Diskrete Mathematik für Informatiker

Markus Lohrey

Universität Siegen

Wintersemester 2014/2015

Organisatorisches zur Vorlesung

Die aktuelle Version der Folien finden Sie unter

`http://www.eti.uni-siegen.de/ti/lehre/ws1415/diskrete_mathematik/folien.pdf`

Literaturempfehlungen:

- Steger, Diskrete Strukturen 1. Kombinatorik, Graphentheorie, Algebra, Springer
- Diekert, Kufleitner, Rosenberger, Elemente der diskreten Mathematik, De Gruyter
- Aigner, Diskrete Mathematik, Vieweg
- Diestel, Graphentheorie, Springer

Die **Übungen** werden von Danny Hucke und Daniel König organisiert.

Mengentheoretische Grundlagen

Naive Definition (Mengen, Elemente, $\in$, $\notin$)

Eine Menge ist die Zusammenfassung von bestimmten unterschiedlichen Objekten (die Elemente der Menge) zu einem neuen Ganzen.

Wir schreiben $x \in M$, falls das Objekt x zur Menge M gehört.
Wir schreiben $x \notin M$, falls das Objekt x nicht zur Menge M gehört.

Falls $x \in M$ und $y \in M$ gilt, schreiben wir auch $x, y \in M$.

Eine Menge, welche nur aus endlich vielen Objekten besteht (eine endliche Menge), kann durch explizite Auflistung dieser Elemente spezifiziert werden.

Beispiel: $M = \{2, 3, 5, 7\}$.

Hierbei spielt die Reihnfolge der Auflistung keine Rolle:
$\{2, 3, 5, 7\} = \{7, 5, 3, 2\}$.

Auch Mehrfachauflistungen spielen keine Rolle:
$\{2, 3, 5, 7\} = \{2, 2, 2, 3, 3, 5, 7\}$.

Mengentheoretische Grundlagen

Eine besonders wichtige Menge ist die leere Menge $\emptyset = \{\}$, die keinerlei Elemente enthält.

In der Mathematik hat man es häufig auch mit unendlichen Mengen zu tun (Mengen, die aus unendlich vielen Objekten bestehen).

Solche Mengen können durch Angabe einer Eigenschaft, welche die Elemente der Menge auszeichnet, spezifiziert werden.

Beispiele:

- $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ (Menge der natürlichen Zahlen)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (Menge der ganzen Zahlen)
- $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ (Menge der ganzen Zahlen)
- $P = \{n \in \mathbb{N} \mid n \geq 2, n \text{ ist nur durch 1 und } n \text{ teilbar}\}$
  (Menge der Primzahlen)

Mengentheoretische Grundlagen

Unser Mengenbegriff ist naiv in dem Sinne, dass es sich um keine formale Definition handelt.

Dies mag schwierig zu vermeiden sein, ist doch der Mengenbegriff das fundamentalste Konzept der Mathematik. Alle Objekte der Mathematik können als Mengen aufgefasst werden.

Wie sollte man also den Mengenbegriff in der Sprache der Mathematik formalisieren?

Logiker haben zu Beginn des 20. Jahrhunderts eine formale Mengenlehre aufgestellt, indem sie eine Liste von Axiomen (Aussagen, deren Wahrheit nicht weiter hinterfragt wird) aufgestellt haben, welche grundlegende Eigenschaften der Elementbeziehung $\in$ beschreibt. Dieses Liste von Axiomen ist als **ZFC** (**Z**ermelo-**F**rankel with **C**hoice) bekannt.

Mengentheoretische Grundlagen

Beispiel: Eines der **ZFC**-Axiome besagt, dass zwei Mengen genau dann gleich sind, wenn sie die gleichen Elemente haben. Etwas formaler:

Für alle Mengen X und Y gilt: X und Y sind gleich, genau dann wenn für alle x gilt: $x \in X$ genau dann, wenn $x \in Y$.

Noch formaler:

$$\forall X \forall Y : (X = Y \longleftrightarrow (\forall x : x \in X \longleftrightarrow x \in Y))$$

Hierbei bedeutet $\forall$ "für alle" und $\exists$ "es existiert".

Bisher konnten Mathematiker kein schlüssiges mathematisches Argument finden, welche nicht mit den **ZFC**-Axiomen ableitbar ist.

Mengentheoretische Grundlagen

Die Notwendigkeit einer formalen Mengenlehre hat sich unter anderem aus diversen Paradoxien entwickelt. Eines der bekanntesten hiervon ist Russel's Paradoxon:

Elemente von Mengen können wieder Mengen sein. Also könnten wir doch die Menge aller Mengen, welche sich nicht selbst als Element haben, definieren:

$$Y = \{x \mid x \notin x\}$$

Gilt nun $Y \in Y$?

- Würde $Y \in Y$ gelten, so würde Y die Eigenschaft, welche die Menge Y definiert, erfüllen. Also müsste $Y \notin Y$ gelten.
- Würde $Y \notin Y$ gelten, so würde Y die Eigenschaft, welche die Menge Y definiert, nicht erfüllen. Also müsste $Y \in Y$ gelten.

Definition ($\subseteq$, $\subsetneq$, Potenzmenge, $\cap$, $\cup$, $\setminus$, disjunkt)

Seien A und B zwei Mengen.

- $A \subseteq B$ bedeutet, dass jedes Element von A auch zu B gehört (A ist eine Teilmenge von B); formal:

$$\forall a : a \in A \rightarrow a \in B$$

- $A \subsetneq B$ bedeutet, dass $A \subseteq B$ und $A \neq B$ gilt.
- $2^A = \{B \mid B \subseteq A\}$ (Potenzmenge von A)
- $A \cap B = \{c \mid c \in A \text{ und } c \in B\}$ (Schnitt von A und B)
- $A \cup B = \{c \mid c \in A \text{ oder } c \in B\}$ (Vereinigung von A und B)
- $A \setminus B = \{c \in A \mid c \notin B\}$ (Differenz von A und B)
- Zwei Mengen A und B sind disjunkt, falls $A \cap B = \emptyset$ gilt.

Beispiele und einige einfache Aussagen:

- $\emptyset \subseteq A$ und $A \subseteq A$ gilt für jede Menge A.
- Für alle Mengen A und B gilt $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$.
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.
- $\{1,2,3\} \cap \{4,5,6\} = \emptyset$, d. h. die beiden Mengen sind disjunkt.
- $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ und $2^{\emptyset} = \{\emptyset\}$
- Für alle Mengen A gilt

$$A \cap \emptyset = \emptyset \text{ und } A \cup \emptyset = A.$$

- Für alle Mengen A, B, und C gilt:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$
$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$

Wir beweisen beispielhaft die Identität

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Hierzu zeigen wir:

(1) Jedes Element von $A \cup (B \cap C)$ gehört auch zu $(A \cup B) \cap (A \cup C)$.

(2) Jedes Element von $(A \cup B) \cap (A \cup C)$ gehört auch zu $A \cup (B \cap C)$.

zu (1). Sei $x \in A \cup (B \cap C)$.

Dann gilt also $x \in A$ oder $x \in (B \cap C)$.

Fall 1: Es gilt $x \in A$.

Dann gilt auch $x \in (A \cup B)$ sowie $x \in (A \cup C)$ und damit $x \in (A \cup B) \cap (A \cup C)$.

Fall 2: Es gilt $x \in (B \cap C)$, d. h. $x \in B$ und $x \in C$.

Wieder gilt $x \in (A \cup B)$ und $x \in (A \cup C)$ und damit $x \in (A \cup B) \cap (A \cup C)$.

zu (2). Sei $x \in (A \cup B) \cap (A \cup C)$

Dann gilt $x \in A \cup B$ und $x \in A \cup C$.

Fall 1: $x \in A$.

Dann gilt $x \in A \cup (B \cap C)$.

Fall 2: $x \notin A$.

Wegen $x \in A \cup B$ muss $x \in B$ gelten, und wegen $x \in A \cup C$ muss $x \in C$ gelten.

Also gilt $x \in B \cap C$, d.h. $x \in A \cup (B \cap C)$. □

Definition (beliebige Vereinigung und Schnitt)

Sei I eine Menge und für jedes $i \in I$ sei A_i wiederum eine Menge. Dann definieren wir:

$$\bigcup_{i \in I} A_i = \{a \mid \exists j \in I : a \in A_j\}$$

$$\bigcap_{i \in I} A_i = \{a \mid \forall j \in I : a \in A_j\}$$

Für Mengen $A_1, A_2, \ldots, A_n$ verwenden wir auch die Schreibweise

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i \in \{1,\ldots,n\}} A_i \text{ und } \bigcap_{i=1}^{n} A_i = \bigcap_{i \in \{1,\ldots,n\}} A_i.$$

Mengentheoretische Grundlagen

Beispiele:

$$\bigcup_{a \in A} \{a\} = A \text{ für jede Menge } A$$

$$\bigcap_{\varepsilon \in \mathbb{R} \setminus \{0\}} \{x \in \mathbb{R} \mid |x - \pi| \leq |\varepsilon|\} = \{\pi\}$$

$$\bigcap_{n \in \mathbb{N}} \{m \in \mathbb{N} \mid m \geq n\} = \emptyset$$

Einfache Aussagen:

$$\left(\bigcap_{i \in I} A_i \right) \cup B = \bigcap_{i \in I} (A_i \cup B)$$

$$\left(\bigcup_{i \in I} A_i \right) \cap B = \bigcup_{i \in I} (A_i \cap B)$$

Mengentheoretische Grundlagen

Es wurde bereits erwähnt, dass alle Objekte der Mathematik als Mengen aufgefasst werden können.

Hier ist ein konkretes Beispiel:

Kuratowskis Definition des geordneten Paares

Für zwei Objekte x und y sei (x, y) das geordnete Paar, bestehend aus x und y. Es zeichnet sich durch die Eigenschaft

$$(x, y) = (x', y') \text{ genau dann, wenn } (x = x' \text{ und } y = y')$$

aus. Kuratowski definierte das geordnete Paar als

$$(x, y) := \{x, \{x, y\}\}.$$

Für Objekte $x_1, x_2, \ldots, x_n$ $(n \geq 3)$ definieren wir dann das n-Tupel

$$(x_1, x_2, \ldots, x_n) := (x_1, (x_2, \ldots, x_n)).$$

Definition (Kartesisches Produkt)

Für zwei Mengen A und B ist

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

das kartesische Produkt von A und B.

Allgemeiner: Für Mengen $A_1, \ldots, A_n$ $(n \geq 2)$ sei

$$\begin{aligned} \prod_{i=1}^{n} A_i &= A_1 \times A_2 \times \cdots \times A_n \\ &= \{(a_1, \ldots, a_n) \mid \text{ für alle } 1 \leq i \leq n \text{ gilt } a_i \in A_i\} \end{aligned}$$

Falls $A_1 = A_2 = \cdots = A_n = A$ schreiben wir auch A^n für diese Menge.

Beispiele und einige einfache Aussagen:

- $\{1,2,3\} \times \{4,5\} = \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\}$
- Für alle Mengen A, B, und C gilt:

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$
$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$
$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Definition (Relationen und Funktionen)

Seien A und B Mengen.

Eine Relation von A nach B ist eine Teilmenge $R \subseteq A \times B$.

Eine (binäre) Relation auf A ist eine Teilmenge $R \subseteq A \times A$.

Eine Funktion (oder Abbildung) von A (dem Definitionsbereich) nach B (dem Wertebereich) ist eine Relation $f \subseteq A \times B$, so dass für alle $a \in A$ genau ein $b \in B$ mit $(a, b) \in f$ existiert. Wir schreiben dann auch $f(a) = b$.

Wir schreiben auch $f : A \to B$ für eine Funktion f von A nach B.

Beispiel: Hier sind zwei Relationen von $\{a, b, c\}$ nach $\mathbb{N}$:

$$R = \{(a, 1), (b, 2), (c, 1)\} \text{ und } Q = \{(a, 1), (a, 2), (b, 2), (c, 1)\}$$

Dann ist R eine Funktion, Q hingegen ist keine Funktion.

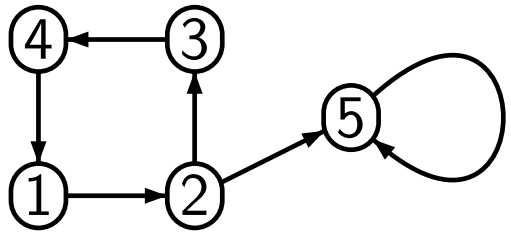
Mengentheoretische Grundlagen

Eine Relation $R \subseteq A \times A$ kann man sich graphisch veranschaulichen.

Beispiel: Sei $A = \{1, 2, 3, 4, 5\}$ und R die Relation

$$R = \{(1, 2), (2, 3), (3, 4), (4, 1), (2, 5), (5, 5)\}.$$

Diese Relation kann durch folgendes Diagram visualisiert werden.



Solche Diagramme werden wir im Kapitel über Graphentheorie noch genauer studieren.

Mengentheoretische Grundlagen

Definition

Für Mengen A und B sei B^A die Menge aller Funktionen von A nach B.

Definition (Bild und Urbild einer Funktion)

Sei $f : A \to B$ eine Funktion.

- Für $A' \subseteq A$ sei $f(A') = \{f(a) \mid a \in A'\}$ das Bild von A' unter f.
- Für $B' \subseteq B$ sei $f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$ das Urbild von B' unter f.

Beispiel: Sei $f : (\mathbb{N} \times \mathbb{N}) \to \mathbb{Z}$ definiert durch $f((n, m)) = n - m$ für $n, m \in \mathbb{N}$. Dann gilt:

- $f(\{(n, m) \mid n \leq m\}) = \{-a \mid a \in \mathbb{N}\}$
- $f^{-1}(\{0\}) = \{(a, a) \mid a \in \mathbb{N}\}$

Einfache Aussagen:

- Für alle Funktionen $f : A \to B$ und alle $A_1, A_2 \subseteq A$ gilt

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2).$$

- Für alle Funktionen $f : A \to B$ und alle $B_1, B_2 \subseteq B$ gilt

$$\begin{aligned} f^{-1}(B_1 \cup B_2) &= f^{-1}(B_1) \cup f^{-1}(B_2). \\ f^{-1}(B_1 \cap B_2) &= f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$

- Im Allgemeinen gilt nicht $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

  Beispiel: Sei $f(a) = c$ und $f(b) = c$. Dann gilt

$$f(\{a\} \cap \{b\}) = f(\emptyset) = \emptyset \text{ und } f(\{a\}) \cap f(\{b\}) = \{c\}.$$

- Für alle Funktionen $f : A \to B$ und $A' \subseteq A$, $B' \subseteq B$ gilt

$$A' \subseteq f^{-1}(f(A')) \text{ und } f(f^{-1}(B')) \subseteq B'.$$

Definition (injektive/surjektive/bijektive Funktionen)

Eine Funktion $f : A \to B$ is injektiv, falls für alle $a, b \in A$ gilt:
Wenn $a \neq b$ gilt, muss auch $f(a) \neq f(b)$ gelten
(verschiedene Elemente werden auf verschieden Elemente abgebildet).

Eine Funktion $f : A \to B$ is surjektiv, falls für alle $b \in B$ ein $a \in A$ mit $f(a) = b$ existiert (jedes Element aus B wird durch f getroffen).
Äquivalent: $f(A) = B$.

Eine Funktion $f : A \to B$ is bijektiv, falls sie injektiv und surjektiv ist.
Wir sagen auch, dass f eine Bijektion ist.

Eine Bijektion $f : A \to B$ ist eine 1-zu-1 Zuordnung zwischen den Elementen aus A und B.

Definition (Permutation)

Eine Permutation der Menge A ist eine Bijektion $f : A \to A$.

Beispiele:

- Die Funktion $f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ mit $f((a,b)) = \frac{a}{b}$ ist surjektiv (jede rationale Zahl ist Quotient zweier ganzer Zahlen) aber nicht injektiv (z. B. $f((1,2)) = f((2,4)) = 0.5$).
- Die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 1$ ist injektiv (aus $n + 1 = m + 1$ folgt $n = m$) aber nicht surjektiv (es gibt keine natürliche Zahl m mit $m + 1 = 0$).
- Die Funktion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = n + 1$ ist bijektiv (also eine Permutation).

Einfache Aussagen:

- $f : A \to B$ is surjektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ nicht leer ist.
- $f : A \to B$ is injektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ höchstens ein Element enthält.
- $f : A \to B$ is bijektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ genau ein Element enthält.
- Wenn $f : A \to B$ injektiv ist, dann gilt für alle $A' \subseteq A$ und $a \in A$: Aus $f(a) \in f(A')$ folgt $a \in A'$.

  Für nicht-injektive Funktionen ist dies im Allgemeinen falsch.
- Wenn $f : A \to B$ injektiv ist, dann gilt für alle $A_1, A_2 \subseteq A$: $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

Definition (Umkehrfunktion)

Für eine bijektive Funktion $f : A \to B$ kann man die Umkehrfunktion $f^{-1} : B \to A$ definieren durch folgende Vorschrift:

$$f^{-1}(b) = a \text{ genau dann, wenn } f(a) = b$$

Beachte: Wenn $f : A \to B$ bijektiv dann gibt es für jedes $b \in B$ genau ein Element a mit $f(a) = b$.

Daher ist die obige Definition von f^{-1} eindeutig!

Die Umkehrfunktion einer Bijektion ist wieder eine Bijektion.

Beispiel: Für die Bijektion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = n + 1$ gilt $f^{-1}(n) = n - 1$.

Beachte: Die Notation f^{-1} für die Umkehrfunktion ist konsistent mit der Notation $f^{-1}(A')$ für das Urbild.

Genauer: Ist $f : A \to B$ eine Bijektion, und ist $g = f^{-1}$ die Umkehrfunktion von f, so gilt für jede Teilmenge $B' \subseteq B$:

$$f^{-1}(B') = g(B').$$

In Worten: Das Urbild von B' unter f ist gleich dem Bild von B' unter der Umkehrfunktion von f.

Mengentheoretische Grundlagen

Mittels des Begriffs der Bijektion können wir definieren, wann zwei Mengen gleich groß sind.

Definition (gleich-mächtig)

Zwei Mengen A und B sind gleich-mächtig, kurz $|A| = |B|$, falls eine Bijektion $f : A \to B$ existiert.

Man schreibt auch $|A| \leq |B|$ (A is höchstens so mächtig wie B), falls eine injektive Funktion $f : A \to B$ existiert.

Den folgenden Satz beweisen wir später.

Satz 1 (Satz von Cantor, Schröder und Bernstein)

Für alle Mengen A und B gilt:

$$|A| = |B| \quad \textit{genau dann, wenn} \quad (|A| \leq |B| \textit{ und } |B| \leq |A|).$$

In anderen Worten: Es existiert eine Bijektion von A nach B genau dann, wenn injektive Funktionen von A nach B sowie B nach A existieren.

Für endliche Mengen A und B gilt $|A| = |B|$ falls A und B im intuitiven Sinne gleich viele Elemente haben.

Der Begriff "gleich-mächtig" kann jedoch auch auf unendliche Mengen angewendet werden.

Beispiel: Die Mengen $\mathbb{N}$ und $\mathbb{Z}$ sind gleich-mächtig.

Wir definieren eine Bijektion $f : \mathbb{Z} \to \mathbb{N}$ wie folgt, wobei $m \in \mathbb{Z}$:

$$f(m) = \begin{cases} -(2m+1) & \text{falls } m < 0 \\ 2m & \text{falls } m \geq 0 \end{cases}$$

Übung: Zeigen Sie, dass f tatsächlich bijektiv ist.

Ebenso sind die Mengen $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$ und $\mathbb{Q}$ gleich-mächtig.

Eine Bijektion zwischen $\mathbb{N} \times \mathbb{N}$ und $\mathbb{N}$ ist die Cantorsche Paarungsfunktion $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ mit

$$p(n_1, n_2) = \frac{1}{2}(n_1 + n_2 + 1)(n_1 + n_2) + n_2.$$

Alternativ kann man die Gleichmächtigkeit von $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ mittels des Satzes von Cantor, Schröder und Bernstein zeigen, indem man injektive Funktionen $i_1 : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ und $i_2 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ angibt, z. B.

$$i_1(n) = (n, 0) \text{ und } i_2(n_1, n_2) = 2^{n_1} 3^{n_2}.$$

(Injektivität von i_2 folgt aus Satz 45.)

Man kann auch zeigen, dass die Mengen $2^{\mathbb{N}}$ und $\mathbb{R}$ (Menge der reellen Zahlen) gleich-mächtig sind.

Aber: Nicht alle unendlichen Mengen sind gleich-mächtig.

Satz 2 (Cantor 1891)

Für jede Menge A sind A und 2^A nicht gleich-mächtig.

Beweis (durch Widerspruch): Sei A eine beliebige Menge.

Angenommen es gäbe eine surjektive Funktion $f : A \to 2^A$.

Definiere die Menge

$$B = \{a \in A \mid a \notin f(a)\} \subseteq A.$$

Da f surjektiv ist, gibt es ein $b \in A$ mit $f(b) = B$.

Dann gilt:

$$b \in B \iff b \notin f(b) \iff b \notin B.$$

Also gibt es keine surjektive (und somit auch keine bijektive) Abbildung $f : A \to 2^A$. □

Definition (abzählbar-unendlich, abzählbar, überabzählbar)

Eine Menge A ist abzählbar-unendlich, falls $|A| = |\mathbb{N}|$ gilt.

Eine Menge A ist abzählbar, falls A endlich oder abzählbar-unendlich ist.

Eine Menge A ist überabzählbar, falls A unendlich aber nicht abzählbar ist.

Beispiele:

Die Mengen $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar-unendlich.

Die Mengen $2^{\mathbb{N}}$, $\mathbb{R}$ und $\mathbb{C}$ (Menge der komplexen Zahlen) sind überabzählbar.

Das eine Menge A abzählbar-unendlich ist, bedeutet, dass man die Elemente der Menge A auflisten kann als

$$a_1, a_2, a_3, a_4, \ldots$$

wobei in dieser Liste jedes Element von A genau einmal vorkommt.

Mengentheoretische Grundlagen

Es gibt in der Mengenlehre durchaus sehr schwierige Fragen.

Z. B. hat Georg Cantor folgende Vermutung aufgestellt:

Kontinuumshypothese (Cantor 1878)

Für jede unendliche Teilmenge $A \subseteq 2^{\mathbb{N}}$ gilt $|A| = |\mathbb{N}|$ oder $|A| = |2^{\mathbb{N}}|$.

Diese Vermutung konnte lange Zeit weder bewiesen noch widerlegt werden. Dies ist unvermeidbar:

- Die Verneinung der Kontinuumshypothese kann nicht aus dem Axiomensystem ZFC hergeleitet werden (Gödel 1938).
- Die Kontinuumshypothese kann nicht aus dem Axiomensystem ZFC hergeleitet werden (Cohen 1966).

Mengentheoretische Grundlagen

Für eine Relation $R \subseteq A \times A$ und $a, b \in A$ schreiben wir auch aRb für $(a, b) \in R$.

Definition ((ir)reflexive/(anti)symmetrische/transitive Relationen)

Sei A eine Menge und $R \subseteq A \times A$ eine Relation auf A.

- R ist reflexiv, falls aRa für alle $a \in A$ gilt.
- R ist irreflexiv, falls kein $a \in A$ mit aRa existiert.
- R ist symmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb, dann auch bRa.
- R ist antisymmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb und bRa, dann $a = b$.
- R ist transitiv, falls für alle $a, b, c \in A$ gilt:
  Wenn aRb und bRc, dann auch aRc.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0 \; R \; 0$.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.
- Ist R irreflexiv?

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.

- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.
- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.
- Ist R symmetrisch?

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.

- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.

- Ist R symmetrisch?

  Ja: Wenn $a\ R\ b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b\ R\ a$.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.
- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.
- Ist R symmetrisch?

  Ja: Wenn $a\ R\ b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b\ R\ a$.
- Ist R antisymmetrisch?

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.
- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.
- Ist R symmetrisch?

  Ja: Wenn $a\ R\ b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b\ R\ a$.
- Ist R antisymmetrisch?

  Nein: Es gilt z.B. $0\ R\ 43$ und $43\ R\ 0$ aber $0 \neq 43$.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.
- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.
- Ist R symmetrisch?

  Ja: Wenn $a\ R\ b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b\ R\ a$.
- Ist R antisymmetrisch?

  Nein: Es gilt z.B. $0\ R\ 43$ und $43\ R\ 0$ aber $0 \neq 43$.
- Ist R transitiv?

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0\ R\ 0$.

- Ist R irreflexiv?

  Ja: Würde $a\ R\ a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.

- Ist R symmetrisch?

  Ja: Wenn $a\ R\ b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b\ R\ a$.

- Ist R antisymmetrisch?

  Nein: Es gilt z.B. $0\ R\ 43$ und $43\ R\ 0$ aber $0 \neq 43$.

- Ist R transitiv?

  Nein: Es gilt z.B. $0\ R\ 43$ und $43\ R\ 0$ aber nicht $0\ R\ 0$.

Definition (partielle Ordnung)

Eine Relation $R \subseteq A \times A$ ist eine partielle Ordnung (auf A), falls R reflexiv, antisymmetrisch, und transitiv ist.

Definition (lineare Ordnung)

Eine partielle Ordnung R auf A ist eine lineare Ordnung (auf A), falls für alle $a, b \in A$ gilt: aRb oder bRa.

Beispiel 1 (Teilmengenbeziehung oder Inklusion): Sei A eine beliebige Menge. Dann ist $\subseteq$ eine partielle Ordnung auf 2^A.

Falls A mindestens zwei Elemente enthält, ist jedoch $\subseteq$ keine lineare Ordnung auf 2^A: Sei $A = \{1, 2\}$. Dann gilt weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$.

Beispiel 2: Die Relation $\leq$ ist eine lineare Ordnung auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

Beispiel 3 (Teilbarkeit): Wir definieren die binäre Relation $|$ auf den ganzen Zahlen $\mathbb{Z}$ wie folgt, wobei $a, b \in \mathbb{Z}$.

$$a|b \text{ genau dann, wenn } \exists q \in \mathbb{Z} : q \cdot a = b$$

Die Relation $|$ ist reflexiv und transitiv, sie ist jedoch nicht antisymmetrisch, denn für alle $a \in \mathbb{Z}$ gilt $a \mid -a$ und $-a \mid a$.

Betrachten wir jedoch $|$ als eine binäre Relation auf den natürlichen Zahlen $\mathbb{N}$, so ist $|$ eine partielle Ordnung, aber keine lineare Ordnung: Es gilt weder $2 \mid 3$ noch $3 \mid 2$.

Definition (Äquivalenzrelation)

Eine Relation $R \subseteq A \times A$ ist eine Äquivalenzrelation (auf A), falls R reflexiv, symmetrisch und transitiv ist.

Beispiel 1: Für jede Menge A ist die Relation

$$\mathrm{Id}_A = \{(a, a) \mid a \in A\}$$

(die Identitätsrelation) reflexiv, symmetrisch, antisymmetrisch, und transitiv. Insbesondere ist Id_A eine Äquivalenzrelation.

Beispiel 2: Sei $f : A \to B$ eine Funktion. Dann ist

$$\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$$

eine Äquivalenzrelation.

Beispiel 3: Sei $q \in \mathbb{Z} \setminus \{0\}$ eine ganze Zahl. Auf der Menge $\mathbb{Z}$ definieren wir die Relation

$$\equiv_q = \{(a, b) \mid a, b \in \mathbb{Z}, q|(a - b)\}.$$

Sprechweise für $a \equiv_q b$: a und b sind kongruent modulo q.

Es gilt $a \equiv_q b$ genau dann, wenn eine ganze Zahl $x \in \mathbb{Z}$ mit $a = b + x \cdot q$ existiert.

Beachte: $a \equiv_q b$ genau dann, wenn $a \equiv_{-q} b$.

Lemma 3

Für jede Zahl $q \in \mathbb{Z} \setminus \{0\}$ ist $\equiv_q$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: Sei $q \in \mathbb{Z} \setminus \{0\}$.

(1) $\equiv_q$ ist reflexiv, denn $q|(a-a)$ (d. h. $q|0$) gilt für jede ganze Zahl a.

(2) $\equiv_q$ ist symmetrisch: Gelte $a \equiv_q b$, d. h. $q|(a-b)$.

Wegen $(b-a) = -(a-b)$ gilt dann auch $q|(b-a)$, d. h. $b \equiv_q a$.

(3) $\equiv_q$ ist transitiv: Seien $a, b, c \in \mathbb{Z}$ mit $a \equiv_q b$ und $b \equiv_q c$.

Also existieren ganze Zahlen $p, s \in \mathbb{Z}$ mit

$$a - b = qp \text{ und } b - c = qs.$$

Dann gilt

$$a - c = (a-b) + (b-c) = qp + qs = q(p+s).$$

Also gilt $a \equiv_q c$. □

Definition (Äquivalenzklassen)

Sei R eine Äquivalenzrelation auf der Menge A und sei $a \in A$. Dann ist $[a]_R = \{b \in A \mid aRb\}$ die Äquivalenzklasse von a (bzgl. R).

Beachte: Es gilt stets $a \in [a]_R$ (denn eine Aquivalenzrelation ist reflexiv).

Eine Äquivalenzklasse kann also nie leer sein, und jedes Element von A gehört zu einer Äquivalenzklasse.

Satz 4

Sei R eine Äquivalenzrelation auf der Menge A und seien $a, b \in A$. Dann sind folgende drei Aussagen äquivalent:

(1) aRb

(2) $[a]_R = [b]_R$

(3) $[a]_R \cap [b]_R \neq \emptyset$.

Beweis (durch Ringschluss):

(1) impliziert (2): Gelte aRb und damit auch bRa (R ist symmetrisch).

Wir zeigen zunächst $[a]_R \subseteq [b]_R$.

Sei also $c \in [a]_R$, d. h. es gilt aRc.

bRa, aRc und R transitiv $\longrightarrow$ bRc, d. h. $c \in [b]_R$.

Analog kann man $[b]_R \subseteq [a]_R$ zeigen.

(2) impliziert (3): Gelte $[a]_R = [b]_R$.

Dann gilt $a \in [a]_R \cap [b]_R$ und damit $[a]_R \cap [b]_R \neq \emptyset$.

(3) impliziert (1): Gelte $[a]_R \cap [b]_R \neq \emptyset$.

Also gibt es ein c mit $c \in [a]_R$ und $c \in [b]_R$.

$\longrightarrow$ aRc und bRc; und damit auch cRb (R ist symmetrisch).

$\longrightarrow$ aRb, wegen R transitiv. □

Beispiele:

- Die Äquivalenzklassen der Identitätsrelation Id_A sind die einelementigen Mengen $\{a\}$ mit $a \in A$.
- Die Äquivalenzklassen der Relation $\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$ (für $f : A \to B$ eine Funktion) sind die Urbilder $f^{-1}(b)$ für $b \in B$.
- Die Äquivalenzklassen von $\equiv_q$ (für $q \in \mathbb{N} \setminus \{0\}$) sind die Mengen

$$\{0 + pq \mid p \in \mathbb{Z}\}$$
$$\{1 + pq \mid p \in \mathbb{Z}\}$$
$$\vdots$$
$$\{(q-1) + pq \mid p \in \mathbb{Z}\}$$

Mengentheoretische Grundlagen

Sei R wieder eine Äquivalenzrelation auf der Menge A.

Seien $\{A_i \mid i \in I\}$ die Menge aller Äquivalenzklassen von R, d. h.

- Für jedes $a \in A$ gibt es ein $i \in I$ mit $[a]_R = A_i$
- Für alle $i, j \in I$ mit $i \neq j$ gilt $A_i \neq A_j$.

Aufgrund von Satz 4 bildet $\{A_i \mid i \in I\} \subseteq 2^A$ eine Partition von A, d. h.

- $\bigcup_{i \in I} A_i = A$
- $\forall i \in I : A_i \neq \emptyset$.
- $\forall i, j \in I : i \neq j \rightarrow A_i \cap A_j = \emptyset$ (verschiedene A_i sind disjunkt)

Ist umgekehrt $\{A_i \mid i \in I\}$ eine Partition von A, so kann man eine Äquivalenzrelation R auf A definieren durch:

$$R = \{(a, b) \mid a, b \in A, \exists i \in I : a, b \in A_i\}$$

Übung: Zeigen Sie, dass dies tatsächlich eine Äquivalenzrelation ist.

Mengentheoretische Grundlagen

Da eine Relation $R \subseteq A \times B$ eine Menge (von Paaren) ist, können wir die Operationen $\cap$ und $\cup$ auch auf Relationen anwenden.

Es gibt aber noch zwei weitere wichtige Operationen auf Mengen:

Definition (R^{-1}, $R \circ S$)

Seien $R \subseteq A \times B$ und $S \subseteq B \times C$ binäre Relationen. Dann definieren wir:

- $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$
- $R \circ S = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R \text{ und } (b, c) \in S\}$

R^{-1} ist die Umkehrrelation von R.

$R \circ S$ ist die Komposition (oder Verknüpfung) von R und S.

Beispiel 1: Sei

$$R = \{(a,1),(b,1),(b,2)\} \text{ und } S = \{(1,x),(1,y),(2,y)\}$$

Dann gilt:

- $R^{-1} = \{(1,a),(1,b),(2,b)\}$
- $R \circ S = \{(a,x),(a,y),(b,x),(b,y)\}$

Beispiel 2: Sei R eine lineare Ordnung auf der Menge A. Dann gilt

$$R \cap R^{-1} = \mathrm{Id}_A$$
$$R \cup R^{-1} = A \times A$$

Ein wichtiger Spezialfall der Komposition von Relationen ist die Komposition von Funktionen:

Wenn $f : A \to B$ und $g : B \to C$ Funktionen sind, dann ist $f \circ g : A \to C$ eine Funktion und es gilt

$$(f \circ g)(a) = g(f(a))$$

für alle $a \in A$.

Vorsicht: Manchmal wird die Funktion $f \circ g$ auch durch die Vorschrift $(f \circ g)(a) = f(g(a))$ definiert.

Bemerkungen: Sei $R \subseteq A \times A$ eine Relation auf A.

- R is reflexiv, genau dann, wenn $\mathrm{Id}_A \subseteq R$.
- R is irreflexiv, genau dann, wenn $\mathrm{Id}_A \cap R = \emptyset$.
- R ist symmetrisch, genau dann, wenn $R^{-1} = R$.
- R is transitiv, genau dann, wenn $R \circ R \subseteq R$.
- R is antisymmetrisch, genau dann, wenn $R \cap R^{-1} \subseteq \mathrm{Id}_A$.
- Für alle binären Relationen R, S und T auf der Menge A gilt:

$$R \circ \mathrm{Id}_A = \mathrm{Id}_A \circ R = R$$
$$(R \circ S) \circ T = R \circ (S \circ T)$$
$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$$

Mengentheoretische Grundlagen

- Ist die Relation $R \subseteq A \times B$ eine Bijektion (also insbesondere eine Funktion) dann ist die Umkehrrelation R^{-1} genau die Umkehrfunktion von R.
- Wenn $f : A \to B$ und $g : B \to C$ injektiv sind, dann ist auch $f \circ g$ injektiv.
- Wenn $f : A \to B$ und $g : B \to C$ surjektiv sind, dann ist auch $f \circ g$ surjektiv.
- Wenn $f : A \to B$ und $g : B \to C$ bijektiv sind, dann ist auch $f \circ g$ bijektiv.
- Konsequenz: Sei M eine Menge von Mengen. Dann ist Relation

$$\{(X, Y) \in M \times M \mid |X| = |Y|\}$$

eine Äquivalenzrelation.

Satz 5 (Prinzip der vollständigen Induktion)

Sei $A \subseteq \mathbb{N}$. Angenommen es gilt

- $0 \in A$ *und*
- *für alle $n \in A$ gilt auch $n+1 \in A$.*

Dann gilt $A = \mathbb{N}$.

Beweis (durch Widerspruch): Angenommen für $A \subseteq \mathbb{N}$ gilt:

(1) $0 \in A$ und

(2) für alle $n \in A$ gilt auch $n+1 \in A$.

Angenommen es gilt $A \neq \mathbb{N}$.

Wir leiten einen Widerspruch ab.

Da $\mathbb{N} \setminus A \neq \emptyset$ gilt, hat diese Menge ein kleinstes Element $m \notin A$ (jede nicht-leere Menge von natürlichen Zahlen hat ein kleinstes Element)

Da $0 \in A$ nach (1) gilt, muss $m > 0$ gelten.

Da m das kleinste Element von $\mathbb{N} \setminus A$ ist, muss $m - 1 \notin \mathbb{N} \setminus A$, d. h. $m - 1 \in A$ gelten.

Dann gilt aber nach (2) auch $m \in A$, was ein Widerspruch ist. □

In Anwendungen ist häufig A die Menge aller natürlichen Zahlen mit einer gewissen Eigenschaft, und man will zeigen, dass alle natürlichen Zahlen diese Eigenschaft haben.

Beispiel 1: Wir beweisen mittels vollständiger Induktion, dass für alle natürlichen Zahlen n gilt:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Hierbei ist $\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$ die Summe der n ersten natürlichen Zahlen.

Induktionsanfang: Es gilt $\sum_{i=1}^{0} i = 0 = \frac{0 \cdot 1}{2}$.

Induktionsschritt: Angenommen es gilt

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Dann gilt auch

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= (\sum_{i=1}^{n} i) + n + 1 \\
&= \frac{n(n+1)}{2} + n + 1 \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Beispiel 2: Wir beweisen mittels vollständiger Induktion, dass für alle natürlichen Zahlen $n \geq 1$ und alle reellen Zahlen $x_1, \ldots, x_n \geq 0$ gilt:

$$\prod_{i=1}^{n}(1 + x_i) \geq 1 + \sum_{i=1}^{n} x_i$$

Hierbei ist $\prod_{i=1}^{n}(1 + x_i) = (1 + x_1)(1 + x_2) \cdots (1 + x_n)$ das Produkt der Zahlen $1 + x_1, \ldots, 1 + x_n$

Induktionsanfang: Es gilt $\prod_{i=1}^{1}(1 + x_i) = 1 + x_1 = 1 + \sum_{i=1}^{1} x_i$.

Induktionsschritt: Angenommen es gilt

$$\prod_{i=1}^{n}(1 + x_i) \geq 1 + \sum_{i=1}^{n} x_i$$

Dann gilt:

$$\begin{aligned}
\prod_{i=1}^{n+1}(1+x_i) &= (1+x_{n+1})\cdot\prod_{i=1}^{n}(1+x_i) \\
&\geq (1+x_{n+1})\cdot(1+\sum_{i=1}^{n}x_i) \\
&= 1+(\sum_{i=1}^{n}x_i)+x_{n+1}+x_{n+1}\cdot(\sum_{i=1}^{n}x_i) \\
&\geq 1+\sum_{i=1}^{n+1}x_i
\end{aligned}$$

Bemerkung: Die Ungleichung $\prod_{i=1}^{n}(1+x_i) \geq 1+\sum_{i=1}^{n}x_i$ gilt auch für $n=0$, wenn man definiert

$$\prod_{i=1}^{0} a_i = 1.$$

Das Prinzip der vollständigen Induktion kann auch dazu verwendet werden, um Objekte zu definieren.

Beispiel: Sei $R \subseteq A \times A$ eine Relation.

Wir definieren für jede Zahl $n \in \mathbb{N}$ die Relation R^n (n-fache Komposition von R) wie folgt:

- $R^0 = \mathrm{Id}_A$ (entspricht Induktionsanfang)
- $R^{n+1} = R \circ R^n$ für alle $n \in \mathbb{N}$ (entspricht Induktionsschritt).

Bemerkungen:

- $R^1 = R \circ \mathrm{Id}_A = R$.
- Für ein $n \geq 1$ gilt $(a, b) \in R^n$ genau dann, wenn Elemente $a_0, a_1, a_2, \ldots, a_n \in A$ existieren, so dass gilt:

$$a = a_0 \; R \; a_1 \; R \; a_2 \; R \cdots a_{n-1} \; R \; a_n = b$$

- $R^n \circ R^m = R^{n+m}$

Vorsicht: Die Notation R^n für eine Relation R könnte auch mißverstanden werden:

Wir hatten für eine Menge A und $n \geq 1$ die Menge A^n definiert als die Menge aller n-Tupel mit Komponenten aus A:

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in A\}.$$

Eine Relation R ist auch eine Menge (von Paaren).

Im Allgemeinen meinen wir aber mit R^n nicht die Menge aller n-Tupel

$$\{((a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)) \mid (a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n) \in R\},$$

sondern die n-fache Komposition von R.

Die n-fache Komposition kann auch für eine Funktion $f : A \to A$ angewendet werden.

Dann ist f^n die n-fache Anwendung von f:

- $f^0(x) = x$ für alle $x \in A$.
- $f^{n+1}(x) = f(f^n(x))$ für alle $x \in A$ und $n \geq 0$.

Beispiel: Sei $R = \{(x, x+1) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

Dann gilt für alle $n \geq 0$:

$$R^n = \{(x, x+n) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

In diesem Fall ist R gleich der Funktion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x + 1$.

Die Funktion $f^n : \mathbb{Z} \to \mathbb{Z}$ ist dann die n-fache Anwendung von f, d.h. $f^n(x) = x + n$.

Definition (transitive Hülle, reflexiv-transitive Hülle)

Sei $R \subseteq A \times A$ eine Relation.

Die transitive Hülle von R ist die Relation

$$R^+ = \bigcup_{n \in \mathbb{N} \setminus \{0\}} R^n = R^1 \cup R^2 \cup R^3 \cup R^4 \cup \cdots .$$

Die reflexiv-transitive Hülle von R ist die Relation

$$R^* = \bigcup_{n \in \mathbb{N}} R^n = \mathrm{Id}_A \cup R^+.$$

Dann gilt:

- $R \subseteq R^+$ und $R \subseteq R^*$.
- R^+ ist transitiv: Wenn $(a, b), (b, c) \in R^+$ gilt, dann existieren $n, m \geq 1$ mit $(a, b) \in R^n$, $(b, c) \in R^m$.

  Also gilt: $(a, c) \in R^n \circ R^m = R^{n+m} \subseteq R^+$.
- R^* ist auch transitiv (gleiches Argument wie für R^+) und zusätzlich reflexiv.
- Wenn $S \subseteq A \times A$ transitiv ist und $R \subseteq S$ gilt, dann gilt $R^+ \subseteq S$.
- Wenn $S \subseteq A \times A$ transitiv und reflexiv ist und $R \subseteq S$ gilt, dann gilt $R^* \subseteq S$.
- Es gilt $(a, b) \in R^+$ genau dann, wenn ein $n \geq 1$ und $a_0, a_1, \ldots, a_n \in A$ existieren, so dass

$$a = a_0 \; R \; a_1 \; R \; a_2 \; R \cdots a_{n-1} \; R \; a_n = b$$

Beispiel 1: Sei R die Relation

$$R = \{(1,2),(2,3),(3,4),(4,1),(2,5),(5,5)\}$$

(siehe Folie 18).

Dann gilt

$$R^+ = R^* = (\{1,2,3,4\} \times \{1,2,3,4\}) \cup (\{1,2,3,4\} \times \{5\}) \cup \{(5,5)\}.$$

Beispiel 2: Sei $R = \{(x, x+1) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

Dann gilt

$$\begin{aligned} R^+ &= \{(x,y) \mid x,y \in \mathbb{Z}, x < y\} \\ R^* &= \{(x,y) \mid x,y \in \mathbb{Z}, x \leq y\}. \end{aligned}$$

Kombinatorik: Abzählen von Mengen

Für eine endliche Menge A bezeichnen wir mit $|A|$ die Anzahl der Elemente von A.

Falls A unendlich ist, schreiben wir $|A| = \infty$.

Ein Grundprinzip der Kombinatorik ist der folgende Satz:

Satz 6

Für endliche Mengen A und B mit $A \cap B = \emptyset$ gilt $|A \cup B| = |A| + |B|$.

Definition (paarweise disjunkte Mengen)

Mengen $A_1, \ldots, A_n$ sind paarweise disjunkt falls für alle $i, j \in \{1, \ldots, n\}$ gilt: Wenn $i \neq j$, dann gilt $A_i \cap A_j = \emptyset$.

Beispiel: Die Mengen $\{1, 2\}$, $\{3, 4\}$, und $\{5, 6\}$ sind paarweise disjunkt.

Kombinatorik: Abzählen von Mengen

Folgende Verallgemeinerung von Satz 6 kann nun mittels Induktion bewiesen werden.

Satz 7

Seien $A_1, A_2, \ldots, A_n$ paarweise disjunkte endliche Mengen. Dann gilt

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|.$$

Beweis:

Induktionsanfang ($n = 1$): klar.

Induktionsschritt: Sei nun $n \geq 2$ und gelte

$$|\bigcup_{i=1}^{n-1} A_i| = \sum_{i=1}^{n-1} |A_i|.$$

Es gilt

$$\bigcup_{i=1}^{n} A_i = (\bigcup_{i=1}^{n-1} A_i) \cup A_n.$$

Außerdem gilt

$$(\bigcup_{i=1}^{n-1} A_i) \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n) = \bigcup_{i=1}^{n-1} \emptyset = \emptyset.$$

Also erhalten wir mit Satz 6:

$$|\bigcup_{i=1}^{n} A_i| = |(\bigcup_{i=1}^{n-1} A_i) \cup A_n| = |\bigcup_{i=1}^{n-1} A_i| + |A_n| = \sum_{i=1}^{n-1} |A_i| + |A_n| = \sum_{i=1}^{n} |A_i|$$

□

Korollar

Seien A und B endliche Mengen. Dann gilt:

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

Beweis: Es gilt

$$A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B).$$

Außerdem sind die drei Mengen $A \setminus B$, $B \setminus A$, und $A \cap B$ paarweise disjunkt.

Also folgt aus Satz 7:

$$|A \cup B| = |A \setminus B| + |B \setminus A| + |A \cap B|.$$

Indem wir $|A \cap B|$ zu beiden Seiten addieren und $|A| = |A \setminus B| + |A \cap B|$ sowie $|B| = |B \setminus A| + |A \cap B|$ verwenden, erhalten wir

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

Zur Erinnerung: Für Mengen $A_1, \ldots, A_n$ ist $\prod_{i=1}^{k} A_i$ die Menge aller k-Tupel $(a_1, a_2, \ldots, a_k)$ mit $a_1 \in A_1$, $a_2 \in A_2, \ldots, a_k \in A_k$.

Satz 8

Seien $A_1, \ldots, A_k$ endliche Mengen. Dann gilt

$$|\prod_{i=1}^{k} A_i| = \prod_{i=1}^{k} |A_i|.$$

Beweis: Induktion nach k

Induktionsanfang ($k = 1$): klar.

Induktionsschritt: Sei nun $k \geq 2$ und gelte

$$|\prod_{i=1}^{k-1} A_i| = \prod_{i=1}^{k-1} |A_i|.$$

Die Menge $\prod_{i=1}^{k} A_i$ können wir schreiben als

$$\prod_{i=1}^{k} A_i = \bigcup_{a \in A_k} \{(t, a) \mid t \in \prod_{i=1}^{k-1} A_i\}.$$

Für alle $a, b \in A_k$ mit $a \neq b$ gilt

$$\{(t, a) \mid t \in \prod_{i=1}^{k-1} A_i\} \cap \{(t, b) \mid t \in \prod_{i=1}^{k-1} A_i\} = \emptyset.$$

Also folgt aus Satz 7:

$$
\begin{aligned}
|\prod_{i=1}^{k} A_i| &= \sum_{a \in A_k} |\{(t,a) \mid t \in \prod_{i=1}^{k-1} A_i\}| \\
&= \sum_{a \in A_n} \prod_{i=1}^{k-1} |A_i| \\
&= |A_n| \cdot \prod_{i=1}^{k-1} |A_i| \\
&= \prod_{i=1}^{k} |A_i|.
\end{aligned}
$$

□

Satz 9

Sei A eine endliche Menge. Dann gilt $|A^k| = |A|^k$.

Beweis: Wähle $A_1 = A_2 = \cdots A_k = A$ in Satz 8.

Kombinatorik: Abzählen von Mengen

Interpretation: Für eine n-elementige Mengen A gibt es n^k Möglichkeiten k Elemente mit Zurücklegen und mit Berücksichtigung der Reihenfolge aus A zu ziehen.

Intuition: Beim Ziehen des ersten Elements hat man n Alternativen, beim Ziehen des zweiten Elements hat man wieder n Alternativen, u.s.w.

Wieviele Möglichkeiten gibt es, aus einer n-elementigen Menge $k \leq n$ Elemente ohne Zurücklegen und mit Berücksichtigung der Reihenfolge zu ziehen?

Definition (fallende Faktorielle)

Für Zahlen k, n mit $1 \leq k \leq n$ sei

$$n^{\underline{k}} = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) = \prod_{i=0}^{k-1} (n-i)$$

die fallende Faktorielle von n der Länge k. Wir setzen $n^{\underline{0}} = 1$.

Satz 10

Sei A eine endliche Menge. Dann gilt

$$|\{(a_1, \ldots, a_k) \in A^k \mid a_i \neq a_j \text{ falls } i \neq j\}| = |A|^{\underline{k}}.$$

Beweis: Induktion nach n

Induktionsanfang ($k = 1$): klar.

Induktionsschritt: Es gilt:

$$\{(a_1, \ldots, a_k) \in A^k \mid a_i \neq a_j \text{ falls } i \neq j\} =$$
$$\bigcup_{a \in A} \{(a, a_2, \ldots, a_k) \in A^k \mid a_i \neq a, a_i \neq a_j \text{ falls } i \neq j\}$$

Außerdem gilt für $a \neq b$:

$$\{(a, a_2, \ldots, a_k) \in A^k \mid a_i \neq a, a_i \neq a_j \text{ falls } i \neq j\} \cap$$
$$\{(b, a_2, \ldots, a_k) \in A^k \mid a_i \neq b, a_i \neq a_j \text{ falls } i \neq j\} = \emptyset$$

Also gilt nach Satz 7 (mit $n = |A|$)

$$\begin{aligned}
& |\{(a_1, \ldots, a_k) \in A^k \mid a_i \neq a_j \text{ falls } i \neq j\}| \\
= & \sum_{a \in A} |\{(a, a_2, \ldots, a_k) \in A^k \mid a_i \neq a, a_i \neq a_j \text{ falls } i \neq j\}| \\
= & \sum_{a \in A} |\{(a_2, \ldots, a_k) \in (A \setminus \{a\})^{k-1} \mid a_i \neq a_j \text{ falls } i \neq j\}| \\
= & \; n \cdot (n-1)^{\underline{k-1}} \\
= & \; n^{\underline{k}}
\end{aligned}$$

□

Interpretation: Für eine n-elementige Mengen A gibt es $n^{\underline{k}}$ Möglichkeiten k Elemente ohne Zurücklegen und mit Berücksichtigung der Reihenfolge aus A zu ziehen.

Intuition: Beim Ziehen des ersten Elements hat man n Alternativen, beim Ziehen des zweiten Elements hat man $n-1$ Alternativen, ..., beim Ziehen des k-ten Elements hat man $n-k+1$ Alternativen.

Kombinatorik: Abzählen von Mengen

Nun soll die Reihenfolge keine Rolle mehr spielen.

Betrachten wir zunächst die Situation ohne Zurücklegen.

Definition 11

Für eine Menge A mit $|A| = n$ und $k \leq n$ sei $\binom{A}{k}$ die Menge aller k-elementigen Teilmengen von A:

$$\binom{A}{k} = \{B \subseteq A \mid |B| = k\}$$

Dann ist $|\binom{A}{k}|$ genau die Anzahl der Möglichkeiten aus einer n-elementigen Menge k Elemente ohne Zurücklegen und ohne Berücksichtigung der Reihenfolge auszuwählen.

Kombinatorik: Abzählen von Mengen

Betrachten wir zunächst eine andere Frage: Wieviele Möglichkeiten gibt es, eine n-elementige Menge anzuordnen?

Beispiel: Für die Menge $\{1, 2, 3\}$ gibt es folgende 6 Anordnungen:

$$(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)$$

Beachte: Eine Anordnung einer n-elementigen Menge $A = \{a_1, \ldots, a_n\}$ ist nichts anderes als eine Permutation $f : A \to A$:

- Die Anordnung $(a_{i_1}, \ldots, a_{i_n})$ entspricht der Permutation f mit $f(a_j) = a_{i_j}$
- Die Permutation $f : A \to A$ mit $f(a_j) = a_{i_j}$ entspricht der Anordnung $(a_{i_1}, \ldots a_{i_n})$

Definition (Faktorielle)

Für eine Zahl $n \geq 1$ sei $n! = 1 \cdot 2 \cdots (n-1) \cdot n = n^{\underline{n}}$ die Faktorielle von n. Wir setzen $0! = 1$.

Satz 12

Sei A eine endliche Menge mit n Elementen. Es gibt es genau $n!$ viele Permutationen von A.

Beweis: Wähle $k = |A|$ in Satz 10. □

Definition (Binomialkoeffizient)

Für eine Zahlen k, n mit $0 \leq k \leq n$ sei

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)!k!}$$

der Binomialkoeffizient von n und k.

Beachte: Es gilt für alle $n \geq 0$

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Satz 13

Sei A eine endliche Menge und $k \leq |A|$. Dann gilt

$$\left|\binom{A}{k}\right| = \binom{|A|}{k}.$$

Beweis: Sei $|A| = n$.

Wegen Satz 10 gibt es $n^{\underline{k}}$ Möglichkeiten, aus den n vielen Elementen von A genau k Elemente ohne Zurücklegen und mit Berücksichtigung der Reihenfolge auszuwählen.

Eine solche Auswahl können wir auch wie folgt treffen:

1. Wähle eine k-elementige Teilmenge von A aus ($\left|\binom{A}{k}\right|$ Möglichkeiten)
2. Ordne die k ausgewählten Elemente beliebig an ($k!$ Möglichkeiten).

Kombinatorik: Abzählen von Mengen

Also gilt $n^{\underline{k}} = |\binom{A}{k}| \cdot k!$, d.h. $|\binom{A}{k}| = \frac{n^{\underline{k}}}{k!} = \binom{n}{k}$. □

Letzter Fall: Anzahl der Möglichkeiten, aus n Elementen k Elemente mit Zurücklegen und ohne Berücksichtigung der Reihenfolge auszuwählen.

In diesem Fall kann eine konkrete Auswahl (mit Zurücklegen und ohne Berücksichtigung der Reihenfolge) als eine Multimenge mit k Elementen verstanden werden: Ein Element kann mehrfach in der Multimenge enthalten sein, aber die Reihenefolge spielt keine Rolle.

Definition (Multimenge über der Menge A)

Sei A eine Menge. Eine Multimenge über A ist eine Abbildung $M : A \to \mathbb{N}$.

Die Größe dieser Multimenge ist $\|M\| = \sum_{a \in A} M(a)$.

Satz 14

Sei A eine endliche Menge mit n Elementen. Die Anzahl der Multimengen über A der Größe k ist $\binom{n+k-1}{k}$.

Beweis: Eine Multimenge über $A = \{a_1, a_2, \ldots, a_n\}$ der Größe k entspricht einem Tupel $(k_1, k_2, \ldots, k_n) \in \mathbb{N}^n$ mit $\sum_{i=1}^{n} k_i = k$.

Solch ein Tupel kann man mit der wie folgt konstruierten Folge der Länge $n + k - 1$ identifizieren:

- Notiere zunächst k_1 mal das Symbol $\square$.
- Notiere danach einmal das Trennsymbol $|$.
- Notiere danach k_2 mal das Symbol $\square$.
- Notiere danach einmal das Trennsymbol $|$.

  $\vdots$
- Notiere k_n mal das Symbol $\square$.

Beispiel: Das Tupel $(2, 0, 3, 1, 0)$ entspricht der Folge

$$\square\,\square\,|\,|\,\square\,\square\,\square\,|\,\square\,|.$$

Solch eine Folge kann man dadurch auswählen, indem man aus $n + k - 1$ (= Länge der Folge) vielen Positionen genau die k Positionen auswählt, wo das Zeichen $\square$ steht.

Nach Satz 13 gibt es dafür $\binom{n+k-1}{k}$ Möglichkeiten. $\square$

Satz 15

Seien A und B endliche Mengen. Dann gilt $|B^A| = |B|^{|A|}$.

Beweis: Sei $A = \{a_1, a_2, \ldots, a_n\}$.

Eine Abbildung $f : A \to B$ kann mit dem n-Tupel

$$(f(a_1), f(a_2), \ldots, f(a_n)) \in B^n$$

identifiziert werden.

Umgekehrt kann ein n-Tupel $(b_1, \ldots, b_n) \in B^n$ mit der Abbildung $f : A \to B$ mit $f(a_i) = b_i$ für $1 \leq i \leq n$ identifiziert werden.

Es folgt: $|B^A| = |B^n| = |B|^{|A|}$ mit Satz 9. □

Satz 16

Für eine endliche Menge A gilt $|2^A| = 2^{|A|}$.

Beweis: Sei $A = \{a_1, \ldots, a_n\}$.

Eine Teilmenge $B \subseteq A$ kann mit der Abbildung $f_B : A \to \{0, 1\}$ mit

$$f_B(a) = \begin{cases} 0 & \text{falls } a \notin B \\ 1 & \text{falls } a \in B \end{cases}$$

identifiziert werden.

Umgekehrt entspricht eine Abbildung $f : A \to \{0, 1\}$ der Teilmenge $A_f = f^{-1}(1)$.

Wir müssen also die Anzahl der Funktionen $f : \{a_1, \ldots, a_n\} \to \{0, 1\}$ zählen.

Diese ist nach Satz 15 gleich 2^n. □

Satz 17

Es gilt $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Beweis: Sei A eine Menge mit n Elementen. Dann gilt

$$2^A = \bigcup_{k=0}^{n} \binom{A}{k}$$

Außerdem gilt für $i \neq j$:

$$\binom{A}{i} \cap \binom{A}{j} = \emptyset$$

Mit Satz 7 und Satz 13 ergibt sich

$$2^n = |2^A| = |\bigcup_{k=0}^{n} \binom{A}{k}| = \sum_{k=0}^{n} |\binom{A}{k}| = \sum_{k=0}^{n} \binom{n}{k}.$$

Satz 18

Es gilt $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.

Beweis: Sei A eine Menge mit $|A| = n$ und sei $a \in A$ beliebig. Dann gilt

$$\binom{A}{k} = \binom{A \setminus \{a\}}{k} \cup \{B \cup \{a\} \mid B \in \binom{A \setminus \{a\}}{k-1}\}.$$

Die beiden Mengen in dieser Vereinigung sind disjunkt, weshalb gilt:

$$\begin{aligned} \binom{n}{k} &= |\binom{A}{k}| \\ &= |\binom{A \setminus \{a\}}{k}| + |\{B \cup \{a\} \mid B \in \binom{A \setminus \{a\}}{k-1}\}| \\ &= \binom{n-1}{k} + \binom{n-1}{k-1}. \end{aligned}$$

Satz 19 (Symmetrie der Binomialkoeffizienten)

Es gilt $\binom{n}{k} = \binom{n}{n-k}$.

Beweis:

Sei A eine Menge mit $|A| = n$ und sei $k \leq n$.

Dann ist die Abbildung $f : \binom{A}{k} \to \binom{A}{n-k}$ mit

$$f(B) = A \setminus B \text{ für } B \in \binom{A}{k}$$

eine Bijektion.

Also gilt

$$\binom{n}{k} = |\binom{A}{k}| = |\binom{A}{n-k}| = \binom{n}{n-k}.$$

Satz 20 (Vandermondische Identität)

Es gilt:

$$\sum_{j=0}^{k} \binom{m}{j} \cdot \binom{n}{k-j} = \binom{m+n}{k}.$$

Beweis: Seien A und B Mengen mit $|A| = m$, $|B| = n$ und $A \cap B = \emptyset$.

Es gilt

$$\binom{A \cup B}{k} = \bigcup_{j=0}^{k} \{S \cup T \mid S \in \binom{A}{j}, T \in \binom{B}{k-j}\}$$

Die Mengen in dieser Vereinigung sind paarweise disjunkt. Also gilt:

Kombinatorik: Einfache Identitäten

$$
\begin{aligned}
\binom{m+n}{k} &= |\binom{A \cup B}{k}| \\
&= \sum_{j=0}^{k} |\{S \cup T \mid S \in \binom{A}{j}, T \in \binom{B}{k-j}\}| \\
&= \sum_{j=0}^{k} |\{(S,T) \mid S \in \binom{A}{j}, T \in \binom{B}{k-j}\}| \\
&= \sum_{j=0}^{k} |\binom{A}{j} \times \binom{B}{k-j}| \\
&= \sum_{j=0}^{k} \binom{m}{j} \cdot \binom{n}{k-j}.
\end{aligned}
$$

Satz 21 (Binomischer Lehrsatz)

Für alle natürlichen Zahlen $n \geq 0$ und alle reellen Zahlen $x, y \in \mathbb{R}$ gilt:

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

Beweis 1: Induktion über n.

Induktionsanfang: Für $n = 0$ gilt

$$(x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k}.$$

Induktionsschritt: Angenommen es gilt

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

$$
\begin{aligned}
& (x+y)^{n+1} \\
= \quad & (x+y) \cdot \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\
= \quad & \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1} \\
= \quad & \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} \\
= \quad & \binom{n}{0} x^0 y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) x^k y^{n+1-k} + \binom{n}{n} x^{n+1} y^0 \\
= \quad & \binom{n+1}{0} x^0 y^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + \binom{n+1}{n+1} x^{n+1} y^0 \\
= \quad & \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}
\end{aligned}
$$

Beweis 2: Kombinatorischer Ansatz

Schreiben wir

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdot(x+y)\cdots(x+y)}_{n \text{ viele}} \tag{1}$$

und multiplizieren das Produkt auf der rechten Seite in Gedanken aus.

Dabei entstehen Terme der Form $x^k y^{n-k}$.

Wie oft entsteht der Term $x^k y^{n-k}$?

Beim Ausmultiplizieren der rechten Seite der Gleichung (1) gibt es genau $\binom{n}{k}$ viele Möglichkeiten k mal den Term x (und damit $n-k$ mal den Term y) auszuwählen.

Also kommt der Term $x^k y^{n-k}$ genau $\binom{n}{k}$ oft vor. □

Kombinatorik: Der Binomische Lehrsatz

Die klassischen binomischen Formeln

$$\begin{aligned}(x+y)^2 &= x^2+2xy+y^2\\ (x-y)^2 &= x^2-2xy+y^2\end{aligned}$$

sind Spezialfälle des Binomischen Lehrsatzes.

Ebenso folgt Satz 17 sofort aus dem Binomischen Lehrsatz:

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}.$$

Graphentheorie: Grundbegriffe

Definition (gerichteter Graph)

Ein gerichteter Graph (engl. directed graph oder Digraph) ist ein Paar $G = (V, E)$, wobei $V \neq \emptyset$ eine beliebige nicht-leere Menge ist (die Menge der Knoten), und $E \subseteq V \times V$ eine binäre Relation auf V ist (die Menge der Kanten oder die Kantenrelation).

Definition (ungerichteter Graph, einfacher Graph)

Ein Digraph $G = (V, E)$ ist ungerichtetet, falls die Kantenrelation E symmetrisch ist (d.h. wir können die Richtung der Kanten vergessen).

Ein einfacher Graph ist ein ungerichteter Graph $G = (V, E)$, wobei E zusätzlich irreflexiv ist (d.h. es gibt keine Schlingen).

Konvention:

- Für einen einfachen Graphen $G = (V, E)$ betrachten wir E als eine Menge von 2-elementigen Teilmengen von V, d.h.

$$E \subseteq \{\{x, y\} \mid x, y \in V, x \neq y\}.$$

- Wenn wir im folgenden nur von einem Graphen sprechen, dann meinen wir stets einen einfachen Graphen.

Definition (endliche Graphen)

Ein Graph $G = (V, E)$ ist endlich, falls V endlich ist (dann ist auch E endlich).

Meistens betrachten wir hier nur endliche Graphen.

Definition (isomorphe Graphen)

Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ sind isomorph, falls es eine bijektive Abbildung $f : V_1 \to V_2$ gibt mit

$$\forall x, y \in V_1 : \{x, y\} \in E_1 \iff \{f(x), f(y)\} \in E_2$$

Wir unterscheiden nicht zwischen isomorphen Graphen.

Beispiel: Die folgenden zwei Graphen sind isomorph.

Graphentheorie: Grundbegriffe

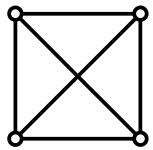
Warum beschäftigen wir uns mit Graphen?

- Graphen können zur Modellierung vieler Systeme verwendet werden (z. B. endliche Automaten, Schaltkreise, Straßennetzwerke, Computernetzwerke, soziale Netzwerke, Internet).
- Graphen treten jedoch auch als Datenstrukturen in Gebieten auf, wo man sie erst nicht vermuten würde.
  So werden z. B. gerichtete Graphen zur Modellierung des dynamischen Verhaltens von Hard- und Softwaresystemen eingesetzt (Model-Checking).
- Graphen sind mathematisch sehr natürliche Gebilde.
  Trotz ihrer Einfachheit ermöglichen sie eine mathematisch umfangreiche Theorie.
- Graphen sind anschaulich, man kann Bilder malen.

K_n bezeichnet den vollständigen Graphen auf n Knoten:

$$K_n = (\{1, \ldots, n\}, \{\{x, y\} \mid 1 \leq x, y \leq n, x \neq y\})$$

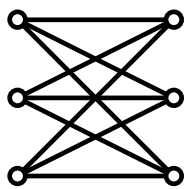
Beispiel: K_4:



Für $n, m \geq 1$ ist $K_{n,m}$ der folgende Graph:

$$K_{n,m} = (\{\langle i, 0\rangle \mid 1 \leq i \leq n\} \cup \{\langle j, 1\rangle \mid 1 \leq j \leq m\},$$
$$\{\{\langle i, 0\rangle, \langle j, 1\rangle\} \mid 1 \leq i \leq n, 1 \leq j \leq m\})$$

Beispiel: $K_{3,3}$:



P_n ($n \geq 2$) bezeichnet den Pfad auf n Knoten:

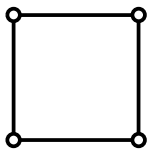
$$P_n = (\{1, \ldots, n\}, \{\{x, y\} \mid 1 \leq x, y \leq n, y = x + 1\})$$

Beispiel: P_4:

C_n ($n \geq 3$) bezeichnet den Kreis (engl. circuit) auf n Knoten:

$$C_n = (\{1, \ldots, n\}, \{\{x, y\} \mid 1 \leq x, y \leq n, y - x \in \{1, n - 1\}\})$$

Beispiel: C_4:



Definition (Teilgraphen)

Sei G ein Graph.

1. Ein Teilgraph des Graphen $G = (V, E)$ ist ein Graph $G' = (V', E')$ mit $V' \subseteq V$ und $E' \subseteq E$.
2. Ein induzierter Teilgraph des Graphen $G = (V, E)$ ist ein Teilgraph $G' = (V', E')$ von G, für den gilt:

$$\forall x, y \in V' : \{x, y\} \in E \Rightarrow \{x, y\} \in E'$$

Offenbar ist der induzierte Teilgraph $G' = (V', E')$ von G schon eindeutig durch V' bestimmt. Wir können also definieren:

3. Sei $G = (V, E)$ ein Graph und $V' \subseteq V$. Dann ist $G[V']$ der durch G und V' eindeutig bestimmte induzierte Teilgraph, d.h.

$$G[V'] = (V', \{\{x, y\} \mid x, y \in V', \{x, y\} \in E\}).$$

Sprechweise: Seien G und H Graphen.

Wir sagen, *in G gibt es einen H*, falls G einen zu H isomorphen Teilgraphen hat.

Wir sagen, *in G gibt es einen induzierten H*, falls G einen zu H isomorphen induzierten Teilgraphen hat.

Beispiel:

Für jedes $n \geq 3$ gibt es in C_n einen P_n aber keinen induzierten P_n.

Es gibt aber einen induzierten P_{n-1} in C_n.

Definition

Sei $G = (V, E)$ ein Graph. Für $e \in E$ sei $G \setminus e = (V, E \setminus \{e\})$ und für $v \in V$ sei $G \setminus v = G[V \setminus \{v\}]$.

Der Graph $G \setminus v$ entsteht also aus G durch Entfernen von v und allen Kanten, die v enthalten.

Definition (Nachbarn, Grad eines Knoten)

Sei $G = (V, E)$ ein Graph und $U \subseteq V$.

$N_G(U) = \{y \in V \mid \exists x \in U : \{x, y\} \in E\}$ ist die Nachbarschaft von U.

Für $U = \{u\}$ schreiben wir $N_G(u)$ anstatt $N_G(U)$.

Der Grad (engl. degree) von $x \in V$ ist $d_G(x) = |N_G(x)| \in \mathbb{N} \cup \{\infty\}$ (die Anzahl der Nachbarn von x).

Definition (Wege)

Ein Weg (der Länge $n \geq 2$) im Graphen $G = (V, E)$ ist eine Folge von Knoten $[x_1, x_2, \ldots, x_n]$ mit $\{x_i, x_{i+1}\} \in E$ für alle $1 \leq i \leq n-1$.

Ein Weg $[x_1, x_2, \ldots, x_n]$ mit $x_i \neq x_j$ für alle $i \neq j$ ist ein einfacher Weg.

Die Knoten x_1 und x_n sind die Endpunkte des Weges $[x_1, x_2, \ldots, x_n]$.

Ein einfacher Weg der Länge n in G ist also ein zu P_n isomorpher Teilgraph von G.

Definition (zusammenhängende Graphen)

Ein Graph $G = (V, E)$ ist zusammenhängend, wenn es für je zwei Knoten $x, y \in V$ mit $x \neq y$ in G einen Weg mit den Endpunkten x und y gibt.

Definition (Zusammenhangskomponenten)

Eine Zusammenhangskomponente des Graphen $G = (V, E)$ ist ein induzierter Teilgraph $G[V']$ $(V' \subseteq V)$ mit:

- $G[V']$ ist zusammenhängend.
- $\forall x \in V \setminus V' : G[V' \cup \{x\}]$ ist nicht zusammenhängend.

Definition (bipartite Graphen)

Ein Graph $G = (V, E)$ ist bipartit, wenn es eine Partition $V = A \cup B$ $(A \cap B = \emptyset)$ gibt mit $E \subseteq \{\{a, b\} \mid a \in A, b \in B\}$.

Beispiele:

- Der Graph $K_{n,m}$ $(n, m \geq 1)$ ist offensichtlich bipartit.
- P_n ist bipartit für jedes $n \geq 2$.
- C_n ist bipartit genau dann, wenn n gerade ist.

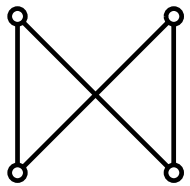
Definition (planare Graphen)

Ein Graph $G = (V, E)$ ist planar, wenn er in die Ebene so eingezeichnet werden kann, dass sich die Kanten nicht schneiden.

Diese Definition ist noch nicht wirklich formal (kommt noch), sie ist jedoch hoffentlich unmissverständlich.

Beispiel:

Ist der folgende Graph planar?



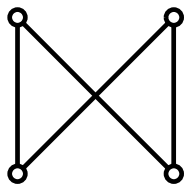
Definition (planare Graphen)

Ein Graph $G = (V, E)$ ist planar, wenn er in die Ebene so eingezeichnet werden kann, dass sich die Kanten nicht schneiden.

Diese Definition ist noch nicht wirklich formal (kommt noch), sie ist jedoch hoffentlich unmissverständlich.

Beispiel:

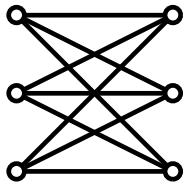
Ist der folgende Graph planar?



Ja, denn dieser Graph ist genau C_4.

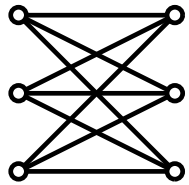
Beispiel:

Ist der folgende Graph $K_{3,3}$ planar?



Beispiel:

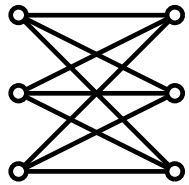
Ist der folgende Graph $K_{3,3}$ planar?



Er scheint nicht planar zu sein, aber wer weiß!

Beispiel:

Ist der folgende Graph $K_{3,3}$ planar?



Er scheint nicht planar zu sein, aber wer weiß!

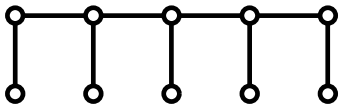
Später werden wir beweisen, dass $K_{3,3}$ nicht planar ist.

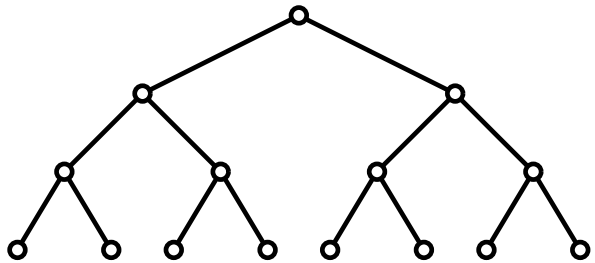
Definition (Bäume)

Ein Baum ist ein zusammenhängender Graph G ohne echte Kreise.

Letzteres bedeutet, dass es in G keinen C_n gibt, falls $n \geq 3$.

Beispiele für Bäume:





P_n ist stets ein Baum.

Satz 22

(1) $G = (V, E)$ *ist ein Baum* $\iff$

- G *ist zusammenhängend und*
- $\forall e \in E : G \setminus e$ *ist nicht zusammenhängend.*

(2) *Sei* $G = (V, E)$ *ein endlicher Baum. Dann gilt:*

(a) *Es gibt einen Knoten* $x \in V$ *mit* $d_G(x) \leq 1$

(b) $|V| = |E| + 1$.

(c) G *ist planar.*

Beweis von (1):

"$\Leftarrow$": Sei $G = (V, E)$ kein Baum aber dennoch zusammenhängend.

Wir zeigen, dass es in G eine Kante gibt, nach deren Entfernen der Graph immer noch zusammenhängend ist.

In G muss es einen Kreis C_n mit $n \geq 3$ geben, d.h. es gibt Kanten

$$\{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{n-1}, x_n\}, \{x_n, x_1\} \in E$$

mit $x_i \neq x_j$ für $i \neq j$.

$\rightsquigarrow$ $G \setminus \{x_1, x_2\}$ weiterhin zusammenhängend, denn zwischen x_1 und x_2 gibt es einen Weg in $G \setminus \{x_1, x_2\}$: $[x_2, \ldots, x_n, x_1]$.

"$\Rightarrow$": Sei $G = (V, E)$ ein Baum, und sei $e = \{x, y\} \in E$ beliebig.

Angenommen $G \setminus e$ ist zusammenhängend.

$\rightsquigarrow$ In $G \setminus e$ gibt es einen einfachen Weg $[x, z_1, \ldots, z_n, y]$ von x nach y.

Da die Kante $e = \{x, y\}$ in $G \setminus e$ nicht vorhanden ist, muss $n \geq 1$ gelten.

Damit erhalten wir aber einen Kreis in G aus mindestens 3 Knoten:
$[x, z_1, \ldots, z_n, y, x]$

Also ist G doch kein Baum.

Beweis von (2a):

Sei $G = (V, E)$ ein endlicher Graph mit $\forall x \in V : d_G(x) \geq 2$.

Wir zeigen, dass G kein Baum sein kann.

Wir konstruieren hierzu einen unendlichen Weg $[x_0, x_1, x_2, \ldots]$ ($\{x_i, x_{i+1}\} \in E$ für alle $i \geq 0$) wie folgt:

- Seien $x_0, x_1 \in V$ beliebig mit $\{x_0, x_1\} \in E$.
- Angenommen, $x_0, \ldots, x_n$ sind bereits gewählt ($n \geq 1$).

  Wähle $x_{n+1} \in N_G(x_n) \setminus \{x_{n-1}\}$
  (geht, da x_n mindestens 2 Nachbarn hat).

Da G endlich ist, gibt es $i < j$ mit $x_i = x_j$.

O.B.d.A. sind die Knoten $x_i, x_{i+1}, \ldots, x_{j-1}$ paarweise verschieden.

Aus der Konstruktion der Folge $[x_0, x_1, x_2, \ldots]$ folgt außerdem $j \geq i + 3$.

$\rightsquigarrow$ $[x_i, x_{i+1}, \ldots, x_{j-1}, x_i]$ ist ein Kreis mit mindestens 3 Knoten.

Beweis von (2b):

Induktion über $|V|$.

IA: $|V| = 1$. Dieser Fall ist trivial, da $|E| = 0$.

IS: Die Gleichung $|V| = |E| + 1$ sei korrekt für alle Bäume mit maximal n Knoten.

Sei $G = (V, E)$ ein Baum mit $|V| = n + 1 \geq 2$.

Wegen (2a) gibt es in G einen Knoten $x \in V$ mit $d_G(x) \leq 1$.

Wegen $|V| \geq 2$ muss $d_G(x) = 1$ gelten.

Sei y der eindeutige Nachbar von x.

Dann ist $G \setminus x$ ein Baum mit n vielen Knoten.

Induktionsvoraussetzung $\rightsquigarrow |V| - 1 = |V \setminus \{x\}| = |E \setminus \{\{x, y\}\}| + 1 = |E|$.

Also gilt $|V| = |E| + 1$.

Beweis von (2c):

Induktion über $|V|$.

IA: $|V| = 1$. Dann ist G offensichtlich planar.

IS: Sei jeder Baum mit maximal n Knoten planar.

Sei $G = (V, E)$ ein Baum mit $|V| = n + 1 \geq 2$.

Wie bei (2b) gibt es einen Knoten $x \in V$ mit genau einen Nachbarn y.

Dann ist $G \setminus x$ ein Baum mit n vielen Knoten und somit planar.

Den fehlenden Knoten x mit der Kante $\{x, y\}$ können wir aber dann problemlos zu einer planaren Darstellung von G' hinzufügen (die Kante $\{x, y\}$ darf dabei beliebig kurz sein). □

Ein Baum G mit mehr als zwei Knoten kann keinen Knoten x mit $d_G(x) = 0$ enthalten (sonst wäre G nicht zusammenhängend).

Also muss G nach Satz 22 einen Knoten x mit $d_G(x) = 1$ enthalten.

Die Knoten von G mit $d_G(x) = 1$ nennt man auch die Blätter von G.

Satz 23

Sei $G = (V, E)$ ein endlicher Graph ohne echte Kreise (man nennt einen solchen Graphen auch einen Wald). Sei z die Anzahl der Zusammenhangskomponenten von G. Dann gilt $|V| = |E| + z$.

Beweis:

Seien (V_i, E_i) $(1 \leq i \leq z)$ die Zusammenhangskomponenten von G.

$\rightsquigarrow$ (V_i, E_i) ist ein Baum.

$\rightsquigarrow$ $|V_i| = |E_i| + 1$.

$\rightsquigarrow$ $|V| = \sum_{i=1}^{z} |V_i| = \sum_{i=1}^{z} (|E_i| + 1) = |E| + z$. □

Graphentheorie: Planare Graphen

Ein Linienzug im $\mathbb{R}^2$ ist eine Teilmenge $L \subseteq \mathbb{R}^2$, so dass eine stetige Bijektion $f : [0,1] \to L$ mit f^{-1} stetig existiert.

Die Punkte $f(0)$ und $f(1)$ sind die Endpunkte von L.

Eine planare Einbettung des Graphen $G = (V, E)$ in den $\mathbb{R}^2$ ist ein Paar (p, ℓ), wobei gilt:

- $p : V \to \mathbb{R}^2$ ist injektiv und ordnet jedem Knoten einen Punkt des $\mathbb{R}^2$ zu.
- $\ell : E \to 2^{\mathbb{R}^2}$ ordnet jeder Kante $\{x, y\} \in E$ einen Linienzug $\ell(x, y)$ mit den Endpunkten $p(x)$ und $p(y)$ zu, so dass für alle Kanten $\{u, v\}, \{x, y\} \in E$ mit $\{u, v\} \neq \{x, y\}$ gilt:

$$(\ell(u, v) \setminus \{p(u), p(v)\}) \cap \ell(x, y) = \emptyset$$

Definition (planare Graphen)

Ein Graph G ist planar, falls er eine planare Einbettung (p, ℓ) in den $\mathbb{R}^2$ hat.

Beachte: Im allgemeinen muss $\ell(x, y)$ keine Gerade sein, aber es gilt der folgenden Satz, auf dessen Beweis wir hier verzichten.

Satz 24 (Satz von Wagner und Fáry)

Sei $G = (V, E)$ planar. Dann gibt es eine planare Einbettung (p, ℓ) von G, so dass für alle Kanten $\{x, y\} \in E$ gilt:

$$\ell(x, y) = \{\alpha \cdot p(x) + (1 - \alpha) \cdot p(y) \mid \alpha \in [0, 1]\}.$$

Graphentheorie: Planare Graphen

Betrachte wieder eine planare Einbettung (p, ℓ) eines planaren endlichen Graphen $G = (V, E)$ in den $\mathbb{R}^2$.

Eine Facette dieser Einbettung ist eine maximale Teilmenge $F \subseteq \mathbb{R}^2$ mit:

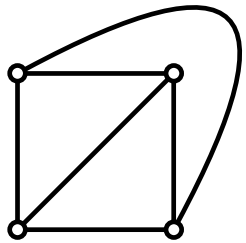
- F ist zusammenhängend, d.h. für alle Punkte $p_1, p_2 \in F$ $(p_1 \neq p_2)$ gibt es einen Linienzug $L \subseteq F$ mit den Endpunkten p_1 und p_2.
- F ist disjunkt zu allen Linienzügen der Einbettung: $\forall \{x, y\} \in E : F \cap \ell(x, y) = \emptyset$

Beachte: Da G endlich ist, gibt es genau eine unendliche Facette.

Satz 25 (Eulers Formel, 1758)

Sei $G = (V, E)$ ein planarer endlicher Graph mit z vielen Zusammenhangskomponenten. Sei k die Anzahl der Facetten einer planaren Einbettung von G. Dann gilt: $|V| + k = |E| + z + 1$.

Beispiel: Hier ist eine planare Einbettung des K_4:



K_4 hat somit 4 Facetten, 4 Knoten und 6 Kanten.

In der Tat gilt $4 + 4 = 6 + 1 + 1$.

Beweis von Eulers Formel: Induktion über die Anzahl k der Facetten.

IA: $k = 1$, d.h. es gibt nur die unendliche Facette.

$\rightsquigarrow$ in G kann es keinen Kreis C_m $(m \geq 3)$ geben.

$\rightsquigarrow$ jede Zusammenhangskomponente von G ist ein Baum.

$\rightsquigarrow$ $|V| = |E| + z$ (siehe Satz 23)

$\rightsquigarrow$ $|V| + k = |E| + z + 1$.

IS: $k \geq 2$, es gibt also eine endliche Facette.

Sei $e = \{x, y\} \in E$ eine beliebige Kante auf dem Rand dieser endlichen Facette.

$\rightsquigarrow$ $G \setminus e$ hat weiterhin z viele Zusammenhangskomponenten aber nur noch $k - 1$ viele Facetten.

Induktionsvoraussetzung für $G \setminus e \rightsquigarrow |V| + k - 1 = |E| - 1 + z + 1$.

$\rightsquigarrow |V| + k = |E| + z + 1$. □

Aus der Eulerformel folgt sofort, dass die Anzahl der Facetten eines planaren Graphen unabhängig von der konkreten planaren Einbetttung ist.

Die Eulerformel ist auch als Eulerscher Polyedersatz bekannt, denn aus ihr folgt:

Eulerscher Polyedersatz

Für einen (beschränkten und konvexen) Polyeder (z.B. Tetraeder, Würfel, Oktaeder) mit e Ecken, k Kanten, und f Flächen gilt

$$e + f - k = 2$$

Korollar 1 aus Eulers Formel

Sei $G = (V, E)$ endlich und planar, $|V| \geq 3$.

1. Es gilt $|E| \leq 3 \cdot |V| - 6$.
2. Es gibt einen Knoten x mit $d_G(x) \leq 5$.
3. Ist G zusätzlich bipartit, so gilt $|E| \leq 2 \cdot |V| - 4$.

Beweis: Sei $G = (V, E)$ endlich, planar.

Durch Hinzufügen weiterer Kanten können wir erreichen, dass G zusammenhängend (und weiterhin planar) ist.

Zu (1): Falls G nur eine Facette hat, ist G ein Baum und es gilt

$$|E| = |V| - 1 \leq 3 \cdot |V| - 6 \text{ da } |V| \geq 3.$$

Falls G mindestens 2 Facetten hat, wird jede Facette von ≥ 3 Kanten berandet.

Ausserdem kommt jede Kante nur im Rand von ≤ 2 Facetten vor.

$\rightsquigarrow$ Anzahl der Facetten $\leq \frac{2}{3} \cdot |E|$.

Eulerformel $\rightsquigarrow$ $|V| + \frac{2}{3} \cdot |E| \geq |E| + 2$

$\rightsquigarrow$ $|E| \leq 3 \cdot |V| - 6$

Zu (2): Es gilt $|E| = \frac{1}{2} \sum_{x \in V} d_G(x) \leq 3 \cdot |V| - 6$, d.h.

$$\sum_{x \in V} d_G(x) \leq 6 \cdot |V| - 12.$$

Würde $d_G(x) \geq 6$ für jeden Knoten $x \in V$ gelten, so würden wir den folgenden Widerspruch erhalten:

$$6 \cdot |V| \leq \sum_{x \in V} d_G(x) \leq 6 \cdot |V| - 12$$

Zu (3): Sei G nun noch zusätzlich bipartit.

Dann wird jede Facette von mindestens 4 Kanten berandet.

$\rightsquigarrow$ Anzahl der Facetten $\leq \frac{1}{2} \cdot |E|$.

Eulerformel $\rightsquigarrow$ $|V| + \frac{1}{2} \cdot |E| \geq |E| + 2$

$\rightsquigarrow$ $|E| \leq 2 \cdot |V| - 4$ □

Korollar 2 aus der Eulerformel

K_5 und $K_{3,3}$ sind nicht planar.

Beweis:

Wäre K_5 planar, so würde aus Korollar 1 folgen:

$$10 = |E| \leq 3 \cdot |V| - 6 = 3 \cdot 5 - 6 = 9.$$

Wäre $K_{3,3}$ planar, so würde aus Korollar 1 folgen:

$$9 = |E| \leq 2 \cdot |V| - 4 = 2 \cdot 6 - 4 = 8.$$

In einem gewissen Sinn gilt auch eine Umkehrung von Korollar 2.

Definition (Unterteilung)

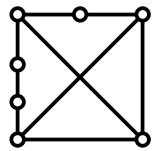
Ein Graph H ist eine Unterteilung des Graphen G, falls ein $n \geq 1$ und Graphen $G_1 = (V_1, E_1), G_2 = (V_2, E_2), \ldots, G_n = (V_n, E_n)$ existieren mit folgenden Eigenschaften:

- $G_1 = G$, $G_n = H$
- Für alle $1 \leq i \leq n-1$ gibt es $z \in V_{i+1} \setminus V_i$ und $e = \{x, y\} \in E_i$ mit

$$V_{i+1} = V_i \cup \{z\}, \quad E_{i+1} = (E_i \setminus \{e\}) \cup \{\{x, z\}, \{z, y\}\}.$$

Der Graph G_{i+1} entsteht also aus G_i, indem die Kante $e = \{x, y\}$ durch einen neuen Knoten z in zwei Kanten unterteilt wird.

Eine Unterteilung des K_4:



Auf den Beweis des folgenden sehr berühmten Satzes müssen wir leider aus Zeitgründen verzichten.

Satz 26 (Satz von Kuratowski, 1930)

Ein endlicher Graph G ist genau dann planar, wenn er keine Unterteilung von K_5 oder $K_{3,3}$ enthält.

Graphentheorie: Färbungen von Graphen

Sei $G = (V, E)$ ein Graph und $k \geq 1$. Eine k-Färbung von G ist eine Abbildung $c : V \to \{1, \ldots, k\}$, so dass gilt:

$$\forall \{x, y\} \in E : c(x) \neq c(y).$$

Die Färbungszahl $\chi(G)$ von G ist die kleinste Zahl $k \geq 1$, so dass eine k-Färbung von G existiert.

Beispiele:

- $\chi(K_n) = n$
- $\chi(K_{m,n}) = 2$
- $\chi(G) \leq 2$ genau dann, wenn G bipartit ist.
- $\chi(P_n) = 2$
- Falls n gerade: $\chi(C_n) = 2$, falls n ungerade: $\chi(C_n) = 3$

Anwendungsbeispiel: Stundenplanung

Das Erstellen eines Stundenplans bei dem alle Wünsche von Lehrenden und Studierenden erfüllt sind, kann auf ein Färbungsproblem reduziert werden.

- Knoten des Graphen: Alle Vorlesungen des aktuellen Semesters (DMI, ADS, etc.)
- Farben: mögliche Zeiten (z.B. Mo 16-18, Mi 14-16)
- Kanten: Die Vorlesungen A und B sind durch eine Kante verbunden, falls A und B von der gleichen Lehrkraft angeboten werden, oder es einen Studierenden gibt, der sowohl A als auch B besuchen will.

Wir gehen hier von genügend Räumen aus.

Der Maximalgrad $\Delta(G)$ des Graphen G ist $\Delta(G) = \max\{d_G(x) \mid x \in V\}$.

Satz 27

Für jeden endlichen Graphen G gilt $\chi(G) \leq \Delta(G) + 1$.

Beweis: Wir definieren eine Färbung $c : V \to \{1, \ldots, \Delta(G) + 1\}$ von G mit dem folgenden Greedy-Algorithmus:

$C := \emptyset$

while $C \neq V$ **do**

Wähle $x \in V \setminus C$ beliebig.

Wähle $f \in \{1, \ldots, \Delta(G) + 1\} \setminus \{c(y) \mid y \in C \cap N_G(x)\}$ beliebig. (*)

$c(x) := f$; $C := C \cup \{x\}$

endwhile

Beachte: Wegen $|\{c(y) \mid y \in C \cap N_G(x)\}| \leq \Delta(G)$ gibt es die Farbe f in (*) tatsächlich. □

Im Allgemeinen gilt $\chi(G) = \Delta(G) + 1$, z. B.

- $\chi(K_n) = n = \Delta(K_n) + 1$
- Für m ungerade gilt $\chi(C_m) = 3 = \Delta(C_m) + 1$

Dies sind aber auch alle Beispiele:

Satz 28 (Brooks, 1941)

Sei der endliche zusammenhängende Graph G kein K_n und kein C_m für m ungerade. Dann gilt $\chi(G) \leq \Delta(G)$.

Für den Beweis benötigen wir das folgende Lemma:

Lemma 1

Sei $G = (V, E)$ ein endlicher zusammenhängender Graph, so dass ein $x \in V$ mit $d_G(x) < \Delta(G)$ existiert. Dann gilt $\chi(G) \leq \Delta(G)$.

Beweis von Lemma 1:

Sei $G = (V, E)$ endlich und zusammenhängend und sei $d_G(x) < \Delta(G)$.

Sei $S_0 := \{x\}$.

Für $i \geq 1$ definiere nun sukzessive Schichten S_i durch

$$S_i := N_G(S_{i-1}) \setminus (S_{i-1} \cup S_{i-2} \cup \cdots \cup S_0).$$

Beachte:

- $S_i \cap S_j = \emptyset$ für $i \neq j$.
- Alle Nachbarn eines Knoten $x \in S_i$ liegen in $S_{i-1} \cup S_i \cup S_{i+1}$.
- Jeder Knoten $x \in S_i$ mit $i \geq 1$ hat einen Nachbarn in Schicht S_{i-1}.
- G endlich $\rightsquigarrow$ $\exists p \geq 1 : S_p \neq \emptyset$ und $\forall q > p : S_q = \emptyset$.
- G zusammenhängend $\rightsquigarrow$ $V = S_0 \cup S_1 \cup \cdots \cup S_p$.

Wir nummerieren nun die Knoten aus V mit $v_1, \ldots, v_n$ ($n = |V|$) durch:

- Zähle alle Knoten in Schicht S_p auf. $\rightsquigarrow$ $v_1, \ldots, v_{|S_p|}$
- Zähle alle Knoten in Schicht S_{p-1} auf. $\rightsquigarrow$ $v_{|S_p|+1}, \ldots, v_{|S_p|+|S_{p-1}|}$

  $\vdots$
- Der Knoten x wird schließlich v_n.

$\rightsquigarrow$ $\forall i < n : v_i$ hat einen Nachbarn in $\{v_{i+1}, \ldots, v_n\}$

$\rightsquigarrow$ $\forall i < n : |N_G(v_i) \cap \{v_1, \ldots, v_{i-1}\}| \leq \Delta(G) - 1$

Wir können daher den Greedy-Algorithmus benutzen, um G mit $\Delta(G)$ vielen Farben zu färben:

- Färbe die Knoten in der Reihnfolge $v_1, v_2, \ldots, v_n$.
- Dann wird für jeden Knoten $v_1, \ldots, v_{n-1}$ immer eine Farbe aus $\{1, \ldots, \Delta(G)\}$ frei sein.
- Da $d_G(v_n) = d_G(x) \leq \Delta(G) - 1$ gilt, wird auch für v_n am Ende noch eine Farbe aus $\{1, \ldots, \Delta(G)\}$ frei sein. □

Beweis des Satzes von Brooks:

Sei der endliche zusammenhängende Graph G kein K_n und kein C_m für m ungerade.

Falls $\Delta(G) = 0$ gilt, ist $G = K_1$; Widerspruch!

Falls $\Delta(G) = 1$ gilt, ist $G = K_2$; Widerspruch!

Falls $\Delta(G) = 2$ gilt, muss G entweder ein P_n $(n \geq 3)$ oder ein C_m $(m \geq 3)$ mit m gerade sein.

In beiden Fällen gilt $\chi(G) = 2 = \Delta(G)$.

Sei nun $\Delta(G) \geq 3$ im folgenden.

Fall 1: Es gibt $x \in V$ mit $d_G(x) \leq \Delta(G) - 1$.

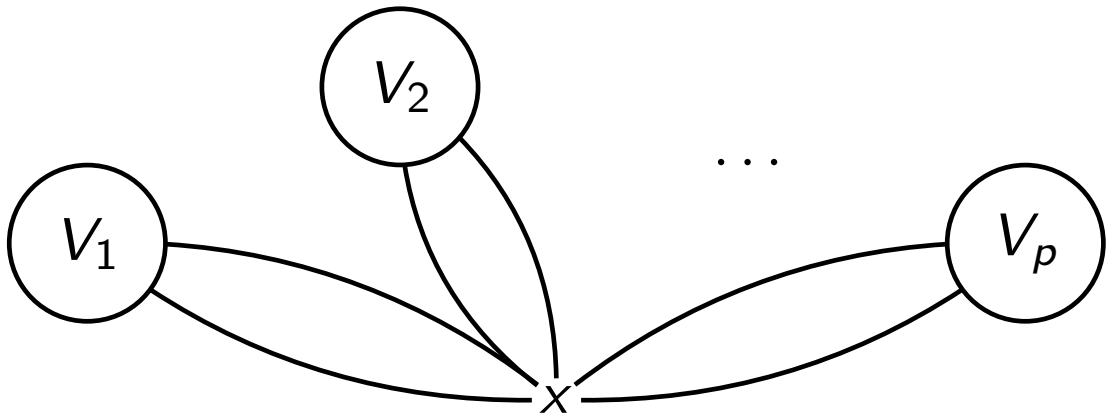
Dann gilt $\chi(G) \leq \Delta(G)$ nach Lemma 1.

Fall 2: $\forall x \in V : d_G(x) = \Delta(G)$.

Alle Knoten haben also den gleichen Grad d $(= \Delta(G) \geq 3)$, man nennt einen solchen Graphen auch d-regulär.

Fall 2a: Es gibt einen Knoten $x \in V$, so dass $G \setminus x$ nicht zusammenhängend ist.

Seien $G[V_1], \ldots, G[V_p]$ $(p \geq 2)$ die Zusammenhangskomponenten von $G \setminus x$, d.h. $V = \{x\} \cup V_1 \cup \cdots \cup V_p$.



Betrachte die zusammenhängenden Graphen $H_i = G[V_i \cup \{x\}]$.

Behauptung: $\chi(H_i) \leq d \ (= \Delta(G))$

Es gilt $d_{H_i}(x) < d_G(x) = d$, d.h. $d_{H_i}(x) \leq d - 1$.

Falls $\Delta(H_i) \leq d - 1$, kann H_i mit $\Delta(H_i) + 1 \leq d$ vielen Farben gefärbt werden.

Gelte also $\Delta(H_i) = d$.

Da in H_i ein Knoten (nämlich x) mit Grad $\leq d - 1 = \Delta(H_i) - 1$ existiert, können wir nach Lemma 1 H_i mit $\Delta(H_i) = d$ vielen Farben färben.

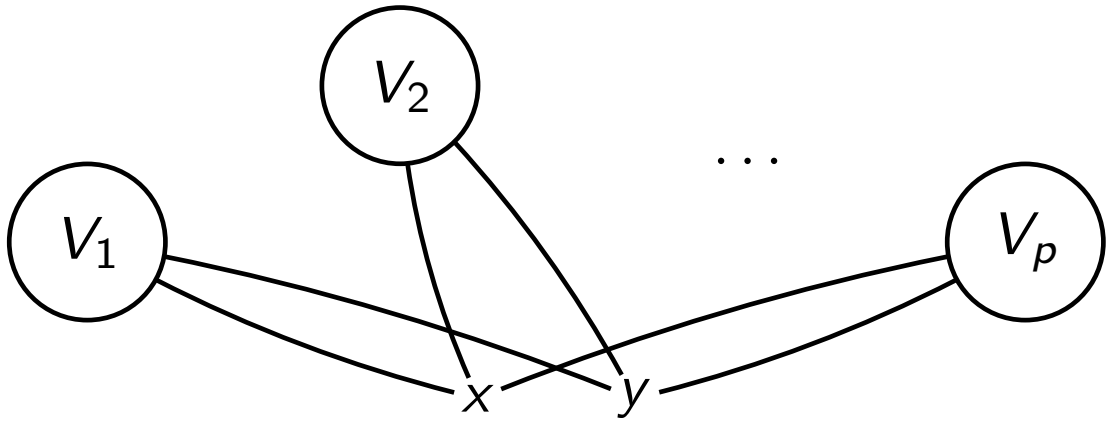
Dies beweist die Behauptung.

In den d-Färbungen der Graphen $H_1 = G[V_1 \cup \{x\}], \ldots, H_p = G[V_p \cup \{x\}]$ können wir davon ausgehen, dass x jeweils die gleiche Farbe bekommt.

Wir können dann diese d-Färbungen zu einer d-Färbung von G vereinigen.

Fall 2b: Für jeden Knoten $x \in V$ ist $G \setminus x$ zusammenhängend, aber es existieren $x, y \in V$, so dass $G[V \setminus \{x, y\}]$ nicht zusammenhängend ist.

Seien $G[V_1], \ldots, G[V_p]$ $(p \geq 2)$ die Zusammenhangskomponenten von $G[V \setminus \{x, y\}]$, d.h. $V = \{x, y\} \cup V_1 \cup \cdots \cup V_p$.



Beachte: Da $G \setminus x$ und $G \setminus y$ zusammenhängend sind, gilt $N_G(x) \cap V_i \neq \emptyset \neq N_G(y) \cap V_i$ für alle $1 \leq i \leq p$.

Betrachte die zusammenhängenden Graphen $H_i = G[V_i \cup \{x, y\}]$.

Völlig analog zu Fall 2a können wir zeigen, dass $\chi(H_i) \leq d$ gilt.

Behauptung: Für alle $1 \leq i \leq p$ existiert eine d-Färbung c_i von H_i mit

$$\forall i \in \{1, \ldots, p\} : c_i(x) = c_i(y) \quad \text{oder} \quad \forall i \in \{1, \ldots, p\} : c_i(x) \neq c_i(y)$$

Wir wissen bereits, dass eine d-Färbung c_i von H_i existiert.

Fall i: $\{x, y\} \in E$.

$\rightsquigarrow \quad \forall i \in \{1, \ldots, p\} : c_i(x) \neq c_i(y)$

Fall ii: $\{x, y\} \notin E$.

Falls $p \geq 3$ gilt $d_{H_i}(x) \leq d_G(x) - 2 = d - 2$ für alle i.

Wir können dann $c_i(x)$ auf eine beliebige Farbe aus $\{1, \ldots, d\} \setminus \{c_i(z) \mid z \in \{y\} \cup N_{H_i}(x)\}$ umsetzen.

Gelte also $p = 2$ und sei o.B.d.A. $c_1(x) = c_1(y)$ und $c_2(x) \neq c_2(y)$.

Beachte: Es gilt $d_{H_1}(x) + d_{H_2}(x) = d$ und $d_{H_1}(y) + d_{H_2}(y) = d$

Falls $d_{H_2}(x) \geq 2$ gilt, folgt $d_{H_1}(x) \leq d - 2$.

Wir können damit in der Färbung c_1 von H_1 die Farbe $c_1(x)$ auf eine beliebige Farbe aus $\{1, \ldots, d\} \setminus \{c_1(z) \mid z \in \{y\} \cup N_{H_1}(x)\}$ umsetzen.

Analog kann man im Fall $d_{H_2}(y) \geq 2$ verfahren.

Sei nun $d_{H_2}(x) = 1 = d_{H_2}(y)$ und sei x' (bzw. y') der eindeutige Nachbar von x (bzw. y) in H_2.

Da $d \geq 3$, gibt es eine Farbe $f \in \{1, \ldots, d\} \setminus \{c_2(x'), c_2(y')\}$.

Also können wir die Färbung c_2 so abändern, dass $c_2(x) = f = c_2(y)$ gilt.

Damit ist die Behauptung bewiesen.

Wie in Fall 2a können wir nun die d-Färbungen c_i aus der Behauptung durch Permutieren der Farben zu einer d-Färbung von G zusammensetzen.

Fall 2c: Für alle $y, z \in V$, ist $G[V \setminus \{y, z\}]$ zusammenhängend.

Da G kein K_n ist, aber zusammenhängend ist, existieren 3 verschiedene Knoten $x, x_1, x_2 \in V$ mit $\{x, x_1\}, \{x, x_2\} \in E$ und $\{x_1, x_2\} \notin E$.

Ausserdem ist $G[V \setminus \{x_1, x_2\}]$ zusammenhängend.

Wir generieren nun wieder eine Auflistung $v_1, \ldots, v_n$ von V:

- Sei $v_1 := x_1$, $v_2 := x_2$, und $v_n = x$.
- Sei $v_{n-1} \in N_G(v_n)$ beliebig, aber verschieden von v_1 und v_2 (beachte: $G[V \setminus \{v_1, v_2\}]$) ist zusammenhängend).

  $\vdots$
- Sei $v_i \in N_G(\{v_{i+1}, \ldots, v_n\})$ beliebig, aber verschieden von v_1, v_2 sowie $v_{i+1}, \ldots, v_n$.

  $\vdots$
- Sei $v_3 \in N_G(\{v_4, \ldots, v_n\})$ beliebig, aber verschieden von v_1, v_2 sowie $v_4, \ldots, v_n$.

Da $G[V \setminus \{v_1, v_2\}]$ zusammenhängend ist, gibt es eine solche Auflistung.

Wir generieren nun eine d-Färbung c von G:

- Wähle eine beliebige Farbe $f \in \{1, \ldots, d\}$ und setze $c(v_1) = c(v_2) = f$ (geht, da $\{v_1, v_2\} = \{x_1, x_2\} \notin E$).
- Färbe nun die Knoten $v_3, \ldots, v_{n-1}$ in dieser Reihnfolge.

  Da v_i für $3 \leq i \leq n-1$ mindestens einen Nachbarn in $\{v_{i+1}, \ldots, v_n\}$ hat, ist immer eine der d vielen Farben für v_i frei.
- Da $v_n = x$ zu v_1 und v_2 benachbart ist, und $c(v_1) = c(v_2)$ gilt, sind die Nachbarn von v_n mit höchstens $d-1$ vielen Farben gefärbt.

  Also ist auch noch für v_n eine Farbe frei.

Dies beendet den Beweis des Satzes von Brooks. □

Graphentheorie: Färbungen von Graphen

Einer der berühmtesten Sätze der Graphentheorie lautet:

Vierfarbensatz (Appel, Haken, 1977)

Für jeden endlichen planaren Graphen G gilt $\chi(G) \leq 4$.

Bemerkungen:

- Es existiert momentan kein Beweis des Vierfarbensatzes der ohne Rechnerunterstützung auskommt.
- Der Vierfarbensatz besagt, dass jede Landkarte mit höchstens 4 Farben so gefärbt werden kann, dass keine zwei aneinander grenzenden Länder die gleiche Farbe erhalten.
- Es gibt planare Graphen G mit $\chi(G) > 3$ (und damit $\chi(G) = 4$). Das Problem, festzustellen, ob ein gegebener planarer Graph mit 3 Farben gefärbt werden kann, ist jedoch relativ schwierig (NP-vollständig, siehe Mastervorlesung Komplexitätstheorie).

Wir werden hier die folgende Abschwächung des Vierfarbensatzes zeigen:

Fünffarbensatz

Für jeden endlichen planaren Graphen G gilt $\chi(G) \leq 5$.

Beweis: Sei $G = (V, E)$ planar.

Induktion über $|V|$.

Der Fall $|V| \leq 5$ ist klar. Sei nun $|V| \geq 6$.

Korollar 1 aus Eulers Formel $\rightsquigarrow$ es gibt $x \in V$ mit $d_G(x) \leq 5$.

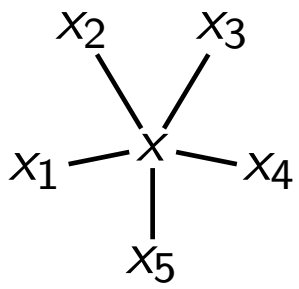
Induktionsannahme $\rightsquigarrow$ $G \setminus x$ hat eine 5-Färbung
$c : V \setminus \{x\} \to \{1, 2, 3, 4, 5\}$.

Sei $C = \{c(y) \mid \{x, y\} \in E\}$ die Menge der Farben der Nachbarn von x.

1.Fall: $|C| \leq 4$. $\rightsquigarrow$ färbe x mit einer Farbe aus $\{1, 2, 3, 4, 5\} \setminus C$.

2.Fall: $|C| = 5$. Insbesondere hat x genau 5 Nachbarn.

Sei x_1, x_2, x_3, x_4, x_5 eine Liste der Nachbarn von x im Uhrzeigersinn:



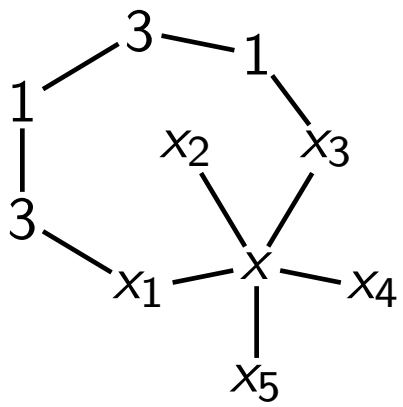
O.B.d.A. gelte $c(x_i) = i$.

Definition: Ein $(1,3)$-Weg zwischen x_1 und x_3 ist ein Weg $[y_1, y_2, \ldots, y_{2n}]$ in $G \setminus x$ $(n \geq 1)$ mit:

- $y_1 = x_1$, $y_{2n} = x_3$, d.h. x_1 und x_3 sind die Endpunkte des Weges.
- $c(y_{2i-1}) = 1$, $c(y_{2i}) = 3$ für alle $1 \leq i \leq n$, d.h. die Farbe entlang des Weges alterniert zwischen 1 und 3.

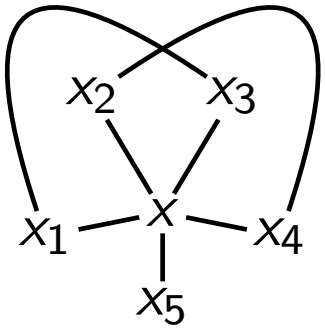
Analog definieren wir den Begriff eines $(2,4)$-Weges in $G \setminus x$ zwischen x_2 und x_4.

Ein $(1,3)$-Weg zwischen x_1 und x_3:



Behauptung: Es kann nicht gleichzeitig ein $(1,3)$-Weg zwischen x_1 und x_3 sowie ein $(2,4)$-Weg zwischen x_2 und x_4 existieren.

Denn wäre dies der Fall, so müssten sich die beiden Wege auf Grund der Planarität von G in einem Knoten schneiden, was aber nicht möglich ist:



O.B.d.A. existiere kein $(1,3)$-Weg zwischen x_1 und x_3.

Wir ändern nun die Färbung c von $G \setminus x$ mit folgenden Algorithmus ab:

$U := \{x_1\}$; $f := 1$;
while $U \neq \emptyset$ **do**
  if $f = 1$ then
    $f := 3$
  else (wir haben dann $f = 3$)
    $f := 1$
  endif
  for all $y \in U$ **do** $c(y) := f$
  $U := \{z \in V \setminus \{x\} \mid c(z) = f, \exists y \in U : \{y,z\} \in E\}$
endwhile

Dieser Algorithmus produziert wieder eine korrekte 5-Färbung c von $G \setminus x$ mit $c(x_1) = 3$.

Da es ausserdem keinen $(1,3)$-Weg von x_1 nach x_3 gibt, wird die Farbe von x_3 durch den obigen Algorithmus nicht verändert, d.h. es gilt weiterhin $c(x_3) = 3$.

Wir können nun c durch $c(x) := 1$ zu einer 5-Färbung des gesamten Graphen G erweitern. □

Definition (Matching)

Sei $G = (V, E)$ ein Graph. Ein Matching (oder eine Paarung) von G ist eine Teilmenge $M \subseteq E$, so dass gilt:

$$\forall e, e' \in M : e \neq e' \Rightarrow e \cap e' = \emptyset$$

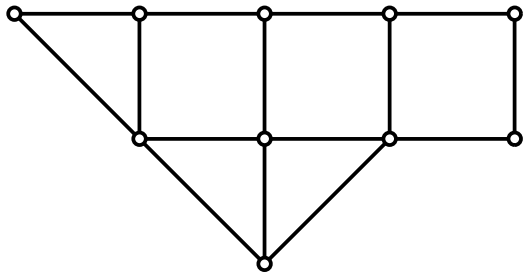
Ist G endlich, so ist ein größtes Matching von G iein Matching M, so dass für alle Matchings M' von G gilt: $|M'| \leq |M|$.

Die Matchingzahl $\mu(G)$ von G ist die Anzahl der Kanten in einem größten Matching von G.

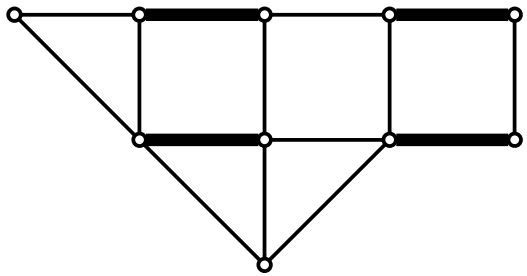
Ein perfektes Matching von G ist ein Matching M, so dass für alle $x \in V$ eine Kante $e \in M$ mit $x \in e$ existiert (d. h. alle Knoten werden von M berührt).

Beachte: Ein endlicher Graph $G = (V, E)$ kann nur dann ein perfektes Matching haben, wenn $|V|$ gerade ist. Ein perfektes Matching ist stets ein

Beispiel:



Beispiel: ein Matching, welches jedoch nicht perfekt ist.



Definition (alternierende Wege)

Sei $G = (V, E)$ ein endlicher Graph und $M \subseteq E$ ein Matching von G.

Ein Knoten $x \in V$ ist M-saturiert, wenn eine Kante $e \in M$ mit $x \in e$ exisitert.

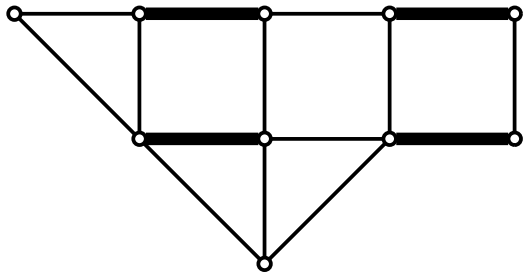
Ein M-alternierender Weg ist ein einfacher Weg $[v_1, v_2, \ldots, v_n]$ in G, so dass für alle $1 \leq i \leq n-2$ gilt:

$$\{v_i, v_{i+1}\} \in M \iff \{v_{i+1}, v_{i+2}\} \notin M.$$

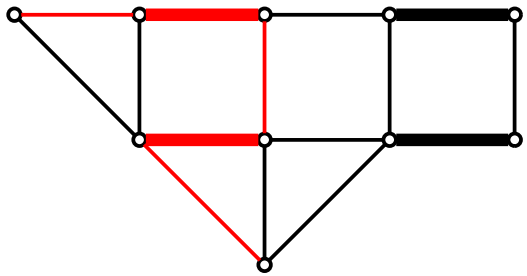
Ein M-alternierender Weg $[v_1, v_2, \ldots, v_n]$ ist M-erweiternd, wenn v_1 und v_n beide nicht M-saturiert sind.

Beachte: Für einen M-erweiternden Weg $[v_1, v_2, \ldots, v_n]$ muss n gerade sein.

Beispiel: ein Matching M



Beispiel: ein M-erweiternder Weg.



Satz 29 (Berge, 1957)

Sei G ein endlicher Graph und sei M ein Matching von G.

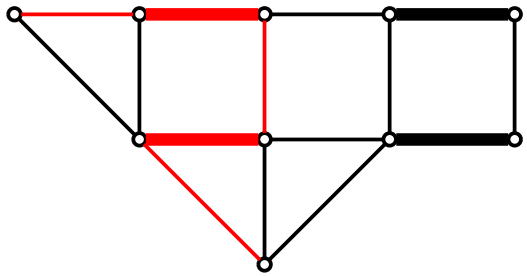
M ist ein größtes Matching von G genau dann, wenn es keinen M-erweiternden Weg gibt.

Satz 29 (Berge, 1957)

Sei G ein endlicher Graph und sei M ein Matching von G.

M ist ein größtes Matching von G genau dann, wenn es keinen M-erweiternden Weg gibt.

Beispiel: ein M-erweiternder Weg.

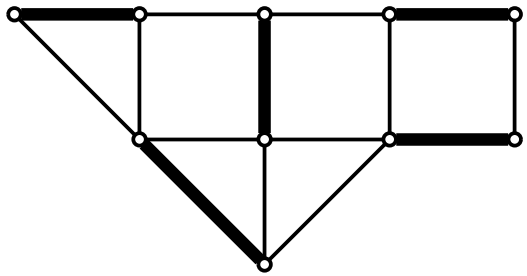


Satz 29 (Berge, 1957)

Sei G ein endlicher Graph und sei M ein Matching von G.

M ist ein größtes Matching von G genau dann, wenn es keinen M-erweiternden Weg gibt.

Beispiel: ein größeres Matching.



Beweis des Satzes von Berge:

"$\Rightarrow$": Sei M ein größtes Matching von $G = (V, E)$.

Angenommen es gibt einen M-erweiternden Weg $[v_1, v_2, \ldots, v_{2m}]$.

Sei $e_i = \{v_i, v_{i+1}\}$ für $1 \leq i \leq 2m - 1$.

$\rightsquigarrow$ $e_1, e_3, \ldots, e_{2m-1} \notin M$ und $e_2, e_4, \ldots, e_{2m-2} \in M$.

Sei $M' = (M \setminus \{e_2, e_4, \ldots, e_{2m-2}\}) \cup \{e_1, e_3, \ldots, e_{2m-1}\}$.

$\rightsquigarrow$ M' ist ein Matching von G mit $|M'| > |M|$, Widerspruch.

"$\Leftarrow$": Angenommen es gibt keinen M-erweiternden Weg.

Angenommen es gibt ein Matching M' von G mit $|M'| > |M|$.

Definiere den Graphen $H = (V,\ (M \setminus M') \cup (M' \setminus M))$.

$\rightsquigarrow$ $\forall x \in V : d_H(x) \leq 2$.

$\rightsquigarrow$ Jede Zusammenhangskomponente ist ein K_1, ein P_n oder ein C_n.

Falls eine Zusammenhangskomponente von H ein Kreis C_n ist, muss n gerade sein, da sich Kanten aus M und M' entlang von C_n abwechseln müssen.

Also gibt es in C_n genauso viele Kanten aus M wie M'.

Wegen $|M'| > |M|$ muss mindestens eine Zusammenhangskomponente H' von H ein Pfad P_n sein, der mit einer Kante aus M' beginnt und endet.

Sei $[x_1, x_2, \ldots, x_n]$ der zu dieser Zusammenhangskomponente gehörende einfache Weg.

$\rightsquigarrow$ $[x_1, x_2, \ldots, x_n]$ ist M-alternierend.

Ausserdem sind x_1 und x_n nicht M-saturiert:

Wäre etwa $\{x_1, y\} \in M$, dann folgt $y \neq x_2$ wegen $\{x_1, x_2\} \notin M$.

Dann würde aber y zur Zusammenhangskomponente H' gehören, Widerspruch!

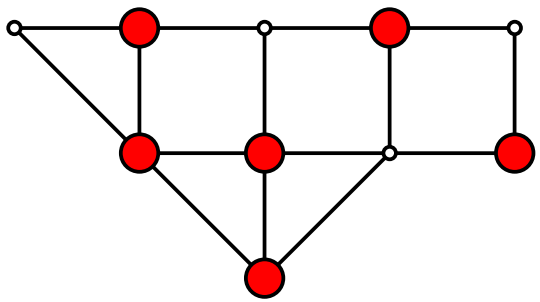
Definition (Knotenüberdeckung)

Sei $G = (V, E)$ ein Graph. Eine Knotenüberdeckung (engl. vertex cover) von G ist eine Teilmenge $C \subseteq V$, so dass gilt:

$$\forall e \in E : e \cap C \neq \emptyset.$$

Die Knotenüberdeckungszahl $\gamma(G)$ von G ist die Anzahl der Knoten in einer kleinsten Knotenüberdeckung von G.

Beispiel: eine Knotenüberdeckung.



Lemma 2

Sei G ein Graph. Dann gilt $\mu(G) \leq \gamma(G)$.

Beweis:

G hat eine Matching M bestehend aus $\mu(G)$ vielen Kanten.

Jede Knotenüberdeckung C von G muss aus jeder Kante in M einen der beiden Endpunkte enthalten.

$\rightsquigarrow \quad |C| \geq |M| = \mu(G)$ □

Bemerkung: Im Allgemeinen gilt $\mu(G) < \gamma(G)$.
Z. B. gilt $\mu(K_3) = 1$ und $\gamma(K_3) = 2$.

Satz 30 (König, 1931)

Sei G ein bipartiter Graph. Dann gilt $\mu(G) = \gamma(G)$.

Beweis:

Sei $G = (A \cup B, E)$ bipartit, $A \cap B = \emptyset$, $E \subseteq \{\{a, b\} \mid a \in A, b \in B\}$.

Wegen Lemma 2 genügt es zu zeigen: $\mu(G) \geq \gamma(G)$

Sei hierzu M ein größtes Matching von G.

Wir konstruieren eine Knotenüberdeckung C mit $|C| = |M| = \mu(G)$.

Hierzu kommt für jede Kante $\{a, b\} \in M$ ($a \in A$, $b \in B$) nach folgender Regel genau ein Knoten nach C:

- Falls in b ein M-alternierender Weg $[a', \ldots, b]$ endet, dessen Anfangsknoten $a' \in A$ nicht M-saturiert ist: b kommt nach C.
- Ansonsten kommt a nach C.

Behauptung: C ist eine Knotenüberdeckung von G.

Sei $\{a, b\} \in E$ eine beliebige Kanten von G. Wir zeigen: $C \cap \{a, b\} \neq \emptyset$.

Fall 1: $\{a, b\} \in M$.

Dann gilt $a \in C$ oder $b \in C$ nach Konstruktion von C.

Fall 2: $\{a, b\} \notin M$.

Da M ein größtes Matching von G ist, ist a oder b M-saturiert (sonst könnten wir die Kante $\{a, b\}$ noch zum Matching hinzunehmen).

Fall 2.1: a ist nicht M-saturiert und b ist M-saturiert.

Dann ist $[a, b]$ ein M-alternierender Weg, der in einem nicht M-saturierten Knoten beginnt.

Da b zu einer Kante aus M gehört, gilt $b \in C$ nach Konstruktion von C.

Fall 2.2: a ist M-saturiert; sei etwa $\{a, b'\} \in M$.

Es gilt entweder $a \in C$ oder $b' \in C$.

Wenn $a \in C$ gilt, sind wir fertig; gelte also $b' \in C$.

Nach Konstruktion von C endet in b' ein M-alternierender Weg $P = [a', \ldots, b']$, dessen Anfangsknoten a' nicht M-saturiert ist.

Aus dem Weg $Pab = [a', \ldots, b', a, b]$ können wir dann einen M-alternierenden Weg $P' = [a', \ldots, b]$ durch Entfernen von eventuellen Zyklen konstruieren.

Wäre b nicht M-saturiert, so wäre P' ein M-erweiternder Weg.

Nach dem Satz von Berge wäre dann M kein größtes Matching, Widerspruch!.

Also ist b M-saturiert.

Dann gilt $b \in C$ nach Konstruktion von C. □

Satz 31 (Heiratssatz von Hall, 1935)

Sei $G = (A \cup B, E)$ ein endlicher bipartiter Graph. Folgende beiden Eigenschaften sind äquivalent:

(1) *Es gibt ein Matching M von G, so dass jeder Knoten in A M-saturiert ist.*

(2) $\forall C \subseteq A : |N_G(C)| \geq |C|$

Beweis:

(1) $\Rightarrow$ (2): Sei M ein Matching von G, so dass jeder Knoten in A M-saturiert ist, und sei $C \subseteq A$.

Dann besteht die Menge $\{b \in B \mid \exists a \in C : \{a, b\} \in M\}$ aus genau $|C|$ vielen Knoten.

$\rightsquigarrow \quad |N_G(C)| \geq |C|$

(2) $\Rightarrow$ (1): Angenommen es gibt kein Matching von G, so dass jeder Knoten in A M-saturiert ist.

$\rightsquigarrow$ $\mu(G) < |A|$.

Satz von König $\rightsquigarrow$ $\gamma(G) < |A|$.

Sei $C \subseteq A \cup B$ eine Knotenüberdeckung von G mit $|C| < |A|$.

Sei $C = A' \cup B'$ mit $A' \subseteq A$ und $B' \subseteq B$.

$\rightsquigarrow$ $|A'| + |B'| = |C| < |A|$, d. h. $|B'| < |A| - |A'| = |A \setminus A'|$

Da $C = A' \cup B'$ eine Knotenüberdeckung ist, kann es keine Kanten in G zwischen $A \setminus A'$ und $B \setminus B'$ geben.

$\rightsquigarrow$ $N_G(A \setminus A') \subseteq B'$, d. h. $|N_G(A \setminus A')| \leq |B'|$

$\rightsquigarrow$ $|N_G(A \setminus A')| < |A \setminus A'|$. $\square$

Definition

Sei $G = (V, E)$ ein endlicher Graph.

- Ein Eulerpfad in G ist ein Weg $[x_1, x_2, \ldots, x_n]$ in G, so dass für jede Kante $e \in E$ genau ein $i \in \{1, \ldots, n-1\}$ mit $e = \{x_i, x_{i+1}\}$ existiert.

  Jede Kante wird also genau einmal besucht.

- Ein Eulerkreis in G ist ein Eulerpfad $[x_1, x_2, \ldots, x_n]$ mit $x_1 = x_n$.

- Ein Hamiltonpfad in G ist ein Weg $[x_1, x_2, \ldots, x_n]$ in G, so dass für jeden Knoten $x \in V$ genau ein $i \in \{1, \ldots, n\}$ mit $x = x_i$ existiert.

  Jeder Knoten wird also genau einmal besucht.

- Ein Hamiltonkreis in G ist ein Hamiltonpfad $[x_1, x_2, \ldots, x_n]$ mit $\{x_n, x_1\} \in E$.

Satz 32 (Euler, 1736)

Sei G ein endlicher Graph ohne Knoten von Grad 0. Sei d_u die Anzahl der Knoten mit ungeraden Grad.

(1) *G hat einen Eulerpfad genau dann, wenn G zusammenhängend ist und $d_u \in \{0, 2\}$.*

(2) *G hat einen Eulerkreis genau dann, wenn G zusammenhängend ist und $d_u = 0$.*

Beweis:

"$\Rightarrow$": Angenommen G hat einen Eulerpfad $P = [x_1, x_2, \ldots, x_n]$.

Da jeder Knoten Grad mindestens 1 hat, muss G zusammenhängend sein.

Sei zunächst $x_1 \neq x_n$, d. h. P ist kein Eulerkreis.

Man kann dann den Grad eines Knoten $x \in V$ zählen, indem man P abläuft:

$$d_G(x) = \begin{cases} 2 \cdot |\{i \mid 2 \leq i \leq n-1, x_i = x\}| & \text{falls } x_1 \neq x \neq x_n \\ 2 \cdot |\{i \mid 2 \leq i \leq n-1, x_i = x\}| + 1 & \text{falls } x = x_1 \text{ oder } x = x_n \end{cases}$$

Also hat jeder Knoten in $V \setminus \{x_1, x_n\}$ geraden Grad, und x_1 und x_n haben ungeraden Grad, d. h. es gilt $d_u = 2$.

Gilt hingegen $x_1 = x_n$ (d. h. P ist ein Eulerkreis), so haben auch x_1 und x_n geraden Grad, d. h. es gilt $d_u = 0$.

"$\Leftarrow$": Sei G zusammenhängend und gelte $d_u = 0$ oder $d_u = 2$.

Betrachte zunächst den Fall $d_u = 0$.

Wir zeigen, dass G einen Eulerkreis hat.

Sei $P = [x_1, x_2, \ldots, x_n]$ ein längster Weg in G, der keine Kante zweimal durchläuft.

Da jeder Knoten geraden Grad hat, kann P nicht mit einem Knoten aus $V \setminus \{x_1\}$ enden.

Also gilt $x_n = x_1$.

Angenommen es gibt eine Kante $e \in E$, die in P nicht durchlaufen wird.

Da G zusammenhängend ist, gibt es dann auch eine solche Kante $e = \{x, y\}$ mit $x \in \{x_1, \ldots, x_n\}$, die in P nicht durchlaufen wird.

Sei etwa $x = x_i$. Dann ist $[y, x_i, x_{i+1}, \ldots, x_n, x_2, \ldots, x_i]$ ein Weg, der keine Kante zweimal durchläuft und länger als P ist, Widerspruch!

Also besucht P jede Kante aus G und ist somit ein Eulerkreis.

Der Fall $d_u = 2$ kann ähnlich behandelt werden (Übung). □

Graphentheorie: Euler- und Hamiltonpfade

Es gibt keine so einfach Charakterisierung von Graphen mit Hamiltonpfaden (Hamiltonkreisen) wie im Satz von Euler.

Dies hat einen tieferen Grund: Die Frage, ob ein gegebener Graph einen Hamiltonpfad (Hamiltonkreis) hat, ist NP-vollständig (siehe Mastervorlesung Komplexitätstheorie), und ist damit wohl recht schwierig zu lösen.

Es gibt jedoch eine Reihe von hinreichenden Kriterien für die Existenz von Hamiltonkreisen, z. B.:

Satz 33 (Ore, 1960)

Sei $G = (V, E)$ ein endlicher zusammenhängender Graph mit $n = |V|$ Knoten, so dass für alle Knoten $x, y \in V$ gilt:

$$(\{x, y\} \notin E \text{ und } x \neq y) \quad \Longrightarrow \quad d_G(x) + d_G(y) \geq n.$$

Dann hat G einen Hamiltonkreis.

Beweis: Angenommen, die Aussage im Satz von Ore wäre falsch.

Sei der Graph $G = (V, E)$ ein Gegenbeispiel zum Satz von Ore, d. h.:

1. $\forall x, y \in V : (\{x, y\} \notin E \text{ und } x \neq y) \implies d_G(x) + d_G(y) \geq n = |V|$
2. G hat keinen Hamiltonkreis.

Wir können davon ausgehen, dass G einen Hamiltonkreis hat, falls wir eine beliebige Kante zu G hinzufügen, denn:

- fügt man Kanten zu G hinzu, so bleibt Bedingung (1) weiterhin wahr
- und spätestens K_n hat einen Hamiltonkreis.

Da G kein K_n ist, existieren $x, y \in V$ mit $x \neq y$ und $\{x, y\} \notin E$.

Dann hat $G' = (V, E \cup \{\{x, y\}\})$ einen Hamiltonkreis, und dieser muss die Kante $\{x, y\}$ durchlaufen (sonst hätte bereits G einen Hamiltonkreis).

Also gibt es in G einen Hamiltonpfad $[x = v_1, v_2 \ldots, v_n = y]$ von x nach y.

Sei $A = N_G(x)$ und $B = \{v_i \mid 2 \leq i \leq n, v_{i-1} \in N_G(y)\}$.

Wegen $v_n = y \notin N_G(y)$, gilt $|B| = |N_G(y)| = d_G(y)$.

$\rightsquigarrow$ $|A| + |B| = d_G(x) + d_G(y) \geq n$, da $\{x, y\} \notin E$ und $x \neq y$.

Aber $v_1 = x \notin A \cup B$, d. h. $|A \cup B| \leq n - 1$.

$\rightsquigarrow$ $A \cap B \neq \emptyset$, sei $v_i \in A \cap B$.

Wegen $v_i \in B$ gilt $i \geq 2$ und $\{v_{i-1}, y\} \in E$

Dann hat aber G (entgegen unserer Annahme) doch einen Hamiltonkreis:

$$[x = v_1, v_2, \ldots, v_{i-1}, y = v_n, v_{n-1}, \ldots, v_i]$$

Beachte hierbei: $\{v_i, x\} \in E$ wegen $v_i \in A$. □

Graphentheorie: Beweis des Satzes von Cantor, Schröder und Bernstein (Satz 1)

Erinnerung: Der Satz von Cantor, Schröder und Bernstein besagt: Wenn für Mengen A und B injektive Abbildungen $f : A \to B$ und $g : B \to A$ existieren, dann existiert auch eine bijektive Abbildung $h : A \to B$.

Beweis: Seien $f : A \to B$ und $g : B \to A$ injektiv, o.B.d.A. $A \cap B \neq \emptyset$.

Wir definieren einen unendlichen bipartiten Graphen $G = (V, E)$ wie folgt:

- $V = A \cup B$
- $E = \{\{a, f(a)\} \mid a \in A\} \cup \{\{b, g(b)\} \mid b \in B\}$

Dann hat jeder Knoten in G Grad 1 oder 2.

Graphentheorie: Beweis des Satzes von Cantor, Schröder und Bernstein (Satz 1)

Um eine Bijektion $h : A \to B$ zu konstruieren, genügt es, für jede Zusammenhangskomponente $H = G[U]$ von G eine Bijektion $h_U : U \cap A \to U \cap B$ zu konstruieren.

Sei $H = G[U]$ eine Zusammenhangskomponente von G.

Fall 1: U enthält einen Knoten $a_1 \in A \setminus g(B)$.

Dann gilt $U = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots\}$ mit $f(a_i) = b_i$ und $g(b_i) = a_{i+1}$ für alle $i \geq 1$.

Dann gilt $a_i \neq a_j$ und $b_i \neq b_j$ für $i \neq j$, d.h. alle Knoten in der Liste $a_1, b_1, a_2, b_2, a_3, b_3, \ldots$ sind paarweise verschieden.

Dann definiert $h_U(a_i) = b_i$ eine Bijektion von $U \cap A$ nach $U \cap B$.

Graphentheorie: Beweis des Satzes von Cantor, Schröder und Bernstein (Satz 1)

Fall 2: U enthält einen Knoten $b_1 \in B \setminus f(A)$.

Dann gilt $U = \{b_1, a_1, b_2, a_2, b_3, a_3, \ldots\}$ mit $g(b_i) = a_i$ und $f(a_i) = b_{i+1}$.

Dann gilt wieder $a_i \neq a_j$ und $b_i \neq b_j$ für $i \neq j$, d.h. alle Knoten in der Liste $b_1, a_1, b_2, a_2, b_3, a_3, \ldots$ sind paarweise verschieden.

Dann definiert $h_U(a_i) = b_i$ eine Bijektion von $U \cap A$ nach $U \cap B$.

Fall 4: $U \cap A \subseteq g(B)$ und $U \cap B \subseteq f(A)$ gilt.

Dann ist aber die Abbildung $h_U : U \cap A \to U \cap B$ mit $h_U(a) = f(a)$ für $a \in U \cap A$ eine Bijektion:

- Da f injektiv ist, ist auch h_U injektiv.
- Sei $b \in U \cap B$. Wegen $U \cap B \subseteq f(A)$ existiert ein $a \in A$ mit $f(a) = b$. Da a in der gleichen Zusammenhangskomponente wie b liegt, muss $a \in U \cap A$ gelte.

Grundidee: Finde geordnete Teilstrukturen in beliebigen Strukturen.

Im Folgenden bezeichnet $[n]$ das Interval $\{1, \ldots, n\}$ und $\binom{[n]}{2}$ die Menge aller 2-elementigen Teilmengen von $[n]$.

Sei $c : \binom{[n]}{2} \to [r]$ eine Färbung aller 2-elementigen Teilmengen von $[n]$ mit r vielen Farben.

Eine Teilmenge $A \subseteq [n]$ heißt c-monocromatisch, falls eine Farbe $i \in [r]$ gibt mit

$$\forall x, y \in A : x \neq y \implies c(\{x, y\}) = i.$$

Ramseys Theorem, 1930

Für alle $r \geq 1, k \geq 2$ existiert eine Zahl R mit folgender Eigenschaft:

Für jede Färbung $c : \binom{[R]}{2} \to [r]$ existiert eine c-monocromatische Teilmenge $A \subseteq [R]$ mit $|A| \geq k$.

Mit $R(r, k)$ bezeichnen wir die kleinste Zahl mit dieser Eigenschaft.

Ramseys Theorem kann als eine 2-dimensionale Verallgemeinerung des klassischen Schubfachprinzips angesehen werden.

Schubfachprinzip

Für alle $r \geq 1, k \geq 2$ existiert eine Zahl S mit folgender Eigenschaft:

Für jede Färbung $c : [S] \to [r]$ existiert Farbe $i \in [r]$ und eine Teilmenge $A \subseteq [S]$ mit (i) $|A| \geq k$ und (ii) $\forall a \in A : c(a) = i$.

Wir können natürlich $S = r \cdot k$ wählen.

Etwas umgangssprachlicher: Färbt man $r \cdot k$ viele Objekte mit r Farben (jedes Objekt bekommt genau eine Farbe), so muss eine Farbe mindestens k mal vorkommen.

Korollar aus Ramseys Theorem

Sei G ein Graph mit mindestens $R(2, m)$ vielen Knoten. Dann gibt es in G oder im Komplementgraphen $\overline{G}$ einen K_m.

Beispiel ($m = 3$): In jedem Graph $G = (V, E)$ mit 6 Knoten gibt es entweder in G oder in $\overline{G}$ einen K_3:

Begründung: Sei $V = \{1, 2, 3, 4, 5, 6\}$.

Für Knoten 1 gilt $d_G(1) + d_{\overline{G}}(1) = 5$.

Also gilt entweder $d_G(1) \geq 3$ oder $d_{\overline{G}}(1) \geq 3$.

Sei etwa ersteres der Fall, und gelte etwa $\{1, 2\}, \{1, 3\}, \{1, 4\} \in E$.

Falls es eine Kante zwischen den 3 Knoten $2, 3, 4$ gibt, haben wir einen K_3 in G gefunden.

Falls es keine Kante zwischen den 3 Knoten $2, 3, 4$ gibt, haben wir einen K_3 in $\overline{G}$ gefunden.

Für Graphen mit nur 5 Knoten gilt diese Konklusion nicht mehr notwendigerweie:

Es gilt also $R(2,3) = 6$.

Intuitiv: Auf jeder Party mit mindestens 6 Leuten gibt es immer 3 Leute, die sich gegenseitig kennen, oder es gibt 3 Leute, die sich nicht kennen.

Bemerkung: Im Satz von Ramsey können wir natürlich die Menge $[R]$ durch eine beliebige Menge mit R Elementen ersetzen. Dies haben wir im obigen Beispiel bereits getan, und wir werden es auch im folgenden Beweis tun.

Beweis des Satzes von Ramsey:

Durch Induktion über die Zahlen $r, k_1, \ldots, k_r$ zeigen wir die folgende allgemeinere Aussage:

Für alle $r \geq 1, k_1, \ldots, k_r \geq 2$ existiert eine Zahl $R_*(r, k_1, \ldots, k_r)$ mit:
Für jede Färbung $c : \binom{[R_*(r,k_1,\ldots,k_r)]}{2} \to [r]$ existiert eine Farbe $i \in [r]$ und eine Teilmenge $A \subseteq [R_*(r, k_1, \ldots, k_r)]$ mit:

- $\forall x, y \in A : x \neq y \implies c(\{x, y\}) = i$
- $|A| \geq k_i$

Fall 1: $r = 1$. Wähle $R_*(1, k_1) = k_1$.

Fall 2: $r \geq 2$ und es gibt ein i mit $k_i = 2$, sei o.B.d.A. $i = 1$.

Nach Induktion existiert $R_*(r - 1, k_2, \ldots, k_r)$ und wir können

$$R_*(r, 2, k_2 \ldots, k_r) = R_*(r - 1, k_2, \ldots, k_r)$$

setzen (warum?).

Fall 3: $r \geq 2$ und $k_i > 2$ für alle i.

Nach Induktion existieren die Zahlen

$$K_i = R_*(r, k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r).$$

Definiere dann $R = 1 + \sum_{i=1}^{r} K_i$.

Sei nun $c : \binom{[R]}{2} \to [r]$ eine beliebige Färbung. Wir zeigen, dass eine Farbe i und eine Teilmenge $A \subseteq [R]$ mit $|A| \geq k_i$ existiert, deren 2-elementige Teilmengen alle mit i gefärbt sind.

Definiere eine Färbung c' der Elemente aus $[R-1] = [\sum_{i=1}^{r} K_i]$ wie folgt:

$$\forall x \in [R-1] : c'(x) = c(\{x, R\}).$$

Nach dem Schubfachprinzip muss es eine Farbe i und eine Teilmenge $B \subseteq [R-1]$ geben mit:

- $\forall x \in B : c'(x) = i \quad (\rightsquigarrow \quad \forall x \in B : c(\{x, R\}) = i)$
- $|B| \geq K_i = R_*(r, k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r)$

Wir betrachten nun die Färbung $c : \binom{[R]}{2} \to [r]$, eingeschränkt auf die Menge B.

Nach Definition von $R_*(r, k_1, \ldots, k_{i-1}, k_i - 1, k_{i+1}, \ldots, k_r)$ muss einer der beiden folgenden Fälle existieren.

Fall 3.1: Es gibt eine Farbe $j \neq i$ und eine Teilmenge $C \subseteq B$ mit $|C| \geq k_j$, so dass alle 2-elementigen Teilmengen von C durch c mit der Farbe j gefärbt werden.

Dann sind wir fertig.

Fall 3.2: Es gibt eine Teilmenge $C \subseteq B$ mit $|C| \geq k_i - 1$, so dass alle 2-elementigen Teilmengen von C durch c mit der Farbe i gefärbt werden.

Dann werden alle 2-elementigen Teilmengen von $C \cup \{R\}$ durch c mit der Farbe i gefärbt.

Ausserdem gilt $|C \cup \{R\}| \geq k_i$. □

Ramseytheorie

Wir hatten uns überzeugt, dass $R(2,3) = 6$ gilt (für jeden Graphen G mit mindestens 6 Knoten enthält entweder G oder $\overline{G}$ einen K_3).

Weiterhin ist $R(2,4) = 18$ bekannt, aber bereits $R(2,5)$ ist nicht bekannt.

Im Allgemeinen ist jedoch das Wissen über die genauen Werte der Ramseyzahlen $R(r,k)$ sehr beschränkt.

Die besten allgemeinen Schranken für den Fall $r = 2$ (2 Farben) sind:

- $R(2,m) \leq \frac{2^{2m}}{m}$ (Thomason 1988)
- $R(2,m) \geq 2^{m/2}$ (Erdös 1961)

Ramseytheorie

Ein weiteres berühmtes Resultat aus der Ramseytheorie behandelt arithmetische Progressionen.

Eine arithmetische Progression ist eine endliche Teilmenge $A \subseteq \mathbb{N}$, so dass drei Zahlen $b, k, p \in \mathbb{N}$ existieren mit:

$$A = \{b + x \cdot p \mid 0 \leq x \leq k\}$$

Der Abstand zwischen aufeinanderfolgenden Zahlen in A ist also stets gleich (hier p).

Van der Wardens Theorem, 1927

Für alle $r \geq 1, k \geq 2$ existiert eine Zahl W mit folgender Eigenschaft:

Für jede Färbung $c : [W] \to [r]$ existiert eine Farbe $i \in [r]$ und eine arithmetische Progession $A \subseteq [W]$ mit $|A| \geq k$ und $\forall a \in A : c(a) = i$.

Mit $W(r, k)$ wird die kleinste Zahl mit dieser Eigenschaft bezeichnet.

Ramseytheorie

Die Bestimmung von möglichst genauen unteren und oberen Schranken für die Zahlen $W(r,k)$ ist ein berühmtes Problem der Kombinatorik (und noch schwieriger als für die Ramseyzahlen $R(r,k)$).

Der aktuelle Kenntnisstand ist:

- $W(2,p) \geq (p-1)2^{p-1}$ falls p eine Primzahl ist (Berlekamp 1968)
- $W(r,k) \leq 2^{2^{r^{2^{2^{k+9}}}}}$ (Gowers 2001)

Definition (Operationen auf einer Menge)

Sei A eine Menge und $n \geq 1$. Eine *n*-stellige Operation auf der Menge A ist eine Abbilding

$$f : A^n \to A.$$

Besonders wichtig im Folgenden sind 2-stellige Operationen auf der Menge A, d.h. Abbildungen $f : A \times A \to A$.

Beispiel: $+$ können wir als eine 2-stellige Operation auf der Menge $\mathbb{N}$ (oder $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) betrachten.

Wir schreiben natürlich anstatt $+(a, b)$ immer $a + b$.

Definition (Monoid, Gruppe)

Ein Monoid ist ein Paar $(A, \circ)$, wobei gilt:

- A ist eine beliebige Menge.
- $\circ : A \times A \to A$ ist eine 2-stellige Operation auf A; anstatt $\circ(a, b)$ schreiben wir $a \circ b$.
- $\circ$ ist assoziativ, d. h. $\forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c)$.
- Es existiert ein neutrales Element e bzgl. $\circ$, d. h. $\exists e \in A \; \forall a \in A : a \circ e = e \circ a = a$.

Ein Monoid $(A, \circ)$ ist eine Gruppe, falls für jedes $a \in A$ ein Inverses existiert: $\forall a \in A \; \exists b \in A : a \circ b = b \circ a = e$ (wobei e neutral ist).

Aufgrund der Assoziativität von $\circ$ können wir auf Klammern verzichten, $a_1 \circ a_2 \circ \cdots \circ a_n$ ist wohldefiniert; manchmal schreiben wir hierfür auch einfach $a_1 a_2 \cdots a_n$.

Das neutrale Element eines Monoids wird auch häufig mit 1 bezeichnet.

Algebraische Strukturen: Monoide und Gruppen

Einfache Beobachtungen: Sei $\mathbb{M} = (A, \circ)$ ein Monoid.

- Das neutrale Element ist eindeutig bestimmt: Sind 1 und $1'$ neutral, so folgt $1 = 1 \circ 1' = 1'$.
- Ist $\mathbb{M}$ eine Gruppe, so existiert zu jedem Element $a \in A$ genau ein inverses Element: Seien b und c invers zu a. Dann gilt

$$b = b \circ 1 = b \circ (a \circ c) = (b \circ a) \circ c = 1 \circ c = c.$$

  Wir können daher das zu a inverse Element mit a^{-1} bezeichnen.
  Es gilt dann $(a^{-1})^{-1} = a$ und $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ für alle $a, b \in A$.

Anstatt $\underbrace{a \circ a \circ \cdots \circ a}_{n\text{-mal}}$ schreiben wir auch a^n, wobei $a^0 = 1$.

Ist $\mathbb{M}$ eine Gruppe, so schreiben wir anstatt $\underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n\text{-mal}}$ auch a^{-n}.

Beachte: Es gilt $a^m a^n = a^{m+n}$ für alle $m, n \in \mathbb{Z}$.

Definition (Kommutative Monoide und Gruppen)

Ein Monoid (eine Gruppe) $(A, \circ)$ ist kommutativ, falls für alle $a, b \in A$ gilt: $a \circ b = b \circ a$.

Kommutative Gruppen nennt man auch Abelsche Gruppen.

Definition (zykliche Gruppen)

Eine Gruppe $(G, \circ)$ ist zyklisch, falls ein $g \in G$ existiert mit $G = \{g^n \mid n \in \mathbb{Z}\}$.

Das Element g bezeichnen wir dann auch als einen Erzeuger von G.

Offensichtlich ist jede zyklische Gruppe kommutativ, denn es gilt

$$g^m \circ g^n = g^{m+n} = g^{n+m} = g^n \circ g^m.$$

Beispiele 1: (Rechnen mit Zahlen)

$(\mathbb{R}, \cdot)$ und $(\mathbb{Q}, \cdot)$ sind kommutative Monoide.

$(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind Abelsche Gruppen.

$(\mathbb{Z}, +)$ ist eine zyklische Gruppe.

Die einzigen beiden Erzeuger von $\mathbb{Z}$ sind -1 und 1.

Vorsicht: Wir haben in unseren allgemeinen Definitionen Gruppen multiplikativ geschrieben: Die Gruppenoperation war $\circ$ und

$$a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n\text{-mal}}$$

In der Gruppe $(\mathbb{Z}, +)$ ist die Operation $+$.

Hier schreiben wir $n \cdot a$ anstatt a^n.

Beispiele 2: (Rechnen mit Matrizen)

Für $n \geq 1$ sei:

$$\begin{aligned} \mathrm{M}_n(\mathbb{R}) &= \mathbb{R}^{n \times n} \quad \text{(Menge der } (n \times n)\text{-Matrizen über } \mathbb{R}) \\ \mathrm{GL}_n(\mathbb{R}) &= \{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0\} \end{aligned}$$

Wir betrachten die Matrixmultiplikation $\cdot$ als Operation auf diesen Mengen.

Dann gilt für alle $n \geq 2$:

- $(\mathrm{M}_n(\mathbb{R}), \cdot)$ ist ein Monoid, aber keine Gruppe. Außerdem ist $(\mathrm{M}_n(\mathbb{R}), \cdot)$ nicht kommutativ.
- $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ ist eine Gruppe, die nicht Abelsch ist.

Neutrales Element ist die Einheitsmatrix.

Ist die Determinante einer Matrix M nicht 0, so hat M eine inverse Matrix M^{-1}.

Beispiel 3: (Funktionen)

Zur Erinnerung: Für eine Menge A ist A^A die Menge aller Funktionen auf der Menge A.

Auf A^A haben wir die Operation $\circ$ (Komposition oder Verknüpfung von Funktionen):

$$(f \circ g)(a) = g(f(a))$$

Dann ist $(A^A, \circ)$ ein Monoid, aber keine Gruppe und auch nicht kommutativ (falls A mindestens 2 Elemente hat)

Das neutrale Element ist die Abbildung $\mathrm{id}_A : A \to A$ mit $\mathrm{id}_A(a) = a$ für alle $a \in A$.

Beispiel 4: (Permutationen)

Sei S_A die Menge aller Permutationen (bijektive Abbildungen) auf der Menge A. Dann ist $(S_A, \circ)$ eine Gruppe, die symmetrische Gruppe auf A.

Sie wird auch einfach mit S_A bezeichnet.

Für $S_{\{1,\ldots,n\}}$ schreiben wir auch S_n, dies ist eine endliche Gruppe mit $n!$ Elementen: die symmetrische Gruppe auf n Elementen.

S_n ist für $n \geq 3$ nicht kommutativ.

Beispiel 5: (Rechnen modulo n)

Für $x \in \mathbb{Z}$ seien $x \bmod n$ und $x \operatorname{div} n$ die eindeutig bestimmten Zahlen mit

$$x = (x \operatorname{div} n) \cdot n + (x \bmod n) \quad \text{und} \quad 0 \leq x \bmod n \leq n - 1$$

(ganzzahlige Division mit Rest).

Die auf Folie 37 definierte Relation $\equiv_n$ auf $\mathbb{Z}$ kann man auch definieren durch:

$$x \equiv_n y \iff (x \bmod n) = (y \bmod n).$$

Dies ist eine Äquivalenzrelation.

Anstatt $x \equiv_n y$ schreibt man auch $x \equiv y \bmod n$.

Offensichtlich gilt $x \equiv y \bmod n$ genau dann, wenn $x - y$ durch n teilbar ist (kurz: $n \mid (x - y)$).

Lemma 34

Es gilt für alle $x, y, n \in \mathbb{Z}$ mit $n \geq 2$:

$$((x \bmod n) + (y \bmod n)) \bmod n = (x + y) \bmod n \quad (2)$$

$$((x \bmod n) \cdot (y \bmod n)) \bmod n = (x \cdot y) \bmod n \quad (3)$$

Beweis: (2) und (3) sind äquivalent zu

$$n \mid (x + y - (x \bmod n) - (y \bmod n)) \quad (4)$$

$$n \mid (x \cdot y - (x \bmod n) \cdot (y \bmod n)) \quad (5)$$

Es sei $(x \bmod n) = x - \lambda \cdot n$ und $(y \bmod n) = y - \mu \cdot n$ (hierbei ist $\lambda = x \operatorname{div} n$ und $\mu = y \operatorname{div} n$).

Also gilt

$$\begin{aligned} x + y - (x \bmod n) - (y \bmod n) &= x + y - x + \lambda \cdot n - y + \mu \cdot n \\ &= (\lambda + \mu) \cdot n \\ x \cdot y - (x \bmod n) \cdot (y \bmod n) &= x \cdot y - (x - \lambda \cdot n) \cdot (y - \mu \cdot n) \\ &= \lambda \cdot n \cdot y + \mu \cdot n \cdot x - \lambda \cdot \mu \cdot n^2 \\ &= (\lambda \cdot y + \mu \cdot x - \lambda \cdot \mu \cdot n) \cdot n. \end{aligned}$$

d. h. (4) und (5). □

Eine alternative Formulierung von Lemma 34 ist:

Wenn $x_1 \equiv y_1 \bmod n$ und $x_2 \equiv y_2 \bmod n$, dann gilt auch $x_1 + x_2 \equiv y_1 + y_2 \bmod n$ und $x_1 \cdot x_2 \equiv y_1 \cdot y_2 \bmod n$.

Man sagt auch, dass $\equiv \pmod n$ eine Kongruenzrelation auf $\mathbb{Z}$ bezüglich $+$ und $\cdot$ ist.

Algebraische Strukturen: Monoide und Gruppen

Auf den Zahlen $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ definieren wir Operationen $+_n$ und $\cdot_n$ wie folgt:

$$(x +_n y) = (x + y) \bmod n, \qquad (x \cdot_n y) = (x \cdot y) \bmod n$$

Wegen Lemma 34 sind diese Operationen assoziativ.

$(\mathbb{Z}_n, +_n)$ ist eine endliche zyklische Gruppe (mit Erzeuger 1) und $(\mathbb{Z}_n, \cdot_n)$ ein endliches kommutatives Monoid.

Lemma 34 erlaubt es sehr große Zahlen modulo n zu berechnen.

Beispiel: Wir berechnen $7^{30} \bmod 5$. Es gilt:

$$\begin{aligned}
7^2 &= 49 \equiv 4 \bmod 5 \\
7^4 &= 49^2 \equiv 4^2 = 16 \equiv 1 \bmod 5 \\
7^8 &= (7^4)^2 \equiv 1 \bmod 5 \\
7^{16} &= (7^8)^2 \equiv 1 \bmod 5 \\
7^{30} &= 7^{16} \cdot 7^8 \cdot 7^4 \cdot 7^2 \equiv 4 \bmod 5
\end{aligned}$$

Definition (Homomorphismen)

Seien $\mathbb{G}_1 = (G_1, \circ_1)$ und $\mathbb{G}_2 = (G_2, \circ_2)$ Gruppen. Eine Homomorphismus von $\mathbb{G}_1$ nach $\mathbb{G}_2$ ist eine Abbildung $h : G_1 \to G_2$ mit:

$$\forall a, b \in G_1 : h(a \circ_1 b) = h(a) \circ_2 h(b)$$

Beispiel: Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}_n$ mit $f(x) = (x \bmod n)$ ist wegen Lemma 34 ein Homomorphismus von der Gruppe $(\mathbb{Z}, +)$ auf die Gruppe $(\mathbb{Z}_n, +_n)$, dieser Homomorphismus ist sogar surjektiv.

Wichtig: Für jeden Homomorphismus h von $\mathbb{G}_1$ nach $\mathbb{G}_2$ gilt:

- Wenn e_i das neutrale Element von $\mathbb{G}_i$ ist ($i \in \{1,2\}$), dann gilt $h(e_1) = e_2$, denn:

$$h(e_1) = h(e_1 \circ_1 e_1) = h(e_1) \circ_2 h(e_1)$$

und damit: $e_2 = h(e_1) \circ_2 h(e_1)^{-1} = h(e_1) \circ_2 h(e_1) \circ_2 h(e_1)^{-1} = h(e_1)$.

- $\forall a \in G_1 : h(a^{-1}) = h(a)^{-1}$: Es gilt:

$$\begin{aligned} e_2 &= h(e_1) = h(a \circ_1 a^{-1}) = h(a) \circ_2 h(a^{-1}) \text{ sowie} \\ e_2 &= h(e_1) = h(a^{-1} \circ_1 a) = h(a^{-1}) \circ_2 h(a) \end{aligned}$$

Wegen der Eindeutigkeit von Inversen impliziert dies $h(a^{-1}) = h(a)^{-1}$.

Definition (Isomorphismus)

Ein bijektiver Homomorphismus ist ein Isomorphismus.

Zwei Gruppen $\mathbb{G}_1$ und $\mathbb{G}_2$ sind isomorph, falls es einen Isomorphismus von $\mathbb{G}_1$ nach $\mathbb{G}_2$ gibt.

Beispiel: Seien A und B endliche Mengen mit $|A| = |B|$. Dann sind die Gruppen S_A und S_B isomorph.

Auch die Gruppen S_2 und $(\mathbb{Z}_2, +_2)$ sind isomorph.

Definition (Untergruppen)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe. Eine nicht-leere Teilmenge $U \subseteq G$ ist eine Untergruppe von $\mathbb{G}$, wenn gilt:

$$\forall a \in U : a^{-1} \in U \quad \text{und} \quad \forall a, b \in U : a \circ b \in U$$

Wichtig: Wenn U eine Untergruppe von $\mathbb{G} = (G, \circ)$ ist, dann gilt $1 \in U$, denn sei $a \in U$ beliebig (existiert wegen $U \neq \emptyset$).

Dann gehören auch a^{-1} und damit $1 = a \circ a^{-1}$ zu U.

Also ist $(U, \circ)$ (wobei hier $\circ$ eigentlich die Einschränkung der Operation $\circ$ auf die Teilmenge $U \subseteq G$ ist) eine Gruppe, die wir mit der Menge U identifizieren.

Für zwei Gruppen $\mathbb{H}$ und $\mathbb{G}$ schreiben wir $\mathbb{H} \leq \mathbb{G}$, falls in $\mathbb{G}$ eine Untergruppe U existiert, so dass U und $\mathbb{H}$ isomorph sind.

Beispiel 1: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

Beispiel 2: Für jede Zahl $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \{a \cdot n \mid a \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$.

Man kann zeigen, dass für jede Untergruppe U von $(\mathbb{Z}, +)$ eine ganze Zahl $n \in \mathbb{Z}$ mit $U = n\mathbb{Z}$ existiert.

Beispiel 3: $A = \{2a + 1 \mid a \in \mathbb{Z}\}$ (die Menge der ungeraden ganzen Zahlen) ist keine Untergruppe von $(\mathbb{Z}, +)$.

Z.B. gilt $1, 3 \in A$ aber $1 + 3 = 4 \notin A$.

Beispiel 4: Für $n \leq m$ gilt $S_n \leq S_m$.

Eine zu S_n isomorphe Untergruppe von S_m ist z.B.

$$U = \{f \in S_m \mid \text{Für alle } i \in \{n+1, \ldots, m\} \text{ gilt } f(i) = i\}.$$

Beispiel 5: Sei $m = k \cdot n$ für $k \geq 1$ und $m, n \geq 2$. Dann gilt $(\mathbb{Z}_n, +_n) \leq (\mathbb{Z}_m, +_m)$.

Eine zu $(\mathbb{Z}_n, +_n)$ isomorphe Untergruppe in $(\mathbb{Z}_m, +_m)$ ist

$$U = \{0, k, 2 \cdot k, \ldots, (n-1) \cdot k\}.$$

Um zu sehen, dass U tatsächlich eine Untergruppe von $(\mathbb{Z}_m, +_m)$ ist, seien $a, b \in \mathbb{Z}_n$ beliebig.

Wir zeigen, dass $a \cdot k +_m b \cdot k \in U$ gilt.

Sei $(a + b) \bmod n = r \in \mathbb{Z}_n$ und $(a + b) \operatorname{div} n = q$, d.h. $a + b = q \cdot n + r$.

Dann gilt:

$$\begin{aligned} a \cdot k +_m b \cdot k &= (a \cdot k + b \cdot k) \bmod m \\ &= ((a + b) \cdot k) \bmod m \\ &= ((q \cdot n + r) \cdot k) \bmod m \\ &= (q \cdot n \cdot k + r \cdot k) \bmod m \\ &= (q \cdot m + r \cdot k) \bmod m \\ &= (r \cdot k) \bmod m \\ &= r \cdot k = (a +_n b) \cdot k \in U \end{aligned}$$

Also gilt für alle $x, y \in U$ auch $x +_m y \in U$.

Da $(\mathbb{Z}_m, +_m)$ eine endliche Gruppe ist, folgt aus Satz 35 (übernächste Folie) bereits, dass U eine Untergruppe ist.

Ausserdem ist $(U, +_m)$ isomorph zu $(\mathbb{Z}_n, +_n)$:

Definiere die Abbildung $h : \mathbb{Z}_n \to U$ durch $h(a) = a \cdot k$ für alle $a \in \mathbb{Z}_n$.

Offensichtlich ist h bijektiv und es gilt

$$h(a) +_m h(b) = a \cdot k +_m b \cdot k \overset{(*)}{=} (a +_n b) \cdot k = h(a +_n b).$$

Die Gleichung (*) folgt dabei aus der Rechnung auf der vorhergehenden Folie.

Satz 35

Sei $\mathbb{G} = (G, \circ)$ eine endliche Gruppe. Eine Teilmenge $U \subseteq G$ ist Untergruppe von $\mathbb{G}$, genau dann, wenn gilt: $\forall a, b \in U : a \circ b \in U$

Beweis:

Sei $U \subseteq G$, so dass gilt: $\forall a, b \in U : a \circ b \in U$.

Wir müssen zeigen: $\forall a \in U : a^{-1} \in U$.

Sei also $a \in U$ und betrachte die Potenzen $a^1, a^2, a^3, \ldots$.

Es gilt $a^i \in U$ für alle $i \geq 1$.

Da G (und damit auch U) endlich ist, existieren $1 \leq i < j$ mit $a^i = a^j$.

$\rightsquigarrow$ $a^{j-i} = 1$, wobei $j - i > 0$ (insbesondere also $1 \in U$)

$\rightsquigarrow$ $a \circ a^{j-i-1} = a^{j-i-1} \circ a = 1$

$\rightsquigarrow$ $a^{-1} = a^{j-i-1} \in U$ □

Beachte: Satz 35 ist im Allgemeinen falsch für unendliche Gruppen: Betrachte $(\mathbb{Z}, +)$. Dann ist $\mathbb{N} \subseteq \mathbb{Z}$ keine Untergruppe von $(\mathbb{Z}, +)$, aber es gilt: $\forall a, b \in \mathbb{N} : a + b \in \mathbb{N}$.

Satz 36

Seien U und V Untergruppen von $\mathbb{G} = (G, \circ)$. Dann ist auch $U \cap V$ eine Untergruppe von $\mathbb{G}$.

Beweis: Wegen $1 \in U \cap V$ gilt $U \cap V \neq \emptyset$.

Seien nun $a, b \in U \cap V$, d.h. $a, b \in U$ und $a, b \in V$.

Da U und V Untergruppen von $\mathbb{G}$ sind, gilt auch

$$a^{-1} \in U, \quad a^{-1} \in V, \quad a \circ b \in U, \quad a \circ b \in V.$$

Also gilt $a^{-1} \in U \cap V$ und $a \circ b \in U \cap V$. □

Beispiel: Betrachte die beiden Untergruppen $2\mathbb{Z}$ und $3\mathbb{Z}$ von $(\mathbb{Z}, +)$.

Eine ganze Zahl ist durch 2 und 3 teilbar, genau dann, wenn sie durch 6 teilbar ist.

Also: $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$, was wieder eine Untergruppe ist

Bemerkung: Im Allgemeinen ist die Vereinigung von zwei Untergruppen keine Untergruppe.

Beispiel: Es gilt $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ und $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$.

Wäre $2\mathbb{Z} \cup 3\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$, so müsste auch $3 - 2 = 1 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ gelten, was aber nicht der Fall ist.

Definition (Nebenklassen)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe und sei U eine Untergruppe von $\mathbb{G}$.

- Eine Linksnebenklasse von U ist eine Teilmenge von $\mathbb{G}$ der Form $a \circ U = \{a \circ u \mid u \in U\}$ (kurz aU), wobei $a \in G$.
- Eine Rechtsnebenklasse von U ist eine Teilmenge von $\mathbb{G}$ der Form $U \circ a = \{u \circ a \mid u \in U\}$ (kurz Ua), wobei $a \in G$.

Beispiel:

Betrachte die Gruppe $(\mathbb{Z}_6, +_6)$ und die zu $(\mathbb{Z}_2, +_2)$ isomorphe Untergruppe $U = \{0, 3\}$.

U hat 3 verschiedene Linksnebenklassen:

- $0 +_6 U = 3 +_6 U = \{0, 3\}$
- $1 +_6 U = 4 +_6 U = \{1, 4\}$
- $2 +_6 U = 5 +_6 U = \{2, 5\}$

Beispiel (Fortsetzung):

Dies sind auch die Rechtnebenklassen von U.

Beachte: Ist $\mathbb{G} = (G, \circ)$ eine Abelsche Gruppe und U eine Untergruppe, so gilt $a \circ U = U \circ a$ für alle $a \in G$.

Insbesondere ist jede Linksnebenklasse von U auch eine Rechtsnebenklasse von U (für nicht-Abelsche Gruppen ist dies im Allgemeinen falsch).

Lemma 37

Sei U eine Untergruppe der endlichen Gruppe $\mathbb{G} = (G, \circ)$. Jede Linksnebenklasse sowie jede Rechtsnebenklasse von U besteht aus genau $|U|$ vielen Elementen von G.

Beweis:

Sei $aU = \{a \circ u \mid u \in U\}$ eine Linksnebenklasse.

Wir definieren eine Funktion $f : U \longrightarrow aU$ durch die Vorschrift

$$f(u) = a \circ u \ (u \in U).$$

Offensichtlich ist f surjektiv.

Ausserdem ist f injektiv:

$$f(u_1) = f(u_2) \ \rightsquigarrow \ a \circ u_1 = a \circ u_2 \ \rightsquigarrow \ u_1 = a^{-1} \circ a \circ u_1 = a^{-1} \circ a \circ u_2 = u_2.$$

Also ist f bijektiv, d.h. $|U| = |aU|$.

Der gleiche Beweis funktioniert auch für Rechtsnebenklassen. □

Lemma 38

Sei U eine Untergruppe von $\mathbb{G} = (G, \circ)$. Es gilt für alle $a, b \in G$:

$$aU = bU \iff a^{-1}b \in U$$
$$Ua = Ub \iff ab^{-1} \in U$$

Beweis: Wir zeigen die Aussage für Linksnebenklassen, der gleiche Beweis funktioniert auch für Rechtsnebenklassen.

"$\Rightarrow$": Gelte $aU = bU$.

Wegen $1 \in U$ folgt $b = b1 \in bU = aU$.

Also gibt es ein $u \in U$ mit $b = au$.

$\rightsquigarrow \quad a^{-1}b = u \in U$.

"$\Leftarrow$": Gelte $a^{-1}b \in U$.

Sei etwa $a^{-1}b = u_0 \in U$, d. h. $au_0 = b$.

$$\rightsquigarrow \quad bU = \{bu \mid u \in U\} = \underbrace{\{au_0u \mid u \in U\}}_{X}.$$

Offensichtlich gilt

$$X = \{au_0u \mid u \in U\} \subseteq \{au' \mid u' \in U\} = aU.$$

Aber es gilt auch

$$aU = \{au \mid u \in U\} = \{au_0(u_0^{-1}u) \mid u \in U\} \subseteq \{au_0u' \mid u' \in U\} = X.$$

Also gilt in der Tat $bU = X = aU$. □

Lemma 39

Sei U eine Untergruppe von $\mathbb{G} = (G, \circ)$ und seien aU und bU (bzw. Ua und Ub) zwei verschiedene Linksnebenklassen (bzw. Rechtsnebenklassen) von U. Dann gilt $aU \cap bU = \emptyset$ (bzw. $Ua \cap Ub = \emptyset$).

Beweis: Wir zeigen die Aussage für Linksnebenklassen, der gleiche Beweis funktioniert auch für Rechtsnebenklassen.

Angenommen es gilt $aU \cap bU \neq \emptyset$.

Wir werden $aU = bU$ zeigen.

Sei $x \in aU \cap bU$, d.h. es gibt $u_1, u_2 \in U$ mit $x = au_1 = bu_2$.

$\rightsquigarrow \quad a^{-1}b = u_1 u_2^{-1} \in U$.

Lemma 38 impliziert $aU = bU$. □

Satz 40 (Satz von Lagrange, 1770)

Sei U eine Untergruppe der endlichen Gruppe $\mathbb{G} = (G, \circ)$. Dann ist $|U|$ ein Teiler von $|G|$ und der Quotient $\frac{|G|}{|U|}$ ist gleich der Anzahl der Linksnebenklassen (sowie gleich der Anzahl der Rechtsnebenklassen), und wird als der Index $[\mathbb{G} : U]$ von U in $\mathbb{G}$ bezeichnet.

Beweis:

Betrachte die Menge $\mathcal{L} = \{aU \mid a \in G\}$ aller Linksnebenklassen und die Menge $\mathcal{R} = \{Ua \mid a \in G\}$ aller Rechtsnebenklassen.

Nach Lemma 39 gehört jedes $x \in G$ zu genau einer Linksnebenklasse sowie zu genau einer Rechtsnebenklasse.

$\rightsquigarrow \; |G| = \sum_{X \in \mathcal{L}} |X| = \sum_{X \in \mathcal{R}} |X|.$

Mit Lemma 37 folgt:

$$|G| = \sum_{X \in \mathcal{L}} |X| = \sum_{X \in \mathcal{L}} |U| = |\mathcal{L}| \cdot |U| \text{ sowie}$$

$$|G| = \sum_{X \in \mathcal{R}} |X| = \sum_{X \in \mathcal{R}} |U| = |\mathcal{R}| \cdot |U|$$

□

Beispiel 1:

Sei p eine Primzahl und sei $U \subseteq \mathbb{Z}_p$ eine Untergruppen von $(\mathbb{Z}_p, +_p)$.

Aus dem Satz von Lagrange folgt, dass $|U|$ ein Teiler von p ist.

Da p eine Primzahl ist, muss $|U| = 1$ oder $|U| = p$ gelten.

$\rightsquigarrow$ $U = \{0\}$ oder $U = \mathbb{Z}_p$.

Beispiel 2:

Im Allgemeinen muss für jede Untergruppe U von $(\mathbb{Z}_n, +_n)$ gelten: $|U|$ teilt n.

Andererseits hat $(\mathbb{Z}_n, +_n)$ für jeden Teiler m von n auch eine Untergruppe U mit $|U| = m$: Sei $n = k \cdot m$ und

$$U = \{0, k, 2 \cdot k, \ldots, (m-1) \cdot k\}.$$

Definition (Multiplikation von Teilmengen)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe. Für $A, B \subseteq G$ sei

$$A \circ B = \{a \circ b \mid a \in A, b \in B\} \subseteq G.$$

Anstatt $A \circ B$ schreiben wir auch kurz AB.

Definition (Normalteiler)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe. Eine Untergruppe $U \subseteq G$ ist ein Normalteiler von $\mathbb{G}$ falls gilt:

$$\forall g \in G \; \forall u \in U : g^{-1} u g \in U$$

Man sagt auch, dass U unter Konjugation mit beliebigen Elementen aus G abgeschlossen ist.

Für einen Normalteiler U von $\mathbb{G}$ bezeichnen wir mit G/U die Menge aller Linksnebenklassen von U.

Beispiele:

- Wenn $\mathbb{G}$ Abelsch ist, dann ist jede Untergruppe von $\mathbb{G}$ ein Normalteiler, denn es gilt für alle $g \in G$ und $u \in U$:

$$g^{-1} u g = u g^{-1} g = u \in U.$$

- Betrachte S_3 (die Menge aller Permutationen auf $\{1,2,3\}$) und sei τ die Permutation mit $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 3$.

  In Zykleschreibweise: $\tau = (1,2)(3)$.

  $U = \{\mathrm{id}, \tau\}$ ist eine Untergruppe von S_3, die kein Normalteiler ist:

  Sei σ die Permutation mit $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$

  In Zykleschreibweise: $\sigma = (1,2,3)$.

  Dann gilt:

$$(\sigma^{-1}\tau\sigma)(1) = 1, \quad (\sigma^{-1}\tau\sigma)(2) = 3, \quad (\sigma^{-1}\tau\sigma)(3) = 2,$$

  d.h. $\sigma^{-1}\tau\sigma \notin U$.

Lemma 41

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe und U ein Normalteiler von $\mathbb{G}$. Seien $g_1U, g_2U \in G/U$. Dann gilt

$$g_1U \circ g_2U = (g_1g_2)U \in G/U.$$

Beweis: Für alle $x \in G$ gilt:

$$\begin{aligned}
x \in g_1U \circ g_2U &\iff \exists u_1, u_2 \in U : x = g_1u_1g_2u_2 \\
&\iff \exists u_1, u_2 \in U : x = (g_1g_2)\underbrace{g_2^{-1}u_1g_2u_2}_{\in U} \\
&\iff \exists u \in U : x = (g_1g_2)u \\
&\iff x \in (g_1g_2)U
\end{aligned}$$

Satz 42 (Quotientengruppen)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe und U ein Normalteiler von $\mathbb{G}$. Dann ist $(G/U, \circ)$ wieder eine Gruppe.

Beweis:

Nach Lemma 41 ist $\circ$ eine Operation auf der Menge G/U der Linksnebenklassen: $g_1U \circ g_2U = (g_1g_2)U \in G/U$.

Die Assoziativität dieser Operation ergibt sich sofort aus der Assoziativität von $\circ$ auf G:

$$(g_1U \circ g_2U) \circ g_3U = (g_1g_2)U \circ g_3U = ((g_1g_2)g_3)U = (g_1(g_2g_3))U = g_1U \circ (g_2g_3)U = g_1U \circ (g_2U \circ g_3U)$$

Das neutrale Element ist $U = 1U$ und das inverse Element von gU ist $g^{-1}U$: $gU \circ g^{-1}U = (gg^{-1})U = U = (g^{-1}g)U = g^{-1}U \circ gU$. □

Die Gruppe $(G/U, \circ)$ bezeichen wir kurz mit $\mathbb{G}/U$ und nennen sie den Quotienten von $\mathbb{G}$ bezüglich des Normalteilers U.

Beispiel: $3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\}$ ist eine Normalteiler von $(\mathbb{Z}, +)$, da diese Gruppe Abelsch ist.

Der Quotient $(\mathbb{Z}, +)/3\mathbb{Z}$ ist isomorph zu $(\mathbb{Z}_3, +_3)$.

Beachte auch, dass die Funktion $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ mit

$$\varphi(n) = n \bmod 3$$

ein surjektiver Homomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}_3, +_3)$ ist.

Die Untergruppe $3\mathbb{Z}$ ist die Menge aller $n \in \mathbb{Z}$ mit $\varphi(n) = 0$; der sogenannte Kern von φ.

Definition (Kern und Bild eines Homomorphismus)

Seien $\mathbb{G} = (G, \circ)$, $\mathbb{H} = (H, *)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus von $\mathbb{G}$ nach $\mathbb{H}$.

Der Kern von φ, kurz $\ker(\varphi)$, ist definiert als

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_{\mathbb{H}}\}.$$

Das Bild von φ, kurz $\mathrm{im}(\varphi)$, ist definiert als

$$\mathrm{im}(\varphi) = \{\varphi(g) \in H \mid g \in G\}.$$

Lemma 43

Die Menge $\ker(\varphi)$ *ist ein Normalteiler von* $\mathbb{G}$ *und die Menge* $\mathrm{im}(\varphi)$ *ist eine Untergruppe von* $\mathbb{H}$.

Beweis:

$\mathrm{im}(\varphi)$ ist eine Untergruppe von $\mathbb{H}$:

Seien $h, h' \in \mathrm{im}(\varphi)$.

$\rightsquigarrow$ es gibt $g, g' \in G$ mit $h = \varphi(g)$ und $h' = \varphi(g')$.

$\rightsquigarrow$ $h * h' = \varphi(g) * \varphi(g') = \varphi(g \circ g') \in \mathrm{im}(\varphi)$ und
$h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \mathrm{im}(\varphi)$.

Ausserdem gilt $\mathrm{im}(\varphi) \neq \emptyset$, da $G \neq \emptyset$.

Also ist $\mathrm{im}(\varphi)$ eine Untergruppe von $\mathbb{H}$.

$\ker(\varphi)$ ist ein Normalteiler von $\mathbb{G}$:

Seien $g, g' \in \ker(\varphi)$, d.h. $\varphi(g) = \varphi(g') = 1_{\mathbb{H}}$.

$\rightsquigarrow$ $\varphi(g \circ g') = \varphi(g) * \varphi(g') = 1_{\mathbb{H}}$ und $\varphi(g^{-1}) = \varphi(g)^{-1} = 1_{\mathbb{H}}^{-1} = 1_{\mathbb{H}}$.

$\rightsquigarrow$ $g \circ g', g^{-1} \in \ker(\varphi)$.

Ausserdem gilt $\ker(\varphi) \neq \emptyset$, da $1_{\mathbb{G}} \in \ker(\varphi)$.

Also ist $\ker(\varphi)$ eine Untergruppe von $\mathbb{G}$.

Sei nun wieder $g \in \ker(\varphi)$ und sei $x \in G$ beliebig.

$\rightsquigarrow \varphi(x^{-1} \circ g \circ x) = \varphi(x)^{-1} * \varphi(g) * \varphi(x) = \varphi(x)^{-1} * \varphi(x) = 1_{\mathbb{H}}$.

Also gilt $x^{-1} \circ g \circ x \in \ker(\varphi)$.

$\ker(\varphi)$ ist also ein Normalteiler von $\mathbb{G}$. □

1. Isomorphiesatz der Gruppentheorie

Seien $\mathbb{G} = (G, \circ)$, $\mathbb{H} = (H, *)$ Gruppen und sei $\varphi : G \to H$ ein Homomorphismus von $\mathbb{G}$ nach $\mathbb{H}$.
Dann sind die Gruppen $\mathbb{G}/\ker(\varphi)$ und $\mathrm{im}(\varphi)$ isomorph.

Beweis: Wir definieren eine Abbildung $\theta : G/\ker(\varphi) \to \mathrm{im}(\varphi)$ durch folgende Vorschrift:

$$\theta(g \circ \ker(\varphi)) = \varphi(g) \text{ für } g \in G.$$

Zunächst ist nicht klar, ob dies überhaupt eine Funktion definert.

Die folgende Äquivalenzkette zeigt, dass dies tatsächlich der Fall ist, und dass θ ausserdem injektiv ist.

Seien $g_1, g_2 \in G$:

$$
\begin{aligned}
g_1 \circ \ker(\varphi) = g_2 \circ \ker(\varphi) &\overset{\text{Lemma 38}}{\iff} g_1^{-1} \circ g_2 \in \ker(\varphi) \\
&\iff \varphi(g_1^{-1} \circ g_2) = 1_{\mathbb{H}} \\
&\iff \varphi(g_1)^{-1} * \varphi(g_2) = 1_{\mathbb{H}} \\
&\iff \varphi(g_1) = \varphi(g_2) \\
&\iff \theta(g_1 \circ \ker(\varphi)) = \theta(g_2 \circ \ker(\varphi))
\end{aligned}
$$

Ausserdem ist θ trivialerweise surjektiv, d.h. θ ist bijektiv.

Wir müssen noch zeigen, dass $\theta : \mathbb{G}/\ker(\varphi) \to \mathrm{im}(\varphi)$ ein Homomorphismus ist.

Seien $g_1, g_2 \in G$:

$$\begin{aligned}
\theta(g_1 \circ \ker(\varphi) \circ g_2 \circ \ker(\varphi)) &\overset{\text{Lemma 41}}{=} \theta((g_1 \circ g_2) \circ \ker(\varphi)) \\
&= \varphi(g_1 \circ g_2) \\
&= \varphi(g_1) * \varphi(g_2) \\
&= \theta(g_1 \circ \ker(\varphi)) * \theta(g_2 \circ \ker(\varphi)).
\end{aligned}$$

□

Definition (Teilbarkeit, größter gemeinsamer Teiler)

Wiederholung: Für zwei Zahlen $a, b \in \mathbb{Z}$ schreiben wir $a \mid b$, wenn es ein $k \in \mathbb{Z}$ gibt mit $b = k \cdot a$ (a teilt b).

Der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ von $a, b \in \mathbb{Z}$ ist definiert als

$$\mathrm{ggT}(a, b) = \max\{k \in \mathbb{N} \mid (k \mid a) \text{ und } (k \mid b)\}$$

Beachte: $\mathrm{ggT}(0, 0)$ ist nicht definiert.

Offensichtlich gilt: $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$, $\mathrm{ggT}(a, b) = \mathrm{ggT}(-a, b)$, $\mathrm{ggT}(0, a) = a$ für $a \neq 0$, und $\mathrm{ggT}(1, a) = 1$.

Beispiel: $\mathrm{ggT}(28, 16) = 4$

Definition (Primzahlen)

Eine Zahl $p \in \mathbb{N}$ mit $p \geq 2$ ist eine Primzahl, wenn für alle $n \in \mathbb{N} \setminus \{0\}$ gilt:

$$(n \mid p) \longrightarrow (n = 1 \text{ oder } n = p)$$

Eine Zahl $p \geq 2$ ist also eine Primzahl, falls 1 und p die einzigen Teiler von n unter den natürlichen Zahlen sind.

Die ersten 25 Primzahlen: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$

Den Beweis des folgenden Satzes schieben wir auf:

Satz 44 (Lemma von Euklid)

Sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid (a \cdot b)$. Dann gilt $p \mid a$ oder $p \mid b$.

Zahlentheorie: Fundamentalsatz der Arithmetik

Satz 45 (Fundamentalsatz der Arithmetik)

Jede Zahl $n \in \mathbb{N}$ mit $n \geq 2$ lässt sich eindeutig (also auf genau eine Weise) als Produkt von Primzahlen darstellen:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k},$$

wobei $p_1 < p_2 < \cdots p_k$ Primzahlen sind und $e_1, e_2, \ldots, e_k \in \mathbb{N} \setminus \{0\}$.

Beweis:

Wir zeigen zunächst, dass sich jede Zahl $n \in \mathbb{N}$ mit $n \geq 2$ als Produkt von Primzahlen schreiben lässt.

Angenommen es gibt eine Zahl $n \geq 2$ welche sich nicht als Produkt von Primzahlen schreiben lässt.

Zahlentheorie: Fundamentalsatz der Arithmetik

Sei $n \geq 2$ eine kleinste Zahl mit dieser Eigenschaft.

Dann kann n keine Primzahl sein.

Also hat n einen Teiler $a \in \mathbb{N}$ mit $2 \leq a < n$.

Es gibt dann eine Zahl $b \in \mathbb{N}$ mit $2 \leq b < n$ und $n = a \cdot b$.

Da n eine kleinste Zahl in $\{x \in \mathbb{N} \mid x \geq 2\}$ ist, welche sich nicht nicht als Produkt von Primzahlen schreiben lässt, lassen sich a und b als Produkt von Primzahlen schreiben.

Also kann auch n als Produkt von Primzahlen geschrieben werden.
Widerspruch!

Sprechweise: Schreiben wir eine Zahl n als ein Produkt von Primzahlen, so spricht man auch von einer Primfaktorzerlegung von n.

Zahlentheorie: Fundamentalsatz der Arithmetik

Wir zeigen nun die Eindeutigkeit.

Angenommen, es gibt eine Zahl $n \geq 2$, welche sich auf zwei verschiedene Arten als Produkt von Primzahlen schreiben lässt.

Sei $n \geq 2$ eine kleinste solche Zahl und seien

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} = q_1^{d_1} \cdot q_2^{d_2} \cdots q_m^{d_m},$$

zwei verschiedene Primfaktorzerlegungen von n.

Dass es sich hierbei um verschiedene Primfaktorzerlegungen handelt, kann formal durch die Bedingung

$$\{(p_1, e_1), (p_2, e_2), \ldots, (p_k, e_k)\} \neq \{(q_1, d_1), (q_2, d_2), \ldots, (q_m, d_m)\}$$

ausgedrückt werden.

Jedenfalls teilt p_1 das Produkt $q_1^{d_1} \cdot q_2^{d_2} \cdots q_m^{d_m}$.

Zahlentheorie: Fundamentalsatz der Arithmetik

Lemma von Euklid $\rightsquigarrow$ p_1 teilt eine der Primzahlen $q_1, \ldots, q_m$.

Da $p_1 \geq 2$, muss p_1 gleich einer der Zahlen $q_1, \ldots, q_m$ sein.

Durch Umbenennen können wir davon ausgehen, dass $p_1 = q_1$ gilt.

Also gilt

$$n/p_1 = p_1^{e_1-1} \cdot p_2^{e_2} \cdots p_k^{e_k} = q_1^{d_1-1} \cdot q_2^{d_2} \cdots q_m^{d_m},$$

Wir erhalten so zwei verschiedene Primfaktorzerlegungen für $n/p_1 < n$.
Widerspruch! □

Zahlentheorie: Primfaktorzerlegung

Beispiele:

- Die Primfaktorzerlegung von 30 ist $2 \cdot 3 \cdot 5$.
- Die Primfaktorzerlegung von 10000 ist $2^4 \cdot 5^4$.

Seien $n, m \geq 2$ natürliche Zahlen mit den Primfaktorzerlegungen

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \text{ und } m = p_1^{d_1} \cdot p_2^{d_2} \cdots p_k^{d_k}$$

Hierbei müssen wir auch $e_i = 0$ und $d_j = 0$ erlauben.

Dann gilt offensichtlich $\mathrm{ggT}(n, m) = p_1^{\min(e_1, d_1)} \cdot p_2^{\min(e_2, d_2)} \cdots p_k^{\min(e_k, d_k)}$.

Zahlentheorie: Es gibt unendlich viele Primzahlen

Satz 46 (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis:

Angenommen es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$.

Wir leiten einen Widerspruch ab.

Sei $m = 1 + p_1 \cdot p_2 \cdots p_n$.

1. Fall: m ist eine Primzahl. Da $m > p_i$ für alle $i \in \{1, \ldots, n\}$ gilt, haben wir einen Widerspruch erhalten.

2. Fall: m ist keine Primzahl.

Zahlentheorie: Es gibt unendlich viele Primzahlen

Sei p eine Teiler von m, welcher eine Primzahl ist (existiert nach dem Fundamentalsatz der Arithmetik).

Dann muss $p = p_i$ für ein $i \in \{1, \ldots, n\}$ gelten.

Also gibt es eine Zahl a mit

$$a \cdot p_i = m = 1 + p_1 \cdot p_2 \cdots p_n = 1 + p_i \cdot b$$

(wobei $b = p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_n$).

Also gilt $1 = a \cdot p_i - p_i \cdot b = p_i \cdot (a - b)$.

Wegen $p_i \geq 2$ und $a - b \in \mathbb{Z}$ ergibt dies einen Widerspruch. □

Zahlentheorie: Euklidischer Algorithmus

Der $\mathrm{ggT}(m, n)$ kann sehr effizient mittels des Euklidischen Algorithmus berechnet werden.

Der Euklidische Algorithmus beruht auf der einfachen Tatsache:

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(m, n \bmod m).$$

Allgemeiner gilt: $\mathrm{ggT}(m, n) = \mathrm{ggT}(m, n + \lambda m)$ für alle $\lambda \in \mathbb{Z}$, denn:

- Wenn $t \mid m$ und $t \mid n$, dann gilt auch $t \mid m$ und $t \mid (n + \lambda m)$.
- Wenn $t \mid m$ und $t \mid (n + \lambda m)$, dann gilt auch $t \mid m$ und $t \mid n$.

In seiner erweiterten Form berechnet der Euklidische Algorithmus $\mathrm{ggT}(m, n)$ als Linearkombination von m und n.

Zahlentheorie: Euklidischer Algorithmus

EUKLID(m, n) $(m, n > 0)$

if $m > n$ **then**

  $(x, y) :=$ EUKLID(n, m)

  return(y, x)

elseif m teilt n **then**

  return$(1, 0)$

else

  $(x', y') :=$ EUKLID$(n \bmod m, m)$;

  $x := y' - x' \cdot (n \operatorname{div} m)$;

  $y := x'$

  return(x, y)

endif

Zahlentheorie: Euklidischer Algorithmus

Satz 47 (Korrektheit von Euklids Algorithmus)

Für alle $m, n > 0$ liefert EUKLID(m, n) zwei ganze Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(m, n) = x \cdot m + y \cdot n$ zurück.

Beweis:

Zunächst ist klar, das Euklids Algorithmus nach endlich vielen Schritten anhält:

Bei einem Aufruf von EUKLID(m, n) mit $m \leq n$ hält der Algorithmus entweder an (falls $m|n$), oder es erfolgt der Aufruf EUKLID$(n \bmod m, m)$.

Es gilt aber $n \bmod m < m$ und $m \leq n$, die Argumente werden also nicht größer und das erste Argument wird echt kleiner.

Nun zur Korrektheit: Wenn EUKLID(m, n) das Paar (x, y) zurückliefert, dann gilt $\mathrm{ggT}(m, n) = x \cdot m + y \cdot n$.

Zahlentheorie: Euklidischer Algorithmus

Dies kann durch eine Induktion über die Anzahl der rekursiven Aufrufe von Euklids Algorithmus gezeigt werden.

Induktionsanfang: Es erfolgt kein rekursiver Aufruf, d.h. m teilt n.

Dann gilt $\mathrm{ggT}(m,n) = m = 1 \cdot m + 0 \cdot n = x \cdot m + y \cdot n$.

Induktionsschritt: Wir nehmen nun an, dass der Aufruf EUKLID(m,n) zu dem Aufruf EUKLID$(n \bmod m, m)$ führt und dieser Aufruf das Paar (x', y') zurück liefert.

Nach Induktionsannahme gilt $\mathrm{ggT}(n \bmod m, m) = x' \cdot (n \bmod m) + y' \cdot m$.

Wir erhalten dann:

$$\begin{aligned} x \cdot m + y \cdot n &= (y' - x' \cdot (n \operatorname{div} m)) \cdot m + x' \cdot n \\ &= x' \cdot (n - (n \operatorname{div} m) \cdot m) + y' \cdot m \\ &= x' \cdot (n \bmod m) + y' \cdot m \\ &= \mathrm{ggT}(n \bmod m, m) \\ &= \mathrm{ggT}(m,n) \end{aligned}$$

Zahlentheorie: Euklidischer Algorithmus

Aus Satz 47 folgt insbesondere, dass $\mathrm{ggT}(m, n)$ als Linearkombination von m und n (also als $x \cdot m + y \cdot n$ mit $x, y \in \mathbb{Z}$) dargestellt werden kann.

Beispiel:

m	n	n div m	n mod m	x	y
300	10002	33	102	-100	3
102	300	2	96	3	-1
96	102	1	6	-1	1
6	96	16	0	1	0

Also gilt $\mathrm{ggT}(300, 10002) = 6 = -100 \cdot 300 + 3 \cdot 10002$.

Wir können nun das Lemma von Euklid (Satz 44) beweisen:

Sei p eine Primzahl und $a, b \in \mathbb{Z}$ mit $p \mid (a \cdot b)$.

Angenommen p ist kein Teiler von a. Wir zeigen $p \mid b$.

Da p Primzahl ist und kein Teiler von a ist, gilt $\mathrm{ggT}(p, a) = 1$.

Satz 47 $\rightsquigarrow$ $x, y \in \mathbb{Z}$ mit $1 = x \cdot p + y \cdot a$.

Wegen $p \mid (a \cdot b)$ gibt es $z \in \mathbb{Z}$ mit $a \cdot b = z \cdot p$.

Es folgt

$$b = x \cdot p \cdot b + y \cdot a \cdot b = x \cdot p \cdot b + y \cdot z \cdot p = p \cdot (x \cdot b + y \cdot z).$$

Also gilt $p \mid b$. □

Lemma 48

Wenn $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$, *dann auch* $\mathrm{ggT}(a \cdot b, n) = 1$.

Beweis: Gelte $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$.

Angenommen $\mathrm{ggT}(a \cdot b, n) = t \geq 2$.

Wegen des Fundamentalsatzes der Arithmetik gibt es dann eine Primzahl p mit $p \mid t$.

Also gilt auch $p \mid (a \cdot b)$ und $p \mid n$.

Satz 44 $\rightsquigarrow$ $p \mid a$ oder $p \mid b$.

Also gilt $\mathrm{ggT}(a, n) \geq 2$ oder $\mathrm{ggT}(b, n) \geq 2$, ein Widerspruch! □

Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$.

Für $n \geq 2$ sei $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \text{ggT}(x, n) = 1\} \subseteq \{1, \ldots, n-1\}$.

Beispiel:

- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
- Ist p eine Primzahl, so gilt $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.

Im folgenden Satz schränken wir die Operation $\cdot_n$ (Multiplikation modulo n) auf $\mathbb{Z}_n^*$ ein.

Satz 49

Für alle $n \geq 2$ ist $(\mathbb{Z}_n^*, \cdot_n)$ eine Gruppe.

Beweis:

(1) $\mathbb{Z}_n^*$ ist abgeschlossen bezüglich $\cdot_n$:

Seien $a, b \in \mathbb{Z}_n^*$, d. h. $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$.

Lemma 48 $\rightsquigarrow$ $\mathrm{ggT}(a \cdot b, n) = 1$.

Es gibt ein $\lambda \in \mathbb{Z}$ mit $a \cdot_n b = a \cdot b + \lambda \cdot n$.

$\rightsquigarrow$ $\mathrm{ggT}(a \cdot_n b, n) = \mathrm{ggT}(a \cdot b + \lambda \cdot n, n) = \mathrm{ggT}(a \cdot b, n) = 1$

$\rightsquigarrow$ $a \cdot_n b \in \mathbb{Z}_n^*$

(2) $\cdot_n$ ist assoziativ auf $\mathbb{Z}_n^*$:

Dies folgt direkt aus der Assoziativität von $\cdot_n$ auf $\mathbb{Z}_n$.

(3) Das neutrale Element in $(\mathbb{Z}_n^*, \cdot_n)$ ist offensichtlich 1.

(4) Existenz von Inversen:

Sei $a \in \mathbb{Z}_n^*$, d. h. $\mathrm{ggT}(a, n) = 1$.

Satz 47 $\rightsquigarrow$ Es gibt Zahlen $x, y \in \mathbb{Z}$ mit $1 = x \cdot a + y \cdot n$.

$\rightsquigarrow x \cdot a \equiv 1 \bmod n$.

Lemma 34 $\rightsquigarrow$ $(x \bmod n) \cdot_n a = 1$.

Außerdem gilt auch $(x \bmod n) \in \mathbb{Z}_n^*$:

Angenommen $t \geq 2$ wäre ein Teiler von n und $x \bmod n$.

Dann wäre t auch ein Teiler von $(x \bmod n) + (x \operatorname{div} n) \cdot n = x$ und damit auch ein Teiler von $x \cdot a + y \cdot n = 1$ – ein Widerspruch!

Also ist $(x \bmod n) \in \mathbb{Z}_n^*$ das Inverse von a in $(\mathbb{Z}_n^*, \cdot_n)$. □

Beispiel (zur Inversenbildung):

In der Gruppe $(\mathbb{Z}_7^*, \cdot_n)$ gilt:

$$1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 4^{-1} = 2,\ 5^{-1} = 3,\ 6^{-1} = 6.$$

Die Eulersche φ-Funktion ist definiert durch: $\varphi(n) = |\mathbb{Z}_n^*|$ für $n \geq 2$.

Beispiele:

- $\varphi(7) = 6$
- $\varphi(8) = 4$
- Ist p eine Primzahl, so gilt $\varphi(p) = p - 1$.
- Für Primzahlen p, q mit $p \neq q$ gilt: $\varphi(p \cdot q) = (p-1) \cdot (q-1)$:

  Seien M_p (bzw. M_q) die Vielfachen von p (bzw. q) in $\mathbb{Z}_{pq}$.

  $\rightsquigarrow \; |M_p| = q, \; |M_q| = p, |M_p \cap M_q| = 1$

  $\rightsquigarrow \; \varphi(p \cdot q) = |\mathbb{Z}_{pq}^*| = pq - |M_p| - |M_q| + |M_p \cap M_q| =$
  $pq - p - q + 1 = (p-1) \cdot (q-1)$

Satz 50 (Satz von Euler)

Für alle $n \geq 2$ und alle $a \in \mathbb{Z}_n^*$ gilt $a^{\varphi(n)} \equiv 1 \bmod n$.

Der Satz von Euler folgt sofort aus dem folgenden Satz:

Satz 51

Sei $\mathbb{G} = (G, \circ)$ eine beliebige endliche Gruppe (mit neutralem Element 1) und sei $n = |G|$. Dann gilt $a^n = 1$ für alle $a \in G$.

Beweis:

Sei k die kleinste Zahl mit $k > 0$ und $a^k = 1$ (existiert, da G endlich!).

Diese Zahl wird auch als die Ordnung von a in $\mathbb{G}$ bezeichnet, kurz ord(a).

Die Menge $\{a^i \mid 0 \leq i \leq k-1\}$ bildet eine (zyklische) Untergruppe von $\mathbb{G}$ mit genau k Elementen!

Satz von Lagrange $\rightsquigarrow$ k teilt n.

Sei $n = \lambda \cdot k$ $(\lambda \geq 1)$.

$\rightsquigarrow$ $a^n = (a^k)^\lambda = 1^\lambda = 1$. □

Satz 52 (Kleiner Satz von Fermat)

Für alle $n \geq 2$ gilt:

$$n \text{ ist Primzahl} \iff \forall a \in \mathbb{Z}_n \setminus \{0\} : a^{n-1} \equiv 1 \text{ mod } n.$$

Beweis:

"$\Rightarrow$": Sei n eine Primzahl.

Dann gilt $\varphi(n) = n - 1$.

Satz von Euler $\rightsquigarrow$ $\forall a \in \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\} : a^{n-1} \equiv 1 \text{ mod } n$.

"$\Leftarrow$": Gelte $a^{n-1} \equiv 1 \bmod n$ für alle $a \in \mathbb{Z}_n \setminus \{0\}$.

Sei nun $1 \leq t \leq n-1$ ein Teiler von n.

$\rightsquigarrow$ $t^{n-1} \equiv 1 \bmod n$.

$\rightsquigarrow$ Es gibt eine Zahl $k \in \mathbb{N}$ mit: $t^{n-1} - 1 = k \cdot n$.

$\rightsquigarrow$ Es gibt eine Zahl $k' \in \mathbb{N}$ mit: $t^{n-1} - 1 = k' \cdot t$.

Wäre $t \geq 2$, so würde $-1 \equiv 0 \bmod t$ folgen, ein Widerspruch.

Also hat n keinen Teiler im Bereich $\{2, \ldots, n-1\}$ und ist somit eine Primzahl. □

Wir werden den kleinen Satz von Fermat für den Korrektheitsbeweis des wichtigsten kryptographischen Protokolls (RSA-Verfahren) benutzen. Zuvor benötigen wir noch den sogenannten Chinesischen Restsatz.

Satz 53 (Chinesischer Restsatz)

Seien $m_1, m_2, \ldots, m_k \geq 2$ und gelte $ggT(m_i, m_j) = 1$ für $i \neq j$.
Sei $M = m_1 \cdot m_2 \cdots m_k$. Dann ist die wie folgt definierte Abbildung
$\mu : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ bijektiv:

$$\mu(x) = (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k).$$

Beweis: Wegen $|\mathbb{Z}_M| = |\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}| = M$ genügt es zu zeigen, dass μ injektiv ist.

Angenommen es gilt $\mu(x) = \mu(y)$ für $x, y \in \mathbb{Z}_M$.

$\rightsquigarrow$ $x \equiv y \bmod m_i$ für alle $1 \leq i \leq k$.

$\rightsquigarrow$ $m_i \mid (x - y)$ für alle $1 \leq i \leq k$.

Da m_i und m_j teilerfremd sind ($ggT(m_i, m_j) = 1$) für $i \neq j$, ist auch $M = m_1 \cdot m_2 \cdots m_k$ ein Teiler von $x - y$.

$\rightsquigarrow$ $x \equiv y \bmod M$, d.h. $x = y$. □

Beispiel:

Hier ist Abbildung $\mu : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$:

x	x mod 2	x mod 3
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

Sei $a_i \in \mathbb{Z}_{m_i}$ für $1 \leq i \leq k$ und gelte $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$.

Sei $M = m_1 \cdot m_2 \cdots m_k$.

Nach dem Chinesischen Restsatz existiert genau ein $x \in \mathbb{Z}_M$, so dass $a_i \equiv x \bmod m_i$ für $1 \leq i \leq k$ gilt.

Dieses x können wir wie folgt berechnen:

Sei $M_i = (m_1 \cdot m_2 \cdots m_k)/m_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ für $1 \leq i \leq k$.

Dann folgt aus $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$ und Lemma 48, dass auch $\text{ggT}(m_i, M_i) = 1$ für $i \neq j$ gilt.

Nach Satz 47 existieren für $1 \leq i \leq k$ ganze Zahlen $x_i, N_i \in \mathbb{Z}$ mit

$$x_i \cdot m_i + N_i \cdot M_i = 1.$$

Sei $x = \sum_{i=1}^{k} a_i \cdot N_i \cdot M_i \bmod M$.

Da $M_i = (\prod_{j=1}^{k} m_j)/m_i$ gilt

$$M_i \bmod m_j = 0 \text{ für } i \neq j.$$

Daraus folgt für alle $1 \leq i \leq k$:

$$x \bmod m_i = a_i \cdot N_i \cdot M_i \bmod m_i.$$

Wegen $x_i \cdot m_i + N_i \cdot M_i = 1$ für $1 \leq i \leq k$ folgt

$$N_i \cdot M_i \bmod m_i = 1,$$

Also gilt:

$$x \bmod m_i = a_i \cdot N_i \cdot M_i \bmod m_i = a_i.$$

Beispiel: $a_1 = 2,\ a_2 = 3,\ a_3 = 4,\ m_1 = 3,\ m_2 = 5,\ m_3 = 11.$

$$2 = x \bmod 3$$

$$3 = x \bmod 5$$

$$4 = x \bmod 11$$

$$M = m_1 \cdot m_2 \cdot m_3 = 165$$

$$\rightsquigarrow M_1 = M/m_1 = 55,\ M_2 = M/m_2 = 33,\ M_3 = M/m_3 = 15$$

$$\text{EUKLID}(m_1, M_1) \rightsquigarrow \text{ggT}(m_1, M_1) = 1 = (-18) \cdot m_1 + 1 \cdot M_1$$
$$\text{EUKLID}(m_2, M_2) \rightsquigarrow \text{ggT}(m_2, M_2) = 1 = (-13) \cdot m_2 + 2 \cdot M_2$$
$$\text{EUKLID}(m_3, M_3) \rightsquigarrow \text{ggT}(m_3, M_3) = 1 = (-4) \cdot m_3 + 3 \cdot M_3$$

$$\rightsquigarrow N_1 = 1,\ N_2 = 2,\ N_3 = 3$$

$$x = \sum_{i=1}^{3} a_i \cdot N_i \cdot M_i \bmod M = 2 \cdot 1 \cdot 55 + 3 \cdot 2 \cdot 33 + 4 \cdot 3 \cdot 15 \bmod 165 = 158$$

Zahlentheorie: RSA-Verschlüsselung

Idee der Public Key Cryptography:

- Wollen zwei Parteien, die sich bisher noch nicht kennen, Daten geheim austauschen, so ergibt sich das Problem der Übermittlung eines Schlüssels über einen unsicheren Kanal.
- Bei Public-Key-Verfahren erzeugt der (zukünftige) Empfänger E einen Kodierungsschlüssel c sowie den dazu passenden Dekodierungsschlüssel d.
- E hält d geheim und schickt c an den (zukünftigen) Sender S über einen unsicheren Kanal.
- Für die Sicherheit des Verfahrens ist folgende Forderung entscheidend: Aus dem öffentlichen Kodierungsschlüssel c darf der geheime Dekodierungsschlüssel d nicht effizient (d.h. mit vertretbaren Zeitaufwand) berechenbar sein.

Das bekannteste und am meisten verbreitete Verfahren, das diesem Schema folgt, ist das RSA-Verfahren (Rivest, Shamir, Adleman; 1978).

Zahlentheorie: RSA-Verschlüsselung

RSA-Verfahren:

1. Der Empfänger E wählt zwei (große — z. B. 1000 Bits lange) verschiedene Primzahlen p und q (werden geheim gehalten).
2. E berechnet $n = p \cdot q$ und $\varphi(n) = (p-1) \cdot (q-1)$.
3. E berechnet zwei Zahlen k und ℓ mit $\mathrm{ggT}(k, \varphi(n)) = 1$ und $k \cdot \ell \equiv 1 \mod \varphi(n)$.
4. Öffentlicher Kodierungsschlüssel: n und k
5. Geheimer Dekodierschlüssel: ℓ.
6. Nachrichten sind Elemente aus $\mathbb{Z}_n$
7. Verschlüsseln: $m \mapsto (m^k \bmod n)$ für $m \in \mathbb{Z}_n$
8. Entschlüsseln: $m \mapsto (m^\ell \bmod n)$ für $m \in \mathbb{Z}_n$

Satz 54 (Korrektheit des RSA-Verfahrens)

Es gilt $(m^k)^\ell \equiv m \bmod n$ für alle $m \in \mathbb{Z}_n$.

Beweis: Sei $m \in \mathbb{Z}_n$.

Wir müssen zeigen: $m^{k \cdot \ell} \equiv m \bmod n$

Wegen $n = p \cdot q$ ist dies nach dem Chinesischen Restsatz äquivalent zu: $m^{k \cdot \ell} \equiv m \bmod p$ und $m^{k \cdot \ell} \equiv m \bmod q$.

Aus Symmetriegründen genügt es $m^{k \cdot \ell} \equiv m \bmod p$ zu zeigen.

1. Fall: p ist ein Teiler von m.

Dann gilt $m^{k \cdot \ell} \equiv 0 \equiv m \bmod p$.

2. Fall: p ist kein Teiler von m, d.h. $m \not\equiv 0 \bmod p$.

Aus dem kleinen Satz von Fermat folgt: $m^{p-1} \equiv 1 \bmod p$.

Die Zahlen k und ℓ sind so gewählt, dass ein $t \in \mathbb{Z}$ mit

$$k \cdot \ell = t \cdot \varphi(n) + 1 = t \cdot (p-1) \cdot (q-1) + 1$$

existiert.

$\rightsquigarrow \quad m^{k \cdot \ell} = m^{t \cdot (p-1) \cdot (q-1) + 1} = m \cdot \left(m^{p-1}\right)^{t \cdot (q-1)} \equiv m \bmod p.$ □

Zahlentheorie: RSA-Verschlüsselung

Bemerkungen zur Implementierung von RSA:

- Es gibt sehr effiziente Verfahren, mit denen man große Primzahlen zufällig generieren kann.
- Die Zahl k mit $\mathrm{ggT}(k, \varphi(n)) = 1$ wird in der Praxis wieder durch einen Zufallsprozess erzeugt:

  Wähle zufällig eine Zahl k (nicht zu klein) und berechne mittels des erweiterten Euklidischen Algorithmus $\mathrm{ggT}(k, \varphi(n))$.

  Falls, $\mathrm{ggT}(k, \varphi(n)) = 1$, so haben wir ein k mit der gewünschten Eigenschaft gefunden.

  Andernfalls wiederholen wir obigen Schritt.

  Man kann zeigen, dass dieser randomisierte Algorithmus mit überwältigender Wahrscheinlichkeit sehr schnell ein k mit der gewünschten Eigenschaft findet.

Zahlentheorie: RSA-Verschlüsselung

- Der erweiterte Euklidische Algorithmus liefert dann gleichzeitig auch zwei ganze Zahlen x und y mit $1 = x \cdot k + y \cdot \varphi(n)$.

  Also gilt $x \cdot k \equiv 1 \bmod \varphi(n)$ und wir können $\ell = x$ wählen.

- Das eigentliche Effizienzproblem beim RSA-Verfahren sind das Verschlüsseln und Entschlüsseln (Exponentation großer Zahlen modulo n).

Die Sicherheit von RSA beruht auf der Tatsache, dass kein Verfahren bekannt ist, welches effizient aus dem öffentlichen Schlüssel (n, k) den geheimen Schlüssel ℓ berechnet.

Insbesondere scheitern alle bekannten Verfahren hierfür, wenn n ca 2000 Bits lang ist.

Zahlentheorie: RSA-Verschlüsselung

Beispiel: Wähle die Primzahlen $p = 11$ und $q = 17$.

Dann gilt $n = 187$ und $\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160$.

Wähle $k = 7$. Dann gilt $\mathrm{ggT}(k, \varphi(n)) = 1$.

EUKLID$(7, 160)$:

a	b	b div a	b mod a	x	y
7	160	22	6	23	-1
6	7	1	1	-1	1
1	6	6	0	1	0

Es gilt also $\mathrm{ggT}(k, \varphi(n)) = 1 = 23 \cdot 7 + (-1) \cdot 160$.

Also gilt $23 \cdot k = 23 \cdot 7 \equiv 1 \bmod \varphi(n)$.

Wir können also $\ell = 23$ wählen.

Zahlentheorie: RSA-Verschlüsselung

Die Verschlüsselung der Nachricht $5 \in \mathbb{Z}_n$ ist damit 5^7 mod 187. Es gilt:

$$\begin{aligned} 5^7 &= 5^4 \cdot 5^3 = 625 \cdot 5^3 = 64 \cdot 5^3 = 320 \cdot 5^2 \equiv 133 \cdot 5^2 \\ &= 665 \cdot 5 \equiv 104 \cdot 5 \equiv 146 \bmod 187 \end{aligned}$$

Also: $5^7 \bmod 187 = 146$

Die Entschlüsselung der Nachricht 146 ist 146^{23} mod 187. Es gilt:

- $146^2 \equiv (-41)^2 = 1681 \equiv (-2) \bmod 187$
- $146^4 \equiv (-2)^2 = 4 \bmod 187$
- $146^8 \equiv 16 \bmod 187$
- $146^{16} \equiv 256 \equiv 69 \bmod 187$

Zahlentheorie: RSA-Verschlüsselung

Damit gilt

$$\begin{aligned} 146^{23} &= 146^{16} \cdot 146^4 \cdot 146^2 \cdot 146 \equiv 69 \cdot 4 \cdot (-2) \cdot 146 \\ &\equiv 276 \cdot (-2) \cdot 146 \equiv 89 \cdot (-2) \cdot 146 \equiv (-178) \cdot 146 \\ &\equiv 9 \cdot 146 = 1314 \equiv 5 \bmod 187 \end{aligned}$$

Also gilt $146^{23} \bmod 187 = 5$.

Zahlentheorie: RSA-Verschlüsselung

Zwei Möglichkeiten, RSA zu brechen:

- Berechne p und q aus $n = p \cdot q$ (Faktorisieren), berechne dann $\varphi(n) = (p-1) \cdot (q-1)$ und schließlich ℓ mittels des Euklidischen Algorithmus aus k und $\varphi(n)$.

  Problem: Es gibt bisher keinen effizienten Faktorisierungsalgorithmus.

- Berechne direkt aus der verschlüsselten Nachricht $s := m^k \bmod n$ den Geheimtext m (diskretes Wurzelziehen).

  Problem: Es gibt bisher keinen effizienten Algorithmus zum diskreten Wurzelziehen.

Zahlentheorie: Fibonacci-Zahlen

Definition (Fibonacci-Zahlen)

Die n-te Fibonacci-Zahl ($n \in \mathbb{N}$) ist induktiv wie folgt definiert:

- $F_0 = 0$
- $F_1 = 1$
- $F_{n+2} = F_{n+1} + F_n$ für alle $n \geq 0$

Die ersten Fibonacci-Zahlen lauten:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots$$

Zahlentheorie: Fibonacci-Zahlen

Betrachte die Gleichung $x^2 = x + 1$. Sie hat zwei Lösungen:

$$\phi = \frac{1+\sqrt{5}}{2} \approx 1,618 \text{ und } \psi = \frac{1-\sqrt{5}}{2} 1 - \phi = -0,618$$

Aus $\phi^2 = \phi + 1$ und $\psi^2 = \psi + 1$ folgt für alle $n \geq 0$:

$$\phi^{n+2} = \phi^{n+1} + \phi^n \text{ und } \psi^{n+2} = \psi^{n+1} + \psi^n.$$

Satz 55

Für alle $n \geq 0$ gilt

$$F_n = \frac{1}{\sqrt{5}}(\phi^n - \psi^n).$$

Beweis: Induktion über n.

Induktionsanfang: Wir müssen die Aussage zunächst für $n = 0$ und $n = 1$ beweisen.

$n = 0$: $F_0 = 0 = \frac{1}{\sqrt{5}}(1 - 1) = \frac{1}{\sqrt{5}}(\phi^0 - \psi^0)$

$n = 1$: $F_1 = 1 = \frac{1}{\sqrt{5}} \cdot (\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}) = \frac{1}{\sqrt{5}}(\phi^1 - \psi^1)$

Induktionsschritt: Sei nun $n \geq 0$ und sei die Aussage des Satzes bereits für n und $n + 1$ bewiesen, d.h. es gilt

$$\begin{aligned} F_{n+1} &= \frac{1}{\sqrt{5}}(\phi^{n+1} - \psi^{n+1}) \\ F_n &= \frac{1}{\sqrt{5}}(\phi^n - \psi^n) \end{aligned}$$

Dann gilt:

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ &= \frac{1}{\sqrt{5}}(\phi^{n+1} - \psi^{n+1}) + \frac{1}{\sqrt{5}}(\phi^n - \psi^n) \\ &= \frac{1}{\sqrt{5}}(\phi^{n+1} + \phi^n - (\psi^{n+1} + \psi^n)) \\ &= \frac{1}{\sqrt{5}}(\phi^{n+2} - \psi^{n+2}) \end{aligned}$$

□

Zahlentheorie: Fibonacci-Zahlen

Für eine reelle Zahl $r \in \mathbb{R}$ ist $[r]$ die ganze Zahl, die am nächsten an r ist (wenn $r = n + 0,5$ für $n \in \mathbb{Z}$ gilt, setzen wir willkürlich $[r] = n$):

$$[r] = \begin{cases} n & \text{falls } r = n + \delta \text{ mit } 0 \leq \delta \leq 0,5 \\ n & \text{falls } r = n - \delta \text{ mit } 0 \leq \delta < 0,5 \end{cases}$$

Beispiel: Es gilt $[3,4999] = 3$ und $[3,5001] = 4$.

Satz 56

Für alle $n \geq 0$ gilt

$$F_n = \left[\frac{\phi^n}{\sqrt{5}} \right].$$

Beweis: Es gilt

$$F_n = \frac{\phi^n}{\sqrt{5}} - \frac{\psi^n}{\sqrt{5}} \in \mathbb{N}.$$

Da $|\frac{\psi^n}{\sqrt{5}}| < 0,5$ für alle $n \geq 0$ gilt, muss

$$\left| F_n - \frac{\phi^n}{\sqrt{5}} \right| < 0.5$$

gelten, woraus die Aussage des Satzes folgt. □

Zahlentheorie: Fibonacci-Zahlen

Wir verwenden Fibonacci-Zahlen um die Laufzeit des Euklidischen Algorithmus zu analysieren.

Satz 57

Sei $1 \leq m \leq n$. Angenommen, der Aufruf EUKLID(m, n) führt zu k rekursiven Aufrufen von EUKLID. Dann gilt $m \geq F_k$ und $n \geq F_{k+1}$.

Beweis: Induktion über k.

Induktionsanfang: $k = 0$.

Es gilt $m \geq 1 > F_0$ und $n \geq 1 = F_1$.

Induktionsschritt: Sei nun $k > 0$ und gelte die Aussage des Satzes für $k - 1$.

Der Aufruf EUKLID(m, n) führt zu dem Aufruf EUKLID$(n \bmod m, m)$ und dieser führt zu $k - 1$ rekursiven Aufrufen von EUKLID.

Nach Induktionsannahme gilt also $n \bmod m \geq F_{k-1}$ und $m \geq F_k$.

Damit erhalten wir:

$$n = (n \bmod m) + m \cdot (n \operatorname{div} m) \geq (n \bmod m) + m \geq F_{k-1} + F_k = F_{k+1}.$$

□

Mit Satz 56 folgt: Wenn $1 \leq m \leq n$ und der Aufruf EUKLID(m, n) zu k rekursiven Aufrufen von EUKLID führt, dann gilt

$$n \geq F_{k+1} = \left[\frac{\phi^{k+1}}{\sqrt{5}} \right] \geq \frac{\phi^{k+1}}{\sqrt{5}} - \frac{1}{2}.$$

Also gilt

$$k \leq \log_\phi(\sqrt{5} \cdot (n + 0,5)) - 1 = \log_\phi(n + 0,5) + \log_\phi(\sqrt{5}) - 1.$$

Definition (Ringe)

Ein Ring ist ein Tripel $(A, \oplus, \odot)$, wobei gilt:

- A ist eine beliebige Menge
- $\oplus : A \times A \to A$ und $\odot : A \times A \to A$ sind 2-stellige Operationen auf A.
- $(A, \oplus)$ ist eine Abelsche Gruppe.

  Sei 0 das neutrale Element von $(A, \oplus)$.
- $(A, \odot)$ ist ein Monoid.

  Sei 1 das neutrale Element von $(A, \odot)$.
- Für alle $a, b, c \in A$ gilt (Distributivgesetze):

$$\begin{aligned} a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c) \\ (b \oplus c) \odot a &= (b \odot a) \oplus (c \odot a) \end{aligned}$$

Ein Ring $(A, \oplus, \odot)$ ist kommutativ, falls $(A, \odot)$ kommutativ ist.

Definition (Körper)

Ein Körper ist ein Tripel $(A, \oplus, \odot)$, wobei gilt:

- A ist eine beliebige Menge
- $\oplus : A \times A \to A$ und $\odot : A \times A \to A$ sind 2-stellige Operationen auf A.
- $(A, \oplus)$ ist eine Abelsche Gruppe.

  Sei 0 das neutrale Element von $(A, \oplus)$.
- $(A \setminus \{0\}, \odot)$ ist eine Abelsche Gruppe.

  Sei 1 das neutrale Element von $(A \setminus \{0\}, \odot)$.
- Für alle $a, b, c \in A$ gilt: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Beachte: In jedem Körper gilt $1 \neq 0$. Dies muss jedoch nicht in einem Ring gelten (ein Ring kann nur aus einem einzigen Element bestehen).

Algebraische Strukturen: Ringe und Körper

Konventionen:

- Für Ring $(A, \oplus, \odot)$: Das inverse Element von $a \in A$ in $(A, \oplus)$ wird mit $-a$ bezeichnet.
- Für Körper $(A, \oplus, \odot)$: Das inverse Element von $a \in A \setminus \{0\}$ in $(A \setminus \{0\}, \odot)$ wird mit a^{-1} bezeichnet.
- Für Ring $(A, \oplus, \odot)$: Anstatt $a \odot b$ schreiben wir häufig nur ab.

Beispiele:

- Jede Körper ist ein Ring.
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring (aber kein Körper).
- Für $n \geq 2$ ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer Ring (aber im allgemeinen kein Körper).
- $(\mathbb{N}, +, \cdot)$ ist kein Ring.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, und $(\mathbb{C}, +, \cdot)$ sind Körper.
- $(\mathbb{R}^{n \times n}, +, \cdot)$ ist ein Ring, der für $n \geq 2$ nicht kommutativ ist.

Einige wichtige Eigenschaften von Körpern:

Lemma 58

Sei $(K, \oplus, \odot)$ ein Körper. Dann gilt:

(1) $\forall a \in K : a \odot 0 = 0 \odot a = 0$

(2) $\forall a, b \in K : ab = 0 \implies (a = 0$ *oder* $b = 0)$ *(Nullteilerfreiheit)*

(3) $\forall a \in K : -a = (-1) \odot a$

Beweis:

(1) Es gilt $0 \oplus (a \odot 0) = a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0)$.

Da $(A, \oplus)$ eine Gruppe ist, folgt $a \odot 0 = 0$ durch Kürzen von $a \odot 0$.

(2) Angenommen, es gilt $ab = 0$ und $a \neq 0$.

Also existiert a^{-1}.

Mit (1) folgt $b = 1 \odot b = a^{-1}ab = a^{-1}0 = 0$.

(3) Es gilt
$a \oplus ((-1) \odot a) = (1 \odot a) \oplus ((-1) \odot a) = (1 \oplus (-1)) \odot a = 0 \odot a = 0.$

Also gilt in der Tat $(-1) \odot a = -a$. □

Sei $\mathbb{K} = (K, \oplus, \odot)$ ein Körper und sei wie immer 1 das neutrale Element der Gruppe $(K \setminus \{0\}, \odot)$.

Wir definieren eine Abbildung $\varphi : \mathbb{Z} \to K$ wie folgt, wobei $n \in \mathbb{Z}$:

$$\varphi(n) = \begin{cases} \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{n \text{ mal}} & \text{wenn } n > 0 \\ 0 & \text{wenn } n = 0 \\ -\varphi(-n) & \text{wenn } n < 0 \end{cases}$$

Aus den Körpergesetzen folgt leicht für alle $m, n \in \mathbb{Z}$:

- $\varphi(m) \oplus \varphi(n) = \varphi(m + n)$
- $\varphi(m) \odot \varphi(n) = \varphi(m \cdot n)$

Man sagt auch: φ ist ein Ringhomomorphismus von dem Ring $(\mathbb{Z}, +, \cdot)$ in den Ring (sogar Körper) $\mathbb{K}$.

Im folgenden bezeichnen wir das Element $\varphi(n) \in K$ einfach mit n. Aus dem Zusammenhang wird sich stets ergeben, ob wir mit n ein Element aus $\mathbb{Z}$ oder ein Element des Körpers $\mathbb{K}$ meinen.

Definition (Charakteristik eines Körpers)

Sei $\mathbb{K} = (K, \oplus, \odot)$ ein Körper.

Die Charakteristik $\text{char}(\mathbb{K})$ des Körpers $\mathbb{K}$ ist wie folgt definiert:

- Falls $n = \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{n \text{ mal}} \neq 0$ für alle $n \geq 1$, so ist $\text{char}(\mathbb{K}) = 0$.
- Falls ein $n \geq 1$ mit $n = \underbrace{1 \oplus 1 \oplus \cdots \oplus 1}_{n \text{ mal}} = 0$ existiert, so ist $\text{char}(\mathbb{K})$ die kleinste Zahl n mit dieser Eigenschaft.

Die unendlichen Körper $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, und $(\mathbb{C}, +, \cdot)$ haben offensichtlich alle die Charakteristik 0.

Satz 59

Sei $\mathbb{K} = (K, \oplus, \odot)$ ein Körper mit $char(\mathbb{K}) \neq 0$.
Dann ist $char(\mathbb{K})$ eine Primzahl.

Beweis:

Sei $n = \text{char}(\mathbb{K}) > 0$.

Da in jedem Körper $0 \neq 1$ gilt, muss $n \geq 2$ gelten.

Angenommen n wäre keine Primzahl, $n = k \cdot m$ mit $1 < k, m < n$.

Aufgrund der Definition der Charakteristik gilt in $\mathbb{K}$: $k \neq 0 \neq m$.

Andererseits gilt aber in $\mathbb{K}$: $n = 0 = k \odot m$.

Dies widerspricht Aussage (2) in Lemma 58. □

Satz 60

Für alle $n \geq 2$ gilt: $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper genau dann, wenn n eine Primzahl ist.

Beweis: Offensichtlich ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein Körper genau dann, wenn $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ eine Gruppe ist.

Ist n eine Primzahl, so gilt $(\mathbb{Z}_n \setminus \{0\}, \cdot_n) = (\mathbb{Z}_n^*, \cdot_n)$, und dies ist eine Gruppe nach Satz 49.

Ist n hingegen keine Primzahl, so existieren $k, \ell \in \{1, \ldots, n-1\}$ mit $n = k \cdot \ell$.

$\rightsquigarrow k \cdot_n \ell = 0$ in $(\mathbb{Z}_n, \cdot_n)$.

Wegen $k, \ell \in \{1, \ldots, n-1\}$ gilt ausserdem $k \neq 0 \neq \ell$ in $\mathbb{Z}_n$.

Nach Aussage (2) in Lemma 58 ist $(\mathbb{Z}_n, +_n, \cdot_n)$ kein Körper. □

Der endliche Köper $(\mathbb{Z}_p, +_p, \cdot_p)$ (mit p prim) wird mit $\mathbb{F}_p$ bezeichnet.

Algebraische Strukturen: Ringe und Körper

Für jede Primzahl gibt es also einen endlichen Körper mit p Elementen.

Unser Ziel im Weiteren ist, die Struktur endlicher Körper genauer zu beschreiben (Anwendung: fehlerkorrigierende Kodes)

Zunächst müssen wir uns mit Polynomen über Körpern beschäftigen.

Definition (Polynome)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper, wobei 0 (bzw. 1) das neutrale Element bzgl. $+$ (bzw. $\cdot$) ist. Ein Polynom über $\mathbb{K}$ vom Grad $n \geq 0$ ist ein Ausdruck der Form $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, wobei $a_n, \ldots, a_0 \in \mathbb{K}$ und ($a_n \neq 0$ oder $n = 0$) gilt.

$\mathbb{K}[x]$ bezeichnet die Menge aller Polynome über $\mathbb{K}$ (von beliebigen Grad).

Wir schreiben auch $\text{grad}(p(x)) = n$, falls $p(x)$ ein Polynom über $\mathbb{K}$ vom Grad n ist.

Polynome vom Grad 0 sind also Elemente des Körpers $\mathbb{K}$.

Definition (Addition von Polynomen)

Seien $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ zwei Polynome vom Grad n bzw. m.

Wir definieren das Polynom $a(x) + b(x)$ wie folgt:

Sei $k = \max\{n, m\}$.

Setze $a_i = 0$ für $n + 1 \leq i \leq k$ und $b_i = 0$ für $m + 1 \leq i \leq k$.

Sei $c_i = a_i + b_i$ für $0 \leq i \leq k$.

1. Fall: $c_i = 0$ für alle $0 \leq i \leq k$: $a(x) + b(x) = 0$

2. Fall: Es gibt ein $0 \leq i \leq k$ mit $c_i \neq 0$.

Sei $\ell = \max\{i \mid 0 \leq i \leq k, c_i \neq 0\}$.

Dann ist $a(x) + b(x) = c_\ell x^\ell + \cdots + c_1 x + c_0$.

Definition (Multiplikation von Polynomen)

Seien $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ zwei Polynome vom Grad n bzw. m (d.h. $a_n \neq 0$ und $b_m \neq 0$).

Wir definieren das Polynome $a(x) \cdot b(x)$ vom Grad $n + m$ wie folgt:

Setze $a_i = 0$ für $n + 1 \leq i \leq n + m$ und $b_i = 0$ für $m + 1 \leq i \leq n + m$.

Sei $c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$ für $0 \leq i \leq n + m$.

1. Fall: $c_i = 0$ für alle $0 \leq i \leq n + m$: $a(x) \cdot b(x) = 0$

2. Fall: Es gibt ein $0 \leq i \leq n + m$ mit $c_i \neq 0$.

Sei $\ell = \max\{i \mid 0 \leq i \leq n + m, c_i \neq 0\}$.

Dann ist $a(x) \cdot b(x) = c_\ell x^\ell + \cdots + c_1 x + c_0$.

Bemerkung: Wir haben die Addition und Multiplikation von Polynomen aus $\mathbb{K}[x]$ wieder mit $+$ bzw. $\cdot$ bezeichnet, d. h. wir verwenden für diese Operationen die gleichen Bezeichnungen wie für die entsprechenden Operationen im Körper $\mathbb{K}$. Dies ist dadurch gerechtfertigt, dass $\mathbb{K} \subseteq \mathbb{K}[x]$.

Der folgende Satz ist leicht durch (etwas mühsames Nachrechnen) zu beweisen:

Satz 61 (Polynome bilden einen Ring)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper. Dann ist $(\mathbb{K}[x], +, \cdot)$ ein kommutativer Ring (der Polynomring über $\mathbb{K}$).

Das neutrale Element des Monoids $(\mathbb{K}[x], +)$ ist 0, während 1 das neutrale Element des Monoids $(\mathbb{K}[x], \cdot)$ ist.

Das additive Inverse $-a(x)$ des Polynoms $a(x) = a_n x^n + \cdots + a_1 x + a_0$ ist $(-a_n)x^n + \cdots + (-a_1)x + (-a_0)$.

Algebraische Strukturen: Ringe und Körper

Angenommen $a(x)$ und $b(x)$ sind Polynome mit $a(x) \neq 0 \neq b(x)$.

Wir können also $a(x)$ und $b(x)$ schreiben als

$$\begin{aligned} a(x) &= a_n x^n + \cdots + a_1 x + a_0 \\ b(x) &= b_m x^m + \cdots + b_1 x + b_0 \end{aligned}$$

wobei $a_n \neq 0 \neq b_m$ gilt.

Dann ist das Polynom $a(x) \cdot b(x)$ von der Form $a_n b_m x^{n+m} + c(x)$ wobei entweder $\text{grad}(c(x)) < n + m$ oder $c(x) = 0$ gilt.

Aus $a_n \neq 0 \neq b_m$ folgt $a_n \cdot b_m \neq 0$ (Körper sind nullteilerfrei).

Also gilt $a(x) \cdot b(x) \neq 0$.

Wir haben somit gesehen, dass jeder Polynomring über einem Körper nullteilerfrei ist.

Jedoch ist ein Polynomring über einem Körper niemals selbst ein Körper:

Das Polynom $a(x) = x \neq 0$ hat kein multiplikatives Inverses.

Definition (Auswerten von Polynomen)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $k \in \mathbb{K}$.

Definiere die Abbildung $\nu_k : \mathbb{K}[x] \to \mathbb{K}$ durch:

$$\nu_k(a_n x^n + \cdots + a_1 x + a_0) = a_n k^n + \cdots a_1 k + a_0.$$

Anstelle von $\nu_k(p(x))$ schreiben wir auch einfach $p(k)$.

Addition und Multiplikation von Polynomen wurden so definiert, dass gilt:

Satz 62

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $k \in \mathbb{K}$. Dann gilt für alle Polynome $a(x), b(x) \in \mathbb{K}[x]$:

$$a(k) + b(k) = (a(x) + b(x))(k) \quad \textit{und} \quad a(k) \cdot b(k) = (a(x) \cdot b(x))(k).$$

Die Abbildung ν_k ist also ein Ringhomomorphismus von dem Ring $\mathbb{K}[x]$ in den Ring (sogar Körper) $\mathbb{K}$.

Für Polyome kann wie für ganze Zahlen eine Division mit Rest definiert werden.

Satz 63 (Polynomdivision)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und seien $a(x), b(x) \in \mathbb{K}[x]$, wobei $b(x) \neq 0$. Dann existieren eindeutig bestimmte Polynome $q(x)$ und $r(x)$ mit:

- $a(x) = q(x) \cdot b(x) + r(x)$ *und*
- $grad(r(x)) < grad(b(x))$ *oder* $r(x) = 0$.

Wir schreiben $a(x)$ div $b(x) = q(x)$ und $a(x)$ mod $b(x) = r(x)$

Beweis:

Wir zeigen zunächst die Existenz der Polynome $q(x)$ und $r(x)$ durch Induktion über $\text{grad}(a(x))$.

Fall 1: $\text{grad}(a(x)) < \text{grad}(b(x))$

Dann setzen wir $q(x) = 0$ und $r(x) = a(x)$.

Fall 2: $\text{grad}(a(x)) \geq \text{grad}(b(x))$.

Sei $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$, wobei $b_m \neq 0$.

Fall 2.1: $\text{grad}(a(x)) = 0$, d. h. $a(x) = a_0$ und $b(x) = b_0 \neq 0$.

Setze $q(x) = a_0 \cdot b_0^{-1}$ und $r(x) = 0$.

Fall 2.2: $\text{grad}(a(x)) = n > 0$

Definiere $\widetilde{a}(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$.

Dann gilt $\text{grad}(\widetilde{a}(x)) < \text{grad}(a(x))$.

Nach Ind.hyp. existieren also Polynome $\widetilde{q}(x)$ und $\widetilde{r}(x)$ mit

- $\widetilde{a}(x) = \widetilde{q}(x) \cdot b(x) + \widetilde{r}(x)$ und
- $\text{grad}(\widetilde{r}(x)) < \text{grad}(b(x))$ oder $\widetilde{r}(x) = 0$.

Definiere nun $q(x) = \frac{a_n}{b_m} x^{n-m} + \widetilde{q}(x)$ und $r(x) = \widetilde{r}(x)$.

Dann gilt

- $a(x) = \frac{a_n}{b_m} x^{n-m} b(x) + \widetilde{a}(x) = \frac{a_n}{b_m} x^{n-m} b(x) + \widetilde{q}(x) \cdot b(x) + \widetilde{r}(x) = q(x) \cdot b(x) + r(x)$ und
- $\text{grad}(r(x)) < \text{grad}(b(x))$ oder $r(x) = 0$.

Um die Eindeutigkeit von $q(x)$ und $r(x)$ zu zeigen, nehmen wir an, dass es auch noch Polynome $\widetilde{q}(x)$ und $\widetilde{r}(x)$ gibt mit:

- $q(x) \cdot b(x) + r(x) = a(x) = \widetilde{q}(x) \cdot b(x) + \widetilde{r}(x)$ und
- $\text{grad}(\widetilde{r}(x)) < \text{grad}(b(x))$ oder $\widetilde{r}(x) = 0$.

$\rightsquigarrow \; (q(x) - \widetilde{q}(x)) \cdot b(x) = \widetilde{r}(x) - r(x).$

Angenommen es gilt $q(x) - \widetilde{q}(x) \neq 0$. Es folgt

$$\text{grad}(\widetilde{r}(x) - r(x)) = \text{grad}((q(x) - \widetilde{q}(x)) \cdot b(x)) \geq \text{grad}(b(x)).$$

Fall 1: $\widetilde{r}(x) \neq 0 \neq r(x)$

$\rightsquigarrow \; \text{grad}(r(x)) < \text{grad}(b(x)) > \text{grad}(\widetilde{r}(x))$.

$\rightsquigarrow \; \text{grad}(\widetilde{r}(x) - r(x)) < \text{grad}(b(x))$. Widerspruch!

Fall 2: $r(x) = 0$ und $\widetilde{r}(x) \neq 0$ (und damit $\text{grad}(\widetilde{r}(x)) < \text{grad}(b(x))$).

$\rightsquigarrow \; \text{grad}(\widetilde{r}(x)) = \text{grad}(\widetilde{r}(x) - r(x)) \geq \text{grad}(b(x))$. Widerspruch!

Fall 3: $\widetilde{r}(x) = 0$ und $r(x) \neq 0$. Analog

Fall 4: $\widetilde{r}(x) = 0 = r(x)$

$\rightsquigarrow \; (q(x) - \widetilde{q}(x)) \cdot b(x) = 0.$

Wegen $b(x) \neq 0$ folgt $q(x) - \widetilde{q}(x) = 0$. Widerspruch!

Also gilt in jedem Fall $q(x) - \widetilde{q}(x) = 0$, d. h. $q(x) = \widetilde{q}(x)$.

$\rightsquigarrow$ $\widetilde{r}(x) - r(x) = 0$, d.h. $r(x) = \widetilde{r}(x)$. □

Polynomdivision mit Rest kann analog zur Schulmethode für die Division ganzer Zahlen gemacht werden.

Beispiel: Wir berechnen $(x^5 + x)$ div $(2x^2 + 1)$ und $(x^5 + x)$ mod $(2x^2 + 1)$

Also gilt in jedem Fall $q(x) - \widetilde{q}(x) = 0$, d. h. $q(x) = \widetilde{q}(x)$.

$\rightsquigarrow\ \widetilde{r}(x) - r(x) = 0$, d.h. $r(x) = \widetilde{r}(x)$. □

Polynomdivision mit Rest kann analog zur Schulmethode für die Division ganzer Zahlen gemacht werden.

Beispiel: Wir berechnen $(x^5 + x)$ div $(2x^2 + 1)$ und $(x^5 + x)$ mod $(2x^2 + 1)$

$$(x^5 + x) : (2x^2 + 1) = \frac{1}{2}x^3$$
$$-(x^5 + \frac{1}{2}x^3)$$

Also gilt in jedem Fall $q(x) - \widetilde{q}(x) = 0$, d. h. $q(x) = \widetilde{q}(x)$.

$\rightsquigarrow\ \widetilde{r}(x) - r(x) = 0$, d.h. $r(x) = \widetilde{r}(x)$. □

Polynomdivision mit Rest kann analog zur Schulmethode für die Division ganzer Zahlen gemacht werden.

Beispiel: Wir berechnen $(x^5 + x)$ div $(2x^2 + 1)$ und $(x^5 + x)$ mod $(2x^2 + 1)$

$$(x^5 + x) : (2x^2 + 1) = \frac{1}{2}x^3$$
$$\underline{-(x^5 + \frac{1}{2}x^3)}$$
$$(-\frac{1}{2}x^3 + x)$$

Also gilt in jedem Fall $q(x) - \widetilde{q}(x) = 0$, d. h. $q(x) = \widetilde{q}(x)$.

$\rightsquigarrow$ $\widetilde{r}(x) - r(x) = 0$, d.h. $r(x) = \widetilde{r}(x)$. □

Polynomdivision mit Rest kann analog zur Schulmethode für die Division ganzer Zahlen gemacht werden.

Beispiel: Wir berechnen $(x^5 + x)$ div $(2x^2 + 1)$ und $(x^5 + x)$ mod $(2x^2 + 1)$

$$(x^5 + x) : (2x^2 + 1) = \frac{1}{2}x^3 - \frac{1}{4}x$$
$$-\underline{(x^5 + \frac{1}{2}x^3)}$$
$$(-\frac{1}{2}x^3 + x)$$
$$-(-\frac{1}{2}x^3 - \frac{1}{4}x)$$

Also gilt in jedem Fall $q(x) - \widetilde{q}(x) = 0$, d. h. $q(x) = \widetilde{q}(x)$.

$\rightsquigarrow$ $\widetilde{r}(x) - r(x) = 0$, d.h. $r(x) = \widetilde{r}(x)$. □

Polynomdivision mit Rest kann analog zur Schulmethode für die Division ganzer Zahlen gemacht werden.

Beispiel: Wir berechnen $(x^5 + x)$ div $(2x^2 + 1)$ und $(x^5 + x)$ mod $(2x^2 + 1)$

$$(x^5 + x) : (2x^2 + 1) = \frac{1}{2}x^3 - \frac{1}{4}x$$
$$-\underline{(x^5 + \frac{1}{2}x^3)}$$
$$(-\frac{1}{2}x^3 + x)$$
$$-\underline{(-\frac{1}{2}x^3 - \frac{1}{4}x)}$$
$$\frac{5}{4}x \text{ (Rest)}$$

Völlig analog zu Lemma 34 kann das folgende Lemma beweisen werden:

Lemma 64

Es gilt für alle $a(x), b(x), q(x) \in \mathbb{K}[x]$ *mit* $q(x) \neq 0$*:*

$$((a(x) \bmod q(x)) + (b(x) \bmod q(x))) \bmod q(x) = (a(x) + b(x)) \bmod q(x)$$

$$((a(x) \bmod q(x)) \cdot (b(x) \bmod q(x))) \bmod q(x) = (a(x) \cdot b(x)) \bmod q(x)$$

Anders ausgedrückt: Die Relation

$$R_{q(x)} = \{(a(x), b(x)) \mid a(x), b(x) \in \mathbb{K}[x], a(x) \bmod q(x) = b(x) \bmod q(x)\}$$

ist eine Kongruenzrelation auf $\mathbb{K}[x]$ bezüglich der Addition und Multiplikation von Polynomen:

- Wenn $(a_1(x), b_1(x)), (a_2(x), b_2(x)) \in R_{q(x)}$ dann auch $(a_1(x) + a_2(x), b_1(x) + b_2(x)) \in R_{q(x)}$.
- Wenn $(a_1(x), b_1(x)), (a_2(x), b_2(x)) \in R_{q(x)}$ dann auch $(a_1(x) \cdot a_2(x), b_1(x) \cdot b_2(x)) \in R_{q(x)}$.

Definition (Nullstellen)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $a(x) \in \mathbb{K}[x]$. Ein Element $k \in \mathbb{K}$ ist eine Nullstelle des Polynoms $a(x)$, falls $a(k) = 0$ gilt.

Polynomdivision kann benutzt werden, um den folgenden Satz zu zeigen.

Satz 65 (Anzahl der Nullstellen $\leq$ Grad)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $a(x) \in \mathbb{K}[x]$ mit $a(x) \neq 0$.

(1) *Ist k eine Nullstelle von $a(x)$, so gibt es ein Polynom $b(x)$ mit $a(x) = (x - k) \cdot b(x)$.*

(2) *$a(x)$ hat höchstens $grad(a(x))$ viele Nullstellen.*

Beweis: Wir zeigen zunächst (1).

Sei also k eine Nullstelle von $a(x)$, d. h. $a(k) = 0$.

Aus Satz 63 folgt, dass Polynome $q(x)$ und $r(x)$ existieren mit:

- $a(x) = q(x) \cdot (x - k) + r(x)$ und
- $\text{grad}(r(x)) < \text{grad}(x - k) = 1$ oder $r(x) = 0$.

Angenommen es gilt $r(x) \neq 0$ und damit $\text{grad}(r(x)) = 0$.

$\rightsquigarrow \quad r(x) = r_0 \in \mathbb{K} \setminus \{0\}$.

$\rightsquigarrow \quad 0 = a(k) = q(k) \cdot (k - k) + r(k) = r_0$. Widerspruch!

Also gilt $a(x) = q(x) \cdot (x - k)$.

Wir zeigen nun Aussage (2) durch Induktion über $\text{grad}(a(x))$.

IA: $\text{grad}(a(x)) = 0$.

Wegen $a(x) \neq 0$ gilt $a(x) = a_0 \in \mathbb{K} \setminus \{0\}$.

$\rightsquigarrow$ $a(x)$ hat $0 = \text{grad}(a(x))$ viele Nullstellen.

IS: Sei $\text{grad}(a(x)) > 0$.

Falls $a(x)$ keine Nullstelle hat, ist die Aussage des Satzes offenbar richtig.

Sei also k eine Nullstelle von $a(x)$.

(1) $\rightsquigarrow$ Es gibt ein Polynom $b(x)$ mit $a(x) = (x - k) \cdot b(x)$.

$\rightsquigarrow$ $\text{grad}(b(x)) = \text{grad}(a(x)) - 1$.

Mit der IH folgt, dass $b(x)$ höchstens $\text{grad}(a(x)) - 1$ viele Nullstellen hat.

Ausserdem ist jede weitere Nullstelle $k' \neq k$ von $a(x)$ eine Nullstelle von $b(x)$: $0 = a(k') = b(k') \cdot (k' - k)$ und $(k' - k) \neq 0$ impliziert $b(k') = 0$.

Also hat $a(x)$ höchstens $\text{grad}(a(x))$ viele Nullstellen. □

Bemerkung: Der Körper $(\mathbb{C}, +, \cdot)$ ist ein Körper, in dem jedes Polynom vom Grad mindestens 1 eine Nullstelle hat. Solche Körper bezeichnet man auch als algebraisch abgeschlossen.

Der Körper $(\mathbb{R}, +, \cdot)$ ist z. B. nicht algebraisch abgeschlossen, da das Polynom $x^2 + 2$ keine Nullstelle in $\mathbb{R}$ hat.

Definition (mehrfache Nullstelle)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $a(x) \in \mathbb{K}[x]$. Ein Element $k \in \mathbb{K}$ ist eine mehrfache Nullstelle des Polynoms $a(x)$, falls ein Polynom $b(x)$ mit $a(x) = (x - k)^2 \cdot b(x)$ existiert.

Um festzustellen, ob k eine mehrfache Nullstelle von $a(x)$ ist, kann man analog zu reellwertigen Polynomen Ableitungen verwenden:

Definition (Ableitung eines Polynoms)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper und sei $a(x) = a_n x^n + \cdots a_1 x + a_0 \in \mathbb{K}[x]$ ein Polynom vom Grad n.

Die Ableitung $a'(x) \in \mathbb{K}[x]$ ist wie folgt definiert.

Für $0 \leq i \leq n-1$ sei $b_i = (i+1)a_{i+1} = \underbrace{a_{i+1} + \cdots + a_{i+1}}_{i+1 \text{ mal}}$.

Falls $b_i = 0$ für alle $0 \leq i \leq n-1$ gilt, so ist $a'(x) = 0$.

Ansonsten sei $k = \max\{i \mid b_i \neq 0\}$.

Dann ist $a'(x) = b_k x^k + \cdots + b_1 x + b_0$ ein Polynom vom Grad k.

Durch einfaches Nachrechnen kann man zeigen, dass die üblichen Rechenregeln für Ableitungen von reellwertigen Polynomen auch in $\mathbb{K}[x]$ gelten.

Insbesondere gelten die Summenregel und Produktregel:

Produktregel

Für $a(x), b(x) \in \mathbb{K}[x]$ gilt:

- $(a(x) + b(x))' = a'(x) + b'(x)$
- $(a(x) \cdot b(x))' = a'(x) \cdot b(x) + a(x) \cdot b'(x)$.

Satz 66

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper, sei $a(x) \in \mathbb{K}[x]$ ein Polynom, $a(x) \neq 0$, $a'(x) \neq 0$, und sei $k \in \mathbb{K}$ eine Nullstelle von $a(x)$.

Dann ist k eine mehrfache Nullstelle von $a(x)$ genau dann, wenn k eine Nullstelle von $a'(x)$ ist.

Beweis:

Da k eine Nullstelle von $a(x) \neq 0$ ist, können wir nach Satz 65 das Polynom $a(x)$ schreiben als $a(x) = (x - k) \cdot c(x)$.

Mit der Produktregel erhalten wir $a'(x) = c(x) + (x - k) \cdot c'(x)$.

Wegen $a'(x) \neq 0$ gilt $c(x) \neq 0$.

Ist nun k eine Nullstelle von $a'(x)$, so folgt $0 = a'(k) = c(k)$.

Also gibt es ein Polynom $b(x)$ mit $c(x) = (x - k) \cdot b(x)$.

$\rightsquigarrow$ $a(x) = (x - k)^2 \cdot b(x)$ und k ist mehrfache Nullstelle von $a(x)$.

Ist andererseits k eine mehrfache Nullstelle von $a(x)$, so gibt es ein Polynom $b(x)$ mit $a(x) = (x - k)^2 \cdot b(x)$.

Mit der Produktregel folgt $a'(x) = 2 \cdot (x - k) \cdot b(x) + (x - k)^2 \cdot b'(x)$.

$\rightsquigarrow$ $a'(k) = 0$. □

Definition (Teilbarkeit von Polynomen)

Für Polynome $a(x), b(x) \in \mathbb{K}[x]$ schreiben wir $b(x) \mid a(x)$ ($b(x)$ teilt $a(x)$) falls ein Polynom $q(x) \in \mathbb{K}[x]$ mit $a(x) = b(x) \cdot q(x)$ existiert.

Bemerkungen: Für ein Polynom $a(x) \in \mathbb{K}[x]$ und $k \in \mathbb{K} \setminus \{0\}$ gilt $a(x) \mid k \cdot a(x)$ und $k \cdot a(x) \mid a(x)$.

Dies entspricht in $\mathbb{Z}$ der Tatsache, dass $a \mid -a$ und $-a \mid a$ für alle $a \in \mathbb{Z}$.

Definition (irreduzible Polynome)

Ein Polynome $p(x) \in \mathbb{K}[x]$ mit $p(x) \neq 0$ ist irreduzibel, falls für alle Polynome $a(x), b(x) \in \mathbb{K}[x]$ gilt:

$$p(x) = a(x) \cdot b(x) \quad \Longrightarrow \quad \text{grad}(a(x)) = 0 \text{ oder } \text{grad}(b(x)) = 0.$$

Irreduzible Polynome sind die "Primzahlen in $\mathbb{K}[x]$".

Definition (Größter gemeinsamer Teiler von zwei Polynomen)

Seien $a(x), b(x) \in \mathbb{K}[x]$ Polynome wobei $a(x) \neq 0$ oder $b(x) \neq 0$ gilt.

Ein größter gemeinsamer Teiler von $a(x)$, $b(x)$ ist ein Polynom $c(x)$ mit

- $c(x) \mid a(x)$ und $c(x) \mid b(x)$
- $\forall d(x) \in \mathbb{K}[x]\ (d(x) \mid a(x)\ \text{ und }\ d(x) \mid b(x) \quad \Rightarrow \quad d(x) \mid c(x)$.

Beachte: Sind $c_1(x)$ und $c_2(x)$ größte gemeinsame Teiler von $a(x)$ und $b(x)$, so gilt $c_1(x) \mid c_2(x)$ und $c_2(x) \mid c_1(x)$.

Hieraus folgt, dass es $k \in \mathbb{K} \setminus \{0\}$ mit $c_1(x) = k \cdot c_2(x)$ gibt.

Insbesondere gibt es einen größten gemeinsamen Teiler von $a(x)$ und $b(x)$ von der Gestalt $x^n + c(x)$ mit $\text{grad}(c(x)) < n$ (der führende Koeffizient ist 1), und es gibt genau einen solchen.

Wir bezeichnen diesen größten gemeinsamen Teiler von $a(x)$ und $b(x)$ mit $\text{ggT}(a(x), b(x))$.

Polynomdivision mit Rest erlaubt $\mathrm{ggT}(a(x), b(x))$ als Linearkombination von $a(x)$ und $b(x)$ mittels des erweiterten Euklidischen Algorithmus völlig analog zu den ganzen Zahlen zu berechnen.

Insbesondere erhalten wir den folgenden Satz:

Satz 67 (Lineardarstellung des ggT von Polynomen)

Seien $a(x), b(x) \in \mathbb{K}[x]$ Polynome, wobei $a(x) \neq 0$ oder $b(x) \neq 0$ gilt. Dann existieren $c(x), d(x) \in \mathbb{K}[x]$ mit

$$\mathrm{ggT}(a(x), b(x)) = c(x) \cdot a(x) + d(x) \cdot b(x).$$

Beispiel: In dem Polynomring $\mathbb{Q}[x]$ gilt:

$b(x)$	$a(x)$	$a(x)$ div $b(x)$	$a(x)$ mod $b(x)$	$c(x)$	$d(x)$
x^2+2	x^5+x	x^3-2x	$5x$	$\frac{1}{10}x^4-\frac{1}{5}x^2+\frac{1}{2}$	$-\frac{1}{10}x$
$5x$	x^2+2	$\frac{1}{5}x$	2	$-\frac{1}{10}x$	$\frac{1}{2}$
2	$5x$	$\frac{5}{2}x$	0	$\frac{1}{2}$	0

Also gilt

$$\mathrm{ggT}(x^5+x, x^2+2) = 1 = (-\frac{1}{10}x)\cdot(x^5+x)+(\frac{1}{10}x^4-\frac{1}{5}x^2+\frac{1}{2})\cdot(x^2+2).$$

Lemma 68

Seien $p(x), a(x), b(x) \in \mathbb{K}[x]$ Polynome, wobei $p(x) \neq 0$ irreduzibel ist. Aus $p(x) \mid a(x)b(x)$ folgt ($p(x) \mid a(x)$ oder $p(x) \mid b(x)$).

Beweis:

Angenommen es gilt $p(x) \mid a(x)b(x)$, aber $p(x)$ teilt $a(x)$ nicht.

Da $p(x)$ irreduzible ist, folgt $\mathrm{ggT}(p(x), a(x)) = 1$!

Also existieren $c(x), d(x) \in \mathbb{K}[x]$ mit $1 = c(x)p(x) + d(x)a(x)$.

$\rightsquigarrow \quad b(x) = c(x)b(x)p(x) + d(x)a(x)b(x)$.

Da $p(x) \mid a(x) \cdot b(x)$ existiert $e(x) \in \mathbb{K}[x]$ mit $a(x)b(x) = e(x)p(x)$.

$\rightsquigarrow \quad b(x) = c(x)b(x)p(x) + d(x)e(x)p(x) = (c(x)b(x) + d(x)e(x))p(x)$.

$\rightsquigarrow p(x) \mid b(x)$ □

Algebraische Strukturen: Ringe und Körper

Wir übertragen nun die Konstruktion des Restklassenrings $(\mathbb{Z}_n, +_n, \cdot_n)$ auf Polynome.

Sei $q(x) \in \mathbb{K}[x]$ ein Polynom und sei $n = \text{grad}(q(x)) > 0$.

Sei $\mathbb{K}[x]_n = \{a(x) \in \mathbb{K}[x] \mid \text{grad}(a(x)) < n\}$.

Wir definieren dann auf der Menge $\mathbb{K}[x]_n$ Operationen $+_{q(x)}$ und $\cdot_{q(x)}$ wie folgt:

$$\begin{aligned} a(x) +_{q(x)} b(x) &= (a(x) + b(x)) \bmod q(x) \\ a(x) \cdot_{q(x)} b(x) &= (a(x) \cdot b(x)) \bmod q(x) \end{aligned}$$

Wir bezeichnen die Struktur $(\mathbb{K}[x]_n, +_{q(x)}, \cdot_{q(x)})$ mit $\mathbb{K}[x]_{q(x)}$.

Aus Satz 61 und Lemma 64 folgt sofort:

Satz 69

$\mathbb{K}[x]_{q(x)}$ ist ein kommutativer Ring.

Der folgende Satz ist ein Analogon zu Satz 60.

Satz 70

$\mathbb{K}[x]_{q(x)}$ ist ein Körper genau dann, wenn $q(x)$ irreduzibel ist.

Beweis:

Sei zunächst das Polynom $q(x)$ nicht irreduzibel. Dann gibt es Polynome $a(x)$ und $b(x)$ mit $q(x) = a(x) \cdot b(x)$ und $\text{grad}(a(x)) \geq 1 \leq \text{grad}(b(x))$.

Wir zeigen, dass $a(x)$ kein Inverses in $\mathbb{K}[x]_{q(x)}$ hat.

Angenommen es gibt ein Polynom $c(x)$ mit $a(x) \cdot_{q(x)} c(x) = 1$.

$\rightsquigarrow$ Es gibt ein Polynom $d(x)$ mit $a(x) \cdot c(x) + d(x) \cdot q(x) = 1$.

$\rightsquigarrow$ $a(x) \cdot c(x) + d(x) \cdot a(x) \cdot b(x) = a(x) \cdot (c(x) + d(x)b(x)) = 1$.

Dies widerspricht aber $\text{grad}(a(x)) \geq 1$.

Sei nun $q(x)$ irreduzibel.

Um zu zeigen, dass $\mathbb{K}[x]_{q(x)}$ ein Körper ist, müssen wir zu jedem Polynom $a(x) \in \mathbb{K}[x]_n \setminus \{0\}$ ein multiplikatives Inverses finden.

Sei also $a(x) \in \mathbb{K}[x]_n \setminus \{0\}$.

Da $q(n)$ irreduzibel ist, folgt $\mathrm{ggT}(a(x), q(x)) = 1$.

Also gibt es $c(x), d(x) \in \mathbb{K}[x]$ mit $1 = a(x) \cdot c(x) + q(x) \cdot d(x)$.

$\rightsquigarrow \quad a(x) \cdot_{q(x)} (c(x) \bmod q(x)) = (a(x) \cdot c(x)) \bmod q(x) = 1.$

Also ist $c(x) \bmod q(x)$ ein multiplikatives Inverses von $a(x)$. □

Satz 70 erlaubt uns aus existierenden Körpern neue Körper zu konstruieren.

Bemerkungen: Sei $\text{grad}(q(x)) > 0$ und $q(x) \in \mathbb{K}[x]$ irreduzibel.

- Offensichtlich ist der Körper $\mathbb{K}$ ein Teilkörper von $\mathbb{K}[x]_{q(x)}$.

  Wir sagen auch, dass $\mathbb{K}[x]_{q(x)}$ ein Erweiterungskörper von $\mathbb{K}$ ist.
- Für ein Polynom der Form $x + k$ mit $k \in \mathbb{K}$ gilt $\mathbb{K}[x]_{x+k} = \mathbb{K}$.
- Das Polynom $q(y)$ hat in dem Körper $\mathbb{K}[x]_{q(x)}$ eine Nullstelle, nämlich $x \in \mathbb{K}[x]_n$ falls $n = \text{grad}(q(x)) > 1$.

  Falls $\text{grad}(q(x)) = 1$ hat $q(y)$ bereits eine Nullstelle in $\mathbb{K}$.

Beispiele:

(a) Das Polynom $x^2 - 2$ ist irreduzibel in $\mathbb{Q}[x]$
(es hat keine Nullstelle in $\mathbb{Q}$).

Also ist $\mathbb{Q}[x]_{x^2-2}$ ein Körper, der auch mit $\mathbb{Q}[\sqrt{2}]$ bezeichnet wird.

Intuitiv erhält man diesen Körper, indem man zu $\mathbb{Q}$ ein neues Element x, welches die Gleichung $x^2 - 2 = 0$ erfüllt (also entweder $\sqrt{2}$ oder $-\sqrt{2}$), hinzunimmt (adjungiert) — daher auch die Bezeichnung $\mathbb{Q}[\sqrt{2}]$.

Man kann $\mathbb{Q}[\sqrt{2}]$ mit dem Teilkörper $(\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}, +, \cdot)$ von $(\mathbb{R}, +, \cdot)$ identifizieren.

Beachte: Die Menge $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist unter Addition und Multiplikation abgeschlossen.

(b) Das Polynom $x^2 + 1$ ist irreduzibel in $\mathbb{R}[x]$.

Es gilt $\mathbb{R}[x]_{x^2+1} = \mathbb{C}$.

(c) Das Polynom $q(x) = x^2 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$, da es keine Nullstellen hat.

Der Körper $\mathbb{F}_2[x]_{q(x)}$ besteht aus den vier Elementen $0, 1, x, x+1$.

In $\mathbb{F}_2[x]_{q(x)}$ gilt z. B.

$$\begin{aligned} x \cdot x &= x^2 &&= x+1 \\ x \cdot (x+1) &= x^2 + x &&= 1 \\ (x+1) \cdot (x+1) &= x^2 + 1 &&= x \end{aligned}$$

(d) Das Polynom $p(x) = x^3 + x^2 + 1$ ist ebenfalls irreduzibel in $\mathbb{F}_2[x]$, da es keine Nullstellen hat (ein Polynom vom Grad ≤ 3 ist irreduzible genau dann, wenn es keine Nullstellen hat).

Der Körper $\mathbb{F}_2[x]_{p(x)}$ besteht aus den acht Elementen $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$.

Algebraische Strukturen: Ringe und Körper

Wir wollen nun Satz 70 für den Spezialfall $\mathbb{F}_p$ (mit p eine Primzahl) anwenden.

Angenommen $q(x) \in \mathbb{F}_p[x]$ ist ein irreduzibles Polynom vom Grad n.

Dann besteht der Körper $\mathbb{F}_p[x]_{q(x)}$ aus genau p^n Elementen, da es in $\mathbb{F}_p[x]$ genau p^n Elemente vom Grad $< n$ gibt.

Es stellt sich nun die Frage, ob es irreduzible Polynome von beliebigen Grad in $\mathbb{F}_p[x]$ gibt.

Durch ein Abzählargument kann man in der Tat zeigen, dass es in $\mathbb{F}_p[x]$ für jedes n ein irreduzibles Polynom vom Grad n gibt.

Wir werden einen anderen Weg gehen.

Wir sagen, dass das Polynom $a(x) \in \mathbb{K}[x]$ über dem Körper $\mathbb{K}$ in Linearfaktoren zerfällt, falls sich $a(x)$ schreiben lässt als

$$a(x) = k \cdot (x - k_1) \cdots (x - k_n),$$

wobei $k, k_1, \ldots, k_n \in \mathbb{K}$ gilt.

Hierbei ist n offensichtlich der Grad von $a(x)$ und $k_1, \ldots, k_n$ sind die Nullstellen von $a(x)$ (diese müssen nicht alle verschieden sein).

Z. B. zerfällt über dem Körper $\mathbb{C}$ jedes Polynom in Linearfaktoren.

Satz 71

Sei $\mathbb{K}$ ein Körper und $a(x) \in \mathbb{K}[x]$ ein Polynom. Dann existiert ein Erweiterungskörper $\mathbb{K}' \supseteq \mathbb{K}$, so dass $a(x)$ über dem Körper $\mathbb{K}'$ in Linearfaktoren zerfällt.

Man nennt $\mathbb{K}'$ einen Zerfällungskörper von $a(x)$.

Beweis: Induktion über $\text{grad}(a(x))$.

Der Fall $\text{grad}(a(x)) = 0$ ist klar, sei also $\text{grad}(a(x)) > 0$.

Fall 1. $a(x)$ hat eine Nullstelle $k \in \mathbb{K}$.

Nach Satz 65 existiert ein Polynom $b(x)$ mit $a(x) = (x - k) \cdot b(x)$.

Da $\text{grad}(b(x)) < \text{grad}(a(x))$ existiert nach Induktionshypothese ein Erweiterungskörper $\mathbb{K}' \supseteq \mathbb{K}$, so dass $b(x)$ über dem Körper $\mathbb{K}'$ in Linearfaktoren zerfällt, d. h.

$$b(x) = k' \cdot (x - k_1) \cdots (x - k_n) \text{ in } \mathbb{K}'[x],$$

wobei $k, k_1, \ldots, k_n \in \mathbb{K}'$ gilt.

Also gilt in $\mathbb{K}'[x]$:

$$a(x) = k' \cdot (x - k) \cdot (x - k_1) \cdots (x - k_n) \text{ in } \mathbb{K}'[x],$$

und $a(x)$ zerfällt über $\mathbb{K}'$ in Linearfaktoren.

Fall 2. $a(x)$ hat keine Nullstelle in $\mathbb{K}$.

Sei $b(x) \in \mathbb{K}[x]$ ein irreduzibler Faktor von $a(x)$, d. h. $a(x) = b(x) \cdot c(x)$ (für ein Polynom $c(x) \in \mathbb{K}[x]$) und $b(x)$ ist irreduzibel.

Da $a(x)$ keine Nullstelle hat, muss der Grad von $b(x)$ mindestens 2 sein.

Nach Satz 70 ist $\mathbb{K}[y]_{b(y)}$ ein Erweiterungskörper von $\mathbb{K}$, in dem das Polynom $b(x)$ die Nullstelle y hat.

In dem Ring $(\mathbb{K}[y]_{b(y)})[x] \supseteq \mathbb{K}[x]$ können wir also $a(x)$ schreiben als

$$a(x) = (x - y) \cdot \widetilde{a}(x) \text{ mit } \widetilde{a}(x) \in (\mathbb{K}[y]_{b(y)})[x].$$

Da $\text{grad}(\widetilde{a}(x)) < \text{grad}(a)$ ist, gibt es nach Induktionshypothese einen Erweiterungskörper $\mathbb{K}'$ von $\mathbb{K}[y]_{b(y)}$, über dem $\widetilde{a}(x)$ in Linearfaktoren zerfällt.

Dann zerfällt auch $a(x)$ über $\mathbb{K}'$ in Linearfaktoren. □

Satz 72

Sei p eine Primzahl, sei $\mathbb{K} = (K, +, \cdot)$ ein Körper der Charakteristik p, und sei $q = p^r$ für ein $r > 0$.

(1) *Das Polynom $x^q - x$ hat keine mehrfachen Nullstellen in $\mathbb{K}$.*

(2) *Die Menge $\{k \in K \mid k^q - k = 0 \text{ in } \mathbb{K}\}$ aller Nullstellen des Polynoms $x^q - x$ bildet einen Teilkörper von $\mathbb{K}$.*

Beweis:

Zu (1): Die Ableitung des Polynoms $x^q - x$ ist $q \cdot x^{q-1} - 1$.

Da der Körper $\mathbb{K}$ die Charakteristik p hat, gilt in $\mathbb{K}$:
$p = 0$ und somit auch $q = p^r = 0$.

Also gilt $(x^q - x)' = -1$ und $(x^q - x)'$ hat keine Nullstelle.

Nach Satz 66 hat also $x^q - x$ keine mehrfachen Nullstellen.

Zu (2): Nach Aufgabe ?? gilt in $\mathbb{K}$ für alle $a, b \in K$:

$$(a+b)^p = a^p + b^p.$$

Wir zeigen nun durch Induktion über $r \geq 1$, dass für alle $a, b \in K$ gilt:

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

Der Induktionsanfang ($r = 1$) folgt aus obiger Bemerkung.

Für $r > 1$ erhalten wir:

$$\begin{aligned}
(a+b)^{p^r} &= (a+b)^{p^{r-1} \cdot p} \\
&= \left((a+b)^{p^{r-1}}\right)^p \\
&\overset{\text{IH}}{=} (a^{p^{r-1}} + b^{p^{r-1}})^p \\
&= a^{p^{r-1} \cdot p} + b^{p^{r-1} \cdot p} \\
&= a^{p^r} + b^{p^r}
\end{aligned}$$

Also gilt $(a+b)^q = a^q + b^q$ für alle $a, b \in K$.

Nun können wir zeigen, dass die Menge

$$N = \{k \in K \mid k^q - k = 0 \text{ in } \mathbb{K}\}$$

aller Nullstellen des Polynoms $x^q - x$ ein Teilkörper von $\mathbb{K}$ bildet.

Seien $a, b \in N$, d. h. $a^q = a$ und $b^q = b$.

Dann gilt $(a \cdot b)^q = a^q \cdot b^q = a \cdot b$ und $(a + b)^q = a^q + b^q = a + b$.

Also gilt $a \cdot b, a + b \in N$.

Gilt weiter $a, b \in N \setminus \{0\}$ so gilt auch $a \cdot b \neq 0$ und somit $a \cdot b \in N \setminus \{0\}$.

Aus Satz 35 folgt, dass $(N, +)$ und $(N \setminus \{0\}, \cdot)$ Untergruppen von $(K, +)$ bzw. $(K \setminus \{0\}, \cdot)$ bilden.

Also ist $(N, +, \cdot)$ ein Teilkörper von $\mathbb{K}$. □

Satz 73

Sei p eine Primzahl und sei $q = p^r$ für ein $r > 0$.
Dann existiert ein Körper mit q Elementen.

Beweis:

Der Fall $r = 1$ ist klar, denn $\mathbb{F}_p = (\mathbb{Z}_p, +_p, \cdot_p)$ ist ein Körper mit $p = p^1 = q$ vielen Elementen.

Sei nun $r > 1$ und sei $\mathbb{K}$ ein Erweiterungskörper von $\mathbb{F}_p$, über dem das Polynom $x^q - x$ in Linearfaktoren zerfällt (existiert nach Satz 71).

Dann hat auch $\mathbb{K}$ Charakterisitik p.

Also hat nach Satz 72(1) das Polynom $x^q - x$ keine mehrfachen Nullstellen in $\mathbb{K}$.

Da $x^q - x$ über $\mathbb{K}$ in Linearfaktoren zerfällt, hat $x^q - x$ genau q viele Nullstellen in $\mathbb{K}$.

Nach Satz 72(2) bilden diese q vielen Nullstellen einen Körper mit q Elementen. □

Wir haben nun also gezeigt, dass für jede Primzahlpotenz q ein endlicher Körper mit q Elementen existiert.

Man kann weiter zeigen, dass dieser Körper eindeutig bestimmt ist:

Satz 74 (ohne Beweis)

Sei p eine Primzahl und sei $q = p^r$ für ein $r > 0$. Dann gibt es bis auf Isomorphie genau einen Körper mit q Elementen.

Den eindeutig bestimmten Körper mit $q = p^r$ vielen Elementen bezeichnet man als $\mathrm{GF}(q)$.

"GF" steht hierbei für "Galois field" (benannt nach Evariste Galois, 1811–1832; "field" ist der englische Begriff für Körper).

Den Körper GF(p^r) kann man als $\mathbb{F}_p[x]_{a(x)}$ für ein in $\mathbb{F}_p[x]$ irreduzibles Polynom $a(x)$ vom Grad r erhalten.

Der Körper GF(p^r) darf nicht mit dem Ring $(\mathbb{Z}_{p^r}, +_{p^r}, , \cdot_{p^r},)$ verwechselt werden, letzterer ist nur dann ein Körper, wenn $r = 1$ gilt.

Schließlich kann man noch zeigen, dass die Anzahl der Elemente eines endlichen Körpers stets eine Primzahlpotenz ist:

Satz 75

Sei $\mathbb{K} = (K, +, \cdot)$ ein endlicher Körper. Dann existiert eine Primzahl p und $r \geq 1$ mit $|K| = p^r$.

Satz 75 zeigt man am einfachsten durch Verwendung linearer Algebra.

Hierfür müssen wir Vektorräume über beliebigen Körpern betrachten.

Definition (Vektorraum)

Sei $\mathbb{K} = (K, +, \cdot)$ ein Körper. Ein Vektorraum über dem Körper $\mathbb{K}$ ist ein Tripel $\mathbb{V} = (V, \oplus, \odot)$, wobei gilt:

- $(V, \oplus)$ ist eine Abelsche Gruppe.
- $\odot : K \times V \to V$ ist eine Abbildung (Skalarmultiplikation) mit den folgenden Eigenschaften:
  - $\forall a, b \in K \; \forall v \in V : a \odot (b \odot v) = (a \cdot b) \odot v$
  - $\forall a \in K \; \forall u, v \in V : a \odot (u \oplus v) = (a \odot u) \oplus (a \odot v)$
  - $\forall a, b \in K \; \forall v \in V : (a + b) \odot v = (a \odot v) \oplus (b \odot v)$
  - $\forall v \in V : 1 \odot v = v$

Anstatt $a \odot v$ schreibt man überlicherweise kurz av.

Im folgenden sei $0_{\mathbb{V}}$ (bzw. $0_{\mathbb{K}}$) das neutrale Element der Abelschen Gruppe $(V, \oplus)$ (bzw. $(K, +)$).

Beachte: Für alle $v \in V$ gilt

$$(0_{\mathbb{K}} \odot v) \oplus (0_{\mathbb{K}} \odot v) = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \odot v = 0_{\mathbb{K}} \odot v,$$

d. h. $0_{\mathbb{K}} \odot v = 0_{\mathbb{V}}$.

Definition (lineare Unabhängigkeit, Basis)

Sei $\mathbb{V} = (V, \oplus, \odot)$ ein Vektorraum über dem Körper $\mathbb{K} = (K, +, \cdot)$.

Eine Menge $U \subseteq V$ ist linear unabhängig, falls für alle $a_1, \ldots, a_n \in K$ und alle paarweise verschiedenen $v_1, \ldots, v_n \in U$ gilt:

$$a_1 v_1 \oplus a_2 v_2 \oplus \cdots \oplus a_n v_n = 0_{\mathbb{V}} \implies a_1 = a_2 = \cdots = a_n = 0_{\mathbb{K}}.$$

Eine Basis von $\mathbb{V}$ ist eine linear unabhängige Teilmenge $B \subseteq V$ mit:

$$\forall v \in V \; \exists a_1, \ldots, a_n \in K, v_1, \ldots, v_n \in B : v = a_1 v_1 \oplus a_2 v_2 \oplus \cdots \oplus a_n v_n.$$

Man kann zeigen, dass jeder Vektorraum $\mathbb{V}$ eine Basis hat.

Es kann zwar mehrere verschiedene Basen geben, je zwei Basen von $\mathbb{V}$ haben aber stets die gleiche Kardinalität, welche als die Dimension $\dim(\mathbb{V})$ von $\mathbb{V}$ bezeichnet wird.

Ist $\dim(\mathbb{V})$ endlich, so ist $\mathbb{V}$ ein endlich-dimensionaler Vektorraum (über dem Körper $\mathbb{K}$).

Gilt $\dim(\mathbb{V}) = n < \infty$, und ist $\{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$, so hat jedes Element $v \in \mathbb{V}$ eine eindeutige Darstellung von der Form

$$v = a_1 v_1 \oplus a_2 v_2 \oplus \cdots \oplus a_n v_n$$

mit $a_1, \ldots, a_n \in \mathbb{K}$, und man kann v mit dem Tupel $(a_1, \ldots, a_n)$ identifizieren.

Insbesondere: Ist $\mathbb{V}$ ein endlich-dimensionaler Vektorraum über dem endlichen Körper $\mathbb{K}$, so besteht $\mathbb{V}$ aus $|\mathbb{K}|^{\dim(\mathbb{V})}$ vielen Elementen.

Beweis von Satz 75:

Sei $\mathbb{K} = (K, +, \cdot)$ ein endlicher Körper.

Die Charakterisitk von $\mathbb{K}$ muss nach Satz 59 eine Primzahl p sein.

Man zeigt leicht, dass die Struktur $(\{0, 1, \ldots, p-1\}, +, \cdot)$ isomorph zum Körper $\mathbb{F}_p$ ist, d. h. $\mathbb{K}$ ist ein Erweiterungskörper von $\mathbb{F}_p$.

Ausserdem bildet $\mathbb{K}$ einen endlich-dimensionalen Vektorraum über dem Unterköper $\mathbb{F}_p$ (Übung: Rechnen Sie die Vektorraumaxiome nach).

Ist $r \geq 1$ die Dimension dieses Vektorraums, so hat $\mathbb{K}$ genau p^r viele Elemente. □

Algebraische Strukturen: Ringe und Körper

Wie wir gesehen haben, spielen irreduzible Polynome bei der Konstruktion endlicher Körper die zentrale Rolle.

Es stellt sich somit die Frage, wie man feststellt, ob ein gegebenes Polynom $a(x) \in \mathbb{F}_p[x]$ irreduzible ist.

Der folgende Satz liefert ein Verfahren, um dies zu entscheiden.

Satz 76 (ohne Beweis)

Ein Polynom $a(x) \in \mathbb{F}_p[x]$ vom Grad $n \geq 2$ ist irreduzibel, genau dann, wenn gilt:

- *$a(x)$ ist Teiler des Polynoms $x^{p^n} - x$ und*
- *$ggT(a(x), x^{p^{n/t}} - x) = 1$ für jede Primzahlen t, welche n teilt.*

Beachte: Dass $a(x)$ ein Teiler des Polynoms $x^{p^n} - x$ ist, bedeutet, dass $x^{p^n} \bmod a(x) = x$ gilt.

Wir müssen also $x^{p^n} \bmod a(x)$ berechnen.

Dies kann man effizient dadurch machen, indem man mit $a_0(x) = x$ beginnend, die Folge der Polynome $a_{i+1}(x) = a_i(x)^p \bmod a(x)$ berechnet $(0 \leq i \leq n-1)$.

Dann gilt $a_n(x) = x^{p^n} \bmod a(x)$.

Man kann zeigen, dass die Wahrscheinlichkeit, dass ein zufällig gewähltes Polynom $a(x) \in \mathbb{F}_p[x]$ vom Grad $n \geq 2$ irreduzibel ist, ungefähr $1/n$ ist.

Wählt man n zufällige Polynome vom Grad n, so ist die Wahrscheinlichkeit, dass keines davon irreduzibel ist, ungefähr $(1 - 1/n)^n \leq 1/e$, d .h. mit Wahrscheinlichkeit $1 - 1/e \geq 0.6$ findet man so ein irreduzibles Polynom vom Grad n.

Algebraische Strukturen: Ringe und Körper

Als letzte Aussage über endliche Körper beweisen wir die folgende Aussage:

Satz 77

Sei $\mathbb{K} = (K, +, \cdot)$ ein endlicher Körper. Dann ist die Abelsche Gruppe $(K \setminus \{0\}, \cdot)$ (die multiplikative Gruppe von $\mathbb{K}$) zyklisch.

Ein Erzeuger der multiplikativen Gruppe des Körpers $\mathbb{K} = (K, +, \cdot)$ wird auch als ein primitives Element von $\mathbb{K}$ bezeichnet.

Dies ist also ein $p \in \mathbb{K}$ mit $p^{|K|-1} = 1$ und $p^i \neq 1$ für alle $1 \leq i < |K| - 1$.

Für den Beweis von Satz 77 benötigen wir noch einige Resultate zu endlichen Gruppen.

Zur Erinnerung (Folie 237): Sei $\mathbb{G} = (G, \circ)$ eine endliche Gruppe.

- Die Ordnung $\text{ord}(a)$ eines Elements $a \in G$ ist die kleinste Zahl $k > 0$, so dass $a^k = 1$ in $\mathbb{G}$ gilt (solch eine Zahl k existiert, da G endlich ist).
- Für alle $a \in G$ gilt: $\text{ord}(a)$ teilt $|G|$ und $a^{|G|} = 1$.

Lemma 78

Sei $\mathbb{G} = (G, \circ)$ eine endliche Gruppe. Dann gilt für alle $a \in G$ und $k \geq 0$:
$a^k = 1 \iff ord(a) \mid k$

Beweis:

Falls $\text{ord}(a) \mid k$ gilt, gibt es eine Zahl ℓ mit $k = \ell \cdot \text{ord}(a)$.

$\rightsquigarrow \quad a^k = a^{\ell \cdot \text{ord}(a)} = (a^{\text{ord}(a)})^\ell = 1^\ell = 1.$

Sei nun $a^k = 1$.

Division mit Rest liefert $q, r \in \mathbb{Z}$ mit $0 \leq r < \text{ord}(a)$ und $k = q \cdot \text{ord}(a) + r$.

$\rightsquigarrow \quad 1 = a^k = a^{q \cdot \text{ord}(a) + r} = (a^{\text{ord}(a)})^q \circ a^r = a^r.$

Da $\text{ord}(a)$ die kleinste Zahl $\alpha > 0$ mit $a^\alpha = 1$ ist, folgt $r = 0$, d. h. $\text{ord}(a) \mid k$. □

Lemma 79

Sei $\mathbb{G} = (G, \circ)$ eine endliche Abelsche Gruppe. Dann gilt für alle $a, b \in G$: Wenn $ggT(ord(a), ord(b)) = 1$, dann gilt $ord(a \circ b) = ord(a) \cdot ord(b)$.

Beweis:

Da $\mathbb{G}$ Abelsch ist, folgt

$$(a \circ b)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)} = (a^{\mathrm{ord}(a)})^{\mathrm{ord}(b)} \circ (b^{\mathrm{ord}(b)})^{\mathrm{ord}(a)} = 1.$$

Lemma 78 $\rightsquigarrow$ $\mathrm{ord}(a \circ b) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

Angenommen es gilt $\mathrm{ord}(a \circ b) < \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

Da $\mathrm{ord}(a \circ b)$ ein Teiler von $\mathrm{ord}(a) \cdot \mathrm{ord}(b)$ ist, gibt es eine Primzahl p mit

$$\mathrm{ord}(a \circ b) \mid \frac{\mathrm{ord}(a) \cdot \mathrm{ord}(b)}{p}. \tag{6}$$

Da $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, kann p nicht sowohl $\mathrm{ord}(a)$ als auch $\mathrm{ord}(b)$ teilen.

O.B.d.A. gelte: $p \mid \mathrm{ord}(a)$ und $p \nmid \mathrm{ord}(b)$.

Aus (6) und Lemma 78 folgt:

$$1 = (a \circ b)^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)/p} = a^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)/p} \circ (b^{\mathrm{ord}(b)})^{\mathrm{ord}(a)/p} = a^{\mathrm{ord}(a)\cdot\mathrm{ord}(b)/p}.$$

Lemma 78 $\rightsquigarrow$ $\mathrm{ord}(a) \mid \frac{\mathrm{ord}(a)\cdot\mathrm{ord}(b)}{p}$.

Da $p \nmid \mathrm{ord}(b)$ und $\mathrm{ggT}(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$ gilt, muss $\mathrm{ord}(a)$ bereits ein Teiler von $\mathrm{ord}(a)/p$ sein — ein Widerspruch. □

Lemma 80

Sei $\mathbb{G} = (G, \circ)$ eine endliche Abelsche Gruppe und sei $k = max\{ord(a) \mid a \in G\}$. Dann gilt für alle $b \in G$: $b^k = 1$.

Beweis: Sei die Ordnung von a maximal und sei $k = \mathrm{ord}(a)$.

Angenommen $b \in G$ ist ein Element mit $b^k \neq 1$. Sei $\ell = \mathrm{ord}(b) < k$.

Dann gilt $\ell \not| k$ (sonst würde $b^k = 1$ nach Lemma 78 gelten).

Also gibt es eine Primzahl p und ein $i \geq 0$ mit:

$$p^i \mid k, \quad p^{i+1} \not| k, \quad p^{i+1} \mid \ell.$$

Sei $a' = a^{p^i}$ und $b' = b^{\ell/p^{i+1}}$.

$\rightsquigarrow$ $\mathrm{ord}(a') = k/p^i$, $\mathrm{ord}(b') = p^{i+1}$ und somit $\mathrm{ggT}(\mathrm{ord}(a'), \mathrm{ord}(b')) = 1$

Lemma 79 $\rightsquigarrow$ $\mathrm{ord}(a' \circ b') = \mathrm{ord}(a') \cdot \mathrm{ord}(b') = k \cdot p > k$.

Dies ist ein Widerspruch. □

Beweis von Satz 77:

Wir wenden Lemma 80 auf die endliche Abelsche Gruppe $(K \setminus \{0\}, \cdot)$ an.

Sei $n = |K \setminus \{0\}| = |K| - 1$.

Um zu zeigen, dass $(K \setminus \{0\}, \cdot)$ zyklisch ist, genügt es ein Element $a \in K \setminus \{0\}$ der Ordnung n zu finden.

Denn dann sind die Potenzen $a^0, a^1, \ldots, a^{n-1}$ alle verschieden, und es gilt $K \setminus \{0\} = \{a^0, a^1, \ldots, a^{n-1}\}$.

Sei hierzu $k = \max\{\text{ord}(b) \mid b \in K \setminus \{0\}\}$ ($\rightsquigarrow$ $k \leq n$).

Nach Lemma 80 ist jedes Element $b \in K \setminus \{0\}$ Nullstelle des Polynoms $x^k - 1$.

Also hat das Polynom $x^k - 1$ genau n Nullstellen (beachte: 0 ist keine Nullstelle von $x^k - 1$).

Satz 65 $\rightsquigarrow$ $k \geq n$.

Also gilt $k = n$ und es gibt ein Element der Ordnung n. □

Beispiel:

Betrachte den Körper $\mathbb{F}_2[x]_{x^3+x^2+1}$, welcher aus den acht Elementen $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ besteht.

Die multiplikative Gruppe dieses Körpers ist isomorph zu $\mathbb{Z}_7$.

Ein primitives Element von $\mathbb{F}_2[x]_{x^3+x^2+1}$ ist z. B. x:

$$\begin{aligned} x^1 &= x \\ x^2 &= x^2 \\ x^3 &= x^2+1 \\ x^4 &= x^3+x = x^2+x+1 \\ x^5 &= x^3+x^2+x = x+1 \\ x^6 &= x^2+x \\ x^7 &= x^3+x^2 = 1 \end{aligned}$$

Bemerkungen zum Rechnen in dem endlichen Körper GF(2^m)

GF(2^m) ist isomorph zu $\mathbb{F}_2[x]_{q(x)}$, wobei $q(x) \in \mathbb{F}_2[x]$ ein irreduzibles Polynom vom Grad m ist.

Die Elemente von $\mathbb{F}_2[x]_{q(x)}$ sind also Polynome aus $\mathbb{F}_2[x]$ vom Grad $< m$ (kurz $\mathbb{F}_2[x]_m$).

Ein solches Polynom kann als Bitstring repräsentiert werden:

$$a_k x^k + \cdots a_1 x + a_0 \quad \text{entspricht} \quad (a_k \cdots a_1 a_0),$$

wobei $k < m$ und $a_k, \ldots, a_1, a_0 \in \{0, 1\}$.

Addition in $\mathbb{F}_2[x]_{q(x)}$ entspricht dann dem bitweisen XOR von Bitstrings.

Beispiel: Sei $q(x) = x^3 + x^2 + 1$ (irreduzibel in $\mathbb{F}_2[x]$).

Betrachte $x^2 + 1, x^2 + x \in \mathbb{F}_2[x]_3$.

$\rightsquigarrow (x^2 + 1) + (x^2 + x) = x + 1$ in $\mathbb{F}_2[x]_{q(x)}$.

Dies entspricht für Bitstrings: (101) XOR (110) = (011) = (11).

Algebraische Strukturen: Ringe und Körper

Die Multiplikation in $\mathbb{F}_2[x]_{q(x)}$ ist etwas komplizierter.

Betrachte $a(x) \in \mathbb{F}_2[x]_m$ und $b(x) = b_k x^k + \cdots + b_1 x + b_0 \in \mathbb{F}_2[x]_m$.

$$\rightsquigarrow \quad a(x) \cdot b(x) = (((a(x)b_k x + a(x)b_{k-1}) \cdot x + a(x)b_{k-2}) \cdots) \cdot x + a(x)b_0$$

Dies führt auf k Additionen und k Multiplikationen mit x sowie 0 bzw. 1.

Multiplikation mit x entspricht einem Linksshift für Bitstrings.

Multiplikation mit 1 bzw. 0 liefert den gleichen Bitstring bzw. den String 0 zurück.

Nach jeder Multiplikation mit x überprüfen wir, ob der Grad des resultierenden Polynoms m ist (d. h. ob der Bitstring Länge m hat).

Ist dies der Fall, so kann durch eine Addition von $q(x)$, d. h. einem XOR mit dem $q(x)$ entsprechenden Bitstring, der Grad wieder unter die Grenze m gebracht werden.

Beispiel: Sei wieder $q(x) = x^3 + x^2 + 1 = 1101$ (irreduzibel in $\mathbb{F}_2[x]$).

Betrachte $a(x) = x^2 + 1 = 101, b(x) = x^2 + x = 110 \in \mathbb{F}_2[x]_3$, d.h. $b_2 = b_1 = 1, b_0 = 0$.

Wir wollen $a(x) \cdot b(x)$ in $\mathbb{F}_2[x]_{q(x)}$ berechnen.

Es gilt $a(x) \cdot b(x) = (a(x) \cdot b_2 \cdot x + a(x) \cdot b_1) \cdot x + a(x) \cdot b_0$.

1. Multiplikation von $a(x) = 101$ mit $b_2 = 1 \rightsquigarrow 101$
2. Multiplikation mit x, d. h. Linkshift $\rightsquigarrow 1010$
3. Addition von $q(x)$, d. h. XOR mit 1101 $\rightsquigarrow$ 1010 XOR 1101 $= 111$
4. Addition von $a(x) \cdot b_1$, d. h. XOR mit 101 $\rightsquigarrow$ 101 XOR 111 $= 10$
5. Multiplikation mit x, d. h. Linkshift $\rightsquigarrow 100$
6. Addition von $a(x) \cdot b_0 = 0 \rightsquigarrow 100$

Also gilt $(x^2 + 1) \cdot (x^2 + x) = x^2$ in $\mathbb{F}_2[x]_{q(x)}$.

Kodierungstheorie

Wir wollen nun endliche Körper zur Erstellung von fehlerkorrigierenden Kodes verwenden.

Die Grundidee von fehlerkorrigierenden Kodes ist, an Nachrichten redundante Information anzuhängen.

Dies erlaubt es, Übertragungsfehler zu erkennen und evtl. sogar zu korrigieren.

Sei Σ ein endliches Alphabet von Symbolen.

Seien $k, n \geq 1$ mit $k \leq n$.

Ein (k, n)-Kode über dem Alphabet Σ ist eine injektive Abbildung $f : \Sigma^k \to \Sigma^n$.

Ein Wort $u \in \Sigma^k$ ist dabei eine zu versendende Nachricht, $f(u) \in \Sigma^n$ ist die tatsächlich versendete Nachricht.

Kodierungstheorie

Seien $u, v \in \Sigma^n$ zwei Wörter der gleichen Länge n.

Sei $u = a_1 a_2 \cdots a_n$ und $v = b_1 b_2 \cdots b_n$ mit $a_i, b_j \in \Sigma$.

Die Hamming-Distanz $d_H(u, v)$ zwischen u und v ist definiert als

$$d_H(u, v) = |\{i \mid 1 \leq i \leq n, a_i \neq b_i\}|.$$

Dies ist also die Anzahl aller Positionen, in denen sich u und v unterscheiden.

Definition (t-fehlerkorrigierende Kodes)

Sei f ein (k, n)-Kode über dem Alphabet Σ und sei $t \geq 0$.

Dann ist f t-fehlerkorrigierend, falls gilt:

$$\forall u, v \in \Sigma^k : u \neq v \implies d_H(f(u), f(v)) \geq 2t + 1.$$

Dieser Begriff ist wie folgt motiviert:

Sei f ein t-fehlerkorrigierender (k, n)-Kode über dem Alphabet Σ.

Sei $u \in \Sigma^k$.

Angenommen in $f(u) \in \Sigma^n$ werden an $\leq t$ vielen Positionen Änderungen vorgenommen ($\leq t$ viele Übertragungsfehler).

Für das resultierende Wort $w \in \Sigma^n$ gilt also $d_H(f(u), w) \leq t$.

Angenommen es gäbe noch ein weiteres Wort $v \in \Sigma^k \setminus \{u\}$ mit $d_H(f(v), w) \leq t$.

Dann würde $d_H(f(u), f(v)) \leq 2t$ gelten (Dreiecksungleichung), was aber nicht geht, da f t-fehlerkorrigierend ist.

Also ist u das einzige Wort in Σ^k mit $d_H(f(u), w) \leq t$.

Somit kann ein Dekodierer aus w die ursprüngliche Nachricht u rekonstruieren.

Definition (t-fehlererkennende Kodes)

Sei f ein (k, n)-Kode über dem Alphabet Σ und sei $t \geq 0$.

Dann ist f t-fehlererkennend, falls gilt:

$$\forall u, v \in \Sigma^k : u \neq v \implies d_H(f(u), f(v)) \geq t + 1.$$

Dieser Begriff ist wie folgt motiviert:

Sei f ein t-fehlererkennender (k, n)-Kode über dem Alphabet Σ und sei $u \in \Sigma^k$.

Angenommen in $f(u) \in \Sigma^n$ werden an $\leq t$ vielen Positionen Änderungen vorgenommen ($\leq t$ viele Übertragungsfehler).

Dann ist das resultierende Wort w nicht von der Form $f(v)$ mit $v \in \Sigma^k$, denn wäre dies der Fall, so würde $d_H(f(u), f(v)) \leq t$ gelten, und f wäre nicht t-fehlererkennend.

Ein Empfänger der Nachricht $f(u)$ kann somit zumindestens noch erkennen, dass ein Übertragungsfehler vorliegt.

Beachte: Ein t-fehlerkorrigierender Kode ist stets $2t$-fehlererkennend.

Beispiel:

Für $k, m \geq 1$ definieren wir einen $(k, m \cdot k)$-Kode $W_{k,m}$ über dem Alphabet $\{0, 1\}$ wie folgt:

$$W_{k,m}(u) = u^m \text{ für alle } u \in \{0,1\}^k.$$

Dann gilt $d_H(W_{k,m}(u), W_{k,m}(v)) \geq m$ für alle $u, v \in \{0,1\}^k$ mit $u \neq v$.

Für m ungerade ist $W_{k,m}$ somit $(m-1)/2$-fehlerkorrigierend.

Für alle $m \geq 1$ ist $W_{k,m}$ noch $(m-1)$-fehlererkennend.

Wir betrachten nun sogenannte Reed-Solomon Kodes.

Seien $s, k, t \geq 1$ Parameter, wobei $k + 2t \leq 2^s - 1$.

Der Reed-Solomon Kode $\mathrm{RS}_{s,k,t}$ ist ein $(k, 2t + k)$-Kode über dem endlichen Alphabet $\mathrm{GF}(2^s)$, d. h.

$$\mathrm{RS}_{s,k,t} : \mathrm{GF}(2^s)^k \to \mathrm{GF}(2^s)^{2t+k}.$$

Wie bereits gesehen, können wir Elemente des endlichen Körpers $\mathrm{GF}(2^s)$ mit Elementen aus $\{0,1\}^s$ identifizieren.

Nach Satz 77 ist die multiplikative Gruppe $(\mathrm{GF}(2^s) \setminus \{0\}, \cdot)$ zyklisch.

Sei $\alpha \in \mathrm{GF}(2^s) \setminus \{0\}$ ein Erzeuger dieser Gruppe.

Dann gilt $\alpha^i \neq 1$ für alle $1 \leq i \leq 2^s - 2$ und $\alpha^{2^s-1} = 1$.

Sei $g(x) = (x - \alpha) \cdot (x - \alpha^2) \cdots (x - \alpha^{2t}) \in \mathrm{GF}(2^s)[x]$.

$\rightsquigarrow$ $\mathrm{grad}(g(x)) = 2t$.

Sei nun $u = u_{k-1} \cdots u_1 u_0 \in \mathrm{GF}(2^s)^k$ die Eingabe für das Reed-Solomen Kodierungsverfahren, wobei $u_i \in \mathrm{GF}(2^s)$ für $0 \leq i \leq k-1$.

Sei $u(x)$ das Polynom $u(x) = u_{k-1}x^{k-1} + \cdots + u_1 x + u_0 \in \mathrm{GF}(2^s)[x]$.

$\rightsquigarrow$ $\mathrm{grad}(u(x)) \leq k-1$ (beachte: es könnte $u_{k-1} = 0$ sein).

Berechne aus $u(x)$ das Polynom $w(x) = g(x) \cdot u(x) \in \mathrm{GF}(2^s)[x]$.

$\rightsquigarrow$ $\mathrm{grad}(w(x)) = \mathrm{grad}(g(x)) + \mathrm{grad}(u(x)) \leq 2t + k - 1$.

Also können wir das Polynom $w(x)$ schreiben als

$$w(x) = w_{2t+k-1}x^{2t+k-1} + \cdots + w_1 x + w_0$$

(dabei können einige der führenden Koeffizienten w_i gleich 0 sein).

Dann ist $\mathrm{RS}_{s,k,t}(u) = w_{2t+k-1} \cdots w_1 w_0$, dies ist die Ausgabe des Reed-Solomon Kodierungsverfahren.

Lemma 81

Die Funktion $RS_{s,k,t} : GF(2^s)^k \to GF(2^s)^{2t+k}$ ist injektiv, d. h. $RS_{s,k,t}$ ist in der Tat ein $(k, 2t+k)$-Kode.

Beweis:

Sei $\mathrm{RS}_{s,k,t}(u) = \mathrm{RS}_{s,k,t}(v)$ für $u, v \in \mathrm{GF}(2^s)^k$.

$\rightsquigarrow \quad g(x) \cdot u(x) = g(x) \cdot v(x)$

$\rightsquigarrow \quad g(x) \cdot (u(x) - v(x)) = 0.$

Da $g(x) \neq 0$ gilt, und der Ring $\mathrm{GF}(2^s)[x]$ nullteilerfrei ist (siehe Folie 148), folgt $u(x) - v(x) = 0$, d. h. $u(x) = v(x)$.

Also gilt $u = v$. □

Um aus $\mathrm{RS}_{s,k,t}(u)$ die ursprüngliche Nachricht u zu berechnen (dekodieren) müssen wir lediglich das Polynom, dass zu $\mathrm{RS}_{s,k,t}(u)$ gehört, durch $g(x)$ teilen.

Beispiel: Sei $s = 3$, $k = 3$, $t = 2$, dann gilt $k + 2t = 4 \leq 2^3 - 1$.

Es gilt $\mathrm{GF}(8) = \mathbb{F}_2[x]_{x^3+x+1}$ und $\alpha = x$ ist ein primitives Element.

Eine einfache Rechnung in $\mathbb{F}_2[x]_{x^3+x+1}$ zeigt, dass

$$\begin{aligned} g(y) &= (y-x)(y-x^2)(y-x^3)(y-x^4) \\ &= (y+x)(y+x^2)(y+x^3)(y+x^4) \\ &= (y+x)(y+x^2)(y+x+1)(y+x^2+x) \\ &= y^4 + (x+1)y^3 + y^2 + xy + (x+1). \end{aligned}$$

Sei nun $u = 101\ 100\ 001 \in \mathrm{GF}(8)^3$.

$\rightsquigarrow\ u(y) = (x^2+1)y^2 + x^2y + 1.$

Eine einfache Rechnung in $\mathbb{F}_2[x]_{x^3+x+1}$ zeigt, dass $g(y) \cdot u(y)$ das folgende Polynom ist:

$$(x^2+1)y^6 + (x+1)y^4 + (x^2+x)y^3 + (x^2+x)y^2 + (x^2+1)y + (x+1).$$

$\rightsquigarrow\ \mathrm{RS}_{s,k,t}(u) = 101\ 000\ 011\ 110\ 110\ 101\ 011 \in \mathrm{GF}(8)^7.$

Satz 82

Seien $s, k, t \geq 1$ mit $k + 2t \leq 2^s - 1$. Dann ist $RS_{s,k,t}$ ein t-fehlerkorrigierender $(k, k + 2t)$-Kode über dem Alphabet $GF(2^s)$.

Beweis:

Annahme: $d_H(\mathrm{RS}_{s,k,t}(u), \mathrm{RS}_{s,k,t}(v)) = r \leq 2t$ für $u, v \in \mathrm{GF}(2^s)^k$.

Wir müssen $u = v$ zeigen.

Sei $u = u_{k-1} \cdots u_1 u_0$ und $v = v_{k-1} \cdots v_1 v_0$ mit $u_i, v_i \in \mathrm{GF}(2^s)$.

Definiere:

$$\begin{aligned} u(x) &= u_{k-1}x^{k-1} + \cdots + u_1 x + u_0 \in \mathrm{GF}(2^s)[x] \\ v(x) &= v_{k-1}x^{k-1} + \cdots + v_1 x + v_0 \in \mathrm{GF}(2^s)[x] \\ g(x) &= (x - \alpha) \cdot (x - \alpha^2) \cdots (x - \alpha^{2t}) \in \mathrm{GF}(2^s)[x], \end{aligned}$$

wobei α ein primitives Element von $\mathrm{GF}(2^s)$ ist.

Dann ist $\mathrm{RS}_{s,k,t}(u)$ (bzw. $\mathrm{RS}_{s,k,t}(v)$) die Folge der Koeffizienten des Polynoms $g(x) \cdot u(x)$ (bzw. $g(x) \cdot v(x)$).

Sei $d(x) = g(x) \cdot u(x) - g(x) \cdot v(x) = g(x) \cdot (u(x) - v(x))$.

Dann gilt:

(1) Wegen $d_H(\mathrm{RS}_{s,k,t}(u), \mathrm{RS}_{s,k,t}(v)) = r \leq 2t$ sind in $d(x)$ nur $r \leq 2t$ viele Koeffizienten von 0 verschieden.

Sei $d(x) = d_{2t+k-1}x^{2t+k-1} + \cdots + d_1 x + d_0$, wobei alle Koeffizienten d_i ausser $d_{i_1}, \ldots, d_{i_r}$ $(r \leq 2t)$ gleich 0 sind.

Sei $0 \leq i_1 < i_2 < \cdots i_r \leq 2t + k - 1$.

(2) Aus $\forall 1 \leq j \leq 2t : g(\alpha^j) = 0$ folgt $\forall 1 \leq j \leq 2t : d(\alpha^j) = 0$.

Also gilt für alle $1 \leq j \leq 2t$:

$$\begin{aligned} d_{2t+k-1}\alpha^{j(2t+k-1)} + \cdots + d_1\alpha^j + d_0 &= 0 \quad \text{bzw.} \\ d_{i_r}\alpha^{j \cdot i_r} + \cdots + d_{i_1}\alpha^{j \cdot i_1} + d_{i_0}\alpha^{j \cdot i_0} &= 0 \end{aligned}$$

Punkt (2) können wir in Matrixform wie folgt schreiben:

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \cdots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \alpha^{2i_3} & \cdots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \alpha^{3i_3} & \cdots & \alpha^{3i_r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{2t\cdot i_1} & \alpha^{2t\cdot i_2} & \alpha^{2t\cdot i_3} & \cdots & \alpha^{2t\cdot i_r} \end{pmatrix} \cdot \begin{pmatrix} d_{i_1} \\ d_{i_2} \\ d_{i_3} \\ \vdots \\ d_{i_r} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Aus der linearen Algebra folgt, dass für die Determinante der sogenannten Vandermonde-Matrix gilt:

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_m \\ x_1^2 & x_2^2 & \cdots & x_m^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{m-1} & x_2^{m-1} & \cdots & x_m^{m-1} \end{pmatrix} = \prod_{1 \leq i < j \leq m} (x_j - x_i)$$

Hierbei sind die Einträge $x_1, \ldots, x_m$ aus einem beliebigen Körper $\mathbb{K}$.

Gilt daher $x_j \neq x_i$ für alle $1 \leq i < j \leq m$, so ist die Determinante der Vandermonde-Matrix von Null verschieden (hier ist wieder die Nullteilerfreiheit von Körpern wichtig).

Gilt also $x_j \neq x_i$ für alle $1 \leq i < j \leq m$, so sind die m vielen Spaltenvektoren

$$\begin{pmatrix} 1 \\ x_i \\ x_i^2 \\ \vdots \\ x_i^{m-1} \end{pmatrix} \quad \text{für} \quad 1 \leq i \leq m$$

linear unabhängig.

Gilt weiterhin $x_i \neq 0$ für alle $1 \leq i \leq m$, so sind auch die folgenden m vielen Spaltenvektoren linear unabhängig:

$$\begin{pmatrix} x_i \\ x_i^2 \\ x_i^3 \\ \vdots \\ x_i^m \end{pmatrix} = x_i \cdot \begin{pmatrix} 1 \\ x_i \\ x_i^2 \\ \vdots \\ x_i^{m-1} \end{pmatrix} \quad \text{für} \quad 1 \leq i \leq m$$

Natürlich ist dann auch jede Teilmenge dieser m vielen Vektoren linear unabhängig.

Dies wollen wir nun auf die folgende Matrix anwenden:

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \alpha^{2i_3} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \alpha^{3i_3} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{2t\cdot i_1} & \alpha^{2t\cdot i_2} & \alpha^{2t\cdot i_3} & \dots & \alpha^{2t\cdot i_r} \end{pmatrix} \tag{7}$$

Zur Erinnerung: $r \leq 2t$, $0 \leq i_1, \dots, i_r \leq 2t + k - 1$ und diese Zahlen sind paarweise verschieden.

Da α ein primitives Element von GF(2^s) ist (d. h. $\alpha^i \neq 1$ für alle $1 \leq i \leq 2^s - 2$ und $\alpha^{2^s-1} = 1$) gilt $\alpha^i \neq 0$ für alle i und $\alpha^i \neq \alpha^j$ für alle $0 \leq i < j \leq 2t + k - 1 \leq 2^s - 2$.

Also sind die Spaltenvektoren der Matrix (7) linear unabhängig.

Dies scheint jedoch dem Gleichungssystem

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \alpha^{i_3} & \cdots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \alpha^{2i_3} & \cdots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \alpha^{3i_3} & \cdots & \alpha^{3i_r} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{2t\cdot i_1} & \alpha^{2t\cdot i_2} & \alpha^{2t\cdot i_3} & \cdots & \alpha^{2t\cdot i_r} \end{pmatrix} \cdot \begin{pmatrix} d_{i_1} \\ d_{i_2} \\ d_{i_3} \\ \vdots \\ d_{i_r} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

zu widersprechen!

Tut es aber nicht, es folgt lediglich, dass $r = 0$ gelten muss.

Also gilt $d_H(\mathrm{RS}_{s,k,t}(u), \mathrm{RS}_{s,k,t}(v)) = 0$, d. h. $\mathrm{RS}_{s,k,t}(u) = \mathrm{RS}_{s,k,t}(v)$.

Da $\mathrm{RS}_{s,k,t}$ injektiv ist, folgt $u = v$. □

Bemerkungen

- Das Reed-Solomon Kodierungsverfahren wird z. B. für CDs und DVDs verwendent.
- In Implementierungen des Reed-Solomon Kodierungsverfahren werden Elemente aus $\mathrm{GF}(2^s)$ durch Bitstrings aus $\{0,1\}^s$ repräsentiert, so wie wir dies auch schon früher getan haben.
- Man kann sich also $\mathrm{RS}_{s,k,t}$ als $(k \cdot s, (2t+k) \cdot s)$-Kode über $\{0,1\}$ (anstatt als $(k, 2t+k)$-Kode über $\mathrm{GF}(2^s)$) vorstellen.
- Welchen Vorteil hat nun ein größerer Parameter s?

  Ein Fehlerburst der Länge ℓ ist eine Folge von ℓ fehlerhaften Bits (z. B. verursacht durch einen Kratzer auf einer CD).

  Das folgende Beispiel stammt aus *Steger, Diskrete Strukturen 1. Kombinatorik, Graphentheorie, Algebra, Springer.*
  Wieviele Bits benötigen wir, um 10^6 Bits so zu kodieren, dass Fehlerbursts der Länge 100 korrigiert werden können?

Kodierungstheorie

- Ein Feherbursts der Länge 100 betrifft höchstens $\lceil 100/s \rceil$ viele Blöcke der Länge s.
- Also muss $t \geq \lceil 100/s \rceil$ gelten. Setzen wir $t = \lceil 100/s \rceil$.
- Mit $2t + k \leq 2^s - 1$ folgt $k \leq 2^s - 1 - 2\lceil 100/s \rceil$.

  Setzen wir $k = 2^s - 1 - 2\lceil 100/s \rceil$.
- Zur Kodierung werden die 10^6 Bits in $\lceil 10^6/(k \cdot s) \rceil$ viele Blöcke der Länge $k \cdot s$ zerlegt.

  Jeder dieser Blöcke wird dann mit $(2t + k) \cdot s$ vielen Bits kodiert.
- Die Anzahl der insgesamt benötigten Bits ist also

  $$\lceil 10^6/(k \cdot s) \rceil \cdot (2t + k) \cdot s = \lceil 10^6/((2^s - 1 - 2\lceil 100/s \rceil) \cdot s) \rceil (2^s - 1) \cdot s.$$

  Für $s = 6$ liefert dies z. B. 2 172 744 Bits, während wir für $s = 10$ mit nur 1 023 000 Bits auskommen.
- Der Nachteil eines größeren s-Werts ist, dass die Arithmetik in $\mathrm{GF}(2^s)$ aufwändiger wird.