Algebra Vorlesungsmitschrift

nach der 2023S Vorlesung von Michael Pinsker

Ian Hornik, Daniel Mayr, Alexander Zach

Stand vom 23. August 2023

Wir bedanken uns bei Peter Holy für seine umfangreichen und ausführlichen Korrekturen, sowie 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 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 Einführungsvorlesung* in den Kapiteln *2. Grundbegriffe* und *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 vorgestellt. 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 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 oder auch τ*-Algebra*. Die einzelnen Funktionen f_i nennt man *fundamentale Operationen* und haben *Stelligkeit* oder auch *Arität* n_i. Die Gesamtheit der Funktionssymbole $(f_i)_{i\in I}$ nennen wir *Signatur* oder *Sprache*.

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 (siehe Definition 1.4.1) 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. $(\mathbb{N}, +, 0, \cdot), (\mathbb{R}^{2\times 2}, +, 0$[1]$, \cdot)$ 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* oder *(kommutativen) 1-Ring.*

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

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

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

Verlangen wir von $\cdot$ keine Kommutativität, so nennen wir $\mathfrak{A}$ *Schiefkörper* oder *Divisionsring*.

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

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

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

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 $\mathfrak{V}$ ist ein Vektorraum (über $\mathfrak{R}$), wenn $\mathfrak{R}$ ein Körper ist und $1 \odot u = u$ für alle $u \in V$ gilt.

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

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

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

gilt.

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

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

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

gilt, wobei die letzten zwei Gesetze *Verschmelzungsgesetze* genannt werden. 01.03.2023

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

gilt.

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

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 Infimum bzw. Supremum zweier Elemente, so ist $(\{0, 1, 2, 3, 4\}, \wedge, \vee)$ ein nicht distributiver Verband[a], da

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

[a]Nach diesem System kann jede endliche, partielle Ordnung mit einer solchen Abbildung identifiziert werden, letztere nennt man auch *Hasse-Diagramm*

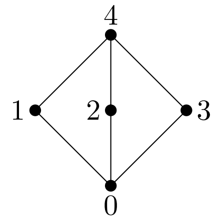

Abbildung 1.1: Hasse-Diagramm einer Ordnungsrelation

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

Bemerkung 1.1.28. Alle Booleschen Algebren werden durch den Darstellungssatz von Stone bis auf Isomorphie beschrieben.

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

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

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

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

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

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

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

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

$(\mathrm{End}(\mathfrak{A}), \circ, \mathrm{id}_A)$ ist dann ein Monoid, das *Endomorphismenmonoid von* $\mathfrak{A}$. Wie wir in Satz 2.1.10 sehen werden, ist jedes Monoid isomorph zu einem Endomorphismenmonoid.

$(\mathrm{Aut}(\mathfrak{A}), \circ, \mathrm{id}_A, ^{-1})$ ist eine Gruppe, die *Automorphismengruppe von* $\mathfrak{A}$. Eine Folgerung von Satz 2.2.41 ist, dass jede endliche Gruppe isomorph zu einer Automorphismengruppe ist.

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 $T(X) := T$[4] 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* oder *Signatur*[5] 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 $\mathrm{var}(t) := \bigcup_{j\in\{1,\dots,n_i\}} \mathrm{var}(t_j)$. Für einen Term t werden wir auch $t(\mathrm{var}(t))$ beziehungsweise im Fall $\mathrm{var}(t) = \{x_1, \dots, x_n\}$ auch $t(x_1, \dots, x_n)$ schreiben.

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 $\mathfrak{T}(X, (f_i)_{i\in I}) := (T, (f_i^{\mathfrak{T}})_{i\in I})$, 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 $\overline{\varphi}|_X = \varphi$.*

[4] Hier gilt es zu beachten, dass die Notation $T(X)$ die Funktionssymbole zwar nicht beinhaltet, aber die Menge der Terme dennoch von der Sprache $(f_i)_{i\in I}$ abhängt.

[5] Wegen Definition 1.2.3 ist diese erneute Belegung der Begriffe *Sprache* und *Signatur* aus Definition 1.1.1 gerechtfertigt.

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 $\overline{\varphi}(f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})) = \overline{\varphi}(f_i(t_1, \dots, f_{n_i})) \stackrel{\text{Def.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i}))$, 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 $\widetilde{\varphi}(t) = \widetilde{\varphi}(f_i(t_1, \dots, t_{n_i})) = \widetilde{\varphi}(f_i^{\mathfrak{T}}(t_1, \dots, t_{n_i})) = f_i^{\mathfrak{A}}(\widetilde{\varphi}(t_1), \dots, \widetilde{\varphi}(t_{n_i})) \stackrel{\text{I.V.}}{=} f_i^{\mathfrak{A}}(\overline{\varphi}(t_1), \dots, \overline{\varphi}(t_{n_i})) = \overline{\varphi}(t)$. □

02.03.2023
08.03.2023

Definition 1.2.5. Seien $X^{(k)} = \{x_1, \dots, x_k\} \subseteq X$ eine Teilmenge der Variablenmenge, $\mathfrak{T}^{(k)} = \mathfrak{T}(X^{(k)}, (f_i)_{i\in I}) = (T^{(k)}, (f_i^{\mathfrak{T}})_{i\in I})$[6] die erzeugte Termalgebra und $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i\in I})$ eine Algebra vom selben Typ. Für $a_1, \dots, a_k \in A$ heißt $\alpha_{a_1,\dots,a_k} : X^{(k)} \to A, x_j \mapsto a_j$ eine *Variablenbelegung*. Nach Satz 1.2.4 kann diese nun zum *Einsetzungshomomorphismus* $\overline{\alpha}_{a_1,\dots,a_k} : T^{(k)} \to A$ fortgesetzt werden.

Für einen beliebigen Term $t \in T^{(k)}$ ist die *durch t in $\mathfrak{A}$ induzierte Termoperation* oder auch *Termfunktion* 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 $X = \{x_1, x_2, \dots\}$. 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.

[6] Streng genommen müsste $(f_i^{\mathfrak{T}^{(k)}})_{i\in I}$ in der Definition stehen, wegen $f_i^{\mathfrak{T}^{(k)}} = f_i^{\mathfrak{T}}|_{T^{(k)}(X)}$ ist auch die hier gegebene Notation sinnvoll, welche wir zwecks besserer Lesbarkeit verwenden werden.

1.3 Varietäten und Klone

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

Definition 1.3.1. Sei Σ eine Menge von Gesetzen über einer 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

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

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 $g_1, \dots, g_n : M^k \to M$ definieren wir hier als

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

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

1.4 Konstruktion neuer Algebren

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

1.4.1 Unteralgebren

Definition 1.4.1. Sei $\mathfrak{A} = (A, (f_i^{\mathfrak{A}})_{i \in I})$ eine Algebra und $S \subseteq A$. Dann heißt das Tupel $\mathfrak{S} = (S, (f_i^{\mathfrak{A}}|_{S^{n_i}})_{i \in I})$[7] *Subalgebra* oder *Unteralgebra* von $\mathfrak{A}$, wenn

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

Wir schreiben in diesem Fall $\mathfrak{S} \leq \mathfrak{A}$. Ist $\mathcal{A}$ eine Gruppe (ein Monoid, ein Ring,...[8]) so nennen wir $\mathcal{S}$ auch *Untergruppe* (*Untermonoid*, *Unterring*,...).

Beispiel 1.4.2. Sei $\mathfrak{V} = (V, +, 0, -, (m_k)_{k \in \mathfrak{K}})$ ein Vektorraum über einem Körper $\mathfrak{K}$. Dann stimmen die Definition des Untervektorraumes aus Definition 1.4.1 und aus der Linearen Algebra überein.

Weitere Beispiele für Unteralgebren sind $(\mathbb{N}, +) \leq (\mathbb{Z}, +)$ und die spezielle lineare Gruppe (das sind alle $n \times n$-Matrizen mit Determinante 1) als Untergruppe der allgemeinen linearen Gruppe $(\mathrm{Sl}_n(K), \cdot) \leq (\mathrm{Gl}_n(K), \cdot)$.

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

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 $(\{0\}, +, 0, -, (m_k)_{k \in \mathfrak{K}})$ 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 $\mathfrak{A}$. □

[7] Zwecks besserer Lesbarkeit werden wir dafür meist $\mathfrak{S} = (S, (f_i^{\mathfrak{S}})_{i \in I})$ schreiben.
[8] Körper nehmen eine Sonderrolle ein, siehe dazu Definition 4.1.1

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* $\langle S\rangle^9 := \bigcap\{\mathfrak{U} \mid S \subseteq U \wedge \mathfrak{U} = (U, (f_i^{\mathfrak{A}}|_{U^{n_i}})_{i\in I}) \leq \mathfrak{A}\}$ *die kleinste* S *enthaltende Unteralgebra von* $\mathfrak{A}$.

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

$$S_0 := S, \quad S_{k+1} := S_k \cup \{f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i}) \mid i \in I \wedge a_1, \ldots a_{n_i} \in S_k\}, \quad {S_\infty}^{10} := \bigcup_{k\geq 0} S_k.$$

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

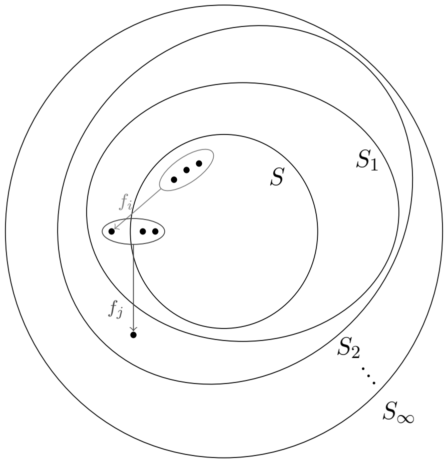

Abbildung 1.2: Subalgebra von unten

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

1. $\langle S\rangle = S_\infty$
2. $\langle S\rangle = \{t^{\mathfrak{A}}(a_1, \ldots, a_n) \mid n \in \mathbb{N}, a_1, \ldots, a_n \in S, t(x_1, \ldots, x_n) \in T(X)\}$

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

1. Da ${S_\infty}^{11}$ 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 $a \in S_{k+1}$ beliebig. Falls $a \in S_k$ ist, so folgt aus der Induktionsvoraussetzung dass $a \in \langle S\rangle$ gilt. Andernfalls existieren ein $i \in I$ und $a_1, \ldots, a_{n_i} \in S_k$, sodass $a = f_i^{\mathfrak{A}}(a_1, \ldots, a_{n_i})$. Auch hier kann die Induktionsvoraussetzung angewandt werden, weshalb $a_1, \ldots, a_{n_i} \in \langle S\rangle$ ist. Da $(\langle S\rangle, (f_i^{\mathfrak{A}}|_{\langle A\rangle^{n_i}})_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$ ist, gilt auch $a = f_i^{\mathfrak{A}}(a_1 \ldots, a_{n_i}) \in \langle S\rangle$. Daraus folgt die gewünschte Mengeninklusion $S_{k+1} \subseteq \langle S\rangle$.

[9] Die hier gegebene Notation $\langle S\rangle$ ist nur dann sinnvoll, wenn die Algebra $\mathfrak{A}$ im Kontext klar ist. Ansonsten sollte die Notation $\langle S\rangle_{\mathfrak{A}}$ verwendet werden.
[10] Auch hier ist die Notation nur dann sinnvoll, wenn die Algebra $\mathfrak{A}$ im Kontext offensichtlich ist.
[11] Hier wird die Algebra für bessere Lesbarkeit mit der Trägermenge identifiziert

2. Definiere $M := \{t^{\mathfrak{A}}(a_1,\dots,a_n) \mid n \in \mathbb{N}, a_1,\dots,a_n \in S, t(x_1,\dots,x_n) \in T(X)\}$. 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 $t := f_i^{\mathfrak{T}}(t_1(x_1^{(1)},\dots,x_{m_1}^{(1)}),\dots,t_{n_i}(x_1^{(n_i)},\dots,x_{m_{n_i}}^{(n_i)}))$, 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 mit mindestens n Elementen. Dann gilt für die von S erzeugte Unteralgebra*

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

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

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

1.4.2 Produktalgebren

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

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

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

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

Beispiel 1.4.17. Abbildung 1.3 visualisiert die Bildung einer Produktalgebra.

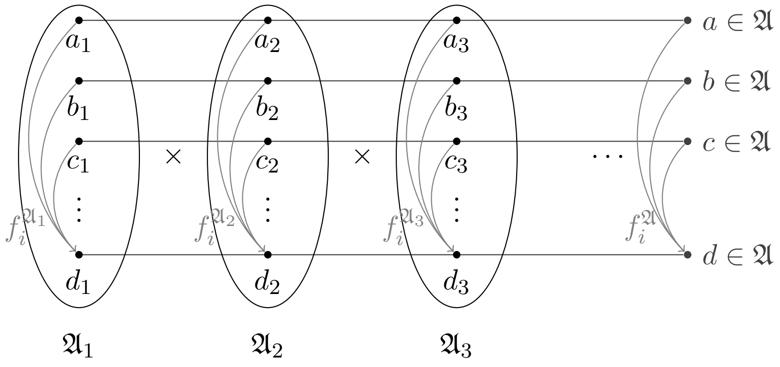

Abbildung 1.3: Visualisierung von Produktalgebren

Bemerkung 1.4.18. Ist $\mathfrak{A} = \prod_{j \in J} \mathfrak{A}_j$ eine Produktalgebra und $j \in J$, so ist durch die Projektionsabbildung $\pi_k : \mathfrak{A} \to \mathfrak{A}_j, (a_j)_{j \in J} \mapsto a_k$ 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 $\mathbf{a}^{(1)} = (a_j^{(1)})_{j \in J}, \dots, \mathbf{a}^{(n)} \in A$ beliebig. Dann gilt laut Voraussetzung für alle $j \in J : s^{\mathfrak{A}_j}(a_j^{(1)}, \dots, a_j^{(n)}) = t^{\mathfrak{A}_j}(a_j^{(1)}, \dots, a_j^{(n)})$. Daher folgt $s^{\mathfrak{A}}(\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)})_j = s^{\mathfrak{A}_j}(a_j^{(1)}, \dots, a_j^{(n)}) = t^{\mathfrak{A}_j}(a_j^{(1)}, \dots, a_j^{(n)}) = t^{\mathfrak{A}}(\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)})_j$ für alle $j \in J$, also insbesondere $s^{\mathfrak{A}}(\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)}) = t^{\mathfrak{A}}(\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)})$ und damit $s^{\mathfrak{A}} = t^{\mathfrak{A}}$. $\square$

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

Bemerkung 1.4.21. Auch an dieser Stelle wird deutlich, dass die Klasse der Körper keine Varietät ist. Für einen Körper $\mathfrak{K}$ und den Produktraum $\mathfrak{K} \times \mathfrak{K}$ gilt $(1,0) \cdot (0,1) = (0,0)$. Da Körper immer nullteilerfrei sind, kann dieser Produktraum folglich kein Körper sein. 09.03.2023

15.03.2023

1.4.3 Faktoralgebren

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

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

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 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[12] ist und die Funktionen definiert[13] sind durch $f_i^{\mathfrak{A}/\sim}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) := [f_i(a_1, \ldots, a_{n_i})]_\sim$.

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

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

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

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

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

$$\begin{tikzcd}
\mathfrak{A} \arrow[r, "h"] \arrow[d, "\varphi"'] & \mathfrak{B} \\
\mathfrak{A}/_{\ker h} \arrow[ur, dashed, "\tilde{h}"'] &
\end{tikzcd}$$

Abbildung 1.4: Visualisierung der Aussage des Homomorphiesatzes

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

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

Beweis. 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 $[a_1], \dots, [a_{n_i}] \in A/_{\ker h}$ beliebig. Dann gilt laut Definition $\tilde{h}(f_i^{\mathfrak{A}/_{\ker h}}([a_1], \dots, [a_{n_i}])) = \tilde{h}([f_i^{\mathfrak{A}}(a_1, \dots, a_{n_i})]) = h(f_i^{\mathfrak{A}}(a_1, \dots, a_{n_i})) = f_i^{\mathfrak{B}}(h(a_1), \dots, h(a_{n_i})) = f_i^{\mathfrak{B}}(\tilde{h}([a_1]), \dots, \tilde{h}([a_{n_i}]))$, 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 $[a] = [b]$.

Für die Surjektivität von $\tilde{h}$ ist nichts zu zeigen. □

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

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

15.03.2023

16.03.2023

1.4.4 Der Satz von Birkhoff

Definition 1.4.35. Sei $\mathcal{K}$ eine Klasse von Algebren. Dann definieren[14] 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 denen 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 alle $\mathfrak{A}_j \in \mathcal{K}$ sind.

Wir sagen, dass $\mathcal{K}$ unter HSP abgeschlossen ist, wenn HSP$\mathcal{K} = \mathcal{K}$ gilt. Ist $\mathcal{A}$ eine Algebra, so ist auch $H\mathfrak{A} := H\mathfrak{A}$ eine Kurzschreibweise. Entsprechendes gilt auch für $S\mathfrak{A}$ und $P\mathfrak{A}$.

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

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

[14] Die Notationen „S“ und „P“ kommen von den Wörtern (beziehungsweise ihren englischen Übersetzungen) „Subalgebra“ und „Produktalgbra“. Die Notation „H“ hat ihre Abstammung von den „homomorphen Bildern“, was durch Satz 1.4.32 gerechtfertigt wird.

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

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

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

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

Beweis des Satzes von Birkhoff. Ist $\mathcal{K}$ eine Varietät, so ist $\mathcal{K}$ laut 1.4.5, 1.4.20 und 1.4.34 unter HSP abgeschlossen. Es bleibt die andere Implikation zu zeigen. Sei also $\mathcal{K}$ unter HSP abgeschlossen und definiere $\Sigma := \Sigma(\mathcal{K})$ und $\mathcal{V} := \mathcal{V}(\Sigma)$, womit es hinreichend ist, $\mathcal{V} = \mathcal{K}$ zu zeigen. 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 $\Sigma(\mathfrak{B}) = \Sigma \subseteq \Sigma(\mathfrak{A})$. Es ist nun hinreichend zu zeigen, dass $\mathfrak{A} \in \mathrm{HSP}\mathfrak{B}$ gilt.

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 $t^{\mathfrak{S}}(\pi_{a_1}, \dots, \pi_{a_n})$ mit $a_1 \dots, a_n \in A$. Daher wird $\varphi(t^{\mathfrak{S}}(\pi_{a_1}, \dots, \pi_{a_n})) := t^{\mathfrak{A}}(a_1, \dots, a_n)$ 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 $a_1, \dots, a_n, a'_1, \dots, a'_m \in A$ sind, sodass $u^{\mathfrak{S}}(\pi_{a_1}, \dots, \pi_{a_n}) = v^{\mathfrak{S}}(\pi_{a'_1}, \dots, \pi_{a'_m})$ gilt, dann soll auch $u^{\mathfrak{A}}(a_1, \dots, a_n) = v^{\mathfrak{A}}(a'_1, \dots, a'_m)$ gelten. Dafür werden $x_i := a_i$ und $x'_i := a'_i$ als Variablen eingeführt. Es ist nun hinreichend zu zeigen, dass $\mathfrak{B} \models u(x_1, \dots, x_n) \approx v(x'_1, \dots, x'_m)$ gilt, da dieses Gesetz wegen $\Sigma(\mathfrak{B}) \subseteq \Sigma(\mathfrak{A})$ dann auch in $\mathfrak{A}$ gilt, was insbesondere $u^{\mathfrak{A}}(a_1, \dots, a_n) = v^{\mathfrak{A}}(a'_1, \dots, a'_m)$ bedingen würde. Sind $b_i, b'_i \in B$ beliebige Werte für die Variablen x_i respektive x'_i, so muss $u^{\mathfrak{B}}(b_1, \dots, b_n) = v^{\mathfrak{B}}(b'_1, \dots, b'_m)$ 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 $u^{\mathfrak{S}}(\pi_{a_1}, \dots, \pi_{a_n}) = v^{\mathfrak{S}}(\pi_{a'_1}, \dots, \pi_{a'_m})$ erfüllt ist, gilt diese Gleichheit insbesondere wenn α als Argument eingesetzt wird. Dies liefert $u^{\mathfrak{B}}(b_1, \dots, b_n) = u^{\mathfrak{S}}(\pi_{a_1}, \dots, \pi_{a_n})(\alpha) = v^{\mathfrak{S}}(\pi_{a'_1}, \dots, \pi_{a'_m})(\alpha) = v^{\mathfrak{B}}(b'_1, \dots, b'_m)$, 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 $g_1, \dots, g_{n_i} \in S$ beliebig. Zu zeigen ist $\varphi(f_i^{\mathfrak{S}}(g_1, \dots, g_{n_i})) = f_i^{\mathfrak{A}}(\varphi(g_1), \dots, \varphi(g_{n_i}))$. Für jedes $j \in \{1, \dots, n_i\}$ 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 und somit $\mathfrak{A} \in \mathrm{HSP}\mathcal{K}$, was zu zeigen war. □

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

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

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

1.5 Freie Algebren

Definition 1.5.1. Sei $\tau = (n_i)_{i\in I}$, $\mathcal{K}$[15] eine Klasse von τ-Algebren, $\mathfrak{F} \in \mathcal{K}$ und $X \subseteq F$. Dann heißt $\mathfrak{F}$ *frei über X in $\mathcal{K}$*, wenn es für alle $\mathfrak{A} \in \mathcal{K}$ und alle $\varphi : X \to A$ genau einen Homomorphismus $\overline{\varphi} : \mathfrak{F} \to \mathfrak{A}$ mit $\overline{\varphi}|_X = \varphi$ gibt.

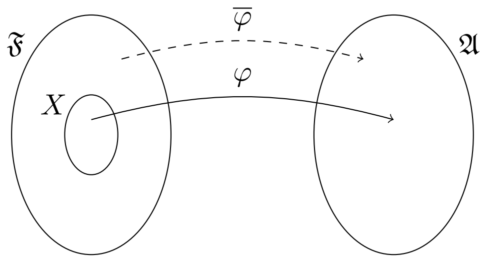

Abbildung 1.5: $\mathfrak{F}$ frei über X

Beispiel 1.5.2. Sei $\mathcal{K}$ die Klasse der Vektorräume über dem Körper $\mathbb{C}$, $\mathfrak{V} \in \mathcal{K}$ beliebig, $\tau = (2, 0, 1, (1)_{m\in\mathbb{C}})$ und $X \subseteq V$ eine Basis von $\mathfrak{V}$. Dann ist $\mathfrak{V}$ frei über X in $\mathcal{K}$.

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

Beispiel 1.5.3. Sei $\mathcal{K}$ eine Varietät definiert durch Gesetze Σ in der Sprache $(f_i)_{i\in I}$, 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 $\mathfrak{S}$ – ebenfalls nach dem Beweis des Satzes von Birkhoff – frei über $\{\pi_x \mid x \in X\}$ in $\mathcal{K}$.

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

[15] Die Familie der Funktionssymbole $(f_i)_{i\in I}$ spielt in diesem Unterkapitel eine untergeordnete Rolle und wird daher meist weggelassen. Implizit werden sie durch τ eingeführt.

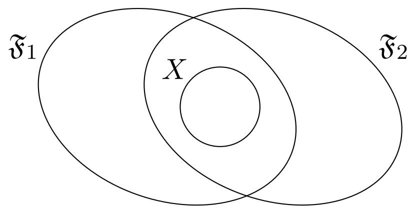

Abbildung 1.6: $\mathfrak{F}_1, \mathfrak{F}_2$ frei über X

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

16.03.2023
22.03.2023

Bemerkung 1.5.5. Sind $\mathfrak{C}, \mathfrak{D}$ Algebren in derselben Sprache, $C = \langle S \rangle$ und $\varphi, \psi : \mathfrak{C} \to \mathfrak{D}$ Homomorphismen mit $\varphi|_S = \psi|_S$, so folgt $\varphi = \psi$. Das heißt, dass zwei Homomorphismen übereinstimmen, wenn sie dies auf einem Erzeuger tun.

Proposition 1.5.6. *Sei $\mathcal{K}$ eine Klasse von Algebren mit Typ $(n_i)_{i\in I} =: \tau$ in der Signatur $(f_i)_{i\in I}$. Sei $\mathrm{S}\mathcal{K} \subseteq \mathcal{K}$ was insbesondere der Fall ist, falls $\mathcal{K}$ eine Varietät ist. Sei $\mathfrak{F}$ in $\mathcal{K}$ frei über $X \subseteq F$, so ist $\mathfrak{F} = \langle X \rangle$.*

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

Nun ist $\langle X \rangle$ frei über X in $\mathcal{K}$: Um dies einzusehen, seien $\mathfrak{A} \in \mathcal{K}, \varphi : X \to A$ beliebig. Zu zeigen ist, dass es einen eindeutigen, φ fortsetzenden Homomorphismus $\overline{\varphi} : \langle X \rangle \to \mathfrak{A}$ gibt mit $\overline{\varphi}|_X = \varphi$. Wir wissen es gibt einen eindeutigen Homomorphismus $\overline{\overline{\varphi}} : F \to A$ mit $\overline{\overline{\varphi}}|_X = \varphi$. Definiere $\overline{\varphi} := \overline{\overline{\varphi}}|_{\langle X \rangle}$, so erfüllt dieser Homomorphismus die geforderte Eigenschaft. Die Eindeutigkeit folgt aus Bemerkung 1.5.5.

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

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

frei über X in der Klasse der τ-Algebren.

Ist $\mathcal{K}$ eine Varietät von τ-Algebren, so stellt sich also 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. Im Folgenden werden wir daher versuchen, aus dieser Termalgebra eine passende Faktoralgebra zu gewinnen, welche frei über X in $\mathcal{K}$ ist. Dazu wird mithilfe einer Menge von Gesetzen eine Kongruenzrelation auf der Termalgebra definiert.

Proposition 1.5.8. *Sei $\mathcal{K}$ eine Varietät in der Sprache $(f_i)_{i\in I}$, X eine beliebige Menge und definiere*

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

so ist $\Sigma_{X,\mathcal{K}}$ eine Kongruenzrelation auf $T(X)$.

Beweis. $\Sigma_{X,\mathcal{K}}$ 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 $s,t \in T(X), (s,t) \in \Sigma_{X,\mathcal{K}}$, so gilt

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

  also $(t,s) \in \Sigma_{X,\mathcal{K}}$.
- transitiv: Sind $s,t,u \in T(X), (s,t),(t,u) \in \Sigma_{X,\mathcal{K}}$, so gilt

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

  also $(s,u) \in \Sigma_{X,\mathcal{K}}$.

Um zu sehen, dass $\Sigma_{X,\mathcal{K}}$ auch eine Kongruenzrelation ist, seien $i \in I, (s_1,t_1), ..., (s_{n_i}, t_{n_i}) \in \Sigma_{X,\mathcal{K}}$. Zu zeigen ist $(f_i(s_1,...,s_{n_i}), f_i(t_1,...,t_{n_i})) \in \Sigma_{X,\mathcal{K}}$. 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 $(f_i(s_1,...,s_{n_i}), f_i(t_1,...,t_{n_i})) \in \Sigma_{X,\mathcal{K}}$. $\square$

Definition 1.5.9. Sei $\tau = (n_i)_{i\in I}$ eine Signatur, $\mathcal{K}$ eine Varietät in der Sprache $(f_i)_{i\in I}$, X eine beliebige Menge. Dann definieren wir $\mathfrak{T}^{X,\Sigma_{X,\mathcal{K}}} := \mathfrak{T}^X/_{\Sigma_{X,\mathcal{K}}}$.

Satz 1.5.10. *Sei $\tau = (n_i)_{i\in I}$ eine Signatur, $\mathcal{K}$ eine Varietät in der Sprache $(f_i)_{i\in I}$, X eine beliebige Menge. Dann ist $\mathfrak{T}^{X,\Sigma_{X,\mathcal{K}}}$ frei über $\{[x]_{\Sigma_{X,\mathcal{K}}} \mid x \in X\}$ in $\mathcal{K}$.*

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

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

Betrachte

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

Zunächst ist φ wohldefiniert: Seien dazu $u,v \in T(X)$ mit $u^{\mathfrak{S}}(\pi_{x_1},...,\pi_{x_n}) = v^{\mathfrak{S}}(\pi_{x'_1},...,\pi_{x'_m})$ und $x_1,\dots,x_n,x'_1,\dots,x'_m \in X$, 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 $(u(x_1,...,x_n), v(x'_1,...,x'_m)) \in \Sigma_{X,\mathcal{K}}$ und damit $[u(x_1,...,x_n)]_{\Sigma_{X,\mathcal{K}}} = [v(x'_1,...,x'_m)]_{\Sigma_{X,\mathcal{K}}}$ folgt.

Weiters ist φ surjektiv, da mit beliebigem $[t(x_1,...,x_n)]_{\Sigma_{X,\mathcal{K}}} \in \mathfrak{T}^{X,\Sigma_{X,\mathcal{K}}}$ sofort $t^{\mathfrak{S}}(\pi_{x_1},...,\pi_{x_n}) \overset{\varphi}{\mapsto} [t(x_1,...,x_n)]_{\Sigma_{X,\mathcal{K}}}$ 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 $\mathfrak{T}^{X,\Sigma_{X,\mathcal{K}}}$ frei über $\{[x]_{\Sigma_{X,\mathcal{K}}} \mid x \in X\}$ ist. $\square$

22.03.2023
23.03.2023

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

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

Falls[16] es ein neutrales Element e gibt, so wird $a^0 := e$ definiert und im Fall, dass a ein inverses Element a^* besitzt wird rekursiv definiert:

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

Bemerkung 1.5.12. Ist $(G,\cdot,e,^{-1})$ eine Gruppe so gilt $\forall m,n \in \mathbb{Z} \forall a \in G : a^m \cdot a^n = a^{m+n}$ und $(a^m)^n = a^{m\cdot n}$. Falls $\cdot$ kommutativ ist, gilt weiters $\forall a,b \in G \forall m \in \mathbb{Z} : (a\cdot b)^m = a^m \cdot b^m$.

Beispiel 1.5.13. Bezeichne $(\cdot,e,^{-1})$ vom Typ $\tau = (2,0,1)$ die Sprache der Gruppen. Sei $X = \{x_1,x_2,...\}$ eine Variablenmenge so sind[17]

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

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

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

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

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

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

Beispiel 1.5.14. Es sei $(\cdot,e,^{-1})$ die Sprache der Gruppen und $X = \{x_1,x_2,\dots\}$ eine Variablenmenge. Ausgehend von Beispiel 1.5.13 kann analog die freie kommutative Gruppe über X in der Klasse aller kommutativen Gruppen konstruiert werden. Jedes Element der Termalgebra besitzt dann einen Repräsentanten der Form $x_{i_1}^{m_1},\dots,x_{i_k}^{m_k}$ mit $m_1,\dots,m_k \in \mathbb{Z}$ und $\forall j,\ell \in \{1,\dots,k\} : j<\ell \Rightarrow i_j < i_\ell$.

[16]Insbesondere sind diese Notationen für Monoide und Gruppen definiert.
[17]Dass $\mathfrak{T}(X)$ frei über X in der Klasse aller τ-Algebren ist gilt allgemein und wurde hier nur als Vergleich zur Faktoralgebra angeführt.

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

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

Beispiel 1.5.17. Es sei $\mathfrak{K}$ ein Körper, $(+, 0, -, (m_r)_{r\in\mathfrak{K}})$ die Sprache der Vektorräume über $\mathfrak{K}$ in der Signatur $\tau = (2, 0, 1, (1)_{m\in\mathfrak{K}})$. Sei $X = \{x_1, x_2, \ldots\}$ eine Variablenmenge so sind[18]

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

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

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

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

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

Jedes Element t von $T(X)/_{\Sigma_X}$ hat einen Repräsentanten der Form $c_1 \odot x_{i_1} + \ldots + c_n \odot x_{i_n}$ mit $\forall j, k \in \{1, \ldots, n\} : j < k \Rightarrow i_j < i_k$. Identifiziert man $x \in X$ mit $[x] \in T(X)/_{\Sigma_X}$, so kann man daher $[x_1], [x_2], \ldots$ als Basis des freien Vektorraumes über der Menge X[19] sehen.

[18] Dass $\mathfrak{T}(X)$ frei über X in der Klasse aller τ-Algebren ist gilt allgemein und wurde hier nur als Vergleich zur Faktoralgebra angeführt.

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

Kapitel 2

Elementare Strukturentheorie

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

2.1 Halbgruppen und Monoide

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

Zu Beginn wollen wir auf die Definitionen 1.1.4, 1.1.6 und 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. Besitzt a ein inverses Element, so heißt a *Einheit*.

Lemma 2.1.3. *Neutrale Elemente in Halbgruppen und inverse Elemente in Monoiden 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 sind. 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 definitionsgemäß 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*

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

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, $e \cdot x_1, x_1 \cdot (x_1 \cdot x_1), \ldots$ als Terme 2-ter Stufe etc. Nach Faktorisieren wie im Beweis von 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 unendlich, so ist das erzeugte Monoid *total frei* über X, das heißt es gelten genau die Gesetze, die in der Varietät gelten, wie man aus folgender Bemerkung erkennt.

Bemerkung 2.1.9. Sei X eine beliebige Variablenmenge. Ist $\mathcal{K}$ eine Varietät in der Sprache $(f_i)_{i \in I}$, $\mathfrak{F}$ frei über X in $\mathcal{K}$, dann gilt

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

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

Satz 2.1.10 (Darstellungssatz von Cayley für Monoide)**.** *Sei $\mathfrak{M} = (M, \cdot, e)$ ein Monoid, so existiert ein injektiver Homomorphismus $\varphi : \mathfrak{M} \to (M^M, \circ, \mathrm{id}_M)$*[1]*.*

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. ☐

Wichtig für Satz 2.1.11 ist die Menge der Primzahlen, welche wir mit dem Symbol $\mathbb{P}$ bezeichnen.

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*

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

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

[1]Wie man leicht nachrechnet ist $(M^M, \circ, \mathrm{id}_M)$ für jede beliebige nicht leere Menge M ein Monoid.

Beweis. Definieren wir $\varphi : S \to \mathbb{N} \setminus \{0\}, (s_p)_{p\in\mathbb{P}} \mapsto \prod_{p\in\mathbb{P}} p^{s_p}$ 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 $\varphi((s_p)_{p\in\mathbb{P}} +^{\mathfrak{S}} (t_p)_{p\in\mathbb{P}}) = \prod_{p\in\mathbb{P}} p^{s_p+t_p} = \prod_{p\in\mathbb{P}} p^{s_p} \cdot \prod_{p\in\mathbb{P}} p^{t_p} = \varphi((s_p)_{p\in\mathbb{P}}) \cdot \varphi((t_p)_{p\in\mathbb{P}})$.
- Surjektivität: Zeigen wir mittels 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 den Fall $n \notin \mathbb{P}$. Wir wissen, dass es $i, j < n$ 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 $n \in \mathbb{N} \setminus \{0\}$ bis auf die Reihenfolge der Faktoren 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 $n = p_1 \cdot ... \cdot p_\ell = q_1 \cdot ... \cdot q_m$, 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 die Reihenfolge der Faktoren). 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 $r_i \neq p_1, q_i \neq p_1$. Da auch $n' = p_1 \cdot (p_2 \cdots p_l - q_2 \cdots q_m)$ gilt und sich der zweite Faktor in Primfaktoren zerlegen lässt, haben wir zwei verschiedene Primfaktorenzerlegungen von $n' < n$ gefunden, 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 $(S, \wedge, \vee)$.

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. $(\mathbb{N} \setminus \{0\}, |)$ *ist eine Halbordnung und induziert durch* $n \vee m := \mathrm{kgV}(n, m)$, $n \wedge m := \mathrm{ggT}(n, m)$ *einen Verband* $(\mathbb{N} \setminus \{0\}, \wedge, \vee)$.

Beweis. Seien $n, m \in \mathbb{N} \setminus \{0\}$ und definiere für obiges $\varphi : S \to \mathbb{N} \setminus \{0\}$

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

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

□

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*.
- Ist a links- und rechtskürzbar, so heißt a *kürzbar*.

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 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 (siehe Satz 2.1.18). Es sei angemerkt, dass die Kommutativität im Allgemeinen nicht notwendig 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. Betrachten wir die freie Gruppe über $\{x, y\}$, so erhalten wir mit der Menge aller Wörter von der Form $x^{n_1} y^{m_1} \cdot \ldots \cdot x^{n_l} y^{m_l}$ $(n_i, m_i \geq 0)$ ein nicht kommutatives Untermonoid. Das Beispiel zeigt, ebenfalls, dass Kommutativität nicht notwendig ist.

Satz 2.1.18. *Sei $\mathfrak{H} = (H, \cdot, e)$ ein kommutatives Monoid und jedes $a \in H$ kürzbar*[2]*. Dann gilt*

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

2. $\mathfrak{H}^2/_\sim$ *ist eine Gruppe.*

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 injektiven Homomorphismen $\psi : \mathfrak{H} \to \mathfrak{G}$ einen injektiven Homomorphismus $\overline{\psi} : \mathfrak{H}^2/_\sim \to \mathfrak{G}$ mit $\overline{\psi} \circ \varphi = \psi$.*

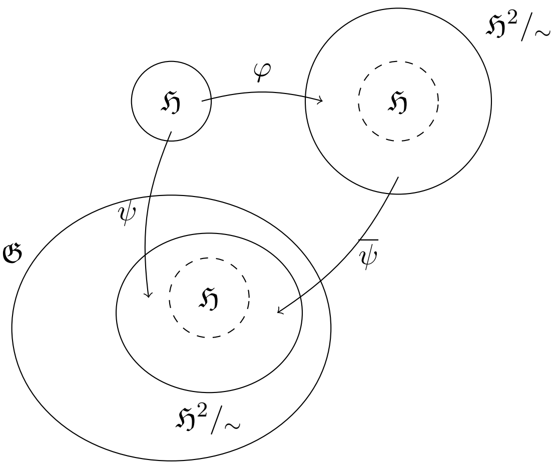

Abbildung 2.1: Visualisierung der Einbettung von $\mathfrak{H}$ in die Gruppen $\mathfrak{G}, \mathfrak{H}^2/_\sim$

Beweis.

1. Prüfen wir zunächst, dass $\sim$ eine Äquivalenzrelation ist.
   a) reflexiv: Es gilt $(a, b) \sim (a, b)$, da $ab = ba$.
   b) symmetrisch: Es gilt
   $$(a, b) \sim (c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d) \sim (a, b).$$
   c) transitiv: Seien $(a, b) \sim (c, d) \sim (u, v)$, dann ist $ad = bc$ und $cv = du$. Dann folgt
   $$(av)(cd) = addu = bcdu = (bu)(cd)$$
   und damit $av = bu$ und $(a, b) \sim (u, v)$ 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] Aufgrund der Kommutativität reicht es sogar lediglich Links- oder Rechtskürzbarkeit zu fordern.

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 ein 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. $\psi = \mathrm{id}_H$[3] und definiere $\overline{\psi}: \mathfrak{H}^2/_\sim \to \mathfrak{G}$, $[(a,b)]_\sim \mapsto a \cdot b^{-1}$.

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

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

□

2.2 Gruppen

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

- Wir nennen $|G|$ die *Ordnung* der Gruppe.
- Sei $g \in G$, so erzeugt dieses Element eine Untergruppe
$$\langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$
  Wir nennen $|\langle \{g\} \rangle|$ die *Ordnung* von g und schreiben auch $\mathrm{ord}(g)$. Ist $\mathrm{ord}(g)$ endlich, so heißt g *Torsionselement.*
- $\mathfrak{G}$ heißt *zyklisch*, falls es ein $g \in G$ mit $G = \langle \{g\} \rangle$ gibt.

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

Beispiel 2.2.3.

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

[3] Diese Einschränkung ist möglich, da ψ ein injektiver Homomorphismus ist.

Beispiel 2.2.4.

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

29.03.2023

30.03.2023

2.2.1 Nebenklassen und Normalteiler

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

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

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

1. *Die Menge $\{gU \mid g \in G\}$ aller Linksnebenklassen von g nach U bildet eine Partition von G.*
2. *Es gilt $gU = g'U$ genau dann, wenn $g^{-1}g' \in U$.*
3. *Die Partition aus Punkt 1 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. "$\Rightarrow$": Sei vorausgesetzt, dass $x \sim y$ gilt. Dann gibt es $g \in G$ und $u, u' \in U$, sodass $x = gu$ und $y = gu'$ gilt. Es ist also $x^{-1}y = u^{-1}g^{-1} \cdot gu' = u^{-1}u' \in U$.

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

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

$\square$

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

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

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

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

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

$U = eU$	g_1U	g_2U	g_3U
g_4U	g_5U	g_6U	g_7U

G

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*
- $\operatorname{ord}(g)$ *teilt* $|G|$.

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

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

Sei G eine Gruppe mit $|G| = p \in \mathbb{P}$. Für $g \in G \setminus \{e\}$ gilt nun $\operatorname{ord}(g) = p \Rightarrow \langle g \rangle = G$, 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 $V \leq U \leq G$ 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 $N \triangleleft G$.

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. Zuletzt ist für $n \in N$ auch $n^{-1} \in N$ nötig. Das gilt wegen $\varphi(n^{-1}) = \varphi(n)^{-1} = e^{-1} = e$, daher ist $N \leq G$.

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 alle $y \in G$ 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

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

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

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

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

  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

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

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

$\square$

Bemerkung 2.2.18. Satz 2.2.17 beschreibt einige Eigenschaften von Normalteilern.

- (1), (1') liefern den bijektiven Zusammenhang von Normalteilern und Kongruenzrelationen auf Gruppen. Betrachtet man die Menge N aller Normalteiler einer Gruppe G mit den Operationen $A \wedge_N B := A \cap B$ und $A \vee_N B := A \cdot B$ mit dem Komplexprodukt aus Definition 2.2.29, so erhält man einen Verband. Weiters kann man die Menge aller Kongruenzrelationen auf G betrachten, welche wir mit $\mathrm{Cong}(G)$ bezeichnen. Für $R, S \in \mathrm{Cong}(G)$ definiert man $R \wedge_\sim S := R \cap S$. Weiters bezeichnen wir mit $\mathrm{cl}_G(\sim) := \bigcap\{R \in \mathrm{Cong}(G) \mid \sim \subseteq R\}$ die kleinste Kongruenzrelation, die $\sim$ enthält. Dann ist mit $R \vee_\sim S := \mathrm{cl}_G(R \cup S)$ durch $(\mathrm{Cong}(G), \wedge_\sim, \vee_\sim)$ ein Verband gegeben. Die beiden beschriebenen Verbände sind isomorph, wobei die genannte Bijektionen einen Verbandsisomorphismus darstellt.
- (2), (2') beschreiben die Darstellung des Normalteilers über den Kern eines Homomorphismus $\varphi : G \to H$. Es ist $\ker\varphi = \{g \in G \mid \varphi(g) = e_H\} = \varphi^{-1}(\{e_H\}) = N$.
- (3), (3') liefern direkt, dass Normalteiler unter Abbildungen $\pi_x : G \to G, g \mapsto xgx^{-1}$ abgeschlossen sind. So eine Abbildung nennt man *inneren Automorphismus*.
- (4), (4') besagen, dass die Links- und Rechtsnebenklassen einer Untergruppe genau dann gleich sind, wenn die Untergruppe ein Normalteiler ist.

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

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

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

30.03.2023

19.04.2023

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

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

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

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

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

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

Dabei ist

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

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

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

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

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

In dieser Gruppe rechnet man

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

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

Im Falle $n = 4$ ist beispielsweise

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

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

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

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

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

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

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

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

Bemerkung 2.2.25. Sei G eine Gruppe, $\sim$ eine Kongruenzrelation und $N = [e]_\sim$. Wir fragen uns, wann $G/_\sim$ kommutativ ist. Dazu bemerken wir

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

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

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

Wir nennen $[a, b]$ den *Kommutator* von (a, b). Wir stellen fest, dass $G/_\sim$ genau dann kommtuativ ist, wenn die Menge aller Kommutatoren in N enthalten ist (siehe dazu auch Satz 2.2.28).

Definition 2.2.26. Definiere

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

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

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

Beweis. Ist G abelsch so ist

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

□

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

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

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

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

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

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

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

so ist h_x ein Automorphismus[4]. Also ist

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

womit $G' \lhd G$ nach Satz 2.2.17 Punkt (3') folgt. □

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

2.2.2 Innere direkte Produkte

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

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

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

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

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

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

Für $i \in \{1, \ldots, n\}$ definiere $V_i := U_1 \cdot \ldots \cdot U_{i-1} \cdot U_{i+1} \cdot \ldots \cdot U_n$, so muss $U_i \cap V_i = \{e\}$ gelten: Sonst gäbe es $(u_j)_{j=1}^n \in (U_j)_{j=1}^n, u_i \neq e$ mit

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

womit φ nicht injektiv wäre.

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

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

Diese ist ein Homomorphismus, womit

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

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

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

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

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

Beweis. Es gilt

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

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

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

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

$$\begin{aligned}\varphi((u_1, \ldots, u_n) \cdot (v_1, \ldots, v_n)) = \varphi(u_1v_1, \ldots, u_nv_n) = u_1v_1 \ldots u_nv_n = \\ = u_1 \ldots u_nv_1 \ldots v_n = \varphi(u_1, \ldots, u_n)\varphi(v_1, \ldots, v_n).\end{aligned}$$

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

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

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

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

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

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

Definiere weiters

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

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

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

Es sei angemerkt, dass Proposition 2.2.33 nach demselben Argument entsprechend auch für solche inneren direkten Produkte gilt.

19.04.2023
20.04.2023

2.2.3 Zyklische Gruppen

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

Beispiel 2.2.35. Für $m \in \mathbb{Z}$ sind $\mathbb{Z} = \langle\{1\}\rangle_{\mathbb{Z}}$ und $\mathbb{Z}_m = \langle\{1\}\rangle_{\mathbb{Z}_m}$ zyklische Gruppen.

Proposition 2.2.36. *Für eine Gruppe G gilt:*

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

Beweis.

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

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

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

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

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

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

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

$\square$

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

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

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

Definition 2.2.39. Für $m \in \mathbb{N}\setminus\{0\}$ bezeichnen wir mit C_m die Gruppe $(\{0, \ldots, m-1\}, +, 0, -)$ wobei

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

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

2.2.4 Symmetrische und Permutationsgruppen

Definition 2.2.40. Für eine Menge A sei

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

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

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

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

Beweis. Definieren wir die Abbildungen

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

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

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

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

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

Bemerkung 2.2.43. Ein Beispiel einer Gruppenaktionen von G nach G ist also die Linkstranslation φ aus dem Beweis von Satz 2.2.41. Eine weitere bekannte Gruppenaktion ist die Abbildung

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

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

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

Definition 2.2.44. Sei G eine Gruppe. Dann ist das *Zentrum von G* definiert als

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

Definition 2.2.45. Sei $n \in \mathbb{N}$ beliebig. Eine *Permutation* ist eine bijektive Abbildung $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Eine Darstellung von Permutationen ist die sogenannte *Zyklenschreibweise*. Es wird die Permutation dabei dargestellt als

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

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

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

Proposition 2.2.46. *Für $n \in \mathbb{N}_{\geq 2}$ gilt*

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

Beweis.

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

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

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

2. Wir zeigen die Aussage mittels vollständiger Induktion:

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

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

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

   Es reicht also zu zeigen, dass die Identität keine ungerade Darstellung besitzt. Dazu definieren wir für jedes Element π aus S_n auf der Menge $M := \{(i,j) \mid 1 \leq i, j \leq n, i \neq j\}$ die Abbildung

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

   Sei $(i,j) \in M, i < j$, dann nennen wir (i,j) einen Fehlstand von π, wenn $\pi(i) > \pi(j)$ und mit $f(\pi)$ bezeichnen wir die Anzahl der Fehlstände von π. Sei $1 \leq a < b \leq n$ und betrachte die Transposition π_{ab} von a und b. Ein Fehlstand von π_{ab} muss klarerweise immer a oder b enthalten. Dann hat π_{ab} die Fehlstände (a,b), (a,j), wobei $a < j < b$ und (j,b), wobei $a < j < b$. Insgesamt ist die Anzahl der Fehlstände also ungerade. In der Übung wurde gezeigt: Wenn π eine Permutation und τ eine Transposition ist, dann gilt $f(\tau \circ \pi) = f(\pi) + 1 \,(\mathrm{mod} 2)$.

   Damit hat eine ungerade Anzahl an verketteten Transpositionen immer eine ungerade Anzahl an Fehlständen. Die Identität hat jedoch eine gerade Anzahl (nämlich 0), also kann die Identität nicht aus einer ungeraden Anzahl von Permutationen erzeugt werden.

□

Korollar 2.2.47. *Sei $n \in \mathbb{N}$ beliebig. Die Abbildung*

$$\mathrm{sgn} : S_n \to \{-1, 1\}, \pi \mapsto (-1)^{\#\ \text{Transpositionen in der Darstellung von } \pi \bmod 2}$$

ist ein Gruppenhomomorphismus.

Beweis. Zuerst bemerken wir, dass die Abbildung aufgrund von Proposition 2.2.46 wohldefiniert ist. Zeigen wir nun die Verträglichkeit mit den Operationen. Es gilt klarerweise $\operatorname{sgn}(\mathrm{id}) = 1$. Seien nun $\pi, \pi' \in S_n$. Betrachten wir den Fall, dass π und π' Darstellungen durch eine gerade Anzahl an Permutationen haben, dann hat auch $\pi \circ \pi'$ eine Darstellung durch eine gerade Anzahl an Permutationen und es gilt $\operatorname{sgn}(\pi)\operatorname{sgn}(\pi') = \operatorname{sgn}(\pi \circ \pi')$. Die anderen drei Fälle sind analog. Zuletzt sei noch $\pi \in G$, dann ist $1 = \operatorname{sgn}(\mathrm{id}) = \operatorname{sgn}(\pi \circ \pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1})$. Ist nun $\operatorname{sgn}(\pi) = 1$, so folgt $\operatorname{sgn}(\pi^{-1}) = 1 = \operatorname{sgn}(\pi)^{-1}$, der andere Fall ist analog. □

Bemerkung 2.2.48. Es ist die *alternierende Gruppe* $A_n := \ker \operatorname{sgn} \lhd S_n$ ein Normalteiler der symmetrischen Gruppe. Mit dem Homomorphiesatz erhält man, dass $S_n/A_n \cong \operatorname{ran} \operatorname{sgn} = (\{-1, 1\}, \cdot)$.

20.04.2023

26.04.2023

2.2.5 Abelsche Gruppen

Bemerkung 2.2.49. Sei $(G, \cdot, e, ^{-1})$ eine abelsche Gruppe, so ist G auch ein unitärer Modul über dem kommutativen 1-Ring $(\mathbb{Z}, +, 0, -, *, 1)$. Für $n \in \mathbb{Z}, g \in G$ definieren wir dazu $n \odot g := g^n$. Prüfen wir die Anforderungen an einen Modul. Seien $n, m \in \mathbb{Z}, g, h \in G$ beliebig. Dann ist

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

$$(n + m) \odot g = g^{n+m} = g^n \cdot g^m = (n \odot g) \cdot (m \odot g),$$
$$n \odot (g \cdot h) = (g \cdot h)^n = g^n \cdot h^n = (n \odot g) \cdot (n \odot h),$$
$$1 \odot g = g^1 = g$$

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

Es stellt sich die Frage ob G auch ein Modul über einem anderen Ringen ist. Falls es ein $m \in \mathbb{Z}$ gibt, sodass für alle $g \in G$ gilt $g^m = e$, so ist G ein unitärer Modul über $(\mathbb{Z}_m, +, 0, -, *, 1)$.

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

Definition 2.2.50. Der *Exponent* einer Gruppe G ist definiert als

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

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

Bemerkung 2.2.51. Ist G also eine abelsche Gruppe mit $\exp(G) = m < \infty$, so ist G ein unitärer $\mathbb{Z}_m$-Modul vermöge $k \odot g := g^k$ für $k \in \mathbb{Z}_m$.

Definition 2.2.52. Sei G eine Gruppe, $g \in G, p \in \mathbb{P}$, so nennen wir g ein *p-Element*, wenn es ein $k \in \mathbb{N}$ mit $\operatorname{ord}(g) = p^k$ gibt. Weiters definieren wir den *p-Anteil* von G als

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

Ist $G = G_p$, so nennen wir G eine *p-Gruppe*. Hier sei daran erinnert, dass g *Torsionselement* heißt, wenn es ein $k \in \mathbb{Z} \setminus \{0\}$ mit $g^k = e$ gibt. Wir definieren die *Torsionsgruppe von G*:

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

Lemma 2.2.53. *Sei G eine abelsche Gruppe und seien $a_1, \ldots, a_n \in G_t$, so gelten:*

1. $\operatorname{ord}(a_1 \cdot \ldots \cdot a_n) \mid \operatorname{ord}(a_1) \cdot \ldots \cdot \operatorname{ord}(a_n)$

2. $[\forall i,j \in \{1,\dots,n\}, i \neq j : \mathrm{ggT}(\mathrm{ord}(a_i),\mathrm{ord}(a_j)) = 1] \Rightarrow \mathrm{ord}(a_1 \cdot \ldots \cdot a_n) = \mathrm{ord}(a_1) \cdot \ldots \cdot \mathrm{ord}(a_n)$

3. $\exists a \in G : \mathrm{ord}(a) = \mathrm{kgV}(\mathrm{ord}(a_1),\dots,\mathrm{ord}(a_n))$

Beweis.

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

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

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

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

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

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

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

□

Korollar 2.2.54. *Sei G eine abelsche Gruppe mit $\exp(G) = m < \infty$. Dann gibt es ein $g \in G$ mit $\mathrm{ord}(g) = m$.*

Beweis. Für $h \in G$ beliebig, gilt $h^m = e$ und damit $\mathrm{ord}(h) \mid m$. Damit ist $M := \{\mathrm{ord}(h) \mid h \in G\}$ endlich, wir können also $M = \{\mathrm{ord}(h_1),\dots,\mathrm{ord}(h_n)\}$, mit $h_i \in G$, schreiben. Nach *Lemma* 2.2.53 gibt es nun ein $g \in G$ mit $\mathrm{ord}(g) = \mathrm{kgV}(\mathrm{ord}(h_1),\dots,\mathrm{ord}(h_n))$. Insgesamt folgt damit

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

die erste Ungleichung gilt wegen $h^{\mathrm{ord}(g)} = e$ für alle $h \in G$ und die zweite wegen $\exp(G) = m$ und $g \in G$. □

Lemma 2.2.55. *Sei G eine abelsche Gruppe und sei $p \in \mathbb{P}$. Dann gilt:*

1. $G_p \leq G$

2. $G_t \leq G$

Beweis.

1. Seien $a, b \in G_p$, so gibt es $u, v \in \mathbb{N}$ mit $\operatorname{ord}(a) = p^u, \operatorname{ord}(b) = p^v$ und es gilt nach Lemma 2.2.53 $\operatorname{ord}(a \cdot b) \mid \operatorname{ord}(a) \cdot \operatorname{ord}(b) = p^{u+v}$, also folgt $a \cdot b \in G_p$. Wegen $\operatorname{ord}(a^{-1}) = \operatorname{ord}(a)$ folgt auch $a^{-1} \in G_p$.
2. Seien $a, b \in G_t$ mit $\operatorname{ord}(a) = x, \operatorname{ord}(b) = y$, so gilt $\operatorname{ord}(a \cdot b) \mid x \cdot y$, also $a \cdot b \in G_t$.

□

Lemma 2.2.56. *Sei G eine abelsche Gruppe und seien $p, p_1, \dots, p_n \in \mathbb{P}$ paarweise verschieden, so ist*

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

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

Lemma 2.2.57. *Sei G eine abelsche Gruppe und sei $a \in G$ mit $\operatorname{ord}(a) = p_1^{e_1} \cdot \dots \cdot p_n^{e_n}$, wobei $p_1, \dots, p_n \in \mathbb{P}$ paarweise verschieden und $e_1, \dots, e_n \in \mathbb{N}_{\geq 1}$ sind. Dann ist $a \in G_{p_1} \cdot \dots \cdot G_{p_n}$.*

Beweis. Wir definieren

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

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

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

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

Betrachte nun

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

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

26.04.2023

27.04.2023

Satz 2.2.58. *Sei G eine abelsche Torsionsgruppe. Dann ist $G = \overset{w}{\prod}_{p \in \mathbb{P}} G_p$.*

Beweis. Wir müssen lediglich zeigen, dass für alle $p \in \mathbb{P}, G_p \lhd G$ gilt, dann folgt die Aussage aus den Lemmata 2.2.56 und 2.2.57 und Proposition 2.2.33. Seien also $p \in \mathbb{P}, g \in G$ beliebig, wir wollen $gG_pg^{-1} \subseteq G_p$ zeigen. Da der p-Anteil nach Lemma 2.2.55 eine Untergruppe ist und G abelsch ist, ist die Behauptung offensichtlich wahr. □

Lemma 2.2.59. *Sei $p \in \mathbb{P}$, G eine abelsche p-Gruppe $a \in G$ mit maximaler Ordnung, also $\operatorname{ord}(a) = \max\{\operatorname{ord}(g) \mid g \in G\} = p^n$ für ein $n \in \mathbb{N}$. Dann gilt:*

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

Beweis.

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

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

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

   Zunächst gilt für alle $V \leq G/_U, V \neq \{U\}$, dass $\langle aU\rangle \cap V \neq \{U\}$: Angenommen es wäre $\langle aU\rangle \cap V \neq \{U\}$. Wir definieren $U' := \{c \in G \mid \exists bU \in V : c \in bU\} \leq G$. Offensichtlich handelt sich dabei um eine echte Obermenge von U. Für $b \in \langle a\rangle \cap U'$ gilt $bU \in \langle aU\rangle \cap V$. Wegen der indirekten Annahme folgen $b \in U$, $b \in \langle a\rangle \cap U, b = e$ und schließlich $U' \cap \langle a\rangle = \{e\}$. Das ist ein Widerspruch, da U maximal mit dieser Eigenschaft gewählt wurde.

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

   Nun existiert für alle $b \in G$ ein $n \in \mathbb{N}$ mit $(aU)^n = bU$, also existieren $u_1, u_2 \in U$ mit $a^n u_1 = bu_2$, also $a^n u_1 u_2^{-1} = b$ und damit $G = \langle a\rangle \odot U$.

□

Satz 2.2.60. *Sei G eine endliche, abelsche Gruppe. Dann gibt es $p_1, \dots, p_n \in \mathbb{P}, e_1, \dots e_n \in \mathbb{N} \setminus \{0\}$ und $m_1, \dots, m_n \in \mathbb{N} \setminus \{0\}$, sodass für alle $i < j$ gilt $(p_i, e_i) <_{lex} (p_j, e_j)$, und*

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

Diese Darstellung ist eindeutig.

Beweis. Zuerst wollen wir die Existenz zeigen: Es existieren nach Satz 2.2.58 $p_1, \dots, p_\ell \in \mathbb{P}$ verschieden, sodass $G \cong G_{p_1} \times \ldots \times G_{p_\ell}$. Wir können also o. B. d. A. annehmen, dass G eine p-Gruppe ist ($p \in \mathbb{P}$).

Sei $a \in G$ mit maximaler Ordnung p^{e_n}, so wissen wir nach Lemma 2.2.59 $G \cong \langle a\rangle \times U$, wobei $\langle a\rangle \cong C_{p^{e_n}}$. Dies wird induktiv mit U wiederholt, wobei wir dies nur endlich oft machen müssen, da G endlich ist.

Zeigen wir nun noch die Eindeutigkeit: Sei

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

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

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

ist. Mit Induktion erhält man damit die Eindeutigkeit der Darstellung. □

27.04.2023
03.05.2023

2.3 Ringe

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

Beispiel 2.3.1. Ringe sind unter anderem

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

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

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

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

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

Bemerkung 2.3.4. Ein Ideal I eines Ringes R ist ein Unterring von R, da I nach Definition unter der Multiplikation abgeschlossen ist.

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

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

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

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

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

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

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

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

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

Letzerer Ausdruck ist jedoch gleich

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

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

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

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

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

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

Dabei ist

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

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

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

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

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

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

Bemerkung 2.3.13. Wir bemerken, dass gilt

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

Ist R sogar ein kommutativer Ring mit 1, so gilt

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

Beispiel 2.3.14. Es ist $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ein Hauptidealring, da alle Unterringe von der Form $m\mathbb{Z} = (m)$ sind.

Definition 2.3.15. Ein Ring R heißt *nullteilerfrei*, wenn

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

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

Beispiel 2.3.16. Ist R ein Körper, so ist R nullteilerfrei, da mit $0 \neq a \in R, b \in R$ gilt

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

Beispiel 2.3.17. Es ist $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ein Integritätsbereich, jedoch kein Körper.

Definition 2.3.18. Sei R ein Ring. Wir nennen $I \lhd R$ *Hauptideal*, wenn gilt

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

Weiters nennen wir R einen *Hauptidealring*, wenn R ein Integritätsbereich ist und

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

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

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

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

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

Proposition 2.3.20. *Sei R ein kommutativer Ring mit $1 \neq 0$, dann ist R ein Körper genau dann, wenn*

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

Beweis.

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

□

Korollar 2.3.21. *Seien K, L Körper und $\varphi : K \to L$ ein Körperhomomorphismus. Dann ist φ injektiv.*

Beweis. Es ist $\ker \varphi \lhd K$ ein Ideal mit $1 \notin \ker \varphi$. Da der Körper K nur die trivialen Ideale hat, folgt $\ker \varphi = \{0\}$ und φ ist injektiv. □

Definition 2.3.22. Sei $I \lhd R$. Wir nennen I

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

Beispiel 2.3.23. Sei $p \in \mathbb{P}$, so ist $p\mathbb{Z} \lhd \mathbb{Z}$ prim. Ist $m \in \mathbb{N}_{\geq 2} \setminus \mathbb{P}$, so ist $m\mathbb{Z}$ nicht prim.

Proposition 2.3.24. *Sei R ein kommutativer Ring mit 1 und $I \lhd R$. Dann gilt:*

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

Beweis.

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

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

2. Es gilt

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

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

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

$\square$

03.05.2023

04.05.2023

Beispiel 2.3.25. Betrachte den Ring $\mathbb{Z}$, $p \in \mathbb{P}$ und $p\mathbb{Z} \lhd \mathbb{Z}$, so erhalten wir $\mathbb{Z}/_{p\mathbb{Z}} = \mathbb{Z}_p$. $p\mathbb{Z}$ ist dabei ein Primideal und $\mathbb{Z}_p$ ein Körper.

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

Beispiel 2.3.26. Sei P die Menge der Polynomfunktionen auf $\mathbb{R}$ und $(x^2 + 1) \cdot P \lhd P$, so ist dies ein Primideal, und $P/_{(x^2+1)\cdot P}$ ein Integritätsbereich. Jedoch ist es kein Körper, da $(x^2 + 1) \cdot P$ nicht maximal ist – betrachte dazu beispielsweise

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

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

Definition 2.3.27. Wir definieren die *Charakteristik* eines Rings als

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

Beispiel 2.3.28. Für $m \in \mathbb{N}$ ist $\mathbb{Z}_m$ ein bekanntes Beispiel für einen Ring mit Charakteristik m. $(\mathbb{Z}_m)^{\mathbb{N}}$ ist beispielsweise ein unendlicher Ring mit Charakteristik m.

Proposition 2.3.29. *Sei R ein kommutativer Ring mit 1,* $\operatorname{char} R = p \in \mathbb{P}$ *und $k \in \mathbb{N}$. Dann ist*

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

ein Homomorphismus.

Beweis. Wir zeigen die Aussage mittels Induktion nach k.

Induktionsanfang ($k = 1$): Für $a, b \in R$ gilt

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

Wir beobachten

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

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

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

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

□

Bemerkung 2.3.30. Sei R ein kommutativer Ring mit 1, wir wollen R in einen Körper einbetten. Es gelte $0 \neq 1$ (da sonst für alle x gilt $x = 1 \cdot x = 0 \cdot x = 0$). Wir sammeln nun notwendige Voraussetzungen.

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

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

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

Dann ist

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

eine Einbettung von R als multiplikatives Monoid in M.

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

$$\forall x \in R^\times \exists y \in N : y\psi(x) = \psi(x)y = 1$$

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

Auf $(R \times R^\times)$ definieren wir nun eine Addition

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

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

Lemma 2.3.31. *Die in Bemerkung 2.3.30 definierte Äquivalenzrelation* $\sim \subset (R \times R^\times)^2$ *ist eine Kongruenzrelation bezüglich* $+$.

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

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

□

Satz 2.3.32. *Sei* R *ein Integritätsbereich mit* $1 \neq 0$ *und sei weiters* $\sim \subseteq (R \times R^\times)^2$ *wie in Bemerkung 2.3.30 definiert. Dann gilt:*

1. $K := (R \times R^\times)/_\sim$ *mit* $+, \cdot$ *aus Bemerkung 2.3.30 ist ein Körper.*
2. $\varphi : R \to K, x \mapsto [(x, 1)]_\sim$ *ist eine Einbettung.*
3. *Für alle Einbettungen* $\psi : R \to L$ *in einen Körper* L *gibt es eine Einbettung* $\bar{\psi} : K \to L$ *mit* $\bar{\psi} \circ \varphi = \psi$.

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

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

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

Das Distributivgesetz verifiziert man unmittelbar durch Nachrechnen.

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

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

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

□

Proposition 2.3.33. *Sei* K' *ein Körper mit Eigenschaft (3) aus Satz 2.3.32, so gilt bereits* $K' \cong K$, *wobei* K *unser konstruierter Körper aus Satz 2.3.32 (1) ist.*

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

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

Insbesondere gilt daher $\bar{\varphi} \circ \bar{\varphi_0} = \mathrm{id}_K$, da $(\bar{\varphi} \circ \bar{\varphi_0} \circ \varphi)(a) = (\bar{\varphi} \circ \varphi_0)(a) = \varphi(a)$ gilt. Damit ist $\bar{\varphi}$ ein Isomorphismus von K' nach K. □

Definition 2.3.34. Sei R ein kommutativer Ring mit $1 \neq 0$ und ein Integritätsbereich. Dann wird der Körper $(R \times R^\times)/_\sim$ aus Satz 2.3.32 *Quotientenkörper von* R genannt. Für $[(z,n)]_\sim$ schreibt man auch $\frac{z}{n}$.

Bemerkung 2.3.35. Die letzten beiden Theoreme liefern uns folgendes Ergebnis: Zu einem Integritätsbereich mit $1 \neq 0$, kann der Quotientenkörper konstruiert werden. Dieser ist (bis auf Isomorphie) eindeutig bestimmt und der kleinste Körper der R enthält.

Definition 2.3.36. Sei R ein Ring mit 1. Wir definieren den *Polynomring über* R

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

mit den Operationen

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

Elemente von $R[x]$ bezeichnen wir als *Polynome* und die einzelnen Folgenglieder der Elemente als *Koeffizienten*. Außerdem definieren wir für $(x_n)_{n\in\mathbb{N}} \in R[x]$ den *Grad*:

$$\deg((x_n)_{n\in\mathbb{N}}) := \begin{cases} -\infty, & (x_n)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}} \\ \max\{n \in \mathbb{N} : x_n \neq 0\}, & \text{sonst.} \end{cases}$$

Weiter definieren wir den Ring der *formalen Potenzreihen*

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

mit denselben Operation wie oben.

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

Bemerkung 2.3.37. Alternativ kann der Polynomring wie folgt definiert werden:

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

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

wobei $\sim$ die von Gesetzen der kommutativen Ringe mit 1 und in R erfüllten Gesetzen[5] erzeugte Äquivalenzrelation ist. In $R[x]$ gilt also beispielsweise

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

Vorteil von Definition 2.3.36 ist, dass analog auch die Verallgemeinerung der formalen Potenzreihen definiert werden kann, was mit diesem Ansatz nicht möglich ist.

Folgende Punkte sind einfach nachzurechnen:

Proposition 2.3.38. *Sei R ein kommutativer Ring mit 1. Dann gilt:*

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

04.05.2023

10.05.2023

Definition 2.3.39. Sei R ein Integritätsbereich mit $1 \neq 0$. Dann nennen wir den Quotientenkörper von $R[x]$

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

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

Bemerkung 2.3.40. Ist R ein Integritätsbereich mit $1 \neq 0$, so kann der Quotientenkörper K und dann von diesem der Polynomring $K[x]$ betrachten werden. Dieser besitzt nun einen Quotientenkörper $K(x)$. Andererseits kann man auch den Quotientenkörper des Polynomrings über R betrachten und erhält durch $R(x)$ einen dazu isomorphen Körper, also $K(x) \cong R(x)$.

Bemerkung 2.3.41. Als Verallgemeinerung des Polynomrings kann man auch den Polynomring in n Variablen $x_1, \ldots, x_n$ rekursiv definieren durch $R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$. Auch für eine beliebige Variablenmenge X kann eine Verallgemeinerung getroffen werden, indem man mit $R[x]$ die Terme über der Sprache $(+, 0, -, \cdot, 1, (x)_{x \in X}, (m_r)_{r \in R})$ nach den Ringgesetzen und Gleichheiten in R faktorisiert.

Definition 2.3.42. Sei K ein Körper. Dann heißt K *algebraisch abgeschlossen*, wenn

$$\forall p(x) \in K[x] : p(x) \notin {}^6 K \Rightarrow \exists a \in K : p(a)^7 = 0$$

gilt.

Satz 2.3.43 (Nullstellensatz von Hilbert, klein)**.** *Sei K ein algebraisch abgeschlossener Körper und $I \lhd K[x_1, \ldots, x_n]$ ein echtes Ideal. Dann gilt $\exists (a_1, \ldots, a_n) \in K^n : \forall p(x_1, \ldots, x_n) \in I : p(a_1, \ldots, a_n) = 0$.*

[5] Gemeint sind hierbei Gesetze wie beispielsweise $(2 \cdot 3)x = 6x$ im Ring $(\mathbb{Z}, +, 0, -, \cdot)$.
[6] Hier wird K mittels der Einbettung aus Proposition 2.3.38 als Teilmenge betrachtet.
[7] Der Ausdruck $p(a)$ wird mithilfe des Einsetzungshomomorphismus definiert.

Bemerkung 2.3.44. Satz 2.3.43 ist nicht Teil dieser Lehrveranstaltung, sondern soll nur einen Ausblick auf die Algebra 2 Vorlesung geben. Die Anforderung an ein echtes Ideal sind dabei sehr natürlich. Ein echtes Ideal kann nämlich keine Konstanten c enthalten, da sonst $c \in I \Rightarrow c^{-1}c \in I \Rightarrow I = K[x_1, \ldots, x_n]$ gilt. Ist außerdem F eine beliebige Menge von Polynomen mit einer gemeinsamen Nullstelle, so überzeugt man sich leicht davon, dass auch jedes Polynom aus dem erzeugten Ideal von F an dieser Stelle den Wert 0 annimmt. Daher kann o. B. d. A. angenommen werden, dass F sogar ein Ideal ist.

Proposition 2.3.45. *Sei R ein kommutativer Ring mit 1 und $X \neq \emptyset$ eine Variablenmenge. Dann gilt:*

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

Beweis. Der Beweis verläuft analog wie bei Satz 1.2.4. □

Definition 2.3.46. Sei R ein Ring und $I \lhd R$. Dann definieren wir für $r, s \in R$:

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

Wir sagen auch r *ist* s *modulo* I.

Satz 2.3.47 (Chinesischer Restsatz, allgemein)**.** *Seien R ein kommutativer Ring mit 1 und $I_1, \ldots, I_n \lhd R$ mit $\forall i \neq j \Rightarrow I_i + I_j = R$.*

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

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

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

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

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

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

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

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

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

Die Multiplikation zeigt man analog. $\square$

Aus dem obigen Satz folgt unmittelbar:

Korollar 2.3.48 (Chinesischer Restsatz, klassisch)**.** *Seien* $m_1,\dots,m_n \geq 2$ *und* $\forall i \neq j : m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ *oder äquivalent dazu* $ggT(m_i,m_j) = 1$*. Dann gilt*

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

Kapitel 3

Teilbarkeit

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

3.1 Grundlagen

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

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

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

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

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

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

Beweis.

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

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

$\square$

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

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

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

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

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

10.05.2023

11.05.2023

3.2 Faktorielle Ringe

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

$$\forall r \in R \setminus [1]_\sim, r \neq 0 : \exists r_1, \ldots, r_n \in R \text{ irreduzibel} : r = r_1 \cdot \ldots \cdot r_n,$$

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

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

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

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

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

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

Induktiv folgt dadurch die Eindeutigkeit.

Tatsächlich haben wir hier nicht verwendet, dass die q_i prim sind - wir haben also die stärkere Aussage gezeigt, dass es, sobald es eine Zerlegung in Primelemente gibt, es keine andere Zerlegung in irreduzible Elemente, bis auf die Reihenfolge und Assoziiertheit der Faktoren, gibt.

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

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

Beweis.

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

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

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

wobei alle auftretenden Faktoren irreduzibel sind. Nach (1) gibt es nun noch i mit $r \sim a_i$ oder j mit $r \sim b_j$, womit $r \mid a$ oder $r \mid b$ folgt und r prim ist.

(3) ⇒ (1): Folgt aus Bemerkung 3.2.2.

(3) ⇒ (2): Trivial.

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

□

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

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

Nun gilt

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

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

Für den Beweis von Proposition 3.2.7 werden die folgenden Definitionen sowie Lemma 3.2.6 benötigt.

Definition 3.2.5. Ein *ungerichteter Graph* (oder auch nur *Graph*) ist ein Paar (V, E) bestehend aus einer Menge V und einer beliebigen Menge $E \subseteq \{\{x, y\} \mid x, y \in V\}$. Die Elemente von V heißen *Knoten*, die Elemente von E *Kanten*. Zwei Elemente $x, y \in V$ heißen *benachbart*, wenn $\{x, y\} \in E$. Ein *Pfad* ist eine endliche Folge paarweise verschiedener Knoten $v_1, \ldots, v_n \in V$ mit $\{v_i, v_{i+1}\} \in E$ für alle $i \in \{1, \ldots, n-1\}$. Ein *Zyklus* ist ein Pfad $v_1, \ldots, v_n$ mit $v_1 = v_n$, wobei $n \geq 3$ gilt. Besitzt ein Graph keinen Zyklus, so nennen wir den Graphen *zyklenfrei*. Ein Graph heißt *zusammenhängend*, wenn es für je zwei verschiedene Elemente $x, y \in V$ einen Pfad gibt, welcher x mit y verbindet. Ein *Baum* ist ein zusammenhängender, zyklenfreier, ungerichteter Graph. Für einen Knoten $v \in V$ ist der Grad von v definiert als $|\{u \in V : \{u, v\} \in E\}|$.

Lemma 3.2.6 (Königs Lemma)**.** *Sei $G = (V, E)$ ein Baum bestehend aus unendlich vielen Knoten und jeder Knoten habe endlichen Grad. Dann besitzt G einen unendlichen Pfad.*

Beweis. Sei $v_1 \in V$ beliebig. Mit $v_1^{(1)}, \ldots, v_1^{(n_1)}$ bezeichnen wir die benachbarten Element von v_1. Für jedes Element $w \in V \setminus \{v_1\}$ gibt es nun einen Pfad Γ_w, welcher in v_1 beginnt und in w endet. Jeder dieser Pfade verbindet v_1 mit einem seiner benachbarten Elemente. Wegen

$$\{w \in V \setminus \{v_1\}\} = \bigcup_{j=1}^{n_1} \{w \in V \mid \{v_1, v_1^{(j)}\} \in \Gamma_w\}$$

und der Unendlichkeit von V muss es ein $j \in \{1, \dots, n_1\}$ geben, sodass $\{w \in V \mid \{v_1, v_1^{(j)}\} \in \Gamma_w\}$ unendlich ist. Wir definieren $v_2 := v_1^{(j)}$. Induktiv finden wir so eine unendliche Folge, sodass für jedes $k \in \mathbb{N}$ die Menge $\{w \in V \mid \forall i \le k : \{v_i, v_{i+1}\} \in \Gamma_w\}$ unendlich ist: Sind $v_1, \dots, v_k$ bereits gewählt, so bezeichnen wir mit $v_k^{(1)}, \dots, v_k^{(n_k)}$ die benachbarten Elemente von v_k ohne v_{k-1}. Wegen

$$\{w \in V \mid \forall i \le k-1 : \{v_i, v_{i+1}\} \in \Gamma_w\} = \bigcup_{j=1}^{n_k} \{w \in V \mid \{v_i, v_{i+1}\} \in \Gamma_w \land \{v_k, v_k^{(j)}\} \in \Gamma_w\}$$

und der Unendlichkeit der linken Menge muss es ein $j \in \{1, \dots, n_k\}$ geben, sodass auch $\{w \in V \mid \{v_i, v_{i+1}\} \in \Gamma_w \land \{v_k, v_k^{(j)}\} \in \Gamma_w\}$ unendlich ist. Dann definieren wir $v_{k+1} := v_k^{(j)}$. Mit Hilfe des Auswahlaxioms ist daher die Wahl einer solchen Folge $v_1, v_2, \dots$ möglich. Diese Folge bildet offensichtlich einen unendlichen Pfad. □

Proposition 3.2.7. *Jeder Hauptidealring ist ein faktorieller Ring.*

Beweis. Sei $r \in R$ irreduzibel, wir zeigen, dass r prim ist. Wir bemerken, dass $(r) \lhd R$ echt ist, womit es nach Proposition 2.3.24 ein maximales Ideal I gibt mit $(r) \subseteq I \lhd R$. Da R ein Hauptidealring ist gibt es ein $c \in R$ mit $I = (c)$. c ist prim, da I maximal und nach Proposition 2.3.24 damit prim ist. Nun gilt $r \in (c)$, womit $c \mid r$ folgt. Da r irreduzibel und $c \not\sim 1$ ist, folgt $r \mid c$, also folgt $r \sim c$ und damit, dass r prim ist.

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

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

Sei T der Baum der $r_{i_1 \dots i_n}$. Ist T endlich, so haben wir eine gewünschte Zerlegung gefunden. Sei indirekt angenommen T wäre unendlich, es gibt also einen unendlichen Pfad (siehe Lemma 3.2.6) – o. B. d. A. betrachten wir den Pfad $r_0, r_{00}, r_{000}, \dots$. Nun gilt

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

Sei indirekt angenommen $r \sim r_0$, so gibt es ein x mit $r_0 = r \cdot x = r_0 \cdot r_1 \cdot x$, also folgt $1 = r_1 \cdot x$, also $r_1 \sim 1$, im Widerspruch. Offensichtlich gilt diese Argumentation für alle Elemente des Astes. Die obige Schachtelung ist also sogar echt, wir haben eine echt aufsteigende Kette von Idealen. Setze

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

Nun gibt es ein c mit $I = (c)$, womit es ein $i \in \mathbb{N}$ mit $c \in (r_{\underbrace{0 \dots 0}_{i-\text{mal}}})$ gint. Also folgt $c \sim r_{0 \dots 0}$ und weiters $I = (r_{0 \dots 0})$, im Widerspruch dazu, dass diese Kette echt aufsteigend war. □

Beispiel 3.2.8. Betrachte $\mathbb{Z}[x]$. Sei $a \in \mathbb{Z}, a \not\sim 1, a \neq 0$. Betrachte $(\{a, x\}) \lhd \mathbb{Z}[x]$, welches zwar echt, aber kein Hauptideal ist. Wäre nämlich $(\{a, x\}) = (b)$, so würde wegen $a \in (b)$ direkt $\deg b = 0$ folgen. Wegen $x \in (b)$ folgt dadurch $b \sim 1$, im Widerspruch.

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

Definition 3.2.9. Sei R ein kommutativer Ring mit 1, $A \subseteq R$ und $d \in R$. Dann ist d ein *größter gemeinsamer Teiler* von A (wir schreiben auch $d = \mathrm{ggT}(A)$, obwohl diese Gleichheit formal nicht korrekt ist, da der größte gemeinsame Teiler nicht eindeutig sein muss), wenn

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

Im Fall der Existenz ist der größte gemeinsame Teiler eindeutig bis auf Assoziiertheit.

Entsprechend kann man auch das *kleinste gemeinsame Vielfache* einer Menge A definieren (wir schreiben analog $v = \mathrm{kgV}(A)$, wobei diese Gleichheit mit derselben Begründung nicht formal korrekt ist).

Bemerkung 3.2.10. Ist R ein faktorieller Ring, so gibt es zu je zwei Elementen $a, b \in R$ stets einen größten gemeinsamen Teiler: Falls eines der beiden Elemente 0 ist, so ist das andere Element der größte gemeinsame Teiler. Ist eines der beiden Elemente zur 1 assoziiert, so ist 1 der größte gemeinsame Teiler. Andernfalls können wir zwei Primfaktorzerlegungen $a = a_1 \cdot \ldots \cdot a_u$, $b = b_1 \cdot \ldots \cdot b_v$ finden. Durch Umnummerierung können wir $r \in \mathbb{N}, 0 \leq r \leq \min\{u, v\}$ mit

$$a_i \sim b_i \text{ für } i \leq r \quad \text{und} \quad a_i \not\sim b_j \text{ für } i, j > r$$

wählen. Die Behauptung lautet: $d := \prod_{i=1}^{r} a_i = \mathrm{ggT}(\{a, b\})$. Offensichtlich teilt d sowohl a als auch b. Sei t ein weiterer gemeinsamer Teiler von a und b. Findet man nun eine Primfaktorzerlegung $t_1, \ldots, t_w$ von t, so erhält man, dass es $i \leq u$ und $j \leq v$ mit $a_i \sim t_1 \sim b_j$ geben muss. Wegen der Wahl von r muss $i \leq r$ oder $j \leq r$ gelten und wieder wegen der Wahl von r kann man sogar $i = j \leq r$ verlangen, o. B. d. A. $t_1 \sim a_1 \sim b_1$. Mit Hilfe von Division der Elemente a, b und t durch a_1, b_1 beziehungsweise t_1 zeigt: Die analoge Argumentation gilt für $k \in \{2, \ldots, w\}$, das heißt die Elemente können so umnummeriert werden, dass $t_k \sim a_k \sim b_k$ für alle $k \in \{1, \ldots, w\}$ gilt. Wieder wegen der Wahl von r folgt schließlich $w \leq r$, also $t \mid d$.

11.05.2023

17.05.2023

Bemerkung 3.2.11. Sei R ein Integritätsbereich und seien $a, b \in R$. Dann gilt die Äquivalenz $a \mid b \Leftrightarrow (b) \subseteq (a)$. Es ist daher die Struktur $(R/_\sim, |)$ ordnungstheoretisch isomorph zu der Menge aller Hauptideale mit Mengeninklusion, vermöge der Abbildung $\psi([a]_\sim) := (a)$. Dabei ist $\sim$ die Assoziiertheitsrelation. Im Fall eines Hauptidealrings kann „Menge der Hauptideale" offensichtlich mit „Menge der Ideale" ersetzt werden. Für $A \subseteq R$ ist $\inf_|(A) = \mathrm{ggT}(A)$ und $\sup_|(A) = \mathrm{kgV}(A)$. Aufgrund dieser Tatsachen folgt nun, dass es in einem Hauptidealring R zu $A \subseteq R$ eine zugehörige Menge von Idealen $A' = \psi(A)$ gibt. Da R ein Hauptidealring ist, existiert ein $d \in R$ mit $(A) = (d)$ und es folgt

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

Lemma 3.2.12 (Lemma von Bézout)**.** *Sei R ein Hauptidealring und $A \subseteq R$. Dann existieren $n \in \mathbb{N}$, $a_1, \ldots, a_n \in A$ und $r_1, \ldots, r_n \in R$, sodass $\mathrm{ggT}(A) = \sum_{i=1}^{n} r_i a_i$.*

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

Beispiel 3.2.13. Ein Beispiel in $R = \mathbb{Z}$ ist $\mathrm{ggT}(5, 3) = 1 = (-1) \cdot 5 + 2 \cdot 3$.

3.3 Teilen mit Rest

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

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

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

gibt. Die Funktion H heißt *euklidische Bewertung*.

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

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

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

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

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

Satz 3.3.6 (Euklidischer Algorithmus)**.** *Seien $a, b \in R, a \neq 0$. Wähle $q_1, r_1 \in R : b = aq_1 + r_1$ mit $r_1 = 0 \vee H(r_1) < H(a)$. Wenn $r_1 = 0$ ist, dann terminiert der Algorithmus. Ansonsten wählt man $q_2, r_2 \in R$ mit $a = r_1 q_2 + r_2$ und $r_2 = 0 \vee H(r_2) < H(r_1)$. Falls $r_2 = 0$ ist, so terminiert der Algorithmus, ansonsten verfahren wir induktiv. Wenn r_i, r_{i+1} und q_{i+1} bereits gewählt sind, dann wählt man q_{i+2}, r_{i+2} mit $r_i = r_{i+1} q_{i+2} + r_{i+2}$ mit $r_{i+2} = 0 \vee H(r_{i+2}) < H(r_{i+1})$. Aufgrund der Schachtelung $H(a) > H(r_1) > H(r_2) > \ldots$ terminiert der Algorithmus, das heißt es ist $r_k = 0$ für ein $k \in \mathbb{N}$. Dann ist r_{k-1} der letzte von 0 verschiedene Rest und es gilt $r_{k-1} = \mathrm{ggT}(a, b)$.*

Beweis. Zunächst wird gezeigt, dass r_{k-1} ein Teiler von a und b ist. Das folgt induktiv, da $r_{k-1} \mid r_{k-2}$ (wegen $r_k = 0$) und $r_{k-1} \mid r_{k-2} q_{k-1} + r_{k-1} = r_{k-3}$. Mit Induktion folgt, dass $r_{k-1} \mid a$ und $r_{k-1} \mid b$ gilt.

Ist nun t ein beliebiger Teiler von a und b, so müssen wir zeigen, dass $t \mid r_{k-1}$ gilt. Diese Aussage folgt ähnlich da $t \mid b - aq_1 = r_1$ und man wieder mit Induktion $t \mid r_{k-1}$ leicht folgert. Daher folgt, dass $r_{k-1} = \mathrm{ggT}(a, b)$ gilt. □

Bemerkung 3.3.7. Eine Anwendung des euklidischen Algorithmus ist die Berechnung von Koeffizienten x, y mit $ax + by = \mathrm{ggT}(a, b)$. Mit der Notation aus Satz 3.3.6 folgt

$$\begin{aligned}\mathrm{ggT}(a, b) &= r_{k-1} \\ &= r_{k-3} - r_{k-2}q_{k-1} \\ &= r_{k-3} - (r_{k-4} - r_{k-3}q_{k-2})q_{k-1} \\ &= r_{k-4}(-q_{k-1}) + r_{k-3}(1 + q_{k-2}q_{k-1}) \\ &= \ldots = ax + by.\end{aligned}$$

Die Koeffizienten x, y sind klarerweise nicht eindeutig, so ist in $\mathbb{Z}$ beispielsweise $1 = \mathrm{ggT}(5, 3) = 5(-1) + 3 \cdot 2 = 5 \cdot 2 + 3(-3)$.

Bemerkung 3.3.8. Wir wollen an dieser Stelle noch einen kurzen Überblick über die verschiedenen Arten von Ringen geben und vor allem auch auf die Unterschiede über darin gültigen Aussagen eingehen.

In Faktoriellen Ringen gibt es zu $a, b \in R$ einen größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$.

In einem Hauptidealring gibt es nicht nur den größten gemeinsamen Teiler, sondern dieser kann auch als Linearkombination dargestellt werden, das heißt für $a, b \in R$ existieren $x, y \in R$ mit $\mathrm{ggT}(a, b) = ax + by$.

In einem euklidischen Ring gibt es den ggT, dieser kann linearkombiniert werden und mithilfe des euklidischen Algorithmus können Faktoren berechnet werden.

Proposition 3.3.9. *Sei R ein faktorieller Ring, K der Quotientenkörper und $\frac{p}{q} \in K$. Dann gibt es $p', q' \in R, q' \neq 0$ sodass $\frac{p}{q} = \frac{p'}{q'}$ und $\mathrm{ggT}(p', q') = 1$. Wenn $\frac{p''}{q''} = \frac{p}{q}$ mit $\mathrm{ggT}(p'', q'') = 1$, dann gilt $p'' \sim p'$ und $q'' \sim q'$.*

Beweis. Mit $p' := \frac{p}{\mathrm{ggT}(p,q)}$ und $q' := \frac{q}{\mathrm{ggT}(p,q)}$ folgt die Existenz, wobei $\frac{p'}{q'} = \frac{p}{q}$ nach Definition gilt und man $(\mathrm{ggT})(p, q) = 1$ über die Primfaktorenzerlegung nachweist. Ist $\frac{p''}{q''}$ ebenfalls eine solche Darstellung von $\frac{p}{q}$, so überzeugt man sich von $p' \sim p''$ und $q' \sim q''$ ebenfalls mithilfe der Primfaktorenzerlegung in R. $\square$

Bemerkung 3.3.10. Die folgenden beiden Lemmata waren nicht Teil der Vorlesung und wurden nachträglich ergänzt. Sie können beispielsweise für den Beweis von Satz 4.2.52 (Satz vom primitiven Element) verwendet werden.

Lemma 3.3.11. *Sei R ein euklidischer Ring. Dann existiert eine euklidische Bewertung $H' : R \setminus \{0\} \to \mathbb{N}$ mit $\forall a, b \in R \setminus \{0\} : H'(ab) \geq H'(a)$.*

Beweis. Sei H eine euklidische Bewertung auf R und definiere $H'(a) := \min_{x \in R \setminus \{0\}} H(ax)$ für $a \in R \setminus \{0\}$. Seien nun $a, b \in R, b \neq 0$ beliebig. Dann existieren $q, r \in R$ mit $b = aq + r$ und $r = 0$ oder $H(r) < H(a)$. Nun gilt nach Definition $H'(a) = H(ax)$ für ein $x \in R \setminus \{0\}$. Wieder existieren q', r' mit $b = (ax)q' + r'$, wobei $r' = 0$ oder $H(r') < H(ax)$ gilt. Insgesamt folgt also $b = a(xq') + r'$ mit $r' = 0$ oder $H'(r') \leq H(r') < H(ax) = H'(a)$, also ist H' eine euklidische Bewertung. Die Ungleichung $H'(a) \leq H'(ab)$ gilt offensichtlich, da wegen $bR \setminus \{0\} \subseteq R \setminus \{0\}$ das Minimum auf der rechten Seite der Ungleichung über eine kleinere Menge gebildet wird. $\square$

Lemma 3.3.12. *Sei R ein euklidischer Ring, $x, y \in R$, $(\{x, y\}) =: I$ und $d \in I \setminus \{0\}$. Sei weiters H eine euklidische Bewertung mit $H(ab) \geq H(a)$ für alle $a, b \in R \setminus \{0\}$. Dann gilt: d ist genau dann ein ggT von x und y, wenn $H(d) = \min\{H(z) : z \in I \setminus \{0\}\}$ gilt.*

Beweis. Sei d ein ggT von x, y und sei $z \in I \setminus \{0\}$ beliebig. Da d jede Linearkombination von x und y teilt, gilt $d \mid z$, das heißt es existiert ein c mit $z = cd$. Laut Voraussetzung gilt nun $H(z) = H(cd) \geq H(d)$. Da $d \in I \setminus \{0\}$ nach dem Lemma von Bezout erfüllt ist, folgt dass H bei d auf $I \setminus \{0\}$ das Minimum annimmt.

Sei nun $d \in I \setminus \{0\}$ mit $H(d) = \min\{H(I \setminus \{0\})\}$. Es ist zu zeigen, dass d ein Teiler von einem beliebigen ggT ist, da diese dann assoziiert sind, also auch d ein ggT von x und y ist. Sei daher d' ein ggT von x, y. Aufgrund von Bemerkung 2.3.13 existieren $a, b \in R$ mit $d = ax + by$. Nach dem Lemma von Bezout existieren $a', b' \in R$ mit $d' = a'x + b'y$. Die Division mit Rest von d' durch d liefert die Existenz von $q, r \in R$ mit $d' = qd + r$ und $r = 0$ oder $H(r) < H(d)$. Im Fall $r = 0$ sind wir fertig, daher zeigen wir dass der andere Fall nicht eintreten kann. Es gilt $r = d' - qd = (a'x + b'y) - q(ax + by) = (a' - qa)x + (b' - qb)y \in I$ und wegen der Minimalität von $H(d)$ muss $r = 0$ gelten. $\square$

17.05.2023

24.05.2023

3.4 Der Satz von Gauß

Satz 3.4.1 (Satz von Gauß)**.** *Ist R ein faktorieller Ring, so ist auch $R[x]$ faktoriell.*

Korollar 3.4.2. *Sei R ein faktorieller Ring. Dann gilt:*

- *Der Polynomring $R[x_1, \ldots, x_n]$ ist faktoriell.*
- *Ist X eine beliebige Menge, so ist auch $R[X]$ faktoriell.*

Korollar 3.4.3. *$\mathbb{Z}[x]$ ist faktoriell.*

Definition 3.4.4. Ist R ein Ring und $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit $a_0, \ldots, a_n \in R$, so nennen wir f *leer* (oder auch *primitiv*), wenn

$$\operatorname{ggT}(a_0, \ldots, a_n) = 1.$$

Bemerkung 3.4.5. Ist R ein faktorieller Ring, so existiert für alle $f \in R[x]$ eine Darstellung

$$f = \operatorname{ggT}(a_0, \ldots, a_n) \cdot f_0,$$

wobei $f_0 \in R[x]$ leer ist.

Lemma 3.4.6. *Sei R ein faktorieller Ring, $f, g \in R[x]$, $p \in R$ prim. Dann gilt*

$$p \mid fg \Rightarrow p \mid f \vee p \mid g.$$

Beweis. Wir zeigen die Aussage mittels Induktion nach $\deg fg = n + m$, wobei

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j \quad \text{mit } a_0, \ldots, a_n, b_0, \ldots, b_m \in R.$$

Induktionsanfang ($n + m = 0$): Es sind $f, g \in R$, womit aus $p \mid fg$ folgt $p \mid f \vee p \mid g$, da p prim in R ist.

Induktionsschritt ($n+m \to n+m+1$): Gilt $p \mid fg$, so gilt $p \mid a_n b_m$, da $a_n b_m$ der Leitkoeffizient ist und damit, da p prim in R ist, $p \mid a_n \vee p \mid b_m$. Nehmen wir o. B. d. A. $p \mid a_n$ an. Schreiben wir nun $f = a_n x^n + f'$. Es gilt

$$fg = a_n x^n g + f'g.$$

Nun teilt p jedoch fg, a_n und damit auch $f'g$. Nach Induktionsvoraussetzung gilt damit $p \mid f' \vee p \mid g$, und damit entweder direkt die Behauptung oder $p \mid a_n, p \mid f'$ und damit $p \mid f$. □

Korollar 3.4.7. *Sei R ein faktorieller Ring, $f, g \in R[x]$ leer, so ist auch fg leer.*

Lemma 3.4.8. *Sei R ein faktorieller Ring, Q der Quotientenkörper von R und $f \in Q[x]$. Dann existieren $c_f \in Q, f_0 \in R[x]$ leer, mit*

$$f = c_f \cdot f_0.$$

Diese Darstellung ist eindeutig bis auf Multiplikation mit einer Einheit (aus R).

Weiters gibt es zu $f, g \in Q[x]$ eine Einheit $e \in R$ mit

$$c_{f \cdot g} = e \cdot c_f \cdot c_g.$$

Beweis. Die Koeffizienten a_i von f in Q haben eine Darstellung als Quotient mit teilerfremden Elementen z_i, n_i aus dem Ring, also $a_i = \frac{z_i}{n_i}$, wir können also schreiben

$$f = \sum_{i=0}^{\ell} a_i x^i = \sum_{i=0}^{\ell} \frac{z_i}{n_i} x^i = \frac{\operatorname{ggT}(z_0, \ldots, z_n)}{\operatorname{kgV}(n_0, \ldots, n_\ell)} \sum_{i=0}^{\ell} b_i x^i,$$

wobei die $b_i \in R$ teilerfremd sind und sich somit sofort die geforderte Darstellung ergibt.

Seien nun $f = d \cdot g$ eine weitere Darstellung von f, wobei $g = \sum_{i=0}^{\ell} t_i x^i \in R[x]$ leer ist. Durch Koeffizientenvergleich folgt, dass für alle i gilt $c_f \cdot b_i = d \cdot t_i$. Schreiben wir $c_f = \frac{c_f^z}{c_f^n}, d = \frac{d^z}{d^n}$, so gilt $c_f^z b_i d^n = d^z t_i c_f^n$. Offensichtlich stimmen dann $\operatorname{ggT}(\{c_f^z b_i d^n \mid i = 1, \ldots, \ell\})$ und $\operatorname{ggT}(\{d^z t_i c_f^n \mid i = 1, \ldots, \ell\})$ überein. Man sieht leicht ein, dass $c_f^z d^n$ ein ggT von $\{c_f^z b_i d^n \mid i = 1, \ldots, \ell\}$ und $d^z c_f^n$ ein ggT von $\{c_f^z b_i d^n \mid i = 1, \ldots, \ell\}$ ist. Aufgrund der Eindeutigkeit des ggT (bis auf Assoziiertheit) folgt $c_f^z d^n \sim d^z c_f^n$ und damit die Existenz einer Einheit e mit $e \cdot c_f = d$.

Sind nun $f = c_f \cdot f_0, g = c_g \cdot g_0$, so folgt

$$f \cdot g = (c_f \cdot c_g) \cdot (f_0 \cdot g_0)$$

und damit sofort die Aussage. □

Lemma 3.4.9. *Sei R ein faktorieller Ring und Q der Quotientenkörper von R. Sei $f \in R[x]$ irreduzibel in $R[x]$, $\deg f \geq 1$, so ist f irreduzibel in $Q[x]$.*

Beweis. Sei $f = g \cdot h$, $g, h \in Q[x]$. Gilt $\deg g = 0 \vee \deg h = 0$, so folgt sofort die Assoziiertheit von g oder h zu 1 in $Q[x]$. Sind $\deg g, \deg h \geq 1$, so schreibe mit obigem Lemma $g = c_g \cdot g_0, h = c_h \cdot h_0$. Wir nehmen o. B. d. A. $c_f = c_g \cdot c_h$ an. f ist irreduzibel in $R[x]$, insbesondere ist f also leer. Wir können somit o. B. d. A. $c_f = 1$ annehmen. Damit ist also

$$f = g \cdot h = c_g \cdot g_0 \cdot c_h \cdot h_0 = g_0 \cdot h_0,$$

im Widerspruch dazu, dass f irreduzibel in $R[x]$ ist. □

Lemma 3.4.10. *Sei R ein faktorieller Ring. Ist $f \in R[x]$ irreduzibel, so ist f prim.*

Beweis. Seien $g, h \in R[x], f \mid g \cdot h$. Wir wollen $f \mid g \vee f \mid h$ zeigen. Da R faktoriell ist, können wir aus Gradgründen o. B. d. A. $\deg f \geq 1$ annehmen. Nach Lemma 3.4.9 ist f dann irreduzibel in $Q[x]$. Da $Q[x]$ als euklidischer Ring insbesondere ein faktorieller Ring ist, gilt nach Proposition 3.2.3, dass f in $Q[x]$ prim ist, also $f \mid g \vee f \mid h$ in $Q[x]$, o. B. d. A. sei $p \in Q[x]$ mit $f \cdot p = g$. Nun können wir also

$$f \cdot c_p \cdot p_0 = g = c_g \cdot g_0$$

schreiben, also $c_p \cdot (f \cdot p_0) = c_g \cdot g_0$. Da f irreduzibel ist, is $f \cdot p_0$ leer. Aufgrund der Eindeutigkeit dieser Darstellung gibt es eine Einheit $e \in R$ mit $c_p = e \cdot c_g$. Damit ist jedoch auch $c_p \in R$, womit $p \in R[x]$ folgt. Damit gilt $f \mid g$ in $R[x]$. □

Beweis (Satz von Gauß). Sei $f \in R[x]$, dann existieren $c_f^1, \ldots, c_f^n \in R$ prim und $f_0^1, \ldots, f_0^\ell \in R[x]$ irreduzibel mit

$$f = c_f \cdot f_0 = c_f^1 \cdot \ldots \cdot c_f^n \cdot f_0^1 \cdot \ldots \cdot f_0^\ell.$$

Die Zerlegung von c_f in Primelemente existiert, da R faktoriell ist und c_f^i prim in $R[x]$ ist, nach obigem Lemma. Die Existenz der Zerlegung von f_0 in irreduzible Polynome argumentiert man mit Hilfe des Grades, wobei die f_0^j prim nach obigem Lemma sind. □

Kapitel 4

Körper

Das Ziel dieses Kapitels ist es die Konzepte, beziehungsweise das Verhalten, von Körpererweiterungen zu verstehen, beispielsweise von $\mathbb{R}$ auf $\mathbb{C}$, oder von $\mathbb{Q}$ auf $\mathbb{R}$. Weiters soll versucht werden alle endlichen Körper vollständig zu klassifizieren. Die Inhalte können auch in Goldstern et al.: *Algebra – Eine grundlagenorientierte Einführungsvorlesung* in dem Kapitel *6. Körper* gefunden werden.

4.1 Einführung

Definition 4.1.1. Sei L ein Körper. Wir nennen $K \subseteq L$ einen *Unterköper*, wenn $1 \in K$ und K mit den von L auf K eingeschränkten Operationen ein Körper ist. Dafür schreiben wir auch $K \leq L$. In diesem Kontext heißt L auch *Oberkörper* von K.

Durch

$$\bigcap\{U \leq L \mid U \text{ Unterkörper von } L\}$$

ist ein Unterkörper von L gegeben, welchen wir den *Primkörper* von L nennen.

Sei $K \leq L, S \subseteq L$ so definieren wir die *Körpererweiterung von K um S* durch

$$K(S) := \bigcap\{U \mid K \leq U \leq L, U \supseteq S\}.$$

Ist $S = \{\alpha_1, \dots, \alpha_n\}$, so schreiben wir auch $K(\alpha_1, \dots, \alpha_n)$.

Analog ist die *Ringerweiterung von K um S* definiert:

$$K[S] := \bigcap\{U \mid U \text{ Ring} \wedge K \subseteq U \subseteq L, U \supseteq S\}.$$

Ist $S = \{\alpha_1, \dots, \alpha_n\}$, so schreiben wir auch $K[\alpha_1, \dots, \alpha_n]$.

Bemerkung 4.1.2. Beispielsweise gilt $\mathbb{R}(i) = \mathbb{C}$, wie wir später noch sehen werden.

Bemerkung 4.1.3. Sei K ein Körper, dann ist K ein Unterkörper des Quotientenkörpers Q von $K[x]$. Also ist $K \leq Q$ eine Körpererweiterung.

Definition 4.1.4. Ein Körper K heißt *Primkörper*, wenn K keine echten Unterkörper hat.

Bemerkung 4.1.5. Sei L ein Körper und K der Primkörper von L. Dann ist K ein Primkörper.

Satz 4.1.6. *Sei K ein Primkörper.*

- *Ist* $\operatorname{char} K = 0$*, so ist* $K \cong \mathbb{Q}$.
- *Ist* $\operatorname{char} K = p \in \mathbb{P}$*, so ist* $K \cong \mathbb{Z}_p$.

Beweis. Wir weisen zunächst die erste Behauptung nach. Sei K ein Körper mit Charakteristik 0. Dann definieren wir eine Abbildung $\varphi : \mathbb{Q} \to K$ durch $\varphi(\pm\frac{a}{b}) = \pm\frac{\overbrace{1+\ldots+1}^{a}}{\underbrace{1+\ldots+1}_{b}}$, mit $a \in \mathbb{N}$, $b \in \mathbb{N}\setminus\{0\}$. Diese Abbildung ist wohldefiniert, da der Nenner laut Voraussetzung niemals 0 wird und sie unabhängig von der Wahl der Repräsentanten ist (kürzbare Ausdrücke in $\mathbb{Q}$ sind auch in K kürzbar). Wie man leicht sieht, ist die Abbildung ein Homomorphismus. Und φ ist außerdem injektiv, denn gilt $\varphi(\frac{a}{b}) = 0$, so folgt sofort $\frac{a}{b} = 0$, da wir $\text{char}(K) = 0$ vorausgesetzt haben. Da $\varphi(\mathbb{Q})$ einen Unterkörper von K darstellt und K aber ein Primkörper ist, folgt die Surjektivität von φ, also $K \cong \mathbb{Q}$.

Der Beweis, dass $K \cong \mathbb{Z}_p$ für $\text{char}(K) = p$ gilt, verläuft ähnlich. Dieses Mal definieren wir $\varphi : \mathbb{Z}_p \to K$ durch $\varphi(i) := \overbrace{1+\ldots+1}^{i}$. Zunächst zeigen wir dieses Mal, dass φ ein Homomorphismus ist: Für die Addition müssen zwei Fälle unterschieden werden: Falls $i + j < p$ gilt, so folgt klarerweise die Verträglichkeit. Ansonsten gilt $i + j = k + p$ mit $0 \leq k < p$ und wir folgern $\varphi(i+j) = \varphi(k) = \overbrace{1+\ldots+1}^{k} = \overbrace{1+\ldots+1}^{k+p} = \overbrace{1+\ldots+1}^{i} + \overbrace{1+\ldots+1}^{j} = \varphi(i) + \varphi(j)$, wobei wir verwendet haben, dass K Charakteristik p hat. Die Verträglichkeit mit der Multiplikation zeigt man ähnlich und die Homomorphiebedingung für die neutralen Elemente gilt definitionsgemäß. Die Abbildung φ ist außerdem injektiv, denn aus $\varphi(i) = 0$ folgt klarerweise $i = 0$. Damit ist $\varphi(\mathbb{Z}_p)$ ein Unterkörper von K und da K ein Primkörper ist, folgt wieder die Surjektivität, also $K \cong \mathbb{Z}_p$.

□

4.2 Körpererweiterungen

Im Folgenden werden wir oft $K \leq L$ schreiben, dabei ist stets K ein Körper und L ein Oberkörper (beziehungsweise eine Körpererweiterung) davon.

4.2.1 Einfache algebraische Erweiterungen

Definition 4.2.1. Sei $K \leq L$, so definieren wir $[L : K]$ als die Dimension von L als Vektorraum über K.

Satz 4.2.2 (Gradsatz). *Sei $K \leq E \leq L$, $[L : E], [E : K] < \infty$. Dann ist*

$$[L : K] = [L : E] \cdot [E : K] < \infty.$$

Beweis. Übungsaufgabe. □

Definition 4.2.3. Sei $K \leq L, \alpha \in L$. Dann nennen wir α *algebraisch über* K (kurz α alg./$_K$), wenn

$$\exists f \in K[x] \setminus \{0\} : f(\alpha) = 0.$$

Ansonsten ist α *transzendent über* K (kurz α transz./$_K$).

Außerdem heißt L *einfache algebraische Erweiterung von* K, wenn es ein über K algebraisches Element $\alpha \in L$ mit $L = K(\alpha)$ gibt.

Beispiel 4.2.4. Sei K ein Körper und betrachte $K \leq K(x)$. Dann ist x nicht algebraisch, da x klarerweise nicht annullierbar ist.

Beispiel 4.2.5. Betrachte $\mathbb{R} \leq \mathbb{C}$. Dann ist $i \in \mathbb{C}$ algebraisch$/_{\mathbb{R}}$, da wir $f(x) = x^2 + 1$ wählen können.

Beispiel 4.2.6. Betrachte $\mathbb{Q} \leq \mathbb{R}$. Dann ist $\sqrt{2} \in \mathbb{R}$ algebraisch$/_{\mathbb{Q}}$. Jedoch sind $\pi, e \in \mathbb{R}$ nicht algebraisch$/_{\mathbb{Q}}$.

Bemerkung 4.2.7. Ist α algebraisch über K, so können wir das nichttriviale Ideal

$$I := \{f \in K[x] \mid f(\alpha) = 0\} \lhd K[x]$$

wählen. Nun gibt es ein $\mu_\alpha \in K[x]$ normiert, mit $I = (\mu_\alpha)$, da $K[x]$ ein Hauptidealring ist. Diese Erzeuger sind eindeutig bis auf Assoziiertheit, denn ist $I = (\mu_\alpha) = (g)$, so gilt $\mu_\alpha \mid g$ und $g \mid \mu_\alpha$, womit $g \sim \mu_\alpha$. Insbesondere ist das normierte Polynom μ_α mit dieser Eigenschaft eindeutig bestimmt.

Definition 4.2.8. Sei $K \leq L$ und $\alpha \in L$ algebraisch$/_K$. Dann heißt das eindeutig bestimmte Polynom μ_α aus Bemerkung 4.2.7 das *Minimalpolynom von α über K*.

Verschiedene α, β können dasselbe Minimalpolynom besitzen. In diesem Fall stimmen jedoch die jeweiligen Körpererweiterungen überein, wie wir in folgender Proposition sehen werden.

Proposition 4.2.9. *Sei $K \leq L, \alpha \in L$ algebraisch über K und $\deg \mu_\alpha = k$. Dann gilt:*

1. *Die Abbildung $\varphi : K[x]/_{(\mu_\alpha)} \to K[\alpha], f + (\mu_\alpha) \mapsto f(\alpha)$ ist ein Ring-Isomorphismus.*
2. *$K[\alpha] = K(\alpha)$*
3. *$\forall \beta \in K(\alpha) \exists! a_0, \ldots, a_{k-1} \in K : \beta = \sum_{i=0}^{k-1} a_i \alpha^i$*
4. *$\alpha^0, \ldots, \alpha^{k-1}$ bildet eine Basis von $K(\alpha)/_K$ als Vektorraum.*
5. *$[K(\alpha) : K] = k$*
6. *Ist $\beta \in L, \mu_\alpha = \mu_\beta$, so existiert ein eindeutiger Isomorphismus $\psi : K(\alpha) \to K(\beta)$ mit $\psi(\alpha) = \beta$ und $\psi|_K = \mathrm{id}_K$.*

Beweis.

1. Folgt sofort aus dem Homomorphiesatz, angewandt auf den Einsetzungshomomorphismus.
2. Es ist $K[\alpha]$ ein Unterring von L und damit ein Integritätsbereich. Nach (1) ist also auch $K[x]/_{(\mu_\alpha)}$ ein Integritätsbereich, womit (μ_α) prim ist. Damit ist μ_α prim, insbesondere irreduzibel. Wir behaupten nun, dass (μ_α) ein maximales Ideal ist. Um dies einzusehen sei J ein echtes Ideal von $K[x]$ mit $(\mu_\alpha) \subseteq J$. Dann gibt es ein $g \in K[x]$ mit $J = (g)$, also $(\mu_\alpha) \subseteq (g)$, womit $g \mid \mu_\alpha$ folgt. Da μ_α irreduzibel ist folgt dadurch $g \sim \mu_\alpha$ und damit $J = (\mu_\alpha)$. Also ist (μ_α) maximal. Damit ist jedoch $K[x]/_{(\mu_\alpha)}$ nach Proposition 2.3.24 ein Körper und nach (1) isomorph zu $K[\alpha]$, womit $K[\alpha] = K(\alpha)$ folgt.
3. Existenz: Nach (1) und (2) gibt es ein $f \in K[x]$ mit $\varphi(f + (\mu_\alpha)) = f(\alpha) = \beta$. Nun ist $f = g \cdot \mu_\alpha + f'$ mit einem Polynom f' mit Grad kleiner k. Damit ist $f'(\alpha) = f(\alpha) = \beta$.

   Eindeutigkeit: Ist $f(\alpha) = \beta = g(\alpha)$, wobei der Grad von f, g kleiner als k ist, so folgt $(f - g)(\alpha) = 0$, womit $(f - g) \in (\mu_\alpha)$, also gilt $\mu_\alpha \mid (f - g)$, womit $f - g = 0$ und damit $f = g$ ist.

4. Folgt sofort aus (3).
5. Folgt sofort aus (4).
6. Existenz: Nach (1) gibt und (2) gibt es Isomorphismen $\varphi : K[x]/_{(\mu_\alpha)} \to K(\alpha)$ und $\varphi' : K[x]/_{(\mu_\alpha)} \to K(\beta)$ welche $\varphi|_K = \mathrm{id}_K$ und $\varphi'|_K = \mathrm{id}_K$ erfüllen. Wegen $\varphi(x + (\mu_\alpha)) = \alpha$ und $\varphi'(x + (\mu_\alpha)) = \beta$ liefert $\varphi' \circ \varphi^{-1} : K(\alpha) \to K(\beta)$ einen gewünschten Isomorphismus.

   Eindeutigkeit: Sei $\psi : K(\alpha) \to K(\beta)$ ein Isomorphismus mit $\psi(\alpha) = \beta$ und $\psi|_K = \mathrm{id}_K$. Dann gilt insbesondere $\psi(\alpha^i) = \beta^i$, da ψ ein Körperautomorphismus ist. Daher ist ψ als lineare Abbildung von $K(\alpha)$ als Vektorraum über K in den Vektorraum $K(\beta)$ bereits auf einer Basis eindeutig festgelegt, womit ψ insbesondere als Körperautomorphismus eindeutig ist.

□

4.2.2 Nicht-einfache algebraische Erweiterungen

Definition 4.2.10. Wir nennen $K \leq L$ *(rein) algebraisch*, wenn

$$\forall \alpha \in L : \alpha \text{ ist algebraisch über } K.$$

Proposition 4.2.11.

1. *Sei $K \leq L$. Gilt $[L : K] < \infty$, so ist $K \leq L$ algebraisch.*
2. *Sei $K \leq K(\alpha)$ algebraisch, so ist $[K(\alpha) : K] < \infty$.*
3. *Sei $K \leq L$ algebraisch und $L \leq M$ algebraisch, so ist $K \leq M$ algebraisch.*
4. *Sei $K \leq L$ und $S := \{\alpha \in L \mid \alpha \text{ ist algebraisch über } K\}$, so ist $K \leq S \leq L$.*

Beweis.

1. Sei $\alpha \in L \setminus \{0\}$. Da die Dimension der Erweiterung endlich ist, ist die Folge der Potenzen $\alpha^0, \alpha^1, \ldots$ linear abhängig über K. Es gibt also $a_0, \ldots, a_n \in K$ mit $\sum_{i=0}^n a_i \alpha^i = 0$, womit wir $f(x) = \sum_{i=0}^n a_i x^i$ wählen können. Es ist $f(\alpha) = 0$ und $f \neq 0$, womit α algebraisch ist.
2. Es gilt $[K(\alpha) : K] = \deg \mu_\alpha < \infty$.
3. Sei $\alpha \in M$ beliebig, so gibt es ein $f(x) = \sum_{i=0}^n a_i x^i \in L[x], f(\alpha) = 0$, wobei $a_i \in L$, also algebraisch über K sind. Es ist dann auch α algebraisch über $K(a_0, \ldots, a_n)$. Nun gilt

$$\begin{aligned}
[K(\alpha) : K] \leq{} & [K(\alpha, a_0, \ldots, a_n) : K] = \\
&= [K(\alpha, a_0, \ldots, a_n) : K(a_0, \ldots, a_n)] \cdot [K(a_0, \ldots, a_n) : K] = \\
&= [K(\alpha, a_0, \ldots, a_n) : K(a_0, \ldots, a_n)] \cdot [K(a_0, \ldots, a_n) : K(a_1, \ldots, a_n)] \cdot \ldots \\
&\quad \cdot [K(a_{n-1}, a_n) : K(a_n)] \cdot [K(a_n) : K] < \infty
\end{aligned}$$

   und nach (1) ist $K(\alpha)$ algebraisch über K, also insbesondere α über K.
4. Seien $\alpha, \beta \in S$, es reicht $\alpha \cdot \beta, \alpha + \beta, \alpha^{-1} \in S$ zu zeigen. Nach (1) ist $K \leq K(\alpha)$ algebraisch, genauso ist $K(\alpha) \leq K(\alpha, \beta)$ algebraisch, wobei letzteres ein Körper ist, womit $\alpha \cdot \beta, \alpha + \beta, \alpha^{-1} \in K(\alpha, \beta)$ folgt und diese damit nach (3) algebraisch über K sind, also in S liegen.

□

4.2.3 Transzendente Erweiterungen

Proposition 4.2.12. *Sei $K \leq L, \alpha \in L$ transzendent über K. Dann existiert ein eindeutiger Isomorphismus $\psi : K(x) \to K(\alpha)$ mit $\psi(x) = \alpha, \psi|_K = \mathrm{id}_K$.*

Beweis. Existenz: Sei $\varphi : K[x] \to K[\alpha]$ der Einsetzungshomomorphismus, $\varphi(f(x)) = f(\alpha)$. Da α transzendent ist, ist $\ker\varphi$ trivial. Damit ist φ ein Ringisomorphismus. Nun ist $K(x)$ der Quotientenkörper von $K[x]$, genauso ist $K(\alpha)$ der Quotientenkörper von $K[\alpha]$. Aufgrund der Eindeutigkeit des Quotientenkörpers existiert genau ein $\psi : K(x) \to K(\alpha)$ mit $\psi|_{K[x]} = \varphi$.

Eindeutigkeit: Sei $\widetilde{\psi} : K(x) \to K(\alpha)$ ein weiterer Isomorphismus mit $\widetilde{\psi}(x) = \alpha$ und $\widetilde{\psi}|_K = \mathrm{id}_K$. Damit folgt $\widetilde{\psi}|_{K[x]} = \varphi$. Nach der oben erwähnten Eindeutigkeit des Quotientenkörpers folgt dadurch bereits $\widetilde{\psi} = \psi$. □

24.05.2023

31.05.2023

Definition 4.2.13. Sei $K \leq E$.

- Sei $S \subseteq E$. Wir nennen S *algebraisch abhängig über K*, wenn es $a_1, \ldots, a_n \in S$ paarweise verschieden und $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n], f \neq 0$ mit $f(a_1, \ldots, a_n) = 0$ gibt. Sonst nennen wir S *algebraisch unabhängig*.
- Wir nennen E *rein transzendent über K*, wenn es eine algebraisch unabhängige Teilmenge $S \subseteq E$ gibt mit $E = K(S)$. Weiters heißt E *einfache transzendente Erweiterung von K*, wenn es ein über K transzendentes Element $\alpha \in E$ mit $E = K(\alpha)$.
- Sei $S \subseteq E$. Wir nennen S *Transzendenzbasis von E über K*, wenn S maximal algebraisch unabhängig ist.

Bemerkung 4.2.14. Ist S eine Transzendenzbasis von E über K, so bedeutet das *nicht* unbedingt $E = K(S)$, wie wir gleich sehen werden.

Proposition 4.2.15. *Sei $K \leq E, S \subseteq E$. Dann sind äquivalent:*

1. *S ist maximal algebraisch unabhängig, also eine Transzendenzbasis.*
2. *S ist minimal, sodass E algebraisch über $K(S)$ ist.*
3. *S ist algebraisch unabhängig und E ist algebraisch über $K(S)$.*

Beweis. Übungsaufgabe. □

Proposition 4.2.16. *Seien $K \leq L_1, L_2$ und $S_1 \subseteq L_1, S_2 \subseteq L_2$ algebraisch unabhängig über K, sowie $\varphi : S_1 \to S_2$ eine Bijektion. Dann gibt es eine eindeutige Fortsetzung $\overline{\varphi} : K(S_1) \to K(S_2)$ sodass $\overline{\varphi}$ ein Isomorphismus ist und $\overline{\varphi}|_K = \mathrm{id}_K, \overline{\varphi}|_{S_1} = \varphi$.*

Beweis. Übungsaufgabe. □

Proposition 4.2.17. *Sei $K \leq E$, dann gibt es eine Transzendenzbasis S von E über K.*

Beweis. Betrachte

$$\mathcal{S} := \{S \subseteq E \mid S \text{ ist algebraisch unabhängig über } K\}.$$

Wegen $\emptyset \in \mathcal{S}$ ist $\mathcal{S}$ nicht leer und daher $(\mathcal{S}, \subseteq)$ eine Halbordnung. Ist $\mathcal{M} \subseteq \mathcal{S}$ eine beliebige Kette, so ist $\bigcup \mathcal{M} \in \mathcal{S}$. Nach dem Lemma von Zorn gibt es ein maximales Element, welches gerade unsere Transzendenzbasis darstellt. □

Korollar 4.2.18. *Sei $K \leq E$ und $S \subseteq E$ eine Transzendenzbasis von E über K. Dann ist $K \leq K(S) \leq E$, wobei der erste Schritt (von K auf $K(S)$) rein transzendent und der zweite Schritt (von $K(S)$ auf E) rein algebraisch ist.*

Definition 4.2.19. Sei $K \leq E, A \subseteq E$. Dann definieren wir die *algebraische Hülle von A* als

$$[A] := \{b \in E \mid b \text{ ist algebraisch über } K(A)\}.$$

Gilt $E = [A]$, so heißt A *algebraisches Erzeugendensystem von E über K.*

Lemma 4.2.20. *Sei $K \leq E, A \subseteq E$. Dann gilt $[[A]] = [A]$.*

Beweis. Es gilt $K(A) \leq [A]$ als Körper, sowie $[A] \leq [[A]]$. Beide dieser Körpererweiterungen sind algebraisch, womit auch $K(A) \leq [[A]]$ eine algebraische Erweiterung ist. Also gilt für alle $b \in [[A]]$ bereits $b \in [A]$. □

Lemma 4.2.21 (Austauschlemma)**.** *Seien $K \leq E, A \subseteq E, b, c \in E$ mit $c \in [A \cup \{b\}], c \notin [A]$. Dann ist $b \in [A \cup \{c\}]$.*

Beweis. Sei $f \in K(A \cup \{b\})[x] \setminus \{0\}$ mit $f(c) = 0$, o. B. d. A. setzen wir voraus, dass $f \in K[A \cup \{b\}][x]$ gilt, also f ein Polynom über der Ringerweiterung von K um $A \cup \{b\}$ ist. Sei $g(x, y) \in K[A][x, y]$ mit $g(x, b) = f(x)$. Wähle $h(y) := g(c, y) \in K[A \cup \{c\}][y]$. Dann ist $\deg h(y) \geq 1$. Nun gilt $h(b) = g(c, b) = f(c) = 0$, womit b algebraisch über $K(A \cup \{c\})$ ist. □

Korollar 4.2.22. *Seien $K \leq E, A \subseteq E, b, c \in E$ mit $c \in [A \cup \{b\}], c \notin [A]$. Dann gilt:*

- $[A \cup \{b\}] = [A \cup \{c\}]$
- *Ist A algebraisch unabhängig, so ist auch $A \cup \{b\}$ algebraisch unabhängig.*

Beweis. Es ist $c \in [A \cup \{b\}]$, womit $[A \cup \{c\}] \subseteq [A \cup \{b\}]$ folgt. Mit dem Austauschlemma folgt die andere Mengeninklusion.

Sei nun A algebraisch unabhängig. Wäre $A \cup \{b\}$ algebraisch abhängig, so wäre $b \in [A]$ und damit $c \in [A]$, im Widerspruch. □

Korollar 4.2.23. *Seien B, C Transzendenzbasen von E über K. Dann gibt es für alle $b \in B$ ein $c \in C$, sodass $(B \setminus \{b\}) \cup \{c\}$ eine Transzendenzbasis ist.*

Beweis. Zunächst gibt es ein $c \in C$ mit $c \notin [B \setminus \{b\}]$, da wir sonst eine kleinere Transzendenzbasis hätten. Wegen $c \in [B]$ folgt mit dem Austauschlemma, dass $b \in [(B \setminus \{b\}) \cup \{c\}]$. Damit ist E algebraisch über $K((B \setminus \{b\}) \cup \{c\})$. Weiters ist $(B \setminus \{b\}) \cup \{c\}$ algebraisch unabhängig. □

Lemma 4.2.24. *Seien $K \leq E$, B, C Transzendenzbasen und B endlich. Dann ist $|B| = |C|$.*

Beweis. Wir tauschen induktiv Basisvektoren aus. Dazu sei $B_0 := B = \{b_1, \ldots, b_n\}$. Wähle $c_0 \in C_0$, sodass $B_1 := B \setminus \{b_0\} \cup \{c_0\}$ eine Transzendenzbasis ist. Es ist $c_0 \notin B \setminus \{b_0\}$, da sonst B keine Transzendenzbasis wäre. Fährt man induktiv fort, so erhält man nach n Schritten, dass $B_n \subseteq C$ eine Transzendenzbasis ist, also folgt $|B| = |B_n| = |C|$. □

Für den folgenden Satz erwähnen wir einige relevante Eigenschaften über Kardinalitäten. Für zwei Mengen B und C schreiben wir $|B| = |C|$, wenn es eine Bijektion zwischen B und C gibt. Falls es eine injektive Abbildung von B nach C gibt, so schreiben wir $|B| \leq |C|$, andernfalls schreiben wir $|B| > |C|$. Dieses „$\leq$“ erfüllt alle Eigenschaften einer linearen Ordnung, sie ist also reflexiv, transitiv und antisymmetrisch. Ist I eine beliebige Indexmenge und sind M_i beliebige Mengen, so bezeichnet $\sum_{i \in I} |M_i|$ die Kardinalität der Menge $\bigcup_{i \in I} M_i \times \{i\}$. Im Beweis von Satz 4.2.25 verwenden wir diese Tatsache: Ist I unendlich und sind alle M_i endlich, so gilt $\sum_{i \in I} |M_i| = |I|$.

Satz 4.2.25. *Seien $K \leq E$, B, C Transzendenzbasen. Dann ist $|B| = |C|$.*

Beweis. Sind B oder C endlich so folgt die Aussage aus dem vorigen Lemma. Seien also B, C unendlich. Es gibt für alle $c \in C$ ein $B_c \subseteq B$ endlich mit $c \in [B_c]$. Es gilt $\bigcup_{c \in C} B_c = B$, womit $|B| \leq \sum_{c \in C} |B_c| = |C|$ folgt. Aus Symmetriegründen folgt die andere Ungleichung und damit die Gleichheit. □

Definition 4.2.26. Sei $K \leq E$. Wir definieren den *Transzendenzgrad von E über K* als $|B|$, wobei $B \subseteq E$ eine beliebige Transzendenzbasis ist.

4.2.4 Adjunktion einer Nullstelle

Lemma 4.2.27. *Sei K ein Körper, $f \in K[x]$ irreduzibel mit $\deg f \geq 2$. Dann hat f keine Nullstellen in K.*

Beweis. Wir behaupten $f(a) = 0 \Leftrightarrow (x-a) \mid f$. Die Implikation von rechts nach links ist klar. Ist a eine Nullstelle von f, so können wir mit dem Divisionsalgorithmus $f(x) = q(x) \cdot (x-a) + r(x)$ mit $\deg r < 1$ schreiben. Dann ist $0 = f(a) = 0 + r(0)$, womit $r = 0$ folgt und die Aussage gezeigt ist. □

Beispiel 4.2.28. Betrachte $\mathbb{R} \leq \mathbb{C}$. Es ist $f(x) = x^2 + 1$ irreduzibel über $\mathbb{R}$. Wir wollen i zu einer Nullstelle machen, dann gilt also $i^2 + 1 = 0$. Damit können wir auf $i^3 = i \cdot i^2 = i \cdot (-1)$ schließen, analog für $i^4, \ldots$. Wir können also das Verhalten von i nur durch die Eigenschaft eine Nullstelle zu sein analysieren.

Proposition 4.2.29 (Kronecker)**.** *Sei $f \in K[x]$ irreduzibel. Dann gilt:*

1. *$K[x]/_{(f)} =: L$ ist ein Körper.*
2. *Die Abbildung $\varphi : K \to L, c \mapsto c + (f)$ ist eine Körpereinbettung.*
3. *Es gibt eine eindeutige Ringeinbettung $\overline{\varphi} : K[x] \to L[x]$ mit $\overline{\varphi}|_K = \varphi, \overline{\varphi}(x) = x$.*
4. *Identifiziert man $K[x]$ mit $\varphi(K[x])$ und K mit $\varphi(K)$, so ist $x + (f) \in L$ eine Nullstelle von f (formal von $\overline{\varphi}(f)$).*
5. *$[L : K] = \deg f < \infty$, insbesondere ist L algebraisch über K.*

31.05.2023
01.06.2023

Beweis.

1. Es ist nur zu zeigen, dass (f) ein maximales Ideal ist, da dann bereits die Aussage aus Proposition 2.3.24 folgt. In Hauptidealringen sind die maximalen Ideale gerade die von den irreduziblen Elementen erzeugten Ideale – da $K[x]$ ein Hauptidealring ist, folgt also das zu Zeigende.

2. Klarerweise ist φ ein Homomorphismus. Für die Injektivität betrachten wir $c + (f) = d + (f)$. Es ist also $c - d \in (f)$, also $f \mid c - d$, womit jedoch bereits $c = d$ folgt.

3. Klarerweise ist $\overline{\varphi}$ ein Homomorphismus. Für die Injektivität betrachten wir $\overline{\varphi}(g) = \overline{\varphi}(h)$, wegen Koeffizientenvergleich müssen dann jedoch bereits die Polynome übereinstimmen, es gilt also $g = h$. Für die Eindeutigkeit bemerken wir, dass $K[x]$ von $K \cup \{x\}$ erzeugt wird. Quasi ist $K[x]$ also frei erzeugt von x über K.

4. Es ist $f(x + (f)) = f(x) + (f) = 0 + (f) = 0_L$, da $f(x) \in (f)$.

5. Es gilt $L = K(x + (f))$, da $K[x]$ von $K \cup \{x\}$ erzeugt wird. Weiters ist gerade f das Minimalpolynom von $x + (f)$ über K, womit $[L : K] = \deg f$ folgt.

□

Definition 4.2.30. Sei $K \leq E$ und $P \subseteq K[x]$.

- E heißt *Nullstellenkörper* von P (über K), wenn jedes $f \in P$ über E in Linearfaktoren zerfällt, das heißt es gibt $\alpha_1, \dots, \alpha_n \in E, a \in K$ mit $f(x) = a(x - \alpha_1)\dots(x - \alpha_n)$, wobei die Linearfaktoren nicht paarweise verschieden sein müssen.

- Wenn E minimal mit dieser Eigenschaft ist (das heißt, dass E von K und den Nullstellen aller $f \in P$ erzeugt wird), dann heißt E *Zerfällungskörper* von P (über K).

- K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom in $K[x]$ über K in Linearfaktoren zerfällt.

- Ein *algebraischer Abschluss* von K ist ein Erweiterungskörper L, sodass $K \leq L$ algebraisch und L algebraisch abgeschlossen ist.

Beispiel 4.2.31. Betrachte $K = \mathbb{Q}, P = \{x^2 - 2\}$, so ist $E = \mathbb{Q}(\sqrt{2})$ ein Zerfällungskörper.

Mit $P = \{x^3 - 2\}$ ist beispielsweise $\mathbb{C}$ ein Nullstellenkörper. Es ist $\mathbb{Q}(\sqrt[3]{2})$ *kein* Zerfällungskörper und auch kein Nullstellenkörper, da die komplexen Wurzeln fehlen. $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}})$ hingegen ist ein Zerfällungskörper.

Bemerkung 4.2.32. Wie wir später sehen werden sind Zerfällungskörper (bis auf Isomorphie) eindeutig – es macht also durchaus Sinn von *dem* Zerfällungskörper zu sprechen.

Proposition 4.2.33. *Sei K ein Körper, dann sind äquivalent:*

1. *K ist algebraisch abgeschlossen.*

2. *Jedes nicht konstante Polynom in $K[x]$ hat eine Nullstelle in K.*

3. *Jedes nicht konstante irreduzible Polynom in $K[x]$ hat eine Nullstelle in K.*

4. *Jedes nicht konstante irreduzible Polynom in $K[x]$ hat Grad 1.*

5. *Für jede algebraische Erweiterung $L \geq K$ gilt $L = K$.*

Beweis. Übungsaufgabe. □

Proposition 4.2.34. *Sei $K \leq L$, dann sind äquivalent:*

1. *L ist ein algebraischer Abschluss von K.*
2. *L ist ein Nullstellenkörper von $K[x]$ und L ist algebraisch über K.*
3. *L ist ein Zerfällungskörper von $K[x]$.*
4. *L ist algebraisch über K und für alle $L' \geq L$ gilt, dass wenn L' algebraisch über K ist, dann ist bereits $L' = L$.*

Beweis. Übungsaufgabe. □

Proposition 4.2.35. *Sei K ein Körper. Dann gibt es einen Zerfällungskörper von $K[x]$ über K. Dieser ist insbesondere algebraisch über K. Damit gibt es insbesondere einen algebraischen Abschluss von K.*

Beweis. Wir geben einen Beweis an, welcher die Idee besonders gut widerspiegelt, allerdings technisch nicht korrekt ist, siehe dazu die nächste Bemerkung. Betrachte

$$\mathcal{S} := \{E \mid E \text{ ist Körper}, K \leq E \text{ algebraische Erweiterung }\}.$$

Dann ist $(\mathcal{S}, \leq)$ eine Halbordnung. Klarerweise ist $\mathcal{S} \neq \emptyset$, da zumindest $K \in \mathcal{S}$ gilt, weiters sind alle Ketten beschränkt. Um dies einzusehen, sei $\mathcal{K} = \{E_i \mid i \in I\}$ eine Kette in $\mathcal{S}$. Wir wollen ein $E \in \mathcal{S}$ finden mit $E_i \leq E$ für alle $i \in I$: Wähle dazu $E := \bigcup_{i\in I} E_i$. Wie man (aufgrund der Ketteneigenschaft) verifiziert, ist E ein Oberkörper, wobei $x+y := x+^{E_i} y$ mit einem $i \in I$ sodass $x, y \in E_i$ gilt definiert wird. Aufgrund der Ketteneigenschaft ist die Definition unabhängig von der Wahl von i, das heißt die Addition auf E ist wohldefiniert, die anderen Operationen definiert man analog. Klarerweise gilt auch $K \leq E$. Da alle Elemente der Vereinigung algebraisch sind, ist auch E algebraisch, womit tatsächlich $E \in \mathcal{S}$ folgt. Mit dem Lemma von Zorn erhalten wir also ein maximales $E \in \mathcal{S}$. Wir wollen zeigen, dass E algebraisch abgeschlossen ist, da dann E bereits der Zerfällungskörper ist. Sei dazu $f \in E[x]$ irreduzibel, wir wollen zeigen, dass f eine Nullstelle in E hat. Nach Kronecker gibt es ein $E_1 \in \mathcal{S}$ sodass $E \leq E_1$ eine algebraische Erweiterung ist und f eine Nullstelle in E_1 hat. Da E maximal ist folgt jedoch $E_1 = E$, womit das zu Zeigende folgt. □

Bemerkung 4.2.36. Streng genommen ist der obige Beweis "falsch", da $\mathcal{S}$ keine Menge sein muss. Da es beliebig viele isomorphe algebraische Körpererweiterungen gibt (mittels Umbenennung) ist $\mathcal{S}$ im Allgemeinen eine echte Klasse, womit wir das Lemma von Zorn nicht mehr anwenden können.

Wir reparieren dies, indem wir stattdessen definieren

$$\mathcal{S} = \{E \mid E \text{ ist Körper}, K \leq E \text{ algebraische Erweiterung}, E \subseteq X\}$$

mit einer festen Menge X. Dann ist nämlich

$$\mathcal{S} \subseteq \mathcal{P}(X) \times \mathcal{P}((X \times X) \times X) \times \dots,$$

wobei die Potenzmengen gerade die Körperoperationen umfangen, und damit eine Menge.

Bleibt zu klären was X sein soll. Wir wählen X als eine beliebige Menge mit $|X| > \max(|K|, |\mathbb{N}|)$. Beispielsweise könnte man $X = K \cup \mathcal{P}(K) \cup \mathbb{R}$ wählen.

Weiters muss man noch darauf achten, dass E_1 hier nicht unbedingt in $\mathcal{S}$ sein muss. Da E_1 jedoch vergleichsweise "klein" ist, können wir E_1 problemlos in eine Menge $\widetilde{E_1} \in \mathcal{S}$ umbenennen:

Proposition 4.2.37. *Sei $K \leq L$ algebraisch. Dann gilt $|L| \leq \max(|K|, |\mathbb{N}|)$.*

Beweis. Wir beweisen zuerst noch, dass $|K[x]| = \max(|K|, |\mathbb{N}|)$ gilt.

Offensichtlich gilt $|K[x]| \geq \max(|K|, |\mathbb{N}|)$, wenn man etwa die Polynome c für $c \in K$ und x^n für $n \in \mathbb{N}$ betrachtet. Definieren wir $M_n := \{f \in K[x] : \deg f \leq n\}$ für $n \in \mathbb{N}$, so gilt

$$K[x] = \bigcup_{n\in\mathbb{N}} M_n.$$

Jede der Mengen M_n hat $n \cdot |K|$ Elemente. Ist K endlich, so sind also alle M_n endlich und es folgt $|K[x]| = |\mathbb{N}|$. Andernfalls gilt $n \cdot |K| = |K|$ und damit $|K[x]| \leq \sum_{n\in\mathbb{N}} |M_n| = \sum_{n\in\mathbb{N}} n \cdot |K| = \sum_{n\in\mathbb{N}} |K| = \max(|K|, |\mathbb{N}|)$. Also folgt in jedem Fall $|K[x]| = \max(|K|, |\mathbb{N}|)$.

Sei $a \in L$, dann gibt es ein $f \in K[x] \setminus \{0\}$ mit $f(\alpha) = 0$. Nun ist

$$N_f := \{\beta \in L \mid f(\beta) = 0\}$$

endlich. Weiters ist

$$L \subseteq \bigcup_{f\in K[x]\setminus\{0\}} N_f,$$

womit wegen $|K[x]| = \max(|K|, |\mathbb{N}|)$ folgt $|L| \leq |K[x]| \cdot |\mathbb{N}| = \max(|K|, |\mathbb{N}|)$. □

01.06.2023

07.06.2023

Satz 4.2.38. *Sei K ein Köper, dann gilt:*

1. $\forall P \subseteq K[x] \exists Z_P \geq K$ *Zerfällungskörper von* $P \wedge Z_P$ *alg.*$/_K$

Beweis. $Z_{K[x]}$ existiert nach Proposition 4.2.35. Sei $P \subseteq K[x]$ beliebig und definieren wir $Z_P := K(S)$ mit $S := \{\alpha \in Z_{K[x]} \mid \exists f \in P \setminus \{0\} : f(\alpha) = 0\}$. Z_P ist ein Nullstellenkörper von P, da er um genau um die Nullstellen erweitert wird. Die Minimalität von Z_P folgt aus der Konstruktion. □

Satz 4.2.39. *Seien K ein Körper, $P \subseteq K[x]$ und Z_1, Z_2 Zerfällungskörper von P über K. Es gibt dann einen Isomorphismus $\varphi : Z_1 \to Z_2$ mit $\varphi|_K = \mathrm{id}_K$.*

Bemerkung 4.2.40. Im Allgemeinen ist der Isomorphismus aus Satz 4.2.39 nicht eindeutig.

Betrachten wir zum Beispiel $\mathbb{R} \leq \mathbb{C}$ und $\varphi : \mathbb{C} \to \mathbb{C}, z \to \overline{z}$, so ist φ ein Automorphismus mit $\varphi|_\mathbb{R} = \mathrm{id}_\mathbb{R}$. Die Identität ist allerdings ein zweiter Isomorphismus der $\mathbb{R}$ festhält.

Es ist für einen Körper K und einen algebraischen Abschluss $\overline{K}$ die Menge $\mathrm{Aut}_K(\overline{K})$[1] $= \{\varphi \in \mathrm{Aut}(\overline{K}) \mid \varphi|_K = \mathrm{id}_K\}$ mit der Komposition eine Gruppe. Die Galoistheorie stellt einen Zusammenhang zwischen dieser Gruppe und den Körpererweiterungen her.

Beweis von Satz 4.2.39. Betrachten wir

$$\mathcal{S} := \{\widetilde{\varphi} \mid K \leq \operatorname{dom} \widetilde{\varphi} \leq Z_1, K \leq \operatorname{ran} \widetilde{\varphi} \leq Z_2, \widetilde{\varphi} \text{ Isomorphismus }, \widetilde{\varphi}|_K = \mathrm{id}_K\},$$

so stellen wir fest, dass $(\mathcal{S}, \subseteq)$ eine Halbordnung ist, $\mathcal{S} \neq \emptyset$, da $\mathrm{id}_K \in \mathcal{S}$ und für jede Kette $K \subset \mathcal{S}$ auch $\bigcup K \in \mathcal{S}$ ist. Nach dem Lemma von Zorn folgt die Existenz eines maximalen Elements φ in $\mathcal{S}$.

[1] Diese Gruppe wird auch als Galoisgruppe bezeichnet

Wir zeigen, dass für $\widetilde{\varphi} \in \mathcal{S}$ mit $\operatorname{dom} \widetilde{\varphi} \neq Z_1$ ein $\widehat{\varphi} \in \mathcal{S}$ existiert mit $\widehat{\varphi} \supsetneq \widetilde{\varphi}$.

Es ist Z_1 ein minimaler Nullstellenkörper von P, also existieren $f \in P$ und $\alpha \in Z_1 \setminus \operatorname{dom} \widetilde{\varphi}$ mit $f(\alpha) = 0$. Sei μ_α das Minimalpolynom von α über $\operatorname{dom} \widetilde{\varphi}$, also $\mu_\alpha \in (\operatorname{dom} \widetilde{\varphi})[x]$. Als Minimalpolynom ist μ_α irreduzibel über $\operatorname{dom} \widetilde{\varphi}$. Wenden wir nun $\widetilde{\varphi}$ auf die Koeffizienten von μ_α an und schreiben dafür $\widetilde{\varphi}(\mu_\alpha)$, dann ist auch $\widetilde{\varphi}(\mu_\alpha)$ irreduzibel in $\operatorname{ran} \widetilde{\varphi}$ und aus $\mu_\alpha \mid f$ folgt $\widetilde{\varphi}(\mu_\alpha) \mid f$. Es zerfällt f über Z_2 in Linearfaktoren (da $f \in P$) und wegen $\widetilde{\varphi}(\mu_\alpha) \mid f$ zerfällt damit auch $\widetilde{\varphi}(\mu_\alpha)$ über Z_2 in Linearfaktoren. Es gibt daher ein $\beta \in Z_2$ mit $\widetilde{\varphi}(\mu_\alpha)(\beta) = 0$. Da $\widetilde{\varphi}(\mu_\alpha)$ als Minimalpolynom irreduzibel über $\operatorname{ran} \widetilde{\varphi}$ ist, erhält man $\beta \notin \operatorname{ran} \widetilde{\varphi}$. $\widetilde{\varphi}(\mu_\alpha)$ ist also das Minimalpolynom von β, womit es ein $\widehat{\varphi} : (\operatorname{dom} \widetilde{\varphi})(\alpha) \to (\operatorname{ran} \widetilde{\varphi})(\beta)$ mit $\widehat{\varphi}|_{\operatorname{dom} \widetilde{\varphi}} = \widetilde{\varphi}$ und $\widehat{\varphi}(\alpha) = \beta$ gibt.

Es muss nun also φ auf ganz Z_1 definiert sein, da wir es sonst wie eben gezeigt erweitern könnten, was ein Widerspruch zur Maximalität wäre. Dass $\operatorname{ran} \varphi = Z_2$ ist erhält man entweder indem man den Beweis mit vertauschten Rollen wiederholt oder mit folgendem Widerspruch. Sei indirekt angenommen $\operatorname{ran} \varphi \subsetneq Z_2$. Es ist $\operatorname{ran} \varphi$ ein Nullstellenkörper, da er isomorph zu Z_1 ist. Dies ist ein Widerspruch zur Minimalität von Z_2 als Zerfällungskörper. □

Korollar 4.2.41. *Sei K ein Körper, $Z \geq K$ Zerfällungskörper von $P \subseteq K[x]$, dann ist Z algebraisch über K.*

Beweis. Wir kennen einen algebraischen Zerfällungskörper und da alle anderen isomorph zu diesem sind, sind alle algebraisch. □

Bemerkung 4.2.42. Proposition 4.2.35 und die Sätze 4.2.38 und 4.2.39 liefern die Existenz und Eindeutigkeit bis auf Isomorphie von algebraischen Abschlüssen und Zerfällungskörpern. Damit ist die folgende Definition sinnvoll:

Definition 4.2.43. Sei K ein Körper, dann schreiben wir $\overline{K}$ für den algebraischen Abschluss. Ist $P \subseteq K[x]$, so schreiben wir Z_P für den Zerfällungskörper von P über K.

Bemerkung 4.2.44. Es gilt $\mathbb{Q} \leq \overline{\mathbb{Q}} \leq \mathbb{C}$. Die erste Erweiterung ist eine algebraische, abzählbare Erweiterung von $\mathbb{Q}$. Die zweite Erweiterung ist transzendent und überabzählbar.

4.2.5 Mehrfache Nullstellen

Es stellt sich die Frage, wann ein irreduzibles $f \in K[x]$ in $\overline{K}$ mehrfache Nullstellen hat.

Definition 4.2.45. Sei $p \in K[x]$ mit einer Darstellung

$$p(x) = q(x) \cdot \prod_{i=1}^{n} (x - \alpha_i)^{e_i}$$

mit $e_i \in \mathbb{N}^+$, $q \in K[x]$ ohne Nullstellen in K und paarweise verschiedenen α_i. Wir nennen e_i die *Vielfachheit* der Nullstelle α_i. Ist $e_i > 1$, so nennen wir α_i *mehrfache Nullstelle*.

Beispiel 4.2.46. Sei $f(x) = x^p - 1$ mit $p \in \mathbb{P}$.

Betrachten wir $K = \mathbb{Q}$: $e^{\frac{2\pi i k}{p}}$ mit $k = 0, \dots p-1$ sind verschiedene (einfache) Nullstellen und bereits alle.

Betrachten wir K mit $\operatorname{char} K = p$. Es ist $x^p - 1 = x^p - 1^p = (x-1)^p$. Es gibt also nur die p-fache Nullstelle 1.

Definition 4.2.47. Sei K ein Körper, $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, dann definieren wir die *formale Ableitung*

$$f'(x) := \sum_{i=1}^{n} \underbrace{\overbrace{i \cdot a_i}^{}}_{\underbrace{a_i + \ldots + a_i}_{i-mal}} x^{i-1}.$$

Bemerkung 4.2.48. Die allgemein bekannten Rechenregeln für Ableitungen (wie zum Beispiel Linearität oder Produktregel) gelten auch für die formale Ableitung.

Lemma 4.2.49. *Seien K ein Körper, $f \in K[x] \setminus \{0\}$ und $\alpha \in \overline{K}$. Es sind folgende Aussagen äquivalent:*

1. *α ist mehrfache Nullstelle von f.*
2. $\mathrm{ggT}(f, f')(\alpha) = 0$.

Beweis.

- $\Rightarrow$: Es gibt ein $g \in \overline{K}[x]$ mit $f = (x-\alpha)^2 g$. Es ist dann $f' = 2(x-\alpha)g + (x-\alpha)^2 g'$, also $f'(\alpha) = 0$. Es gilt also $\mu_\alpha \mid f', f$ also weiter $\mu_\alpha \mid \mathrm{ggT}(f, f')$ und damit $\mathrm{ggT}(f, f')(\alpha) = 0$.
- $\Leftarrow$: Nehmen wir an $\mathrm{ggT}(f, f')(\alpha) = 0$. Da α eine Nullstelle von $\mathrm{ggT}(f, f')$ ist, ist auch $f(\alpha) = 0$ und es gibt ein $g \in \overline{K}[x]$ mit $f = (x-\alpha)g$. Damit ist $f' = g + (x-\alpha)g'$. Es ist $0 = f'(\alpha) = g(\alpha) + 0$. Damit gibt es $h \in \overline{K}[x]$ mit $g = (x-\alpha)h$ und daher ist $f = (x-\alpha)^2 h$, also α eine mehrfache Nullstelle von f.

$\square$

Lemma 4.2.50. *Seien K ein Körper und $f \in K[x]$ irreduzibel. Dann hat f genau dann eine mehrfache Nullstelle in $\overline{K}$, wenn* $\mathrm{char}\, K = p \in \mathbb{P}$ *und*[2] $\exists g \in K[x] : f(x) = g(x^p)$.

Beweis.

- $\Rightarrow$: Sei angenommen f hat eine mehrfache Nullstelle in $\overline{K}$. f ist irreduzibel, also wissen wir $\mathrm{ggT}(f, f') \in \{1, f\}$. Nach obigem Lemma hat $\mathrm{ggT}(f, f')$ eine Nullstelle womit wir $\mathrm{ggT}(f, f') = f$ erhalten. Es gilt daher $f \mid f'$ und da $f \neq 0$ ist, muss $\deg f' < \deg f$ gelten. Gemeinsam impliziert das $f' = 0$. Da f eine mehrfache Nullstelle in $\overline{K}$ hat, muss $\deg f \geq 2$ gelten. Aus der Definition der formalen Ableitung wird klar, dass K endliche Charakteristik haben muss. Da die Charakteristik immer eine Primzahl sein muss, gibt es $p \in \mathbb{P}$ mit $\mathrm{char}\, K = p$. Schreiben wir $f(x) = \sum_{i=0}^{n} a_i x^i$, dann ist $0 = f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Wir erhalten also, dass $i a_i = 0$ gilt, womit also für alle $i \in \{1, \ldots, n\}$ gilt: Aus $a_i \neq 0$ folgt $p \mid i$. Das liefert die Darstellung $f = g(x^p)$.
- $\Leftarrow$: Sei angenommen $\sum_{i=0}^{n} a_i a x^i = f(x) = g(x^p)$ und $\mathrm{char}\, K = p \in \mathbb{P}$. Es gilt dann $f' = 0$, da $p \mid i$ wenn $a_i \neq 0$. Daher ist $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, 0) = f$. In $\overline{K}$ hat f eine Nullstelle, womit $\mathrm{ggT}(f, f')$ eine Nullstelle hat und nach obigem Lemma f damit eine mehrfache Nullstelle hat.

$\square$

07.06.2023
14.06.2023

Lemma 4.2.51. *Seien $K \leq K'$ Körper und $s, t \in K[x]$. Dann gilt* $\mathrm{ggT}_{K[x]}(s, t) \sim \mathrm{ggT}_{K'[x]}(s, t)$.

[2]Wir setzen hier x^p für x in g ein.

Beweis. Sei d ein ggT in $K[x]$ und d' ein ggT in $K'[x]$, beide von (s,t). Klarerweise gilt $d \mid d'$ (in $K'[x]$). Nun existieren nach dem Lemma von Bezout $u, v \in K[x]$ mit $d = us+vt$. Wegen $d' \mid s$ und $d' \mid t$ existieren $s', t' \in K[x]$ mit $s = d's'$ und $t = d's'$. Also folgt $d = us + vt = u(d's') + v(d't') = d'(us' + vs')$, daher gilt auch $d' \mid d$ (wieder in $K'[x]$). Also folgt die Behauptung $d \sim d'$. $\square$

Satz 4.2.52 (vom primitiven Element)**.** *Sei $K \leq L$ eine endlichdimensionale Erweiterung mit* $\operatorname{char} K = 0$*, so gibt es ein $\alpha \in L$, sodass $L = K(\alpha)$.*

Beweis. Sei $L = K(u_1, \dots, u_r)$ mit r minimal. Wir zeigen die Aussage mittels Induktion nach r. Ist $r = 1$ so ist die Aussage trivial. Sonst ist $L = K(u_1, \dots, u_{r+1}) = K(u_1, \dots, u_r)(u_{r+1}) = K(\alpha)(u_{r+1})$. Nennen wir $\beta := u_{r+1}$. Wir müssen also nur die Existenz eines $\delta \in L$ zeigen mit $K(\delta) = K(\alpha, \beta)$. Betrachte in $\overline{K}[x]$:

$$\mu_\alpha = (x - \alpha_1) \dots (x - \alpha_s) \quad \text{und} \quad \mu_\beta = (x - \beta_1) \dots (x - \beta_t),$$

o. B. d. A. sei $\alpha = \alpha_1, \beta = \beta_1$. Wegen $\operatorname{char} K = 0$ gilt $i \neq \ell \Rightarrow \alpha_i \neq \alpha_\ell$ und $j \neq k \Rightarrow \beta_j \neq \beta_k$. Betrachten wir nun Gleichungen der Form

$$\alpha_i + x\beta_j = \alpha + x\beta,$$

wobei $i \geq 1, j \geq 2$. Jede dieser Gleichungen besitzt höchstens eine Lösung. Da der Körper K wegen $\operatorname{char} K = 0$ unendlich ist, existiert ein $c \in K$ sodass für alle solchen Gleichungen gilt:

$$\alpha_i + c\beta_j \neq \alpha + c\beta.$$

Definiere $\delta := \alpha + c\beta \in K(\alpha, \beta)$. Es bleibt $\alpha, \beta \in K(\delta)$ zu zeigen. Definiere

$$f(x) := \mu_\alpha(\delta - cx) \in K(\delta)[x].$$

Dann ist $f(\beta) = \mu_\alpha(\delta - c\beta) = \mu_\alpha(\alpha) = 0$. Für $j \geq 2$ ist $f(\beta_j) = \mu_\alpha(\delta - c\beta_j) \neq 0$. Also gilt $(x - \beta) \mid f, (\mu_\beta)$, sowie für $j \geq 2$ $(x - \beta_j) \nmid f$ (aber $\mid \mu_\beta$). Es folgt $\operatorname{ggT}(f, \mu_\beta) = (x - \beta)$ in $\overline{K}[x]$ und wegen dem letzten Lemma auch in $K(\delta)[x]$. Damit muss $x - \beta \in K(\delta)[x]$ gelten, also $\beta \in K(\delta)$ und auch $\alpha = \delta - c\beta \in K(\delta)$. $\square$

Bemerkung 4.2.53. Sei $K < Z \leq K(x)$ eine einfache transzendente Erweiterung. Dann besagt der Satz von Lüroth (welcher hier nicht bewiesen wird), dass $K \leq Z$ auch eine einfache, transzendente Erweiterung ist.

4.3 Endliche Körper

Satz 4.3.1.

1. *Ist K ein endlicher Körper mit* $\operatorname{char} K = p \in \mathbb{P}$*, so gibt es ein $n \geq 1$ mit $|K| = p^n$.*
2. *Für alle $p \in \mathbb{P}$ und $n \geq 1$ gibt es einen bis auf Isomorphie eindeutigen Körper K mit* $\operatorname{char} K = p$ *und $|K| = p^n$.*

Beweis.

1. Sei nach Satz 4.1.6 $K \geq \mathbb{Z}_p$ und wähle $n := [K : \mathbb{Z}_p]$. Es gilt klarerweise $|K| = p^n$.

2. Betrachte
$$f(x) = x(x^{p^n-1} - 1),$$
so ist
$$f'(x) = p^n x^{p^n-1} - 1 = -1,$$
also folgt $\mathrm{ggT}(f, f') = 1$, womit die Nullstellen von f nach Lemma 4.2.49 paarweise verschieden sind. Wähle
$$N := \{\alpha \in Z_{\{f\}}(\mathbb{Z}_p) \mid f(\alpha) = 0\},$$
so gilt gerade $|N| = p^n = \deg f$. Wir behaupten, dass N ein Körper ist. Klarerweise sind $0, 1 \in N$. Sind $\alpha, \beta \in N$, so ist $\alpha^{p^n} = \alpha, \beta^{p^n} = \beta$, also ist $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Damit ist $\alpha + \beta \in N$. Ist $\alpha \in N$, so gilt $(-\alpha)^{p^n} = (-1)^{p^n}(\alpha)^{p^n} = (-1)^{p^n}\alpha$. Falls $p = 2$ ist, so gilt $-1 = 1$ und daher folgt $-\alpha \in N$. Andernfalls ist p^n ungerade und daher folgt ebenfalls $-\alpha \in N$. Entsprechend verifiziert man $\cdot$ und $^{-1}$.

□

Bemerkung 4.3.2. Für diesen bis auf Isomorphie eindeutigen Körper im obigen Satz schreiben wir auch $\mathrm{GF}(p^n)$. Tatächlich gilt der Satz von Wedderburn – jeder endliche Schiefkörper ist ein Körper, also $\mathrm{GF}(p^n)$ für ein $p \in \mathbb{P}$ und $n \in \mathbb{N}$. Wir werden diesen Satz hier nicht beweisen.

Lemma 4.3.3. *Seien $k, n \geq 1, k \mid n$ und $p \in \mathbb{P}$. Dann gilt:*

1. $(x^k - 1) \mid (x^n - 1)$
2. $(p^k - 1) \mid (p^n - 1)$
3. $(x^{p^k-1} - 1) \mid (x^{p^n-1} - 1)$

Beweis.

1. Es gilt $(x^n - 1) = (x^k - 1)(x^{n-k} + x^{n-2k} + \ldots + x^k + 1)$, da man durch ausmultiplizieren eine Teleskopsumme erhält.
2. Folgt aus (1) mit dem Einsetzungshomomorphismus.
3. Folgt direkt aus (1) und (2).

□

Lemma 4.3.4. *Seien $K_1, K_2 \leq L, |K_1| = |K_2| < \infty$. Dann gilt $K_1 = K_2$.*

Beweis. Wähle $p^n := |K_1| = |K_2|$ mit $p \in \mathbb{P}, n \geq 1$, so ist $\mathbb{Z}_p \leq K_1, K_2$. Nun ist K_1 der Zerfällungskörper von $x^{p^n} - x$, ebenso K_2. Nun gilt nach dem Beweis von Satz 4.3.1, dass K_1 und K_2 genau die Nullstellenmenge von $x^{p^n} - x$ sind, also folgt $K_1 = K_2$. □

Proposition 4.3.5. *Seien $k, n \geq 1$ und $p \in \mathbb{P}$. Dann existiert ein $K \leq \mathrm{GF}(p^n)$ mit $|K| = p^k$ genau dann wenn $k \mid n$.*

Beweis.
"⇒": Es gilt $n = [\mathrm{GF}(p^n) : \mathbb{Z}_p] = [\mathrm{GF}(p^n) : K] \cdot [K : \mathbb{Z}_p] = [\mathrm{GF}(p^n) : K] \cdot k$.

"⇐": Es gilt $g := x^{p^k-1} - 1 \mid x^{p^n-1} - 1 =: f$. Damit folgt
$$\mathbb{Z}_p \leq \mathrm{GF}(p^k) = Z_{\{g\}}(\mathbb{Z}_p) \leq Z_{\{f\}}(\mathbb{Z}_p) = \mathrm{GF}(p^n).$$

□

Lemma 4.3.6. *Sei $n \geq 1, p \in \mathbb{P}$. Dann gilt:*

1. *Für alle $f \in \mathbb{Z}_p[x]$ irreduzibel, $\deg f = n$, gilt:*
   a) $\mathrm{GF}(p^n) = Z_{\{f\}}(\mathbb{Z}_p)$
   b) *Für alle $\alpha \in \mathrm{GF}(p^n)$ mit $f(\alpha) = 0$ folgt $\mathrm{GF}(p^n) = \mathbb{Z}_p(\alpha)$.*
   c) $f \mid x^{p^n} - x$
   d) *f hat nur einfache Nullstellen.*
2. *Ist $g \in \mathbb{Z}_p[x]$ irreduzibel, $\deg g = k$, so gilt $g \mid x^{p^n} - x$ genau dann wenn $k \mid n$. Weiters gilt $g^2 \nmid x^{p^n} - x$.*

Beweis.

1. a) Es gilt $[Z_{\{f\}}(\mathbb{Z}_p) : \mathbb{Z}_p] = n$ und damit $Z_{\{f\}}(\mathbb{Z}_p) = \mathrm{GF}(p^n)$.
   b) Sei $f(\alpha) = 0$. Da f irreduzibel ist folgt $f = \mu_\alpha$. Dann bilden $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ eine Basis von $\mathrm{GF}(p^n)$ über $\mathbb{Z}_p$, also folgt bereits $\mathbb{Z}_p(\alpha) = \mathrm{GF}(p^n)$.
   c) Sei $\alpha \in \mathrm{GF}(p^n), f(\alpha) = 0$, so gilt $f = \mu_\alpha$ und $\alpha^{p^n} - \alpha = 0$, also gilt $f \mid x^{p^n} - x$.
   d) Aus (c) erhalten wir $f \mid x^{p^n} - x$, wobei $x^{p^n} - x$ nur einfache Nullstellen hat, also hat auch f nur einfache Nullstellen.
2. "$\Rightarrow$": Es gilt $\mathbb{Z}_p \leq Z_{\{g\}}(\mathbb{Z}_p) \leq \mathrm{GF}(p^n)$. Nach (1a) gilt $Z_{\{g\}}(\mathbb{Z}_p) = \mathrm{GF}(p^k)$, womit $k \mid n$ folgt.

   "$\Leftarrow$": Nach (1c) gilt $g \mid x^{p^k} - x \mid x^{p^n} - x$. Weiters gilt $g^2 \nmid x^{p^n} - x$, da $x^{p^n} - x$ nur einfache Nullstellen hat.

□

14.06.2023 | 15.06.2023

Definition 4.3.7. Ein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ mit $\deg f = n$ heißt *primitiv*, wenn

$$\exists \alpha \in \mathrm{GF}(p^n) : f(\alpha) = 0 \wedge \mathrm{GF}(p^n) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots\}.$$

Bemerkung 4.3.8. In der Tat ist die Forderung $\exists \alpha \in \mathrm{GF}(p^n) : f(\alpha) = 0 \wedge \mathrm{GF}(p^n) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots\}$ in der Definition des primitiven Polynoms äquivalent zu $\forall \alpha \in \mathrm{GF}(p^n) : (f(\alpha) = 0 \Rightarrow GF(p^n) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots\})$.

Lemma 4.3.9. *Ist K ein Körper und $G \leq (K \setminus \{0\}, \cdot, 1, ^{-1})$ eine endliche Untergruppe, dann ist G zyklisch.*

Beweis. Nach Korollar 2.2.54 gibt es ein $g \in G$, sodass für alle $h \in G$ gilt $\operatorname{ord} h \mid \operatorname{ord} g =: \ell \mid |G|$. Nun ist jedes $h \in G$ eine Nullstelle von $x^\ell - 1$ und da dieses nur ℓ Nullstellen haben kann, ist $\ell \geq |G|$. Es gilt daher $\operatorname{ord} g = |G|$, womit G zyklisch ist. □

Korollar 4.3.10. *Für $n \in \mathbb{N}$ gibt es ein primitives Polynom in $\mathbb{Z}_p[x]$ vom Grad n.*

Beweis. Es ist $(\mathrm{GF}(p^n) \setminus \{0\}, \cdot, 1, ^{-1})$ nach dem vorherigen Lemma zyklisch, womit es ein α mit $\mathrm{GF}(p^n) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots\}$ gibt. Dann ist μ_α primitiv. □

Lemma 4.3.11. *Sei $f \in \mathbb{Z}_p[x]$ irreduzibel, $n := \deg f$, $\alpha_1, \ldots, \alpha_n \in \mathrm{GF}(p^n)$ Nullstellen von f. Dann gilt*

1. $\forall \varphi \in \mathrm{Aut}(\mathrm{GF}(p^n)) : \varphi|_{\{\alpha_1,\ldots,\alpha_n\}}$ *ist eine Permutation von* $\{\alpha_1, \ldots, \alpha_n\}$.
2. *Für alle $i \in \{1, \ldots, n\}$ existiert ein eindeutiger Automorphismus φ_i mit $\varphi_i(\alpha_1) = \alpha_i$.*

Beweis.

1. Mit $\varphi(f)$ bezeichnen wir jenes Polynom, welches man erhält, wenn man φ auf die Koeffizienten von f anwendet. Da sich jedes Element von $\mathbb{Z}_p$ als Summe der 1 darstellen lässt, gilt $\varphi|_{\mathbb{Z}_p} = \mathrm{id}_{\mathbb{Z}_p}$. Da f ein Polynom mit Koeffizienten in $\mathbb{Z}_p$ ist, folgt $\varphi(f) = f$. Es ist $\varphi \in \mathrm{Aut}(\mathrm{GF}(p^n))$, also gilt $\forall \alpha \in \mathrm{GF}(p^n) : f(\alpha) = 0 \Rightarrow f(\varphi(\alpha)) = \varphi(f)(\varphi(\alpha)) = 0$. Daher werden Nullstellen von f durch φ auf Nullstellen von f abgebildet. Da $\varphi|_{\{\alpha_1,\ldots,\alpha_n\}}$ injektiv ist und $\{\alpha_1, \ldots, \alpha_n\}$ endlich ist, ist $\varphi|_{\{\alpha_1,\ldots,\alpha_n\}}$ surjektiv und damit eine Permutation.
2. Es ist $f = \mu_{\alpha_1} = \mu_{\alpha_i}$, also gibt es nach Proposition 4.2.9 einen eindeutigen Isomorphismus $\varphi_i : \mathbb{Z}_p(\alpha_1) \to \mathbb{Z}_p(\alpha_i)$ mit $\varphi_i|_{\mathbb{Z}_p} = \mathrm{id}_{\mathbb{Z}_p}$ und $\varphi_i(\alpha_1) = \alpha_i$. Da $\mathrm{GF}(p^n) = \mathbb{Z}_p(\alpha_1) = \mathbb{Z}_p(\alpha_i)$ folgt die Aussage.

□

Satz 4.3.12.

1. *Für alle $k \in \mathbb{N}$ ist die Abbildung $\varphi_k : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n), x \mapsto x^{p^k}$ ein Automorphismus (genannt* Frobeniusautomorphismus*).*
2. $\forall \varphi \in \mathrm{Aut}(\mathrm{GF}(p^n)) \exists k < n : \varphi = \varphi_k$.

Beweis.

1. Es ist wegen Proposition 2.3.29 ein Ringhomomorphismus gegeben. Man sieht leicht, dass φ_k sogar ein Körperhomomorphismus ist. Nach Korollar 2.3.21 ist φ_k injektiv und da $\mathrm{GF}(p^n)$ endlich ist, ist die Abbildung surjektiv, also ein Körperautomorphismus.
2. Das vorherige Lemma liefert $|\mathrm{Aut}(\mathrm{GF}(p^n))| = n$. Wir müssen nun noch zeigen, dass für $i, j < n$, $i \neq j$ auch $\varphi_i \neq \varphi_j$ gilt. Sei nun $f \in \mathbb{Z}_p[x]$ ein primitives Polynom vom Grad n und $\alpha \in \mathrm{GF}(p^n)$ mit $f(\alpha) = 0$ und $\mathrm{GF}(p^n) \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots\}$. Es ist nun $\alpha^{p^i} \neq \alpha^{p^j}$, womit $\varphi_i(\alpha) \neq \varphi_j(\alpha)$ ist.

□

Definition 4.3.13. Wir definieren

$$\mathrm{GF}\left(p^{\infty}\right) := \bigcup_{k \geq 1} \mathrm{GF}\left(p^{k!}\right).$$

Bemerkung 4.3.14. $\mathrm{GF}(p^{\infty})$ ist ein Körper, algebraisch über $\mathbb{Z}_p$. Der Beweis davon verläuft analog wie im Beweis der Existenz des algebraischen Abschlusses. Weiter ist $\mathrm{GF}(p^{\infty})$ algebraisch abgeschlossen, denn sei $f \in \mathrm{GF}(p^{\infty})[x]$ nicht konstant, dann gibt es ein k, sodass $f \in \mathrm{GF}(p^{k!})[x]$ und ein ℓ, sodass $Z_{\{f\}}(\mathbb{Z}_p) \leq \mathrm{GF}(p^{l!})$. Daher hat f eine Nullstelle in $\mathrm{GF}(p^{\infty})$.

Bezeichnet $(\{GF(p^n) \mid n \in \mathbb{N}\}, \iota)$ die Halbordnung aller $GF(p^n)$ mit der Einbettungsabbildung ι, so kann diese Konstruktion auch mit einer beliebigen anderen cofinalen Kette durchgeführt werden. Cofinal bedeutet, dass für jedes $GF(p^n)$ ein Element in der Kette vorkommen muss, welches in der Halbordnung nach $GF(p^n)$ liegt. Offensichtlich erfüllt die von uns gewählte Folge diese Voraussetzungen.

Kapitel 5

Boolesche Algebren

Das Ziel dieses Kapitels ist den Darstellungssatz für Boolesche Algebren von Stone zu beweisen. Die Inhalte können auch in Goldstern et al.: *Algebra – Eine grundlagenorientierte Einführungsvorlesung* in dem Kapitel *3.6. Verbände und Boolesche Algebren* gefunden werden.

5.1 Einführung

Zuerst sei an die Definition 1.1.26 einer *Booleschen Algebra* erinnert.

Beispiel 5.1.1. Für eine Menge M ist $(\mathcal{P}(M), \cap, \cup, \emptyset, M, \bar{\cdot})$ eine Boolesche Algebra. $\{A \subseteq M \mid |A| < \infty \vee |\overline{A}| < \infty\}$ ist eine Unteralgebra davon. Im Fall, dass $|M| = |\mathbb{N}|$ gilt, liefert das zweite Beispiel eine abzählbare Boolesche Algebra, während $\mathcal{P}(M)$ dann überabzählbar ist.

Beispiel 5.1.2. $\mathfrak{B}_2 = (\{0,1\}, \wedge, \vee, 0, 1, \neg)$ ist eine Boolesche Algebra. Diese ist offensichtlich die einzige zweielementige Boolesche Algebra und erzeugt die gesamte Varietät der Booleschen Algebren. Mit Hilfe von Produktbildung erhält man eine zu $(\mathcal{P}(M), \cap, \cup, \emptyset, M, \bar{\cdot})$ isomorphe Algebra. Die Abbildung

$$\varphi : \begin{cases} \mathcal{P}(M) \to \{0,1\}^M \\ A \mapsto \chi_A \end{cases}$$

stellt einen Isomorphismus zwischen diesen beiden Booleschen Algebren dar, wobei χ_A die Indikatorfunktion der Menge A ist. Mit dem noch folgenden Darstellungssatz ist jede Boolesche Algebra isomorph zu einer Unteralgebra einer Booleschen Algebra von der Form $(\mathcal{P}(M), \cap, \cup, \emptyset, M, \bar{\cdot})$. Das heißt wenn $\mathcal{K}$ die Varietät der Booleschen Algebren bezeichnet, so gilt $\mathcal{K} = SP(\mathfrak{B}_2)$. Insbesondere gelten in $\mathfrak{B}_2$ genau alle Gesetze die in der gesamten Varietät gelten.

Beispiel 5.1.3. Für einen beliebigen topologischen Raum bilden die clopen Mengen (also jene die sowohl offen als auch abgeschlossen sind) eine Boolesche Algebra, analog wie beim ersten Beispiel.

Beispiel 5.1.4. Die freie Boolesche Algebra über der Variablenmenge $\{x_1, x_2, \ldots\}$ bildet ebenfalls eine interessante Boolesche Algebra. Sie ist bis auf Isomorphie die einzige abzählbare Boolesche Algebra ohne Atome, das heißt für jeden Term $t \neq 0$ (wobei die Terme nach den Gesetzen der Varietät faktorisiert werden) existiert ein Element $s \neq 0$ das in der induzierten Halbordnung unter t liegt. Insbesondere existieren auch keine Co-Atome.

Lemma 5.1.5. *Sei $\mathfrak{B}$ eine Boolesche Algebra und $a, b \in B$.*

1. *Gilt $a \vee b = 1, a \wedge b = 0$, dann gilt $a' = b$ (das heißt die Abbildung $'$ ist eindeutig festgelegt).*
2. *Es ist $a'' = a$.*
3. *$0' = 1, 1' = 0$.*
4. *$(a \vee b)' = a' \wedge b'$, $(a \wedge b)' = a' \vee b'$.*

Beweis. Wir zeigen zunächst den ersten Punkt. Es gilt $\overbrace{(a \vee b)}^{=1} \wedge a' = a'$. Nach dem Distributivgesetz gilt aber auch $(a \vee b) \wedge a' = (a \wedge a') \vee (b \wedge a') = b \wedge a'$. Insgesamt folgt also $a' = b \wedge a'$ und daher gilt in der induzierten Halbordnung $a' \leq b$. Analog zeigt man $b \leq a'$ und es folgt $a' = b$.

Wendet man das auf a' und a an, so erhält man $a = a''$. Offensichtlich folgt aus dem ersten Punkt auch sofort $0' = 1$ und $1' = 0$.

Wegen $(a \vee b) \vee (a' \wedge b') = ((a \vee b) \vee a') \wedge ((a \vee b) \vee b') = 1 \wedge 1 = 1$ und $(a \vee b) \wedge (a' \wedge b') = (a \wedge (a' \wedge b')) \vee (b \wedge (a' \wedge b)) = 0 \vee 0 = 0$ folgt wieder aus dem ersten Punkt $(a \vee b)' = a' \wedge b'$. Das zweite Gesetz folgt aus diesem gemeinsam mit dem zweiten Punkt. □

15.06.2023

21.06.2023

Definition 5.1.6. Sei R ein kommutativer Ring mit 1, dann heißt R *Boolesch*, wenn

$$\forall x \in R : x \cdot x = x.$$

Lemma 5.1.7. *Sei R ein Boolescher Ring, dann gilt*

$$\forall x \in R : x = -x.$$

Beweis. Es gilt

$$1 + x = (1 + x)(1 + x) = x \cdot x + x + x + 1 = x + x + x + 1,$$

womit durch Kürzen $0 = x + x$ folgt. □

Proposition 5.1.8.

1. *Sei R ein Boolescher Ring. Dann definieren wir die Operationen*[1]

$$x \wedge y := x \cdot y, \quad x \vee y := x + y + x \cdot y, \quad x' := -x.$$

   Dann ist $(R, \wedge, \vee, 0, 1, ')$ eine Boolesche Algebra.

2. *Sei B eine Boolesche Algebra. Dann definieren wir die Operationen*

$$x \cdot y := x \wedge y, \quad x + y := (x \wedge y') \vee (y \wedge x') =: x \Delta y, \quad -x := x.$$

   Dann ist $(B, +, 0, -, \cdot, 1)$ ein Boolescher Ring.

3. *Die durch die obigen Operationen beschriebenen Übersetzungen von Booleschen Ringen auf Boolesche Algebren und umgekehrt sind zueinander invers.*

4. *Die Homomorphismen auf den Strukturen übersetzen sich, das heißt eine Abbildung φ von einem Booleschen Ring R_1 in einen Booleschen Ring R_2 ist genau dann ein Ring-Homomorphismus, wenn sie ein Homomorphismus bezüglich der zugehörigen Booleschen Algebren ist.*

Beweis.

1. Folgt durch Nachrechnen.

2. Folgt durch Nachrechnen.

[1] Mit dem obigen Lemma sehen wir $x \vee y = x + y - x \cdot y$.

3. Folgt durch Nachrechnen.
4. Für jeden Term t gilt $t^{R_1} = t^{B_1}$. Da die Eigenschaft ein Homomorphismus zu sein lediglich von den Termfunktionen abhängt, und die Termfunktionen übereinstimmen, ist auch der Homomorphismus-Begriff derselbe.

□

Definition 5.1.9. Sei $\mathfrak{V}$ ein Verband und sei $\emptyset \neq A \subseteq \mathfrak{V}$. Dann heißt A *Filter*, wenn

- $\forall x \in A \forall y \in \mathfrak{V} : (x \leq y \implies y \in A)$,
- $\forall x, y \in A : x \wedge y \in A$.

Ist A ein Filter, so nennen wir A *prim*, wenn

$$\forall x, y \in \mathfrak{V} : (x \vee y \in A \implies x \in A \vee y \in A).$$

Definition 5.1.10. Sei $\mathfrak{V}$ ein Verband und sei $\emptyset \neq A \subseteq \mathfrak{V}$. Dann heißt A *Ideal*, wenn

- $\forall x \in A \forall y \in \mathfrak{V} : (y \leq x \implies y \in A)$,
- $\forall x, y \in A : x \vee y \in A$.

Ist A ein Ideal, so nennen wir A *prim*, wenn

$$\forall x, y \in \mathfrak{V} : (x \wedge y \in A \implies x \in A \vee y \in A).$$

Proposition 5.1.11. *Seien R und B die zueinander "assoziierten" Booleschen Ringe, beziehungsweise Booleschen Algebren. Ist $I \subseteq B$ ein Ideal von B, so ist I ein Ideal von R. Ist entsprechend $I \subseteq R$ ein Ideal von R, so ist I ein Ideal von B.*

Beweis.

1. Seien $x, y \in I$. Dann ist $x + y = (x \wedge y') \vee (y \wedge x') \in I$.

   Sind $x \in I, y \in R$, so ist $x \cdot y = x \wedge y \in I$.
2. Seien $x, y \in I$. Dann ist $x \vee y = x + y + x \cdot y \in I$.

   Sind $x \in I, y \leq x$, so ist $y = y \wedge x = y \cdot x \in I$.

□

Bemerkung 5.1.12. Sei B eine Boolesche Algebra und $F \subseteq B$ ein Filter. Dann ist

$$\{a' \mid a \in F\}$$

ein Ideal.

Bemerkung 5.1.13 (Homomorphiesatz für Boolesche Algebren)*.* Seien B_1, B_2 Boolesche Algebren und $f : B_1 \to B_2$ ein surjektiver Homomorphismus. Dann induziert dies einen Isomorphismus $\widetilde{f} : B_1/_{\ker f} \to B_2$. In diesem gilt $(x, y) \in \ker f$ genau dann, wenn $x + y \in f^{-1}(0)$.

Definition 5.1.14. Sei B eine Boolesche Algebra. Dann heißt $a \in B$ *Atom*, wenn $a \neq 0$ und $\forall b \in B \setminus \{0\} : b \leq a \Rightarrow b = a$. a ist also ein minimales Element, wenn wir die 0 nicht berücksichtigen.

Beispiel 5.1.15. Betrachte $\mathcal{P}(\mathbb{N})$ und $I := \{A \in \mathcal{P}(\mathbb{N}) \mid A \text{ endlich}\}$, so ist I ein Ideal. Da I abzählbar ist, ist jedoch $\mathcal{P}(\mathbb{N})/_I$ immer noch überabzählbar. Es handelt sich dabei außerdem um ein weiteres Beispiel einer atomfreien Booleschen Algebra.

5.2 Der Satz von Stone

Satz 5.2.1 (Satz von Stone)**.**

- *Sei B eine Boolesche Algebra. Dann gibt es eine Menge M und einen injektiven Homomorphismus $f : B \to \mathcal{P}(M)$.*
- *Sei B eine endliche Boolesche Algebra. Dann gibt es eine Menge M und einen bijektiven Homomorphismus $f : B \to \mathcal{P}(M)$.*

Korollar 5.2.2. *Ist B eine Boolesche Algebra, so ist $B \in \mathrm{SP}(\mathfrak{B}_2)$.*

Beweis. Diese Aussage folgt sofort aus dem Darstellungssatz von Stone, mit der Bemerkung, dass $\prod_{m\in M} \mathfrak{B}_2 = \mathfrak{B}_2^M$ isomorph zu $\mathcal{P}(M)$ ist. Dazu betrachte man die Abbildung die jede Menge auf ihre Indikatorfunktion abbildet, also $\varphi : \mathcal{P}(M) \to B_2^M, A \mapsto \chi_A$, wobei χ_A wie folgt definiert ist:

$$\chi_A : M \to \{0,1\}, x \mapsto \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

□

Lemma 5.2.3. *Sei B eine Boolesche Algebra, $\emptyset \neq I \subsetneq B$ ein Ideal. Dann ist I ein maximales echtes Ideal genau dann wenn*

$$\forall a \in B : (a \in I \vee a' \in I).$$

Beweis.
“$\Leftarrow$”: Sei $I \subsetneq J$, dann gibt es ein a mit $a \in I \wedge a' \in I$, womit $1 \in I$ ist und damit I nicht echt ist.

“$\Rightarrow$”: Angenommen es gäbe ein $a \in B$ mit $a \notin I, a' \notin I$. Betrachte

$$J := \{x \in B \mid \exists y \in I : x \leq y \vee a\}.$$

Klarerweise gilt $I \subseteq J$. Weiters ist J ein Ordnungsideal nach Definition. Sind $x, \widetilde{x}$ in J, dann gibt es $y, \widetilde{y} \in I$ mit $x \leq y \vee a, \widetilde{x} \leq \widetilde{y} \vee a$, womit folgt $x \vee \widetilde{x} \leq (y \vee \widetilde{y}) \vee a$. Weiters ist $1 \notin J$, sonst gäbe es ein $y \in I$ mit $1 = a \vee y$, womit folgen würde $a' = y \wedge a'$, damit $a' \leq y$ und damit $a' \in I$, im Widerspruch. □

Definition 5.2.4. Sei B eine Boolesche Algebra. Wir nennen $F \subseteq B$ einen *Ultrafilter*, wenn F ein maximaler echter Filter ist, was genau dann der Fall ist, wenn F' ein maximales echtes Ideal ist.

Satz 5.2.5. *Jeder echte Filter in einer Booleschen Algebra ist in einem Ultrafilter enthalten.*

Beweis. Folgt mit dem Lemma von Zorn. □

Lemma 5.2.6. *Sei B eine Boolesche Algebra, $|B| \geq 2$, und $I \subsetneq B$ ein maximales echtes Ideal. Dann ist $B/_I \cong \mathfrak{B}_2$.*

Beweis. Seien $a, b \in B \setminus I$, dann ist $a - b = a + b = (a \wedge b') \vee (b \wedge a') \in I$, womit $a + I = b + I$ folgt. Damit ist $|B/_I| = 2$, womit bereits die Aussage folgt. □

Beweis vom Satz von Stone. Sei B eine Boolesche Algebra. Definiere

$$M := \{F \subseteq B \mid F \text{ ist Ultrafilter}\},$$

$$f : B \to \mathcal{P}(M),\ x \mapsto \{F \in M \mid x \in F\}.$$

f ist injektiv: Wir wollen zeigen, dass wenn $x \neq y$, dann gibt es ein $F \in M$ mit $x \in F, y \notin F$ oder andersherum. Dazu unterscheiden wir:

$x \leq y$: Wir wählen F mit $x' \wedge y \in F$. Dies ist möglich, da der einzige Problemfall $x' \wedge y = 0$ ist. In diesem Fall wäre jedoch $y \vee x = x$, im Widerspruch zu $x \leq y$.

$y \leq x$: Analog mit vertauschten Rollen.

$x \nleq y, y \nleq x$: Wähle F wie im ersten Fall.

f ist ein Homomorphismus:

- $f(1) = M$
- $f(0) = \emptyset$
- $x \in B : f(x') = M \setminus f(x)$
- $x, y \in B : f(x \vee y) = \{F \in M \mid x \vee y \in F\} \overset{(*)}{=} \{F \in M \mid x \in F \vee y \in F\} = f(x) \cup f(y)$
- $x, y \in B : f(x \wedge y) = \{F \in M \mid x \wedge y \in F\} = \{F \in M \mid x \in F \wedge y \in F\} = f(x) \cap f(y)$

An der mit $(*)$ markierten Stelle wurde in der Mengeninklusion „$\subseteq$“ verwendet, dass Ultrafilter insbesondere prim sind. An allen anderen Stellen wurden nur die Filteraxiome verwendet.

Sei nun B endlich. Wir bemerken, dass wenn a ein Atom ist, dann ist

$$F_a := \{b \in B \mid b \geq a\}$$

ein Ultrafilter, da wenn $b \notin F_a$, also wenn $b \ngeq a$ erfüllt ist, dann ist $b \wedge a = 0$ und damit $b' \in F_a$.

Sei $x \in B$, dann ist

$$f(x) = \{F_a \mid a \leq x\}.$$

Jedes $F \in M$ ist von der Form F_a, indem wir $a := \bigcap F$ setzen.

f ist surjektiv: Seien $F_{a_1}, \ldots, F_{a_n} \in M$ beliebig. Wähle $x := a_1 \vee \ldots \vee a_n$. Dann gilt zunächst sicher $F_{a_1}, \ldots, F_{a_n} \in f(x)$. Sei angenommen a ist ein Atom und $F_a \in f(x)$, dann ist $a \leq x = a_1 \vee \ldots \vee a_n$. Schneiden mit a liefert $a \leq (a_1 \wedge a) \vee (a_2 \wedge a) \vee \ldots (a_n \wedge a)$. Falls $a_i \neq a$ für alle $i = 1, \ldots, n$ gilt, so ist $a \leq 0 \vee \ldots \vee 0$ ein Widerspruch. $\square$

Index

Abbildungsverzeichnis