

Mathematik I für Studierende der Informatik

– Diskrete Mathematik –

Mathias Schacht

Fachbereich Mathematik
Universität Hamburg

WiSe 2024/25

Stand: 7. April 2025

Termine

Vorlesung Mi 10:15 – 11:45 Audimax 2 (VMP 4)
 Do 10:15 – 11:45 Audimax 2 (VMP 4)

Übung

- 12 Gruppen (Zuordnung über STiNE)
- Do 12-14 und Do 14-16 (jeweils eine Gruppe auf Englisch)
- 45 Minuten Hausaufgabenbesprechung
- 45 Minuten Präsenzübung
- **Beginn morgen**

Tutorium

- 2 reguläre Termine
- Di 16-18 und Do 16-18
- **Beginn am 22./24.10.**

- **Probeklausur:** im Semester während der VL am Do 05.12.24
- **Klausurtermine:** 1. Termin Do 06.02.25, 11-14 Uhr
 2. Termin Do 27.03.25, 09-12 Uhr

Spielregeln

Übungsblätter

- wöchentliche Aus- und schriftliche Abgabe in den Übungsgruppen
- Abgabe in bis zu 3er Gruppen (kleinere Gruppen erlaubt)
- bestehend aus 3 Teilen:
 - **Präsenzaufgaben:** Bearbeitung und Besprechung in der gleichen Übung
 - **Formaler Teil:** konzeptionelle, mathematische Hausaufgaben (Beweise)
 - **Allgemeiner Teil:** Hausaufgaben mit Fokus auf Aufwendung der Inhalte
- **Zulassungskriterium** für die Klausur ist das Erreichen von:
 - mindestens 50% aller Punkte im formalen Teil über alle Übungsblätter
 - **und** mindestens 50% aller Punkte (formaler und allgemeiner Teil zusammen) über alle Übungsblätter

Klausur

- zwei mögliche Termine in der vorlesungsfreien Zeit
- Ergebnis der Probeklausur wird positiv angerechnet
- Klausurergebnis entspricht der Modulnote Mafl1
→ Abschneiden bei den UE-Blättern nur für die Teilnahme wichtig

Weitere Informationen

Moodle-Seite

- Skript, UE-Blätter, UE-Gruppenverwaltung:

<https://lernen.min.uni-hamburg.de/course/view.php?id=4846>

Wichtige Ankündigungen

- E-Mailverteiler in STiNE an die dort hinterlegten E-Mailadressen:

`vorname.nachname@studium.uni-hamburg.de`

Fragen

- Inhaltlich:

→ Tutorium (Can Turan), UE-Leiter

- UE-Blätter/Korrektur:

→ UE-Leiter

- Moodle/Klausuranmeldung/Fehler auf UE-Blatt:

→ Stefan Geschke

- Sonstiges:

→ Mathias Schacht

1. Mathematische Grundlagen und Logik

Naive Mengenlehre

Fragen im 19. Jahrhundert:

- Was sind die Grundlagen der Mathematik/Arithmetik?
- Was sind Zahlen? Was sind Mengen? Darf es unendliche Mengen geben?

Idee/Definition (Ende 19. Jahrhundert, CANTOR 1895)

Mengen sind ungeordnete Zusammenfassungen von wohlunterschiedenen Objekten (unseres Denkens) zu einem Ganzen.

Beispiele: $\{10^{10}, 1, \pi, 19, 2001\}$, Menge der natürlichen Zahlen, $\{A, x, 1, B\}$

Definition (FREGE 1893)

Für jedes sprachliche Prädikat P gibt es die **Menge** M_P aller der Objekte O , auf die das Prädikat P zutrifft

$$M_P = \{O : P(O) \text{ gilt}\}.$$

Objekte O für die $P(O)$ gilt, heißen **Elemente von** M_P

$$O \in M_P.$$

RUSSELS Paradoxon

Antinomie (RUSSEL 1903)

Sei P das Prädikat „ x enthält sich nicht selbst als Element“, d. h.

$$M_P := \{O : P(O) \text{ gilt}\} = \{O : O \notin O\}.$$

Widerspruch: $M_P \notin M_P$ genau dann, wenn $M_P \in M_P$.

Beweis: Auf der einen Seite erhalten wir

$$\begin{aligned} M_P \notin M_P &\stackrel{\text{Def.}\notin}{\implies} M_P \text{ enthält sich nicht selbst als Element} \\ &\stackrel{\text{Def.}P}{\implies} P(M_P) \text{ gilt} \stackrel{\text{Def.}M_P}{\implies} M_P \in M_P \end{aligned} \quad \downarrow$$

und auf der anderen Seite erhalten wir

$$\begin{aligned} M_P \in M_P &\stackrel{\text{Def.}\in}{\implies} M_P \text{ enthält sich selbst als Element} \\ &\stackrel{\text{Def.}P}{\implies} P(M_P) \text{ gilt nicht} \stackrel{\text{Def.}M_P}{\implies} M_P \notin M_P \end{aligned} \quad \downarrow \quad \square$$

$\implies M_P$ kann nicht existieren

Freges Ansatz ist nicht **widerspruchsfrei!**

Auflösung des Paradoxons

Probleme in FREGES Definition:

- Was ist ein Prädikat? Wann ist ein Prädikat „wahr“, wann „gilt“ es?
- Was sind Objekte? Gibt es eine „Grundmenge“ aller Objekte?

Ausweg:

- Formalisierung mathematischer Sprache (**Aussagen**) und **Regeln**
→ mathematische Logik
- Benennung als wahr angenommener Grundaussagen (**Axiome**)
→ axiomatische Mengenlehre
- der Wahrheitswert **aller** anderen **Aussagen** wird formal mit Hilfe der **Regeln**
aus den **Axiomen** hergeleitet (**Beweis**) → Mathematik

Probleme:

- (innere) Widerspruchsfreiheit der Regeln und Axiome unentscheidbar
- Vollständigkeit – Sind alle wahren Aussagen beweisbar? **Nein**, GÖDEL

Bemerkungen

- Standardaxiomensystem benannt nach ZERMELO und FRAENKEL
- hinzu kommt oft das sogenannte **Auswahlaxiom (Axiom of Choice)**
→ ZFC-Axiome
- Axiome etablieren Grundmengen und zulässige Operationen, um aus bestehenden Mengen weitere Mengen abzuleiten
- Großteil der Mathematik kann innerhalb **ZFC** bewiesen werden
- Innerhalb von ZFC lassen sich die *üblichen* Zahlenmengen

\mathbb{N} = Menge der natürlichen Zahlen,

\mathbb{Z} = Menge der ganzen Zahlen,

\mathbb{Q} = Menge der rationalen Zahlen,

\mathbb{R} = Menge der reellen Zahlen,

\mathbb{C} = Menge der komplexen Zahlen

definieren und Aussagen darüber beweisen.

- 1 Existenz der leeren Menge:** Es existiert eine Menge, die kein Element enthält.

$$(\exists x)(\forall y)(y \notin x)$$

- 2 Extensionalitätsaxiom:** Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.

$$(\forall x)(\forall y)\left((x = y) \Leftrightarrow \left((\forall z)((z \in x) \Leftrightarrow (z \in y))\right)\right)$$

- 3 Paarmengenaxiom:** Für je zwei Mengen A, B existiert die Menge $\{A, B\}$.

$$(\forall x)(\forall y)(\exists z)(\forall u)\left((u \in z) \Leftrightarrow ((u = x) \vee (u = y))\right)$$

- 4 Vereinigungsmengenaxiom:** Für jede Menge A gibt es eine Menge $\bigcup A$, deren Elemente die Elemente der Elemente von A sind.

$$(\forall x)(\exists y)(\forall z)\left((z \in y) \Leftrightarrow ((\exists u)((u \in x) \wedge (z \in u)))\right)$$

- 5 Potenzmengenaxiom:** Für jede Menge A existiert die **Potenzmenge** $\wp(A)$, die alle Teilmengen von A als Elemente enthält.

$$(\forall x)(\exists y)(\forall z)\left((z \in y) \Leftrightarrow ((\forall u \in z)(u \in x))\right)$$

- 6 Aussonderungsaxiom:** Für jede Menge A und jede Aussageform $p(x)$ existiert die Menge $\{A' \in A : p(A')\}$, die Teilmenge von A deren Elemente $p(x)$ erfüllen.

$$(\forall x)(\exists y)(\forall z)\left((z \in y) \Leftrightarrow (z \in x \wedge p(z))\right)$$

- 7 Unendlichkeitsaxiom:** Es gibt eine Menge N , die die leere Menge als Element enthält und für jede Menge A , die ein Element von N ist, auch den **Nachfolger** $A^+ := A \cup \{A\}$ in N als Element enthält.

$$(\exists x) \left((\emptyset \in x) \wedge (\forall y \in x) ((y \cup \{y\}) \in x) \right)$$

- 8 Ersetzungsaxiom:** Das „Bild einer Menge unter einer Funktion“ ist eine Menge. Für jede Aussagenform $p(x, y)$ mit der Eigenschaft, dass für jede Menge A **genau eine** Menge B existiert, für die $p(A, B)$ gilt und für jede Menge M ist die Zusammenfassung der N' , für die eine $N \in M$ mit $p(N, N')$ existiert, eine Menge.

$$(\forall x)(\exists y)(\forall z)((z \in y) \Leftrightarrow ((\exists u \in x)p(u, z)))$$

- 9 Fundierungsaxiom:** Jede nicht leere Menge A enthält ein Element A' , deren Schnitt mit A leer ist.

$$((\forall x)(x \neq \emptyset)) \Rightarrow ((\exists y \in x)(\forall z \in y)(z \notin x))$$

- 10 Auswahlaxiom:** Für jede nicht leere Menge A bestehend aus paarweise disjunkten nicht leeren Mengen existiert eine Menge B , die aus jeder Menge $A' \in A$ genau ein Element enthält.

$$\begin{aligned} (\forall x) \left(((\forall y \in x)(y \neq \emptyset)) \wedge (\forall y \in x)(\forall z \in x)((y \neq z) \Rightarrow (y \cap z = \emptyset)) \right) \\ \Rightarrow (\exists u)(\forall y \in x)(\exists! z \in y)(z \in u) \end{aligned}$$

Hierbei steht $\exists!$ für „es existiert genau ein“, d. h. $(\exists! x)p(x)$ ist genau dann **wahr**, wenn die Aussage $(\exists x)(p(x) \wedge (\forall y)((y \neq x) \Rightarrow \neg p(y)))$ wahr ist.

Mengen

- Angabe der Axiome in dieser VL nur zur Kenntnisnahme
→ explizit **nicht** klausurrelevant
- in dieser VL reicht der folgende intuitive Mengenbegriff von CANTOR

Definition (Mengen)

Eine **Menge** ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte, die die **Elemente** der Menge genannt werden.

- Vermeidung des RUSSELSchen Paradoxon wird dadurch erreicht, dass in Mengendefinitionen jeweils eine **Grundmenge** angegeben werden muss

$$M = \{x \in X : x \text{ erfüllt } \dots\}$$

und die „Menge aller Mengen“ **keine** Menge ist.

- Außerdem gibt es keine Mengen, die sich selbst als Element enthalten.

Mengenlehre

- Mengen sind **ungeordnet**, d. h. Elemente haben keine Reihenfolge
 - Elemente können **nicht mehrfach** in Mengen vorkommen
- ⇒ jede Menge ist eindeutig durch ihre Elemente bestimmt und zwei Mengen sind **gleich**, wenn sie dieselben Elemente enthalten

$$\{x, y, z\} = \{y, z, x\} = \{y, z, x, x, z\}$$

- $x \in M$ steht für „ x ist ein Element der Menge M “
- $B \subseteq A$ steht für „die Menge B enthält nur Elemente aus A “
→ B ist eine **Teilmenge** von A
- \emptyset (auch $\{\}$) steht für die **leere Menge**, die Menge ohne Elemente

Beispiel

$$M = \{m, n, o\}, \quad N_1 = \{a, b, \dots, z\}, \quad N_2 = \{\{a, b, c\}, \{b, c, d\}, \dots, \{x, y, z\}\}$$

Dann gilt:

$$\emptyset \neq M \subseteq N_1, \quad M \notin N_1, \quad M \not\subseteq N_2 \quad \text{und} \quad M \in N_2.$$

Aussagenlogik

Definition (Aussagen)

Aussagen sind Zeichenfolgen (Ausdrücke) bestehend aus (u. U. verzierten) lateinischen, griechischen, hebräischen, ... Buchstaben (Bezeichner) und Symbolen $(,), \{, \},$ usw., $\emptyset, \in, \subseteq, =, :, \neg, \vee, \wedge, \Rightarrow, \Leftrightarrow,$ und xor.

Hierbei liest man „:“ als „*so dass*“ und

\neg als *nicht ...*, xor als *entweder ..., oder ...*,

\vee als *... oder ...*, \wedge als *... und ...*,

\Rightarrow als *wenn ..., dann ...*, \Leftrightarrow als *... genau dann, wenn ...*.

- Für je zwei Mengen A und B sind die Ausdrücke „ $A \in B$ “ und „ $A \subseteq B$ “ **primitive Aussagen**.
- Für zwei Aussagen p und q sind „ $\neg p$ “, „ $p \text{ xor } q$ “, „ $p \vee q$ “, „ $p \wedge q$ “, „ $p \Rightarrow q$ “ und „ $p \Leftrightarrow q$ “ **zusammengesetzte Aussagen**.

Bemerkung

- Etwas allgemeiner gefasst ist eine Aussage ein Satz, für den man im Prinzip eindeutig feststellen kann, ob er **wahr** oder **falsch** ist.

Verknüpfte Aussagen

Definition (Zusammengesetzte Aussagen)

Für Aussagen p und q nennt man

$\neg p$	die Negation von p	nicht p
$p \text{ xor } q$	die ausschließende Disjunktion von p und q	entweder p oder q
$p \vee q$	die Disjunktion von p und q	p oder q
$p \wedge q$	die Konjunktion von p und q	p und q
$p \Rightarrow q$	die Implikation von p nach q	wenn p , dann q
$p \Leftrightarrow q$	die Äquivalenz von p und q	p genau dann, wenn q

und diese Aussagen heißen **zusammengesetzte Aussagen**.

- **xor** heißt auch **exklusives Oder** bzw. **ausschließendes Oder**
- an Stelle von \Rightarrow und \Leftrightarrow benutzt man auch \rightarrow und \leftrightarrow
- für $p \Rightarrow q$ sagt man auch **p impliziert q** bzw. **q folgt aus p**

Wahrheitsgehalt von Aussagen

- *Primitive Aussagen* der Form „ $a \in A$ “ (bzw. „ $A \subseteq B$ “) sind **wahr**, wenn a , A und B in der Beziehung $a \in B$ (bzw. $A \subseteq B$) stehen und ansonsten sind sie **falsch**.
- Für aus Aussagen p und q *zusammengesetzte Aussagen* gilt:

$$\neg p \text{ ist } \begin{cases} \text{wahr} & \text{wenn } p \text{ falsch ist,} \\ \text{falsch} & \text{sonst, d. h. wenn } p \text{ wahr ist,} \end{cases}$$
$$p \text{ xor } q \text{ ist } \begin{cases} \text{wahr} & \text{wenn genau eine der Aussagen } p \text{ oder } q \text{ wahr ist,} \\ \text{falsch} & \text{sonst, d. h. wenn beide Aussagen } p \text{ und } q \text{ wahr oder falsch sind,} \end{cases}$$
$$p \vee q \text{ ist } \begin{cases} \text{wahr} & \text{wenn mindestens eine der Aussagen } p \text{ oder } q \text{ wahr ist,} \\ \text{falsch} & \text{sonst, d. h. wenn keine der Aussagen } p \text{ und } q \text{ wahr ist,} \end{cases}$$
$$p \wedge q \text{ ist } \begin{cases} \text{wahr} & \text{wenn beide Aussagen } p \text{ und } q \text{ wahr sind,} \\ \text{falsch} & \text{sonst, d. h. wenn höchstens eine der Aussagen } p, q \text{ wahr ist,} \end{cases}$$
$$p \Rightarrow q \text{ ist } \begin{cases} \text{wahr} & \text{wenn } q \text{ wahr ist oder wenn } p \text{ falsch ist,} \\ \text{falsch} & \text{sonst, d. h. wenn } p \text{ wahr und } q \text{ falsch ist,} \end{cases}$$
$$p \Leftrightarrow q \text{ ist } \begin{cases} \text{wahr} & \text{wenn } p \text{ und } q \text{ beide wahr oder wenn beide falsch sind,} \\ \text{falsch} & \text{sonst, d. h. wenn } p \text{ und } q \text{ unterschiedliche W'werte haben.} \end{cases}$$

- **wahr** wird oft durch **w**, **1** und **falsch** durch **f**, **0** abgekürzt

Wahrheitstafeln

- Wahrheitswerte zusammengesetzter Aussagen lassen sich einfach über **Wahrheitstafeln** darstellen

p	q	$\neg p$	$\neg q$	$p \text{ xor } q$	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	1	1	0	0	0	1	1
0	1	1	0	1	1	0	1	0
1	0	0	1	1	1	0	0	0
1	1	0	0	0	1	1	1	1

Mit Wahrheitstafeln kann man leicht folgende Aussagen beweisen:

Satz

Für Aussagen p , q und q' gilt

- $\neg(\neg p)$ ist äquivalent zu p (doppelte Negation)
- $\neg(p \text{ xor } q)$ ist äquivalent zu $p \Leftrightarrow q$
- $p \wedge (q \vee q')$ ist äquivalent zu $(p \wedge q) \vee (p \wedge q')$ (Distributivität)
- $p \Rightarrow q$ ist äquivalent zu $(\neg q) \Rightarrow (\neg p)$ (Kontraposition)

Distributivgesetz: $p \wedge (q \vee q') \Leftrightarrow (p \wedge q) \vee (p \wedge q')$

Beweis (mit Wahrheitstafeln)

p	q	q'	$q \vee q'$	$p \wedge (q \vee q')$	$p \wedge q$	$p \wedge q'$	$(p \wedge q) \vee (p \wedge q')$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1



Reductio ad absurdum

Widerspruchsbeweis bzw. indirekter Beweis

Mit Hilfe der Kontraposition kann eine Aussage p durch **Widerspruch** bewiesen werden. Dafür muss für eine bekannte **falsche** Aussage q die Implikation

$$(\neg p) \Rightarrow q$$

bewiesen werden, d. h. man beweist die Richtigkeit der Aussage
„wenn p falsch ist, dann ist q wahr.“

Da q aber falsch ist, kann p somit nicht falsch sein, also muss p wahr sein.

Bsp.: $p =$ „ $\sqrt{2}$ ist irrational“ und $q =$ „es gibt teilerfremde a, b für die a/b kürzbar ist“

- q ist offensichtlich falsch
- Angenommen $\neg p$ ist wahr $\Rightarrow \sqrt{2} = a/b$ für teilerfremde natürliche Zahlen a, b
 $\Rightarrow 2b^2 = a^2 \Rightarrow 2$ teilt a^2
 \Rightarrow da 2 eine Primzahl ist, teilt 2 somit auch a , d. h. $a = 2a_1$ für geeignetes a_1
 $\Rightarrow 2b^2 = a^2 = 4a_1^2 \Rightarrow b^2 = 2a_1^2 \Rightarrow 2$ teilt $b^2 \Rightarrow 2$ teilt b , d. h. $b = 2b_1$
 $\Rightarrow a/b = (2a_1)/(2b_1) = a_1/b_1 \Rightarrow q$ ist wahr $\quad \Downarrow$
- Also muss $\neg p$ falsch sein und somit ist p wahr, d. h. $\sqrt{2}$ ist irrational □

Aussageformen

Definition (Aussageform)

Eine **Aussageform** ist eine Aussage, in der eine Konstante durch eine **freie Variable** ersetzt wurde. So erhält man aus einer Aussage p eine Aussageform $p(x)$.

Beispiel

Sei $p(x)$ die Aussageform „ x ist gerade“ und $q(x)$ die Form „ x^2 ist durch 4 teilbar“.

- $p(x) \Rightarrow q(x)$ bedeutet „**wenn** x gerade ist, **dann** ist x^2 durch 4 teilbar“
wahr für natürliche Zahlen x
- $q(x) \Rightarrow p(x)$ bedeutet „**wenn** x^2 durch 4 teilbar ist, **dann** ist x gerade“
wahr für natürliche Zahlen x

Für natürliche Zahlen x gilt also

$p(x) \Leftrightarrow q(x)$, „ x ist **genau dann** gerade, **wenn** x^2 durch 4 teilbar ist“

Quantoren: Allquantor \forall und Existenzquantor \exists

Definition (Allaussagen und Existenzaussagen)

Sei $p(x)$ eine Aussageform und M eine Menge. Dann ist

- $(\forall x \in M)p(x)$ eine Aussage – **Allaussage** „für alle x in M gilt $p(x)$ “
- $(\exists x \in M)p(x)$ eine Aussage – **Existenzaussage** „es gibt ein x in M , so dass $p(x)$ gilt“

Die freie Variable x in $p(x)$ heißt dann **gebundene Variable** in der All-/Existenzaussage.

In All-/Existenzaussagen kann durch Einführung neuer Variablen eine neue Aussageform gebildet werden, die durch weitere Quantoren wieder gebunden werden können.

Definition (Wahrheitswerte von All- und Existenzaussagen)

Für eine Aussageform $p(x)$ und eine Menge M gilt:

$$\begin{aligned} (\forall x \in M)p(x) \text{ ist } & \begin{cases} \text{wahr} & \text{wenn } p(x) \text{ für jedes } x \in M \text{ wahr ist} \\ \text{falsch} & \text{sonst, d. h. wenn es ein } x \in M \text{ gibt, für das } p(x) \text{ falsch ist,} \end{cases} \\ (\exists x \in M)p(x) \text{ ist } & \begin{cases} \text{wahr} & \text{wenn es ein } x \in M \text{ gibt, so dass } p(x) \text{ wahr ist} \\ \text{falsch} & \text{sonst, d. h. } p(x) \text{ ist falsch für jedes } x \in M. \end{cases} \end{aligned}$$

$$\neg((\forall x \in M)p(x)) \Leftrightarrow ((\exists x \in M) \neg p(x)), \quad \neg((\exists x \in M)p(x)) \Leftrightarrow ((\forall x \in M) \neg p(x))$$

Mengenoperationen

Definition

Seien A und B Mengen, dann ist

- $A \cup B := \{x: x \in A \vee x \in B\}$ die **Vereinigung** von A und B ,
- $A \cap B := \{x: x \in A \wedge x \in B\}$ der **Schnitt** von A und B ,
- $A \setminus B := \{x: x \in A \wedge x \notin B\}$ die **Differenz** A ohne B ,
- $\wp(A) := \{x: x \subseteq A\}$ die **Potenzmenge** von A .

Für eine feste Grundmenge M mit $A \subseteq M$, ist

$$\bar{A} := M \setminus A = \{x \in M: x \notin A\}$$

das **Komplement** von A in M .

- mengentheoretische \cup (bzw. \cap) „entspricht“ logischem \vee (bzw. \wedge)
- Potenzmenge wird auch mit $\mathcal{P}(A)$, 2^A , $\mathbb{P}(A)$, $\text{pow}(A)$ bezeichnet
- $\wp(\emptyset) = \{\emptyset\} \neq \emptyset$ und $\wp(\wp(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
- $\emptyset \in \wp(A)$ für jede Menge A , da $\emptyset \subseteq A$ für jede Menge A
- $\overline{(\bar{A})} = \bar{\bar{A}} = \overline{M \setminus A} = M \setminus (M \setminus A) = A$ für jede Menge $A \subseteq M$

Distributivitätsgesetz für Mengen

Satz

Für beliebige Mengen $A, B, C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis (mit Wahrheitstafeln)

Aus den Definitionen der Vereinigung und des Schnittes folgt

$$A \cap (B \cup C) = \{x \in M : x \in A \wedge (x \in B \vee x \in C)\}.$$

Für ein beliebiges $x \in M$ seien a_x , b_x und c_x die (primitiven) Aussagen $x \in A$, $x \in B$ und $x \in C$. Somit gilt

$$x \in A \cap (B \cup C) \iff a_x \wedge (b_x \vee c_x) \text{ ist wahr.}$$

Wegen des Distributivgesetzes des logischen „und“ und „oder“ (bewiesen durch Wahrheitstafeln) gilt

$$a_x \wedge (b_x \vee c_x) \iff (a_x \wedge b_x) \vee (a_x \wedge c_x),$$

und somit gilt

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (a_x \wedge b_x) \vee (a_x \wedge c_x) \text{ ist wahr} \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \text{ ist wahr} \end{aligned}$$

und die Aussage des Satzes folgt, da $x \in M$ beliebig war. □

Satz

Für beliebige Mengen $A, B, C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis

Wir beweisen beide **Teilmengenbeziehungen**

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{und} \quad A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

einzelnen, wodurch sich die Gleichheit ergibt.

„ \subseteq “ Sei $x \in A \cap (B \cup C)$ beliebig. Das bedeutet $x \in A$ und

$$x \in B \cup C. \quad (*)$$

Falls $x \in B$, dann gilt auch $x \in A \cap B$ und somit auch $x \in (A \cap B) \cup (A \cap C)$.

Falls $x \notin B$, dann gilt $x \in C$ wegen $(*)$ und somit auch $x \in A \cap C$ und wieder folgt $x \in (A \cap B) \cup (A \cap C)$.

In jedem Fall gilt also $x \in (A \cap B) \cup (A \cap C)$ und da x beliebig aus $x \in A \cap (B \cup C)$ gewählt war, folgt die gesuchte Inklusion

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

Satz

Für beliebige Mengen $A, B, C \subseteq M$ gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Beweis

Wir beweisen beide **Teilmengenbeziehungen**

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{und} \quad A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

einzelnen, wodurch sich die Gleichheit ergibt.

„ \supseteq “ Sei nun $x \in (A \cap B) \cup (A \cap C)$ beliebig.

$$\Rightarrow x \in A \cap B \text{ oder } x \in A \cap C$$

■ Falls $x \in A \cap B$

$$\Rightarrow x \in A \text{ und } x \in B$$

$$\Rightarrow x \in A \text{ und } x \in B \cup C$$

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

■ Der Fall $x \in A \cap C$ ist analog mit B und C vertauscht.

Somit gilt $x \in A \cap (B \cup C)$ und da x beliebig gewählt war, folgt auch die Inklusion $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Beide Inklusionen zusammen ziehen die Gleichheit der Mengen nach sich. □

DE MORGANSche Regeln

Satz (DE MORGAN)

Für beliebige Mengen $A, B \subseteq M$ gilt

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{und} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Beweis

• Sei $x \in \overline{A \cap B}$.

$\Rightarrow x \notin (A \cap B) \Rightarrow x \notin A$ oder $x \notin B \Rightarrow x \in \overline{A}$ oder $x \in \overline{B} \Rightarrow x \in \overline{A} \cup \overline{B}$.

Somit gilt $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

• Sei umgekehrt $x \in \overline{A} \cup \overline{B}$.

$\Rightarrow x \in \overline{A}$ oder $x \in \overline{B} \Rightarrow x \notin A$ oder $x \notin B \Rightarrow x \notin (A \cap B) \Rightarrow x \in \overline{A \cap B}$.

Somit gilt auch $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ und die erste Gleichheit folgt.

• Für die zweite Identität folgern wir zuerst aus der ersten Regel (angewandt auf \overline{A} und \overline{B})

$$\overline{\overline{A \cap B}} = \overline{\overline{A} \cup \overline{B}} = A \cap B$$

und Komplementbildung auf beiden Seiten ergibt $\overline{A \cap B} = \overline{\overline{\overline{A \cap B}}} = \overline{A \cap B}$. □

BOOLEsche Algebren

DE MORGAN für Mengen: $\overline{A \cap B} = \overline{A} \cup \overline{B}$ und $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Satz (DE MORGAN für Aussagen)

Für Aussagen p und q gilt: $\neg(p \wedge q) = \neg p \vee \neg q$ und $\neg(p \vee q) = \neg p \wedge \neg q$.

Beweis: Wahrheitstabeln (Übung/Selbststudium) □

Bemerkungen

- Distributivgesetze, DE MORGAN-Regel gibt es jeweils für Mengen und Aussagen
- enger Zusammenhang zwischen Mengen und Aussagen

	Komplement	Vereinigung	Schnitt
Mengen	\overline{A}	$A \cup B$	$A \cap B$
Aussagen	$\neg p$	$p \vee q$	$p \wedge q$
	Negation	Disjunktion	Konjunktion

wobei Komplementbildung (bzw. Negation) \cup/\cap (bzw. \vee/\wedge) vertauscht.

- Abstraktion führt zum Begriff der **BOOLEschen Algebra**, z. B.
 - die **Schaltkreisalgebra** $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ auf den Wahrheitswerten 0 und 1 mit den logischen Verknüpfungen,
 - die **Potenzmengenalgebra** $(\wp(M), \cup, \cap, \overline{}, \emptyset, M)$ in $\wp(M)$ für eine nichtleere Menge $M \neq \emptyset$ mit den mengentheoretischen Verknüpfungen.
- in diesem Kontext entspricht die DE MORGANSche Regel dem **Dualitätspinzip**

Kartesisches Produkt

Definition

Für Mengen A und B ist das **kartesische Produkt/Kreuzprodukt** definiert durch

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

als die Menge aller **geordneten** Paare mit dem ersten Element aus A und dem zweiten B .

Allgemeiner definieren wir für Mengen A_1, \dots, A_n durch

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) : a_1 \in A_1, \dots, a_n \in A_n\}$$

die Menge aller entsprechenden **geordneten n -Tupel**.

- falls $A_1 = \dots = A_n = A$ gilt, dann schreiben wir A^n für $A_1 \times \dots \times A_n$
- falls $A_i = \emptyset$ für ein i , dann ist $A_1 \times \dots \times A_n = \emptyset$
- für $n = 0$ ist $A^0 = \{()\}$ die Menge bestehend aus dem leeren Tupel $()$

Abbildungen/Funktionen

Definition

Eine **Abbildung/Funktion** f von einer Menge A in eine Menge B ist eine **Zuordnung**, die jedem Element von A ein Element von B zuordnet und wir schreiben abkürzend

$$f: A \longrightarrow B$$

und sagen, f ist eine Abbildung/Funktion von A nach B .

Die Menge A heißt **Definitionsbereich** und B ist der **Wertevorrat** von f .

Für jedes $a \in A$ bezeichnen wir mit $b = f(a)$ das Element $b \in B$, das die Funktion f dem Element a zuordnet und wir sagen, f bildet a auf b ab und schreiben

$$a \longmapsto b,$$

wenn klar ist, welche Funktion f gemeint ist.

Die Teilmenge $\{f(a) : a \in A\}$ des Wertevorrats heißt **Bild von f** .

Eigenschaften von Funktionen

Definition

Eine Funktion $f: A \longrightarrow B$ heißt

- **injektiv**, falls für alle $a, a' \in A$ gilt $f(a) = f(a') \Rightarrow a = a'$.
- **surjektiv**, falls für alle $b \in B$ ein $a \in A$ existiert, so dass $f(a) = b$ gilt.
- **bijektiv**, falls sie sowohl **injektiv**, als auch **surjektiv** ist.

Beispiele

- $f_1: \mathbb{N} \longrightarrow \mathbb{N}$ mit $x \longmapsto x^2$ ist injektiv, aber nicht surjektiv
- $f_2: \mathbb{Z} \longrightarrow \mathbb{Z}$ mit $x \longmapsto x^2$ ist weder injektiv, noch surjektiv
- $f_3: \mathbb{R} \longrightarrow \mathbb{R}$ mit $x \longmapsto x^3 + x^2$ ist nicht injektiv, aber surjektiv
- $f_4: \mathbb{R} \longrightarrow \mathbb{R}$ mit $x \longmapsto x^3$ ist bijektiv
- $g: \mathbb{R} \longrightarrow \mathbb{R}$ mit $x \longmapsto \exp(x)$ ist injektiv, aber nicht surjektiv mit dem Bild $\{r \in \mathbb{R}: r > 0\}$
- **konstante Funktionen** $h \equiv z$, $h: M \longrightarrow M$ mit $x \longmapsto z$ für festes $z \in M$ sind im Allgemeinen weder injektiv, noch surjektiv
- **Identität auf M** $\text{id}_M: M \longrightarrow M$ mit $x \longmapsto x$ ist bijektiv

Operationen

Definition

Eine n -stellige Operation / (innere) n -stellige Verknüpfung auf einer Menge M ist eine Abbildung $f: M^n \longrightarrow M$.

Beispiele

- jede 0-stellige Operation auf einer Menge M ordnet dem leeren Tupel $()$ ein Element in M zu und kann als **konstante Funktion** bzw. einfach als Darstellung einer Konstante angesehen werden
- Negation (\neg) ist eine 1-stellige (**unäre**) Operation auf den Aussagen
- Komplement $(\bar{})$ ist eine 1-stellige Operation auf $\mathcal{P}(M)$ für jedes M
- die logischen (xor , \vee , \wedge , \Rightarrow , \Leftrightarrow) und mengentheoretischen (\cup , \cap , \setminus) Verknüpfungen sind 2-stellige (**binäre**) Operationen
- oft schreiben wir bei binären Operationen den Operator zwischen die beiden Argumente (**Infixnotation**), z. B. $A \cap B$ an Stelle von $\cap(A, B)$
- Grundrechenarten Addition $(+)$, Subtraktion $(-)$, Multiplikation (\cdot) und Division $(/)$ sind bekannte Beispiele für binäre Operationen

Summen- und Produktzeichen

Definition (\sum und \prod)

Für Zahlen x_1, \dots, x_n sei

$$\sum_{i=1}^n x_i := x_1 + x_2 + \dots + x_n \quad \text{und} \quad \prod_{i=1}^n x_i := x_1 \cdot x_2 \cdot \dots \cdot x_n.$$

Dabei heißt i der **Laufindex**, 1 ist die **untere Summations-/Produktgrenze** und n ist die **obere Summations-/Produktgrenze**.

Für $n = 0$ definieren wir die **leere Summe** $\sum_{i=1}^0 x_i$ als **0** und das **leere Produkt** $\prod_{i=1}^0 x_i$ als **1**.

- Laufindex muss nicht mit i bezeichnet werden und mit 1 beginnen

$$\sum_{k=-2}^3 2^{k+1} = 2^{-1} + 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 31,5 = \sum_{i=1}^6 2^{i-2}$$

- Potenzen von -1 ermöglichen **alternierende** Summen/Produkte mit wechselndem Vorzeichen

$$\sum_{i=0}^3 (-1)^i 3^i = 1 - 3 + 9 - 27 = -20 \quad \text{und} \quad \sum_{i=0}^3 (-1)^{i+1} 3^i = -1 + 3 - 9 + 27 = 20$$

Rechenregeln

- für $x_1 = \dots = x_n = x$ erhalten wir

$$\sum_{i=1}^n x = n \cdot x \quad \text{und} \quad \prod_{i=1}^n x = x^n$$

- **Linearität** der Summe: folgt aus dem **Distributivgesetz**

$$a \sum_{i=1}^n x_i = a \cdot (x_1 + \dots + x_n) = ax_1 + \dots + ax_n = \sum_{i=1}^n ax_i$$

und aus der **Assoziativität** und **Kommutativität** der Addition

$$\sum_{i=1}^n (x_i + y_i) = (x_1 + y_1) + \dots + (x_n + y_n)$$

$$= (x_1 + \dots + x_n) + (y_1 + \dots + y_n) = \sum_{i=1}^n x_i + \sum_{i=1}^n y_i$$

- Ausmultiplizieren ergibt

$$\begin{aligned} \left(\sum_{i=1}^n x_i \right) \left(\sum_{j=1}^m y_j \right) &= (x_1 + \cdots + x_n) \cdot (y_1 + \cdots + y_m) \\ &= x_1 y_1 + x_1 y_2 + \cdots + x_1 y_m \\ &\quad + x_2 y_1 + \cdots + x_2 y_m \\ &\quad + \cdots + \\ &\quad + x_n y_1 + \cdots + x_n y_m \\ &= \sum_{i=1}^n \sum_{j=1}^m x_i y_j \end{aligned}$$

- Kommutivität erlaubt dann die Vertauschung

$$\sum_{i=1}^n \sum_{j=1}^m x_i y_j = \sum_{j=1}^m \sum_{i=1}^n x_i y_j$$

2. Natürliche Zahlen und vollständige Induktion

Natürliche Zahlen

Definition

Mit \mathbb{N} bezeichnen wir die Menge der **natürlichen Zahlen**

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

und mit \mathbb{N}_0 die natürlichen Zahlen einschließlich der Null

$$\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

- oftmals wird auch die Null als natürliche Zahl angesehen
- die Existenz der natürlichen Zahlen (so wie wir sie kennen) kann aus den ZERMELO-FRAENKEL-Axiomen abgeleitet werden (Unendlichkeitsaxiom)
- in dieser VL werden wir \mathbb{N} mit der Addition (+) und Multiplikation (\cdot) und den geltenden Rechenregeln erstmal als gegeben annehmen

Rechengesetze für natürliche Zahlen

Für alle Zahlen $a, b, c \in \mathbb{N}_0$ gelten:

- **Assoziativgesetze:**

$$a + (b + c) = (a + b) + c \quad \text{und} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- **Kommutativgesetze:**

$$a + b = b + a \quad \text{und} \quad a \cdot b = b \cdot a$$

- **Distributivgesetz:**

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

- **Existenz der neutralen Elemente:**

$$a + 0 = a \quad \text{und} \quad a \cdot 1 = a$$

Vollständige Induktion

Beweisprinzip der vollständigen Induktion

Sei $A(n)$ eine Aussageform. Die Aussage „für alle $n \in \mathbb{N}$ gilt $A(n)$ “ ist wahr, wenn folgende zwei Bedingungen erfüllt sind:

- 1 $A(1)$ ist wahr Induktionsanfang
- 2 und für jedes $n \in \mathbb{N}$ gilt die Implikation $A(n) \Rightarrow A(n + 1)$. Induktionsschritt

Bemerkungen

- vielseitiges Beweisprinzip, welches oft Anwendung findet
- andere Varianten der vollständigen Induktion betrachten wir später
- die im Induktionsschritt als wahr angenommene Aussage $A(n)$ heißt **Induktionsannahme/Induktionsvoraussetzung** und die herzuleitende Aussage $A(n + 1)$ heißt **Induktionsbehauptung**
- in kondensierter Form kann man das Beweisprinzip selbst als folgende Aussage formulieren

$$A(1) \wedge (\forall n \in \mathbb{N}: A(n) \Rightarrow A(n + 1)) \implies \forall n \in \mathbb{N}: A(n)$$

Beispiel: GAUSSsche Summenformel

Satz

Für alle $n \in \mathbb{N}$ gilt

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

Beweis

Sei $A(n)$ die Aussageform $\sum_{i=1}^n i = \frac{(n+1)n}{2}$. Wir zeigen mit vollständiger Induktion, dass für alle $n \in \mathbb{N}$ die Aussage $A(n)$ gilt.

Induktionsanfang: Die Aussage $A(1)$ lautet $\sum_{i=1}^1 i = \frac{(1+1) \cdot 1}{2}$. Diese gilt, da

$$\sum_{i=1}^1 i = 1 = \frac{(1+1) \cdot 1}{2}. \quad (\checkmark)$$

Induktionsschritt: Wir zeigen $A(n) \Rightarrow A(n+1)$ für alle $n \in \mathbb{N}$. Sei also $n \in \mathbb{N}$ beliebig und es gelte die Induktionsannahme $A(n)$, d. h. $\sum_{i=1}^n i = \frac{(n+1)n}{2}$ gilt. Unter dieser Annahme leiten wir $A(n+1)$ her, d. h. wir zeigen $\sum_{i=1}^{n+1} i = \frac{(n+1+1)(n+1)}{2} = \frac{(n+2)(n+1)}{2}$

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

Somit gilt $A(n)$, also die im Satz behauptete Formel, für alle $n \in \mathbb{N}$. □

Beispiel: BERNOULLISCHE Ungleichung

Satz

Sei $q \geq -1$ eine reelle Zahl. Für alle $n \in \mathbb{N}$ gilt

$$(1 + q)^n \geq 1 + nq.$$

Beweis (durch vollständige Induktion für ein reelles $q \geq -1$)

Induktionsanfang: Für $n = 1$ gilt

$$(1 + q)^1 = 1 + q = 1 + 1 \cdot q. \quad (\checkmark)$$

Induktionsschritt: Es gelte die Induktionsannahme $(1 + q)^n \geq 1 + nq$ und wir zeigen damit $(1 + q)^{n+1} \geq 1 + (n + 1)q$. Tatsächlich gilt

$$\begin{aligned} (1 + q)^{n+1} &= (1 + q)^n \cdot (1 + q) \stackrel{\text{I. Annahme}}{\geq} (1 + nq) \cdot (1 + q) \\ &= 1 + nq + q + nq^2 \geq 1 + nq + q = 1 + (n + 1)q. \quad (\checkmark) \end{aligned}$$

Somit gilt also die im Satz behauptete Ungleichung für alle $n \in \mathbb{N}$. \square

Wo wurde $q \geq -1$ benötigt?

Erste Ungleichung im I.Schritt!

Beispiel: Teilbarkeit

- Für ganze Zahlen a und b schreiben wir $a \mid b$, falls a ein Teiler von b ist, d. h. es gibt eine ganze Zahl z mit $a \cdot z = b$.

Satz

Für alle $n \in \mathbb{N}$ ist $n^3 - n$ durch 3 teilbar, d. h. $3 \mid (n^3 - n)$ für alle $n \in \mathbb{N}$.

Beweis

Sei $A(n)$ die Aussageform $3 \mid (n^3 - n)$. Wir zeigen mit vollständiger Induktion, dass für alle $n \in \mathbb{N}$ die Aussage $A(n)$ gilt.

Induktionsanfang: Die Aussage $A(1)$ lautet $3 \mid (1^3 - 1)$, also $3 \mid 0$. Somit ist $A(1)$ wahr, da die 3 Teiler der 0 ist. (✓)

Induktionsschritt: Für alle $n \in \mathbb{N}$ zeige $A(n+1)$, d. h. $3 \mid ((n+1)^3 - (n+1))$, unter der Induktionsannahme $A(n)$. Es gelte also $3 \mid (n^3 - n)$. Durch elementares Umformen erhalten wir

$$(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + 3(n^2 + n). \quad (*)$$

Wegen der Induktionsannahme $A(n)$ gilt $3 \mid (n^3 - n)$ und da $3(n^2 + n)$ durch 3 teilbar ist, folgt auch

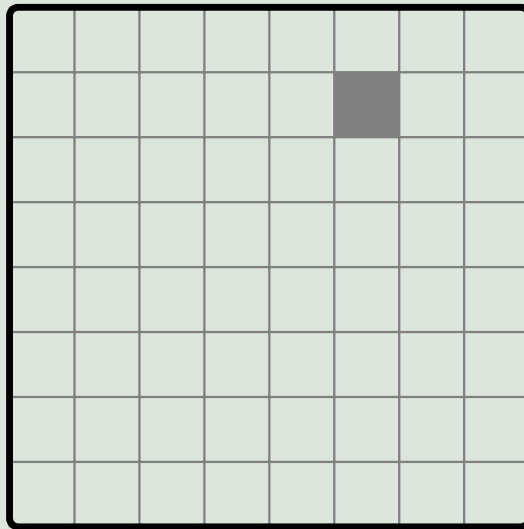
$$3 \mid ((n^3 - n) + 3(n^2 + n)) \quad \stackrel{(*)}{\iff} \quad 3 \mid ((n+1)^3 - (n+1)). \quad (\checkmark)$$

Somit gilt $A(n)$ für alle $n \in \mathbb{N}$. □

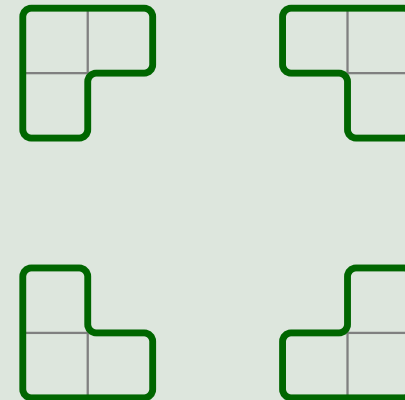
Beispiel: Geometrische Knobelei

Hof-Fliesen-Problem

Ein quadratischer Hof mit Seitenlängen 2^n soll mit L-förmigen Fliesen ausgelegt werden. Dabei soll ein vorgegebenes Quadrat mit der Seitenlänge 1 im Hof frei bleiben, weil da eine Statue aufgestellt werden soll. Die L-förmigen Fliesen haben die Form von drei aneinander gesetzten Quadraten mit Seitenlänge eins.



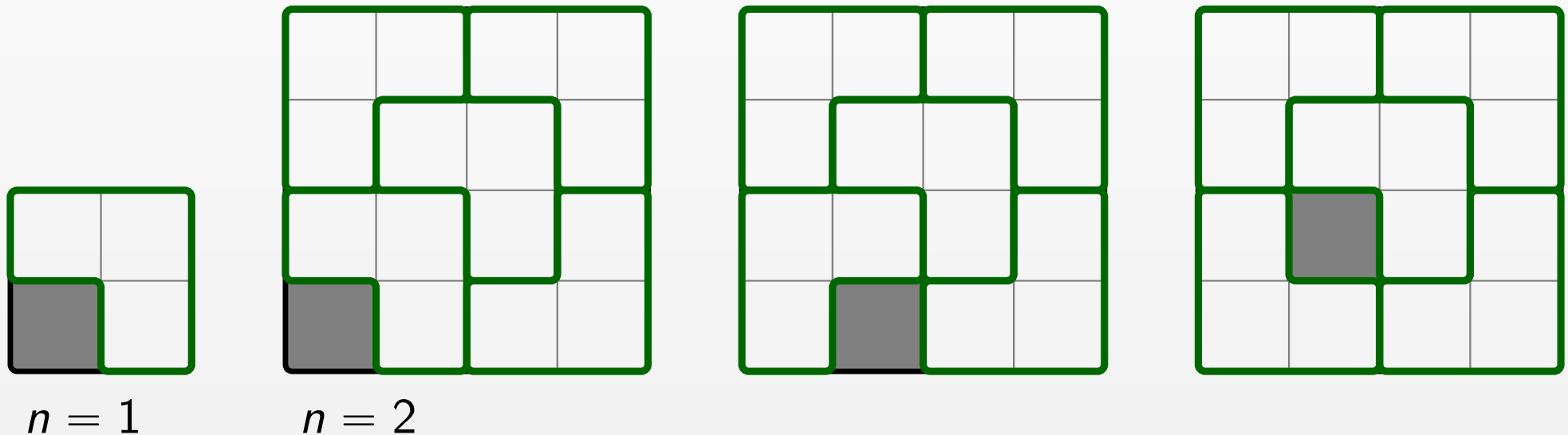
Hof



Fliesen

Ist es möglich, den Hof wie oben beschrieben vollständig mit L-förmigen Fliesen so zu überdecken, dass die Fliesen sich nicht überlappen und nicht zerschnitten werden müssen?

Wir betrachten zunächst die Fälle $n = 1$ und $n = 2$ und sehen, dass wir den Hof wie gewünscht fliesen können. Schon der Fall $n = 1$ genügt für den Induktionsanfang.



Die anderen Fälle sind symmetrisch zu einem der dargestellten Fälle.

Lösung vom Hof-Fliesen-Problem

Für alle $n \in \mathbb{N}$ gibt es ein Lösung für das Hof-Fliesen-Problem eines quadratischen Hofes mit Seitenlänge 2^n und beliebig vorgegebenem freien Quadrat mit Seitenlänge 1.

Beweis: Sei $A(n)$ die Aussage „jeder quadratische Hof mit Seitenlänge 2^n und beliebig vorgegebenem freien Quadrat mit Seitenlänge 1 kann mit L-förmigen Fliesen ausgelegt werden“.

Induktionsanfang: Die Aussage $A(1)$ gilt, da wie im Beispiel gesehen, das Entfernen eines Einheitsquadrats aus einem Quadrat mit Seitenlänge 2 genau eine L-Fliese ergibt. (✓)

Induktionsschritt: Sei $n \in \mathbb{N}$ beliebig und es gelte $A(n)$. Sei ein quadratischer Hof mit Seitenlänge 2^{n+1} und einem vorgegebenem freien Quadrat gegeben.

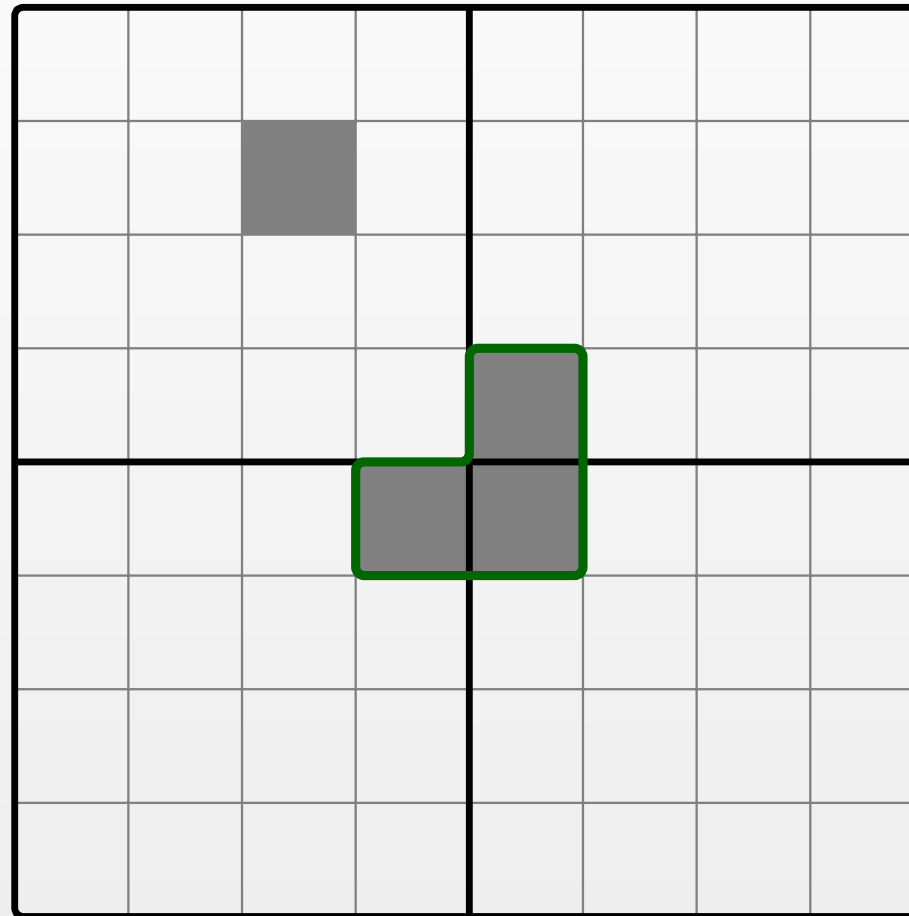
Zerlege den Hof in vier quadratische Höfe mit Seitenlänge 2^n , wobei genau einer das vorgegebene freie Quadrat enthält. Die Induktionsannahme liefert eine Fliesenüberdeckung für diesen Hof.

In die „Mitte“ können wir eine L-förmige Fliese F so legen, dass jeweils genau ein Quadrat der restlichen 3 Höfe belegt wird und so liefert die Induktionsannahme jeweils für jeden dieser 3 Höfe eine Fliesenüberdeckung, sodass jeweils das durch F belegte Quadrat frei bleibt. (siehe Bild nächste Folie)

Diese 4 Überdeckungen zusammen bilden eine Lösung für den ursprünglichen Hof. □

Hof-Fliesen-Problem – Zerlegung für den Induktionsschritt

Zerlegung des Hofes mit Seitenlänge 2^{n+1} in 4 Höfe mit Seitenlänge 2^n und Lage der mittigen Fliese F :



Der induktive Beweis liefert ein **rekursives** Verfahren zum fliesen eines so gegebenen Hofes:

- Wenn der Hof die Seitenlänge 2 hat, so bleibt neben dem markierten Quadrat genau Platz für eine L-förmige Fliese.
- Wenn der Hof für ein $n > 1$ die Seitenlänge 2^n hat, so unterteile den Hof in vier Höfe mit Seitenlänge 2^{n-1} und lege eine Fliese F so in die Mitte, dass sie genau die drei Höfe der Seitenlänge 2^{n-1} trifft, die nicht das markierte Quadrat enthalten.
- Führe den Algorithmus für die vier Höfe mit Seitenlänge 2^{n-1} durch, wobei das ursprünglich markierte Quadrat und die drei Quadrate, die von der ersten Fliese F überdeckt werden, markiert werden.

Bemerkung

Umgekehrt lassen sich die Laufzeit und Korrektheit eines rekursiven Algorithmus oft gut mit vollständiger Induktion analysieren.

Varianten der vollständigen Induktion

Vollständige Induktion

(Standardvariante)

Sei $A(n)$ eine Aussageform. Die Aussage „für alle $n \in \mathbb{N}$ gilt $A(n)$ “ ist wahr, wenn folgende zwei Bedingungen erfüllt sind:

- 1 $A(1)$ ist wahr
- 2 und für jedes $n \in \mathbb{N}$ gilt die Implikation $A(n) \Rightarrow A(n + 1)$.

Vollständige Induktion mit beliebigem Startwert

Sei $A(n)$ eine Aussageform und sei n_0 eine ganze Zahl. Die Aussage „für alle ganzzahligen $n \geq n_0$ gilt $A(n)$ “ ist wahr, wenn:

- 1 $A(n_0)$ wahr ist
- 2 und für jedes ganzzahlige $n \geq n_0$ die Implikation $A(n) \Rightarrow A(n + 1)$ gilt.

Vollständige Induktion mit mehreren Vorgängern (und bel. Startwert)

Sei $A(n)$ eine Aussageform und sei n_0 eine ganze Zahl. Die Aussage „für alle ganzzahligen $n \geq n_0$ gilt $A(n)$ “ ist wahr, wenn:

- 1 $A(n_0)$ ist wahr
- 2 und für jedes ganzzahlige $n \geq n_0$ gilt $(A(n_0) \wedge \dots \wedge A(n)) \Rightarrow A(n + 1)$.

Beispiele: Induktion mit anderem Startwert

Satz

Für alle natürlichen Zahlen $n \geq 3$ gilt $2n + 1 < 2^n$.

- Aussage ist tatsächlich falsch für ganzzahlige $n < 3$.

Beweis (durch vollständige Induktion mit Startwert $n_0 = 3$)

Induktionsanfang: Für $n = n_0$ gilt

$$2 \cdot 3 + 1 = 7 < 8 = 2^3. \quad (\checkmark)$$

Induktionsschritt: Es gelte die Induktionsannahme $2n + 1 < 2^n$ für $n \geq n_0$ und wir zeigen damit $2(n + 1) + 1 < 2^{n+1}$. Tatsächlich gilt

$$2(n + 1) + 1 = 2n + 1 + 2 \stackrel{\text{I. Annahme}}{<} 2^n + 2 \stackrel{n \geq 1}{<} 2^n + 2^n = 2^{n+1}. \quad (\checkmark)$$

Somit gilt also die behauptete Ungleichung für ganzzahlige $n \geq n_0 = 3$. \square

Geometrische Reihe

Satz (Geometrische Summenformel)

Sei $q \neq 1$ eine reelle Zahl und $n \in \mathbb{N}_0$. Dann gilt

$$\sum_{i=0}^n q^i = \frac{1 - q^{n+1}}{1 - q}.$$

Beweis (durch vollständige Induktion mit Startwert $n_0 = 0$ für ein $q \in \mathbb{R} \setminus \{1\}$)

Induktionsanfang: Für $n = 0$ gilt (mit der Konvention $0^0 = 1$ falls $q = 0$)

$$\sum_{i=0}^0 q^i = q^0 = 1 = \frac{1 - q}{1 - q} = \frac{1 - q^{0+1}}{1 - q}. \quad (\checkmark)$$

Induktionsschritt: Es gelte die Induktionsannahme für ein beliebiges $n \geq 0$ und wir zeigen die Induktionsbehauptung für $n + 1$. Tatsächlich gilt

$$\sum_{i=0}^{n+1} q^i = q^{n+1} + \sum_{i=0}^n q^i \stackrel{\text{l.A.}}{=} q^{n+1} + \frac{1 - q^{n+1}}{1 - q} = \frac{q^{n+1} - q^{n+2} + 1 - q^{n+1}}{1 - q} = \frac{1 - q^{n+2}}{1 - q}. \quad (\checkmark)$$

Somit gilt also die behauptete Gleichung für alle $n \in \mathbb{N}_0$. □

Rekursiv definierte Folgen

Definition (Folgen)

Eine **Folge** reeller Zahlen ist eine Abbildung $\mathbb{N} \longrightarrow \mathbb{R}$, die jeder natürlichen Zahl $n \in \mathbb{N}$ eine reelle Zahl $a_n \in \mathbb{R}$ zuordnet. Dafür schreibt man

$$(a_n)_{n \in \mathbb{N}} \quad \text{und} \quad (a_1, a_2, \dots)$$

und die a_n heißen auch **Folglied**.

Eine solche Folge $(a_n)_{n \in \mathbb{N}}$ ist **rekursiv definiert**, wenn für ein $k \in \mathbb{N}$ die ersten k Folglied a_1, \dots, a_k festgelegt werden und es eine Funktion $g: \mathbb{R}^k \longrightarrow \mathbb{R}$ gibt, sodass für $n \geq k$ gilt $a_{n+1} = g(a_{n-k+1}, \dots, a_n)$.

Allgemeiner kann als **Indexmenge** statt \mathbb{N} auch \mathbb{N}_0 oder Mengen $\{n_0 \in \mathbb{Z}: n \geq n_0\}$ ganzer Zahlen größer-gleich einem bestimmten n_0 genommen werden.

Beispiele

- Sei $(a_n)_{n \in \mathbb{N}}$ definiert durch $a_1 := 1$ und $a_{n+1} := 2a_n + 1$ für alle $n \in \mathbb{N}$.
 $(k = 1, g(x) = 2x + 1)$
- **FIBONACCI-Folge**: $f_0 := 0$, $f_1 := 1$ und $f_{n+1} := f_{n-1} + f_n$ für alle $n \geq 1$
 $(k = 2, g(x, y) = x + y)$

Abstecher: Rekursive Algorithmen

$a_{n+1} = 2a_n + 1$ in C

```
int a(int n) {
    if (n>1) {
        /* a(n)=2a(n-1)+1 */
        return 2*a(n-1) + 1;
    }
    else {
        /* a(1)=1 */
        return 1;
    }
}
```

Fibonacci-Folge in C

```
int f(int n) {
    switch (n) {
        case 0: /* f(0)=0 */
            return 0;
        case 1: /* f(1)=1 */
            return 1;
        default: /* Rekursion */
            return f(n-1)+f(n-2);
    }
}
```

Bemerkung

- rekursive Definition läßt sich einfach implementieren
- für rekursive Folgen mit $k \geq 2$ oft ineffektiv → Mehrfachberechnungen
- **Bsp.:** f_{90} mit 1,4 GHz Intel i5 Prozessor: rekursiv über 300 Jahre
direkt unter 2 Millisekunden

Rekursion vs. Induktion

- $a_1 = 1, a_2 = 3, a_3 = 7, a_4 = 15, a_5 = 31, \dots, a_{10} = 1023$

Satz

Die Folge $(a_n)_{n \in \mathbb{N}}$ sei definiert durch $a_1 := 1$ und $a_{n+1} := 2a_n + 1$. Dann gilt für alle $n \in \mathbb{N}$

$$a_n = 2^n - 1.$$

Beweis (durch vollständige Induktion)

Induktionsanfang: Für $n = 1$ gilt offensichtlich

$$a_1 := 1 = 2^1 - 1. \quad (\checkmark)$$

Induktionsschritt: Es gelte die Induktionsannahme für ein beliebiges $n \in \mathbb{N}$ und wir zeigen die Induktionsbehauptung für $n + 1$. Tatsächlich gilt

$$a_{n+1} := 2a_n + 1 \stackrel{\text{I. Annahme}}{=} 2(2^n - 1) + 1 = 2^{n+1} - 1. \quad (\checkmark)$$

Somit gilt also die behauptete Gleichung für alle $n \in \mathbb{N}$. □

FIBONACCI-Zahlen

- $f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, f_8 = 21$

Satz (DE MOIVRE-BINET-Formel)

Sei $(f_n)_{n \in \mathbb{N}_0}$ die Folge der FIBONACCI-Zahlen definiert durch $f_0 := 0, f_1 := 1$ und $f_{n+1} := f_{n-1} + f_n$. Dann gilt für alle $n \in \mathbb{N}$ mit $\varphi := \frac{1+\sqrt{5}}{2}$ und $\psi := \frac{1-\sqrt{5}}{2}$

$$f_n = \frac{1}{\sqrt{5}} (\varphi^n - \psi^n) .$$

- Echt jetzt? Wie kommt man darauf? → Lineare Algebra
- die reelle Zahl φ heißt auch **goldener Schnitt**

Beobachtung

Die Konstanten φ und ψ erfüllen die Gleichung $1 + \frac{1}{x} = x$.

Beweis: Für $x \neq 0$ gilt

$$1 + \frac{1}{x} = x \quad \iff \quad x + 1 = x^2$$

und p - q -Formel liefert $x_{1/2} = \frac{1}{2} \pm \frac{\sqrt{5}}{2}$.

$$f_n = \frac{1}{\sqrt{5}} (\varphi^n - \psi^n)$$

Beweis (durch vollständige Induktion mit zwei Vorgängern)

Induktionsanfang: Für $n = 0$ gilt

$$\frac{1}{\sqrt{5}} (\varphi^0 - \psi^0) = \frac{1}{\sqrt{5}} (1 - 1) = 0 =: f_0$$

und für $n = 1$ haben wir

$$\frac{1}{\sqrt{5}} (\varphi - \psi) = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} - \frac{1 - \sqrt{5}}{2} \right) = \frac{1}{\sqrt{5}} (\sqrt{5}) = 1 =: f_1. \quad (\checkmark)$$

Induktionsschritt: Es gelte die Induktionsannahme für $n - 1$ und für n und wir zeigen die Induktionsbehauptung für $n + 1$. Es gilt

$$f_{n+1} := f_{n-1} + f_n \stackrel{\text{i.A.}}{=} \frac{\varphi^{n-1} - \psi^{n-1}}{\sqrt{5}} + \frac{\varphi^n - \psi^n}{\sqrt{5}} = \frac{\varphi^n}{\sqrt{5}} \left(\frac{1}{\varphi} + 1 \right) - \frac{\psi^n}{\sqrt{5}} \left(1 + \frac{1}{\psi} \right).$$

Wegen der Beobachtung wissen wir $\frac{1}{\varphi} + 1 = \varphi$ und $1 + \frac{1}{\psi} = \psi$ und somit folgt

$$f_{n+1} = \frac{\varphi^n}{\sqrt{5}} \left(\frac{1}{\varphi} + 1 \right) - \frac{\psi^n}{\sqrt{5}} \left(1 + \frac{1}{\psi} \right) = \frac{1}{\sqrt{5}} (\varphi^{n+1} - \psi^{n+1}). \quad (\checkmark)$$

Somit gilt also die behauptete Formel für alle $n \in \mathbb{N}_0$. □

- Beweis der DE MOIVRE-BINET-Formel für f_n benötigt Induktionsanfang für beide Anfangswerte $n = 0$ und $n = 1$, da der Induktionsschritt für $n + 1$ (unabhängig von n) auf beiden vorherigen Aussagen für n und $n - 1$ beruht. Der Fall $n = 1$ ist somit **nicht** im Induktionsschritt abgedeckt, da wir nicht auf eine Aussage für $n = -1$ zurückgreifen können.
- Üblicherweise benötigen Aussagen über rekursive Folgen mit $k \in \mathbb{N}$ einen Induktionsanfang für die ersten k Fälle.

Fragen

- Warum gilt denn eigentlich das Prinzip der vollständigen Induktion?
- Kann man beweisen, dass ein Beweisprinzip gilt?
- für die Beantwortung der Fragen brauchen wir klarere Vorstellungen von den natürlichen Zahlen → **Axiomatisierung**

PEANO-Axiome

Definition (Natürliche Zahlen \mathbb{N})

Die Menge der natürlichen Zahlen \mathbb{N} erfüllt die folgenden Axiome mit der **Nachfolgerfunktion** $N(\cdot)$:

- 1** $1 \in \mathbb{N}$ 1 ist eine natürliche Zahl
- 2** $N(n) \in \mathbb{N}$ für alle $n \in \mathbb{N}$ jede Zahl n hat einen Nachfolger
- 3** $N(n) \neq 1$ für alle $n \in \mathbb{N}$ 1 ist kein Nachfolger
- 4** Funktion N ist injektiv Nachfolgerfunktion ist injektiv
- 5** Sei M eine beliebige Menge mit
 - $1 \in M$ und $N(n) \in M$ für alle $n \in M$,dann gilt $\mathbb{N} \subseteq M$. vollständige Induktion gilt (Induktionsaxiom)

Bemerkungen

- für $N(n)$ schreiben wir einfach $n + 1$, d. h. $n + 1 := N(n)$
 - **Addition** wird dann rekursiv definiert: $n + N(m) := N(n + m)$
 - ebenso die **Multiplikation**: $n \cdot 1 := n$ und $n \cdot N(m) := n \cdot m + n$
- ⇒ diese Definitionen erlauben die Rechengesetze für $+$ und \cdot auf \mathbb{N} zu beweisen
- Mengen M wie in Axiom 5 heißen **induktive Mengen** und das Axiom besagt, dass \mathbb{N} die „kleinste“ induktive Menge ist

Ordnung der natürlichen Zahlen

- Nachfolgerfunktion definiert Ordnung ($<$, \leq) auf \mathbb{N} : $n < N(m)$, falls

$$m = n \quad \text{oder} \quad N(n) < N(m)$$

und $n \leq m$, falls $n < m$ oder $n = m$.

- das **kleinste Element** ($\min M$) einer Teilmenge $M \subseteq \mathbb{N}$ ist das Element $m \in M$ mit $m \leq m'$ für alle $m' \in M$.

Satz

Jede nichtleere Teilmenge der natürlichen Zahlen hat ein kleinstes Element.

Beweis (Widerspruchsbeweis)

Sei $\emptyset \neq M \subseteq \mathbb{N}$ ohne ein kleinstes Element und betrachte das Komplement

$$\overline{M} = \mathbb{N} \setminus M.$$

Mit vollständiger Induktion werden wir $\overline{M} = \mathbb{N}$ zeigen, was zum Widerspruch $M = \emptyset$ führt. □

$$\overline{M} = \mathbb{N}$$

Mit vollständiger Induktion (mit mehreren Vorgängern) zeigen wir $n \in \overline{M}$ für jedes $n \in \mathbb{N}$.

Induktionsanfang: Die 1 ist das kleinste Element von \mathbb{N} , da die Definitionen sofort $1 < N(1) < N(N(1)) < \dots$ nach sich ziehen. Da wir annehmen dass M kein (eigenes) kleinstes Element hat, gilt also $1 \notin M$ und somit

$$1 \in \overline{M}. \quad (\checkmark)$$

Induktionsschritt: Für ein beliebiges $n \in \mathbb{N}$ gelte die Induktionsannahme für $1, \dots, n$, d.h. $\{1, \dots, n\} \subseteq \overline{M}$. Wir zeigen die Induktionsbehauptung $(n+1) \in \overline{M}$.

Falls $(n+1) \in M$, dann wäre $n+1$ das kleinste Element von M , wegen der Induktionsannahme, also gilt $(n+1) \notin M$ und somit

$$(n+1) \in \overline{M}. \quad (\checkmark)$$

Somit erhalten wir tatsächlich den Widerspruch $\overline{M} = \mathbb{N}$.

3. Elementare Zahlentheorie

Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen (\mathbb{N} und \mathbb{N}_0) mit den Rechenoperationen $+$ und \cdot und der Ordnung \leq konstruieren wir daraus die **ganzen** (\mathbb{Z}), die **rationalen** (\mathbb{Q}) und schließlich die **reellen Zahlen** (\mathbb{R})
- die ganzen Zahlen \mathbb{Z} erlauben zusätzlich die **Subtraktion** ($-$)
- ganz ähnlich erlauben die rationalen Zahlen \mathbb{Q} die **Division** ($/$)
- \mathbb{Z} und \mathbb{Q} können als **Abschluss/Erweiterung** der natürlichen Zahlen bezüglich der Subtraktion und Division angesehen werden
- die reellen Zahlen \mathbb{R} **vervollständigen** die rationalen Zahlen bezüglich Grenzwerteigenschaften die im Analysis-Teil der Vorlesung (Sommersemester) relevant werden
- für die Konstruktionen dieser Zahlenbereiche brauchen wir den Begriff der **Äquivalenzrelation**

Relationen

Definition (Relation)

Eine **Relation** R auf einer Menge A ist eine Teilmenge der geordneten Paare aus A^2 , d. h. $R \subseteq A^2$. Für $(a, b) \in R$ schreibt man auch aRb .

Definition (Eigenschaften von Relationen)

Eine Relation R auf A heißt

- **reflexiv**: für alle $a \in A$ gilt $(a, a) \in R$.
- **symmetrisch**: für alle $a, b \in A$ gilt $(a, b) \in R \implies (b, a) \in R$.
- **antisymmetrisch**: für alle $a, b \in A$ gilt $(a, b) \in R \wedge (b, a) \in R \implies a = b$.
- **transitiv**: für alle $a, b, c \in A$ gilt $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.

Definition (Spezielle Relationen)

Eine Relation R auf A ist eine

- **Teilordnung** (auch **Halbordnung**, **Ordnung**, **partielle Ordnung** genannt), falls R reflexiv, antisymmetrisch und transitiv ist. z. B. \leq auf \mathbb{N} und \subseteq auf $\wp(M)$
- **Äquivalenzrelation**, falls R reflexiv, symmetrisch und transitiv ist.

Beispiel: Äquivalenzrelation

Paritäten

Wir definieren eine Relation \equiv_2 auf \mathbb{N}_0 durch

$$x \equiv_2 y \quad :\iff \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$ ist gerade $\iff x, y$ gerade oder beide ungerade

Behauptung: \equiv_2 ist eine Äquivalenzrelation auf \mathbb{N}_0 .

Beweis: Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- **Reflexivität:** $x + x$ ist gerade für jedes $x \in \mathbb{N}_0$ ✓
- **Symmetrie:** $x + y = y + x$ für alle $x, y \in \mathbb{N}_0$ ✓
- **Transitivität:** Falls $x + y$ und $y + z$ gerade sind, dann ist $x + 2y + z$ gerade und, da $2y$ gerade ist, ist auch $x + z$ gerade. D. h. aus $x \equiv_2 y$ und $y \equiv_2 z$ folgt $x \equiv_2 z$ für beliebige $x, y, z \in \mathbb{N}_0$ ✓

Relation \equiv_2 ist reflexiv, symmetrisch und transitiv und die Beh. folgt. □

Bemerkung: \equiv_2 zerlegt \mathbb{N}_0 in zwei disjunkte Mengen (gerade und ungerade Zahlen) innerhalb denen jeweils alle Paare in Relation stehen.

Partitionen

Definition (Partition)

Ein **Partition/Zerlegung** einer Menge A ist eine Menge $\mathcal{Z} \subseteq \mathcal{P}(A)$ von Teilmengen von A , sodass

- 1 $Z \neq \emptyset$ für alle $Z \in \mathcal{Z}$, nichtleere Teilmengen
- 2 $Z \cap Z' = \emptyset$ für alle verschiedenen $Z, Z' \in \mathcal{Z}$ paarweise disjunkt
- 3 und $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$. Überdeckung von A

Die Teilmengen aus \mathcal{Z} heißen **Partitionsklassen**.

Bemerkung: Disjunkte Vereinigungen werden wir manchmal mit einem Punkt im Vereinigungszeichen anzeigen (z. B. $\bigcup \{Z : Z \in \mathcal{Z}\}$, $A \cup B$, ...).

Beispiele

- $\{\{n \in \mathbb{N}_0 : n \text{ gerade}\}, \{n \in \mathbb{N}_0 : n \text{ ungerade}\}\}$ ist Partition von \mathbb{N}_0
- die Menge $\mathcal{Z} = \{Z_k : k \in \mathbb{N}_0\}$ bestehend aus den Mengenfamilien $Z_k = \{A \subseteq \mathbb{N} : A \text{ hat genau } k \text{ Elemente}\}$ partitioniert die Menge der endlichen Teilmengen von \mathbb{N} in unendlich viele Partitionsklassen

Äquivalenzrelationen und Partitionen

Satz

Sei \mathcal{Z} eine Partition der Menge A . Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\iff \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation $\sim_{\mathcal{Z}}$ auf A .

Beweis: Sei \mathcal{Z} eine Partition von A und $\sim_{\mathcal{Z}}$ wie in der Behauptung definiert. Wir zeigen, dass $\sim_{\mathcal{Z}}$ reflexiv, symmetrisch und transitiv ist.

- **Reflexivität:** Sei $a \in A$. Da $A = \bigcup \{Z : Z \in \mathcal{Z}\}$ gibt es genau eine Menge $Z \in \mathcal{Z}$ mit $a \in Z$ und somit gilt $a \sim_{\mathcal{Z}} a$. ✓
- **Symmetrie:** Seien $a, b \in A$ mit $a \sim_{\mathcal{Z}} b$. D. h. es gibt eine Menge $Z \in \mathcal{Z}$ mit $a, b \in Z$ und somit $b \sim_{\mathcal{Z}} a$. ✓
- **Transitivität:** Seien a, b und $c \in A$ mit $a \sim_{\mathcal{Z}} b$ und $b \sim_{\mathcal{Z}} c$. Nach Definition von $\sim_{\mathcal{Z}}$ gibt es Z und $Z' \in \mathcal{Z}$ mit $a, b \in Z$ und $b, c \in Z'$. Also gilt $b \in Z \cap Z'$ und da \mathcal{Z} eine Partition ist (paarweise disjunkte Elemente), folgt $Z = Z'$. Somit enthält Z neben a und b auch c und es folgt $a \sim_{\mathcal{Z}} c$.

Also erfüllt $\sim_{\mathcal{Z}}$ die notwendigen Eigenschaften einer Äquivalenzrelation. \square

Satz

Sei \sim eine Äquivalenzrelation auf der Menge A . Dann gibt es **genau** eine Partition \mathcal{Z} von A mit $\sim = \sim_{\mathcal{Z}}$.

Beweis: Sei \sim eine Äquivalenzrelation auf A . Zuerst zeigen wir die Existenz einer Partition \mathcal{Z} mit $\sim = \sim_{\mathcal{Z}}$ und dann die Eindeutigkeit.

■ **Definition von \mathcal{Z} :** Setze $\mathcal{Z} := \{Z_a : a \in A\}$, wobei für jedes $a \in A$
 $Z_a := \{b \in A : a \sim b\}$.

■ **\mathcal{Z} ist Partition:** Wir zeigen, dass die Mengen Z_a nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz A ergibt.

- **nichtleer und $\bigcup \mathcal{Z} = A$:** \sim reflexiv $\Rightarrow a \sim a$ für jedes $a \in A$
 $\Rightarrow a \in Z_a$ für jedes $a \in A \Rightarrow Z_a \neq \emptyset$ für jedes $a \in A$ und $\bigcup_{a \in A} Z_a = A$ ✓
- **disjunkt:** Angenommen $c \in Z_a \cap Z_b \Rightarrow a \sim c$ und $b \sim c$ und wegen der Symmetrie und Transitivität von \sim folgt $a \sim b$.

Wir zeigen nun $Z_a \subseteq Z_b$: Sei $x \in Z_a$ beliebig $\Rightarrow a \sim x$ und wegen der Symmetrie und Transitivität und $a \sim b$ folgt auch $b \sim x \Rightarrow x \in Z_b$.

Da $x \in Z_a$ beliebig war, gilt $Z_a \subseteq Z_b$ und die gleiche Argumentation zeigt auch $Z_b \subseteq Z_a$ und somit $Z_a = Z_b$, falls $Z_a \cap Z_b \neq \emptyset$. ✓

Als nächstes zeigen wir $\sim = \sim_{\mathcal{Z}}$ und dann die Eindeutigkeit von \mathcal{A} .

- $\sim \subseteq \sim_{\mathcal{Z}}$: Sei $a \sim b$, also $(a, b) \in \sim$. Dann gilt $a, b \in Z_a$ und aus der Definition von $\sim_{\mathcal{Z}}$ folgt $a \sim_{\mathcal{Z}} b$, also $(a, b) \in \sim_{\mathcal{Z}}$. ✓
- $\sim_{\mathcal{Z}} \subseteq \sim$: Sei nun $a \sim_{\mathcal{Z}} b$, also $(a, b) \in \sim_{\mathcal{Z}}$. Dann existiert ein $Z \in \mathcal{Z}$ mit $a, b \in Z$. Wegen der Definition von \mathcal{Z} gibt es ein $a' \in Z$ mit $Z = Z_{a'}$.
Da also a, b aus $Z_{a'}$ sind, folgt $a' \sim a$ und $a' \sim b$ und mit Symmetrie und Transitivität von \sim auch $a \sim b$. D. h. $(a, b) \in \sim$ wie gewünscht. ✓
- **Eindeutigkeit**: Sei \mathcal{Y} eine weitere Partition mit $\sim_{\mathcal{Y}} = \sim$. Aus dem bereits Gezeigten folgt also $\sim_{\mathcal{Y}} = \sim = \sim_{\mathcal{Z}}$ und somit gilt für alle $a, b \in A$

$$a \sim_{\mathcal{Y}} b \iff a \sim b \iff a \sim_{\mathcal{Z}} b.$$

Folglich gilt für alle $a \in A$ auch

$$Y_a := \{b \in A : a \sim_{\mathcal{Y}} b\} = \{b \in A : a \sim b\} = Z_a.$$

Somit ist $\{Y_a : a \in A\} = \mathcal{Z}$.

Des Weiteren ist Y_a offensichtlich eine Teilmenge der Menge $Y \in \mathcal{Y}$, die a enthält. Aber wegen der Transitivität von $\sim_{\mathcal{Y}}$ gilt tatsächlich $Y_a = Y$. D. h.

$\{Y_a : a \in A\} = \mathcal{Y}$, also $\mathcal{Y} = \mathcal{Z}$ was den Beweis abschließt. □

Äquivalenzklassen

Definition (Äquivalenzklassen)

Sei \sim eine Äquivalenzrelation auf A .

- Die eindeutig bestimmte Partition \mathcal{Z} aus dem letzten Satz bezeichnet man mit A/\sim und sie heißt **Faktormenge/Quotientenmenge**.
- Die Elemente von A/\sim heißen **Äquivalenzklassen**, welche man mit $[a]$ (manchmal auch \bar{a}) statt Z_a bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die **Repräsentanten** dieser Äquivalenzklasse und wir sagen, sie sind **äquivalent** zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.
- Zwei Elemente a und $b \in A$ repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind
$$[a] = [b] \iff a \sim b.$$
- Die Funktion $a \mapsto [a]$ heißt **kanonische Projektion** von A nach A/\sim .

Beispiel: Partitioniert man \mathbb{N} in die geraden und ungeraden Zahlen und bezeichnet diese Partition mit \mathcal{Z} , so ist $\sim_{\mathcal{Z}}$ die Äquivalenzrelation mit zwei Äquivalenzklassen und zwei Zahlen sind genau dann äquivalent, wenn sie die gleiche Parität haben. Jede ungerade Zahl repräsentiert die Äquivalenzklasse der ungeraden Zahlen usw.

Wie macht man Funktionen injektiv?

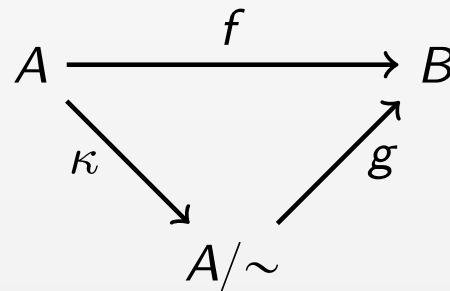
Satz

Sei $f: A \longrightarrow B$ eine Funktion. Für $a, a' \in A$ definiere die Relation \sim durch

$$a \sim a' \quad :\iff \quad f(a) = f(a').$$

Dann ist \sim eine Äquivalenzrelation und $[a] \mapsto f(a)$ eine injektive Funktion $g: A/\sim \longrightarrow B$.

Sei κ die kanonische Projektion von \sim . Dann besagt der Satz, es gibt inj. g mit $f = g \circ \kappa$



Beweis

Zu zeigen ist:

- 1 \sim ist eine Äquivalenzrelation, ✓
- 2 g ist **wohldefiniert**, d. h. $g([a])$ ist unabhängig vom gewählten Repräsentanten! ✓
- 3 g ist injektiv. ✓

□

Relationen und Graphen

Idee: Relation $R \subseteq M^2$ auf einer Menge M kann graphisch dargestellt werden, indem man die geordneten Paare in R als Pfeile zwischen den Elementen von M zeichnet

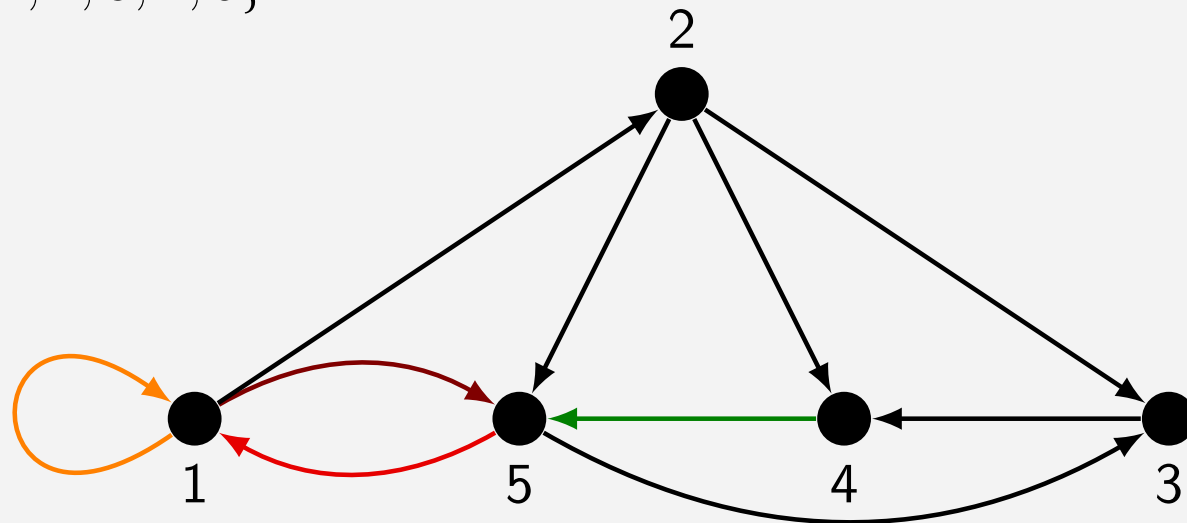
Definition (Gerichteter Graph)

Ein **gerichteter Graph** ist ein Paar $D = (V, A)$ mit $A \subseteq V^2$ und **Kantenmenge** A und **Ecken/Knotenmenge** V . Kanten der Form (v, v) heißen **Schlingen**.

Beispiel

Gerichteter Graph der Relation:

- $R := \{(1, 1), (1, 2), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (4, 5), (5, 1), (5, 3)\}$
- auf $M := \{1, 2, 3, 4, 5\}$



Eigenschaften von Relationen und Graphen

Sei R eine Relation auf der Menge V :

- R ist reflexiv, falls jeder Ecke $v \in V$ im zugehörigen gerichteten Graphen eine Schlinge hat.
- R ist irreflexiv, falls keine Ecke $v \in V$ im zugehörigen gerichteten Graphen eine Schlinge hat.
- R ist symmetrisch, falls im gerichteten Graphen für jede Kante $(u, v) \in A$ auch die „umgekehrte“ Kante (v, u) in A vorhanden ist.
- R ist antisymmetrisch, falls für je zwei verschiedene Ecken $u, v \in V$ im gerichteten Graphen höchstens eine Kante vorhanden ist.
- R ist transitiv, falls für den gerichteten Graphen folgendes gilt: Immer wenn man entlang der gerichteten Kanten einen Weg (bzw. Kreis falls $u = v$) von einer Ecke u zu einer Ecke v finden kann, dann ist bereits die Kante (u, v) vorhanden.

HASSEdiagramme von Ordnungsrelationen

Ordnungsrelation/Teilordnung/partielle Ordnung:

reflexiv, antisymmetrisch, transitiv

Vereinfachte Darstellung:

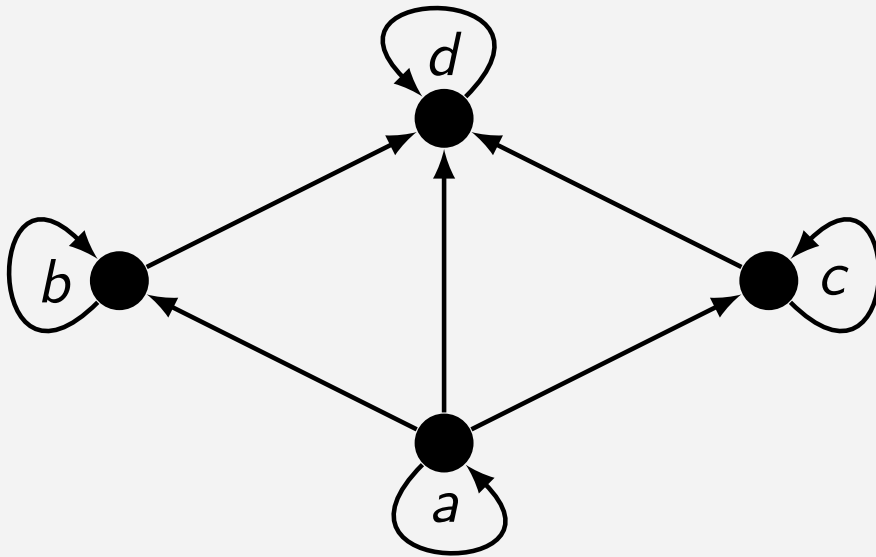
- reflexiv \Rightarrow Graph hat an jeder Ecke eine Schlinge
 \longrightarrow Schlingen einfach weglassen
- transitiv \Rightarrow Wege erzwingen „abkürzende Kanten“
 \longrightarrow nur Wege ohne Abkürzungen zeichnen
 $\Rightarrow (u, v)$ nur darstellen, wenn es **keinen** gerichteten Weg von u nach v mit mindestens zwei Kanten im Graphen der Relation gibt
- restlichen Graphen so zeichnen, dass alle Pfeilspitzen nach oben zeigen
 \longrightarrow und dann Pfeilspitzen weglassen
- die sich ergebende Darstellung einer Ordnungsrelation heißt:

HASSEdiagramm

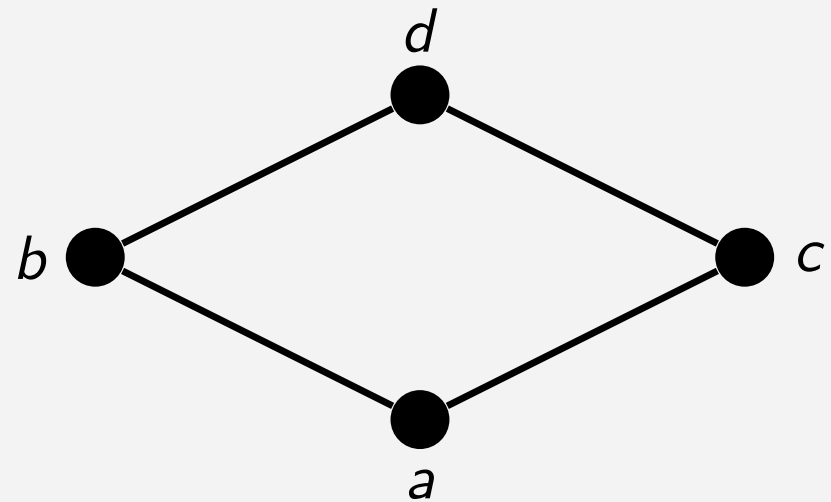
HASSEdiagramme – Beispiel

- $R := \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, d), (c, d)\}$
- auf $M := \{a, b, c, d\}$

gerichteter Graph von R



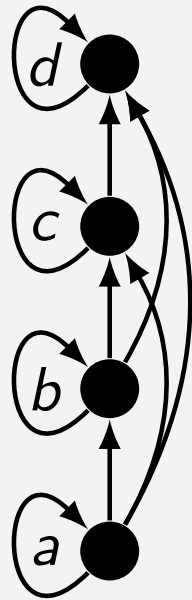
HASSEdiagramm von R



HASSEdiagramme – Beispiel 2

- $R := \{(a, a), \dots, (d, d), (a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$
- auf $M := \{a, b, c, d\}$

gerichteter Graph von R



HASSEdiagramm von R



Hüllenbildung

Idee:

- falls Relation R nicht ... erfüllt, dann erweitere/verringere R so **wenig** wie möglich bis ... erfüllt ist

Definition (Reflexive Hülle)

Für eine Relation R auf einer Menge M sei

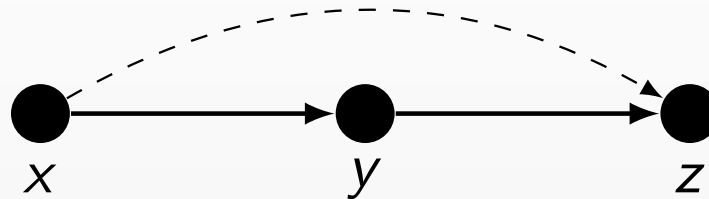
$$R' := R \cup \{(x, x) : x \in M\}.$$

Dann ist R' die kleinste reflexive Relation, die R umfasst, und diese wird die **reflexive Hülle** von R genannt.

Bsp.: Für $<$ auf \mathbb{N} ist \leq die reflexive Hülle.

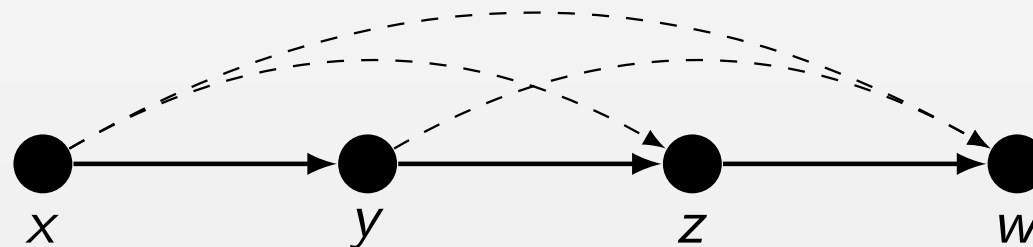
Transitive Hülle – Beispiele

- $R_1 := \{(x, y), (y, z)\}$ auf $M_1 = \{x, y, z\}$



⇒ für Transitivität fehlt (x, z)

- $R_2 := \{(x, y), (y, z), (z, w)\}$ auf $M_2 = \{x, y, z, w\}$



⇒ für Transitivität fehlen nicht nur (x, z) und (y, w) , sondern auch (x, w)

Transitive Hülle

Allgemein:

- wir brauchen für Transitivität die Eigenschaft:

$$\text{falls } (x_1, x_2), \dots, (x_{n-1}, x_n) \in R \implies (x_1, x_n) \in R$$

Definition (Transitive Hülle)

Für eine Relation R auf einer Menge A ist

$$R^+ := \left\{ (x, y) : \text{es gibt } n \geq 2 \text{ und } x_1, \dots, x_n \in A \text{ mit} \right. \\ \left. x = x_1, y = x_n \text{ und } (x_1, x_2), \dots, (x_{n-1}, x_n) \in R \right\}$$

die kleinste transitive Relation mit $R \subseteq R^+$, die **transitive Hülle** von R heißt.

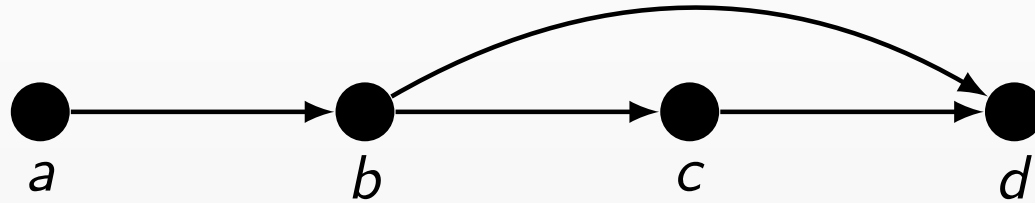
Des Weiteren ist $R^* = R^+ \cup R'$ die **reflexive, transitive Hülle** von R und R^* ist die kleinste reflexive, transitive Relation, die R umfasst.

Bemerkung

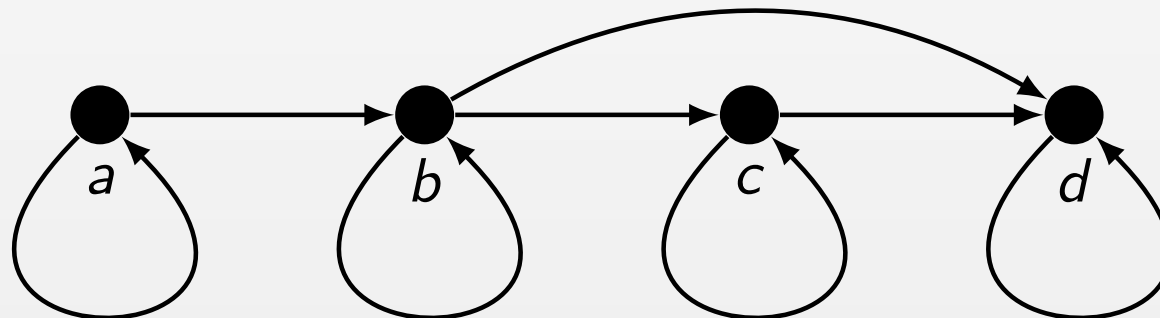
- Relationen die transitiv und reflexiv sind, heißen **Quasiordnungen**

Beispiel

$$R = \{(a, b), (b, c), (c, d), (b, d)\}$$

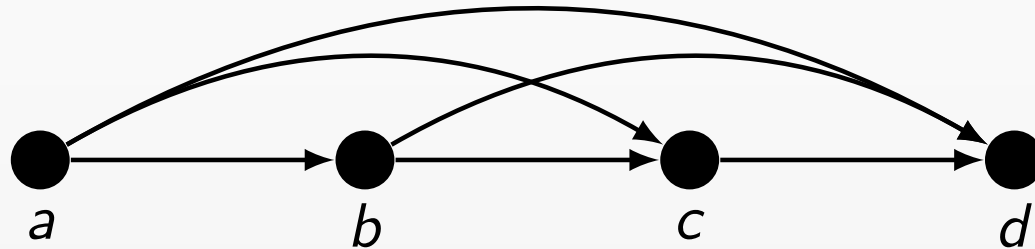


$$R' = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (c, d), (b, d)\}$$

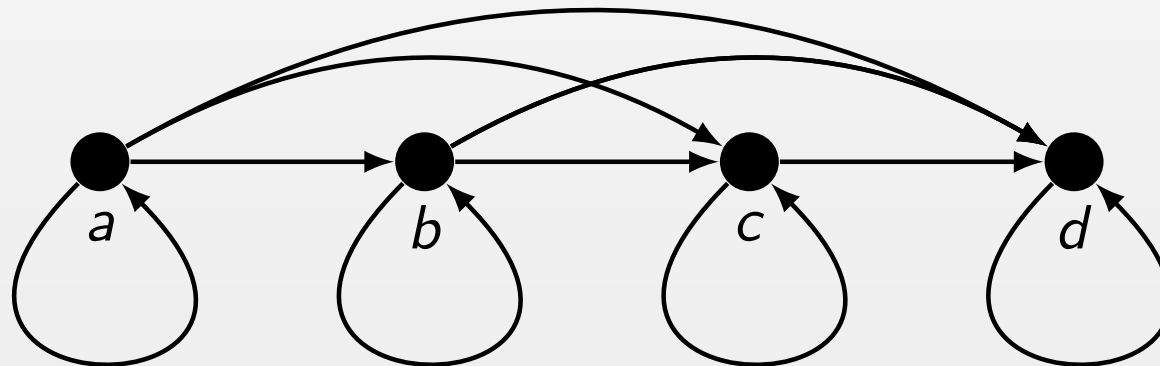


Beispiel

$$R^+ = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$$



$$R^* = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$$



Quasiordnungen zu Teilordnungen

Definition (Quasiordnung)

Eine reflexive und transitive Relation heißt **Quasiordnung**.

Idee:

- „entferne“ symmetrische Paare der Quasiordnung durch gleichsetzen/Äquivalenzen

Satz

Für jede Quasiordnung \leq auf einer Menge A wird durch

$$a \sim b \quad :\Leftrightarrow \quad (a \leq b \text{ und } b \leq a)$$

eine Äquivalenzrelation auf A definiert. Auf A/\sim definiert dann

$$[a] \leq [b] \quad :\Leftrightarrow \quad a \leq b$$

eine Teilordnung.

Beweis des Satzes

Beweis: Der Beweis hat drei Teile

- 1** \sim ist eine Äquivalenzrelation,
- 2** \leq ist wohldefiniert und
- 3** \leq ist eine Teilordnung.

zu 1: Reflexivität und Transitivität vererben sich von \leq und Symmetrie folgt von der Definition von \sim .

zu 2: Es ist zu zeigen, dass die Definition unabhängig von den gewählten Repräsentanten ist. D. h. für alle $a' \in [a]$ und $b' \in [b]$ muss gelten:

$$a \leq b \iff a' \leq b'.$$

Es gilt: $a' \in [a] \Rightarrow a' \sim a \Rightarrow a' \leq a$ und $a \leq a'$.

Ebenso $b' \in [b] \Rightarrow b' \leq b$ und $b \leq b'$.

Wegen der Transitivität von \leq gilt also $a \leq b \Rightarrow a' \leq a \leq b \leq b' \Rightarrow a' \leq b'$ und ebenso $b \leq a \Rightarrow b' \leq a'$.

zu 3: Reflexivität und Transitivität vererben sich von \leq .

Für die Antisymmetrie seien $a, b \in A$ mit $[a] \leq [b]$ und $[b] \leq [a]$. Aus der Definition von \leq folgern wir $a \leq b \leq a$ und somit $a \sim b$, also $[a] = [b]$. \square

Ganze Zahlen

Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von \mathbb{N}_0 definiert werden. Z. B. $7 - 12$ liegt nicht in \mathbb{N}_0 .
- Vervollständige \mathbb{N}_0 für die Abgeschlossenheit der Subtraktion.
- Definiere die ganze Zahl z als Menge der Paare $(a, b) \in \mathbb{N}_0^2$ mit „ $a - b = z$ “ (z. B. $(7, 12)$ und $(0, 5)$ sind Repräsentanten von -5).
- Da es aber kein „ $-$ “ in \mathbb{N}_0 gibt, drücken wir diese Beziehung innerhalb von \mathbb{N}_0 durch „umstellen“ wie folgt aus

$$\text{„} a - b = a' - b' \text{“} \iff a + b' = a' + b.$$

- Damit definieren wir eine Äquivalenzrelation auf \mathbb{N}_0^2 deren Äquivalenzklassen den ganzen Zahlen entsprechen.

Ganze Zahlen

formale Definition

Idee

Definition (\mathbb{Z})

Durch

$$(a, b) \sim (a', b') : \iff a + b' = a' + b \quad \text{„}a - b = a' - b'\text{“}$$

wird auf \mathbb{N}_0^2 eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge \mathbb{N}_0^2 / \sim mit \mathbb{Z} und nennen ihre Elemente die **ganzen Zahlen**. Ganze Zahlen der Form $[(n, 0)]$ bezeichnen wir kürzer durch die natürliche Zahl n und ganze Zahlen der Form $[(0, n)]$ als $-n$.

Die Operationen $+$ und \cdot und die Ordnung \leq von \mathbb{N} erweitert man auf ganz \mathbb{Z} durch:

$$[(a, b)] +_{\mathbb{Z}} [(a', b')] : \iff [(a + a', b + b')], \quad \text{„}(a - b) + (a' - b') = (a + a') - (b + b')\text{“}$$

$$[(a, b)] \cdot_{\mathbb{Z}} [(a', b')] : \iff [(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')], \quad \text{„}(a - b) \cdot (a' - b') = (a \cdot a' + b \cdot b') - (a \cdot b' + b \cdot a')\text{“}$$

$$[(a, b)] \leq_{\mathbb{Z}} [(a', b')] : \iff a + b' \leq a' + b. \quad \text{„}(a - b) \leq (a' - b')\text{“}$$

Bemerkungen:

- $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$ und $\leq_{\mathbb{Z}}$ sind **wohldefiniert** und wir schreiben einfach $+$, \cdot und \leq
- \mathbb{Z} **“erbt”** die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von \mathbb{N}_0
- für jedes $z \in \mathbb{Z}$ gibt es genau ein $z' \in \mathbb{Z}$ mit $z + z' = 0$ $[(a, b)] + [(b, a)] \sim [(0, 0)]$
- z' bezeichnen wir mit $-z$
- allgemein definieren wir dann die **Subtraktion** $x - y := x + (-y)$
 $- : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ mit $(x, y) \mapsto x + (-y)$

Rationale Zahlen

Idee:

- vervollständige \mathbb{Z} für die Abgeschlossenheit bezüglich der Division
- Definiere die rationale Zahl q durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen (a, b) mit $b \neq 0$ soll die rationale Zahl $q = a/b$ repräsentieren und verschiedene Bruchdarstellungen der selben Zahl q werden gleich (äquivalent) gesetzt.
- Ähnlich wie bei der Darstellung von „–“, stellen wir um

$$\text{„} \frac{a}{b} = \frac{a'}{b'} \text{“} \iff a \cdot b' = a' \cdot b.$$

- Damit definieren wir eine Äquivalenzrelation auf der Menge

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$$

deren Äquivalenzklassen den rationalen Zahlen entsprechen.

Rationale Zahlen

Definition (\mathbb{Q})

Durch

$$(a, b) \approx (a', b') \iff a \cdot b' = a' \cdot b$$

$$\text{„} \frac{a}{b} = \frac{a'}{b'} \text{“}$$

wird auf der Menge $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$ mit \mathbb{Q} und nennen ihre Elemente die **rationalen Zahlen**. Rationale Zahlen der Form $[(z, 1)]$ bezeichnen wir kürzer durch die ganze Zahl z und rationale Zahlen der Form $[(1, z)]$ als $1/z$ bzw. z^{-1} .

Die Operationen $+$ und \cdot und die Ordnung \leq aus \mathbb{Z} erweitert man auf ganz \mathbb{Q} durch:

$$[(a, b)] +_{\mathbb{Q}} [(a', b')] \iff [(a \cdot b' + a' \cdot b, b \cdot b')],$$

$$\text{„} \frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \text{“}$$

$$[(a, b)] \cdot_{\mathbb{Q}} [(a', b')] \iff [(a \cdot a', b \cdot b')],$$

$$\text{„} \frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} \text{“}$$

$$[(a, b)] \leq_{\mathbb{Q}} [(a', b')] \iff a \cdot b' \leq a' \cdot b.$$

$$\text{„} \frac{a}{b} \leq \frac{a'}{b'} \text{“}$$

- $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ und $\leq_{\mathbb{Q}}$ sind **wohldefiniert** und wir schreiben einfach $+$, \cdot und \leq
- wir definieren die Subtraktion analog wie in \mathbb{Z} , d. h. für $q = [(a, b)]$ setze $-q = [(-a, b)]$
- \mathbb{Q} “erbt” die Rechengesetze (Kommutativität, Assoziativität, Distributivität) von \mathbb{Z}
- für jedes $q \in \mathbb{Q} \setminus \{0\}$ gibt es genau ein $q' \in \mathbb{Q}$ mit $q \cdot q' = 1$ $[(a, b)] \cdot [(b, a)] \approx [(1, 1)]$
- q' bezeichnen wir mit $1/q$ bzw. q^{-1}
- allgemein definieren wir dann die **Division** $x/y := x \cdot (y^{-1})$

Körper

Definition (Körper)

Sei K eine Menge

- mit zwei verschiedenen Elementen $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen $+: K \times K \longrightarrow K$ und $\cdot: K \times K \longrightarrow K$.

Wir sagen K (genauer $(K, +, \cdot)$ bzw. $(K, +, \cdot, 0_K, 1_K)$) ist ein **Körper**, wenn für alle $a, b, c \in K$ die folgenden Rechengesetze gelten:

(K1) **Assoziativgesetze:** $a + (b + c) = (a + b) + c$ und $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) **Kommutativgesetze:** $a + b = b + a$ und $a \cdot b = b \cdot a$

(K3) **Distributivgesetz:** $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) **Neutrale Elemente:** $a + 0_K = a$ und $1_K \cdot a = a$

(K5) **Existenz inverser Elemente:**

- es existiert ein $-a \in K$ mit $a + (-a) = 0_K$.
- falls $a \neq 0_K$, dann existiert ein $a^{-1} \in K$ mit $a \cdot a^{-1} = 1_K$.

Bemerkungen

- für 0_K und 1_K schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- \mathbb{N}_0 erfüllt (K1)–(K4) mit der üblichen Addition und Multiplikation
- \mathbb{Z} erfüllt (K1)–(K4) und den ersten Teil von (K5)
- \mathbb{Q} erfüllt (K1)–(K5) und ist ein Körper

Beispiele: Körper

- neben \mathbb{Q} sind die bekannten Erweiterungen \mathbb{R} und \mathbb{C} Körper
- weitere wichtige Beispiele sind die **endlichen** Körper \mathbb{F}_q (auch $GF(q)$) mit q Elementen, wobei $q = p^n$ für eine Primzahl p und $n \in \mathbb{N}$
- der kleinste Körper \mathbb{F}_2 hat zwei Elemente 0 und 1 und ist auf der Menge $\{0, 1\}$ mit der Addition und Multiplikation definiert durch

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- $-0 = 0$, $-1 = 1$, und $1^{-1} = 1$
- die anderen Rechengesetze (K1)–(K4) kann man einfach nachprüfen
- \mathbb{F}_2 ist der „einzige“ Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
 - (K4) und (K2) definieren alle Ergebnisse bis auf $1 + 1$ und $0 \cdot 0$
 - $1 + 1 = 0$ ist erzwungen, da sonst keine -1 existieren würde
 - $0 \cdot 0 = 1$ würde zu folgendem Widerspruch führen:

$$1 = 0 \cdot 0 = 0 \cdot (1 + 1) \stackrel{(K3)}{=} 0 \cdot 1 + 0 \cdot 1 = 0 + 0 = 0$$

Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf \mathbb{N} , \mathbb{Z} und \mathbb{Q} eine Ordnung \leq definiert.
- Dabei ist \leq sogar eine **Totalordnung** (auch **lineare**, **vollständige** oder **totale Ordnung**), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente a und b

$$a \leq b \quad \text{oder} \quad b \leq a.$$

Es sind also **alle** Elemente miteinander vergleichbar (im Gegensatz zur Teilmengenrelation, die nur eine Ordnung aber **keine** Totalordnung ist) und für zwei verschiedene a und b gilt **genau eine** der Beziehungen

$$a < b \quad \text{oder} \quad b < a,$$

wobei $a < b$ durch $a \leq b \wedge a \neq b$ definiert ist.

- Darüber hinaus ist es praktisch, wenn die Totalordnung mit den Rechenoperationen „kompatibel“ ist und dies führt zum Begriff des **geordneten Körper**.

Geordnete Körper

Definition (Angeordneter Körper)

Ein Körper K mit einer totalen Ordnung \leq auf K heißt **angeordnet**, falls die folgenden **Anordnungsaxiome** für alle $a, b, c \in K$ gelten:

(A1) Falls $a \leq b$, dann gilt auch $a + c \leq b + c$.

(A2) Falls $a \leq b$ und $c \geq 0$, dann gilt auch $a \cdot c \leq b \cdot c$.

Bemerkungen

- \mathbb{N}_0 , \mathbb{Z} und \mathbb{Q} mit ihrer Ordnung erfüllen die Anordnungsaxiome
- \mathbb{Q} und die Erweiterung \mathbb{R} sind angeordnete Körper
- \mathbb{C} und endliche Körper können nicht angeordnet werden, z. B. für \mathbb{F}_2 führt sowohl die Festlegung $0 < 1$ als auch $1 < 0$ wegen $1 + 1 = 0$ zu einem Widerspruch:

$$0 < 1 \stackrel{(A1)}{\implies} 0 + 1 < 1 + 1 \iff 1 < 0$$

- (A1) und (A2) implizieren auch $a \cdot c \geq b \cdot c$ für $a \leq b$ und $c \leq 0$, da:

$$a \leq b \stackrel{(A1)}{\implies} a + ((-a) + (-b)) \leq b + ((-a) + (-b)) \implies -b \leq -a$$

und Multiplikation mit $-c \geq 0$ und Anwendung von (A2) ergibt $b \cdot c \leq a \cdot c$.

Reelle Zahlen

- \mathbb{Q} läßt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
 - \mathbb{Q} ist **dicht** in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
 - auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass $\sqrt{2}$ keine rationale Zahl ist (aber $\sqrt{2}$ entspricht einem Punkt auf der Zahlengeraden)
 - man kann \mathbb{Q} so zur Menge \mathbb{R} der **reellen Zahlen** erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
 - die formale Konstruktion von \mathbb{R} aus \mathbb{Q} überspringen wir hier
 - Standardkonstruktionen basieren auf **DEDEKINDSchen Schnitten** oder auf **Äquivalenzklassen von CAUCHY-Folgen** → Analysis
 - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf \mathbb{R} ($a \leq b$, wenn a links von b auf der Zahlengeraden liegt)
- ⇒ mit der üblichen Addition, Multiplikation und Ordnung ist die Menge der reellen Zahlen \mathbb{R} ein **angeordneter Körper**
- im Gegensatz zu \mathbb{Q} ist \mathbb{R} auch noch **vollständig** (siehe Analysis) und bis auf Isomorphie ist \mathbb{R} der einzige vollständige und angeordnete Körper
 - die Zahlen in $\mathbb{R} \setminus \mathbb{Q}$ heißen **irrationale Zahlen**, z. B. $\sqrt{2}$, e , π

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} ?$

Streng genommen geht aus den vorangegangenen Definitionen von \mathbb{Z} , \mathbb{Q} und \mathbb{R} nicht hervor, dass \mathbb{N} eine Teilmenge von \mathbb{Z} oder \mathbb{Z} eine Teilmenge von \mathbb{Q} ist. Zum Beispiel wurde \mathbb{Z} als die Faktormenge einer Äquivalenzrelation auf $\mathbb{N}_0 \times \mathbb{N}_0$ definiert und diese Faktormenge enthält formal \mathbb{N} nicht!

Auf der anderen Seite, haben wir eine injektive Funktion $n \mapsto [(n, 0)]$ von \mathbb{N} in diese Faktormenge angegeben, für die sich die auf \mathbb{N} definierte Addition und Multiplikation erhält, z. B. für die Addition ergibt sich aus der Definition sofort für alle natürlichen Zahlen ℓ , m und n , dass $\ell + m = n$ genau dann gilt, wenn $[(\ell, 0)] +_{\mathbb{Z}} [(m, 0)] = [(n, 0)]$. Diese Einbettung von \mathbb{N} erlaubt es \mathbb{N} als Teilmenge von \mathbb{Z} zu betrachten und wir werden von nun an \mathbb{N} immer als diese Teilmenge von \mathbb{Z} ansehen.

Genauso kann mit Hilfe der Funktion $z \mapsto [(z, 1)]$ die Menge der ganzen Zahlen in \mathbb{Q} eingebettet werden, welche wiederum durch $q \mapsto [(q)_{n \in \mathbb{N}}]$ als eine Teilmenge von \mathbb{R} aufgefasst werden kann. Von nun an werden wir auf Grund dieser Einbettungen sowohl die rationalen, als auch die ganzen und die natürlichen Zahlen als durch \leq vollständig geordnete Teilmengen der reellen Zahlen betrachten und die Addition und Multiplikation einfach mit $+$ und \cdot bezeichnen. Insbesondere gilt also

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Mächtigkeiten von Mengen

- Mengen A und B sind **gleichmächtig** $:\Leftrightarrow$ es gibt Bijektion zwischen A und B
- für $n \in \mathbb{N}_0$ schreiben wir $[n]$ als Kurzform für die Menge $\{1, \dots, n\}$

Definition

Eine Menge M heißt:

- **endlich**: falls M gleichmächtig zu $[n]$ für ein $n \in \mathbb{N}_0$, d. h. M hat genau n Elemente (M ist **n -elementig**, M ist eine **n -Menge**) und wir schreiben

$$|M| := n.$$

- **unendlich**: falls M **nicht** endlich ist.
- **abzählbar**: falls M endlich ist **oder** gleichmächtig mit \mathbb{N} ist.
- **überabzählbar**: falls M **nicht** abzählbar ist.

Bemerkungen

- $M \neq \emptyset$ ist abzählbar genau dann, wenn es eine surjektive Abbildung $f: \mathbb{N} \rightarrow M$ gibt und f heißt **Aufzählung** von M
- $n \mapsto n - 1$ zeigt \mathbb{N}_0 ist abzählbar
- $n \mapsto (-1)^n \lfloor n/2 \rfloor$ zeigt \mathbb{Z} ist abzählbar, wobei für $x \in \mathbb{R}$ mit $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$ bezeichnet wird

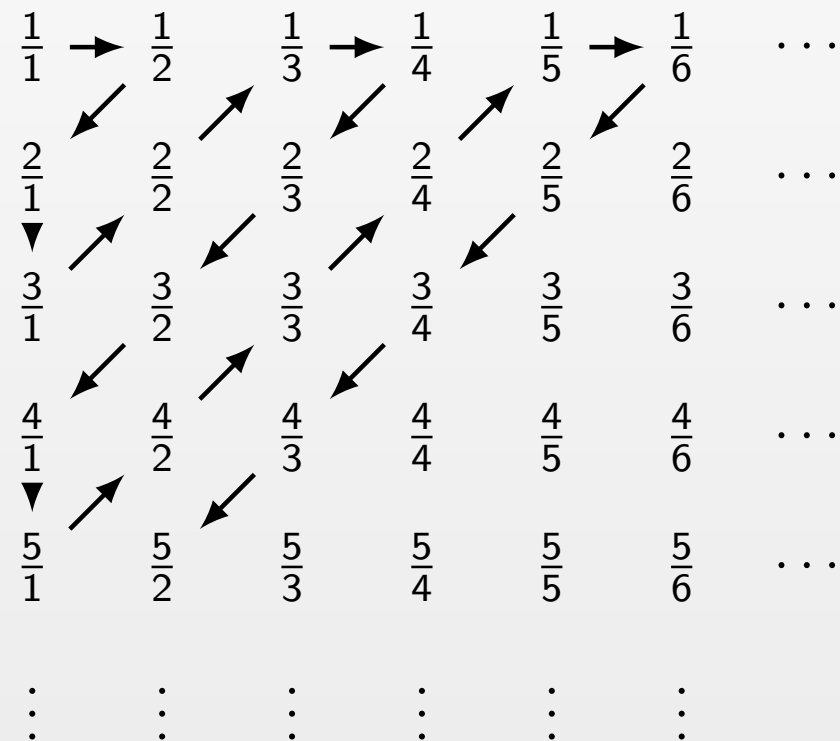
Mächtigkeit von \mathbb{Q}

Satz

Die Menge der rationalen Zahlen \mathbb{Q} ist abzählbar.

Beweis

Wir geben eine Aufzählung q_1, q_2, \dots der Menge der rationalen Zahlen > 0 an. Man erhält die Aufzählung, indem man im folgenden Bild bei den Bruch $\frac{1}{1}$ beginnt und den Pfeilen folgt:



Satz

Die Menge der rationalen Zahlen \mathbb{Q} ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, dass viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als $\frac{1}{1}$ und $\frac{2}{2}$ spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss. Es ist aber klar, dass jede rationale Zahl > 0 in dieser Aufzählung irgendwann einmal auftritt.

Mit dieser Aufzählung der rationalen Zahlen > 0 können wir nun aber leicht eine Aufzählung aller rationalen Zahlen angeben:

$$0, q_1, -q_1, q_2, -q_2, \dots$$

leistet das Gewünschte. □

Mächtigkeit von \mathbb{R}

Satz (CANTOR 1874)

Die Menge der reellen Zahlen \mathbb{R} ist überabzählbar.

Beweis: Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung s_1, s_2, s_3, \dots der reellen Zahlen s mit $0 < s < 1$. Die Zahlen s_n , $n \in \mathbb{N}$ lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle $i, j \in \mathbb{N}$ sei s_{ij} die Ziffer, die in der j -ten Nachkommastelle der Dezimaldarstellung von s_i steht:

$$s_1 = 0.s_{11}s_{12}s_{13}\dots$$

$$s_2 = 0.s_{21}s_{22}s_{23}\dots$$

$$\vdots \qquad \qquad \qquad \vdots$$

Nun definieren wir eine weitere reelle Zahl a , die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen $a_1a_2a_3\dots$ der Zahl a an. Für $i \in \mathbb{N}$ sei

$$a_i := \begin{cases} 4, & \text{falls } s_{ii} \neq 4 \text{ ist und} \\ 5, & \text{sonst.} \end{cases}$$

Es ist klar, dass $a = 0.a_1a_2a_3\dots$ echt zwischen 0 und 1 liegt. Die Zahl a ist so gewählt, dass es sich an der i -ten Nachkommastelle von s_i unterscheidet. Damit ist a von allen s_i , $i \in \mathbb{N}$ verschieden. \square

Teilbarkeit

Definition (Teiler)

Eine ganze Zahl $x \in \mathbb{Z}$ ist ein **Teiler** von $y \in \mathbb{Z}$, falls ein $d \in \mathbb{Z}$ existiert, sodass

$$y = d \cdot x.$$

- Wir sagen auch, y ist ein **Vielfaches** von x ist und schreiben $x \mid y$.
- Falls x kein Teiler von y ist, dann schreiben wir $x \nmid y$.

Bemerkungen

- jede ganze Zahl $x \in \mathbb{Z}$ teilt also die 0 $0 = 0 \cdot x$
- 0 ist nur Teiler von der 0
- es gilt für alle $x, y \in \mathbb{Z}$

$$x \mid y \iff -x \mid y \iff x \mid -y \iff -x \mid -y$$

- Teilbarkeiten in \mathbb{Z} lassen sich also auf Teilbarkeiten in \mathbb{N}_0 zurückführen

Teilbarkeitsrelation

Satz

Teilbarkeitsbeziehung $|$ definiert eine Relation auf \mathbb{Z} (bzw. auf \mathbb{N}_0) mit folgenden Eigenschaften:

- **reflexiv**, da $x | x$
- **transitiv**, da $x | y$ und $y | z$ bedeutet, dass es d_1, d_2 mit $y = d_1 \cdot x$ und $z = d_2 \cdot y$ gibt $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x | z$
- **antisymmetrisch auf \mathbb{N}_0** (aber **nicht** auf \mathbb{Z}), da $x | y$ und $y | x$ bedeutet $y = d_1 \cdot x$ und $x = d_2 \cdot y$ für geeignete d_1 und d_2
 $\implies y = d_1 \cdot d_2 \cdot y$ und $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$ oder $y = x = 0$

Des Weiteren gilt:

- $x_1 | y_1$ und $x_2 | y_2 \implies (x_1 \cdot x_2) | (y_1 \cdot y_2)$
- $(x \cdot y_1) | (x \cdot y_2)$ und $x \neq 0 \implies y_1 | y_2$
- $x | y_1$ und $x | y_2 \implies x | (y_1 \cdot z_1 + y_2 \cdot z_2)$ für alle z_1, z_2 .

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition (ggT und kgV)

Für ganze Zahlen $x, y \in \mathbb{Z}$ ist der **größte gemeinsame Teiler** ($\text{ggT}(x, y)$) von x und y ist die größte natürliche Zahl $n \in \mathbb{N}$, die sowohl x als auch y teilt, wobei man für $x = y = 0$ üblicherweise $\text{ggT}(0, 0) := 0$ setzt.

Das **kleinste gemeinsame Vielfache** ($\text{kgV}(x, y)$) von x und y ist die kleinste natürliche Zahl $n > 0$, die sowohl von x als auch von y geteilt wird, wobei man für $x = 0$ oder $y = 0$ üblicherweise $\text{kgV}(x, y) := 0$ setzt.

Beispiele

- $\text{ggT}(18, 45) = 9$ und $\text{kgV}(18, 45) = 90$ und $9 \cdot 90 = 810 = 18 \cdot 45$
- $\text{ggT}(24, 18) = 6$ und $\text{kgV}(24, 18) = 72$ und $6 \cdot 72 = 432 = 24 \cdot 18$
- Allgemein gilt tatsächlich (Beweis folgt später):

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|,$$

wobei $|z|$ der **Absolutbetrag** einer ganzen Zahl $z \in \mathbb{Z}$ ist.

Berechnung des ggT

- $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$ für alle $x, y \in \mathbb{Z} \implies$ o. B. d. A. seien $x, y \in \mathbb{N}_0$

Proposition

Für alle $x, y \in \mathbb{N}_0$ mit $x \geq y$ gilt $\text{ggT}(x, y) = \text{ggT}(x - y, y)$.

Beweis

Jeder Teiler von x und y teilt auch $x - y$. Somit gilt auch

$$\text{ggT}(x, y) \mid x - y \quad \text{und} \quad \text{ggT}(x, y) \mid y \implies \text{ggT}(x, y) \leq \text{ggT}(x - y, y).$$

Auf der anderen Seite teilt auch jeder Teiler von $x - y$ und y auch $x - y + y = x$ und somit gilt auch

$$\text{ggT}(x - y, y) \mid x \quad \text{und} \quad \text{ggT}(x - y, y) \mid y \implies \text{ggT}(x - y, y) \leq \text{ggT}(x, y).$$

Also muss gelten $\text{ggT}(x, y) = \text{ggT}(x - y, y)$ □

- Proposition liefert rekursiven Algorithmus für die Berechnung des ggT

Einfacher EUKLIDISCHER Algorithmus

Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

Einfacher rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x-y,y);  
    else  
        return ggT(x,y-x);  
}
```

- Algorithmus berechnet den $\text{ggT}(|x|, |y|)$ (Korrektheit):
 - Induktion über $n = |x| + |y|$ mit mehreren Vorgängern
 - Induktionsanfang $x = 0$ oder $y = 0$ klar wegen der Definition des ggT
 - Induktionsschritt für $|x| > 0$ und $|y| > 0$ durch Proposition
- **Problem:** langsamer Algorithmus – Laufzeit $O(|x| + |y|)$ **keine** polynomielle Laufzeit in der Länge der Eingabe $\log |x| + \log |y|$

Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn x sehr groß und y sehr klein ist, dann wird sehr oft y von x abgezogen
- z. B. $x = 2^{51}$ und $y = 2$ resultiert in $2^{50} \sim 10^{15}$ Subtraktionen für die mein Rechner mehr als **6 Tage** braucht
- für $x = 2^{61}$ und $y = 2$ braucht der Algorithmus dann ~ 1000 -mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist
→ exponentielle Laufzeit

Beobachtung

- beim einfachen EUKLIDischen Algorithmus ziehen wir y solange ab, bis $z = x - y < y$ erreicht ist
- ⇒ **Division mit Rest** von x und y liefert uns dieses z in einem Schritt

Division mit Rest

Definition und Satz

Für je zwei ganze Zahlen $x, y \in \mathbb{Z}$ mit $y \neq 0$ gibt es **eindeutig** bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$, sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leq r < |y|. \quad (*)$$

Die Zahl q heißt **Quotient** und r heißt **Rest** der Division.

- **div**: $\mathbb{Z}^2 \rightarrow \mathbb{Z}$ ordnet (x, y) den Quotienten q zu,
- **mod**: $\mathbb{Z}^2 \rightarrow \mathbb{N}_0$ ordnet (x, y) den Rest r zu.

Beweis

- **Existenz**: Eine der $|y| \geq 1$ hintereinander liegenden ganzen Zahlen

$$x - 0, x - 1, \dots, x - (|y| - 1)$$

ist ein Vielfaches von y .

\implies es gibt $r \in \{0, 1, \dots, |y| - 1\}$ und $q \in \mathbb{Z}$ mit $x - r = q \cdot y$. ✓

- **Eindeutigkeit**: Falls $qy + r = x = q'y + r'$ wie in (*), dann gilt

$$0 = (q - q')y + (r - r') \quad \text{mit} \quad |r - r'| < |y|.$$

$\implies y \mid (r - r')$, da $y \mid 0$ und $y \mid (q - q')y$

\implies wegen $|r - r'| < |y|$ folgt dann $r = r'$

$\implies qy = q'y$ und wegen $y \neq 0$ folgt $q = q'$ ✓ □

Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest
- Proposition 2: $\text{ggT}(x, y) = \text{ggT}(\text{mod}(x, y), y)$
→ Beweis wie bei der Proposition zuvor

Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {
    if ( x==0 ) return y;
    if ( y==0 ) return x;
    if ( x>=y )
        return ggT(x%y, y); /* x%y = mod(x, y) */
    else
        return ggT(x, y%x);
}
```

- **Korrektheit:** Algorithmus berechnet den $\text{ggT}(|x|, |y|)$,
→ Induktionsbeweis wie zuvor mit Proposition 2
- mod ist etwas teurer (Laufzeit) als Subtraktion, aber der verbesserte EUKLIDische Algorithmus hat polynomielle Laufzeit in der Länge der Eingabe $\log |x| + \log |y|$

Kongruenzen

Definition

Ganze Zahlen $x, y \in \mathbb{Z}$ sind **kongruent modulo m** für eine natürliche Zahl $m \in \mathbb{N}$, falls

$$\text{mod}(x, m) = \text{mod}(y, m),$$

d. h. x und y haben denselben Rest bei Division durch m . In diesem Fall sagen wir auch, **x ist kongruent zu y modulo m** und schreiben

$$x \equiv y \pmod{m}.$$

Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo m definiert Äquivalenzrelation auf \mathbb{Z} :
 - Reflexivität ✓
 - Symmetrie ✓
 - Transitivität: $m \mid x - y$ und $m \mid y - z \implies m \mid x - y + y - z$ ✓

Restklassen

Definition (Restklassen)

Für jede natürliche Zahl $m \in \mathbb{N}$ und jede ganze Zahl $x \in \mathbb{Z}$ heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

die **Restklasse von x modulo m** .

Folgerungen

- für jedes $m \in \mathbb{N}$ gibt es genau m verschiedene Restklassen modulo m

$$[0]_m, [1]_m, \dots, [m-1]_m.$$

- die Restklassen bilden eine Partition von \mathbb{Z} , d. h. sie sind paarweise disjunkt und

$$\mathbb{Z} = [0]_m \cup \dots \cup [m-1]_m$$

- Menge der Restklassen (Faktormenge der Äquivalenzrelation kongruent modulo m)

$$\mathbb{Z}/m\mathbb{Z} := \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

Modulare Arithmetik

- mit Restklassen kann man gut rechnen
- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m + [z']_m := [z + z']_m$ ist **wohldefinierte** Addition auf $\mathbb{Z}/m\mathbb{Z}$
 - Addition auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
 - $[0]_m$ ist neutrales Element der Addition auf $\mathbb{Z}/m\mathbb{Z}$
 - Subtraktion kann durch $[z]_m - [z']_m := [z - z']_m$ definiert werden
 - $[-z]_m$ ist invers zu $[z]_m$, d. h. $-[z]_m = [-z]_m$
 - für $\ell \in \{0, \dots, m-1\}$ gilt $[-\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \cdot [z']_m := [z \cdot z']_m$ ist **wohldefinierte** Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$
 - Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
 - $[1]_m$ ist neutrales Element der Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$
 - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
$$\begin{aligned} [2]_4 \cdot [0]_4 &= [0]_4, & [2]_4 \cdot [1]_4 &= [2]_4, \\ [2]_4 \cdot [2]_4 &= [4]_4 = [0]_4, & [2]_4 \cdot [3]_4 &= [6]_4 = [2]_4 \end{aligned}$$
- $\Rightarrow [2]_4$ hat kein multiplikativ Inverses in $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes $m \in \mathbb{N}$ heißt $\mathbb{Z}/m\mathbb{Z}$ mit Verknüpfungen $+$ und \cdot **Restklassenring modulo m** .

- $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{\mathbb{Z}\}$ ist **trivial (Nullring)**, aber $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ist sogar ein Körper

GAUSSklammer

Definition

Sei $\xi \in \mathbb{R}$ eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$ die kleinste ganze Zahl $z \in \mathbb{Z}$ mit $z \geq \xi$.
- $\lfloor \xi \rfloor$ die größte ganze Zahl $z \in \mathbb{Z}$ mit $z \leq \xi$.

Beobachtung

Für alle $z \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt

$$\operatorname{div}(z, n) = \left\lfloor \frac{z}{n} \right\rfloor \quad \text{und} \quad \operatorname{mod}(z, n) = z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor.$$

Primzahlen

Definition (Primzahlen)

Eine natürliche Zahl $p \geq 2$ heißt **Primzahl**, falls 1 und p die einzigen Teiler von p in \mathbb{N} sind.

- Menge der Primzahlen $\{2, 3, 5, 7, 11, 13, \dots, 2011, 2017, 2027, \dots\}$
- 1 und n heißen auch die **trivialen (natürlichen) Teiler** von $n \in \mathbb{N}$
- 1, -1 , z und $-z$ sind die **trivialen (ganzen) Teiler** von $z \in \mathbb{Z}$

Definition (teilerfremd)

Zwei ganze Zahlen heißen **teilerfremd** (auch **relativ prim**), falls die 1 der einzige gemeinsame Teiler in \mathbb{N} ist. Es gilt also

$$x, y \in \mathbb{Z} \text{ sind teilerfremd} \iff \text{ggT}(x, y) = 1$$

- Teilerfremdheit ist **nicht** reflexiv, **nicht** transitiv, aber symmetrisch
- Für teilerfremde $z \in \mathbb{Z}$ und $m \in \mathbb{N}$ gilt:
 $(z \cdot x) \equiv (z \cdot y) \pmod{m} \implies x \equiv y \pmod{m}$ für alle $x, y \in \mathbb{Z}$.

Falls $p \in \mathbb{N}$ eine Primzahl ist, dann ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper.

Primfaktorzerlegung

Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl $n \in \mathbb{N}$ gibt es

- ein $k \in \mathbb{N}_0$,
- paarweise verschiedene Primzahlen p_1, \dots, p_k
- und natürliche Zahlen $\alpha_1, \dots, \alpha_k \in \mathbb{N}$,

sodass

$$n = \prod_{i=1}^k p_i^{\alpha_i}.$$

Diese Produktdarstellung von n heißt **Primfaktorzerlegung** und ist bis auf die Reihenfolge der Faktoren eindeutig.

Bemerkungen

- für $n = 1$ ist $k = 0$ und der Satz folgt, da das leere Produkt 1 ist
- für $n \geq 2$ ist immer $k \geq 1$
- Sicherheit vieler Verschlüsselungsverfahren beruht auf der Annahme, dass für gegebenes n die Primfaktorzerlegung **nicht** effizient berechenbar ist
 - theoretisch effizient berechenbar mit Quantencomputern
 - Entscheidungsproblem liegt in **NP** \cap **coNP**

Existenz der Primfaktorzerlegung

Beweis (Widerspruch)

Sei n die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$, da das leere Produkt eine Primfaktorzerlegung der 1 ist
- n ist keine Primzahl, da sonst $n = p^\alpha$ mit $p = n$ und $\alpha = 1$ eine Primfaktorzerlegung von n ist


⇒ n hat von 1 und n verschiedene Teiler

⇒ es gibt $x, y \in \mathbb{N}$ mit

$$1 < x < n, \quad 1 < y < n \quad \text{und} \quad n = xy$$

Da n die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von x und y , d. h. für geeignete $k, \ell \in \mathbb{N}$, Primzahlen $p_1, \dots, p_k, q_1, \dots, q_\ell$ und $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$ gilt:

$$x = \prod_{i=1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{j=1}^{\ell} q_j^{\beta_j}.$$

Somit ist $n = xy = \prod_{i=1}^k p_i^{\alpha_i} \prod_{j=1}^{\ell} q_j^{\beta_j}$ und ggf. durch das Zusammenfassen von Faktoren (falls $p_i = q_j$), erhalten wir eine Primfaktorzerlegung von n . 

Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem **Lemma von EUKLID**, welches eine Konsequenz des **Lemmas von BÉZOUT** ist

Lemma (BÉZOUT)

Für alle ganzen Zahlen $x, y \in \mathbb{Z}$ gibt es ganze Zahlen $s, t \in \mathbb{Z}$, sodass

$$\text{ggT}(x, y) = sx + ty.$$

- Der $\text{ggT}(x, y)$ kann als **Linearkombination** von x und y dargestellt werden.
- Für teilerfremde $x, y \in \mathbb{Z}$ gibt es somit $s, t \in \mathbb{Z}$ mit $sx + ty = 1$.

Beweis (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A. $x, y \in \mathbb{N}_0$ (**Warum?**) und $x \geq y$ (**Warum?**)
- Induktion nach $x + y$ mit mehreren Vorgängern
- Induktionsanfang: $y = 0$, klar da dann $\text{ggT}(x, 0) = x$ für alle x
- Induktionsschritt:

$$\text{ggT}(x, y) \stackrel{\text{Prop.}}{=} \text{ggT}(x - y, y) \stackrel{\text{l.A.}}{=} s'(x - y) + t'y = s'x + (t' - s')y$$

und die Aussage folgt mit $s = s'$ und $t = t' - s'$ □

Erweiterter EUKLIDISCHER Algorithmus

rekursive Berechnung von $\text{ggT}(x, y)$, s und t mit $\text{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s, int *t) {
    if ( x==0 ) { *s=0; *t=1; return y; }
    if ( y==0 ) { *s=1; *t=0; return x; }
    int ggT, sp, tp;           /* Zwischenergebnisse speichern */
    if ( x>y ) {
        ggT = erwEuklid(x%y, y, &sp, &tp);      /* % = mod, / = div */
        *s = sp; *t = tp - sp*(x/y);           /* s und t verrechnen */
        return ggT;
    }
    else {
        ggT = erwEuklid(x, y%x, &sp, &tp);
        *s = sp - tp*(y/x); *t = tp;           /* s und t verrechnen */
        return ggT;
    }
}
```

Korrektheit folgt induktiv mit $x = q \cdot y + r$ für $q = \text{div}(x, y)$ und $r = \text{mod}(x, y)$ durch:

$$\text{ggT}(x, y) = \text{ggT}(r, y) = s'r + t'y$$

und wegen $r = x - q \cdot y$ folgt $\text{ggT}(x, y) = s'x + (t' - s' \cdot q)y$.

Lemma von EUKLID

Lemma (EUKLID)

Für alle ganzen Zahlen $x, y \in \mathbb{Z}$ und jede natürliche Zahl $n \in \mathbb{N}$ gilt

$$n \mid xy \quad \text{und} \quad \text{ggT}(x, n) = 1 \quad \implies \quad n \mid y.$$

Insbesondere teilt also jede Primzahl p einen Faktor x oder y , falls p Teiler des Produkts xy ist.

Beweis

Wegen BÉZOUTS Lemma (für x und n) gibt es $s, t \in \mathbb{Z}$ mit

$$sx + tn = \text{ggT}(x, n) = 1 \quad \implies \quad sxy + tny = y.$$

Da $n \mid xy$ gibt es ein $d \in \mathbb{Z}$ mit $xy = dn$ und damit erhalten wir

$$y = s \cdot dn + tny = (sd + ty)n.$$

Somit ist y ein Vielfaches von n . □

Eindeutigkeit der Primfaktorzerlegung

Beweis (Widerspruch)


Sei n die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$, da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
- n ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
- beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor p haben, da sonst n/p eine kleinere Zahl mit verschiedenen Primfaktorzerlegungen wäre
 \Rightarrow es gibt unterschiedliche Primzahlen p und q und $x, y \in \mathbb{N}$ mit

$$1 < x < n, \quad 1 < y < n, \quad x \neq y \quad \text{und} \quad px = n = qy$$

Insbesondere haben wir

$$p \mid qy \quad \text{und} \quad \text{ggT}(p, q) = 1.$$

Nach dem Lemma von EUKLID ist p also ein Teiler von y , aber dies widerspricht der obigen Beobachtung, dass wegen der minimalen Wahl von n keine Primzahl in beiden Primfaktorzerlegungen vorkommt. 

ggT und kgV und Primfaktoren

Satz

Für alle ganzen Zahlen x und $y \in \mathbb{Z}$ gilt

$$\text{ggT}(x, y) \cdot \text{kgV}(x, y) = |x \cdot y|.$$

Beweis

- o. B. d. A. $x, y \in \mathbb{N}_0$ (Warum?)
- falls $x = 0$ oder $y = 0$, dann $\text{kgV}(x, y) = 0$ und die Formel folgt
- seien p_1, \dots, p_ℓ alle gemeinsamen Primfaktoren von x und y und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}$$

die Primfaktorzerlegungen von x und y

Damit folgt

$$\text{ggT}(x, y) = \prod_{i=1}^{\ell} p_i^{\min(\alpha_i, \beta_i)}$$

$$\text{kgV}(x, y) = \prod_{i=1}^{\ell} p_i^{\max(\alpha_i, \beta_i)} \cdot \prod_{i=\ell+1}^k p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^m q_i^{\beta_i}.$$

Da $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$ folgt die Aussage. □

Wieviele Primzahlen gibt es?

Satz (EUKLID 300v. Chr.)

Es gibt unendlich viele Primzahlen.

Beweis (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen p_1, \dots, p_k .


- **Beobachtung:** N und $N + 1$ haben keinen gemeinsamen Teiler ≥ 2 , da jeder Teiler auch $N + 1 - N = 1$ teilt

- betrachte das Produkt $N = p_1 \cdot \dots \cdot p_k$

$\Rightarrow N$ und $N + 1$ haben keine gemeinsamen Primfaktoren

\Rightarrow alle Primzahlen aus der Primfaktorzerlegung von $N + 1$ sind verschieden von p_1, \dots, p_k

- wegen $N + 1 > 1$ gibt es auch mindestens einen Primfaktor q von $N + 1$

Es gibt also eine weitere Primzahl q verschieden von p_1, \dots, p_k . 

4. Elementare Kombinatorik

Rechenregeln für endliche Mengen

- **Erinnerung:** für endliche Mengen M ist $|M|$ die Anzahl der Elemente von M , auch **Kardinalität von M** genannt
 $|M| = n \Leftrightarrow M$ gleichmächtig wie $[n] = \{1, \dots, n\} \Leftrightarrow \exists$ Bijektion $M \longrightarrow [n]$

- falls $A \cap B = \emptyset$ dann gilt $|A \cup B| = |A| + |B|$ und im Allgemeinen für paarweise disjunkte endliche Mengen A_1, \dots, A_k gilt die **Additionsregel**

$$\left| \bigcup_{i=1}^k A_i \right| = |A_1 \cup \dots \cup A_k| = |A_1| + \dots + |A_k| = \sum_{i=1}^k |A_i|.$$

Wieso? Beweis?

klar ✓

- für beliebige endliche Mengen A, B gilt $|A \times B| = |A| \cdot |B|$ und im Allgemeinen für endliche Mengen A_1, \dots, A_k gilt die **Multiplikationsregel**

$$\left| \prod_{i=1}^k A_i \right| = |A_1 \times \dots \times A_k| = |A_1| \cdot \dots \cdot |A_k| = \prod_{i=1}^k |A_i|.$$

Wieso? Beweis?

z. B. Induktion nach k und $|A_k|$ ✓

- $|A| = |B| \iff \exists$ Bijektion $A \longrightarrow B$ **Gleichheitsregel**

Geordnete Teilmengen/Tupel

k -Tupel von n -elementigen Mengen

Für natürliche Zahlen $n, k \in \mathbb{N}_0$ ist die Anzahl der k -Tupel einer n -elementigen Menge M gegeben durch

$$|M^k| \stackrel{\text{Multiplikationsregel}}{=} |M|^k = n^k.$$

Für $n = k = 0$ gilt $0^0 = 1$, gerechtfertigt durch den leeren 0-Tupel.

Bsp.: es gibt $2^3 = 8$ verschiedene **binäre Tripel** (3-Tupel mit Elementen aus $\{0, 1\}$)
 $(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)$

k -Tupel von n -Mengen ohne Doppelungen/Wiederholungen

Für natürliche Zahlen $n, k \in \mathbb{N}_0$ ist die Anzahl der k -Tupel einer n -elementigen Menge M , in denen kein Element doppelt vorkommt, gegeben durch

$$|M| \cdot (|M| - 1) \cdot \dots \cdot (|M| - (k - 1)) = n \cdot (n - 1) \cdot \dots \cdot (n - (k - 1)) =: (n)_k.$$

Für die **fallende Faktorielle** $(n)_k$ schreibt man auch $n^{\underline{k}}$ (z. B. im Skript).

- wegen des leeren Produkts ist $(n)_0 = 1$ und tatsächlich ist das leere 0-Tupel das einzige Tupel, welches hier gezählt wird
- für $n < k$ gilt $(n)_k = 0$ und für $n = k$ erhält man die Anzahl der Auflistungen

Permutationen

Definition (Permutation)

Eine bijektive Abbildung $\pi: M \longrightarrow M$ auf einer (abzählbaren) Menge M heißt **Permutation**.

Ist M eine endliche Menge $\{m_1, \dots, m_n\}$, wobei wir annehmen, dass die m_i paarweise verschieden sind, so kann man eine Permutation $\pi: M \longrightarrow M$ darstellen durch

$$\begin{pmatrix} m_1 & m_2 & \dots & m_n \\ \pi(m_1) & \pi(m_2) & \dots & \pi(m_n) \end{pmatrix}.$$

Falls $M = [n]$, dann schreiben wir auch abkürzend nur die „untere Zeile“ $(\pi(1), \dots, \pi(n))$ an Stelle von $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$.

Bsp.: $\pi(1) = 2$, $\pi(2) = 4$, $\pi(3) = 3$ und $\pi(4) = 1$ definiert eine Permutation auf $[4]$ und wird beschrieben durch:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{bzw.} \quad (2, 4, 3, 1).$$

Fakultät

Definition (Fakultät)

Für jede natürliche Zahl $n \in \mathbb{N}_0$ heißt

$$n! := \prod_{i=1}^n i = (n)_n$$

Fakultät von n . Insbesondere ist $0! = 1$.

Bemerkungen

- Bsp.: $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$
- Fakultät ist schnell wachsende Funktion auf \mathbb{N}_0 , z. B. $70! > 10^{100}$
- Anzahl Permutationen einer n -elementigen Menge M
 - = Anzahl Bijektion von M nach M
 - = Anzahl der n -Tupel von M ohne Doppelungen = $(n)_n = n!$
- $0! = 1$ entspricht der leeren Abbildung, die eine Bijektion auf \emptyset ist

Ungeordnete Teilmengen

k -elementige Teilmengen n -elementigen Mengen

Für natürliche Zahlen $n, k \in \mathbb{N}_0$ mit $n \geq k$ ist die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge M gegeben durch

$$|\{A \subseteq M : |A| = k\}| = \binom{n}{k} := \frac{n!}{k! \cdot (n-k)!}.$$

Für $k > n$ gibt es offensichtlich keine k -elementigen Teilmengen von M .

Insbesondere $\binom{n}{k} \in \mathbb{N}_0$ und heißt **Binomialkoeffizient**.

Beweis: Sei M eine n -elementige Menge und $k \in \mathbb{N}_0$ mit $n \geq k$.

- es gibt $(n)_k$ geordnete k -Tupel (k -elementige Teilmengen) mit Elementen aus M ohne Wiederholungen und es gilt

$$(n)_k = n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

- hierbei zählen wir jede k -elementige Teilmenge $A \subseteq M$ genau so oft, wie wir die Elemente von A anordnen können, also $|A|! = k!$ Mal

$$\Rightarrow |\{A \subseteq M : |A| = k\}| = \frac{(n)_k}{k!} = \frac{n!}{k! \cdot (n-k)!}$$

□

Rekursive Identität der Binomialkoeffizienten

Satz

Für alle natürlichen Zahlen $n, k \in \mathbb{N}$ mit $n > k$ gilt

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

1. **Beweis** (einsetzen und nachrechnen):

$$\begin{aligned} \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} \\ &= \frac{(n-k)(n-1)!}{k!(n-k)!} + \frac{k(n-1)!}{k!(n-k)!} \\ &= \frac{(n-k+k)(n-1)!}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} = \binom{n}{k}. \end{aligned}$$



Rekursive Identität der Binomialkoeffizienten

Satz

Für alle natürlichen Zahlen $n, k \in \mathbb{N}$ mit $n > k \geq 1$ gilt

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

2. Beweis (kombinatorische Interpretation ausnutzen):

Sei M eine n -elementige Menge und $x \in M$ (existiert wegen $n \geq 2$).

■ die Menge der k -elementigen Teilmengen von M kann man aufspalten in die Mengen solcher Teilmengen,

■ die x nicht enthalten

davon gibt es $\binom{n-1}{k}$

■ die x enthalten

davon gibt es $\binom{n-1}{k-1}$

\Rightarrow

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

Bemerkung:

■ rekursive Berechnung wegen vieler Doppelberechnungen nicht effizient

□

Binomischer Lehrsatz

Satz (Binomischer Lehrsatz)

Seien $x, y \in \mathbb{R}$. Dann gilt für alle $n \in \mathbb{N}_0$

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

Konsequenzen:

- für $x = y = 1$ folgt die Identität $2^n = (1 + 1)^n = \sum_{\ell=0}^n \binom{n}{\ell}$
- für $n = 2$ folgen die **binomischen Formeln**

$$(x + y)^2 = x^2 + 2xy + y^2 \quad \text{und} \quad (x - y)^2 = x^2 - 2xy + y^2$$

- für $n = 3$ gilt $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$.

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

Beweis (Induktion nach n)

- Induktionsanfang $n = 0$: klar, wegen $(x + y)^0 = 1 = \binom{0}{0} x^0 y^0$
- Induktionsschritt von n nach $n + 1$:

✓

$$(x + y)^{n+1} \stackrel{\text{l.A.}}{=} (x + y) \cdot \sum_{\ell=0}^n \binom{n}{\ell} x^{n-\ell} y^\ell$$

Es gilt

$$x \sum_{\ell=0}^n \binom{n}{\ell} x^{n-\ell} y^\ell = \sum_{\ell=0}^n \binom{n}{\ell} x^{n+1-\ell} y^\ell = x^{n+1} + \sum_{\ell=1}^n \binom{n}{\ell} x^{n+1-\ell} y^\ell$$

sowie

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

Mit $\binom{n+1}{\ell} = \binom{n}{\ell} + \binom{n}{\ell-1}$ folgt also

$$(x + y)^{n+1} = \underbrace{\binom{n+1}{0} x^{n+1} y^0}_{=x^{n+1}} + \sum_{\ell=1}^n \binom{n+1}{\ell} x^{n+1-\ell} y^\ell + \underbrace{\binom{n+1}{n+1} x^0 y^{n+1}}_{=y^{n+1}} = \sum_{\ell=0}^{n+1} \binom{n+1}{\ell} x^{n+1-\ell} y^\ell$$

□

Kugeln auf Gefäße aufteilen

Partitionen einer natürlichen Zahl

Für natürliche Zahlen $m \in \mathbb{N}_0$ und $\ell \in \mathbb{N}$ gibt es genau

$$\binom{m + \ell - 1}{\ell - 1} = \binom{\ell + m - 1}{m}$$

Möglichkeiten, um m als Summe von ℓ natürlichen Zahlen $m_1, \dots, m_\ell \in \mathbb{N}_0$ darzustellen, d. h. $|\{(m_1, \dots, m_\ell) \in \mathbb{N}_0^\ell : m_1 + \dots + m_\ell = m\}| = \binom{m + \ell - 1}{\ell - 1}$.

Interpretation: Verteile m ununterscheidbare Kugel auf ℓ unterscheidbare Gefäße
Gefäß i bekommt m_i Kugeln

Beweis: Betrachte m als Folge von m Einsen und für $i = 1, \dots, \ell - 1$ „trenne“ m_i von m_{i+1} durch das Einfügen einer Null. Z. B. für $m = 6$ und $\ell = 4$ kodiert

110111001

die Zerlegung

$$m_1 = 2, \quad m_2 = 3, \quad m_3 = 0 \quad \text{und} \quad m_4 = 1.$$

Tatsächlich definiert dies eine Bijektion zwischen den Zerlegungen von m und den 0-1-Folgen der Länge $m + \ell - 1$ mit m Einsen. Eine solche 0-1-Folge ist bestimmt durch die Platzierung der Nullen und dafür gibt es $\binom{m + \ell - 1}{\ell - 1}$ Möglichkeiten. \square

Anagramme

Zeichenketten mit vorgegebener Buchstabenverteilung

Für natürliche Zahlen $\ell \in \mathbb{N}$ und $m_1, \dots, m_\ell \in \mathbb{N}_0$ und Buchstaben/Zeichen Z_1, \dots, Z_ℓ gibt es genau

$$\frac{(\sum_{i=1}^{\ell} m_i)!}{\prod_{i=1}^{\ell} (m_i!)} =: \binom{m_1 + \dots + m_\ell}{m_1, \dots, m_\ell}$$

verschiedene Zeichenketten der Länge $m := \sum_{i=1}^{\ell} m_i$, für $i = 1, \dots, \ell$ jeweils m_i -Mal das Zeichen Z_i enthalten.

Insbesondere $\binom{m_1 + \dots + m_\ell}{m_1, \dots, m_\ell} \in \mathbb{N}_0$ und heißt **Multinomialkoeffizient**.

Bemerkungen:

- Wörter, die aus einem Wort durch Vertauschung/Permutation der Buchstaben entstehen, nennt man **Anagramme**, z. B.

AMPEL LAMPE PALME oder ERLE LEER

- in dem Problem oben müssen die Wörter nicht unbedingt Sinn ergeben
- für $m_1 = \dots = m_\ell = 1$ ergibt jede Permutation ein anderes Anagramm

→ $\ell!$ „Anagramme“

Anagramme – Beweis

Zeichenketten mit vorgegebener Buchstabenverteilung

Für natürliche Zahlen $\ell \in \mathbb{N}$ und $m_1, \dots, m_\ell \in \mathbb{N}_0$ und Buchstaben/Zeichen Z_1, \dots, Z_ℓ gibt es genau

$$\frac{(\sum_{i=1}^{\ell} m_i)!}{\prod_{i=1}^{\ell} (m_i!)} = \binom{m_1 + \dots + m_\ell}{m_1, \dots, m_\ell}$$

verschiedene Zeichenketten der Länge $m := \sum_{i=1}^{\ell} m_i$, für $i = 1, \dots, \ell$ jeweils m_i -Mal das Zeichen Z_i enthalten.

Beweis

- ausgehend von der Zeichenkette beginnend mit m_1 Zeichen Z_1 , gefolgt von m_2 Zeichen Z_2 , hinzu m_ℓ Zeichen Z_ℓ , gibt es $(\sum_{i=1}^{\ell} m_i)!$ Permutationen dieser Zeichenkette
- allerdings ergeben Permutationen die gleiche Zeichenkette, wenn sie jeweils nur Zeichen vom gleich Typ vertauschen
- so gibt es für jede Permutation genau $\prod_{i=1}^{\ell} (m_i!)$ Permutationen, die die gleiche Zeichenkette erzeugen (unabhängig kann man jeweils auf $m_i!$ Weisen die Zeichen vom Typ Z_i vertauschen)
- es gibt also nur $(\sum_{i=1}^{\ell} m_i)! / \prod_{i=1}^{\ell} (m_i!)$ Permutationen, die unterschiedliche Zeichenketten erzeugen □

Multinomialatz

- für $\ell = 2$ reduzieren **Multinomialkoeffizienten** zu Binomialkoeffizienten

$$\binom{m_1 + m_2}{m_1} = \frac{(m_1 + m_2)!}{m_1! m_2!} = \binom{m_1 + m_2}{m_1, m_2} = \binom{m_1 + m_2}{m_2}$$

- der Multinomialatz erweitert dementsprechend den binomischen Lehrsatz

Satz (Multinomialatz)

Seien $\ell \in \mathbb{N}_0$ und $x_1, \dots, x_\ell \in \mathbb{R}$. Dann gilt für alle $n \in \mathbb{N}_0$

$$\begin{aligned} (x_1 + \dots + x_\ell)^n &= \left(\sum_{i=1}^{\ell} x_i \right)^n = \sum_{n_1 + \dots + n_\ell = n} \binom{n}{n_1, \dots, n_\ell} \prod_{i=1}^{\ell} x_i^{n_i} \\ &= \sum_{n_1 + \dots + n_\ell = n} \binom{n}{n_1, \dots, n_\ell} x_1^{n_1} \cdot \dots \cdot x_\ell^{n_\ell}, \end{aligned}$$

wobei die Summe über alle ℓ -Tupel $(n_1, \dots, n_\ell) \in \mathbb{N}_0^\ell$ mit $\sum_{i=1}^{\ell} n_i = n$ läuft.

Multinomialsatz – Beweis

Satz (Multinomialsatz)

Seien $\ell \in \mathbb{N}_0$ und $x_1, \dots, x_\ell \in \mathbb{R}$. Dann gilt für alle $n \in \mathbb{N}_0$

$$(x_1 + \dots + x_\ell)^n = \sum_{n_1 + \dots + n_\ell = n} \binom{n}{n_1, \dots, n_\ell} x_1^{n_1} \cdot \dots \cdot x_\ell^{n_\ell}.$$

Beweis: Wir können

$$(x_1 + \dots + x_\ell)^n = \underbrace{(x_1 + \dots + x_\ell) \cdot \dots \cdot (x_1 + \dots + x_\ell)}_{n \text{ Faktoren}}$$

durch Ausmultiplizieren berechnen. Für $n_1, \dots, n_\ell \in \mathbb{N}_0$ mit $n_1 + \dots + n_\ell = n$ zählen wir, wie oft das Produkt $x_1^{n_1} \cdot \dots \cdot x_\ell^{n_\ell}$ beim Ausmultiplizieren auftritt. Beim Ausmultiplizieren wählen wir aus jedem der n Faktoren $(x_1 + \dots + x_\ell)$ eine Variable aus. Wir wählen also eine Zeichenkette der Länge n aus den Zeichen x_1, \dots, x_ℓ . Um das Produkt $x_1^{n_1} \cdot \dots \cdot x_\ell^{n_\ell}$ zu erhalten, muss in der Zeichenkette, die wir auswählen, die Variable x_1 genau n_1 -mal auftreten, die Variable x_2 n_2 -mal und so weiter. Wir wissen bereits (siehe Anagramme), dass es genau $\binom{n}{n_1, \dots, n_\ell}$ solche Zeichenketten gibt. Damit ist der Koeffizient vor $x_1^{n_1} \cdot \dots \cdot x_\ell^{n_\ell}$, der sich beim Ausmultiplizieren von $(x_1 + \dots + x_\ell)^n$ ergibt, der Multinomialkoeffizient $\binom{n}{n_1, \dots, n_\ell}$. \square

Ziehen von Elementen

Grundproblem

Wieviele Möglichkeiten gibt es, k Elemente aus einer n -elementigen Menge zu ziehen?

Hierbei unterscheidet man folgende Varianten:

- ziehen **mit** Zurücklegen, wobei die Reihenfolge, in der die Elemente gezogen werden, **mit** berücksichtigt wird

$$k\text{-Tupel} \implies n^k$$

- ziehen **ohne** Zurücklegen, **mit** Berücksichtigung der Reihenfolge

$$k\text{-Tupel ohne Wiederholung} \implies (n)_k$$

- ziehen **ohne** Zurücklegen, **ohne** Berücksichtigung der Reihenfolge

$$k\text{-elementige Teilmengen} \implies \binom{n}{k}$$

- ziehen **mit** Zurücklegen, **ohne** Berücksichtigung der Reihenfolge

???

Ziehen mit Zurücklegen ohne Reihenfolge

Satz

Für natürliche Zahlen $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$ gibt es genau $\binom{n+k-1}{k}$ Möglichkeiten, k Elemente mit Zurücklegen aus einer n -elementigen Menge zu ziehen, wobei die Reihenfolge, in der die Elemente gezogen werden, nicht berücksichtigt wird.

Beweis:

Wenn die Reihenfolge, in der die Elemente gezogen werden, keine Rolle spielt, so müssen wir nur zählen, wie oft jedes Element der n -elementigen Menge gezogen wurde.

D. h. wir zählen Zerlegungen der natürlichen Zahl $m = k$ in $\ell = n$ Summanden $m_1, \dots, m_\ell \in \mathbb{N}_0$ mit

$$m_1 + \dots + m_\ell = m.$$

Für diese Problem wissen wir bereits, dass es $\binom{m+\ell-1}{\ell-1} = \binom{\ell+m-1}{m}$ unterschiedliche Kombinationen gibt und wegen $m = k$ und $\ell = n$ folgt der Satz. \square

Ziehen von Elementen

Grundproblem

Wieviele Möglichkeiten gibt es, k Elemente aus einer n -elementigen Menge zu ziehen?

Hierbei unterscheidet man folgende Varianten:

- ziehen **mit** Zurücklegen, wobei die Reihenfolge, in der die Elemente gezogen werden, **mit** berücksichtigt wird

$$k\text{-Tupel} \implies n^k$$

- ziehen **ohne** Zurücklegen, **mit** Berücksichtigung der Reihenfolge

$$k\text{-Tupel ohne Wiederholung} \implies (n)_k$$

- ziehen **ohne** Zurücklegen, **ohne** Berücksichtigung der Reihenfolge

$$k\text{-elementige Teilmengen} \implies \binom{n}{k}$$

- ziehen **mit** Zurücklegen, **ohne** Berücksichtigung der Reihenfolge

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

Taubenschlag-/Schubfachprinzip

Beobachtung (Schubfachprinzip)

Für natürliche Zahlen m und $n \in \mathbb{N}$ mit $m > n$ gilt, falls m Objekte auf n Fächer verteilt werden, so gibt es mindestens ein Fach mit mindestens zwei Objekten.

Für $m > n$ gibt es keine injektive Abbildung von einer m -elementigen Menge M in eine n -elementige Menge N .

Allgemeiner gilt, wenn m Objekte auf n Fächer verteilt werden, so gibt es mindestens ein Fach mit mindestens $\lceil \frac{m}{n} \rceil$ Objekten.

Satz (Unendliche Variante)

Sei M eine unendliche Menge und $n \in \mathbb{N}$. Sind M_1, \dots, M_n Teilmengen von M mit $M = M_1 \cup \dots \cup M_n$, so ist (mindestens) eine der Mengen M_1, \dots, M_n unendlich.

Beweis: Angenommen, M_1, \dots, M_n sind endlich. Dann existiert $m \in \mathbb{N}_0$ definiert als das Maximum der Mächtigkeiten der M_i , d. h. $m = \max_{1 \leq i \leq n} |M_i|$. Dann gilt aber

$$|M| \leq \sum_{i=1}^n |M_i| \leq m \cdot n$$

und somit ist auch M endlich. ⚡



Zwei einfache Anwendungen des Schubfachprinzips

Teilerfremde und teilende Paare

Für $n \in \mathbb{N}$ seien $n + 1$ beliebige natürliche Zahlen $1 \leq x_1 < \dots < x_{n+1} \leq 2n$ gegeben. Dann gibt es

- zwei Indizes $1 \leq i < j \leq n$, sodass x_i und x_j teilerfremd sind
- und es gibt zwei Indizes $1 \leq k < \ell \leq n$, sodass $x_k \mid x_\ell$.

Beweis: Für die erste Aussage müssen wir uns nur klar machen, dass es unter $n + 1$ Zahlen zwischen 1 und $2n$, in jedem Fall ein Zahlenpaar der Form $a, a + 1$ gibt. D. h. es gibt ein i und a sodass $x_i = a$ und $x_{i+1} = a + 1$ gilt und offensichtlich sind $x_i = a$ und $x_{i+1} = a + 1$ teilerfremd. Formal können wir auch die Zahlen zwischen 1 und $2n$ in n Schubladen S_1, \dots, S_n der Form $S_j = \{2j - 1, 2j\}$ unterteilen und wegen des Schubfachprinzips muss eine der Schubladen mindestens zwei der x_i enthalten.

Für die zweite Aussage betrachten wir als Schubladen die n ungeraden Zahlen zwischen 1 und $2n$ und wir legen x_i in die Schublade der ungeraden Zahl u , falls u der größte ungerade Teiler von x_i ist. Wegen des Schubfachprinzips gibt es also ein ungerades u und $x_k < x_\ell$, sodass u der größte ungerade Teiler von x_k und x_ℓ ist. Also ist $x_k = 2^a u$ und $x_\ell = 2^b u$ für $a < b$ aus \mathbb{N}_0 . Somit gilt $x_\ell = 2^{b-a} x_k$. \square

Allgemeine Additionsregel

$$A_1, \dots, A_n \text{ paarweise disjunkt und endlich} \implies \left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|$$

Frage

Was passiert wenn die Mengen A_i nicht paarweise disjunkt sind?

Antworten:

- Elemente die in mehreren A_i vorkommen, werden in der Summe mehrfach gezählt, z. B. für zwei Mengen A, B gilt:

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

- **allgemein:** seien $A_1, \dots, A_n \subseteq X$ und $f: X \rightarrow \mathbb{N}_0$ ordne jedem Element seine Vielfachheit in der Mengenfamilie zu

$$f(x) = |\{i \in [n] : x \in A_i\}| = \sum_{i=1}^n \mathbb{1}_{A_i}(x),$$

wobei die **Indikatorfunktion** $\mathbb{1}_A(\cdot)$ einer Menge A durch $\mathbb{1}_A(x) = 1$ falls $x \in A$ und $\mathbb{1}_A(x) = 0$ sonst definiert ist, dann gilt

$$\left| \bigcup_{i=1}^n A_i \right| \leq \sum_{i=1}^n |A_i| = \sum_{i=1}^n \sum_{x \in X} \mathbb{1}_{A_i}(x) = \sum_{x \in X} \sum_{i=1}^n \mathbb{1}_{A_i}(x) = \sum_{x \in X} f(x)$$

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

Für drei Mengen A , B und C gilt:

- $|A| + |B| + |C|$ zählt alle Elemente in $A \cup B \cup C$ mindestens einmal, aber die Elemente in den paarweisen Schnitten $A \cap B$, $A \cap C$ und $B \cap C$ werden mindestens zweimal gezählt
- **Idee:** paarweise Schnitte einfach abziehen

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$$

Problem: Elemente in $A \cap B \cap C$ werden in $|A| + |B| + |C|$ dreimal gezählt, aber durch $-|A \cap B| - |A \cap C| - |B \cap C|$ auch dreimal abgezogen, da sie in jedem der drei Schnitte enthalten sind, d. h. Elemente in $A \cap B \cap C$ werden oben gar nicht mehr mitgezählt

⇒ einfach wieder hinzuaddieren, ergibt die richtige Formel:

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

Siebformel – Prinzip von Inklusion und Exklusion

Satz (Siebformel)

Für endliche Mengen A_1, \dots, A_n gilt

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq J \in \mathcal{P}([n])} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right|.$$

Bemerkungen:

- die Summe läuft über alle nicht-leeren Teilmengen von $[n] = \{1, \dots, n\}$
- für die 1-elementigen Mengen $J = \{j\}$ erhält man die Summanden $|A_j|$
- für $n = 2$ und 3 erhalten wir die bekannten Formeln
- Durchschnitte mit leerer Indexmenge definiert man als Grundmenge, hier $\bigcap_{j \in \emptyset} A_j = \bigcup_{i=1}^n A_i$, und so erhält man durch umstellen die elegante Identität

$$\sum_{J \in \mathcal{P}([n])} (-1)^{|J|} \left| \bigcap_{j \in J} A_j \right| = 0$$

Nützliches Lemma

Lemma

Für jede natürliche Zahl $\ell \geq 1$ und jede ℓ -elementige Menge gibt es genauso viele Teilmengen mit gerader, wie mit ungerader Anzahl von Elementen.

Beweis: Sei L eine nicht-leere ℓ -elementige Menge. Wegen $\ell > 0$ folgt aus dem binomischen Lehrsatz

$$0 = (1 - 1)^\ell = \sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^k.$$

Durch Umstellen erhalten wir

$$\begin{aligned} |\{K \subseteq L : |K| \text{ ungerade}\}| &= \sum_{\substack{0 \leq k \leq \ell \\ k \text{ ungerade}}} \binom{\ell}{k} \\ &= \sum_{\substack{0 \leq k \leq \ell \\ k \text{ gerade}}} \binom{\ell}{k} = |\{K \subseteq L : |K| \text{ gerade}\}| \end{aligned}$$



Beweis der Siebformel

Siebformel

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq J \in \mathcal{P}([n])} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right|.$$

Beweis: Sei $x \in \bigcup_{i=1}^n A_i$ beliebig und $I_x = \{i \in [n] : x \in A_i\}$.

- x wird in $\left| \bigcup_{i=1}^n A_i \right|$ genau einmal gezählt
- x trägt zur Summe $\sum_{\emptyset \neq J \in \mathcal{P}([n])} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right|$ bei $\iff J \subseteq I_x, J \neq \emptyset$
 $\implies x$ trägt in der Summe genau $\sum_{\emptyset \neq J \in \mathcal{P}(I_x)} (-1)^{|J|-1}$ bei

Wegen der Definition ist $I_x \neq \emptyset$ und $\ell := |I_x| \geq 1$ und wegen dem Lemma gilt

$$0 = \sum_{j=0}^{\ell} \binom{\ell}{j} (-1)^j = \sum_{J \in \mathcal{P}(I_x)} (-1)^{|J|} = (-1)^0 + \sum_{\emptyset \neq J \in \mathcal{P}(I_x)} (-1)^{|J|}.$$

Durch Umstellen erhalten wir also

$$\sum_{\emptyset \neq J \in \mathcal{P}(I_x)} (-1)^{|J|-1} = - \sum_{\emptyset \neq J \in \mathcal{P}(I_x)} (-1)^{|J|} = 1.$$

$\implies x$ wird in $\sum_{\emptyset \neq J \in \mathcal{P}([n])} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right|$ genau einmal gezählt □

Fixpunktfreie Permutation

Briefe falsch verschicken

Es werden n unterschiedliche Briefe zufällig auf n voradressierte Briefumschläge verteilt. Was ist die Wahrscheinlichkeit, dass **jeder** Brief in einen falschen Umschlag kommt?

Mathematisch: Eine Permutation $\pi: [n] \rightarrow [n]$ heisst **fixpunktfrei**, falls $\pi(i) \neq i$ für alle $i \in [n]$. Wieviele Permutationen auf $[n]$ sind fixpunktfrei?

Antwort

EULERSche Zahl $e = 2,718281828\dots$

Es gibt ungefähr (für große n) $n!/e$ fixpunktfreie Permutationen auf $[n]$, d. h. mit Wahrscheinlichkeit $1/e \approx 0,367$ liegen alle Briefe im falschen Umschlag für große n . Die Wahrscheinlichkeit liegt zwischen 0,36 und 0,37 für alle $n \geq 5$.

Beweis: Sei A_i die Menge der Permutationen π auf $[n]$ mit Fixpunkt $\pi(i) = i$. Die Siebformel ergibt also für die Anzahl der Permutationen **mit** Fixpunkt

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq J \in \mathcal{P}([n])} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right| = \sum_{k=1}^n \binom{n}{k} (-1)^{k-1} (n-k)! = n! \sum_{k=1}^n \frac{(-1)^{k-1}}{k!}.$$

Wegen $\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = e^{-1} = 1/e$ (**Analysis**) folgt $\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k!} = 1 - 1/e$. \square

5. Restklassenringe und RSA

Erinnerung: Kongruenzen und Restklassen

Definition

Ganze Zahlen $x, y \in \mathbb{Z}$ sind **kongruent modulo m** für eine natürliche Zahl $m \in \mathbb{N}$, falls x und y denselben Rest bei Division durch m haben und wir schreiben

$$x \equiv y \pmod{m} \iff m \mid x - y.$$

Dies definiert eine Äquivalenzrelation und die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} : x \equiv y \pmod{m}\}$$

ist die **Restklasse von x modulo m** .

Bemerkungen:

- $\mathbb{Z} = [0]_m \cup \dots \cup [m-1]_m$ für jedes $m \in \mathbb{N}$
- Für die Menge der Restklassen (Faktormenge der Äquivalenzrelation kongruent modulo m) schreiben wir

$$\mathbb{Z}/m\mathbb{Z} := \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

Erinnerung: Modulare Arithmetik

- mit Restklassen kann man gut rechnen
- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$
- $\Rightarrow [z]_m \oplus [z']_m := [z + z']_m$ ist **wohldefinierte** Addition auf $\mathbb{Z}/m\mathbb{Z}$
 - Addition auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
 - $[0]_m$ ist neutrales Element der Addition auf $\mathbb{Z}/m\mathbb{Z}$
 - Subtraktion kann durch $[z]_m \ominus [z']_m := [z - z']_m$ definiert werden
 - $[-z]_m$ ist invers zu $[z]_m$, d. h. $-[z]_m = [-z]_m$
 - für $\ell \in \{0, \dots, m-1\}$ gilt $[-\ell]_m = [m - \ell]_m$
- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$
- $\Rightarrow [z]_m \odot [z']_m := [z \cdot z']_m$ ist **wohldefinierte** Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$
 - Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
 - $[1]_m$ ist neutrales Element der Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$
 - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:
$$\begin{aligned} [2]_4 \odot [0]_4 &= [0]_4, & [2]_4 \odot [1]_4 &= [2]_4, \\ [2]_4 \odot [2]_4 &= [4]_4 = [0]_4, & [2]_4 \odot [3]_4 &= [6]_4 = [2]_4 \end{aligned}$$
- $\Rightarrow [2]_4$ hat kein multiplikativ Inverses in $\mathbb{Z}/4\mathbb{Z}$
- Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes $m \in \mathbb{N}$ heißt $\mathbb{Z}/m\mathbb{Z}$ mit Verknüpfungen \oplus und \odot **Restklassenring modulo m** .

- $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{\mathbb{Z}\}$ ist **trivial (Nullring)**, aber $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ist sogar ein Körper

Wohldefiniertheit von \oplus und \odot in $\mathbb{Z}/m\mathbb{Z}$

Definition von \oplus : $[z]_m \oplus [z']_m := [z + z']_m$

- Es ist zu zeigen, dass diese Definition **unabhängig** von der Wahl der Repräsentanten der Restklassen ist. D. h. wenn y kongruent zu z und y' kongruent zu z' ist, dann muss auch $y + y'$ kongruent zu $z + z'$ sein.
 - Sei also y kongruent zu z modulo $m \Rightarrow m \mid z - y$ und es gelte analog $m \mid z' - y'$.
- $\Rightarrow m \mid ((z - y) + (z' - y')) \Rightarrow m \mid ((z + z') - (y + y'))$
- $\Rightarrow y + y'$ und $z + z'$ sind kongruent modulo m ✓

Definition von \odot : $[z]_m \odot [z']_m := [z \cdot z']_m$

- Analog betrachte y und y' mit y kongruent z und y' kongruent z' modulo m .
- $\Rightarrow z = q_z m + r$ und $y = q_y m + r$, sowie
 $z' = q_{z'} m + r'$ und $y' = q_{y'} m + r'$
mit $q_z, q_{z'}, q_y, q_{y'} \in \mathbb{Z}$ und $r, r' \in \{0, \dots, m - 1\}$
- $\Rightarrow zz' = m(q_z q_{z'} m + q_z r' + q_{y'} r) + rr' \Rightarrow zz' \in [rr']_m$
genauso rechnet man nach, dass $yy' \in [rr']_m$
- $\Rightarrow yy'$ und zz' sind kongruent modulo m ✓

Rechenregeln in $\mathbb{Z}/m\mathbb{Z}$ vererben sich von \mathbb{Z}

Exemplarisch überprüfen wir das Distributivgesetz:

$$[x]_m \odot ([y]_m \oplus [z]_m) = ([x]_m \odot [y]_m) \oplus ([x]_m \odot [z]_m)$$

für alle ganzen Zahlen $x, y, z \in \mathbb{Z}$ und $m \in \mathbb{N}$.

Beweis:

$$[x]_m \odot ([y]_m \oplus [z]_m) \stackrel{\text{Def.}\oplus}{=} [x]_m \odot ([y + z]_m) = [x]_m \odot [y + z]_m$$

$$\stackrel{\text{Def.}\odot}{=} [x \cdot (y + z)]_m \stackrel{\text{DG. in } \mathbb{Z}}{=} [x \cdot y + x \cdot z]_m \stackrel{\text{Def.}\oplus}{=} [x \cdot y]_m \oplus [x \cdot z]_m$$

und zwei weitere Anwendungen der Definition von \odot liefern das Gewünschte:

$$[x \cdot y]_m \oplus [x \cdot z]_m \stackrel{\text{Def.}\odot}{=} ([x]_m \odot [y]_m) \oplus ([x]_m \odot [z]_m).$$

Restklassenringe

Satz

Für alle natürlichen Zahlen $m \in \mathbb{N}$ sind die Operationen

$$\oplus: \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \text{ definiert durch } [a]_m \oplus [b]_m := [a + b]_m,$$

$$\odot: \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \text{ definiert durch } [a]_m \odot [b]_m := [a \cdot b]_m$$

wohldefiniert und für alle $[a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$ gelten

- die **Assoziativgesetze**:

$$[a]_m \oplus ([b]_m \oplus [c]_m) = ([a]_m \oplus [b]_m) \oplus [c]_m$$

$$\text{und } [a]_m \odot ([b]_m \odot [c]_m) = ([a]_m \odot [b]_m) \odot [c]_m,$$

- die **Kommutativgesetze**:

$$[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$$

$$\text{und } [a]_m \odot [b]_m = [b]_m \odot [a]_m,$$

- das **Distributivgesetz**: $[a]_m \odot ([b]_m \oplus [c]_m) = ([a]_m \odot [b]_m) \oplus ([a]_m \odot [c]_m),$

- die **Existenz neutraler Elemente**: $[a]_m \oplus [0]_m = [a]_m$ und $[1]_m \odot [a]_m = [a]_m$

- und die **Existenz inverser Elemente für \oplus** : $[a]_m \oplus [-a]_m = [0]_m.$

Wir benutzen vereinfachend von nun an $+$ und \cdot an Stelle von \oplus und \odot .

Prime Restklassengruppe

Definition

Für $m \geq 2$ heißt eine Restklasse $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ **multiplikativ invertierbar**, falls es ein $[b]_m \in \mathbb{Z}/m\mathbb{Z}$ gibt, sodass

$$[a]_m \cdot [b]_m = [1]_m$$

und $[b]_m$ heißt **(multiplikativ) Inverses von $[a]_m$** . Die Menge invertierbarer Elemente

$$(\mathbb{Z}/m\mathbb{Z})^\times := \{[a]_m \in \mathbb{Z}/m\mathbb{Z} : [a]_m \text{ ist multiplikativ invertierbar}\}$$

heißt **prime Restklassengruppe** und die Elemente heißen **Einheiten**.

Bemerkungen:

- Es gibt höchstens ein multiplikativ Inverses für jedes $[a]_m \in \mathbb{Z}/m\mathbb{Z}$:
Falls $[a]_m \cdot [b]_m = [1]_m$ und $[a]_m \cdot [b']_m = [1]_m$, dann gilt

$$[b]_m = [b]_m \cdot [1]_m = [b]_m \cdot ([a]_m \cdot [b']_m) = ([b]_m \cdot [a]_m) \cdot [b']_m = [1]_m \cdot [b']_m = [b']_m,$$

d. h. $[b]_m = [b']_m$. ✓

- Wir bezeichnen somit das **Inverse von $[a]_m$** (falls es existiert) mit $[a]_m^{-1}$.

Bemerkungen zu $(\mathbb{Z}/m\mathbb{Z})^\times$

- $[0]_m$ ist nicht multiplikativ invertierbar, da für alle $m \geq 2$ und $z \in \mathbb{Z}$ gilt $0 \cdot z = 0 \not\equiv 1 \pmod{m}$.

$$\Rightarrow |(\mathbb{Z}/m\mathbb{Z})^\times| \leq m - 1$$

- $(\mathbb{Z}/m\mathbb{Z})^\times$ ist unter Multiplikation abgeschlossen, d. h.

$$[a]_m, [b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times \quad \Longrightarrow \quad [a]_m \cdot [b]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$$

Beweis: Da $[a]_m$ und $[b]_m$ multiplikativ invertierbar sind, gibt es $[y]_m := [b]_m^{-1} \cdot [a]_m^{-1} \in \mathbb{Z}/m\mathbb{Z}$ und es gilt

$$([a]_m \cdot [b]_m) \cdot ([b]_m^{-1} \cdot [a]_m^{-1}) = [a]_m \cdot ([b]_m \cdot [b]_m^{-1}) \cdot [a]_m^{-1} = [a]_m \cdot [1]_m \cdot [a]_m^{-1} = [1]_m.$$

und somit hat $[a]_m \cdot [b]_m$ multiplikativ Inverses $[y]_m$ und ist in $(\mathbb{Z}/m\mathbb{Z})^\times$. \square

- Für $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$ ist $[x]_m \mapsto [a]_m \cdot [x]_m$ eine Bijektion auf $(\mathbb{Z}/m\mathbb{Z})^\times$:

- **Injektivität:** $[a]_m \cdot [x]_m = [a]_m \cdot [y]_m$

$$\Rightarrow [a]_m^{-1} \cdot [a]_m \cdot [x]_m = [a]_m^{-1} \cdot [a]_m \cdot [y]_m \Rightarrow [x]_m = [y]_m \quad \checkmark$$

- **Surjektivität:** $[z]_m \in (\mathbb{Z}/m\mathbb{Z})^\times \Rightarrow [y]_m := [a]_m^{-1} \cdot [z]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$

$$\Rightarrow [a]_m \cdot [y]_m = [z]_m, \text{ d. h. } [z]_m \text{ ist im Bild der Abbildung} \quad \checkmark$$

Multiplikative Inverse

Beispiele:

- Wir hatten bereits gesehen, dass $[2]_4$ kein multiplikativ Inverses hat.
- $[2]_5^{-1} = [3]_5$, da $[2]_5 \cdot [3]_5 = [6]_5 = [1]_5$
- $[3]_4$ ist **selbstinvers**, da

$$[3]_4 \cdot [3]_4 = [9]_4 = [1]_4,$$

$$\text{d. h. } [3]_4^{-1} = [3]_4$$

Satz

Ein Element $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ ist genau dann multiplikativ invertierbar/eine Einheit, wenn $\text{ggT}(a, m) = 1$ (d. h. wenn a und m teilerfremd sind).

Korollar

$(\mathbb{Z}/p\mathbb{Z}, +, \cdot, [0]_p, [1]_p)$ ist genau dann ein Körper, wenn p eine Primzahl ist.

$[a]_m$ multiplikativ invertierbar $\iff \text{ggT}(a, m) = 1$

Beweis:

„ \implies “ Sei $[a]_m$ multiplikativ invertierbar und $[b]_m = [a]_m^{-1}$.

$$\implies a \cdot b \equiv 1 \pmod{m} \quad (\text{Welches } \cdot ?)$$

$$\implies \text{es existiert } q \in \mathbb{Z} \text{ mit } a \cdot b = q \cdot m + 1$$

$$\implies a \cdot b - q \cdot m = 1$$

\implies d. h. jeder Teiler von a und m teilt auch 1

$$\implies \text{ggT}(a, m) = 1 \quad \checkmark$$

„ \impliedby “ Sei $\text{ggT}(a, m) = 1$.

- Wegen dem Lemma von Bézout (siehe Elementare Zahlentheorie) gibt es $s, t \in \mathbb{Z}$, sodass

$$s \cdot a + t \cdot m = \text{ggT}(a, m) = 1 \quad \implies \quad s \cdot a = (-t) \cdot m + 1.$$

$$\implies s \cdot a \equiv 1 \pmod{m}$$

$$\implies [s]_m \text{ ist multiplikativ Inverses von } [a]_m \quad \checkmark \quad \square$$

Berechnung von multiplikativen Inversen

- **Zur Erinnerung:** Der erweiterte EUKLIDISCHE Algorithmus lieferte einen algorithmischen Beweis des Lemmas von Bézout.
- ⇒ $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot m = \text{ggT}(a, m)$ können mit dem erweiterten EUKLIDISCHEN Algorithmus effizient berechnet werden
- ⇒ Repräsentant $s \in [a]_m^{-1}$ kann effizient berechnet werden, falls ein multiplikativ Inverses von $[a]_m$ existiert (d. h. genau dann, wenn $\text{ggT}(a, m) = 1$)

Beispiel: $[13]_{2412}$ invertierbar?

$$2412 = 185 \cdot 13 + 7$$

$$13 = 1 \cdot 7 + 6$$

$$7 = 1 \cdot 6 + 1$$

⇒ $\text{ggT}(13, 2412) = 1$ und Rückwärtseinsetzen ergibt:

$$1 = 7 - 1 \cdot 6 = 7 - 1 \cdot (13 - 1 \cdot 7) = 2 \cdot 7 - 1 \cdot 13 = 2 \cdot (2412 - 185 \cdot 13) - 1 \cdot 13$$

$$\Rightarrow -371 \cdot 13 + 2 \cdot 2412 = 1 \Rightarrow [-371]_{2412} = [2041]_{2412} = [13]_{2412}^{-1}$$

$$\text{Probe: } 13 \cdot 2041 = 26533 = 11 \cdot 2412 + 1 \Rightarrow 13 \cdot 2041 \equiv 1 \pmod{2412}$$

Kleiner Satz von FERMAT

Satz (FERMAT 1640)

Sei $a \in \mathbb{N}$ und p eine Primzahl mit $p \nmid a$. Dann gilt

$$a^{p-1} \equiv 1 \pmod{p}$$

und somit $[a^{p-2}]_p = [a]_p^{-1}$.

Beweis: Mit Induktion über a für eine feste Primzahl p zeigen wir $a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{N}$. Der Satz folgt dann, da wir wegen der Voraussetzung ($\text{ggT}(a, p) = 1$) auf beiden Seiten mit $b \in [a]_p^{-1}$ „kürzen“ können.

- **Induktionsanfang für $a = 1$:** klar, da $1^p = 1 \equiv 1 \pmod{p}$ für $p \geq 2$ ✓
- **Induktionsschritt $a \rightarrow a + 1$:** Mit dem binomischen Lehrsatz folgt

$$(a + 1)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} 1^i a^{p-i} + 1^p.$$

Da jeder der Summanden in $\sum_{i=1}^{p-1} \binom{p}{i} 1^i a^{p-i}$ wegen dem Binomialkoeffizienten $\binom{p}{i}$ durch p teilbar ist (p Primzahl $\Rightarrow \text{ggT}(i!(p-i)!, p) = 1$ für $0 < i < p$), gilt

$$(a + 1)^p \equiv a^p + 1 \pmod{p}.$$

Nach der Induktionsvoraussetzung gilt $a^p \equiv a \pmod{p}$

$$\Rightarrow (a + 1)^p \equiv a + 1 \pmod{p} \quad \square$$

Bemerkungen zum kleinen Satz von FERMAT

- Für a, p wie in dem Satz können wir für „große“ x bei Berechnungen der Form $a^x \pmod{p}$ die Rechnung vereinfachen, da

$$a^{p-1} \equiv 1 \pmod{p} \implies a^x \equiv a^{x-(p-1)} \pmod{p} \equiv a^r \pmod{p}$$

für den Rest $r = \text{mod}(x, p - 1)$ der ganzzahligen Division x durch $p - 1$.

Satz (FERMAT und EULER)

Seien $a, m \in \mathbb{N}$ teilerfremd und sei $\varphi(m)$ die Anzahl der zu m teilerfremden natürlichen Zahlen kleiner m . Dann gilt

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

Bemerkungen:

- $\varphi: \mathbb{N} \longrightarrow \mathbb{N}$ heißt **EULERSche φ -Funktion**
- für Primzahlen p ist $\varphi(p) = p - 1 \implies$ Satz von FERMAT und EULER verallgemeinert den kleinen Satz von FERMAT

Beweis von FERMAT-EULER

Beweis: Sei $\text{ggT}(a, m) = 1$ und seien $x_1, \dots, x_{\varphi(m)} \in \mathbb{N}$ die zu m teilerfremden natürlichen Zahlen kleiner m .

$\Rightarrow (\mathbb{Z}/m\mathbb{Z})^\times = \{[x_1]_m, \dots, [x_{\varphi(m)}]_m\}$ und $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$

- wir hatten bereits gesehen, dass $[x]_m \mapsto [a]_m \cdot [x]_m$ eine Bijektion auf $(\mathbb{Z}/m\mathbb{Z})^\times$ ist, d. h.

$$\{[ax_1]_m, \dots, [ax_{\varphi(m)}]_m\} = \{[x_1]_m, \dots, [x_{\varphi(m)}]_m\}$$

\Rightarrow

$$\prod_{i=1}^{\varphi(m)} [x_i]_m = \prod_{i=1}^{\varphi(m)} [ax_i]_m = \left[a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} x_i \right]_m = [a^{\varphi(m)}]_m \prod_{i=1}^{\varphi(m)} [x_i]_m$$

- da $[x_1]_m, \dots, [x_{\varphi(m)}]_m$ Einheiten sind, können wir auf beiden Seiten mit $\prod_{i=1}^{\varphi(m)} [x_i]_m^{-1}$ multiplizieren und erhalten

$$[1]_m = [a^{\varphi(m)}]_m \implies a^{\varphi(m)} \equiv 1 \pmod{m}.$$

□

EULERSche φ -Funktion

Für jede natürliche Zahl $m \in \mathbb{N}$ definiert durch

$$\varphi(m) = |\{x \in \mathbb{N}: \text{ggT}(x, m) = 1 \text{ und } 1 \leq x < m\}|.$$

■ $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times| \leq m - 1$

■ $\varphi(p) = p - 1$ für Primzahlen p

■ $\varphi(p \cdot q) = (p - 1)(q - 1) = \varphi(p)\varphi(q)$ für Primzahlen $p \neq q$:

Beweis: Neben den trivialen Teilern teilen nur p und q das Produkt pq .

\Rightarrow alle $x < pq$ nicht teilerfremd zu pq sind Vielfache von p oder q

diese Vielfachen sind: $p, 2p, \dots, (q - 1)p$ und $q, 2q, \dots, (p - 1)q$

$\Rightarrow \varphi(pq) = pq - 1 - (q - 1) - (p - 1) = (p - 1)(q - 1)$ □

■ **Aber:** Berechnung von $\varphi(n)$ für $n = pq$ mit Primzahlen $p \neq q$ **ohne** Kenntnis von p und q ist *schwer*

\longrightarrow so schwer, wie Berechnung der Primfaktorzerlegung von n als $n = pq$

Beweis: $\varphi(n) = (p - 1)(q - 1) = pq + 1 - (p + q) = n + 1 - (p + q)$

\Rightarrow bekanntes $\varphi(n)$ liefert die Summe $p + q = n + 1 - \varphi(n)$

\Rightarrow mit $p = n/q$ erhält man quadratische Gleichung in einer Variable (in q)

\Rightarrow Lösung der quadratischen Gleichung ergibt q und dann p □

■ kein effizienter Algorithmus bekannt

\longrightarrow eine Grundlage des RSA-Verfahrens

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems.

A message is encrypted by representing it as a number M , raising M to a publicly specified power e , and then taking the remainder when the result is divided by the publicly specified product, n , of two large secret prime numbers p and q . Decryption is similar; only a different, secret, power d is used, where $e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$. The security of the system rests in part on the difficulty of factoring the published divisor, n .

RSA-Verfahren

- benannt nach den Erfindern RIVEST, SHAMIR und ADLEMAN
- Public-Key-Verschlüsselungsverfahren von 1977
- basiert auf **öffentlichen** und (geheimen) **privaten** Schlüssel des Empfängers
- Sender verschlüsselt (engl. **encrypt**) Nachricht M mit öffentlichem Schlüssel
- verschlüsselte Nachricht C wird an den Empfänger geschickt
- Empfänger entschlüsselt (engl. **decrypt**) C und rekonstruiert so M
- Nachrichten werden hierbei als Zahlen codiert, d. h. o. B. d. A. ist $M \in \mathbb{N}$

RSA-Verfahren

- 1 Schlüsselgenerierung:** Empfänger wählt zwei große Primzahlen p und q
 - berechnet $N = pq$ und $\varphi(N) = (p - 1)(q - 1)$
 - wählt e teilerfremd zu $\varphi(N)$ mit $1 < e < \varphi(N)$
 - berechnet $d \in [e]_{\varphi(N)}^{-1}$, d. h. $ed = r\varphi(N) + 1$ für ein $r \in \mathbb{Z}$
 - veröffentlicht (e, N) und speichert geheim (d, N)
- 2 Verschlüsselung:** Sender berechnet $C \equiv M^e \pmod{N}$ für Nachricht $M < N$ und schickt Nachricht C an Empfänger
- 3 Entschlüsselung:** Empfänger berechnet kanonisches $M' \equiv C^d \pmod{N}$

$$\text{FERMAT-EULER: } M' \equiv C^d \equiv (M^e)^d \equiv M^{r\varphi(N)+1} \equiv (M^{\varphi(N)})^r \cdot M \equiv 1^r \cdot M \equiv M \pmod{N}$$

- die Kongruenz $M' \equiv M$ auf der letzten Folie verwendete den Satz von FERMAT und EULER für

$$M^{\varphi(N)} \equiv 1 \pmod{N}$$

- der Satz benötigt aber die Annahme $\text{ggT}(M, N) = 1$

- Da $N = pq$ ergeben sich die Sonderfälle $p \mid M$ bzw. $q \mid M$. Sei also $p \mid M$

$$\Rightarrow M \equiv 0 \pmod{p} \Rightarrow M^{r\varphi(N)+1} \equiv M \pmod{p}$$

wegen $p \mid M$ und $M < pq$ gilt in diesem Fall $q \nmid M$

$\Rightarrow M^{q-1} \equiv 1 \pmod{q}$, wegen dem kleinen Satz von FERMAT

$$\Rightarrow M^{r\varphi(N)+1} = (M^{q-1})^{r(p-1)} \cdot M \equiv 1^{r(p-1)} M \pmod{q} \equiv M \pmod{q}$$

Schließlich zeigt man (**Übung**), dass für Primzahlen $p \neq q$ und $x, y \in \mathbb{Z}$ gilt:

$$x \equiv y \pmod{p} \quad \text{und} \quad x \equiv y \pmod{q} \quad \Rightarrow \quad x \equiv y \pmod{pq}.$$

Somit folgt für $x = M^{r\varphi(N)+1}$ und $y = M$ auch das gewünschte

$$M^{r\varphi(N)+1} \equiv M \pmod{N}.$$



Beispiel: RSA-Verfahren

- 1** Bob wählt Primzahlen $p = 3$ und $q = 11$, berechnet

$$N = 3 \cdot 11 = 33, \quad \varphi(N) = 2 \cdot 10 = 20,$$

wählt $e = 7$ (teilerfremd zu $\varphi(N) = 20$) und berechnet mit erw. EUKLIDISCHEM Algorithmus

$$d = 3$$

⇒ öffentlicher Schlüssel: $(7, 33)$ und privater Schlüssel: $(3, 33)$

- 2** Alice möchte $M = 4$ senden und berechnet

$$4^7 = 16384 = 496 \cdot 33 + 16$$

$$\Rightarrow C = 16 \equiv 4^7 \pmod{33}$$

- 3** Bob empfängt $C = 16$ und berechnet

$$16^3 = 4096 = 124 \cdot 33 + 4$$

$$\Rightarrow M' = M = 4$$

Beispiel aus dem Originalartikel

VIII A Small Example

Consider the case $p = 47, q = 59, n = p \cdot q = 47 \cdot 59 = 2773$, and $d = 157$. Then $\phi(2773) = 46 \cdot 58 = 2668$, and e can be computed as follows:

$$\begin{aligned}x_0 &= 2668, & a_0 &= 1, & b_0 &= 0, \\x_1 &= 157, & a_1 &= 0, & b_1 &= 1, \\x_2 &= 156, & a_2 &= 1, & b_2 &= -16 \text{ (since } 2668 = 157 \cdot 16 + 156) \text{ ,} \\x_3 &= 1, & a_3 &= -1, & b_3 &= 17 \text{ (since } 157 = 1 \cdot 156 + 1) \text{ .}\end{aligned}$$

Therefore $e = 17$, the multiplicative inverse $(\text{mod } 2668)$ of $d = 157$.

With $n = 2773$ we can encode two letters per block, substituting a two-digit number for each letter: blank = 00, A = 01, B = 02, ..., Z = 26. Thus the message

ITS ALL GREEK TO ME

(Julius Caesar, I, ii, 288, paraphrased) is encoded:

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

Since $e = 10001$ in binary, the first block ($M = 920$) is enciphered:

$$M^{17} = ((((((1)^2 \cdot M)^2)^2)^2)^2)^2 \cdot M = 948 \pmod{2773} .$$

Sicherheit von RSA

Nachricht M kann nur schwer aus $C \equiv M^e \pmod{N}$ mithilfe des öffentlichen Schlüssels (e, N) berechnet werden, da

- in $\mathbb{Z}/N\mathbb{Z}$ kein effizientes Verfahren zum „Wurzelziehen“ bekannt ist
→ diskreter Logarithmus
- kein effizientes Verfahren zur Berechnung von $\varphi(N)$ bekannt ist
→ so schwer wie Primfaktorisierung von N

Aber:

- für die praktische Anwendung sollten wichtige Nebenbedingungen für die Wahl von p , q und e beachtet werden
- vollständige Sicherheit gibt es nicht
- mit „sehr großer“ Rechenleistung kann jede RSA-verschlüsselte Nachricht entschlüsselt werden

RSA-Factoring Challenge

RSA Number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA-100	100	330	US\$1,000 ^[4]	April 1, 1991 ^[5]	Arjen K. Lenstra
RSA-110	110	364	US\$4,429 ^[4]	April 14, 1992 ^[5]	Arjen K. Lenstra and M.S. Manasse
RSA-120	120	397	\$5,898 ^[4]	July 9, 1993 ^[6]	T. Denny et al.
RSA-129 ^[**]	129	426	\$100 USD	April 26, 1994 ^[5]	Arjen K. Lenstra et al.
RSA-130	130	430	US\$14,527 ^[4]	April 10, 1996	Arjen K. Lenstra et al.
RSA-140	140	463	US\$17,226	February 2, 1999	Herman te Riele et al.
RSA-150 ^{[?] ?}	150	496		April 16, 2004	Kazumaro Aoki et al.
RSA-155	155	512	\$9,383 ^[4]	August 22, 1999	Herman te Riele et al.
RSA-160	160	530		April 1, 2003	Jens Franke et al., University of Bonn
RSA-170 ^[?]	170	563		December 29, 2009	D. Bonenberger and M. Krone ^[***]
RSA-576	174	576	\$10,000 USD	December 3, 2003	Jens Franke et al., University of Bonn
RSA-180 ^[?]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University ^[7]
RSA-190 ^[?]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA-640	193	640	\$20,000 USD	November 2, 2005	Jens Franke et al., University of Bonn
RSA-200 ^{[?] ?}	200	663		May 9, 2005	Jens Franke et al., University of Bonn
RSA-210 ^[?]	210	696		September 26, 2013 ^[8]	Ryan Propper
RSA-704 ^[?]	212	704	\$30,000 USD	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA-220	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA-230	230	762			
RSA-232	232	768			
RSA-768 ^[?]	232	768	\$50,000 USD	December 12, 2009	Thorsten Kleinjung et al.
RSA-240	240	795			
RSA-250	250	829			
RSA-260	260	862			
RSA-270	270	895			
RSA-896	270	896	\$75,000 USD		
RSA-280	280	928			
RSA-290	290	962			
RSA-300	300	995			
RSA-309	309	1024			
RSA-1024	309	1024	\$100,000 USD		

RSA-Factoring Challenge

RSA-768 IS FACTORED!

A six-institution research team led by T. Kleinjung has successfully factored the RSA-768 challenge number. While the RSA Factoring Challenge is no longer active, the factoring of RSA-768 represents a major milestone for the community. The factors were found on December 12, 2009 and reported shortly thereafter. The academic paper describing the work can be found at: <http://eprint.iacr.org/2010/006.pdf>.

The factors are:

334780716989568987860441698482126908177047
949837137685689124313889828837938780022876
14711652531743087737814467999489

and

3674604366679959042824463379962795263227915
8164343087642676032283815739666511279233373
417143396810270092798736308917

The effort took almost 2000 2.2GHz-Opteron-CPU years according to the submitters, just short of 3 years of calendar time.

6. Algebraische Strukturen

Allgemeine algebraische Struktur

Definition

Eine algebraische Struktur ist eine Menge X zusammen mit endlich vielen endlichstelligen Operationen f_1, \dots, f_k auf X , d. h. für $i = 1, \dots, k$ ist f_i eine Abbildung $f_i: X^{\ell_i} \longrightarrow X$ mit $\ell_i \in \mathbb{N}_0$.

Bemerkungen

- oftmals sind die Operationen zweistellig/binär, d. h. $\ell_i = 2$
- formal schreibt man $\mathcal{X} = (X, f_1, \dots, f_k)$ und X heißt **unterliegende Menge**
- meistens sind die Operationen klar vom Kontext und man identifiziert die Struktur mit der unterliegenden Menge

Beispiele

- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, Körper im Allgemeinen
- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
- BOOLSche Algebren: z. B. $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ und $(\wp(M), \cup, \cap, \bar{}, \emptyset, M)$
- $F(A) = \{f \mid f: A \longrightarrow A\}$ mit der Komposition \circ , d. h. $(f \circ g)(x) = f(g(x))$
- $(\mathcal{S}(A), \circ)$ für die Bijektionen $\mathcal{S}(A) = \{f \in F(A) : f \text{ bijektiv}\}$ auf A

Neutrale Elemente

Definition

Sei $(X, *)$ eine algebraische Struktur mit einem zweistelligen Operator $*$. Ein Element $e \in X$ heißt **neutrales Element**, falls für alle $x \in X$ gilt

$$e * x = x = x * e.$$

Proposition

Ist $*$ eine zweistellige Operation auf X , so gibt es höchstens ein neutrales Element bezüglich $*$.

Beweis:

Seien $e, e' \in X$ neutral. Dann gilt

$$e \stackrel{e' \text{ neutral}}{=} e * e' \stackrel{e \text{ neutral}}{=} e'.$$

Somit ist $e = e'$. □

Neutrale Elemente – Beispiele

- 0 ist neutral in $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ und $(\mathbb{N}_0, +)$
- 1 ist neutral in (\mathbb{R}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{N}, \cdot) und (\mathbb{N}_0, \cdot)
- in jedem Körper ist die 0 neutral bezüglich $+$ und die 1 neutral bezüglich \cdot .
- 0 und 1 sind neutral bezüglich $+$ und \cdot in $(\mathbb{Z}, +, \cdot)$
- $[0]_n$ und $[1]_n$ sind neutral bezüglich $+$ und \cdot in $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

- $(\mathbb{N}, +)$ hat **kein** neutrales Element

- Identität $\text{id}_A: A \longrightarrow A$ mit $a \longmapsto a$ für alle $a \in A$ ist neutral in $(F(A), \circ)$
- id_A ist eine Bijektion und so auch neutrales Element in $(\mathcal{S}(A), \circ)$

- 0 ist neutral für \vee und 1 ist neutral für \wedge in $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$
- \emptyset ist neutral für \cup und M ist neutral für \cap in $(\mathcal{P}(M), \cup, \cap, \overline{}, \emptyset, M)$

Inverse Elemente

Definition

Sei $(X, *)$ eine algebraische Struktur mit einem zweistelligen Operator $*$ mit einem neutralen Element e . Ein Element $x \in X$ heißt **invertierbar**, falls ein Element $y \in X$ existiert, so dass

$$x * y = e = y * x.$$

In so einem Fall sagen wir **y ist invers zu x** (bezüglich $*$).

Beispiele

- $-x$ invers zu x bezüglich $+$ für $x \in \mathbb{R}, \mathbb{Q}$ oder \mathbb{Z}
- x^{-1} invers zu x bezüglich \cdot für $x \in \mathbb{R} \setminus \{0\}$ oder $\mathbb{Q} \setminus \{0\}$
- 0 hat kein Inverses bezüglich \cdot in \mathbb{R} oder \mathbb{Q}
- $[-x]_n$ invers zu $[x]_n$ in $\mathbb{Z}/n\mathbb{Z}$ bezüglich $+$
- $[2]_4$ hat kein Inverses in $\mathbb{Z}/4\mathbb{Z}$ bezüglich \cdot
- $[3]_4$ ist selbstinvers in $\mathbb{Z}/4\mathbb{Z}$ bezüglich \cdot

Gruppen

Definition (Gruppe)

Eine **Gruppe** ist eine algebraische Struktur $(G, *)$ mit einer zweistelligen Verknüpfung $*$, die folgende Eigenschaften erfüllt:

- 1 Assoziativgesetz:** $x * (y * z) = (x * y) * z$ für alle $x, y, z \in G$,
- 2 neutrales Element:** es gibt ein neutrales Element $e \in G$
- 3 inverse Elemente:** und jedes x in G ist invertierbar (bezüglich $*$).

Gilt zusätzlich das

- 4 Kommutativgesetz:** $x * y = y * x$ für alle $x, y \in G$,

dann heißt die Gruppe $(G, *)$ **ABELSsch/kommutativ**.

Bemerkungen

- algebraische Strukturen die **1** erfüllen, heißen **Halbgruppen**
- algebraische Strukturen die **1** und **2** erfüllen, heißen **Monoide**

Beispiele

- algebraische Strukturen (\mathbb{N}, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}, \cdot) und $(F(A), \circ)$ sind Monoide
 - $(\mathbb{N}, +)$ ist kein Monoid, da es in \mathbb{N} bezüglich $+$ kein neutrales Element gibt
 - $(\mathbb{N}, +)$ ist eine Halbgruppe.
 - für eine Menge A , die wir in diesem Zusammenhang **Alphabet** nennen, sei
 - A^* die Menge aller endlichen Folgen von Zeichen aus A
 - Elemente von A^* heißen **Wörter** über A
 - für zwei Wörter $v = a_1 \dots a_n$ und $w = b_1 \dots b_m$ definieren wir die **Verkettung** $v \frown w$ von v und w als das Wort $a_1 \dots a_n b_1 \dots b_m$
- ⇒ dann ist (A^*, \frown) ein Monoid mit dem leeren Wort als neutralem Element
- für jedes $n \geq 2$ ist $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ ein Monoid

Eindeutigkeit der Inversen

Satz

Ist $(M, *)$ ein Monoid, so besitzt jedes $x \in M$ höchstens ein Inverses.

Beweis: Seien y und $y' \in M$ Inverse von $x \in M$. Dann gilt

$$y \stackrel{2}{=} y * e = y * (x * y') \stackrel{1}{=} (y * x) * y' = e * y' = y'.$$

□

Proposition

Ist (G, \cdot) eine Gruppe, so gilt $(xy)^{-1} = y^{-1}x^{-1}$ für alle $x, y \in G$.

Beweis: Seien $x, y \in G$. Dann gilt

$$(xy)(y^{-1}x^{-1}) \stackrel{1}{=} x(yy^{-1})x^{-1} = x \cdot e \cdot x^{-1} = xx^{-1} = e.$$

$\implies y^{-1}x^{-1}$ ist invers zu xy

\implies wegen der Eindeutigkeit der Inversen gilt $(xy)^{-1} = y^{-1}x^{-1}$

□

Multiplizieren und Kürzen

- für eine Gruppe G (ohne Angabe der Operation) nehmen wir standardmäßig an, dass \cdot die Operation ist, d. h. für $a, b \in G$ ist die Gruppenoperation $a \cdot b = ab$
- das neutrale Element bezeichnen wir mit e
- für $a \in G$ bezeichnet a^{-1} das Inverse von a

Lemma

Sei G eine Gruppe. Dann gilt für alle $a, b, c \in G$:

- 1 falls $ab = ac$, dann ist $b = c$. (Genauso folgt aus $ba = ca$ auch $b = c$.)
- 2 die Gleichung $ax = b$ (ebenso $xa = b$), wobei x eine Unbekannte ist, ist eindeutig lösbar.

Beweis:

- 1 multipliziere beide Seiten der Gleichung mit a^{-1} von links ✓
- 2 Multiplikation mit a^{-1} von links zeigt $x = a^{-1}b$ ist eine Lösung
Sei c auf der anderen Seite eine Lösung $\Rightarrow ac = b = aa^{-1}b$ und somit gilt wegen dem ersten Teil auch $c = a^{-1}b$. □

Gruppen – Beispiele

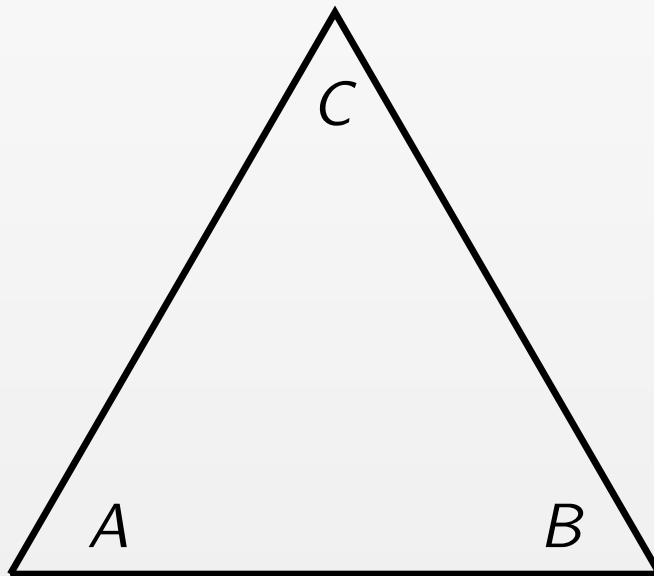
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen
- für jedes $n \geq 1$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen
- ist p eine Primzahl, so ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}, \cdot)$ eine abelsche Gruppe
- für jedes $n \geq 2$ ist die Einheitengruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ eine abelsche Gruppe
- für eine Menge A bildet die Menge $\mathcal{S}(A)$ der Bijektionen von A nach A zusammen mit der Komposition (Hintereinanderausführung) \circ die Gruppe $(\mathcal{S}(A), \circ)$
 - für jede Bijektion $f \in \mathcal{S}(A)$ gibt es eine Umkehrfunktion f^{-1} , die das zu f inverse Element ist
 - $(\mathcal{S}(A), \circ)$ heißt die **symmetrische Gruppe** auf A
 - für $A = [n] = \{1, \dots, n\}$ mit $n \in \mathbb{N}_0$ ist $\mathcal{S}([n])$ die Menge der Permutationen auf $[n]$ und wir bezeichnen die symmetrische Gruppe mit $\mathcal{S}_n := ([n], \circ)$ bzw. bezeichnen sie auch als **Permutationsgruppe**
 - für $n \geq 3$ ist \mathcal{S}_n **nicht** abelsch:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Geometrisches Beispiel

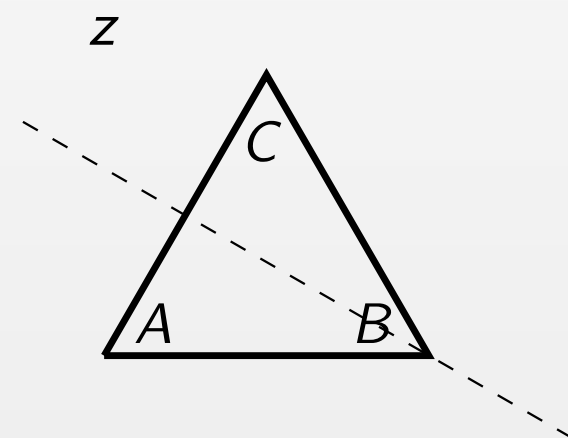
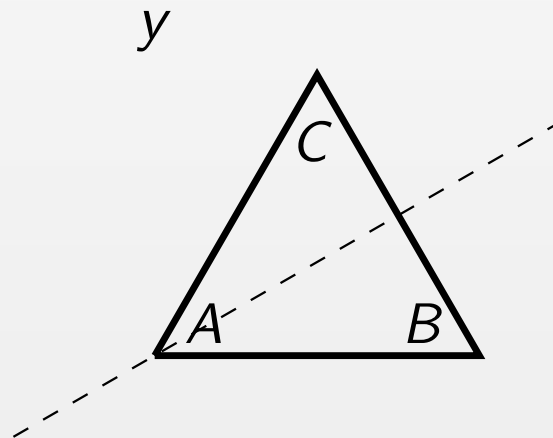
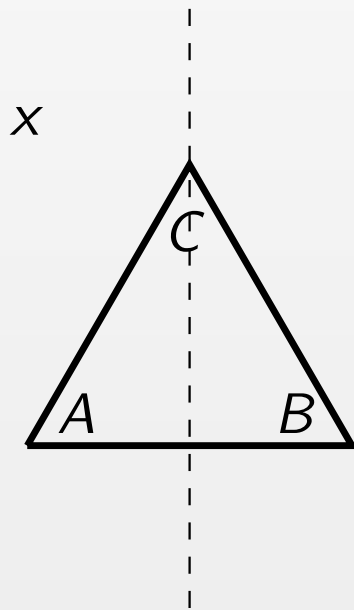
Dreiecksgruppe G_{\triangle} :

- Gruppe auf der Menge der Symmetrien eines gleichseitigen Dreiecks (Transformationen der Ebene, die das Dreieck auf das Dreieck abbilden)
- mit der zweistelligen Operation der Komposition von Abbildungen \circ



Elemente von G_{\triangle}

- **Identität i** : die jeden Punkt der Ebene auf sich selbst abbildet
- **Drehung r um 120°** : um den Mittelpunkt des Dreiecks entgegen dem Uhrzeigersinn (mathematisch positiver Drehsinn)
- **Drehung s um 240°** : um den Mittelpunkt des Dreiecks entgegen dem Uhrzeigersinn
- **Spiegelungen x, y und z** : entlang der Mittelsenkrechten des Dreiecks



G_{Δ} und S_3

Beobachtung

- alle Symmetrien i, r, s, x, y und z sind eindeutig durch die Abbildung der Ecken aufeinander bestimmt
- ⇒ jede Symmetrie entspricht einer Permutation der Menge der Ecken $\{A, B, C\}$

i	r	s
$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$
x	y	z
$\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$

- Zwei Gruppen (G, \cdot) und (H, \odot) sind **isomorph** (geschrieben $G \cong H$), falls es eine Bijektion $\varphi: G \rightarrow H$ mit

$$\varphi(x) \odot \varphi(y) = \varphi(x \cdot y)$$

für alle $x, y \in G$ gilt und φ heißt **Gruppenisomorphismus**.

Gruppentafeln

- für (kleine) endliche Gruppen kann man alle Produkte von zwei Gruppenelementen in einer **Multiplikationstabelle/Gruppentafel** angeben
- in der Zeile für das Element a und der Spalte für das Element b steht das Produkt ab

Gruppentafel von G_{Δ} :

\circ	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	z	x	y
s	s	i	r	y	z	x
x	x	y	z	i	r	s
y	y	z	x	s	i	r
z	z	x	y	r	s	i

- Vergleich der Gruppentafeln von G_{Δ} und \mathcal{S}_3 zeigt, dass die Gruppen isomorph sind

$$\Rightarrow G_{\Delta} \cong \mathcal{S}_3$$

Gruppenisomorphismen

- $G \cong H$, falls es eine Bijektion zwischen den unterliegenden Mengen gibt, die mit den Gruppenoperationen verträglich ist

Lemma

- 1** Ist $\varphi: G \longrightarrow H$ ein Gruppenisomorphismus, so auch $\varphi^{-1}: H \longrightarrow G$.
- 2** Sind $\varphi: G \longrightarrow H$ und $\psi: H \longrightarrow I$ Gruppenisomorphismen, so auch $\psi \circ \varphi: G \longrightarrow I$.
- 3** Ist $\varphi: G \longrightarrow H$ ein Gruppenisomorphismus. Dann gilt
 - $\varphi(e_G) = e_H$ für die neutralen Elemente $e_G \in G$ und $e_H \in H$.
 - $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für jedes $a \in G$.

Bemerkung

- Teil **1** \Rightarrow Relation \cong ist symmetrisch auf jeder Menge von Gruppen
 - Teil **2** \Rightarrow Relation \cong ist transitiv
 - Identität $\text{id}_G \Rightarrow$ Relation \cong ist reflexiv
- $\Rightarrow \cong$ definiert Äquivalenzrelation

Gruppenisomorphie ist symmetrisch

Beweis von Teil 1:

Sei $\varphi: G \longrightarrow H$ ein Gruppenisomorphismus von (G, \cdot) nach (H, \odot) .

Insbesondere φ ist bijektiv und so auch $\varphi^{-1}: H \longrightarrow G$. Wir zeigen, dass φ^{-1} verträglich mit den Gruppenoperationen ist, d. h. wir zeigen

$$\varphi^{-1}(x) \cdot \varphi^{-1}(y) = \varphi^{-1}(x \odot y)$$

für alle $x, y \in H$.

Seien $x, y \in H$ beliebig und seien $a, b \in G$ die Urbilder (unter φ), d. h.

$$a = \varphi^{-1}(x) \quad \text{und} \quad b = \varphi^{-1}(y).$$

Da φ ein Gruppenisomorphismus ist, gilt insbesondere auch

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) = x \odot y \quad \Longrightarrow \quad a \cdot b = \varphi^{-1}(x \odot y).$$

Somit folgt die gewünschte Identität

$$\varphi^{-1}(x) \cdot \varphi^{-1}(y) = a \cdot b = \varphi^{-1}(x \odot y).$$



Gruppenisomorphie ist transitiv

Beweis von Teil 2:

Seien $\varphi: G \longrightarrow H$ und $\psi: H \longrightarrow I$ Gruppenisomorphismen für die Gruppen (G, \cdot) , (H, \odot) und (I, \odot) . Insbesondere sind φ und ψ bijektiv und so ist auch $\psi \circ \varphi: G \longrightarrow I$ bijektiv. Wir zeigen die Verträglichkeit von $\psi \circ \varphi$ mit den Gruppenoperationen \cdot und \odot , d. h.

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a \cdot b))$$

für alle $a, b \in G$.

Seien $a, b \in G$ beliebig. Da ψ ein Gruppenisomorphismus ist, ist ψ verträglich mit \odot und \odot und wir haben

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a) \odot \varphi(b)).$$

Genauso ist der Gruppenisomorphismus φ verträglich mit \odot und \cdot und wir erhalten die gewünschte Identität

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a) \odot \varphi(b)) = \psi(\varphi(a \cdot b)).$$



Gruppenisomorphie erhält neutrale und inverse Elemente

Beweis von Teil 3:

Sei $\varphi: G \longrightarrow H$ ein **Gruppenisomorphismus** zwischen den Gruppen (G, \cdot) und (H, \odot) mit neutralen Elementen e_G und e_H .

Sei $x \in H$ beliebig und sei $a \in G$ mit $\varphi(a) = x$. Dann gilt

$$x = \varphi(a) = \varphi(a \cdot e_G) = \varphi(a) \odot \varphi(e_G) = x \odot \varphi(e_G).$$

Genauso zeigt man $x = \varphi(e_G) \odot x$ für alle $x \in H$ und durch die Eindeutigkeit des neutralen Elements in H , gilt $e_H = \varphi(e_G)$. ✓

Sei nun $a \in G$ beliebig. Aufgrund des gerade Gezeigten haben wir

$$e_H = \varphi(e_G) = \varphi(a \cdot a^{-1}) = \varphi(a) \odot \varphi(a^{-1}).$$

Multiplikation mit $(\varphi(a))^{-1}$ von links auf beiden Seiten ergibt die gesuchte Identität

$$(\varphi(a))^{-1} = \varphi(a^{-1}).$$



Potenzen in Gruppen

Definition

Sei G eine Gruppe und $a \in G$. Für jedes $n \in \mathbb{N}_0$ definieren wir rekursiv

$$a^0 := e \quad \text{und} \quad a^{n+1} := a^n \cdot a$$

Für negative Exponenten definieren wir

$$a^{-n} := (a^{-1})^n$$

- wie für Potenzen reeller Zahlen rechnet man schnell für alle $a \in G$ und alle $m, n \in \mathbb{Z}$ die folgenden Rechenregeln nach:

$$a^m a^n = a^{m+n} \quad \text{und} \quad (a^m)^n = a^{mn}.$$

Ordnung von Gruppenelementen

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$.

Falls ein $m \geq 1$ existiert, so dass $a^m = e$ gilt, so definiert man die **Ordnung** von a als das kleinste solche $m > 0$.

Falls kein solches m existiert, so sagen wir, dass a die Ordnung ∞ hat.

Die **Ordnung der Gruppe G** ist einfach $|G|$.

Satz

In einer endlichen Gruppe G hat jedes Element eine endliche Ordnung $\leq |G|$.

Beweis: Sei $n = |G|$ und $a \in G$. Wir betrachten die Potenzen a^1, \dots, a^n . Falls keine Potenz e ergibt und es nur $n - 1$ weitere Gruppenelemente gibt, können nicht alle diese Potenzen verschieden sein (Schubfachprinzip).

\Rightarrow es gibt $1 \leq \ell < m \leq n$, so dass $a^\ell = a^m$

$\Rightarrow a^\ell \cdot e = a^\ell a^{m-\ell}$

(Rechenregeln für Potenzen)

$\Rightarrow e = a^{m-\ell}$

(Kürzen in Gruppen)

\Rightarrow da $1 \leq m - \ell \leq n$, ist die Ordnung von a höchstens $m - \ell \leq n$ \square

Ordnung von Gruppenelementen – Beispiele

- Permutation $(2, 3, 4, 1, 5)$ hat in \mathcal{S}_5 die Ordnung 4
- in G_Δ haben r und s die Ordnung 3, x , y und z die Ordnung 2 und i ist neutral und hat Ordnung 1
- $[7]_{10}$ ist in der Einheitengruppe $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot)$, da $\text{ggT}(7, 10) = 1$
Potenzen von $[7]_{10}$ sind: $[7]_{10}$, $[7]_{10}^2 = [9]_{10}$, $[7]_{10}^3 = [7 \cdot 9]_{10} = [3]_{10}$ und $[7]_{10}^4 = [7 \cdot 3]_{10} = [1]_{10} \Rightarrow$ Ordnung von $[7]_{10}$ ist 4
- **Achtung:** für die Addition in $(\mathbb{Z}, +)$ ist 0 neutral ($e = 0$) und a^n entspricht $a + \dots + a = n \cdot a$
 \Rightarrow jede ganze Zahl $x \neq 0$ hat unendliche Ordnung in $(\mathbb{Z}, +)$
- in $(\mathbb{Z}/15\mathbb{Z}, +)$ hat $[5]_{15}$ die Ordnung 3 und $[4]_{15}$ hat die Ordnung 15

Proposition

Sei G eine Gruppe, in der jedes Element $\neq e$ Ordnung 2 hat. Dann ist G abelsch.

Beweis: Seien $x, y \in G$ beliebig. Dann gilt

$$xy = (xy)e = (xy)(yx)^2 = (xy)(yx)(yx) = (x(yy)x)(yx) = (xx)(yx) = yx.$$

□

Vielfache der Ordnung

Satz

Sei G eine Gruppe und sei $a \in G$ ein Element von endlicher Ordnung m . Dann gilt für alle $n \in \mathbb{Z}$ genau dann $a^n = e$, wenn m ein Teiler von n ist.

Beweis

„ \Leftarrow “ für $n = qm$ mit $q \in \mathbb{Z}$ gilt

$$a^n = (a^m)^q = e^q = e$$

(auch für $q < 0$) ✓

„ \Rightarrow “ Sei $n = qm + r$ mit $0 \leq r < m$. Wir werden zeigen, dass $r = 0$ gelten muss. Tatsächlich gilt

$$e = a^n = a^{qm+r} = (a^m)^q \cdot a^r = e^q \cdot a^r = a^r.$$

Da m die kleinste Zahl ≥ 1 mit $a^m = e$ ist, folgt aus $r < m$ dann $r = 0$. □

Zyklische Gruppen

Definition (Zyklische Gruppe)

Ein Gruppe (G, \cdot) heißt **zyklisch**, falls sie durch Potenzen über ein Element $a \in G$ **erzeugt** wird, d. h.

$$G = \{a^z : z \in \mathbb{Z}\}.$$

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch und sowohl 1 als auch -1 erzeugen die Gruppe
Erinnerung: multiplikative Schreibweise $\Rightarrow a^z = z \cdot a$
- für alle $n \in \mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ zyklisch; erzeugt von $[1]_n$
Bemerkung: für $n = 1$ ist $\mathbb{Z}/1\mathbb{Z}$ einelementig \Rightarrow zyklisch
- S_2 ist zyklisch und wird von der Permutation $(2, 1)$ erzeugt
Bemerkung: alle zweielementigen Gruppen sind isomorph
- G_Δ ist **nicht** zyklisch:
 - Potenzen (Hintereinanderausführungen) von i bleiben i
 - Drehungen r und s haben jeweils Ordnung 3 und können somit nur 3, nicht aber alle 6 Elemente, von G_Δ erzeugen
 - Spiegelungen x, y, z haben Ordnung 2 und erzeugen nur 2 Elemente

Klassifizierung zyklischer Gruppen

Satz

Eine Gruppe (G, \cdot) ist zyklisch genau dann, wenn sie isomorph zu $(\mathbb{Z}, +)$ oder isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}$ ist.

- Rückrichtung hatten wir bereits durch die Beispiele gezeigt
- Satz \implies zyklische Gruppen sind abelsch

Beweis: Sei $G = \{a^z : z \in \mathbb{Z}\}$ durch a erzeugt mit neutralem Element e_G .

1. Fall: (a hat Ordnung ∞ in G)

Betrachte die Abbildung $\varphi: \mathbb{Z} \longrightarrow G$ gegeben durch $z \longmapsto a^z$.

- φ ist surjektiv, da G durch a erzeugt wird
 - φ ist injektiv, da sonst aus $a^z = a^{z'}$ für $z > z'$ wegen $a^{z-z'} = e_G$ folgt, dass a endliche Ordnung $z - z' > 0$ hätte ⚡ zur Fallannahme
- $\implies \varphi$ ist bijektiv
- φ ist ein Isomorphismus, da

$$\varphi(z + z') = a^{z+z'} = a^z \cdot a^{z'} = \varphi(z) \cdot \varphi(z')$$



Klassifizierung zyklischer Gruppen – endliche Ordnung

2. Fall: (a hat Ordnung n in G)

Betrachte nun die Abbildung $\psi: \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ gegeben durch $[z]_n \longmapsto a^z$.

- ψ ist wohldefiniert: Seien $z \equiv z' \pmod{n}$

$$\Rightarrow n \mid z - z'$$

$$\Rightarrow a^{z-z'} = e_G$$

(Satz über Vielfache der Ordnung)

$$\Rightarrow a^z = a^{z'} \quad \checkmark$$

- ψ ist injektiv: falls $\psi([z]_n) = a^z = a^{z'} = \psi([z']_n)$

$$\Rightarrow a^{z-z'} = e_G$$

$$\Rightarrow n \mid z - z'$$

(Satz über Vielfache der Ordnung)

$$\Rightarrow z \equiv z' \pmod{n} \Rightarrow [z] = [z'] \quad \checkmark$$

- ψ ist surjektiv, da a die Gruppe G erzeugt

$\Rightarrow \psi$ ist bijektiv

- ψ ist ein Isomorphismus, da

$$\psi([z]_n + [z']_n) = a^{z+z'} = a^z \cdot a^{z'} = \psi([z]_n) \cdot \psi([z']_n)$$

Untergruppen

Definition (Untergruppe)

Sei (G, \cdot) eine Gruppe. Eine Menge $U \subseteq G$ heißt **Untergruppe** von G , falls (U, \cdot) eine Gruppe ist, wobei man die Einschränkung von \cdot auf $U \times U$ betrachtet:

- 1 für alle $u, v \in U$ gilt $u \cdot v \in U$,
- 2 es existiert $e_U \in U$ mit $u \cdot e_U = u = e_U \cdot u$ für alle $u \in U$
- 3 und für jedes $u \in U$ gibt es $u' \in U$ mit $u \cdot u' = e_U = u' \cdot u$.

Bemerkungen

- Assoziativität muss nicht extra gefordert werden, da diese sich von G auf U vererbt
- wir werden sehen (Untergruppenkriterium), dass e_U das neutrale Element von G sein muss
- ebenso entsprechen die inversen Elementen denen aus G , d. h. $u' = u^{-1}$

Beispiele

- für $m \in \mathbb{N}_0$ ist $m\mathbb{Z} := \{m \cdot z : z \in \mathbb{Z}\} \subseteq \mathbb{Z}$ die Menge aller Vielfachen von m eine Untergruppe von $(\mathbb{Z}, +)$:
 - 1 $u, v \in m\mathbb{Z} \implies m \mid u$ und $m \mid v \implies m \mid (u + v) \implies u + v \in m\mathbb{Z}$
 - 2 $0 \in m\mathbb{Z}$ und 0 ist neutral
 - 3 $u \in m\mathbb{Z} \implies m \mid -u \implies -u \in m\mathbb{Z}$ $\implies (m\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$
- jede Gruppe G mit neutralem Element e hat triviale Untergruppen:
 - Untergruppe $\{e\}$ „kleinste Untergruppe“
 - G selbst ist eine Untergruppe von G „größte Untergruppe“
- G_Δ hat die folgenden Untergruppen:
 - triviale Untergruppen $\{i\}$ und G_Δ ,
 - $\{i, x\}, \{i, y\}, \{i, z\}$ sind Untergruppen, da Spiegelungen selbstinvers sind,
 - die Drehungen bilden mit der Identität die Untergruppe $\{i, r, s\}$ von G_Δ
 - da zwei Spiegelungen eine Drehung erzeugen und jede Drehung zusammen mit jeder beliebigen Spiegelung alle Elemente von G_Δ erzeugt, gibt es keine anderen Untergruppen in G_Δ
- $\{[0]_{15}, [5]_{15}, [10]_{15}\}$ und $\{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$ sind Untergruppen von $\mathbb{Z}/15\mathbb{Z}$
- für $a \in G$ ist $\langle a \rangle := \{a^z : z \in \mathbb{Z}\}$ die von a erzeugte Untergruppe

Untergruppenkriterien

Satz

Sei (G, \cdot) eine Gruppe mit neutralem Element e und $U \subseteq G$. Folgende Aussagen sind äquivalent:

- 1 U ist eine Untergruppe von G ,
- 2 $e, u^{-1}, uv \in U$ für alle $u, v \in U$,
- 3 $U \neq \emptyset$ und $uv^{-1} \in U$ für alle $u, v \in U$.

Beweis: („1 \Rightarrow 2“)

Sei U eine Untergruppe mit neutralem Element $e_U \in U$. Dann gilt:

$$e_U \cdot e_U \stackrel{e_U \text{ neutral in } U}{=} e_U \stackrel{e \text{ neutral in } G}{=} e_U \cdot e \implies e_U = e.$$

Seien $u \in U$ und $u' \in U$ das Inverse von u in U . Dann gilt:

$$u \cdot u' = e_U = e \quad \text{und} \quad u' \cdot u = e_U = e \implies u' = u^{-1},$$

wegen der Eindeutigkeit Inverser Elemente in G .



Beweis der Untergruppenkriterien

„**2** \Rightarrow **3**“

- $e \in U \implies U$ ist nicht leer
- $u, v \in U \implies v^{-1} \in U \implies uv^{-1} \in U$



„**3** \Rightarrow **1**“

- $U \neq \emptyset \implies$ es gibt $u \in U \implies uu^{-1} \in U \implies uu^{-1} = e \in U$
- da $e \in U$ gilt für $u \in U$ somit auch $eu^{-1} = u^{-1} \in U$
- seien nun $u, v \in U \implies v^{-1} \in U \implies u \cdot (v^{-1})^{-1} = uv \in U$



Korollar

Sei (G, \cdot) eine Gruppe und für endliches U mit $\emptyset \neq U \subseteq G$ gilt $uv \in U$ für alle $u, v \in U$. Dann ist U eine Untergruppe von G .

Beweis: Sei $U = \{u_1, \dots, u_n\}$ für ein $n \geq 1$. Für jedes $i \in [n]$ sind die n Produkte
 $u_i u_1, u_i u_2, \dots, u_i u_n$

paarweise verschieden und liegen alle in U . D. h. für jedes $u \in U$ gibt es ein $j \in [n]$ mit $u_i u_j = u$

\implies für $u = u_i$ gibt es $j \in [n]$, sodass $u_i u_j = u_i \implies e = u_j \in U$

\implies für $u = e$ gibt es $k \in [n]$, sodass $u_i u_k = e \implies u_i^{-1} = u_k \in U$

$\implies U$ ist eine Untergruppe nach Teil **2** des vorherigen Satzes.



Nebenklassen

Definition (Nebenklassen)

Sei G eine Gruppe, sei $U \subseteq G$ eine Untergruppe und $a \in G$. Wir definieren

$$aU := \{au : u \in U\} \quad \text{und} \quad Ua := \{ua : u \in U\}.$$

Wir nennen die Mengen der Form aU **Linksnebenklassen** von U und die Mengen der Form Ua **Rechtsnebenklassen**.

Beispiele:

- G abelsch $\Rightarrow aU = Ua$ für alle $a \in G$ und Untergruppen U
- für $G = (\mathbb{Z}, +)$ und $U = 6\mathbb{Z}$ ist $\{\dots, -2, 4, 10, \dots\} = [4]_6$ die Linksnebenklasse $4 + 6\mathbb{Z}$ **additive Schreibweise hier**
- für $U = \{i, x\}$ in G_Δ gilt

$$iU = \{i, x\}, \quad rU = \{r, y\}, \quad sU = \{s, z\}$$

und

$$Ui = \{i, x\}, \quad Ur = \{r, z\}, \quad Us = \{s, y\}.$$

Struktur der Nebenklassen

Satz

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt:

- 1** für alle $a \in G$ ist $a \in aU$.
- 2** für alle $u \in U$ ist $uU = U$.
- 3** für $a, b \in G$ mit $b \in aU$ gilt $aU = bU$.
- 4** für $a, b \in G$ sind aU und bU entweder disjunkt oder gleich.
- 5** für alle $a \in G$ gilt $|aU| = |U|$.

Die Aussagen gelten analog für Rechtsnebenklassen.

Bemerkungen:

- Teile **1** und **4** \Rightarrow Links- bzw. Rechtsnebenklassen von U partitionieren G
 - Linksnebenklassen entsprechen Äquivalenzrelation $x \sim y :\Leftrightarrow x^{-1}y \in U$
 - Rechtsnebenklassen entsprechen Äquivalenzrelation $x \approx y :\Leftrightarrow xy^{-1} \in U$
- Beweise der Teile **1** und **2** folgen direkt aus den Gruppeneigenschaften $e \in U$ und $uv \in U$ für alle $u, v \in U$

Beweise

Teil 3: Sei $b \in aU$, d. h. $b = au_0$ für ein $u_0 \in U$.

\Rightarrow für jedes $u \in U$ gilt $bu = (au_0)u = a(u_0u) \in aU$, da $u_0, u \in U$

$\Rightarrow bu \in aU$ für alle $u \in U$

$\Rightarrow bU \subseteq aU$

Andererseits gilt für jedes $u \in U$ auch $au = (bu_0^{-1})u = b(u_0^{-1}u) \in bU$.

$\Rightarrow aU \subseteq bU$. ✓

Teil 4: Falls $aU \cap bU \neq \emptyset$, dann gibt ein $c \in G$ mit $c \in aU$ und $c \in bU$ und wegen **3** gilt

$$aU = cU \quad \text{und} \quad bU = cU \quad \Longrightarrow \quad aU = bU.$$

Teil 5: Betrachte die Abbildung $f: aU \rightarrow U$ gegeben durch $v \mapsto a^{-1}v$. ✓

■ f ist surjektiv: für $u \in U$ ist $au \in aU$ und $f(au) = u$ ✓

■ f ist injektiv: falls $f(v) = f(w)$ für $v = au_v$ und $w = au_w \in aU$, dann gilt $u_v = u_w$ und somit auch $v = au_v = au_w = w$ ✓

$\Rightarrow f$ ist eine Bijektion $\Rightarrow |aU| = |U|$ □

Satz von LAGRANGE

Korollar (Satz von LAGRANGE)

Ist G eine endliche Gruppe und U eine Untergruppe von G , so ist die Ordnung $|U|$ von U ein Teiler der Ordnung $|G|$ von G .

Wegen der erzeugten Untergruppe $\langle a \rangle$ teilt somit die Ordnung von $a \in G$ auch die Ordnung $|G|$ von G .

Beweis: Da die Linksnebenklassen von U die Menge G partitionieren (Teile **1** und **4**) und alle Nebenklassen die gleiche Größe $|U|$ haben (Teil **5**), gilt

$$|G| = |U| \cdot \text{Anzahl der Linksnebenklassen von } U.$$



Definition (Index)

Für eine Untergruppe U von G ist die Anzahl der Links- bzw. Rechtsnebenklassen der **Index von U** und wird mit $[G : U]$ bezeichnet.

Satz von LAGRANGE

$|G| = [G : U] \cdot |U|$ für jede Untergruppe U einer endlichen Gruppe G .

LAGRANGE \implies Satz von FERMAT und EULER

Satz (FERMAT und EULER)

Seien $a, m \in \mathbb{N}$ teilerfremd und sei $\varphi(m)$ die EULERSche φ -Funktion (d. h. die Anzahl der zu m teilerfremden natürlichen Zahlen kleiner m). Dann gilt

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis:

Da a und m teilerfremd sind, gilt $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$. Des Weiteren hat die Gruppe $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ die Ordnung $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ und nach dem Satz von LAGRANGE teilt die Ordnung k von $[a]_m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ somit $\varphi(m)$, d. h. es gibt $\ell \in \mathbb{N}$ mit $k\ell = \varphi(m)$ und es gilt

$$[a]_m^{\varphi(m)} = ([a]_m^k)^\ell = [1]_m^\ell = [1]_m \implies a^{\varphi(m)} \equiv 1 \pmod{m}.$$



Zyklizität vererbt sich auf Untergruppen

Satz

Jede Untergruppe U einer zyklischen Gruppe G ist zyklisch.

Beweis:

Sei $G = \{a^z : z \in \mathbb{Z}\} = \langle a \rangle$.

Falls $U = \{e\}$, dann ist U offensichtlich zyklisch.

Sei also $a^z \in U$ mit $a^z \neq e$.

$\Rightarrow (a^z)^{-1} = a^{-z} \in U$ und entweder $z \in \mathbb{N}$ oder $-z \in \mathbb{N}$

\Rightarrow es gibt ein **kleinstes** $n \geq 1$ mit $a^n \in U$.

Wir zeigen nun $U = \{(a^n)^z : z \in \mathbb{Z}\} = \langle a^n \rangle$.

■ $\langle a^n \rangle \subseteq U$ ist klar, da U eine Gruppe ist und $a^n \in U$

■ sei $a^z \in U$ und $z = qn + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < n$

\Rightarrow da $a^{-qn} \in \langle a^n \rangle \subseteq U$, ist $a^r = a^{-qn} \cdot a^z \in U$

\Rightarrow wegen der **minimalen Wahl von n** und $0 \leq r < n$ folgt also $r = 0$

$\Rightarrow a^z = a^{qn} \in \langle a^n \rangle$



Gruppen mit Primzahlordnung

Satz

Jede endliche Gruppe G deren Ordnung p eine Primzahl ist, ist zyklisch und hat nur triviale Untergruppen.

Beweis: Sei $a \in G$. Da $p = |G|$ eine Primzahl ist, ist nach dem Satz von LAGRANGE die Ordnung von a entweder 1 oder p .

- Ordnung von a ist $1 \iff a = e$
 - da $|G| \geq 2$, gibt es ein $a \in G$ mit $a \neq e$
- \Rightarrow Ordnung von a ist $p \Rightarrow a^0, a^1, \dots, a^{p-1}$ sind paarweise verschiedene Elemente von G
- $\Rightarrow G = \{a^0, a^1, \dots, a^{p-1}\} = \langle a \rangle$



Permutationen

Erinnerung:

- $\mathcal{S}(A)$ ist die Menge aller Bijektionen von A nach A
- $(\mathcal{S}(A), \circ)$ ist eine Gruppe, genannt **symmetrische Gruppe** bzw. **Permutationsgruppe** auf A mit neutralem Element id_A
- für $A = [n]$ bezeichnen wir mit \mathcal{S}_n die Permutationsgruppe $(\mathcal{S}([n]), \circ)$
- Permutationsgruppen sind „universell“ für endliche Gruppen:

Satz (CAYLEY)

Jede endliche Gruppe G ist isomorph zu einer Untergruppe von $\mathcal{S}(G)$.

Beweis: Sei (G, \cdot) eine endliche Gruppe. Für jedes $a \in G$ ist die Abbildung $\sigma_a: G \longrightarrow G$ mit $b \longmapsto a \cdot b$ eine Bijektion, d. h. $\sigma_a \in \mathcal{S}(G)$. Nun betrachtet man die Abbildung $f: G \longrightarrow \mathcal{S}(G)$ gegeben durch

$$a \longmapsto \sigma_a .$$

Man überprüft nun:

- 1 $\{\sigma_a: a \in G\}$ ist Untergruppe von $\mathcal{S}(G)$ und
- 2 f ein Gruppenisomorphismus zwischen G und $\{\sigma_a: a \in G\}$.

$\{\sigma_a : a \in G\}$ ist Untergruppe von $\mathcal{S}(G)$

Für alle $a, b, c \in G$ gilt:

$$\blacksquare \sigma_e(c) = e \cdot c = c$$

$$\implies \sigma_e = \text{id}_G \in \{\sigma_a : a \in G\}$$

$$\blacksquare (\sigma_{a^{-1}} \circ \sigma_a)(c) = \sigma_{a^{-1}}(\sigma_a(c)) = \sigma_{a^{-1}}(a \cdot c) = a^{-1} \cdot (a \cdot c) = c$$

$$\implies \sigma_{a^{-1}} \circ \sigma_a = \text{id}_G$$

$$\implies \sigma_a^{-1} = \sigma_{a^{-1}} \in \{\sigma_a : a \in G\}$$

$$\blacksquare (\sigma_a \circ \sigma_b)(c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = \sigma_{a \cdot b}(c)$$

$$\implies \sigma_a \circ \sigma_b = \sigma_{a \cdot b} \in \{\sigma_a : a \in G\}$$

Untergruppenkriterium $\implies \{\sigma_a : a \in G\}$ ist Untergruppe von $\mathcal{S}(G)$. ✓

Gruppenisomorphismus $f: G \longrightarrow \{\sigma_a: a \in G\}$

- f ist surjektiv: per Definition auf $\{\sigma_a: a \in G\} \subseteq \mathcal{S}(G)$
- f ist injektiv: $\sigma_a = \sigma_b$ bedeutet $ac = bc$ für alle $c \in G \Rightarrow a = b$

$\Rightarrow f$ ist eine Bijektion



Seien $a, b \in G$ beliebig. Die Abbildung $\sigma_{a \cdot b} = f(a \cdot b)$ ist eine Bijektion auf G , d. h. $f(a \cdot b)$ ordnet jedem $c \in G$ ein $\sigma_{a \cdot b}(c) = (a \cdot b) \cdot c \in G$ zu. Somit gilt für jedes $c \in G$

$$f(a \cdot b)(c) = \sigma_{a \cdot b}(c) = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot \sigma_b(c)$$

und somit gilt

$$f(a \cdot b)(c) = a \cdot \sigma_b(c) = \sigma_a(\sigma_b(c)) = (\sigma_a \circ \sigma_b)(c) = (f(a) \circ f(b))(c).$$

Da diese Identität für alle $c \in G$ gilt, gilt also $f(a \cdot b) = f(a) \circ f(b)$ und da $a, b \in G$ beliebig waren, ist f somit ein Gruppenisomorphismus. \square

Notation

- wir studieren Permutationsgruppen \mathcal{S}_n für $n \in \mathbb{N}_0$
- Permutationen werden oft mit kleinen griechischen Buchstaben π , σ , oder τ bezeichnet
- manchmal geben wir Permutationen explizit an, z. B.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in \mathcal{S}_5$$

bildet 1 auf 3, 2 auf 2, 3 auf 5, 4 auf 1 und 5 auf 4 ab,

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 5, \quad \sigma(4) = 1 \quad \text{und} \quad \sigma(5) = 4.$$

- da die erste Zeile in der expliziten Darstellung von σ redundant ist, schreiben wir manchmal auch nur $\sigma = (3, 2, 5, 1, 4)$

ACHTUNG: nicht verwechseln mit der späteren Zykelschreibweise

- da \mathcal{S}_5 endlich ist ($|\mathcal{S}_5| = 5! = 120$), hat σ endliche Ordnung (die nach LAGRANGE ein Teiler von 120 ist), d. h. es gibt ein k mit $k \mid 120$, sodass

$$\sigma^k = \sigma \circ \dots \circ \sigma = \text{id}_{[5]} .$$

Für dieses Beispiel prüft man leicht nach, dass $k = 4$ ist.

Beispiel

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in \mathcal{S}_5$$

- iterierte Anwendungen von σ fixiert die 2 fest ($\sigma(2) = 2$) und „zykelt“ (ausgehend von 1) durch die Elemente 3, 5, 4, 1

$$\sigma(1) = 3, \quad \sigma^2(1) = \sigma(3) = 5, \quad \sigma^3(1) = \sigma(5) = 4$$

und

$$\sigma^4(1) = \sigma^3(3) = \sigma^2(5) = \sigma(4) = 1$$

und danach wiederholt sich diese Sequenz

- σ „zerfällt“ in einen Zyklus (1 3 5 4) und einen Fixpunkt (2) (trivialer Zyklus)

Zyklen

Definition (Zyklus)

Sei $X \subseteq [n]$ mit $X = \{x_1, \dots, x_k\}$ für $k \geq 2$.

Wir bezeichnen mit $(x_1 x_2 \dots x_k)$ die Permutation $\sigma \in \mathcal{S}_n$ definiert durch

$$\sigma(x) = \begin{cases} x & \text{falls } x \notin X, \\ x_{i+1} & \text{falls } x = x_i \text{ für } i = 1, \dots, k-1, \\ x_1 & \text{falls } x = x_k. \end{cases}$$

Die Permutation σ ist dann ein **Zyklus** der Länge k und Zyklen der Länge 2 (Vertauschung von zwei Elementen) heißen **Transpositionen**.

Zwei Zyklen $(x_1 x_2 \dots x_k)$ und $(y_1 y_2 \dots y_\ell)$ sind **disjunkt**, wenn die beiden Mengen $\{x_1, \dots, x_k\}$ und $\{y_1, \dots, y_\ell\}$ disjunkt sind.

Neben den Schreibweisen $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ und $(3, 2, 5, 1, 4)$ gibt es so noch die Zykelschreibweisen

$$(1354) = (3541) = (5413) = (4135) \in \mathcal{S}_5.$$

Zyklenzerlegung

Satz

Sei $n \in \mathbb{N}_0$. Dann gilt:

- Jede Permutation $\sigma \in \mathcal{S}_n$ ist ein Produkt von paarweise disjunkten Zyklen. Eine solche Darstellung nennt man **Zyklenzerlegung** von σ und diese ist bis auf die Reihenfolge eindeutig.
 - Jeder Zyklus ist ein Produkt von Transpositionen.
- ⇒ Jede Permutation $\sigma \in \mathcal{S}_n$ ist ein Produkt von Transpositionen.

Beispiel:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix} \in \mathcal{S}_6$$

$$\Rightarrow \sigma = (1\ 4\ 3) \circ (2\ 5\ 6)$$

$$\Rightarrow (1\ 4\ 3) = (1\ 4) \circ (4\ 3) \text{ und } (2\ 5\ 6) = (2\ 5) \circ (5\ 6)$$

$$\Rightarrow \sigma = (1\ 4) \circ (4\ 3) \circ (2\ 5) \circ (5\ 6)$$

Beweis der Zyklenzerlegung

Beweis: Betrachte die Relation $i \sim j$ auf $[n]$ gegeben durch

$$\exists z \in \mathbb{Z}: \sigma^z(i) = j.$$

- man prüft direkt nach, dass \sim eine Äquivalenzrelation ist
- für jede Äquivalenzklasse $[i]$ gibt es ein $m_i \in \mathbb{N}_0$, sodass

$$[i] = \{\sigma^0(i), \sigma^1(i), \dots, \sigma^{m_i}(i)\}$$

- ist $m_i = 0$, dann ist i ein Fixpunkt von σ
 - ist $m_i > 0$, dann ist $(\sigma^0(i) \sigma(i) \dots \sigma^{m_i}(i))$ ein Zykel von σ
- ⇒ Partition durch Äquivalenzklassen codiert disjunkte Zyklen von σ ✓

Der zweite Teil folgt direkt aus der Darstellung

$$(x_1 x_2 \dots x_k) = (x_1 x_2) \circ (x_2 x_3) \circ \dots \circ (x_{k-2} x_{k-1}) \circ (x_{k-1} x_k).$$



Gerade und ungerade Permutationen

Satz

Sei $\sigma \in \mathcal{S}_n$. Die Parität (gerade/ungerade) der Anzahl der Transpositionen in jeder Darstellung von σ als Transpositionen ist gleich. Dementsprechend sagen wir eine Permutation ist **gerade** bzw. **ungerade**.

Bemerkung: Einen Beweis von diesem Satz finden Sie im Skript.

Korollar

Die Menge der geraden Permutationen $\mathcal{A}_n \subseteq \mathcal{S}_n$ bildet eine Untergruppe vom Index 2 und heißt **alternierende Gruppe**.

Beweis:

- $\text{id}_{[n]}$ wird durch 0 Transpositionen dargestellt und ist somit in \mathcal{A}_n
- da die Summe zweier gerader Zahlen gerade ist, ist die Komposition zweier gerader Permutationen wieder gerade
- da Transpositionen selbstinvers sind, gilt

$$\sigma = \tau_1 \circ \cdots \circ \tau_k \implies \sigma^{-1} = (\tau_1 \circ \cdots \circ \tau_k)^{-1} = \tau_k^{-1} \circ \cdots \circ \tau_1^{-1} = \tau_k \circ \cdots \circ \tau_1$$

\implies wenn $\sigma \in \mathcal{A}_n$, dann ist auch $\sigma^{-1} \in \mathcal{A}_n$

Somit zeigt das Untergruppenkriterium, dass \mathcal{A}_n eine Untergruppe von \mathcal{S}_n ist. \square

Körper

- mithilfe von Gruppen kann man Körper kompakter definieren

Definition (Körper)

Eine Menge K mit verschiedenen Elementen $0_K, 1_K \in K$ und binären Operationen $+: K \times K \longrightarrow K$ und $\cdot: K \times K \longrightarrow K$ ist ein **Körper**, falls gilt:

- 1 $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0_K ,
- 2 $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K ,
- 3 für alle $a, b, c \in K$ gelten die Distributivgesetze

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

Bemerkung:

- mit den Distributivgesetzen folgt $a \cdot 0_K = 0_K \cdot a = 0_K$ für alle $a \in K$:

$$a \cdot 0_K = a \cdot (0_K + 0_K) = a \cdot 0_K + a \cdot 0_K \quad \Longrightarrow \quad 0_K = a \cdot 0_K$$

$$0_K \cdot a = (0_K + 0_K) \cdot a = 0_K \cdot a + 0_K \cdot a \quad \Longrightarrow \quad 0_K = 0_K \cdot a.$$

Komplexen Zahlen

Einer der Gründe, warum man anstelle der rationalen Zahlen mit den reellen Zahlen arbeitet ist der, dass sich gewisse Gleichungen in \mathbb{Q} nicht lösen lassen, während in \mathbb{R} Lösungen existieren.

Ein Beispiel ist die Gleichung $x^2 = 2$, die die irrationalen Lösungen $\pm\sqrt{2}$ hat. Da das Quadrat jeder reellen Zahl ≥ 0 ist, lässt sich aber zum Beispiel die Gleichung $x^2 = -1$ in \mathbb{R} nicht lösen.

Dieses Problem lösen wir, indem wir ein letztes Mal den Zahlenbereich erweitern und von den reellen Zahlen zu den *komplexen Zahlen* übergehen.

Die komplexen Zahlen werden in vielen Anwendungen der Mathematik benötigt, etwa in der Physik oder in der Elektrotechnik.

Komplexe Zahlen

Definition (\mathbb{C})

Wir definieren die Menge \mathbb{C} der **komplexen Zahlen**

$$\mathbb{C} = \mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}.$$

Auf \mathbb{C} definieren wir eine Addition und eine Multiplikation wie folgt für alle $(a, b), (c, d) \in \mathbb{C}$

- $(a, b) + (c, d) = (a + c, b + d)$
- $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

Satz

Die Menge \mathbb{C} bildet mit der definierten Addition und Multiplikation einen Körper mit Nullelement $(0, 0)$ und Einselement $(1, 0)$.

Beweis der Körpereigenschaften

- Assoziativ-, Kommutativ- und Distributivgesetze überprüft man durch nachrechnen.
- $(\mathbb{C}, +)$ ist eine abelsche Gruppe mit neutralem Element $(0, 0)$ und inversen Elementen $-(a, b) = (-a, -b)$.
- $(\mathbb{C} \setminus \{(0, 0)\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element $(1, 0)$ und inversen Elementen

$$(a, b)^{-1} = (A, B) \quad \text{für} \quad A = \frac{a}{a^2 + b^2} \quad \text{und} \quad B = \frac{-b}{a^2 + b^2}$$

da

$$(a, b)^{-1} \cdot (a, b) = (A, B) \cdot (a, b) = (Aa - Bb, Ab + Ba)$$

und

$$(Aa - Bb, Ab + Ba) = \left(\frac{aa}{a^2 + b^2} - \frac{-bb}{a^2 + b^2}, \frac{ab}{a^2 + b^2} + \frac{-ba}{a^2 + b^2} \right) = (1, 0).$$

Komplexe Zahlen als Erweiterung der reellen Zahlen

Um nun den Körper \mathbb{C} der komplexen Zahlen als Erweiterung von \mathbb{R} auffassen zu können, müssen wir \mathbb{R} mit einer geeigneten Teilmenge von \mathbb{C} identifizieren.

Diese Teilmenge ist die x -Achse in \mathbb{R}^2 , also die Menge $\{(a, 0) : a \in \mathbb{R}\}$. In der Tat rechnet man schnell nach, dass für alle $a, b \in \mathbb{R}$ gilt:

$$(a, 0) + (b, 0) = (a + b, 0)$$

und

$$(a, 0) \cdot (b, 0) = (ab - 0 \cdot 0, a \cdot 0 + 0 \cdot b) = (ab, 0).$$

Das zeigt, dass die Abbildung $a \mapsto (a, 0)$ ein Isomorphismus von Körpern zwischen dem Körper \mathbb{R} der reellen Zahlen und dem Unterkörper $\{(a, 0) : a \in \mathbb{R}\}$ von \mathbb{C} ist.

Wir können also tatsächlich \mathbb{R} als eine Teilmenge von \mathbb{C} auffassen.

Konventionen

Wir vereinfachen nun unsere Notation wie folgt:

Definition

- Das Nullelement $(0, 0)$ bezeichnen wir oftmals mit $0 \in \mathbb{C}$.
- Das Einselement $(1, 0)$ bezeichnen wir oftmals mit $1 \in \mathbb{C}$.
- Die komplexe Zahl $(0, 1)$ heißt **imaginäre Einheit** und wird mit **i** bezeichnet.
- Anstelle von $(a, b) \in \mathbb{C}$ schreiben wir $a + ib$, dabei nennen wir a den **Realteil** der komplexen Zahl $a + ib$ und b den **Imaginärteil**.

Es gilt

$$i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1 + i0 = -1.$$

Praktisch kann man mit komplexen Zahlen in der Form $a + ib$ rechnen:

- Es dürfen die bekannten Rechenregeln in Körpern angewendet werden.
- Der Term i^2 , kann durch -1 ersetzt werden.
- Nach dem Verrechnen ordnen wir wieder die Terme um $c + id$ mit $c, d \in \mathbb{R}$ zu erhalten.

Beispiele

- Es gilt

$$(a + \mathbf{i}b) + (c + \mathbf{i}d) = a + c + \mathbf{i}(b + d)$$

entsprechend der Definition $(a, b) + (c, d) = (a + c, b + d)$.

- Es gilt

$$(a + \mathbf{i}b) \cdot (c + \mathbf{i}d) = ac + \mathbf{i}ad + \mathbf{i}bc + \mathbf{i}^2bd = ac - bd + \mathbf{i}(ad + bc)$$

entsprechend der Definition von $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

- Wir dividieren zwei komplexe Zahlen wie folgt: Sei $c + \mathbf{i}d \neq 0$, d.h., wir nehmen an, dass c und d nicht beide 0 sind. Dann gilt

$$\frac{a + \mathbf{i}b}{c + \mathbf{i}d} = \frac{(a + \mathbf{i}b) \cdot (c - \mathbf{i}d)}{(c + \mathbf{i}d) \cdot (c - \mathbf{i}d)} = \frac{ac + bd + \mathbf{i}(bc - ad)}{c^2 + d^2}.$$

Insbesondere gilt

$$\frac{1}{c + \mathbf{i}d} = \frac{c - \mathbf{i}d}{c^2 + d^2}.$$

Konjugation

Definition (konjugiert komplexe Zahl)

Für eine komplexe Zahl $z = a + \mathbf{i}b$ ist $\bar{z} = a - \mathbf{i}b$ die zu z **konjugiert komplexe Zahl**. Der **Betrag** von z ist die Zahl $|z| = \sqrt{a^2 + b^2}$.

Satz

- 1 Für jede komplexe Zahl $z \in \mathbb{C}$ ist $|z|^2 = z \cdot \bar{z}$.
- 2 Der Realteil von z ist die Zahl $\frac{1}{2}(z + \bar{z})$.
- 3 Der Imaginärteil ist die Zahl $\frac{1}{2}(z - \bar{z})$.
- 4 Für zwei komplexe Zahlen $z_1, z_2 \in \mathbb{C}$ gilt

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \quad \text{und} \quad \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$$

Beweis Es gilt

$$(a + \mathbf{i}b) \cdot (a - \mathbf{i}b) = a^2 - \mathbf{i}^2 b^2 = a^2 + b^2 = |z|^2.$$

Die anderen Aussagen rechnet man ebenfalls einfach nach. □

Wurzeln aus negativen Zahlen

Der Grund, warum die komplexen Zahlen eine so wichtige Rolle spielen, ist die Tatsache, dass wir in den komplexen Zahlen beliebige Wurzeln auch aus negativen Zahlen ziehen können.

Warum das so ist, werden wir im nächsten Semester klären, wenn wir die trigonometrischen Funktionen \sin und \cos zur Verfügung haben.

Allerdings können die komplexen Zahlen die reellen Zahlen nicht ersetzen, weil sie keinen angeordneten Körper bilden, da es in \mathbb{C} Zahlen gibt, deren Quadrate negativ sind, zum Beispiel i und $-i$.

Ringe

- Ringe benötigen weniger multiplikative Struktur als Körper

Definition (Ring)

Eine Menge R mit binären Operationen $+: R \times R \longrightarrow R$ und $\cdot: R \times R \longrightarrow R$ ist ein **Ring**, falls gilt:

- 1** $(R, +)$ ist eine abelsche Gruppe,
- 2** (R, \cdot) ist eine Halbgruppe,
- 3** für alle $a, b, c \in R$ gelten die Distributivgesetze

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

Das neutrale Element der Addition ist das **Nullelement** 0_R von R . Wenn die Multiplikation kommutativ ist, dann ist R ein **kommutativer Ring**. Ist (R, \cdot) sogar ein Monoid mit neutralem Element 1_R , dann ist R ein **Ring mit 1/unitärer Ring**.

- wie in Körpern folgert man $0_R \cdot a = 0_R = a \cdot 0_R$ aus den Distributivgesetzen
- wir betrachten nur Ringe mit 1 und meinen bei einem Ring immer einen mit 1
- falls $0_R = 1_R$, dann ist $R = \{0_R\}$ der Nullring mit nur einem Element, da dann für jedes $a \in R$ gilt:

$$a = a \cdot 1_R = a \cdot 0_R = 0_R.$$

Beispiele und Notation

- $(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind Körper
- jeder Körper ist ein kommutativer Ring (mit 1)
- ein Ring ist nur dann ein Körper, wenn $(R \setminus \{0_R\}, \cdot)$ eine abelsche Gruppe ist
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring (mit 1), aber kein Körper
- für jedes $n \in \mathbb{N}$ ist der Restklassenring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring (mit 1)
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist nur dann ein Körper, wenn n eine Primzahl ist
- wenn die Operationen klar sind, dann identifizieren wir Körper und Ringe mit ihrer Grundmenge
- an Stelle von 0_R , 1_K etc. schreiben wir oft nur 0 und 1
- für ein Element a bezeichnen wir mit $-a$ und a^{-1} die inversen Elemente bezüglich der Addition und Multiplikation

Einheitengruppe

- in einem Monoid sind die inversen Elemente (wenn sie existieren) eindeutig

Definition (Einheiten)

Sei R ein Ring (mit 1). Die Menge der Elemente a die ein multiplikatives Inverses a^{-1} haben, heißt **Einheitengruppe** $R^\times \subseteq R$, d. h.

$$R^\times := \{a \in R : \text{es gibt } b \in R \text{ mit } a \cdot b = b \cdot a = 1\},$$

und die Elemente von R^\times heißen **Einheiten**.

Satz

Für jeden Ring (mit 1) ist die Einheitengruppe (R^\times, \cdot) eine Gruppe.

Beweis

- $a, b \in R^\times \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \in R \Rightarrow ab \in R^\times$ (\cdot wohldef. auf R^\times)
- $1 \in R^\times$ und $a \in R^\times \Rightarrow a^{-1} \in R^\times$
- Assoziativität vererbt sich vom Monoid (R, \cdot) □

Beispiele

- für jeden Körper K ist $K^\times = K \setminus \{0\}$
- insbesondere

$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\} \quad \text{und} \quad \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$$

und für jede Primzahl p gilt

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$$

- für die ganzen Zahlen gilt: $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$
- $(\mathbb{Z}/15\mathbb{Z})^\times = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$
- allgemein wissen wir für $n \in \mathbb{N}$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : \text{ggT}(a, n) = 1\}$$

8. Polynome

Polynome über Körpern

Definition (Polynome)

Sei K ein Körper und X ein Unbekannte/Variable. Ein Ausdruck der Form

$$a_0X^0 + a_1X^1 + a_2X^2 + \dots + a_nX^n = \sum_{i=0}^n a_iX^i$$

mit $n \in \mathbb{N}_0$ und **Koeffizienten** $a_0, \dots, a_n \in K$, heißt **Polynom (über K)**.

- Die Menge aller Polynome über K bezeichnen wir mit $K[X]$.
- Polynome der Form a_0X^0 heißen **konstant**.
- Der Körper K läßt sich in $K[X]$ durch $a \mapsto aX^0$ mit den konstanten Polynomen identifizieren und als Teilmenge von $K[X]$ auffassen.
- **Bem.:** Im Allgemeinen werden Polynome oft auch über kommutative Ringe mit 1 (z. B. über \mathbb{Z}) betrachtet.

Beispiel

$$1X^0 + \frac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + (5 - 3i)X^5 + \sqrt{2}X^6 \in \mathbb{C}[X]$$

Konventionen

- die Reihenfolge der Terme eines Polynoms ist unerheblich, aber zur besseren Übersicht gibt man die Terme meistens monoton aufsteigend oder absteigend in den Potenzen an
- X^0 ist für alle möglichen Werte $1 \in K$ und wird oft weggelassen und nur der Koeffizient a_0 geschrieben
- für X^1 schreibt man einfach X
- Terme mit Koeffizient $0 \in K$ läßt man meistens weg
- Koeffizienten $a_i = 1$ läßt man auch meistens weg, außer für $i = 0$
- für Terme der Form $(-a)X^i$ „zieht“ man das Minus in die Summe der Terme

Angewandt auf das Beispiel

$$1X^0 + \frac{7}{3}X^1 + (-0.01)X^2 + 0X^3 + 1X^4 + (5 - 3i)X^5 + \sqrt{2}X^6$$

ergibt sich die vereinfachte Darstellung

$$\sqrt{2}X^6 + (5 - 3i)X^5 + X^4 - 0.01X^2 + \frac{7}{3}X + 1.$$

Polynome über $\mathbb{Z}/p\mathbb{Z}$

- neben den Polynomen über die unendlichen Körper \mathbb{C} , \mathbb{R} und \mathbb{Q} , können wir auch Polynome über $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p betrachten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

- Zur Vereinfachung der Notation schreiben wir für die Koeffizienten anstelle der Restklassen einfach den Standardrepräsentanten:

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 + 3X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X],$$

wobei

$$[4]_5 X^3 + [-2]_5 X^2 + [1]_5 = 4X^3 - 2X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

auch üblich ist.

Grad eines Polynoms

Definition (Grad)

Sei $p = \sum_{i=0}^n a_i X^i \in K[X]$ ein Polynom über einem Körper K . Der **Grad von p** ist das größte $i \in \{0, \dots, n\}$ mit $a_i \neq 0$ und wird mit $\text{grad}(p)$ bezeichnet. Gilt $a_i = 0$ für alle $i \in \{0, \dots, n\}$, so nennt man p das **Nullpolynom** und setzt $\text{grad}(p) = -\infty$.

Konstante Polynome sind dann entweder das Nullpolynom oder Polynome mit Grad 0.

Wenn p nicht das Nullpolynom ist, bezeichnet $a_{\text{grad}(p)}$ den **Leitkoeffizienten** und p heißt **normiert**, falls der Leitkoeffizient 1 ist.

- zwei Polynome $p = \sum_{i=0}^n a_i X^i$ und $q = \sum_{i=0}^m b_i X^i$ über dem gleichen Körper K sind gleich, wenn:
 - $\text{grad}(p) = \text{grad}(q)$
 - und $a_i = b_i$ für alle $i = 0, \dots, \text{grad}(p)$.

$$0X^3 - X^2 + 0X + 3 = -X^2 + 0X + 3 = -X^2 + 3$$

Addition von Polynomen

Definition

Seien $p = \sum_{i=0}^n a_i X^i$ und $q = \sum_{i=0}^m b_i X^i$ Polynome über dem gleichen Körper K . Wir definieren die Summe $p + q$ koeffizientenweise

$$p + q := \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) X^i,$$

wobei $b_{m+1} = \dots = b_n = 0$ (falls $n > m$) bzw. $a_{n+1} = \dots = a_m = 0$ (falls $m > n$).

Somit gilt $\text{grad}(p + q) \leq \max\{\text{grad}(p), \text{grad}(q)\}$.

Beispiel: Für $p = X^4 + 3X^2 + 2$ und $q = 4X^4 + X^3 + 2X^2 - 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p + q = 5X^4 + X^3 + 5X^2 + 1 = X^3 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$$

$\implies \text{grad}(p + q) = 3 < 4 = \max\{\text{grad}(p), \text{grad}(q)\}$ hier

Im Allgemeinen gilt: $\text{grad}(p + q) < \max\{\text{grad}(p), \text{grad}(q)\}$

$\iff \text{grad}(p) = \text{grad}(q)$ und die Leitkoeffizienten sind additive Inverse in K .

Multiplikation von Polynomen

Definition

Seien $p = \sum_{i=0}^n a_i X^i$ und $q = \sum_{i=0}^m b_i X^i$ Polynome über dem gleichen Körper K . Wir definieren das Produkt $p \cdot q$ „durch ausmultiplizieren“

$$p \cdot q := \sum_{i=0}^{m+n} c_i X^i \quad \text{mit} \quad c_i := \sum_{j=0}^i a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$$

wobei (ähnlich wie bei der Addition) dafür $b_{m+1} = \dots = b_{m+n} = 0$ und $a_{n+1} = \dots = a_{m+n} = 0$ gesetzt wird.

Aus der Definition folgt direkt:

$$\text{grad}(p \cdot q) \leq \text{grad}(p) + \text{grad}(q) \quad \text{mit} \quad c_{\text{grad}(p) + \text{grad}(q)} = a_{\text{grad}(p)} \cdot b_{\text{grad}(q)}$$

Da in Körpern das Produkt $a_{\text{grad}(p)} \cdot b_{\text{grad}(q)}$ zweier von Null verschiedener Elemente niemals Null ist, folgt somit auch

$$\text{grad}(p \cdot q) = \text{grad}(p) + \text{grad}(q)$$

für Polynome über einem Körper K .

Beispiel

Für $p = X^3 + 3X^2 + 2$ und $q = 2X^2 - X + 4 \in (\mathbb{Z}/5\mathbb{Z})[X]$ erhalten wir

$$p \cdot q = (X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4)$$

ausmultiplizieren ergibt

$$= 2X^5 + (-1 + 3 \cdot 2)X^4 + (4 - 3)X^3 + (3 \cdot 4 + 2 \cdot 2)X^2 - 2X + 8$$

und zusammenfassen und umrechnen in Standardrepräsentanten führt zu

$$= 2X^5 + 5X^4 + X^3 + 16X^2 - 2X + 8 = 2X^5 + X^3 + X^2 + 3X + 3.$$

Es gilt in $(\mathbb{Z}/5\mathbb{Z})[X]$ also

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3.$$

Abstecher zu Polynomen über kommutativen Ringen

Betrachtet man Polynome über kommutative Ringe (mit 1), dann gilt die Gradformel für das Produkt im Allgemeinen nicht.

Beispiel: Für $p = 2X^3$ und $q = 3X^2 + 1$ in $(\mathbb{Z}/6\mathbb{Z})[X]$ gilt

$$p \cdot q = 6X^5 + 2X^3 = 2X^3 \in (\mathbb{Z}/6\mathbb{Z})[X]$$

$$\implies \text{grad}(p \cdot q) = 3 < 5 = \text{grad}(p) + \text{grad}(q)$$

Polynomringe

Satz

Für jeden Körper K ist die Menge der Polynome $K[X]$ zusammen mit der definierten Addition und Multiplikation für Polynome ein **kommutativer Ring mit 1**, wobei das Nullpolynom das neutrale Element der Addition und das konstante Polynom $1 = 1X^0$ das neutrale Element der Multiplikation ist.

Wir nennen $K[X]$ deswegen **Polynomring (über K)**.

Beweis:

- Assoziativität und Kommutativität von $+$ vererbt sich von K
 - Nullpolynom ist offensichtlich neutral bezüglich der Addition
 - $p = \sum_{i=0}^n a_i X^i \in K[X] \implies -p := \sum_{i=0}^n (-a_i) X^i \in K[X]$
- $\implies (K[X], +)$ ist eine abelsche Gruppe
- Assoziativität und Kommutativität von \cdot vererbt sich von K
 - konstantes Einspolynom $1 = 1X^0$ ist neutral bezüglich der Multiplikation
- $\implies (K[X], \cdot)$ ist ein kommutatives Monoid
- Distributivgesetzte kann man nachrechnen □

Auch Polynome $R[X]$ über kommutative Ringe R mit 1 bilden einen solchen.

Teilbarkeit für Polynome

Definition

Sei K ein Körper und $p, q \in K[X]$ Polynome. Das Polynom p ist ein **Vielfaches** von q , falls es ein Polynom $m \in K[X]$ gibt, sodass

$$p = q \cdot m.$$

Wir schreiben dafür $q \mid p$ und sagen **q teilt p** , oder **q ist ein Teiler von p** .

Teilt ein Polynom $r \in K[X]$ sowohl p als auch q , dann ist r ein **gemeinsamer Teiler** von p und q .

Das Polynom r ist ein **größter gemeinsamer Teiler** von p und q (\neq Nullpolynom), wenn es ein gemeinsamer Teiler mit maximalem Grad ist.

Der größte gemeinsame Teiler von einem Polynom p und dem Nullpolynom ist p , insbesondere auch, falls p selbst das Nullpolynom ist.

Beispiel: In $\mathbb{Z}/5\mathbb{Z}$ gilt

$$(X^3 + 3X^2 + 2) \cdot (2X^2 - X + 4) = 2X^5 + X^3 + X^2 + 3X + 3.$$

$\Rightarrow X^3 + 3X^2 + 2$ und $2X^2 - X + 4$ sind Teiler von $2X^5 + X^3 + X^2 + 3X + 3$.

Einheiten in $K[X]$

- $p \in (K[X])^\times$, falls es ein $q \in K[X]$ mit $p \cdot q = 1 = 1X^0$ gibt
- $\text{grad}(1) = 0$ und da K ein Körper ist, gilt

$$\text{grad}(p \cdot q) = \text{grad } p + \text{grad } q$$

⇒ nur die konstanten Polynome mit Grad 0 können Einheiten sein

- tatsächlich gibt es für jedes $a \in K \setminus \{0\}$ ein multiplikativ Inverses $a^{-1} \in K \setminus \{0\}$ und für die konstanten Polynome $p = aX^0$ und $q = a^{-1}X^0$ gilt

$$p \cdot q = (a \cdot a^{-1})X^0 = 1X^0$$

Satz

Für jeden Körper K sind die Einheiten des Polynomrings $K[X]$ genau die konstanten Polynome vom Grad 0, d. h.

$$(K[X])^\times = \{aX^0 : a \in K \setminus \{0\}\}.$$

Größte gemeinsame Teiler

- wie man an den konstanten Polynomen leicht sieht, sind größte gemeinsame Teiler nicht eindeutig bestimmt
- z. B. für $p_1 = aX^0$, $p_2 = bX^0 \in K[X]$ mit $a, b \neq 0$ teilt jedes Polynom $m = cX^0$ mit $c \neq 0$ sowohl p_1 als auch p_2 und da jeder Teiler von p_1 und p_2 Grad 0 haben muss, ist ein jedes solches m ein größter gemeinsamer Teiler

- auch für Polynome mit höheren Grad tritt diese Phänomen auf, da

$$m \mid p_1 \quad \text{und} \quad m \mid p_2 \quad \implies \quad a \cdot m \mid p_1 \quad \text{und} \quad a \cdot m \mid p_2$$

für alle $m, p_1, p_2 \in K[X]$ und $a \in K \setminus \{0\}$

- ein größter gemeinsamer Teiler zweier Polynome läßt sich wie der ggT zweier ganzer Zahlen mit dem EUKLIDISCHEN Algorithmus bestimmen
- EUKLIDISCHER Algorithmus in \mathbb{Z} beruht auf der Division mit Rest
- analog führen wir die Division mit Rest in $K[X]$ ein

→ Polynomdivision

Polynomdivision

Satz

Sei K ein Körper und seien $p, m \in K[X]$ Polynome mit $m \neq 0$, dann gibt es Polynome $q, r \in K[X]$ mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m)$.

Beweis: Sei $p = \sum_{i=0}^n a_i X^i$ und $m = \sum_{i=0}^k b_i X^i$ mit $\text{grad}(p) = n$ und $\text{grad}(m) = k$. Der folgende Algorithmus der Polynomdivision ermittelt Polynome q und r mit den gewünschten Eigenschaften.

1 Falls $n < k$, dann geben wir $q = 0$ und $r = p$ aus.

2 Initialisiere $s = p$

3 Solange $\ell := \text{grad}(s) \geq k$ und $s = \sum_{i=0}^{\ell} d_i X^i$:

■ Setze $c_{\ell-k} = \frac{d_{\ell}}{b_k}$.

■ Setze $s := s - c_{\ell-k} X^{\ell-k} \cdot m$.

4 Gib $r = s$ und $q = \sum_{i=0}^{n-k} c_i X^i$ aus.

Algorithmus terminiert, da sich in jedem Durchlauf von **3** der Grad von s um mindestens 1 verringert und $k \geq 0$ gilt. Tatsächlich hat $c_{\ell-k} X^{\ell-k} \cdot m$ Leitkoeffizienten $c_{\ell-k} \cdot b_k = d_{\ell}$ und Grad ℓ genau wie s . Somit hat das Polynom $s - c_{\ell-k} X^{\ell-k} \cdot m$ einen geringeren Grad.

Korrektheit der Polynomdivision

Die Korrektheit beweisen wir mit Induktion nach n und betrachten dafür die rekursive Version des Algorithmus:

- 1 Falls $n < k$, dann gib $q = 0$ und $r = p$ zurück.
- 2 Finde rekursiv q' und r für die Division von $p' = p - \frac{a_n}{b_k} X^{n-k} \cdot m$ durch m , sodass

$$p' = q' \cdot m + r \quad \text{und} \quad \text{grad}(r) < k = \text{grad}(m). \quad (*)$$

- 3 Gib $q = q' + \frac{a_n}{b_k} X^{n-k}$ und r zurück.

Induktionsanfang für $n < k$: In diesem Fall liefert **1** eine Lösung, da dann $\text{grad}(p) = n < k = \text{grad}(r)$ und offensichtlich $p = 0 \cdot m + p$.

Induktionsschritt (mit allen Vorgängern) auf n : Da $\text{grad}(p') < \text{grad}(p) = n$, folgt mit der Induktionsvoraussetzung, dass in Schritt **2** q' und $r \in K[X]$ gefunden werden, die $(*)$ erfüllen. Einsetzen ergibt dann

$$p = p' + \frac{a_n}{b_k} X^{n-k} \cdot m \stackrel{(*)}{=} q' \cdot m + r + \frac{a_n}{b_k} X^{n-k} \cdot m = \left(q' + \frac{a_n}{b_k} X^{n-k} \right) \cdot m + r = q \cdot m + r.$$

□

Bemerkungen zur Polynomdivision

- die im Beweis angegebenen Algorithmen der Polynomdivision lassen sich effizient implementieren, wenn die Division im entsprechenden Körper K effizient realisierbar ist
- bei der Berechnung der Koeffizienten von q wird durch den Leitkoeffizienten von m geteilt, was in Polynomringen über Körpern immer möglich ist
- in Polynomringen $R[X]$ über kommutativen Ringen R mit 1 müßte man zusätzlich fordern, dass der Leitkoeffizient b_k von m eine Einheit ist, d. h. $b_k \in R^\times$
- mithilfe der Polynomdivision lässt sich der EUKLIDISCHE Algorithmus von \mathbb{Z} direkt auf Polynomringe $K[X]$ übertragen, um einen größten gemeinsamen Teiler von zwei gegebenen Polynomen $p_1, p_2 \in K[X]$ zu berechnen

Beispiel Polynomdivision

Gegeben seien Polynome $p = X^4 - 3X^2 + 5X - 3$ und $m = X - 1$ aus $\mathbb{R}[X]$ und gesucht sind q und r mit $p = q \cdot m + r$ und $\text{grad}(r) < \text{grad}(m) = 1$.

$$\begin{array}{r} X^4 \quad - 3X^2 + 5X - 3 = (X - 1)(X^3 + X^2 - 2X + 3) \\ - X^4 + X^3 \\ \hline \quad X^3 - 3X^2 \\ \quad - X^3 + X^2 \\ \hline \qquad - 2X^2 + 5X \\ \qquad 2X^2 - 2X \\ \hline \qquad \qquad 3X - 3 \\ \qquad \qquad - 3X + 3 \\ \hline \qquad \qquad \qquad 0 \end{array}$$

$\implies q = X^3 + X^2 - 2X + 3$ und $r = 0$

- über den Strichen auf der linken Seite steht der aktuelle Term $-c_{\ell-k}X^{\ell-k} \cdot m$
- unter den Strichen steht der aktuell relevante Teil von s
- unter dem letzten Strich (wenn $\text{grad}(s) < \text{grad}(m)$) steht das Restpolynom r
- auf der rechten Seite steht $m \cdot (c_{n-k}X^{n-k} + \dots + c_{\ell-k}X^{\ell-k} \dots)$ und am Ende der Rechnung $m \cdot q$
- wegen dem „=“ muß am Ende der Rechnung auf der rechten Seite noch $+r$ ergänzt werden (entfällt oben, da hier $r = 0$)

Weiteres Beispiel Polynomdivision

Für $p = X^4 - X^2 + 3X + 2$ und $m = X^2 - 2X + 1$ aus $\mathbb{R}[X]$ ergibt die Polynomdivision:

$$\begin{array}{r} X^4 \\ - X^4 + 2X^3 \\ \hline 2X^3 - 2X^2 + 3X \\ - 2X^3 + 4X^2 - 2X \\ \hline 2X^2 + X + 2 \\ - 2X^2 + 4X - 2 \\ \hline 5X \end{array} = (X^2 - 2X + 1)(X^2 + 2X + 2) + 5X$$

Hier ist der Quotient $q = X^2 + 2X + 2$ und der Rest $r = 5X$.

Erinnerung – EUKLIDISCHER Algorithmus in \mathbb{Z}

- da $\text{ggT}(x, y) = \text{ggT}(|x|, |y|)$, können wir uns auf \mathbb{N}_0 beschränken

Rekursiver EUKLIDISCHER Algorithmus

```
int ggT(int x, int y) {  
    if ( x==0 ) return y;  
    if ( y==0 ) return x;  
    if ( x>=y )  
        return ggT(x%y, y); /* x%y = mod(x,y) */  
    else  
        return ggT(x, y%x);  
}
```

EUKLIDISCHER Algorithmus in Polynomringen

- wie in \mathbb{Z} kann man größte gemeinsame Teiler von Polynomen mit Hilfe des EUKLIDISCHEN Algorithmus berechnen
- der Grad übernimmt die Rolle des Betrages bei den ganzen Zahlen und die Polynomdivision die Rolle der ganzzahligen Division in \mathbb{Z}
- dabei teilt man ausgehend von p_1 und p_2 , also in jedem Schritt mit der Polynomdivision das Polynom p_1 mit dem größeren Grad durch das Polynom mit dem kleineren Grad p_2 und ersetzt dann p_1 durch p_2 und p_2 durch r
- sobald p_2 das Nullpolynom ist, ist p_1 ein größter gemeinsamer Teiler gefunden
- im Unterschied zur Situation bei ganzen Zahlen, kann es bei Polynomen passieren, dass die beiden gegebenen Polynome p_1 und p_2 denselben Grad haben, ohne dass die beiden Polynome einander teilen
- in diesem Falle ist es egal, ob man zunächst das eine Polynom durch das andere teilt oder umgekehrt
- die Korrektheit dieses Verfahrens beweist man ebenso wie die Korrektheit des EUKLIDISCHEN Algorithmus in \mathbb{Z} , mit Induktion nach $\text{grad}(p_1) + \text{grad}(p_2)$, kombiniert mit der Proposition, dass für $p_1 = q \cdot p_2 + r$ mit $\text{grad}(r) < \text{grad}(p_2)$ jeder größte gemeinsame Teiler von p_2 und r auch ein größter gemeinsamer Teiler von p_1 und p_2 ist

Beispiel größter gemeinsamer Teiler in Polynomringen

Für $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$ aus $\mathbb{R}[X]$ suchen wir einen größten gemeinsamen Teiler.

Beide Grade sind gleich und es ist egal, wie wir beginnen. Wir teilen p_1 durch p_2 :

$$\begin{array}{r} X^3 - 3X^2 + 5X - 3 = (X^3 - 1)1 - 3X^2 + 5X - 2 \\ - X^3 + 1 \\ \hline - 3X^2 + 5X - 2 \end{array}$$

Der Rest ist $r_1 = -3X^2 + 5X - 2$ und im nächsten Schritt teilen wir p_2 durch r_1 .

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $p_2 = X^3 - 1$ durch $r_1 = -3X^2 + 5X - 2$ ergibt:

$$\begin{array}{r} X^3 - 1 = \left(-3X^2 + 5X - 2\right) \left(-\frac{1}{3}X - \frac{5}{9}\right) + \frac{19}{9}X - \frac{19}{9} \\ -X^3 + \frac{5}{3}X^2 - \frac{2}{3}X \\ \hline \frac{5}{3}X^2 - \frac{2}{3}X - 1 \\ -\frac{5}{3}X^2 + \frac{25}{9}X - \frac{10}{9} \\ \hline \phantom{\frac{5}{3}X^2 -} \frac{19}{9}X - \frac{19}{9} \end{array}$$

Der Rest ist $r_2 = \frac{19}{9}(X - 1)$ und im nächsten Schritt teilen wir $r_1 = -3X^2 + 5X - 2$ durch r_2 . Da das Polynom $\frac{19}{9}(X - 1)$ genau dieselben Teiler wie $X - 1$ hat und auch genau dieselben Polynome teilt, können wir aber einfach auf $r'_2 = X - 1$ übergehen.

Beispiel größter gemeinsamer Teiler in Polynomringen

Polynomdivision $r_1 = -3X^2 + 5X - 2$ durch $r'_2 = X - 1$ ergibt:

$$\begin{array}{r} -3X^2 + 5X - 2 = (X - 1)(-3X + 2) \\ \underline{3X^2 - 3X} \\ 2X - 2 \\ \underline{-2X + 2} \\ 0 \end{array}$$

Der Rest ist 0, also ist $X - 1$ ein größter gemeinsamer Teiler von den Ausgangspolynomen $p_1 = X^3 - 3X^2 + 5X - 3$ und $p_2 = X^3 - 1$.

Tatsächlich ist $X - 1$ ein gemeinsamer Teiler:

$$p_1 = X^3 - 3X^2 + 5X - 3 = (X - 1) \cdot (X^2 - 2X + 3)$$

und

$$p_2 = X^3 - 1 = (X - 1) \cdot (X^2 + X + 1).$$

Polynomfunktionen

- Polynome wurden bis jetzt als algebraische Objekte des Rings $K[X]$ betrachtet
- im Folgenden betrachten wir Polynome (wie aus der Schule bekannt) als Funktionen von K nach K

Definition (Polynomfunktion)

Sei K ein Körper und $p = \sum_{i=0}^n a_i X^i$ ein Polynom in $K[X]$. Die **Polynomfunktion** $f_p: K \rightarrow K$ ist gegeben durch

$$x \mapsto \sum_{i=0}^n a_i x^i \in K \quad \text{für alle } x \in K.$$

- Üblicherweise wird das Polynom p und die Polynomfunktion f_p gleichgesetzt und wir schreiben einfach $p(x)$ für $f_p(x)$.
- In diesem Fall ist aber x ein Element aus dem Körper K , welches **NICHT** mit der Unbekannten X des Polynomrings zu verwechseln ist.

Polynomfunktion vs. Polynom

- für jeden Körper K gibt es unendlich viele verschiedene Polynome in $K[X]$, z. B. die Polynome X^n für $n \in \mathbb{N}$
- für endliche Körper K gibt es aber nur endlich viele verschiedene Polynomfunktionen, da es höchstens $|K|^{|K|}$ verschiedene Funktionen $g: K \rightarrow K$ gibt

Bemerkung: tatsächlich hat für eine gegebene Funktion $g: K \rightarrow K$ das Polynom

$$p = \sum_{a \in K} g(a) \prod_{b \in K \setminus \{a\}} \frac{X - b}{a - b}$$

eine Polynomfunktion, die jedem $a \in K$ den Wert $g(a)$ zuordnet

⇒ für endliche Körper K gibt es verschiedene Polynome p und $q \in K[X]$, die die gleiche Polynomfunktion haben → Schubfachprinzip

Beispiel: $p = X$ und $q = X^3$ in $(\mathbb{Z}/3\mathbb{Z})[X]$

$$p(0) = 0, \quad p(1) = 1, \quad p(2) = 2$$

und

$$q(0) = 0, \quad q(1) = 1, \quad q(2) = 2$$

Nullstellen

Definition (Nullstelle)

Sei K ein Körper und $p \in K[X]$. Ein Element $a \in K$ heißt **Nullstelle** von (der Polynomfunktion) p , falls $p(a) = 0$.

Satz

Ein Element $a \in K$ ist genau dann eine Nullstelle von p , wenn das Polynom $X - a$ ein Teiler von p im Polynomring $K[X]$ ist.

Beweis: („ \implies “) Sei $p(a) = 0$ und betrachte $q, r \in K[X]$ gegeben durch die Polynomdivision von p geteilt durch $m = X - a$, d. h. $p = q \cdot (X - a) + r$ und wegen $\text{grad}(r) < \text{grad}(X - a) = 1$, ist $r = r' \cdot X^0$ konstant für ein $r' \in K$. Somit gilt für die Polynomfunktion

$$0 = p(a) = q(a) \cdot (a - a) + r(a) = q(a) \cdot 0 + r' = r'.$$

$\implies r = 0 \cdot X^0$ ist das Nullpolynom und $p = q \cdot (X - a)$, d. h. $(X - a) \mid p$ in $K[X]$ ✓

(„ \impliedby “) Falls p ein Vielfaches von $(X - a)$ ist, dann existiert $q \in K[X]$ mit $p = q \cdot (X - a)$. Für die Polynomfunktion ergibt sich also

$$p(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

und somit ist a eine Nullstelle. □

Nullstellen und Grad

Korollar

Ein Polynom $p \in K[X]$ vom Grad $n \geq 0$ hat höchstens n Nullstellen.

Beweis: (Induktion nach n)

Induktionsanfang für $n = 0$: klar, da konstante Polynome vom Grad 0 die Form $p = a_0 X^0$ mit $a_0 \in K \setminus \{0\}$ haben (Nullpolynom hat Grad $-\infty$)

$\Rightarrow p(a) = a_0 \neq 0$ für alle $a \in K \Rightarrow$ keine Nullstelle

✓

Induktionsschritt $n \rightarrow n + 1$: Sei $p \in K[X]$ mit Grad $n + 1$ und a eine beliebige Nullstelle. Nach dem Satz gibt es $q \in K[X]$, sodass

$$p = q \cdot (X - a).$$

Wegen der Gradformel für Produkte von Polynomen über Körpern ist $\text{grad}(q) = n$. Nach Induktionsvoraussetzung hat q höchstens n Nullstellen. Für jede Nullstelle $b \in K \setminus \{a\}$ von p gilt wegen $0 = p(b) = q(b) \cdot (b - a)$ auch $q(b) = 0$, d. h. b ist auch eine Nullstelle von q .

$\Rightarrow p$ hat neben a höchstens n weitere Nullstellen (die von q)

□

Nullstellen bestimmen

- für Polynome $p = a_1X + a_0 \in K[X]$ vom Grad 1 können wir einfach auflösen und dann ist

$$a = -a_0 a_1^{-1}$$

die Nullstelle der Polynomfunktion p

- für (normierte) Polynome vom Grad 2 in $\mathbb{R}[X]$ gibt es die p - q -Formel
- für Polynome vom Grad 3 und 4 in $\mathbb{R}[X]$ gibt es ebenfalls geschlossene Formeln (CARDANO-Formeln), die allerdings recht kompliziert sind
- mithilfe tieferer Methoden der Algebra kann man zeigen, dass es für Polynome vom Grad mindestens 5 in $\mathbb{R}[X]$ keine geschlossene Formel gibt
- es gibt aber numerische Verfahren zur Approximation von Nullstellen für beliebige Polynome aus $\mathbb{R}[X]$
- für Polynome $p \in K[X]$ von beliebigen Grade kann man mithilfe des Satzes, nachdem eine Nullstelle $a \in K$ gefunden wurde, mithilfe der Polynomdivision das Polynom q mit

$$p = q \cdot (X - a)$$

bestimmt werden und dann können die Nullstellen für q gesucht werden

→ hilfreich da $\text{grad}(q) < \text{grad}(p)$

p - q -Formel

Satz

Sei $X^2 + pX + q$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad 2 in $\mathbb{R}[X]$ mit Nullstelle $a \in \mathbb{R}$. Dann gilt $q \leq p^2/4$ und

$$a = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q} \quad \text{oder} \quad a = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}.$$

Bemerkung: p und q sind hier reelle Zahlen und keine Polynome

Beweis: Sei a eine Nullstelle von $X^2 + pX + q$. Dann gilt

$$0 = a^2 + pa + q = a^2 + 2\frac{p}{2}a + \left(\frac{p}{2}\right)^2 - \left(\frac{p}{2}\right)^2 + q.$$

Die ersten drei Terme können wir mit der binomischen Formel zusammenfassen und nach Umstellen erhalten wir

$$\left(a + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q.$$

Da die linke Seite nicht negativ ist, muss $q \leq p^2/4$ gelten und Wurzelziehen und Auflösen nach a ergibt die Behauptung. □

Ganzzahlige Nullstellen

Satz (Lemma von GAUSS)

Sei $p = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0 .

Beweis von $b \in \mathbb{Z}$: Sei $b \in \mathbb{Q} \setminus \{0\}$ eine Nullstelle von p und $b = \frac{y}{z}$ für teilerfremde ganze Zahlen y und z mit $y \neq 0$ and $z \geq 1$. Wir zeigen $z = 1$.

Da $b = y/z$ eine Nullstelle von p ist, gilt

$$0 = p(b) = \left(\frac{y}{z}\right)^n + a_{n-1} \cdot \left(\frac{y}{z}\right)^{n-1} + \dots + a_1 \cdot \left(\frac{y}{z}\right) + a_0. \quad (*)$$

Wir multiplizieren die Gleichung mit z^n , stellen nach y^n um und erhalten

$$y^n = z \cdot \left(-a_{n-1}y^{n-1} - \dots - a_1yz^{n-2} - a_0z^{n-1} \right).$$

Da alle Koeffizienten a_{n-1}, \dots, a_0 sowie y und z ganzzahlig sind, ist die rechte Seite ein ganzzahliges Vielfaches von z . Somit muss y^n ein ganzzahliges Vielfaches von z sein. Da $y \neq 0$ und $z \geq 1$ teilerfremd sind, kann z nur 1 sein. Insbesondere ist $b = y$ also ganzzahlig.

Lemma von GAUSS – Beweis von $b \mid a_0$

Satz (Lemma von GAUSS)

Sei $p = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{R}[X]$ ein normiertes (d. h. Leitkoeffizient ist 1) Polynom vom Grad $n > 0$ mit ganzzahligen Koeffizienten. Dann ist jede Nullstelle $b \in \mathbb{Q}$ von p ein ganzzahliger (es gilt also sogar $b \in \mathbb{Z}$) Teiler von a_0 .

Beweis von $b \mid a_0$: Es ist zu zeigen, dass $b = y$ ein ganzzahliger Teiler von a_0 ist. Ausgangspunkt ist wieder (*). Da wir aber bereits wissen, dass $z = 1$ ist und somit $b = y \neq 0$ ist, erhalten wir nun

$$0 = b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0.$$

Diesmal stellen wir nach a_0 um und Klammern b aus. Somit gilt

$$a_0 = b(-b^{n-1} - a_{n-1}b^{n-2} - \dots - a_2b - a_1).$$

Nun folgt aus der Ganzzahligkeit von $b = y$ und a_{n-1}, \dots, a_1 , dass die rechte Seite ein ganzzahliges Vielfaches von b ist.

Da $a_0 \in \mathbb{Z}$ folgt somit auch, dass a_0 ein ganzzahliges Vielfaches von b ist. □

Beispiel 1

Gesucht sind die Nullstellen von $p = X^3 - 6X^2 + 11X - 6 \in \mathbb{R}[X]$. Falls es ganzzahlige Nullstellen b gibt, so sind dies nach dem Lemma von GAUSS ganzzahlige Teiler des konstanten Terms -6 , d. h.

$$b \in \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Wir probieren die 1 und erhalten $p(1) = 1 - 6 + 11 - 6 = 0$.

Polynomdivision p durch $X - 1$ liefert

$$\begin{array}{r} X^3 - 6X^2 + 11X - 6 = (X - 1)(X^2 - 5X + 6) \\ - X^3 + X^2 \\ \hline - 5X^2 + 11X \\ 5X^2 - 5X \\ \hline 6X - 6 \\ - 6X + 6 \\ \hline 0 \end{array}$$

Die Nullstellen von $X^2 - 5X + 6$ bestimmen wir mit der p - q -Formel und erhalten

$$\frac{5}{2} \pm \sqrt{\frac{25}{4} - 6} = \frac{5}{2} \pm \sqrt{\frac{1}{4}} = \frac{5}{2} \pm \frac{1}{2} \implies \text{Nullstellen 2 und 3.}$$

Beispiel 2 und Linearfaktoren

- Gesucht sind die Nullstellen von $q = X^4 - X^3 - 7X^2 + 5X + 10 \in \mathbb{R}[X]$
 - GAUSS: Probieren von $\{\pm 1, \pm 2, \pm 5, \pm 10\}$ ergibt Nullstellen -1 und 2
 - $(X + 1)(X - 2) = X^2 - X - 2$ und Polynomdivision führt zu
$$(X^4 - X^3 - 7X^2 + 5X + 10) : (X^2 - X - 2) = X^2 - 5$$
 - Lemma von GAUSS ergibt keine Nullstellen von $X^2 - 5$ bei ± 1 oder ± 5
 - aber p - q -Formel (bzw. 3. binom. Formel) ergeben Nullstellen $\sqrt{5}$ und $-\sqrt{5}$
- $\Rightarrow q = X^4 - X^3 - 7X^2 + 5X + 10 = (X + 1)(X - 2)(X - \sqrt{5})(X + \sqrt{5})$
- die Polynome vom Grad 1 auf der rechten Seite nennt man **Linearfaktoren**
 - q zerfällt über \mathbb{R} in **Linearfaktoren**, da q das Produkt dieser ist

Bsp.: $p = (X - 1)(X^2 + 1) = X^3 - X^2 + X - 1$ (nicht jedes Polynom zerfällt über \mathbb{R})

Für alle $x \in \mathbb{R}$ ist $(x^2 + 1) \geq 1$ und damit hat p nur eine reelle Nullstellen bei 1 und ist kein Produkt von Linearfaktoren über \mathbb{R} .

Bemerkung (jedes Polynom zerfällt über \mathbb{C})

Über \mathbb{C} zerfällt jedes nichtkonstante Polynom in Linearfaktoren und dies besagt der **Fundamentalsatz der Algebra** den wir hier nicht beweisen.

Bsp.: $X^2 + 1 = (X + i)(X - i)$ und $p = X^3 - X^2 + X - 1 = (X - 1)(X + i)(X - i)$ in \mathbb{C}

9. Vektoren und Matrizen

Vektorräume

Definition (Vektoren)

Für einen Körper K und $n \in \mathbb{N}$ ist K^n die Menge aller n -Tupel mit Einträgen aus K , die wir **Vektoren** nennen.

- Wir definieren die **Vektoraddition** $+: K^n \times K^n \longrightarrow K^n$ komponentenweise, d. h.

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

für alle $(a_1, \dots, a_n), (b_1, \dots, b_n) \in K^n$.

- Wir definieren eine **Multiplikation** $\cdot: K \times K^n$ von Körperelementen mit Vektoren durch

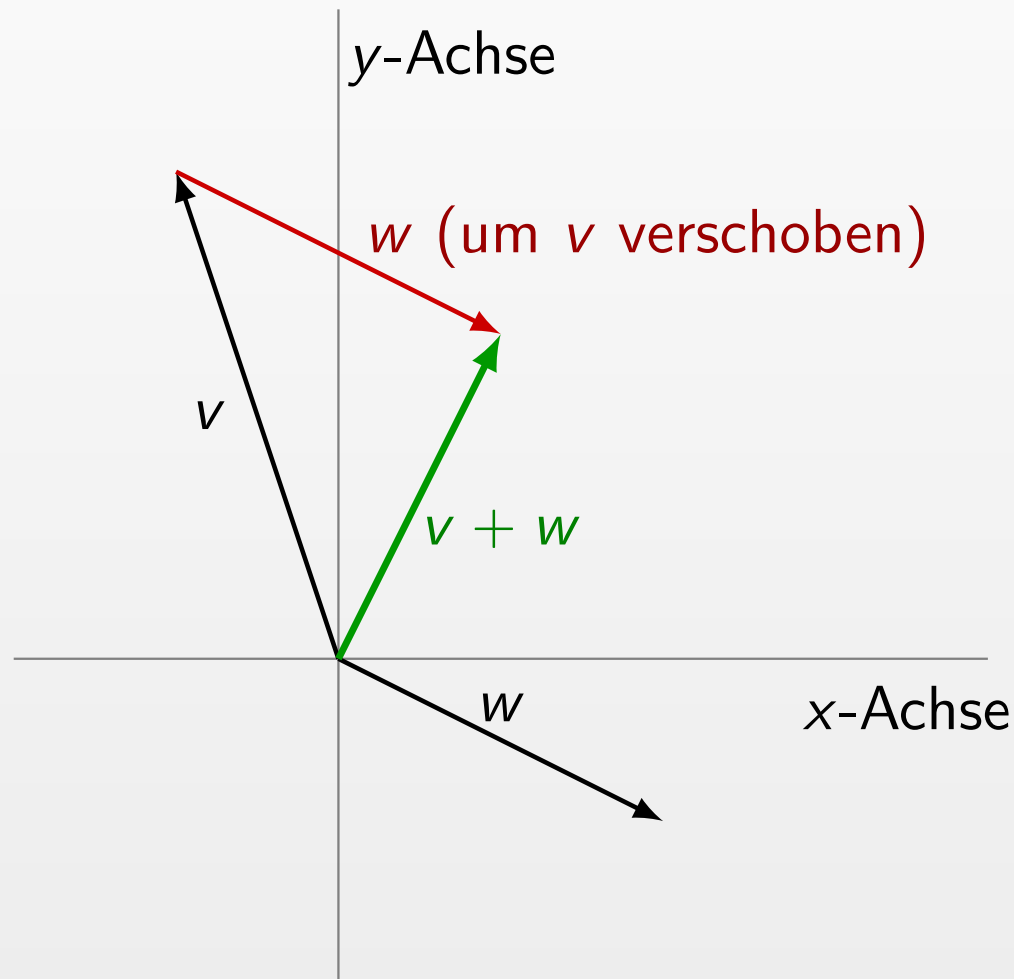
$$\alpha \cdot (a_1, \dots, a_n) = (\alpha a_1, \dots, \alpha a_n),$$

für alle **Skalare** $\alpha \in K$ und $(a_1, \dots, a_n) \in K^n$.

Beispiel: \mathbb{R}^2 bzw. allgemeiner \mathbb{R}^n

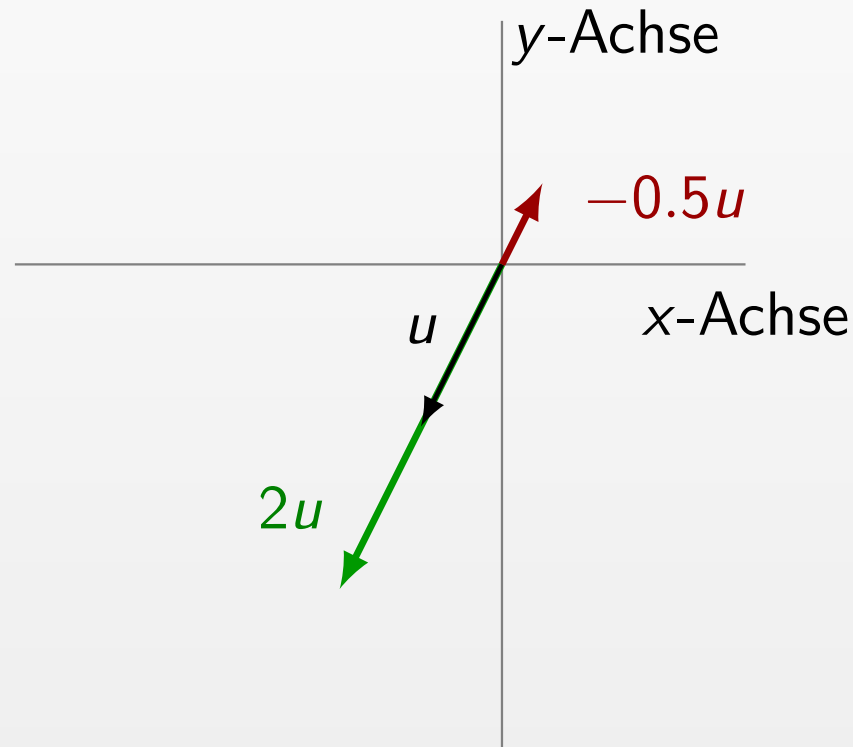
Reelle Zahlenebene - Addition

- interpretiere Vektoren in \mathbb{R}^2 als Punkte oder „Pfeile“ vom Nullpunkt $(0, 0)$ zum Punkt in der Ebene vor
- ⇒ Vektoraddition entspricht „Aneinanderreihung“ der Pfeile



Reelle Zahlenebene - Multiplikation mit Skalar

- Multiplikation mit α entspricht **Streckung** ($|\alpha| > 1$) bzw. **Stauchung** ($|\alpha| < 1$) um α , wobei ein negatives Vorzeichen zusätzlich die Richtung „umkehrt“



Vektorräume

Satz

Für jeden Körper K und $n \in \mathbb{N}$ gilt:

- 1 $(K^n, +)$ ist eine abelsche Gruppe mit dem **Nullpunkt** $(0, \dots, 0)$ als neutralem Element
- 2 für alle $v, w \in K^n$ und alle $\alpha, \beta \in K$ gilt:
 - $\alpha(v + w) = \alpha v + \alpha w$ und $(\alpha + \beta)v = \alpha v + \beta v$
 - $(\alpha \cdot \beta)v = \alpha(\beta v)$ und $1 \cdot v = v$

Beweis: Definitionen einsetzen und nachrechnen □

Bemerkung

- Strukturen mit den obigen Eigenschaften heißen Vektorräume und sind die zentralen Untersuchungsgegenstände der **Linearen Algebra**.
- Im Allgemeinen ist ein **K -Vektorraum V** gegeben durch eine abelsche Gruppe $(V, +)$ und eine Multiplikation $\cdot : K \times V \longrightarrow V$, so dass die obigen Rechenregeln gelten.
- Insbesondere muss V erstmal nichts mit K zu tun haben, solange die Multiplikation mit Skalaren entsprechend der Rechenregeln 2 definiert ist.

Untervektorraum

Betrachte den \mathbb{R} -Vektorraum \mathbb{R}^2 , $u \in \mathbb{R}^2 \setminus \{(0, 0)\}$ fest gewählt und

$$U = \{\alpha u : \alpha \in \mathbb{R}\}.$$

1 $(U, +)$ ist eine Untergruppe von $(\mathbb{R}^2, +)$

Beweis: Untergruppenkriterium

$$v = \alpha u \in U, w = \beta u \in U \implies v - w = (\alpha - \beta)u \in U \quad \square$$

2 Multiplikation eingeschränkt auf $\mathbb{R} \times U$ ist wohldefiniert auf U

$$\text{Beweis: } v = \alpha u \in U \text{ und } \beta \in \mathbb{R} \implies \beta v = (\beta\alpha)u \in U \quad \square$$

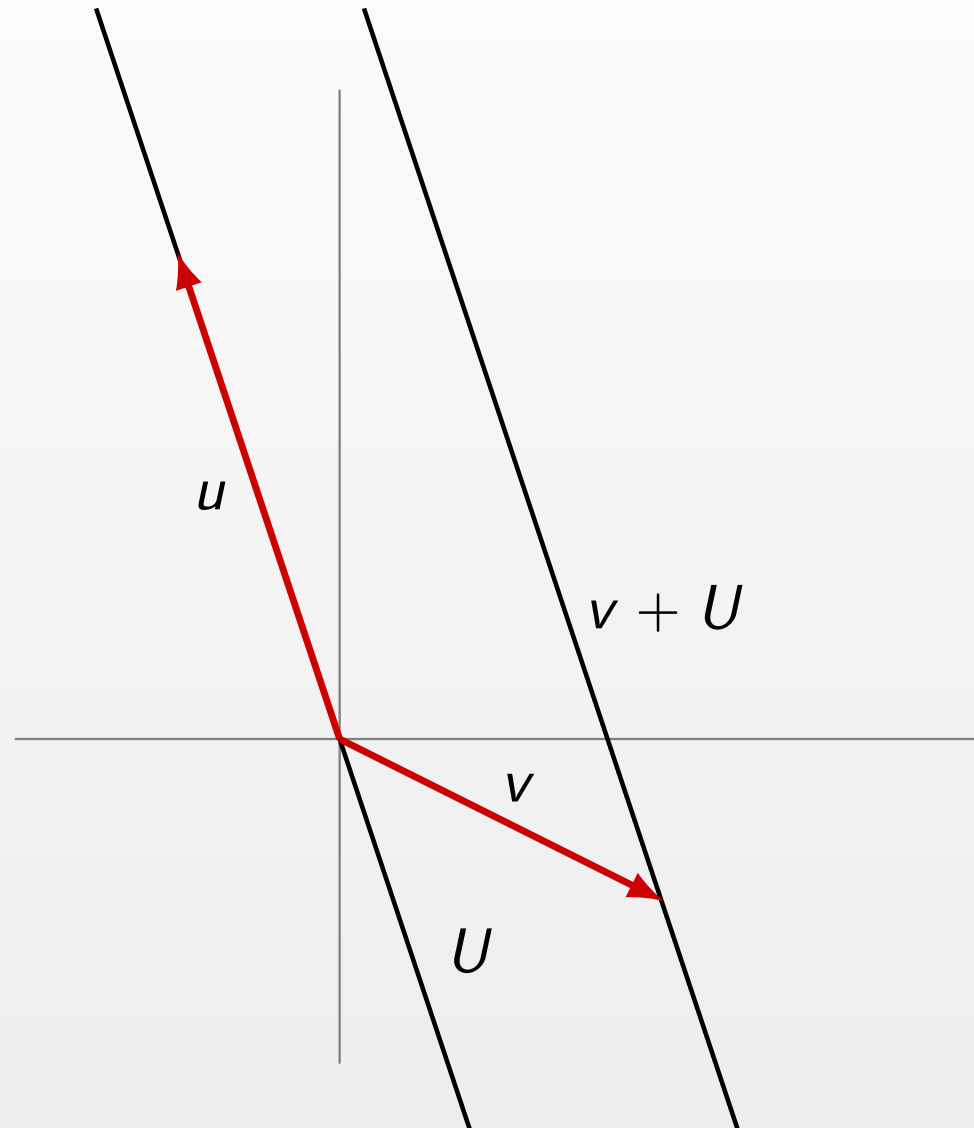
$\implies U$ ist ein **Untervektorraum** von \mathbb{R}^2

Geometrische Interpretation:

- U ist die Gerade durch den Nullpunkt die u enthält
- die Nebenklassen der Untergruppe U von \mathbb{R}^2 sind die Parallelen der Gerade U

Beispiel

Sei $u = (-1, 3)$ und $v = (2, -1)$ und $U = \{\alpha u : \alpha \in \mathbb{R}\}$.



Skalarprodukt

Definition

Für Vektoren $v = (a_1, \dots, a_n)$, $w = (b_1, \dots, b_n) \in K^n$ definieren wir das **(Standard)Skalarprodukt**

$$\langle v, w \rangle = \begin{cases} a_1 b_1 + \dots + a_n b_n = \sum_{i=1}^n a_i b_i, & \text{falls } K \neq \mathbb{C}, \\ a_1 \bar{b}_1 + \dots + a_n \bar{b}_n = \sum_{i=1}^n a_i \bar{b}_i, & \text{falls } K = \mathbb{C}, \end{cases}$$

d. h. wir definieren die Abbildung $\langle \cdot, \cdot \rangle: K^n \times K^n \longrightarrow K$.

ACHTUNG

Skalarprodukt bildet zwei Vektoren v, w auf ein Skalar in K ab

$$K^n \times K^n \longrightarrow K.$$

Wohingegen die Multiplikation mit einem Skalar ein Skalar aus K und einen Vektor v auf einen Vektor abbildet

$$K \times K^n \longrightarrow K^n.$$

Beispiele

- $v = (1, 2, 3), w = (-1, 2, 1) \in \mathbb{R}^3 \implies \langle v, w \rangle = -1 + 4 + 3 = 6$
- $v = (1, 2, 3, 4), w = (3, 4, 2, 1) \in \mathbb{F}_5^4$
 $\implies \langle v, w \rangle \equiv 3 + 8 + 6 + 4 \pmod{5} = 1$
- $v = (1 + 2i, i), w = (-1, 5 - 3i) \in \mathbb{C}^2$
 $\implies \langle v, w \rangle = (1 + 2i)(\overline{-1}) + i(\overline{5 - 3i}) = (-1 - 2i) + (-3 + 5i) = -4 + 3i$

Definition (Betrag/EUKLID'sche Norm)

Für $K = \mathbb{R}$ oder \mathbb{C} definieren wir den **Betrag** $|\cdot|$ auf K^n durch

$$|v| = \sqrt{\langle v, v \rangle}$$

für $v \in K^n$.

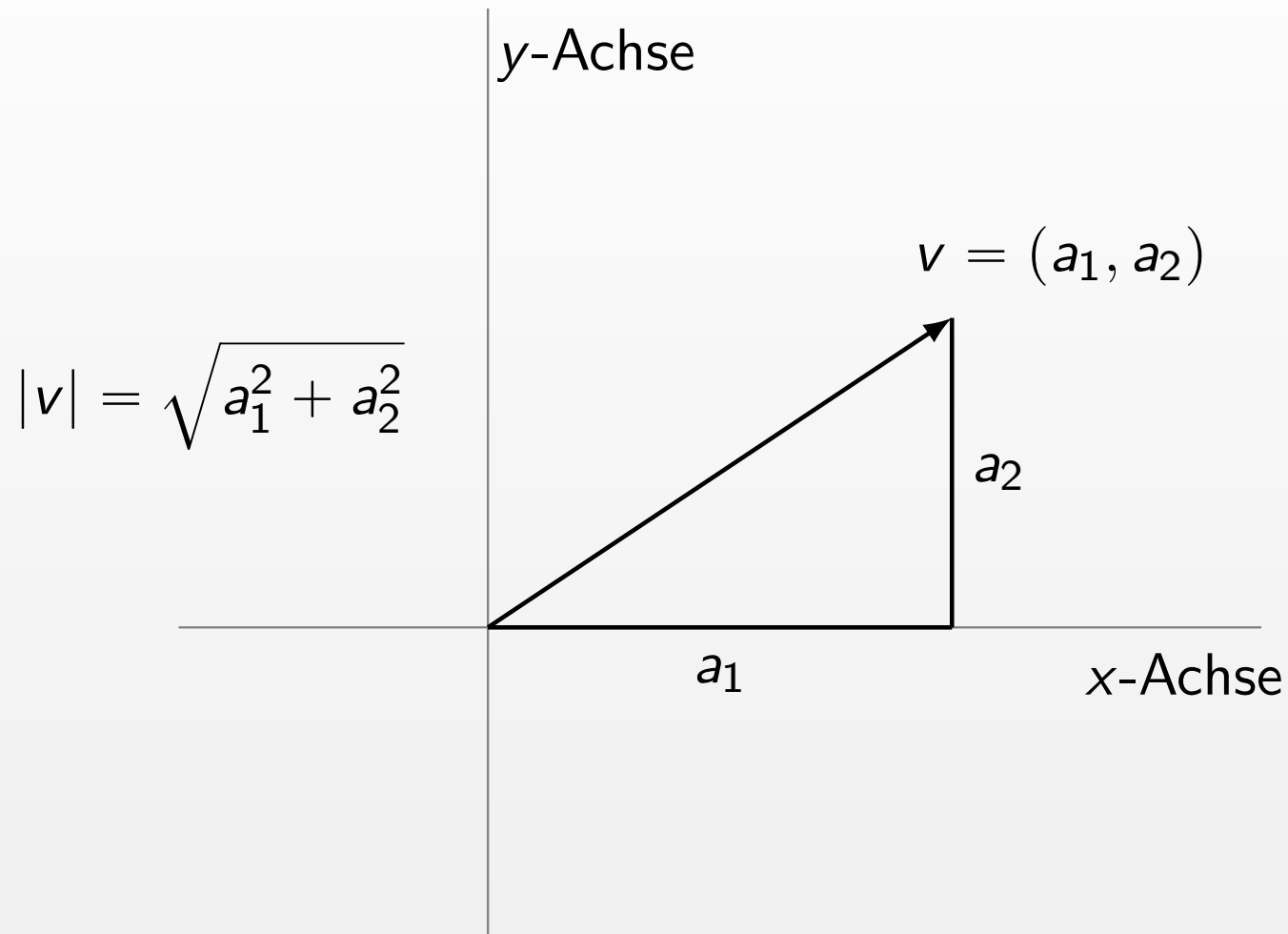
Bemerkungen

- Für $v \in \mathbb{C}^n$ ist $\langle v, v \rangle$ eine Summe nicht-negativer reeller Zahlen, da

$$(a + bi)(\overline{a + bi}) = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{R}_{\geq 0}.$$

- Wegen dem Satz des PYTHAGORAS entspricht der Betrag $|v|$ für $v = (a_1, a_2) \in \mathbb{R}^2$ dem Abstand $\sqrt{a_1^2 + a_2^2}$ des Punktes v vom Nullpunkt und in höheren Dimensionen gilt das Entsprechende.

EUKLID'scher Abstand



Eigenschaften des Skalarproduktes

Satz

Sei K ein Körper und $n \in \mathbb{N}$. Dann gilt für alle $\alpha \in K$ und alle $u, v, w \in K^n$

1 $\langle v, w \rangle = \langle w, v \rangle$ für $K \neq \mathbb{C}$ und $\langle v, w \rangle = \overline{\langle w, v \rangle}$ für $K = \mathbb{C}$

2 $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$

3 $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$

Beweis: Alle Eigenschaften ergeben sich direkt aus der Definition des Skalarproduktes und den Rechenregeln

$$z \cdot \bar{z}' = \overline{\bar{z} \cdot z'} = \overline{z' \cdot \bar{z}}$$

für komplexe Zahlen $z, z' \in \mathbb{C}$. □

Bemerkungen

- Eigenschaft ?? nennt man **Symmetrie** bzw. **Hermitizität** (in \mathbb{C})
- Eigenschaften ?? und ?? nennt man **Linearität im ersten Argument**
- mit ?? ergibt sich auch **Linearität im zweiten Argument** für $K \neq \mathbb{C}$ und **Sesquilinearität** $\langle u, \alpha v + w \rangle = \bar{\alpha} \langle u, v \rangle + \langle u, w \rangle$ über \mathbb{C}

Eigenschaften des Betrages

Satz

Sei $K = \mathbb{R}$ oder \mathbb{C} und $n \in \mathbb{N}$. Dann gilt für alle $\lambda \in K$ und alle $v, w \in K^n$

1 $|v| \in \mathbb{R}_{\geq 0}$ und es gilt $|v| = 0 \iff v = (0, \dots, 0)$ positiv definit

2 $|\lambda v| = |\lambda| \cdot |v|$ homogen

3 $|v + w| \leq |v| + |w|$ Dreiecksungleichung

Beweis: Die ersten beiden Eigenschaften ergeben sich aus der Definition des Betrages, den Rechenregeln des Skalarproduktes und aus der Definition des Betrages für komplexe Zahlen $\lambda = a + bi$

$$|\lambda| = \sqrt{a^2 + b^2} = \sqrt{(a + bi)(a - bi)} = \sqrt{\lambda \cdot \bar{\lambda}}$$

mit

$$|\lambda v| = \sqrt{\langle \lambda v, \lambda v \rangle} = \sqrt{(\lambda \cdot \bar{\lambda}) \langle v, v \rangle} = \sqrt{\lambda \cdot \bar{\lambda}} \cdot \sqrt{\langle v, v \rangle} = |\lambda| \cdot |v|.$$

Der Beweis der Dreiecksungleichung basiert auf der CAUCHY-SCHWARZ-Ungleichung und wird später nachgeholt. □

Matrizen

Definition (Matrix)

Seien $m, n \in \mathbb{N}$ und sei K ein Körper. Eine $(m \times n)$ -Matrix \mathbf{A} über K ist ein rechteckiges Zahlenschema mit m Zeilen und n Spalten der Form

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

wobei die Einträge a_{ij} Elemente von K sind und wir bezeichnen die Menge dieser $(m \times n)$ -Matrizen mit $K^{m \times n}$.

Schreibweisen:

- Wir schreiben auch $\mathbf{A} = (a_{ij})_{i \in [m], j \in [n]}$ oder einfach nur $\mathbf{A} = (a_{ij})$, wenn die Dimension $m \times n$ der Matrix \mathbf{A} klar oder irrelevant ist.
- Wir nennen (a_{i1}, \dots, a_{in}) die i -te Zeile bzw. den i -ten Zeilenvektor von \mathbf{A} .
- Analog ist $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ die j -te Spalte bzw. der j -te Spaltenvektor von \mathbf{A} .

Matrizen als Vektorraum

- Für zwei $(m \times n)$ -Matrizen $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij}) \in K^{m \times n}$ definieren wir die Matrizenaddition

$$\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij}) \in K^{m \times n}$$

- Die $(m \times n)$ -Matrix, deren Einträge alle 0 sind, heisst **Nullmatrix**.
- $\Rightarrow (K^{m \times n}, +)$ ist eine abelsche Gruppe mit der Nullmatrix als neutralem Element und inversen Elementen $-\mathbf{A} = (-a_{ij})$

- Wir definieren eine Multiplikation mit einem Skalar
 $\cdot: K \times K^{m \times n} \longrightarrow K^{m \times n}$ für $\alpha \in K$ und $\mathbf{A} = (a_{ij}) \in K^{m \times n}$ durch

$$\alpha \mathbf{A} = (\alpha a_{ij}) \in K^{m \times n}$$

$\Rightarrow K^{m \times n}$ ist ein K -Vektorraum

Bemerkung: Der K -Vektorraum $K^{m \times n}$ ist in kanonischer Weise isomorph zum K -Vektorraum K^N für $N = m \cdot n$ aus den letzten Vorlesungen.

Matrizenmultiplikation

Definition (Matrix)

Seien $\ell, m, n \in \mathbb{N}$ und sei K ein Körper. Wir definieren die **Matrizenmultiplikation**

$$\cdot: K^{\ell \times m} \times K^{m \times n} \longrightarrow K^{\ell \times n}$$

für zwei Matrizen $\mathbf{A} \in K^{\ell \times m}$ und $\mathbf{B} \in K^{m \times n}$ durch

$$\mathbf{AB} = \mathbf{C} = (c_{ik})_{i \in [\ell], k \in [n]}$$

für

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk} = \sum_{j=1}^m a_{ij}b_{jk}.$$

Bemerkungen:

- erster Matrixfaktor **muss** genauso viele Spalten haben, wie der zweite Zeilen
- Eintrag c_{ik} im Produkt ergibt sich aus dem „Produkt“ der i -ten Zeile des ersten Matrixfaktors und der k -ten Spalte des zweiten Faktors, ähnlich dem Skalarprodukt über \mathbb{R} (beide Vektoren haben die gleiche Länge m)

Spezialfall: Multiplikation von Matrizen und Vektoren

- Multiplikation einer Matrix \mathbf{A} mit dem passenden Spaltenvektor der nur Einsen enthält (von rechts), ergibt die Summe der Spaltenvektoren von \mathbf{A}

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 9 \end{pmatrix} + \begin{pmatrix} 2 \\ 6 \\ 10 \end{pmatrix} + \begin{pmatrix} 3 \\ 7 \\ 11 \end{pmatrix} + \begin{pmatrix} 4 \\ 8 \\ 12 \end{pmatrix} = \begin{pmatrix} 10 \\ 26 \\ 42 \end{pmatrix}$$

- allgemeiner ist das Produkt einer Matrix \mathbf{A} mit einem passenden Spaltenvektor v (von rechts) eine gewichtete Summe der Spalten von \mathbf{A} , wobei die i -te Spalte von \mathbf{A} mit dem i -ten Eintrag von v gewichtet wird

$$\begin{pmatrix} 10 & 11 & 12 \\ 13 & 14 & 15 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = 2 \cdot \begin{pmatrix} 10 \\ 13 \end{pmatrix} + 3 \cdot \begin{pmatrix} 11 \\ 14 \end{pmatrix} + 4 \cdot \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 101 \\ 128 \end{pmatrix}$$

- analog entspricht das Produkt eines Zeilenvektors (von links) mit einer passenden Matrix der entsprechend gewichteten Summe der Zeilenvektoren

$$(4 \quad 2 \quad 3) \begin{pmatrix} 10 & 11 \\ 12 & 13 \\ 14 & 15 \end{pmatrix} = 4 (10 \quad 11) + 2 (12 \quad 13) + 3 (14 \quad 15) = (106 \quad 115)$$

Matrizenmultiplikation ist assoziativ

Satz

Für alle Matrizen $\mathbf{A} \in K^{k \times \ell}$, $\mathbf{B} \in K^{\ell \times m}$ und $\mathbf{C} \in K^{m \times n}$ gilt

$$(\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}).$$

Beweis: Man sieht leicht ein, dass beide Produkte eine $(k \times n)$ -Matrix ergeben. Für $i \in [k]$ und $j \in [n]$ seien d_{ij} und d'_{ij} die entsprechend indizierten Einträge in den Produktmatrizen der behaupteten Identität. Wir werden zeigen $d_{ij} = d'_{ij}$.

Sei \mathbf{A}_i die i -te Zeile von \mathbf{A} und \mathbf{C}^j die j -te Spalte von \mathbf{C} . Dann folgt

$$(d_{ij}) = (\mathbf{A}_i \cdot \mathbf{B}) \cdot \mathbf{C}^j \quad \text{und} \quad (d'_{ij}) = \mathbf{A}_i \cdot (\mathbf{B} \cdot \mathbf{C}^j)$$

(Formal ergeben die beiden Matrix-Vektoren-Produkte jeweils eine (1×1) -Matrix und deswegen sind d_{ij} und d'_{ij} hier geklammert.)

Die Überlegungen der letzten Folie ergeben, dass d_{ij} und d'_{ij} die gewichtete Summe aller Einträge der Matrix \mathbf{B} sind, wobei b_{st} mit dem Produkt des s -ten Eintrags des Zeilenvektors \mathbf{A}_i und dem t -ten Eintrag des Spaltenvektors \mathbf{C}^j gewichtet wird. D. h.

$$d_{ij} = \sum_{s=1}^{\ell} \sum_{t=1}^m (a_{is} c_{tj}) \cdot b_{st} = d'_{ij} . \quad \square$$

Matrizenmultiplikation ist nicht kommutativ

- beide Produkte \mathbf{AB} und \mathbf{BA} sind nur definiert, wenn für ℓ und $m \in \mathbb{N}$:

$$\mathbf{A} \in K^{\ell \times m} \quad \text{und} \quad \mathbf{B} \in K^{m \times \ell}$$

- in dem Fall ist \mathbf{AB} eine $(\ell \times \ell)$ -Matrix und \mathbf{BA} ist eine $(m \times m)$ -Matrix
- beliebige Produkte sind also nur für **quadratische** Matrizen möglich, d. h. für Matrizen aus $K^{n \times n}$ für festes $n \in \mathbb{N}$
- auch mit dieser Einschränkung ist die Matrizenmultiplikation für $n \geq 2$ im Allgemeinen nicht kommutativ

Beispiel:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \neq \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

Ring der Matrizen

- die Beobachtungen über Matrizen ergeben den folgenden Satz

Satz

Für jede natürliche Zahl $n \in \mathbb{N}$ und Körper K ist $(K^{n \times n}, +, \cdot)$ ein Ring mit Eins, wobei die **Einheitsmatrix**

$$E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in K^{n \times n}$$

mit Einsen auf der Diagonalen und sonst nur Nullen, das neutrale Element bezüglich der Multiplikation ist. □

Bemerkungen:

- für $n = 1$ ist $K^{1 \times 1}$ offensichtlich isomorph zum Körper K
- für $n \geq 2$ ist der Ring $K^{n \times n}$ nicht kommutativ und kein Körper
- Einheiten in $K^{n \times n}$ heissen **invertierbare Matrizen** → Mafl 2