Algebra Vorlesungsmitschrift

nach der 2023S Vorlesung von Michael Pinsker

Ian Hornik, Daniel Mayr, Alexander Zach

Stand vom 26. März 2023

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, 4.1. Freie Algebren und der Satz von Birkhoff* gefunden werden können.

1.1 Einführung

Zu Beginn wird der Begriff einer allgemeinen (oder auch universellen) Algebra definiert und es werden weiter einige spezielle Algebren gezeigt. 01.03.2023

Definition 1.1.1. Seien A eine beliebige Menge, $\tau = (n_i)_{i \in I}$ eine Familie aus $\mathbb{N}_0$ über eine beliebige 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 haben die *Stelligkeit* oder *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 $+$)

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
- $\forall x \in A : e + x = x + e = x$. ($e$ *neutrales Element* bezüglich $+$)

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*)

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 mit Gruppe der Begriff aus Definition 1.1.8 gemeint ist.

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 $+$)

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 ist und
- $\cdot$ ist links- und rechtsdistributiv über $+$.

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.

Definition 1.1.16. Ein kommutativer Ring mit 1 $\mathfrak{A}$ heißt *Körper*, wenn

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

Ist $\cdot$ nicht kommutativ, dann 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 gilt

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

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

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. Wir erhalten die Algebra $\mathfrak{G}^{\mathfrak{R}} := (G, \tilde{+}, \tilde{0}, \tilde{-}, (m_r)_{r \in \mathfrak{R}})$, 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, 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,
- $\forall x \in A : x \wedge x = x.$ ($\wedge$ ist *idempotent*)

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*, 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

Ein Verband heißt *distributiv*, wenn $\wedge$ distributiv[2] über $\vee$ und $\vee$ distributiv über $\wedge$ ist. 02.03.2023

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
- $\forall a \in A : a \vee 1 = 1.$

Beispiel 1.1.24. Mit einer beliebigen Menge M, einen $\mathfrak{K}$-Vektorraum $\mathfrak{V}$ und einer linearen Ordnung $(L, \leq)$ 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 eine jeweils die höher stehenden Elemente größer als die niedrigeren sind und sei $\wedge, \vee$ das Supremum bzw. Infimum zweier Elemente. Es ist dann $(\{0, 1, 2, 3, 4\}, \wedge, \vee)$ ein nicht distributiver Verband, da

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

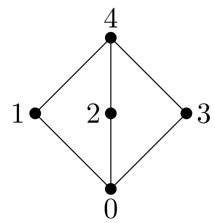

Abbildung 1.1: Hasse-Diagramm einer Ordnungsrelation

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

Es ist $(\mathcal{P}(M), \cap, \cup, \emptyset, M)$ 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 Menge* $V = \{v_1, \ldots, v_n\}$ *kann zu einem beschränkten Verband gemacht werden.*

Beweis. Sei $1 := v_1 \vee \ldots \vee v_n$, dann gilt für beliebiges $v_j \in V$, 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 $0 := v_1 \vee \ldots \vee v_n$. 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 *Boolsche Algebra*, wenn

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

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

Bemerkung 1.1.28. Alle boolschen 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

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

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

Beispiel 1.1.30. Sei $\mathfrak{A}$ eine Algebra. Definieren wir die Mengen

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

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

$(\mathrm{Aut}(\mathfrak{A}), \circ, \mathrm{id}_A, \cdot^{-1})$ 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 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* und die Menge T beschreibt alle *Terme über* $(X, (f_i)_{i\in I})$. Für einen Term $t \in T$ heißt $\mathrm{lvl}(t) := \min\{k \mid t \in T_k\}$ *Stufe von* t.

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

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

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

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

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 $t = f_i(t_1, \dots, t_{n_1})$ geschrieben werden kann, die Terme $t_1, \dots, t_{n_i}$ von niedrigerer Stufe als t sind.

Aus dieser Definition ist klar, dass $\overline{\varphi}|_X = \varphi$, es muss die Verträglichkeit von $\overline{\varphi}$ mit den Operationen gezeigt werden. Für $i \in I$ und $t_1, \dots, t_{n_i} \in T$ gilt $\overline{\varphi}(f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})) = \overline{\varphi}(f_i(t_1, \dots, f_{n_i})) \overset{\text{Def.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i}))$.

Es bleibt noch die Eindeutigkeit zu zeigen. Sei $\widetilde{\varphi} : T \to A$ ein beliebiger Homomorphismus mit $\widetilde{\varphi}|_X = \varphi$, so zeigt man 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 $\widetilde{\varphi}(t) = \widetilde{\varphi}(f_i(t_1, \dots, t_{n_i})) = \widetilde{\varphi}(f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})) = f_i^{\mathfrak{A}}(\widetilde{\varphi}(t_1), \dots, \widetilde{\varphi}(t_{n_i})) \overset{\text{I.V.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i})) = \overline{\varphi}(t)$. □

02.03.2023
08.03.2023

Definition 1.2.5. Seien $X^{(k)} = \{x_1, \dots, x_k\} \subseteq X$ 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 $a_1, \dots, a_k$ heißt $\alpha_{a_1,\dots,a_k} : X^{(k)} \to A, x_j \mapsto a_j$ eine *Variablenbelegung.* Nach Theorem 1.2.4 kann diese nun zum *Einsetzungshomomorphismus* $\overline{\alpha}_{a_1,\dots,a_k} : T^{(k)} \to A$ fortgesetzt werden.

Für einen beliebigen Term $t \in T^{(k)}$ ist die *durch t in $\mathfrak{A}$ induzierte Termoperation* als $t^{\mathfrak{A}} : A^k \to A, (a_1, \dots, a_k) \mapsto \overline{\alpha}_{a_1,\dots a_k}(t)$ 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 im Allgemeinen $t \neq s$.

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

1.3 Varietäten

1.4 Konstruktion neuer Algebren

1.5 Freie Algebren