# Kapitel 2

# Grundlegende algebraische Methoden

## 2.1 Unteralgebren

**2.1.1 Definition.** Sei $A$ eine Menge, $\omega : A^n \to A$ eine $n$-stellige Operation auf $A$ ($n \in \mathbb{N}_0$), $T \subseteq A$, dann heißt $T$ *abgeschlossen* bezüglich $\omega :\Leftrightarrow \omega(T^n) \subseteq T$ (d.h., $t_1, \ldots, t_n \in T \Rightarrow \omega t_1 \ldots t_n \in T$; im Fall $n = 0$: $\omega \in T$). (Vgl. auch 1.1.30.)

**2.1.2 Definition.** Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra vom Typ $(n_i)_{i\in I}$, $T \subseteq A$, dann heißt $T$ *abgeschlossen* bezüglich $(\omega_i)_{i\in I} :\Leftrightarrow T$ abgeschlossen bezüglich $\omega_i$ für alle $i \in I$. In diesem Fall wird durch $\omega_i^* x_1 \ldots x_{n_i} := \omega_i x_1 \ldots x_{n_i}$, $(x_1, \ldots, x_{n_i}) \in T^{n_i}$, eine $n_i$-stellige Operation $\omega_i^*$ auf $T$ definiert: $\omega_i^* = \omega_i \restriction T^{n_i}$. Die Algebra $(T, (\omega_i^*)_{i\in I})$ heißt dann eine *Unteralgebra* von $\mathfrak{A}$. Meist schreiben wir: $\omega_i^* =: \omega_i$, das heißt, wir identifizieren[1] die Operation $\omega_i$ mit ihrer Einschränkung $\omega_i^*$.

**2.1.3 Anmerkung.** Oft heißt auch nur die Menge $T$ selbst eine Unteralgebra von $\mathfrak{A}$.

**2.1.4 Satz.** *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $\mathfrak{T} = (T, (\omega_i)_{i\in I})$ eine Unteralgebra von $\mathfrak{A}$. Gilt in $\mathfrak{A}$ das Gesetz $t_1(x_1, \ldots, x_n) \approx t_2(x_1, \ldots, x_n)$ (hierbei sind $t_1, t_2$ Terme in den Variablen $x_1, \ldots, x_n$), d.h. es gilt*

$$\forall a_1, \ldots, a_n \in A : \quad t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n), \tag{2.1}$$

*dann gilt das Gesetz $t_1(x_1, \ldots, x_n) \approx t_2(x_1, \ldots, x_n)$ auch in der Unteralgebra $\mathfrak{T}$.*

*Beweis.* Aus der Gültigkeit von (2.1) für alle $a_1, \ldots, a_n \in A$ folgt natürlich die Gültigkeit von (2.1) für alle $a_1, \ldots, a_n \in T \subseteq A$. □

### 2.1.A Unteralgebren spezieller algebraischer Strukturen

1) Sei $(H, \cdot)$ eine Halbgruppe. $T \subseteq H$ ist eine Unteralgebra von $(H, \cdot) \Leftrightarrow (x, y \in T \Rightarrow xy \in T)$. Es ist dann $\cdot = \cdot \restriction T \times T$ eine binäre Operation auf $T$, und $(T, \cdot)$ ist eine Halbgruppe, denn das Assoziativgesetz gilt in $H$ und damit erst recht in $T$ (Satz 2.1.4).

$(T, \cdot)$ heißt *Unterhalbgruppe* von $(H, \cdot)$.

2) Sei $(G, \cdot)$ eine Gruppe vom Typ (2) und $(T, \cdot)$ Unterhalbgruppe von $(G, \cdot)$. Dann ist im Allgemeinen $(T, \cdot)$ *keine* Gruppe!

[1] Siehe Fußnote auf Seite 12.

**2.1.5 Beispiel.** $(G, \cdot) = (\mathbb{Z}, +)$, $(T, \cdot) = (\mathbb{N}, +)$.

3) Sei $(G, \cdot, e, ^{-1})$ eine Gruppe vom Typ $(2, 0, 1)$. $T \subseteq G$ ist Unteralgebra

$$\Leftrightarrow \left\{ \begin{array}{l} x, y \in T \Rightarrow xy \in T \\ e \in T \\ x \in T \Rightarrow x^{-1} \in T \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} T \neq \emptyset \\ x, y \in T \Rightarrow xy^{-1} \in T \end{array} \right\}.$$

Da die definierenden Gesetze einer Gruppe vom Typ $(2, 0, 1)$ in $G$ und damit auch in $T$ gelten, ist die Unteralgebra $(T, \cdot, e, ^{-1})$ wieder eine Gruppe, genannt *Untergruppe* von $(G, \cdot, e, ^{-1})$.

4) Ist $(R, +, 0, -, \cdot)$ ein Ring vom Typ $(2, 0, 1, 2)$, dann ist jede Unteralgebra $(T, +, 0, -, \cdot)$ wieder ein Ring, genannt *Unterring* von $(R, +, 0, -, \cdot)$. Dies gilt nicht für Ringe vom Typ $(2, 2)$.

**2.1.6 Beispiel.** $(\mathbb{N}, +, \cdot)$ ist Unter*algebra* von $(\mathbb{Z}, +, \cdot)$, aber nicht Unter*ring*.

5) Sei $(K, +, 0, -, \cdot, 1)$ ein Körper vom Typ $(2, 0, 1, 2, 0)$ und $(T, +, 0, -, \cdot, 1)$ eine Unteralgebra (d.h. ein Unterring mit demselben Einselement). Ist $(T, +, 0, -, \cdot, 1)$ selbst ein Körper, so heißt dieser ein *Unterkörper* von $(K, +, 0, -, \cdot, 1)$. Es gilt: $T$ ist Unterkörper

$$\Leftrightarrow \left\{ \begin{array}{l} x, y \in T \Rightarrow x + y \in T \\ 0 \in T \\ x \in T \Rightarrow -x \in T \\ x, y \in T \Rightarrow xy \in T \\ 1 \in T \\ x \in T, x \neq 0 \Rightarrow x^{-1} \in T. \end{array} \right.$$

**2.1.7 Beispiel.** $(\mathbb{R}, +, 0, -, \cdot, 1)$ ist Unterkörper von $(\mathbb{C}, +, 0, -, \cdot, 1)$, aber $(\mathbb{Z}, +, 0, -, \cdot, 1)$ ist *kein* Unterkörper.

6) Sei $(V, +, 0, -, K)$ ein Vektorraum über $K$ und $(T, +, 0, -, K)$ eine Unteralgebra, d.h.,

$$\begin{array}{l} x, y \in T \Rightarrow x + y \in T \\ 0 \in T \\ x \in T \Rightarrow -x \in T \\ \lambda \in K, x \in T \Rightarrow \lambda x \in T. \end{array}$$

Dann ist auch $(T, +, 0, -, K)$ ein Vektorraum über $K$, genannt ein *Unter-(Vektor-)Raum*.

7) Betrachten wir das Monoid $M = (\{0, 1\}, \cdot)$. Jede Teilmenge von $\{0, 1\}$ (insbesondere also auch die leere Menge) ist eine Unterhalbgruppe der Halbgruppe $(\{0, 1\}, \cdot)$. Die Unterhalbgruppen $(\{0\}, \cdot)$, $(\{1\}, \cdot)$ und natürlich $(\{0, 1\}, \cdot)$ sind überdies Monoide. Allerdings bezeichnen wir nur die Unterhalbgruppen $(\{1\}, \cdot)$ und $(\{0, 1\}, \cdot)$ als *Untermonoide*, weil nur diese das selbe neutrale Element wie $M$ haben. Wenn wir von Untermonoiden eines Monoids $M$ sprechen, interpretieren wir $M$ immer als Monoid vom Typ $(2, 0)$.

**2.1.8 Satz.** *Sei $(A, \Omega)$ eine Algebra und $(T_j)_{j \in J}$ eine Familie von Unteralgebren. Dann ist $\bigcap_{j \in J} T_j$ ebenfalls eine Unteralgebra.*

**2.1.9 Anmerkung.** Der in diesem Satz auftretende allgemeine Durchschnitt ist definiert durch $\bigcap_{j \in J} T_j := \{ x \in A \mid \forall j \in J : x \in T_j \}$. Für $J = \emptyset$ ist $\bigcap_{j \in J} T_j = A$.

*Beweis.* Sei $\Omega = (\omega_i)_{i\in I}$, $\omega_i$ eine $n_i$-stellige Operation und $T := \bigcap_{j\in J} T_j$. Sei $i \in I$ mit $n_i > 0$, und seien $x_1, \ldots, x_{n_i} \in T$. Dann gilt: $\forall j \in J : x_1, \ldots, x_{n_i} \in T_j \Rightarrow \omega_i x_1 \ldots x_{n_i} \in T_j$ $\Rightarrow \omega_i x_1 \ldots x_{n_i} \in T$. Für $n_i = 0$ gilt: $\forall j \in J : \omega_i \in T_j \Rightarrow \omega_i \in T$. □

**2.1.10 Satz.** *Sei $(A, \Omega)$ eine Algebra und $S \subseteq A$, dann ist*

$$\langle S\rangle := \bigcap\{T \mid T \supseteq S \text{ und } T \text{ ist Unteralgebra von } (A,\Omega)\}$$

*die* kleinste *Unteralgebra von $(A, \Omega)$, die $S$ enthält.*
*($\langle S\rangle$ ist der Abschluss von $S$ unter allen Operationen in $\Omega$, siehe* 1.1.E.)

**2.1.11 Definition.** $\langle S\rangle$ heißt die *von $S$ erzeugte Unteralgebra* von $(A, \Omega)$. $S$ heißt ein *Erzeugendensystem* von $\langle S\rangle$.

**2.1.12 Satz.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, $x \in G$, $S = \{x\}$ dann gilt:*

$$\langle x\rangle := \langle S\rangle = \{x^k \mid k \in \mathbb{Z}\}.$$

*Beweis.* Zu zeigen: $\langle x\rangle = \{x^k \mid k \in \mathbb{Z}\} =: T$.
$\subseteq$: $T$ ist eine Untergruppe von $(G, \cdot, e, ^{-1})$, denn seien $x^k, x^l \in T$, $k, l \in \mathbb{Z}$. Dann gilt: $x^k x^l = x^{k+l} \in T$ (wegen $k + l \in \mathbb{Z}$); $x^0 \in T$ (wegen $0 \in \mathbb{Z}$); $(x^k)^{-1} = x^{-k} \in T$ (wegen $-k \in \mathbb{Z}$). Weiters gilt $x = x^1 \in T$, also $\{x\} \subseteq T$, woraus $\langle x\rangle \subseteq T$ folgt.
$\supseteq$: Sei $U$ eine Untergruppe von $(G, \cdot, e, ^{-1})$ mit $\{x\} \subseteq U$, d.h., $x \in U$. Dann gilt: $x^n \in U$ $(n \in \mathbb{N})$, $e = x^0 \in U$, $x^{-n} = (x^n)^{-1} \in U \Rightarrow T \subseteq U \Rightarrow T \subseteq \langle x\rangle$. □

**2.1.13 Definition.** $\langle x\rangle$ heißt die *von $x$ erzeugte Untergruppe* von $(G, \cdot, e, ^{-1})$.

**2.1.14 Anmerkungen.** 1) Analog gilt[2] für Vektorräume:

$$\langle\{x_1, \ldots, x_n\}\rangle = \{\sum_{1\le i\le n} \lambda_i x_i \mid \lambda_1, \ldots, \lambda_n \in K\}.$$

2) Ist $(G, \cdot, e, ^{-1})$ eine *abelsche* Gruppe, dann gilt:

$$\langle\{x_1, \ldots, x_n\}\rangle = \{\, x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z}\,\}.$$

Schreibt man die abelsche Gruppe in der Form $(G, +, 0, -)$, dann gilt:

$$\langle\{x_1, \ldots, x_n\}\rangle = \{k_1 x_1 + k_2 x_2 + \cdots + k_n x_n \mid k_i \in \mathbb{Z} \text{ für alle } i\}.$$

3) Für *nichtabelsche* Gruppen gilt z.B.:

$$\langle\{x_1, x_2\}\rangle = \{x_1^{k_{11}} x_2^{k_{12}} x_1^{k_{21}} x_2^{k_{22}} \cdots x_1^{k_{n1}} x_2^{k_{n2}} \mid n \in \mathbb{N},\, k_{ij} \in \mathbb{Z}\}.$$

4) Allgemein gilt:

$$\langle\{x_1, \ldots, x_n\}\rangle = \{t(x_1, \ldots, x_n) \mid t \text{ ist ein beliebiger } n\text{-stelliger } \textit{Term} \text{ in der Algebra } (A,\Omega)\}.$$ (Vgl. auch 1.1.31.)

**2.1.15 Definition.** Eine Gruppe $(G, \cdot, e, ^{-1})$ heißt *zyklisch* $:\Leftrightarrow \exists x \in G : G = \langle x\rangle$. $x$ heißt dann *erzeugendes Element.*

[2] Die leere Summe $\sum_{i\in\emptyset} x_i$ definieren wir als 0. Dadurch gilt erstens die Gleichung $\sum_{i\in A\cup B} x_i = \sum_{i\in A} x_i + \sum_{j\in B} x_j$ für alle disjunkten Mengen $A, B$, und zweitens passt dann die angeführte Formel zur Tatsache, dass der von der leeren Menge erzeugte Vektorraum genau aus dem Nullvektor besteht: $\langle\emptyset\rangle = \{0\}$.

**2.1.16 Lemma.** *Sei $(G, \cdot, e, ^{-1})$ eine zyklische Gruppe und $\langle x \rangle = G$. Dann gibt es zwei Fälle:*

a) *Ist $\mathrm{o}(x) = \infty$, dann ist auch $G$ unendlich, und es gilt $G = \{e, x, x^{-1}, x^2, x^{-2}, \ldots\}$.*

b) *Ist $\mathrm{o}(x) = n \in \mathbb{N}$, dann ist $|G| = n$, und es gilt $G = \{e, x, x^2, \ldots, x^{n-1}\}$.*

*In beiden Fällen sind die angeführten Potenzen paarweise verschieden.*

**2.1.17 Beispiel.** Zu a): Für $(\mathbb{Z}, +, 0, -)$ gilt $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
Zu b): Für $(\mathbb{Z}_m, +, 0, -)$ (Operationen modulo $m$, siehe Abschnitt 2.2.B) gilt $\mathbb{Z}_m = \langle 1 \rangle = \langle k \rangle$ mit $\mathrm{ggT}(m, k) = 1$ (Übungsbeispiel 38).

## 2.1.B Nebenklassenzerlegung einer Gruppe nach einer Untergruppe

**Bezeichnung:** Falls kein Irrtum möglich ist, setzen wir im folgenden häufig $G := (G, \cdot, e, ^{-1})$ bzw. $G := (G, \cdot)$, d.h., wir bezeichnen eine Gruppe mit demselben Symbol wie ihre Grundmenge. In weiterer Folge wird dies auch für Ringe getan.

**2.1.18 Satz.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und $(H, \cdot, e, ^{-1})$ eine Untergruppe von $G$. Sei weiters $\pi$ auf $G$ definiert durch $x \,\pi\, y :\Leftrightarrow x^{-1}y \in H$, $x, y \in G$. Dann ist $\pi$ eine Äquivalenzrelation auf $G$.*

*Beweis.* 1) $\pi$ ist reflexiv: $\forall x : x \,\pi\, x$, denn $x^{-1}x = e \in H$.
2) $\pi$ ist symmetrisch: $x \,\pi\, y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \,\pi\, x$.
3) $\pi$ ist transitiv: $x \,\pi\, y$, $y \,\pi\, z \Rightarrow x^{-1}y \in H$, $y^{-1}z \in H \Rightarrow (x^{-1}y)(y^{-1}z) = x^{-1}z \in H \Rightarrow x \,\pi\, z$. □

**2.1.19 Anmerkung.** Analog gilt: durch $x \varrho y :\Leftrightarrow xy^{-1} \in H$ ist ebenfalls eine Äquivalenzrelation auf $G$ definiert.

**2.1.20 Definition (Komplexprodukt).** Sei $(G, \cdot, e, ^{-1})$ Gruppe, $A, B \subseteq G$. Dann heißt $AB := \{ab \mid a \in A, b \in B\}$ das *Komplexprodukt* von $A$ und $B$.
Spezialfälle: $A = \{a\}$: $AB =: aB = \{ab \mid b \in B\}$, $B = \{b\}$: $AB =: Ab = \{ab \mid a \in A\}$.
Für eine Untergruppe $H$ von $G$ heißt $aH$ eine *Linksnebenklasse* von $G$ nach $H$ und $Ha$ eine *Rechtsnebenklasse* von $G$ nach $H$ ($a \in G$ fest, aber beliebig).

**2.1.21 Lemma.** *Sei $G$ Gruppe, $H \subseteq G$, $a \in G$.*
*Dann gilt für alle $x \in G$: $ax \in aH \Leftrightarrow x \in H$.*
*Weiters gilt für alle $y \in G$: $y \in aH \Leftrightarrow a^{-1}y \in H$.*

*Beweis.* Wenn $x \in H$ ist, dann ist (nach Definition von $aH$) $ax \in aH$. Wenn umgekehrt $ax \in aH$ ist, muss $ax = ah$ für ein $h \in H$ gelten; durch Multiplikation mit $a^{-1}$ (oder: weil die Gruppenmultiplikation regulär ist) erhalten wir $x = h \in H$.
Für die zweite Folgerung schreiben wir $y = aa^{-1}y = ax$ mit $x := a^{-1}y$.
Dann gilt $y \in aH \Leftrightarrow ax \in aH \Leftrightarrow x \in H \Leftrightarrow a^{-1}y \in H$. □

**2.1.22 Satz.** *Seien $\pi, \varrho$ die oben definierten Äquivalenzrelationen. Dann gilt für alle $a \in G$: $[a]_\pi = aH$ (also $b \,\pi\, a \Leftrightarrow b \in aH$) und $[a]_\varrho = Ha$.*

*Beweis.* $b \in [a]_\pi \Leftrightarrow a \,\pi\, b \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH$.

Der Beweis von $[a]_\varrho = Ha$ verläuft analog. □

**2.1.23 Folgerung.** $\{aH \mid a \in G\}$ ist eine Klasseneinteilung von $G$, genannt *Linksnebenklassenzerlegung* von $G$ nach $H$. Entsprechend nennt man $\{Ha \mid a \in G\}$ die *Rechtsnebenklassenzerlegung* von $G$ nach $H$.

**2.1.24 Beispiel.** $G = S_3 = \{(1), (123), (132), (12), (23), (13)\}$, $H = \{(1), (23)\}$.

$$\begin{array}{ll} (1)H{=}H & H(1){=}H \\ (123)H{=}\{(123), (12)\} & H(123){=}\{(123), (13)\} \\ (132)H{=}\{(132), (13)\} & H(132){=}\{(132), (12)\} \end{array}$$

Im allgemeinen gilt also $Ha \neq aH$! Für $a = e$ gilt jedoch stets $He = eH = H$. In abelschen Gruppen gilt $Ha = aH$ für alle $a \in G$.

**2.1.25 Satz.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, $H$ eine Untergruppe, $a, b \in G$, dann ist durch*

$$i : \begin{cases} aH \to bH \\ ax \mapsto bx \end{cases}$$

*eine bijektive Abbildung definiert.*

*Beweis.* 1) $i$ ist wohldefiniert: $ax_1 = ax_2 \Rightarrow x_1 = x_2$.
2) $i$ ist injektiv: $i(ax_1) = i(ax_2) \Rightarrow bx_1 = bx_2 \Rightarrow x_1 = x_2$.
3) $i$ ist surjektiv: jedes $bx \in bH$ ist Bild von $ax \in aH$. □

**2.1.26 Folgerung.** $\forall a, b \in G : |aH| = |bH| = |H|$. (Analog: $\forall a \in G : |Ha| = |H|$.)

**2.1.27 Satz.** *Durch $aH \mapsto Ha^{-1}$, $a \in G$, ist eine bijektive Abbildung $\varphi$ von der Linksnebenklassenzerlegung auf die Rechtsnebenklassenzerlegung von $G$ nach $H$ definiert.*

*Beweis.* 1) Es gilt: $Ha^{-1} = H^{-1}a^{-1} = (aH)^{-1}$. Daraus folgt die Wohldefiniertheit von $\varphi$.
2) $\varphi$ ist surjektiv: $\forall a \in G : \varphi(a^{-1}H) = Ha$.
3) $\varphi$ ist injektiv: $\varphi(aH) = \varphi(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow (aH)^{-1} = (bH)^{-1} \Rightarrow ((aH)^{-1})^{-1} = ((bH)^{-1})^{-1} \Rightarrow aH = bH$. □

**2.1.28 Definition.** Die Anzahl aller verschiedenen Linksnebenklassen (Rechtsnebenklassen) von $G$ nach $H$ heißt der *Index von $H$ in $G$*, in Zeichen: $[G : H] := |\{aH \mid a \in G\}| = |\{Ha \mid a \in G\}|$.

**2.1.29 Satz (von Lagrange).** *Sei $(G, \cdot, e, ^{-1})$ eine endliche Gruppe, $H$ eine Untergruppe, dann gilt:*

$$[G : H] \cdot |H| = |G|.$$

**2.1.30 Anmerkung.** Der Satz von Lagrange gilt auch für unendliche Gruppen.

**2.1.31 Folgerung.** a) $|H|$ teilt $|G|$.

b) $x \in G \Rightarrow \mathrm{o}(x) = |\{x^n \mid n \in \mathbb{Z}\}| = |\langle x \rangle|$ teilt $|G|$. „Die Ordnung jedes Elements ist Teiler der Gruppenordnung."

c) $|G| = p$ Primzahl, $H$ Untergruppe $\Rightarrow H = \{e\}$ oder $H = G$. Für $x \in G$, $x \neq e$, ist daher $\langle x \rangle = G$, also $G$ zyklisch.

## 2.2 Isomorphismen und Homomorphismen

**2.2.1 Definition.** Seien $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ und $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$. Eine Abbildung $f : A \to A^*$ heißt *Homomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}^*$ :$\Leftrightarrow$

1) für $i \in I$ mit $n_i > 0$ gilt $\forall x_1, \ldots, x_{n_i} \in A : f(\omega_i x_1 \ldots x_{n_i}) = \omega_i^* f(x_1) \ldots f(x_{n_i})$,

2) für $i \in I$ mit $n_i = 0$ gilt $f(\omega_i) = \omega_i^*$.

**2.2.2 Lemma.** *Seien* $(G, \cdot, e, ^{-1})$ *und* $(H, \cdot, e, ^{-1})$ *Gruppen,* $f : G \to H$*. Dann gilt:* $f$ *ist Homomorphismus von* $(G, \cdot, e, ^{-1})$ *nach* $(H, \cdot, e, ^{-1}) \Leftrightarrow f$ *ist Homomorphismus von* $(G, \cdot)$ *nach* $(H, \cdot)$*.*

*Beweis.* $\Rightarrow$: trivial.
$\Leftarrow$: Voraussetzung: $f(xy) = f(x)f(y)$. Zu zeigen: $f(e) = e$, $f(x^{-1}) = (f(x))^{-1}$.
$ee = e \Rightarrow f(e)f(e) = f(e) \Rightarrow f(e) = e$.
$xx^{-1} = e \Rightarrow f(x)f(x^{-1}) = f(e) = e = f(x)(f(x))^{-1} \Rightarrow f(x^{-1}) = (f(x))^{-1}$. □

**2.2.3 Folgerung.** 1) Seien $\mathfrak{V} = (V, +, 0, -, K)$ und $\mathfrak{W} = (W, +, 0, -, K)$ Vektorräume über demselben Körper $K$ und $f : V \to W$. Dann gilt: $f$ ist Homomorphismus von $\mathfrak{V}$ nach $\mathfrak{W} \Leftrightarrow$ $f$ ist lineare Abbildung, d.h., $\forall x, y \in V : f(x + y) = f(x) + f(y)$, $\forall \lambda \in K, x \in V : f(\lambda x) = \lambda f(x)$.
2) Seien $(R, +, 0, -, \cdot)$ und $(S, +, 0, -, \cdot)$ Ringe, $f : R \to S$, dann gilt: $f$ ist Homomorphismus von $(R, +, 0, -, \cdot)$ nach $(S, +, 0, -, \cdot) \Leftrightarrow f$ ist Homomorphismus von $(R, +, \cdot)$ nach $(S, +, \cdot)$.

**2.2.4 Definition.** Seien $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ und $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$ und $f : A \to A^*$ ein Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{A}^*$. $f$ heißt

1) *Isomorphismus*, falls $f$ bijektiv (in diesem Fall sagt man: $\mathfrak{A}$ ist *isomorph* zu $\mathfrak{A}^*$, in Zeichen: $\mathfrak{A} \cong \mathfrak{A}^*$),

2) *Endomorphismus*, falls $\mathfrak{A} = \mathfrak{A}^*$,

3) *Automorphismus*, falls $\mathfrak{A} = \mathfrak{A}^*$ und $f$ Isomorphismus,

4) *Epimorphismus*, falls $f$ surjektiv (in diesem Fall heißt $\mathfrak{A}^*$ *homomorphes Bild* von $\mathfrak{A}$),

5) *Monomorphismus*, falls $f$ injektiv (in diesem Fall heißt $\mathfrak{A}$ *isomorph eingebettet in* $\mathfrak{A}^*$).

**2.2.5 Satz.** a) *Seien* $\mathfrak{A}$, $\mathfrak{A}^*$, $\mathfrak{A}^{**}$ *Algebren vom selben Typ,* $f$ *Homomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}^*$*,* $g$ *Homomorphismus von* $\mathfrak{A}^*$ *nach* $\mathfrak{A}^{**}$*. Dann ist* $g \circ f$ *Homomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}^{**}$*. Sind* $f, g$ *beide Isomorphismen, so ist auch* $g \circ f$ *ein Isomorphismus.*

b) *Ist* $f$ *Isomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}^*$*, so ist* $f^{-1}$ *Isomorphismus von* $\mathfrak{A}^*$ *nach* $\mathfrak{A}$*.*

c) *Sind* $\mathfrak{A} = (A, (\omega_i)_{i\in I})$, $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i\in I})$ *zwei Algebren,* $f$ *ein Homomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{A}^*$ *und* $\mathfrak{T} = (T, (\omega_i)_{i\in I})$ *eine Unteralgebra von* $\mathfrak{A}$*, so ist das Bild* $f(T) := \{f(x) \mid x \in T\}$ *eine Unteralgebra von* $\mathfrak{A}^*$*. Kurz: Bilder von Unteralgebren unter Homomorphismen sind wieder Unteralgebren.*

d) *Bezeichnungen wie in* c)*. Sei jetzt* $\mathfrak{U} = (U, (\omega_i^*)_{i\in I})$ *eine Unteralgebra von* $\mathfrak{A}^*$*. Dann ist das (vollständige) Urbild* $f^{-1}(U) := \{x \in A \mid f(x) \in U\}$ *eine Unteralgebra von* $\mathfrak{A}$*. Kurz: (vollständige) Urbilder von Unteralgebren unter Homomorphismen sind wieder Unteralgebren.*

*Beweis.* Übungsbeispiele 41 und 43. □

## 2.2.A Homomorphismen und Gesetze

**2.2.6 Satz.** *Sei $(H,\cdot)$ eine Halbgruppe, $(H^*,\cdot)$ ein Gruppoid und $f: H \to H^*$ ein Homomorphismus. Dann ist die Unteralgebra $(f(H),\cdot)$ von $(H^*,\cdot)$ eine Halbgruppe.*

*Beweis.* Seien $x,y,z \in f(H)$. Dann gibt es $a,b,c \in H$ mit $f(a)=x$, $f(b)=y$ und $f(c)=z$. Da $(H,\cdot)$ Halbgruppe, gilt $a(bc)=(ab)c$ und damit $f(a)(f(b)f(c)) = (f(a)f(b))f(c)$, also $x(yz)=(xy)z$. □

Allgemeiner gilt:

**2.2.7 Satz.** *Seien $\mathfrak{A}=(A,(\omega_i)_{i\in I})$ und $\mathfrak{A}^*=(A^*,(\omega_i^*)_{i\in I})$ Algebren vom selben Typ, $f: A \to A^*$ ein Epimorphismus (d.h., $\mathfrak{A}^*$ ist homomorphes Bild von $\mathfrak{A}$). Gilt mit geeigneten Termen $t_1,t_2$ in $\mathfrak{A}$ eine Gleichung (ein Gesetz) $t_1 \approx t_2$, d.h.*

$$\forall a,b,c,\ldots:\ t_1(a,b,c,\ldots) = t_2(a,b,c,\ldots),$$

*so ist das Gesetz $t_1 \approx t_2$ auch in $\mathfrak{A}^*$ gültig.*

*Beweis.* Terme sind aus endlich vielen Variablen und Operationssymbolen (für $A$ bzw. $A^*$) aufgebaut. Durch Induktion nach dem Aufbau von Termen zeigt man, dass für alle Terme $t$ gilt:

$$t(f(a),f(b),f(c),\ldots) = f(t(a,b,c,\ldots)).$$

Daraus folgt

$$t_1(f(a),f(b),f(c),\ldots) = f(t_1(a,b,c,\ldots)) = f(t_2(a,b,c,\ldots)) = t_2(f(a),f(b),f(c),\ldots).$$

Aus der Surjektivität von $f$ folgt, das die Gleichung $t_1 \approx t_2$ auch in $\mathfrak{A}^*$ gilt. □

**2.2.8 Anmerkung.** Ist $(A,(\omega_i)_{i\in I})$ Algebra, so nennt man $(\omega_i)_{i\in I}$ die *fundamentalen* Operationen, Terme dagegen *abgeleitete* Operationen.

Interpretation des letzten Satzes: Jedes homomorphe Bild einer Halbgruppe ist eine Halbgruppe. Analog zeigt man: Jedes homomorphe Bild
1) einer (abelschen) Gruppe ist eine (abelsche) Gruppe,
2) eines (kommutativen) Ringes ist ein (kommutativer) Ring,
3) eines Ringes mit Einselement ist ein Ring mit Einselement,
4) eines Verbandes ist ein Verband[3],
5) einer Booleschen Algebra ist eine Boolesche Algebra,
6) eines Vektorraumes über $K$ ist ein Vektorraum über $K$.

Sei $(A,\cdot)$, $A=\{a_1,\ldots,a_n\}$, ein Gruppoid, $(A^*,\circ)$ ein weiteres Gruppoid mit $|A^*|=n$, $f: A \to A^*$ Isomorphismus, $A^*=\{a_1^*,\ldots,a_n^*\}$ mit $a_i^*=f(a_i)$, $1\le i\le n$. Die Operationstafeln der beiden Algebren sehen dann so aus:

| $\cdot$ | $a_1$ | $\ldots$ | $a_n$ |
|---|---|---|---|
| $a_1$ | $a_1a_1$ | $\ldots$ | $a_1a_n$ |
| $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| $a_n$ | $a_na_1$ | $\ldots$ | $a_na_n$ |

| $\circ$ | $a_1^*$ | $\ldots$ | $a_n^*$ |
|---|---|---|---|
| $a_1^*$ | $a_1^*\circ a_1^*$ | $\ldots$ | $a_1^*\circ a_n^*$ |
| $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| $a_n^*$ | $a_n^*\circ a_1^*$ | $\ldots$ | $a_n^*\circ a_n^*$ |

[3]Verbände und Boolesche Algebren werden wir in einem späteren Kapitel als algebraische Strukturen kennen lernen.

Ist (links) $a_i a_j = a_k$ so ist (rechts) $a_i^* \circ a_j^* = a_k^*$. Vom Standpunkt der Algebra ist daher ein Isomorphismus lediglich eine „Umbezeichnung“. Isomorphe Algebren sind „als gleich zu betrachten“.

*Algebraische Eigenschaften* sind solche, die bei Isomorphismen erhalten bleiben. So sind etwa alle Gesetze algebraische Eigenschaften, da sie nach obiger Anmerkung sogar bei Epimorphismen erhalten bleiben. Da Umkehrabbildungen von Isomorphismen ebenfalls Isomorphismen sind, gilt: Isomorphe Algebren erfüllen die gleichen Gesetze.

Oft ist es möglich, algebraische Strukturen „bis auf Isomorphie“ zu charakterisieren. So sind z.B. alle endlich-dimensionalen Vektorräume über $K$ bis auf Isomorphie gegeben durch $K^n$, $n \in \mathbb{N}_0$ (mit den üblichen Operationen). Analoge Aussagen werden wir für endliche Körper und endliche Boolesche Algebren kennenlernen. Ein weiteres Ergebnis in diese Richtung ist der folgende

**2.2.9 Satz (Darstellungssatz von Cayley).** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, dann ist $G$ isomorph zu einer Untergruppe der symmetrischen Gruppe $(S_G, \circ, \mathrm{id}_G, ^{-1})$.*
Kurz: *Jede Gruppe ist isomorph zu einer Permutationsgruppe.*

*Beweis.* Wir konstruieren eine Einbettung (Monomorphismus) $\pi : G \to S_G$, $a \mapsto \pi_a$, auf folgende Weise:

$$\forall g \in G : \pi_a(g) := ag.$$

1) $\pi_a \in S_G$, d.h., $\pi_a$ ist injektiv und surjektiv (injektiv: $\pi_a(g_1) = \pi_a(g_2) \Rightarrow ag_1 = ag_2 \Rightarrow g_1 = g_2$; surjektiv: $h \in G \Rightarrow h = \pi_a(a^{-1}h)$).
2) $\pi$ ist injektiv: $\pi_{a_1} = \pi_{a_2} \Rightarrow \pi_{a_1}(e) = \pi_{a_2}(e) \Rightarrow a_1 e = a_2 e \Rightarrow a_1 = a_2$.
3) $\pi_{ab} = \pi_a \circ \pi_b$: $\pi_{ab}(g) = (ab)g = a(bg) = \pi_a(bg) = \pi_a(\pi_b(g)) = (\pi_a \circ \pi_b)(g)$. □

**2.2.10 Anmerkung.** Ein analoger Satz gilt auch für Monoide.

## 2.2.B Kongruenzrelationen und Faktoralgebren

**2.2.11 Definition.** Sei $\mathfrak{A} = (A, (\omega_i)_{i \in I})$ eine Algebra vom Typ $(n_i)_{i \in I}$; weiters sei $\pi$ Äquivalenzrelation auf $A$. $\pi$ heißt *Kongruenz(relation)* auf $\mathfrak{A} :\Leftrightarrow$
für alle $i \in I$ mit $n_i > 0$, $a_1, \ldots, a_{n_i}, b_1, \ldots, b_{n_i} \in A$ gilt:

$$a_1 \,\pi\, b_1, \ldots, a_{n_i} \,\pi\, b_{n_i} \Rightarrow \omega_i a_1 \ldots a_{n_i} \,\pi\, \omega_i b_1 \ldots b_{n_i}.$$

**2.2.12 Beispiel.** Sei $\mathfrak{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$ der Integritätsbereich der ganzen Zahlen und $n \in \mathbb{N}_0$ fest ($n$ heißt Modul). $\pi$ sei definiert durch:

$$a \,\pi\, b :\Leftrightarrow \exists c \in \mathbb{Z} : a - b = cn, \qquad a, b \in \mathbb{Z}.$$

Im folgenden schreiben wir — wie bereits in den Abschnitten 1.5 und 1.7 — $a \equiv b \bmod n$ anstelle von $a \,\pi\, b$. Es gilt: $\equiv \bmod n$ ist Kongruenzrelation, denn:
1) $\equiv \bmod n$ ist Äquivalenzrelation: $a \equiv a \bmod n$ wegen $a - a = 0 = 0n$; $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow b - a = (-c)n \Rightarrow b \equiv a \bmod n$; $a \equiv b \bmod n$ und $b \equiv c \bmod n \Rightarrow a - b = d_1 n$ und $b - c = d_2 n \Rightarrow a - c = (d_1 + d_2)n \Rightarrow a \equiv c \bmod n$.
2) Operation $+$: $a_1 \equiv b_1 \bmod n$ und $a_2 \equiv b_2 \bmod n \Rightarrow a_1 - b_1 = c_1 n$ und $a_2 - b_2 = c_2 n \Rightarrow (a_1 + a_2) - (b_1 + b_2) = (c_1 + c_2)n \Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) \bmod n$.
3) Operation $-$: $a \equiv b \bmod n \Rightarrow a - b = cn \Rightarrow (-a) - (-b) = (-c)n \Rightarrow (-a) \equiv (-b) \bmod n$.
4) Operation $\cdot$: $a_1 \equiv b_1 \bmod n$ und $a_2 \equiv b_2 \bmod n \Rightarrow a_1 = b_1 + c_1 n$ und $a_2 = b_2 + c_2 n \Rightarrow a_1 a_2 = b_1 b_2 + (b_1 c_2 + b_2 c_1 + c_1 c_2 n)n \Rightarrow a_1 a_2 \equiv b_1 b_2 \bmod n$.

Zugehörige Klasseneinteilung: Es ist $[a] = \{a + kn \mid k \in \mathbb{Z}\}$. Für $n = 0$ gilt $[a] = \{a\}$ für alle $a \in \mathbb{Z}$ ($\equiv \bmod n$ ist dann die Gleichheitsrelation). Für $n \neq 0$ gilt: $\mathbb{Z}_n := \mathbb{Z}/\equiv \bmod n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], \ldots, [n-1]\}$. Für die Äquivalenzklasse $[a]$ wird in diesem Zusammenhang oft auch die Bezeichnung $\bar{a}$ verwendet.

**2.2.13 Satz.** *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra und $\pi$ eine Kongruenz auf $\mathfrak{A}$. Dann sind durch*

$$\omega_i^*[a_1]_\pi \ldots [a_{n_i}]_\pi := [\omega_i a_1 \ldots a_{n_i}]_\pi, \quad n_i > 0,\ a_1, \ldots, a_{n_i} \in A,$$
$$\omega_i^* := [\omega_i]_\pi, \quad n_i = 0,$$

*Operationen auf der Quotientenmenge $A/\pi$ definiert.*

*Beweis.* Die Operationen sind wohldefiniert:[4]

$$\left.\begin{array}{c} [a_1]_\pi = [b_1]_\pi \\ \vdots \\ [a_{n_i}]_\pi = [b_{n_i}]_\pi \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a_1 \pi b_1 \\ \vdots \\ a_{n_i} \pi b_{n_i} \end{array}\right\} \Rightarrow \omega_i a_1 \ldots a_{n_i} \pi \omega_i b_1 \ldots b_{n_i}.$$

Daher ist $[\omega_i a_1 \ldots a_{n_i}]_\pi = [\omega_i b_1 \ldots b_{n_i}]_\pi$. □

**2.2.14 Definition.** Die so erhaltene Algebra $\mathfrak{A}/\pi := (A/\pi, (\omega_i^*)_{i\in I})$ heißt *Faktoralgebra* von $\mathfrak{A}$ nach der Kongruenz $\pi$. Oft werden die Operationen $\omega_i^*$ der Faktoralgebra $\mathfrak{A}/\pi$ wieder mit $\omega_i$ bezeichnet.

**2.2.15 Beispiel.** $\mathfrak{A} = (\mathbb{Z}, +, 0, -, \cdot, 1)$, $\pi = (\equiv \bmod n)$. Die Faktoralgebra $\mathfrak{A}/\pi$ ist dann gegeben durch $(\mathbb{Z}_n, +^*, 0^*, -^*, \cdot^*, 1^*)$ mit $[a] +^* [b] = [a+b]$, $0^* = [0]$, $-^*[a] = [-a]$, $[a] \cdot^* [b] = [ab]$, $1^* = [1]$ (d.h., man rechnet mit den Repräsentanten der Klassen). Im folgenden wird „$^*$“ bei den Operationen weggelassen. Es gilt (siehe folgender Satz): $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ ist ein kommutativer Ring mit Einselement, genannt der *Restklassenring modulo $n$*.

**2.2.16 Satz.** *Sei $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ eine Algebra, $\pi$ eine Kongruenz auf $\mathfrak{A}$. Dann ist die Abbildung*

$$\nu : \left\{\begin{array}{l} A \to A/\pi \\ a \mapsto [a]_\pi \end{array}\right.$$

*ein surjektiver Homomorphismus von $\mathfrak{A}$ auf $\mathfrak{A}/\pi$, der so genannte* natürliche Homomorphismus.

*Beweis.*

$$\nu(\omega_i a_1 \ldots a_{n_i}) = [\omega_i a_1 \ldots a_{n_i}]_\pi = \omega_i [a_1]_\pi \ldots [a_{n_i}]_\pi = \omega_i \nu(a_1) \ldots \nu(a_{n_i}), \quad n_i > 0,$$
$$\nu(\omega_i) = [\omega_i]_\pi = \omega_i, \quad n_i = 0.$$

□

[4] Was heißt es, dass eine Funktion wohldefiniert ist? Wenn wir eine Funktion $f$ auf einer Menge $X$ durch eine Rechenvorschrift (etwa einen Term) $t$ definieren, also $f(x) := t(x)$ setzen, dann bedeutet das Wort „wohldefiniert“ nur soviel, dass die Rechenvorschrift $t$ tatsächlich für jede Eingabe $x$ ein Resultat $t(x)$ ausgibt.
Wenn wir aber $f$ durch eine Formel

$$(*) \qquad f(t_1(x)) := t_2(x)$$

definieren, enthält diese „Definition“ implizit die Behauptung, dass es tatsächlich eine Funktion gibt, die jedem Element der Form $t_1(x)$ das Element $t_2(x)$ zuordnet. Notwendig und hinreichend für die Gültigkeit dieser Behauptung ist die Implikation

$$(**) \qquad \forall x, y\ (t_1(x) = t_1(y) \Rightarrow t_2(x) = t_2(y)).$$

Wenn wir also eine Funktion $f$ durch eine Vorschrift $(*)$ definieren, müssen wir uns immer erst vergewissern, dass $(**)$ erfüllt ist.

**2.2.17 Folgerung.** a) $\mathfrak{A}/\pi$ ist ein homomorphes Bild von $\mathfrak{A}$.

b) Jedes Gesetz, welches in $\mathfrak{A}$ gilt, gilt auch in $\mathfrak{A}/\pi$, insbesondere ist also

i) jede Faktoralgebra einer Halbgruppe eine Halbgruppe,

ii) jede Faktoralgebra einer (abelschen) Gruppe eine (abelsche) Gruppe,

iii) jede Faktoralgebra eines Vektorraumes ein Vektorraum (vgl. den Begriff „Quotientenraum“ aus der Linearen Algebra),

iv) jede Faktoralgebra eines (kommutativen) Ringes ein (kommutativer) Ring,

v) jede Faktoralgebra eines Ringes mit Einselement ein Ring mit Einselement,

vi) jede Faktoralgebra eines Verbandes ein Verband

**2.2.18 Anmerkung.** Eine Faktoralgebra eines Integritätsbereiches braucht kein Integritätsbereich zu sein, wie das Beispiel $(\mathbb{Z}_n, +, 0, -, \cdot, 1)$ zeigt (homomorphes Bild von $(\mathbb{Z}, +, 0, -, \cdot)$).

**2.2.19 Satz (Homomorphiesatz).** *Seien $\mathfrak{A} = (A, (\omega_i)_{i\in I})$ und $\mathfrak{A}^* = (A^*, (\omega_i^*)_{i\in I})$ Algebren vom selben Typ $(n_i)_{i\in I}$ und $f : A \to A^*$ ein Homomorphismus. Dann ist der Kern $\pi_f$ eine Kongruenz auf $\mathfrak{A}$, und es gibt* genau einen *injektiven Homomorphismus $g$ von $\mathfrak{A}/\pi_f$ nach $\mathfrak{A}^*$, sodass $f = g \circ \nu$ ($\nu$ ist die natürliche Abbildung).*

*Beweis.* 1) $\pi_f$ ist eine Äquivalenzrelation, und es gibt eine injektive Abbildung $g : A/\pi_f \to A^*$ mit $f = g \circ \nu$ (siehe 1.5.8).

2) $\pi_f$ ist Kongruenz: Sei $i \in I$, $n_i > 0$. Wir haben:

$$\left.\begin{array}{c} a_1\pi_f b_1 \\ \vdots \\ a_{n_i}\pi_f b_{n_i} \end{array}\right\} \Rightarrow \left\{\begin{array}{c} f(a_1) = f(b_1) \\ \vdots \\ f(a_{n_i}) = f(b_{n_i}) \end{array}\right\} \Rightarrow \omega_i^* f(a_1)\dots f(a_{n_i}) = \omega_i^* f(b_1)\dots f(b_{n_i})$$

$\Rightarrow f(\omega_i a_1 \dots a_{n_i}) = f(\omega_i b_1 \dots b_{n_i})$ ($f$ Homomorphismus!) $\Rightarrow \omega_i a_1 \dots a_{n_i}\ \pi_f\ \omega_i b_1 \dots b_{n_i}$. Die Eindeutigkeit von $g$ ist trivial: $g([a]_{\pi_f}) = g(\nu(a)) = (g \circ \nu)(a) = f(a)$.

3) $g$ ist ein Homomorphismus: Sei $i \in I$, $n_i > 0$, dann gilt:

$$\begin{aligned} &g(\omega_i[a_1]_{\pi_f} \dots [a_{n_i}]_{\pi_f}) = g([\omega_i a_1 \dots a_{n_i}]_{\pi_f}) = f(\omega_i a_1 \dots a_{n_i}) \\ &= \omega_i^* f(a_1) \dots f(a_{n_i}) = \omega_i^* g([a_1]_{\pi_f}) \dots g([a_{n_i}]_{\pi_f}). \end{aligned}$$

Analog gilt für $n_i = 0$: $g(\omega_i) = g([\omega_i]_{\pi_f}) = f(\omega_i) = \omega_i^*$. □

**2.2.20 Folgerung.** 1) Für die Unteralgebra $(f(A), (\omega_i^*)_{i\in I})$ von $\mathfrak{A}^*$ gilt $(f(A), (\omega_i^*)_{i\in I}) \cong \mathfrak{A}/\pi_f$, also ist jedes homomorphe Bild einer Algebra isomorph zu einer Faktoralgebra.

2) Kongruenzrelationen und (surjektive) Homomorphismen sind im Wesentlichen das selbe. Das heißt:
i) Aus jeder Kongruenzrelation $\pi$ auf $(A, (\omega_i)_{i\in I})$ kann man in natürlicher Weise eine Algebra $(A/\pi, (\omega_i)_{i\in I})$ und einen surjektiven Homomorphismus $\nu_\pi : A \to A/\pi$ konstruieren.

ii) Aus jedem surjektiven Homomorphismus $f : A \to B$ kann man in natürlicher Weise eine Kongruenzrelation $\pi_f$ in der Algebra $(A, (\omega_i)_{i\in I})$ konstruieren.

iii) Diese beiden Konstruktionen sind invers zu einander: Ausgehend von einer Kongruenzrelation $\pi$ erhält man einen surjektiven Homomorphismus $\nu_\pi$; die daraus konstruierte Kongruenzrelation $\pi_{\nu_\pi}$ ist genau $\pi$, und ausgehend von einem surjektiven Homomorphismus $f$ erhält man eine Kongruenzrelation $\pi_f$; der daraus konstruierte Homomorphismus $\nu_{\pi_f}$ ist im Wesentlichen das gleiche wie $f$.

**2.2.21 Anmerkung.** Die Gleichheitsrelation $\iota = \{(x,x) \mid x \in A\}$ und die Allrelation $\alpha = A \times A$ sind stets Kongruenzen auf $\mathfrak{A}$, genannt die *trivialen* Kongruenzen auf $\mathfrak{A}$. Es gilt: $\mathfrak{A}/\iota \cong \mathfrak{A}$ und $|\mathfrak{A}/\alpha| \leq 1$. $\mathfrak{A}/\iota$ und $\mathfrak{A}/\alpha$ sind die *trivialen* Faktoralgebren.

**2.2.22 Definition.** Eine Algebra $\mathfrak{A}$ heißt *einfach*[5], wenn sie nur die trivialen Kongruenzen besitzt.

**2.2.23 Anmerkung.** Die Algebra $\mathfrak{A}$ ist einfach genau dann, wenn sie nur *triviale* homomorphe Bilder hat (d.h., jeder Homomorphismus $h : A \to B$ ist entweder konstant oder injektiv).

### 2.2.C Kongruenzrelationen auf Gruppen

**2.2.24 Satz.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe und $\pi$ eine Äquivalenzrelation auf $G$. Dann gilt:*

a) *$\pi$ ist Kongruenz auf $(G, \cdot, e, ^{-1}) \Leftrightarrow$ $\pi$ ist Kongruenz auf $(G, \cdot)$.*

b) *Ist $\pi$ Kongruenz auf $(G, \cdot)$ und $[e]_\pi =: N$, dann gilt:*

i) *$N$ ist Untergruppe von $(G, \cdot, e, ^{-1})$.*

ii) *$xNx^{-1} = \{xnx^{-1} \mid n \in N\} \subseteq N$ für alle $x \in G$.*

iii) *$x\pi y \Leftrightarrow x^{-1}y \in N$ für alle $x, y \in G$ (d.h., $[x]_\pi = xN$ für alle $x \in G$).*

*Beweis.* a) $\Rightarrow$: trivial. $\Leftarrow$:

$$\left.\begin{matrix} x\pi y \\ x^{-1}\pi x^{-1} \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} e = xx^{-1}\pi yx^{-1} \\ y^{-1}\pi y^{-1} \end{matrix}\right\} \Rightarrow y^{-1}\pi y^{-1} yx^{-1} = x^{-1}.$$

b) i) $e \in N$ wegen $e\pi e$. $x, y \in N \Rightarrow x\pi e$ und $y\pi e \Rightarrow xy\pi ee = e \Rightarrow xy \in N$.
$x \in N \Rightarrow x\pi e \Rightarrow x^{-1}\pi e^{-1} = e \Rightarrow x^{-1} \in N$.
ii) $y \in N \Rightarrow y\pi e \Rightarrow xyx^{-1}\pi xex^{-1} = e \Rightarrow xyx^{-1} \in N$.
iii) $\Rightarrow$: $x\pi y \Rightarrow e = x^{-1}x\pi x^{-1}y \Rightarrow x^{-1}y \in N$.
$\Leftarrow$: $x^{-1}y \in N \Rightarrow x^{-1}y\pi e \Rightarrow y = xx^{-1}y\pi xe = x$. □

**2.2.25 Lemma.** *Sei $(G, \cdot, e, ^{-1})$ Gruppe und $x \in G$. Dann ist die Abbildung*[6]

$$\varphi_x : \left\{\begin{matrix} G \to G \\ g \mapsto xgx^{-1} \end{matrix}\right.$$

*ein Automorphismus von $(G, \cdot, e, ^{-1})$, genannt ein* innerer *Automorphismus von $G$. Wir nennen diese Abbildung* Konjugation *mit $x$.*

*Beweis.* Übungsbeispiel 45. □

**2.2.26 Anmerkung.** Die Eigenschaft ii) in obigem Satz ist dann gleichbedeutend mit: $\varphi_x(N) \subseteq N$ für alle $x \in G$.

[5] englisch: *simple*

[6] Statt $\varphi_{x^{-1}}(g)$ schreibt man oft $g^x$. In dieser Schreibweise gilt dann: $(g^x)^y = g^{xy}$.

**2.2.27 Definition.** Zwei Elemente $g, h \in G$ heißen „konjugiert“ zu einander, wenn es ein $x$ mit $xgx^{-1} = h$ gibt; Konjugiertheit ist offenbar eine Äquivalenzrelation.

**2.2.28 Definition.** Sei $N$ eine Untergruppe von $(G, \cdot, e, ^{-1})$, dann heißt $N$ eine *invariante* Untergruppe oder ein *Normalteiler*[7] von $G$:$\Leftrightarrow xNx^{-1} \subseteq N$ für alle $x \in G$.
Statt „$U$ ist Untergruppe von $G$“ schreiben wir $U \leq G$; die Notation $N \lhd G$ bedeutet, dass $N$ Normalteiler von $G$ ist.

**2.2.29 Anmerkung.** In einer abelschen Gruppe ist jede Untergruppe Normalteiler. Für nicht abelsche Gruppen ist dies nicht der Fall. Z.B. gibt es Untergruppen der $S_3$, die nicht Normalteiler sind, nämlich: $\{(1), (12)\}$, $\{(1), (13)\}$ und $\{(1), (23)\}$.

**2.2.30 Lemma.** *Für eine Untergruppe $N$ einer Gruppe $G$ sind folgende Aussagen äquivalent:*

a) *$N$ ist Normalteiler von $G$.*

b) $\forall x \in G : \varphi_x(N) = N$.

c) $\forall x \in G : xNx^{-1} = N$.

d) $\forall x \in G : Nx = xN$, *d.h., Rechtsnebenklasse = Linksnebenklasse.*

*Beweis.* a) $\Rightarrow$ b): $N$ Normalteiler $\Rightarrow \forall x \in G : xNx^{-1} \subseteq N \Rightarrow \forall x \in G : x^{-1}Nx \subseteq N \Rightarrow$
$\forall x \in G : N = xx^{-1}Nxx^{-1} \subseteq xNx^{-1} \Rightarrow \forall x \in G : \varphi_x(N) = xNx^{-1} = N$. □

b) $\Rightarrow$ a) und b) $\Leftrightarrow$ c) sind trivial.

c) $\Leftrightarrow$ d): $xNx^{-1} = N \Rightarrow xN = xNx^{-1}x = Nx \Rightarrow xNx^{-1} = Nxx^{-1} = N$ für alle $x \in G$.

**2.2.31 Satz.** *Sei $(G, \cdot, e, ^{-1})$ eine Gruppe, $N \lhd G$ und $\pi$ durch $x\pi y :\Leftrightarrow x^{-1}y \in N$, $x, y \in G$ definiert. Dann ist $\pi$ eine Kongruenzrelation auf $G$ mit $[e]_\pi = N$.*

*Beweis.* $\pi$ ist eine Äquivalenzrelation und $[x]_\pi = xN = Nx$. $\pi$ ist Kongruenz:

$$\left.\begin{array}{l} x_1\pi y_1 \\ x_2\pi y_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x_1 = y_1n_1 \text{ mit } n_1 \in N \text{ (da } x_1 \in y_1N) \\ x_2 = n_2y_2 \text{ mit } n_2 \in N \text{ (da } x_2 \in Ny_2) \end{array}\right\} \Rightarrow$$
$$\Rightarrow x_1x_2 = y_1n_1n_2y_2 \in y_1Ny_2 = y_1y_2N \Rightarrow x_1x_2\pi y_1y_2.$$

Weiters gilt $[e]_\pi = eN = N$. □

**2.2.32 Anmerkung.** Für einen Normalteiler $N$ gilt $x^{-1}y \in N \Leftrightarrow xy^{-1} \in N$:

$$x^{-1}y \in N \Leftrightarrow y \in xN = Nx \Leftrightarrow yx^{-1} \in N \Leftrightarrow xy^{-1} = (yx^{-1})^{-1} \in N.$$

**2.2.33 Satz.** *Durch $\pi \mapsto [e]_\pi$ ist eine bijektive Abbildung von der Menge der Kongruenzen auf der Gruppe $G$ auf die Menge aller Normalteiler von $G$ definiert. Die Umkehrabbildung ist gegeben durch $N \mapsto \pi$ mit $x\pi y :\Leftrightarrow x^{-1}y \in N$.*

*Beweis.* Die beiden Zuordnungen sind invers: $\pi \mapsto [e]_\pi =: N \mapsto \pi_1$ mit $x\pi_1 y :\Leftrightarrow x^{-1}y \in N \Leftrightarrow x\pi y$, d.h., $\pi = \pi_1$. Umkehrung: $N \mapsto \pi \mapsto [e]_\pi = N$. □

[7] englisch: *normal subgroup*

Um — bis auf Isomorphie — alle homomorphen Bilder einer Gruppe $G$ zu finden, kann man daher alle Normalteiler $N$ von $G$ bestimmen und mit den entsprechenden Kongruenzen $\pi$ die Faktoralgebren $G/\pi$ bilden. Entspricht dem Normalteiler $N$ die Kongruenz $\pi$, so schreiben wir $G/N := G/\pi = \{xN \mid x \in G\}$. Eine solche Faktoralgebra heißt *Faktorgruppe* von $G$.

In der Faktorgruppe $G/N$ wird wie folgt gerechnet:

$$(xN)(yN) = (xy)N, \quad eN = N \text{ ist Einselement}, \quad (xN)^{-1} = x^{-1}N.$$

Den trivialen Kongruenzen $\iota = \{(x,x) \mid x \in G\}$ und $\alpha = G \times G$ entsprechen die so genannten *trivialen* Normalteiler $\{e\}$ und $G$. Daher gilt: $G$ ist einfach $\Leftrightarrow$ $G$ hat nur die beiden trivialen Normalteiler.

**2.2.34 Beispiele.** 1) Jede zyklische Gruppe $G = \langle x \rangle$ mit $\mathrm{o}(x) = p$ (Primzahl) ist einfach (Satz von Lagrange). Umgekehrt gilt: Jede einfache abelsche Gruppe $G$ mit $|G| > 1$ ist zyklisch und von Primzahlordnung (Übungsbeispiel 47).

2) Die alternierende Gruppe $A_n = \{\pi \in S_n \mid \mathrm{sign}(\pi) = 1\}$ ist einfach für $n \neq 4$. (Wichtig für die Theorie der algebraischen Gleichungen.)

3) Die symmetrische Gruppe $S_n$ ist für $n \geq 3$ nicht einfach, denn es gilt: $A_n \lhd S_n$. Die Links(Rechts)nebenklassenzerlegung von $S_n$ nach $A_n$ ist gegeben durch $\{A_n, S_n \setminus A_n\}$, und es ist $[S_n : A_n] = 2$ (Index von $A_n$ in $S_n$).

**2.2.35 Satz.** *Sei $G$ Gruppe, $U$ Untergruppe mit $[G : U] = 2$. Dann gilt $U \lhd G$.*

*Beweis.* $x \in U \Rightarrow xU = Ux = U$. $x \notin U \Rightarrow xU = Ux = G \setminus U$. □

**2.2.36 Anmerkung.** Auch für Vektorräume gilt ein ähnliches Ergebnis wie für Gruppen: Durch $\pi \mapsto [0]_\pi$ ist eine umkehrbar eindeutige Zuordnung von der Menge aller Kongruenzrelationen des Vektorraumes $(V, +, 0, -, K)$ auf die Menge aller Unterräume von $V$ definiert (Beweis wie bei Gruppen).

Ist $U$ Unterraum von $V$, so ist $V/U = \{x + U \mid x \in V\}$ (*Faktorraum*) mit den Operationen $(x + U) + (y + U) = (x + y) + U$, $0 + U = U$ (neutrales Element), $-(x + U) = (-x) + U$, $\lambda(x + U) = (\lambda x) + U$, $x, y \in V$, $\lambda \in K$.

**2.2.37 Anmerkung.** Wir haben für eine beliebige Abbildung $f : A \to B$ den *Kern* von $f$ als die von $f$ induzierte Äquivalenzrelation $\sim_f := \{(x,y) \mid f(x) = f(y)\}$ definiert.

Wenn $f : G \to H$ aber ein Gruppenhomomorphimus ist, mit $N_f := f^{-1}(e)$, dann wissen wir, dass die durch $f$ induzierte Partition genau die Nebenklassenzerlegung von $G$ modulo $N_f$ ist; es gilt nämlich

$$x \sim_f y \Leftrightarrow x^{-1}y \in N_f.$$

Da also $N_f$ (zusammen mit den Gruppenoperationen) den Kern $\sim_f$ von $f$ definiert, nennt man auch meistens die Menge $N_f$ selbst den Kern von $f$; statt $N_f$ schreibt man oft $\ker(f)$. Dies ist einerseits praktisch, weil Normalteiler (als Teilmengen von $G$) einfachere Objekte sind als Kongruenzrelationen (als Teilmengen von $G \times G$), ist aber andererseits eben nur auf Gruppen (somit auch auf Ringe und Vektorräume) anwendbar, nicht aber auf andere algebraische Strukturen (wie z.B. Verbände).

In dieser Notation lässt sich der Homomorphiesatz also so schreiben:

**2.2.38 Satz.** *Seien $G$, $H$ Gruppen, $f : G \to H$ ein Epimorphismus. Sei $N$ der Kern von $f$, und sei $\nu : G \to G/N$ die kanonische Abbildung $a \mapsto aN$.*
*Dann gibt es einen eindeutig bestimmten Isomorphismus $g : G/N \to H$ mit $g \circ \nu = f$. Für jedes $y \in H$ ist $f^{-1}(y) \in G/N$ (d.h., Nebenklasse von $N$ in $G$), und $g$ bildet diese Nebenklasse auf $y$ ab.*

## 2.2.D Kongruenzrelationen auf Ringen

**2.2.39 Definition.** Sei $(R, +, 0, -, \cdot)$ ein Ring und $I$ Unterring von $R$. Dann heißt $I$
- ein *Linksideal* von $R :\Leftrightarrow \forall r \in R : rI := \{ri \mid i \in I\} \subseteq I$,
- ein *Rechtsideal* von $R :\Leftrightarrow \forall r \in R : Ir := \{ir \mid i \in I\} \subseteq I$,
- ein *Ideal* von $R$ (in Zeichen: $I \lhd R$) $:\Leftrightarrow \forall r \in R : rI \subseteq I$ und $Ir \subseteq I$.

**2.2.40 Beispiele.** 1) $\{0\}$ und $R$ sind stets Ideale von $R$, die so genannten *trivialen* Ideale.
2) In $(\mathbb{Z}, +, 0, -, \cdot)$ ist $\{nk \mid k \in \mathbb{Z}\}$, $n \in \mathbb{Z}$, ein Ideal. Dies sind bereits alle Ideale in $\mathbb{Z}$ (Beweis siehe spätere Abschnitte 5.3 und 5.4).

**2.2.41 Lemma.** *Sei $(R, +, 0, -, \cdot, 1)$ ein Ring mit Einselement und $I$ ein Ideal von $R$. Dann gilt: $1 \in I \Leftrightarrow I = R$.*

*Beweis.* trivial. □

**2.2.42 Satz.** *Jeder Körper hat nur die trivialen Ideale.*

*Beweis.* Sei $I$ Ideal des Körpers $(K, +, 0, -, \cdot, 1)$ und $I \neq \{0\}$. Dann gibt es $x \in I$ mit $x \neq 0$ und wegen $1 = x^{-1}x \in x^{-1}I \subseteq I$ ist $I = K$. □

**2.2.43 Satz.** *Sei $(R, +, 0, -, \cdot, 1)$ ein kommutativer Ring mit Einselement, der nur die trivialen Ideale besitzt. Dann ist $R$ ein Körper oder $R = \{0\}$.*

*Beweis.* $x \in R$, $x \neq 0 \Rightarrow xR = \{xr \mid r \in R\}$ ist ein Ideal von $R$ (analog zu $\mathbb{Z}$) mit $x = x1 \in xR \Rightarrow xR \neq \{0\} \Rightarrow xR = R \Rightarrow \exists r \in R : 1 = xr \Rightarrow x$ besitzt ein Inverses. □

**2.2.44 Folgerung.** Ein kommutativer Ring $R$ mit Einselement und $R \neq \{0\}$ ist ein Körper $\Leftrightarrow R$ besitzt nur die trivialen Ideale.

**2.2.45 Satz.** *Sei $(R, +, 0, -, \cdot)$ ein Ring.*

a) *Ist $\pi$ eine Kongruenz auf $R$, dann ist $I := [0]_\pi$ ein Ideal von $R$, und es gilt: $R/\pi = R/I = \{x + I \mid x \in R\}$.*

b) *Ist $I$ Ideal von $R$ und $\pi$ definiert durch $x\pi y :\Leftrightarrow y - x \in I$, $x, y \in R$, dann ist $\pi$ Kongruenz auf $R$ und $[0]_\pi = I$.*

c) *$\pi \mapsto [0]_\pi$ definiert eine bijektive Abbildung von der Menge aller Kongruenzen auf $R$ auf die Menge aller Ideale von $R$. Die Umkehrabbildung ist definiert durch $I \mapsto \pi$ gemäß* b).

*Beweis.* a) $\pi$ ist insbesondere Kongruenz der Gruppe $(R, +)$, also ist $I = [0]_\pi$ ein Normalteiler von $(R, +)$. Weiters gilt: $i \in I$ und $r \in R \Rightarrow i\pi 0$ und $r\pi r \Rightarrow ir\pi 0r = 0$ und $ri\pi r0 = 0$ $\Rightarrow ir, ri \in I$. Damit ist $I$ ein Ideal.

b) $x_1\pi y_1$ und $x_2\pi y_2 \Rightarrow y_1 = x_1 + i_1$ und $y_2 = x_2 + i_2$, $i_1, i_2 \in I \Rightarrow y_1y_2 = x_1x_2 + i$ mit $i = x_1i_2 + i_1x_2 + i_1i_2 \in I$ ($I$ Ideal!) $\Rightarrow x_1x_2\pi y_1y_2$. Die Verträglichkeit von $\pi$ mit $+$ wurde schon für die Gruppe $(R, +)$ gezeigt.

c) $\pi \mapsto [0]_\pi = I \mapsto \pi$, $I \mapsto \pi \mapsto [0]_\pi = I$ (analog zum entsprechenden Beweis für Normalteiler). □

Ist $I$ Ideal von $R$, dann ist die Faktoralgebra $(R/I, +, I, -, \cdot)$ ein Ring, genannt der *Faktor- oder Restklassenring* von $R$ modulo $I$. Die Operationen in $R/I$ sind:

$$(x + I) + (y + I) = (x + y) + I$$

(deckt sich mit der Komplexsumme $A + B = \{a + b \mid a \in A,\ b \in B\}$),

$$(x + I)(y + I) = xy + I$$

(deckt sich *nicht* mit dem Komplexprodukt $AB = \{ab \mid a \in A,\ b \in B\}$),

$$-(x + I) = (-x) + I, \quad 0 + I = I \text{ ist Nullelement.}$$

**2.2.46 Beispiel.** $\mathbb{Z}_n = \mathbb{Z}/I$ mit $I = \{kn \mid k \in \mathbb{Z}\}$, denn: $x \in I \Leftrightarrow x \equiv 0 \bmod n \Leftrightarrow x - 0 = x = kn$, $k \in \mathbb{Z}$. Also entspricht das angegebene Ideal $I$ der Relation $\equiv \bmod n$. Schreibweise: $I =: (n)$.

**2.2.47 Anmerkung.** Ein Ring $R$ ist einfach $\Leftrightarrow$ $R$ besitzt nur die trivialen Kongruenzen $\Leftrightarrow$ $R$ besitzt nur die trivialen Ideale $\{0\} =: (0)$ und $R$.

**2.2.48 Satz.** *Ein kommutativer Ring $R$ mit Einselement und $R \neq \{0\}$ ist einfach genau dann, wenn er ein Körper ist.*

**2.2.49 Beispiel.** Jeder Matrizenring $M_n(K)$ über einem Körper $K$ ist einfach (Übungsbeispiel 48).

## 2.3 Direkte Produkte von Algebren

**2.3.1 Definition.** Seien $\mathfrak{A}_k = (A_k, (\omega_i^{(k)})_{i \in I})$, $k \in K$, Algebren vom selben Typ $(n_i)_{i \in I}$ und $A := \prod_{k \in K} A_k = \{(a_k)_{k \in K} \mid a_k \in A_k\}$ das cartesische Produkt aller Mengen $A_k$. Die Elemente von $A$ sind $K$-Tupel; wir bezeichnen Elemente von $A$ auch manchmal als Vektoren $\vec{a} = (a_k : k \in K)$.
Für alle $i \in I$ sei die Operation $\omega_i$ auf $A$ „komponentenweise“ so definiert:

- Wenn $n_i = 0$ ist (d.h. die Abbildungen $\omega_i^{(k)}$ sind nullstellige Operationen bzw. Konstante), dann kennen wir bereits die ausgezeichneten Elemente $\omega_i^{(k)} \in A_k$ und können sie zu einem $K$-Tupel in $A$ zusammenfassen:

$$\omega_i := (\omega_i^{(k)})_{k \in K}.$$

- Wenn $n_i = n > 0$ ist, dann ist jede Operation $\omega_i^{(k)}$ auf $A_k$ $n$-stellig. Für Vektoren

$$\begin{aligned} \vec{a}^{(1)} &= (a_k^{(1)} : k \in K) \in A \\ \vdots \qquad & \qquad \vdots \\ \vec{a}^{(n)} &= (a_k^{(n)} : k \in K) \in A \end{aligned}$$

definieren wir

$$\omega_i(\vec{a}^{(1)}, \ldots, \vec{a}^{(n)}) := \vec{b} = (b_k : k \in K) \in A,$$

wobei $b_k := \omega_i^{(k)}(a_k^{(1)}, \ldots, a_k^{(n)})$ ist.

In der $k$-ten Komponente wenden wir also die Operation $\omega_i^{(k)}$ auf Elemente von $A_k$ an. Die Algebra $(A, (\omega_i)_{i\in I})$ heißt das *direkte Produkt* der Algebren $\mathfrak{A}_k$ und wird mit $\prod_{k\in K} \mathfrak{A}_k$ bezeichnet.

**2.3.2 Beispiel.** $K = \{1, 2\}$, $\mathfrak{A}_1 = (A_1, \cdot, e, {}^{-1})$, $\mathfrak{A}_2 = (A_2, +, 0, -)$ seien Gruppen. Dann wird in $\mathfrak{A}_1 \times \mathfrak{A}_2 = (A_1 \times A_2, \circ, (e, 0), \overline{\ \ })$ folgendermaßen gerechnet:

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 b_1, a_2 + b_2),$$
$$\overline{(a_1, a_2)} = (a_1^{-1}, -a_2).$$

Es gilt: $\mathfrak{A}_1 \times \mathfrak{A}_2$ ist eine Gruppe. Assoziativgesetz:

$$((a_1, a_2) \circ (b_1, b_2)) \circ (c_1, c_2) = (a_1 b_1 c_1, a_2 + b_2 + c_2) = (a_1, a_2) \circ ((b_1, b_2) \circ (c_1, c_2))$$

$(e, 0)$ ist neutrales Element:

$$(e, 0) \circ (a_1, a_2) = (ea_1, 0 + a_2) = (a_1, a_2) = (a_1 e, a_2 + 0) = (a_1, a_2) \circ (e, 0)$$

$\overline{(a_1, a_2)}$ ist Inverses von $(a_1, a_2)$:

$$(a_1, a_2) \circ \overline{(a_1, a_2)} = (a_1, a_2) \circ (a_1^{-1}, -a_2) = (a_1 a_1^{-1}, a_2 + (-a_2)) = (e, 0),$$

analog $\overline{(a_1, a_2)} \circ (a_1, a_2) = (e, 0)$.

**2.3.3 Satz.** *Gilt mit geeigneten Termen $t_1, t_2$ ein Gesetz der Form*

$$\forall x_1, \ldots, x_n : t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$$

*in allen Algebren $\mathfrak{A}_k$, $k \in K$, so gilt es auch in $\prod_{k\in K} \mathfrak{A}_k$.*

*Beweis.* Durch Induktion nach Termaufbau zeigt man, dass für einen beliebigen Term $t(x_1, \ldots, x_n)$ und Elementen $\vec{a}^{(j)} = (a_k^{(j)})_{k\in K} \in \prod_{k\in K} A_k$, $j = 1, \ldots, n$, gilt

$$t(\vec{a}^{(1)}, \ldots, \vec{a}^{(n)}) = (t(a_k^{(1)}, \ldots, a_k^{(n)}))_{k\in K}.$$

Daraus folgt dann sofort

$$t_1(\vec{a}^{(1)}, \ldots, \vec{a}^{(n)}) = (t_1(a_k^{(1)}, \ldots, a_k^{(n)}))_{k\in K} =$$
$$= (t_2(a_k^{(1)}, \ldots, a_k^{(n)}))_{k\in K} = t_2(\vec{a}^{(1)}, \ldots, \vec{a}^{(n)})$$

□

**2.3.4 Folgerung.** Direkte Produkte von Halbgruppen (Gruppen, Vektorräumen über dem selben Körper $K$, Ringen, Booleschen Algebren) sind wieder Halbgruppen (Gruppen, Vektorräume über $K$, Ringe, Boolesche Algebren).

Achtung! Das direkte Produkt von (mindestens zwei) Integritätsbereichen ist *nie* ein Integritätsbereich, denn $(0, 1) \cdot (1, 0) = (0, 0)$. (Beachte: $0 \neq 1$.)

**2.3.5 Anmerkungen.** 1) Das direkte Produkt $\prod_{k\in K} \mathfrak{A}_k$ ist — bis auf Isomorphie — unabhängig von der Reihenfolge. Z.B.: $\mathfrak{A}_1 \times \mathfrak{A}_2 \cong \mathfrak{A}_2 \times \mathfrak{A}_1$.

2) Man kann Produkte „zusammenfassen“. Z.B.: $\mathfrak{A}_1 \times \mathfrak{A}_2 \times \mathfrak{A}_3 \cong (\mathfrak{A}_1 \times \mathfrak{A}_2) \times \mathfrak{A}_3 \cong \mathfrak{A}_1 \times (\mathfrak{A}_2 \times \mathfrak{A}_3)$.

**2.3.6 Satz.** *Seien $C_n$ bzw. $C_m$ zyklische Gruppen der Ordnungen $n$ bzw. $m$. Dann gilt: $C_n \times C_m$ ist zyklisch $\Leftrightarrow \mathrm{ggT}(m,n) = 1$.*

*Beweis.* Sei $C_n = \langle x \rangle$, $C_m = \langle y \rangle$.

$\Rightarrow$ (indirekt): $\mathrm{ggT}(n,m) > 1 \Rightarrow k := \mathrm{kgV}(n,m) < nm$ (wegen $\mathrm{kgV}(n,m) = nm/\mathrm{ggT}(n,m)$) und $(x^i, y^j)^k = (x^{ki}, y^{kj}) = (e,e)$ (wegen $n|ki$ und $m|kj$) $\Rightarrow \mathrm{o}(x^i, y^j)|k < nm \Rightarrow$ die Ordnung aller Elemente von $C_n \times C_m$ ist kleiner als $nm = |C_n \times C_m| \Rightarrow C_n \times C_m$ ist nicht zyklisch.

$\Leftarrow$: Wir zeigen, dass $C_n \times C_m = \langle (x,y) \rangle$ gilt. $(x,y)^t = (e,e) \Rightarrow x^t = e$ und $y^t = e \Rightarrow n|t$ und $m|t \Rightarrow \mathrm{kgV}(n,m) = nm|t$ (wegen $\mathrm{ggT}(n,m) = 1$). Andererseits gilt: $(x,y)^{nm} = (x^{nm}, y^{nm}) = ((x^n)^m, (y^m)^n) = (e,e)$. Also ist $\mathrm{o}(x,y) = nm$. □

**2.3.7 Folgerung.** Ist $n = p_1^{e_1} \cdots p_k^{e_k}$ die Primfaktorzerlegung von $n \in \mathbb{N}$, dann gilt $C_n \cong C_{p_1^{e_1}} \times \cdots \times C_{p_k^{e_k}}$.

**2.3.8 Satz (Hauptsatz über endlich erzeugte abelsche Gruppen).** *Ist $G = \langle \{x_1, \ldots, x_m\} \rangle$ eine von den Elementen $x_1, \ldots, x_m$ erzeugte* abelsche *Gruppe, dann gilt:*

$$G \cong C_\infty^k \times C_{n_1} \times \cdots \times C_{n_r},$$

*wobei $k \geq 0$ ($C_\infty^0 := \{e\}$), $n_i \in \mathbb{N}$, $r \geq 0$. Dabei gilt: $G$ endlich $\Leftrightarrow k = 0$.*

($C_\infty$ bezeichnet eine unendliche zyklische Gruppe; sie ist isomorph zur additiven Gruppe $(\mathbb{Z}, +)$.)

**2.3.9 Beispiel.** 1) Alle abelschen Gruppen mit 12 Elementen sind — bis auf Isomorphie — gegeben durch $C_{12}$ ($\cong C_3 \times C_4$) und $C_2 \times C_6$ ($\cong C_2 \times C_2 \times C_3$).

2) Alle abelschen Gruppen mit 8 Elementen sind — bis auf Isomorphie — gegeben durch $C_8$, $C_2 \times C_4$ und $C_2 \times C_2 \times C_2$.

Zur nächsten Definition vgl. den Begriff „direkte Summe“ $V = U_1 \oplus U_2 \oplus \cdots \oplus U_n$ aus der Linearen Algebra ($U_1, U_2, \ldots, U_n$ Unterräume eines Vektorraumes $V$).

**2.3.10 Definition.** Sei $G$ Gruppe, und seien $U, V$ Untergruppen von $G$. $G$ heißt *inneres direktes Produkt* von $U$ und $V$ genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U \times V \to G \\ (u,v) \mapsto uv \end{cases}$$

ein Isomorphismus von $U \times V$ auf $G$ ist.

**2.3.11 Beispiel.** Seien $G_1$ und $G_2$ Gruppen mit neutralem Element $e_1$ bzw $e_2$. Dann sind $U := G_1 \times \{e_2\}$ und $V := \{e_1\} \times G_2$ Untergruppen von $G := G_1 \times G_2$, und $G$ ist das innere direkte Produkt von $U$ und $V$.

Wir verallgemeinern diese Definition auf das Produkt von endlich vielen Gruppen.

**2.3.12 Definition.** Sei $G$ Gruppe, $U_1, \ldots, U_n$ Untergruppen von $G$. Dann heißt $G$ *inneres direktes Produkt* von $U_1, \ldots, U_n$ genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U_1 \times \cdots \times U_n \to G \\ (u_1, \ldots, u_n) \mapsto u_1 \cdots u_n \end{cases}$$

ein Isomorphismus von $U_1 \times \cdots \times U_n$ auf $G$ ist.

**2.3.13 Anmerkung.** $G \cong G_1 \times \cdots \times G_n \Leftrightarrow$ es gibt Untergruppen $U_i$ von $G$ mit $U_i \cong G_i$, $i = 1, \ldots, n$, sodass $G$ inneres direktes Produkt von $U_1, \ldots, U_n$ ist. (Beweis: Übungsbeispiel 54.)

**2.3.14 Satz.** *Sei $G$ Gruppe, $U_1, \ldots, U_n$ Untergruppen von $G$. Dann sind die folgenden Aussagen äquivalent:*

a) *$G$ ist inneres direktes Produkt von $U_1, \ldots, U_n$.*

b) i) *Die oben definierte Abbildung $\varphi : U_1 \times \cdots \times U_n \to G$, $(u_1, \ldots, u_n) \mapsto u_1 \cdots u_n$, ist bijektiv und*

ii) *für $1 \leq i < j \leq n$, $x \in U_i$, $y \in U_j$ gilt stets $xy = yx$.*

*Beweis.* a) $\Rightarrow$ b): i) gilt, da $\varphi$ Isomorphismus.
Zu ii): Für $x \in U_i$, $y \in U_j$, $1 \leq i < j \leq n$ gilt

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

b) $\Rightarrow$ a): Da $\varphi$ bijektiv ist, muss nur mehr gezeigt werden, dass $\varphi$ Homomorphismus ist. Für $\vec{a} := (a_1, \ldots, a_n)$, $\vec{b} := (b_1, \ldots, b_n) \in U_1 \times \cdots \times U_n$ gilt:

$$\varphi(\vec{a}\vec{b}) = \varphi(a_1 b_1, \ldots, a_n b_n) = a_1 b_1 \cdots a_n b_n \overset{*}{=} a_1 \cdots a_n b_1 \cdots b_n = \varphi(\vec{a})\varphi(\vec{b}).$$

Die mit $^*$ bezeichnete Gleichheit gilt wegen ii). □

**2.3.15 Satz.** *Sei $G$ Gruppe, $U_1, \ldots, U_n$ Untergruppen von $G$. Dann sind die folgenden Aussagen äquivalent:*

a) *$G$ ist inneres direktes Produkt von $U_1, \ldots, U_n$.*

b) I) *$G = U_1 \cdots U_n = \{u_1 \cdots u_n \mid u_i \in U_i\}$ (d.h., $\varphi$ ist surjektiv),*

II) *$(U_1 \cdots U_i) \cap U_{i+1} = \{e\}$ für $i = 1, \ldots, n-1$,*

III) *$U_i \lhd G$ für $i = 1, \ldots, n$.*

*Beweis.* a) $\Rightarrow$ b): I) ist erfüllt.
Zu II): $a \in (U_1 \cdots U_i) \cap U_{i+1} \Rightarrow a = a_1 \cdots a_i e \cdots e = e \cdots e a_{i+1} e \cdots e$ mit $a_k \in U_k \Rightarrow$ $a_1 = \cdots = a_i = a_{i+1} = e$ (da $\varphi$ injektiv).
Zu III): Für $g \in G$, $g = a_1 \cdots a_n$, $a_i \in U_i$, gilt:

$$gU_i = a_1 \cdots a_n U_i \overset{*}{=} a_1 \cdots a_i U_i a_{i+1} \cdots a_n \overset{**}{=} a_1 \cdots a_{i-1} U_i a_i \cdots a_n \overset{*}{=} U_i a_1 \cdots a_n = U_i g$$

(dabei gilt $^*$ wegen ii) im vorigen Satz und $^{**}$, weil $a_i \in U_i$).

b) $\Rightarrow$ a): Wegen I) ist $\varphi$ surjektiv. Wir zeigen nun ii) (im vorigen Satz): Für $1 \leq i < j \leq n$, $a_i \in U_i$, $a_j \in U_j$, gilt

$$a_i a_j (a_j a_i)^{-1} = a_i a_j a_i^{-1} a_j^{-1} = a_i \cdot \underbrace{(a_j a_i^{-1} a_j^{-1})}_{\in U_i, \text{ da } U_i \lhd G} = \underbrace{(a_i a_j a_i^{-1})}_{\in U_j, \text{ da } U_j \lhd G} \cdot a_j^{-1} \in U_i \cap U_j.$$

Wegen $U_i \cap U_j \subseteq (U_1 \cdots U_i \cdots U_{j-1}) \cap U_j = \{e\}$ ist $a_i a_j (a_j a_i)^{-1} = e$ woraus $a_i a_j = a_j a_i$ folgt.
Abschließend zeigen wir i) (im vorigen Satz), d.h., dass $\varphi$ injektiv ist: Sei $a_1 \cdots a_n = b_1 \cdots b_n$, $a_i, b_i \in U_i$. Dann gilt $b_{n-1}^{-1} \cdots b_1^{-1} a_1 \cdots a_{n-1} = b_n a_n^{-1}$, woraus (mit ii)) $b_1^{-1} a_1 \cdots b_{n-1}^{-1} a_{n-1} = b_n a_n^{-1} \in (U_1 \cdots U_{n-1}) \cap U_n = \{e\}$ folgt. Damit ist $a_n = b_n$. Analog erhält man $a_{n-1} = b_{n-1}$, $\ldots$, $a_1 = b_1$. □

Spezialfall: Seien $U$, $V$ Normalteiler von $G$. Dann ist $G$ genau dann das innere direkte Produkt von $U$ und $V$, wenn $UV = G$ und $U \cap V = \{1\}$ gilt.

**2.3.16 Definition.** Sei $R$ ein Ring, $U_1, \ldots, U_n$ Unterringe von $R$. Dann heißt $R$ *innere direkte Summe* von $U_1, \ldots, U_n$ genau dann, wenn die Abbildung

$$\varphi : \begin{cases} U_1 \times \cdots \times U_n \to R \\ (u_1, \ldots, u_n) \mapsto u_1 + \cdots + u_n \end{cases}$$

ein Ring-Isomorphismus ist.

**2.3.17 Satz.** *Sei $R$ ein Ring, $U_1, \ldots, U_n$ Unterringe von $R$. Dann sind die folgenden Aussagen* a), b) *und* c) *zueinander äquivalent:*

a) *$R$ ist innere direkte Summe von $U_1, \ldots, U_n$.*

b) i) *$\varphi$ (von oben) ist bijektiv und*
   ii) *für $1 \leq i \neq j \leq n$, $x \in U_i$, $y \in U_j$ gilt stets $xy = 0$.*

c) I) *$R = U_1 + \cdots + U_n$,*
   II) *$(U_1 + \cdots + U_i) \cap U_{i+1} = \{0\}$ für $i = 1, \ldots, n-1$,*
   III) *Jedes $U_i$ ist Ideal, d.h., $U_i \lhd R$ für $i = 1, \ldots, n$.*

*Beweis.* a) $\Rightarrow$ b): i) ist erfüllt.

Zu ii): Für $x \in U_i$, $y \in U_j$, $i \neq j$ gilt

$$(0, \ldots, 0, \underbrace{x}_{i-\text{te Stelle}}, 0, \ldots, 0) \cdot (0, \ldots, 0, \underbrace{y}_{j-\text{te Stelle}}, 0, \ldots, 0) = (0, \ldots, 0),$$

woraus — nach Anwendung von $\varphi$ — $xy = 0$ folgt.

b) $\Rightarrow$ c): I) und II) folgen aus dem zweiten Satz über Gruppen. Zu III): Für $b_i \in U_i$, $r = a_1 + \cdots + a_n \in R$ gilt

$$r b_i = (a_1 + \cdots + a_n) b_i = a_1 b_i + \cdots + a_i b_i + \cdots + a_n b_i = 0 + \cdots + 0 + a_i b_i + 0 + \cdots + 0 = a_i b_i \in U_i.$$

Analog zeigt man $b_i r \in U_i$.

c) $\Rightarrow$ a): Da $\varphi$ nach I) und II) bijektiv ist (folgt aus dem Satz über Gruppen), muss nur mehr gezeigt werden, dass $\varphi$ Homomorphismus ist. Bezüglich $+$ folgt dies ebenfalls aus dem Satz über Gruppen, bezüglich $\cdot$ gilt:

$$\begin{aligned}\varphi((a_1,\ldots,a_n)(b_1,\ldots,b_n)) &= \varphi(a_1b_1,\ldots,a_nb_n) = \\ &= a_1b_1+\cdots+a_nb_n = (a_1+\cdots+a_n)(b_1+\cdots+b_n) = \\ &= \varphi(a_1,\ldots,a_n)\varphi(b_1,\ldots,b_n).\end{aligned}$$

Die hierbei verwendete Beziehung $a_1b_1+\cdots+a_nb_n = (a_1+\cdots+a_n)(b_1+\cdots+b_n)$ folgt aus II) und III): Für $i<j$ ist $a_ib_j \in U_i$ (wegen $U_i \lhd R$) und $a_ib_j \in U_j$ (wegen $U_j \lhd R$), d.h., $a_ib_j \in (U_1+\cdots+U_{j-1})\cap U_j = \{0\}$, woraus $a_ib_j = 0$ folgt. Analog erhält man $a_ib_j = 0$ für $i>j$. $\square$