# Allgemeine Algebra WS 2004/05

für Informatiker und Wirtschaftsinformatiker

von Prof. Thomas Ihringer

Simon Fuhrmann · Christian M. Meyer
Christian Schäck

17. Februar 2005

---

**Vorbemerkungen:** Dieses Skript beschäftigt sich mit *strukturellen* Grundlagen der Mathematik, nämlich solchen aus den Bereichen

- Kapitel 0: Grundlagen (Mengensprache, Kombinatorik, Beweistechniken)
- Kapitel 1: Diskrete Mathematik (kombinatorischen Strukturen)
- Kapitel 2: Algebra (algebraischen Strukturen)
- Kapitel 3: Logik (logischen Strukturen)

Hierzu können, in der Reihenfolge dieser Kapitel, die folgenden Bücher als „Basis“ dienen. Aber das Skript enthält alles Wesentliche, und außerdem gibt es viele andere passende Bücher (worüber sich jeder Interessierte selbst informieren möge):

- Christoph Meinel, Martin Mundhenk: Mathematische Grundlagen der Informatik. Teubner, Stuttgart, 2002.
- Thomas Ihringer: Diskrete Mathematik.
  Heldermann, Lemgo, 2002
- Thomas Ihringer: Allgemeine Algebra.
  Heldermann, Lemgo, 2003
- Uwe Schöning: Logik für Informatiker.
  Spektrum, Heidelberg, 2002

# Inhaltsverzeichnis

# 0 Grundlagen

Dieses Kapitel beschäftigt sich mit der für die moderne Mathematik als Sprachmittel grundlegenden Mengensprache, mit einigen damit verbundenen kombinatorischen Sachverhalten sowie mit elementaren Beweistechniken.

## 0.1 Mengen, Relationen, Abbildungen

Der Begründer der **Mengenlehre** war Ende des 19. Jahrhunderts *Georg Cantor*. Er verwendete folgende recht informelle Definition:

> Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente der Menge genannt werden) zu einem Ganzen.

Dieser Gedanke war bahnbrechend für die moderne Mathematik, weil er eine einheitliche formale Sprache begründete. Aber er stellte sich als zu „naiv“ heraus. Dazu später mehr!

### 0.1.1 Operationen auf Mengen

Zunächst einige elementare Tatsachen über Mengen. Es gibt eine Reihe wichtiger **Operationen auf Mengen**, mit denen man aus bekannten Mengen (z.B. $A$ und $B$) neue Mengen erhält. Beispielsweise:

| | |
|---|---|
| $A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$ | **Vereinigung** von $A$ und $B$ |
| $A \cap B := \{x \mid x \in A \text{ und } x \in B\}$ | **(Durch-)Schnitt** von $A$ und $B$ |
| $\mathcal{P}(A) := \{X \mid X \subseteq A\}$ | **Potenzmenge** von $A$ |

Man kann **Eigenschaften** verwenden, um aus bekannten Mengen neue Mengen zu erhalten. Ein Beispiel für $\mathbb{N}$ (Menge der **natürlichen Zahlen**):

| | |
|---|---|
| $\mathbb{N}_g := \{n \in \mathbb{N} \mid 2 \text{ teilt } n\}$ | Menge der geraden natürlichen Zahlen |

### 0.1.2 Das kartesische Produkt

Eine allgemeine Konstruktion für beliebige Mengen $A_1, \ldots, A_n$ enthält alle $n$-**Tupel** $(a_1, \ldots, a_n)$ mit $a_1 \in A_1, \ldots, a_n \in A_n$:

$$A_1 \times \ldots \times A_n := \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$$

Dies ist das **direkte** (oder **kartesische**) **Produkt** der Mengen $A_i$.

Im Sonderfall $A_1 = \cdots = A_n = A$ ergibt dies

$$A^n := A \times \cdots \times A$$

die $n$-te **Potenz** von $A$.

### 0.1.3 Relationen

Jede Teilmenge $R \subseteq A_1 \times \cdots \times A_n$ wird eine $n$-stellige **Relation** zwischen den Mengen $A_i$ genannt. Mathematische Relationen sind überall, sogar im „wirklichen“ Leben:

**Beispiel:** Sei

$A_1 :=$ Menge aller Darmstädter Haltestellen,
$A_2 :=$ Menge aller Darmstädter Bus- und Bahnlinien,
$A_3 :=$ Menge aller möglichen Endstationen,
$A_4 :=$ Menge aller möglichen Abfahrtszeiten
(z.B. $A_4 = \{0.00, 0.01, 0.02, \ldots, 23.59\}$).

Die Fahrpläne sämtlicher Haltestellen können (zum Beispiel) in einer Relation $R \subseteq A_1 \times A_2 \times A_3 \times A_4$ zusammengefasst werden. Hierzu ein mögliches Element von $R$ (ohne Gewähr!):

| Station | Linie | Endstation | Abfahrtszeit |
|---|---|---|---|
| (Hofgasse, | 8, | Alsbach, | 19.02) $\in R$ |

**Bemerkung:** Relationen können das Grundmaterial von *Datenbanken* bilden. In obigem Beispiel sollte es eine *Datenbankoperation* geben, die zum Beispiel alle Direktverbindungen von Hofgasse nach Eberstadt zwischen 19 und 20 Uhr findet, also etwa die Menge:

$$\{(a_1, a_2, a_3, a_4) \mid a_1 = \text{Hofgasse}, a_3 = \text{Eberstadt} \vee \text{Alsbach}, 19.00 \leq a_4 \leq 20.00\}$$

Besonders wichtig sind **binäre** (das heißt 2-stellige) Relationen von der Form $R \subseteq A^2$, also binäre Relationen auf einer Menge $A$. Nachfolgend zwei bedeutende Typen solcher Relationen:

### 0.1.4 Äquivalenzrelationen

Sei $A$ eine beliebige Menge. Eine Teilmenge $R \subseteq A^2$ heißt **Äquivalenzrelation** auf $A$, falls folgendes gilt: Für alle $a, b, c, \in A$ (wie üblich wird $xRy$ anstelle von $(x, y) \in R$ geschrieben)

| | | | | | |
|---|---|---|---|---|---|
| (Refl) | $aRa$ | | | | **Reflexivität** |
| (Sym) | $aRb$ | $\Rightarrow$ | $bRa$ | | **Symmetrie** |
| (Trans) | $aRb$ und $bRc$ | $\Rightarrow$ | $aRc$ | | **Transitivität** |

### 0.1.5 Ordnungsrelationen

Eine Teilmenge $R \subseteq A^2$ heißt **Ordnung** oder **Ordnungsrelation** auf $A$ (und das Paar $(A, R)$ eine **geordnete Menge**), falls für alle $a, b, c \in A$ die folgenden Axiome gelten:

| | | | | | |
|---|---|---|---|---|---|
| (Refl) | $aRa$ | | | | **Reflexivität** |
| (Anti) | $aRb$ und $bRa$ | $\Rightarrow$ | $a = b$ | | **Antisymmetrie** |
| (Trans) | $aRb$ und $bRc$ | $\Rightarrow$ | $aRc$ | | **Transitivität** |

**Beispiel (a):** Jede Relation der Form $R = \{(a, a) \mid a \in A\}$ (genannt **Gleichheitsrelation** auf $A$) ist trivialerweise eine Äquivalenzrelation *und* eine Ordnungsrelation (in der nichts geordnet ist),

**Beispiel (b):** Äquivalenzrelationen beschreiben oft, dass gewisse Objekte bezüglich bestimmter *Eigenschaften gleich* sind. Sei zum Beispiel $A$ die Menge aller Informatikstudenten an der TUD, die im Herbst 2005 ihr Vordiplom abschließen. Für $a, b \in A$ sei

$$aRb \quad :\Leftrightarrow \quad a \text{ und } b \text{ haben die selbe Vordiplomsnote in Mathematik.}$$

Dann ist $R$ eine Äquivalenzrelation auf $A$.

**Beispiel (c):** Für $x, y \in \mathbb{Z}$, sei $xRy \quad :\Leftrightarrow \quad 2$ teilt $x - y$. Dann ist $R$ eine Äquivalenzrelation. Sie hat zwei **Äquivalenzklassen** (nämlich Teilmengen von $\mathbb{Z}$ maximaler Größe, die aus paarweise äquivalenten Elementen bestehen):

$$[0]_R := \{x \in \mathbb{Z} \mid xR0\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \quad \text{(gerade Zahlen)}$$
$$[1]_R := \{x \in \mathbb{Z} \mid xR1\} = \{\ldots, -3, -1, 1, 3, 5 \ldots\} \quad \text{(ungerade Zahlen)}$$

*Ohne formale Definition:* Die Äquivalenzklassen jeder Äquivalenzrelation bilden eine **Partition** der Grundmenge $A$, das heißt sie sind paarweise disjunkt und ihre Vereinigung ist ganz $A$.

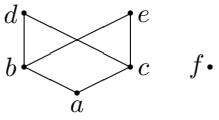
**Beispiel (d):** Jetzt eine vielleicht auf den ersten Blick umständlich definierte Ordnungsrelation: Die Schüler einer Klasse haben folgende Noten (andere Fächer werden der Einfachheit halber nicht betrachtet):

| | Adam | Bernd | Chris | Doris | Emma | Ferdi |
|---|---|---|---|---|---|---|
| Deutsch | 2 | 3 | 3 | 5 | 4 | 1 |
| Mathematik | 2 | 2 | 2 | 3 | 4 | 5 |

Für alle Schüler $x$ gelte $xRx$ und für je zwei verschiedene Schüler $x$ und $y$ werde definiert:

$$xRy \quad :\Leftrightarrow \quad \begin{array}{l} x \text{ hat in keinem Fach eine schlechtere Note als } y \\ \text{und in mindestens einem Fach eine bessere Note.} \end{array}$$

Dann ist $R$ eine Ordnungsrelation. Sie kann durch ein **Hasse-Diagramm** (auch: **Liniendiagramm**) dargestellt werden. Eine Linie aufwärts von $x$ nach $y$ heißt: $xRy$, und kein Element dazwischen.




$f$•

Abbildung 1: Liniendiagramm

**Beispiel (e):** Für jede Menge $M$ ist $(\mathcal{P}(M), \subseteq)$ eine geordnete Menge: Die Teilmengen von $M$, geordnet durch Inklusion.

**Bemerkung:** Für Ordnungsrelationen wird sehr oft $\leq$ geschrieben, statt $R$ oder anderen Symbolen; $\leq$ wird „kleiner gleich“ gelesen.

Die folgende Sorte von Relationen ist sehr wichtig.

### 0.1.6 Abbildungen

**Definition:** Eine **Abbildung** (oder **Funktion**) ist ein Tripel $(A, B, f)$, bestehend aus einer Menge $A$ (dem **Definitionsbereich** oder **Urbild**), eine Menge $B$ (dem **Wertebereich**) und einer 2-stelligen Relation $f \subseteq A \times B$ mit:

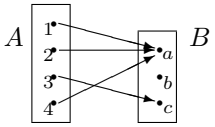
$$\text{(Abb)} \quad \forall x \in A\ \dot{\exists} y \in B\colon (x, y) \in f$$

Lies: „Für jedes $x \in A$ existiert genau ein $y \in B$ mit...“. Man nennt $\forall$ einen **Allquantor**, $\exists$ einen **Existenzquantor**, und der Punkt, $\dot{\exists}$, bedeutet „genau ein“.

Man nennt $f$ eine Abbildung von $A$ nach $B$ und schreibt dafür kurz $f\colon A \longrightarrow B$. Statt $(x, y) \in f$ wird üblicherweise $f(x) = y$ geschrieben, und $y$ heißt das **Bild** von $x$, und $y$ das **Urbild** von $y$ (möglicherweise nicht das einzige). Die Menge aller Bilder von $f$ heißt der **Bildbereich** von $f$, kurz $f(A)$ oder auch:

$$\text{bild}(f) := \{f(x) \mid x \in A\}$$

**Beispiel:** Sei $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $f = \{(1, a), (2, a), (3, c), (4, a)\}$. Das ist eine Abbildung $f\colon A \longrightarrow B$ mit $\text{bild}(f) = \{a, c\}$.




Wertetabelle von $f$:

| $x$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $f(x)$ | $a$ | $a$ | $c$ | $a$ |

Abbildung 2: Pfeildiagramm von $f$

In der Wertetabelle wird die vollständige Information im Grunde in der unteren Zeile gegeben: Wenn die Reihenfolge $1, 2, 3, 4$ der Urbildelemente vorgegeben ist, wird $f$ durch das 4-Tupel $(a, a, c, a)$ beschrieben. In derselben Weise entspricht jede Abbildung $f\colon A \longrightarrow B$ einem

$$A\text{-Tupel } \big(f(x)\big)_{x \in A} \in B^A$$

und jedes Tupel in $B^A$ entspricht einer Abbildung $A$ in $B$. Also:

Die Menge aller Abbildungen $f\colon A \longrightarrow B$ kann als $B^A$ geschrieben werden.

Weitere wichtige, hoffentlich schon vertraute Begriffe:

### 0.1.7 Injektivität, Surjektivität, Bijektivität

**Definition:** Eine Abbildung $f\colon A \longrightarrow B$ heißt

| | | |
|---|---|---|
| (i) | **injektiv**, | falls $\forall x, y \in A\colon f(x) = f(y) \Longrightarrow x = y$, |
| (ii) | **surjektiv** | falls $\forall y \in B \exists x \in A\colon f(x) = y$, |
| (iii) | **bijektiv**, | falls sie injektiv und surjektiv ist. |

**Beispiel (a):** Die Funktion $f\colon A \longrightarrow B$ aus Abbildung 2 ist weder injektiv noch surjektiv.

**Beispiel (b):** Sei $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) := x^2$. Diese Abbildung ist weder injektiv noch surjektiv. Aber mit abgeändertem Definitions- oder Wertebereich lässt sich das ändern, ohne die Abbildungsvorschrift zu ändern.

Beispielsweise ist die Abbildung $g\colon \mathbb{R} \longrightarrow \mathbb{R}_0^+$, $g(x) := x^2$ (Einschränkung des Wertebereichs auf die nichtnegativen reellen Zahlen) surjektiv, aber immer noch nicht injektiv. Mit ähnlichen Einschränkungen lassen sich aus $f$ auch injektive, nicht surjektive oder bijektive Abbildungen gewinnen.

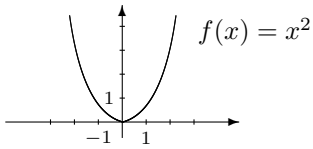



Abbildung 3: Injektivität, Surjektivität, Bijektivität

### 0.1.8 Russel'sches Paradoxon

Zum Abschluss dieses Abschnitts noch einmal zu Cantors Mengendefinition: Nach Cantor ist sicherlich

$$A := \{X \mid X \text{ ist eine Menge}\}$$

eine Menge, nämlich **die Menge aller Mengen**. Sicherlich sollte es immer möglich sein, mit Hilfe bestimmter Eigenschaften für die Elemente einer vorhandenen Menge, **Teilmengen** dieser Mengen zu gewinnen. Dem entsprechend sollte, wenn $A$ eine Menge ist, auch die Gesamtheit

$$B := \{X \in A \mid X \notin X\}$$

die Menge aller Mengen, die sich selbst nicht als Element enthalten, eine Menge sein. Enthält $B$ sich selbst als Element? Es gibt zwei Möglichkeiten, die beide zu einem Widerspruch führen:

| | | |
|---|---|---|
| Fall 1: | $B \in B$ | Nach Definition folgt sofort $B \notin B$ |
| Fall 2: | $B \notin B$ | Doch das impliziert $B \in B$! ↯ |

Dieser Widerspruch wird **Russellsches Paradoxon** genannt, nach seinem Entdecker, dem Philosophen und Mathematiker **Bertrand Russell**.

**Randbemerkung:** Natürlich gibt es solche „Gesamtheiten“ wie die „Gesamtheit aller Mengen“. Solche Gesamtheiten werden **Klassen** genannt. Alle Mengen sind auch Klassen, aber nicht bei allen Klassen handelt es sich um Mengen. Faustregel: Mengen müssen rein mengensprachlich mit Hilfe schon bekannter Mengen definierbar sein.

## 0.2 Kombinatorik

In der Kombinatorik beschäftigt man sich mit der Bestimmung der **Elementzahlen** verschiedener (endlicher) Mengen. Dabei werden verschiedenste Zähltechniken verwendet. Ein typisches Zählproblem: Wieviele Elemente hat die Potenzmenge (= Menge aller Teilmengen) einer gegebenen endlichen Menge?

### 0.2.1 Die Kardinalität von Mengen

**Definition:** Die Anzahl der Elemente einer Menge $A$ heißt die **Kardinalität** (oder **Mächtigkeit**) von $A$, in Zeichen: $|A|$. Beispielsweise gilt:

$$|\emptyset| = 0 \qquad |\{1,2,3\}| = |\{x, \square, 5\}| = 3$$
$$|\{1,2,\ldots,100\}| = 100 \qquad |\{100,102,104,\ldots,200\}| = 51$$

Für endliche Mengen ist klar, was obige Definition bedeutet. Für unendliche Mengen ist die Situation komplizierter. Die folgenden wichtigen Tatsachen gelten für beliebige Mengen $A$ und $B$ (werden aber hier nicht näher erläutert oder bewiesen):

**Satz:**

(a) Für zwei Mengen $A$ und $B$ gilt genau dann $|A| = |B|$, wenn es eine bijektive Abbildung $f\colon A \longrightarrow B$ gibt.
(b) Für jede Menge $A$ gilt: $|A| < |\mathcal{P}(A)|$.

**Bemerkungen:**

(a) Die Menge $\mathbb{Q}$ der rationalen Zahlen hat scheinbar „unendlich mal soviele“ Elemente wie die Menge der natrülichen Zahlen. Dennoch gilt (überraschenderweise) $|\mathbb{Q}| = |\mathbb{N}|$.
(b) Es gilt $|\mathbb{Q}| < |\mathbb{R}|$, das heißt $\mathbb{Q}$ ist **abzählbar unendlich**. (Und es ist unentscheidbar, ob es „zwischen“ $|\mathbb{Q}|$ und $|\mathbb{R}|$ noch eine weitere Kardinalität gibt.)

Es folgen einige wichtige Abzählprinzipien:

### 0.2.2 Additionsprinzip

Die Mengen $A$ und $B$ seien disjunkt (das heißt $A \cap B = \emptyset$). Dann gilt:

$$|A \cup B| = |A| + |B|$$

**Beispiel:** Wenn ein Verein 8 männliche und 13 weibliche Mitglieder hat, dann hat der Verein insgesamt $8 + 13 = 21$ Mitglieder.

Das nächste Prinzip benutzt **direkte Produkte**:

### 0.2.3 Multiplikationsprinzip

Für beliebige Mengen $A$ und $B$ gilt:

$$|A \times B| = |A| \cdot |B|$$

**Beispiel:** Wieviele mögliche Nummernschilder Darmstädter Fahrzeuge sind möglich? Jedes Nummernschild fängt mit DA an, gefolgt von 1-2 Buchstaben (des üblichen 26-elementigen Alphabets), gefolgt von einer höchstens 4-stelligen natürlichen Zahl. Der Buchstaben-Teil hat $26 + 26^2$ Möglichkeiten (Additionsprinzip!), und der Zahlen-Teil hat 9999 Möglichkeiten. Das Multiplikationsprinzip liefert deshalb insgesamt $(26 + 26^2) \cdot 9999$ mögliche Nummernschilder.

Die nächste Regel wurde schon erwähnt. Sie ist zwar sehr wichtig, wird aber dennoch oft verwendet, ohne explizit erwähnt zu werden:

### 0.2.4 Gleichheitsprinzip

Wenn $f\colon A \longrightarrow B$ eine bijektive Abbildung ist, dann gilt:

$$|A| = |B|$$

Es folgt ein letztes Prinzip (obwohl es natürlich viele weiter gibt). Es beruht auf der offensichtlichen Tatsache, dass es nicht darauf ankommt, in welcher Reihenfolge man die Elemente einer zweistelligen Relation $R \subseteq A \times B$ auf zwei Arten zu zählen. Für jedes $a \in A$ und für jedes $b \in B$ sei:

$$r_1(a) := |\{y \in B \mid (a, y) \in \mathbb{R}\}|$$
$$r_2(b) := |\{x \in A \mid (x, b) \in \mathbb{R}\}|$$

Es macht keinen Unterschied, ob man die Elemente von $R$ „$A$-weise“ oder „$B$-weise“ zählt:

### 0.2.5 Prinzip der doppelten Abzählung

Für jeder zweistellige Relation $R \subseteq A \times B$ gilt:

$$\sum_{a \in A} r_1(a) \;=\; \sum_{b \in B} r_2(b)$$

Beide Seiten dieser Gleichung ergeben $|R|$, die Anzahl der Elemente von $R$. Viele Mathemetiker betrachten dieses Prinzip als das wichtigste der Kombinatorik. Später werden wichtige Anwendungen betrachtet. Zum Warmwerden folgt hier ein etwas künstliches Beispiel:

$$R: \quad \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \hline \left(\begin{array}{cccc} \times & & \times & \\ & \times & \times & \times \\ \times & \times & \times & \end{array}\right) \end{array} \quad \left|\begin{array}{l} 1 \\ 2 \\ 3 \end{array}\right.$$

Abbildung 4: Kreuztabelle von $R$

**Beispiel:** Sei $A = \{1, 2, 3\}$ und $B = \{a, b, c, d\}$. Die Relation $R \subseteq A \times B$ sei durch obige Kreuztabelle gegeben (ein Kreuz an Stelle $ix$ bedeutet $(i, x) \in R$).

Es gilt:

$$r_1(1) = 2, \quad r_1(2) = r_1(3) = 3$$
$$r_2(a) = r_2(b) = 2, \quad r_2(c) = 3, \quad r_2(d) = 1$$

Tatsächlich gilt (keine Überaschung):

$$r_1(1) + r_1(2) + r_1(3) = 2 + 2 + 3 = 8$$
$$r_2(a) + r_2(b) + r_2(c) + r_2(d) = 2 + 2 + 3 + 1 = 8$$

### 0.2.6 Teilmengen endlicher Mengen

Jetzt werden die Teilmengen endlicher Mengen gezählt. Der Kürze halber wird jede $n$-elementige Menge eine $n$-Menge genannt. Der Menge aller Teilmengen einer Menge $N$ wird mit $\mathcal{P}(N)$ bezeichnet (Potenzmenge von $N$).

**Bemerkung:** Jede $n$-Menge $N$ hat genau $2^n$ Teilmengen, das heißt

$$|\mathcal{P}(N)| = 2^n$$

**Beweis:** Sei oBdA. (ohne Beschränkung der Allgemeinheit) $N = \{1, 2, \ldots, n\}$. Jede Teilmenge $S \subseteq N$ ist durch ihre Elemente bestimmt. Für $1 \in N$ gibt es zwei Möglichkeiten: $1 \in S$ oder $1 \notin S$. Und zwei Möglichkeiten für $2 \in N$: $2 \in S$ oder $2 \notin S$. Ebenso zwei Möglichkeiten für $3 \in N$. .... Zwei Möglichkeiten für $n \in N$.
Diese Möglichkeiten werden multipliziert (Multiplikationsprinzip). Zusammen ergeben sich $2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 = 2^n$ Möglichkeiten für Teilmengen von $N$. □

**Aufgabe:** Finde einen streng formalen Beweis für obige Bemerkung, der das Gleichheitsprinzip und das Multiplikationsprinzip verwendet.

**Beispiel:** Sei $N = \{1, 2, 3\}$. Es gibt genau $2^3 = 8$ Teilmengen von $N$:

$$\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\},\ \{1, 2, 3\}$$

### 0.2.7 $k$-Teilmengen endlicher Mengen

Jetzt werden die Teilmengen einer $n$-Menge $N$ in detaillierter Weise betrachtet: Die Menge aller $k$-Teilmengen ($k$-elementige Teilmengen) von $N$ wird mit $\mathcal{P}_k(N)$ bezeichnet. Weiter sei $\binom{n}{k} := |\mathcal{P}_k(N)|$ (die Mächtigkeit von $\mathcal{P}_k(N)$). Man spricht $\binom{n}{k}$ als $n$ *über* $k$. Aus Gründen, die später klar werden, nennt man die Zahlen $\binom{n}{k}$ **Binomialkoeffizienten**.

**Beobachtung:** Seien $n, k \in \mathbb{N}_0$ (der Menge der natürlichen Zahlen plus 0). Dann gilt:

(a) $\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = \binom{n}{n-1} = n$
(b) $\binom{n}{k} = \binom{n}{n-k}$

**Beweis:** (a) ist offensichtlich. Für (b) beachte man, dass durch

$$\mathcal{P}_k(N) \longrightarrow \mathcal{P}_{n-k}(N), \quad S \mapsto N \setminus S := \{x \in N \mid x \notin S\}$$

eine bijektive Abbildung gegeben ist. Also folgt (b) mit dem Gleichheitsprinzip.

Das Additionsprinzip liefert mit der Bemerkung von Seite 8 sofort:

**Folgerung:** $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$ für alle $n \in \mathbb{N}_0$.

Als nächstes wird eine Formel für $\binom{n}{k}$ entwickelt: Es wird das Prinzip der doppelten Abzählung auf die durch

$$(x, S) \in \mathbb{R} \quad :\Leftrightarrow \quad x \in S$$

definierte Relation $R \subseteq N \times \mathcal{P}_k(N)$ angewandt (wieder mit $N = \{1, 2, \ldots, n\}$). Für jedes $x \in N$ gilt dann:

$$\begin{aligned} r_1(x) &= |\{S \in \mathcal{P}_k(N) \mid x \in S\}| \\ &= |\mathcal{P}_{k-1}(N \setminus \{x\})| \\ &= \binom{n-1}{k-1} \end{aligned}$$

Für jedes $S \in \mathcal{P}_k(N)$ gilt offenbar $r_2(S) = |S| = k$.
Also liefert $\sum r_1(x) = \sum r_2(S)$:

$$\underbrace{n}_{\substack{\text{Anzahl Ele-}\\ \text{mente in } N}} \cdot \underbrace{\binom{n-1}{k-1}}_{r_1(x)} = \underbrace{\binom{n}{k}}_{\substack{\text{Anzahl Ele-}\\ \text{mente in } \mathcal{P}_k(N)}} \cdot \underbrace{k}_{r_2(S)}$$

Dies lässt sicht schreiben als

$$(*) \qquad \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$

Hiermit lässt sich sofort die gewünschte Formel herleiten:

**Satz:** Es gilt $\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot \ldots \cdot 1}$ für alle $n, k \in \mathbb{N}_0$ mit $k \leq n$.

**Beweis** mit einer etwas informell durchgeführten Induktion über $n$. Bekanntlich gilt $\binom{n-k}{0} = 1$. Jetzt wird $(*)$ der Reihe nach auf $\binom{n}{k}$, $\binom{n-1}{k-1}$, $\binom{n-2}{k-2}$, $\ldots$, $\binom{n-k+1}{1}$ angewandt:

$$\begin{aligned} \binom{n}{k} &= \frac{n}{k}\binom{n-1}{k-1} = \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \binom{n-2}{k-2} \\ &= \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \frac{n-2}{k-2} \cdot \binom{n-3}{k-3} = \ldots \\ &= \frac{n}{k} \cdot \frac{n-1}{k-1} \cdot \frac{n-2}{k-2} \cdot \ldots \cdot \frac{n-k+1}{1} \cdot \binom{n-k}{0} \\ &= \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot 1} \end{aligned}$$

wie behauptet. □

**Frage:** Warum gilt diese Formel auch für $k = 0$?

**Beispiel:** Eine Bäckerei bietet 8 verschiedene Brotsorten an. Wieviele Möglichkeiten hat ein Kunde, in dieser Bäckerei drei Brote zu kaufen, die alle von unterschiedlicher Sorte sind (rein von den Kombinationsmöglichkeiten her)? **Antwort:** Es gibt genau $\binom{8}{3} = \frac{8\cdot 7\cdot 6}{3\cdot 2\cdot 1} = 56$ Möglichkeiten.

Jetzt folgt die Anwendung der Binomialkoeffizienten, die ihnen den Namen gibt:

### 0.2.8 Die Binomische Formel

Für alle $n \in \mathbb{N}_0$ und alle $x, y \in \mathbb{C}$ (komplexe Zahlen) gilt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

**Beweis:** Die Multiplikation der $n$ Klammern von

$$(x+y)^n = (x+y)\cdot \ldots \cdot (x+y)$$

führt man üblicherweise so durch:

(i) Entscheide in jeder Klammer, ob $x$ oder $y$ genommen werden soll,
(ii) Tue dies auf alle möglichen Arten.

Ein Produkt $x^k y^{n-k}$ ergibt sich genau dann, wenn in (i) in genau $k$ Klammern $x$ gewählt wird und in den anderen Klammern $y$. Da es genau $\binom{n}{k}$ Möglichkeiten gibt, $k$ von $n$ Klammern auszuwählen, ergibt sich genau $\binom{n}{k}$ mal $x^k y^{n-k}$. □

**Beispiel:**

$$\begin{aligned}(x+y)^3 &= \binom{3}{0}x^0y^3 + \binom{3}{1}x^1y^2 + \binom{3}{2}x^2y^1 + \binom{3}{3}x^3y^0 \\ &= y^3 + 3xy^2 + 3x^2y + x^3\end{aligned}$$

Bekanntlich gilt $\binom{n}{k} = \frac{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)}{k\cdot(k-1)\cdot(k-2)\cdot\ldots\cdot 1}$. Man kann die Binomialkoeffizienten aber auch mit folgender Formel berechnen:

### 0.2.9 Binomialrekursion

Für alle $n, k \in \mathbb{N}$ gilt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Diese Gleichung kann mit obiger üblicher Formel für die Binomialkoeffizienten leicht nach gerechnet werden. (Ein ganz anderer, begrifflicher Beweis wird in den Übungen vorgestellt!)

Mit Hilfe der Binomialrekursion können die Binomialkoeffizienten **rekursiv** berechnet werden, das heißt Schritt für Schritt für $n = 1, 2, 3, \ldots$. Auf diese Art ergibt sich das **Pascal'sche Dreieck**:

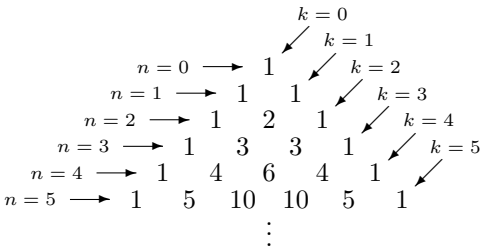



Abbildung 5: Das Pascal'sche Dreieck

Jede der folgenden Gleichungen kann man in diesem Schema veranschaulichen. Es gibt unzählige weitere Gleichungen für Binomialkoeffizienten, zum Teil von geradezu „magischer" Schönheit:

**Satz:** Die nachfolgenden Gleichungen verdeutlicht man sich am Besten an dem Pascal'schen Dreieck:

(a) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ für alle $n \in \mathbb{N}_0$

(b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ für alle $n \in \mathbb{N}_0$

(c) $\sum_{i=k-1}^{n-1} \binom{i}{k-1} = \binom{n}{k}$ für alle $n \in \mathbb{N}_0, k \in \mathbb{N}$

(d) $\sum_{i=0}^{k} \binom{n-1-k+i}{i} = \binom{n}{k}$ für alle $n \in \mathbb{N}, k \in \mathbb{N}_0, n > k$

(e) $\sum_{i=0}^{k} (-1)^i \binom{n+1}{i} = (-1)^k \binom{n}{k}$ für alle $n, k \in \mathbb{N}_0$

(f) $\sum_{i=0}^{k} \binom{n}{i} \binom{m}{k-i} = \binom{n+m}{k}$ für alle $n, m, k \in \mathbb{N}_0$
(**Vandermondesche Gleichung**)

**Beweis:**

(a) Das wurde bereits auf Seite 9 gezeigt. Alternative Argumentation: Verwende die Binomische Formel mit $x = y = 1$.

(b) Binomische Formel mit $x = 1, y = -1$!

(c) Hier wird (erstmals) eine **vollständige Induktion** verwendet. Näheres zu diesem Beweisprinzip folgt später in diesem Kapitel!
Induktion über $n$:
**Induktionsbasis:** Die Behauptung gilt für $n = 0$: Die Summe auf der linken Seite ist leer, ergibt also 0. Die rechte Seite ist $\binom{0}{k}$, wegen $k \geq 1$ ebenfalls 0.
**Induktionsvoraussetzung:** Es werde vorausgesetzt, dass die Behauptung für (irgend ein) $n \in \mathbb{N}_0$ gilt:

$$\text{(Vor)} \quad \sum_{i=k-1}^{n-1} \binom{i}{k-1} = \binom{n}{k}$$

**Indukionsschritt:** Jetzt wird die Induktionsvoraussetzung (Vor) verwendet, um die Behauptung für $n + 1$ zu zeigen. Das funktioniert folgendermaßen:

$$\begin{aligned}\sum_{i=k-1}^{n}\binom{i}{k-1} &= \left(\sum_{i=k-1}^{n-1}\binom{i}{k-1}\right)+\binom{n}{k-1}\\ &\overset{\text{(Vor)}}{=} \binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}\end{aligned}$$

(d) Dieser Beweis kann ebenfalls mit Induktion durchgeführt werden. Die restlichen Beweise sind dem interessierten Leser überlassen.
(e) ist sehr trickreich,
(f) bei geeigneter Idee recht einfach.

### 0.2.10 Permutationen

Bei den Elementen einer Menge kommt es nicht auf die Reihenfolge an (die Elemente sind „ungeordnet“) und Elemente können nicht doppelt vorkommen. Das kann man auch anderers betrachten. Zuerst das *geordnete Analogon*: Eine **$k$-Permutation** einer Menge $N$ ist eine Folge $(a_1,\ldots,a_k)\in N^k$ mit $a_i\neq a_j$ für $i\neq j$, also ein $k$-Tupel mit $k$ unterschidlichen Elementen.

**Satz:** Es gibt genau $n\cdot(n-1)\cdot\ldots\cdot(n-k+1)$ $k$-Permutationen in einer gegebenen $n$-Menge $N$.

**Beweis:** Für eine $k$-Permutation $(a_1,\ldots,a_k)\in N^k$ gibt es $n$ Möglichkeiten für $a_1$, $n-1$ Möglichkeiten für $a_2,\ldots,n-k+1$ Möglichkeiten für $a_k$. Insgesamt ergibt das $n\cdot(n-1)\cdot\ldots\cdot(n-k+1)$ Möglichkeiten. □

### 0.2.11 Multimengen

In $k$-Mengen und in $k$-Permutationen gibt es keine Wiederholungen von Elementen. Jetzt werden Wiederholungen erlaubt. Zuerst eine sehr informelle Definition: Eine **$k$-Multimenge** einer Menge $N$ ist eine „Ansammlung“ $\{\{a_1,\ldots,a_k\}\}$ von $k$ Elementen $a_1,\ldots,a_k\in N$, wobei Wiederholungen von Elementen vorkommen dürfen. Die Anzahl der $k$-Mulitmengen in einer gegebenen $n$-Menge $N$ wird mit $\left(\!\binom{n}{k}\!\right)$ bezeichnet.

**Beispiel:** Sei $N=\{a,b\}$. Es gibt folgende 3-Mulimengen in $N$:

$$\{\{a,a,a\}\},\{\{a,a,b\}\},\{\{a,b,b\}\},\{\{b,b,b\}\}$$

also (mit $n=2,k=3$): $\left(\!\binom{2}{3}\!\right)=4$.

**Satz:** Die Anzahl aller $k$-Multimengen, die in einer gegebenen $n$-Menge $N$ enthalten sind, beträgt

$$\left(\!\binom{n}{k}\!\right)=\binom{n+k-1}{k}$$

**Beweis** mit Hilfe eines Beispiels: Es werde die 5-Multimenge

$$K=\{\{1,1,4,6,6\}\}\quad\text{in}\quad N=\{1,2,3,4,5,6\}$$

betrachtet. Man kann $K$ folgendermaßen mit $k = 5$ Kreuzen und $n-1 = 5$ Strichen kodieren: $\times\times|||\times||\times\times$. Bedeutung: Erst zwei Einsen, dann null Zweien, dann null Dreien, dann eine Vier, dann null Fünfen, dann zwei Sechsen. In der Kreuz-Strich-Kodierung ist $K$ durch die Positionen der $k = 5$ Kreuze (Positionen 1, 2, 6, 9, 10) innerhalb der $k+n-1 = 10$ Zeichen langen Kreuz-Strich-Folge eindeutig bestimmt. Es gibt genau $\binom{10}{5} = \binom{k+n-1}{k}$ Auswahlmöglichkeiten für diese Positionen der Kreuze, also ebensoviele $k$-Multimengen in $\{1, \ldots, 6\}$. □

Es bleibt die Anzahl aller $k$-Tupel $(a_1, \ldots, a_k) \in N^k$ zu bestimmen. Doch das ist einfach (Multiplikationsregel):

**Satz:** Es gibt genau $n^k$ verschiedene $k$-Tupel in einer gegebenen $n$-Menge $N$.

Die Tabelle fasst obige Resultate zusammen:

| „Zusammenstellung“ von $k$ Objekten einer $n$-Menge | nicht geordnet | geordnet |
|---|---|---|
| ohne Wiederholungen | $k$-Mengen: $\binom{n}{k}$ | $k$-Permutationen: $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ |
| mit Wiederholungen | $k$-Multimengen: $\left(\binom{n}{k}\right) = \binom{n+k-1}{k}$ | $k$-Tupel: $n^k$ |

Die folgende Aufgabe gibt einfache Anwendungen:

**Aufgabe:** Eine Bäckerei bietet 8 Brotsorten an. Wieviele Möglichkeiten (von den Kombinationsmöglichkeiten der Brotsorten) gibt es dort für 5 Studenten

(a) insgesamt 5 Brote zu kaufen (alles verschiedene Sorten),
(b) insgesamt 5 Brote zu kaufen (Sortenwiederholungen möglich),
(c) 5 Brote zu kaufen, für jeden Studenten eins (ohne Wiederholungen),
(d) 5 Brote zu kaufen, für jeden Studenten eins (beliebige Sorten)?

Dieser Abschnitt wird mit dem *Zählen von Abbildungen* abgeschlossen:

### 0.2.12 Zählen von Abbildungen

**Satz:** Sei $N$ eine $n$-Menge und $K$ eine $k$-Menge.

(a) Es gibt genau $n^k$ Abbildungen $K \longrightarrow K$
(b) Es gibt genau $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ injektive Abbildungen $K \longrightarrow N$
(c) Es gibt genau $S(k,n)$ surjektive Abbildungen $K \longrightarrow N$ mit

$$S(k,n) = \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^k$$

**Beweis**

(a) Hierfür muss man alle $k$-Tupel in $N$ zählen (siehe vorherige Seite)
(b) Das bedeutet, alle $k$-Permutationen in $N$ zu zählen
(c) Der Beweis ist recht schwierig und wird hier weggelassen □

**Aufgabe:** Man „teste“ Aussage (c) für kleine Werte, zum Beispiel für $n = 3$, $k = 4$.

## 0.3 Beweismethoden

Mathematische **Aussagen** haben häufig die Form „wenn $p$, dann $q$“, in symbolischer Schreibweise: $p \to q$. Dabei sind dann $p$ und $q$ selbst Aussagen, die **wahr** ($= w$) oder **falsch** ($= f$) sein können. Die Aussage $p \to q$ hat folgende **Wahrheitstafel**:

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| $w$ | $w$ | $w$ |
| $w$ | $f$ | $f$ |
| $f$ | $w$ | $w$ |
| $f$ | $f$ | $w$ |

Also muss man sich beim Nachweis der Aussage $p \to q$ nur um den Fall kümmern, dass $p$ wahr ist, und muss dann nachweisen, dass auf $q$ wahr ist. Dabei wird $p$ die **Hypothese** genannt, (und $q$ zum Beispiel die **Behauptung**).

Ein **direkter Beweis** von $p \to q$ besteht darin, dass man eine Reihe von Aussagen $p \to p_1 \to p_2 \to \ldots \to p_k \to q$ nachweist (wobei man alle schon bekannten Tatsachen „verwenden“, das heißt voraussetzen darf). Andere Stategien bestehen darin, dass man zu $p \to q$ logisch äquivalente Aussagen nachweist. Logisch äquivalent zu $p \to q$ ist zum Beispiel $\neg q \to \neg p$. Wenn man dies verwendet, muss man aus der Aussagen $\neg q$ die Aussage $\neg p$ herleiten (**Kontraposition**). Zu $p \to q$ ist aber auch die Aussage $(p \wedge \neg q) \to f$ äquivalent. Man muss also aus der Gültigkeit von $p$ und von $\neg q$ die Aussage $f$ (falsch) herleiten (**Widerspruchsbeweis**).

Diese Methoden werden im Folgenden anhand von Beispielen vorgestellt. Außerdem wird das Beweisprinzip der **vollständigen Induktion** vorgestellt.

### 0.3.1 Direkter Beweis

Es soll schrittweise die Behauptung

wenn $a$ durch 6 teilbar ist, dann ist $a$ auch durch 3 teilbar

nachgewiesen werden (für $a \in \mathbb{Z}$). Die Hypothese ist

$p$ : $a$ ist durch 6 teilbar,

und die Behauptung ist

$q$ : $a$ ist durch 3 teilbar.

Für den Nachweis werden mehrere Zwischenschritte verwendet. Nach Definition bedeutet $p$:

$p_1$ : $a = 6k$ für ein $k \in \mathbb{Z}$.

Wegen $6 = 3 \cdot 2$ lässt sich dies schreiben als

$p_2$ : $a = (3 \cdot 2)k$ für ein $k \in \mathbb{Z}$.

Bekanntlich gilt $(3 \cdot 2)k = 3(2 \cdot k)$ (Assoziativität), also

$p_3$ : $a = 3(2 \cdot k)$ für ein $k \in \mathbb{Z}$.

Da mit $k$ auch $k' = 2 \cdot k$ eine ganze Zahl ist, folgt

$p_4$ : $a = 3k'$ für ein $k' \in \mathbb{Z}$.

Letzteres bedeutet, dass $a$ durch drei teilbar ist. Also ist die Behauptung $q$ jetzt bewiesen. Die **Beweisstruktur** in diesem Fall war

$$p \rightarrow p_1 \rightarrow p_2 \rightarrow p_3 \rightarrow p_4 \rightarrow q$$

Natürlich lassen sich Aussage und Beweis oft viel informeller und knapper formulieren, in diesen Fall zum Beispiel so:

**Behauptung:** Wenn eine ganze Zahl $a$ durch 6 teilbar ist, dann ist $a$ auch durch 3 teilbar.

**Beweis:** Ist $a$ durch 6 teilbar, dann gilt $a = 6k$ für ein $k \in \mathbb{Z}$. Umformung ergibt $a = (2 \cdot 3)k = 3(2k)$ und da mit $k \in \mathbb{Z}$ auch $2k \in \mathbb{Z}$ gilt, folgt schießlich, dass $a$ durch 3 teilbar ist. □

### 0.3.2 Beweis durch Kontraposition

Anstelle einer Implikation $p \rightarrow q$ wird die dazu logisch äquivalente Implikation $\neg q \rightarrow \neg p$ direkt bewiesen (die **Kontraposition** von $p \rightarrow q$). Ein Beispiel:

**Behauptung:** Sei $a \in \mathbb{Z}$. Wenn $a^2$ ungerade ist, dann ist $a$ ungerade.

In diesem Beispiel ist $p$ die Aussage „$a^2$ ungerade“ und $q$ die Aussage „$a$ gerade“. Jetzt wird aus der Aussage $\neg q$ („$a$ gerade“) direkt die Aussage $\neg p$ („$a^2$ gerade“) bewiesen:

**Beweis der Behauptung:** „$a$ gerade“ bedeutet $a = 2k$ für ein $k \in \mathbb{Z}$. Dann gilt $a^2 = (2k)^2 = 4k^2 = 2(2k^2)$, wobei $2k^2 \in \mathbb{Z}$ gilt. Doch das bedeutet „$a^2$ gerade“. □

### 0.3.3 Widerspruchsbeweis

Anstelle einer Implikation $p \rightarrow q$ wird die dazu logische äquivalente Implikation $(p \wedge \neg q) \rightarrow f$ bewiesen (also: $p$ *und* $\neg q$ können nicht gleichzeitig gelten). Hier ein berühmtes Beispiel:

**Behauptung:** Es gibt unendlich viele Primzahlen.

Hier handelt es sich um einen degenerierten Widerspruchsbeweis. Die Aussage $q$ sei „es gibt unendlich viele Primzahlen“ und die Aussage $q$ sei „wahr“, also $p = w$. Zu zeigen ist $(w \wedge \neg q) \rightarrow f$, also $\neg q \rightarrow f$. Dabei bedeutet $\neg q$ „es gibt nur endlich viele Primzahlen“.

**Beweis der Behauptung:** Werde angenommen, dass es nur endlich viele Primzahlen $z_1, \ldots, z_k$ gibt. Dann ist $z = z_1 \cdot \ldots \cdot z_k + 1$ eine ganze Zahl, die aber durch keine der Primzahlen $z_1, \ldots, z_k$ teilbar ist (denn teilt man $z$ durch $z_i$, bleibt immer Rest 1). Also muss auch $z$ eine Primzahl sein. $\lightning$ □

Noch zwei Beweisprinzipien, die oben nicht angekündigt waren:

### 0.3.4 Äquivalenzbeweis

Eine Aussage der Form $p \leftrightarrow q$ bedeutet: „$p$ gilt **genau dann, wenn** $q$ gilt“. Sie ist logisch äquivalent zu $(p \rightarrow q) \wedge (q \rightarrow q)$. Man muss also zwei Beweise führen, nämlich einen für $p \rightarrow q$ und einen für $q \rightarrow p$. Ein Beispiel:

**Behauptung:** Sei $a \in \mathbb{Z}$. Dann ist $a^2$ genau dann gerade, wenn $a$ gerade ist. Hier werden die Aussagen $p$ („$a^2$ gerade“) und $q$ („$a$ gerade“) betrachtet:

**Beweis der Behauptung:** Aus „$a$ gerade“ folgt „$a^2$ gerade“. Das erhält man mit Kontraposition aus der Behauptung aus Seite 15. Jetzt sei $a^2$ gerade. Zu zeigen ist, dass dann auch $a$ gerade ist. Auch das gelingt sehr einfach mit Kontraposition: Sei $a$ ungerade, also von der Form $a = 2k + 1, k \in \mathbb{Z}$. Dann ist $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, wobei $2k^2 + 2k \in \mathbb{Z}$ gilt. Doch das bedeutet „$a^2$ ungerade“. □

### 0.3.5 Fallunterscheidung

Jede Aussage $p$ ist logisch äquivalent zur Aussage $(q \rightarrow p) \wedge (\neg q \rightarrow p)$, wobei (im Prinzip) $q$ irgendeine Aussage sein kann. Also ist $p$ logisch äquivalent zu: „Wenn $q$, dann $p$, *und*: wenn nicht $q$, dann $p$“. Natürlich wählt man kein beliebiges $q$, sondern ein zur Aussage $p$ passendes $q$. Ein Beispiel:

**Behauptung:** Sei $a \in \mathbb{Z}$. Teilt man $a^2$ durch 4, so ergibt sich immer Rest 0 oder Rest 1.

Als Aussage $p$ nimmt man hier natürlich die Aussage der Behauptung. Als Aussage $q$ eignet sich „$a$ gerade“:

**Beweis der Behauptung:** Mit Fallunterscheidung:
Fall 1: Sei $a$ gerade, also von der Form $a = 2k, k \in \mathbb{Z}$. Dann gilt $a^2 = (2k)^2 = 4k^2$, wobei $k^2 \in \mathbb{Z}$ gilt. Das bedeutet, dass $a^2$ durch 4 den Rest 0 ergibt.
Fall 2: Sei $a$ ungerade, also von der Form $a = 2k + 1, k \in \mathbb{Z}$. Dann gilt $a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, wobei $k^2 + k \in \mathbb{Z}$ gilt. Doch das bedeutet, dass $a^2$ durch 4 den Rest 1 ergibt. □

### 0.3.6 Vollständige Induktion

Damit kann man (bisweilen) unendliche „Serien“ von Aussagen beweisen, zum Beispiel die Aussagen $p(n), n \in \mathbb{N}_0$. Diese kann man beweisen, indem man die beiden folgenden Aussagen zeigt:

**Induktionsbasis:** Es wird $p(0)$ gezeigt.

**Induktoinsschritt:** Es wird gezeigt, dass folgende Aussage gilt:

$$\forall n \in \mathbb{N}_0 \colon p(n) \rightarrow p(n+1)$$

Die letzte Zeile liest man „für alle $n$ aus $\mathbb{N}_0$ gilt: die Aussage $p(n)$ impliziert die Aussage $p(n+1)$“. Wenn Induktionsbasis und Induktionsschritt nachgewiesen sind, dann weiß man die Gültigkeit aller in folgender Implikationstabelle vorkommenden Aussagen:

$$p(0) \rightarrow p(1) \rightarrow p(2) \rightarrow p(3) \rightarrow p(4) \rightarrow \ldots$$

Also:
**Induktionssatz**: Gelten die beiden Aussagen $p(0)$ und

$$\forall n \in \mathbb{N}_0 \colon p(n) \rightarrow p(n+1)$$

dann gilt auch die Aussage $\forall n \in \mathbb{N}_0 \colon p(n)$. Das folgende Beispiel kann allerdings auch anders bewiesen werden:

**Behauptung:** Für alle $n \in \mathbb{N}_0$ gilt:

$$p(n): \quad \sum_{k=0}^{n} k = \frac{n \cdot (n+1)}{2}$$

**Beweis** mit Induktion über $n$.
**Induktionsbasis:** Sei $n = 0$. Dann ergibt die linke Seite $p(0) : \sum_{k=0}^{0} i = 0$. Die rechte Seite von $p(0)$ ist $\frac{0 \cdot (0+1)}{2} = 0$. Damit ist $p(0)$ gezeigt.
**Induktionsschritt:** Es wird $p(n)$ vorausgesetzt (die sogenannte **Induktionsvoraussetzung**) und $p(n+1)$ muss gezeigt werden. Das funktioniert so:

$$\begin{aligned} \sum_{k=0}^{n+1} k &= \left( \sum_{k=0}^{n} k \right) + n + 1 = \frac{n \cdot (n+1)}{2} + n + 1 \\ &= (n+1) \left( \frac{n}{2} + 1 \right) = \frac{(n+1) \cdot (n+2)}{2} \end{aligned}$$

Die linke und die rechte Seite dieser Gleichungskette bilden insgesamt die nachzuweisende Gleichung $p(n+1)$. □

Der obige Induktionssatz läßt sich verallgemeinern:
**Verallgemeinerter Induktionssatz:** Gelten die beiden Aussagen $p(0)$ und $\forall n \in \mathbb{N}_0 \colon (p(0) \wedge p(1) \wedge ... \wedge p(n)) \rightarrow p(n+1)$, dann gilt auch die Aussage $\forall n \in \mathbb{N}_0 : p(n)$.

Ein sehr simples Beispiel hierfür:

**Behauptung:** Jede natürliche Zahl $n \geq 2$ ist ein Produkt von Primzahlen.

**Beweis** mit Induktion über $n$.
**Induktionsbasis** (für $n = 2$). Die Zahl 2 ist das Produkt von *einer* Primzahl, nämlich der Zahl 2 selbst.

**Induktionsschritt** mit Fallunterscheidung: Gelte die Behauptung für alle natürlichen Zahlen zwischen 2 und $n$ (jeweils inklusive). Jetzt wird die Zahl $n+1$ behandelt:

Fall 1: Sei $n+1$ eine Primzahl. Dann ist n+1 das Produkt einer Primzahl (nämlich sich selbst).

Fall 2: Sei $n+1$ keine Primzahl. Dann gilt $n+1 = n_1 \cdot n_2$ mit $2 \leq n_1, n_2 < n+1$. Nach Induktionsvoraussetzung gibt es Primzahlen $s_1, ..., s_k$, $t_1, ..., t_\ell$ mit $n_1 = s_1 \cdot \ldots \cdot s_k$ und $n_2 = t_1 \cdot \ldots \cdot t_\ell$, also mit $n+1 = s_1 \cdot \ldots \cdot s_k \cdot t_1 \cdot \ldots \cdot t_\ell$, womit die Behauptung für $n+1$ gezeigt ist. □

Es gibt **induktive Definitionen**, auch **Rekursionen** genannt. Oft lassen sich Eigenschaften der so **rekursiv** definierten Objekte per vollständiger Induktion beweisen.

Ein berühmtes Beispiel: Die **Fibonacci-Zahlen** $f_0, f_1, f_2, ...$ werden rekursiv definiert durch

$$f_0 = 0, \quad f_1 = 1, \quad f_{n+2} = f_{n+1} + f_n \quad \text{für alle } n \geq 0$$

Die ersten Zahlen dieser Folge sind:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $f_n$ | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 |

Tatsächlich gilt folgendes Ergebnis (sehr erstaunlich, da eine Folge ganzer Zahlen mittels Wurzeln und Brüchen beschrieben wird):

**Behauptung:** Für alle Fibonacci-Zahlen $f_n$ gilt:

$$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

Der Beweis ist eine Übungsaufgabe (aber ohne vollständige Induktion!)

# 1 Diskrete Mathematik

Die **Diskrete Mathematik** beschäftigt sich mit endlichen Strukturen, die unter kombinatorischen Gesichtspunkten betrachtet werden können. Vieles in der Diskreten Mathematik ist für moderne Anwendungen, speziell in der Informatik, von größter Bedeutung. Das gilt besonders für **Graphen** (und speziell **Bäume**). Es gibt viele interessante **Algorithmen** für Graphenprobleme, anhand von Graphen kann man die Begriffe **Symmetrie** und **Gruppe** einführen, und (Permutations-)Gruppen sind ein wichtiges Hilfsmittel für eine berühmte kombinatorische Abzählmethode, nämlich die **Pólya-Methode**. Damit endet dieses Kapitel!

## 1.1 Graphen: Beispiele und Grundlagen

Zuerst ein sehr anschauliches Problem, das gleich auf (mindestens) zwei Arten graphentheoretisch betrachtet werden kann:

**Beispiel:** Ein Tischtennisturnier mit fünf Teilnehmern und einem Spieltisch. Regeln:

1. Jeder Teilnehmer spielt genau einmal gegen jeden anderen Teilnehmer
2. Kein Teilnehmer spielt in zwei aufeinanderfolgenden Spielen

**Aufgabe:** Finde einen Spielplan!

**Erster Versuch:** Die fünf Punkte entsprechen den Teilnehmern, die Linien den Spielen. Das Diagramm gibt keinen Spielplan. Man kann so vorgehen: Das erste Spiel sei oBdA ab. Als zweites Spiel kommen die zu ab „disjunkten“ Linien $cd$, $cd$, $de$ in Frage. Und so weiter!

**Zweiter Versuch:** Mit einem anderen Graphen, der aber mehr Informationen enthält: die zehn Punkte entsprechen den zehn Spielen, und eine Linie bedeutet, dass die zugehörigen beiden Spiele (=Punkte) hintereinander stattfinden dürfen. Die dicken Linien verbinden dann Spiele zu einem Spielplan!

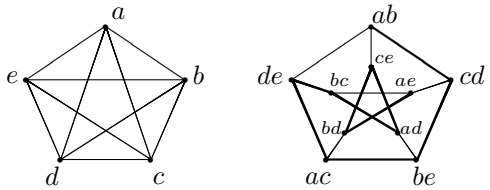



Abbildung 6: Turniergraph

### 1.1.1 Graphen

**Definition:** Ein **Graph** ist ein Paar $G = (V, E)$, bestehend aus einer beliebigen Menge $V$ und einer Menge $E \subseteq \mathcal{P}_2(V)$, das heißt einer Menge zweielementiger Teilmengen von $V$. Die Elemente von $V$ heißen **Ecken** (**Punkte**, **Knoten**) von $G$, die Elemente von $E$ **Kanten** (**Linien**, **Bögen**) von $G$.

Es ist klar, dass man mit Hilfe von Graphen gewisse einfache Zusammenhänge („Objekte, von denen je zwei entweder miteinander in Beziehung stehen oder nicht“) auf einfache Art darstellen und oft auch mit Diagrammen veranschaulichen kann:

**Beispiel:** Sei

$$V = \{1, 2, 3, 4, 5\}$$
$$E = \{\{1, 2\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{4, 5\}\}$$

Dann ist $G = (V, E)$ ein Graph mit $|V| = 5$ Ecken und $|E| = 8$ Kanten. Jedes der folgenden drei Diagramme zeigt diesen Graphen:

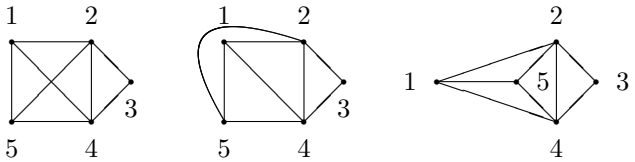



Abbildung 7: Beispiele für Graphen

In der vorliegenden Definition eines Graphen ist folgendes **nicht** vorgesehen:

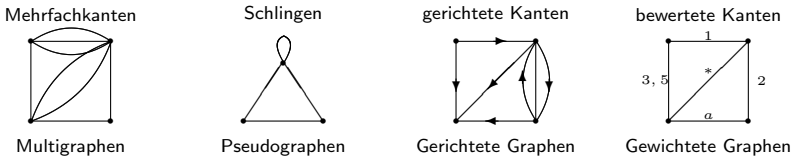



Abbildung 8: Weitere Graphentypen

Sind die Graphen $G_1$ und $G_2$ identisch? Eindeutig nicht. Aber sie sehen identisch aus:

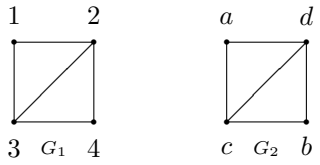



Abbildung 9: Graphenisomorphie I

**Aber:** $G_1$ und $G_2$ sind identisch bis auf die Tatsache, dass die Ecken unterschiedliche Namen haben.

### 1.1.2 Isomorphismen

**Definition:** Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ heißen **isomorph**, falls es eine bijektive Abbildung $\varphi: V_1 \longrightarrow V_2$ gibt mit:

$$\forall x, y \in V_1 : \{x, y\} \in E_1 \quad \Leftrightarrow \quad \{\varphi(x), \varphi(y)\} \in E_2$$

Dann heißt $\varphi$ ein **Isomorphismus** von $G_1$ auf $G_2$, und man schreibt auch $G_1 \cong G_2$ oder $G_1 \overset{\varphi}{\cong} G_2$.

Ein Isomorphismus bildet also benachbarte Ecken auf benachbarte Ecken und nicht benachbarte Ecken auf nicht benachbarte Ecken ab. Ein Isomorphismus ist nichts als eine Umbenennung der Ecken. In obigem Beispiel wird ein Isomorphismus $\varphi$ gegeben durch

| $x$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $\varphi(x)$ | $a$ | $b$ | $c$ | $d$ |

Wie erkennt man in weniger einfachen Fällen, ob zwei Graphen $G_1$ und $G_2$ isomorph bzw. nicht isomorph sind? Es gibt zwei Möglichkeiten:

**Möglichkeit 1:** Probiere alle bijektiven Abbildungen $\varphi : V_1 \to V_2$.
Im Fall $|V_1| = |V_2| = n$ gibt es $n!$ („$n$ Fakultät“) solche Abbildungen, also für große $n$ (z.B. $n = 50$) eine für keinen Computer der Welt durchführbare Aufgabe!

**Möglichkeit 2:** Finde eine (graphentheoretisch formulierbare) Eigenschaft, in der sich $G_1$ und $G_2$ unterscheiden. Wird auch bei nicht isomorphen Graphen nicht immer gelingen!

**Übung:** Finde Eigenschaften, die zeigen, dass die folgenden Graphen paarweise nicht isomorph sind:

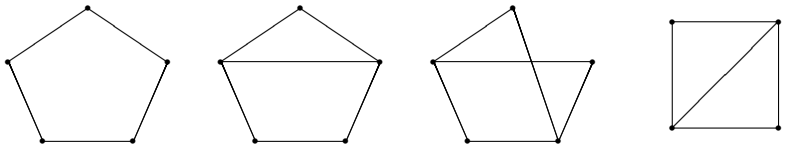


Abbildung 10: Graphenisomorphie II

Für jede Zahl $n \in \mathbb{N}$ gibt es unendlich viele Graphen mit $n$ Ecken. Aber wie viele „wirklich verschiedene“, das heißt paarweise nicht isomorphe Graphen mit $n$ Ecken gibt es? Diese Frage ist durchaus kompliziert; es ist keine einheitliche Formel bekannt. Hier sind die ersten Zahlen:

| $n$ (Anzahl der Ecken) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Anzahl paarweise nicht isomorpher Graphen mit $n$ Ecken | 1 | 2 | 4 | 11 | 34 | 156 | 1044 | 12344 |

Dieser Abschnitt wird mit einigen wichtigen Begriffen abgerundet:

### 1.1.3 Knotengrad

**Definition:** Sei $G = (V, E)$ ein Graph. Für jedes $v \in V$ sei $deg(v) := |\{e \in E | v \in e\}|$, genannt der **Grad** (engl.: degree) von $v$.

**Beispiel:** Der Graph $G_1$ (Seite 20, Abbildung: Graphenisomorphie) erfüllt $deg(1) = deg(4) = 2$, $deg(2) = deg(3) = 3$.

Das erste der beiden folgenden Resultate ist offensichtlich, das zweite ergibt sich recht einfach mit doppelten Abzählen:

**Bemerkung:** Ist $\varphi$ ein Isomorphismus eines Graphen $G_1$ auf einen Graphen $G_2$, dann gilt $deg(v) = deg(\varphi(v))$ für jede Ecke $v$ von $G_1$.

**Handschlag-Lemma:** Für jeden endlichen Graphen $G = (V, E)$ gilt:

$$\sum_{v \in V} deg(v) = 2|E|$$

Eine unmittelbare Folgerung hieraus:

**Korollar:** Jeder endliche Graph hat eine gerade Anzahl von Ecken ungeraden Grads.

### 1.1.4 Kantenzüge

**Definition:** Sei $G = (V, E)$ ein Graph. Eine Folge $(v_0, v_1, \ldots, v_n)$ von Ecken von $G$ heißt ein **Kantenzug**, falls $e_i := (v_i, v_{i+1}) \in E$ gilt für $i = 0, 1, \ldots, n-1$ das heißt falls je zwei aufeinanderfolgende Ecken duch eine Kante verbunden sind. Im Fall $v_0 = v_n$ handelt es sich um einen **geschlossenen**, sonst um einen **offenen Kantenzug**. Wenn alle Kanten eines Kantenzugs verschieden sind, spricht man (im offenen Fall) von einem **Weg**, im geschlossenen Fall von einem **Kreis**. Kommt außerdem auch jede Ecke nur einmal vor, dann heißt der Weg ein **einfacher Weg** bzw. der Kreis ein **einfacher Kreis** (wobei im Fall des Kreises natürlich $v_0 = v_n$ gilt). Die Länge eines Kantenzugs ist die Anzahl seiner Kanten. Der Kantenzug $(v_0, v_1, \ldots, v_n)$ hat also die Länge $n$.

**Randbemerkung:** In der Graphentheorie-Literatur herrscht ein großes Bezeichnungschaos, besonders was die eben gegebenen Bezeichnungen betrifft. Beispielsweise werden Wege oft automatisch als „einfach“ definiert. Man sollte in jedem Buch oder Artikel immer zuerst die grundlegenden Bezeichnungen sorgfältig checken!

**Beispiele:** In folgendem Graphen $G$ ist

| | |
|---|---|
| $(a, b, d, f)$ | kein Kantenzug, |
| $(a, c, d, b, c, e)$ | ein Weg der Länge 5, aber kein einfacher Weg, |
| $(a, c, d, b, c, a)$ | ein geschlossener Kantenzug, aber kein Kreis, |
| $(a, c, a)$ | desgleichen, |
| $(a, c, d, b, a)$ | ein einfacher Kreis. |

Und: es gibt genau 6 verschiedene einfache Wege von $a$ nach $d$.

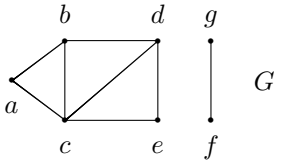



Abbildung 11: Zusammenhängende Graphen

### 1.1.5 Zusammenhängende Graphen

**Definition:** Ein Graph $G = (V, E)$ heißt **zusammenhängend**, falls je zwei Ecken $x, y \in V$ durch einen Kantenzug verbunden sind. Die Relation $R \subseteq V^2$ mit

$$xRy \quad :\Longleftrightarrow \quad \text{es gibt einen Kantenzug von } x \text{ nach } y$$

ist eine Äquivalenzrelation auf $V$. Für jede Äquivalenzklasse $W$ dieser Äquivalenzrelation ist der Untergraph $G_W := (W, E, \mathcal{P}_2(W))$ seine Zusammenhangskomponente von $G$.

**Definition/Anmerkung:** Sei $G = (V, E)$ ein Graph. Jeder Graph $G' = (V', E')$ mit $V' \subseteq V$ und $E' \subseteq E$ ist ein Teilgraph von $G$. Im Fall, dass $E'$ alle möglichen Kanten enthält, das heißt im Fall $E' = E \cap \mathcal{P}_2(V)$, wird $G'$ ein **Untergraph** von $G$ genannt (der von $V'$ induzierte Untergraph).
Die Zusammenhangskomponenten eines Graphen sind also die inzudierten Untergraphen auf den Äquivalenzklassen von $R$. Der obige Graph hat zwei Zusammenhangskomponenten, mit Eckenmengen $W_1 = \{a, b, c, d, e\}$ und $W_2 = \{f, g\}$.

## 1.2 Bäume

Die Graphen dieses Abschnitts spielen gerade in vielen informatischen Anwendungen eine große Rolle.

**Definition:** Ein Baum ist ein zusammenhängender Graph, der keine Kreise enthält (außer den „trivialen“ 1-elementigen Kreisen).
Hier sind alle Bäume mit 6 Ecken:

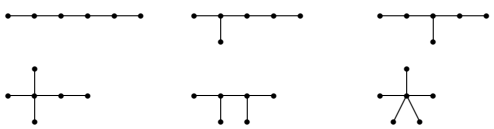


Abbildung 12: Bäume mit 6 Ecken

Hier eine vielbenutzte Charakterisierung von Bäumen:

**Satz:** Für einen Graphen $G$ mit $n$ Ecken sind folgende Aussagen äquivalent:

(i) $G$ ist ein Baum,
(ii) $G$ ist zusammenhängend und hat genau $n - 1$ Kanten.

**Beweis:** **(i) ⇒ (ii):** Sei $e_1 \in E$, $e_1 = \{x_1, y_1\}$. Entfernt man $e_1$ aus $G$, so ergibt sich der Graph $G \setminus e_1 := (V, E - \{e_1\})$. Dieser Graph hat eine Zusammenhangskomponente mehr als $G$, denn $x_1$ und $y_1$ sind jetzt in verschiedenen Komponenten. Entfernt man jetzt eine weitere Kante $e_2$, so ergibt sich ein Graph $G \setminus e_1, e_2$ mit jetzt drei Zusammenhangskomponenten. Setzt man dies schrittweise fort, so erhält man schließlich nach Entfernung von $n-1$ Kanten $e_1, e_2, \ldots, e_{n-1}$ einen Graphen $G \setminus e_1, e_2, \ldots, e_{n-1}$ mit $1 + (n-1) = n$ Komponenten. Jetzt bildet also jede der $n$ Ecken eine Zusammenhangskomponente für sich selbst, das heißt $G \setminus e_1, e_2, \ldots, e_{n-1}$ hat keine Kanten mehr. Es folgt $E = \{e_1, e_1, \ldots, e_{n-1}\}$.

**(ii) ⇒ (i):** Es ist zu zeigen, dass $G$ keinen nichttrivialen Kreis enthält. Werde im Gegenteil angenommen, es gebe einen solchen Kreis: $(v_0, v_1, \ldots, v_0)$. Es wird ein Widerspruch hergeleitet: Sei $e := \{v_0, v_1\}$. Dann ist offenbar $G \setminus e$ immer noch zusammenhängend, denn $(v_1, \ldots, v_0)$ ist ein Kantenzug von $v_1$ nach $v_0$. Sei $E \setminus \{e\} = \{e_1, \ldots, e_{n-2}\}$. Dann hat $G \setminus e, e_1$ höchstens zwei Zusammenhangskomponenten, $G \setminus e, e_1, e_2$ höchstens drei Zusammenhangskomponenten, $\ldots, G \setminus e, e_1, \ldots, e_{n-2}$ höchstens $n-1$ Zusammenhangskomponenten. ↯ (Denn ein Graph ohne Kanten mit $n$ Ecken hat $n$ Zusammenhangskomponenten!) □

### 1.2.1 Wälder

**Anmerkung:** Ein Graph ohne nichttriviale Kreise ist ein **Wald**. Also sind Bäume gerade die zusammenhängenden Wälder! Das Diagramm zeigt einen Wald mit fünf Zusammenhangskomponenten (= Teilbäumen).

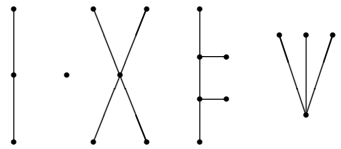
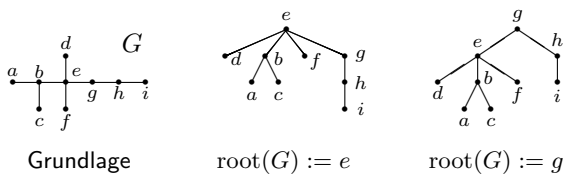


Abbildung 13: Wald

### 1.2.2 Wurzelbäume

In der Informatik werden oft Bäume betrachtet, die noch weitere Eigenschaften oder Zusatzinformationen tragen. Zuerst ein Beispiel hierfür, welches diesen Baum als Grundlage hat:




| Ecke | Kinder |
|---|---|
| $a$ | – |
| $b$ | $a, c$ |
| $c$ | – |
| $d$ | – |
| $e$ | $d, b, f, g$ |
| $f$ | – |
| $g$ | $h$ |
| $h$ | $i$ |
| $i$ | – |

Abbildung 14: Wurzelbäume

Es wird eine Ecke als **Wurzel** von $G$ ausgewählt, genannt root$(G)$. Wählt man in obigem Baum $G$ root$(G) := e$, dann läßt sich der zugehörige Baum wie in der mittleren Abbildung zeichnen, mit root$(G) := g$ wie in der rechten Abbildung.

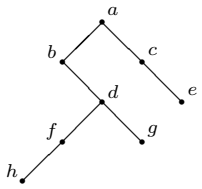
Man zeichnet Wurzelbäume üblicherweise von der Wurzel an abwärts (im Unterschied zu Bäumen in der Natur)!

In einem Wurzelbaum hat jede Ecke entweder **Kinder**, oder sie ist ein **Blatt**. Die Tabelle in der obigen Abbildung gibt eine Darstellung für den Graphen mit $\text{root}(G) = g$ an. Die Blätter sind $a, c, d, f, i$.

### 1.2.3 Binäre Bäume

Dies sind Wurzelbäume mit höchstens zwei Kindern pro Ecke, einem **linken Kind** und einem **rechten Kind**. Die Abbildung auf Seite 25 zeigt ein Beipsiel als Diagramm und als Tabelle.

Binäre Wurzelbäume werden auch **binäre Suchbäume** genannt. Sie können zur Suche in linearen Ordnungen verwandt werden.




| Ecke $x$ | linkes Kind $l(x)$ | rechtes Kind $r(x)$ |
|---|---|---|
| $a$ | $b$ | $c$ |
| $b$ | – | $d$ |
| $c$ | – | $e$ |
| $d$ | $f$ | $g$ |
| $e$ | – | – |
| $f$ | $h$ | – |
| $g$ | – | – |
| $h$ | – | – |

Abbildung 15: Binärbäume

**Beispiel:** Sei folgendes (sehr kleines) Telefonbuch gegeben:

| Namen | Anna | Bernd | Chris | Doris | Emil | Ferdi | Gerd | Hans |
|---|---|---|---|---|---|---|---|---|
| Tel.-Nr. | 3715 | 8102 | 1519 | 2424 | 2426 | 9132 | 2001 | 4567 |

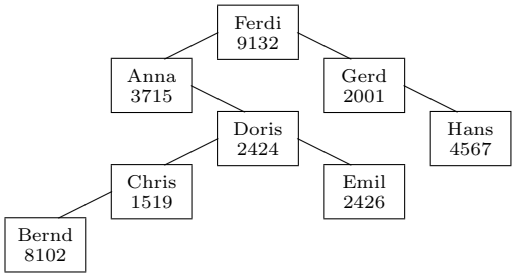



Abbildung 16: Telefonbuch I

Obiges Diagramm erfüllt folgende Regel: Nach links von einer Ecke mit Namen $X$ kommen nur Namen $Y$ mit $Y < X$ („vorher im Alphabet“), nach rechts kommen nur Namen $Y > X$.

Suche nach Chris Nummer: Starte bei Wurzel Ferdi. Chris < Ferdi → nach links zu Anna, Chris > Anna → nach rechts zu Doris, Chris < Doris → nach links zu Chris (Nummer 1519, fertig!)

Dieser binäre Suchbaum hat **Tiefe** 4 (Tiefe = maximale Weglänge von der Wurzel nach unten). Klar ist: geringere Tiefen gibt geringere durchschnittliche Suchzeit. Darum ist der folgende binäre Suchbaum für das selbe Telefonbuch besser (er ist sogar optimal):

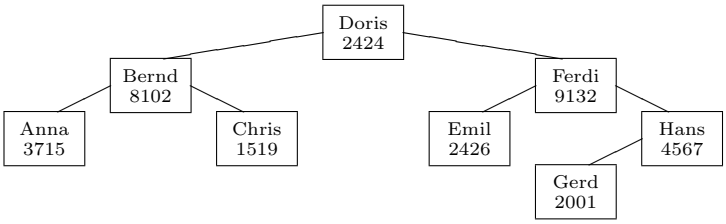



Abbildung 17: Telefonbuch II

Dieses Beispiel hat Tiefe 3. Allgemein: In die „Schichten“ $0, 1, 2, \ldots, k$ eines Suchbaumes passen offenbar maximal $1 + 2 + 4 + \ldots + 2^k = 2^{k+1} - 1$ Ecken. Deshalb gilt $n \leq 2^{k+1} - 1$, wobei $n$ die Anzahl der Ecken ist. Es folgt $n < 2^{k+1}$, also:

$$\log_2(n) - 1 < \text{Tiefe}$$

## 1.3 Abstände in (ungerichteten, unbewerteten) Graphen

In diesem Abschnit wir der „graphentheoretische Abstand“ betrachtet, dabei wird jeder Kante die „Länge“ 1 zugeordnet.

### 1.3.1 Länge von Kantenzügen

**Definition:** Die **Länge** eines **Kantenzugs** ist definiert als die Anzahl der Knoten des Kantenzugs (kam schon auf Seite 22 vor). Der Abstand $\mathrm{d}(a, b)$ zweier Ecken $a$ und $b$ eines Graphen ist das Minimum der Längen aller Kantenzüge von $a$ nach $b$. Dalls es keinen solchen Kantenzug gibt, wird $\mathrm{d}(a, b) = \infty$ gesetzt.

**Beispiel:** In folgendem Graphen hat der Kantenzug $(a, b, d, f, g, c)$ die Länge 5. Ein Kantenzug geringster möglicher Länge von $a$ nach $c$ ist $(a, b, c)$, er hat Länge 2. Daher gilt $\mathrm{d}(a, c) = 2$.

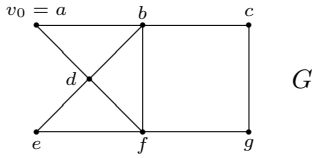



Abbildung 18: Kantenzüge

### 1.3.2 Algorithmus von Moore

Es wird ein Algorithmus vorgestellt (Algorithmus von Moore, 1959), in dem Graphen durch **Adjazenzlisten** gegeben sind, das heißt für Listen, die zu jeder

Ecke die Nachbarecken aufzählen. In obigem Beispiel sind das (bei alphabetischer Anordnung) folgende Listen:

| $A_a$ | $A_b$ | $A_c$ | $A_d$ | $A_e$ | $A_f$ | $A_g$ |
|---|---|---|---|---|---|---|
| $b, d$ | $a, c, d, f$ | $b, g$ | $a, b, e, f$ | $d, f$ | $b, d, e, g$ | $c, f$ |

Sei $G$ ein durch seine Adjazenzlisten $A_v$ gegebener Graph und sei $v_0$ eine Ecke dieses Graphen. Es werden Zahlen $d(v)$ sowie Mengen $V(0), V(1), V(2), \ldots$ berechnet. Der Algorithmus ist in „Pseudo-Pascal“ geschrieben.

```
(1)  d(v_0) ← 0, V(0) ← {v_0}, k ← 1,
(2)  while V(k−1) ≠ ∅ do
(3)    V(k) ← ∅,
(4)    for v ∈ ⋃{A_u | u ∈ V(k−1)} do
(5)      if d(v) ist undefiniert then
(6)        d(v) ← k, V(k) ← V(k) ∪ {v},
(7)      end,
(8)    end,
(9)    k ← k + 1
(10) end.
```

Was dieser Algorithmus tut, ist möglicherweise auf den ersten Blick nicht gut sichtbar. Aber die Idee ist einfach: Ausgehend von $V(0) = \{v_0\}$ werden sukzessive die Mengen $V(1), V(2)$ berechnet. Dabei besteht $V(k)$ aus den Ecken, die mit Ecken aus $V(k-1)$ benachbart sind, aber nicht in $V(0) \cup V(1) \cup \ldots \cup V(k-1)$ liegen. Mit Induktion sieht man, dass $V(k)$ genau aus den Ecken besteht, die Abstand $k$ von $v_0$ haben. Die Laufzeit des Algorithmus ist, in der üblichen pauschalen Weise schnell bestimmt: Zeile (1) erfordert drei Rechenschritte, und jede andere Zeile nicht mehr als insgesamt (das heißt bei sämtlichen Durchläufen) $2m$ Rechenschritte, wobei $m$ die Anzahl der Kanten von $G$ bezeichnet. Zu Zeile (4) beachte man, dass die Vereinigungsmenge nicht wirklich berechnet werden muss, es genügt die Elemente der jeweiligen Listen $A_u$ der Reihe nach aufrufen. Die Komplexität (= Laufzeit) ist also proportional zu $m$, in Symbolen: von der Größenordnung $O(m)$ (sprich: „groß -$O$ von $m$“). Damit ist insgesamt gezeigt:

**Satz:** Nach der Durchführung des Algorithmus von Moore gilt für alle Ecken $v$ von $G$:

$$\mathrm{d}(v, v_0) = \begin{cases} \mathrm{d}(v) & \text{falls d}(v) \text{ definiert ist} \\ \infty & \text{sonst} \end{cases}$$

Der Algorithmus hat die Komplexität $O(m)$.

Da der Algorithmus, ausgehen von Ecke $v_0$, „in die Breite“ gehend sucht, spricht man auch von **breadth first search** (BFS).

Für obiges Beispiel ergibt sich:

$$V(0) = \{a\} \qquad V(1) = \{b, d\} \qquad V(2) = \{c, e, f\}$$
$$V(3) = \{9\} \qquad V(4) = \emptyset$$

und dementsprechend

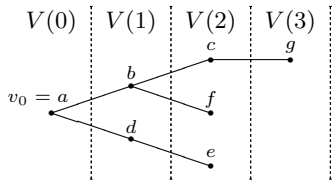



Abbildung 19: Breitensuche

| $v$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ |
|---|---|---|---|---|---|---|---|
| d($v$) | 0 | 1 | 2 | 1 | 2 | 2 | 3 |

Der Algorithmus liefert auch einen Test, ob der Graph $G$ zusammenhängend ist:

**Korollar:** Ein endlicher Graph $G$ ist genau dann zusammenhängend, wenn nach Durchführung des Algorithmus von Moore für jede Ecke $v$ die Zahl $d(v)$ definiert ist.

Für die Laufzeit von Algorithmen ist es sehr wichtig, welche Datenstrukturen verwendet werden. Eine Möglichkeit für Graphen ist die Darstellung mit Adjazenzlisten wie auf Seite 27. Es haldelt sich dabei um $n$ Listen, wobei alle Listen zusammen $2m$ Einträge haben (zwei Einträge pro Kante). Dabei ist wie üblich $n$ die Anzahl der Ecken und $m$ die Anzahl der Kanten eines Graphen.

### 1.3.3 Inzidenzmatrizen

Graphen können auf viele weitere Arten dargestellt werden. Eine davon ist die Darstellung mit **Inzidenzmatrizen**. Der Graph $G$ auf Seite 26 hat zum Beispiel die folgende Inzidenzmatrix $I(G)$:

$$I(G) = \left(\begin{array}{ccccccc} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{|c} a \\ b \\ c \\ d \\ e \\ f \\ g \end{array}$$

$$\begin{array}{ccccccc} a & b & c & d & e & f & g \end{array}$$

Abbildung 20: Inzidenzmatrix von $G$

Die Inzidenzmatirx $I(G)$ hat an der Stelle $(i, j)$ eine 1, falls $\{1, j\}$ eine Kante von $G$ ist, und eine 0 sonst. Jedenfalls hat – ganz allgemein – $I(G)$ $n^2$ Einträge. Würde man im Algorithmus von Moore eine Inzidenzmatrix statt der Adjazenzlisten verwenden, dann hätte der Algorithmus Komplexität $O(n^2)$ statt $O(m)$, was für viele Graphen deutlich mehr ist. Allgemein gilt:

> Für die Komplexität von Algorithmen kommt es darauf an, welche Datenstrukturen verwendet werden.

Der Algorithmus von Moore läßt sich übrigens auch für Graphen verwenden, deren Kanten eine Richtung haben.

### 1.3.4 Gerichtete Graphen

**Definition:** Ein **gerichteter Graph** oder auch **Digraph** (engl.: directed graph) ist ein Paar $G = (V, E)$, wobei $V$ eine Menge ist, und $E$ eine Menge von geordneten Paaren $(v, w)$ mit $v, w \in V$ und $v \neq w$. Man nennt wieder die Elemente von $V$ **Ecken** und die Elemente von $E$ **Kanten** von $G$. Anstelle von $(v, w)$ wird oft kurz $vw$ geschrieben, wobei es im Unterschied zu ungerichteten Graphen auf die Reihenfolge von $v$ und $w$ ankommt.

Viele der Begriffe für ungerichtete Graphen übertragen sich problemlos auf gerichtete Graphen. Beispielsweise heißt eine Folge $(v_0, v_1, \ldots, v_k)$ ein **Kantenzug** des gerichteten Graphen $G$, falls $(v_i, v_{i+1})$ eine Kante ist, für alle $i$. Die Länge dieses Kantenzuges ist $k$. Entsprechend werden **Wege**, **Kreise** und **Abstände** in gerichteten Graphen definiert. (Dabei wird zur Verdeutlichung oft der Zusatz „gerichtet“ verwendet, zum Beispiel von „gerichteten Wegen“ gesprochen.)

In folgendem Digraphen $G$ ist zum Beispiel $d(a, c) = 4$ der Abstand zwischen $a$ und $c$. Ein kürzester Weg von $a$ nach $c$ ist $(a, d, f, g, c)$.

**Aufgabe:** Wende den Algorithmus von Moore auf diesen Digraphen an.

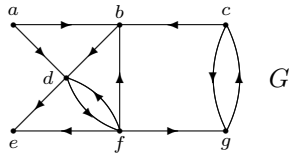



Abbildung 21: Wege in ungerichteten Graphen

In folgendem Digraphen $G$ ist zum Beispiel $d(a, c) = 4$ der Abstand zwischen $a$ und $c$. Ein kürzester Weg von $a$ nach $c$ ist $(a, d, f, g, c)$:

## 1.4 Abstände in Netzwerken

Jetzt wird jeder Kante eines Graphen eine **Länge** zugeordnet. Typische Beispiele sind Straßennetze mit Entfernungsangaben.

### 1.4.1 Netzwerke

**Definition:** Ein **Netzwerk** ist ein Paar $(G, w)$, bestehend aus einem (gerichteten oder ungerichteten) Graphen $G = (V, E)$ sowie einer Bewertung der Kanten von $G$ mit reellen Zahlen, das heißt einer Funktion $w : E \to \mathbb{R}$. Für jede Kante $e \in E$ heißt $w(e)$ die **Länge** (oder das **Gewicht**) von $e$. Für einen Kantenzug $K = (v_0, v_1, \ldots, v_k)$ ist

$$w(k) := w(v_0v_1) + w(v_1v_2) + \ldots + w(v_{k-1}v_k)$$

die **Länge** von $K$. (Hierbei steht z. B. $v_0v_1$ als Abkürzung für $\{v_0, v_1\}$ bzw. $(v_0, v_1)$.)

Je nach Anwendung kann es sich bei den Längen bzw. Gewichten auch um Zeitdauern, Kosten, Gewinne und Verluste und vieles andere handeln. Deshalb ist es gerechtfertigt, auch negative Lösungen zuzulassen. Bei der Definition von Abständen würden negative Längen aber Probleme machen:

### 1.4.2 Der Abstandsbegriff

**Definition:** Sei $(G, w)$ ein *Netzwerk mit nichtnegativen Längen*, das heißt mit $w(e) \geq 0$ für alle Kanten $e$. Der **Abstand** $d(a, b)$ zweier Ecken $a, b$ von $G$ ist definiert als das Minimum der Länge aller Kantenzüge von $a$ nach $b$. Falls es keinen Kantenzug von $a$ nach $b$ gibt, wird $d(a, b) = \infty$ gesetzt.

Der folgende Algorithmus von Dijkstra (1959) berechnet die Abstände von einer gegebenen Ecke $v_0$ eines Netzwerks. Er kann – wie auch der Algorithmus von Moore im vorigen Abschnitt – für gerichtete und ungerichtete Graphen verwendet werden:

### 1.4.3 Algorithmus von Dijkstra

Gegeben sei ein Netzerk $(G, w)$ mit $G = (V, E)$ und einer nichtnegativen Längenfunktion $w$ auf $E$, sowie eine Ecke $v_0$ von $G$. Für jedes $v \in V$ wird ein Wert $d(v)$ berechnet:

(1) $d(v_0) \leftarrow 0$,
(2) `for` $v \in V \setminus \{v_0\}$ `do`
(3) $\quad d(v) \leftarrow \infty$,
(4) `end`,
(5) $U \leftarrow V$,
(6) `while` $U \neq \emptyset$ `do`
(7) $\quad u \leftarrow \arg\min_{v' \in U}\{d(v')\}$,
(8) $\quad$ `for` $v \in \{v' \in U \mid (u, v) \in E\}$ `do`
(9) $\quad\quad d(v) \leftarrow \min\{d(v), d(u) + w(u, v)\}$,
(10) $\quad$ `end`,
(11) $\quad U \leftarrow U \setminus \{u\}$
(12) `end`.

**Satz:** Nach Durchführung des Algorithmus von Dijkstra gilt $d(v) = d(v_0, v)$ für alle $v \in V$. Die Komplexität des Algorithmus ist $O(n^2)$.

**Beweis:** Klar ist, dass (nach Beendigung des Algorithmus) genau dann $d(v) = \infty$ gilt, wenn $v$ von $v_0$ aus nicht erreichbar ist, d. h. im Fall $d(v_0, v) = \infty$. Für alle anderen $v \in V$ ist $d(v)$ offenbar die Länge eines Weges von $v_0$ nach $v$, weshalb $d(v) \geq d(v_0, v)$ gilt.

Es bleibt $d(v) \leq d(v_0, v)$ zu zeigen. Dies gelingt mit *Induktion über die Ecken von* $G$, und zwar in der Reihenfolge, in der sie aus $U$ entfernt wurden: Zuerst wird $v_0$ entfernt und es gilt $d(v_0) = d(v_0, v_0) = 0$. Jetzt wird $d(v) \leq d(v_0, v)$ für alle vor der Ecke $u$ aus $U$ entfernten Ecken $v$ vorausgesetzt. Zu zeigen ist $d(u) \leq d(v_0, u)$. Werde, im Gegenteil, $d(u) > d(v_0, u)$ angenommen und sei $(v_0, v_1, \ldots, v_k = u)$ ein kürzester Weg von $v_0$ nach $u$. Es gibt einen Index $i < k$, so dass $v_i$ vor $u$ aus $U$ entfernt wurde, aber nicht $v_{i+1}$. Nach Induktionsvoraussetzung gilt $d(v_i) \leq d(v_0, v_i)$. Es folgt

$$d(u) > d(v_0, u) = d(v_0, v_i) + w(v_i v_{i+1}) + \ldots + w(v_{k-1} u) \geq d(v_i) + w(v_i v_{i+1})$$

Als $v_i$ aus $U$ entfernt wurde, galt aber $d(v_i) + w(v_i v_{i+1}) = d(v_{i+1}) \leq d(v_0, v_{i+1})$, also $u \neq v_{i+1}$. Das ist ein Widerspruch, da $u$ vor $v_{i+1}$ aus $U$ entfernt wird!

Für die Abschätzung der Komplexität müsste Zeile (3) eigentlich genauer formuliert werden. Aber es ist klar, dass man bei jedem Durchlauf von (3) mit maximal $|U|-1$ Vergleichen auskommt. In (4) sind jedesmal maximal $|U|$ Wertzuweisungen nötig. Die Schleife (2) bis (5) wird insgesamt $|V|$ mal durchlaufen. Da immer $|U| \leq |V|$ gilt, ergibt sich die behauptete Komplexität. □

**Beispiel:** Für folgendes Netzwerk liefert der Algorithmus von Dijkstra die Abstände von $v_0$. Die Werte $d(v)$ sind in der Reihenfolge aufgelistet, in der die Ecken aus $U$ entfernt werden:

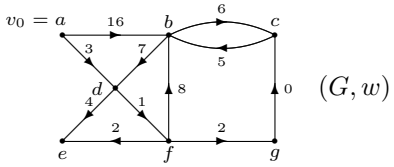



Abbildung 22: Algorithmus von Dijkstra

Übrigens: Der Algorithmus von Dijkstra kann leicht so abgewandelt werden, dass er nicht nur die Abstände, sondern auch die *kürzesten Wege* berechnet.

## 1.5 Flüsse in Netzwerken

Dieser Abschnitt stellt ein Beispiel eines „**Min-Max-Satzes**“ vor, nämlich den wohl berühmtesten („max flow = min cut“, Ford-Fulkerson 1956). Es geht darum, wieviel in einem Netzwerk mit gegebenen Kapazitäten transportiert werden kann. Man denke an ein Stromnetz, ein Wasserleitungssystem, ein Straßennetz oder an Datenübertragungsnetzwerke.

### 1.5.1 Flussnetzwerke

**Definition:** Ein **Flussnetzwerk** (auch: **Kapazitätsnetzwerk**) besteht aus

- einem **Digraphen** $G = (V, E)$,
- einer **Kapazitätsfunktion** $c : E \to \mathbb{R}_0^+$,
- zwei ausgezeichneten Ecken $s, t \in V$ (**Quelle**, **Senke**).

Ein **Fluss** in einem solchen Netzwerk ist eine Abbildung $f : E \to \mathbb{R}_0^+$, so dass folgendes gilt:

(F1) $0 \leq f(e) \leq c(e)$ für alle $e \in E$,

(F2) $\sum_{\substack{x \in V \\ (v,x) \in E}} f(v,x) = \sum_{\substack{y \in V \\ (y,v) \in E}} f(y,v)$ für alle $v \in V, v \neq s, t$.

Bedingung (F1) bedeutet, dass der Fluss nirgends negativ ist und immer die Kapazitäten eingehalten werden, (F2) bedeutet, dass in jede Ecke soviel hineinfließt wie herausfließt, allerdings mit Ausnahme der Quelle $s$ und der Senke $t$.

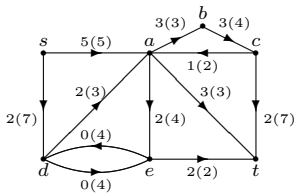



Abbildung 23: Flussnetzwerke

In diesem Beispiel fließt aus der Quelle $s$ ein Gesamtfluss von $f(s,a)+f(s,d) = 5+2 = 7$, und in die Senke $f(a,t)+f(c,t)+f(e,t) = 3+2+2 = 7$. Die Übereinstimmung der Werte ist kein Zufall, denn auf dem Weg von $s$ nach $t$ geht nichts verloren und wird nichts gewonnen.

**Bemerkung:** Für jede Flussfunktion f eines Flussnetzwerks mit Quelle $s$ und Senke $t$ gilt

$$\sum_{\substack{x\in V\\(s,x)\in E}} f(s,x) - \sum_{\substack{y\in V\\(y,s)\in E}} f(y,s) = \sum_{\substack{y\in V\\(y,t)\in E}} f(y,t) - \sum_{\substack{x\in V\\(t,x)\in E}} f(t,x)$$

**Beweis:** Die folgende Gleichung gilt, da auf beiden Seiten über alle Kanten $e \in E$ summiert wird:

$$\sum_{v\in V}\sum_{(v,x)\in E} f(v,x) = \sum_{v\in V}\sum_{(y,v)\in E} f(y,v)$$

Hieraus folgt:

$$\begin{aligned} 0 &= \sum_{v\in V}\left(\sum_{(v,x)\in E} f(v,x) - \sum_{(y,v)\in E} f(y,v)\right) \\ &= \left(\sum_{(s,x)\in E} f(s,x) - \sum_{(y,s)\in E} f(y,s)\right) + \left(\sum_{(t,x)\in E} f(t,x) - \sum_{(y,t)\in E} f(y,t)\right) \end{aligned}$$

wobei die letzte Gleichheit wegen (F2) gilt. □

### 1.5.2 Maximale Flüsse, zunehmende Wege

Falls es keine Kanten $(y,s)$ und keine Kanten $(t,x)$ gibt, dann schreibt sich die Gleichung der letzten Bemerkung kürzer als:

$$\sum_x f(s,x) = \sum_y f(y,t)$$

Die Zahl auf beiden Seiten der Gleichung (oder der Gleichung in der letzten Bemerkung) wird der **Wert** des Flusses $f$ genannt, in Zeichen: $\phi(f)$. Es ist immer das Ziel, einen **maximalen Fluss** zu finden, d. h. einen Fluss $f$ mit maximalem Wert $\phi(f)$. Jetzt wird gezeigt, wie dies gelingt:

**Definition:** Ein **zunehmender Weg** (engl.: augmenting path) bzgl. eines gegebenen Flusses f ist eine Folge $(s = v_0, v_1, \ldots, v_k = t)$, so dass für jedes $i \in \{1, \ldots, k\}$ eine der folgenden beiden Bedingungen gilt:

$(v_{i-1}, v_i) \in E$ und $f(v_{i-1}, v_i) < c(v_{i-1}, v_i)$ „Vorwärtskante“
$(v_i, v_{i-1} \in E$ und $f(v_i, v_{i-1}) > 0$ „Rückwüartskante“


Abbildung 24: Zunehmender Weg

### 1.5.3 Augmenting Path Theorem

Ein Fluss $f$ in einem Flussnetzwerk ist genau dann ein maximaler Fluss, wenn bezüglich $f$ kein zunehmender Weg existiert.

**Beweisskizze:** $\Longrightarrow$: Beweis mit Kontraposition. Sei $W$ ein zunehmender Weg bezüglich $f$. Dann kann der Flusswert $\phi(f)$ entlang $W$ um das Minimum folgender Werte gesteigert werden:

$$\{c(e) - f(w) \mid e \text{ Vorwärtskante in } W\} \cup \{f(e) \mid e \text{ Rückwärtskante in } W\}$$

$\Longleftarrow$: Es gebe keinen zunehmenden Weg bezüglich $f$. Werde definiert:
$S := \{v \in V \mid$ es gibt einen zunehmenden Weg von $s$ nach $v\}$, $\quad T := V \setminus S$
Es gilt $s \in S$ und, nach Voraussetzung, $t \in T$. Die Kanten zwischen $S$ und $T$ sind „gesättigt“:

- für jedes $(v, w) \in E$ mit $v \in S$, $w \in T$ gilt $f(v, w) = c(v, w)$
- für jedes $(w, v) \in E$ mit $w \in T$, $v \in S$ gilt $f(w, v) = 0$.

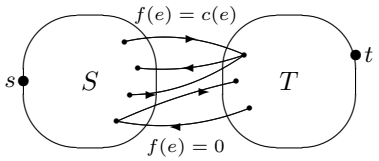



Abbildung 25: Minimaler Kantenschnitt

Also: die Kanten zwischen $S$ und $T$ bilden einen *Engpass*, der eine Flusswertvergrößerung verhindert. □

Der Beweis kann mit Hilfe der Flussgraphen (F1) und (F2) streng formal geführt werden. Aber das soll hier nicht geschehen, auch für die folgenden Überlegungen nicht: Die **Kapazität einer Kantenmenge** $F \subseteq E$ ist definiert als

$$c(F) := \sum_{e \in F} c(e)$$

Im Fall einer Zerlegung $V = S \dot\cup T$ mit $s \in S$ und $t \in T$ (wie auf voriger Seite) werden die Kantenmengen $E_{S\to T}$ und $E_{T\to S}$ folgendermaßen definiert:

$$E_{S\to T} := \{(x,y) \in E \mid x \in S, y \in T\} \qquad \text{(Kanten von } S \text{ nach } T\text{)}$$
$$E_{T\to S} := \{(x,y) \in E \mid x \in T, y \in S\} \qquad \text{(Kanten von } T \text{ nach } S\text{)}$$

Intuitiv sollte – wegen (F1) und (F2) – klar sein, dass folgendes gilt:

**Lemma:** Sei $f$ ein Fluss und $V = S \dot\cup T$ mit $s \in S$, $t \in T$. Dann gilt

$$\phi(f) = \sum_{e\in E_{S\to T}} f(e) - \sum_{e\in E_{T\to S}} f(e) \le c(E_{S\to T})$$

Insbesondere ist für jeden Fluss $f$ der Wert $\phi(f)$ beschränkt durch die Kapazität $c(E_{S\to T})$ der Kantenmenge $E_{S\to T}$. (Jede solche Kantenmenge wird $s$ **und** $t$ **trennender Schnitt** genannt.)

### 1.5.4 Minimaler Schnitt

Wie in der Beweisskizze des Augmenting Path Theorems angedeutet, existiert im Fall eines maiximalen Flusses $f$ ein $s$ und $t$ **trennender Schnitt** $E_{S\to T}$ mit $\phi(f) = c(E_{S\to T})$.

Dieser Schnitt ist ein **minimaler Schnitt**, das heißt ein $s$ und $t$ trennender Schnitt von minimaler Kapazität (denn sonst wäre $\phi(f)$ durch die Kapazität eines anderen Schnitts beschränkt). Deshalb gilt der berühmte Satz von L.R. Ford und D.R. Fulkerson (1956):

### 1.5.5 Max-Flow Min-Cut Theorem

**Satz:** In jedem Flussnetzwerk ist der Wert eines maximalen Flusses von Quelle $s$ zur Senke $t$ gleich der Kapazität eines minimalen $s$ und $t$ trennenden Schnitts.

Der Beweis des Augmenting path Theorems gibt eine Idee für einen Algorithmus zum Auffinden maximaler Flüsse und minimaler Schnitte.

**Skizze eines Algorithmus:** Sei ein Fluss $f$ von $s$ nach $t$ gegeben ($f(e) = 0$ für alle $e \in E$ ist möglich ):

1. Falls es keinen zunehmenden Weg von $s$ nach $t$ gibt, dann STOP. Sonst weiter mit 2.

2. Sei $(v_0, v_1, \cdots, v_k)$ ein zunehmender Weg bzgl. $f$. Setze
   $z := min(\{c(v_{i-1}, v_i) - f(v_{i-1}, v_i) \mid (v_{i-1}, v_i)\text{Vorwärtskante}\} \cup$
   $\{f(v_i, v_{i-1}) \mid (v_i, v_{i-1})\text{Rückwärtskante}\})$
   Sei
   $f(v_{i-1}, v_i) := f(v_{i-1}, v_i) + z$ für jede Vorwärtskante und
   $f(v_i, v_{i-1}) := f(v_i, v_{i-1}) - z$ für jede Rückwärtskante. Weiter mit (1).

Wie findet man zunehmende Wege? Dies gelingt schrittweise, indem jede Ecke $y$ eines zunehmenden Weges mit drei Werten $v(y)$, $r(y)$, $z(y)$ **markiert** wird:

| | |
|---|---|
| $v(y)$ | Vorgänger von $y$ im zunehmenden Weg, |
| $r(y)$ | Richtung der Kante von $v(y)$ nach $y$: $r(y) = \rightarrow$ für Vorwärtskante, $r(y) = \leftarrow$ für Rückwärtskante, |
| $z(y)$ | möglicher zusätzlicher Flusswert von $s$ nach $y$. |

### 1.5.6 Markierungs-Algorithmus (Ford-Fulkerson)

Sei ein Flussnetzwerk, bestehend aus einem Digraphen $G$ und einer Kapazitätsfunktion $c$ mit Quelle $s$ und Senke $t$, gegeben. Sei $f$ ein Fluss auf diesem Netzwerk.

(1) $S \leftarrow \{s\},\ R \leftarrow \{s\},\ z(s) \leftarrow \infty,$
(2) `for` $x \in R$ `do`
(3) $R \leftarrow R \setminus \{x\},$
(4) `for` $y \in \{y' \in V \setminus S \mid (x,y') \in E \wedge f(x,y') < c(x,y')\}$ `do`
(5) $S \leftarrow S \cup \{y\},\ R \leftarrow R \cup \{y\},$
(6) $v(y) \leftarrow x,\ r(y) \leftarrow [\Rightarrow],\ z(y) \leftarrow \min\{c(x,y) - f(x,y), z(x)\},$
(7) `end,`
(8) `for` $y \in \{y' \in V \setminus S \mid (y',x) \in E \wedge f(x,y') > 0\}$ `do`
(9) $S \leftarrow S \cup \{y\},\ R \leftarrow R \cup \{y\},$
(10) $v(y) \leftarrow x,\ r(y) \leftarrow [\Leftarrow],\ z(y) \leftarrow \min\{f(y,x), z(x)\},$
(11) `end,`
(12) `???`
(13) $z \leftarrow z(t),\ y \leftarrow t,$
(14) `while` $y \neq s$ `do`
(15) `if` $r(y) = [\Rightarrow]$ `then`
(16) $f(v(y),y) \leftarrow f(v(y),y) + z,$
(17) `end,`
(18) `if` $r(y) = [\Leftarrow]$ `then`
(19) $f(y,v(y)) \leftarrow f(y,v(y)) - z,$
(20) `end,`
(21) $y \leftarrow v(y),$
(22) `end,`
(23) `???`

1. Setze $S{:=}\{s\}$, $R{:=}\{s\}$, $z(s){:=}\infty$.
2. Wähle eine Ecke $x \in R$. Setze $R := R \setminus \{x\}$.
3. Füge jede Ecke $y \in V \setminus S$ mit $(x,y) \in E$ und $f(x,y) < c(x,y)$ zu $S$ und zu $R$ hinzu und setze $v(y){:=}x$, $r(y){:=}\rightarrow$, $z(y){:=}min\{c(x,y){-}f(x,y), z(x)\}$.
4. Füge jede Ecke $y \in V \setminus S$ mit $(y,x) \in E$ und $f(x,y) > 0$ zu $S$ und zu $R$ hinzu und setze $v(y){:=}x$, $r(y){:=}\leftarrow$, $z(y){:=}min\{f(y,x), z(x)\}$.
5. Falls $R = \emptyset$, dann STOP. Falls $t \in S$, dann weiter mit (6). Sonst weiter mit (2).

6. Setze $z := z(t)$, $y := t$.
7. Falls $r(y) = \rightarrow$, setze $f(v(y), y) := f(v(y), y) + z$. Falls $r(y) = \leftarrow$, setze $f(y, v(y)) := f(y, v(y)) - z$.
8. Setze $y := v(y)$. Falls $y = s$, weiter mit (1). Sonst weiter mit (7).

Die Menge $S$ besteht jeweils aus den Ecken, zu denen von $s$ aus ein zunehmender Weg gefunden wurde, und $R$ besteht aus denjenigen Ecken in $S$, die noch nicht benutzt wurden, um längere zunehmende Wege zu erhalten. Im Fall $R = \emptyset$ gibt es keine weiteren zunehmenden Wege, das heißt der bis dahin gefundene Fluss $f$ ist maximal.

Falls alle Kapazitäten ganzzahlig sind, $c(e) \in \mathbb{Z}$ für alle $e \in E$, dann terminiert der Algorithmus (da alle Flusszuwächse ganzzahlig sind). Also wird der STOP-Befehl in Zeile (5) erreicht. Dasselbe gilt, falls alle Kapazitäten rationale Zahlen sind, $c(e) \in \mathbb{Q}$.

**Satz:** Für jedes Flussnetzwerk mit rationalen Kapazitätswerten berechnet der Markierungsalgorithmus einen maximalen Fluss $f$ und eine Eckenmenge $S$, so dass (mit $T := V \setminus S$) $E_{S \to T}$ ein minimaler $s$ und $t$ trennender Schnitt ist.

**Bemerkungen**

(a) Im Fall von irrationalen Kapazitätswerten kann es vorkommen, dass der Algorithmus unendlich viele Flusszunahmen berechnet, also nie stoppt (und möglicherweise nicht einmal in die Nähe eines maximalen Flusses kommt).

(b) Selbst für ganzzahlige Kapazitäten ist die Komplexität des Markierungsalgorithmus nicht polynomial in $n = |V|$ oder $m = |E|$, da die Anzahl der Schritte von der Kapazitätsfunktion $c$ abhängen kann. Zeile (2) im Algorithmus ist sehr unklar formuliert. Organisiert man in (2) die Reihenfolge, in der die Ecken ausgewählt werden, wie im Algorithmus von Moore (Seite 27), also nach dem Schema „breadth first search“, dann wird Komplexität $O(nm^2)$ erreicht. Dies wurde 1992 von *Edmonds und Karp* gezeigt. Mit noch weiter entwickelten Methoden (zum Beispiel von *Sleator und Tarjan*) kann man sogar Komplexität $O(nm \log n)$ eingehalten werden.

**Beispiel:** Es wird der Markierungsalgorithmus auf den Fluss auf Seite 32 angewandt. Dieser hatte den Flusswert $\phi(f) = 7$. Es ergibt sich ein minimaler Schnitt mit $S = \{s, a, b, d, e\}$ und $T = \{c, t\}$. Damit ist der Fluss $f$ maximal mit $\phi(f) = 9$.

Es gibt unzählige Anwendungen des Markierungsalgorithmus und des darauffolgenden Satzes. Beides kann auf viele Situationen angepasst werden, beispielsweise

- auf Flussnetzwerke mit mehreren Quellen und Senken,
- auf Flussnetzwerke mit zusätzlichen Kapazitätsbeschränkungen in Ecken,
- auf Flussnetzwerke mit Gewinnen und Verlusten in den Ecken,

und auf vieles mehr.

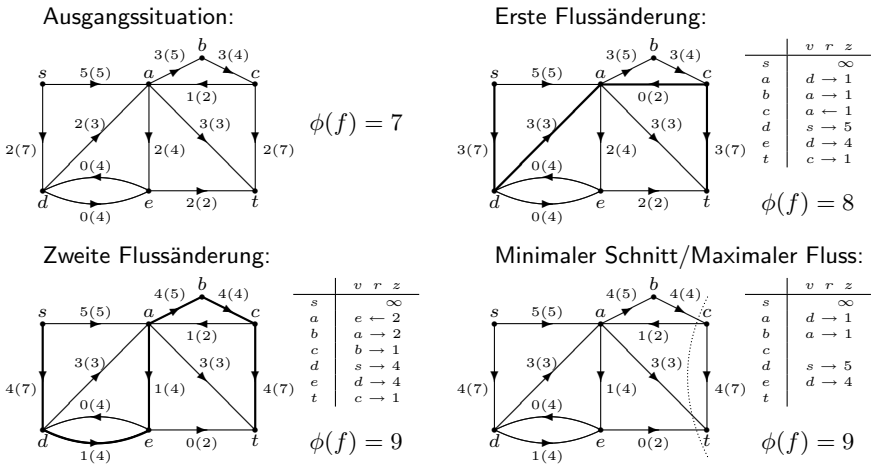



Abbildung 26: Markierungsalgorithmus

## 1.6 Gruppen und Permutationen

Im Rest dieses Kapitels werden „Symmetrien von Graphen“ und das Zählen gewisser Objekte „bis auf Symmetrie“ behandelt. Die mathematische Betrachtung von **Symmetrie** führt direkt zum Begriff „**Permutationsgruppe**“. Damit wird - nebenbei - der Übergang zum nächsten Kapitel über **algebraische Strukturen** vorbereitet. Aber zuerst einige gruppentheoretische Grundbegriffe:

### 1.6.1 Gruppen

**Definition:** Eine Gruppe ist ein Paar $(G, \cdot)$, bestehend aus einer nichtleeren Menge $G$ sowie einer zweistelligen Operation $\cdot$ auf $G$ (das heißt eine Abbildung $G \times G \to G$, $(x, y) \mapsto x \cdot y$), so dass folgende Regeln erfüllt sind:

| | | |
|---|---|---|
| (ass) | $\forall x, y, z \in G: (x \cdot y) \cdot z = x \cdot (y \cdot z)$ | **Assoziativität**, |
| (neu) | $\exists e \in G \forall x \in G: e \cdot x = x = x \cdot e$ | **neutrales Element**, |
| (inv) | $\forall x \in G \exists x^{-1} \in G: x \cdot x^{-1} = e = x^{-1} \cdot x$ | **inverse Elemente**. |

Gilt außerdem noch

(kom) $\forall x, y \in G: x \cdot y = y \cdot x$ **Kommutativität**,

so spricht man von einer **abelschen** (oder **kommutativen**) **Gruppe**.

**Bemerkungen**

(a) Anstelle von $x \cdot y$ wird oft auch einfach $xy$ geschrieben.

(b) Man kann leicht zeigen, dass das neutrale Element $e$ einer Gruppe eindeutig bestimmt ist, das heißt es kann nicht zwei verschiedene solche Elemente geben. Regel (inv) bezieht sich auf das (eindeutig bestimmte) neutrale Element $e$. Für jedes $x \in G$ ist das inverse Element $x^{-1}$ ebenfalls eindeutig bestimmt.

(c) In abelschen Gruppen wird oft $+, -, 0$ anstelle von $\cdot, ^{-1}, e$ geschrieben (**additive Schreibweise**).

**Beispiele**

(a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind abelsche Gruppe. Hingegen sind $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{N}, \cdot)$ und $(\mathbb{N}, +)$ keine Gruppen. Für jedes $n \in \mathbb{N}$ ist $(\mathbb{Z}_n, +)$ eine abelsche Gruppe (auf der Grundmenge $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ wird „**modulo** $n$“ gerechnet.

(b) Die folgende **Verknüpfungstafel** definiert eine Gruppenoperation auf der Grundmenge $G = \{e, s, t, u, v, w\}$:

| · | e | s | t | u | v | w |
|---|---|---|---|---|---|---|
| e | e | s | t | u | v | w |
| s | s | e | w | v | u | t |
| t | t | v | e | w | s | u |
| u | u | w | v | e | t | s |
| v | v | t | u | s | w | e |
| w | w | u | s | t | e | v |

(c) Eine Permutation auf einer Menge $A$ ist eine bijektive Abbildung $f\colon A \to A$. Die Menge aller Permutationen auf $A$ wird mit $S_A$ bezeichnet. (Im Fall $|A| = n$ schreibt man auch $S_n$.) Für zwei Permutationen $f, g$ auf $A$ ist die **Verkettung** (Komposition, Hintereinanderausführung) $f \circ g$ definiert durch

$$(f \circ g)(x) := f(g(x))$$

für alle $x \in A$. Für jede Menge $A$ ist $(S_A, \circ)$ eine Gruppe (die **symmetrische Gruppe** auf $A$)

**Definition:** Ist $(G, \cdot)$ eine Gruppe und $H$ eine Teilmenge von $G$, die mit der auf $G$ erklärten Gruppenoperation selbst eine Gruppe darstellt, dann nennt man $H$ eine **Untergruppe** von $G$ (in Zeichen: $H \leqslant G$).

**Bemerkungen:** Offenbar ist $H$ genau dann eine Untergruppe von $G$, wenn folgendes gilt:

(1) $H$ ist nicht leer,
(2) für alle $a, b \in H$ gilt $ab \in H$,
(3) für alle $a \in H$ gilt $a^{-1} \in H$

Man müsste $H$ eigentlich genauer die „Grundmenge einer Untergruppe“ nennen; die Untergruppe selbst ist das Paar $(H, \cdot)$, wobei man die Gruppenoperation „$\cdot$“ auf $H$ eingeschäntkt betrachten muss.

### 1.6.2 Links- und Rechtsnebenklassen

Sei $H$ eine Untergruppe von $G$. Für jedes $g \in G$ ist die **Linksnebenklasse** von $g$ als die Menge $gH := \{gh \mid h \in H\}$ definiert. (Entsprechend nennt man $Hg := \{hg \mid h \in H\}$ die **Rechtsnebenklasse** von $g$.) Die Menge aller Linksnebenklassen der Untergruppe $H$ wird mit $G/H$ bezeichnet. Für je zwei Elemente $g_1, g_2 \in G$ gilt entweder $g_1H = g_2H$ oder $g_1H \cap g_2H = \emptyset$. Die Linksnebenklassen

bilden also eine **disjunktive Überdeckung** der Menge $G$. Außerdem sind die Linksnebenklassen alle gleich groß, für alle $g \in G$ gilt $|gH| = |H|$. Eine bijektive Abbildung von $G$ auf $gH$ wird gegeben durch $h \longrightarrow gh$. Es folgt:

### 1.6.3 Satz von Lagrange

**Satz:** Sei $G$ eine endliche Gruppe und $H$ eine Untergruppe von $G$. Dann gilt:

$$|H| \;\Big|\; |G|$$

Die **Ordung** (das heißt die Anzahl der Elemente) der Untergruppe $H$ teilt also die Ordnung von $G$.

Die Ordnung eines Elementes $a \in G$ ist definiert als die Zahl $k$ mit $a^k = e$. (Wenn eine solche Zahl nicht existiert, dann setzt man $\mathrm{ord}(a) = \infty$.) Für jedes Element $a \in G$ ist offenbar $\langle a \rangle := \{a^i \mid i \in \mathbb{Z}\}$ die kleinste Untergruppe von $G$, die $a$ enthält (die von $a$ erzeugte Untergruppe, solche von einem Element erzeugten Untergruppen werden **zyklisch** genannt). Wenn die Ordnung von $a$ endlich ist, dann hat die Untergruppe $\langle a \rangle$ genau $\mathrm{ord}(a)$ Elemente, nämlich $a, a^2, \ldots, a^{\mathrm{ord}(a)}$. Mit dem Satz von Lagrange folgt hieraus Teil (a) des Korollars. Die Teile (b) und (c) sind dann klar:

**Korollar:** Für jedes Element $a$ einer endlichen Gruppe $G$ gilt

$$\mathrm{ord}(a) \;\Big|\; |G|$$

Für jedes Gruppenelement $a$ einer endlicher Ordnung und jede Zahl $k \in \mathbb{Z}$ gilt

$$a^k = e \quad \Longleftrightarrow \quad \mathrm{ord}(a) \mid k$$

Für jedes Element $a$ einer endlichen Gruppe $G$ gilt

$$a^{|G|} = e$$

Im Rest des Kapitels richtet sich das Interesse auf Permutationsgruppen:

### 1.6.4 Permutationsgruppen

**Definition:** Sei $A$ eine Menge. Jede Untergruppe $G$ der symmetrischen Gruppe $S_A$ heißt **Permutationsgruppe** auf $A$. Der Anzahl $|A|$ der Elemente von $A$ wird der **Grad** der Permutationsgruppe $G$ genannt.

Eine Permutationsgruppe auf $A$ ist also eine nicht leere Menge von Permutationen der Menge $A$, die gegen Verkettung und Inversenbildung abgeschlossen ist. Klar ist:

**Bemerkungen:** Für alle $n \in \mathbb{N}$ gilt $|S_n| = n!$.
Für jede Permutationsgruppe $G$ auf $A$ von Grad $n$ (also mit $|A| = n$) gilt

$$|G| \;\Big|\; n!$$

Es gibt verschiedene Möglichkeiten, Permutationen darzustellen. Eine Möglichkeit sind Wertetabellen, zum Beispiel:

$$f = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 0 & 5 & 8 & 6 & 1 & 4 & 7 & 3 & 9 & 2 \end{array}\right)$$

$$g = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \hline 0 & 1 & 6 & 8 & 5 & 4 & 2 & 9 & 3 & 7 \end{array}\right)$$

Als Produkt ziffernfremder Zyklen (kurz: **Zyklendarstellung**) schreibt man $f$ und $g$ als

$$f = (154)(289)(367), \qquad g = (26)(38)(45)(79).$$

Hierbei steht zum Beispiel (145) für die Permutation, die 1 auf 5, 5 auf 4, 4 auf 1 abbildet. Solche Permutationen heißen **Zyklen**, und jede Permutation (auf endlicher Grundmenge $A$) ist ein Produkt von endlichen Zyklen.

**Definition:** Die Permutationsgruppe $G$ operiere auf $A$, und es sei $a \in A$. Die Menge

$$a^G := \{g(a) \mid g \in G\}$$

heißt **Bahn** (oder **Orbit**) von $a$ unter $G$. Der **Stabilisator** (oder die **Standuntergruppe**) von $a$ in $G$ ist

$$G_a := \{g \in A \mid g(a) = a\}$$

Allgemeiner definiert man den Stabilisator einer Teilmenge $B \subseteq A$ als

$$G_B := \{g \in G \mid \forall b \in B : g(b) = b\}$$

Im Fall $B = \{b_1, \ldots, b_n\}$ wird statt $G_B$ auch $G_{b_1 \ldots b_n}$ geschrieben.

Die Bahn von $a$ besteht also aus den Elementen von $A$, zu denen man von $a$ aus durch Anwendung von Permutationen aus $G$ gelangen kann. Wenn es nur eine einzige Bahn gibt, das heißt im Fall $a^G = A$, dann nennt man $G$ transitiv. Der Stabilisator von $a$ ist sebst eine Permutationsgruppe, also eine Untergruppe von $G$. Die nächsten beiden Lemmata sind von größter Bedeutung:

**Lemma:** Für jede Permutationsgruppe $G$ auf $A$ und jedes $a \in A$ gilt:

$$|G| = |a^G| \cdot |G_a|$$

**Beweis:** Für $f, g \in G$ gilt genau dann $f(a) = g(a)$, wenn $(g^{-1}f)(a) = a$ gilt. Dies ist äquivalent zu $(g^{-1}f \in G_a)$, was auch als $f \in gG_a$ geschrieben werden kann. Also entspricht jedes Element von $a^G$ genau einer Linksnebenklasse $gG_a$ von $G_a$ in $G$. Bekanntlich gibt es genau $|G|/|G_a|$ solcher Nebenklassen. Es folgt $|a^G| = |G|/|G_a|$.

Bei näherer Betrachtung dieses Beweises erhält man, zusätzlich zur Bestimmung der Anzahl der Elemente von $G$, folgende nähere Beschreibung der Elemente von $G$:

**Lemma:** Die Bahn $a^G$ bestehe aus genau $k$ verschiedenen Elementen $a_1$, ..., $a_k$, und für jedes dieser Elemete sei $g_i$ eine Permutation $g_i \in G$ mit $g_i(a) = a_i$. Dann lässt sich jedes $g \in G$ in genau einer Weise in der Form $g = g_i h$ mit $i \in \{1, \ldots, k\}$ und $h \in G_a$ darstellen.

**Beweis:** $G$ ist die disjunktive Vereinigung der Linksnebenklassen $g_1 G_a$, ..., $g_k G_a$. □

Im nächsten Abschnitt folgen Anwendungsbeispiele!

## 1.7 Symmetrien von Graphen

Die Symmetrien dieses Abschnitts sind nichts als die Automorphismen von Graphen:

### 1.7.1 Automorphismen

**Definition:** Ein **Automorphismus** eines Graphen $\Gamma = (V, E)$ ist eine bijektive Abbildung $\alpha: V \longrightarrow V$, so dass für alle $x, y \in V$ folgendes gilt:

$$\{x, y\} \in E \quad \Longleftrightarrow \quad \{\alpha(x), \alpha(y)\} \in E$$

Ein Automorphismus von $\Gamma$ ist also ein Isomorphismus von $\Gamma$ auf sich selbst.

**Anmerkung:** Graphen werden jetzt mit $\Gamma$ bezeichnet, zur Unterscheidung von Gruppen.

**Beispiel:** Die Permutation $f$ und $g$ von Seite 40 sind Automorphismen des **Petersengraphen**, wenn man die Ecken so bezeichnet wie in der Skizze.

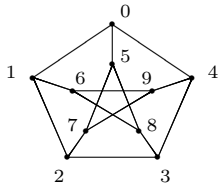



Abbildung 27: Petersengraph

Man kann die Automorphismen als die Symmetrien eines Graphen auffassen. Ist $\alpha$ ein Automorphismus von $\Gamma$ mit $\alpha(x) = y$, dann bedeutet das, dass $\Gamma$ von $x$ aus „genauso aussieht“ wie von $y$ aus.

### 1.7.2 Automorphismengruppe

Für jeden Graphen $\Gamma = (V, E)$ bilden die Automorphismen einer Permutationsgruppe auf $V$. Diese Gruppe wird die **Automorphismengruppe** von $\Gamma$ genannt und mit $G(\Gamma)$ bezeichnet.

**Beispiele**

(a) Die Automorphismengruppe des **vollständigen Graphen** $K_n$ ($n$ Ecken, je zwei Ecken durch eine Kante verbunden) ist die volle **symmetrische Gruppe** $S_n$.

(b) Der $n$-elementige Kreis $C_n$ hat für $n \geq 3$ als Automorphismengruppe die **Diedergruppe** $D_n$ (sprich: Di-eder). Diese Gruppe besteht aus $2n$ Elementen.

(c) Der Graph $\Gamma$ hat nur die identische Abbildung als Automorphismus.

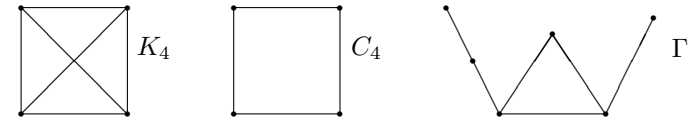



Abbildung 28: Graphenautomorphismen

Mit dem Lemma von Seite 40 ergibt sich unmittelbar das folgende Verfahren:

### 1.7.3 Bestimmung der Automorphismengruppe

Verfahren zur Bestimmung der Automorphismengruppe eines Graphen:
Der Graph sei $\Gamma = (V, E)$, und die Automorphismengruppe $G(\Gamma)$ werde kurz mit $G$ bezeichnet.

1. Wähle eine Ecke $a \in V$. Bestimme eine möglichst kleine Menge $A = \{g_1, \ldots, g_\ell\} \subseteq G$ mit $a^G = \{g_1(a), \ldots, g_\ell(a)\}$. Dann gilt $g_i(a) \neq g_j(a)$ für $i \neq j$, und jedes $g \in G$ lässt sich in genau einer Weise in der Form $g = g_i h$ mit $i \in \{1, \ldots, \ell\}$ und $h = G_a$ schreiben.

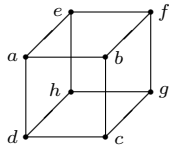
2. Falls die Elemente von $G_a$ nicht bekannt sind, kann das Verfahren mit $G_a$ anstelle $G$ wiederholt werden: Wähle eine Ecke $b \neq a$ und bestimme anschließend eine möglichst kleine Menge $B = \{h_1, \ldots, h_m\} \subseteq G_a$ mit $b^{G_a} = \{h_1(b), \ldots, h_m(b)\}$. Jedes $g \in G$ lässt sich jetzt genau in einer Weise in der Form $g = g_i h_j k$ mit $i \in \{1, \ldots, \ell\}$, $j \in \{1, \ldots, m\}$, $k \in G_{ab}$ schreiben.

3. Diese Prozedur wird solange wiederholt, bis man schießlich einen Stabilisator erhält, dessen Elemente man kennt. Das ist spätestens der Fall, wenn der Stabilisator nur noch aus der identischen Abbildung besteht.

Bei der Auswahl der Elemente $a, b, \ldots$ kann man mehr oder weniger geschickt sein. Im Allgemeinen ist es günstig, wenn die Bahnen $a^G, b^{G_a}, \ldots$ groß sind, da das Verfahren dann nach weniger Durchläufen abbricht als bei kleineren Bahnen. Die Mengen $A, B, \ldots$ findet man im wesentlichen durch Probieren.

**Beispiel:** Es wird der „Würfelgraph“ $\Gamma$ behandelt. Klar ist: $\alpha_1 = (abcd)(efgh)$ und $\alpha_2 = (ae)(bf)(cg)(dh)$ sind Automorphismen von $\Gamma$. Es gilt:

$$id(a) = a,\ \alpha_1(a) = b,\ \alpha_1^2(a) = c,\ \alpha_1^3(a) = d,$$




$\Gamma$

Abbildung 29: Würfelgraph

$$\alpha_2(a) = e,\ \alpha_1\alpha_2(a) = f,\ \alpha_1^2\alpha_2(a) = g,\ \alpha_1^3\alpha_2(a) = h$$

Das liefert $a^G = \{a, b, c, d, e, f, g, h\} = V$. Daher kann man

$$A = \{id, \alpha_1, \alpha_1^2, \alpha_1^3, \alpha_2, \alpha_1\alpha_2, \alpha_1^2\alpha_2, \alpha_1^3\alpha_2\}$$

wählen. Jetzt wird $b^{G_a}$ bestimmt. Klar ist $b^{G_a} \subseteq \{b, d, e\}$, denn da $a$ festbleibt, kann $b$ nur auf zu $a$ benachbarte Ecken abgebildet werden. Mit dem Automorphismus $\beta = (bde)(chf)$ („Drehung um die Würfeldiagonale durch $a$ und $g$“) ergibt sich:

$$id(b) = b, \quad \beta(b) = d, \quad \beta^2(b) = e$$

Daher gilt $b^{G_a} = \{b, d, e\}$, und es kann

$$B = \{id,\ \beta,\ \beta^2\}$$

gewählt werden. Offenbar gilt $G_{a_b} = \{id, \gamma\}$ mit $\gamma = (cf)(de)$. Damit ist $G$ vollständig bestimmt: Jedes $g \in G$ lässt sich auf genau eine Weise in folgender Form schreiben:

$$g = \alpha_1^i\alpha_2^j\beta^k\gamma^\ell \quad \text{mit } i \in \{0, 1, 2, 3\},\ j, \ell \in \{0, 1\},\ k \in \{0, 1, 2\}$$

Es folgt insbesondere $G = \langle \alpha_1, \alpha_2, \beta, \gamma \rangle$, das heißt die Gruppe $G$ wird von den Elementen $\alpha_1, \alpha_2, \beta, \gamma$ erzeugt (wobei es bei dieser Betrachtung nicht darauf ankommt, in welcher Reihenfolge diese Elemente multipliziert werden müssen).

Interessiert man sich nur für die Mächtigkeiten, dann liefert obiges:

$$|a^G| = 8,\ |b^{G_a}| = 3,\ |G_{a_b}| = 2$$

Das Lemma von Seite 40 liefert:

$$|G_a| = |b^{G_a}| \cdot |G_{a_b}| = 3 \cdot 2 = 6, \quad \text{also } |G| = |a^G| \cdot |G_a| = 8 \cdot 6 = 48$$

## 1.8 Die Pólyasche Abzählmethode

In diesem Abschnitt wird eine *gruppentheoretische* Methode zur Lösung des folgenden Problems entwickelt (und natürlich zur Lösung vieler anderer Probleme):

> Wieviele Perlenketten nur aus weißen und schwarzen Perlen gibt es, die genau drei weiße und drei schwarze Perlen enthalten?

Hierbei komme es nur auf die Farbe der Perlen an und auf die Reihenfolge, in der sie aufeinanderfolgen. Zuerst muss geklärt werden, wann zwei Perlenketten als „gleich“ betrachtet werden sollen. Sind die Ketten (i) und (ii) wesentlich

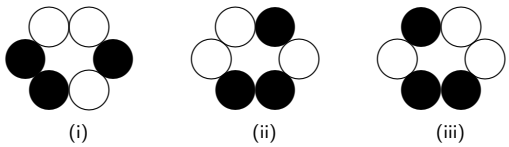



Abbildung 30: Die Pólyasche Abzählmethode

verschieden? Wenn man die Ketten *drehen* darf, dann wohl nicht. Auch die Ketten (ii) und (iii) sind gleich, wenn man die Ketten *wenden* darf. Das Problem ist also: Welches sind die zulässigen Symmetrien?
Diese bilden im Ganzen eine **Permutationsgruppe**. Die in obigen Skizzen auftretenden Symmetrien können in Zyklenschreibweise notiert werden:

| | |
|---|---|
| $\tau := (012345)$ | Drehen der Ketten um eine Perle |
| $\sigma := (0)(3)(15)(24)$ | Wenden einer Kette |

Erlaubt man beides als zulässige Symmetrien, so erhält man insgesamt als Symmetriengruppe die **Diedergruppe** $D_6$, bestehend aus den Drehungen $\tau^i$ und den Spiegelungen $\sigma\tau^i$, $i = 0, \ldots, 5$. Dieses Beispiel wird unten weiter verfolgt.

Es folgt ein für die **Pólya-Theorie** grundlegender Satz über Permutationsgruppen. Darin, oder im Beweis, tauchen $a^G$ für die **Bahn** von $a$ unter der Permutationsgruppe $G$ auf, und $G_a$ für den **Stabilisator** von $a$ unter $G$. Außerdem wird verwendet:

| | |
|---|---|
| $b(G) := \lvert\{a^G \mid a \in A\}\rvert$ | Anzahl der Bahnen von $G$ |
| $\mathrm{Fix}(g) := \{a \in A \mid g(a) = a\}$ | Menge der Fixpunkte von $g \in G$ |

Das folgende Resultat ist höchst erstaunlich. Es besagt: Die Anzahl der Bahnen von $G$ ist gleich der durchschnittlichen Anzahl der Fixpunkte in $G$:

### 1.8.1 Cauchy-Frabenius-Lemma

**Lemma:** Für jede Permutationsgruppe $G$ gilt

$$b(G) = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

**Beweis** mit doppelter Abzählung für die Relation $I \subseteq A \times G$ mit

$$aIg \quad :\Leftrightarrow \quad g(a) = a$$

Jedes $a \in A$ inzidiert mit genau $|G_a|$ Elementen von $G$, und jedes $a \in A$ mit genau $|\mathrm{Fix}(g)|$ Elementen von $A$, also

$$\circledast \qquad \sum_{a \in A} |G_a| = \sum_{g \in G} |\mathrm{Fix}(g)|$$

Umformung der linken Seite mit dem Lemma von Seite 40 liefert

$$\sum_{a \in A} |G_a| = \sum_{a \in A} \frac{|G|}{|a^G|} = |G| \cdot \sum_{a \in A} \frac{1}{|a^G|}$$

Zur Auswertung der letzten Summe beachte man: Für eine gegebene Bahn $c^G$ und alle $a \in c^G$ gilt $a^G = c^G$. Deshalb:

$$\sum_{a \in c^G} \frac{1}{|a^G|} = 1,$$

das heißt *jede* Bahn $a^G$ liefert zur Summe den Beitrag 1. Mit Hilfe von $\circledast$ ergibt sich jetzt die Behauptung. □

### 1.8.2 Färbung

Sei weiterhin $G$ eine auf $A$ operierende Permutationsgruppe. Eine **Färbung** von $A$ mit einer „Farbmenge“ $F$ ist definiert als eine Abbildung $\Phi\colon A \longrightarrow F$ Die Menge aller Färbungen ist dann

$$\tilde{A} := F^A \quad \text{(Menge aller Abbildungen } A \longrightarrow F\text{)}.$$

Aus jedem $g \in G$ wird in natürlicher Weise eine Permutation $\tilde{g}$ auf $\tilde{A}$. Für die „Bildfärbung“ $\tilde{g}\Phi$ (Bild von $\Phi$ unter $\tilde{g}$) sollte $(\tilde{g}\Phi)(ga) = \Phi(a)$ gelten.

**Definition:** Aus $G$ wird eine Permutationsgruppe $\widetilde{G} = \{\tilde{g} \mid g \in G\}$ auf der Menge $\tilde{A} = F^A$ der Färbungen von $A$ gegeben durch

$$(\tilde{g}\Phi)(a) := \Phi(g^{-1}a)$$

Wann gelten zwei Färbungen als gleich? Genau dann, wenn sie in derselben Bahn bezüglich $\widetilde{G}$ liegen! Also mit den Cauchy-Frabenius-Lemma:

**Bemerkung:** Die Anzahl der (bezüglich $G$) wesentlich verschiedenen Färbungen von $A$ ist

$$b(\widetilde{G}) = \frac{1}{|\widetilde{G}|} \sum_{\tilde{g} \in \widetilde{G}} |\mathrm{Fix}(\tilde{g})|$$

Statt $\tilde{g} \in \widetilde{G}$ kann $g \in G$ geschrieben werden, und $|\widetilde{G}| = |G|$ ist ohnehin klar. Für jedes $g \in G$ ist $|\mathrm{Fix}(\tilde{g})|$ zu bestimmen: $\Phi \in \mathrm{Fix}(\tilde{g})$ bedeutet $\tilde{g}\Phi = \Phi$, also $(\tilde{g}\Phi)(a) = \Phi(a)$ für alle $a \in A$. Mit obiger Definition ergibt das

$$\Phi(g^{-1}a) = \Phi(a)$$

Das bedeutet:

**Beobachtung:** $\mathrm{Fix}(\tilde{g})$ besteht aus genau denjenigen Färbungen $\Phi$, die innerhalb jedem Zyklus der Zyklendarstellung von $g$ alle Elemente gleich färben. Also: Gibt es genau $f = |F|$ Farben und hat $g$ genau $k$ Zyklen, dann gilt

$$|\mathrm{Fix}(\tilde{g})| = f^k$$

### 1.8.3 Permutationstypen

Diese Tatsachen lassen sich am besten ausnutzen, wenn man den Permutationstyp $t(g)$ von $g$ verwenden kann. Bei diesem handelt es sich um einen formalen Ausdruck der Form

$$t(g) = \prod_{i=1}^{n} z_i^{k(i)}$$

wobei $n = |A|$ die Anzahl der Elemente der Grundmenge ist, und $k(i)$ die Anzahl der Zyklen von $g$ der Länge $i$ angibt. Ist $k$ die Anzahl *aller* Zyklen von $G$, dann gilt $k = \sum k(i)$. Als Beispiel wird die Diedergruppe $D_6$ betrachtet (siehe Seite 44). Sie besteht aus folgenden Permutationen:

| | |
|---|---|
| $\tau^0 = id = (0)(1)(2)(3)(4)(5)$, | $\sigma\tau^0 = \sigma = (0)(3)(15)(24)$, |
| $\tau^1 = \tau = (012345)$, | $\sigma\tau^1 = \sigma\tau = (05)(14)(23)$, |
| $\tau^2 = (024)(135)$, | $\sigma\tau^2 = (04)(13)(2)(5)$, |
| $\tau^3 = (03)(14)(25)$, | $\sigma\tau^3 = (03)(12)(45)$, |
| $\tau^4 = (042)(153)$, | $\sigma\tau^4 = (02)(1)(35)(4)$, |
| $\tau^5 = (054321)$, | $\sigma\tau^5 = (01)(25)(34)$. |

Diese Permutationen werden im Folgenden noch verwendet. Jedenfalls lässt sich die obige Formel $|\mathrm{Fix}(\tilde{g})| = f^k$ mit den Permutationstypen etwas umständlicher schreiben als:

$$|\mathrm{Fix}(\tilde{g})| = \prod_{i=1}^{n} f^{k(i)}$$

Zu einer weiteren (später nützlichen) Formalisierung kommt es mit dem **Zyklenzeiger** $\mathfrak{Z}(G)$ von $G$ (es handelt sich um ein Polynom in $z_1, \ldots, z_n$):

$$\mathfrak{Z}(G) := \frac{1}{|G|} \sum_{g \in G} t(g)$$

Die Bemerkung von Seite 45 lässt sich damit in kompakter Form schreiben:

**Satz:** Die Anzahl der (bezüglich $G$) wesentlich verschiedenen Färbungen von $A$ mit einer $f$-elementigen Farbenmenge beträgt genau

$$\mathfrak{Z}(G|f)$$

(Diese Zahl entsteht auf $\mathfrak{Z}(G)$ durch Einsetzen von $z_i = f$ für alle $z_i$ und anschließendes Ausrechnen.)

Es wird weiter das **Beispiel** $G = D_6$ betrachtet. Folgende Tabelle (abgeleitet von der Aufstellung aller Permutationen auf voriger Seite) hilft bei der Orientierung:

| Permutation | Zyklengestalt | (Permutations-)Typ |
|---|---|---|
| $\tau^0 = id$ | (x) (x) (x) (x) (x) (x) | $z_1^6$ |
| $\tau$, $\tau^5$ | (xxxxxx) | $z_6^1$ |
| $\tau^2$, $\tau^4$ | (xxx) (xxx) | $z_3^2$ |
| $\tau^3$, $\sigma\tau$, $\sigma\tau^3$, $\sigma\tau^5$ | (xx) (xx) (xx) | $z_2^3$ |
| $\sigma$, $\sigma\tau^2$, $\sigma\tau^4$ | (x) (x) (xx) (xx) | $z_1^2 z_2^2$ |

Also: $\mathfrak{Z}(D_6) = \frac{1}{12}(z_1^6 + 2z_6 + 2z_3^2 + 4z_2^3 + 3z_1^2 z_2^2)$. Einsetzen von $f = 2$ für alle $z_i$ liefert:

$$\mathfrak{Z}(D_6|2) = \frac{1}{12}(2^6 + 2 \cdot 2 + 2 \cdot 2^2 + 4 \cdot 2^3 + 3 \cdot 2^2 \cdot 2^2) = 13$$

Deshalb gibt es genau 13 wesentlich verschiedene Eckenfärbungen des regelmäßigen Sechsecks mit zwei gegebenen Farben. Insbesondere: Es gibt genau 13 wesentlich verschiedene Perlenketten mit insgesamt sechs Perlen und zwei Perlensorten (weiß, schwarz).

Das Beispiel ist klein, und man kann die 13 Ketten leicht finden.

Jetzt soll, ebenso systematisch, die Anzahl der Perlenketten mit drei schwarzen und drei weißen Perlen bestimmt werden. (Es wird auch klar werden, wie solche Berechnungen allgemein durchzuführen sind, für beliebige Permutationsgruppen $G$.) Es muss die Formel aus der Bemerkung von Seite 45 betrachtet werden:

$$\circledast \qquad b(\widetilde{G}) = \frac{1}{|\widetilde{G}|} \sum_{\widetilde{g} \in \widetilde{G}} |\mathrm{Fix}(\widetilde{g})|$$

aber mit $\widetilde{G}$ eingeschränkt auf die jetzt noch zulässigen Färbungen (nämlich dreimal schwarz, dreimal weiß). Die Bestimmung von $\mathrm{Fix}(\widetilde{g})$ gelingt wieder wie auf Seite 45: jeder Zyklus ist eiheitlich einzufärben. Beispiel: Sei

$$g = \sigma = (0)(3)(15)(24).$$

Für jede der Mengen $\{0\}, \{3\}, \{1,5\}, \{2,4\}$ muss man sich für schwarz oder weiß entscheiden. Hierfür gibt es (bei insgesamt drei schwarzen Perlen) genau vier Möglichkeiten, nämlich

$\{0\}$ und $\{1,5\}$ schwarz, $\{0\}$ und $\{2,4\}$ schwarz,
$\{3\}$ und $\{1,5\}$ schwarz, $\{3\}$ und $\{2,4\}$ schwarz.

Also liefert $g = \sigma$ den Beitrag 4 zur Summe in $\circledast$.

Dieses – und alles weitere – kann mit dem Zyklenzeiger $\mathfrak{Z}(G)$ ganz formelmäßig und ganz ohne Nachdenken berechnet werden (aber für den Fortgang der Theorie ist noch ein wenig Denkarbeit erforderlich):

**Definition:** Das einem Polynom $p(z_1, \ldots, z_n)$ **zugeordnete Polynom** entsteht, indem jedes $z_i$ durch $x_1^i + x_2^i$ ersetzt wird.

**Beispiel:** Immer noch $g = \sigma = (0)(3)(15)(24)$: Typ $t(\sigma) = z_1^2 z_2^2$, zugeordnetes Polynom $(x_1^1 + x_2^1)^2 (x_1^2 + x_2^2)^2$. Jede Klammer korrespondiert mit einer der „Zyklenmengen“:

$$\begin{array}{cccc} \{0\} & \{3\} & \{1,5\} & \{2,4\} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ (x_1 + x_2) & (x_1 + x_2) & (x_1^2 + x_2^2) & (x_1^2 + x_2^2) \end{array}$$

Jede Entscheidung „schwarz oder weiß“ für eine der Zyklenmengen entspricht einer Entscheidung „$x_1$ oder $x_2$“ in der zugehörigen Klammer. Dreimal schwarz,

dreimal weiß bedeutet: Ausmultiplizieren, Koeffizient von $x_1^3 x_2^3$ ist dann $|\mathrm{Fix}(\sigma)|$. Führt man dies mit dem gesamten Zyklenzeiger $\mathfrak{Z}(D_6)$ durch, ergibt sich die **erzeugende Funktion** (der Färbungen mit zwei Farben) von $D_6$:

$$\begin{aligned}\mathfrak{Z}(D_6|x_1^i + x_2^i) &= \frac{1}{12}\Big((x_1+x_2)^6 + 2(x_1^6+x_2^6) + 2(x_1^3+x_2^3)^2 \\ &+ 4(x_1^2+x_2^2)^3 + 3(x_1+x_2)^2(x_1^2+x_2^2)^2\Big) \\ &= 1\cdot x_1^6 + 1\cdot x_1^5 x_2 + 3\cdot x_1^4 x_2^2 + 3\cdot x_1^3 x_2^3 \\ &+ 3\cdot x_1^2 x_2^4 + 1\cdot x_1 x_2^5 + 1\cdot x_2^6\end{aligned}$$

Die Koeffizienten sind (wegen $\circledast$) tatsächlich die gesuchten Anzahlen. Es ergibt sich folgende Tabelle:

| Farbverteilung *schwarz* | Farbverteilung *weiß* | Anzahl der Färbungen *(Koeffizienten der erzeugenden Funktion)* |
|---|---|---|
| 6 | 0 | 1 |
| 5 | 1 | 1 |
| 4 | 2 | 3 |
| 3 | 3 | 3 |
| 2 | 4 | 3 |
| 1 | 5 | 1 |
| 0 | 6 | 1 |
| **Summe:** | | **13** |

Obige Argumentation klappt allgemein. Deshalb gilt folgender Satz (wurde 1937 von Pólya gefunden, der sich dafür interessierte, wieviele chemische Verbindungen mit einem vorgegebenen Bauplan es geben kann):

### 1.8.4 Satz von Pólya

Gegeben sei eine Permutationsgruppe $G$ auf $A$, $|A| = n$. Aus dem Zyklenzeiger $\mathfrak{Z}(G)$ entstehe das Polynom $\mathfrak{Z}(G \mid x_1^i + \cdots + x_f^i)$, indem für jedes $z_i$ der Ausdruck $x_1^i + \cdots + x_f^i$ substituiert wird ($i = 1, \ldots, n$). Dieses Polynom ist dann die erzeugende Funktion aller Färbungen mit $f$ Farben: Hierin gibt der Koeffizient von $x_1^{n(1)} \cdot \ldots \cdot x_f^{n(f)}$ die Anzahl der bezüglich $G$ wesentlich verschiedenen Färbungen von $A$ mit einer $f$-Farbenmenge $F = \{F_1, \ldots, F_f\}$ an, in denen die Farbe $F_i$ genau $n(i)$ mal vorkommt.

**Anmerkungen:**

- Man kann in $\mathfrak{Z}(G \mid x_1^i + \cdots + x_f^i)$ immer $x_f = 1$ setzen, ohne Information zu verlieren. Im Fall der Diedergruppe $D_6$ mit $f = 2$ Farben ergibt sich (mit $x_1 = x$, $x_2 = 1$): $\mathfrak{Z}(D_6 \mid x_1^i + x_2^i) = x^6 + x^5 + 3x^4 + 3x^3 + 3x^2 + x + 1$
- Der Satz von Pólya liefert noch einmal die Anzahl *aller* Färbungen, indem $x_i = 1$ gesetzt wird für alle $i$. Es ergibt sich wieder $\mathfrak{Z}(G \mid f)$ – vergleiche Seite 46.

# 2 Algebraische Strukturen

Dieses Kapitel beginnt mit einer Auflistung der wichtigsten und gebräuchlichsten algebraischen Strukturen. Dann werden die wichtigsten algebraischen Begriffe und Sprech- und Denkweisen vorgestellt. Der Bogen wird sich von einer einheitlichen Sprache, in der algebraische Strukturen definiert werden können (Grundmenge, Operationen, Ähnlichkeitstyp) über fortgeschrittene Begriffsbildungen (wie Unteralgebren, Homomorphismen, direkten Produkten, Kongruenzrelationen oder gleichungsdefinierten Klassen) bis zu Gleichungstheorien und Gleichungslogik spannen. Zum Abschluss des Kapitels werden dann Verbände und boolesche Algebren betrachtet, womit ein Übergang zum darauf folgenden (und letzten) Kapitel über Logik möglich ist.

## 2.1 Algebraische Strukturen: Beispiele

In diesem Abschnitt wird eine ganze Reihe der üblichsten algebraischen Strukturtypen mitsamt wichtigen Beispielen vorgestellt.

### 2.1.1 Operationen

**Definition:** Sei $A$ eine Menge und $n \in \mathbb{N}_0$. Dann heißt jede Abbildung

$$f\colon A^n \longrightarrow A$$

eine **n-stellige Operation** auf $A$. Solche Abbildungen (Operationen) werden oft in der Form $f(x_1, \ldots, x_n)$ geschrieben, wobei die Variablen $x_1, \ldots, x_n$ jeden Wert aus $A$ annehmen können.

**Beispiele:**

- Die übliche Addition „$+$“ auf $\mathbb{N}$ ist eine 2-stellige Operation auf $\mathbb{N}$. Anstelle von „$+(x_1, x_2)$“ wird, wie üblich, „$x_1 + x_2$“ geschrieben (**Infix**-Schreibweise).
- Definiert man $f(x_1, x_2, x_3) := x_1 + x_2 + x_3$, so erhält man eine 3-stellige Operation auf $\mathbb{N}$.
- Eine 1-stellige Operation auf $\mathbb{N}$ ist, zum Beispiel, gegeben durch $g(x) := x + 1$.
- Was ist eine 0-stellige Operation auf einer Menge $A$? Dabei handelt es sich um Abbildungen $A^0 \longrightarrow A$, wobei $A^0 = \{()\}$ gilt: Die Menge entält nur das „leere Tupel“ $()$. Solche Operationen hängen nicht von $A$ ab, das Resultat ist ein einziges Element $c \in A$, nämlich $f\big(()\big) = c$. Daher werden 0-stellige Operationen auch Konstanten (in $A$) genannt. Zum Beispiel $q \in \mathbb{N}$ ist eine Konstante in $\mathbb{N}$.
- 2-stellige Operationen auf kleineren Mengen können oft durch Verknüpfungstafeln dargestellt werden. Beim folgenden Beispiel handelt es sich um die „Addition modulo 4“ auf der Menge $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

### 2.1.2 Halbgruppen

**Definition:** Eine **Halbgruppe** (engl.: **semigroup**) ist ein Paar $(S;\cdot)$, bestehend aud aus einer Menge $S$ und einer 2-stelligen Operation $\cdot$ auf $S$, so dass in $S$ folgende Gleichung erfüllt ist:

(ass) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Assoziativität)

**Bemerkung:** Spricht man von „Gleichung auf $A$“, so meint man, dass die Gleichung für alle Elemente von $A$ gilt. Im Fall von Gleichung (ass) bedeutet das:

$$\forall x, y, z \in A\colon\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

**Typische Beispiele (Halbgruppe):** (a) Abbildungen auf einer Menge: Sei $A$ eine Menge, und sei $S$ die Menge aller Abbildungen $f\colon A \longrightarrow A$. Für je zwei Abbildungen $f, g \in S$ werde die Verkettung $f \circ g$ („$f$ nach $g$“) definiert durch

$$(f \circ g)(x) := f(g(x)) \quad \text{für alle } x \in A$$

Es gilt: Verkettung von Abbildungen ist assoziativ, das heißt $(S;\circ)$ ist eine Halbgruppe.

**Beweis:** Es ist für alle $f, g, h \in S$ zu zeigen, dass

$$(f \circ (g \circ h))(x) = ((f \circ g) \circ h)(x) \quad \text{für alle } x \in A$$

gilt. Doch dies ist einfach:

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)$$

(b) Wörter über einem Alphabet: Sei $A$ eine Menge (die jetzt ein **Alphabet** genannt wird). Jedes Tupel $(a_1, a_2, \ldots, a_n)$ wird jetzt kürzer als $a_1 a_2 \ldots a_n$ geschrieben und ein **Wort** von Länge $n$ äber $A$ genannt. Sei $A^*$ die Menge aller Wörter über $A$ (inklusive dem „leeren Wort“ $\lambda$ von Länge 0):

$$A^* := \bigcup_{n=0}^{\infty} A^n \ \ (= A^0 \cup A^1 \cup A^2 \cup \ldots)$$

Die **Konkatenation** (oder **Juxtaposition**) von zwei Wörtern $a_1 a_2 \ldots a_n$ und $b_1 b_2 \ldots b_m$ ist definiert als

$$(a_1 a_2 \ldots a_n) \cdot (b_1 b_2 \ldots b_m) := a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m$$

offensichtlich gilt: Konkatenation ist assoziativ, das heißt $(A^*;\cdot)$ ist eine Halbgruppe.

**Weitere Beispiele (Halbgruppe)**

- $(\mathbb{N};+)$, $(\mathbb{Z};+)$, $(\mathbb{Q};+)$, $(\mathbb{R};+)$, $(\mathbb{C};+)$ und $(\mathbb{N};\cdot)$, $(\mathbb{Z};\cdot)$, $(\mathbb{Q};\cdot)$, $(\mathbb{R};\cdot)$, $(\mathbb{C};\cdot)$ sind Halbgruppen.
- Matrixmultiplikation ist assoziativ: Bezeichne $M(\mathbb{R},n)$ die Menge aller $n \times n$-Matrizen über $\mathbb{R}$, dann ist $(M(\mathbb{R},n);\cdot)$ eine Halbgruppe.
- Sei $M_0(\mathbb{R},n) = \{A \in M(\mathbb{R},n) \mid \det A = 0\}$. Dann ist $(M_0(\mathbb{R},n);\cdot)$ eine Halbgruppe.
- Übung: Zeige, dass die Verknüpfungstafel eine Halbgruppenoeration angibt. (Hinweis: Assoziativität muss mit einem geeigneten Argument nachgewiesen werden, nicht indem alle $4^3 = 64$ Möglichkeiten durchprobiert werden.)

### 2.1.3 Monoide

**Definition, Version A:** Eine Halbgruppe $(M;\cdot)$ wird ein **Monoid** genannt, falls ein **neutrales Element** existiert, das heißt falls

$$\exists 1 \in M \;\; \forall x \in M\colon \;\; x \cdot 1 = x = 1 \cdot x$$

Bei dieser Regel handelt es sich um keine Gleichung (das heißt um keine zwei Gleichungen), da sie einen Existenzquantor enthält. Doch sie kann in eine Gleichung umgewandelt werden, indem das neutrale Element zu einer nullstelligen Operation gemacht wird:

**Definition, Version B:** Ein Tripen $(M;\cdot,1)$ wird ein **Monoid** genannt, falls $(M;\cdot)$ eine Halbgruppe ist und 1 eine nullstellige Operation, die die folgenden Eigenschaften erfüllt:

(neut) $x \cdot 1 = x = 1 \cdot x$ (Assoziativität)

**Typische Beispiele (Monoid):** Die Beispiele in „Typische Beispiele (Halbgruppe)“ sind Monoide:

- Sei wieder $S$ die Menge aller Abbildungen $A \longrightarrow A$, und beizeichne $id_A$ die identische Abbildung auf $A$: $id_A(x) = x$ für alle $x \in A$. Dann: $(S;\circ,id_A)$ ist ein Monoid.
- Sei $A^*$ die Menge aller Wörter über einem Alphabet $A$. Mit Konkatenation $\cdot$ und dem leeren Wort $\lambda$ gilt: $(A^*;\cdot,\lambda)$ ist ein Monoid.

Im weiteren Lauf dieses Kapitels werden „Version B“-Typ Definitionen bevorzugt. Im folgenden Abschnitt wird dann, als allgemeiner Begriff, eine (allgemeine) Algebra definiert, als Menge mit Operationen und weiteren Ordungsmerkmalen auf Operationen.

Doch zunächst weitere wichtige Beispiele algebraischer Strukturen. Hierbei wird der Typ einer algebraischen Struktur verwendet, das heißt die Folge der Stelligkeiten der Operationen:

### 2.1.4 Gruppen

**Definition:** Eine Algebra $(G; \cdot, ^{-1}, 1)$ von Typ $(2, 1, 0)$ (das heißt mit 2-stelliger Operation $\cdot$, mit 1-stelliger Operation $^{-1}$, 0-stelliger Operation 1) heißt **Gruppe**, falls $(G; \cdot, 1)$ ein Monoid ist und außerdem folgende Gleichungen gelten:

(inv) $x \cdot x^{-1} = 1 = x^{-1} \cdot x$ (inverse Elemente)

**Typische Beispiele (Gruppe)**

- Permutationen: Sei $A$ eine Menge und $S_A$ die Menge aller Permutationen auf $A$ (siehe Kapitel 1). Dann ist $(S_A; \circ, ^{-1}, id_A)$ eine Gruppe, genannt die **symmetrische Gruppe** auf $A$.
- Symmetrie: Im vorigen Abschnitt wurden Symmetrien geometrischer Figuren als Permutationen gewisser Punktmengen interpretiert. Als Beispiele wurden die Diedergruppen $(D_n; \circ, ^{-1}, id)$ betrachtet (Symmetriegruppen regelmäßiger $n$-Ecke).

**Weitere Beispiele (Gruppen)**

- $(\mathbb{Z}; +, -, 0)$ ist eine Gruppe mit den üblichen Operationen auf $\mathbb{Z}$ (insbesondere der 1-stelligen Operation $x \mapsto -y$).
- Für $n \in \mathbb{N}$ sei $(\mathbb{Z}_n; +, -, 0)$ eine Gruppe (mit $+$ und $-$ modulo $n$).
- Sei $G(\mathbb{R}, n)$ die Menge aller reellen $n \times n$-Matrizen von Determinante ungleich 0, $G(\mathbb{R}, n) = \{A \in M(\mathbb{R}, n) \mid \det(A) \neq 0\}$.

  Dann ist $(G(\mathbb{R}, n); \cdot, ^{-1}, E_n)$ eine Gruppe, genannt die **allgemeine lineare Gruppe** über $\mathbb{R}$. (Hierbei sei $\cdot$ die übliche Matrizenmultiplikation, $A^{-1}$ die inverse Matrix zu $A$ und $E_n$ die $n \times n$-Einheitsmatrix.)

Eine zweistellige Operation $x \cdot y$ auf einer Menge $A$ wird **kommutativ** genannt, falls folgende Gleichung auf $A$ gilt:

(kom) $x \cdot y = y \cdot x$ (Kommutativität)

Es ist klar, was man unter einer kommutativen Halbgruppe, einem kommutativen Monoid, einer kommutativen Gruppe versteht. Kommutative Gruppen werden üblicherweise abelsche Gruppen genannt.

### 2.1.5 Ringe

**Definition:** Eine Algebra $(R; +, -, 0, \cdot)$ von Typ $(2, 1, 0, 1)$ heißt ein Ring, falls $(R; +, -, 0)$ eine abelsche Gruppe und $(R; \cdot)$ eine Halbgruppe ist, so dass die Operationen $+$ und $\cdot$ durch folgende Gleichungen „verbunden“ sind:

(dist) $x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$ (Distributivität)

Ein **kommutativer Ring** ist ein Ring, in dem die Multiplikation $\cdot$ kommutativ ist. Ein **unitärer Ring** ist ein Ring mit einer zusätzlichen nullstelligen Operation 1, so dass $(R, \cdot)$ ein Monoid ist.

**Bemerkung:** Der Multiplikationspunkt $\cdot$ wird oft ewggelassen, das heißt $xy$ statt $x \cdot y$ geschrieben. Deshalb kann das erste Distributivgesetz als $x(y+z) = xz + yz$ geschrieben wreden. Die Regel „Punktrechnung vor Strichrechnung“ versteht sich von selbst.

**Typische Beispiele (Ring)**

- Ring der ganzen Zahlen: $(\mathbb{Z}; +, -, 0, \cdot, 1)$ ist ein kommutativer unitärer Ring. Dasselbe gilt für $(\mathbb{Z}_n; +, -, 0, \cdot, 1)$ mit $Z_n = \{0, 1, \ldots, n\}$ und allen Operationen modulo $n$.
- Polynomringe: Mit $\mathbb{R}[x]$ werde die Menge der reellen Polynome in der Variablen $x$ bezeichnet:

  $$\mathbb{R}[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid n \in \mathbb{N}_0, a_n, \ldots, a_1, a_0 \in \mathbb{R}\}$$

  (Achtung: Hierbei ist $x$ keine Zahl, sondern ein Symbol. Deshalb sind auch die Plynome keine Zahlen, sondern „formale Ausdrücke“.) Mit den üblichen Operationen ist $\mathbb{R}[x]$ ein kommutativer unitärer Ring.
- Matrixringe: Die Menge $M(\mathbb{R}, n)$ aller reellen $n \times n$-Matrizen bilden mit der üblichen Matrixaddition und -multiplikation einen unitären Ring, der für $n \geq 2$ nicht kommutativ ist.

### 2.1.6 Körper

Ein **Körper** ist ein unitärer Ring $(K; +, -, 0, \cdot, 1)$ mit zusätzlicher einstelliger Operation $^{-1}$ auf $K \setminus \{0\}$, so dass $(K \setminus \{0\}; \cdot, ^{-1}, 1)$ eine Gruppe ist. Ist die Multiplikationsoperation $\cdot$ kommutativ, so spricht man von einem **kommutativen Körper**.

**Beispiele (Körper):** Mit den üblichen Operationen sind die Mengen $\mathbb{C}$, $\mathbb{R}$, $\mathbb{C}$ kommutative Körper. Beispielsweise ist $\mathbb{Z}$ kein Körper, da es keine multiplikativen Inversen gibt (außer für $x = 1$ und $x = -1$).

Einige Tatsachen über Körper (ohne Beweise):

- $Z_n$ ist genau dann ein Körper, wenn $n$ eine Primzahl ist.
- Ein Körper $K$ mit $|K| = n$ Elementen existiert genau dann, wenn $n$ eine Primzahlpotenz ist (das heißt von der Form $n = p^r$ mit einer Primzahl $p$ und $r \in N$).
- Für jede Primzahlpotenz $q = p^r$ gibt es genau einen Körper mit $q$ Elementen (bis auf Isomorphie).
- Alle endlichen Körper sind kommutativ (nicht leicht zu beweisen!)
- Es ist schwierig, nicht-kommutative Körper zu finden.

### 2.1.7 Vektorräume

**Definition:** Sei $K$ ein Körper und sei $(V; +, -, 0, K)$ eine Algebra vom Typ $\big(2, 1, 0, (1)_{k\in K}\big)$, mit einer einstelligen Operation $x \mapsto kx$ für jedes Körperelement $k \in K$. Dann heißt diese Algebra ein **Vektorraum** über $K$, falls $(V; +, -, 0)$ eine abelsche Gruppe ist und für alle $k, \ell \in K$ die folgenden Gleichungen gelten:

(Vekt1) $k(x + y) = kx + ky$
(Vekt2) $(k + \ell)x = kx + \ell x$
(Vekt3) $\big(k(\ell x)\big) = (k\ell)x$
(Vekt4) $1x = x$

**Einige Tatsachen über Vektorräume (ohne Beweise):**

- Eine **Basis** eines Vektorraums $V$ (über $K$) ist eine Teilmenge $B \subseteq V$, so dass jedes $v \in V$ auf *genau eine Art* in der Form

$$v = k_1 b_1 + \cdots + k_r b_r$$

  darstellbar ist, mit unterschiedlichen $b_1, \ldots, b_r \in B$ und $k_1, \ldots, k_r \in K$.

- Falls $B$ eine Basis von $V$ ist, dann nennt man $|B|$ die **Dimension** von $V$. Die Dimension ist *wohldefiniert*: Sind $B$ und $C$ Basen von $V$, dann gilt $|B| = |C|$.

- Jeder Vektorraum besitzt eine Basis.

- Ist $V$ ein Vektorraum über $K$ von *endlicher Dimension* $d$, dann ist $V$ **isomorph** zu $F^d$: $V \cong F^d$

**Typische Beispiele für Vektorräume:**

- Die **reelle Ebene**: Sei $V := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$, wobei hier die Elemente von $V$ als **Spaltenvektoren** geschrieben sind. Dann ist $V$ mit der üblichen Vektoraddition $v + w$ und Skalarmultiplikation $kv$ ein **Vektorraum** über $\mathbb{R}$. Dieser Vektorraum ist 2-dimensional, also $\dim(V) = 2$. Er hat $B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ als **kanonische Basis**: Jedes $v = \begin{pmatrix} x \\ y \end{pmatrix} \in V$ kann in der Form $v = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ geschrieben werden. Entsprechend gibt es die **$n$-dimensionalen reellen Räume** $\mathbb{R}^n$.

- **Polynome von Grad kleiner $n$:** Sei $P_n$ die Menge aller reellen Polynome von Grad kleiner $n$,

$$P_n = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}\}$$

  Definiert man wie üblich für alle $p = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ und $q = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$:

$$\begin{aligned} p + q &:= (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0) \\ rp &:= (ra_{n-1})x^{n-1} + \cdots + (ra_1)x + (ra_0) \end{aligned}$$

Dann erhält man einen **Vektorraum** $(P_n; +, -, 0, \mathbb{R})$ über $\mathbb{R}$. Die Polynome $p_0(x) = 1, p_1(x) = x, p_2(x) = x^2, \ldots, p_{n-1}(x) = x^{n-1}$ bilden eine Basis von $P_n$, deshalb gilt $\dim(P_n) = n$. Ein Isomorphismus $\varphi: P_n \longrightarrow \mathbb{R}^n$ wird durch folgende „Umbenennung“ gegeben:

$$\varphi(a_{n-1}x^{n-1} + \cdots + a_1x + a_0) := \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$$

Alle bisher in diesem Abschnitt vorgestellten Algebren beziehungsweise Klassen von Algebren sind verwandt zueinander: Jeder Vektorraum „enthält“ einen Körper (und eine Gruppe), jeder Körper ist ein (genauer: „enthält“ einen) Ring, jeder Ring enthält eine Gruppe (und eine Halbgruppe), jede Gruppe ist ein Monoid, und - schließlich - ist jedes Monoid eine Halbgruppe. Natürlich gibt es viele weitere und auch ganz andere Klassen von Algebren. In diesem Kapitel werden später noch Beispiele vorgestellt, zum Beispiel **Verbände** und **boolesche Algebren**.

## 2.2 Allgemeine Algebren: Definition und strukturelle Grundbegriffe

Natürlich darf man sich unter einer **Algebra** zunächst einmal ein Gebilde der Form $\underline{A} = (A; F)$ vorstellen, wobei $A$ eine Menge und $F$ eine Menge endlichstelliger Operationen auf $A$ ist. Alle Algebren sind von dieser Bauart, insbesondere alle Beispiele des vorigen Abschnitts. Will man aber Algebren miteinander in Beziehung setzen (zum Beispiel, weil sie verwandt zueinander sind), empfiehlt sich eine „detailliertere“ Sprache:

### 2.2.1 Ähnlichkeitstyp, allgemeine Algebren

**Definition:** Unter einem **(Ähnlichkeits-)Typ** versteht man ein geordnetes Paar $(\mathcal{F}, \sigma)$, wobei $\mathcal{F}$ eine Menge ist (Menge der **Operationssymbole**) und $\sigma: \mathcal{F} \longrightarrow \mathbb{N}_0$ eine Abbildung, die jedem $f \in \mathcal{F}$ eine **Stelligkeit** $\sigma(f)$ zuordnet. Man nennt $f$ dann ein **$\sigma(f)$-stelliges Operationssymbol**.

Eine **allgemeine Algebra** (kurz: **Algebra**) vom Typ $(\mathcal{F}, \sigma)$ ist ein geordnetes Paar $\underline{A} = (A; F)$, bestehend aus einer Menge $A$ und einer Familie

$$F = (f_{\underline{A}}) \mid f \in \mathcal{F})$$

von Operationen auf $A$, wobei jedem Operationssymbol $f \in \mathcal{F}$ eine $\sigma(f)$-stellige Operation $f_{\underline{A}}$ auf $A$ zugeordnet wird. Die Menge $A$ heißt **Grundmenge** von $\underline{A}$ und die Elemente von $F$ heißen die **fundamentalen Operationen** von $\underline{A}$.

**Beispiel:** Als erstes Beispiel für diese Notationen und Sprechweisen wird die **Gruppe** $(\mathbb{Z}; +, -, 0)$ betrachtet (siehe Seite 52). Da diese Gruppe *im Rahmen aller Gruppen* betrachtet werden soll, wird der **Typ**

$$(\mathcal{F}, \sigma) \quad \text{mit} \quad \mathcal{F} = \{\cdot, ^{-1}, 1\}, \quad \sigma(\cdot) = 2, \quad \sigma(^{-1}) = 1, \quad \sigma(1) = 0$$

gewählt. Die zu betrachtende Gruppe ist $\underline{\mathbb{Z}} = (\mathbb{Z}; \{+, -, 0\})$. Die verwendeten *fundamentalen Operationen* sind

$$\cdot_{\underline{z}} = +, \qquad {}^{-1}{}_{\underline{z}} = -, \qquad 1_{\underline{z}} = 0$$

wobei $x + y$, $-x$, 0 auf $\mathbb{Z}$ wie üblich definiert sind. Insbesondere gilt: *Keiner hält einen davon ab, gebräuchliche, einfache Symbole für die Operationen zu verwenden, solange keine Missverständnisse drohen*, also zum Beispiel „+“ anstelle von „$\cdot_{\underline{z}}$“. Statt $(\mathbb{Z}; \{+, -, 0\})$ schreibt man natürlich - unter Einsparung von Klammern - meist $(\mathbb{Z}; +, -, 0)$.

Aus schon vorhandenen Algebren können auf mehrere Arten „neue“ Algebren gewonnen werden. Ein Art ist die folgende:

### 2.2.2 Unteralgebren

**Definition:** Sei $\underline{A} = (A; F)$ eine Algebra vom Typ $(\mathcal{F}, \sigma)$ und $B \subseteq A$ eine Teilmenge von $A$, so dass für alle $f \in \mathcal{F}$ und alle $n$-Tupel $(b_1, \ldots, b_n) \in B^n$ mit $n = \sigma(f)$ folgendes gilt:

$$f_{\underline{A}}(b_1, \ldots, b_n) \in B$$

Die Algebra $\underline{B} = \big(B; (f_{\underline{B}} \mid f \in \mathcal{F})\big)$ heißt dann eine **Unteralgebra** von $A$, wobei $f_{\underline{B}}$ für alle $f \in \mathcal{F}$ die Einschränkung der Operation $f_{\underline{A}}$ auf die Menge $B$ bedeutet. Für „$\underline{B}$ ist Unteralgebra von $\underline{A}$“ schreibt man auch $B \leqslant A$. Die Menge aller Grundmengen von Unteralgebren von $\underline{A}$ wird mit $\mathrm{Sub}(\underline{A})$ bezeichnet, $\mathrm{Sub}(\underline{A}) = \{B \mid \underline{B} \leqslant \underline{A}\}$.

Eine Teilmenge $B \subseteq A$ ist genau dann die Grundmenge einer Unteralgebra von $\underline{A} = (A; F)$, wenn $B$ unter allen fundamentalen Operationen $f_{\underline{A}} \in F$ abgeschlossen ist. Man schreibt dann oft $\underline{B} = (B; F)$, ohne zwischen den Operationsfamilien $F$ in $\underline{A}$ und $F$ in $\underline{B}$ zu unterscheiden. Außerdem bezeichnet man sowohl $f_{\underline{A}}$ als auch $f_{\underline{B}}$ einfach mit dem Operationssymbol $f$.

Am Beispiel der Gruppen lässt sich deutlich machen, dass es bei den Unteralgebren auf den zugrundeliegenden Typ ankommen kann. Betrachtet man Gruppen als Algebren vom Typ $(2, 1, 0)$ (das heißt mit diesem Stelligkeiten für die Operationen) wie auf Seite 51, dann handelt es sich bei den Unteralgebren genau um die Untergruppen. Betrachtet man Gruppen hingegen als Algebren vom Typ (2) (mit der Gruppenmultiplikation als einziger Operation), dann kann es Unteralgebren geben, die keine Unteralgebren sind:

**Beispiel:** Die Algebra $(\mathbb{Z}; +)$ mit der üblichen Addition hat die Menge $\mathbb{N}_0$ der nichtnegativen ganzen Zahlen als Grundmenge einer Unteralgebra, obwohl $\mathbb{N}_0$ nicht die Grundmenge einer Unteralgebra von $(\mathbb{Z}; +, -, 0)$ ist.

Für jede Algebra ist das System der (Grundmengen von) Unteralgebren **gegen Durchschnittsbildung abgeschlossen**:

**Bemerkung:** Sei $\underline{A} = (A; F)$ eine Algebra. Dann gilt:

(a) $A \in \mathrm{Sub}(\underline{A})$
(b) $\bigcap \mathcal{B} \in \mathrm{Sub}(\underline{A})$ für jede nichtleere Teilmenge $\mathcal{B} \subseteq \mathrm{Sub}(\underline{A})$

**Beweis:** (a) ist klar. Für den Nachweis von (b) sei $\mathcal{B} \subseteq \mathrm{Sub}(\underline{A})$, $\mathcal{B} \neq \emptyset$. Es ist zu zeigen, dass $\bigcap \mathcal{B}$ unter allen fundamentalen Operationen $f$ von $\underline{A}$ abgeschlossen ist. Sei $n = \sigma(f)$. Aus $b_1, \ldots, b_n \in \bigcap \mathcal{B}$ folgt $b_1, \ldots, b_n \in B$ für alle $B \in \mathcal{B}$. Da alle $B \in \mathcal{B}$ Grundmengen von Unteralgebren sind, gilt $f(b_1, \ldots, b_n) \in B$ für alle $B \in \mathcal{B}$ Es folgt $f(b_1, \ldots, b_n) \in \bigcap \mathcal{B}$. □

**Folgerung:** Für jede Algebra $\underline{A} = (A; F)$ und jede Teilmenge $X \subseteq A$ ist

$$\langle X \rangle := \bigcap \{B \in \mathrm{Sub}(\underline{A}) \mid B \supseteq X\}$$

die Grundmenge einer Unteralgebra von $\underline{A}$, das heißt es gilt $\langle X \rangle \in \mathrm{Sub}(\underline{A})$. Offenbar ist $\langle X \rangle$ die kleinste $X$ umfassende Grundmenge einer Unteralgebra von $\underline{A}$ (nämlich der von $X$ *erzeugten Unteralgebra*).

**Beispiel:** Es wird die Gruppe $(\mathbb{Z}_6; +, -, 0)$ betrachtet. Mit den Elementen von $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ wird *modulo* 6 gerechnet. Es gilt: $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \mathbb{Z}_6$, $\langle 2 \rangle = \{0, 2, 4\}$, $\langle 3 \rangle = \{0, 3\}$, $\langle 2, 3 \rangle = \mathbb{Z}_6$. Übrigens sind das *alle* Grundmengen von Unteralgebren!

**Bemerkung:** Sei $\underline{A} = (A; F)$ eine Algebra. Für alle Teilmengen $X, Y \subseteq A$ gilt:

| | | |
|---|---|---|
| (a) | $X \subseteq \langle X \rangle$ | **Extensivität** |
| (b) | $X \subseteq Y \Rightarrow \langle X \rangle \subseteq \langle Y \rangle$ | **Monotonie** |
| (c) | $\langle \langle X \rangle \rangle = \langle X \rangle$ | **Idempotenz** |

Der Beweis ergibt sich unmittelbar aus der Definition des Operators $\langle\ \rangle$. □

Man erhält $\langle X \rangle$ tatsächlich durch einen **Erzeugungsprozess** aus $X$. Dazu werde definiert:

$$E^0(X) := X$$
$$E(X) := X \cup \{f(a_1, \ldots . a_n) \mid f \in F, a_1, \ldots, a_n \in X\} \quad \text{mit } n = \sigma(f)$$
$$E^{k+1}(X) := E\big(E^k(X)\big) \quad \text{für alle } k \in \mathbb{N}_0$$

**Satz:** Für jede Algebra $\underline{A} = (A; F)$ und jede Teilmenge $X \subseteq A$ gilt:

$$\langle X \rangle = \bigcup_{k=0}^{\infty} E^k(X)$$

**Beweis:** $\supseteq$: Mit *Induktion über* $k$ wird $\langle X \rangle \supseteq E^k(X)$ gezeigt.
$k = 0$: $\langle X \rangle \supseteq X = E^0(X)$ ist klar. Jetzt werde $\langle X \rangle \supseteq E^k(X)$ vorausgesetzt, um $\langle X \rangle \supseteq E^{k+1}(X)$ zu zeigen. Sei $a \in E^{k+1}(X)$, aber $a \notin E^k(X)$. Dann gibt es $a_1, \ldots, a_n \in E^k(X)$ und $f \in F$ mit $f(a_1, \ldots, f_n) = a$. Wegen $E^k(X) \subseteq \langle X \rangle$, und da $\langle X \rangle$ die Grundmenge einer Unteralgebra ist, folgt $a \in \langle X \rangle$, insgesamt also $E^{k+1}(X) \subseteq \langle X \rangle$. Hiermit folgt $\langle X \rangle = \bigcup_{k=0}^{\infty} E^k(X)$.

$\subseteq$: Es muss gezeigt werden, dass $\bigcup_{k=0}^{\infty} E^k(X)$ die Grundmenge einer Unteralgebra ist. Seien also $a_1, \ldots, a_n \in \bigcup_{k=0}^{\infty} E^k(X)$ und $f \in F$ (mit $\sigma(f) = n$). Dann

gibt es für jedes $a_i$ ein $k(i) \in \mathbb{N}_0$ mit $a_i \in E^{k(i)}(X)$. Sei $m := \max\{k(i) \mid i = 1, \ldots, n\}$. Es gilt $a_i \in E^m(X)$ für alle $i = 1, \ldots, n$. Es folgt sofort

$$f(a_1, \ldots, a_n) \in E^{m+1}(X) \subseteq \bigcup_{k=0}^{\infty} E^k(X)$$

das heißt die letzte Menge ist abgeschlossen unter allen Operationen $f$. □

Der letzte Satz und die beiden vorangegangenen Bemerkungen geben Aufschluss über das Verhalten der **Mengensysteme** $\mathrm{Sub}(\underline{A})$. Dies wird im folgenden Einschub behandelt:

### 2.2.3 Hüllensysteme, Hüllenoperatoren, Verbände

Alle drei Begriffe der Überschrift spielen bezüglich Unteralgebren eine große Rolle. Zwei dieser Begriffe kamen oben schon vor, der dritte („**Verband**“) noch nicht. Diese Begriffe sind aber auch in vielen anderen Zusammenhängen wichtig.

**Definition:** Sei $A$ eine Menge und $\mathcal{M}$ eine Menge von Teilmengen von $A$, also $\mathcal{M} \subseteq \mathcal{P}A$. Dann nennt man $\mathcal{M}$ ein **Mengensystem** auf $A$. Ein Mengensystem $\mathcal{H} \subseteq \mathcal{P}(A)$ heißt **Hüllensystem** auf $A$, falls

(1) $A \in \mathcal{H}$
(2) $\bigcap \mathcal{B} \in \mathcal{H}$ für jede nicht leere Teilmenge $\mathcal{B} \subseteq \mathcal{H}$

Die Elemente $H \in \mathcal{H}$ werden **Hüllen** genannt.

**Beispiele:**

- Für jede Algebra $\underline{A}$ ist $\mathrm{Sub}(\underline{A})$ ein Hüllensystem auf der Grundmenge $A$.
- Die konvexen Teilmengen von $\mathbb{R}^n$ bilden ein Hüllensystem.
- Für jede Menge $A$ ist $\{A\} \cup \{E \subseteq A \mid E \text{ endlich}\}$ ein Hüllensystem auf $A$.
- Für jede Menge $A$ ist die Menge $\mathrm{Eq}(A)$ aller Äquivalenzrelationen auf $A$ ein Hüllensystem auf $A^2$

**Definition:** Sei $A$ eine Menge. Eine Abbildung

$$\mathcal{C}\colon \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$$

wird **Hüllenoperator** auf $A$ genannt, falls für alle Teilmengen $X, Y \subseteq A$ folgendes gilt:

| | | |
|---|---|---|
| (i) | $X \subseteq \mathcal{C}(X)$ | **Extensitivität** |
| (ii) | $X \subseteq Y \;\Rightarrow\; \mathcal{C}(X) \subseteq \mathcal{C}(Y)$ | **Monotonie** |
| (iii) | $\mathcal{C}\big(\mathcal{C}(X)\big) = \mathcal{C}(X)$ | **Idempotenz** |

Man nennt die Mengen der Form $\mathcal{C}(X)$ **abgeschlossen** und sagt, $\mathcal{C}(X)$ ist von $X$ **erzeugt**.

Klar ist: Für jede Algebra $\underline{A}$ ist der Operator $\langle\ \rangle_{\underline{A}}$ ein Hüllenoperator (siehe Seite 57). Hüllensysteme und Hüllenoperatoren sind in folgendem Sinn im wesentlichen das selbe:

**Bemerkung:** Sei $\mathcal{H}$ ein Hüllensystem auf einer Menge $A$. Für alle $X \subseteq A$ sei

$$\mathcal{C}_{\mathcal{H}}(X) := \bigcap \{H \in \mathcal{H} \mid H \supseteq X\}.$$

Dann ist $\mathcal{C}_{\mathcal{H}}$ ein Hüllenoperator auf $A$, und die abgeschlossenen Mengen von $\mathcal{C}_{\mathcal{H}}$ sind gerade die Hüllen von $\mathcal{H}$.

Sei umgekehrt $\mathcal{C}$ ein Hüllenoperator auf $A$. Dann ist

$$\mathcal{H}_{\mathcal{C}} := \{\mathcal{C}(X) \mid X \subseteq A\}$$

ein Hüllensystem auf $A$, und die Hüllen von $\mathcal{H}_{\mathcal{C}}$ sind gerade die abgeschlossenen Mengen von $\mathcal{C}$.

Allerdings haben Unteralgebren-Hüllenoperatoren und Unteralgebren-Hüllensysteme noch weitere Eigenschaften:

**Definition:** Ein Mengensystem $\mathcal{M}$ heißt **induktiv**, falls für jedes nach oben gerichtete Teilsystem $\mathcal{G} \subseteq \mathcal{M}$ gilt:

$$\bigcup \mathcal{G} \in \mathcal{M}$$

(Dabei ist $\mathcal{G}$ *nach oben gerichtet*, falls es für alle $X, Y \in \mathcal{G}$ immer ein $Z \in \mathcal{G}$ gibt mit $X \cup Y \subseteq Z$.) Ein Hüllenoperator $\mathcal{C}$ auf $A$ heißt **induktiv**, falls für alle Teilmengen $X \subseteq A$ folgendes gilt:

$$\mathcal{C}(X) = \bigcup \{\mathcal{C}(E) \mid E \subseteq X, E \text{ endlich}\}$$

Induktivität ist für Mengensysteme und für Hüllensysteme ganz unterschiedlich definiert. Handelt es sich beim Mengensystem aber um ein Hüllensystem, dann stimmen beide Definitionen überein:

**Beobachtung:** Ein Hüllensystem $\mathcal{H}$ ist genau dann induktiv, wenn der zugehörige Hüllenoperator $\mathcal{C}_{\mathcal{H}}$ induktiv ist.

**Beweis:** „⇒“ Sei $\mathcal{H}$ ein induktives Hüllensystem auf $A$ und sei $X \subseteq A$. Offenbar gilt $X \subseteq \bigcup \{\mathcal{C}_{\mathcal{H}}(E) \mid E \subseteq X, E \text{ endlich}\} \subseteq \mathcal{C}_{\mathcal{H}}(X)$. Offenbar ist das Teilsystem $\{\mathcal{C}_{\mathcal{H}}(E) \mid E \subseteq X, E \text{ endlich}\} \subseteq \mathcal{H}$ nach oben gerichtet, denn für je zwei endliche Mengen $E_1, E_2 \subseteq X$ gilt $\mathcal{C}_{\mathcal{H}}(E_1) \cup \mathcal{C}_{\mathcal{H}}(E_2) \subseteq \mathcal{C}_{\mathcal{H}}(E_1 \cup E_2)$. Da $\mathcal{H}$ als induktiv vorausgesetzt ist, folgt $\bigcup \{\mathcal{C}_{\mathcal{H}}(E) \mid E \subseteq X, E \text{ endlich}\} \in \mathcal{H}$ und daher $\mathcal{C}_{\mathcal{H}}(X) = \bigcup \{\mathcal{C}_{\mathcal{H}}(E) \mid E \subseteq X, E \text{ endlich}\}$. Damit is der Hüllenoperator $\mathcal{C}_{\mathcal{H}}$ als induktiv nachgewiesen.

„⇐“ Werde nun der Hüllenoperator $\mathcal{C}_{\mathcal{H}}$ als induktiv vorausgesetzt. Sei das Teilsystem $\mathcal{G} \subseteq \mathcal{H}$ nach oben gerichtet. Es muss $\bigcup \mathcal{G} \in \mathcal{H}$ gezeigt werden: Für jede endliche Teilmenge $E = \{e_1, \ldots, e_n\}$ von $\bigcup \mathcal{G}$ gibt es $G_1, \ldots, G_n \in \mathcal{G}$ mit $e_1 \in G_1, \ldots, e_n \in G_n$, das heißt mit $E \subseteq G_1 \cup \ldots \cup G_n$. Da $\mathcal{G}$ nach oben gerichtet ist und $G_1 \cup \ldots \cup G_n$ eine *endliche* Vereinigung ist, gibt es eine Menge $G_E \in \mathcal{G}$ mit $G_1 \cup \ldots \cup G_n \subseteq G_E$. Also gilt $E \subseteq G_E$ und $\mathcal{C}_{\mathcal{H}}(E) \subseteq \mathcal{C}_{\mathcal{H}}(G_E) = G_E$. Mit der Induktivität von $\mathcal{C}_{\mathcal{H}}$ folgt jetzt:

$$\begin{aligned} \mathcal{C}_{\mathcal{H}}\left(\bigcup \mathcal{G}\right) &= \bigcup \{\mathcal{C}_{\mathcal{H}}(E) \mid E \subseteq X, E \text{ endlich}\} \\ &\subseteq \bigcup \{G_E \mid E \subseteq \bigcup \mathcal{G}, E \text{ endlich}\} \\ &\subseteq \bigcup \mathcal{G} \end{aligned}$$

Wegen der Extensivität von $\mathcal{C}_\mathcal{H}$ folgt $\mathcal{C}_\mathcal{H}(\bigcup \mathcal{G}) = \bigcup \mathcal{G}$, was gleichbedeutend ist mit $\bigcup \mathcal{G} \in \mathcal{H}$. □

**Satz:** (a) Für jede Algebra $\underline{A} = (A, F)$ ist $\mathrm{Sub}(\underline{A})$ ein induktives Hüllensystem, und $\langle\ \rangle_{\underline{A}}$ ist ein induktiver Hüllenoperator.

(b) Umgekehrt gibt es zu jedem induktiven Hüllensystem $\mathcal{H}$ auf $A$ eine Algebra $\underline{A} = (A, F)$ mit $\mathcal{H} = \mathrm{Sub}(\underline{A})$ und $\mathcal{C}_\mathcal{H} = \langle\ \rangle_{\underline{A}}$.

**Beweis:** (a) Sei $\mathcal{G} \subseteq \mathrm{Sub}(\underline{A})$ nach oben gerichtet. Es ist $\bigcup \mathcal{G} \in \mathrm{Sub}(\underline{A})$ nachzuweisen. Sei $f \in F$ ($n$-stellig) und $b_1, \ldots, b_n \in \bigcup \mathcal{G}$. Dann gibt es $G_1, \ldots G_n \in \mathcal{G}$ mit $b_1 \in G_1, \ldots, b_n \in G_n$. Da $\mathcal{G}$ nach oben gerichtet ist, gibt es ein $G \in \mathcal{G}$ mit $G_1 \cup \cdots \cup G_n \subseteq G$, also mit $b_1, \ldots b_n \in G$. Wegen $G \in \mathrm{Sub}(\underline{A})$ folgt $f(b_1, \ldots, b_n) \in G$. Damit ist $\bigcup \mathcal{G} \in \mathrm{Sub}(\underline{A})$ gezeigt. Die Induktivität von $\langle\ \rangle_{\underline{A}}$ folgt aus der von $\mathrm{Sub}(\underline{A})$.

(b) Es wird eine Algebra $\underline{A}$ mit $\mathcal{C}_\mathcal{H} = \langle\ \rangle_{\underline{A}}$ definiert. ($\mathcal{H} = \mathrm{Sub}(\underline{A})$ ist dann automatisch erfüllt): Für jede endliche Teilmenge $E = \{e_1, \ldots e_n\}$ von $A$ und jedes $b \in \mathcal{C}_\mathcal{H}(E)$ wird eine $n$-stellige Operation $f_{E,b}$ auf $A$ definiert:

$$f_{E,b}(x_1, \ldots, x_n) := \begin{cases} b & \text{falls } \{x_1, \ldots, x_n\} = E \\ x_1 & \text{sonst} \end{cases}$$

Die Algebra mit diesen Operationen werde $\underline{A}$ genannt. Zu zeigen ist $\mathcal{C}_\mathcal{H}(X) = \langle X \rangle_{\underline{A}}$ für alle $X \subseteq A$. Sei $b \in \mathcal{C}_\mathcal{H}(X)$. Wegen Induktivität von $\mathcal{C}_\mathcal{H}$ folgt die Existenz einer *endlichen* Menge $E = \{e_1, \ldots, e_n\} \subseteq X$ mit $b \in \mathcal{C}_\mathcal{H}(E)$. Für die Operation $f_{E,b}$ gilt dann $f_{E,b}(e_1, \ldots, e_n) = b$. Es folgt $b \in \langle e_1, \ldots, e_n \rangle_{\underline{A}} \subseteq \langle X \rangle_{\underline{A}}$, womit $\mathcal{C}_\mathcal{H}(X) \subseteq \langle X \rangle_{\underline{A}}$ gezeigt ist. Für die umgekehrte Inklusion $\langle X \rangle_{\underline{A}} \subseteq \mathcal{C}_\mathcal{H}(X)$ genügt der Nachweis, dass $\mathcal{C}_\mathcal{H}(X)$ eine Unteralgebra von $\underline{A}$ ist. Sei also $b_1, \ldots, b_n \in \mathcal{C}_\mathcal{H}(X)$, und sei $f_{E,b}$ eine der oben definierten Operationen, also mit endlichem $E$ und $b \in \mathcal{C}_\mathcal{H}(E)$. Es gibt *zwei Fälle*: 1) Im Fall $\{b_1, \ldots . b_n\} = E$ gilt $f_{E,b}(b_1, \ldots, b_n) = b$ mit $b \in \mathcal{C}_\mathcal{H}(b_1, \ldots, b_n) \subseteq \mathcal{C}_\mathcal{H}\big(\mathcal{C}_\mathcal{H}(X)\big) = \mathcal{C}_\mathcal{H}(X)$. 2) Die einzige andere Möglichkeit ist $f_{E,b}(b_1, \ldots, b_n) = b_1$ (im Fall $\{b_1, \ldots, b_n\} \neq E$). Daher gilt in beiden Fällen $f_{E,b}(b_1, \ldots, b_n) \in \mathcal{C}_\mathcal{H}(X)$ □

Damit ist vollständig geklärt, wie Unteralgebren-Hüllensysteme und Unteralgebren-Hüllenoperatoren aussehen. Jetzt wird noch untersucht, wie die Unteralgebren einer Algebra *abstrakt* angeordnet sein können. Dies wird in der Sprache der **Verbände** formuliert. Es handelt sich dabei um algebraische Strukturen, die aber als geordnete Mengen aufgefasst werden können.

**Definition:** Ein **Verband** ist eine Algebra $(L; \vee, \wedge)$ vom Typ $(2, 2)$, mit den Operationen $\vee$ („*Verbindung*“) und $\wedge$ („*Schnitt*“), so dass folgende Gleichungen erfüllt sind:

| | | |
|---|---|---|
| (komm) | $x \vee y = y \vee x, \qquad x \wedge y = y \wedge x$ | **Kommutativität** |
| (ass) | $x \vee (y \vee z) = (x \vee y) \vee z$ | |
| | $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ | **Assoziativität** |
| (abs) | $x \vee (x \wedge y) = x, \qquad x \wedge (x \vee y) = x$ | **Absorption** |

Man beachte, dass die *duale* Form jeder dieser Gleichungen (die durch Vertauschen von $\vee$ und $\wedge$ entsteht) auch zu diesen Gleichungen gehört. Deshalb gilt:

**Beobachtung:** Leitet man aus diesen Gleichungen eine Aussage ab, dann gilt automatisch auch die dazu duale Aussage.

Zur Illustration eine einfach Anwendung:

**Behauptung:** In jedem Verband gelten die folgenden Gleichungen:

(idem) $x \vee x = x, \qquad x \wedge x = x$ **Idempotenz**

**Beweis:** Aufgrund obiger Beobachtung genügt es, die erste dieser Gleichungen zu zeigen. Dies gelingt sehr leicht:

$$x \vee x \overset{(1)}{=} x \vee \big(x \wedge (x \vee y)\big) \overset{(2)}{=} x$$

wobei für (1) die zweite und für (2) die erste (abs)-Gleichuung verwendet werden kann. □

**Beispiel:** Der Verband $(L; \vee, \wedge)$ wird durch *Verknüpfungstafeln* dargestellt. Die Gültigkeit der Kommutativgesetze ist offensichtlich (ebenso der Idempotenz). Aber Assoziativität und Absorption sind nicht so offensichtlich:

| $\vee$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $b$ | $b$ | $b$ | $d$ | $d$ | $e$ |
| $c$ | $c$ | $d$ | $c$ | $d$ | $e$ |
| $d$ | $d$ | $d$ | $d$ | $d$ | $e$ |
| $e$ | $e$ | $e$ | $e$ | $e$ | $e$ |

| $\wedge$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $a$ | $b$ | $b$ |
| $c$ | $a$ | $a$ | $c$ | $c$ | $c$ |
| $d$ | $a$ | $b$ | $c$ | $d$ | $d$ |
| $e$ | $a$ | $b$ | $c$ | $d$ | $e$ |

Man versteht Verbände viel besser, wenn man sie als geordnete Mengen auffassen kann:

**Beobachtung:** Sei $(L; \vee, \wedge)$ ein Verband. Für alle $x, y \in L$ sei

$$x \leq y \quad :\Leftrightarrow \quad x \wedge y = x$$

Dann ist $(L; \leq)$ eine geordnete Menge, genannt eine **verbandsgeordnete Menge**.

**Beweis:** Für die Relation $\leq$ muss Reflexivität, Antisymmetrie und Transitivität gezeigt werden. *Reflexivität:* wegen (idem) gilt $x \wedge x = x$ für alle $x \in L$, also $x \leq x$. *Antisymmetrie:* Gelte $x \leq y$ und $y \leq x$. Das bedeutet $x \wedge y = x$ und $y \wedge x = y$. Aber (komm) liefert $x \wedge y = y$, also $x = y$. *Transitivität:* Gelte $x \leq y$ und $y \leq z$. Das bedeutet $x \wedge y = x$ und $y \wedge z = y$. Es folgt

$$x \wedge z = (x \wedge y) \wedge z \overset{(\text{ass})}{=} x \wedge (y \wedge z) = x \wedge y = x$$

also $x \leq z$. □

**Übrigens:** Man hätte oben auch

$$x \leq y \quad :\Leftrightarrow \quad x \vee y = y$$

definieren können. Wegen $x \wedge y = x \Leftrightarrow x \vee y = y$ hätte sich nichts geändert!

**Beispiel:** (von Seite 61 fortgesetzt): Alle Informationen über diesen Verband ist in folgendem Diagramm der zugehöhrigen geordneten Menge $(L, \leq)$ enthalten (viel übersichtlicher als in den Verknüpfungstafeln!)

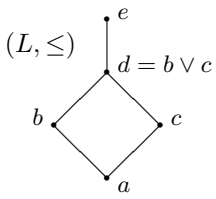



Abbildung 31: Liniendiagramm des Verbandes $(L, \leq)$

Natürlich lassen sich die Verbandsoperationen $\vee$ und $\wedge$ auch umgekehrt aus der Ordnungsrelation $\leq$ zurückerhalten. Dazu einige Begriffe:

**Definition:** Sei $(A, \leq)$ eine geordnete Menge, und seien $x, y \in A$. Ein Element $b \in A$ heißt eine **obere Schranke** von $x$ und $y$, falls $b \geq x$ und $b \geq y$ gilt. Sei $B$ die Menge aller oberen Schranken von $x$ und $y$. Falls es ein kleinstes Element von $B$ gibt, das heißt ein Element $b_0 \in B$ mit $b_0 \leq b$ für alle $b \in B$, dann heißt $b_0$ das **Supremum** (oder die **kleinste obere Schranke** oder – einfacher - - die **Verbindung**) von $x$ und $y$, geschrieben als $b_0 = \sup(x, y)$. Die **dualen Begriffe** (mit „$\leq$“ und „$\geq$“ in vertauschten Rollen) sind: **untere Schranke** von $x$ und $y$, die Menge aller unteren Schranken von $x$ und $y$, größtes Element $c_0$ von $C$ (genannt **Infimum** oder größte untere Schranke oder **Schnitt**) von $x$ und $y$, geschrieben als $c_0 = \inf(x, y)$.

**Beispiele**

- In folgender geordneten Menge $(A, \leq)$ handelt es sich bei den oberen Schranken von $d$ und um die Elemente von $B = \{a, b, c\}$. Diese Menge hat zwei minimale Elemente (nämlich $b$ und $c$), aber kein kleinstes Element. Also gibt es kein Supremum von $d$ und $e$. Übrigens existiert auch kein Infimum von $d$ und $e$.

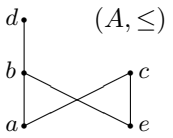



Abbildung 32: Liniendiagramm des Verbandes $(A, \leq)$

- Im Beispiel von Seite 61 beziehungsweise Seite 61 existieren $\sup(x, y)$ und $\inf(x, y)$ für alle $x, y \in L$, zum Beispiel: $\sup(b, c) = d$, $\inf(b, c) = a$, $\inf(e, b) = b$.

**Satz:** Sei $(L; \vee; \wedge)$ ein Verband. Dann existieren in der zugehörigen verbandsgeordneten Menge $(L, \leq)$ alle Suprema $\sup(x, y)$ und alle Infima $\inf(x, y)$, und es gilt: $\sup(x, y) = x \vee y$, $\inf(x, y) = x \wedge y$.

**Kurz gesagt:** Verbände „sind“ nichts anderes als geordnete Mengen, in denen alle Suprema und Infima (von je zwei Elementen) existieren.

**Beweisplan für obigen Satz** (Details seien dem Leser überlassen): Wegen Dualität reicht es, den Sup-Teil zu beweisen. Für alle $x, y \in L$ muss gezeigt werden:

1. $x \leq x \vee y$ (und – dazu symmetrisch – $y \leq x \vee y$)
2. aus $x \leq z$ und $y \leq z$ folgt $x \vee y \leq z$

Für 1. muss $x \vee (x \vee y) = x \vee y$ gezeigt werden. Für 2. muss folgende Implikation nachgewiesen werden: $x \vee z = z$, $y \vee z = z \Longrightarrow (x \vee y) \vee z = z$

**Beispiele:**

- **Mengen**: Für jede Menge $A$ ist die geordnete Menge $(\mathcal{P}(A), \subseteq)$, die Potenzmenge von $A$ mit Mengeninklusion $\subseteq$, ist verbandsgeordnet. Der zugehörige Verband ist $\mathcal{P}(A), \cup, \cap)$.
- **Teiler**: Mit $x|y$ („x teilt y“) erhält man eine verbandsgeordnete menge $(\mathbb{N}, |)$. **Aufgabe**): Was sind die Suprema und die Infima in $(\mathbb{N}, |)$?
- **Unteralgebren** (bzw. deren Grundmengen): Sei $A = (A; F)$ eine Algebra, dann sei $(\mathrm{Sub}(A), \subseteq)$ die geordnete Menge aller Unteralgebren von $A$. Diese ist verbandsgeordnet, für Unteralgebren $B$, $C$ von $A$ gilt: $\inf(B, C) = B \cap C$, $\sup(B, C) = \langle B \cup C \rangle$, die von $B \cup C$ erzeugte Unteralgebra.

Mit dem letzten Beispiel ist geklärt, daß die Unteralgebren einer Algebra einen Verband bilden, aber noch nicht, welche Verbände (abstrakt) als Unteralgebren-Verbände auftreten. Dies wird im Rest dieses Einschubs behandelt (aber ohne alle Beweise).

**Definition:** Sei $(A, \leq)$ eine geordnete Menge und $X \subseteq A$ eine Teilmenge. Falls eine kleinste obere Schranke $sup(X)$ von $X$ existiert, wird diese auch mit $\bigvee X$ bezeichnet, **Supremum** von $X$. Entsprechend wird, falls existent, eine größte untere Schranke $inf(X)$ von $X$ mit $\bigwedge X$ bezeichnet, **Infimum** von $X$.
Eine verbandsgeordnete Menge $(L, \leq)$ (beziehungsweise der zugehörige Verband $(L; \vee; \wedge)$) heißt **vollständiger Verband**, falls für jede Teilmenge $X \subseteq L$ das Supremum $\bigvee X$ und das Infimum $\bigwedge X$ existiert.

Ist $(L, \leq)$ ein vollständiger verband, dann heißt ein Element $a \in L$ **kompakt**, falls es zu jeder Menge $B \subseteq L$ mit $a \leq \bigvee B$ eine **endliche** Teilmenge $B_0 \subseteq B$ gibt mit $a \leq \bigvee B_0$.

Ein **algebraischer Verband** ist ein vollständiger Verband, in dem jedes Element ein Supremum kompakter Elemente ist.

**Beispiele:**

- Die geordnete Menge $(\mathbb{R}, \leq)$, mit der üblichen Ordnung, ist zwar verbandsgeordnet, aber kein vollständiger Verband: Das Supremum $\bigvee X$ existiert genau dann, wenn $X$ nach oben beschränkt ist. Zum Beispiel existiert das Supremum $\bigvee \mathbb{R}$ nicht. In $(\mathbb{R}, \leq)$ gibt es keine kompakten Elemente: Sei $a \in \mathbb{R}$ und $\mathbb{R}_{<a} := \{x \in \mathbb{R} | x < a\}$. Dann gilt $\bigvee \mathbb{R}_{<a} = a$, aber für jede endliche Teilmenge $E \subseteq R_{<a}$ gilt $\bigvee E = \max(E) < a$.
- Fügt man zu $(\mathbb{R}, \leq)$ ein zusätzliches kleinstes Element $-\infty$ und ein zusätzliches größtes Element $+\infty$ hinzu, erhält man einen vollständigen Verband $(\mathbb{R} \cup \{-\infty, +\infty\}, \leq)$, der aber wiederum keine kompakten Elemente enthält und nicht algebraisch ist.
- Sei $\mathcal{H}$ ein Hüllensystem auf $A$. Dann ist $(\mathcal{H}, \subseteq)$ ein vollständiger Verband. Für jede Teilmenge $\chi \subseteq \mathcal{H}$ ist $\bigwedge \chi := \bigcap \chi$ das Infimum von $\chi$ und $\bigvee \chi := \bigcap H \in \mathcal{H} | H \supseteq \bigcup \chi$ das Supremum von $\chi$ (vergleiche die Bemerkung auf Seite 58).

Damit ist klar, daß es sich bei den Unteralgebrenverbänden $(\mathrm{Sub}A, \subseteq)$ um vollständige Verbände handelt. Aber außerdem ist schon bekannt, daß $\mathrm{Sub}A$ für jede Algebra $A$ sogar ein induktives Hüllensystem ist. Dies wirkt sich auf die Verbände $(\mathrm{Sub}A, \subseteq)$ wie folgt aus (ohne Beweis):

**Bemerkung:** Für jede Algebra $A$ ist $(\mathrm{Sub}A, \subseteq)$ ein algebraischer Verband. Aber man weiß sogar viel mehr. Der folgende Satz gibt eine vollständige Charakterisierung von Unteralgebrenverbänden (ebenfalls ohne Beweis):

**Satz:** Ein vollständiger Verband $L$ ist genau dann **isomorph** zum Unteralgebrenverband einer Algebra, wenn $L$ algebraisch ist.

Zwei algebraische Strukturen werden **isomorph** genannt, wenn sie „bis auf eine Umbenennung“ der Elemente der Grundmengen mittels einer bijektiven Abbildung identisch sind. Später in diesem Abschnitt wird das Konzept der „Isomorphie“ von Algebren systematisch betrachtet!

Es folgt eine zweite Art, nach Unteralgebren, wie man aus gegebenen Algebren erhält.

### 2.2.4 Das direkte Produkt

**Definition:** Seien $\underline{A} = (A; F_{\underline{A}})$ und $\underline{B} = (B; F_{\underline{B}})$ Algebren des selben Typs $(\mathcal{F}, \sigma)$. Das **direkte Produkt** $\underline{A} \times \underline{B} = (A \times B; F_{\underline{A} \times \underline{B}})$ hat die Grundmenge $A \times B$ und ist vom selben Typ: für jedes Operationssymbol $f \in \mathcal{F}$ mit $\sigma(f) = n$ und für Elemente $(a_1, b_1), \ldots, (a_n, b_n) \in A \times B$ wird definiert:

$$f_{A \times B}\big((a_1, b_1), \ldots, (a_n, b_n)\big) := \big(f_A(a_1, \ldots, a_n), f_B(b_1, \ldots, b_n)\big)$$

das heißt die Operationen übertragen sich komponentenweise von $\underline{A}$ und $\underline{B}$ auf $\underline{A} \times \underline{B}$. Übrigens werden ganz analog direkte Produkte $\underline{A}_1 \times \ldots \times \underline{A}_k$ von $k$ Algebren $\underline{A}_1, \ldots, \underline{A}_k$ oder sogar direkte Produkte $\prod_{i \in I} \underline{A}_i$ von – eventuell – unendlich vielen Algebren $\underline{A}_i, i \in I$, gebildet werden.

**Beispiele**

- Die Halbgruppen $\underline{S} = (S; \cdot)$ und $\underline{T} = (T; \cdot)$ seien durch ihre Verknüpfungstafeln gegeben, ebenso das direkte Produkt $\underline{S} \times \underline{T}$ (das ebenfalls eine Halbgruppe ist):

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

$\underline{S} = (S; \cdot)$

| $\cdot$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $a$ | $b$ |

$\underline{T} = (T; \cdot)$

| $\cdot$ | $0a$ | $0b$ | $0c$ | $1a$ | $1b$ | $1c$ |
|---|---|---|---|---|---|---|
| $0a$ | $0a$ | $0b$ | $0c$ | $1a$ | $1b$ | $1c$ |
| $0b$ | $0b$ | $0c$ | $0a$ | $1b$ | $1c$ | $1a$ |
| $0c$ | $0c$ | $0a$ | $0b$ | $1c$ | $1a$ | $1b$ |
| $1a$ | $1a$ | $1b$ | $1c$ | $0a$ | $0b$ | $0c$ |
| $1b$ | $1b$ | $1c$ | $1a$ | $0b$ | $0c$ | $0a$ |
| $1c$ | $1c$ | $1a$ | $1b$ | $0c$ | $0a$ | $0b$ |

$\underline{S} \times \underline{T}$

(Hierbei steht „$xy$“ für „$(x, y)$“)

- Seien die Verbände $\underline{L}_1$ und $\underline{L}_2$ durch ihre Liniendiagramme gegeben. Das direkte Produkt $\underline{L}_1 \times \underline{L}_2$ hat dann folgendes Liniendiagramm:

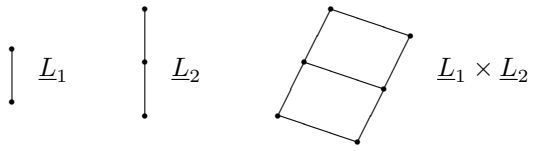



Abbildung 33: Direktes Produkt von Verbänden.

*Aufgabe*: Schreibe für $\underline{L}_1$, $\underline{L}_2$, $\underline{L}_1 \times \underline{L}_2$ die Schnittoperationen $\wedge$ und die Verbindungsoperationen $\vee$ (als Verknüpfungstafeln).

Als nächstes Konzept zum Erhalt „neuer“ Algebren aus „alten“ folgen die Begriffe **Kongruenzrelation** und **Faktoralgebra**:

### 2.2.5 Kongruenzrelation

**Definition:** Sei $\underline{A} = (A; F_A)$ eine Algebra vom Typ $(\mathcal{F}, \sigma)$ und sei $\Theta$ eine Äquivalenzrelation auf $A$. Man nennt $\Theta$ eine **Kongruenzrelation** auf $A$, falls für alle Operationssymbole $f \in \mathcal{F}$ (mit $\sigma(f) = n$) folgendes gilt für alle $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$:

(Vert) $\quad a_1 \Theta b_1, \ldots, a_n \Theta b_n \Longrightarrow f_{\underline{A}}(a_1, \ldots, a_n) \Theta f_{\underline{A}}(b_1, \ldots, b_n)$

Man nennt unter diesen Umständen die Relation $\Theta$ mit der Operation $f_{\underline{A}}$ **verträglich**. Die Kongruenzrelationen auf $A$ sind also gerade die Äquivalenzrelationen, die mit sämtlichen fundamentalen Operationen $f_{\underline{A}}$ verträglich sind.

**Beispiel:** Es werde die Halbgruppe von Seite 51 betrachtet, sie werde mit $S = (S; \cdot)$ bezeichnet.

| $\cdot$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $b$ | $c$ | $d$ |
| $c$ | $c$ | $c$ | $c$ | $d$ |
| $d$ | $d$ | $d$ | $d$ | $d$ |

Es ist übersichtlicher, die Kongruenzrelationen durch ihre Äquivalenzklassen („Kongruenzklassen“) anzugeben. Die Halbgruppe $S$ hat zum Beispiel Kongruenzrelationen $\Theta_1$ und $\Theta_2$ mit den folgenden Kongruenzklassen:

$$\begin{aligned}\Theta_1: &\quad \{a\},\{b,c\},\{d\},\\ \Theta_2: &\quad \{a,b\},\{c,d\}.\end{aligned}$$

Für jede Algebra $\underline{A}$ wird die Menge der Kongruenzrelationen von $A$ mit $\mathrm{Con}(\underline{A})$ bezeichnet. Mit Mengeninklusion „$\subseteq$“ als Ordnung erhält man einen (vollständigen) Verband $\big(\mathrm{Con}(\underline{A}),\subseteq\big)$. Das kleinste Element dieses Verbands ist immer $\Delta_A := \{(a,a) \mid a \in A\}$ („Delta-$A$“, „Identität“) während das größte Element mit $\nabla_A := \{(a,b) \mid a,b \in A\}$ („Nabla-$A$“, „Allrelation“) bezeichnet ist.

*Aufgabe:* Finde alle Kongruenzrelationen der Halbgruppe $S$ oben auf dieser Seite. Zeichne ein Liniendiagramm des Verbands $\big(\mathrm{Con}(\underline{S}),\subseteq\big)$. Folgende Tatsachen helfen beim Verständnis sowie beim Lösen obiger Aufgabe:

Die Menge aller Äquivalenzrelationen auf einer Menge $A$ werde mit $\mathrm{Eq}(A)$ bezeichnet, sie bildet mit Mengeninklusion „$\subseteq$“ einen Verband $\big(\mathrm{Eq}(A),\subseteq\big)$. Das folgende Diagramm zeigt ein **Liniendiagramm** des Verbands $\big(\mathrm{Eq}(A),\subseteq\big)$ für $A=\{1,2,3\}$:

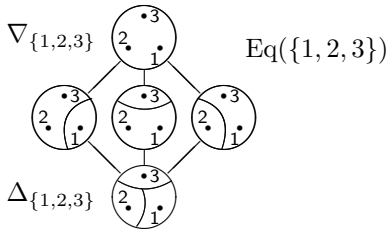



Abbildung 34: Liniendiagramm von $\big(\mathrm{Eq}(A),\subseteq\big)$

Im Verband $\mathrm{Eq}(A)$ (für beliebiges $A$) gilt, für $\Theta_1,\Theta_2 \in \mathrm{Eq}(A)$:

$$\begin{aligned}\Theta_1 \wedge \Theta_2 &= \Theta_1 \cap \Theta_2\\ \Theta_1 \vee \Theta_2 &= \bigcap\{\phi \in \mathrm{Eq}(A) \mid \phi \supseteq \Theta_1 \cup \Theta_2\}\end{aligned}$$

Das Supremum $\Theta_1 \vee \Theta_2$ kann konstruktiv beschrieben werden. Für $\Theta_1,\Theta_2 \in \mathrm{Eq}(A)$ sei das **Relationenprodukt** $\Theta_1 \circ \Theta_2$ definiert wie folgt:

$$\Theta_1 \circ \Theta_2 := \{(x,y) \mid \exists z \in A\colon x\ \Theta_1\ z\ \Theta_2\ y\}$$

Man beachte, dass das Relationenprodukt assoziativ ist, also keine Klammern gesetzt werden müssen. Es gilt:

**Tatsache:** Für jede Menge $A$ und alle $\Theta_1,\Theta 2 \in \mathrm{Eq}A$ gilt

$$\Theta_1 \vee \Theta_2 = \Theta_1 \cup (\Theta_1 \circ \Theta_2) \cup (\Theta_1 \circ \Theta_2 \circ \Theta_1) \cup (\Theta_1 \circ \Theta_2 \circ \Theta_1 \circ \Theta_2) \cup \ldots$$

das heißt $(a,b) \in \Theta_1 \vee \Theta_2$ genau dann, wenn es sin $n \in \mathbb{N}$ und Elemente $c_1,\ldots,c_n \in A$ gibt mit

$$a = c_1\ \Theta_1\ c_2\ \Theta_2\ c_3\ \Theta_1\ c_4\ \ldots\ c_n = b$$

Sind jetzt $\Theta_1,\Theta_2 \in \mathrm{Con}\underline{A}$ für eine Algebra $\underline{A}$, dann gilt, mit den eben definierten Operationen $\vee$ und $\wedge$ auf $\mathrm{Eq}A$:

$$\Theta_1 \vee \Theta_2 \in \mathrm{Con}\underline{A}, \qquad \Theta_1 \wedge \Theta_2 \in \mathrm{Con}\underline{A}$$

**Satz:** Für jede Algebra $\underline{A}$ ist $(\mathrm{Con}\underline{A}, \subseteq)$ ein Unterverband von $(\mathrm{Eq}\underline{A}, \subseteq)$. Außerdem gilt immer $\Delta_A, \nabla_A \in \mathrm{Con}\underline{A}$.

**Beispiele:** (a) Hat eine Algebra $\underline{A}$ keine fundamentalen Operationen, $F = \emptyset$, so gilt $\mathrm{Con}\underline{A} = \mathrm{Eq}A$.

(b) Auf jeder Menge $A$ sind die konstanten Operationen

$$f_c^{(n)}: A^n \longrightarrow A, f(x_1, \ldots, x_n) = c \quad \text{für alle } x_1, \ldots, x_n \in A$$

mit allen $\Theta \in \mathrm{Eq}A$ verträglich. Dasselbe gilt für die (einstellige) identische Abbildung $\mathrm{id}_A$ auf $A$, aber auch für die Projektionsabbildungen

$$P_i^{(n)}: A^n \longrightarrow A, P_i^{(n)}(x_1, \ldots, c_n) := x; \quad \text{für alle } x_1, \ldots, x_n \in A$$

(c) Wie in obigem Satz festgestellt, sind $\Delta_A$ und $\nabla_A$ Kongruenzrelationen für jede Algebra $\underline{A}$. Im Fall, dass es nur diese Kongruenzrelationen gibt, $\mathrm{Con}\underline{A} = \{\Delta_A, \nabla_A\}$, nennt man die Algebra **einfach**. Beispielsweise ist $A = (A; \mathrm{Op}(A))$ einfach (mit der Menge $\mathrm{Op}(A)$ sämtlicher endlichstelliger Operationen auf $A$ als Menge der fundamentalen Operationen).

Wie stellt man allgemein fest, welches die mit einer Operationenmenge $F$ auf $A$ verträglichen Äquivalenzrelationen, das heißt die Kongruenzrelationen der Algebra $\underline{A} = (A; F)$ sind? Hierbei kann folgendes helfen:

**Definition:** Sei $\underline{A} = (A; F)$ eine Algebra. Jede Abbildung der Form

$$A \longrightarrow A, x \mapsto f(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$$

mit $f \in F$ ($n$-stellig) und $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in A$ heißt eine **Translation** von $\underline{A}$.

**Beispiel:** Die Algebra $\underline{S} = (S; \cdot)$ von Seite 65 hat folgende Translationen:

$x \mapsto a \cdot x$ mit Wertetabelle

| $x$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a \cdot x$ | $a$ | $b$ | $c$ | $d$ |

$x \mapsto b \cdot x$ mit Wertetabelle

| $x$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $b \cdot x$ | $b$ | $b$ | $c$ | $d$ |

$x \mapsto c \cdot x$ mit Wertetabelle

| $x$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $c \cdot x$ | $c$ | $c$ | $c$ | $d$ |

$x \mapsto d \cdot x$ mit Wertetabelle

| $x$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $d \cdot x$ | $d$ | $d$ | $d$ | $d$ |

Dies sind alle Translationen von $\underline{S}$. Die entsprechen den Zeilen (bzw. Spalten) der Verknüpfungstafel.

Mit den Translationen lassen sich sämtliche Kongruenzrelationen einer Algebra $\underline{A}$ bestimmen. Zunächst können sämtliche **Hauptkongruenzrelationen** $\Theta(x, y) \in \mathrm{Con}\underline{A}, x \neq y$, bestimmt werden. Es handelt sich bei $\Theta(x, y)$ um die kleinste das Paar $(x, y)$ enthaltende Kongruenzrelation auf $\underline{A}$. Es gilt:

**Bemerkung:** $\Theta(x, y)$ ist die transitive, symmetrische Hülle der Menge

$$T(x, y) := \{(t(x), t(y)) \mid t \text{ Translation von } \underline{A}\}$$

Die Kongruenzrelationen der Form $\Theta(x, y)$ können jetzt benutzt werden, um sämtliche Kongruenzrelationen von $\underline{A}$ zu finden:

**Bemerkung:** Für jede Kongruenzrelation $\Theta \in \mathrm{Con}\underline{A}$ gilt

$$\Theta = \bigvee \{\Theta(x, y) \mid (x, y) \in \Theta\}$$

das heißt $\Theta$ ist ein Supremum von Hauptkongruenzen.

**Beispiel:** Es wird weiter die Halbgruppe $\underline{S}$ von 65 betrachtet. Mit den Translationen vom letzen Beispiel erhält man zum Beispiel folgende Paare, ausgehend von einem Paar $(x, y)$:

| | | |
|---|---|---|
| $(a, b)$: | $(a, b)$, $(b, b)$, $(c, c)$, $(d, d)$ | $\to \Theta(a, b)$ hat Klassen $\{a, b\}$, $\{c\}$, $\{d\}$. |
| $(a, c)$: | $(a, c)$, $(b, c)$, $(c, c)$, $(d, d)$ | $\to \Theta(a, c)$ hat Klassen $\{a, b, c\}$, $\{d\}$. |
| $(a, d)$: | $(a, d)$, $(b, d)$, $(c, d)$, $(d, d)$ | $\to \Theta(a, d)$ hat nur Klasse $\{a, b, c, d\}$. |

Und so weiter! Man erhält alle Hauptkongruenzrelationen, und als Suprema aus diesen dann sämtliche Kongruenzrelationen.

Man kann zueinander äquivalente Elemente bezüglich einer Äquivalenzrelation bekanntlich als „gleich“ auffassen, jedenfalls aus einem gewissen „Blickwinkel“. So soll das auch mit zueinander äquivalenten (das heißt kongruenten) Elementen geschehen:

**Definition:** Sei $\Theta$ eine Kongruenzrelation einer Algebra $\underline{A} = (A; F_{\underline{A}})$. Auf der Menge $A/\Theta := \{[a]\Theta \mid a \in A\}$ der Kongruenzklassen von $\Theta$ wird die Faktoralgebra $\underline{A}/\Theta = (A/\Theta; F_{\underline{A}/\Theta})$, indem für jeden $n$-stelliges Operationssymbol $f \in \mathcal{F}$ und alle $a_1, \ldots, a_n \in A$ folgendes definiert wird:

$$f_{\underline{A}/\Theta}([a_1]\Theta, \ldots, [a_n]\Theta) := [f_{\underline{A}}(a_1, \ldots, a_n)]\Theta$$

Man sagt, dass die Operationen von $f_{\underline{A}/\Theta}$ „räpresentantenweise“ definiert werden, in obiger Definition ist jedes $a_i$ ein „Repräsentant“ der Klasse $[a_i]\Theta$. Aber das könnte schiefgehen, die Ergebisse könnten von der Wahl der Repräsentanten abhängen. Glücklicherweise gilt:

**Satz:** Faktoralgebren $\underline{A}/\Theta$ sind wohldefiniert: Ist $\Theta$ eine Kongruenzrelation einer Algebra $\underline{A}$, ist $f_{\underline{A}}$ eine $n$-stellige, fundamentale Operation von $\underline{A}$, und gilt $[a_1]\Theta = [b_1]\Theta, \ldots, [a_n]\Theta = [b_n]\Theta$, dann gilt auch

$$f_{\underline{A}/\Theta}([a_1]\Theta, \ldots, [a_n]\Theta) = f_{\underline{A}/\Theta}([b_1]\Theta, \ldots, [b_n]\Theta)$$

Der Beweis ist ganz offensichtlich (und klappt nur, weil $\Theta$ eine Kongruenzrelation von $\underline{A}$ ist): Die Vorraussetzung $[a_1]\Theta = [b_1]\Theta, \ldots, [a_n]\Theta = [b_n]\Theta$ lässt sich schreiben als

$$a_1 \Theta b_1, \ldots, a_n \Theta b_n$$

Da $\Theta$ eine Kongruenzrelation ist, folgt mit Bedingung (Vert)

$$f_{\underline{A}}(a_1, \ldots, a_n)\Theta f_{\underline{A}}(b_1, \ldots, b_n)$$

das heißt $f_{\underline{A}/\Theta}([a_1]\Theta, \ldots, [a_n]\Theta) = [f_{\underline{A}}(a_1, \ldots, a_n)]\Theta = [f_{\underline{A}}(b_1, \ldots, b_n)]\Theta = f_{\underline{A}/\Theta}([b_1]\Theta, \ldots, [b_n]\Theta)$, wie behauptet. □

**Beispiele:** (a) Zuerst die Algebra $\underline{S} = (S; \cdot)$ von Seite 65, mit der Kongruenzrelation $\Theta_1$ (mit Kongruenzklassen $\{a\}$, $\{b, c\}$, $\{d\}$). Die Faktoralgebra $\underline{S}/\Theta_1$ hat dann folgende Verknüpfungstafel für ihre wiederum mit $\cdot$ bezeichnete Operation:

| $\cdot$ | $\{a\}$ | $\{b, c\}$ | $\{d\}$ |
|---|---|---|---|
| $\{a\}$ | $\{a\}$ | $\{b, c\}$ | $\{d\}$ |
| $\{b, c\}$ | $\{b, c\}$ | $\{b, c\}$ | $\{d\}$ |
| $\{d\}$ | $\{d\}$ | $\{d\}$ | $\{d\}$ |

(b) Der Klassiker: Werde die Gruppe $\underline{\mathbb{Z}} = (\mathbb{Z}; +, -, 0)$ der ganzen Zahlen betrachtet, und sei $n \in \mathbb{N}$. Durch

$$x\Theta_n y \;:\Leftrightarrow\; n \text{ teilt } x - y$$

wird eine zweistellige Relation $\Theta_n$ auf $\mathbb{Z}$ definiert. Schon (ganz weit) oben wurde gezeigt, dass $\Theta_n$ eine Äquivalenzrelation ist. Natürlich ist $\Theta_n$ sogar eine Kongruenzrelation von $\underline{\mathbb{Z}}$: Aus $a_1\Theta_n b_1$ und $a_2\Theta_n b_2$ folgt

$$n \text{ teilt } a_1 - b_1 \text{ und } a_2 - b_2$$

Deshalb teilt $n$ auch $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$, was $(a_1 + a_2)\Theta_n(b_1 + b_2)$ bedeutet. Außerdem teilt $n$ auch $-a_1 - (-b_1) = -(a_1 - b_1)$, das heißt es folgt $(-a_1)\Theta_n(-b_1)$. Die Faktoralgebra $\underline{\mathbb{Z}}/\Theta_n$ hat die Kongruenzklassen

$$[0]\Theta_n,\ [1]\Theta_n,\ \ldots,\ [n-1]\Theta_n$$

Das Rechnen mit diesen Klassen entspricht dem Rechnen mit modulo $n$ in $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

(c) Noch ein Klassiker: Sei $V$ ein Vektorraum und $U \leq V$ ein Untervektorraum. Sei $\Theta_u$ die Äquivalenzrelation mit den Nebenklassen $a + U$, $a \in V$, als Äquivalenzklassen. Dann ist $\Theta_u$ eine Kongruenzrelation von $V$. Und:

> Alle Kongruenzrelationen eines Vektorraums $V$ sind von der Form $\Theta_u$ für einen Untervektorraum $U$ von $V$.

Zum Abschluss dieses sehr ausführlichen Abschnitts wir eine Möglichkeit vorgeführt, wie man Algebren miteinander „vergleichen“ kann, nämlich mit Hilfe von Homomorphismen. Eine einfache Version hiervon stellen die Isomorphismen dar, das heißt „Umbenennungen“ der Elemente von Algebren mittels bijektiver Abbildungen:

**Definition:** Seien $\underline{A}$ und $\underline{B}$ zwei Algebren des selben Ähnlicheitstyps.
Sei $\varphi\colon A \longrightarrow B$ eine bijektive Abbildung der Grundmengen. Man nennt $\varphi$ einen Isomorphismus von $\underline{A}$ auf $\underline{B}$, falls für jedes Operationssymbol $f \in \mathcal{F}$ (von Stelligkeit $\sigma(f) = n$) und für alle $a_1, \ldots, a_n \in A$ folgendes gilt:

(Hom) $\varphi(f_{\underline{A}}(a_1, \ldots, a_n)) = f_{\underline{B}}(\varphi(a_1), \ldots, \varphi(a_n))$ **Homomorphie**

Die Algebren $\underline{A}$ und $\underline{B}$ werden dann isomorph genannt, in Zeichen $\underline{A} \cong \underline{B}$.

**Beispiele:** (a) Auf Seite 54 wurde ein Isomorphismus zwischen den Vektorräumen $P_n$ (reelle Poynome vom Grad kleiner $n$) und $\mathbb{R}^n$ angegeben.

(b) Die Gruppe $\underline{\mathbb{Z}}_6 = (\mathbb{Z}_6; +, -, 0)$ ist isomorph zum direkten Produkt $\underline{\mathbb{Z}}_2 \times \underline{\mathbb{Z}}_3$. Ein Isomorphismus $\varphi\colon \underline{\mathbb{Z}}_6 \longrightarrow \underline{\mathbb{Z}}_2 \times \underline{\mathbb{Z}}_3$ wird gegeben durch:

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $\varphi(x)$ | 00 | 11 | 02 | 10 | 01 | 12 |

(c) Die ersten beiden der Folgenden Gruppen sind isomorph; ein Isomorphismus wird gegeben durch $\varphi\colon \{0,1,2,3\} \longrightarrow \{a,b,c,d\}$ mit

| $x$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\varphi(x)$ | $a$ | $b$ | $c$ | $d$ |

Die dritte Gruppe ist nicht isomorph zu den ersten beiden:

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$\underline{G}_1 = (\{0,1,2,3\}; +, -, 0)$

| $\cdot$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $c$ | $d$ | $a$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $a$ | $b$ | $c$ |

$\underline{G}_2 = (\{a,b,c,d\}; \cdot, ^{-1}, a)$

| $\circ$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ |
| $B$ | $B$ | $A$ | $D$ | $C$ |
| $C$ | $C$ | $D$ | $A$ | $B$ |
| $D$ | $D$ | $C$ | $B$ | $A$ |

$\underline{G}_3 = (\{A,B,C,D\}; \circ, ^{-1}, A)$

Es ist klar, dass obige Abbildung $\varphi$ ein Isomorphismus von $\underline{G}_1$ auf $\underline{G}_2$ ist. Aber wie kann man sehen, dass $\underline{G}_1$ und $\underline{G}_3$ nicht isomorph sind? Einfache Möglichkeit: $\underline{G}_3$ erfüllt die Gleichung $x^2 = 1$ (das heißt $A \circ A = B \circ B = C \circ C = D \circ D = A$), während $\underline{G}_1$ diese Gleichung nicht erfüllt, zum Beispiel ist $1 + 1 = 2 \neq 0$.

### 2.2.6 Homomorphismen

Jetzt zur angekündigten Verallgemeinerung:

**Definition:** Eine Abbildung $\varphi\colon A \longrightarrow B$ zwischen den Grundmengen zweier Algebren $\underline{A}$ und $\underline{B}$ des selben Ähnlichkeitstyps heißt **Homomorphismus** von $\underline{A}$ nach $\underline{B}$, wenn die Homomorphiebedingung (Hom) von Seite 70 erfüllt ist.

**Bemerkung:** Homomorphismen zwischen Algebren $A$ und $B$ müssen nicht injektiv sein, das heißt verschiedene Elemente von $A$ können auf das selbe Ergebnis abgebildet werden. Sie müssen auch nicht surjektiv sein, das heßt es müssen nicht alle Elemente von $B$ als Ergebnisse des Homomorphismus auftreten. (Dies wird schon im ersten der folgenden Beispiele deutlich.)

**Beispiele:**

- Zwischen den beiden oben definierten Gruppen $\underline{G_1}$ und $\underline{G_3}$ ist ein Homomorphismus $\varphi\colon G_1 \longrightarrow G_3$ gegeben durch:

| $x$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\varphi(x)$ | $A$ | $B$ | $A$ | $B$ |

  (Dieses Beispiel wird im nächsten Abschnitt näher untersucht. Stichwort: **Homomorphiesatz**.)

- Sei $\underline{\mathbb{Z}} = (\mathbb{Z}; +, -, 0)$ die Gruppe der ganzen Zahlen. Für jedes $n \in \mathbb{N}$ ist ein Homomorphismus $\varphi_n\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ (also ein Endomorphismus von $\underline{\mathbb{Z}}$) gegeben durch
$$\varphi_n(x) := nx$$
  *Aufgabe:* Zeige, dass alle Endomorphismen von $\underline{\mathbb{Z}}$ von dieser Form sind.

- Sei $(A^*; \cdot, \lambda)$ das **Wortmonoid** über dem Alphabeth $A = \{\mathtt{a}, \mathtt{b}\}$ (siehe Seite 50) und sei $\big(\mathbb{N}_0^2; +, (0,0)\big)$ das Monoid mit komponentenweiser Addition:
$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2)$$
  (es handelt sich also um das direkte Produkt $\underline{\mathbb{N}_0}^2 = \underline{\mathbb{N}_0} \times \underline{\mathbb{N}_0}$ des Monoids $\underline{\mathbb{N}_0} = (\mathbb{N}_0; +, 0)$ mit sich selbst.) Ein Homomorphismus $\varphi\colon A^* \longrightarrow \mathbb{N}_0^2$ wird gegeben durch
$$\varphi(a_1 a_2 \cdots a_k) = (i, j)$$
  wobei $i$ die Anzahl der $\mathtt{a}$'s und $j$ die Anzahl der $\mathtt{b}$'s in $a_1 a_2 \cdots a_k$ sei.
  Beispielsweise gilt $\varphi(\lambda) = (0,0)$ und $\varphi(\mathtt{abbabaaa}) = (5,2)$

## 2.3 Der Homomorphiesatz der Allgemeinen Algebra

Zu jedem Homomorphismus zwischen zwei Algebren gehört in natürlicher Weise eine Unteralgebra und eine Kongruenzrelation:

**Bemerkung:** Sei $\varphi\colon A \longrightarrow B$ ein Homomorphismus der Algebra $\underline{A}$ in die Algebra $\underline{B}$. Dann gilt $\varphi(A) \in \mathrm{Sub}(\underline{B})$, das heißt $\varphi(A)$ ist die Grundmenge einer Unteralgebra $\underline{\varphi(A)} \leqslant \underline{B}$ („**Bild von** $A$ unter $\varphi$“). Außerdem ist
$$\mathrm{Kern}(\varphi) := \{(a_1, a_2) \in A^2 \mid \varphi(a_1) = \varphi(a_2)\}$$
eine Kongruenzrelation auf $\underline{A}$ („**Kern von** $\varphi$“), das heißt es gilt $\mathrm{Kern}(\varphi) \in \mathrm{Con}(\underline{A})$.

**Beweis:** Für $\varphi(A) \in \mathrm{Sub}(\underline{B})$ muss gezeigt werden, dass $\varphi(A)$ abgeschlossen ist gegen die Operationen $f_{\underline{B}}$ von $\underline{B}$. Sei $f_{\underline{B}}$ $n$-stellig und seien $a_1, \ldots, a_n \in A$ gegeben. Für $\varphi(a_1), \ldots, \varphi(a_n) \in \varphi(A)$ gilt dann:
$$f_{\underline{B}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big)\big) \overset{(\mathsf{Hom})}{=} \varphi\big(f_{\underline{A}}(a_1, \ldots, a_n)\big) \in \varphi(A)$$

Für den Nachweis von $\mathrm{Kern}(\varphi) \in \mathrm{Con}(\underline{A})$ muss gezeigt werden, dass $\mathrm{Kern}(\varphi)$ eine Äquivalenzrelation auf $A$ ist (was aber offensichtlich ist) und dass für $\mathrm{Kern}(\varphi)$ die **Verträglichkeitsbediungung** (Vert) von Seite 65 gilt. Sei also $f_{\underline{A}}$ eine $n$-stellige fundamentale Operation von $A$ und für $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ gelte

$$a_1 \mathrm{Kern}(\varphi) b_1, \ldots, a_n \mathrm{Kern}(\varphi) b_n,$$

das heißt $\varphi(a_1) = \varphi(b_1), \ldots, \varphi(a_n) = \varphi(b_n)$. Dann gilt

$$\begin{aligned} \varphi\big(f_{\underline{A}}(a_1, \ldots, a_n)\big) &\overset{(\mathsf{Hom})}{=} f_{\underline{B}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big) \\ &= f_{\underline{B}}\big(\varphi(b_1), \ldots, \varphi(b_n)\big) \\ &\overset{(\mathsf{Hom})}{=} \varphi\big(f_{\underline{A}}(n_1, \ldots, b_n)\big) \end{aligned}$$

also $f_{\underline{A}}(a_1, \ldots, a_n) \mathrm{Kern}(\varphi) f_{\underline{A}}(b_1, \ldots, b_n)$. □

Als Beispiel wird der Homomorphismus $\varphi\colon \underline{G_1} \longrightarrow \underline{G_3}$ von Seite 70. Tatsächlich gilt $\varphi(G_1) = \{A, B\} \in \mathrm{Sub}(\underline{G_3})$. Die Kongruenzrelation $\mathrm{Kern}(\varphi)$ hat diese Kongruenzklassen $\{0, 2\}$ und $\{1, 3\}$.

Jetzt zum „Kern“ dieses Abschnitts. Dazu zuerst:

**Beobachtungen:** Sei $\underline{C}$ eine Unteralgebra der Algebra $\underline{B}$. Dann ist die Abbildung

$i\colon C \longrightarrow B, \quad x \mapsto x$ **(Inklusionsabbildung)**

ein Homomorphismus $\underline{C} \longrightarrow \underline{B}$.

Sei $\Theta$ eine Kongruenzrelation der Algebra $\underline{A}$. Dann ist die Abbildung

$\pi\colon A \longrightarrow A/\Theta, \quad x \mapsto [x]\Theta$ **(Faktorabbildung)**

ein Homomorphismus $\underline{A} \longrightarrow \underline{A}/\Theta$.

Der Beweis hierfür ist einfach, er sei dem Leser überlassen.

Jetzt werde wieder die Ausgangssituation betrachtet, also ein Homomorphismus $\varphi\colon \underline{A} \longrightarrow \underline{B}$. In den obigen Beobachtungen sei $\underline{C} = \underline{\varphi(A)}$ (die Bildalgebra) und $\Theta = \mathrm{Kern}(\varphi)$ (der Kern von $\varphi$), mit den zugehörigen Homomorphismen $i\colon \varphi(A) \longrightarrow B$ und $\pi\colon A \longrightarrow A/\mathrm{Kern}(\varphi)$.

**Beobachtung:** Für den Homomorphismus $\varphi\colon \underline{A} \longrightarrow \underline{B}$ werde die Abbildung

$$\varphi'\colon A/\mathrm{Kern}(\varphi) \longrightarrow \varphi(A), \quad [x]\mathrm{Kern}(\varphi) \mapsto \varphi(x)$$

definiert. Dann ist $\varphi'$ wohldefiniert. Außerdem ist $\varphi'$ ein Isomorphismus von $\underline{A}/\mathrm{Kern}(\varphi)$ in $\underline{\varphi(A)}$.

**Beweis:** Die Abbildung $\varphi'$ ist tatsächlich *wohldefiniert*: Sie geht tatsächlich von $A/\mathrm{Kern}(\varphi)$ in $\varphi(A)$. Außerdem folgt aus $[x]\mathrm{Kern}(\varphi) = [y]\mathrm{Kern}(\varphi)$ sofort $\varphi(x) = \varphi(y)$. Es handelt sich bei $\varphi'$ um einen *Homomorphismus* (eigentlich klar, wie sollte es anders sein; dennoch – ein letztes Mal – ein derartig „schrecklicher" Beweis): Sei also $f$ ein $n$-stelliges Operatorsymbol und seien $a_1, \ldots, a_n \in A$. Dann gilt

$$\begin{aligned}
& \varphi'\big(f_{\underline{A}/\mathrm{Kern}(\varphi)}([a_1]\mathrm{Kern}(\varphi), \ldots, [a_n]\mathrm{Kern}(\varphi))\big) \\
= \; & \varphi'\big([f_{\underline{A}}(a_1, \ldots, a_n)]\mathrm{Kern}(\varphi)\big) \\
= \; & \phi\big(f_{\underline{A}}(a_1, \ldots, a_n)\big) \\
= \; & f_{\underline{B}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big) \\
= \; & f_{\underline{\varphi(A)}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big) \\
= \; & f_{\underline{\varphi(A)}}\big(\varphi'([a_1]\mathrm{Kern}(\varphi)), \ldots, \varphi'([a_n]\mathrm{Kern}(\varphi))\big)
\end{aligned}$$

Es bleibt zu zeigen, dass $\varphi'$ ein **Isomorphismus**, das heißt auch bijektiv ist: $\varphi'$ ist nach Definition offensichtlich surjektiv. Für die Injektivität werde jetzt $\varphi'\big([x]\mathrm{Kern}(\varphi)\big) = \varphi'\big([y]\mathrm{Kern}(\varphi)\big)$ vorausgesetzt. Das bedeutet $\varphi(x) = \varphi(y)$, also $x\mathrm{Kern}(\varphi)y$, also $[x]\mathrm{Kern}(\varphi) = [y]\mathrm{Kern}(\varphi)$. □

Damit ist insgesamt folgendes bewiesen (Bezeichnungen wie oben):

**Homomorphiesatz:** Sei $\varphi\colon \underline{A} \longrightarrow \underline{B}$ ein Homomorphismus. Dann kann $\varphi$ in ein Produkt $\varphi = i \circ \varphi' \circ \pi$ aus einem surjektiven Homomorphismus $\pi$ (Faktorabbildung), einem Isomorphismus $\varphi'$ und einem injektiven Homomorphismus $i$ (Inklusionsabbildung) zerlegt werden. In anderen Worten, das folgende Diagramm *kommutiert*:

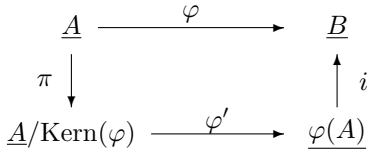



Abbildung 35: Homomorphiesatz

**Quintessenz:** „Arbeitsteilung", $\pi$ macht alles gleich, was unter $\varphi$ gleich wird, $\varphi(A)$ enthält alles, was unter $\varphi$ herauskommt. Kann $\varphi'$ nur noch ein Isomorphismus sein!

Zurück zum Beispiel $\varphi\colon \underline{G_1} \longrightarrow \underline{G_3}$. Es ist sinnvoll, sich die Zusammenhänge auch an den Verknüpfungstafeln von $\underline{G_1}$ und $\underline{G_3}$ auf Seite 70 klar zu machen:

## 2.4 Terme und Polynome

Jetzt werden die aus den fundamentalen Operationen einer Algebra „zusmmengesetzten" Operationen untersucht. Dies wird für die Untersuchung von **Gleichungen** wichtig sein.

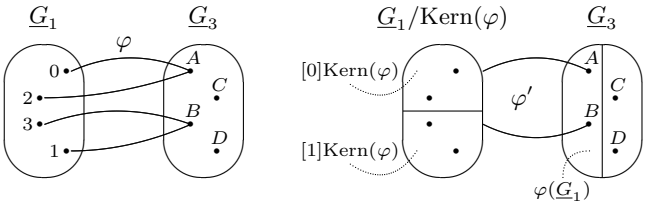



Abbildung 36: Homomorphiesatz (Beispiel)

### 2.4.1 Terme

**Definition:** Sei $(\mathcal{F}, \sigma)$ ein Ähnlichkeitstyp von Algebren, und $X$ eine Menge, deren Elemente **Variablen** genannt werden, mit $X \cap \mathcal{F} = \emptyset$. Mit folgender Rekursionsvorschrift wird die Menge $T(X)$ der **Terme** vom Typ $(\mathcal{F}, \sigma)$ über $X$ definiert:

(1) Für alle Variablen $x \in X$ liegt das 1-Tupel $(x)$ in $T(X)$,

(2) für alle $f \in \mathcal{F}$ (mit $\sigma(f) = n$) und alle $t_1, \ldots, t_n \in T(X)$ gilt $(f, t_1, \ldots, t_n) \in T(X)$.

(3) Es gibt nur die mit den Regel (1) und (2) gebildeten Terme.

Die **Termalgebra** $\underline{T}(X)$ vom Typ $(\mathcal{F}, \sigma)$ über der Variablenmenge $X$ ist definiert als die Algebra mit Grundmenge $T(X)$ und den für jedes $f \in \mathcal{F}$ ($n$-stellig) folgendermaßen definierten Operationen $f_{\underline{T}(X)}$:

$$f_{\underline{T}(X)}(t_1, \ldots, t_n) = (f, t_1, \ldots, t_n)$$

**Bemerkungen:**

- Für $t \in T(X)$ schreibt man oft auch $t(x_1, \ldots, x_n)$, um anzudeuten, dass die in $t$ enthaltenen Variablen alle zur Menge $\{x_1, \ldots, x_n\}$ gehören. Man nennt den Term $t(x_1, \ldots, x_n)$ **$n$-stellig**.
- Für jeden gegebenen Ähnlichkeitstyp $(\mathcal{F}, \sigma)$ besteht $T(X)$ genau aus den „sinnvoll gebildeten Ausdrücken“, die mit den Elementen von $X \cup \mathcal{F}$ gebildet werden können. Sei zum Beispiel $\mathcal{F} = \{+\}$ mit $\sigma(+) = 2$, und sei $X = \{x, y, z\}$. Dann sind (beispielsweise) folgende Ausdrücke Terme über $X$:
$$(x), (y), (z), (+, x, y), (+, x, x), (+, (+, x, y), z)$$
(Diese schreibt man oft in der einfacheren Form $x, y, z, x + y, x + x, (x + y) + z$.) Die folgenden Ausdrücke sind hingegen keine Terme:
$$(x, y, +), (+, x), (+, x, y, z)$$

Unmittelbar aus obiger Definition folgt:

**Bemerkung:** Jede Termalgebra $\underline{T}(X)$ wird von der Variablenmenge $X$ erzeugt, das heißt es gilt $T(X) = \langle X \rangle$.

Es folgt eine wesentliche Eigenschaft der Algebra $\underline{T}(X)$:

**Satz:** („Einsetzungs-Homomorphismus“) Sei $\underline{T}(X)$ die Termalgebra vom Typ $(\mathcal{F}, \sigma)$ über $X$. Für jede Algebra $\underline{A}$ vom Typ $(\mathcal{F}, \sigma)$ und jede Abbildung $\varphi\colon X \longrightarrow A$ gibt es dann genau einen Homomorphismus $\bar{\varphi}\colon \underline{T}(X) \longrightarrow \underline{A}$, der $\varphi$ fortsetzt, das heißt mit $\bar{\varphi}|_x = \varphi$.

**Beweis:** Sei $\underline{A}$ vom Typ $(\mathcal{F}, \sigma)$ und $\varphi\colon X \longrightarrow A$ gegeben. Dann muss offenbar $\bar{\varphi}(x) = \varphi(x)$ für alle $x \in X$ gelten und außerdem

$$\bar{\varphi}(f, t_1, \ldots, t_n) = f_{\underline{A}}\big(\bar{\varphi}(t_1), \ldots, \bar{\varphi}(t_n)\big)$$

für jeden Term der Form $(f, t_1, \ldots, t_n)$. Damit ist $\bar{\varphi}$ auf ganz $T(X)$ definiert. Wegen $f_{\underline{T}(X)}(t_1, \ldots, t_n) = (f, t_1, \ldots, t_n)$ ist $\varphi$ automatisch ein Homomorphismus. □

### 2.4.2 Termfunktionen

**Definition:** Sei $t$ ein Term von Typ $(\mathcal{F}, \sigma)$ über $X = \{x_1, \ldots, x_n\}$ und $\underline{A}$ eine Algebra desselben Typs. Für $a_1, \ldots, a_n \in A$ sei $\varphi_{a_1,\ldots,a_n}$ der nach obigem Satz eindeutig bestimmte Homomorphismus mit $x_i \mapsto a_i$ für $i = 1, \ldots, n$. Dann entsteht eine $n$-stellige Operation $t_{\underline{A}}\colon A^n \longrightarrow A$ durch:

$$t_{\underline{A}}(a_1, \ldots, a_n) := \varphi_{a_1,\ldots,a_n}(t)$$

Die derart gebildeten Operationen $t_{\underline{A}}$ heißen **Termfunktionen** auf $\underline{A}$. Die Menge aller Termfunktionen auf $\underline{A}$ wird mit $T(\underline{A})$ bezeichnet.

> *Also:* Termfunktionen entstehen aus Termen, indem man für diese Variablen Elemente einsetzt und dann das Ergebnis „ausrechnet“.

Die Termfunktionen einer Algebra sind genau die Operationen, die man durch **Superposition** („ineinander einsetzen“) aus den fundamentalen Operationen der Algebra sowie den **Projektionsabbildungen** $p_i^n(x_1, \ldots, x_n) = x_i$ erhält.

Die Termfunktionen liefern für jede Algebra unmittelbar den Unteralgebren. Hüllenoperator (der Beweis ist offensichtlich):

**Tatsache:** Für jede Algebra $A$ und jede Teilmenge $C \subseteq A$ gilt:

$$\langle C \rangle = \{t_A(c_1, \ldots, c_n) \mid n \in \mathbb{N}_0, t \in T(x_1, \ldots, x_n), c_1, \ldots, c_n \in C)\}$$

Termfunktionen verhalten sich bezüglich den Homomorphismen einer Algebra wie fundamentale Operationen (auch ziemlich offensichtlich, aber trotzdem mit Beweis):

**Satz:** Die Algebren $\underline{A}$ und $\underline{B}$ und der $n$-stellige Term $t$ seien alle vom gleichen Typ. Für jeden Homomorphismus $\varphi\colon \underline{A} \longrightarrow \underline{B}$ und alle $a_1, \ldots, a_n \in A$ gilt dann:

$$\varphi\big(t_{\underline{A}}(a_1, \ldots, a_n)\big) = t_{\underline{B}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big)$$

**Beweis** mit Induktion über den Aufbau der Terme („algebraischer Induktion“): Sei $t \in T(x_1, \ldots, x_n)$. Im Fall $t = x_i$ gilt die Behauptung offensichtlich. Nun sei $t = (f, t^1, \ldots, t^m)$, mit $m$-stelligem $f \in \mathcal{F}$ und Termen $t^1, \ldots t^m \in T(x_1, \ldots, x_n)$. Werde angenommen, dass die Behauptung für $t^1, \ldots, t^m$ schon gezeigt sei. Dann gilt:

$$\begin{aligned} & \varphi\big(t_{\underline{A}}(a_1, \ldots, a_n)\big) \\ = \; & \varphi\big(f_{\underline{A}}(t^1_{\underline{A}}(a_1, \ldots, a_n), \ldots, t^m_{\underline{A}}(a_1, \ldots, a_n))\big) \\ = \; & f_{\underline{B}}\big(\varphi(t^1_{\underline{A}}(a_1, \ldots, a_n)), \ldots, \varphi(t^m_{\underline{A}}(a_1, \ldots, a_n))\big) \\ = \; & f_{\underline{B}}\big(t^1_{\underline{B}}(\varphi(a_1), \ldots, \varphi(a_n)), \ldots, t^m_{\underline{B}}(\varphi(a_1), \ldots, \varphi(a_n))\big) \\ = \; & t_{\underline{B}}\big(\varphi(a_1), \ldots, \varphi(a_n)\big) \end{aligned}$$

□

### 2.4.3 Polynome

**Definition:** Sei $\underline{A}$ eine Algebra. Aus einem Term $t \in T(X)$ entsteht ein **Polynom**, indem für einige Variablen von $t$ Elemente von $A$ eingesetzt werden. Die Menge all solcher Polynome werde mit $P_A(X)$ bezeichnet. Indem man für die verbliebenen Variablen eines Polynoms $p(x_1, \ldots, x_n)$ beliebige Elemente $a_1, \ldots, a_n \in A$ einsetzt und dann auswertet, erhält man eine **Polynomfunktion** $p_A(x_1, \ldots, x_n)$ auf $A$. Die Menge aller Polynomfunktionen auf $A$ werde mit $P(A)$ bezeichnet.

Diese Definition war nicht sehr formal, darum zum besseren Verständnis ein Beispiel:

**Beispiel:** Sei $\underline{A} = (A; +)$ eine Algebra des Typs $\mathcal{F} = \{+\}$ mit $\sigma(+) = 2$ und sei $b, c \in A$. Dann sind (zum Beispiel) die folgenden Ausdrücke Polynome von $A$ (aus denen dann jeweils Polynomfunktionen gewonnen werden können):

$$x + y \text{ (alle Terme sind Polynome!)}, \quad b + z,$$

$$(b + y) + z, \quad (b + y) + c, \quad \big((x + b) + c\big) + (z + b)$$

So wie die Termfunktionen die Unteralgebren einer Algebra erhalten (siehe Tatsache auf Seite 75), so erhalten die Polynomfunktionen die Kongruenzrelationen einer Algebra (ohne Beweis):

**Tatsache:** Die Polynomfunktionen einer Algebra $\underline{A}$ sind mit allen Kongruenzrelationen von $A$ verträglich, das heißt für $n \in \mathbb{N}_0$, $p \in P_A(x_1, \ldots, x_n)$, $\Theta \in \mathrm{Con}(\underline{A})$ folgt aus $a_i \Theta b_i$, $i = 1, \ldots, n$, immer:

$$P_{\underline{A}}(a_1, \ldots, a_n) \Theta P_{\underline{A}}(b_1, \ldots, b_n)$$

## 2.5 Gleichungen, freie Algebren, Gleichungstheorie

In diesem Abschnitt wird vieles nur „angerissen“, aber trotzdem einige Grundbegriffe vorgestellt. Im darauffolgenden Abschnitt über **boolesche Algebren** wird einiges verwendet werden. Auf diese Weise wird auch das folgende Kapitel über **Logik** vorbereitet.

### 2.5.1 Gleichungen

**Definition:** Sei $T(X)$ die Menge aller Terme vom Typ $(\mathcal{F}, \sigma)$ über der Variablenmenge $X$. Dann heißt jedes Paar $(s,t) \in T(X) \times T(X)$ eine **Gleichung** über $X$. Anstelle von $(s,t)$ schriebt man oft:

$$s \approx t \quad \text{oder} \quad s(x_1, \ldots x_n) \approx t(x_1, \ldots, x_n)$$

(letzteres um anzudeuten, dass die in $s$ und $t$ vorkommenden Variablen in der Menge $\{x_1, \ldots, x_n\}$ enthalten sind). Eine Algebra $\underline{A}$ vom Typ $(\mathcal{F}, \sigma)$ *erfüllt* die Gleichung $s(x_1, \ldots x_n) \approx t(x_1, \ldots, x_n)$ (oder diese Gleichung *gilt* in $\underline{A}$), falls

$$s_{\underline{A}}(a_1, \ldots, a_n) = t_{\underline{A}}(a_1, \ldots, a_n)$$

gilt für jede Belegung $a_1, \ldots, a_n \in A$. In diesem Fall schreibt man

$$\underline{A} \models s(x_1, \ldots x_n) \approx t(x_1, \ldots, x_n) \quad \text{oder} \quad \underline{A} \models s \approx t$$

Beispielsweise ist eine Algebra $\underline{A} = (A; \cdot)$ mit einer zweistelligen Operation $\cdot$ genau dann *kommutativ*, falls:

$$\underline{A} \models x \cdot y \approx y \cdot x$$

### 2.5.2 Gleichungstheorien

**Definition:** Für jedes **Gleichungssystem** (Gleichungsmenge) $\Sigma \subseteq T(X) \times T(X)$ über der Variablenmenge $X$ sei

$$M(\Sigma) := \{\underline{A} \mid \underline{A} \models s \approx t \text{ für alle } (s,t) \in \Sigma\}$$

die Klasse aller **Modelle** von $\Sigma$.

Für jede Klasse $\mathcal{K}$ von Algebren sei

$$G_X(\mathcal{K}) := \{(s,t) \in T(X) \times T(X) \mid \underline{A} \models s \approx t \text{ für alle } \underline{A} \in \mathcal{K}\}$$

die Menge aller in allen Algebren von $\mathcal{K}$ gültigen Gleichungen über der Variablenmenge $X$.

Die Klassen von Algebren der Form $\mathcal{K} = M(\Sigma)$ heißen **gleichungsdefiniert**. Jede Menge von Gleichungen der Form $\Sigma = G_X(\mathcal{K})$ wird eine **Gleichungstheorie** über $X$ genannt.

**Beispiele und Bemerkungen:**

- Da Gruppen mit Hilfe von Gleichungen definiert sind, ist die Klasse aller Gruppen eine gleichungsdefinierte Klasse. Das selbe gilt für viele andere schon behandelte Klassen von Algebren!
- Beispielsweise bilden alle Gleichungen (über einer gegebener Variablenmenge $X$), die in *allen* Gruppen gelten, eine Gleichungstheorie. Es gibt beliebig viele andere Beispiele. In vielen Fällen ist es ein großes (oft sogar prinzipiell unlösbares!) Problem festzustellen, ob eine vorgegebene Gleichung zu einer gegebenen Gleichungstheorie gehört oder nicht.
- Am bequemsten ist es, immer die abzählbar-unendliche Variablenmenge $X = \{x_1, x_2, x_3, \ldots\}$ zu verwenden. Jedenfalls enthält jede Gleichung nur endlich viele Variablen, also können alle Gleichungen in dieser Variablenmenge $X$ formuliert werden!

**Satz:** Sei $\mathcal{K}$ eine Klasse von Algebren eines gegebenen Typs $(\mathcal{F}, \sigma)$ und sei $\underline{T}(X)$ die Termalgebra dieses Typs über der Variablenmenge $X$. Dann gilt:

$$G_X(\mathcal{K}) = \bigcap\{\text{Kern}(\varphi) \mid \varphi: \underline{T}(X) \longrightarrow \underline{A}, \underline{A} \in \mathcal{K}\}$$

Insbesondere ist $G_X(\mathcal{K})$ immer eine Kongruenzrelation von $\underline{T}(X)$.

Der Beweis dieses Satzes ist recht leicht, wird hier aber nicht geführt. Das selbe gilt für den folgenden Satz, der den entsprechenden Satz für Termalgebren von Seite 75 verallgemeinert. In diesem Satz wird anstelle einer jeden Variablen $x \in X$ die Kongruenzklasse $\bar{x} := [x]G_X(\mathcal{K})$ verwendet und dem entsprechend $\bar{X} = \{\bar{x} \mid x \in X\}$ anstelle von $X$.

**Satz** („Einsetzungs-Homomorphismus“ verallgemeinert): Für jede Algebra $\underline{A} \in \mathcal{K}$ und jede Abbildung $\varphi: \bar{X} \longrightarrow A$ gibt es genau einen Homomorphismus $\bar{\varphi}: \underline{T}(X)/G_X(\mathcal{K}) \longrightarrow \underline{A}$, der $\varphi$ fortsetzt, das heißt mit $\bar{\varphi}|_{\bar{X}} = \varphi$.

Wann liegt die Algebra $\underline{T}(X)/G_X(\mathcal{K})$ selbst in der Klasse $\mathcal{K}$? Jedenfalls dann, wenn $\mathcal{K}$ unter der Bildung homomorpher Bilder von Unteralgebren und direkter Produkte abgeschlossen ist, das heißt falls $\text{H}(\mathcal{K}) \subseteq \mathcal{K}$, $\text{S}(\mathcal{K}) \subseteq \mathcal{K}$ und $\text{P}(\mathcal{K}) \subseteq \mathcal{K}$ gilt. Dies lässt sich übrigens knapper schreiben als $\text{HSP}(\mathcal{K}) \subseteq \mathcal{K}$ (wobei es auf die Reihenfolge von H, S und P sehr wohl ankommt).

### 2.5.3 Frei erzeugte Algebren

**Feststellung:** Für jede HSP-abgeschlossene Klasse $\mathcal{K}$ gilt:

$$\underline{T}(X)/G_X(\mathcal{K}) \in \mathcal{K}$$

**Bemerkungen:** In diesem Fall nennt man $\underline{T}(X)/G_X(\mathcal{K})$ die von $X$ **frei erzeugte Algebra** in $\mathcal{K}$ und bezeichnet sie kürzer mit

$$\underline{F}_{\mathcal{K}}(X)$$

Also ist $\underline{F}_{\mathcal{K}}(X)$ die „allgemeinste“ Algebra mit Erzeugendenmenge $X$ (eigentlich mit Erzeugendenmenge $\bar{X}$).

**Beispiele:** Sei $\mathcal{A}$ die Klasse aller abelschen (kommutativen) Gruppen. Ganz offenbar ist $\mathcal{A}$ HSP-abgeschlossen. Als Operationssymbole werden, wie bei Gruppen üblich, $\cdot$ und $^{-1}$ und 1 verwendet:

- *Einelementige Variablenmenge* $X = \{x\}$: Aus jeder Kongruenzklasse

  $$[t(x)]G_X(\mathcal{K})$$

  wird ein **Repräsentant** verwendet, in diesem Fall naheliegenderweise die Elemente $x^k$, $k \in \mathbb{Z}$. Unter Begehung kleiner „Ungenauigkeiten“ gilt also:

  $$\underline{F}_{\mathcal{A}}(\{x\}) = (\{x^k \mid k \in \mathbb{Z}\}; \cdot, ^{-1}, 1)$$

  Als Beispiel eine Anwendung des Einsetzungs-Homomorphismus: Es gibt genau einen Homomorphismus

  $$\varphi: \underline{F}_{\mathcal{A}}(\{x\}) \longrightarrow \underline{\mathbb{Z}}_6 = (\mathbb{Z}_6; +, -, 0) \quad \text{mit } \varphi(x) = 3$$

nämlich mit $\varphi(x^k) = 0$ für $k$ gerade und $\varphi(x^k) = 3$ für $k$ ungerade.

Übrigens: $\underline{F}_{\mathcal{A}}(\{x\})$ ist isomorph zu $\underline{\mathbb{Z}} = (\mathbb{Z}; +, -, 0)$, ein Isomorphismus ist gegeben durch $x^k \longrightarrow k$.

- Als Übung: Stelle analog Überlegungen für die freie 2-erzeugte abelsche Gruppe $\underline{F}_{\mathcal{A}}(\{x, y\})$ an!

### 2.5.4 Hauptsätze der Gleichungstheorie

Es folgen wiederum ohne Beweis, die zwei Hauptsätze der Gleichungstheorie. Beide wurden in den 30er Jahren von G. Birkhoff gefunden, der in dieser Zeit viele wesentliche Grundlangen der Allgemeinen Algebra entwickelt hat.

**Erster Hauptsatz der Gleichungstheorie** *Birkhoff, 1935:* Eine Klasse $\mathcal{K}$ von Algebren eines gegebenen Typs ist genau dann gleichungsdefiniert, wenn sie HSP-abgeschlossen ist, das heißt wenn $\mathrm{HSP}(\mathcal{K}) \subseteq \mathcal{K}$ gilt.

Es sei eine *kleine* Anwendung dieses Satzes angegeben. Frage: Könnte man Körper (ausschließlich mit Hilfe von Gleichungen definieren, bei Verwendung eines geeigneten Ähnlichkeitstyps, das heißt geeigneter Operationen? Antwort: Nein, denn direkte Produkte von Körpern sind keine Körper!

Es folgt eine Charakterisierung der Gleichungstheorien, das heißt derjenigen Gleichungsmengen $\Sigma$, die von der Form $\Sigma = G_X(\mathcal{K})$ sind. Für jede Gleichungstheorie $G_X(\mathcal{K})$ gelten offenbar folgende Regeln (anstelle von $(s, t)$ wird suggestiver $s \approx t$ geschrieben):

(G1) Für alle $s \in T(X)$ gilt $s \approx s \in G_X(\mathcal{K})$,

(G2) aus $s \approx t \in G_X(\mathcal{K})$ folgt $t \approx s \in G_X(\mathcal{K})$,

(G3) aus $s \approx t \in G_X(\mathcal{K})$ und $t \approx u \in G_X(\mathcal{K})$ folgt $s \approx u \in G_X(\mathcal{K})$,

(G4) aus $f \in \mathcal{F}$ ($n$-stellig) und $s_i \approx t_i \in G_X(\mathcal{K})$ für $i = 1, \ldots, n$ folgt $f(s_1, \ldots, s_n) \approx f(t_1, \ldots, t_n) \in G_X(\mathcal{K})$,

(G5) aus $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n) \in G_X(\mathcal{K})$ und $u_1, \ldots, u_n \in T(X)$ folgt $s(u_1, \ldots, u_n) \approx t(u_1, \ldots, u_n) \in G_X(\mathcal{K})$.

Die Regeln (G1)-(G3) sagen aus, dass $G_X(\mathcal{K})$ eine Äquivalenzrelation auf $T(X)$ ist und (G4) besagt, dass $G_X(\mathcal{K})$ sogar eine Kongruenzrelation von $\underline{T}(X)$ ist (was oben schon festgestellt wurde). Regel (G5) lässt sich (gleichwertig) anders formulieren:

(G5') Ist $\varphi: \underline{T}(X) \longrightarrow \underline{T}(X)$ ein Homomorphismus und gilt $s \approx t \in G_X(\mathcal{K})$, dann gilt auch $\varphi(s) \approx \varphi(t) \in G_X(\mathcal{K})$.

Also ist $G_X(\mathcal{K})$ mit allen Endomorphismen von $\underline{T}(X)$ verträglich. Kongruenzrelationen mit dieser Eigenschaft nennt man **voll-invariant**. Also:

$G_X(\mathcal{K})$ ist eine voll-invariante Kongruenzrelation von $\underline{T}(X)$.

Es gilt aber noch mehr:

**Zweiter Hauptsatz der Gleichungstheorie** *Birkhoff, 1935:* Ein Gleichungssystem $\Sigma \subseteq T(X) \times T(X)$ ist genau dann eine Gleichungstheorie, wenn $\Sigma$ eine voll-invariante Kongruenzrelation von $\underline{T}(X)$ ist.

Eine wesentliche Folgerung dieses Satzes soll noch diskutiert werden. Sei $\Sigma \subseteq T(X) \times T(X)$ ein Gleichungsmenge. Frage: Welche Gleichungen folgen aus $\Sigma$?

Antwort A: Es folgen alle Gleichungen, die sich ausgehend von $\Sigma$, durch – eventuell mehrfache – Anwendung der Regeln (G1)-(G5) erhalten lassen. Folgt auf diese Art eine Gleichung $s \approx t$ aus $\Sigma$, so schreibt man dafür auch:

$$\Sigma \vdash s \approx t$$

Antwort B: Es folgen genau die Gleichungen $s \approx t$ aus $\Sigma$, die in allen Algebren gelten, in denen alle Gleichungen aus $\Sigma$ gelten, das heißt aus $\Sigma$ folgen genau die Gleichungen in $G_X(M(\Sigma))$. Bei dieser Art Folgerung schreibt man:

$$\Sigma \models s \approx t$$

Offenbar enthält Antwort B die „stärkere“ Folgerungsart, es gilt immer

$$\Sigma \vdash s \approx b \;\Rightarrow\; \Sigma \models s \approx t.$$

Aber tatsächlich sind beide Folgerungsarten gleichwertig:

**Vollstïndigkeitssatz der Gleichungslogik:**

$$\vdash \;=\; \models$$

## 2.6 Boolesche Algebra

Dieser letzte Abschnitt des Algebra-Kapitels behandelt ein Thema, das vor allem deshalb interessant ist, weil es einerseits algebraische und andererseits ordnungs- und verbandstheoretische Aspekte miteinander verbindet und weil es in der Aussagelogik unmittelbar anwendbar ist.

**Definition:** Eine Algebra $\underline{B} = (B; +, \cdot, ', 0, 1)$ vom Typ $(2, 2, 1, 0, 0)$ wird **boolesche Algebra** genannt, falls

(verb) $(B; +, \cdot)$ ein Verband ist

und die folgenden Gleichungen gelten:

| | | |
|---|---|---|
| (dist) | $x \cdot (y + z) = x \cdot y + x \cdot z$ | **Distributivität** |
| (komp) | $x \cdot x' = 0, \quad x + x' = 1$ | **Komplemente** |
| (null) | $x \cdot 0 = 0, \quad x + 0 = x$ | **Nullelement** |
| (eins) | $x \cdot 1 = x, \quad x + 1 = 1$ | **Einselement** |

**Bemerkungen:**

- In der zum Verband $(B; +, \cdot)$ gehörigen geordneten Menge $(B, \leq)$ ist 0 das kleinste Elemente und 1 das größte Element.

- In obiger Definition befinden sich „zu viele“ Gleichungen. Zum Beispiel können die ersten Gleichungen in (null) und (eins) aus den anderen Gleichungen hergeleitet werden. Natürlich gilt das selbe auch für die zweiten Gleichungen in (null) und (eins). Von den drei Verbandsgleichungen wird nur (komm) und (abs) benötigt, während (ass) aus den anderen Gleichungen hergeleitet werden kann. Dies sind drei Übungsaufgaben.

Natürlich gelten in jeder booleschen Algebra noch weitere Gleichungen und Eigenschaften, zum Beispiel diese:

**Bemerkung:** In jeder booleschen Algebra $\underline{B}$ gelten für alle $x, y, z \in B$:

| | | |
|---|---|---|
| (a) | $x + (y \cdot z) = (x + y) \cdot (x + z)$ | **duale Distributivität** |
| (b) | $x \cdot y = 0, \quad x + y = 1 \quad \Rightarrow \quad y = x'$ | **Komplementeindeutigkeit** |
| (c) | $(x + y)' = x' \cdot y', \quad (x \cdot y)' = x' + y'$ | **de Morgan'sche Gesetze** |
| (d) | $x'' = x, \quad 0' = 1, \quad 1' = 0$ | |

**Beweis:** (a) Die Verbandsgleichungen und (dist) liefern:

$$(x + y)(x + z) = (x + y)x + (x + y)z = xx + yx + xz + yz = x + yz$$

(b) Es gilt $x(x' + y) = xx' + xy = 0 + 0 = 0$. Dies und $y \leq x' + y$ ergeben:

$$x' + y = 1(x' + y) = (x + y)(x' + y) = x(x' + y) + y(x' + y) = 0 + y = y$$

Ganz ähnlich ergibt sich

$$x' + y = 1(x' + y) = (x + x')(x' + y) = x(x' + y) + x'(x' + y) = 0 + x' = x'$$

also insgesamt $y = x'$.

(c) Es wird $x'y'(x + y) = 0$ und $x'y' + (x + y) = 1$ gezeigt. Die behauptete Gleichung $x'y' = (x+y)'$ folgt dann mit (b). Verwendet wird die Distributivität und duale Distributivität:

$$x'y'(x + y) = x'y'x + x'y'y = y'0 + x'0 = 0 + 0 = 0$$

$$x'y' + (x + y) = (x' + (x + y))(y' + (x + y)) = (1 + y)(1 + x) = 1 \cdot 1 = 1$$

Die zweite Gleichung in (c) kann „dual“ bewiesen werden (indem im eben geführten Beweis + und $\cdot$ vertauscht werden).

(d) $x$ und $x'' = (x')'$ sind beides Komplemente von $x'$, woraus mit (b) sofort $x = x''$ folgt. Mit (null) erhält man $1 \cdot 0 = 0$, $1 + 0 = 1$ und wiederum mit (b) folgt $0 = 1'$. Analog ergibt sich $1 = 0'$ □

**Beispiele:**

- Folgende Operationen liefern eine 2-elementige boolesche Algebra $\underline{B_2} := (\{0, 1\}; +, \cdot, ', 0, 1)$:

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $\cdot$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $x$ | 0 | 1 |
|---|---|---|
| $x'$ | 1 | 0 |

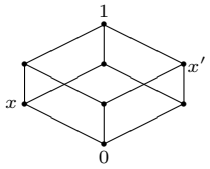



Abbildung 37: Liniendiagramm einer 8-elementigen boolesche Algebra)

- Das Liniendiagramm zeigt eine boolesche Algebra mit acht Elementen.
- Für jede Menge $A$ erhält man eine boolesche Algebra durch

$$(\mathcal{P}(A); \cup, \cap, \overline{\ }, \emptyset, A)$$

(die **Potenzmengenalgebra** auf $A$). Die Operationen sind mengentheoretische Vereinigung und Schnitt, und die Komplementierung $\overline{X} = A \setminus X$.

### 2.6.1 Atome

Die Potenzmengenalgebren sind „typische“ boolesche Algebren. Es wird gezeigt, dass jede *endliche* boolesche Algebra isomorph ist zu einer solchen. Hierfür wird benötigt:

**Definition:** Sei $\underline{B}$ eine boolesche Algebra. Ein Element $a \in B$ heißt ein **Atom** von $\underline{B}$, falls $a$ ein **oberer Nachbar** des kleinsten Elements 0 von $B$ ist (das heißt falls $a > 0$ gilt, es aber kein Element $b$ gibt mit $0 < b < a$). Die Menge aller Atome von $\underline{B}$ wird mit $\mathrm{At}(\underline{B})$ bezeichnet.

**Lemma:** In jeder *endlichen* booleschen Algebra $\underline{B}$ ist jedes Element $b \in B$ eindeutig durch die Elemente unterhalb von $b$ bestimmt.
Genauer: Sei $\{a \in \mathrm{At}(\underline{B}) \mid a \leq b\} = \{a_1, \ldots, a_k\}$ (mit $k$ verschiedenen Elementen). Dann gilt:

$$b = a_1 + \cdots + a_k$$

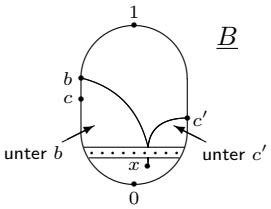



Abbildung 38: Atome

**Beweis:** Sei $c := a_1 + \cdots + a_k$. Es soll $c = b$ gezeigt werden. Wegen $a_1, \ldots, a_k \leq b$ gilt $c \leq b$: Werde jetzt $c < b$ angenommen. Offenbar gilt:

$$bc' + c = bc' + bc = b(c + c') = b \cdot 1 = b$$

Es folgt $bc' > 0$. In jeder endlichen booleschen Algebra hat jedes Element ungleich 0 ein Atom unter sich (Beweis hierfür?). Also gibt es ein Atom $x \leq bc'$

Dann gibt es aber $x \leq c'$ und $x \leq b$, wobei letzteres auch $x \leq c$ impliziert. Daher gilt $x \leq cc' = 0$, ein Widerspruch! Also muss $c = b$ gelten. □

Mit diesem Lemma folgt der angekündigte Sachverhalt:

**Satz:** Sei $\underline{B}$ eine endliche boolesche Algebra. Dann wird ein Isomorphismus von $\underline{B}$ auf die Potenzmengenalgebra auf der Menge $\mathrm{At}(\underline{B})$ der Atome von $\underline{B}$ gegeben durch

$$\varphi(b) := \{a \in \mathrm{At}(\underline{B}) \mid a \leq b\}$$

**Beweis:** Folgendes muss gezeigt werden:

(1) $\varphi$ ist injektiv,

(2) $\varphi$ ist surjektiv,

(3) $\varphi(x + y) = \varphi(x) \cup \varphi(y)$ für alle $x, y \in B$,

(4) $\varphi(xy) = \varphi(x) \cap \varphi(y)$ für alle $x, y \in B$,

(5) $\varphi(x') = \overline{\varphi(x)}$ für alle $x \in B$.

Eigentlich müsste noch $\varphi(0) = \emptyset$ und $\varphi(1) = \mathrm{At}(\underline{B})$ gezeigt werden, aber dies folgt schon aus obigem (beziehungsweise ist sowieso klar).

(1) folgt unmittelbar aus dem Lemma, denn aus $\varphi(b) = \varphi(c)$ ergibt sich

$$b = \sum \varphi(b) = \sum \varphi(c) = c$$

(wobei zum Beispiel $\varphi(b)$ die mit + gebildete Summe aller Elemente von $\varphi(b)$ bezeichnet).

(2) Für jede Teilmenge $A \subseteq \mathrm{At}(\underline{B})$ muss ein $b \in B$ gefunden werden mit $\varphi(b) = A$. Sei $A = \{a_1, \ldots, a_k\}$ und werde $b := \sum A$ gesetzt. Klar ist $\varphi(b) \supseteq A$ und es muss $\varphi(b) = A$ gezeigt werden. Werde im Gegensatz hierzu angenommen, es gäbe ein Element $a \in \varphi(b) \setminus A$. Dann ergibt sich:

$$a = ab = a(a_1 + \ldots + a_k) = aa_1 + \ldots + aa_k = 0 + \ldots + 0 = 0 \qquad \lightning$$

(3) Gelte $\varphi(x) = C$, $\varphi(y) = D$. Dann gilt $x = \sum D$ (Lemma!) und

$$x + y = \sum C + \sum D = \sum (C \cup D) = \sum (\varphi(x) \cup \varphi(y)).$$

Wie im Beweis von (2) folgt hieraus $\varphi(x + y) = \varphi(x) \cup \varphi(y)$.

(4) Gelte wieder $\varphi(x) = C$, $\varphi(y) = D$. Dann besteht $C \cap D$ genau aus den Atomen unter $x$ und unter $y$, das heißt unter $xy$. Nach Definition von $\varphi$ gilt $\varphi(xy) = C \cap D$ $(= \varphi(x) \cap \varphi(y))$.

(5) Gelte $\varphi(x) = C$, $\varphi(x') = D$. Aus $x + x' = 1$ folgt, $C \cup D = At(\underline{B})$, und aus $xx' = 0$ folgt $C \cap D = \emptyset$. Doch das impliziert

$$D = At(B) \setminus C = \overline{C} = \overline{\varphi(x)}$$

□

Alle endlichen booleschen Algebren sind, nach dem eben Bewiesenen, isomorph zu Potenzmengenalgebren, also sehr einfach strukturiert. Im Gegensatz dazu können unendliche boolesche Algebren „unendlich kompliziert“ sein!

Die „praktische“ Bedeutung der 2-elementigen booleschen Algebra

$$\underline{B}_2 = (\{0,1\}; +, \cdot, ', 0, 1)$$

(zum Beispiel für die Konstruktion elektronischer Schaltkreise) liegt sehr stark in den Termoperationen:

### 2.6.2 Boolsche Terme

**Definition:** Die Terme in der Sprache (also dem Typ boolescher Algebren) werden auch **boolesche Terme** genannt.

**Beispiele** über der Variabenmenge $\{x_1, x_2, x_3\}$ sind unter anderen:

$$x_2 + 1, \quad (x_2, x_3')''', \quad x_1 x_2' + x_3, \quad ((x_1 x_2' + x_3)' x_1 + x_2')$$

Bekanntlich werden alle Terme, über Algebren des entsprechenden Typs, zu Termfunktionen der Algebra. Die Termfuktionen boolescher Algebren werden oft **boolesche Funktionen** genannt. Obwohl die 2-elementige boolesche Algebra $\underline{B}_2$ äußerst simpel ist, bringt sie interessante praktische und theoretische Sachverhalte. Darum werden hier zuerst boolesche Funktionen über $\underline{B}_2$ betrachtet:

**Beispiel:** Der boolesche Term $t(x_1, x_2, x_3) = ((x_1 x_2' + x_3)' x_1 + x_2')'$ liefert eine 3-stellige boolesche Funktion $t_{\underline{B}_2}(x_1, x_2, x_3)$ auf $\{0,1\}$, mit

$$t_{\underline{B}_2}(0,0,0) = 0, \quad t_{\underline{B}_2}(0,0,1) = 0, \quad t_{\underline{B}_2}(0,1,0) = 1, \quad t_{\underline{B}_2}(0,1,1) = 1, \quad \text{usw.}$$

Boolsche Funktionen auf $t_{\underline{B}_2}$ liefern alle Operationen auf $\{0,1\}$.

**Satz:** Jede Operation auf $\{0,1\}$ ist eine boolesche Funktion.

Anstelle eines Beweises folgt ein Beispiel, aus dem sich der allgemeine Beweis aber ablesen läßt. Es wird gezeigt, daß folgende 3-stellige Operation $f(x_1, x_2, x_3)$ auf $\{0,1\}$ eine boolesche Funktion ist:

| $x_1$ | $x_2$ | $x_4$ | $f(x_1, x_2, x_3)$ | | |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | $\rightarrow$ | $x_1' x_2' x_3'$ |
| 0 | 0 | 1 | 1 | $\rightarrow$ | $x_1' x_2' x_3$ |
| 0 | 1 | 0 | 0 | | |
| 0 | 1 | 1 | 0 | | |
| 1 | 0 | 0 | 1 | $\rightarrow$ | $x_1 x_2' x_3'$ |
| 1 | 0 | 1 | 0 | | |
| 1 | 1 | 0 | 1 | $\rightarrow$ | $x_1 x_2 x_3'$ |
| 1 | 1 | 1 | 1 | $\rightarrow$ | $x_1 x_2 x_3$ |

Die Produkte rechts in obiger Tabelle werden zu einem booleschen Term summiert:

$$t(x_1, x_2, x_3) = x_1' x_2' x_3' + x_1' x_2' x_3 + x_1 x_2' x_3' + x_1 x_2 x_3' + x_1 x_2 x_3$$

Tatsächlich gilt $t_{B_2}(x_1, x_2, x_3) = f(x_1, x_2, x_3)$ für alle $x_1, x_2, x_3 \in \{0, 1\}$. Dies könnte man leicht nachrechnen. Es soll hier aber systematisch erklärt werden:

Offenbar gilt $t_{B_2}(x_1, x_2, x_3) = 1$ für $x_1, x_2, x_3 \in \{0, 1\}$ genau dann, wenn $x_1 y_2 y_3 = 1$ gilt für einen der Summanden $y_1 y_2 y_3$ von $t$ (wobei $y_i = x_i$ oder $y_i = x_1'$ gelten kann, für $i \in \{1, 2, 3\}$). Aber $y_1 y_2 y_3 = 1$ gilt genau für $y_1 = y_2 = y_3 = 1$. Betrachtet man, zum Beispiel, den dritten Summanden $x_1 x_2' x_3'$, der die zugehörige Zeile der Wertetabelle darstellt:

| 1 | 0 | 0 | 1 | $\rightarrow$ | $x_1$ | $\cdot$ | $x_2$ | $\cdot$ | $x_3$ |
|---|---|---|---|---|---|---|---|---|---|
| eins | null | null | eins | | kein Strich | | Strich | | Strich |

Das Produkt $y_1 y_2 y_3 = x_1 y_2' x_3'$ bewirkt $t_{B_2}(1, 0, 0) = 1$

Indem man diese Methode anwendet, erhält man immer boolesche Terme in der „vollständige Summe-von-Produkten“ Form:

- die Bedeutung von „Summe-von-Produkten“ ist klar,
- „vollständig“ bedeutet, dass in jedem der Produkte jede der Variablen $x_i$ genau einmal vorkommt, entweder als $y_i = x_i$ oder als $y_i = x_i'$.

Der Satz von Seite 84 kann auch so formuliert werden:

**Folgerung:** Die Operationen $+, \cdot, '$ auf $\{0, 1\}$ bilden eine vollständige Menge von Operationen, das heißt mit Hilfe von $+, \cdot, '$ können sämtliche Operationen auf $\{0, 1\}$ „zusammengebaut“ werden.

Dabei kann entweder $+$ oder $\cdot$ sogar weggelassen werden:

**Beobachtung:**

(a) Die Menge $\{\cdot, '\}$ ist eine vollständige Menge von Operationen auf $\{0, 1\}$.
(b) Die Menge $\{+, '\}$ ist eine vollständige Menge von Operationen auf $\{0, 1\}$.

**Beweis:** (a) Es genügt zu zeigen, dass $+$ aus $\cdot$ und $'$ gebildet werden kann. Doch dies ist einfach, denn bekanntlch gelten folgende Gleichungen:

$$x + y = (x + y)'' = (x' \cdot y')$$

(b) Der selbe Beweis mit $+$ und $\cdot$ vertauscht. □

Aber es reicht sogar eine einzige Operation (ohne Beweis):

**Beobachtung:** Die zweistellige Operation $\uparrow$ auf $\{0,1\}$ sei definiert durch:

$$x \uparrow y := x' + y' \qquad \text{Sheffer-Strich}$$

Dann ist $\{\uparrow\}$ eine vollständige Menge von Operationen auf $\{0,1\}$.

Jeder boolesche Term kann mit Hilfe der definierenden Gleichungen für boolesche Algebren in eine Standardform gebracht werden, nämlich in die **disjunkte Normalform (DNF)**. Es folgt ein Beispiel.Da man nach jeder Umformung einen anderen Term erhält, wird – wie bei Gleichungen – $\equiv$ statt $=$ geschrieben:

$$\begin{aligned} t(x_1,x_2,x_3) &= ((x_1x_2' + x_3)'x_1 + x_2')' \\ &\equiv ((x_1x_2' + x_3)'x_1)'x_2 \\ &\equiv ((x_1x_2' + x_3) + x_1')x_2 \\ &\equiv (x_1x_2' + x_3)x_2 + x_1'x_2 \\ &\equiv x_1x_2'x_2 + x_3x_2 + x_1'x_2 \\ &\equiv x_2x_3 + x_1'x_2 \\ &\equiv (x_1 + x_1')x_2x_3 + x_1'x_2(x_3 + x_3') \\ &\equiv x_1x_2x_3 + x_1'x_2x_3 + x_1'x_2x_3 + x_1'x_2x_3' \end{aligned}$$

Das selbe kann mit jedem booleschen Term gemacht werden:

**Feststellung:** Zu jedem booleschen Term gibt es eine disjunkte Normalform, die bis auf die Reihenfolge der Summanden und bis auf die Reihenfolge der Faktoren in jedem Summand eindeutig bestimmt ist.

Als nächstes wird folgende Frage beantwortet: Welches sind die Gleichungen, die in jeder booleschen Algebra gelten? Dies kann auf verblüffend einfache Weise beantwortet werden:

**Satz:** Für belibige boolesche Terme $s(x_1,\ldots,x_n)$ und $t(x_1,\ldots,x_n)$ sind folgende Aussagen äquivalent:

(i) Die Gleichung $s(x_1,\ldots,x_n) \equiv t(x_1,\ldots,x_n)$ gilt in allen booleschen Algebren,

(ii) Die Gleichung $s(x_1,\ldots,x_n) \equiv t(x_1,\ldots,x_n)$ gilt in der 2-elementigen booleschen Algebra $\underline{B}_2$,

(iii) $s(x_1,\ldots x_n)$ und $t(x_1,\ldots,x_n)$ haben dieselbe disjunkte Normalform.

**Beweis:** (i) $\Rightarrow$ (ii) ist offensichtlich.
(ii) $\Rightarrow$ (iii): Die Gültigkeit von $s \equiv t$ in $\underline{B}_2$ bedeutet $s_{\underline{B}_2} = t_{\underline{B}_2}$ für die zugehörigen booleschen Funktionen. Aber das ist nur möglich, falls $s$ und $t$ die selbe disjunkte Normalform haben.
(iii) $\Rightarrow$ (i): Sei $d$ die disjunkte Normalform von $s$ und $t$. Dann gelten in allen booleschen Algebren die Gleichungen $s \equiv d$ und $t \equiv d$ woraus sofort die Gültigkeit von $s \equiv t$ folgt.

# 3 Logik

Die boolesche Algebra, besonders die sehr einfache 2-elementige boolesche Algebra, spielt eine fundamentale Rolle in der Logik. Da diese Vorlesung ihrem Ende entgegen geht, wird die Logik hier nur sehr knapp und Oberflächlich behandelt.

Jetzt folgt ein einführender Abschnitt mit aussagenlogischen Beispielen, dann ein Abschnitt zur Systematik der Aussagenlogik, und schließlich ein Abschnitt, in dem die Prädikatenlogik in Form eines Beispiels vorgestellt wird.

## 3.1 Aussagenlogik und boolesche Algebra

In der Mitte des 19. Jahrhunderts entwickelte der britische Mathematiker G. Boole ein Kalkül für die „Gesetze des Denkens“ und schuf damit gleichermaßen die später nach ihm benannte boolesche Algebra wie auch die Aussagenlogik. Diese beschäftigt sich nicht mit ihnaltlichen Aspekten irgend welcher Aussagen, sondern nur mit den Konsequenzen, die es hat, wenn eine Aussage „wahr“ oder „falsch“ ist: Konsequenzen für andere Aussaugen, die auch „wahr“ oder „falsch“ sein können!

Es gibt folgende aussagenlogische Gundoperationen, mit denen aus vorhandenen Aussaugen (zum Beispiel $A$ oder $B$) neue Aussagen zusammengesetzt werden können:

| | | |
|---|---|---|
| $A \vee B$ | „$A$ oder $B$“ | wahr genau dann, wenn mindestens eine der Aussagen $A$ und $B$ war ist, |
| $A \wedge B$ | „$A$ und $B$“ | wahr genau dann, wenn $A$ und $B$ beide wahr sind, |
| $\neg A$ | „nicht $A$“ | wahr genau dann, wenn $A$ falsch ist. |

Setzt man 1 für „wahr“ und 0 für „falsch“, so ergeben sich folgende Wahrheitswerttabellen:

| $A$ | $B$ | $A \vee B$ | $A \wedge B$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 |

| $A$ | $\neg A$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

Mit den Warheitswerten von Aussagen wird also wie in der 2-elementigen booleschen Algebra gerechnet, wobei aber in der Regel $\vee$, $\wedge$, $\neg$ verwendet wird anstelle von $+$, $\cdot$, $'$. Es werden noch weitere, zusammengesetzte Operationen verwendet, zum Beispiel:

| | | |
|---|---|---|
| $A \to B$ | „wenn $A$ dann $B$“ | wahr genau dann, wenn $A$ falsch oder $B$ wahr ist. |

Die Aussage $A \to B$ kann als Abkürzung für $\neg A \vee B$ aufgefaßt werden (denn beide Aussagen haben die selben Warheitswerte).

**Beispiel:** Mit den Aussagen

$A$: die Katze schreit,
$B$: der Mond scheint

hat $A \to B$ den Wahrheitswert 1, außer $A$ ist „wahr“ und $B$ ist „falsch“. Man beachte: Auf einen „inneren“ Zusammenhang zwischen $A$ und $B$ kommt es nicht an!

Genau genommen werden häufig keine Aussagen betrachtet, sondern **Aussageformen**, das heißt boolesche Terme (aber üblicherweise mit $\vee$, $\wedge$, $\neg$ geschrieben). Erst indem man für die Variablen Aussagen einsetzt, wird aus der Aussageform selbst eine Aussagen. Und eine Wahrheitswerttabelle kann nie für eine konkrete Aussage, sondern nur fr̈ eine AUssageform aufgestellt wrden. es handelt sich um die Wertetabelle der zugehörigen booleschen Funktion.

Es werden folgende Bezeichnungen verwendet: zwei Aussageformen $s$ und $t$ heissen äquivalent, in Zeichen $s \equiv t$, falls $f_{\underline{B}_2} = t_{\underline{B}_2}$ gilt. (das heißt falls wi dieselben Wahrheitswerrabellen haben). Oft sucht man zu einer Aussageform eine äquivalente Aussageform, die einfacher aufgebaut ist:

**Beispiel:** Im Reisebüro schildert ein Kunde seine Wünsche für eine Urlaubsreise: „Wenn der Urlaubsort am Meer liegt, dann dürfen keine Berge in der Nähe sein. An einem Urlaubsort ohne Meer und ohne Berge muss sich ein Schwimmbad befinden. Und wenn es dort kein Meer und kein Schwimmbad gibt, dann geht es nicht ohne Berge!“. Zuerst ist der Angestellte des Reisebüros verwirrt. Doch dann gelingt es ihm, die Aussagen des Kunden zu vereinfachen. Aus erstes ordnet er den Eigenschaften des Urlaubsortes Variablen zu:

$$\text{am Meer} - x, \quad \text{mit Bergen} - y, \quad \text{Schwimmbad} - z$$

Die Urlaubswünsche des Kunden ergeben folgende Aussageform, die anschließend umgeformt wird:

$$\begin{aligned} & (x \to \neg y) \wedge ((\neg x \wedge \neg y) \to z) \wedge ((\neg x \wedge \neg z) \to y) \\ \equiv\ & (x \vee \neg y) \wedge ((\neg x \wedge \neg y) \vee z) \wedge ((\neg x \wedge \neg z) \vee y) \\ \equiv\ & \neg(x \vee y) \wedge (x \vee y \vee z) \end{aligned}$$

Jetzt weiß der Angestellte: der Kunde möchte mindestens eine der Eigenschaften „Meer“, „Berge“ oder „Schwimmbad“, aber nicht „Meer“ und „Berge“ gemeinsam.

## 3.2 Aussagenlogik: Elementare Grundbegriffe

Jetzt wird die Aussagenlogik etwas systematischer angegangen. Die Basis bildet aber immer noch die 2-elementige boolesche Algebra.

### 3.2.1 Syntax der Aussagenlogik

**Definition:** Die **atomen Formen** sind $A_1$, $A_2$, $A_3$, .... (Es können natürlich auch andere Großbuchstaben wie $A$, $B$, $C$ verwendet werden, weil dies das Schreiben vereinfacht.) Alle Ausdrücke, die durch – eventuell wiederholte – Anwendung folgender Schritte erhalten werden können, heißen **Formeln**:

(1) Alle atomaren Formeln sind Formeln

(2) Sind $F$ und $G$ Formeln, dann sind auch $(F \vee G)$ und $(F \wedge G)$ Formeln

(3) Ist $F$ eine Formel, dann ist auch $\neg F$ eine Formel

### 3.2.2 Semantik der Aussagenlogik

**Definition:** Die Elemente 0 und 1 heißen **Wahrheitswerte**. Sei $D$ die Menge atomarer Formeln. Eine **Belegung** von $D$ ist eine Abbildung $\alpha\colon D \longrightarrow \{0,1\}$. Jede soche Abbildung kann auf natürliche Weise zu einer Abbildung $\hat{\alpha}\colon E \longrightarrow \{0,1\}$ fortgesetzt werden, wobei $E$ die Menge aller mit $D$ gebildeten Formeln sei:

(1) Für jede atomare Formel $A \in D$ sei $\hat{\alpha}(A) := \alpha(A)$

(2) $\hat{\alpha}(F \vee G) := \begin{cases} 1 & \text{falls } \hat{\alpha}(F) = 1 \text{ oder } \hat{\alpha}(G) = 1, \\ 0 & \text{sonst} \end{cases}$

(3) $\hat{\alpha}(F \wedge G) := \begin{cases} 1 & \text{falls } \hat{\alpha}(F) = 1 \text{ und } \hat{\alpha}(G) = 1, \\ 0 & \text{sonst} \end{cases}$

(4) $\hat{\alpha}(\neg F) := \begin{cases} 1 & \text{falls } \hat{\alpha}(F) = 0 \\ 0 & \text{falls } \hat{\alpha}(F) = 1 \end{cases}$

Klar ist: Jede Formel $F$ kann als boolesche Funktion aufgefasst werden, und $\hat{\alpha}(F)$ ist ein Wert in der Wahrheitswerttabelle von $F$. Übrigens wird für $\hat{\alpha}(F)$ im Allgemeinen einfacher $\alpha(F)$ geschrieben.

### 3.2.3 Modelle, Gültigkeit, Erfüllbarkeit

**Definition:** Sei $F$ eine Formel und $\alpha$ eine Belegung. Falls $\alpha$ für alle in $F$ vorkommenden atomaren Formeln definiert ist (also falls $\alpha(F)$ definiert ist), dann heißt $\alpha$ zu $F$ **passend**.

Falls $\alpha$ zu $F$ passend ist und $\alpha(F) = 1$ gilt, so wird $\alpha \models F$ geschrieben. Man sagt dann: „$F$ **gilt** unter $\alpha$“ oder „$\alpha$ ist ein **Modell** für $F$“. Ist $\underline{F}$ eine Menge von Formeln, dann ist $\alpha$ ein Modell für $\underline{F}$ (oder $F$ **gilt** unter $\alpha$), falls $\alpha \models \underline{F}$ gilt, das heißt $A \models F$ für alle $F \in \underline{F}$.

Eine Formal $F$ (bzw. Formelmenge $F$) heißt **erfüllbar**, falls $\alpha \models F$ (bzw. $\alpha \models \underline{F}$) gilt für mindestens eine Belegung $\alpha$. Andernfalls heißt $F$ (bzw. $\underline{F}$) **unerfüllbar**.

Eine Formel $F$ heißt **gültig** (oder **Tautologie**), falls jede zu $F$ passende Belegung ein Modell für $F$ ist. Man schreibt $\models F$, falls $F$ eine Tautologie ist, und $\#F$ sonst.

Zum Abschluss dieses Abschnitts eine einfache Aussage:

**Satz:** Eine Formel $F$ ist genau dann eine Tautologie, wenn $\neg F$ unerfüllbar ist.

Beweis: Offensichtlich sind folgende Aussagen äquivalent:

- $F$ ist eine Tautologie
- jede zu $F$ passende Belegung ist ein Modell für $F$
- jede zu $F$, damit auch zu $\neg F$ passende Belegung ist kein Modell für $F$
- $\neg F$ besitzt kein Modell
- $\neg F$ ist unerfüllbar □

## 3.3 Prädikatenlogik erster Stufe

Ein wohlbekannter prädikatenlogischer Ausdruck aus der Analysis ist folgender:

$$\forall \varepsilon > 0 \; \exists n_0 \in \mathbb{N} \; \forall n \geq n_0 : \; |f(n) - f(n_0)| < \varepsilon$$

Dieser Ausdruck hat als Bestandteile: die Quantoren $\forall$ und $\exists$, die Funktionen (= Operationen) $|\cdot|$, $f$, $-$ sowie die Relationen $>$, $\geq$, $<$.

Zuerst wird der syntaktische Sprachrahmen abgesteckt:

### 3.3.1 Syntax der Prädikatenlogik

**Definition:** Es werden die **Variablen** $x_1, x_2, x_3, \ldots$ verwendet (manchmal auch $\ldots, x, y, z$), die **Prädikatssymbole** $P_i^k$ und die **Funktionssymbole** $f_i^k$ (manchmal auch $P, Q, R$ bzw. $f, g, h$), wobei $i$ nur der Unterscheidung dient (**Unterscheidungsindex**) und $k$ die Stelligkeit angibt. Was die mit den Funktionssymbolen $f_i^k$ und den Variablen $x_j$ gebildeten Terme sind, ist aus Abschnitt 2.4 klar. Man erhält die Formeln der Prädikatenlogik durch – eventuell mehrfache – Anwendung folgender Regeln:

(1) Für jedes $k$-stellige Prädikatssymbol $P$ und beliebige Terme $t_1, \ldots, t_k$ ist $P(t_1, \ldots, t_k)$ eine Formel

(2) Für jede Formel $F$ ist $\neg F$ eine Formel

(3) Sind $F$ und $G$ Formeln, dann sind auch $(F \vee G)$ und $(F \wedge G)$ Formeln

(4) Für jede Variable $x$ und jeder Formel $F$ sind auch $\exists x F$ und $\forall x F$ Formeln

Die Formeln in (1) heißen **atomare Formeln**. Eine Formel $F$ heißt **Teilformel** einer Formel $G$, falls $F$ in $G$ vorkommt. Eine Variable $x$ kann in einer Formel **gebunden** vorkommen (das heißt in der Form $\forall x G$ oder $\exists x G$) oder **frei**, das heißt ohne Quantor. Eine Variable kann innerhalb derselben Formel sowohl gebunden als auch frei vorkommen. Eine Formel ohne freie Variablen wird **geschlossen** (oder eine **Aussage**) genannt.

**Beispiel** für eine Formel:

$$F := \left(\exists x_1 P_5^2(x_1, f_2^1(x_2)) \; \vee \; \neg \forall x_2 P_4^2(x_2, f_7^2(f_4^0, f_5^1(x_3)))\right)$$

In $F$ ist $x_1$ überall gebunden, $x_2$ ist beim ersten Auftreten frei und sonst gebunden, und $x_3$ kommt nur frei vor.

### 3.3.2 Semantik der Prädikatenlogik, 1. Teil

Eine **Struktur** ist ein Paar $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$, wobei $U_\mathcal{A}$ eine nicht leere Menge ist (die Grundmenge oder das Universum von $\mathcal{A}$) und $I_\mathcal{A}$ eine Abbildung, die

- jedem $k$-stelligen Prädikatssymbol $P$ (welches im Definitionsbereich von $I_\mathcal{A}$ liegt) ein $k$-stelliges Prädikat (= Relation) $P^\mathcal{A}$ auf $U_\mathcal{A}$ zuordnet,
- jedem $k$-stelligen Funktionssymbol $f$ (im Definitionsbereich von $I_\mathcal{A}$) eine $k$-stellige Funktion $f^\mathcal{A}$ auf $U_\mathcal{A}$ zuordnet,
- jeder Variablen $x$ (im Definitionsbereich von $I_\mathcal{A}$) ein Element $x^\mathcal{A}$ von $U_\mathcal{A}$ zuordnet.

Eine Struktur $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$ heißt zu einer Formel $F$ **passend**, falls $I_\mathcal{A}$ für alle in $F$ vorkommenden Prädikatssymbole, Funktionssymbole und freien Variablen definiert ist.

**Beispiel:** Sei die Formel $F := \forall x P(x, f(x)) \wedge Q(g(a, z))$ gegeben. Hierin ist $P$ ein zweistelliges und $Q$ ein einstelliges Prädikatssymbol, $f$ ein einstelliges, $g$ ein zweistelliges und $a$ ein nullstelliges Funktionssymbol, sowie $x$ eine gebundene und $z$ eine freie Variable. Eine zu $F$ passende Struktur $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$ mit:

$$U_\mathcal{A} := \mathbb{N}, \qquad P^\mathcal{A} := \{(m,n) \in U_\mathcal{A}^2 \mid m < n\}, \qquad Q^\mathcal{A} := \{n \in \mathbb{N} \mid n \text{ prim}$$
$$f^\mathcal{A}(n) := n+1, \qquad g^\mathcal{A}(m,n) := m+n, \qquad a^\mathcal{A} := 2, \quad z^\mathcal{A} := 3$$

In dieser Struktur „gilt“ $F$ offensichtlich (muss aber erst noch definiert werden). Es gibt aber – ziemlich offensichtlich – zu $F$ passende Strukturen, in denen $F$ nicht gilt.

### 3.3.3 Semantik der Prädikatenlogik, 2. Teil

Sei $F$ eine zur Struktur $\mathcal{A}$ passende Formel. Zuerst wird für jeden aus den Variablen und Funktionssymbolen von $F$ gebildeten Term $t$ der Wert $\mathcal{A}(t)$ definiert (induktiv, das heißt über den Aufbau der Terme):

(1) Im Fall $t = x$ (für eine Variable $x$) sei $\mathcal{A}(t) := x^\mathcal{A}$.

(2) Im Fall $t = f(t_1, \ldots, t_n)$ mit einem $k$-stelligen Funktionssymbol $f$ und Termen $t_1, \ldots, t_k$ sei $\mathcal{A}(t) := f^\mathcal{A}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k))$.

Jetzt werden – wieder induktiv – für alle Formeln $F$ die (Warheits-)Werte $\mathcal{A}(F)$ definiert:

(3) Für $F = P(t_1, \ldots, t_k)$ mit $k$-stelligem Prädikatssymbol $P$ und Termen $t_1, \ldots, t_k$ sei
$\mathcal{A}(F) := 1$ falls $(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k)) \in P^\mathcal{A}, \mathcal{A}(F) := 0$ sonst

(4) Für $F = \neg G$ sei
$\mathcal{A}(F) := 1$ falls $\mathcal{A}(G) = 0, \mathcal{A}(F) := 0$ sonst

(5) Für $F = (G \vee H)$ sei
$\mathcal{A}(F) := 1$ falls $\mathcal{A}(G) = 1$ oder $\mathcal{A}(H) = 1, \mathcal{A}(F) := 0$ sonst

(6) Für $F = (G \wedge H)$ sei
$\mathcal{A}(F) := 1$ falls $\mathcal{A}(G) = 1$ und $\mathcal{A}(H) = 1, \mathcal{A}(F) := 0$ sonst

(7) Für $F = \forall x G$ sei
$\mathcal{A}(F) := 1$ falls $\mathcal{A}_{[x/d]}(G) = 1$ für alle $d \in U_{\mathcal{A}}, \mathcal{A}(F) := 0$ sonst

(8) Für $F = \exists x G$ sei
$\mathcal{A}(F) := 1$ falls $\mathcal{A}_{[x/d]}(G) = 1$ für ein $d \in U_{\mathcal{A}}, \mathcal{A}(F) := 0$ sonst

**Anmerkung zu 7/8:** „$\mathcal{A}_{[x/d]}$“ bedeutet, dass $x = d$ gesetzt wird, unabhängig vom Wert $x^{\mathcal{A}}$ (und davon, ob $x^{\mathcal{A}}$ definiert ist). Fall $\mathcal{A}(F) = 1$ gilt, wird wieder $\mathcal{A} \models F$ geschrieben („$F$ gilt in $\mathcal{A}$“ oder „$\mathcal{A}$ ist ein Modell für $F$“). Wenn jede (zu $F$ passende) Struktur ein Modell für $F$ ist, heißt $F$ (**allgemein-**)**gültig**: $\models F$, andernfalls: $\#F$. Falls es mindestens ein Modell für $F$ gibt, heißt $F$ **erfüllbar**, sonst **unerfüllbar**.

**Schlussbemerkung:** (a) Prädikatenlogik „enthält“ die Aussagenlogik: Man nimmt nur 0-stellige Prädikatssymbole (und keine Terme, Variablen und Quantoren).
(b) Die hier angedeutete „Prädikatenlogik erster Stufe“ erlaubt keine Quantifizierung über Prädikats- und Funktionssymbole, dies ist in der „Prädikatenlogik zweiter Stufe“ erlaubt!

**Ende!**

# Abbildungsverzeichnis

# Index