**ALGEBRAISCHE GRUNDLAGEN DER INFORMATIK**

GEORGE CIPRIAN MODOI

Inhaltverzeichnis

Literatur 2
1. Mengen, Abbildungen, Relationen 3
1.1. Logische Grundlagen 3
Übungen zu Logische Grundlagen 3
1.2. Mengen 3
Operationen mit Mengen 4
Übungen zu Mengen 6
1.3. Abbildungen 6
Injektivität, Surjektivität, Bijektivität 8
Die Kardinalanzahl einer Menge 9
Das Cartesisches Produkt 9
Operationen 10
Übungen zu Abbildungen 11
1.4. Relationen 13
Äquivalenzrelationen 15
Ordnungsrelationen 16
Übungen zu Relationen 18
2. Gruppen, Ringe, Körper 20
2.1. Gruppen 20
Untergruppen 21
Gruppenhomomorphismen 22
Zyklische Gruppen und die Ordnung eines Elementes 23
Wirkungen der Gruppen auf Mengen 24
Die Symmetrischegruppe 25
Übungen zu Gruppen 26
2.2. Ringe und Körper 29
Untergrringe und Unterkörper 30
Homomorphismen 31
Spezielle Elemente in einem Ring 31
Übungen zu Ringe 32
3. Lineare Algebra 34
3.1. Vektorräume und lineare Abbildungen 34
Untervektorräume 35
Summe und direkte Summe der Unterraümen 36
Lineare Abbildungen 37
Übungen zu Vektorräume 38

*Date*: November 14, 2015.

3.2. Basen 39
Lineare Unabhängigkeit 40
Basen und Koordinaten 41
Die Dimension eines Vektorräumes 42
Die universelle Eigenschaft der Basis eines Vektorräumes 43
Einige Formeln mit der Dimension gebunden 43
Die Ersetzungslemma 43
Übungen zu Basen 44

## Literatur

[1] M. Artin, *Algebra*, Prentice Hall, 1991.
[2] N. Both, S. Crivei, *Culegere de probleme de algebră*, Lito UBB, 1996.
[3] S. Breaz, T. Coconeţ, C. Conţiu, *Lecţii de Algebră*, Editura Eikon, Cluj, 2010.
[4] P. M. Cohn, *Elements of Linear Algebra*, Springer Verlag, N.Y.-Berlin-Heidelberg, 1994.
[5] I. D. Ion, N. Radu, *Algbera*, Editura Did. Ped. Bucureşti, 1970.
[6] I. D. Ion, N. Radu, C. Niţă, D. Popescu, *Probleme de algebră*, Ed. Did. Ped., Bucureşti, 1970.
[7] B. Külshammer, *Lineare Algebra und Analytische Geometrie*, Vorlesungsskripte, `https://www.minet.uni-jena.de//algebra//skripten/skripten.html`.
[8] C. Năstăsescu, C. Niţă, C. Vraciu, Bazele algebrei, Ed. Academiei, 1986.
[9] C. Năstăsescu, C. Niţă, M. Brandiburu, D. Joiţa, *Exerciţii şi probleme de algebră*, Ed. Did. Ped. Bucureşti, 1983.
[10] I. Purdea, I. Pop, *Algebră*, Ed. Gill, Zalău, 2007.
[11] C. Pelea, I. Purdea, *Probleme de algebră*, Editura EFES, Cluj, 2005.
[12] G. Pic, I. Purdea, *Tratat de algebră modernă*, Editura Academiei, Bucureşti, 1977.
[13] A. E. Schroth, *Algebra für die Studierende der Informatik*, Vorlesungsskripte, `http://www.carsten-buschmann.de/skripte/Algera_fuer_Informatiker.pdf`.

## 1. Mengen, Abbildungen, Relationen

1.1. **Logische Grundlagen.** Logische Aussagen sind nur die Aussagen die entweder wahr oder falsch sind; die andere Aussagen wei die Fragen die nicht wahr oder falsch konnen sein sind nicht erlaubt. Zwischen Aussagen gibt es die Operatoren:

- Negation $\neg$
- logisches und $\wedge$
- logisches oder $\vee$
- ausschlieschendes oder $\oplus$
- Implikation $\Rightarrow$
- logische Äquivalenz $\Leftrightarrow$

Diese Operatoren werden durch die folgende Tabelle definiert (hier $p$ and $q$ sind Aussagen und 0 und 1 bezeichnen falsch, bzw. wahr):

| $p$ | $q$ | $\neg p$ | $p \wedge q$ | $p \vee q$ | $p \oplus q$ | $p \Rightarrow q$ | $p \Leftrightarrow q$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

**Übungen zu Logische Grundlagen.**

**Übung 1.1.1.** Man zeige dass die folgende Formulas Tautologien sind, das heißt sie stäts wahr sind (für alle mögliche Werten der Aussagen $p$, $q$ $r$ etc.).

(a) $((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$
(b) $((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$
(c) $(p \vee q) \Leftrightarrow (q \vee p)$
(d) $(p \wedge q) \Leftrightarrow (q \wedge p)$
(e) $(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$
(f) $(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$
(g) $(p \vee (p \wedge q)) \Leftrightarrow p$
(h) $(p \wedge (p \vee q)) \Leftrightarrow p$
(i) $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
(j) $p \Rightarrow p$
(k) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.

1.2. **Mengen.** Mengen sind Ansammlung von Objekten (die *Elemente* gennant werden) so dass jedes Element ist eindeutig bestimmt. Mengen können direkt durch explizite Angabe ihrer Elemente (d. h. *syntetisch*) oder durch die Bedingungen (Eigenschaften), die die Elemente erfüllen müssen (d. h. *analytisch*), angegeben werden. Man schreibt $x \in A$ (und man spricht "$x$ gehört zu $A$) um zu sagen dass $x$ ein Element der Menge $A$ ist. Man notiert, dass die Begriffe "Menge" und "Eingehörigkeit" sind primäre, d.h. sie werden nicht definiert.

**Beispiel 1.2.1.** a) $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, $C = \{?, 7, *, \vee\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
b) $Z = \{x \mid x \in \mathbb{N} \text{ und } 0 \leq x < 10\}$, $[-3, 8) = \{x \mid x \in \mathbb{R} \text{ und } -3 \leq x < 8\}$.
c) Andere Beispiele ...

**Definition 1.2.2.** Zwei Mengen sind gleich genau dann, wenn diese Mengen dieselbe Elemente erhalten.

**Beispiel 1.2.3.** $\{1,2,3\} = \{x \in \mathbb{N} \mid 1 \leq x \leq 3\} = \{x \in \mathbb{Z} \mid 0 < x < 4\}$, $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$.

**Bemerkung 1.2.4.** a) Die Reihenfolge der Elemente einer Menge ist unerheblich: $\{1,2\} = \{2,1\}$ oder $\{a,b,c\} = \{b,c,a\} = \{a,c,b\}$.

b) Ein Element einer Menge erscheint nur einmal: $\{1,2\}$ und NICHT $\{1,2,2,1\}$.

c) Bei der analitischen Angabe einer Menge ist Vorsicht gefördert. Zum Beispiel führt die Konstruktion $R = \{x \mid x \notin x\}$ zu Wiedersprüchen. Genauer beide Aussagen $R \in R$ und $R \notin R$ führen zum Wiederspruch (das Russelsche Paradoxon). Hier $x \notin A$ ist die Negation der Aussagen $x \in A$). Wir beschäftigen uns nich viel mit Probleme dieser Art, aber wir vermeiden die Widersprüchen wenn wir arbeiten lokal, d.h. wenn $P$ ist eine Eigenschaft (Prädikat) dann wir definieren $A = \{x \in U \mid P(x)\}$ und nicht $A = \{x \mid P(x)\}$, wobei $U$ ist eine umbegriffende Menge (das Universum des Diskution).

**Beispiel 1.2.5.** Zahlenmengen:

Naturliche Zahlen: $\mathbb{N} = \{0,1,2,3,\ldots\}$, $N^* = \{1,2,3\ldots\}$.

Ganze Zahlen: $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$.

Rationale Zahlen: $\mathbb{Q} = \{\frac{m}{n} \mid n,m \in \mathbb{Z}, n \neq 0\}$.

Reele Zahlen: $\mathbb{R}$ ($\mathbb{R} =?$).

Complexe Zahlen: $\mathbb{C} = \{a+ib \mid a,b \in \mathbb{R}\}$ wobei $i^2 = -1$.

**Definition 1.2.6.** Seien $A$ und $B$ Mengen. Man sagt dass $A$ einer *Teilmenge* von $B$ ist, wenn $x \in A$ impliziert $x \in B$. Man schreibt $A \subseteq B$.

**Definition 1.2.7.** Die leere Menge ist die Menge die keine Elemente enthält. Man schreibt $\emptyset$ für die leere Menge.

**Satz 1.2.8.** *Sind $A$, $B$ und $C$ Mengen so gelten die folgende Aussagen:*

(a) $A \subseteq A$ *(Reflexivität).*
(b) *Wenn* $A \subseteq B$ *und* $B \subseteq C$ *dann* $A \subseteq C$ *(Transitivität).*
(c) $A$=$B$ *gdw* $A \subseteq B$ *und* $B \subseteq A$ *(Antisymmetrie).*
(d) $\emptyset \subseteq A$.
(e) *Die leere Menge ist eindeutig.*

*Beweis.* □

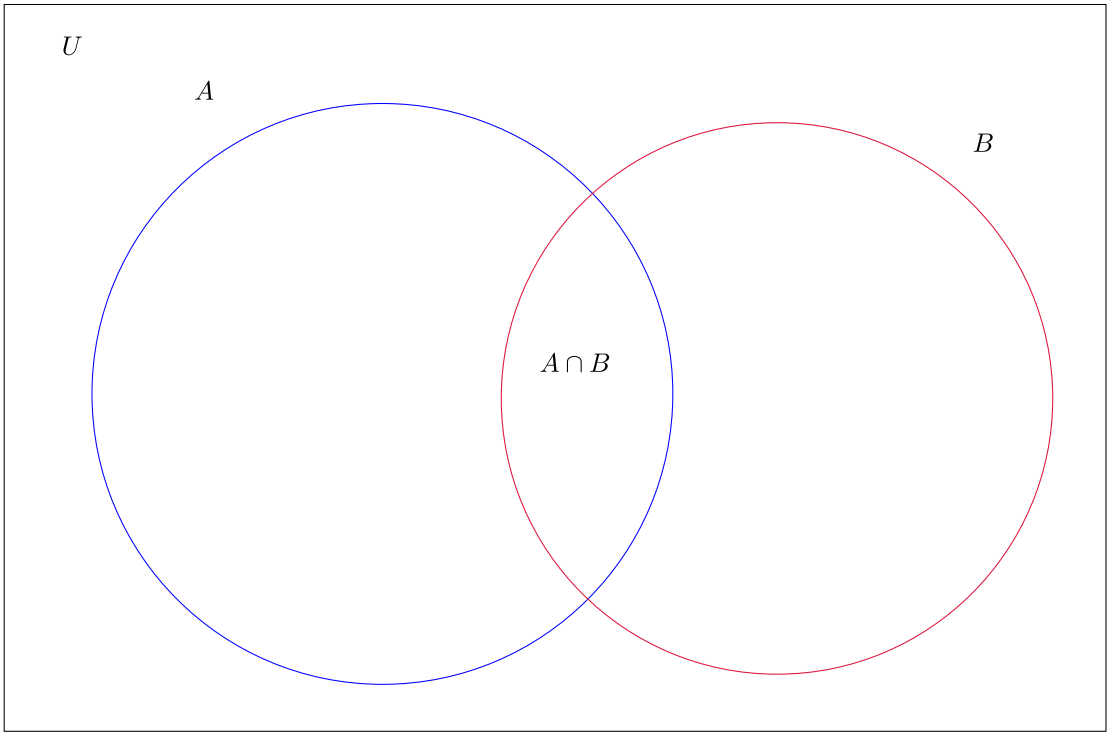
**Operationen mit Mengen.**

**Definition 1.2.9.** Seien $A$ und $B$ Mengen. Man definiert:

(a) Die *Vereinigung* von $A$ und $B$ durch $A \cup B = \{x \mid x \in A \vee x \in B\}$.
(b) Der *(Durch)Schnitt* von $A$ und $B$ durch $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
(c) Die *Differenz* von $A$ und $B$ durch $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

Ist $A \subseteq U$ so nennt man $\mathbf{C}_U A = U \setminus A$ die *Komplementare* von $A$ in $U$.

**Bemerkung 1.2.10.** Die Mengen lassen sich durch die so genannte Euler-Venn Diagramme dargestellt werden. Zum Beispiel:




**Theorem 1.2.11.** *Seien $A$, $B$, $C$, $U$ Mengen, so dass alle $A$, $B$, $C$ Teilmengen von $U$ sind.*

(a) $(A \cup B) \cup C = A \cup (B \cup C)$ *und* $(A \cap B) \cap C = A \cap (B \cap C)$ *(Assoziativität).*
(b) $A \cup B = B \cup A$ *und* $A \cap B = B \cap A$ *(Kommutativität).*
(c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *und* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(Distributivität).*
(d) $A \cup A = A = A \cap A$ *(Idempotenz).*
(e) $A \cup (A \cap B) = A = A \cap (A \cup B)$ *(Absorbtion).*
(f) $\mathbf{C}_U(A \cup B) = \mathbf{C}_U A \cap \mathbf{C}_U B$ *und* $\mathbf{C}_U(A \cap B) = \mathbf{C}_U A \cup \mathbf{C}_U B$ *(die Regels von de Morgan).*

*Beweis.* □

**Definition 1.2.12.** Sei $A$ eine Menge. Die *Potenzmenge* der $A$ ist die Menge aller Teilmengen von $A$, d.h.

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}.$$

**Bemerkung 1.2.13.** Die Definition der Potenzmenge gefördert Vorsicht: welches Universum soll benutzt werden? Zu notieren: das Cantorsche Paradoxon wird mit der Hilfe der Potenzmenge gebaut.

**Definition 1.2.14.** Für zwei Mengen $A$ und $B$, das *Cartesisches Produkt* ist

$$A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\}.$$

Dabei ist $(a, b)$ ein *Paar* (d. h. eine geordnete Menge), die durch

$$(a, b) = \{a, \{a, b\}\}$$

rein mengentheoretisch definiert lässt.

**Bemerkung 1.2.15.** Induktiv kann man das Produkt endlich vieller Mengen definiert:

$$A_1 \times A_2 \times \dots A_{n-1} \times A_n = (A_1 \times A_2 \times \dots A_{n-1}) \times A_n.$$

Ist $A$ eine Menge so ist $A^1 = A$ und $A^n = A^{n-1} \times A$, für alle $n > 1$.

**Übungen zu Mengen.**

**Übung 1.2.16.** Man bestimme $A \cup B$, $A \cap B$, $A \setminus B$, $\mathbf{C}_{\mathbb{N}}(A)$, $A \times B$, wobei

$$A = \{n \in \mathbb{N} \mid \frac{3n+5}{n+1} \in \mathbb{N}\} \text{ und } B = \{x \in \mathbb{Z} \mid x \text{ ist gerade und } -2 \leq x < 3\}.$$

**Übung 1.2.17.** Man bestimme $\mathcal{P}(\emptyset)$, $\mathcal{P}(\{\emptyset\})$, $\mathcal{P}(\{\emptyset, \{\emptyset\}\})$.

1.3. **Abbildungen.**

**Definition 1.3.1.** Eine Abbildung ist ein Tripel $(A, B, f)$ die aus zwei Mengen $A$ und $B$ und eine Korrespondenz $f$ besteht, so dass die Korrespondenz $f$ zu jedes Element aus $A$ ein eindeutig bestimmt Element aus $B$ zugeordnet. Man nennt die Mengen $A$ und $B$ den Definitionsbereich bzw Wertensbereich der Abbildung. Man schreibt $f : A \to B$ oder $A \xrightarrow{f} B$. Für $a \in A$ notiert man $f(a)$ das einzelnes Element aus $B$ das unter $f$ zu $a$ zugeordent wird. Man schriebt auch $a \mapsto f(a)$ und $f(a)$ ist *das Bild von $a$ unter $f$* gennant. Man bezeichnet mit $B^A$ die Menge aller Abbildungen von $A$ nach $B$, d.h.

$$B^A = \{f : A \to B \mid f \text{ ist eine Abbildung}\}.$$

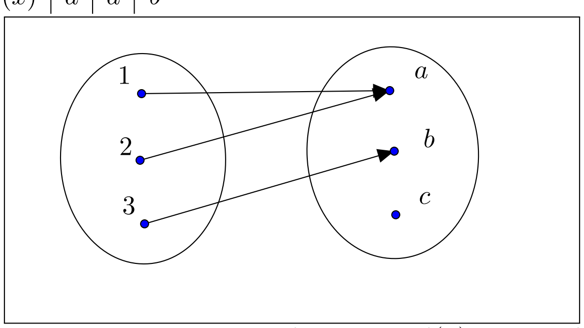
**Bemerkung 1.3.2.** Zwei Abbildungen $f : A \to B$ und $f' : A' \to B'$ sind gleich gdw $A = A'$, $B = B'$ und $f(x) = f(x')$ für alle $x \in A$.

**Bemerkung 1.3.3.** Abbildungen können in verschidene Weisen angegeben werden:

(a) Durch direkte Angabe ihrer Bilden, z. B. $f : \{1, 2, 3\} \to \{a, b, c, d\}$, $f(1) = f(2) = a$ und $f(3) = b$. Varianten (für dieselbe Abbildung): Durch die Tabelle:

| $x$ | 1 | 2 | 3 |
|---|---|---|---|
| $f(x)$ | $a$ | $a$ | $b$ |

oder durch die Diagramme:



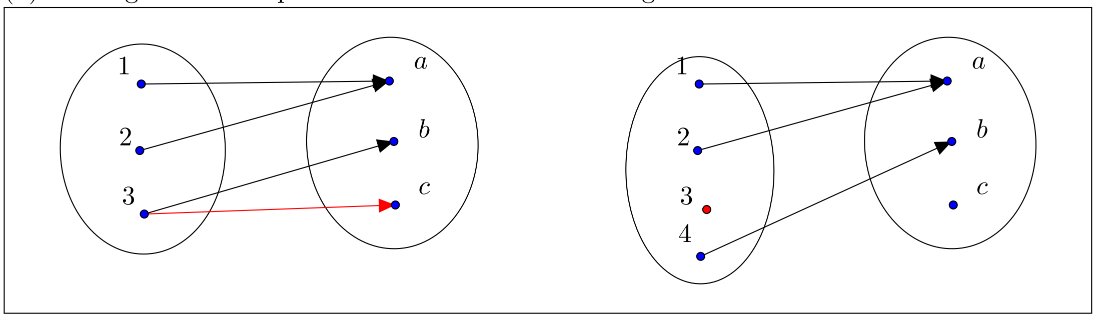

(b) Durch eine Formula, z. B. $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x + 1$ für alle $x \in \mathbb{N}$. Frage: Jede Formula führt zu einer wohl definierten Abbildungen?

**Beispiel 1.3.4.** (a) Ist $A$ eine belibige Menge so ist $1_A : A \to A$, $1_A(x) = x$ für alle $x \in A$ eine Abbildung. Man schreibt manchmal $\mathrm{id}_A = 1_A$ (die *Identitätabbildung* von $A$).

(b) Sind $A$ und $B$ Mengen, so dass $A \subseteq B$, so ist $i = i_{A,B} : A \to B$, $i(x) = x$, für alle $x \in A$ eine Abbildung (die *Inklusionsabbildung* von $A$ in $B$). Man notiere, dass $i_{A,B} = 1_A$ gdw $A = B$, umsonst $i_{A,B} \neq 1_A$.

(c) Sind $A$, $B$, $C$ Mengen so dass $C \subseteq A$ und ist $f : A \to B$ eine Abbildung, so bildet man eine andere Abbildung, die die Restriktion der $f$ zu $C$ gennant wird, bei $f|_C : C \to B$, $f|_C(x) = f(x)$ für alle $x \in C$.

(d) Die folgende Korrespondenzen sind keine Abbildungen:




**Definition 1.3.5.** Sei $f : A \to B$ eine Abbildung und seien $X \subseteq A$ und $Y \subseteq B$ zwei Teilmengen (von $A$ bzw $B$). Man definiert:

(a) Das Bild von $X$ unter $f$, bei

$$f(X) = \{f(x) \mid x \in X\} = \{y \in B \mid \exists x \in X \text{ so dass } f(x) = y\}.$$

Im Fall $X = A$ spricht man über das Bild von $f$, nämlich $f(A) = \mathrm{Im} f$.

(b) Das Gegenbild (inverse Bild) von $Y$ unter $f$, durch

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}.$$

**Definition 1.3.6.** Sind $f : A \to B$ und $g : B \to C$ Abbildungen, so definiert man die *zusammengesetzte Abbildung* oder die *Komposition* $g \circ f : A \to C$, $(g \circ f)(x) = g(f(x))$ für alle $x \in A$.

**Theorem 1.3.7.** *Wenn sie definiert ist, ist die Zusammmengesetztung der Abblidungen assoziativ, d. h. wenn* $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ *dann* $(h \circ g) \circ f = h \circ (g \circ f)$. *Die Identitätsabbildung wirkt als neutrales Element für die Zusammengesetztung, d.h. wenn* $A \xrightarrow{f} B$ *dann* $f = f \circ 1_A = 1_B \circ f$.

*Beweis.* □

**Definition 1.3.8.** Sei $f : A \to B$ eine Abbildung. Man nennt $f$ *invertierbar* wenn eine Abbildung $f' : B \to A$ existiert, so dass $f' \circ f = 1_A$ und $f \circ f' = 1_B$.

**Satz 1.3.9.** *Ist* $f : A \to B$ *invertierbar, so ist die Abbildung* $f' : B \to A$ *bei der Eigenschaften* $f' \circ f = 1_A$ *und* $f \circ f' = 1_B$ *eindeutig bestimmt. Man schreibt* $f^{-1} = f'$, *und man nennt es die Inverseabbildung von* $f$. *Es gilt also* $(f^{-1})^{-1} = f$.

*Beweis.* □

**Beispiel 1.3.10.** $\exp : \mathbb{R} \to (0, \infty)$, $\exp(x) = e^x$ ist inverierbar und hat die Inverse $\ln : (0, \infty) \to \mathbb{R}$. Man bemerke den Zusammenhang zwischen invertierbare Abbildungen und die Lösung der Gleichungen!

**Satz 1.3.11.** *Sind* $A \xrightarrow{f} B \xrightarrow{g} C$ *zwei invertierbare Abbildungen, so ist* $g \circ f$ *auch, und gilt es* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

*Beweis.* □

**Injektivität, Surjektivität, Bijektivität.**

**Definition 1.3.12.** Sein $f : A \to B$ eine Abbildung: Man nennt $f$:

(a) *injektiv* falls für $x_1, x_2 \in A$, $x_1 \neq x_2$ impliziert $f(x_1) \neq f(x_2)$.
(b) *surjektiv* falls für alle $y \in B$ es gibt $x \in A$ so dass $f(x) = y$.
(c) *bijektiv* falls $f$ inketiv und surjektiv ist.

**Bemerkung 1.3.13.** Äquivalent ist eine Abbildung $f : A \to B$

(a) injektiv falls $x_1, x_2 \in A$, $f(x_1) = f(x_2)$ implieziert $x_1 = x_2$.
(b) surjektiv falls $f(A) = B$.

**Bemerkung 1.3.14.** Sei $f : A \to B$ eine Abbildung. Dann ist $f$ injektiv, surjektiv oder bijektiv gdw für irgendeine $y \in B$ die Gleichung $f(x) = y$ hat höchstens, mindestens, bzw genau eine Lösung $x \in A$.

**Satz 1.3.15.** *Seien $A \xrightarrow{f} B \xrightarrow{g} C$ zwei Abbildungen. Die folgende Ausagen gelten:*

(a) *Sind $f$ und $g$ injektiv, so ist $g \circ f$ auch.*
(b) *Sind $f$ und $g$ surjektiv, so ist $g \circ f$ auch.*
(c) *Sind $f$ und $g$ bijektiv, so ist $g \circ f$ auch.*
(d) *Ist $g \circ f$ injektiv, so ist $f$ auch.*
(e) *Ist $g \circ f$ surjektiv, so ist $g$ auch.*
(f) *Ist $g \circ f$ bijektiv, so ist $f$ injektiv und $g$ surjektiv.*

*Beweis.* □

**Satz 1.3.16.** *Sei $f : A \to B$ eine Abbildung, und $A \neq \emptyset$. Die folgende Aussagen sind äquivalent:*

(i) *$f$ ist injektiv.*
(ii) *$f$ hat eine Linksinverse, d.h. existiert $g : B \to A$, so dass $g \circ f = 1_A$.*
(iii) *$f$ ist links verzürzbar, d.h. wenn $h_1, h_2 : A' \to A$ sind Abbildungen, so dass $f \circ h_1 = f \circ h_2$ dann $h_1 = h_2$.*

*Beweis.* □

**Satz 1.3.17.** *Sei $g : B \to A$ eine Abbildung. Die folgende Aussagen sind äquivalent:*

(i) *$g$ ist surjektiv.*
(ii) *$g$ hat eine Rechtsinverse, d.h. existiert $f : A \to B$, so dass $g \circ f = 1_A$.*
(iii) *$g$ ist rechts verzürzbar, d.h. wenn $k_1, k_2 : A' \to A$ sind Abbildungen, so dass $k_1 \circ g = k_2 \circ g$ dann $k_1 = k_2$.*

*Beweis.* □

**Theorem 1.3.18.** *Sei $f : A \to B$ eine Abbildung. Die folgende Aussagen sind äquivalent:*

(i) *$f$ ist bijektiv.*
(ii) *$f$ ist invertierbar.*
(iii) *$f$ ist links und rects verzürzbar.*

*Beweis.* □

**Die Kardinalanzahl einer Menge.**

**Definition 1.3.19.** Man sagt dass zwei Mengen $A$ und $B$ *haben dieselbe Kardinalanzahl* falls eine bijektion $f : A \to B$ gibt. Eine Menge $A$ ist endlich falls $A = \emptyset$ oder $n \in \mathbb{N}^*$ existiert so dass $A$ und $\{1, 2, \ldots, n\}$ dieselbe Kardinalanzahl haben. Im lezten Fall die naturliche Zahl $n$ ist eindeutig bestimmt, weil keine Bijektion zwischen $\{1, 2 \ldots, n\}$ und $\{1, 2, \ldots, m\}$ mit $n \neq m$ existiert; man sagt $A$ hat die Kardinalanzahl $n$, und man schriebt $|A| = n$ oder $\sharp A = n$. Die leere Menge hat keine Elemente, und ihrer Kardinalanzahl ist null; man schreibt $|\emptyset| = 0$.

**Bemerkung 1.3.20.** Für endliche Mengen ist die Kardinalanzahl einfach die Anzahl der Elementen. Aber Kardinalanzahlen können auch für unendliche Mengen definiert werden, und dadurch die "große" dieser unendlichen Mengen vergleichen.

**Satz 1.3.21.** *Für eine endliche Menge $A$ und eine Abbildung $f : A \to A$ sind die folgende Aussagen äquivalent:*
(i) *$f$ ist injektiv.*
(ii) *$f$ ist surjektiv.*
(iii) *$f$ ist bijektiv.*

*Beweis.* □

**Bemerkung 1.3.22.** Eine Unendliche Menge $A$ wird charakterisiert durch die Eigenschaft, dass eine injektive (oder surjektive) Abbildung $f : A \to A$ existiert so dass $f$ ist nicht bijektiv.

**Definition 1.3.23.** Für eine Teilmenge $X$ von $A$ ist die charakteristische Funktion $\chi_X : A \to \{0, 1\}$ von $X$ (bezüglich $A$) definiert durch

$$\chi_X(x) = \begin{cases} 1 \text{ falls } x \in X \\ 0 \text{ falls } x \notin X \end{cases}$$

**Lemma 1.3.24.** *Für jede Menge $A$ ist die Abbildung $\chi : \mathcal{P}(A) \to \{0, 1\}^A$, $\chi(X) = \chi_X$ eine Bijektion.*

*Beweis.* □

**Korollar 1.3.25.** *Für jede Menge $A$ gilt $|\mathcal{P}(A)| = |\{0, 1\}^A|$ und die Mengen $A$ und $\mathcal{P}(A)$ haben nicht dieselbe Kardinalanzahl.*

*Beweis.* □

**Das Cartesisches Produkt.**

**Satz 1.3.26.** *Man betrachte die Mengen $A_1, A_2, \ldots, A_n$, wobei $n \in \mathbb{N}^*$. Man zeige dass*

$$\phi : A_1 \times A_2 \times \ldots \times A_n \to (A_1 \cup A_2 \cup \ldots \cup A_n)^{\{1,2,\ldots,n\}} \textit{ wobei}$$
$$\phi(a_1, a_2, \ldots, a_n)(i) = a_i, \textit{ für alle } i \in I$$

*eine injektive Abbildung ist, mit dass Bild*

$$\mathrm{Im}\phi = \{f \in (A_1 \cup A_2 \cup \ldots \cup A_n)^{\{1,2,\ldots,n\}} \mid f(i) \in A_i \textit{ für alle } i \in I\}.$$

*Folglich induziert $\phi$ eine Bijektion $A_1 \times A_2 \times \ldots \times A_n \to \mathrm{Im}\phi$, $(a_1, a_2, \ldots, a_n) \mapsto \phi(a_1, a_2, \ldots, a_n)$.*

*Beweis.* □

Der vorige Satz erlaubt uns zu erweitern die Definition des Cartesishes Produkt im Fall einer möglich unendlichen Familie von Mengen:

**Definition 1.3.27.** Man betrachten die Familie von Mengen $A_i$ mit $i \in I$. Durch Definition ist das Cartesiscshes Produkt dieser Familie:

$$\prod_{i\in I} A_i = \left\{ f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i \text{ für alle } i \in I \right\}.$$

**Bemerkung 1.3.28.** (1) Falls in der vorigen Definition $A_i = A$ für alle $i \in I$ gilt, dann haben wir:

$$A^I = \prod_{i\in I} A_i = \{f : I \to A \mid f \text{ eine Abbildung ist}\}$$

(man vergleiche mit der Notation $B^A$ aus der Definition 1.3.1).

(2) Die Existenz des Cartesisches Produkt erfordet eine spezielle mengentheoretisch Axiom, nämlich die Axiom der Wahl. Obschon intuitiv klar ist, ist formell nicht möglich ohne diese Axiom eine Abbildung $f : I \to \bigcup_{i\in I} A_i$ zu bilden, so dass $f(i) \in A_i$ für alle $i \in I$ (d. h. zu wählen die Elemente $f(i) \in A_i, i \in I$).

**Operationen.**

**Definition 1.3.29.** Sei $A$ eine Menge. Eine *(binäre) Operation* (oder *Verknupfung*) auf $A$ ist eine Abbildung $* : A \times A \to A$. Oft schreibt man $a * b$ statt $*(a, b)$.

**Definition 1.3.30.** Sei $* : A \times A \to A$ eine Operation auf $A$. Die Operation $*$ nennt man:

(a) *assoziativ* falls $a * (b * c) = (a * b) * c$ für alle $a, b, c \in A$.
(b) *kommutativ* falls $a * b = b * a$ für alle $a, b \in A$.

Ein Element $e \in A$ mit der Eigenschaft $e * a = a * e = a$ für alle $a \in A$ heißt *neutrales Element* für $*$. Hat die Operation $*$ ein neutrales Element $e$, so nennt man ein Element $x \in A$ *invertierbar* falls $x' \in A$ existiert, so dass $x*x' = e = x' * x$.

**Satz 1.3.31.** *Wenn eine Operation $* : A \times A \to A$ ein neutrales Element besitzt, dann ist es eindeutig.*

*Beweis.* □

**Satz 1.3.32.** *Man betrachte eine assoziative Operation $* : A \times A \to A$ die ein neutrales Element $e$ besitzt.*

(a) *Ist $x \in A$ invertierbar, so ist $x' \in A$ mit der Eigenschaft $x * x' = e = x' * x$ eindeutig. Man bezeichent es mit $x^{-1}$ und man nennt es das Inverseelement von $x$. Mehr, gilt es $(x^{-1})^{-1} = x$.*
(b) *Sind $x, y \in A$ invertierbare Elemente, so ist $x * y$ auch, und es gilt $(xy)^{-1} = y^{-1}x^{-1}$.*

*Beweis.* □

**Definition 1.3.33.** Ein *Monoid* ist ein Paar $(M, *)$ wobei $M$ eine Menge ist zusammen mit einer assoziativen Operation $* : M \times M \to M$, die ein neutrales Element besitzt. Sind $(M, *)$ und $(N^8)$ Monoide, so heißt *Monoidhomomorphismus* eine Abbildung $f : M \to N$ mit der Eigenschaft $f(x*y) = f(x)*f(y)$ f ür alle $x, y \in M$.

**Beispiel 1.3.34.** (1). Die folgende Paaren sind Monoide: $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{Q},\cdot)$, $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$, $(\mathbb{C},+)$, $(\mathbb{C},\cdot)$.

(2) Sind $(M,*)$ und $(N,*)$ Monoide so sind $1_M : M \to M$ und $\overline{e} : M \to N$, $\overline{e}(x) = e$ für alle $x \in M$ Monoidhomomorphismen.

**Übungen zu Abbildungen.**

**Übung 1.3.35.** Man betrachte die Abbildungen:
(1) $f_1 : \mathbb{R} \to \mathbb{R}$, $f_1(x) = x^2$
(2) $f_2 : [0,\infty) \to \mathbb{R}$, $f_2(x) = x^2$
(3) $f_3 : \mathbb{R} \to [0,\infty)$, $f_3(x) = x^2$
(4) $f_4 : [0,\infty) \to [0,\infty)$, $f_4(x) = x^2$.
Man entscheide für jede Abbildung ob sie injektiv, surjektiv oder bijektiv ist.

**Übung 1.3.36.** Für die folgende Abbildungen entscheide man ob sie injektiv, surjektiv oder bijektiv sind. Wenn es existiert, bestimme man die Inverseabbildung:
(1) $f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} 2x+1 \text{ falls } x \le 1 \\ x+2 \text{ falls } 1 < x \end{cases}$
(2) $f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} x^2+1 \text{ falls } x \le 0 \\ -x+2 \text{ falls } 0 < x \end{cases}$
(3) $f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} 2x+1 \text{ falls } x \le 0 \\ x+2 \text{ falls } 0 < x \end{cases}$

**Übung 1.3.37.** Man entcheide wenn die Zusammengesetzungen $f \circ g$ und $g \circ f$ sind definiert, und wenn ja, berechne man die Komposition der folgenden Abbildungen:
(1) $f,g : \mathbb{R} \to \mathbb{R}\ f(x) = \begin{cases} x^2-1 \text{ falls } x \le -1 \\ x-1 \text{ falls } \ -1 < x \end{cases}$ und $g(x) = \begin{cases} -x+1 \text{ falls } x < 3 \\ x-2 \text{ falls } 3 \le x \end{cases}$
(2) $f : \mathbb{R} \to [0,\infty), f(x) = |x|$ und $g : \mathbb{N}^* \to \mathbb{R}, g(x) = 1/x$.
(3) $f : R \to [0,\infty), f(x) = x^2+1$ und $g : [0,\infty) \to \mathbb{R}, g(x) = \sqrt{x}$.

**Übung 1.3.38.** Seien $A$, $B$, $C$ Mengen so dass $C \subseteq A$ und sei $f : A \to B$ eine Abbildung. Man zeige, dass $f|_C : f \circ i$, wobei $i : A \to C$ die Inklusionsabbildung ist.

**Übung 1.3.39.** Sei $f : A \to B$ eine inverierbare Abbildung und sei $Y \subseteq B$. Dann durch $f^{-1}(Y)$ können wir entweder das Gegenbild von $Y$ unter $f$oder das Bild von $Y$ unter $f^{-1}$ meinen. Man zeige dass die beide Meinungen sind gleich.

**Übung 1.3.40.** Man finde ein Beispiel von zwei Abbildungen $f, g : \mathbb{N} \to \mathbb{N}$ so dass $g \circ f \ne f \circ g$. (Obwohl die Komposition ist zweiseitig definirt, ist sie nicht kommutativ).

**Übung 1.3.41.** Man zeige, dass jede Abbildung $f : A \to B$ als eine zusammengesetzte Abbildung $f = i \circ p$ geschrieben lass, wobei $i = i_f$ injektiv ist und $p = p_f$ surjektiv ist.

**Übung 1.3.42.** Man finde je ein Beispiel das aus einer Abbildung $f : A \to B$ entsteht, so dass:
(1) $f$ injektiv ist aber sie keine Linksinverse hat.
(2) $f$ hat genau eine Linksinverse, aber sie ist nicht bijektiv.
(3) $f$ hat genau zwei Linksinversen.
(4) $f$ hat unendlich viele Linksinversen.

**Übung 1.3.43.** Man finde je ein Beispiel das aus einer Abbildung $g : B \to A$ entsteht, so dass:

(1) $g$ hat genau zwei Rechtsinversen.
(2) $g$ hat unendlich viele Rechtsinversen.

Man zeige, dass $g$ genau eine Rechtsinverse hat gdw $g$ bijektiv ist.

**Übung 1.3.44.** Man finde je ein Beispiel das aus zwei Abbildungen $A \xrightarrow{f} B \xrightarrow{g} C$ entsteht, so dass:

(1) $g \circ f$ injektiv ist, aber $g$ nicht injektiv ist.
(2) $g \circ f$ surjektiv ist, aber $f$ nicht surjektiv ist.
(3) $g \circ f$ bijektiv ist, aber $g$ nicht injektiv ist und $f$ nicht surjektiv ist.

**Übung 1.3.45.** Sei $f : A \to B$ eine Abbildung, und seien $X, X_1, X_2 \subseteq A$ und $Y, Y_1, Y_2 \subseteq B$ Teilmengen. Man zeige:

(1) $X \subseteq f^{-1}(f(X))$.
(2) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
(3) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.
(4) $f(f^{-1}(Y) \subseteq Y$.
(5) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
(6) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

**Übung 1.3.46.** Für eine Abbildung $f : A \to B$ sind die folgende Aussagen äquivalent:

(i) $f$ ist injektiv.
(ii) $X = f^{-1}(f(X))$ für irgendeine Teilmenge $X \subseteq A$.
(iii) $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ für irgendzweie Teilmengen $X_1, X_2 \subseteq A$.

Man finde je ein Beispiel, um zu zeigen dass die Injektivität von $f$ ist notwendig für die beide Gleichungen (2) und (3).

**Übung 1.3.47.** Für eine Abbildung $f : A \to B$ sind die folgende Aussagen äquivalent:

(i) $f$ ist surjektiv.
(ii) $f(f^{-1}(Y)) = Y$ für irgendeine Teilmenge $Y \subseteq B$.

Man finde ein Beispiel, um zu zeigen dass die Surjektivität von $f$ ist notwendig für die Gleichung (2).

**Übung 1.3.48.** Seien $A$ und $B$ endliche Mengen mit $|A| = n$ und $|B| = m$. Man finde $|B^A|$. Hinweis: Man zeige durch Induktion nach $n$ dass $|B^A| = m^n$.

**Übung 1.3.49.** Seien $A$ und $B$ endliche Mengen mit $|A| = n$ und $|B| = m$. Man finde die Anzahl aller injektiven Abbildungen von $A$ nach $B$. Hinweis: die Anzahl ist $A_m^n = \frac{m!}{(m-n)!}$.

**Übung 1.3.50.** Sei $A$ eine endliche Menge mit $|A| = n$. Man finde die Anzahl aller bijektiven Abbildungen $f : A \to A$ (aller Permutationen).

**Übung 1.3.51.** Sei $B$ eine endliche Menge mit $|B| = m$. Man finde die Anzahl aller Teilmengen von $B$ mit $n$ Elementen. Hinweis: die Anzahl ist $\binom{m}{n} = \frac{m!}{n!(m-n)!}$.

**Übung 1.3.52.** Man zeige: $\sum_{i=0}^{n} \binom{m}{i} = 2^m$.

**Übung 1.3.53.** (das Prinzip von Inklusion und Exklusion) Seien $A_1, A_2, \dots, A_n$ endliche Mengen, wobei $n \in \mathbb{N}^*$. Dann:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

$$|A_1 \cap A_2 \cap \ldots \cap A_n| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cup A_j| + \sum_{1\le i<j<k\le n} |A_i \cup A_j \cup A_k| - \ldots + (-1)^{n-1}|A_1 \cup A_2 \cup \ldots \cup A_n|.$$

**Übung 1.3.54.** Seien $A$ und $B$ Mengen, mit $|A| = n$ und $|B| = m$. Man finde die Anzahl aller surjektiven Abbildungen $f : A \to B$.

**Übung 1.3.55.** Man zeige dass die Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ dieselbe Kardinalanzahl haben.

**Übung 1.3.56.** Man zeige dass $\mathbb{N}$ und $\mathbb{R}$ nicht dieselbe Kardinalanzahl haben. Hinweis: Man zeige, dass $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

**Übung 1.3.57.** Sei $A$ eine endliche Menge mit $|A| = n$.
(1) Wieviele Operationen auf $A$ definieren lassen?
(2) Wieviele davon sind kommutativ?
(3) Wieviele davon ein neutrales Element besizt?

**Übung 1.3.58.** Man betrachte die Operation $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, gegeben durch $x * y = xy + 2ax + by$, für alle $x, y \in \mathbb{R}$. Man bestimme $a, b \in \mathbb{R}$, so dass $*$ assoziativ und kommutativ sei.

**Übung 1.3.59.** Sei $A$ eine Menge (die *Alphabet* gennant wird), und sei $W = W(A) = \bigcup_{n\in\mathbb{N}} A^n$ (die *Menge aller Wörter über* $A$). Hier $A^0 = \{\lambda\}$, wobei $\lambda$ das leeres Wort ist, und $A^n = \{x_1x_2 \dots x_n \mid x_1, x_2, \dots, x_n \in A\}$. Als eine Ausnahme von der allgemeinen Regel, bezeichnet wir hier $x_1x_2 \dots x_n = (x_1, x_2, \dots, x_n)$, so ist $A^n$ die Menge aller Wörter von länge $n$. Man zeige, dass $(W, \cdot)$ ein Monoid ist wobei

$$(x_1x_2 \dots x_n) \cdot (y_1y_2 \dots y_m) = x_1x_2 \dots x_ny_1y_2 \dots y_m \in A^{n+m}.$$

Mehr da $A^1 = A$ gilt, können wir $A$ als eine Teilmenge von $W$ betrachten. Ferner zeige man, dass $(W, \cdot)$ das freies Monoid über $A$ ist, d. h. für jedes Monoid $(M, *)$ und jede Abbildung $f : A \to M$, existiert ein einziges Monoidhomomorphismus $\overline{f} : W \to M$, so dass $\overline{f}|_A = f$.

1.4. **Relationen.**

**Definition 1.4.1.** Eine *Relation* ist ein Tripel $(A, B, R)$, wobei $A$ und $B$ beliebige Mengen sind, und $R \subseteq A \times B$. Manchmal notieren wir $r = (A, B, R)$ und schrieben wir $arb$ stat $(a, b) \in R$, manchmal schrieben wir nur $R \subseteq A \times B$ um die Relation zu bezeichen. Wie im Fall der Abbildungen $A$ und $B$ werden *Definitionsbereich* bzw *Wertensbereich* gennant. Ist $A = B$ so nennt man die Relation $R \subseteq A \times A$ *homogen*.

**Bemerkung 1.4.2.** Abbildungen können als spezielle Relationen betracht werden, nämlich eine Abbildung $f : A \to B$ ist eine Relation $f = (A, B, F)$ mit der zusätzliche Eigenschaft, dass für jedes Element $x \in A$ es gibt ein einzelnes Element $y \in B$ so dass $xfy$. In diesem Fall $F = \{(a, f(a)) \mid a \in A$ ist der Graph der Abbildung.

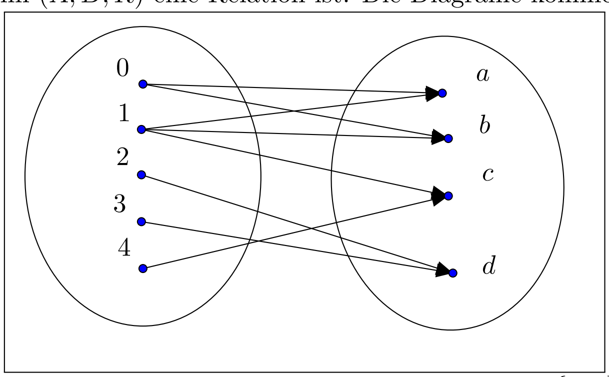
**Beispiel 1.4.3.** Die folgende Beispiele sind Relationen die keine Abbildungen sind:

(1) Die gewönliche kleiner oder Gleich Beziehung ist eine homogene Relation auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$.
(2) Die Teilbarkeit $a|b$ gdw existiert $c$ so dass $b = ac$ ist eine homogene Relation auf $\mathbb{N}$ oder $\mathbb{Z}$.
(3) Sei $n \in \mathbb{N}$, $n > 1$. Die Kongruenz modulo $n$ ist eine homogene Relation auf $\mathbb{Z}$. Erinnerung: Die Kongruenz modulo $n$ wird durch $x \equiv y( \mod n)$ gdw $n|(x-y)$ definiert.
(4) Für jede Menge $A$ ist $\in$ eine Relation zwischen $A$ und $\mathcal{P}(A)$.

**Beispiel 1.4.4.** Für jede Menge ist die Gleichung eine homogene Relation auf $A$. Man bemerke, dass diese Relation auch eine Abbildung ist, nämlich die identische Abbildung der Menge $A$.

**Bemerkung 1.4.5.** Wie im Fall der Abbildungen, es gibt verschiedene Weisen durch die eine Relation gegeben werden kann:

(1) Duch direckte Angabe der Paaren die in Relation sind, z. B. fals $A = \{0, 1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ und $R = \{(0, a), (0, b), (1, a), (1, b), (1, c), (2, d), (3, d), (4, c)\}$, dann $(A, B, R)$ eine Relation ist. Die Diagrame kommen auch hier zu hilfe:




(2) Durch eine Matrix mit Eingaben in der Menge $\{0, 1\}$: Man betrachte zwei endliche Mengen $A = \{a_1, a_2, \ldots, a_m\}$ und $B = \{b_1, b_2, \ldots, b_n\}$ und eine Relation $R \subseteq A \times B$. Diese Relation kann durch eine Matrix $M(R) = (m_{i,j}) \in \mathbb{M}_{m\times n}(\{0, 1\})$ dargestellt werden, wobei

$$m_{i,j} = \begin{cases} 1 \text{ falls } (a_i, b_j) \in R \\ 0 \text{ falls } (a_i, b_j) \notin R \end{cases}$$

Z.B die matrix der vorigen Relation ist:

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Hier $\mathbb{M}_{m\times n}(\{0, 1\})$ bezeichnet die Menge aller Matrizen (d. h. rechteckige Tabelle) mit $m$ Reihen und $n$ Spalten und Eingaben in $\{0, 1\}$.
(3) Durch eine Beziehung zwischen die Elementen die in Relation sind, als im Beispiel 1.4.3.

**Definition 1.4.6.** Für jede Relation $(A, B, R)$ definiert man die Inverserelation durch $(B, A, R^{-1})$, wobei $(b, a) \in R^{-1}$ gdw $(a, b) \in R$ für jede Paar $(a, b) \in A \times B$.

**Bemerkung 1.4.7.** Für jeder Relation $(A, B, R)$ lässt sich Die Inverserelation defieneren werden. Wie jede Abbildung als eine Relation betrachten kann, ist jede Abbildung invertierbar als Relation. Aber ist die Inverserelation einer Abbildung genau dann eine Abbildung wenn die Abbildung bijektv ist.

**Definition 1.4.8.** Sei $r = (A, B, R)$ eine Relation, und $X \subseteq A$, $Y \subseteq B$ Teilmengen. Man definiert $r(X) = \{y \in B \mid \text{es gibt } x \in A \text{ so dass } xry\}$ and $r^{-1}(Y) = \{x \in A \mid \text{es gibt } y \in B \text{ so dass } xry\}$.

**Bemerkung 1.4.9.** Für eine Relation $r = (A, B, R)$ und eine Teilmenge $Y \subseteq B$ gilt es $(r^{-1})(Y) = r^{-1}(Y)$.

**Definition 1.4.10.** Sind $(A, B, R)$ und $(C, D, S)$ zwei Relationen, so definiert man die Zusammengesetzte Relation durch $(A, D, S \circ R)$ wobei

$$S \circ R = \{(a, d) \mid \text{es gibt } x \in B \cap C \text{ so dass } (a, x) \in B \text{ und } (x, d) \in S\}.$$

**Bemerkung 1.4.11.** Um die Zusammengesetzterelation defienert sein ist es nich notwending, wie im Fall der Abbildungen, der Wertensbereich der ersten gleich zum Definitionsbereich der zweiten Relation sein.

**Definition 1.4.12.** Eine homogene Relation $r = (A, A, R)$ nennt man:

(a) *reflexiv* falls $ara$ für alle $a \in A$.
(b) *transitiv* falls für alle $a, b, c \in A$ aus $arb$ und $brc$ folgt $arc$.
(c) *symmetrisch* falls für alle $a, b \in A$ aus $arb$ folgt $bra$.
(d) *antisymmetrisch* falls für alle $a, b \in A$ aus $arb$ und $bra$ folgt $a = b$.

Man nennt *Präordnung* eine homogene Relation die reflexiv und transitiv ist.

**Äquivalenzrelationen.**

**Definition 1.4.13.** Sei $A$ eine Menge. Eine *Äquivalenzrelation* (oder kürzer *Äquivalenz*) auf $A$ ist eine Präordung die auch symmetrisch ist, d.h eine homogene Relation auf $A$ die reflexiv, transitiv und symmetrisch ist.

**Beispiel 1.4.14.** Die folgende Relationen sind Äquivalenzen:

(1) Die Gleicheitrelation auf einer beliebigen Menge.
(2) Die Kongurenz der Dreiecken (auf der Menge aller Draiecken aus der Ebene).
(3) Die Änlichkeit der Dreiecken (auf der Menge aller Draiecken aus der Ebene).

**Definition 1.4.15.** Sei $\equiv$ eine Äquivalenzrelation auf einer Menge $A$. Für $a \in A$ bezeichent man

$$[a] = [a]_{\equiv} = \{x \in A \mid a \equiv x\}$$

die *Äquivalenzklasse* von $a$. Man nennt die *Faktormenge* von $A$ modulo $\equiv$ die Menge aller Äquivalenzklassen, d.h.

$$A/_{\equiv} = \{[a] \mid a \in A\}.$$

Die Abbildung $p = p_{\equiv} : A \to A/_{\equiv}$ gegeben durch $p(x) = [x]$ wird die *kanonische Projektion* von $A$ nach $A/_{\equiv}$ gennant.

**Bemerkung 1.4.16.** In der Definition der Faktormenge ist es möglich (und auch sehr wahrscheinlich) einige Elemente mehrmal erscheinen. Wir wissen dass is einer Menge, ein Element erscheint nur einmal. Aber es Aufmeksamkeit erfördet, da eine falsche Benützung zu nicht wohl definierte Abbildungen führen kann.

**Satz 1.4.17.** *Sei $(A, A, \equiv)$ eine Äquivalenzrelation auf einer Menge $A$, und $a, b \in A$. Dann gilt:*
(a) *$a \in [a]$, so ist $[a] \neq \emptyset$.*
(b) *$[a] = [b]$ gdw $a \equiv b$.*
(c) *$[a] \cap [b] \neq \emptyset$ gdw $[a] = [b]$.*
(d) *$\bigcup_{x \in A} [x] = A$.*

*Beweis.* □

**Definition 1.4.18.** Sei $A$ eine Menge. Eine Partition der Menge $A$ ist eine Teilmenge $\pi \subseteq \mathcal{P}(A)$ (d. h. eine Menge derer Elemente sind Teilmengen von $A$), so dass:
(a) $\emptyset \notin \pi$.
(b) Wenn $X, Y \in \pi$ so dass $X \cap Y \neq \emptyset$ dann $X = Y$.
(c) $\bigcup_{X \in \pi} X = A$.

**Theorem 1.4.19.** *Sei $A$ eine Menge.*
(1) *Ist $(A, A, \equiv)$ eine Äquivalenzrelation auf $A$, so ist $A/_\equiv$ eine Partition der Menge $A$.*
(2) *Ist $\pi \subseteq \mathcal{P}(A)$ eine Partition der Menge $A$, so ist $(A, A, \equiv_\pi)$ eine Äquivalenzrelation auf $A$, wobei für jedewelche $a, b \in A$ wir haben*
$$a \equiv_\pi b \text{ genau dann wenn } X \in \pi \text{ existiert, so dass } a, b \in X.$$
(3) *Die Verfahren (1) and (2) beschreiben zwei gegenseitige Inverseabbildungen, zwischen die Menge aller Äquivalenzrelationen auf $A$ und die Menge aller Partitionen der Menge $A$.*

*Beweis.* □

**Ordnungsrelationen.**

**Definition 1.4.20.** Sei $A$ eine Menge. Eine *Ordungsrelation* (oder kürzer *Ordnung*) auf $A$ ist eine Präordung die auch symmetrisch ist, d.h eine homogene Relation auf $A$ die reflexiv, transitiv und antisymmetrisch ist.

Häufig notiert man $\leq$ eine Odnungsrelation, und man sagt, dass $(A, \leq)$ eine geordnete Menge ist. In diesem Fall man schriebt $x < y$ für $x \leq y$ und $x \neq y$.

**Beispiel 1.4.21.** Die folgende Relationen sind Ördnungen:
(1) Die Gleicheitrelation auf einer beliebigen Menge.
(2) Die gewönliche kleiner oder gleich Beziehung auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ oder $\mathbb{R}$.
(3) Die Eingeschlossenheit auf einer Menge derer Elemente sind Mengen, z. B. $(\mathcal{P}(A), \subseteq)$, wobei $A$ eine beliebige Menge ist.

Man bemerke, dass in $(\mathbb{R}, \leq)$ gilt $x, y \in \mathbb{R} \Rightarrow x \leq y$ oder $y \leq x$ (d. h. $(\mathbb{R}, \leq)$ ist eine *Kette*) aber $(\mathcal{P}(A), \subseteq)$ keine Kette ist, da $X, Y \in \mathcal{P}(A)$ existieren so dass $X \nsubseteq Y$ und $Y \nsubseteq X$ (für $|A| \geq 2$).

**Definition 1.4.22.** Sei $(A, \leq)$ eine geordnete Menge. Ein Element $a \in A$ heißt:

(a) *minimal* fals für jedes $x \in A$ wenn $x \leq a$ dann $x = a$.
(b) *maximal* fals für jedes $x \in A$ wenn $a \leq x$ dann $x = a$.
(c) das *kleinste Element* von $A$ wenn $a \leq x$ für alle $x \in A$.
(d) das *größte Element* von $A$ wenn $x \leq a$ für alle $x \in A$.

**Bemerkung 1.4.23.** Sei $(A, \leq)$ eine geordnete Menge. Man bezeichne $\geq = \leq^{-1}$, d. h. $x \geq y$ gdw $y \leq x$. Es ist leicht zu verifizieren (Übung 1.4.48), dass $\geq$ eine Ordnunsrelation ist. Man bemerke, dass $a \in A$ ist minimal oder das kleinste Element in $(A, \leq)$ gdw $a$ ist maximal bzw das größte Element in $(A, \geq)$ und umgekehrt.

**Lemma 1.4.24.** *Sei $(A, \leq)$ eine geordnete Menge. Falls $A$ die kleinste (größte) Element besitzt, ist dieses Element die einzges minimalen (maximalen) Element auch.*

**Korollar 1.4.25.** *Der kleinste/größte Element einer geordnete Menge, falls existiert, ist eindeutig.*

*Beweis.* □

**Theorem 1.4.26.** *Für eine geordnete Menge $(A, \leq)$ sind die folgende Aussagen äquivalent:*

(i) *Jede nicht leere Teilmenge von $A$ ein minimales Element besitzt (die Minimalitätsbedingung).*
(ii) *Jede fallende Kette von Elementen aus $A$ ist endlich, d. h. falls $a_0 \geq a_1 \geq a_2$ ldots mit $a_0, a_1, a_2, \ldots \in A$, dann existiert $n \in \mathbb{N}$ so dass $a_n = a_{n+1} = \ldots$ (die Bedingung der fallenden Ketten).*
(iii) *Ist $B \subseteq A$ eine Menge mit der Eigenschaften*
   (a) *$B$ enthält alle minimal Elemente aus $A$;*
   (b) *für $a \in A$ wenn $\{x \in A \mid x < a\} \subseteq B$ dann $a \in B$;*
   *so gilt $B = A$ (die Induktivitätsbedingung).*

*Beweis.* □

**Definition 1.4.27.** Sei $(A, \leq)$ eine geordnete Menge und $X \subseteq A$. Eine untere/obere Schranke von $X$ ist ein Element $a \in A$ so dass, $a \leq x$, bzw. $x \leq a$ für alle $x \in X$. Man nennt das Infimum (Supremum) von $X$ in $A$ die größte (bzw. kleinste) untere (obere) Schranke von $X$, d.h.

$$\inf X \in A \text{ gdw } \begin{cases} a \leq x \text{ für alle } x \in X \\ \text{wenn } a' \in A \text{ so dass } a' \leq x \text{ für alle } x \in X \text{ dann } a' \leq a. \end{cases}$$

$$\sup X = a \in A \text{ gdw } \begin{cases} x \leq a \text{ für alle } x \in X \\ \text{wenn } a' \in A \text{ so dass } x \leq a' \text{ für alle } x \in X \text{ dann } a \leq a'. \end{cases}$$

**Bemerkung 1.4.28.** Sei $(A, \leq)$ eine geordnete Menge und $X \subseteq A$.

(1) Falls existieren, sind $\inf X$ und $\sup X$ eindeutig.
(2) Existiert das kleinste (größte) Element $a$ von $X$ so gilt $a = \inf X$ ($a = \sup X$).

**Beispiel 1.4.29.** (1) In $(\mathbb{R}, \leq)$ gilt es $\inf(0,1) = \inf[0,1] = 1$, $\sup\{x \in \mathbb{R} \mid x^2 < 2\} = \sqrt{2}$ und existieren nicht $\inf \mathbb{Z}$ und $\sup(0, \infty)$.
(2) In $(\mathbb{Q}, \leq)$ existiert nicht $\sup\{x \in \mathbb{Q} \mid x^2 < 2\}$.

(3) In einer geordneten Menge $(A, \leq)$ genau dann $\inf \emptyset$ ($\sup \emptyset$) existiert wenn $A$ das größte (bzw. kleinste) Element $a$ besitzt, und gilt $\inf \emptyset = a$ ($\sup \emptyset = a$).

**Definition 1.4.30.** Ein *Verband* ist eine geordnete Menge $(L, \leq)$ mit der Eighenschaft, $\inf\{x, y\}$ und $\sup\{x, y\}$ existieren für jede zwei Elementen $x, y \in L$. Man schreibt $x \vee y = \sup\{x, y\}$ und $x \wedge y = \inf\{x, y\}$. Der Verband $L$ wird *vollständig* gennant, falls $\inf(X)$ und $\sup(X)$ existieren, für jede Teilmenge $X \in L$.

**Theorem 1.4.31.** *Für einen Verband $(L, \leq)$ gelten die Eigenschaften:*
(a) $x \vee (y \vee z) = (x \vee y) \vee z$ *und* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *(Assoziativität).*
(b) $x \vee y = y \vee x$ *und* $x \wedge y = y \wedge x$ *(Kommutativität).*
(c) $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ *(Absorbtion).*
*für alle* $x, y, z \in L$.

*Umgekehrt, ist $L$ eine Menge mit zwei Operationen $\vee, \wedge : L \times L \to L$ so dass die vorige Eigenschaften (a), (b), (c) gelten, so ist $L$ eine geordnete Menge bezüglich die Relation $x \leq y$ gdw $x \wedge y = x$; mehr ist $(L, \leq)$ sogar ein Verband, in dem* $\inf\{x, y\} = x \wedge y$ *und* $\sup\{x, y\} = x \vee y$, *für alle* $x, y \in L$.

*Beweis.* □

**Satz 1.4.32.** *Eine geordnete Menge $(L, \leq)$ genau dann ein vollständiger Verband ist wenn für jede Teilmenge $X \subseteq L$, das Infimum von $X$ existiert.*

*Beweis.* □

**Übungen zu Relationen.**

**Übung 1.4.33.** Seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen. Man zeige dass die Zusamengesetzte Abbildung $g \circ f$ ist dieselbe als die Zusammengesetzte Relation $g \circ f$.

**Übung 1.4.34.** Sei $r = (A, B, R)$ eine Relation, und bezeichne man $\delta_A$ und $\delta_B$ die Gleichkeitsrelationen auf $A$ bzw $B$.
(1) Man zeige, dass $r \circ \delta_A = r = \delta_B \circ r$, d.h. die Gleichkeitsrelation wirkt als neutrales Element für die Zusammengesetzung der Relationen.
(2) Man zeige, dass die Inverserelation $r^{-1} = (B, A, R^{-1})$ ist nicht notwendig die Inverse bezüglich der Zusammengesetzung der Relationen, d.h. finde ein Beispiel einer Relation $r$ so dass $r^{-1} \circ r \neq \delta_A$.

**Übung 1.4.35.** Seien $r = (A, B, R)$ und $s = (B, C, S)$ Relationen, wobei $A$, $B$ und $C$ endliche Mengen sind mit $|A| = m$, $|B| = n$ und $|C| = p$. Man ordne die Elemente von $A$, $B$ und $C$ und betrachte man die Matrizen $M(r) \in \mathbb{M}_{m\times n}(\{0, 1\})$ und $M(s) \in \mathbb{M}_{n\times p}(\{0, 1\})$. Man bestimme $M(r^{-1})$ und $M(s \circ r)$ abhängig von $M(r)$ und $M(s)$. Man scheibe ein Algorithmus, das $M(r)$ und $M(s)$ liesst, und $M(r^{-1})$, $M(s \circ r)$ berechnet.

**Übung 1.4.36.** Man zeige dass die Teilbarkeit auf $\mathbb{Z}$ eine Präordnung ist die nicht symmetrisch und auch nicht antisymetrisch ist.

**Übung 1.4.37.** Man bestimme alle Äquivalenzrelationen die auf der Menge $A = \{a, b, c\}$ definieren lassen.

**Übung 1.4.38.** Man zeige, dass die folgende Relationen sind Äquivalenzen und man bestimme die bezügliche Faktormengen:

(1) $(\mathbb{C}, \mathbb{C}, \equiv)$ gegeben durch $x \equiv y$ gdw $|x| = |y|$.
(2) $(\mathbb{C}^*, \mathbb{C}^*, \equiv)$ gegeben durch $x \equiv y$ gdw $\arg(x) = \arg(y)$.

**Übung 1.4.39.** Man zeige, dass die Relation gegeben durch

$$(a, b) \sim (c, d) \text{ gdw } ad = cb$$

eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z}^*$ ist, und man bestimme die Faktormenge

$$(\mathbb{Z} \times \mathbb{Z}^*)/_\sim.$$

**Übung 1.4.40.** Sind die folgende Abbildungen

$$f : \mathbb{Q} \to \mathbb{Q},\ f\left(\frac{a}{b}\right) = \frac{a+1}{b^2} \text{ für alle } a, b \in \mathbb{Z}, b \neq 0,$$
$$g : \mathbb{Q} \to \mathbb{Q},\ g\left(\frac{a}{b}\right) = \frac{2a+3b}{b} \text{ für alle } a, b \in \mathbb{Z}, b \neq 0,$$
$$h : \mathbb{Z} \to \mathbb{Z},\ h(x) = \frac{x}{2} \text{ für alle } x \in \mathbb{Z},$$
$$k : \mathbb{Z} \to \mathbb{Q},\ k(x) = \frac{1}{x} \text{ für alle } x \in \mathbb{Z}$$

wohl defieniert?

**Übung 1.4.41.** Man betrachte die Menge $\mathbb{Q} = (\mathbb{Z}\times\mathbb{Z}^*)/_\sim$ wie in der Übung 1.4.39. Man zeige, dass die Operationen $+, \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ wohl definiert sind, wobei:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ und } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

für alle $a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0$.

**Übung 1.4.42.** Sei $n \in \mathbb{N}$, $n \geq 2$.

(1) Man zeige, dass die Kongruenz modulo $n$, nämlich $(\mathbb{Z}, \mathbb{Z}, \equiv_n)$ gegeben durch $x \equiv_n y$ (oder $x \equiv y(\mod n)$) gdw $n|(x - y)$ eine Äquivalenzrelation ist.
(2) Man zeige, dass die bezügliche Faktormenge ist

$$\mathbb{Z}_n = \mathbb{Z}/_{\equiv_n} = \{[0]_n, [1]_n, \ldots, [n-1]_n\} \text{ (die Menge aller Restklassen).}$$

(3) Man zeige, dass die Operationen

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ gegeben durch } [x]_n + [y]_n = [x + y]_n \text{ für alle } x, y \in \mathbb{Z} \text{ und}$$
$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ gegeben durch } [x]_n[y]_n = [xy]_n \text{ für alle } x, y \in \mathbb{Z}$$

wohl definirt sind.

**Übung 1.4.43.** Sei $A$ eine Menge und $r = (A, A, R)$ eine Präordnung auf $A$. Man zeige, dass $r \cap r^{-1}$ gegeben durch $x(r \cap r^{-1})y$ gdw $xry$ und $yrx$ eine Äquivalenzrelation auf $A$ ist, und auf der Faktormenge $A/_{(r\cap r^{-1})}$ die Relation $r$ eine Ordnung indiziert: $[x] \leq_r [y]$ gdw $xry$. Man untersuche den Partikularfall wenn $A = \mathbb{Z}$ und die Präordnung die Teilbarkeit ist (man sieht Übung 1.4.36).

**Übung 1.4.44.** Sei $f : A \to B$ eine Abbildung. Der Kernel von $f$ ist eine homogene Relation auf $A$ die durch $a(\ker f)b$ gdw $f(a) = f(b)$ gegeben wird. Man zeige dass $\ker f$ eine Äquivalenzrelation ist. Umgekehrt, für jede Äquivalenzrelation $(A, A, \equiv)$ finde man eine Abbildung $f : A \to B$, so dass $\equiv$ der Kernel von $f$ ist.

**Übung 1.4.45.** Man finde die Anzahl aller Äquivalenzrelationen die auf einer Menge $A$ mit $n$ Elemente definieren lassen.

**Übung 1.4.46.** Man bestimme alle Ordnungsrelationen die auf der Menge $A = \{a, b, c, \}$ definieren lassen. Man identifieziere (in jedem Fall) die minimal/maximal Elemente oder das kleinste/größte Element.

**Übung 1.4.47.** Man finde eind Beispiel einer geordneten Menge mit einem einzigen minimalen Element, aber die nicht das kleinste Element besitzt.

**Übung 1.4.48.** Ist $(A, \leq)$ eine geordnete Menge, so ist $(A, \geq)$ auch, wobei $\geq = \leq^{-1}$.

**Übung 1.4.49.** Jeder endlichen Verband ist vollständig.

**Übung 1.4.50.** Man zeige, dass jede Kette ein Verband ist. Ist jede Kette ein vollständiger Verband?

**Übung 1.4.51.** Jeder volständigen Verband besitzt das kleinste und das größte Element.

**Übung 1.4.52.** $(\mathbb{N}, |)$ ein Verband ist (hier $|$ bezeichnet die Teilbarkeit). Ist $(\mathbb{N}, |)$ vollständig?

**Übung 1.4.53.** Man zeige, dass $(\mathbb{N}, \leq)$ ein Verband der nicht vollständig ist. Man erklärt warum dieses Beispiel den Satz 1.4.32 nicht widerspricht.

**Übung 1.4.54.** Ist $A$ eine Menge, so ist $(\mathcal{P}(A), \subseteq)$ ein vollständiger Verband.

**Übung 1.4.55.** Auf der Menge $\mathcal{L}$ die Menge aller logische Aussagen definiert man die Relation $p \preceq q$ gdw $p \to q$ eine Tautologie ist. Man zeige dass $\preceq$ eine Präordnung ist. Man bestimme die assozierte Aq̈uivalenzrelation $\equiv = (\preceq \cap \preceq^{-1})$ (sieh Übung 1.4.35) und die Faktormenge $\mathcal{L}/_{\equiv}$ (diese Menge wird die *Lindenbaum-Tarski Algebra* gennat). Man zeige, dass $\mathcal{L}/_{\equiv}$ ein vollständiger Verband ist.

## 2. Gruppen, Ringe, Körper

### 2.1. **Gruppen.**

**Definition 2.1.1.** Eine *Gruppe* ist ein Paar $(G, \cdot)$ das aus einer Menge $G$ zusammen mit einer Operation $\cdot : G \times G \to G$ besteht, so dass $\cdot$ assoziativ ist, ein neutrales Element besitzt, und jedes Element aus $G$ invertierbar bezüghlich $\cdot$ ist. Ist $\cdot$ auch kommutativ, so nennt man $G$ *abelsch* oder *kommutativ*.

**Beispiel 2.1.2.** Die folgende Paaren sind (abelsche) Gruppen:
(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.
(b) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$.
(c) $(\mathbb{M}_{m\times n}(\mathbb{Z}), +)$, $(\mathbb{M}_{m\times n}(\mathbb{Q}), +)$, $(\mathbb{M}_{m\times n}(\mathbb{R}), +)$, $(\mathbb{M}_{m\times n}(\mathbb{C}), +)$

**Beispiel 2.1.3.** Die folgende Paaren sind Monoide aber keine Gruppen:
(a) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$.
(b) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$.
(c) $(\mathbb{M}_{n\times n}(\mathbb{Z}), \cdot)$, $(\mathbb{M}_{n\times n}(\mathbb{Q}), \cdot)$, $(\mathbb{M}_{n\times n}(\mathbb{R}), \cdot)$, $(\mathbb{M}_{n\times n}(\mathbb{C}), \cdot)$

**Bemerkung 2.1.4.** Die Operation einer algemeinen Gruppe ist häufig multiplikativ benotet, d. h. $(G, \cdot)$. In diesem Fall ist das neutrales Element mit 1 bezeichnet, und für $x \in G$ ist $x^{-1}$ das Inverseslement. Für eine abelsche Gruppe wird häufig die Operation additiv bennotet, d. h. $(G, +)$. In diesem Fall ist das neutrales Element mit 0 bezeichnet, und für $x \in G$ ist $-x$ das Gegenseitigeselement.

**Satz 2.1.5.** *Sei $(M, \cdot)$ ein Monoid, und man betrachte*

$$\begin{aligned} M^\times &= \{x \in M \mid x \text{ ist invertiebar in } M\} \\ &= \{x \in M \mid \exists x^{-1} \in M \text{ so dass } xx^{-1} = 1 = x^{-1}x\}. \end{aligned}$$

*Man zeige, dass die Operation $\cdot$ eine wohl definierte Operation auf $M^\times$ induziert, und bezüglich die beschrenckte Operation $M^\times$ eine Gruppe bildet.*

*Beweis.* □

**Korollar 2.1.6.** *Die folgende Konstruktionen zu nicht abelsche Gruppen führen:*

*(1) Ist $A$ eine Menge, so ist $\mathrm{S}(A) = \{\sigma : A \to A \mid \sigma \text{ bijektiv ist}\}$ eine Gruppe bezüglich die Zusammengesetzung der Abbildungen, die nicht abelsch ist für $|A| \geq 3$. Die Gruppe $\mathrm{S}(A)$ wird* die symmetrische Gruppe der Menge $A$ *gennant.*

*(2) Ist $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ und $n \in \mathbb{N}^*$, so ist $\mathrm{G}\,L_n(K) = \{A \in \mathbb{M}_{n\times n}(K) \mid \det(A) \neq 0\}$ eine Gruppe die nicht abelsch ist für $n \geq 2$. Die Gruppe $\mathrm{G}\,L_n(K)$ wird* die algemeine lineare Gruppe mit dem Rank $n$ über $K$ *gennant.*

*Beweis.* □

**Untergruppen.**

**Definition 2.1.7.** Sei $(G, \cdot)$ eine Gruppe. Eine *Untergruppe* von $G$ ist eine Teilmenge $H \subseteq G$, so dass die Operation auf $G$ eine wohl definierte Operation auf $H$ induziert (d. h. $x, y \in H \Rightarrow xy \in H$; man sagt also dass $H$ ein *stabiler Teil* von $G$ ist), und $H$ mit der beschrenkten Oparation eine Gruppe bildet. Man schreibt $H \leq G$.

**Beispiel 2.1.8.** (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (mit der Addition).
(2) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$ (mit der Multiplikation).
(3) $\mathbb{R}^*_+ \leq \mathbb{R}^*$, wobei $\mathbb{R}^*_+ = (0, \infty)$.
(4) Jede Gruppe $G$ hat die so gennante triviale Untergrupen, d. h. $\{1\}$ und $G$.

**Satz 2.1.9** (Der Charakterisierungssatz von Untergruppen)**.** *Sei $(G, \cdot)$ eine Gruppe und sei $H \subseteq G$ eine Teilmenge. Die folgende Aussagen sind äquivalent:*

(i) $H \leq G$.
(ii) (a) $1 \in H$.
 (b) $x, y \in H \Rightarrow xy \in H$.
 (c) $x \in H \Rightarrow x^{-1} \in H$.
(iii) (a) $1 \in H$.
 (b) $x, y \in H \Rightarrow xy^{-1} \in H$.

*Beweis.* □

**Satz 2.1.10.** *Sei $(G, \cdot)$ eine Gruppe. Sind $H_i \leq G$, mit $i \in I$, so gilt $\bigcap_{i\in I} H_i \leq G$.*

*Beweis.* □

**Bemerkung 2.1.11.** Die Vereinigung zweier oder mehrerer Untergruppen ist nicht notwendig eine Untergruppe (Übung 2.1.58).

**Definition 2.1.12.** Seien $(G, \cdot)$ eine Gruppe und $X \subseteq G$ eine Teilmenge von $G$. Die *von $X$ erzeugte Untergruppe* wird durch

$$\langle X \rangle = \bigcap \{H \leq G \mid X \subseteq H\}$$

definiert. Ist $X = \{x_1, x_2, \ldots, x_n\}$ eine endliche Menge, so schreibt man $\langle x_1, x_2, \langle, x_n \rangle$ statt $\langle \{x_1, x_2, \langle, x_n\} \rangle$.

**Lemma 2.1.13.** *Seien $(G, \cdot)$ eine Gruppe und $X \subseteq G$ eine Teilmenge von $G$. Dann gelten:*

(a) $\langle X \rangle \leq G$.
(b) $X \subseteq \langle X \rangle$ *und* $X = \langle X \rangle$ *gdw* $X \leq G$.
(c) $\langle X \rangle$ *ist der kleinste Untergruppe von $G$ die $X$ enthält, d. h.*

$$H = \langle X \rangle \text{ gdw } \begin{cases} H \leq G \\ X \subseteq H \\ \text{falls } K \subseteq G \text{ so dass } X \subseteq K \text{ dann } H \leq K \end{cases}.$$

(d) *Gilt $X \subseteq Y \subseteq G$ so gilt auch $\langle X \rangle \leq \langle Y \rangle \leq G$.*

*Beweis.* □

**Satz 2.1.14.** *Seien $(G, \cdot)$ eine Gruppe und $X \subseteq G$ eine Teilmenge von $G$. Dann gilt:*

$$\langle X \rangle = \{x_1 x_2 \ldots x_n \mid n \in \mathbb{N}, x_1, x_2, \ldots, x_n \in X \cup X^{-1}\},$$

*wobei $X^{-1} = \{x^{-1} \mid x \in X\}$. D. h. die von $X$ erzeugte Untergruppe ehthält alle Elemente von $G$ die als einen endlichen Produkt von Elementen aus $X \cup X^{-1}$ geschrieben lassen.*

*Beweis.* □

**Bemerkung 2.1.15.** Sei $(G, \cdot)$ eine Gruppe, und $x \in G$. Für jede $n \in \mathbb{Z}$ defieniert man:

$$x^n = \begin{cases} xx\ldots x \ (n \text{ mal}) \text{ falls } n > 0 \\ 1 \text{ falls } n = 0 \\ x^{-1}x^{-1}\ldots x^{-1} \ (-n \text{ mal}) \text{ falls } n < 0 \end{cases}$$

Ist die Operation additiv geschrieben, d. h $(G, +)$ so schreiben wir

$$nx = \begin{cases} x + x + \ldots + x \ (n \text{ mal}) \text{ falls } n > 0 \\ 0 \text{ falls } n = 0 \\ (-x) + (-x) + \ldots + (-x) \ (-n \text{ mal}) \text{ falls } n < 0 \end{cases}$$

**Korollar 2.1.16.** *Sei $(G, \cdot)$ eine Gruppe.*

(a) *Für $x \in G$ gilt $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.*
(b) *Für $x, y \in G$ mit $xy = yx$ gilt $\langle x, y \rangle = \{x^n y^m \mid n, m \in \mathbb{Z}\}$.*

**Gruppenhomomorphismen.**

**Definition 2.1.17.** Seien $(G, \cdot)$ und $(H, \cdot)$ zwei Gruppen. Man nennt *Gruppenhomomorphismus* zwischen $G$ und $H$ eine Abbildung $f : G \to H$ mit der Eigenschaft $f(xy) = f(x)f(y)$ für alle $x, y \in G$. Man nennt *(Gruppen)isomorphismus* ein Gruppenhomomorphismus der auch bijektiv ist. In diesem Fall die Gruppen sind isomorph gennant, und schreiben wir $G \cong H$.

**Beispiel 2.1.18.** Für jede zwei Gruppen $G$ und $H$ sind die Abbildungen $1_G$ und $e : G \to H$, $e(x) = 1$ ein Isomorphismus bzw ein Homomorphismus. Gilt $G \leq H$ so ist die Inklusionsabbildung $i : G \to H$ ein Gruppenhomomorphismus.

**Lemma 2.1.19.** *Ist $f : G \to H$ ein Gruppenhomomorphismus, so gelten*
(a) $f(1) = 1$.
(b) $f(x^{-1}) = f(x)^{-1}$.

*Beweis.* □

**Lemma 2.1.20.** *Die Zusammengesetzung zweier Gruppenhomomorphismen ist ein Gruppenhomomorphismus auch. Die Inveseabbildung eines Gruppenisomorphismus, ist ein Isomorphismus auch.*

*Beweis.* □

**Definition 2.1.21.** Sei $f : G \to H$ ein Gruppenhomomorphismus. Man nennt den *Kernel* bzw das *Bild* von $f$ die Mengen

$$\mathrm{Ker} f = \{x \in G \mid f(x) = 1\} \text{ und } \mathrm{Im} f = \{f(x) \mid x \in G\}.$$

**Satz 2.1.22.** *Ist $f : G \to H$ ein Gruppenhomomorphismus, so gelten*
(a) $\mathrm{Ker} f \leq G$.
(b) $\mathrm{Im} f \leq H$.
(c) *$f$ ist genau dann injektiv wenn* $\mathrm{Ker} f = \{1\}$.
(d) *$f$ ist genau dann surjektiv wenn* $\mathrm{Im} f = H$.

*Beweis.* □

**Zyklische Gruppen und die Ordnung eines Elementes.**

**Definition 2.1.23.** Eine zyklische Gruppe ist eine Gruppe die von einem eizelnen Element erzeugt wird.

**Definition 2.1.24.** Sei $(G, \cdot)$ eine Gruppe, und $x \in G$. Man sagt, dass $x$ von endlicher Ordnung ist, falls $n \in \mathbb{N}^*$ existiert, so dass $x^n = 1$. In diesem Fall nennt man die (Element)ordnung von $x$ die kleinste $n \in \mathbb{N}^*$ mit dieser Eigenschaft, und schriebt man $n = \mathrm{ord}(x)$. Das Element $x$ ist von unendlicher Ordnung, falls es nicht von endlicher Ordung ist, und dann schreibt man $\mathrm{ord}(x) = \infty$.

**Beispiel 2.1.25.** (1) In jede Gruppe $(G, \cdot)$ existiert ein einziges Element von Ordnung 1, nämlich das neutrales Element, $\mathrm{ord}(1) = 1$.
(2) In $(\mathbb{Z}, +)$ haben wir $\mathrm{ord}(2) = \mathrm{ord}(3) = \infty$ und $\mathrm{ord}(x) = \infty$ für jedes $x \neq 0$.
(3) In $(\mathbb{R}^*, \cdot)$ haben wir $\mathrm{ord}(-1) = 2$ und $\mathrm{ord}(2) = \mathrm{ord}(-2) = \mathrm{ord}(3) = \infty$; mehr, $\mathrm{ord}(x) = \infty$ für jedes $x \in \mathbb{R} \setminus \{1, -1\}$.
(4) In $(\mathbb{C}^*, \cdot)$ haben wir $\mathrm{ord}(i) = \mathrm{ord}(-i) = 4$, $\mathrm{ord}\left(\cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}\right) = 3$, $\mathrm{ord}(2) = \mathrm{ord}(-2) = \infty$; mehr $\mathrm{ord}(x) = \infty$ für alle $x \in \mathbb{C}^*$ mit $|x| \neq 1$.

**Satz 2.1.26.** *Sei $(G, \cdot)$ eine Gruppe, $x \in G$ und $n \in \mathbb{N}^*$. Dann gilt:*

$$\mathrm{ord}(x) = n \text{ gdw } \begin{cases} x^n = 1 \\ \text{falls } m \in \mathbb{Z} \text{ hat die Eigenschaft } x^m = 1 \text{ dann } n | m \end{cases}.$$

*Beweis.* □

**Satz 2.1.27.** *Sei $(G, \cdot)$ eine Gruppe. Für jedes $x \in G$ gilt es* $\mathrm{ord}(x) = |\langle x \rangle|$.

*Beweis.* □

**Wirkungen der Gruppen auf Mengen.**

**Definition 2.1.28.** Seien $A$ eine Menge und $(G,\cdot)$ eine Gruppe. Man nennt *(linke) Wirkung* von $G$ auf $A$ eine Abbildung $\alpha : G \times A \to A$ mit der Eigenschaften:

(1) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ für alle $g, h \in G$ und alle $x \in A$.
(2) $\alpha(1, x) = x$ für alle $x \in A$.

**Bemerkung 2.1.29.** Häufig ist eine Wirkung $\alpha : G \times A \to A$ als eine äußere Operation (Multiplikation) gesehen, und wird durch $gx = \alpha(g, x)$ benotet. In diesem Fall werden die Gleichungen (1) und (2) aus der Definition 2.1.28:

$$g(hx) = (gh)x \text{ bzw } 1x = x, \text{ für alle } g, h \in G \text{ und alle } x \in A.$$

**Theorem 2.1.30.** *Seien $A$ eine Menge und $(G,\cdot)$ eine Gruppe.*

(a) *Ist $G \times A \to A$, $(g, x) \mapsto gx$ eine Wirkung von $G$ auf $A$, so ist $\phi : G \to \mathrm{S}(A)$, $\phi(g) : A \to A$, $\phi(g) : x \mapsto gx$ ein Gruppenhomomorphismus.*
(b) *Ist $\phi : G \to \mathrm{S}(A)$ ein Gruppenhomomorphismus, so ist $G \times A \to A$, $(g, x) \mapsto \phi(g)(x)$ eine Wirkung von $G$ auf $A$.*
(c) *Die Verfahren von (a) und (b) beschreiben gegenseitige Inverseabbildungen zwischen die Menge aller Wirkungen von $G$ auf $A$ und die Menge aller Gruppenhomomorphismen $G \to \mathrm{S}(A)$.*

*Beweis.* □

**Definition 2.1.31.** Sei $G \times A \to A$, $(g, x) \mapsto gx$ eine Wirkung der Gruppe $(G,\cdot)$ auf der Menge $A$. Man nennt die *Permutationsdarstellung* dieser Wirkgung den Gruppenhomomorphism $\phi : G \to \mathrm{S}(A)$ der im Theorem 2.1.30 gebildet wird. Die Wirkung wird *treu* gennant, falls ihre Permutationsdarstellung injektiv ist.

**Satz 2.1.32.** *Sei $G \times A \to A$, $(g, x) \mapsto gx$ eine Wirkung der Gruppe $(G,\cdot)$ auf der Menge $A$. Die Relation $(A, A, \equiv)$ gegeben durch $x \equiv y$ gdw existiert $g \in G$ so dass $gx = y$, für alle $x, y \in A$ ist eine Äquivalenzrelation, derer Äquivalenzklassen (die* Orbits *gennant werden) sind $Gx = \{gx \mid g \in G\}$, mit $x \in A$.*

*Beweis.* □

**Korollar 2.1.33.** *Wenn wir bezeichen mit $[A/_{\equiv}]$ ein Representatensystem für die Menge aller Orbits einer Wirkung $G \times A \to A$ der Gruppe $(G,\cdot)$ auf der Menge $A$, denn gilt es:*

$$|A| = \sum_{Gx \in [A/_{\equiv}]} |Gx|.$$

*Beweis.* □

**Korollar 2.1.34.** *(Der Satz von Lagrange) Sei $G$ eine endliche Gruppe.*

(a) *Falls $H$ eine Untergruppe von $G$ ist, dann ist $|H|$ ein Teiler von $|G|$.*
(b) *Falls $x \in G$ dann ist $\mathrm{ord}(x)$ ein Teiler von $|G|$.*

*Beweis.* □

**Definition 2.1.35.** Die Ordnung einer Gruppe $(G,\cdot)$ ist die Kardinalanzahl $|G|$.

**Die Symmetrischegruppe.**

**Definition 2.1.36.** Seien $n$ eine naturliche Zahl und $G$ eine Untergruppe der symmetrischen Gruppe $\mathrm{S}_n = \mathrm{S}(\{1, 2, \ldots, n\})$. Die Wirkung von $G$ auf $\{1, 2, \ldots, n\}$ derer Permutationsdarstellung ist die Inklusionsabbildung $i : G \to \mathrm{S}_n$ wird *kanonisch* gennat. Für $\sigma \in \mathrm{S}_n$ heißen *$\sigma$-Orbits* die Orbits der kanonischen Wirkung der Gruppe $G = \langle\sigma\rangle$. Man nennt *trivial* ein $\sigma$-Orbit das ein einziges Element enthält. Ein *Zyklus* ist eine Permutation die ein einziges nicht triviales Orbit besitzt; in diesem Fall die Kardinalanzahl dieser nicht triviales Orbit wird die *Länge* des Zyklus gennant. Zwei Zyklen heißen *disjunkt* falls ihre nicht triviale Orbits disjunkte Mengen sind.

**Bemerkung 2.1.37.** Sei $\sigma \in \mathrm{S}_n$.

(1) $\sigma = e$ ($e$ ist die identische Permutation) gdw alle $\sigma$-Orbits trivial sind. D. h. $e$ ist ein Zyklus von Länge 1.
(2) $\sigma$ ist ein Zyklus von Länge $1 < k \leq n$ gdw eine Teilmenge $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ existiert, so dass $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots, \sigma(i_n) = i_1$ und $\sigma(i) = i$ für $i \notin \{i_1, i_2, \ldots, i_k\}$. In diesem Fall ist $\{i_1, i_2, \ldots, i_k\}$ das einzige nicht triviale Orbit von $\sigma$ und notiert man $\sigma = (i_1 i_2, \ldots, i_k)$.

**Lemma 2.1.38.** *Für $\sigma \in \mathrm{S}_n$ und $i \in \{1, 2, \ldots, n\}$ exsitiert die kleinste naturliche Zahl $k \leq 1$, so dass $\sigma^k(i) = i$. Diese Zahl $k$ ist die Länge des Orbites $\langle\sigma\rangle i$ und gilt es:*

$$\langle\sigma\rangle i = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}.$$

*Beweis.* □

**Lemma 2.1.39.** *Sind $\sigma_1$ und $\sigma_2$ disjunkte Zyklen, so gilt $\sigma_1\sigma_2 = \sigma_2\sigma_1$.*

*Beweis.* □

**Theorem 2.1.40.** *Jede Permutation $e \neq \sigma \in \mathrm{S}_n$ lässt sich als ein Produkt $\sigma = \sigma_1\sigma_1 \ldots \sigma_m$ geschrieben werden, wobei $\sigma_1, \sigma_2, \ldots, \sigma_m$ nicht triaviale je zwei disjunkte Zyklen sind. Mehr ist diese Darstellung eindeutig (bis auf die Reihenfolge der Faktoren).*

*Beweis.* □

**Bemerkung 2.1.41.** Man nennt die Zerlegung von $\sigma$ als Produkt von je zwei disjunkte Zyklen die Darstellung gegeben in Theorem 2.1.40. Manchmal diese Zerlegung enthält auch die (triviale) Zykeln $(i) = e$, wobei $i \in \{1, 2, \ldots, n\}$ mit $\sigma(i) = i$, einschließend dem Fall $\sigma = e$ im vorigen Theorem.

**Definition 2.1.42.** Eine *Inversion* für $\sigma \in \mathrm{S}_n$ ist ein Paar $(i, j) \in \{1, 2, \ldots, n\}^2$, so dass $i < j$ und $\sigma(i) > \sigma(j)$. Man bezeichent mit $m(\sigma)$ die Anzahl aller Inversionen, und man definiert das *Zeichen* von $\sigma$ durch $\epsilon(\sigma) = (-1)^{m(\sigma)}$. Die Permutation $\sigma$ heißt *(un)gerade* falls $m(\sigma)$ (un)gerade ist.

**Theorem 2.1.43.** *(Cayley) Jede Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe.*

*Beweis.* □

**Übungen zu Gruppen.**

**Übung 2.1.44.** Man betrachte die Menge

$$\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C} \text{ (here } i^2 = -1).$$

Man zeige, dass $\mathbb{Z} + i\mathbb{Z}$ ein Monoid ist bezüglich die Multiplikation der komplezen Zahlen. Man bestimme $(\mathbb{Z} + i\mathbb{Z})^\times$.

**Übung 2.1.45.** Man betrachte die Operation $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ gegeben durch $x * y = xy - 5x - 5y + 30$. Ist $(\mathbb{R}, *)$ eine Gruppe? Aber $(\mathbb{R} \setminus \{5\}, *)$, $((5, \infty), *)$ oder $((-\infty, 5), *)$?

**Übung 2.1.46.** Man ziege, dass $(\mathbb{Z}_n, +)$ ($n \in \mathbb{N}$, $n \geq 2$) eine abelsche Gruppe ist, und $p_n : \mathbb{Z} \to \mathbb{Z}_n$, $p_n(x) = [x]_n$ ein surjektiver Gruppenhomomorphismus ist (siehe also Übung 1.4.42).

**Übung 2.1.47.** Sei $(G_i, \cdot)$ eine Familie von Gruppen. Man zeige, dass $\left(\prod_{i\in I} G, \cdot\right)$ eine Gruppe ist, wobei

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i y_i)_{i\in I} \text{ für alle } (x_i)_{i\in I}, (y_i)_{i\in I} \in \prod_{i\in I} G_i.$$

Mehr zeige man, dass $p_j : \prod_{i\in I} \to G_j$, $p_j(x_i)_{i\in I} = x_j$ ein surjektiver Gruppenhomomrphismus ist, für jedes $j \in I$.

**Übung 2.1.48.** Sei $G$ eine Gruppe. Man zeige, dass wenn für jede zwei Elemente $x, y \in G$, $k \in \mathbb{Z}$ existiert so dass $(xy)^i = x^i y^i$ für $i = k - 1, k, k + 1$ dann $G$ abelsch ist.

**Übung 2.1.49.** Man zeige, dass ein endlicher stabilen Teil einer Gruppe eine Untergruppe bildet. Aber einer undendlichen stabilen Teil?

**Übung 2.1.50.** Man betrachte eine Gruppe $(G, \cdot)$, und man bezeichne $\text{Sub}(G) = \{H \subseteq G \mid H \leq G\}$ die Menge aller Untergruppen von $G$. Man zeige, dass $(\text{Sub}(G), \leq)$ ein Verband ist.

**Übung 2.1.51.** Sei $A_1A_2 \dots A_n$ ein regelmäßiges Polygon (mit $n$ Ecken und $n$ Seiten) mit dem Zentrum $O$ in einer Ebene $\alpha$. Eine Kongruenzabbildung (oder Isometrie) ist eine Abbildung $f : \alpha \to \alpha$ mit der Eigenschaft $|f(X)f(Y)| = |XY|$ für alle $X, Y \in \alpha$, wobei $|XY|$ die Abstand (Distanz) zwishen $X$ und $Y$ bezeichnet. Man betrachte die Menge aller Kongruenzabbildungen die das Polygon $A_1A_2 \dots A_n$ bewahren d. h.

$$D_n = \{f : \alpha \to \alpha \mid f \text{ ist eine Kongruenzabbildung und } \\ f(A_1A_2 \dots A_n) = A_1A_2 \dots A_n\}.$$

Man bezeichne mit $s$ die Drehung um $O$ mit $\frac{2\pi}{n}$ radian (from $A_1$ nach $A_2$) und mit $t$ die Achsenspiegelung mit der Achse $A_1O$. Man notiere dass $s, t : \alpha \to \alpha$ Kongruenzabbildungen sind. Man zeige, dass

(1) $s^n = 1 = t^2$ (here $1 = 1_\alpha$ ist die Identitätsabbildung).
(2) $ts = s^{n-1}t$.
(3) $D_n = \{1, s, \dots, s^{n-1}, t, st, \dots, s^{n-1}t\}$
(4) $D_n$ ist eine Gruppe bezuglich die Zusammengesetzung der Abbildungen (die *Diedergruppe*)
(5) Man bestimme $\langle s\rangle$, $\langle t\rangle$, $\langle s, t\rangle$

Man bilde die Operationstafeln für die Gruppen $D_3$ und $D_4$.

**Übung 2.1.52.** Auf der Menge $H = \{1, -1, i, -i, j, -j, k, -k\}$ definiert man eine Multiplikation die als folglich gebildet wird:

- 1 ist das neutral Element.
- Die Multiplikation bewährt die Zeichenregel: $(-x)y = x(-y) = -xy$ (umsonst habe die Zeichen $+$ und $-$ noch kein Sinn).
- $i^2 = j^2 = k^2 = -1$.
- $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$.

MAn zeige, dass $(H, \cdot)$ eine Gruppe ist (die *Quaterniongruppe* gennat wird).

**Übung 2.1.53.** Man zeige dass die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_+^*, \cdot)$ isomorph sind.

**Übung 2.1.54.** Man zeige, dass $f : \mathbb{C}^* \to \mathbb{R}$, $f(x) = \arg x$ ein Gruppenhomomorphismus zwischen $(C^*, \cdot)$ und $(\mathbb{R}, +)$ ist, und man bestimme $\mathrm{Ker} f$ und $\mathrm{Im} f$.

**Übung 2.1.55.** Man zeige, dass die Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +)$ ($n \in \mathbb{N}$, $n \geq 2$) zyklisch sind.

**Übung 2.1.56.** Sei $n \in \mathbb{N}$, $n \geq 2$. Man zeige, dass

$$U_n = \{x \in \mathbb{C}^* \mid \text{ existiert } n \in \mathbb{N} \text{ so dass } x^n = 1\}$$

eine Untergruppe von $(\mathbb{C}^*, \cdot)$ ist und $U_n$ ist zyklisch. Man finde ein Isomorphismus zwischen $(\mathbb{Z}_n, +)$ und $(U_n, \cdot)$.

**Übung 2.1.57.** Man finde alle Untergruppen von $(\mathbb{Z}, +)$. Hinweis: Man zeige, dass

$$\mathrm{Sub}(\mathbb{Z}, +) = \{nZ \mid n \in \mathbb{N}\}, \text{ wobei } n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}.$$

**Übung 2.1.58.** Man finde ein Beispiel das aus zwei Untergruppen einer Gruppe bestehet derer Vereinigung keine Unterguppe ist.

**Übung 2.1.59.** Sei $(G, +)$ eine abelsche Gruppe, und $H, K \leq G$ zwei Untergruppen. Man zeige, dass $\langle H \cup K \rangle = H + K$, wobei $H + K = \{x + y \mid x \in H, y \in K\}$.

**Übung 2.1.60.** Sei $(G, \cdot)$ eine Gruppe und $H, K \leq G$. Man zeige, dass $H \cup K \leq G$ gdw $H \subseteq K$ oder $K \subseteq H$.

**Übung 2.1.61.** Let $n, m \in \mathbb{Z}$. Man zeige, dass

(a) $n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m|n$.
(b) $n\mathbb{Z} \cap m\mathbb{Z} = k\mathbb{Z}$, wobei $k = \mathrm{kgV}(n, m)$.
(c) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, wobei $d = \mathrm{ggT}(n, m)$.

**Übung 2.1.62.** Man zeige, dass für $n, m \in \mathbb{N}$ mit $d = \mathrm{ggT}(n, m)$, zwei ganze Zahlen $s, t \in \mathbb{Z}$ existieren, so dass $d = sn + tm$. Man benutze es um zu zeigen, dass $1 = \mathrm{ggT}(n, m)$ gdw $s, t \in \mathbb{Z}$ existieren so dass $1 = sn + tm$.

**Übung 2.1.63.** Man benutze den Euklidschen Algorithmus um für $m, n \in N$ die ganze Zahlen $s, t$ mit der Eigenschaft $\mathrm{ggT}(n, m) = sn + tm$ zu bestimmen.

**Übung 2.1.64.** Man finde alle Gruppen (bis zu einem Isomorphismus) die aus einer Menge mit 4 Elementen definieren lassen.

**Übung 2.1.65.** Sei $(G, \cdot)$ eine Gruppe und $x, y \in G$ so dass $xy = yx$. Dann gelten:

(a) $\mathrm{ord}(x^{-1}) = \mathrm{ord}(x)$

(b) $\operatorname{ord}(xy) = \operatorname{ord}(yx)$.

**Übung 2.1.66.** Sei $f : G \to H$ ein Gruppehomomorphismus. Ist $x \in G$ von endlicher Ordnung, so ist $f(x)$ auch, und gilt es $\operatorname{ord}(f(x))|\operatorname{ord}(x)$.

**Übung 2.1.67.** Zwei unendliche zyklische Gruppen sind isomorph. Zwei endliche zyklische Gruppen sind genau dann isomorph wenn sie dieselbe Kardinalanzahl haben.

**Übung 2.1.68.** Ist $G$ eine zyklische Gruppe, so existiert ein surjektiver Gruppenhomomorphismus $\mathbb{Z} \to G$.

**Übung 2.1.69.** Man zeige dass die folgende Paaren von Gruppen nicht isomorph sind: $(\mathbb{Z}_n, +)$ und $(\mathbb{Z}_m, +)$ mit $n \neq m$; $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$; $(\mathbb{Z}_8, +)$ und $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ (für die Produktgruppe siehe Übung 2.1.47).

**Übung 2.1.70.** Sei $G \times A \to A$, $(g, x) \mapsto gx$ eine Wirkung der Gruppe $(G, \cdot)$ auf der Menge $A$.

(a) Für jedes $x \in A$ ist $\operatorname{Stab}_G(x) = \{g \in G \mid gx = x\}$ eine Untergruppe von $G$.
(b) Die Menge $K = \{g \in G \mid gx = x \text{ für alle } x \in A\}$ ist eine Untergruppe von $G$ (diese Untergruppe wird den *Kern* der Wirkung gennant). Mehr gilt es: $K = \bigcap_{x \in A} \operatorname{Stab}_G(x)$.
(c) Die Wirkung ist genau dann treu wenn sie ein trivialer Kern hat, d. h. $K = \{1\}$.

**Übung 2.1.71.** Seien $N = \{1, x, x^2\}$ und $H = \{1, y, y^2, y^3\}$ zwei zyklische Gruppen die von den Elementen $x$ und $y$ mit $\operatorname{ord}(x) = 3$, $\operatorname{ord}(y) = 4$ erzeugt werden. Dann:

(a) Definiere eine nicht triviale Wirkung von $H$ auf $N$, (d. h. $\cdot : H \times N \to N$) so dass, $h \cdot 1 = h$ für alle $h \in H$.
(b) Was ist der Kernel dieser Wirkung?
(c) Für $h \in H$ betrachte man $\phi_h : N \to N$, $\phi_h(n) = h \cdot n$. Man zeige, dass $\phi_h$ ein Isomorphismus ist.
(d) Man betrachte $G = N \times H$ als Mengen. Defieniere eine Operation auf $G$ durch
$$(n_1, h_1)(n_2, h_2) = (n_1(h_1 \cdot n_2), h_1 h_2).$$
Man zeige, dass $G$ mit dieser Operation eine nicht abelche Gruppe mit 12 Elemente ist.

**Übung 2.1.72.** Eine Gruppe, derer Ordnung eine Primzahl ist, ist zyklisch. Hinweis: Man zeige, dass eine Gruppe, derer Ordnung eine Primzahl ist, keine nicht triviale Untergruppen hat (so eine Gruppe heißt *einfach*).

**Übung 2.1.73.** Haben die Mengen $A$ und $B$ dieselbe Kardinalanzahl, so sind die Gruppen $\mathrm{S}(A)$ und $\mathrm{S}(B)$ isomorph.

**Übung 2.1.74.** Man zerlege $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix} \in \mathrm{S}_8$ als Produkt of je zwei disjunkte Zyklen.

**Übung 2.1.75.** Seien $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \tau == \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in \mathrm{S}_5$.

(a) Man zerlege $\sigma$ und $\tau$ als Produkt of je zwei disjunkte Zyklen.
(b) Man berechne $\sigma\tau$, $\tau\sigma$, $\sigma^{-1}$, $\tau^2$.
(c) Man berechne $\operatorname{ord}(\sigma)$ und $\langle\sigma\rangle$.

(d) Man berechne $\epsilon(\sigma)$ und $\epsilon(\tau)$.

**Übung 2.1.76.** Man zeige, dass
(a) $\epsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$ für alle $\sigma \in \mathrm{S}_n$.
(b) $\epsilon : \mathrm{S}_n \to \{1, -1\} = U_2$ (siehe Übung 2.1.56) ist eine Gruppenhomomorphismus.
(c) $\mathrm{Ker}\epsilon = \mathrm{A}_n$, wobei $\mathrm{A}_n = \{\sigma \in \mathrm{S}_n \mid \sigma \text{ ist gerade}\}$.

**Übung 2.1.77.** Ein Zyklus von der Länge $k$ ist genau dann gerade wenn $k > 1$ eine ungerade ganze Zahl ist. Jede (un)gerade Permutation lässt als ein Produkt von (un)gerade viele Transpositionen geschrieben werden, aber diese Darstellung ist nicht eizig. Man erinnert, dass eine *Transposition* ein Zyklus von der Länge 2 ist.

**Übung 2.1.78.** Sei $\sigma \in \mathrm{S}_n$ ein Zyklus mit der Länge $l$. Man zeige:
(a) Ist $l = 2k + 1$ ungerade, so ist $\sigma^2$ ein Zyklus von der Länge $l$.
(b) Ist $l = 2k$ gerade, so ist $\sigma^2$ ein Produkt von zwei Zyklen beide von der Länge $k$.
(c) $\mathrm{ord}(\sigma) = l$.

**Übung 2.1.79.** Man zeige, dass $(12)(3456) \in \mathrm{S}_6$ ist eine gerade Permutation die ist nicht aus der Form $\sigma^2$ für irdendeine $\sigma \in \mathrm{S}_6$.

## 2.2. **Ringe und Körper.**

**Definition 2.2.1.** Ein *Ring* ist ein Tripel $(R, +, \cdot)$, das aus einer Menge $R$ zusamamen mit zwei Operationen $+, \cdot : R \times R \to R$ besteht, so dass
(a) $(R, +)$ ist eine abelsche Gruppe.
(b) $\cdot$ ist associativ.
(c) $\cdot$ ist zweiseitig distributiv bezüglich $+$, d. h. für alle $x, y, x \in R$ gelten:

$$x(y + z) = xy + xz \text{ und } (y + z)x = yx + zx.$$

Ist $\cdot$ auch kommutativ, so nennt man $R$ *kommutativ*. Hat $\cdot$ ein neutrales Element, so nennt man $R$ *unitär*.

**Bemerkung 2.2.2.** In einem Ring $R$ bezeichnet man mit 0 das neutrale Element für $+$ und mit 1 das neutrales Element für $\cdot$ (falls existiert). Als üblich in einem Ring wirkt erst die Multiplikation und dann die Addition.

**Beispiel 2.2.3.** (a) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind kommutative, unitäre Ringe.
(b) Ist $R$ ein kommutativer Ring, so ist $(\mathbb{M}_{n\times n}(R), +, \cdot)$ ein Ring auch; mehr $(\mathbb{M}_{n\times n}(R), +, \cdot)$ ist nicht notwendig kommutativ. Ist $R$ unitär so ist $(\mathbb{M}_{n\times n}(R), +, \cdot)$ auch, und das netrales Element für die Multiplikation ist

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

(c) Ist $(R, +)$ eine abelsche Gruppe, so ist $(R, +, \cdot)$ ein Ring, wobei $xy = 0$ für alle $x, y \in R$ (so einer Ring wird *Nullquadratring* gennat. Insbesondere ist $R = \{0\}$ ein (unitärer!) Ring, wobei $0 + 0 = 0 \cdot 0 = 0$ (dieser Ring heißt *Nullring* und wird durch $R = 0$ bezeichnet).

(d) Ist $(R,+,\cdot)$ ein Ring, so ist $R^o,+.*$ auch, wobei $R^o = R$ und $x*y = yx$ für alle $x,y \in R$; man nennt $R^0$ den von $R$ gegenseitigen Ring.

**Satz 2.2.4.** *(Rechnenregeln in Ringe) Ist $R$ ein Ring und $x,y,x \in R$, so gelten:*
(a) $x0 = 0x = 0$.
(b) $x(-y) = (-x)y = -xy$.
(c) $x(y-z) = xy - xz$ *und* $(y-z)x = yx - zx$.
(d) *Ist $R \neq 0$ ein unitärer Ring so gilt $1 \neq 0$.*

*Beweis.* □

**Definition 2.2.5.** Ein *Körper* ist ein kommutativer, unitärer ring $(K,+,\cdot)$ mit der Eigenschaft, dass jedes $x \in K^*$ (hier $K^* = K \setminus \{0\}$) invertierbar (bezüglich $\cdot$) ist.

**Bemerkung 2.2.6.** Nach dem Satz 2.1.5, ein unitärer Ring $K$ ist genau dann ein Körper wenn $(K^*,\cdot)$ eine abelsche Gruppe ist.

**Beispiel 2.2.7.** (a) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sind Körper.
(b) $(\mathbb{Z},+,\cdot)$ ist kein Körper.

**Untergrringe und Unterkörper.**

**Definition 2.2.8.** Sei $(R,+,\cdot)$ ein Ring. Ein *Unterring* von $R$ ist eine Teilmenge $S \subseteq R$, so dass die Operationen $+$ und $\cdot$ auf $R$ wohl definierte Operationen auf $S$ induzieren (d. h. $x,y \in S \Rightarrow x+y, xy \in S$; man sagt also dass $S$ ein *stabiler Teil* bezüglich $+$ und $\cdot$ ist), und $S$ mit den beschrenkten Oparationen ein Ring bildet. Man schreibt $S \leq R$. Ist $1 \in R$ so nennt man *unitär* ein Unterring $S \leq R$ mit der Eigenschaft $1 \in S$.

**Beispiel 2.2.9.** (1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
(2) $2\mathbb{Z} \leq \mathbb{Z}$ aber $1 \notin 2\mathbb{Z}$.
(3) Jeder Ring $R$ hat die so gennante triviale Unterringen, d. h. $\{0\}$ und $R$.

**Satz 2.2.10** (Der Charakterisierungssatz von Unterringen)**.** *Sei $(R,+,\cdot)$ ein Ring und sei $S \subseteq R$ eine Teilmenge. Die folgende Aussagen sind äquivalent:*
(i) $S \leq R$.
(ii) (a) $0 \in S$.
  (b) $x,y \in S \Rightarrow x+y \in S$.
  (c) $x \in S \Rightarrow -x \in S$.
  (d) $x,y \in S \Rightarrow xy \in S$.
(iii) (a) $0 \in S$.
  (b) $x,y \in H \Rightarrow x-y \in H$.
  (c) $x,y \in S \Rightarrow xy \in S$.

*Beweis.* □

**Satz 2.2.11.** *Sei $(R,+,\cdot)$ ein Ring. Sind $S_i \leq R$, mit $i \in I$, so gilt $\bigcap_{i\in I} S_i \leq R$.*

**Bemerkung 2.2.12.** Die Vereinigung zweier oder mehrerer Unterringe ist nicht notwendig ein Unterring (siehe also Bemerkung 2.1.11).

**Definition 2.2.13.** Sei $(K,+,\cdot)$ ein Körper. Ein *Unterkörper* von $K$ ist eine Teilmenge $L \subseteq K$, so dass die Operationen $+$ und $\cdot$ auf $K$ definierte Operationen auf $L$ induzieren und $L$ mit den beschrenkten Oparationen ein Körper bildet. Man schreibt $L \leq K$.

**Bemerkung 2.2.14.** Ein Unterkörper ein unitärer Unterring ist.

**Satz 2.2.15** (Der Charakterisierungssatz von Unterkörper)**.** *Sei* $(K, +, \cdot)$ *ein Körper und sei* $L \subseteq K$ *eine Teilmenge. Die folgende Aussagen sind äquivalent:*

(i) $L \leq K$.
(ii) (a) $0, 1 \in L$.
  (b) $x, y \in L \Rightarrow x + y \in L$.
  (c) $x \in L \Rightarrow -x \in L$.
  (d) $x, y \in L \Rightarrow xy \in L$.
  (e) $x \in L^* \Rightarrow x^{-1} \in L$
(iii) (a) $0, 1 \in L$.
  (b) $x, y \in L \Rightarrow x - y \in L$.
  (c) $x, y \in L^* \Rightarrow xy^{-1} \in S$.

*Beweis.* □

**Bemerkung 2.2.16.** Wie im Fall der Gruppen, wir können der von einer Teilmenge erzeugten Unterring oder Unterkörper definieren.

**Homomorphismen.**

**Definition 2.2.17.** Ein *Homomorphismus* von Ringen (bzw Körper) ist eine Abbildung $f : R \to S$ ($f : K \to L$), wobei $R$ und $S$ ($K$ und $L$) zwei Ringe (Körper) sind so dass $f(x + y) = f(x) + f(y)$ und $f(xy) = f(x)f(y)$ für alle $x, y \in R$ ($x, y \in K$). Sind die Ringe $R$ und $S$ unitär, so nennt man der Ringhomomorphismus $f : R \to S$ unitär auch falls $f(1) = 1$. Ein Ringhomomorphismus (Körperhomomorphismus) heißt *Isomorphismus* falls es auch bijektiv ist; in diesem Fall schreibt man $R \cong S$ (oder $K \cong L$).

**Beispiel 2.2.18.** Für jede zwei Ringe (Körper) $R$ und $S$ sind die Abbildungen $1_R$ und $0 : G \to H$, $0(x) = 0$ ein Isomorphismus bzw ein Homomorphismus. Gilt $S \leq R$ so ist die Inklusionsabbildung $i : S \to R$ ein homomorphismus.

**Lemma 2.2.19.** *Ein Körperhomomorphismus ist entweder unitär oder null.*

*Beweis.* □

**Lemma 2.2.20.** *Die Zusammengesetzung zweier Ring- bzw. Körperhomomorphismen ist ein Ring- oder Körperhomomorphismus auch. Die Inveseabbildung eines Ring-Körperisomorphismus ist ein Isomorphismus auch.*

*Beweis.* □

## Spezielle Elemente in einem Ring

Wie im Fall der Monoide, für unitäre Ringe $R$ bezeichen wir

$$R^\times = \{x \in R \mid x \text{ ist invertierbar (bezüglich die Multiplikation)}\}.$$

**Definition 2.2.21.** Sei $R$ ein Ring. Ein Element $x \in R$ heißt:

(1) *Links- oder Rechtsnullteiler* falls $y \in R$, $y \neq 0$ existiert so dass $xy = 0$ bzw $yx = 0$. Ist $x$ auch Links und Rechtsnullteiler, so ist $x$ einfach Nullteiler gennant.
(2) *idempotent* falls $x^2 = x$ gilt.
(3) *nilpotent* falls $n \in \mathbb{N}$ existiert, so dass $x^n = 0$.

**Bemerkung 2.2.22.** Seien $R \neq 0$ ein Ring und $x \in R$.

(a) Offenbar ist 0 ein Nullteiler. Man sagt, dass 0 ist der triviale Nullteiler. Man sagt, $R$ ist *ohne Nullteiler*, falls in $R$ keine nicht triviale Nulteiler enthält.
(b) 0 und 1 (falls $1 \in R$ existiert, d. h. $R$ ist unitär) sind Idempotentelemente; sie werden triviale Idempotentelemente gennant.
(c) Ist $x$ idempotent, so $x^n = x$ gilt, für alle $n \in \mathbb{N}^*$.
(d) Ist $x$ nilpotent und $x^n = 0$ für eine $n \in \mathbb{N}$, so gilt $x^{n+k} = 0$ für alle $k \in \mathbb{N}$.

**Beispiel 2.2.23.** Man betrachte den Ring $(\mathbb{Z}_{12}, +, \cdot)$.

(1) $[3]_{12}$ ist ein Nulteiler, da $[3]_{12}[4]_{12} = [4]_{12}[3]_{12} = [0]_{12}$.
(2) $[4]_{12}$ ist idempotent, da $[4]_{12}^2 = [4]_{12}$.
(3) $[6]_{12}$ ist nilpotent, da $[6]_{12}^2 = [0]_{12}$.

**Satz 2.2.24.** *Sei $R$ ein unitärer Ring.*

*(1) Gilt $x \in R^\times$ so ist $x$ kein Nullteiler.*
*(2) $x \in R$ ist genau dann kein Links- oder Rechtsnulteiller wenn man mit $x$ links bzw rechts verkürzen kann.*
*(3) Ist $e \in R$ ein nicht triviales Idempotent, so ist $e$ ein Nullteiler.*
*(4) Ist $x \in R$ ein Nilpotentelement so ist $x$ ein Nulteiller.*

*Beweis.* □

**Definition 2.2.25.** Ein Integritätsbereich ist ein komutativer, unitärer Ring der auch ohne Nullteiler ist.

**Satz 2.2.26.** *Ist $R$ ein unitärer Unterring eines Körpers $K$ so ist $R$ ein Integritätsbereich.*

*Beweis.* □

**Korollar 2.2.27.** *Ein Körper ist ein Integritätsbereich.*

**Examples 2.2.28.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper, so sind sie Integritätsbereice auch. $\mathbb{Z}$ ist ein Integritätsbereich, der kein Körper ist.

**Satz 2.2.29.** *Ein endlicher Integritätsbereich ist ein Körper.*

*Beweis.* □

**Korollar 2.2.30.** *Ist $p$ eine Primzahl, so ist $(\mathbb{Z}_p, +, \cdot)$ ein Körper.*

**Übungen zu Ringe.**

**Übung 2.2.31.** Man überprüfe, dass $(\mathbb{Z}_n, +, \cdot)$ $(n \leq 2)$ ein kommutativer, unitärer Ring ist, wobei $+$ und $\cdot$ sind als in der Übung 1.4.42 definiert werden.

**Übung 2.2.32.** Für eine abelsche Gruppe $(G, +)$ betrachte man

$$\mathrm{End}(G) = \{f : G \to G \mid f \text{ ein Gruppenhomomorphismus ist}\}.$$

Man zeige, dass $(\mathrm{End}(g), +, \circ)$ ein unitärer Ring ist, wobei für $f, g \in \mathrm{End}(G)$ defieniert man die Addition durch:

$$f + g : G \to G, (f + g)(x) = f(x) + g(x), \text{ für alle } x \in G.$$

$(\mathrm{End}(g), +, \circ)$ wird der *Endomorphismring* von $G$ genannt.

**Übung 2.2.33.** Man betrachte eine beliebige Menge $A$ und ein Ring $R$. Auf der Menge $R^A = \{f : A \to R \mid f \text{ ist eine Abbildung}\}$ definiere man die Operationen $+, \cdot : R^A \times R^A \to R^A$ durch $f+g, fg : A \to R$, $(f+g)(x) = f(x)+g(x)$ und $(fg)(x) = f(x)g(x)$ für alle $f, g \in R^A$ und alle $x \in A$. Man zeige, dass $R^A$ ein Ring ist, der genau dann kommutativ oder unitär ist wenn $R$ dieselbe Eigenschaft hat.

**Übung 2.2.34.** Man überprüfe, dass $(\mathbb{Q}, +, \cdot)$ ein Körper ist, wobei $+$ und $\cdot$ sind als in der Übung 1.4.41 definiert werden.

**Übung 2.2.35.** Man betrachte die Quaterniongruppe $H = \{\}$ (siehe Übung 2.1.52). Man überprüfe dass,

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

ein Schiefkörper ist (das heißt $\mathbb{H}$ alle Axiome einer Körper erfullt mit der Ausnahme der Kommmutativität der Operation $\cdot$), wobei

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k$$

$$\begin{aligned}(a+bi+cj+dk)(a'+b'i+c'j+d'k) &= (aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i \\ &\quad + (ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k\end{aligned}$$

(d. h. die Multiplikation wird von der Multiplikation der Quaterniongruppe induziert).

**Übung 2.2.36.** Sei $R$ kommutativer, unitärer Ring. Man überprüfe, dass die Menge aller Polynome

$$R[X] = \{a_0 + a_1X + \ldots + a_nX^n \mid n \in \mathbb{N}, a_i \in R \text{ für alle } 1 \le i \le n\}.$$

ein kommutativer unitärer Ring bildet, bezüglich die übliche Addition und Multiplikation der Polynome. Man zeige auch, dass $R$ ein Unterring von $R[X]$ ist.

**Übung 2.2.37.** Man finde alle Unterringen von $(\mathbb{Z}, +, \cdot)$.

**Übung 2.2.38.** Sei $n \in \mathbb{N}$, $n \ge 2$. Man zeige, dass $\mathbb{Z}_n^\times = \{[k]_n \mid \mathrm{ggT}(n,k) = 1\}$. Man benutze es um zu beweisen, dass $\mathbb{Z}_n$ genau dann ein Körper ist wenn $n$ eine Primzahl ist.

**Übung 2.2.39.** Man löse die folgende Gleichungen in $\mathbb{Z}_6$: $[4]_6x + [5]_6 = [1]_6$ und $[5]_6x + [3]_6 = [1]_6$

**Übung 2.2.40.** Man zeige, dass $\mathbb{Z} + i\mathbb{Z} = \{a + ib \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$ ist. Man zeige, dass

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

ein Unterring von $(\mathbb{M}(\mathbb{Z}), +, \cdot)$ ist, und $R \cong \mathbb{Z} + i\mathbb{Z}$. Sind $\mathbb{Z} + i\mathbb{Z}$ und/oder $R$ Integritätsbereiche? Aber Körper?

**Übung 2.2.41.** Man bestimme $(\mathbb{Z} + i\mathbb{Z})^\times$.

**Übung 2.2.42.** Man zeige, dass $R[X]^\times = R^\times$, für jedewelchen kommutativen unitären Ring $R$.

**Übung 2.2.43.** Sei $R$ ein kommutativer, unitärer Ring. Man zeige, dass die Ringe $\mathbb{M}_{n\times n}(R)$ und $\mathbb{M}_{n\times n}(R)^o$ isomorph sind. Fölglich beweise man, dass für $A \in \mathbb{M}_{n\times n}(R)$ die folgende Aussagen äquivalent sind:

(i) $A$ ist links invertierbar.
(ii) $A$ ist rechts invertierbar.
(iii) $A$ ist invertierbar.

**Übung 2.2.44.** Man zeige dass die folgende Paare von Ringe nicht isomorph sind: $\mathbb{Z}$ und $\mathbb{Q}$; $\mathbb{Z}$ und $\mathbb{M}_{2\times 2}(\mathbb{Z})$.

**Übung 2.2.45.** Man zeige dass die Körper $\mathbb{R}$ und $\mathbb{C}$ nicht isomorph sind.

**Übung 2.2.46.** Man zeige, dass $\mathbb{Q}+i\mathbb{Q} = \{a+ib \mid a,b\in\mathbb{Q}\}$ ein Unterkörper von $\mathbb{C}$ ist.

**Übung 2.2.47.** Ist $R$ ein Integritätsbereich, so ist $R[X]$ auch.

**Übung 2.2.48.** Man bestimme alle Idempotentelemente aus dem Ring $\mathbb{Z}_n$, wobei $n\in\mathbb{N}$, $n\geq 2$.

**Übung 2.2.49.** Man bestimme alle Nilpotentelemente aus dem Ring $\mathbb{Z}_n$, wobei $n\in\mathbb{N}$, $n\geq 2$.

## 3. Lineare Algebra

In diesem Kapitel wir befasten ein Körper $(K,+,\cdot)$. Als Beispiele von Körper, wir haben insbesondere $K=\mathbb{R}$ oder $K=\mathbb{C}$ aber die Fälle $K=\mathbb{Q}$ oder $K=\mathbb{Z}_p$, wobei $p\in\mathbb{N}$ eine Primzahl ist, sind auch möglich.

### 3.1. **Vektorräume und lineare Abbildungen.**

**Definition 3.1.1.** Ein *Vektorraum über* $K$ oder kürzer $K$*-Vektorraum* bestehet aus einer abelsche Gruppe $(V,+)$ zusamamen mit einer äußeren Operation $\cdot : K\times V\to V$ die die folgende Axiome erfullen soll:
(VR1) $\alpha(x+y)=\alpha x+\alpha y$;
(VR2) $(\alpha+\beta)x=\alpha x+\beta x$;
(VR3) $\alpha(\beta x)=(\alpha\beta)x$;
(VR4) $1x=x$
für alle $x,y\in V$ und alle $\alpha,\beta\in K$. Man schreibt ${}_KV$. Die Elemente von $V$ und $K$ werden *Vektoren* bzw *Skalaren* genannt. Die Addition in $V$ und die äußere Operation werden die *Addition der Vektoren* bzw dei *Skalarmultiplikation* genannt. Vektorraume werden manchmal auch *lineare Raume* gennant.

**Beispiel 3.1.2.** (1) $V=\{0\}$ ist ein Vektorraum, wobei $0+0=0$ und $\alpha 0=0$ für alle $\alpha\in K$. Man bezeichnet diesen Vektorraum mit 0.
(2) $K^n$ ist ein $K$ Vektorraum bezüglich die Addition der Vektoren:
$$[x_1,x_2,\dots,x_n]+[y_1,y_2,\dots,y_n]=[x_1+y_1,x_2+y_2,\dots,x_n+y_n]$$
und die Skalarmultiplication:
$$\alpha[x_1,x_2,\dots,x_n]=[\alpha x_1,\alpha x_2,\dots,\alpha x_n].$$
(3) $\mathbb{M}_{m\times n}(K)$ ist ein $K$-Vektorraum mit der Addition der Matrizen und die Multiplikation einer matrix mit einem Skalar, d. h. für $A=[a_{i,j}]$ und $B=[b_{i,j}]$ und $\alpha\in K$, haben wir $A+B=[a_{i,j}+b_{i,j}]$ und $\alpha A=[\alpha a_{i,j}]$. Was erhalten wir falls wir stellen $m=1$? Aber für $n=1$?

(4) Ist $K$ ein Unterkörper von $L$, so ist $L$ ein $K$-Vektorraum, wobei die Addition der Vektoren ist die Addition in $L$ und die Skalarmultiplikation ist:

$$K \times L \to L, (\alpha, x) \mapsto \alpha x, \text{ für alle } x \in L, \alpha \in K.$$

(5) Die Menge aller Polynome

$$K[X] = \{a_0 + a_1 X + \ldots + a_n X^n \mid n \in \mathbb{N},\ a_0, a_1, \ldots, a_n \in K\}$$

ist ein $K$-Vektorrau bezüglich die Addition der Polynome (Vektoren) un die Multiplikation der Polynome mit Skalaren aus $K$.

(6) Die Menge aller freien Vektoren aus der Ebene (oder dem Raum) bezüglich die Addition der freien Vektoren und die übliche Skalarmultiplikation ist ein Vektorraum.

**Satz 3.1.3.** *(Rechnenregeln in Vektorräume) Seien $V$ ein $K$-Vektorraum, $x, y \in V$ und $\alpha, \beta \in K$. Dann gelten:*

(a) $\alpha 0 = 0 = 0x$.
(b) $\alpha(-x) = (-\alpha)x = -\alpha x$.
(c) $\alpha(x - y) = \alpha x - \alpha y$ *und* $(\alpha - \beta)x = \alpha x - \beta x$.
(d) $\alpha x = 0$ *gdw* $\alpha = 0$ *oder* $x = 0$.

*Beweis.* □

**Untervektorräume.**

**Definition 3.1.4.** Sei $V$ ein $K$-Vektorraum. Ein *Untervektorraum* oder kürzer *Unterräum* von $V$ ist eine Teilmenge $U \subseteq V$, so dass die Addition der Vektoren und die Skalarmultiplication wohl definierte Operationen auf $U$ induzieren (d. h. $x, y \in U, \alpha \in K \Rightarrow x + y, \alpha x \in U$), und $U$ mit den beschrenkten Operationen ein Vektorraum bildet. Man schreibt $U \leq_K V$, oder einfach $U \leq V$.

**Beispiel 3.1.5.** Jeder Vektorraum ${}_K V$ besitzt zwei so gennate *triviale* Untervektorraume, nämlich $0 \leq_K V$ und $V \leq_K V$.

**Satz 3.1.6** (Der Charakterisierungssatz von Unterräumen)**.** *Sei $V$ ein $K$-Vektorraum und sei $U \subseteq V$ eine Teilmenge. Die folgende Aussagen sind äquivalent:*

(i) $U \leq_K V$.
(ii) (a) $0 \in U$.
(b) $x, y \in U \Rightarrow x + y \in U$.
(c) $x \in U, \alpha \in K \Rightarrow \alpha x \in U$.
(iii) (a) $0 \in S$.
(b) $x, y \in U \Rightarrow \alpha x + \beta y \in U$.

*Beweis.* □

**Satz 3.1.7.** *Sei $V$ ein $K$-Vektorraum. Sind $U_i \leq_K V$ Unteräume, mit $i \in I$, so gilt $\bigcap_{i \in I} U_i \leq_K V$.*

*Beweis.* □

**Bemerkung 3.1.8.** Die Vereinigung zweier oder mehrerer Unterräume ist nicht notwendig ein Unterraum (siehe also Bemerkung 2.1.11).

**Definition 3.1.9.** Seien $V$ ein $K$-Vektorraum und $X \subseteq V$ eine Teilmenge von $V$. Die *von $X$ erzeugte* (oder *gespannte*) *Unterraum* wird durch

$$\langle X \rangle = \langle X \rangle_K = \bigcap_{X \subseteq U \leq_K V} U$$

definiert. Ist $X = \{x_1, x_2, \ldots, x_n\}$ eine endliche Menge, so schreibt man $\langle x_1, x_2, \ldots, x_n \rangle_K$ statt $\langle \{x_1, x_2, \ldots, x_n\} \rangle_K$.

**Lemma 3.1.10.** *Seien $V$ ein $K$-Vektorraum und $X \subseteq V$ eine Teilmenge von $V$. Dann gelten:*

(a) $\langle X \rangle_K \leq_K V$.
(b) $X \subseteq \langle X \rangle_K$ *und* $X = \langle X \rangle_K$ *gdw* $X \leq_K V$.
(c) $\langle X \rangle_K$ *ist der kleinste Unterraum von $V$ der $X$ enthält, d. h.*

$$U = \langle X \rangle_K \text{ gdw } \begin{cases} U \leq_K V \\ X \subseteq U \\ \text{falls } W \leq_K V \text{ so dass } X \subseteq W \text{ dann } U \leq_K W \end{cases}.$$

(d) *Gilt $X \subseteq Y \subseteq G$ so gilt auch $\langle X \rangle_K \leq \langle Y \rangle_K \leq V$.*

*Beweis.* □

**Satz 3.1.11.** *Seien $V$ ein $K$-Vektorraum und $X \subseteq V$ eine Teilmenge von $V$. Dann gilt:*

$$\langle X \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \mid n \in \mathbb{N}, x_1, x_2, \ldots, x_n \in X \text{ und } \alpha_1, \alpha_2, \ldots, \alpha_n \in K\}.$$

*Insbesondere, für $X = \{x_1, x_2, \ldots, x_n\}$ haben wir:*

$$\langle x_1, x_2, \ldots, x_n \rangle_K = \{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \mid \alpha_1, \alpha_2, \ldots, \alpha_n \in K\}.$$

*Beweis.* □

**Definition 3.1.12.** Seien $V$ ein $K$-Vektorraum und $X \subseteq V$. Man nennt *lineare Kombination* von Elementen von $X$ eine Ausdrück aus der Form $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ mit $n \in \mathbb{N}$, $x_1, x_2, \ldots, x_n \in X$ und $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Insbesondere, eine lineare Kombination von Vektoren $x_1.x_2, \ldots, x_n \in V$ ist eine Ausdrück aus der Form $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, und eine lineare Kombination von Vektoren $x, y \in V$ ist $\alpha x + \beta y$, mit $\alpha, \beta \in K$.

**Bemerkung 3.1.13.** Satz 3.1.11 sagt dass der von $X$ erzeugte Unterraum enthält alle Vektoren von $V$ die als eine lineare Kombination von Elementen aus $X$ geschrieben lassen.

**Korollar 3.1.14.** *Sei $V$ ein $K$-Vektorraum.*

(a) *Für $x \in V$ gilt $\langle x \rangle_K = \{\alpha x \mid \alpha \in K\}$.*
(b) *Für $x, y \in V$ gilt $\langle x, y \rangle_K = \{\alpha x + \beta y \mid \alpha, \beta \in K\}$.*

**Summe und direkte Summe der Unterraümen.**

**Definition 3.1.15.** Sei $V$ ein $K$-Vektorraum und seien $S, T \leq_K V$ zwei Unteräume. Die Summe dieser Unterräume ist definiert als $S + T = \{x + y \mid x \in S, y \in T\}$.

**Satz 3.1.16.** *Sei $V$ ein $K$-Vektorraum und seien $S, T \leq_K V$ zwei Unteräume. Dann gilt $\langle S \cup T \rangle_K = S + T$. Insbesondere ist die Summe ein Unterraum.*

*Beweis.* □

**Korollar 3.1.17.** *Für einen $K$-Vektorraum $V$, bezeichen man mit* $\mathrm{Sub}_K(V) = \{S \mid S \leq_K V\}$ *die Mange aller Unterräume. Dann ist* $(\mathrm{Sub}_K(V), \leq_K)$ *ein Verband, wobei* $\inf\{S,T\} = S \cap T$ *und* $\sup\{S,T\} = S + T$.

*Beweis.* □

Die Elemente der Summe $S+T$ zweier Unterräume $S, T \leq_K V$ sind die Vektoren die als eine Summe zwischen ain Vektor aus $S$ und ein Vektor aus $T$ geschrieben lassen. Wir sind also interesiert von dem Fall wenn diese Schreibung einzig ist.

**Satz 3.1.18.** *Sei $V$ ein $K$-Vektorraum und seien $S, T \leq_K V$ zwei Unteräume. Die folgende Aussagen sind äquivalent:*

(i) $S \cap T = 0$;
(ii) *Die Schreibung jedem Vektor aus $S + T$ als eine Summe zwischen ain Vektor aus $S$ und ein Vektor aus $T$ ist einzig, d. h. falls für $v \in S + T$ gilt $v = x + y = s + t$ mit $x, s \in S$ und $y, t \in T$ dann haben wir $x = s$ und $y = t$.*

*Beweis.* □

**Definition 3.1.19.** Man nennt *direkt* eine Summe $S + T$ zweier Unterraume $S$ und $T$ die die äquivalente Aussagen aus dem Satz 3.1.18 erfüllen. Man schreibt $S \oplus T = S + T$ in diesem Fall.

**Bemerkung 3.1.20.** Sei $V$ ein $K$-Vektorraum und seien $S, T \leq_K V$ zwei Unteräume. Dann gilt $V = S \oplus T$ gdw $S \cap T = 0$ und $S + T = V$.

**Lineare Abbildungen.**

**Definition 3.1.21.** Seien $V$ und $W$ zwei $K$-Vektorräume. Man nennt *lineare Abbildung* oder Homomorphismus von Vektoräume zwischen $V$ und $W$ eine Abbildung $f : V \to W$ mit den Eigenschaften $f(x + y) = f(x) + f(y)$ und $f(\alpha x) = \alpha f(x)$ für alle $x, y \in V$ und alle $\alpha \in K$. Man nennt *Isomorphismus* eine lineare Abbildung die auch bijektiv ist. In diesem Fall sind die Vektorräume $V$ und $W$ isomorph gennant, und schreiben wir $V \cong W$.

**Beispiel 3.1.22.** Für jede zwei $K$-Vektorräume $V$ und $W$ sind die Abbildungen $1_V$ und $0 : V \to W$, $0(x) = 0$ linear; mehr $1_V$ ist sogar ein Isomorphismus. Gilt $V \leq_K W$ so ist die Inklusionsabbildung $i : V \to W$ linear.

**Notation 3.1.23.** Seien $V$ und $W$ zwei $K$-Vektorräume. Man bezeichnet

$$\mathrm{Hom}_K(V, W) = \{f : V \to W \mid f \text{ ist linear}\} \text{ und } \mathrm{End}_K(V) = \mathrm{Hom}_K(V, V)$$

(eine lineare Abbildung $f : V \to V$ nennt man auch *Endomorphismus* von $V$).

**Bemerkung 3.1.24.** Jede lineare Abbildung $f : V \to W$ ist eine Gruppenhomomorphismus auch, folgilch gelten

(a) $f(0) = 0$.
(b) $f(-x) = -f(x)$.

**Satz 3.1.25.** *Seien $V$ und $W$ zwei $K$-Vektorräume. Eine Abbildung $f : V \to W$ ist genau dann linear wenn $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$, für alle $x, y \in V$ und alle $\alpha, \beta \in K$.*

*Beweis.* □

**Bemerkung 3.1.26.** Durch Induktion kann man sehen, dass eine lineare Abbildung die lineare Kombinationen bewahren, d. h. falls $f : V \to W$ ist linear, $\alpha_1, \ldots, \alpha_n \in K$ und $x_1, \ldots, x_n \in V$ dann gilt:

$$f(\alpha_1 x_1 + \ldots + \alpha_n x_n) = \alpha_1 f(x_1) + \ldots + \alpha_2 f(x_n).$$

**Lemma 3.1.27.** *Die Zusammengesetzung und die Addition zweier linearen Abbildungen, falls existieren, sind eine lineare Abbildungen auch. Die Multiplikation einer linearen Abbildung mit einer Skalar ist linear auch. Die Inveseabbildung eines Isomorphismus, ist ein Isomorphismus auch.*

*Beweis.* □

**Theorem 3.1.28.** *Seien $V$ und $W$ zwei $K$-Vektorräume. Dann ist* $\mathrm{Hom}_K(V, W)$ *ein $K$-Vektorraum bezüglich die Addition der Vektoren (Funktionen):*

$$+ : \mathrm{Hom}_K(V, W) \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W),$$
$$(f + g)(x) = f(x) + g(x) \textit{ für alle } x \in V,$$

*und die Skalarmultiplikation*

$$\cdot : K \times \mathrm{Hom}_K(V, W) \to \mathrm{Hom}_K(V, W), (\alpha f)(x) = \alpha f(x), \textit{ für alle } x \in V.$$

*Insbesondere ist* $(\mathrm{End}_K(V), +, \circ)$ *ein unitärer Ring.*

*Beweis.* □

**Definition 3.1.29.** Sei $f : V \to W$ eine lineare Abbildung. Man nennt den *Kernel* bzw das *Bild* von $f$ die Mengen

$$\mathrm{Ker} f = \{x \in V \mid f(x) = 0\} \text{ und } \mathrm{Im} f = \{f(x) \mid x \in V\}.$$

**Satz 3.1.30.** *Ist $f : V \to W$ eine lineare Abbildung, so gelten*
(a) $\mathrm{Ker} f \leq_K V$.
(b) $\mathrm{Im} f \leq_K W$.
(c) *$f$ ist genau dann injektiv wenn* $\mathrm{Ker} f = 0$.
(d) *$f$ ist genau dann surjektiv wenn* $\mathrm{Im} f = W$.

*Beweis.* □

**Übungen zu Vektorräume.**

**Übung 3.1.31.** Man zeige, dass $\mathbb{R}_+^* = (0, \infty)$ ein $\mathbb{R}$-Vektorraum ist bezüglich die Addition der Vektoren:

$$\boxplus : \mathbb{R}_+^* \times \mathbb{R}_+^* \to \mathbb{R}_+^*,\ x \boxplus y = xy, \text{ für alle } x, y \in \mathbb{R}_+^*,$$

und die Skalarmultiplikation

$$\boxdot : \mathbb{R} \times \mathbb{R}_+^* \to \mathbb{R}_+^*,\ \alpha \boxdot x = x^\alpha \text{ für alle } x \in \mathbb{R}_+^*, \alpha \in \mathbb{R}.$$

**Übung 3.1.32.** Man überprüfe ob die Operationen:

$$\boxplus : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ x \boxplus y = \sqrt[5]{x^5 + y^5}, \text{ für alle } x, y \in \mathbb{R},$$
$$\boxdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R},\ \alpha \boxdot x = \alpha \sqrt[5]{\alpha} x \text{ für alle } \alpha, x \in \mathbb{R}$$

eine $\mathbb{R}$-Vektorraum Struktur auf $\mathbb{R}$ definieren.

**Übung 3.1.33.** Welche aus den folgende Teilmengen von $\mathbb{R}^3$ sind $\mathbb{R}$-Unterräume:

- $A = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 0\}$.

- $B = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid 2x_1 + x_2 - x_3 = 1\}$.
- $C = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$.
- $D = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1^2 + x_2 = 0\}$.
- $E = \mathbb{R}^3 \setminus A$.
- $F = (\mathbb{R}^3 \setminus A) \cup \{0\}$.

**Übung 3.1.34.** Man zeige, dass $K_n[X] = \{f \in K[X] \mid \mathrm{grad}(f) \leq n\}$ ist ein $K$-Unterraum von $K[X]$, wobei $n \in \mathbb{N}$ ist befestigt.

**Übung 3.1.35.** Man finde die Gleichungen die alle Vektoren aus der Unteräume $S = \langle [1, 2, -1] \rangle$ und $T = \langle [1, 2, 1], [-2, 1, -3] \rangle$ von $\mathbb{R}^3$ charakterisieren (die Gleichungen dieser Unterräumen).

**Übung 3.1.36.** Man schreibe die Unterräumen $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x_2 - x_3 = 0\}$ und $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 - x - 2 = x_2 - x_3 = x_3 - x_1\}$ von $\mathbb{R}^3$ als erzugte Unterräume (mit minimale Anzahl der erzeugende Vektoren).

**Übung 3.1.37.** Man betrachte die Teilmengen $S, T \subseteq \mathbb{R}^3$ gegeben durch $S = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$ und $T = \{[x_1, x_2, x_3] \in \mathbb{R}^3 \mid x_1 = x_2 = x_3\}$. Man zeige, dass $S, T \leq \mathbb{R}^3$ und $S \oplus T = \mathbb{R}^3$.

**Übung 3.1.38.** Man betrachte $S = \{\alpha I_2 \in \mathbb{M}_{2\times 2}(\mathbb{R}) \mid \alpha \in \mathbb{R}\}$ und $T = \{A \in \mathbb{M}_{2\times 2}(\mathbb{R}) \mid \mathrm{Tr}(A) = 0\}$, wobei $\mathrm{Tr}(A)$ ist die Summe der Eigaben aus der Haputdiagonale der matrix $A$. Man zeige, dass $S, T \leq_{\mathbb{R}} \mathbb{M}_{2\times 2}(\mathbb{R})$ und $S \oplus T = \mathbb{M}_{2\times 2}(\mathbb{R})$.

**Übung 3.1.39.** Man betrachte eine beliebige Menge $A$ und $\mathbb{R}^A = \{f : A \to \mathbb{R} \mid f \text{ eine Funktion ist}\}$. Man zeige, dass $\mathbb{R}^A$ ein $\mathbb{R}$-Vektorraum ist bezüglich die Addition der Vektoren (Funktionen):

$$+ : \mathbb{R}^A \times \mathbb{R}^A \to \mathbb{R}^A, (f + g)(x) = f(x) + g(x), \text{ für alle } x \in A,$$

und die Skalarmultiplikation

$$\cdot : \mathbb{R} \times \mathbb{R}^A \to \mathbb{R}^A, (\alpha f)(x) = \alpha f(x), \text{ für alle } x \in A.$$

**Übung 3.1.40.** Man betrachte die Teilmengen $S = \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ ist gerade}\}$ und $T = \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ ist ungerade}\}$ von $\mathbb{R}^{\mathbb{R}}$. Man zeige, dass $S, T \leq \mathbb{R}^{\mathbb{R}}$ und $S \oplus T = \mathbb{R}^R$.

**Übung 3.1.41.** Man betrachte eine Primzahl $p \in N$. In jedem $\mathbb{Z}_p$-Vektorraum gilt es: $0 = x + x + \ldots + x(p \text{ mal})$, für alle $x \in V$. Existiert eine $\mathbb{Z}_p$-Vektorraum Struktur auf der Gruppe $(\mathbb{Z}, +)$, wobei $p \in \mathbb{N}$ eine Primzahl ist?

**Übung 3.1.42.** Welche aus den folgenden Abbildungen sind linear:

(1) $f : \mathbb{R}^3 \to \mathbb{R}^3,\ f[x_1, x_2, x_3] = [x_1 - x_2, x_2 - x_3, x_3 - x_1]$.
(2) $f : \mathbb{R}^3 \to \mathbb{R}^3,\ f[x_1, x_2, x_3] = [x_1 - 1, x_2 + 2, x_3 + 1]$.
(3) $f : \mathbb{R}^3 \to \mathbb{R}^2,\ f[x_1, x_2, x_3] = [2x_1 - 3x_2 + x_3, -x_1 + x_2 + 3x_3, x_1 + x_2 + x_3]$.
(4) $f : \mathbb{R}^2 \to \mathbb{R}^3,\ f[x_1, x_2] = [x_1 + x_2, x_1 - x_2, 2x_1 + x_2]$.
(5) $f : \mathbb{R}^2 \to \mathbb{R},\ f[x_1, x_2] = x_1^2 - x_2^2$.
(6) $f : \mathbb{R}^2 \to \mathbb{R}^2,\ f[x_1, x_2] = [a_{1,1}x_1 + a_{2,1}x_2, a_{1,2}x_1 + a_{2,2}x_2]$, wobei $a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2} \in \mathbb{R}$ sind befestigt.

Für die Abbildungen die linear sind, bestimme man die Gleichungen der Unteräume $\mathrm{Ker} f$ und $\mathrm{Im} f$.

3.2. **Basen.**

**Lineare Unabhängigkeit.**

**Definition 3.2.1.** Sei $V$ ein $K$-Vektorraum. Man nennt *Liste von Vektoren* ein Element $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ aus $V^{n\times 1}$, wobei $n \in \mathbb{N}$ beliebig ist. Eine Liste von Vektoren $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ heißt *linear unaghängig* falls für Skalaren $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ gilt $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$. Man nennt *linear abhänging* eine Liste von Vektoren die nicht linear unabhängig ist. In diesem Fall eine linear abhängige Relation ist eine Glaichung aus der Form $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ mit Skalaren $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ nicht alle null.

**Bemerkung 3.2.2.**
(1) Die Definition der lineare Unabhángigkeit der Liste $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ könnte als
$$[\alpha_1, \alpha_2, \ldots, \alpha_n][v_1, v_2, \ldots, v_n]^t = 0 \Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$$
geschrieben werden. Das ist der Grund dafür wir $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ statt $[v_1, v_2, \ldots, v_n] \in V^n$ betrachten.
(2) Die leere Liste von Vektoren ist auch erlaubt (für $n = 0$). Insbesondere ist die leere Liste linear unabhängig.
(3) Eine Liste mit eienm einzigen Element $[v_1]^t$ ist genau dann linear unabhängig wenn $v_1 \neq 0$.
(4) Ist $v_i = 0$, so ist $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ linear abhängig, da
$$0v_1 + \ldots + 1v_i + \ldots + 0v_n = 0.$$
(5) Gilt $v_i = v_j$ mit $i \neq j$ so ist $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ linear abhängig, da
$$0v_1 + \ldots + 1v_i + \ldots + (-1)v_j + \ldots 0v_n = 0.$$
(6) Manchmal wir sind nicht interesiert von der Ordnung der Vektoren aus der Liste $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t$ und wir sagen dass die Vektoren $v_1, v_2, \ldots, v_n$ linear (un)abhängig sind statt die Liste $\mathbf{v}$ jeweilige Eigenschaft hat.

**Beispiel 3.2.3.**
(1) Die Liste $[v_1, v_2, v_3]^t$ von Vektoren $v_1 = [1, 0, 1]$, $v_2 = [1, 2, 3]$ und $v_3 = v_1 + v_2 = [2, 2, 4]$ in $\mathbb{R}^3$ sind linear abhängig, da
$$1v_1 + 1v_2 + (-1)v_3 = v_1 + v_2 - v_3 = 0.$$
(2) Die Liste $[e_1, e_2, e_3]^t$ von Vektoren $e_1 = [1, 0, 0]$, $e_2 = [0, 1, 0]$, $e_3 = [0, 0, 1]$ ist linear unabhängig in $\mathbb{R}^3$.

Man sagt dass die Liste von Vektoren $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ eine Unterliste der Liste $[w_1, w_2, \ldots, w_m]^t \in V^{m\times 1}$ ist falls $\{v_1, v_2, \ldots, v_n\} \subseteq \{w_1, w_2, \ldots, w_m\}$ gilt. Mit anderen Wörten $[w_1, w_2, \ldots, w_m] = [v_{i_1}, v_{i_2}, \ldots, v_{i_m}]$, mit $i_1, i_2, \ldots, i_n \in \{1, \ldots, n\}$.

**Satz 3.2.4.** *Man betrachte* $\mathbf{w} = [v_{i_1}, v_{i_2}, \ldots, v_{i_m}]^t \in V^{m\times 1}$ *eine Unterliste der Liste* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$. *Ist* $\mathbf{w}$ *linear abhängig so ist* $\mathbf{v}$ *auch. Äquivalent, ist* $\mathbf{v}$ *linear unabhängig so ist* $\mathbf{w}$ *auch.*

*Beweis.* □

**Notation 3.2.5.** Sei $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ eine Liste von Vektoren. Für $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$ wir bezeichnen $\mathbf{v}^{\setminus i_1, i_2, \ldots, i_k}$ die Unterliste die aus $\mathbf{v}$ durch die Elimination der Vektoren $v_{i_1}, v_{i_2}, \ldots, v_{i_n}$ gebildet ist.

Für eine Liste von Vektoren $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ schreiben wir einfach $\langle \mathbf{b} \rangle = \langle b_1, b_2, \ldots, b_n \rangle$ und sprechen wir über den von der Liste $\mathbf{b}$ erzeugten Unterraum.

**Satz 3.2.6.** *Sei* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *eine Liste von Vektoren. Die Liste* $\mathbf{v}$ *ist genau dann linear unabhängig, falls ein* $i \in \{1, 2, \ldots, n\}$ *existiert, so dass* $v_i$ *ist eine lineare Kombination der Vektoren aus der Liste* $\mathbf{v}^{\setminus i}$.

*Beweis.* □

**Korollar 3.2.7.** *Sei* $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ *eine Liste von Vektoren, so dass ein* $i \in \{1, 2, \ldots, n\}$ *existiert, mit der Eigenschaft dass* $v_i$ *eine lineare Kombination der Vektoren aus der Liste* $\mathbf{v}^{\setminus i}$ *ist. Dann gilt* $\langle \mathbf{v} \rangle = \langle \mathbf{v}^{\setminus i} \rangle$.

*Beweis.* □

**Definition 3.2.8.** Eine endliche Teilmenge $\{v_1, v_2, \ldots, v_n\} \subseteq V$ heißt *frei* falls die Liste $[v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ linear unabhängig ist. Eine (möglich unedliche) Menge von Vektoren $B \subseteq V$ heißt *frei* falls jede endliche Teilmenge von $B$ ist frei.

**Basen und Koordinaten.**

**Definition 3.2.9.** Eine *(geordnete) Basis* eines $K$-Vektorräumes $V$ ist eine Liste $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$ von Vektoren die linear unabhängig ist und $\langle \mathbf{b} \rangle = V$ gilt (d. h. die Vektoren der Liste erzeugen $V$).

**Bemerkung 3.2.10.** (a) Often sind wir interesiert von nicht geordnete Basen, d. h. Teilmengen

$$\{b_1, b_2, \ldots, b_n\} \subseteq V$$

so dass $[b_1, b_2, \ldots, b_n]^t$ eine (geordnete) Basis in der Sinne der Definition 3.2.9 ist.

(b) Der Fall einer Basis mit (möglich) unedlich viele Elemente ist auch erlaubt, obwohl wir es nicht studieren: Eine Basis eines Vektorräumes $V$ ist eine Teilmenge $B \subseteq V$ so dass $B$ frei ist und $\langle B \rangle = V$.

**Beispiel 3.2.11.** Die Liste $\mathbf{e} = [e_1, e_2, \ldots, e_n]^t$ wobei $e_1 = [1, 0, \ldots, 0] \in K^n$, $e_2 = [0, 1, \ldots, 0] \in K^n$, …, $e_n = [0, 0, \ldots, 1] \in K^n$, ist eine Basis von $K^n$. Man nennt $\mathbf{e}$ die *kanonische Basis* von $K^n$. Die kanonische Basis lässt sich mit der Hilfe der so gennanten Kronecker Symbole geschrieben:

$$e_i = [\delta_{i,j}]_{1\le j\le n} \in K^n, \text{ wobei } \delta_{i,j} = \begin{cases} 1 \text{ falls } i = j \\ 0 \text{ falls } i \neq j \end{cases} \quad \text{für alle } i \in \{1, \ldots, n\}.$$

**Satz 3.2.12.** *Seien* $V$ *ein* $K$*-Vektorraum und* $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. *Die folgende Aussagen sind äquivalent:*

(i) $\mathbf{b}$ *ist eine maximale linear unabhängige Liste von Vektoren, d. h.* $\mathbf{b}$ *ist linear unabhängig und für jedes* $x \in V$ *hat die Liste* $\mathbf{b}' = [b_1, b_2, \ldots, b_n, x]$ *diese Eigenschaft nicht mehr.*

(ii) $\mathbf{b}$ *ist eine minimale Liste derer Vektoren erzeugen* $V$*, d. h.* $\langle \mathbf{b} \rangle = V$ *und für jedes* $i \in \{1, \ldots, n\}$*, es gilt* $\langle \mathbf{b}^{\setminus i} \rangle \neq V$.

(iii) $\mathbf{b}$ *ist eine Basis von* $V$.

*Beweis.* □

**Definition 3.2.13.** Man nennt *endlich erzeugt* einen $K$-Vektorraum $V$ mit der Eigenschaft dass eine endliche Teilmenge $\{b_1, b_2, \ldots, b_n\} \subseteq V$ existiert, so dass $\langle b_1, b_2, \ldots, b_n \rangle = V$.

**Korollar 3.2.14.** *Jeder endlich erzeugten $K$-Vektorraum $V$ hat eine Basis.*

*Beweis.* □

**Bemerkung 3.2.15.** Hier und in was folgt, betrachten wir nur endlich erzeugten Vektorräume. Troztdem gelten viele Ergebnisse (z. B. Korollar 3.2.14, Theorem 3.2.24, Korollar 3.2.19 etc.) für Vektorräume die nicht endlich erzeugt sind.

**Satz 3.2.16.** *Seien $V$ ein $K$-Vektorraum und $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. Die folgende Aussagen sind äquivalent:*

(i) $\mathbf{b}$ *ist eine Basis von $V$.*
(ii) *Für jeden Vektor $x \in V$ existiert einen einzigen System von Skalaren*

$$\alpha = [\alpha_1, \ldots, \alpha_n] \in K^n \text{ so dass } x = \alpha\mathbf{b} = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n.$$

*Beweis.* □

**Definition 3.2.17.** Seien $V$ ein $K$-Vektorraum und $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t \in V^{n\times 1}$. Für einen Vektor $x \in V$ nennt man die *Koordinaten* von $x$ bezüglich $\mathbf{b}$ die einzig bestimmten Skalaren $[\alpha_1, \ldots, \alpha_n]$ mit der Eigenschaft $x = \alpha_1 b_1 + \ldots + \alpha_n b_n$.

**Die Dimension eines Vektorräumes.**

**Lemma 3.2.18.** *(Lemma von Steinitz) Man betrachte zwei Liste von Vektoren $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ und $\mathbf{w} = [w_1, w_2, \ldots, w_m]^t \in V^{m\times 1}$ in einem $K$-Vektorraum $V$, wobei $n, m \in \mathbb{N}$. Wenn $\mathbf{v}$ linear unabhängig ist und $\langle \mathbf{w} \rangle = V$, dann gelten $n \leq m$ und, nach einer eventuelle Numerierung, $\langle v_1, \ldots, v_n, w_{n+1}, \ldots, w_m \rangle = V$.*

*Beweis.* □

**Korollar 3.2.19.** *Jede zwei Basen eines (endlich erzeugten) $K$-Vektorraumes haben dieselbe Anzahl von Elemente.*

*Beweis.* □

**Definition 3.2.20.** Durch Definition ist die *Dimension* eines (endlich erzeugten) $K$-Vektorraumes $V$ die Anzahl der Elemente einer Basis (folglich aller Basen) von $V$. Man schreibt $\dim_K V$ oder einfach $\dim V$. Man spricht nicht mehr uber endlich erzeugten sondern *endlich dimensionalen* Vektorräume.

**Beispiel 3.2.21.** (1) $\dim 0 = 0$.
(2) $\dim_K K^n = n$; insbesondere $\dim_{\mathbb{R}} \mathbb{R} = 1$, $\dim_{\mathbb{R}} \mathbb{R}^2 = 2$, $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$

**Bemerkung 3.2.22.** In einem endlich dimensionalen $K$-Vektorraum $V$ die folgende Aussagen sind wahr:

(a) Jede lineare unabhängige Liste lässt sich zu einer Basis fertigzustellen.
(b) Aus jeder Liste die $V$ erzeugt, kann man eine Basis herausfinden.
(c) $\dim V$ ist die größte Anzahl der Elemente einer Liste die linear unabhängig ist.
(d) $\dim V$ ist die kleinste Anzahl der Elemente einer liste die $V$ erzeugt.

**Satz 3.2.23.** *Seien $V$ ein $K$-Vektorraum mit $\dim_K V = n$ und $\mathbf{b} = [b_1, b_2, \ldots, b_n] \in V^{n\times 1}$ eine liste von Vektoren. Die folgende Aussagen sind äquivalnet:*

(i) $\mathbf{b}$ *ist linear unabhängig.*
(ii) $\langle \mathbf{b} \rangle = V$.
(iii) $\mathbf{b}$ *ist eine Basis.*

*Beweis.* □

**Die universelle Eigenschaft der Basis eines Vektorräumes.**

**Theorem 3.2.24.** *[die universelle Eigenschaft der Basis] Seien $V$ und $W$ zwei $K$-Vektorräume und $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ eine Basis von $V$. Für jede Funktion $f : \{v_1, v_2, \ldots, v_n\} \to W$ existiert eine eizige lineare Abbildung $\bar{f} : V \to W$ so dass $\bar{f}(v_i) = f(v_i)$ für alle $1 \leq i \leq n$ (d. h. $\bar{f}$ verlängert $f$ oder $f$ eine Beschrenkung von $\bar{f}$ ist).*

*Beweis.* □

**Korollar 3.2.25.** *Seien $V$ und $W$ zwei $K$-Vektorräume und $\mathbf{v} = [v_1, v_2, \ldots, v_n]^t \in V^{n\times 1}$ eine Basis von $V$.*

(a) *Sind $f, g : V \to W$ lineare Abbildungen so dass $f(v_i) = g(v_i)$ für alle $1 \leq i \leq n$, so gilt $f = g$.*
(b) *Ist $\dim_K W = n$ so gilt $V \cong W$.*
(c) *Es gilt $V \cong K^n$.*

**Einige Formeln mit der Dimension gebunden.**

**Satz 3.2.26.** *Man betrachte einen $K$-Vektorraum $V$ un $S, T \leq_K$ zwei Unterräume. Dann gilt:*

$$\dim S + \dim T = \dim(S + T) - \dim(S \cap T).$$

*Beweis.* □

**Korollar 3.2.27.** *Ist $V$ ein endlich dimensionaler $K$-Vektorraum und $S \leq_K V$, so gilt $\dim S \leq \dim V$. Mehr, $\dim S = \dim V$ gdw $S = V$.*

*Beweis.* □

**Satz 3.2.28.** *Sei $f : V \to W$ eine lineare Abbildung zwichen zwei $K$-Vektorräume $V$ and $W$. Dann gilt:*

$$\dim V = \dim \mathrm{Ker} f + \dim \mathrm{Im} f.$$

*Beweis.* □

**Korollar 3.2.29.** *Seien $V$ und $W$ zwei $K$-Vektorräume mit $\dim V = \dim W$ und $f : V \to W$ eine lineare Abbildung. Die folgende Aussagen sind äquivalnet:*

(i) *$f$ ist injektiv.*
(ii) *$f$ ist surjektiv.*
(iii) *$f$ ist bijektiv.*

*Beweis.* □

**Die Ersetzungslemma.**

**Theorem 3.2.30.** *(die Ersetzungslemma) Seien $\mathbf{b} = [b_1, b_2, \ldots, b_n]^t$ eine Basis des $K$-Vektorräumes $V$ und $v \in V$ mit den Koordinaten $[\alpha_1, \alpha_2 \ldots, \alpha_n]$ bezüglich der Basis $\mathbf{b}$ (d. h. $v = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n$). Man betrachte die Liste von Vektoren $\mathbf{v}' = [b_1, \ldots, v, \ldots, b_n]$ die aus $\mathbf{v}$ durch die Ersetzung des Vektors $b_i$ mit $v$ entstanden. Dann:*

(a) *$\mathbf{b}'$ ist eine Basis gdw $\alpha_i \neq 0$.*

(b) *Ist* $\mathbf{b}'$ *eine Basis und ist* $x \in V$ *mit den Koordinaten* $[x_1, x_2 \dots, x_n]$ *bezüglich* $\mathbf{v}$ *und* $[x'_1, x'_2 \dots, x'_n]$ *bezüglich* $\mathbf{v}'$ *so gelten:*

$$\begin{cases} x'_i = \alpha_i^{-1} x_i \\ x'_j = \alpha_i^{-1}(\alpha_i x_j - \alpha_j x_i) \text{ für } j \neq i \end{cases}.$$

*Beweis.* □

**Definition 3.2.31.** Man nennt den Rang einer Liste von Vektoren $\mathbf{v} = [v_1, \dots, v_n]^t$ die Dimension des von $\mathbf{v}$ erzeugten Unterraum, d. h. $\operatorname{rank} \mathbf{v} = \dim\langle \mathbf{v} \rangle$.

**Bemerkung 3.2.32.** Da jede linear unabhängige Liste lässt sich zu einer Basis fertigzustellen, können wir die Ersetzungslemma um den Rang einer Liste von Vektoren zu berechnen.

**Übungen zu Basen.**

**Übung 3.2.33.** Man zeige, dass eine Liste mit zwei Vektoren $[x, y]^t \in V^{2\times 1}$ ist genau dann linear abhängig wenn existiert $\alpha \in K$ so dass $x = \alpha y$ oder $y = \alpha x$. Man finde eine geometrische Interpretation der Gleichungen $x = \alpha y$ oder $y = \alpha x$ im Fall $K = \mathbb{R}$, und $V = \mathbb{R}^3$. Wenn ist eine liste von Vektoren $[x, y, z]^t \in (\mathbb{R}^3)^{3\times 1}$ linear abhängig?

**Übung 3.2.34.** Sei $V$ ein $K$-Vektorraum mit $\dim V = n$. Man zeige, dass für jede naturliche Zahl $m \leq n$ ein Unterraum $S \leq_K V$ existiert so dass $\dim S = m$.

**Übung 3.2.35.** Sei $f : V \to W$ eine lineare Abbildung und $X \subseteq V$. Man zeige, dass $f(\langle X \rangle) = \langle f(X) \rangle$.

**Übung 3.2.36.** Man zeige, dass $\mathbb{Q}+\mathbb{Q}\sqrt{2} = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ein $\mathbb{Q}$-Vektorraum ist, und bestimme man eine Basis und die Dimension.

**Übung 3.2.37.** Sei $p$ eine Primzahl. Man zeige, dass

$$\mathbb{Q} + \mathbb{Q}\sqrt[3]{p} + \mathbb{Q}\sqrt[3]{p^2} = \{a + b\sqrt[3]{p} + \sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$$

ein $\mathbb{Q}$-Vektorraum ist, und bestimme man eine Basis und die Dimension.

**Übung 3.2.38.** Sei $f : V \to W$ eine lineare Abbildung und $\mathbf{v} = [v_1, \dots, v_n]^t \in V^{n\times 1}$ eine liste von Vektoren. Man bezeichne $f(\mathbf{v}) = [f(v_1), \dots, f(v_n)]^t \in W^{n\times 1}$. Dann:

(a) Ist $f$ injektiv und $\mathbf{v}$ linear unabhängig, so ist $f(\mathbf{v})$ linear unabhängig auch.
(b) Ist $f$ surjektiv und $\langle \mathbf{v} \rangle = V$, so gilt $\langle f(\mathbf{v}) \rangle = W$.
(c) Ist $f$ bijektiv und $\mathbf{v}$ eine Basis, so ist $f(\mathbf{v})$ eine Basis auch.

**Übung 3.2.39.** Sei $V$ ein $K$-Vektorraum mit $\dim V = n$ und $S \leq_K V$. Man zeige, dass $T \leq_K V$ existiert, so dass $S \oplus T = V$.

**Übung 3.2.40.** Man betrachte in $\mathbb{R}^3$ die Liste von Vektoren $\mathbf{v} = [v_1, v_2, v_3]^t$. Man benutze zwei Methoden (die Definition einer Basis bzw. die Ersetzungslemma) um $a \in \mathbb{R}$ zu finden, so dass $\mathbf{v}$ eine Basis von $\mathbb{R}^3$ ist, wobei:

(1) $v_1 = [1, -2, 0]$, $v_2 = [2, 1, 1]$, $v_3 = [0, a, 1]$.
(2) $v_1 = [2, 1, -1]$, $v_2 = [0, 3, -1]$, $v_3 = [1, a, 1]$.

**Übung 3.2.41.** Man zeige dass $\mathbf{b} = [b_1, b_2, b_3, b_4]^t$ wobei

$$b_1 = [1, 2, -1, 2], b_2 = [1, 2, 1, 4], b_3 = [2, 3, 0, -1], b_4 = [1, 3, -1, 0]$$

eine Basis von $\mathbb{R}^4$ ist und man bestimme die Koordinaten von $x = [2, 3, 2, 10]$.

**Übung 3.2.42.** Man bestimme $a \in \mathbb{R}$ so dass die Liste $\mathbf{v} = [v_1, v_2, v_3]^t$ eine Basis von $\mathbb{R}^3$ ist, wobei:

$$v_1 = (a, 1, 1), v_2 = (1, a, 1), v_3 = (1, 1, a).$$

**Übung 3.2.43.** Man bestimme den Rang der Listen von Vektoren in $\mathbb{R}^4$:

(1) $[[0, 1, 3, 2], [1, 0, 5, 1], [-1, 0, 1, 1], [3, -1, -3, -4], [2, 0, 1, -1]]^t$;
(2) $[1, 2, 3, 0], [0, 1, -1, 1], [3, 7, 8, 1], [1, 3, 2, 1]]^t$;
(3) $[[1, 2, -1, 2], [2, 3, 0, -1], [2, 4, 0, 6], [1, 2, 1, 4], [3, 6, -1, -1], [1, 3, -1, 0]]^t$.

**Übung 3.2.44.** Man betrachte die Unterräumen

$$S = \langle [2, 0, 1, -1], [0, 1, 2, 3], [-1, 0, 1, 1], [1, 1, 5, 2] \rangle$$
$$T = \langle [1, 0, 2, 0], [2, 1, -1, 2], [-1, -1, 3, -2] \rangle$$

von dem reelen Vektorraum $\mathbb{R}^4$. Man benutze die Ersetzungslemma die Dimensionen je eine Basis und die Dimensionen der Unterräume $S$, $T$, $S + T$ und $S \cap T$ zu berechnen.

**Übung 3.2.45.** Man benutze die Ersetzungslemma die Dimensionen und je eine Basis der Unterräume $\mathrm{Ker} f$ und $\mathrm{Im} f$ zu berechnen, falls:

(1) $f : \mathbb{R}^3 \to \mathbb{R}^3$ $f[x_1, x_2, x_3] = [x_1 + 2x_2, x_2 + x_3, x_1 - 2x_3]$.
(2) $f : \mathbb{R}^4 \to \mathbb{R}^3$ $f[x_1, x_2, x_3, x_4] = [x_1 - x_2 - x_3, 3x_2 + x_4, 3x_1 - 3x_3 + x_4]$
(3) $f : \mathbb{R}^3 \to \mathbb{R}^2$ $f[x_1, x_2, x_3] = [-x_1 + 2x_2, x_1 - x_2 + x_3, x_2 + 2x_3]$.
(4) $f : \mathbb{R}^2 \to \mathbb{R}^3$ $f[x_1, x_2] = [x_1 - 3x_2, 2x_1, -x_1 + x_2]$.

Babeş-Bolyai Universität, Facultät für Mathematik und Informatik, 1, Mihail Kogălniceanu, 400084 Klausenburg, Rumänien

*E-mail address*: cmodoi@math.ubbcluj.ro