c^{-1}c \in I \Rightarrow I = K[x_1, \ldots, x_n]$ gilt. Ist außerdem F eine beliebige Menge von Polynomen mit einer gemeinsamen Nullstelle, so überzeugt man sich leicht davon, dass auch jedes Polynom aus dem erzeugten Ideal von F an dieser Stelle den Wert 0 annimmt. Daher kann o. B. d. A. angenommen werden, dass F sogar ein Ideal ist.

Proposition 2.3.44. *Sei R ein kommutativer Ring mit* 1 *und X eine Variablenmenge. Dann gilt:*

[4] Hier wird K mittels der Einbettung aus Proposition 2.3.37 als Teilmenge betrachtet.

1. $R \leq R[X]$
2. *Für jeden Ring S mit $R \leq S$ und jeden Homomorphismus $\varphi : X \to S$ existiert genau ein Homomorphismus $\bar{\varphi} : R[X] \to S$, sodass $\bar{\varphi}|_X = \varphi$ und $\bar{\varphi}|_R = \mathrm{id}_R$ gilt.*

Beweis. Der Beweis verläuft analog wie bei den freien Algebren. □

Definition 2.3.45. Sei R eine Ring und $I \lhd R$. Dann definieren wir für $r, s \in R$:

$$r \equiv s \mod I :\Leftrightarrow r - s \in I.$$

Wir sagen auch *r ist s modulo I*.

Satz 2.3.46 (Chinesischer Restsatz, allgmeien)**.** *Seien R ein kommutativer Ring mit 1 und $I_1, \ldots, I_n \lhd R$ mit $\forall i \neq j \Rightarrow I_i + I_j = R$.*

Dann wird $I := \bigcap_{i=1}^n I_i$ definiert und es gilt:

1. *$\forall r_1 \ldots, r_n \in R \, \exists r \in R : \forall i \in \{1, \ldots, n\} : r \equiv r_i \mod I_i$. Weiters ist r modulo I eindeutig bestimmt.*
2. *$\varphi : R/_I \to R/_{I_1} \times \ldots \times R/_{I_n}, r + I \mapsto (r + I_1, \ldots, r + I_n)$ ist ein Isomorphismus.*

Beweis. Zuerst stellen wir die Behauptung $\forall i = 2, \ldots, n : I_1 + (I_2 \cap \ldots \cap I_n) = R$ auf, welche wir mit Induktion beweisen wollen:

Induktionsanfang ($i = 2$): Die Behauptung gilt laut Voraussetzung.

Induktionsschritt ($i \to i + 1$): Da R ein Ring mit 1 ist gilt $R = R \cdot R$. Nun kann die Induktionsannahme auf den ersten Faktor und die Voraussetzung des Satzes auf den zweiten Faktor angewendet werden, woraus man $R \cdot R = (I_1 + (I_2 \cap \ldots \cap I_i)) \cdot (I_1 + I_{i+1})$ erhält. Das ist offensichtlich eine Teilmenge von $I_1 + (I_2 \cap \ldots \cap I_i) \cdot I_{i+1}$. Der zweite Summand ist eine Teilmenge von I_{i+1}, da I_{i+1} ein (Links-)Ideal ist. Gleichzeitig ist er eine Teilmenge von $I_2 \cap \ldots \cap_i$, da diese Menge ein (Rechts-)Ideal ist. Damit folgt, dass $R = R \cdot R$ schon in $I_1 + (I_2 \cap \ldots \cap I_{i+1})$ enthalten sein muss, also die Gleichheit.

Analog gilt mit der Definition $I_i' := \bigcap_{j \neq i} I_j$, dass für alle $i \in \{1, \ldots, n\}$ auch $I_i + I_i' = R$ ist. Daher existieren für jedes $i \in \{1, \ldots, n\}$ ein $a_i \in I_i$ und ein $a_i' \in I_i'$ mit $r_i = a_i + a_i'$. Definiert man nun $r := \sum_{i=1}^n a_i'$, so erhält man für alle $i \in \{1, \ldots, n\}$, dass $r \equiv a_i' \equiv r_i \mod I_i$ gilt, also die Existenz.

Dieses Element ist eindeutig modulo I bestimmt, denn falls r' und r beide die gewünschte Eigenshaft haben, so folgt $r' - r \in I_i$ für alle i, also $r' - r \in \bigcap_{i=1}^n I_i = I$.

Schließlich ist die Abbildung φ laut Definition wohldefiniert. Die Surjektivität ist die Existenz vonb r im ersten Punkt, die Injektivität ist die Eindeutigkeit modulo I. Für die Homomorphiebedingung rechnen wir exemplarisch nach, dass φ mit der Addition verträglich ist:

$$\varphi(r + I + s + I) = \varphi((r + s) + I) = ((r + s) + I_1, \ldots, (r + s) + I_n) = \varphi(r + I) + \varphi(s + I).$$

Die Multiplikation zeigt man analog. □

Korollar 2.3.47 (Chinesischer Restsatz, klassisch)**.** *Seien $m_1, \ldots, m_n \geq 2$ und $\forall i \neq j : m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ oder äquivalent dazu $ggT(m_i, m_j) = 1$. Dann gilt*

1. *$\forall a_1, \ldots, a_n \in \mathbb{Z} \, \exists a \in \mathbb{Z} : \forall i \in \{1, \ldots, n\} : a \equiv a_i \mod m_i$. Weiters ist dieses a eindeutig modulo $\bigcap_{i=1}^n m_i\mathbb{Z} = m_1 \ldots m_n\mathbb{Z}$.*
2. *$\varphi : \mathbb{Z}_{m_1 \ldots m_n} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_n}, [a] \mapsto (a \mod m_1, \ldots, a \mod m_n)$ ist ein Isomorphismus.*

Kapitel 3

Teilbarkeit

Dieses Kapitel behandelt die Inhalte der Vorlesung, welche auch in Goldstern et al.: *Algebra – Eine grundlagenorientierte Einführunsvorlesung* in dem Kapitel *5. Teilbarkeit* gefunden werden können.

3.1 Grundlagen

Definition 3.1.1. Sei $(H, \cdot)$ eine Halbgruppe und $a, b \in H$. Dann sind definiert:

- $a \mid b :\Leftrightarrow \exists c \in H : a \cdot c = b$ (a *teilt* b)
- $a \sim b :\Leftrightarrow a \mid b \wedge b \mid a$ (a *ist assoziiert zu* b)

Bemerkung 3.1.2. Ist $(H, \cdot)$ eine Halbgruppe, so ist die Teilbarkeitsrelation $\mid$ transitiv. Falls H ein neutrales Element e besitzt, so ist $\mid$ auch reflexiv. Relationen mit diesen beiden Eigenschaften werden auch *Quasiordnung* genannt. Im Falle eines kommutativen Monoides handelt es sich bei $\sim$ um eine Kongruenzrelation.

Beispiel 3.1.3. In $(\mathbb{Z}, \cdot)$ gilt beispielsweise für alle $a \in \mathbb{Z} : a \mid a$ und $a \mid -a$.

Proposition 3.1.4. *Sei R ein kommutativer Ring mit 1 und $p \in R$. Dann sind äquivalent:*

1. *$(p) \lhd R$ ist prim.*
2. *Falls $p \not\sim 1$ gilt, so folgt für alle $a, b \in R$ aus $p \mid a \cdot b$, dass $p \mid a$ oder $p \mid b$ gilt.*

Beweis.

(1) $\Rightarrow$ (2): Da (p) prim ist, ist das erzeugte Ideal insbesondere echt, daher ist $1 \notin (p)$, also gilt $p \nmid 1$ und $p \not\sim 1$. Seien $a, b \in R$ beliebig mit $p \mid a \cdot b$. Dann ist $ab \in (p)$, also $a \in (p)$ oder $b \in (p)$, da (p) prim ist. Das ist aber äquivalent zu $p \mid a$ oder $p \mid b$.

(1) $\Leftarrow$ (2): Da $p \not\sim 1$ gilt, folgt dass $(p) \neq R$ ist, also ist das erzeugt Ideal echt. Seien weiters $a, b \in R$ mit $a, b \in (p)$. Dann gilt $p \mid ab$ und gemäß Voraussetzung folgt $p \mid a$ oder $p \mid b$. Das ist widerum äquivalent zu $a \in (p)$ oder $b \in (p)$.

□

Definition 3.1.5. Sei R ein kommutativer Ring mit 1 und $p \in R$. Dann heißt p

- *prim* $:\Leftrightarrow p \neq 0, p \not\sim 1 \wedge \forall a, b \in R : p \mid ab \Rightarrow p \mid a \vee p \mid b$,
- *irreduzibel* $:\Leftrightarrow p \not\sim 1 \wedge \forall a, b \in R : ab = p \Rightarrow a \sim 1 \vee b \sim 1$.

Proposition 3.1.6. *Sei R ein Integritätsbereich und $p \in R$. Dann folgt wenn p prim ist, dass p auch irreduzibel ist.*

Beweis. Seien $a, b \in R$ mit $ab = p$. Dann gilt nach Definition $p \mid ab$, also $p \mid a$ oder $p \mid b$. o. B. d. A. gelte $p \mid a$, das heißt es existiert $c \in R$ sodass $pc = a$. Dann gilt $p = pcb \Leftrightarrow p(1 - cb) = 0$ und da $p \neq 0$ ist und R ein Integritätsbereich ist, folgt $1 - cb = 0$, also $cb = 1$ und $b \sim 1$. □

Beispiel 3.1.7. Die Umkehrung dieser Proposition stimmt nicht. Durch $\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ ist ein Integritätsbereich gegeben, in welchem es irreduzible Element gibt, welche nicht prim sind, beispielweise 2 oder 3.

10.05.2023
11.05.2023

3.2 Faktorielle Ringe

Definition 3.2.1. Sei R ein Integritätsbereich, so heißt R *faktorieller Ring* (oder *Gaußscher Ring*, oder auch *ZPE-Ring*) genau dann wenn

$$\forall r \in R \exists r_1, \ldots, r_n \in R \setminus \{[1]_\sim\} \text{ irreduzibel} : r = r_1 \cdot \ldots \cdot r_n,$$

wobei die r_i bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt sind[1].

Bemerkung 3.2.2. Wir bemerken, dass eine Zerlegung in Primelemente *immer* eindeutig ist (wieder bis auf Reihenfolge und Assoziiertheit).

Um dies einzusehen sei $a \in R$ mit zwei Zerlegungen

$$a = p_1 \cdot \ldots \cdot p_u = q_1 \cdot \ldots \cdot q_v,$$

wobei p_i, q_i prim sind. Damit folgt $p_1 \mid q_1 \cdot \ldots \cdot q_v$, da p_1 prim ist gibt es also ein j mit $p_1 \mid q_j$. Nach Voraussetzung ist q_j irreduzibel, also folgt $p_1 \sim q_j$ und damit $x \cdot p_1 = q_j$ mit einem $x \sim 1$. Kürzen von p_1 liefert

$$p_2 \cdot \ldots \cdot p_u = q_1 \cdot \ldots \cdot q_{j-1} \cdot x \cdot q_{j+1} \cdot \ldots \cdot q_v.$$

Induktiv folgt dadurch die Eindeutigkeit.

Tatsächlich haben wir hier nicht verwendet, dass die q_i prim sind - wir haben also die stärkere Aussage gezeigt, dass es, sobald es eine Zerlegung in Primelemente gibt, diese bereits eindeutig ist (es gibt also keine andere Zerlegung in Nichtprimelemente, bis auf Reihenfolge und Assoziiertheit).

Proposition 3.2.3. *Sei R ein Integritätsbereich, dann sind äquivalent:*

1. *R ist faktoriell.*
2. *$\forall r \in R \setminus \{0\}, r \not\sim 1 \exists p_1, \ldots, p_s \in R$ prim $: r = p_1 \cdot \ldots \cdot p_s$*
3. *Für alle $r \in R \setminus \{0\}, r \not\sim 1$ gilt:*
   i. *$\exists r_1, \ldots, r_t \in R$ irreduzibel $: r = r_1 \cdot \ldots \cdot r_t$*
   ii. *r irreduzibel $\Rightarrow r$ prim*

[1] Wir haben also zwei geforderte Eigenschaften für faktorielle Ringe, die Existenz und die Eindeutigkeit. In der Literatur werden oft Ringe mit der ersten Eigenschaft mit *factorization domain (FD)* bezeichnet, Ringe wo zusätzlich die letztere gilt oft mit *unique factorization domain (UFD)*.

Beweis.

(1) ⇒ (3): Die erste Aussage gilt nach Definition. Ist nun $r \in R$ irreduzibel, so wähle $a, b \in R$ mit $r \mid a \cdot b$, es gibt also ein c mit $r \cdot c = a \cdot b$. Mit (1) erhalten wir eine Zerlegung

$$r \cdot (c_1 \cdot \ldots \cdot c_u) = (a_1 \cdot \ldots \cdot a_v) \cdot (b_1 \cdot \ldots \cdot b_w),$$

wobei die geklammerten Terme jeweils irreduzibel sind. Nach (1) gibt es nun noch i, j mit $r \sim a_i$ und $r \sim b_j$, womit $r \mid a$ und $r \mid b$ folgt, womit r prim ist.

(3) ⇒ (1): Wir haben oben bereits gezeigt dass Zerlegungen in Primelemente eindeutig sind, somit folgt sofort die Aussage.

(3) ⇒ (2): Trivial.

(2) ⇒ (3): Die erste Aussage folgt da Primelemente irreduzibel sind. Für die zweite sei $r \in R$ irreduzibel, nach (2) gibt es eine Zerlegung $r = r_1 \cdot \ldots \cdot r_s$ in Primelemente. Da r irreduzibel ist folgt $s = 1$, womit r prim ist.

□

Beispiel 3.2.4. Betrachte $R = \mathbb{Q} + x \cdot \mathbb{R}[x] \leq \mathbb{R}[x]$, so ist R ein Integritätsbereich. Nun gilt jedoch $x \mid (\sqrt{2}x)^2 = 2x^2$, aber $x \nmid \sqrt{2}x$, womit x nicht prim ist.

Weiters ist x irreduzibel, da $x = p \cdot q$ implizieren würde $\deg p = 0$ und $\deg q = 0$. Dann wäre jedoch $p \in \mathbb{Q}$, also $p \sim 1$.

Nun gilt

$$x \cdot x = x^2 = \left(\frac{\sqrt{2}}{2}x\right)(\sqrt{2}x),$$

wobei alle Faktoren rechts und links irreduzibel sind. Die Zerlegungen sind unterschiedlich, da $x \not\sim \sqrt{2}x, \frac{\sqrt{2}}{2}x$, da $\sqrt{2}, \frac{\sqrt{2}}{2} \notin R$.

Proposition 3.2.5. *Jeder Hauptidealring ist ein faktorieller Ring.*

Beweis. Sei $r \in R$ irreduzibel, wir zeigen, dass r prim ist. Wir bemerken, dass $(r) \lhd R$ echt ist, womit es ein maximales, echtes Ideal gibt mit $(r) \subseteq I \lhd R$. Da R ein Hauptidealring ist gibt es ein $c \in R$ mit $I = (c)$. c ist prim, da I maximal und damit prim ist. Nun gilt $r \in (c)$, womit $c \mid r$ folgt. Da r irreduzibel ist folgt $r \mid c$, also folgt $r \sim c$ und damit, dass r prim ist.

Sei nun $r \in R \setminus \{0\}, r \not\sim 1$, wir suchen eine Zerlegung in irreduzible Elemente. Ist r nicht irreduzibel, so können wir $r = r_0 \cdot r_1$ schreiben, wobei $r_0, r_1 \not\sim 1$. Entsprechend können wir, wenn r_0 beziehungsweise r_1 nicht irreduzibel sind r_{00}, r_{01} finden. Induktiv zerlegen wir also

$$r_{i_1 \ldots i_n} = r_{i_1 \ldots i_n 0} \cdot r_{i_1 \ldots i_n 1}.$$

Sei T der Baum der $r_{i_1 \ldots i_n}$. Ist T endlich, so haben wir eine gewünschte Zerlegung gefunden. Sei indirekt angenommen T wäre unendlich, es gibt also einen unendlichen Ast (König's Lemma) – o. B. d. A. betrachten wir den Ast $r_0, r_{00}, r_{000}, \ldots$. Nun gilt

$$(r) \subseteq (r_0) \subseteq (r_{00}) \subseteq \ldots$$

Sei indirekt angenommen $r_0 \sim r_{00}$, so gibt es ein x mit $r_{00} = r_0 \cdot x = r_{00} \cdot r_{01} \cdot x$, also folgt $1 = r_{01} \cdot x$, also $r_{01} \sim 1$, im Widerspruch. Die obige Schachtelung ist also sogar echt, wir haben eine echt aufsteigende Kette von Idealen. Setze

$$I := (r_0) \cup (r_{00}) \cup \ldots \lhd R.$$

Nun gibt es ein c mit $I = (c)$, womit es ein i gibt mit $c \in (r_{0\ldots0})$, wobei $0 \ldots 0$ i-mal, also folgt $c \sim r_{0\ldots0}$, also $I = (r_{0\ldots0})$, im Widerspruch dazu, dass unsere Kette aufsteigend war. □

Beispiel 3.2.6. Betrachte $\mathbb{Z}[x]$. Sei $a \in \mathbb{Z}, a \not\sim 1, a \neq 0$. Betrachte $(a, x) \lhd \mathbb{Z}[x]$, was zwar echt aber kein Hauptideal ist. Wäre nämlich $(a, x) = (b)$, so würde wegen $a \in (b)$ direkt $\deg b = 0$ folgen. Wegen $x \in (b)$ folgt dadurch $b = 1$, im Widerspruch.

Es ist aber $\mathbb{Z}[x]$ sehr wohl faktoriell, wie wir später noch sehen werden.

Definition 3.2.7. Sei R ein kommutativer Ring mit 1, $A \subseteq R$ und $d \in R$. Dann ist d ein *größter gemeinsamer Teiler* von A (wir schreiben auch $d = \mathrm{ggT}(A)$, obwohl diese Gleichheit formal nicht korrekt ist), wenn

$$(\forall a \in A : d \mid a) \wedge (\forall d' \in R : (\forall b \in A : d' \mid b) \Rightarrow d' \mid d).$$

Dieser größte gemeinsame Teiler ist eindeutig bis auf Assoziiertheit.

Entsprechend kann man auch das *kleinste gemeinsame Vielfache* einer Menge definieren.

11.05.2023
17.05.2023

Bemerkung 3.2.8. Sei R ein Ring und Integritätsbereich und seien $a, b \in R$. Dann gilt die Äquivalenz $a \mid b \Leftrightarrow (b) \subseteq (a)$. Es ist daher die Struktur $(R/_\sim, |)$ ordnungstheoretisch isomorph zu der Menge aller Hauptideale mit Mengeninklusion, vermöge der Abbildung $\psi([a]_\sim) := (a)$. Dabei ist $\sim$ die Assoziiertheit. Im Fall eines Hauptidealrings kann „Menge der Hauptideale“ offensichtlich mit „Menge der Ideale“ ersetzt werden. Für $A \subseteq R$ ist $\inf_|(A) = \mathrm{ggT}(A)$ und $\sup_|(A) = \mathrm{kgV}(A)$. Aufgrund von dieser Tatsachen folgt nun, dass es in einem Hauptidealring R zu $A \subseteq R$ eine Menge von Idealen $A' = \psi(A)$ gibt. Da R ein Hauptidealring ist, existiert ein $d \in R$ mit $(A) = (d)$ und es folgt

$$\mathrm{ggT}(A) = \inf{}_|(A) \widehat{=} \inf{}_\supseteq\{(a) \mid a \in A\} = \sup{}_\subseteq\{(a) \mid a \in A\} = (A) = (d).$$

Lemma 3.2.9 (Lemma von Bézout)**.** *Sei R ein Hauptidealring und $A \subseteq R$. Dann existieren $n \in \mathbb{N}$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$, sodass $\mathrm{ggT}(A) = \sum_{i=1}^n r_i a_i$.*

Beweis. Aus der vorangegangen Bemerkung folgt $(\mathrm{ggT}(A)) = (A)$. Aufgrund der Darstellung über das erzeugte Ideal folgt die Behauptung. □

Beispiel 3.2.10. Ein Beispiel in $R = \mathbb{Z}$ ist $\mathrm{ggT}(5, 3) = 1 = (-1) \cdot 5 + 2 \cdot 3$.

3.3 Teilen mit Rest

Beispiel 3.3.1. Das folgende Beispiel illustriert die Motivation dieses Kapitels: In den ganzen Zahlen kann die bekannte Division mit Rest, durchgeführt werden. Das heißt für zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $a \neq 0$ existieren $q, r \in \mathbb{Z}$ sodass $b = qa + r$ gilt, wobei $0 \leq r < |a|$. Beispielsweise ist $16 = 5 \cdot 3 + 1$ eine solche Division mit Rest, während $16 = 4 \cdot 3 + 4$ diese Definition nicht erfüllt.

Definition 3.3.2. Sei R ein Ring und Integritätsbereich. Dieser heißt *euklidischer Ring*, wenn es eine Funktion $H : R \setminus \{0\} \to \mathbb{N}$ mit

$$\forall a \in R \setminus \{0\}, b \in R \exists^2 q, r \in R : b = aq + r \quad \wedge \quad (r = 0 \vee H(r) < H(a))$$

gibt. Die Funktion H heißt *euklidische Bewertung*.

Beispiel 3.3.3. Ein Beispiel für einen euklidischen Ring ist $\mathbb{Z}$ mit $H(x) = |x|$. Weiters ist für einen Körper K der Polynomring $K[x]$ ein euklidischer Ring, wobei die Bewertung der Grad ist. Jeder Körper K mit einer beliebigen Funktion $H : R \setminus \{0\} \to \mathbb{N}$ ist ein triviales Beispiel, da man immer 0 als Divisionsrest erhalten kann.

Beispiel 3.3.4. Wie wir gleich sehen werden, ist jeder euklidische Ring auch ein Hauptidealring. Da $\mathbb{Z}[x]$ kein Hauptidealring ist, ist $\mathbb{Z}[x]$ insbesondere kein euklidischer Ring. Ein Beispiel für einen Hauptidealring der kein euklidischer Ring ist, wäre $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}] \subseteq \mathbb{C}$ (ohne Beweis).

Satz 3.3.5. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R ein euklidischer Ring und I ein Ideal. Falls $I = \{0\}$ ist, so gilt trivialerweise $I = (0)$. Falls $I \neq \{0\}$ gilt, so muss ein $a \in R$ mit $I = (a) = \{aq \mid q \in R\}$ gefunden werden. Wähle daher $a \in I \setminus \{0\}$ mit $H(a) = \min\{H(x) \mid x \in I\}$. Dieses Minimum existiert, da jede nichtleere Teilmenge natürlicher Zahlen ein Minimum hat. Offensichtlich gilt $(a) \subseteq I$.

Für die andere Mengeninklusion sei $b \in (a)$. Da R ein euklidischer Ring ist, existieren $q, r \in R$ mit $b = aq + r$ und $r = 0 \vee H(r) < H(a)$. Wegen $r = b - aq \in I$ und der Minimalität von $H(a)$ folgt, dass $r = 0$ gilt, also $b = aq$ und $b \in (a)$. □

Satz 3.3.6 (Euklidischer Algorithmus)**.** *Seien $a, b \in R, a \neq 0$. Wähle $q_1, r_1 \in R : b = aq_1 + r_1$ mit $r_1 = 0 \vee H(r_1) < H(a)$. Wenn $r_1 = 0$ ist, dann terminiert der Algorithmus. Ansonsten wählt man $q_2, r_2 \in R$ mit $a = r_1 q_2 + r_2$ und $r_2 = 0 \vee H(r_2) < H(r_1)$. Falls $r_2 = 0$ ist, so terminiert der Algorithmus, ansonsten verfahren wir induktiv. Wenn r_i, r_{i+1} und q_{i+1} bereits gewählt sind, dann wählt man q_{i+2}, r_{i+2} mit $r_i = r_{i+1} q_{i+2} + r_{i+2}$ mit $r_{i+2} = 0 \vee H(r_{i+2}) < H(r_{i+1})$. Aufgrund der Schachtelung $H(a) > H(r_1) > H(r_2)$ terminiert der Algorithmus, das heißt es ist $r_k = 0$ für ein $k \in \mathbb{N}$. Dann ist r_{k_1} der letzte von 0 verschieden Rest und es gilt $r_{k-1} = \mathrm{ggT}(a, b)$.*

Beweis. Zunächst wird gezeigt, dass r_{k-1} ein Teiler von a und b ist. Das folgt induktiv, da $r_{k-1} \mid r_{k-2}$ (wegen $r_k = 0$) und $r_{k-1} \mid r_{k-2} q_{k-1} + r_{k-1} = r_{k-3}$. Mit Induktion folgt, dass $r_{k-1} \mid a$ und $r_{k-1} \mid b$ gilt.

Ist nun t ein beliebiger Teiler von a und b, so müssen wir zeigen, dass $t \mid r_{k-1}$ gilt. Diese Aussage folgt ähnlich da $t \mid b - aq_1 = r_1$ und man wieder mit Induktion $t \mid r_{k-1}$ leicht folgert. Daher folgt, dass $r_{k-1} = \mathrm{ggT}(a, b)$ gilt. □

Bemerkung 3.3.7. Eine Anwendung des euklidischen Algorithmus ist die Berechnung von Koeffizienten x, y mit $ax + by = \mathrm{ggT}(a, b)$. Mit der Notation aus Satz 3.3.6 folgt

$$\begin{aligned}
\mathrm{ggT}(a, b) &= r_{k-1} \\
&= r_{k-3} - r_{k-2} q_{k-1} \\
&= r_{k-3} - (r_{k-4} - r_{k-3} q_{k-2}) q_{k-1} \\
&= r_{k-4}(-q_{k-1}) + r_{k-3}(1 + q_{k-2} q_{k-1}) \\
&= \ldots = ax + by.
\end{aligned}$$

[2] Diese Elemente müssen nicht eindeutig sein!

Die Koeffizienten x, y sind klarerweise nicht eindeutig, so ist in $\mathbb{Z}$ beispielsweise $1 = \mathrm{ggT}(5,3) = 5(-1) + 3 \cdot 2 = 5 \cdot 2 + 3(-3)$.

Bemerkung 3.3.8. Wir wollen an dieser Stelle noch einen kurzen Überblick über die verschiedenen Arten von Ringen geben und vor allem auch auf die Unterschiede über darin gültigen Aussagen eingehen.

In Faktoriellen Ringen gibt es zu $a, b \in R$ einen größten gemeinsamen Teiler $\mathrm{ggT}(a,b)$.

In einem Hauptidealring gibt es nicht nur den größten gemeinsamen Teiler, sondern dieser kann auch als Linearkombination dargestellt werden, das heißt für $a, b \in R$ existieren $x, y \in R$ mit $\mathrm{ggT}(a,b) = ax + by$.

In einem euklidischen Ring gibt es den ggT, dieser kann linearkombiniert werden und mithilfe des euklidischen Algorithmus können Faktoren berechnet werden.

Proposition 3.3.9. *Sei R ein faktorieller Ring, K der Quotientenkörper und $\frac{p}{q} \in K$. Dann gibt es $p', q' \in R, q' \neq 0$ sodass $\frac{p}{q} = \frac{p'}{q'}$ und $\mathrm{ggT}(p', q') = 1$. Wenn $\frac{p''}{q''} = \frac{p}{q}$ mit $\mathrm{ggT}(p'', q'') = 1$, dann gilt $p'' \sim p'$ und $q'' \sim q'$.*

Beweis. Mit $p' := \frac{p}{\mathrm{ggT}(p,q)}$ und $q' := \frac{q}{\mathrm{ggT}(p,q)}$ folgt die Existenz, wobei man $\frac{p'}{q'} = \frac{p}{q}$ über die Primfaktorenzerlegung nachweist. Ist $\frac{p''}{q''}$ ebenfalls eine solche Darstellung von $\frac{p}{q}$, so überzeugt man sich von $p' \sim p''$ und $q' \sim q''$ ebenfalls mithilfe der Primfaktorenzerlegung in R. □

17.05.2023
24.05.2023

3.4 Der Satz von Gauß

Satz 3.4.1 (Satz von Gauß)**.** *Ist R ein faktorieller Ring, so ist auch $R[x]$ faktoriell.*

Korollar 3.4.2. *Sei R ein faktorieller Ring. Dann gilt:*

- *Der Polynomring $R[x_1, \ldots, x_n]$ ist faktoriell.*
- *Ist X eine beliebige Menge, so ist auch $R[X]$ faktoriell.*

Korollar 3.4.3. *$\mathbb{Z}[x]$ ist faktoriell.*

Definition 3.4.4. Ist R ein Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$, so nennen wir f *leer* (oder auch *primitiv*), wenn

$$\mathrm{ggT}(a_0, \ldots, a_n) = 1.$$

Bemerkung 3.4.5. Ist R ein faktorieller Ring, so existiert für alle $f \in R[x]$ eine Darstellung

$$f = \mathrm{ggT}(a_0, \ldots, a_n) \cdot f_0,$$

wobei $f \in R[x]$ leer ist.

Lemma 3.4.6. *Sei R faktoriell, $f, g \in R[x]$, $p \in R$ prim. Dann gilt*

$$p \mid fg \Rightarrow p \mid f \vee p \mid g.$$

Beweis. Wir zeigen die Aussage mittels Induktion nach $\deg fg = n + m$, wobei

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{n} b_j x^j.$$

Induktionsanfang ($n + m = 0$): Es sind $f, g \in R$, womit aus $p \mid fg$ folgt $p \mid f \vee p \mid g$, da p prim in R ist.

Induktionsschritt ($n + m \to n + m + 1$): Gilt $p \mid fg$, so gilt $p \mid a_n b_m$, da $a_n b_m$ der Leitkoeffizient ist und damit, da p prim in R ist, $p \mid a_n \vee p \mid b_m$. Nehmen wir o. B. d. A. $p \mid a_n$ an. Schreiben wir nun $f = a_n x^n + f'$. Es gilt

$$fg = a_n x^n g + f' g.$$

Nun teilt p jedoch fg, a_n und damit auch $f'g$. Nach Induktionsvoraussetzung gilt damit $p \mid f' \vee p \mid g$, und damit entweder direkt die Beauptung oder $p \mid a_n, p \mid f'$ und damit $p \mid f$. □

Korollar 3.4.7. *Sei R faktoriell, $f, g \in R[x]$ leer, so ist auch fg leer.*

Lemma 3.4.8. *Sei R faktoriell, Q der Quotientenkörper von R und $f \in Q[x]$. Dann existieren $c_f \in Q, f_0 \in R[x]$ leer, mit*

$$f = c_f \cdot f_0.$$

Diese Darstellung ist eindeutig bis Multiplikation mit einer Einheit (aus R).

Weiters gibt es zu $f, g \in Q[x]$ eine Einheit $e \in R$ mit

$$c_{f \cdot g} = e \cdot c_f \cdot c_g.$$

Beweis. Die Koeffizienten von f in Q haben eine Darstellung als Quotient mit teilerfremden Elementen aus dem Ring, wir können also schreiben

$$f = \sum_{i=0}^{\ell} a_i x^i = \sum_{i=0}^{\ell} \frac{z_i}{n_i} x^i = \frac{\mathrm{ggT}(z_0, \ldots, z_n)}{\mathrm{kgV}(n_0, \ldots, n_\ell)} \sum_{i=0}^{\ell} b_i x^i,$$

wobei $b_i \in R$ teilerfremd und sich somit sofort die geforderte Darstellung ergibt.

Seien nun $c_f \cdot f_0 = f = d \cdot g$ zwei Darstellungen. Schreiben wir

$$f_0 = \sum_{i=0}^{\ell} b_i x^i, \quad g = \sum_{i=0}^{\ell} t_i x^i,$$

so folgt durch Koeffizientenvergleich, dass für alle i gilt $c_f \cdot b_i = d \cdot t_i$. Schreiben wir $c_f = \frac{c_f^z}{c_f^n}, d = \frac{d^z}{d^n}$. Damit gilt $c_f^z b_i d^n = d^z t_i c_f^n$, aufgrund der Eindeutigkeit des ggT's (bis auf Assoziiertheit) folgt $c_f^z d^n \sim d^z c_f^n$ und damit die Existenz einer Einheit e mit $e \cdot c_f = d$.

Sind nun $f = c_f \cdot f_0, g = c_g \cdot g_0$, so folgt

$$f \cdot g = (c_f \cdot c_g) \cdot (f_0 \cdot g_0)$$

und damit sofort die Aussage. □

Lemma 3.4.9. *Sei R faktoriell und Q der Quotientenkörper von R. Sei $f \in R[x]$ irreduzibel in $R[x]$, $\deg f \geq 1$, so ist f irreduzibel in $Q[x]$.*

Beweis. Sei $f = g \cdot h$, $g, h \in Q[x]$. Gilt $\deg g = 0 \vee \deg h = 0$, so folgt sofort die Assoziiertheit von g oder h zu 1 in $Q[x]$. Sind $\deg f, \deg h \geq 1$, so schreibe mit obigem Lemma $g = c_g \cdot g_0, h = c_h \cdot h_0$. Wir nehmen o. B. d. A. $c_f = c_g \cdot c_h$ an. f ist irreduzibel in $R[x]$, insbesondere ist f also leer. Wir können also o. B. d. A. $c_f = 1$ annehmen. Damit ist also

$$f = g \cdot h = c_g \cdot g_0 \cdot c_h \cdot h_0 = g_0 \cdot h_0,$$

im Widerspruch dazu, dass f irreduzibel in $R[x]$ ist. □

Lemma 3.4.10. *Sei R ein faktorieller Ring. Ist $f \in R[x]$ irreduzibel, so ist f prim.*

Beweis. Seien $g, h \in R[x], f \mid g \cdot h$. Wir wollen $f \mid g \vee f \mid h$ zeigen. In $Q[x]$ gilt $f \mid g \vee f \mid h$, o. B. d. A. sei $p \in Q[x]$ mit $f \cdot p = g$. Nun können wir also

$$f \cdot c_p \cdot p_0 = g = c_g \cdot g_0$$

schreiben, also $c_p \cdot (f \cdot p_0) = c_g \cdot g_0$. Aufgrund der Eindeutigkeit dieser Darstellung gibt es eine Einheit $e \in R$ mit $c_p = e \cdot c_g$. Damit ist jedoch auch $c_p \in R$, womit $p \in R[x]$ folgt. Damit gilt $f \mid g$ in $R[x]$. □

Beweis (Satz von Gauß). Sei $f \in R[x]$, dann ist

$$f = c_f \cdot f_0 = c_f^1 \cdot \ldots \cdot c_f^n \cdot f_0^1 \cdot \ldots \cdot f_0^\ell,$$

wobei die erste Zerlegung in Primelemente existiert da R faktoriell ist und c_f^i prim in $R[x]$ ist, nach obigem Lemma. Letztere Zerlegung in irreduzible Polynome existiert aus Gradgründen, wobei f_0^j prim nach obigem Lemma sind. □

Kapitel 4

Körper

Das Ziel dieses Kapitels ist es die Konzepte, beziehungsweise das Verhalten, von Körpererweiterungen zu verstehen, beispielsweise von $\mathbb{R}$ auf $\mathbb{C}$, oder von $\mathbb{Q}$ auf $\mathbb{R}$. Weiters soll versucht werden alle endlichen Körper vollständig zu klassifizieren.

4.1 Einführung

Definition 4.1.1. Sei L ein Körper. Wir nennen $K \subseteq L$ einen *Unterköper*, wenn $1 \in K$ und K ein Körper ist. Dafür schreiben wir auch $K \leq L$. In diesem Kontext heißt L auch *Oberkörper* von K.

Wir nennen

$$\bigcap \{U \leq L \mid U \text{ Unterkörper von } L\}$$

den *Primkörper* von L.

Sei $K \leq L, S \subseteq L$ so definieren wir die *Körpererweiterung von K um S* durch

$$K(S) := \bigcap \{U \mid K \leq U \leq L, U \supset S\}.$$

Ist $S = \{\alpha_1, \ldots, \alpha_n\}$, so schreiben wir auch $K[\alpha_1, \ldots, \alpha_n]$.

Bemerkung 4.1.2. Beispielsweise gilt $\mathbb{R}(i) = \mathbb{C}$, wie wir später noch sehen werden.

Bemerkung 4.1.3. Sei K ein Körper, dann ist K ein Unterkörper des Quotientenkörpers Q von $K[x]$. Also ist $K \leq Q$ eine Körpererweiterung.

Definition 4.1.4. Ein Körper K heißt *Primkörper*, wenn K keine echten Unterkörper hat.

Satz 4.1.5. *Sei K ein Primkörper.*

- *Ist* $\operatorname{char} K = 0$*, so ist* $K \cong \mathbb{Q}$*.*
- *Ist* $\operatorname{char} K = p \in \mathbb{P}$*, so ist* $K \cong \mathbb{Z}_p$*.*

Index

Abbildungsverzeichnis