Course Notes

Diskrete Mathematik
(Discrete Mathematics)

Daniel Smertnig

Winter Term 2021/22
University of Graz

for Bachelor students, 2h/week

made available online: 17.5.2026

Diskrete Mathematik
VO, 2 SSt, WS 2021/22

0. GRUNDLAGEN

0.1 LOGIK

Eine (mathematische bzw. logische) **Aussage** ist eine Formulierung mit eindeutigem Wahrheitswert (wahr / falsch).

zB: „$2 < 6$" (w) „$3 < 1$" (f.), „$\frac{1}{2}$ ist eine ganze Zahl" (f.)
„$3 + 11 = 14$" (w.)

KEINE Aussagen: „Was ist eine Primzahl?", „$4 + 12$"
„Diese Aussage ist falsch", „Das Wetter ist schön"

Bsp: „Jede gerade Zahl $n > 2$ ist Summe von zwei Primzahlen" (Goldbachsche Vermutung): ist Aussage, aber w/f unbekannt.

Eine **Aussageform** (Prädikat) enthält ein oder mehrere Variablen. Durch Einsetzen konkreter Werte entsteht eine Aussage.

zB $A(x) := \boxed{5 \leq x}$ $A(7)$ w.A, $A(3)$ f.A.

$B(x,y) := \boxed{x < y}$

$C(n) := \boxed{\text{„}n \text{ ist eine Primzahl"}}$

Aus ein oder mehreren Aussagen [Aussageformen] wird mittels logischer Verknüpfungen eine neue Aussage [Aussageform] gebildet. Seien A, B Aussagen

- „nicht A", $\neg A$, ist genau dann wahr, wenn A falsch ist (Negation)

A	$\neg A$
f	w
w	f

- „$\mathcal{A}$ und $\mathcal{B}$", $\mathcal{A} \wedge \mathcal{B}$, ist genau dann wahr, wenn $\mathcal{A}$ und $\mathcal{B}$ beide wahr sind (Konjunktion)
- „$\mathcal{A}$ oder $\mathcal{B}$", $\mathcal{A} \vee \mathcal{B}$, ist genau dann wahr, wenn zumindest eines von $\mathcal{A}$ und $\mathcal{B}$ wahr ist (Disjunktion)

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$
f	f	f	f	w	w
f	w	f	w	w	f
w	f	f	w	f	f
w	w	w	w	w	w

- „$\mathcal{A}$ impliziert $\mathcal{B}$", „aus $\mathcal{A}$ folgt $\mathcal{B}$", „$\mathcal{B}$ ist notwendig für $\mathcal{A}$", „$\mathcal{A}$ ist hinreichend für $\mathcal{B}$", $\mathcal{A} \Rightarrow \mathcal{B}$ ist nur dann falsch, wenn $\mathcal{B}$ falsch aber $\mathcal{A}$ wahr ist (Implikation)
- „$\mathcal{A}$ ist äquivalent zu $\mathcal{B}$", „$\mathcal{A}$ genau dann, wenn $\mathcal{B}$", $\mathcal{A} \Leftrightarrow \mathcal{B}$ ist genau dann wahr, wenn $\mathcal{A}$ und $\mathcal{B}$ denselben Wahrheitswert haben. (Äquivalenz)

Bsp:

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	$\neg\mathcal{A}$	$\neg\mathcal{A} \vee \mathcal{B}$	$(\mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow (\neg\mathcal{A} \vee \mathcal{B})$
f	f	w	w	w	w
f	w	w	w	w	w
w	f	f	f	f	w
w	w	w	f	w	w

→ Tautologie

ausgelassen

Quantoren: Sei $\mathcal{A}(x)$ eine Aussageform

$\forall x: \mathcal{A}(x)$ $\Leftrightarrow$ Für alle x gilt $\mathcal{A}(x)$

$\exists x: \mathcal{A}(x)$ $\Leftrightarrow$ Es existiert (zumindest) ein x, für das $\mathcal{A}(x)$ gilt.

z.B: $\exists x: x<2$ w.A. $\exists x \in \mathbb{R}: x<2$

$(\Leftrightarrow \exists x: x \in \mathbb{R} \wedge x<2)$

$\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}: x<y$ F.A.

$\exists x \in \mathbb{R}\ \forall y \in \mathbb{R}: x<y$ F.A.

$\forall y \in \mathbb{R}\ \exists x \in \mathbb{R}: x<y$ w.A.

Reihenfolge verändert Bedeutung!

Negation: $[\neg \forall x: \mathcal{A}(x)] \Leftrightarrow \exists x: \neg \mathcal{A}(x)$

$[\neg \exists x: \mathcal{A}(x)] \Leftrightarrow \forall x: \neg \mathcal{A}(x)$

0.2 MENGEN

Eine Menge ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen. Von jedem Objekt muss eindeutig feststehen, ob es zur Menge gehört oder nicht. Die zur Menge gehörenden Objekte nennt man die Elemente der Menge. (Georg CANTOR, 1845-1918)

Bsp: $\{1,3,5,7,9\}$, $\mathbb{N} = \{1,2,3,\dots\}$ natürliche Zahlen,

$\mathbb{N}_0 = \{0,1,2,3,\dots\}$, $\{n \in \mathbb{N}: \underbrace{n \text{ ungerade}}_{\text{Aussageform}}\} = \{1,3,5,7,\dots\}$

Ist M eine Menge, so schreiben wir $x \in M$ falls x ein Element von M ist, und $x \notin M$ sonst. N ist eine Teilmenge von M, $N \subseteq M$, wenn jedes Element von N auch Element von M ist (d.h. $\forall x: x \in N \Rightarrow x \in M$ bzw. $\forall x \in N: x \in M$)

Zwei Mengen M, N sind gleich, $M = N$, wenn $N \subseteq M$ und $M \subseteq N$.

z.B. $\{1, 2, 3\} = \{3, 2, 1\} = \{3, 2, 1, 1\}$

Die leere Menge $\emptyset$ ist die Menge, die kein Element enthält. (d.h.: $\forall x: x \notin \emptyset$). Es gilt $\emptyset \subseteq M$ für jede Menge M.

Bsp: $\emptyset \neq \{\emptyset\}$, denn $\emptyset \in \{\emptyset\}$.

Die Anzahl der Elemente einer Menge M heißt Kardinalität von M, $|M|$. Wir nennen M endlich wenn $|M| \in \mathbb{N}_0$, und ansonsten unendlich ($|M| = \infty$).

Für Mengen M, N ist

- die Vereinigung $M \cup N = \{x: x \in M \vee x \in N\}$
- die Schnittmenge $M \cap N = \{x: x \in M \wedge x \in N\}$
- die Differenz $M \setminus N = \{x: x \in M \wedge x \notin N\}$
- die symmetrische Differenz $M \triangle N = (M \setminus N) \cup (N \setminus M)$
- das kartesische Produkt $M \times N = \{(m, n): m \in M, n \in N\}$

Die Mengen M, N sind disjunkt, wenn $M \cap N = \emptyset$.

Die Potenzmenge $\mathcal{P}(M)$ von M ist die Menge aller Teilmengen von M, d.h. $\mathcal{P}(M) = \{N: N \subseteq M\}$.

Bsp: $M = \{1, 2, 3\}$

$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}\}$

$\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

Bemerkung: Die naive Mengenlehre ist in sich widersprüchlich

Russell 1902: $M = \{X: X \notin X\}$

Fall 1: $M \in M \Rightarrow M \notin M$ ↯

Fall 2: $M \notin M \Rightarrow M \in M$ ↯

Reparatur durch eine streng axiomatische Mengenlehre
(Zermelo und Fraenkel, Anfang des 20. Jhdts)
→ Grundlagen VO

Wir treffen solche Probleme nicht an, und verwenden den naiven Mengenbegriff intuitiv.

0.3 BEWEISE.

Ein Beispiel:

Satz 0.1 Sei n eine ungerade natürliche Zahl. Dann ist auch n^2 ungerade.

Beweis: Da n ungerade ist, gibt es ein $m \in \mathbb{N}_0$, sodass $n = 2m+1$.
Dann ist

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2\underbrace{(2m^2+2m)}_{=:k \in \mathbb{N}_0} + 1.$$

Also ist $n^2 = 2k+1$ mit $k \in \mathbb{N}_0$, also n^2 ungerade. □

Typischer Aufbau eines mathematischen **Satzes** (bzw. **Lemma** = Hilfssatz, **Korollar** = Folgerung, **Proposition**):

(I) Vereinbarung der verwendeten Begriffe, Bezeichnungen, Objekte.

(II) **Voraussetzung**: Aussage (Form) p, die für die verwendeten Objekte wahr sein soll.

(III) **Behauptung** Aussage q, deren Wahrheit bewiesen werden soll.

Beweismethoden:

Direkter Beweis: $(p \wedge (p \Rightarrow q)) \Rightarrow q$
(p: w.A. Voraussetzung; $(p \Rightarrow q)$: w. Beweis; q: Ergebnis: w.)

Kettenschluss: $((p \Rightarrow r) \wedge (r \Rightarrow q)) \Rightarrow (p \Rightarrow q)$
($(p \Rightarrow r)$, $(r \Rightarrow q)$: „w. Beweisschritte")

Indirekter Beweis (Kontraposition): $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ [Ü]

Nehme an, dass $\neg q$ gilt, und folgere, dass $\neg p$ gilt

z.B. **Satz 0.2** Sei n eine natürliche Zahl. Wenn n^2 gerade ist, dann ist auch n gerade.

Beweis: Indirekt. Wir müssen also zeigen: Wenn n ungerade ist, dann ist auch n^2 ungerade. Das folgt aber aus obigem Satz! □

Beweis durch Widerspruch $(p \Rightarrow q) \Leftrightarrow \neg(p \wedge \neg q)$ [Ü]

Zeige, dass $\neg q \wedge p$ falsch ist!

Nehme dazu an, dass $\neg q$ und p beide wahr sind und leite einen logischen Widerspruch her. Dann muss $\neg q \wedge p$ falsch sein.

z.B. **Satz 0.3.** $\sqrt{2}$ ist irrational, d.h. $\sqrt{2} \notin \mathbb{Q}$

Beweis: Angenommen $\sqrt{2} \in \mathbb{Q}$. Dann gibt es teilerfremde $p, q \in \mathbb{N}$ mit $\sqrt{2} = \frac{p}{q}$. $\Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow p^2$ ist gerade

$\overset{\text{Satz 0.2}}{\Longrightarrow}$ p ist gerade $\Rightarrow \exists m \in \mathbb{N}: p = 2m \Rightarrow 2q^2 = p^2 = 4m^2$

$\Rightarrow q^2$ ist gerade $\overset{\text{S.0.2}}{\Rightarrow} q$ ist gerade

$\Rightarrow p, q$ gerade $\lightning$ zu p, q teilerfremd. □

Fallunterscheidung: $((r \Rightarrow q) \wedge (\neg r \Rightarrow q)) \Rightarrow q$

Zeige: Ist r wahr, so ist auch q wahr
Ist r falsch, so ist q wahr
$\Rightarrow q$ ist wahr.

(Vollständige) Induktion:

Man möchte zeigen, dass alle natürlichen Zahlen n eine Eigenschaft $A(n)$ besitzen.

Induktionsprinzip: Sei $M = \{n \in \mathbb{N} : A(n)\}$. Gilt

- $1 \in M$ und
- $\forall n \in \mathbb{N}: \; n \in M \Rightarrow n+1 \in M$,

so ist $M = \mathbb{N}$.

Anwendung: Induktionsverankerung: $A(1)$ beweisen
Induktionsschritt: $A(n) \Rightarrow A(n+1)$ beweisen.

Beispiel: Satz 0.4 (Gaußsche Summenformel) Für alle $n \in \mathbb{N}$ gilt:

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

Beweis: $n=1$: $\sum_{j=1}^{1} j = 1 = \frac{1\cdot(1+1)}{2}$ ✓

$n \geq 1$, $n \to n+1$:

$$\sum_{j=1}^{n+1} j = \sum_{j=1}^{n} j + (n+1) \underset{(IV)}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+2)(n+1)}{2}$$

Bem: Stimmt auch für $n=0$, wobei eine leere Summe, z.B. $\sum_{j=1}^{0} j$, nach Def. $=0$ ist. □

Bem: Varianten (äquivalent zum Induktionsprinzip):

(1) Sei $k \in \mathbb{Z}$ und $A(n)$ für $n \geq k$ sinnvoll.
Gilt: $A(k)$ und $\forall n \geq k: A(n) \Rightarrow A(n+1)$,
so gilt: $A(n)$ für alle $n \geq k$.

(2) Es genügt im Induktionsschritt zu zeigen:
Wenn $A(m)$ für alle $m \leq n$ gilt, so folgt $A(n+1)$

0.4 RELATIONEN

Def. Eine Relation zwischen Mengen A und B ist eine Teilmenge $R \subseteq A \times B$. Ist $A = B$, so heißt R Relation auf A. Anstelle $(a,b) \in R$ schreibt man auch aRb.

Bsp: (1) S = Menge der Studierenden
L = Menge aller LVs
$R = \{(s,e) \in S \times L : s \text{ nimmt an } e \text{ teil}\}$

(2) Teilbarkeitsrelation auf $\mathbb{N}$:
$| := \{(m,n) \in \mathbb{N}^2 : \exists k \in \mathbb{N}: n = mk\}$
(m teilt n).

Def Eine Relation R auf A heißt

- reflexiv, wenn $\forall a \in A: (a,a) \in R$
- symmetrisch, wenn $\forall a,b \in A: (a,b) \in R \Rightarrow (b,a) \in R$
- antisymmetrisch, wenn $\forall a,b \in A: (a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$
- transitiv, wenn $\forall a,b,c \in A: (a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$
- (Partial-) Ordnung, wenn R reflexiv, antisymmetrisch und transitiv ist.
- Totalordnung, wenn R eine Ordnung ist und $\forall a,b \in A: (a,b) \in R \vee (b,a) \in R$
- Äquivalenzrelation, wenn R reflexiv, symmetrisch und transitiv ist.

Bsp:
- Teilbarkeit auf $\mathbb{N}$ ist eine Partialordnung,
  $R = \{(a,b) \in \mathbb{N}^2 : a \leq b\}$ ist eine Totalordnung
- Sei M eine Menge. Dann ist
  $\{(A,B) \in \mathcal{P}(M) \times \mathcal{P}(M) : A \subseteq B\}$
  eine Ordnung auf $\mathcal{P}(M)$
- $R = \{(a,b) \in \mathbb{N}^2 : a, b$ sind beide gerade oder beide ungerade$\}$
  ist eine Äquivalenzrelation auf $\mathbb{N}$.

1. KOMBINATORIK (Abzählprobleme)

1.1 Ziehen von Elementen aus Mengen

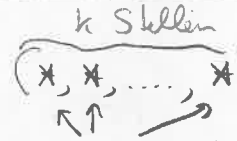
Wieviele Möglichkeiten gibt es, k Elemente aus einer n-elementigen Menge auszuwählen?

Notation: $[n] := \{1, 2, \ldots, n\}$ für $n \in \mathbb{N}_0$ $([0] = \emptyset)$

Bsp. $[3] = \{1,2,3\}$, $k=2$

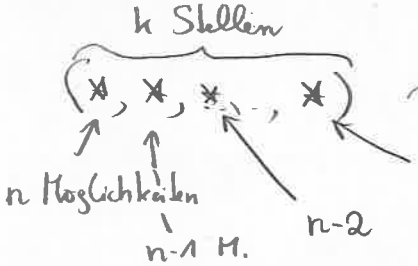
	geordnet (Variationen)	ungeordnet (Kombinationen)	
mit Zurücklegen	(1,1), (1,2), (1,3) (2,1), (2,2), (2,3) (3,1), (3,2), (3,3)	(1,1), (1,2), (1,3) (2,2), (2,3), (3,3)	(geordnete Paare oder Multimengen $\{1,1\}, \ldots$)
ohne Zurücklegen	(1,2), (1,3), (2,1) (2,3), (3,1), (3,2)	$\{1,2\}, \{1,3\}, \{2,3\}$	

(i) Geordnet, mit Zurücklegen



$\rightsquigarrow$ n^k Möglichkeiten $\quad (n^0 := 1$ für $n \in \mathbb{N}_0)$

(ii) Geordnet, ohne Zurücklegen



$\rightsquigarrow$ $n(n-1)\cdot\ldots\cdot(n-k+1) = \prod_{j=0}^{k-1}(n-j)$ Möglichkeiten

Def. (1) Für $n, k \in \mathbb{N}_0$ mit $k \le n$ sei $n^{\underline{k}} = \begin{cases} 1 & \text{falls } k=0 \\ n(n-1)^{\underline{k-1}} & \text{falls } k>0 \end{cases}$ (Rekursive Definition)

die fallende Faktorielle (Fallende Fakultät) von n der Länge k.

(2) Für $n \in \mathbb{N}_0$ sei $n! = \begin{cases} 1 & \text{falls } n=0 \\ n(n-1)! & \text{falls } n>0 \end{cases}$

die Faktorielle (Fakultät) von n.

Bem:
$$n! = n(n-1)\cdots 2\cdot 1 = \prod_{j=1}^{n} j = n^{\underline{n}}$$

$$n^{\underline{k}} = n(n-1)\cdots(n-k+1) = \prod_{j=0}^{k-1}(n-j) = \frac{n!}{(n-k)!}$$

(iii) Ungeordnet, ohne Zurücklegen (k-elementige Teilmengen)

Unterschied zu (ii): Reihenfolge der k (verschiedenen) Elemente spielt keine Rolle.

Wieviele mögliche Reihenfolgen gibt es für k Elemente?
(ii) $\Rightarrow k^{\underline{k}} = k!$ Möglichkeiten

Es gibt $n^{\underline{k}}$ Möglichkeiten k Elemente (o.Z.) geordnet auszuwählen; je $k!$ dieser Möglichkeiten führen auf dieselbe ungeordnete Auswahl

$$\rightsquigarrow \quad \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!(n-k)!} =: \binom{n}{k} \text{ Möglichkeiten}$$

Binomialkoeffizient „n über k"

Für $k>n$: $\binom{n}{k} := 0$.

(iv) Ungeordnet, mit Zurücklegen

Geordnete Typen bzw. Multimengen: Jedes Element kann mit einer Vielfachheit auftreten.

z.B. $M = \{1,1,2,2,2,3\}$. Als Multimenge $M = \{1,2,3\}$, aber

$M = \{2,1,3,2,2,1\}$

Die Kardinalität einer Multimenge ist die Anzahl aller Elemente, gezählt mit ihren jeweiligen Vielfachheit, z.B $|M|=6$.

Gesucht: Anzahl der k-elementigen Multimengen über einer n-elementigen Menge $S = \{a_1, a_2, \ldots, a_n\}$

Jede solche Multimenge lässt sich als Folge von k „Symbolen" "x" und n-1 Symbolen "|" kodieren

z.B $S = \{a,b,c,d,e\}$, $M = \{a,a,a,c,d,d,e\}$ entspricht xxx||x|xx|x

Jede Multimenge entspricht einer eindeutigen Folge von Symbolen und umgekehrt.

Anzahl der Zeichenketten: Aus $n+k-1$ Positionen wählen wir jene k aus, die "*" enthalten.

(iii) $\Longrightarrow$ $\binom{n+k-1}{k}$ Möglichkeiten

1.2 Kombinatorische Beweisprinzipien

Satz 1.1 (Binomische Formel) Für $a,b \in \mathbb{R}$, $n \in \mathbb{N}_0$ gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Beweis I: Induktion nach n (einfach)

Beweis II: Kombinatorisch.

(*) $(a+b)^n = (a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)$ (n Faktoren)

Ausmultiplizieren liefert eine Summe über alle Produkte der "a"s und "b"s der Länge n. Jeder Summand hat die Form $a^k b^{n-k}$ mit $0 \le k \le n$. Ein Produkt $a^k b^{n-k}$ entsteht durch „Ziehen" von k "a"s, es tritt also $\binom{n}{k}$ mal auf. D.h. die rechte Seite von (*) ist

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

□

Satz 1.2 (Summenregel) Sind $A_1, \ldots, A_n$ paarweise disjunkte endliche Mengen, und $A = \bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$, so ist

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

Bem: Für beliebige Mengen gilt $|A| \le \sum_{i=1}^{n} |A_i|$

Bsp: Wie viele Teilmengen $A \subseteq [10]$ mit $|A|=5$ enthalten 1 oder 2, aber nicht beide?

$M_1 := \{ A \subseteq [10] : 1 \in A \wedge 2 \notin A \wedge |A|=5 \}$

$|M_1| = \binom{8}{4}$ (A enthält 1 sowie 4 Elemente aus $[10] \setminus \{1,2\}$)

$M_2 := \{ A \subseteq [10] : 2 \in A \wedge 1 \notin A \wedge |A|=5 \}$

$|M_2| = \binom{8}{4}$ (A enthält 2 sowie 4 Elemente aus $[10] \setminus \{1,2\}$)

$\rightarrow |M_1 \cup M_2| = |M_1| + |M_2| = 2\binom{8}{4} = 2 \cdot \frac{8!}{4!\cdot 4!} = 2 \cdot \frac{\cancel{8}^{2} \cdot 7 \cdot \cancel{6} \cdot 5}{\cancel{4} \cdot 3 \cdot \cancel{2}} = 4 \cdot 35 = \underline{140}$.

Satz 1.3 (Produktregel) Seien $A_1, \dots, A_n$ endliche Mengen und $A = A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) : \forall i \in [n]: a_i \in A_i\}$ das kartesische Produkt. Dann ist $|A| = \prod_{i=1}^{n} |A_i|$

Bsp: Für wieviele 4-stellige Zahlen ist die i-te Ziffer durch i teilbar (für alle i)

1. Ziffer: $\{0, \dots, 9\}$
2. Ziffer: $\{0, 2, 4, 6, 8\}$
3. Ziffer: $\{0, 3, 6, 9\}$
4. Ziffer: $\{0, 4, 8\}$

$\Rightarrow 10 \cdot 5 \cdot 4 \cdot 3 = 600$ solch Zahlen.

Schubfachprinzip: Verteilt man n Elemente auf m Fächer und gilt $\boxed{n > m}$, so gibt es mindestens ein Fach, das zwei Elemente enthält.

Satz 1.4 (Schubfachprinzip) Seien X, Y endliche Mengen und $f: X \to Y$ eine Abbildung. Ist $|X| > |Y|$, so gibt es ein $y \in Y$ mit $|f^{-1}(\{y\})| \geq 2$.

Bsp: Von 13 Personen haben mindestens zwei im selben Monat Geburtstag.

Bsp: In einer Menge von n Personen ($|P| \geq 2$) gibt es immer mindestens zwei Personen, die die gleiche Anzahl von Personen in P kennen. (Ann: Relation „kennen" ist symmetrisch)

Bew:
Sei $P = \{p_1, \dots, p_n\}$ und $f: P \to \{0, \dots, n-1\}$ die Abb., so dass $f(p_i)$ die Anzahl der Personen ist, die p_i kennt.

zz: $\exists p,q \in P: p \neq q \wedge f(p) = f(q)$

Fall 1: $\exists p \in P: f(p) = 0$

$\Rightarrow \forall q \in P$ (n EU): $f(q) \in \{0, \dots, n-2\}$ ($n-1$ EU) $\overset{\text{Schubfach-prinzip}}{\Longrightarrow} \exists q, q' \in P: q \neq q' \wedge f(q) = f(q')$

Fall 2: $\forall p \in P: f(p) > 0$

$\Rightarrow \forall p \in P$ (n EU): $f(p) \in \{1, \dots, n-1\}$ ($n-1$ EU) $\Rightarrow \exists p,q \in P: f(p) = f(q)$

□

Satz 1.5 (Verallgemeinertes Schubfachprinzip) Seien $\emptyset \neq X, Y$ endliche Mengen. Ist $f: X \to Y$ eine Abbildung, so gibt es ein $y \in Y$ mit $|f^{-1}(\{y\})| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$

($\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geq x\}$ Aufrundung $\mathbb{R} \to \mathbb{Z}$)

Beweis: Durch Widerspruch.

Angenommen, es gibt $f: X \to Y$ mit $|f^{-1}(\{y\})| < \left\lceil \frac{|X|}{|Y|} \right\rceil$. für alle $y \in Y$. Dann ist

$$|f^{-1}(\{y\})| \leq \left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \leq \left(\frac{|X|}{|Y|} + \frac{|Y|-1}{|Y|} \right) - 1 = \frac{|X|-1}{|Y|}$$

$$\Rightarrow \sum_{y \in Y} |f^{-1}(\{y\})| \leq |Y| \left(\frac{|X|-1}{|Y|} \right) = |X| - 1 \quad (*)$$

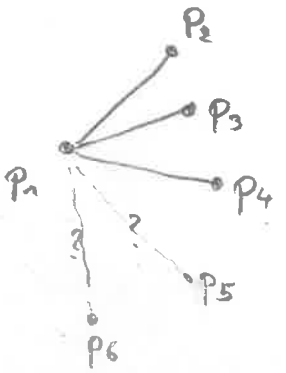
Andererseits

$$|X| = \left| \bigcup_{y \in Y} f^{-1}(\{y\}) \right| = \sum_{y \in Y} |f^{-1}(\{y\})| \overset{(*)}{\leq} |X| - 1 \quad \lightning$$

□

Bsp: In jeder Menge von 6 Personen gibt es 3 Personen die sich alle untereinander kennen oder alle nicht kennen.

Bew: Sei $P = \{p_1, p_2, \dots, p_6\}$. Es gibt entweder mindestens $\lceil \frac{5}{2} \rceil = 3$ Personen, die p_1 kennen, oder min 3 Personen, die p_1 nicht kennen.
Ohne Einschränkung (o.E.), gebe es 3 Personen die p_1 kennen
(der andere Fall geht analog, wenn wir im Folgenden „kennen" durch „nicht kennen" ersetzen)
O.E sind das p_2, p_3, p_4



Fall 1: Zwei der Personen p_2, p_3, p_4 kennen sich
O.E. p_2 kennt p_3
$\Rightarrow$ p_1, p_2, p_3 kennen sich.

Fall 2: p_2, p_3, p_4 kennen sich gegenseitig nicht.

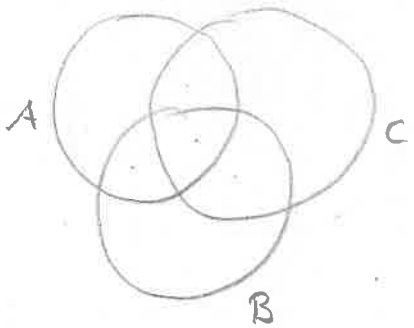
□

Prinzip der Inklusion und Exklusion

Für Mengen A, B gilt: $|A \cup B| = |A| + |B| - |A \cap B|$

Für A, B, C:

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



Satz 1.6 Für endliche Mengen $A_1, \dots, A_n$ $(n \geq 0)$ gilt:

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \left| \bigcap_{j=1}^{k} A_{i_j} \right| \qquad (*)$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{J \subseteq [n] \\ |J| = k}} \left| \bigcap_{j \in J} A_j \right|.$$

Beweis (Kombinatorisch)

Sei $a \in \bigcup_{i=1}^{n} A_i$. [Ansonsten wird a links und rechts je 0 mal gezählt]

zz: a wird auf der rechten Seite von (*) genau einmal gezählt

Sei a in ℓ (genau) der Mengen $A_1, \dots, A_n$ enthalten; $(\ell \geq 1)$.

$\Rightarrow \forall 1 \leq i_1 < \dots < i_k \leq n: \quad a \in \bigcap_{j=1}^{k} A_{i_j} \iff \{i_1, \dots, i_k\} \subseteq \{i \in [n] : a \in A_i\}$

Für festes ℓ gibt es genau $\binom{\ell}{k}$ Möglichkeiten für $i_1, \dots, i_k$.

D.h. in $\sum_{1 \leq i_1 < \dots < i_k \leq n} \left| \bigcap_{j=1}^{k} A_{i_j} \right|$ wird a genau $\binom{\ell}{k}$ mal gezählt.

$\Rightarrow$ a wird auf der rechten Seite $\sum_{k=1}^{\ell} (-1)^{k-1} \binom{\ell}{k}$ mal gezählt.

Binomische Formel:

$$0 \underset{\ell \geq 1}{=} (1 + (-1))^{\ell} = \sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^k 1^{\ell-k} = -\sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^{k-1} = 1 - \sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^{k-1}$$

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

□

Beweis (Induktion) $n=1$ ✓ $n=2$ ✓

$n \geq 3$, $n-1 \to n$: $\quad B := \bigcup_{i=1}^{n-1} A_i$

$$\left| \bigcup_{i=1}^{n} A_i \right| = |B \cup A_n| \underset{(*)}{=} |B| + |A_n| - |B \cap A_n| = (*)$$

IVR: $|B \cap A_n|$: $\quad B \cap A_n = \left(\bigcup_{i=1}^{n-1} A_i \right) \cap A_n = \bigcup_{i=1}^{n-1} \underbrace{(A_i \cap A_n)}_{=: B_i}$

$$\Rightarrow |B \cap A_n| = \left| \bigcup_{i=1}^{n-1} B_i \right| \underset{IV}{=} \sum_{k'=1}^{n-1} (-1)^{k'-1} \sum_{1 \leq i_1 < \dots < i_{k'} \leq n} \left| \bigcap_{j=1}^{k'} B_{i_j} \right|$$

$$= \sum_{k'=1}^{n-1} (-1)^{k'-1} \sum_{1 \leq i_1 < \dots < i_{k'} \leq n} \left| \left(\bigcap_{j=1}^{k'} A_{i_j} \right) \cap A_n \right| = \sum_{k=2}^{n} (-1)^{k} \sum_{\substack{1 \leq i_1 < \dots < i_k \leq n \\ i_k = n}} \left| \bigcap_{j=1}^{k} A_{i_j} \right|$$

Nun folgt

$$(*) \underset{IV}{=} \underbrace{\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \dots < i_k \le n-1} \left| \bigcap_{j=1}^{k} A_{i_j} \right|}_{= |B|} + |A_n| + \sum_{k=2}^{n} (-1)^{k-1} \sum_{\substack{1 \le i_1 < i_2 < \dots < i_k \le n \\ i_k = n}} \left| \bigcap_{j=1}^{k} A_{i_j} \right|$$

($|A_n|$: $k=1$)

$$= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} \left| \bigcap_{j=1}^{k} A_{i_j} \right|$$

□

Bsp: $|\{n \in [100] : 2 \mid n, 3 \mid n \text{ oder } 5 \mid n\}|$

$A_k := \{n \in [100] : k \mid n\}$ $(k \in \mathbb{N})$

Gesucht: $|A_2 \cup A_3 \cup A_5|$

$|A_k| = \left\lfloor \frac{100}{k} \right\rfloor$

$A_2 \cap A_3 = A_6, \quad A_3 \cap A_5 = A_{15}, \quad A_2 \cap A_5 = A_{10}$

$$\Rightarrow |A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}|$$

$$= 50 + 33 + 20 - 16 - 10 - 6 + 3$$

$$= \underline{\underline{74}}$$

Bsp „Derangements", $f: [n] \to [n]$ ist fixpunktfrei, wenn $f(i) \neq i$ für alle $i \in [n]$ gilt. Wieviele solche bijektiven Abb. gibt es?

$d_n = n! - \xi_n$, wobei ξ_n die Anzahl der Abb. mit Fixpunkt ist.

$A_i := \{ f: [n] \to [n] : f \text{ bijektiv}, f(i) = i \}$ für $i \in [n]$.

$$\xi_n = \left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < \dots < i_k \le n} \underbrace{\left| \bigcap_{j=1}^{k} A_{i_j} \right|}_{= (n-k)!} = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)!$$

$$= \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}$$

$$\Rightarrow \underline{\underline{d_n = n! \left(1 - \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!} \right) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}}}$$

1.3 Wichtige Zählprobleme

1.3.1 Teilmengen & Binomialkoeffizienten

Satz 1.7 Sei A eine endliche Menge mit $|A| = n$. Dann ist $|\mathcal{P}(A)| = 2^n$.

Beweis: Induktion nach n. $\underline{n=0}$: $\Rightarrow A = \emptyset$, $\mathcal{P}(A) = \{\emptyset\} \Rightarrow |\mathcal{P}(A)| = 1 = 2^0$ ✓

$\underline{n-1 \to n,\ n \ge 1}$: Sei $a_0 \in A$.

$$\mathcal{P}(A) = \underbrace{\{B \subseteq A : a_0 \notin A\}}_{=: M_1} \overset{\text{disjunkte Vereinigung}}{\cup} \underbrace{\{B \subseteq A : a_0 \in A\}}_{=: M_2}$$

$$|M_1| = |\mathcal{P}(A \setminus \{a_0\})| \overset{\text{IV}}{=} 2^{n-1}$$

$f: \begin{cases} M_1 \to M_2 \\ B \mapsto B \cup \{a_0\} \end{cases}$ ist bijektiv mit Umkehrabb. $f^{-1}: \begin{cases} M_2 \to M_1 \\ B \mapsto B \setminus \{a_0\} \end{cases}$

(nachrechnen!) $\to |M_2| = |M_1| = 2^{n-1} \Rightarrow |\mathcal{P}(A)| = 2 \cdot 2^{n-1} = 2^n$ □

Der Binomialkoeffizient

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{falls } 0 \le k \le n \\ 0 & \text{falls } k > n \end{cases} \qquad (n \in \mathbb{N}_0)$$

gibt die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge an.

Korollar (zu Satz 1.7): $2^n = \sum_{k=0}^{n} \binom{n}{k}$

Bemerkung: Alternativ folgt das Korollar aus der Binomischen Formel, Satz 1.1, mit $a=b=1$. Damit ergibt sich ein weiterer Beweis für Satz 1.7.

Satz 1.8 Seien $k, n \in \mathbb{N}_0$ mit $k \le n$.

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

(2) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ für $n \ge k \ge 1$ (Pascalsche Identität)

Beweis: (1) Nach Def.

(2) Beweis I (Nachrechnen)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!\,(n-k)!} + \frac{(n-1)!}{k!\,(n-1-k)!}$$

$$= \frac{k \cdot (n-1)!}{k!\,(n-k)!} + \frac{(n-k)\,(n-1)!}{k!\,(n-k)!} = \frac{\overbrace{(k+(n-k))}^{n}\,(n-1)!}{k!\,(n-k)!} = \frac{n!}{k!(n-k)!}$$

$$= \binom{n}{k}$$

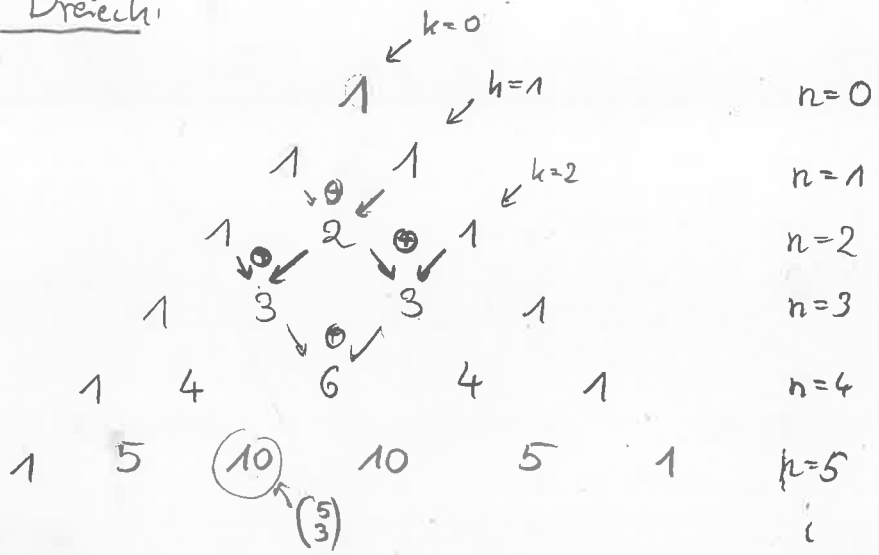
Beweis II **Links:** Anzahl der k-elementigen Teilmengen von $[n]$.

Rechts: $\binom{n-1}{k}$ ... Anzahl k-elementigen TM. von $[n]$ $\setminus\{n\}=[n-1]$

$\binom{n-1}{k-1}$ — " — " — $[n]$, die n enthalten.

□

Pascalsches Dreieck:



Satz 1.9 (Vandermondsche Identität) Für $m,n,k \in \mathbb{N}_0$ gilt

$$\binom{n+m}{k} = \sum_{e=0}^{k} \binom{n}{e}\binom{m}{k-e}$$

Beweis: Seien A, B disjunkte Mengen mit $|A|=n$, $|B|=m$

Links: Anzahl k-elementigen Teilmengen von $A \cup B$.

Rechts: $\binom{n}{e}\binom{m}{k-e}$ zählt die Anzahl der k-elementigen TM, wobei ℓ Elemente aus A und $k-\ell$ Elemente aus B gewählt werden.

□

1.3.2 Mengenpartitionen

Def. Eine k-Partition einer Menge A ist eine Menge $\{A_1, \dots, A_k\}$ nicht-leerer, paarweise disjunkter Teilmengen von A, so dass $A = \bigcup_{i=1}^{k} A_i$.

Bsp: $A = [6]$ $\quad \{\{1,6\}, \{2\}, \{3,4,5\}\}$ ist 3-Partition von $[6]$

$$[6] = \{1,6\} \cup \{2\} \cup \{3,4,5\}$$

Def: Für $n, k \in \mathbb{N}_0$ sei $\left\{ n \atop k \right\}$ die Anzahl der k-Partitionen einer n-elementigen Menge.
Die Zahlen $\left\{ n \atop k \right\}$ heißen Stirlingzahlen zweiter Art.

Bem: $\left\{ n \atop k \right\} = 0$ falls $k > n$, $\left\{ 0 \atop k \right\} = \begin{cases} 0 & \text{falls } k > 0 \\ 1 & \text{falls } k = 0 \end{cases}$ [denn $\bigcup_{A \in \emptyset} A = \emptyset$]

Satz 1.10 Für $n \geq k \geq 1$ gilt $\left\{ n \atop k \right\} = \left\{ n-1 \atop k-1 \right\} + k \left\{ n-1 \atop k \right\}$

Beweis: Wir teilen die k-Partitionen von $A = \{a_1, a_2, \dots, a_n\}$ in zwei disjunkte Klassen:

(1) $\{a_n\}$ ist eine Teilmenge der Partition, Die restlichen $k-1$ Teilmengen bilden eine $(k-1)$-Partition von $A \setminus \{a_n\}$. Dafür gibt es $\left\{ n-1 \atop k-1 \right\}$ Möglichkeiten.

(2) a_n befindet sich nicht allein in einer Teilmenge. Dann befindet a_n sich in einer der k Mengen auf die sich die anderen $n-1$ Elemente verteilen. Es gibt $k \cdot \left\{ n-1 \atop k \right\}$ Möglichkeiten. □

Bem (Nachtrag zum Binomialkoeffizienten) Man kann die Definition des Binomialkoeffizienten erweitern: für $\alpha \in \mathbb{C}$, $k \in \mathbb{Z}$

sei $$\binom{\alpha}{k} = \begin{cases} \frac{\prod_{j=0}^{k-1}(\alpha - j)}{k!} = \frac{\alpha \cdot (\alpha-1) \cdot \ldots \cdot (\alpha-(k-1))}{k!} & \text{für } k \geq 0, \\ 0 & \text{für } k < 0. \end{cases}$$

Insbesondere: $\binom{-1}{k} = (-1)^k$ für $k \geq 0$.

Satz 1.8 gilt dann für alle $n, k \in \mathbb{Z}$. (Fehlende Fälle sind trivial → nachprüfen!)

1.3.3 Permutationen

Sei A eine endliche Menge.

Def: Eine Permutation von A ist eine bijektive Abb $\sigma: A \to A$. Der Träger von σ ist $\operatorname{supp}(\sigma) := \{a \in A : \sigma(a) \neq a\}$.

Die Menge S_A der Permutationen von A bildet mit der Hintereinanderausführung $\circ$ die symmetrische Gruppe auf A. (→ Lineare Algebra VO)

$S_n := S_{[n]}$. Ist $|A| = n$, so ist $|S_A| = |S_n| = n!$ $(n \geq 0)$

Bsp: $$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix} \in S_{11}$$

3, 9 sind Fixpunkte: $\pi(3) = 3$, $\pi(9) = 9$

$\pi(1) = 5$, $\pi(\pi(1)) = \pi(5) = 2$, $\pi^3(1) = \pi(2) = 8$, $\pi^4(1) = \pi(8) = 1$

Zyklus der Länge 4, Schreibweise: $(1\ 5\ 2\ 8)$

$\pi = (3)(9)(1\ 5\ 2\ 8)(4\ 6\ 7)(10\ 11) = (1\ 5\ 2\ 8)(4\ 6\ 7)(10\ 11)$

Transposition (Zyklus der Länge 2)

Def: $\sigma \in S_A$ heißt **Zyklus der Länge k** (**k-Zyklus**, **k-Zykel**), $k \geq 1$,
wenn es paarweise verschiedene $i_1, \dots, i_k \in A$ gibt, so dass
$\sigma(i_j) = i_{j+1}$ für $1 \leq j < k$, $\sigma(i_k) = i_1$ und $\sigma(a) = a$ für $a \in A \setminus \{i_1, \dots, i_k\}$. Man schreibt $\sigma = (i_1\, i_2 \dots i_k)$ und $|\sigma| = k$. σ ist **nicht-trivial** falls $k \geq 2$.

Für einen Zyklus $\sigma = (i_1\, i_2 \dots i_k)$ mit $k \geq 2$ gilt $\operatorname{supp} \sigma = \{i_1, i_2, \dots, i_k\}$.
Sind $\sigma, \tau \in S_A$ mit $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$, so heißen σ, τ **disjunkt**.
Für disjunkte $\sigma, \tau \in S_A$ gilt $\sigma\tau = \tau\sigma$.

In einem Zyklus kommt es auf die Reihenfolge der Elemente an, aber bei zyklischer Vertauschung der Elemente bleibt der Zyklus gleich: $(i_1\, i_2\, i_3 \dots i_k) = (i_2\, i_3 \dots i_k\, i_1) = (i_3\, i_4 \dots i_k\, i_1\, i_2)$

Bsp: $(4\,6\,7) = (6\,7\,4) = (7\,4\,6) \neq (4\,7\,6)$

Satz 1.11 Jedes $\sigma \in S_A$ ist Produkt paarweise verschiedener, nicht-trivialer Zyklen. Die Darstellung ist bis auf Reihenfolge der Faktoren eindeutig. D.h., ist $\sigma = \tau_1 \cdots \tau_m = \pi_1 \cdots \pi_n$ mit τ_i, π_j nicht-trivial und $\tau_1, \dots, \tau_m$ bzw. $\pi_1, \dots, \pi_n$ jeweils pw. disjunkt, so ist $m = n$ und es existiert $\gamma \in S_n$: $\tau_i = \pi_{\gamma(i)}$ für alle $i \in [n]$.

Beweis: (*) **Existenz** Induktion nach $\ell = |\operatorname{supp}(\sigma)|$.

$\ell = 0$: $\sigma = \mathrm{id}$ ist das leere Produkt

$\ell > 0$, Die Aussage gelte für alle σ' mit $|\operatorname{supp}(\sigma')| < \ell$.

Sei $i_1 \in \operatorname{supp}(\sigma)$. $\{\sigma^j(i_1) : j \geq 0\} \subseteq A$ ist endlich
$\Rightarrow \exists\, \ell, \ell' \geq 0$: $\ell < \ell'$ und $\sigma^\ell(i_1) = \sigma^{\ell'}(i_1) \Rightarrow \sigma^{\ell'-\ell}(i_1) = i_1$
Sei $k \geq 1$ minimal mit $\sigma^k(i_1) = i_1$. Wegen $i_1 \in \operatorname{supp}(\sigma)$ ist $k \geq 2$.

Für $j, j' \in \{0, \dots, k-1\}$ gilt: $\sigma^j(i_1) = \sigma^{j'}(i_1) \Rightarrow j = j'$.
(denn: O.E $j < j'$. $\sigma^j(i_1) = \sigma^{j'}(i_1) \Rightarrow \sigma^{j'-j}(i_1) = i_1 \underset{k \text{ minimal}}{\Rightarrow} j' - j = 0$)

(*) Vorbemerkung: Sind $\tau_1, \dots \tau_m$ pw. disjunkt, nicht-trivial Zykel, so gilt
$\operatorname{supp}(\tau_1 \cdots \tau_m) = \bigcup_{i=1}^{m} \operatorname{supp}(\tau_i)$

For $j \in [k]$ sei $i_j := \sigma^{j-1}(i_1)$. Dann ist $\tau = (i_1\, i_2 \dots i_k)$ ein k-Zykel

$\operatorname{supp}(\tau^{-1}\sigma) = \operatorname{supp}(\sigma) \setminus \{i_1, \dots, i_k\} \Rightarrow |\operatorname{supp}(\tau^{-1}\sigma)| < |\operatorname{supp}(\sigma)|$

$\overset{IV}{\Rightarrow} \tau^{-1}\sigma = \tau_2 \cdots \tau_m$ mit nicht-trivialen, pw. disjunkten Zykeln $\tau_2, \dots, \tau_m$.

Wegen $\bigcup_{j=2}^{m} \operatorname{supp}(\tau_j) = \operatorname{supp}(\tau_2 \cdots \tau_m) = \operatorname{supp}(\tau^{-1}\sigma) = \operatorname{supp}(\sigma) \setminus \{i_1, \dots, i_k\}$

und $\operatorname{supp}(\tau) = \{i_1, \dots, i_k\}$ ist $\operatorname{supp}(\tau) \cap \operatorname{supp}(\tau_j) = \emptyset$ für $j \in \{2, \dots, m\}$.

$\Rightarrow \sigma = \tau\tau_2 \cdots \tau_m$ ist Produkt pw. disjunkter Zykeln.

Eindeutigkeit Induktion nach $\ell = |\operatorname{supp}(\sigma)|$. $\underline{\ell = 0}$ ✓

$\underline{\ell > 0}$, die Aussage gelte für σ' mit $|\operatorname{supp}(\sigma')| < \ell$.

Sei $\sigma = \tau_1 \cdots \tau_m = \pi_1 \cdots \pi_n$ mit nicht-trivialen Zykeln τ_i, π_j, wobei $\tau_1, \dots, \tau_m$ und $\pi_1, \dots, \pi_n$ jeweils pw. disjunkt sind

$\ell > 0 \Rightarrow m > 0$. Sei $i_1 \in \operatorname{supp}(\tau_1)$. Es gibt $j \in [n]$ mit $i_1 \in \operatorname{supp}(\pi_j)$,

o.E. sei $i_1 \in \operatorname{supp}(\pi_1)$.

Beh A: $\tau_1 = \pi_1$.

Bew Genügt zz: $\forall j \geq 0: \tau_1^j(i_1) = \pi_1^j(i_1)$

Induktion nach j: $\underline{j = 0}$ ✓,

$\underline{j-1 \to j}$: $i := \tau_1^{j-1}(i_1) = \pi_1^{j-1}(i_1) \Rightarrow i \in \operatorname{supp}(\tau_1) \cap \operatorname{supp}(\pi_1)$

$\Rightarrow \tau_1^j(i_1) = \tau_1(i) = \tau_1\tau_2 \cdots \tau_m(i) = \sigma(i) = \pi_1\pi_2 \cdots \pi_m(i) = \pi_1(i) = \pi_1^j(i_1)$. $\square$(A)

$\tau_1 = \pi_1 \Rightarrow \tau_2 \cdots \tau_m = \pi_2 \cdots \pi_n \overset{IV}{\Rightarrow} m = n$, und nach Umnummerierung: $\tau_j = \pi_j$ für $j \in \{2, \dots, m\}$.

$\square$

Korollar: Jedes $\sigma \in S_A$ besitzt eine, bis auf die Reihenfolge der Faktoren, eindeutige Darstellung $\sigma = \tau_1 \cdots \tau_m$ mit pw. disjunkten Zykeln $\tau_1, \dots, \tau_m$, so dass jeder Fixpunkt ab genau ein 1-Zykel dargestellt wird.

(Ergänze vorhergehende Darstellung um 1-Zykeln für Fixpunkte)

Def: Für $k,n \in \mathbb{N}_0$ mit $k \leq n$ sei $\begin{bmatrix} n \\ k \end{bmatrix}$ die Anzahl der Permutationen von $[n]$ mit genau k Zyklen (wobei Fixpunkte als 1-Zyklen gezählt werden). Diese Zahlen heißen Stirlingzahlen erster Art.

Bem: (1) $S_{[0]} = \{id : \emptyset \to \emptyset\}$, also $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$,

- für $k > n$ ist $\begin{bmatrix} n \\ k \end{bmatrix} = 0$
- für $n \geq 1$ ist $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$

} $\sigma \in S_n$ enthält zumindest einen, höchstens n, Zyklen.

(2) $\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$ (3) $\begin{bmatrix} n \\ n \end{bmatrix} = 1$ für $n \in \mathbb{N}_0$

Satz 1.12 Für $k,n \in \mathbb{N}$ mit $n \geq k$ gilt $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}$

Beweis: Permutationen σ von $[n]$ mit k Zyklen zerfallen in zwei Klassen:

(1) n ist Fixpunkt (1-Zyklel), $\sigma|_{[n-1]}$ ist eine Permutation von $[n-1]$ mit $k-1$ Zyklen: $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ Möglichkeiten.

(2) σ entsteht aus einer Permutation von $[n-1]$ mit k Zyklen, indem man n an einer Stelle eines Zyklus einfügt. In einem Zyklus der Länge ℓ gibt es ℓ verschiedene Möglichkeiten n einzufügen:

$(n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}$ Möglichkeiten

Bsp $n=[4]$, $k=3$

Fall (1)	Fall (2)
(1 2)(3)|(4)	(1)(2)(3 4)
(1 3)(2)|(4)	(1)(2 4)(3)
(1)(2 3)|(4)	(1 4)(2)(3)

1.3.4 Zahlpartitionen

Sei $k \in \mathbb{N}_0$. [ausgelassen → UE]

Auf wieviele Arten lässt sich $n \in \mathbb{N}_0$ als Summe $n = n_1 + \dots + n_k$ mit $n_1, \dots, n_k \in \mathbb{N}$ schreiben?

Ungeordnete Zahlpartitionen: $4 = 3+1$ ist dieselbe Partition wie $4 = 1+3$

$P_{n,k} = 0$ falls $k > n$, $P_{n,0} = 0$ für $n > 0$, $P_{0,0} = 1$.

Satz 1.13 Für $n \geq k \geq 1$ gilt $P_{n,k} = \sum_{j=0}^{k} P_{n-k,j}$

Beweis: Sei $j \in \{0, \dots, k\}$. Zähle Partitionen in denen 1 genau j mal vorkommt: $n = \underbrace{1 + \dots + 1}_{j \text{ Summanden}} + \underbrace{n_{j+1} + \dots + n_k}_{k-j \text{ Summanden, alle} \geq 2}$.

Mit $n_i' := n_i - 1$ ist $n-k = n_{j+1}' + \dots + n_k'$ eine Partition von $n-k$. (und umgekehrt)

$$\Rightarrow P_{n,k} = \sum_{j=0}^{k} P_{n-k,k-j} = \sum_{j=0}^{k} P_{n-k,j}. \qquad \square$$

Geordnete Zahlpartitionen: $4 = 3+1 = 1+3 = 2+2$

$$n = \underbrace{1 + \dots + 1}_{n_1} + \underbrace{1 + \dots + 1}_{n_2} + \dots + \underbrace{1 + \dots + 1}_{n_k}$$

(n Einsen, $k-1$ Pluszeichen)

G. Partition $\hat{=}$ Wahl von $k-1$ der $n-1$ „+" Zeichen. Damit gilt:

Satz 1.14 Für $n \geq k \geq 1$ gilt: Es gibt genau $\binom{n-1}{k-1}$ k-Partitionen von n.

2. GRAPHEN

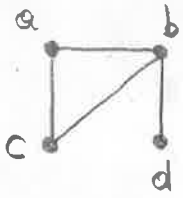
2.1 Definition, Isomorphismus, Teilgraphen

Definition Ein (einfacher) Graph ist ein Paar $G=(V,E)$, bestehend aus einer Menge V, deren Elemente Knoten (Ecken, engl: vertex/-ices, nodes) heißen, und einer Menge E von 2-elementigen Teilmengen von V (d.h. $E \subseteq \binom{V}{2} := \{\{x,y\} : \substack{x,y \in V \\ x \neq y}\}$), deren Elemente Kanten (engl: edges) heißen.

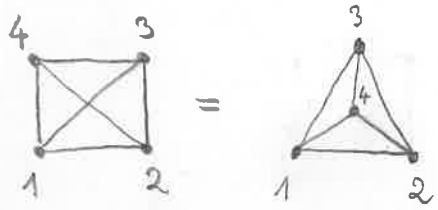
Ist V endlich, so heißt G endlicher Graph.

Ist G ein Graph, so sei $V(G)$ bzw. $E(G)$ die Menge seiner Knoten bzw. Kanten, und $|G| := |V(G)|$ seine Ordnung.

Bsp:



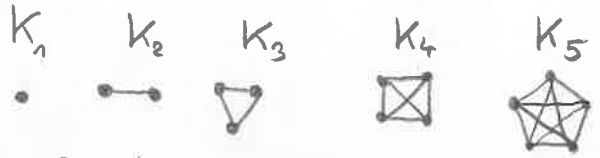
$V=\{a,b,c,d\}$, $E=\{\{a,b\},\{a,c\},\{b,c\},\{b,d\}\}$



Darstellungen desselben Graphs!

Bsp Sei $n \in \mathbb{N}_0$.

a) Der vollständige Graph K_n: $V=[n]$, $E=\binom{[n]}{2}=\{\{i,j\} : 1 \leq i < j \leq n\}$



n Knoten, $\binom{n}{2}$ Kanten

b) Die (n-stabile Menge) E_n: $V=[n]$, $E=\emptyset$

n Knoten, 0 Kanten

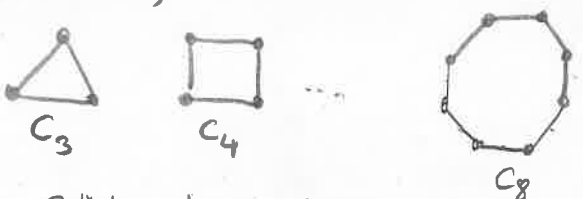
c) Der Weg (lineare Graph, Pfad) der Länge n, P_n:

$V=\{0,1,\dots,n\}$, $E=\{\{i-1,i\} : 1 \leq i \leq n\}$ $n+1$ Knoten, n Kanten

d) Der Kreis der Länge $n \geq 3$, C_n

$V = [n]$, $E = \{\{i, i+1\} : 1 \leq i \leq n-1\} \cup \{n, 1\}$

n Knoten, n Kanten

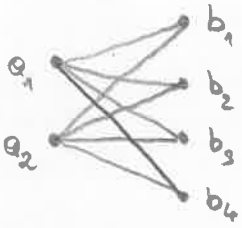


e) $m, n \in \mathbb{N}$, der vollständige bipartite Graph $K_{m,n}$:

$V = \{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}$ m+n Knoten

$E = \{\{a_i, b_j\} : 1 \leq i \leq m, 1 \leq j \leq n\}$ mn Kanten

$K_{2,4}$:



f) der leere Graph: $V = E = \emptyset$,

Triviale Graphen ($|G| \leq 1$) werden oft großzügig ignoriert (wenn lösbig).

Bem: (1) Es gibt viele andere Varianten von Graphen, z.B.

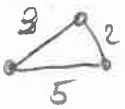
- gerichtete Graphen

- Graphen mit Mehrfachkanten: (Multidigraph)

, Schlaufen ("loops")

,

- Kanten mit Gewicht



,

und unterschiedliche Kombinationen davon. Wir behandeln nur ungerichtete, einfache Graphen ohne Schlaufen.

(2) {Graphen mit Knotenmenge V} $\overset{\text{bij.}}{\longleftrightarrow}$ {Symmetrische, irreflexive Relationen auf V} ($a \neq a$)

$(V, E) \longmapsto v \sim w :\Leftrightarrow \{v, w\} \in E$

Definition $G=(V,E)$ sei ein Graph.

- Knoten $v,w \in V$ heißen **benachbart** (**adjazent**), wenn $\{v,w\} \in E$.
  Für $v \in V$ ist $N(v) := \{w \in V : \{v,w\} \in E\}$ die **Nachbarschaft** von v. Der **Grad** (die **Valenz**) von v ist $\deg v := \deg_G v := |N(v)|$, die Anzahl der Nachbarn von v. Ein Knoten mit Grad 0 heißt **isoliert**, ein Knoten mit Grad 1 heißt **Blatt**.
  G heißt **k-regulär** ($k \geq 0$), wenn alle Knoten den gleichen Grad k haben.
- Ein Knoten v und eine Kante e **inzidieren** miteinander, und heißen **inzident**, wenn $v \in e$. Die beiden Knoten einer Kante sind ihre **Endknoten**, die Kante **verbindet** die beiden Knoten.

Lemma 2.1 Sei $G=(V,E)$ ein endlicher Graph. Dann gilt

(1) [Handshake-Lemma] $\sum_{v \in V} \deg(v) = 2 \cdot |E|$

(2) Die Anzahl der Knoten ungeraden Grades ist gerade

(3) Ist $|V| \geq 2$, so hat G mindestens zwei Knoten gleichen Grades.

Beweis (1) Inzidenzrelation $R \subseteq V \times E$: $v \sim e :\Leftrightarrow v \in e$

$$|R| = \sum_{v \in V} |\{e \in E : v \sim e\}| = \sum_{v \in V} |N(v)| = \sum_{v \in V} \deg(v)$$

$$|R| = \sum_{e \in E} |\{v \in V : v \sim e\}| = \sum_{e \in E} 2 = 2|E|$$

(2) $2|E| \overset{(1)}{=} \underbrace{\sum_{\substack{v \in V \\ \deg(v) \text{ gerade}}} \deg(v)}_{\text{gerade}} + \underbrace{\sum_{\substack{v \in V \\ \deg(v) \text{ ungerade}}} \deg(v)}_{\text{gerade}} \Rightarrow \sum_{\substack{v \in V \\ \deg(v) \text{ ungerade}}} \deg(v)$ ist gerade

$\Rightarrow |\{v \in V : \deg(v) \text{ ungerade}\}|$ ist **gerade**.

(3) [Ü], vgl.: in einer Menge von P Personen, $|P| \geq 2$, kennen zwei Personen die gleiche Anzahl von Personen [Bsp. nach Satz 1.4] $\square$

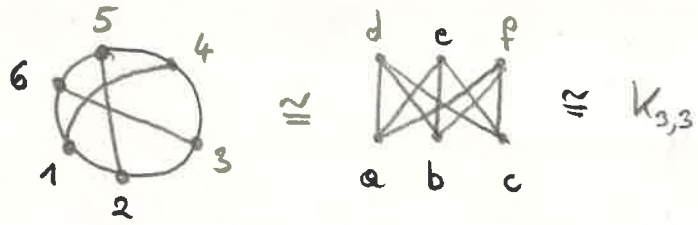
$G = G' \Leftrightarrow V(G) = V(G')$ und $E(G) = E(G')$

Def: Zwei Graphen $G=(V,E)$ und $G'=(V',E')$ heißen isomorph, wenn es eine Bijektion $f: V \to V'$ gibt, so dass

$$\{v,w\} \in E \Leftrightarrow \{f(v), f(w)\} \in E'$$

für alle $v,w \in V$ mit $v \neq w$ gilt. In Zeichen: $G \cong G'$.
So eine Funktion f heißt Isomorphismus der Graphen G und G'

Bsp:



$\cong K_{3,3}$

$f: 1 \mapsto a,\ 2 \mapsto d,\ 3 \mapsto b,\ 4 \mapsto e,\ 5 \mapsto c,\ 6 \mapsto f.$

Bem: ·) „isomorph sein" ist eine Äquivalenzrelation für Graphen

·) Ist $f: G \to G'$ ein Isomorphismus von Graphen, so gilt $\deg(v) = \deg(f(v))$ für alle $v \in V$. [Ü]

Def: Seien $G=(V,E)$ und $G'=(V',E')$ Graphen. G' heißt Teilgraph von G, wenn $V' \subseteq V$ und $E' \subseteq E$ gelt.
In Zeichen: $G' \subseteq G$. Ein Teilgraph G' von G heißt induzierter Teilgraph von G, wenn $E' = E \cap \binom{V'}{2}$ (d.h., G' enthält alle Kanten von G, welche Knoten aus V' verbinden). In Zeichen: $G' = G[V']$.

Bsp:

$G \supseteq G'$ Teilgraph

Induzierter Teilgraph

Def (Wege, Kantenzüge, Kreise) Sei $G=(V,E)$ ein Graph, $n \in \mathbb{N}_0$

(1) Ein Teilgraph $G' \subseteq G$ heißt

(i) ein Weg (der Länge n) (engl. path), wenn $G' \cong P_n$. D.h. es gibt eine Folge paarweise verschiedener Knoten $v_0, v_1, \dots, v_n$ von G, so dass für alle $1 \le i \le n$ gilt $\{v_{i-1}, v_i\} \in E(G)$. ($n=0$ ist erlaubt!)
v_0, v_n heißen Endknoten des Wegs G', G' heißt Weg von v_0 nach v_n. Schreibweise: $v_0 v_1 \dots v_n$ (Achtung: Weg hat keine Richtung)

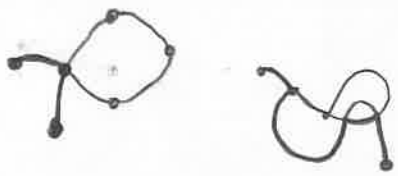
(ii) ein Kreis (der Länge $n \ge 3$), wenn $G' \cong C_n$. Sind $v_1, \dots, v_n$ die Knoten von G' schreibt man $v_1 v_2 \dots v_n v_1$ für G'.

(iii) eine Clique (der Größe n) bzw. n-Clique, wenn $G' \cong K_n$

(2) Ein Kantenzug (der Länge n) ist eine Folge $(v_0, e_1, v_1, e_2, \dots, e_n, v_n)$ von abwechselnd Knoten und Kanten aus G mit $e_i = \{v_{i-1}, v_i\}$ für $1 \le i \le n$.
Ist $v_n = v_0$, so heißt der Kantenzug geschlossen.

Lemma 2.2 Ist $(v_0, e_1, v_1, e_2, \dots, e_n, v_n)$ ein Kantenzug, so gibt es einen Weg von v_0 nach v_n, dessen Knoten eine Teilmenge von $\{v_0, v_1, \dots, v_n\}$ bilden.

Bew: Übung, man entferne auftretende Kreise / mehrfache Kanten.

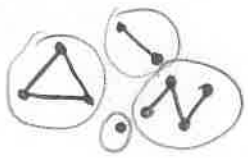


Def: Ein Graph $G=(V,E)$ heißt zusammenhängend, wenn $|G| \ge 1$ und für alle $v, w \in V$ existiert ein Weg von v nach w.

Allgemeiner: Für $v, w \in V$ sei die Relation „erreichbar", $v \leftrightsquigarrow w$, wie folgt definiert: $v \leftrightsquigarrow w :\Leftrightarrow \exists$ Weg von v nach $w \Leftrightarrow \exists$ Kantenzug von v nach w.
„$\leftrightsquigarrow$" ist eine Äquivalenzrelation auf V. Die von den Äquivalenzklassen $[v]_{\leftrightsquigarrow}$ induzierten Teilgraphen $G[[v]_{\leftrightsquigarrow}]$ heißen Komponenten von G.
Schreibweise: $K(v) := K_G(v) := G[[v]_{\leftrightsquigarrow}]$
Jede Komponente von G ist zusammenhängend.

G ist genau dann zusammenhängend, wenn G genau eine Komponente hat.

Bsp:



Der leere Graph ist nicht zshg.!

Satz 2.3 Sei $G=(V,E)$ ein Graph

(1) G enthält mindestens $|V|-|E|$ viele Komponenten

(2) Ist G zusammenhängend, so gilt $|E| \geq |V|-1$.

Beweis: (1) Induktion nach $m=|E|$.

$m=0$: G enthält $|V|$ Komponenten ✓

$m \geq 0$, $m \to m+1$: Sei $e \in E$, $E' := E \setminus \{e\}$

$\Rightarrow |E'|=m$ und $G'=(V,E')$ hat nach IV mindestens $|V|-m$ Komponenten.

Durch Hinzufügen von $e=\{v,w\}$ ändert sich entweder die Zahl der Komponenten nicht (wenn $K_{G'}(v)=K_{G'}(w)$), oder sie verringert sich um 1 (wenn $K_{G'}(v) \neq K_{G'}(w)$). Jedenfalls hat G mindestens $|V|-m-1$ Komponenten.

(2) Aus (1) folgt $|V|-|E| \leq 1$. □

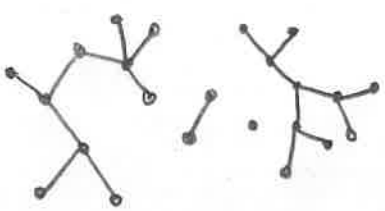
2.2 Bäume und Wälder

Def (*) Ein Graph G heißt

(i) kreisfrei (oder ein Wald), wenn G keinen Kreis enthält

(ii) ein Baum, wenn G kreisfrei und zusammenhängend ist.

Bsp:



(*) Notation: Für einen Graph $G=(V,E)$ und $v \in V$, $e \in E$ sei

$G-v := G[V \setminus \{v\}]$ und $G-e := (V, E \setminus \{e\})$.

Für $e \in \binom{V}{2}$ sei $G+e := (V, E \cup \{e\})$

Lemma 2.4

(1) Die Komponenten eines Waldes sind Bäume.

(2) Jeder endliche Baum T mit $|T| \geq 2$ hat mindestens zwei Blätter.

(3) Sei G ein Graph und v ein Blatt. Dann ist G genau dann ein Baum, wenn $G - v$ ein Baum ist.

Beweis: (1) Klar.

(2) Sei $P \subseteq T$ ein Weg maximaler Länge mit Endknoten v_0, v_n (existiert wegen $|P| \leq |T| < \infty$). Wegen $|T| \geq 2$ ist $|E(T)| \geq 1$ und deshalb $v_0 \neq v_n$. Weil v_0, v_n auf einem nicht-trivialen Weg liegen, ist $\deg v_0, \deg v_n \geq 1$. Wäre $\deg v_0 > 1$ oder $\deg v_n > 1$, könnten wir P verlängern.(*) Also ist $\deg v_0 = \deg v_n = 1$.

(3) „$\Rightarrow$" Weil G kreisfrei ist, gilt das auch für $G' := G - v$. Wir zeigen: G' ist zusammenhängend. Seien $w, w' \in V(G')$ mit $w \neq w'$. Dann gibt es in G einen Weg $P = w v_1 \dots v_{n-1} w'$ mit $v_i \in V(G)$. Wegen $\deg v = 1$ ist $v \notin \{v_1, \dots, v_{n-1}\}$, also $P \subseteq G'$.

„$\Leftarrow$" Durch Hinzufügen von v kann kein Kreis entstehen. G ist zusammenhängend: Sind $w, w' \in V(G')$, so gibt es einen w-w' Weg in G' und damit auch in G. Sei nun $w \in V(G')$ und v' der Nachbar von v. Dann gibt es in G' einen Weg $P = v' v_1 - v_{n-1} w$ von v' nach w, und $vP = vv' v_1 - v_{n-1} w$ ist ein Weg von v nach w. □

Satz 2.5 (Charakterisierung von Bäumen)

Folgende Aussagen sind für einen Graph $G = (V, E)$ äquivalent:

(a) G ist ein Baum

(b) Zu je zwei Knoten v, w gibt es genau einen Weg von v nach w.

(c) G ist minimal zusammenhängend, d.h. G ist zusammenhängend und für alle $e \in E$ ist $G - e$ nicht zusammenhängend.

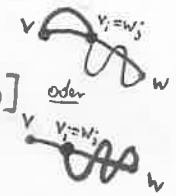
(d) G ist maximal kreisfrei, d.h. G ist kreisfrei, aber für alle $e \in \binom{V}{2} \setminus E$ enthält $G + e$ einen Kreis.

[(*) Ann.: $v' \in N(v_0) \setminus \{v_1\}$. Dann ist $v' \notin \{v_0, \dots, v_n\}$, da T sonst einen Kreis enthalten würde]

Ist G endlich, so ist weiters äquivalent:

(e) G ist zusammenhängend und $|V| = |E| + 1$.

Beweis: (a) $\Rightarrow$ (b) Da G zusammenhängend ist, gibt es für alle Knoten v, w einen v-w Weg. Angenommen es gibt Knoten v, w zwischen denen es zwei Wege $v v_1 \dots v_{m-1} w$ und $v w_1 \dots w_{n-1} w$ gibt $(m, n \geq 2)$. Wir wählen v, w und die beiden Wege so, dass $m+n$ minimal ist. Dann ist $v_i \neq w_j$ für $1 \leq i \leq m-1$ und $1 \leq j \leq n-1$. [Denn wäre $v_i = w_j$, so sind $v v_1 - v_i$ und $v w_1 - w_j$ oder $v_i v_{i+1} - v_{m-1} w$ und $w_j w_{j+1} \dots w_n w$ kürzere Wege, im Widerspruch zur Minimalität von $m+n$] Dann ist $v v_1 \dots v_{m-1} w w_{n-1} \dots w_1 v$ ein Kreis. ↯.



(b) $\Rightarrow$ (c) G ist zusammenhängend. Angenommen es gibt ein $e = \{v, w\} \in E$, so dass $G - e$ zusammenhängend ist. Sei $v v_1 \dots v_{n-1} w$ ein Weg in $G - e$ $(n \geq 2)$. Dann ist $v v_1 \dots v_{n-1} w \underbrace{v}_{e}$ ein Kreis in G ↯.

(c) $\Rightarrow$ (d) G ist kreisfrei: Ang. es gibt einen Kreis C in G. Ist e eine Kante von C, so ist $G - e$ zusammenhängend ↯ [Details: Ü]. Sei jetzt $e \in \binom{V}{2} \setminus E$, und $e = \{v, w\}$. Sei $v v_1 \dots v_{n-1} w$ ein v-w Weg in G. Dann ist $v v_1 \dots v_{n-1} w \underbrace{v}_{e}$ ein Kreis in $G + e$. Also ist G maximal kreisfrei.

(d) $\Rightarrow$ (a) z.z: G ist zusammenhängend. Seien $v, w \in V$ mit $v \neq w$. Ist $\{v, w\} \in E$, so gibt es offenbar einen v-w Weg. Sei also $e = \{v, w\} \notin E$. Dann gibt es in $G + e$ einen Kreis C. Weil G kreisfrei ist, muss C aber e enthalten. Dann ist $C - e \subseteq G$ ein v-w Weg.

Sei nun G endlich, $n = |V(G)|$ und $m = |E(G)|$.

(a) $\Rightarrow$ (e) Induktion nach n. $\underline{n=1}$: $n = 1$ und $m = 0$ ✓

$\underline{n>1,\ n-1 \to n}$ Nach Lemma 2.4(2) besitzt G ein BGM v, nach Lemma 2.4(3) ist $T' = T - v$ ein Baum, mit $|V(T')| = n-1$, $|E(T')| = m-1$.

Nach IV ist $n-1 = (m-1)+1$, also $n = m+1$.

(e) $\Rightarrow$ (a) Induktion nach n. $\underline{n=1}$ ✓

$\underline{n>1, n-1 \to n}$: Es ist $\sum_{v \in V} \deg v = 2|E| = 2m = 2n-2$. (↑ Lemma 2.1; ↑ Voraussetzung) Weil G zshg. ist, ist $\deg(v) \geq 1$ für $v \in V$. Denn muss es aber ein $v_0 \in V$ mit $\deg(v_0) = 1$ geben.

Dann ist v_0 ein Blatt, $G' := G - v_0$ erfüllt $|V(G')| = n-1$, $|E(G')| = m-1$ und, deshalb $|V(G')| = |E(G')| + 1$. Nach IV ist G' ein Baum, und nach Lemma 2.4(3) auch G. □

Def: Sei $G = (V, E)$ ein Graph. Ein Baum der Form $T = (V, E')$ mit $E' \subseteq E$ heißt Spannbaum (aufspannender Baum, engl.: spanning tree) von G.

Offensichtlich kann nur ein zshg. der Graph einen Spannbaum besitzen.

Satz 2.6 Jeder endliche, zshg. de Graph $G = (V, E)$ enthält einen Spannbaum.

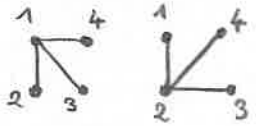
Beweis: Sei Ω die Menge aller zusammenhängenden Teilgraphen $G' \subseteq G$ für die gilt $V(G') = V$. Wegen $G \in \Omega$ ist $\Omega \neq \emptyset$. Sei $T \in \Omega$ mit $|E(T)|$ minimal. Dann ist T minimal zshg, also ein Baum.

Bem. (1) Gilt auch für unendliche Graphen ($\Leftrightarrow$ Zornsches Lemma / Auswahlaxiom)

(2) Konstruktion durch Tiefen- bzw. Breitensuche. Für gewichtete Graphen gibt es Algorithmen um einen minimalen Spannbaum (d.h. Summe der Gewichte ist minimal) zu berechnen (Alg. von Kruskal, Jarnik/Prim, Borůvka). Das ist in Anwendungen sehr wichtig!

Wie viele Spannbäume hat K_n?

markierte Spannbäume (Namen der Knoten sind wichtig)



od. unmarkierte Spannbäume (bis auf Isomorphie)

Satz 2.7 (Satz v. Cayley) K_n besitzt genau n^{n-2} markierte Spannbäume, d.h., es gibt genau n^{n-2} markierte Bäume auf n Knoten.

(Hier ohne Beweis, es gibt viele, zum Teil elementare Beweise, z.B. mit Prüferfolgen)

Graphen insgesamt: $2^{\binom{n}{2}} = 2^{\frac{n(n-1)}{2}}$

2.3 Eulersche Graphen

Def: Ein geschlossener Kantenzug in einem Graph G heißt eulersch, wenn er jede Kante genau einmal durchläuft.
G heißt eulersch, wenn er einen eulerschen Kantenzug enthält.

Inspiration: Königsberger Brückenproblem (Euler 1736)

Satz 2.8 (Euler 1736) Ein endlicher, zshg. Graph $G=(V,E)$ ist genau dann eulersch, wenn jeder seiner Knoten geraden Grad hat.

Beweis: „$\Rightarrow$" Ang. es existiert ein eulerscher Kantenzug K. Sei $v \in V$. Jede mit v inzidente Kante erscheint in K genau einmal, und hat eine entsprechende Richtung in Bezug auf K: „hinein" od. „hinaus" in/aus v. Da K geschlossen ist, gibt es gleich viele Kanten „hinein" wie „hinaus" in/aus v, also ist $\deg(v)$ gerade.

„$\Leftarrow$" Eine Tour sei ein Kantenzug in dem keine Kante mehrfach vorkommt. (Knoten dürfen mehrfach auftreten). Sei $T=(v_0, e_1, v_1, \dots, e_m, v_m)$ eine Tour größtmöglicher Länge in G.

Beh: T ist eulersch, d.h.

(i) $v_0 = v_m$, und

(ii) $\{e_1, \dots, e_m\} = E$.

zu (i): Ist $v_0 \neq v_m$, so ist v_0 zu einer ungeraden Anzahl von Kanten in T inzident. Weil $\deg v_0$ gerade ist, gibt es eine Kante $e \in E \setminus \{e_1, \dots, e_m\}$, die mit v_0 inzidiert. Ist $e=\{v', v_0\}$, so ist $(v', e, v_0, e_1, v_1, \dots, e_m, v_m)$ eine längere Tour. ↯

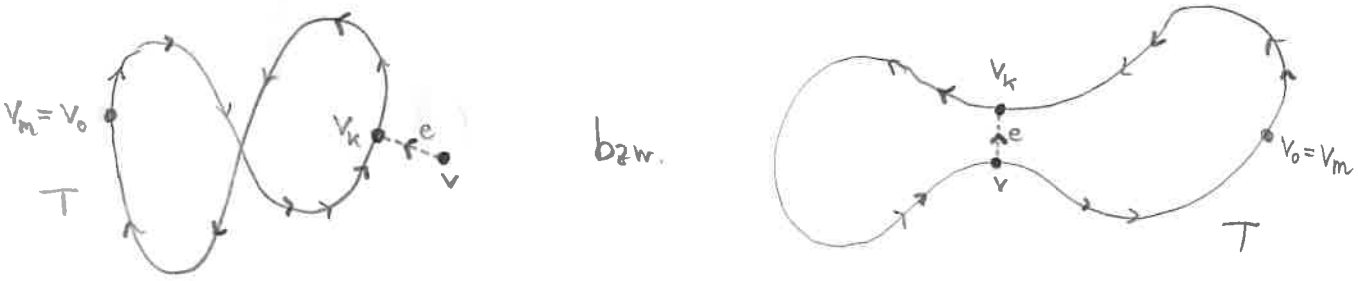
2.0 (ii) Angenommen $\{e_1, \dots, e_m\} \subsetneq E$. Weil G zshgd ist, gibt es eine Kante $e \in E \setminus \{e_1, \dots, e_m\}$, die mit einem der Knoten von T inzidiert.

[Denn: Sei $e' = \{v', w'\} \in E \setminus \{e_1, \dots, e_m\}$ beliebig. Ist $v' \in \{v_0, \dots, v_m\}$, so nehmen wir $e = e'$. Andernfalls gibt es einen v_0-v' Weg $W = w_0 w_1 \dots w_n$ mit $w_0 = v_0$ und $w_n = v'$ $n \geq 1$. Wegen $w_n \notin \{v_0, \dots, v_m\}$ gibt es ein minimales $1 \leq e \leq m$ mit $w_e \notin \{v_0, \dots, v_m\}$. Dann ist $w_{e-1} \in \{v_0, \dots, v_m\}$, und $e = \{w_{e-1}, w_e\}$ eine solche Kante.]

Sei $e = \{v_k, v\}$ mit $0 \leq k \leq m$ und $v \in V$. Dann ist

$(v, e, v_k, e_{k+1}, v_{k+1}, \dots, e_m, v_m, e_1, v_1, \dots, e_k, v_k)$

eine Tour der Länge $m+1$ ($v_m = v_0$)



2.4 Hamiltonsche Graphen

Gibt es in einem Graphen G einen geschlossenen Kantenzug, der jeden Knoten genau einmal enthält? Ist $|G| \geq 3$, so entspricht ein solcher Kantenzug einem Kreis der jeden Knoten von G enthält.

Def: Sei G ein Graph. Ein Kreis $C \subseteq G$ heißt **Hamiltonkreis**, wenn er jeden Knoten von G enthält. G heißt **hamiltonsch**, wenn er einen Hamiltonkreis enthält.

Bem: (1) Keine einfache Charakterisierung bekannt! Entscheidungsproblem ist NP-vollständig (Komplexitätstheorie)

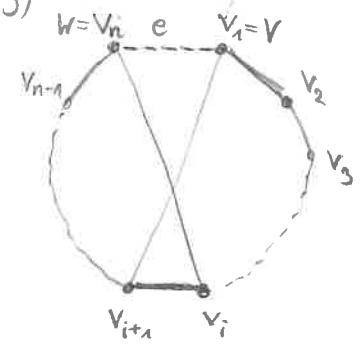
(2) Gewichtete Version: Travelling Salesman Problem → Kombinatorische Optimierung.

Satz 2.9 (Ore) Erfüllt ein endlicher Graph $G=(V,E)$ mit $|V|\geq 3$ die Bedingung $\deg(v)+\deg(w)\geq |V|$ für alle $v,w\in V$ mit $\{v,w\}\notin E$, so enthält G einen Hamiltonkreis.

Insbesondere: Erfüllt der Minimalgrad $\delta(G):=\min\{\deg(v): v\in V\}$ $(G\neq(\emptyset,\emptyset))$ die Ungl. $\delta(G)\geq \frac{|V|}{2}$, so enthält G einen Hamiltonkreis.

Beweis: (Durch Widerspruch) Angenommen es gibt einen Graph $G=(V,E)$, der die Bedingung des Satzes erfüllt, aber nicht hamiltonsch ist. Unter all solchen Graphen mit fester Knotenmenge V wählen wir einen mit $|E|$ maximal. Da K_n offensichtlich hamiltonsch ist, ist G nicht vollständig, also $E\neq\binom{V}{2}$. Sei $e=\{v,w\}\in\binom{V}{2}\setminus E$. $G+e$ enthält einen Hamiltonkreis C, und $e\in E(C)$.

Sei $C=v_1v_2\cdots v_nv_1$ mit $v_1=v$ und $v_n=w$. $(n\geq 3)$



Sei $S:=\{v_i : 1\leq i<n,\ \{v,v_{i+1}\}\in E\}$

$T:=\{v_i : 1\leq i<n,\ \{w,v_i\}\in E\}$

Wegen $v_n=w\notin S\cup T$ ist $|S\cup T|<|V|=n$.

Andererseits ist $|S|+|T|=\deg_G v+\deg_G w\geq n$, also $S\cap T\neq\emptyset$.

Sei $v_i\in S\cap T$. Dann ist

$$v_1v_2\cdots \underbrace{v_i}_{v_i\in T}v_n v_{n-1}\cdots \underbrace{v_{i+1}}_{v_i\in S}v_1 \quad \text{ein Hamiltonkreis in } G.$$

□

2.5 Planare Graphen

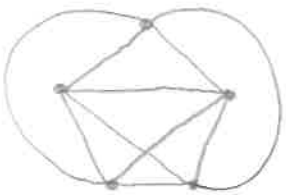
In diesem Abschnitt betrachten wir stets endliche Graphen.
Wir bleiben etwas informell: keine Problematisierung geometrischer Begriffe.

„Def" Ein Graph ist planar, wenn er sich so in der Ebene zeichnen lässt, dass sich keine Kanten schneiden (außer in den jeweiligen Knoten). Eine solche Zeichnung heißt planare Einbettung

Bsp:

K_4

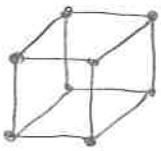
planare Einbettung



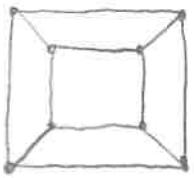
K_5

keine planare Einbettung

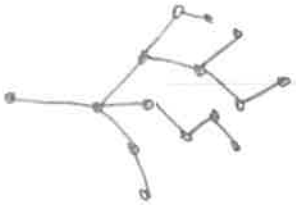
Q_3 (Würfel)



→



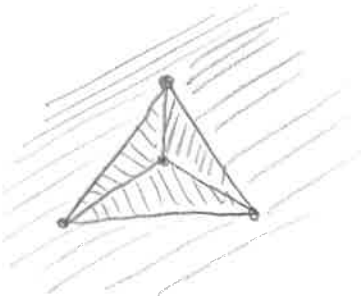
planare Einbettung



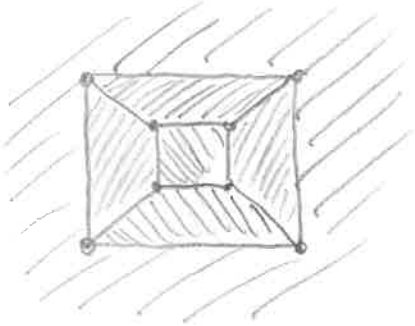
Jeder Baum / Wald ist planar

Satz 2.10 (Wagner und Fáry) Jeder planare Graph hat eine planare Einbettung, in der alle Kanten Liniensegmente sind (ohne Beweis)

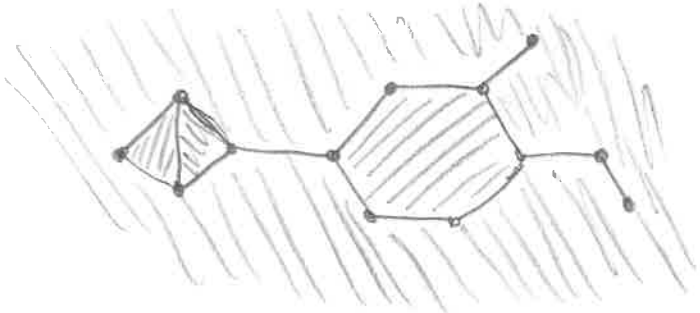
Ein Gebiet einer planaren Einbettung ist ein Teil der Ebene, den man erhält, wenn man die Ebene entlang der Kanten „zerschneidet".



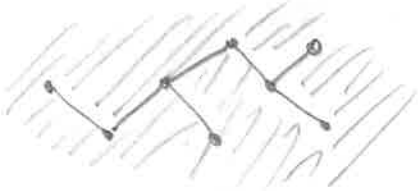
4 Gebiete: 3 beschränkte (innere) Gebiete,
1 unbeschränktes (äußeres)



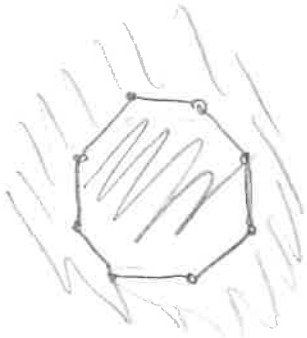
6 Gebiete



4 Gebiete



1 Gebiet



2 Gebiete

Beobachtung:
- Es gibt genau ein unbeschränktes Gebiet
- Der Rand jedes beschränkten Gebiets bildet einen Kreis des Graphen. Insbesondere hat eine planare Einbettung eines Baums/Walds genau ein Gebiet.
- Die pl. Einbettung eines Kreises hat genau zwei Gebiete. Enthält ein Graph G einen Kreis, so ist jedes Gebiet einer planaren Einbettung von G entweder vollständig im Kreis enthalten oder vollständig außerhalb. Insbesondere: Jede Kante eines Kreises grenzt an genau zwei Gebiete

[Beweis: [D]]

Satz 2.11 (Eulersche Polyederformel) Sei $G=(V,E)$ ein zshg., planarer Graph. Für jede planare Einbettung gilt

$$f = |E| - |V| + 2$$

wobei f die Anzahl der Gebiete ist. Insb. ist f unabhängig von der gewählten planaren Einbettung!

Beweis: Induktion nach $|E|$. Weil G zshg ist, gilt $|E| \geq |V|-1$ (Satz 2.3).

IA, $|E|=|V|-1$: Nach Satz 2.5 ist G ein Baum, also

$$|E| - |V| + 2 = 1 = f.$$

Sei nun $|E| > |V|-1$. Dann hat G einen Kreis C (Satz 2.5)
Sei $e \in E(C)$. $G' := G-e$ ist zshg. Aus der planaren Einbettung von G erhalten wir durch Entfernen von e eine planare Einbettung von G'. Die beiden an e grenzenden Gebiete verschmelzen dabei zu einem, also hat die planare Einbettung von G' genau $f-1$ Gebiete. Nach IV ist

$$f-1 = |E(G')| - |V(G')| + 2 = |E|-1 - |V| + 2$$

□

Satz 2.12 Für jeden planaren Graphen $G=(V,E)$ mit $|V| \geq 3$ gilt

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

Bem: Planare Graphen haben „wenige" Kanten: $|E| \in O(|V|)$

Beweis: O.E. sei G zshg. Betrachten eine planare Einbettung mit f Gebieten. Jedes Gebiet (auch das äußere) wird von mindestens 3 Kanten begrenzt. Jede Kante begrenzt höchstens zwei Gebiete. Also folgt: $3f \leq 2|E|$. Mit Satz 2.11:

$$\frac{2}{3}|E| \geq f = |E| - |V| + 2 \implies |V| - 2 \geq \frac{1}{3}|E|.$$

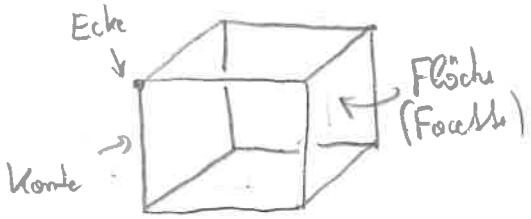
□

Kor: K_5 ist nicht planar.

Bew. K_5 hat $\binom{5}{2} = 10$ Kanten, aber $3 \cdot 5 - 6 = 9 < 10$.

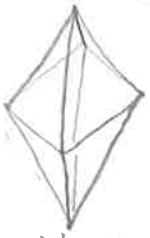
Ähnliche Argumentation: $K_{3,3}$ ist nicht planar.

Anwendung: Ein konvexer Polyeder ist eine beschränkte Teilmenge in $\mathbb{R}^3$, die sich als Schnitt endlich vieler (abgeschlossener) Halbräume schreiben lässt.



Würfel

Tetraeder



Oktaeder

	Würfel	Tetraeder	Oktaeder
E.	8	4	6
K.	12	6	12
F.	6	4	8

(*S.43)

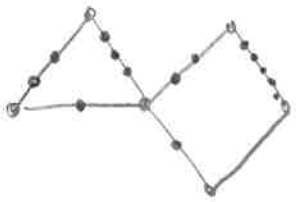
Satz 2.13 Für jeden konvexen Polyeder gilt:

$$\#\text{Ecken} - \#\text{Kanten} + \#\text{Facetten} = 2.$$

Beweisskizze: Die Ecken & Kanten des Polyeders bilden einen Graph. Dieser ist planar: Man „entfernt" eine Facette und bläht durch diese in den Polyeder. Durch Auseinanderziehen der Kanten der gewählten Facette erhält man eine planare Einbettung. Das äußere Gebiet wird durch die Kanten der gewählten Facette begrenzt. Die Anzahl der Gebiete ist die Anzahl der Facetten des Polyeders, die Beh. folgt aus Satz 2.11.

Eine Unterteilung eines Graphen $G = (\ ,\ )$ ist ein Graph G', den man durch Einfügen von Knoten entlang der Kanten von G erhält.

Bsp:



Beobachtung: G ist planar $\Leftrightarrow$ Jede Unterteilung von G ist planar.

Satz 2.14 (Kuratowski) Ein Graph ist genau dann planar, wenn er keine Unterteilung von K_5 oder $K_{3,3}$ enthält

(ohne Beweis, siehe [D])

Bsp (Kreispackungen) Wir möchten n „Münzen" so am Tisch platzieren, dass sich möglichst viele Paare berühren. Sei $B(n)$ die max. Anzahl sich berührender Paare $\Rightarrow B(n) \leq \binom{n}{2}$

$n=3$

$B(3)=3$

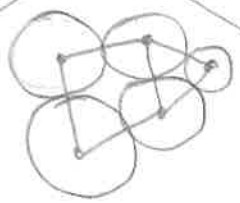
$n=4$

$B(4)=\binom{4}{2}=6$

$n=5$

$B(5)=?$

Planarer Graph (Kontaktgraph):



$\Rightarrow B(n) \leq 3n-6$

Umkehrung (Koebe-Andreev-Thurston): Zu jedem planaren Graphen G gibt es eine Kreispackung, sodass G isomorph zum Kontaktgraphen ist

ausgelassen

2.6 Bipartite Graphen

Def: Ein Graph $G=(V,E)$ heißt **bipartit**, wenn V in zwei disjunkte Mengen A, B aufgeteilt werden kann, so dass jede Kante einen Knoten aus A mit einem Knoten aus B verbindet. D.h.

$$E \subseteq \{\{a,b\} : a \in A, b \in B\} \text{ und } V = A \cup B.$$

Bsp: a) $K_{n,m}$ b)  c)  C_6, C_{2n}

d)  e)  C_5, C_{2n+1}

Satz 2.15 Folgende Aussagen sind für einen endlichen Graph $G=(V,E)$ äquivalent.

(a) G ist bipartit

(b) G enthält keinen Kreis ungerader Länge

(c) G enthält keinen geschlossenen Kantenzug ungerader Länge

Beweis: (a) $\Rightarrow$ (b) Klar, da Teilgraphen eines bipartiten Graphen wieder bipartit sind, aber C_{2n+1} für $n \geq 0$ nicht bipartit ist.

(b) $\Rightarrow$ (c) Indirekt: Ein geschl. Kantenzug *minimaler* ungerader Länge ergibt einen Kreis [Details: Ü]

(c) $\Rightarrow$ (a) Es genügt zz., dass jede Komponente von G bipartit ist. Sei also o.E. $G=(V,E)$ zshgd. Wähle $v_0 \in V$. Sei

$A = \{v \in V :$ es gibt einen v_0-v-Kantenzug gerader Länge$\}$

$B = \{v \in V :$ —"— ungerader —"$\}$

Dann ist $V = A \cup B$. zz: (i) $A \cap B = \emptyset$

(ii) Es gibt keine Kante von A nach A, bzw. von B nach B.

zu (i): Durch Widerspruch. Ang. $v \in A \cap B$. Dann gibt es einen v_0-v-Weg gerader Länge und einen ungerader Länge. Zusammenfügen ergibt einen geschl. Kantenzug ungerader Länge. $\lightning$

zu (ii) Ang $e \in E$ mit $e = \{a, a'\}$ und $a, a' \in A$.

Es gibt einen V_0-a Kantenzug gerader Länge. Erweitert man diesen mit e, erhält man einen V_0-a' Kantenzug ungerader Länge $\Rightarrow a' \in A \cap B$ ↯ (i)

Analog mit B statt A.

□

3. Zahlentheorie

3.1 Division mit Rest

$$113 : 12 = 9.4$$
$$57$$
$$9R$$

Satz 3.1 (Division mit Rest) Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Dann gibt es eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \{0, 1, \dots, b-1\}$, sodass gilt $a = bq + r$. Ist $a \geq 0$, so ist auch $q \geq 0$.

Beweis: Existenz: Sei $S = \{a - bk : k \in \mathbb{Z}\}$. Wegen $a - b(-|a|) = a + b|a| \geq 0$ ist $S \cap \mathbb{N}_0 \neq \emptyset$. Nach dem Wohlordnungsprinzip besitzt $S \cap \mathbb{N}_0$ ein Minimum. Sei $r := \min(S \cap \mathbb{N}_0)$ und $q \in \mathbb{Z}$ mit $r = a - bq$. Noch zz: $r < b$.
Angenommen $r \geq b$. Dann ist $0 \leq r - b = a - b(q+1) \in S \cap \mathbb{N}_0$, im Widerspruch zur Minimalität von r.

Eindeutigkeit: Seien $q, q' \in \mathbb{Z}$ und $r, r' \in \{0, \dots, b-1\}$ mit
$a = bq + r = bq' + r'$ (*)
$\Rightarrow r - r' = b(q' - q) \Rightarrow \underbrace{|r - r'|}_{<b} = |b|\,|q' - q| \Rightarrow |q' - q| = 0 \Rightarrow q' = q.$
Aus (*) folgt dann auch $r = r'$.

Zusatz: Ist $q < 0$, so ist auch $bq + r = \underbrace{b}_{\leq 0}\underbrace{(q+1)}_{\leq 0} - b + r < 0.$ □

Def: Seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Sind $q \in \mathbb{Z}$ und $r \in \{0, 1, \dots, b-1\}$ mit $a = bq + r$, so heißt q der Quotient und r der Rest der Division von a durch b.

Bsp: (1) Jedes $a \in \mathbb{Z}$ lässt sich darstellen in der Form $4k$, $4k+1$, $4k+2$ oder $4k+3$ mit $k \in \mathbb{Z}$. Ist a eine Quadratzahl, so gilt $a = 4k$ oder $a = 4k+1$ mit $k \in \mathbb{Z}$.

Beweis: Sei $a = b^2$ mit $b \in \mathbb{Z}$. Sei $\ell \in \mathbb{Z}$ und $s \in \{0,1\}$ mit $b = 2\ell + s$. Dann ist $b^2 = (2\ell+s)^2 = 4\ell^2 + 4\ell s + s^2 = 4\underbrace{(\ell^2 + \ell s)}_{\in \mathbb{Z}} + \underbrace{s^2}_{\in \{0,1\}}$.

(2) Keine Zahl der Form 11, 111, 1111, ... ist eine Quadratzahl.

Denn:

$$\underbrace{11\ldots111}_{n \geq 2 \text{ mal}} = \underbrace{11\ldots11}_{n-2 \text{ mal}} \cdot 100 + 11 = c \cdot 25 \cdot 4 + 11 = (c \cdot 25 + 2) \cdot 4 + 3$$

$\| \; c$

3.2 Teilbarkeit

Def Seien $a, b \in \mathbb{Z}$. b heißt teilbar durch a, in Zeichen $a \mid b$, wenn es ein $k \in \mathbb{Z}$ gibt mit $b = ak$.

Weitere Sprechweisen: „a teilt b", „b ist ein Vielfaches von a", „a ist ein Teiler von b", „a geht in b auf"

Gilt $a \mid b$ nicht, schreibt man $a \nmid b$.

Lemma 3.2 Seien $a, b, c, d \in \mathbb{Z}$.

(1) $a \mid 0$, $1 \mid a$, $a \mid a$ und $(0 \mid a \Leftrightarrow a = 0)$

(2) $a \mid b \Leftrightarrow |a| \mid |b| \Leftrightarrow \pm a \mid \pm b$

(3) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(4) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(5) Seien $k \geq 1$, $a_1, \ldots, a_k, x_1, \ldots, x_k \in \mathbb{Z}$. Ist $a \mid a_i$ für alle $1 \leq i \leq k$, so gilt $a \mid a_1 x_1 + \ldots + a_k x_k$

(6) Ist $c \neq 0$; $a \mid b \Leftrightarrow ac \mid bc$

(7) $a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$

(8) $a \mid b \wedge b \mid a \Leftrightarrow |a| = |b| \Leftrightarrow a = \pm b$.

Beweis: sehr einfache Übung!

Bem: „$|$" ist auf $\mathbb{Z}$ eine reflexive und transitive Relation. Eingeschränkt auf $\mathbb{N}$ (oder $\mathbb{N}_0$) ist „$|$" auch antisymmetrisch, also eine Ordnungsrelation.

Def Für $a \in \mathbb{Z}$ sei $T(a) := \{d \in \mathbb{N} : d \mid a\}$ die Menge der positiven Teiler von a.

Bsp: $T(\pm 6) = \{1, 2, 3, 6\}$, $T(1) = \{1\}$, $T(13) = \{1, 13\}$, $T(0) = \mathbb{N}$.

Lemma 3.2 Sei $a \in \mathbb{Z}$.

(1) $\{1, |a|\} \subseteq T(a)$, insb. $T(a) \neq \emptyset$

(2) Ist $a \neq 0$, so ist $T(a) \subseteq \{1, 2, \dots, |a|\}$. Insb. $|T(a)| < \infty$.

Beweis: (1) Lemma 3.2(1) und (2); (2) Lemma 3.2(7). □

Seien $k \geq 1$ und $a_1, \dots, a_k \in \mathbb{Z}$. Dann ist $T := T(a_1) \cap \dots \cap T(a_k)$ die Menge aller positiven gemeinsamer Teiler von $a_1, \dots, a_k$. Wegen $1 \in T$ ist $T \neq \emptyset$. Ist zumindest ein $a_i \neq 0$, so ist wegen $T \subseteq T(a_i)$ die Menge T endlich. Ist $a_1 = \dots = a_k = 0$, so ist $T = \mathbb{N}$.

Def: Seien $k \geq 1$ und $a_1, \dots, a_k$ nicht alle Null. Dann heißt

$$ggT(a_1, \dots, a_k) := \max(T(a_1) \cap \dots \cap T(a_k)) \in \mathbb{N}$$

der größte gemeinsame Teiler von $a_1, \dots, a_k$.

Bem: ·) $ggT(a) = |a|$ und $ggT(a, 0) = |a|$ für $a \in \mathbb{Z} \setminus \{0\}$.

·) $ggT(a_1, \dots, a_k) = ggT(\pm a_1, \dots, \pm a_k) = ggT(|a_1|, \dots, |a_k|)$ und der ggT hängt nicht von der Reihenfolge der Zahlen ab.

Der euklidische Algorithmus: Berechnung von $ggT(a,b)$.

Lemma 3.4 Für $a,b,k \in \mathbb{Z}$ gilt $T(a) \cap T(b) = T(a+bk) \cap T(b)$.

Insbesondere: $ggT(a,b) = ggT(a+bk, b)$

Beweis: „$\subseteq$": Sei $d \in T(a) \cap T(b) \Rightarrow d|a \wedge d|b \overset{\text{Lemma 3.2(5)}}{\Longrightarrow} d|a+bk \wedge d|b$
$\Rightarrow d \in T(a+bk) \cap T(b)$

„$\supseteq$" Sei $a' := a+bk$. Dann ist $a = a' + b(-k)$ und aus dem bereits gezeigten folgt:

$$T(a+bk) \cap T(b) = T(a') \cap T(b) \subseteq T(a' + b(-k)) \cap T(b) = T(a) \cap T(b). \quad \square$$

Sind also $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $a = bq + r$ mit $q \in \mathbb{Z}$ und $0 \le r < b$, so ist $ggT(a,b) = ggT(b,r)$. Durch mehrfaches Anwenden können wir $ggT(a,b)$ berechnen:

Bsp: $ggT(200, 140) = ggT(140, 60) = ggT(60, 20) = ggT(20, 0) = \underline{20}$

$200 = 140 \cdot 1 + 60$

$140 = 60 \cdot 2 + 20$

$60 = 20 \cdot 3 + 0$

Euklidischer Algorithmus Sei o.E. $a > b \ge 0$

$r_{-1} \leftarrow a$, $r_0 \leftarrow b$, $n \leftarrow 0$

while $r_n \neq 0$:

Seien $q_{n+1} \in \mathbb{N}_0$ und $0 \le r_{n+1} < r_n$ mit $r_{n-1} = r_n q_{n+1} + r_{n+1}$ (Div. m. Rest)

$n \leftarrow n+1$.

Ergebnis: r_{n-1}.

Der Algorithmus terminiert nach höchstens b Schleifendurchläufen, weil $b \ge \dots \ge r_n > r_{n+1} \ge \dots \ge 0$. Wegen Lemma 3.4 liefert er das korrekte Ergebnis.

Bsp: $200 \overset{(*)}{=} 140 \cdot 1 + 60$

$140 \overset{(**)}{=} 60 \cdot 2 + 20$

$60 = 20 \cdot 3 + 0$

$\Rightarrow 20 \overset{(**)}{=} 140 - 60 \cdot 2 \underset{(*)}{=} 140 - 2 \cdot (200 - 1 \cdot 140) = 3 \cdot 140 - 200$

Beobachtung: Durch Rückeinsetzen erhalten wir den erweiterten eukl. Alg.

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} = r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2} r_{n-3})$$
$$= (1 + q_{n-1} q_n) r_{n-3} - q_{n-1} r_{n-4}$$
$$= \ldots = x r_0 + y r_{-1} \quad \text{mit } x, y \in \mathbb{Z}.$$

Damit ergibt sich ein konstruktiver Beweis für

Lemma 3.5 (Bézout) Seien $a, b \in \mathbb{Z}$ mit $(a,b) \neq (0,0)$ und $d = ggT(a,b)$.
Dann gibt es $x, y \in \mathbb{Z}$ mit $d = ax + by$.

Bem: Der eukl. Alg. benötigt höchstens $5 \log_{10} b + 1$ Schritte (Lamé, 1844).

Satz 3.6 Seien $k \geq 1$, $a_1, \ldots, a_k \in \mathbb{Z}$ nicht alle 0.
Dann sind äquivalent:

(a) $d = ggT(a_1, \ldots, a_k)$

~~(b) $\forall i \in \{1, \ldots, k\}$: $d \mid a_i$ und ist $d' \in \mathbb{N}$ so dass für alle $i \in \{1, \ldots, k\}$ gilt $d' \mid a_i$, so gilt $d' \mid d$~~

~~(c) $\forall i \in \{1, \ldots, k\}$: $d \mid a_i$ und es gibt $x_1, \ldots, x_k \in \mathbb{Z}$: $d = a_1 x_1 + \ldots + a_k x_k$.~~

(b) $d \in T(a_1) \cap \ldots \cap T(a_k)$ und ist $d' \in T(a_1) \cap \ldots \cap T(a_k)$, so gilt $d' \mid d$

(c) $d \in T(a_1) \cap \ldots \cap T(a_k)$ und es gibt $x_1, \ldots, x_k \in \mathbb{Z}$: $d = a_1 x_1 + \ldots + a_k x_k$

Beweis: Wir zeigen (b) $\Rightarrow$ (a) $\Rightarrow$ (c) $\Rightarrow$ (b)

(b) $\Rightarrow$ (a): Für alle $d' \in T(a_1) \cap \dots \cap T(a_k)$ ist $d' \mid d$, also $d' \leq d$.
Wegen $d \in T(a_1) \cap \dots \cap T(a_k)$ ist $d = \max(T(a_1) \cap \dots \cap T(a_k))$

(a) $\Rightarrow$ (c): Sei $M = \{a_1 x_1 + \dots + a_k x_k : x_1, \dots, x_k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
Wegen $0 < a_1^2 + \dots + a_k^2 \in M$ ist $M \cap \mathbb{N} \neq \emptyset$. Sei $d' := \min(M \cap \mathbb{N})$ und seien $x_1, \dots, x_k \in \mathbb{Z}$ mit $d' = a_1 x_1 + \dots + a_k x_k$. Weil $d \mid a_i$ für alle $1 \leq i \leq k$, folgt $d \mid d'$ (Lemma 3.2(5)). Wir zeigen $d' \mid d$, dann ist $d = d'$ und die Aussage (c) gezeigt.

Für $1 \leq i \leq k$ sei $a_i = q_i d' + r_i$ mit $q_i \in \mathbb{Z}$, $0 \leq r_i < d'$.

$$\Rightarrow r_i = a_i - q_i d' = a_i - q_i \sum_{j=1}^{k} a_j x_j = a_i (1 - q_i x_i) + \sum_{\substack{j=1 \\ j \neq i}}^{k} a_j (-x_j q_i) \in M \cap \mathbb{N}_0$$

Wegen $d' = \min(M \cap \mathbb{N})$ ist $r_i = 0$, also $d' \mid a_i$. Es folgt $d' \leq d$ aus (a).

(c) $\Rightarrow$ (b) Seien $x_1, \dots, x_k \in \mathbb{Z}$ mit $d = a_1 x_1 + \dots + a_k x_k$ und $d \in T(a_1) \cap \dots \cap T(a_k)$. Ist $d' \in T(a_1) \cap \dots \cap T(a_k)$, so folgt $d' \mid a_1 x_1 + \dots + a_k x_k = d$. □

Definition: Sei $k \geq 2$ und seien $a_1, \dots, a_k \in \mathbb{Z}$ nicht alle 0.
$a_1, \dots, a_k$ heißen **teilerfremd**, wenn gilt $\gcd(T(a_1, \dots, a_k)) = 1$.

Bem: (1) $a_1, \dots, a_k$ sind teilerfremd $\Leftrightarrow T(a_1) \cap \dots \cap T(a_k) = \{1\}$
$\Leftrightarrow \exists x_1, \dots, x_k \in \mathbb{Z}: 1 = a_1 x_1 + \dots + a_k x_k$.

(2) Sind $a_1, \dots, a_k$ paarweise teilerfremd, so sind $a_1, \dots, a_k$ teilerfremd.
Die Umkehrung gilt nicht (z.B. 6, 10, 15 sind teilerfremd, aber keine zwei der Zahlen sind teilerfremd!)

Satz 3.7 Seien $a, b, c, d, a_1, \dots, a_k \in \mathbb{Z} \setminus \{0\}$, $k \geq 1$.

(1) $ggT(da_1, \dots, da_k) = |d| \, ggT(a_1, \dots, a_k)$

Insbesondere: Gilt $d \mid a_i$ für alle $1 \leq i \leq k$, so ist

$ggT(a_1, \dots, a_k) = |d| \Leftrightarrow ggT\left(\frac{a_1}{d}, \dots, \frac{a_k}{d}\right) = 1$.

(2) Ist $d = ggT(a,b)$, so gilt $a \mid bc \Leftrightarrow a \mid dc$

Insbesondere: Ist $ggT(a,b) = 1$, so gilt $a \mid bc \Leftrightarrow a \mid c$.

(3) Ist $ggT(a,b) = 1$, so gilt: $a \mid c \wedge b \mid c \Rightarrow ab \mid c$.

(4) Ist $ggT(a_i, b) = 1$ für alle $1 \leq i \leq k$, so ist $ggT(a_1 \cdots a_k, b) = 1$.

Insbesondere: Aus $ggT(a,b) = 1$ folgt $ggT(a^m, b^n) = 1$ für alle $m, n \geq 1$.

Beweis: (1) Sei $c = ggT(a_1, \dots, a_k) \Rightarrow |d|c \in T(da_1) \cap \dots \cap T(da_k)$

Wegen Satz 3.6 gibt es $x_1, \dots, x_k \in \mathbb{Z}$ mit $c = a_1 x_1 + \dots + a_k x_k$.

Sei $e \in \{\pm 1\}$ mit $d = e|d|$. Dann ist

$$|d|c = \sum_{i=1}^{k} a_i |d| x_i = \sum_{i=1}^{k} (a_i d) e x_i, \text{ also } |d|c = ggT(da_1, \dots, da_k) \text{ nach Satz 3.6.}$$

(2) „$\Leftarrow$" ✓ „$\Rightarrow$" Sei $d = ax + by$ mit $x, y \in \mathbb{Z}$.

$\Rightarrow dc = axc + byc$.

Wegen $a \mid axc$ und $a \mid byc$ folgt $a \mid dc$.

(3) Seien $x, y \in \mathbb{Z}$ mit $1 = ax + by$ und $m, n \in \mathbb{Z}$ mit $c = am$, $c = bn$.

$\Rightarrow c = c \cdot 1 = c(ax + by) = (ac)x + (bc)y = (ab)nx + (ab)my$

$= (ab)(nx + my)$

$\Rightarrow ab \mid c$.

(4) Seien $x_i, y_i \in \mathbb{Z}$ mit $1 = a_i x_i + b y_i$

$$\Rightarrow 1 = \prod_{i=1}^{k} (a_i x_i + b y_i) = \left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{k} x_i\right) + b \cdot M \quad \text{mit } M \in \mathbb{Z}.$$

$$\rightarrow ggT\left(\prod_{i=1}^{k} a_i, b\right) = 1.$$

„Insb.": $1 = ggT(a,b) \Rightarrow ggT(a^m, b) = 1 \Rightarrow ggT(a^m, b^n) = 1$.

□

3.3 Primzahlen und der Fundamentalsatz der Arithmetik

Definition Eine natürliche Zahl $p \in \mathbb{N}$ heißt **Primzahl**, wenn $p > 1$ gilt und 1 und p die einzigen positiven Teiler von p sind. (d.h. $p > 1$ und $T(p) = \{1, p\}$). $\mathbb{P} \subseteq \mathbb{N}$ bezeichne die Menge aller Primzahlen

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$$

Satz 3.8 Für $p \in \mathbb{N}_{\geq 2}$ sind äquivalent:

(a) $p \in \mathbb{P}$

(b) Sind $a, b \in \mathbb{Z}$ mit $p \mid ab$, so gilt $p \mid a$ oder $p \mid b$

(c) Ist $p = ab$ mit $a, b \in \mathbb{Z}$, so ist $a \in \{\pm 1\}$ oder $b \in \{\pm 1\}$. („p ist *irreduzibel*")

Beweis: (a) $\Rightarrow$ (b) Sei $p \mid ab$. Wegen $T(p) = \{1, p\}$ ist $\operatorname{ggT}(p, a) \in \{1, p\}$. Ist $\operatorname{ggT}(p, a) = p$, so ist $p \mid a$. Andernfalls ist $p \mid b$ nach Satz 3.7(2).

(b) $\Rightarrow$ (c) Aus $p = ab$ folgt $p \mid ab$. Nach Voraussetzung gilt $p \mid a$ oder $p \mid b$. O.E. $p \mid a$. Sei $k \in \mathbb{Z}$ mit $a = pk$.

$$\Rightarrow p = ab = pkb \xRightarrow{\text{kürzen}} 1 = kb \xRightarrow[k,b \in \mathbb{Z}]{} k, b \in \{\pm 1\}.$$

(c) $\Rightarrow$ (a) Sei $d \in T(p) \setminus \{1\}$ und $k \in \mathbb{Z}$ mit $p = dk$. Aus $d \neq 1$ folgt $k \in \{\pm 1\}$. Wegen $p, d > 0$ ist $k > 0$, also $k = 1$ und $p = d$. □

Lemma 3.9 Seien $p \in \mathbb{P}$ und $a_1, \ldots, a_k \in \mathbb{Z}$ $(k \geq 1)$. Ist $p \mid a_1 \cdots a_k$, so gibt es ein $1 \leq i \leq k$ mit $p \mid a_i$.

Beweis: Induktion nach k mit Satz 3.8(b). □

Lemma 3.10 Sei $a \in \mathbb{N}_{\geq 2}$ und $p = \min(T(a) \setminus \{1\})$.

(1) $p \in \mathbb{P}$

(2) Ist $a \notin \mathbb{P}$, so ist $p \leq \sqrt{a}$

(3) $a \in \mathbb{P}$ genau dann, wenn a von keinem $b \in \mathbb{N}$ mit $1 < b \leq \sqrt{a}$ geteilt wird.

Beweis: (1) Sei $b \in T(p) \setminus \{1\}$. Aus $b \mid p$ und $p \mid a$ folgt $b \mid a$, also $p \leq b$ nach Def. von p. Da $b \mid p$ aber $b \leq p$ impliziert, folgt $p = b$. Also $p \in \mathbb{P}$.

(2) Sei $a = pb$ mit $b \in \mathbb{N}$. Wegen $a \notin \mathbb{P}$ ist $b > 1$.
$\Rightarrow p \leq b$ aufgrund der Minimalität von p.
$\Rightarrow p^2 \leq pb = a \Rightarrow p \leq \sqrt{a}$.

(3) „$\Rightarrow$" V „$\Leftarrow$" Durch Widerspruch. Angenommen $a \notin \mathbb{P}$. Nach (2) ist $p \in T(a)$ mit $1 < p \leq \sqrt{a}$.

Bem: Lemma 3.10 bildet die Grundlage des Sieb des Eratosthenes: Um alle Primzahlen $\leq N$ zu bestimmen, genügt es die Zahlen $1 \leq m \leq N$ aufzuschreiben und sukzessive die Vielfachen der Primzahlen $\leq \sqrt{N}$ zu streichen.

Satz 3.11 (Fundamentalsatz der Arithmetik) Jede natürliche Zahl $\neq 1$ lässt sich als Produkt von Primzahlen darstellen. Diese Darstellung ist, bis auf die Reihenfolge der Faktoren, eindeutig.

Explizit: Für $a \in \mathbb{N}$ gibt es $k \in \mathbb{N}_0$ und $p_1, \dots, p_k \in \mathbb{P}$ mit $a = p_1 \cdots p_k$. Ist auch $a = q_1 \cdots q_\ell$ mit $\ell \in \mathbb{N}_0$ und $q_1, \dots, q_\ell \in \mathbb{P}$, so gilt $k = \ell$ und es gibt eine Permutation $\sigma \in S_k$, sodass für $1 \leq i \leq k$ gilt: $p_i = q_{\sigma(i)}$.

Beweis: Existenz: Sei $a \in \mathbb{N}$. Induktion nach a. Ist $a = 1$, so ist a das leere Produkt (nach Def.). Sei nun $a > 1$ und die Aussage gelte für alle $a' \in \mathbb{N}$ mit $a' < a$. Nach Lemma 3.10(1) gibt es ein $p_1 \in \mathbb{P}$ mit $p_1 \mid a$. Dann ist $a = p_1 b$ mit $b < a$ (wegen $p \geq 2$). Nach IV gibt es $p_2, \dots, p_k \in \mathbb{P}$ mit $b = p_2 \cdots p_k$. Es folgt $a = p_1 \cdots p_k$.

Eindeutigkeit: Induktion nach a. Ist $a = 1$, so lässt sich a nur als das leere Produkt darstellen. (Jedes andere Produkt von Primzahlen ist > 1).

Sei $a>1$ und die Aussage gelte für alle $a' \in \mathbb{N}$ mit $a'<a$.

Angenommen $a = p_1 \cdots p_k = q_1 \cdots q_\ell$ mit $k, \ell \geq 0$, $p_1, \dots, p_k, q_1, \dots, q_\ell \in \mathbb{P}$.

Wegen $p_1 \mid a = q_1 \cdots q_\ell$ gibt es ein i, $1 \leq i \leq \ell$, mit $p_1 \mid q_i$ (Lemma 3.9).

Durch Umnummerieren der q_i's können wir o.E. annehmen $p_1 \mid q_1$.

Wegen $q_1 \in \mathbb{P}$ ist $p_1 = q_1$. Es folgt $p_2 \cdots p_k = q_2 \cdots q_\ell =: a'$ mit $a'<a$.

Nach IV ist $k=\ell$ und, o.E. nach Umnummerierung, $p_i = q_i$ für alle $2 \leq i \leq k$.

Beispiel: $12 = 2 \cdot 3 \cdot 2 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$.

Korollar: Für jedes $a \in \mathbb{N}$ gibt es eindeutig bestimmte $k \in \mathbb{N}_0$, $p_1, \dots, p_k \in \mathbb{P}$ mit $p_1 < p_2 < \dots < p_k$ und $e_1, \dots, e_k \in \mathbb{N}$, sodass gilt

$$a = p_1^{e_1} \cdots p_k^{e_k}.$$

Bem: $1 \notin \mathbb{P}$. Wäre $1 \in \mathbb{P}$, so würde man keine eindeutige Zerlegung in Primfaktoren erhalten, denn $p_1 \cdots p_k = 1 \cdot p_1 \cdots p_k = 1^n p_1 \cdots p_k$, für $n \geq 0$.

(*) $v_{p_i}(a) := e_i$ heißt p_i-adische Bewertung von a; für $p \in \mathbb{P}$ mit $p \nmid a$ ist $v_p(a) := 0$.

Satz 3.12 (Euklid) $|\mathbb{P}| = \infty$.

Beweis: Durch Widerspruch. Angenommen $|\mathbb{P}| < \infty$. Sei $\mathbb{P} = \{p_1, p_2, \dots, p_m\}$ und $a := p_1 \cdots p_m + 1$. Wegen $2 \in \mathbb{P}$ ist $a \geq 3 > 1$. Nach Lemma 3.10(1) gibt es ein $p \in \mathbb{P}$ mit $p \mid a$. Dann gibt es ein i, $1 \leq i \leq m$, mit $p = p_i$. Also folgt $p \mid a - p_1 \cdots p_m = 1$ ↯ $p \geq 2$. □

Satz 3.13 (Dirichlet, 1837) Seien $a, b \in \mathbb{Z}$ mit $\operatorname{ggT}(a,b) = 1$. Dann gibt es unendlich viele Primzahlen der Form $ak+b$ mit $k \in \mathbb{Z}$.

(ohne Beweis)

Def: Die Funktion $\pi: \mathbb{R}_{\geq 0} \to \mathbb{N}_0$,
$\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$
heißt Zählfunktion der Primzahlen

Satz 3.13 (Primzahlsatz, 1896) $\pi(x) \sim \frac{x}{\log x}$, ← natürlicher Logarithmus, Basis $e = 2{,}718\ldots$
d.h. $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1$.

3.4 Kongruenzen und Restklassen

Def: Seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißt a kongruent (zu) b modulo m, in Zeichen $a \equiv b \bmod m$, wenn gilt $m \mid a - b$; m heißt Modul der Kongruenz.

Andere Schreibweisen: $a \equiv b\ (m)$, $a \equiv b\ (\bmod m)$, $a \equiv_m b$,
$a \equiv b$ falls der Modul klar ist.

Bem: (1) $a \equiv b \bmod m \iff \exists k \in \mathbb{Z}: a = b + km$
$\iff$ a und b lassen bei Division durch m denselben Rest

(2) $\equiv_m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$

Def: Sei $m \in \mathbb{N}$. Für $a \in \mathbb{Z}$ heißt
$\overline{a} := [a] := a + m\mathbb{Z} = \{a + mk : k \in \mathbb{Z}\} = \{b \in \mathbb{Z} : a \equiv b \bmod m\}$
die Restklasse von a modulo m, a heißt Repräsentant der Restklasse $\overline{a}$,
und $\mathbb{Z}/m\mathbb{Z} := \mathbb{Z}_m := \{\overline{a} \mid a \in \mathbb{Z}\}$ der Restklassenring modulo m.

Für $a \in \mathbb{Z}$ existiert genau ein $0 \leq r < m$ mit $a \equiv r \bmod m$ (Div. mit Rest),
d.h. $\overline{a} = \overline{r}$.
$\to$ $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ hat m Elemente.

Ist $m' \mid m$, so folgt aus $a \equiv b \bmod m$ auch $a \equiv b \bmod m'$

Satz 3.14 Seien $m \in \mathbb{N}$, $a, a', b, b' \in \mathbb{Z}$ mit $a \equiv a' \bmod m$ und $b \equiv b' \bmod m$.

(1) $a \pm b \equiv a' \pm b' \bmod m$ und $ab \equiv a'b' \bmod m$.

(2) $\forall k \geq 0: \quad a^k \equiv (a')^k \bmod m$

(3) $ggT(a,m) = ggT(a',m)$

(4) Ist $c \in \mathbb{Z}$, so ist

$$ac \equiv bc \bmod m \iff a \equiv b \bmod \frac{m}{ggT(c,m)}$$

Insb: Ist $ggT(c,m)=1$, so ist $ac \equiv bc \bmod m \iff a \equiv b \bmod m$.

Beweis: (1) $m \mid a-a' \wedge m \mid b-b' \Rightarrow m \mid (a-a') \pm (b-b') = (a \pm b) - (a' \pm b')$

$\Rightarrow a \pm b \equiv a' \pm b' \bmod m$.

$ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + b'(a-a')$, also gilt $m \mid ab - a'b'$.

(2) Induktion nach k und (1).

(3) Sei $k \in \mathbb{Z}$ mit $a' = a + mk$.

$\Rightarrow ggT(a',m) = ggT(a+mk, m) \overset{\text{Lemma 3.4}}{=} ggT(a,m)$.

(4) Sei $d = ggT(c,m)$ und $m' = \frac{m}{d} \in \mathbb{N}$.

„$\Leftarrow$" Sei $k \in \mathbb{Z}$ mit $a - b = m'k \Rightarrow ac - bc = m'ck$.

Wegen $m = m'd \mid m'c$ folgt $m \mid ac - bc$.

„$\Rightarrow$" Wegen $m' \mid m$ ist $m' \mid ac - bc = (a-b)c$.

Nach Satz 3.7(1) ist $ggT(m', c) = 1$ und nach Satz 3.12) folgt $m' \mid a - b$. □

Bsp: i.A. kann man nicht kürzen, z.B.:

$2 \cdot 2 \equiv 5 \cdot 2 \bmod (6)$, aber $2 \not\equiv 5 \bmod 6$.

Aber $2 \equiv 5 \bmod 3$ (3.14(4))

Bsp: $M_n = 2^n - 1$ mit $n = 82.589.933$ ist die größte bekannte (Mersenne-) Primzahl. ($\approx 24{,}9$ Mio Dezimalstellen)

Gesucht: Letzte Dezimalziffer von M_n, d.h., $0 \le r < 10$ mit $2^n - 1 \equiv r \bmod 10$

$2^2 \equiv 4 \ (10)$, $2^3 \equiv 8 \ (10)$, $2^4 \equiv 6 \ (10)$, $2^5 \equiv 2 \ (10)$

$\Rightarrow 2^{10^k} \equiv (2^{5^k})^{2^k} \equiv 2^{2^k} \ (10)$

$2^{2^3} \equiv 2^8 \equiv (2^4)^2 \equiv 36 \equiv 6 \ (10)$ insb. $6^2 \equiv 6 \ (10)$

$\Rightarrow 2^{2^k} \equiv (2^4)^{2^{k-2}} \equiv 6^{2^{k-2}} \equiv 6 \ (10)$ für $k \ge 2$

Also: $2^n - 1 = 2^{325.899 \cdot 10^2 + 3 \cdot 10 + 3} - 1 \equiv \underbrace{(2^{10^2})^{325\,899}}_{\equiv 2^4 \equiv 6} \cdot \underbrace{2^{3 \cdot 2}}_{\equiv 64 \equiv 4} \cdot 2^3 - 1$

$\equiv 6 \cdot \underbrace{4 \cdot 8}_{\equiv 32 \equiv 2} - 1 \equiv 12 - 1 \equiv \underline{1} \bmod 10$

Satz 3.15 Sei $m \in \mathbb{N}$. $\mathbb{Z}/m\mathbb{Z}$ bildet mit den Operationen

$\bar{a} + \bar{b} := \overline{a+b}$ und $\bar{a} \cdot \bar{b} := \overline{ab}$ $\quad (a, b \in \mathbb{Z})$

einen kommutativen Ring (mit Einselement $\bar{1}$ und Nullelement $\bar{0}$).

D.h. $(\mathbb{Z}/m\mathbb{Z}, +, \bar{0})$ ist eine abelsche Gruppe, $(\mathbb{Z}/m\mathbb{Z}, \cdot, \bar{1})$ ist ein kommutatives Monoid, und es gilt das Distributivgesetz:

$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$ $\quad (a, b, c \in \mathbb{Z})$

Beweis: Einfaches nachrechnen – man muss auch die Wohldefiniertheit der Operationen überprüfen!

Satz 3.16 Seien $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Dann sind äquivalent:

(a) $aX \equiv b \bmod m$ ist lösbar, d.h., $\exists x \in \mathbb{Z}: \ ax \equiv b \bmod m$

(b) $\exists \bar{x} \in \mathbb{Z}/m\mathbb{Z}: \ \bar{a} \cdot \bar{x} = \bar{b}$

(c) Die (lineare) Diophantische Gl. $aX + mY = b$ ist lösbar, d.h., $\exists x, y \in \mathbb{Z}: \ ax + my = b$.

(d) $\mathrm{ggT}(a, m) \mid b$.

Beweis: (a) $\Leftrightarrow$ (b) ✓

(a) $\Leftrightarrow$ (c): $\exists x \in \mathbb{Z}$: $ax \equiv b \bmod m \Leftrightarrow \exists x \in \mathbb{Z}\ \exists y \in \mathbb{Z}$: $ax = b + my$.

(c) $\Rightarrow$ (d) Sei $d = ggT(a,m)$ und $b = ax + my$ mit $x, y \in \mathbb{Z}$
$d \mid a \wedge d \mid m \Rightarrow d \mid b$.

(d) $\Rightarrow$ (c) Sei $d = ggT(a,m)$. Nach Satz 3.6 gibt es $x_0, y_0 \in \mathbb{Z}$: $d = ax_0 + by_0$.
Sei $k \in \mathbb{Z}$ mit $b = dk \Rightarrow b = a(\underbrace{x_0 k}_{:= x_0}) + b(\underbrace{y_0 k}_{:= y})$. □

Def Sei R ein kommutativer Ring (mit Eins).

(1) $a \in R$ heißt Einheit (od. invertierbar), wenn es ein $b \in R$ gibt, so dass gilt $ab = 1$.

(2) $R^\times = \{a \in R : a \text{ ist Einheit}\}$ heißt Einheitengruppe von R.

(3) R heißt Körper, wenn $R \setminus \{0\} = R^\times$.

Bem: (1) $1 \in R^\times$ und $0 \in R^\times \Leftrightarrow 0 = 1 \Leftrightarrow R = \{0\}$, der Nullring.
Der Nullring ist kein Körper!

(2) $R^\times$ ist bzgl. $\cdot$ eine abelsche Gruppe, a^{-1} bezeichnet das zu a inverse Element und $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ für $a, b \in R^\times$.

Bsp: $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

Satz 3.17 Sei $m \in \mathbb{N}$.

(1) $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} : ggT(a,m) = 1\}$

(2) $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\Leftrightarrow m \in \mathbb{P}$.

Beweis: (1) nach Satz 3.16. hat $\bar{a}\bar{x} = \bar{1}$ genau dann eine Lsg. wenn $ggT(a,m) = 1$.

(2) „$\Leftarrow$" Sei $m = p \in \mathbb{P}$ und $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{a} \neq \bar{0}$. Dann ist $p \nmid a$.
Wegen $ggT(p,a) \in T(p) = \{1, p\}$ folgt $ggT(p,a) = 1$, also $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

„$\Rightarrow$" Indirekt. Angenommen $m \notin \mathbb{P}, m \neq 2$. Dann ist $m = kl$ mit $1 < k, l < m$.
Wegen $ggT(k,m) = k > 1$ ist $\bar{k} \notin (\mathbb{Z}/m\mathbb{Z})^\times$, aber $\bar{k} \neq \bar{0}$, denn $m \nmid k$.

$m = 1$: $\mathbb{Z}/1\mathbb{Z} = \{\bar{0}\}$ ist kein Körper. □

3.4. Chinesischer Restsatz

Satz 3.17 (CRT) Sei $k \in \mathbb{N}$ und seien $m_1, \dots, m_k \in \mathbb{N}$ paarweise teilerfremd. Sind $a_1, \dots, a_k \in \mathbb{Z}$, so hat das Kongruenzsystem

$$x \equiv a_i \bmod m_i \quad \text{für alle } 1 \le i \le k$$

eine Lösung. Diese ist eindeutig modulo $m := m_1 \cdots m_k$.

(D.h. $\exists x \in \mathbb{Z}: \forall i \in \{1, \dots, k\}: x \equiv a_i \bmod m_i$. Ist $x' \in \mathbb{Z}$ eine weitere solche Zahl, so gilt $x \equiv x' \bmod m$)

Beweis: **Existenz:** Für $1 \le i \le k$ sei $t_i := \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j = \frac{m}{m_i}$.

Satz 3.7(4) $\Longrightarrow \operatorname{ggT}(m_i, t_i) = 1 \rightsquigarrow \exists y_i \in \mathbb{Z}: t_i y_i \equiv 1 \bmod m_i$.

Sei $x := \sum_{j=1}^{n} a_j y_j t_j$. Dann ist für alle $1 \le i \le k$

$$x = a_i \underbrace{y_i t_i}_{\equiv 1} + \sum_{\substack{j=1 \\ j \neq i}}^{k} a_j \underbrace{y_j t_j}_{\equiv 0} \equiv a_i \cdot 1 \equiv a_i \bmod m_i.$$

Eindeutigkeit: Zeigen zeigt durch Induktion nach k: Ist $b \in \mathbb{Z}$ und $m_i \mid b$ für $1 \le i \le k$, so ist $m_1 \cdots m_k \mid b$.

$k=1$: ✓

$k>1, k-1 \to k$: $m_1 \cdots m_{k-1} \mid b$ und $m_k \mid b$. Nach Satz 3.7(4) ist $\operatorname{ggT}(m_k, m_1 \cdots m_{k-1}) = 1$. Nach Satz 3.7(3) folgt $m_1 \cdots m_k \mid b$.

Nun folgt: $x \equiv a_i \equiv x' \bmod m_i$ für $1 \le i \le k$, also $m_i \mid x - x'$

$\Rightarrow m \mid x - x' \Rightarrow x \equiv x' \bmod m$. □

Beispiel: Finde alle $x \in \mathbb{Z}$ mit $x \equiv 2 \bmod 3$, $x \equiv 4 \bmod 5$ und $x \equiv 3 \bmod 7$.

t_i's: $5 \cdot \underbrace{7}_{=35} \equiv 2 \cdot 1 = 2 \bmod 3$, $\underbrace{3 \cdot 7}_{=21} \equiv 3 \cdot 2 \equiv 1 \bmod 5$,

$3 \cdot \underbrace{5}_{=15} \equiv 1 \bmod 7$

y_i's: $2 \cdot 2 \equiv 1 \bmod 3$.

Also: $x = \underline{2} \cdot \underline{2} \cdot \underline{35} + \underline{4} \cdot 1 \cdot 21 + \underline{3} \cdot 1 \cdot 15 = 140 + 84 + 45 = 269$

Die Lösungsmenge ist $\underbrace{5 \cdot 7}_{=35}$-also $269 + 105\mathbb{Z} = 59 + 105\mathbb{Z}$

Def: Seien R, S (kommutative) Ringe (mit Eins).

(1) Eine Abbildung $f: R \to S$ heißt (Ring-)Homomorphismus wenn für alle $r, r' \in R$ gilt:

$$f(r+r') = f(r) + f(r'), \quad f(rr') = f(r)f(r') \quad \text{und} \quad f(1_R) = 1_S.$$

(2) Ein Homomorphismus $f: R \to S$ heißt Isomorphismus, wenn f bijektiv ist.

Bem: (1) Ist $f: R \to S$ ein Isomorphismus von Ringen, so ist $f^{-1}: S \to R$ ein Ringhomomorphismus.

(2) Ist $f: R \to S$ ein Homomorphismus, so gilt $f(R^\times) \subseteq S^\times$

[denn: Sei $r \in R^\times \Rightarrow 1_R = rr^{-1} \Rightarrow 1_S = f(1_R) = f(rr^{-1}) = f(r)f(r^{-1})$, also $f(r) \in R^\times$ mit $f(r)^{-1} = f(r^{-1})$.]

Ist f ein Isomorphismus, so gilt sogar $f(R^\times) = S^\times$ [denn $f^{-1}(S^\times) \subseteq R^\times$], und $f|_{R^\times}: R^\times \to S^\times$ ist ein Isomorphismus der Einheitengruppen. Insb: $R^\times \cong S^\times$.

(3) Sind $R_1, \dots, R_k$ ($k \geq 1$) kommutative Ringe (mit Eins), so ist $R_1 \times \dots \times R_k$ ein kommutativer Ring (mit Eins), wobei

$$(a_1, \dots, a_k) + (b_1, \dots, b_k) := (a_1 + b_1, \dots, a_k + b_k), \quad (a_1, \dots, a_k)(b_1, \dots, b_k) := (a_1 b_1, \dots, a_k b_k)$$

und $(1_{R_1}, \dots, 1_{R_k})$ das Einselement ist.

Es ist $(R_1 \times \dots \times R_k)^\times = R_1^\times \times \dots \times R_k^\times$, und für $(a_1, \dots, a_k) \in R_1^\times \times \dots \times R_k^\times$ gilt $(a_1, \dots, a_k)^{-1} = (a_1^{-1}, \dots, a_k^{-1})$.

Satz 3.18 Sei $k \in \mathbb{N}$ und seien $m_1, \dots, m_k \in \mathbb{N}$ paarweise teilerfremd und $m := m_1 \cdots m_k$.

Dann gibt es einen Isomorphismus von Ringen

$$f: \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}, \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}),$$

und einen Gruppenisomorphismus

$$f^\times \begin{cases} (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/m_k\mathbb{Z})^\times, \\ a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \dots, a + m_k\mathbb{Z}) \quad (\text{ggT}(a,m) = 1) \end{cases}$$

Beweis: Wohldefiniertheit von f: Seien $a, a' \in \mathbb{Z}$ mit $a+m\mathbb{Z} = a'+m\mathbb{Z}$.

$\Leftrightarrow$ $\forall i \in \{1,\dots,k\}$: $a+m_i\mathbb{Z} = a'+m_i\mathbb{Z}$.

$m \mid a-a' \wedge m_i \mid m \Rightarrow m_i \mid a-a'$ ✓

f ist Ringhomomorphismus: nachrechnen (einfach), z.B. Seien $a, b \in \mathbb{Z}$

$$\Rightarrow f((a+m\mathbb{Z})(b+m\mathbb{Z})) = f(ab+m\mathbb{Z}) = (ab+m_1\mathbb{Z},\dots,ab+m_k\mathbb{Z}) =$$

$$= (a+m_1\mathbb{Z},\dots,a+m_1\mathbb{Z})(b+m_1\mathbb{Z},\dots,b+m_k\mathbb{Z}) = f(a+m\mathbb{Z})\,f(b+m\mathbb{Z}).$$

[...]

f ist bijektiv: Injektivität: Sei $f(a+m\mathbb{Z}) = f(b+m\mathbb{Z})$ mit $a, b \in \mathbb{Z}$

$\Rightarrow \forall i \in \{1,\dots,k\}$: $a+m_i\mathbb{Z} = b+m_i\mathbb{Z} \Rightarrow a \equiv b \bmod m_i$.

$\overset{\text{Sol}_2 3.17}{\Longrightarrow}$ a, b lösen beide das System $X \equiv b \bmod m_i$

$\Rightarrow a \equiv b \bmod m \Rightarrow a+m\mathbb{Z} = b+m\mathbb{Z}$.

Surjektivität: Da f eine injektive Abb. zwischen endlichen Mengen gleicher Mächtigkeit ist, ist f auch surjektiv

ODER: Seien $a_1,\dots,a_k \in \mathbb{Z}$. Nach Sol_2 3.17 gibt es ein $x \in \mathbb{Z}$ mit $x+m_i\mathbb{Z} = a_i+m_i\mathbb{Z}$ für alle $1 \le i \le k$. Dann ist

$$f(x+m\mathbb{Z}) = (a_1+m_1\mathbb{Z},\dots,a_k+m_k\mathbb{Z})$$

□

Bsp: $\mathbb{Z}/60\mathbb{Z} \overset{\simeq}{\nearrow} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

$60 = 5 \cdot 4 \cdot 3$

und $(\mathbb{Z}/60\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$ hat 16 Elemente

$\{\bar{1},\bar{3}\}$ $\quad$ $\{\bar{1},\bar{2}\}$ $\quad$ $\{\bar{1},\bar{2},\bar{3},\bar{4}\}$

3.5 Prime Restklassen

Def: Die Eulersche Phi-Funktion $\varphi: \mathbb{N} \to \mathbb{N}$ sei definiert durch $\varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^\times| = |\{a \in \{0,1,\dots,m-1\} : \operatorname{ggT}(a,m)=1\}|$

Bsp: $\forall p \in \mathbb{P}: \varphi(p) = p-1$, da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist

Satz 3.19 (Euler 1763) Sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,m)=1$. Dann gilt $a^{\varphi(m)} \equiv 1 \bmod m$.

Beweis: zz: $\bar{a}^{\varphi(m)} = 1$ in $\mathbb{Z}/m\mathbb{Z}$

Die Funktion $\mu_{\bar{a}}: \begin{cases} (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \\ \bar{x} \mapsto \bar{a}\cdot\bar{x} \end{cases}$ ist wohldefiniert (da $\bar{a}\bar{x} \in (\mathbb{Z}/m\mathbb{Z})^\times$) und bijektiv (mit $\mu_{\bar{a}^{-1}}: \begin{cases} (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \\ \bar{y} \mapsto \bar{a}^{-1}\bar{y} \end{cases}$ die Umkehrfunktion ist)

$$\Rightarrow \prod_{\bar{x}\in(\mathbb{Z}/m\mathbb{Z})^\times} \bar{x} = \prod_{\bar{x}\in(\mathbb{Z}/m\mathbb{Z})^\times} \mu_{\bar{a}}(\bar{x}) = \prod_{\bar{x}\in(\mathbb{Z}/m\mathbb{Z})^\times} \bar{a}\cdot\bar{x} = \bar{a}^{|(\mathbb{Z}/m\mathbb{Z})^\times|} \prod_{\bar{x}\in(\mathbb{Z}/m\mathbb{Z})^\times} \bar{x} = \bar{a}^{\varphi(m)} \prod_{\bar{x}\in(\mathbb{Z}/m\mathbb{Z})^\times} \bar{x}$$

$$\Rightarrow \bar{a}^{\varphi(m)} = 1.$$

□

Satz 3.20 (Kleiner Satz v. Fermat 1640) Seien $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist $a^{p-1} \equiv 1 \bmod p$.

Insbesondere: $a^p \equiv a \bmod p$ für alle $a \in \mathbb{Z}$.

Beweis: Satz 3.19 mit $m=p$ und $\varphi(p) = p-1$.

Insb.: Falls $p \nmid a$: $a^{p-1} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$.

Falls $p \mid a$: $a^p \equiv 0 \equiv a \bmod p$.

□

Bsp: 11^{104} modulo 17 berechnen: $\varphi(17) = 16$

und $104 = 6 \cdot 16 + 8$

$\Rightarrow 11^{104} \equiv 11^{6 \cdot 16} 11^8 \equiv 11^8 \mod 17$

$11^2 \equiv (-6)^2 \equiv 36 \equiv 2 \mod 17$

$\Rightarrow 11^8 \equiv 2^4 \equiv -1 \mod 17$, also $11^{104} \equiv -1 \equiv 16 \mod 17$.

Bem: Anwendungen bei Primzahltests ($a^{m-1} \not\equiv 1 \mod m \Rightarrow m \notin \mathbb{P}$) und in der Kryptografie. (RSA-Verfahren)

Satz 3.21 Ist $m = p_1^{e_1} \cdots p_r^{e_r}$ mit $p_1 < p_2 < \dots < p_r \in \mathbb{P}$ und $e_1, \dots, e_r \in \mathbb{N}$, so gilt $\varphi(m) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$

Insb.: Für $p \in \mathbb{P}$, $e \in \mathbb{N}$ gilt $\varphi(p^e) = p^{e-1}(p-1)$

Beweis: $p_1^{e_1}, \dots, p_r^{e_r}$ sind pw. teilerfremd. Darum gilt (Satz 3.18)

$$\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times\right| \cdot \dots \cdot \left|(\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times\right|$$

$$= \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$$

Es genügt also $\varphi(p^e) = p^{e-1}(p-1)$ für $p \in \mathbb{P}$, $e \in \mathbb{N}$ zu zeigen.

$\mathbb{Z}/p^e\mathbb{Z} = \{\bar{x} : 1 \le x \le p^e\}$ hat p^e Elemente

$M := \{\bar{x} \in \mathbb{Z}/p^e\mathbb{Z} : \bar{x} \notin (\mathbb{Z}/p^e\mathbb{Z})^\times\} = \{\bar{x} : 1 \le x \le p^e, \ ggT(x, p^e) > 1\}$

$= \{\bar{x} : 1 \le x \le p^e, \ p \mid x\} = \{\overline{py} : 1 \le y \le p^{e-1}\}$

$\Rightarrow |M| = p^{e-1}$

$\rightsquigarrow \left|(\mathbb{Z}/p^e\mathbb{Z})^\times\right| = \left|(\mathbb{Z}/p^e\mathbb{Z})\right| - |M| = p^e - p^{e-1} = p^{e-1}(p-1)$.

□

~ ENDE ~