Algebra Vorlesungsmitschrift

nach der 2023S Vorlesung von Michael Pinsker

Ian Hornik, Daniel Mayr, Alexander Zach

Stand vom 3. April 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 1.1.8 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 $\mathbb{Z}_9$.

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

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

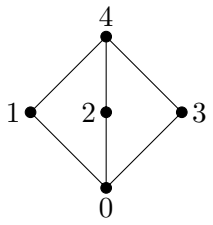

Abbildung 1.1: Hasse-Diagramm einer Ordnungsrelation

$(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ 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*.

Beispiel 1.1.30. 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 $t = f_i(t_1, \dots, t_{n_i}) \in T_{m+1}$ mit $t_1, \dots, t_{n_i} \in T_m$, 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.

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 $(\mathrm{Sl}_n(K), \cdot) \leq (\mathrm{Gl}_n(K), \cdot)$.

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 $\mathfrak{S} \models s \approx t$. □

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

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 $a_1, \dots, a_{n_i} \in S$ beliebig. Dann gilt für alle $j \in J$: $a_1, \dots, a_{n_i} \in S_j$ und da $\mathfrak{S}_j$ eine Unteralgebra von $\mathfrak{A}$ ist auch $f_i^{\mathfrak{S}_j}(a_1, \dots, a_{n_i}) \in S_j$. Das ist genau die Definition von $f^{\mathfrak{S}}(a_1, \dots, a_{n_i}) \in \bigcap_{j\in J} S_j = S$, 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

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

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

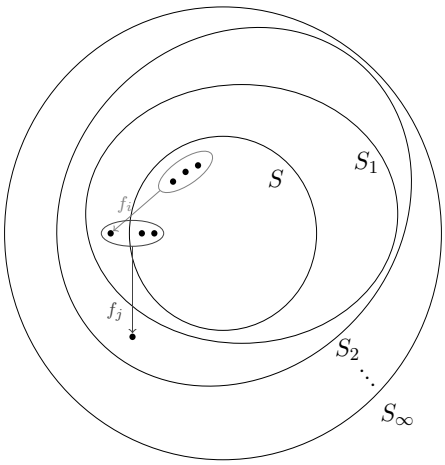

Abbildung 1.2: Subalgebra von unten

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

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

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 $a_1, \dots, a_{n_i} \in S_k$, sodass $a = f_i^{\mathfrak{A}}(a_1, \dots, a_{n_i})$. Auch hier kann die Induktionsvoraussetzung angewandt werden, weshalb $a_1, \dots, a_{n_i} \in \langle S\rangle$ ist. Da $(\langle S\rangle, (f_i^{\mathfrak{A}})_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$ ist, gilt auch $a = f_i^{\mathfrak{A}}(a_1 \dots, a_{n_i}) \in \langle S\rangle$. Daraus folgt die gewünschte Mengeninklusion $S_{k+1} \subseteq \langle S\rangle$.

2. Definiere $M := \{t^{\mathfrak{A}}(a_1, \dots, a_n) | a_1, \dots, a_n \in S \wedge t \in T(X)\}$. Es gilt $S \subseteq M$, da die Projektionen $\pi_j^{(n)} : A^n \to A, (a_1, \dots, a_n) \mapsto a_j$ 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 $b_1, \dots, b_{n_i} \in M$, dann können diese Elemente als $b_j = t_j^{\mathfrak{A}}(a_1^{(j)}, \dots, a_{m_j}^{(j)})$ mit $a_1^{(j)}, \dots, a_{m_j}^{(j)} \in S$ für $j \in \{1, \dots, n_i\}$ dargestellt werden. Definiert man nun $a := f_i^{\mathfrak{A}}(b_1, \dots, b_{n_i})$ und den Term $t := f_i^{\mathfrak{T}}(t_1(x_1^{(1)}, \dots, x_{m1}^{(1)}), \dots, t_{n_i}(x_1^{(n_i)}, \dots, x_{m_{n_i}}^{(n_i)}))$, so erhält man eine passende Termfunktion, das heißt es gilt $t^{\mathfrak{A}}(a_1^{(1)}, \dots, a_{m_1}^{(1)}, \dots, a_1^{(n_i)}, \dots, a_{m_{n_i}}^{(n_i)}) = a$, also insbesondere $a \in M$. Für die andere Mengeninklusion ist erneut eine Induktion nötig. Sei $a = t^{\mathfrak{A}}(a_1, \dots, a_n) \in M$ 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 $a = t^{\mathfrak{A}}(a_1, \dots, a_n) = \pi_j^n(a_1, \dots, a_n) = a_j \in S \subseteq \langle S\rangle$.
   Induktionsschritt ($m < k \to k$): Dann ist $t = f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})$ und $a = t^{\mathfrak{A}}(a_1, \dots, a_{n_i}) = f_i^{\mathfrak{A}}(t_1^{\mathfrak{A}}(a_1, \dots, a_n), \dots, t_{n_i}^{\mathfrak{A}}(a_1, \dots, a_n)) \in \langle S\rangle$, da die Terme $t_j^{\mathfrak{A}}$ für $j \in \{1, \dots, n_i\}$ kleinere 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. 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 $\tilde{t}^{\mathfrak{A}}(s_1, \dots, s_n) = t^{\mathfrak{A}}(a_1, \dots, a_\ell) = a \in \{t^{\mathfrak{A}}(s_1, \dots, s_n) \mid t(x_1, \dots, x_n) \in T(X)\}$. □

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

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.

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 $f_i^{\mathfrak{A}} : \mathfrak{A}^{n_i} \to \mathfrak{A}, ((a_j^{(1)})_{j \in J}, \ldots (a_j^{(n_i)})_{j \in J}) \mapsto (f_i^{\mathfrak{A}_j}(a_j^{(1)}, \ldots, a_j^{(n_i)}))_{j \in J}$ definiert werden.

Beispiel 1.4.17. Abbildung 1.3 visualisiert die Bildung einer Produktalgebra.

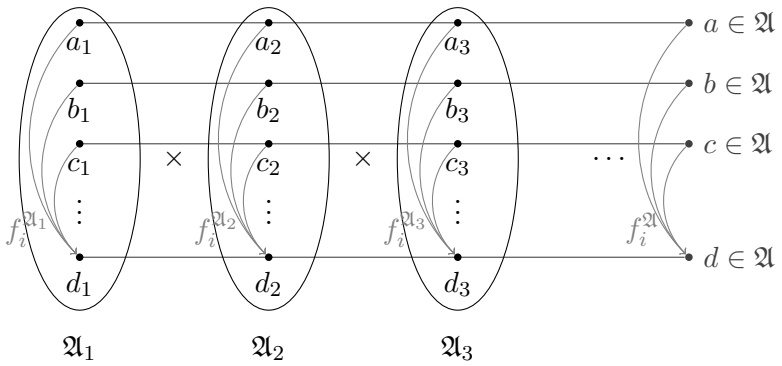

Abbildung 1.3: Visualisierung von Produktalgebren

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.

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* $\mathfrak{A}$.

[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.

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, $\varphi : \mathfrak{A} \to \mathfrak{A}/_{\ker h}$ die kanonische Faktorabbildung und sei $h : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus. 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.*

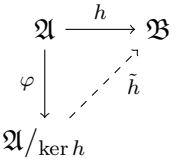

Abbildung 1.4: Visualisierung der Aussage des Homomorphiesatzes

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.

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

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

Für eine Menge von Gesetzen Σ definiere die Klasse $\mathcal{V}(\Sigma) := \{\mathfrak{A} \mid \forall s \approx t \in \Sigma : \mathfrak{A} \models s \approx t\}$.

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 $j \in 1, \dots, n$ können ein Term t_j sowie $a_1^{(j)}, \dots, a_{m_j}^{(j)} \in A$ gewählt werden, sodass $g_j = t_j^{\mathfrak{S}}(\pi_{a_1^{(j)}}, \dots, \pi_{a_{m_j}^{(j)}})$ gilt. Nun wird $t := f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})$ als neuer Term definiert und es folgt

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

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

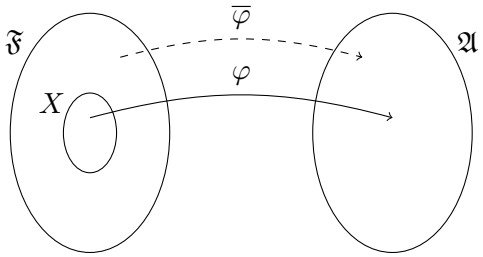

Abbildung 1.5: $\mathfrak{F}$ frei über X

Beispiel 1.5.2. Sei $\mathcal{K}$ die Klasse der Vektorräume über den Körper $\mathbb{C}$, $\mathfrak{V} \in \mathcal{K}$ beliebig und $X \subseteq V$ eine Basis von $\mathfrak{V}$, d. h. $\mathfrak{B}$ ist 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 $\mathfrak{F}_1 \cong \mathfrak{F}_2$.*

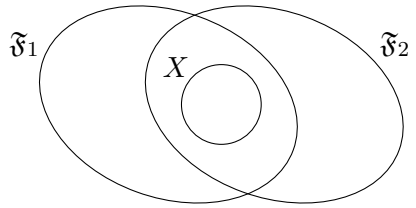

Abbildung 1.6: $\mathfrak{F}_1, \mathfrak{F}_2$ frei über X

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 $\phi \circ \varphi = \mathrm{id}_{F_1}$, 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 eine eindeutigen, φ fortsetzenden Homomorphismen $\overline{\varphi} : \langle X \rangle \to \mathfrak{A}$ 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

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

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 $\mathcal{K}$.

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. □

Beispiel 1.5.11. Bezeichne $(\cdot, e, ^{-1})$ vom Typ $\tau = (2, 0, 1)$ die Sprache der Gruppen. Sei $X = \{x_1, x_2, ...\}$ eine Variablenmenge so sind

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

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

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

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

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

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.

22.03.2023
23.03.2023

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 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 1.1.8 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)**.** *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 $\overline{\psi} \circ \varphi = \psi$.*

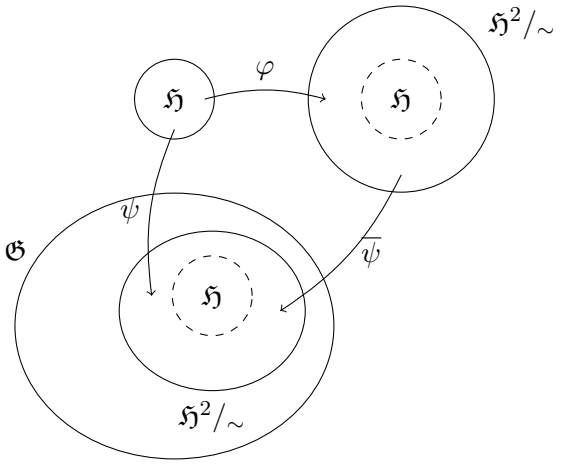

Abbildung 2.1: Visualisierung der Einbettung von $\mathfrak{H}$ in die Gruppen $\mathfrak{G}, \mathfrak{H}^2/_\sim$

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 $\mathfrak{G}, \cdot, \mathfrak{e}, {}^{-1}$ 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

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 Injektivtät 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.

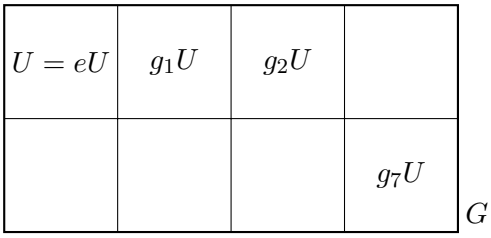

Abbildung 2.2: Nebenklassenzerlegung einer endlichen Gruppe

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 $x'^{-1}n = n'x'^{-1}$.

– 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 $\ker \varphi = \{g \in G \mid \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\}) = N$.[2]

– (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.

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. □

[2]Hier besteht eine Ähnlichkeit zum Kern von linearen Abbildungen der ein Unterraum ist.

Index

Abbildungsverzeichnis