§1 Mengen, Logik und Beweismethoden

1.1 Def.

Eine Menge ist eine Ansammlung von wohlbestimmten Elementen.

Bsp.:

- die Buchstaben des Alphabets $A = \{a, b, c, \dots, z\}$
- $B = \{$ Hörer der Vorlesung $\}$
- $C = \{2, 3, 5, 7\} = \{p \mid p \text{ Primzahl} \leq 10\}$

Wir können Elemente aufzählen oder charakt. Eigenschaft der Elemente angeben.

Spezielle Mengen:

$\emptyset = \{\} \neq \{0\}$

$\mathbb{N} = \{0, 1, 2, \dots\}$ natürliche Zahlen

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ ganze Zahlen

$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ rationale Zahlen

$\mathbb{R} = \{$ nicht notwendig period. Dezimalzahlen $\}$ reelle Zahlen

Ist x ein Element von M, dann schreiben wir $x \in M$.

Ist jedes Element einer Menge N auch Element von M, dann heißt N Teilmenge von M : $N \subset M$ (auch gebr. $N \subseteq M$). $N \subsetneq M$ heißt: N ist echt kleinere Teilmenge. $N \not\subset M$: N ist keine Teilmenge.

1.2 Def.

Mit $|M|$ bezeichnen wir die Anzahl der Elemente einer Menge M.

Bsp.:

$|\emptyset| = 0$, $|\{0\}| = 1$

$|\{a, b, c, \dots, z\}| = 26$

Hat M unendlich viele Elemente, dann $|M| = \infty$

Andere Schreibweise: $\#M = |M|$

Bsp.:

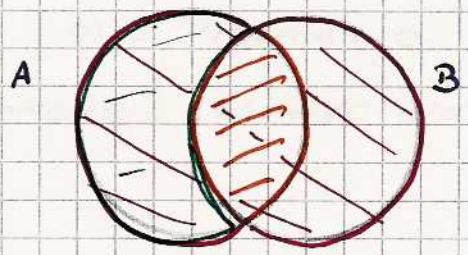
$\#\{\text{Hörer der Vorlesung} \mid \text{Alter} \geq 40\} = 0$

1.3 Durchschnitte, Vereinigung, Differenz

$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$

$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$

$A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$



2 Mengen heißen <u>disjunkt</u>, wenn $A \cap B = \emptyset$.

<u>Für disjunkte Mengen gilt:</u>

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

allgemein:

$|A \cup B| + |A \cap B| = |A| + |B|$ (Durchschnitt wird 2x gezählt)

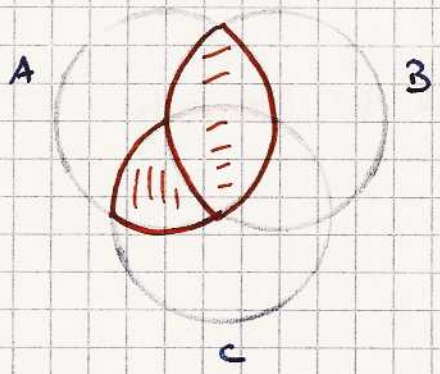
Bsp.: $A = \{1,2,3\}$, $B = \{3,4,5,6\}$ $|A| = 3$, $|B| = 4$

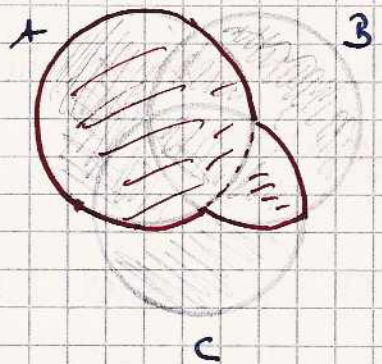
$A \cup B = \{1,2,3,4,5,6\}$, $A \cap B = \{3\}$ $|A \cup B| = 6$, $|A \cap B| = 1$

Distributivgesetze:

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

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





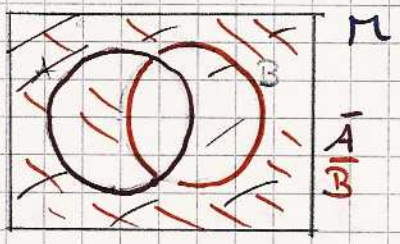
Betrachten wir Teilmengen einer festen Menge M, so heißt zu $A \subset M$

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

das Komplement

Gesetze von De Morgan

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



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

$\overline{(\bar{A})} = A$

1.4. Kartesisches Produkt, Potenzmenge

Def:

Seien A, B Mengen. Dann heißt die Menge der Paare

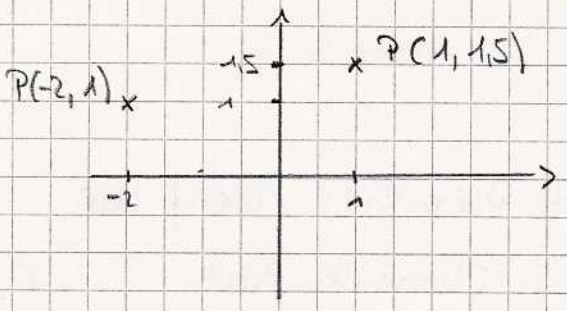
$A \times B = \{ (a,b) \mid a \in A, b \in B \}$

(kart.) Produkt von A und B

Bsp.:

$\{a, b, c, \dots, h\} \times \{1, 2, 3, \dots, 8\}$ (Schachspiel)

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a,b) \mid a \in \mathbb{R}, b \in \mathbb{R}\}$



Es gilt:

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

Def:

Sei $\mathcal{M}$ eine feste Menge. Die Potenzmenge von $\mathcal{M}$ ist

$$2^{\mathcal{M}} = \{ A \mid A \subset \mathcal{M} \}$$

1.5 Satz

Sei $\mathcal{M}$ eine endliche Menge. Dann gilt:

$$|2^{\mathcal{M}}| = 2^{|\mathcal{M}|}$$

Mit anderen Worten: Eine Menge mit n Elementen hat 2^n Teilmengen

Bsp.:

$\mathcal{M} = \emptyset$, $2^{|\emptyset|} = \{\emptyset\}$ $2^0 = 1$ ok.

$\mathcal{M} = \{1\}$, $2^{\{1\}} = \{\emptyset, \{1\}\}$ $2^1 = 2$

$\mathcal{M} = \{1,2\}$, $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ $2^2 = 4$

? (1.6) Wie beweist man dies?

Wir lernen 2 Beweismethoden kennen:

- Widerspruchsbeweis
- Beweis durch vollständige Induktion

Satz 1.5 beweist man mit vollständiger Induktion.

Zunächst ein Beispiel für einen Widerspruchsbeweis:

Grundschema:
- wollen eine Aussage A beweisen
- nehmen an, A ist nicht wahr
- folgern den Widerspruch
- also muß A wahr sein

Bsp.:

Erinnerung $p \in \mathbb{N} \geq 2$ heißt Primzahl, wenn die Menge der Teiler von p nur 2 Elemente hat: $\{1, p\}$

1.7 Satz

Es gibt unendlich viele Primzahlen

Beweis (Euklid)

Angenommen, es gibt endlich viele Primzahlen, etwa die Zahlen $p_1, \dots, p_n$

Betrachte $q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

Dann wird q von keinem p_i geteilt. Also hat q einen Primteiler p, der in $\{p_1, \dots, p_n\}$ nicht vorkommt. Widerspruch!

1.8 Aussagenlogik

In komplizierten Beweisen und für die Formalisierung auf dem Computer ist eine knappe Schreibweise nützlich.

Seien A und B Aussagen. Dann ist

$A \wedge B$: "A und B sind wahr"

$A \vee B$: "A oder B (oder beide Aussagen) sind wahr"

$A \Rightarrow B$: "Wenn A wahr ist, ist auch B wahr"
"A impliziert B"

$A \Leftrightarrow B$: "A ist genau dann wahr, wenn B wahr ist"
"A äquivalent zu B"

Einige Gesetze:

Wenn $A \Rightarrow B$ und $B \Rightarrow C$ gilt, dann gilt $A \Rightarrow C$

anders: Die Aussage

$$[((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)]$$

ist immer wahr.

$A \Rightarrow B$ darf mit $B \Rightarrow A$ nicht verwechselt werden

Bsp.

A: "Die Schranke ist zu"

B: "Ein Zug fährt durch"

$A \Rightarrow B$ gilt nicht : Die Schranke ist vorher zu

$B \Rightarrow A$ ist hoffentlich wahr

$\neg A$ heißt "A gilt nicht"

Also $A \vee \neg A$ ist immer wahr

$A \Rightarrow B = (\neg A) \vee B$

1.9 Gesetz von De Morgan

$$\neg(A \vee B) = (\neg A) \wedge (\neg B)$$
$$\neg(A \wedge B) = (\neg A) \vee (\neg B)$$

Wollen wir die Gültigkeit dieser Gesetze einsehen, so können wir A und B als Variable ansehen, die die Werte "wahr" oder "falsch" annehmen können.

Übrigen: wahr = 1, falsch = 0

Verknüpfungstafeln:

$A \wedge B$	B 0	1
A 0	0	0
1	0	1

$A \vee B$	B 0	1
A 0	0	1
1	1	1

A	$\neg A$
0	1
1	0

A	B	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$	$A \vee B$	$\neg(A \vee B)$
0	0	1	1	1	0	1
1	0	0	1	0	1	0
0	1	1	0	0	1	0
1	1	0	0	0	1	0

Sind gleich

1.10 Distributivgesetze

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

Kommutativgesetz

$A \wedge B = B \wedge A$

$A \vee B = B \vee A$

Assoziativgesetz

$A \vee (B \vee C) = (A \vee B) \vee C$

$A \wedge (B \wedge C) = (A \wedge B) \wedge C$

1.M $[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$ $\quad (x \Rightarrow y) = \neg x \vee$

$= \neg [(A \Rightarrow B) \wedge (B \Rightarrow C)] \vee (A \Rightarrow C)$

$= \neg [(\neg A \vee B) \wedge (\neg B \vee C)] \vee (\neg A \vee C)$

de Morgan

$= \neg (\neg A \vee B) \vee \neg (B \vee C) \vee (\neg A) \vee C$

$= (A \wedge \neg B) \vee (B \wedge \neg C) \vee (\neg A) \vee C$

$= [(A \wedge \neg B) \vee (\neg A)] \vee [(B \wedge \neg C) \vee C]$

$= [(A \vee \neg A) \wedge (\neg B \vee \neg A)] \vee [(B \vee C) \wedge (\neg C \vee C)]$

$= [1 \wedge (\neg B \vee \neg A)] \vee [(B \vee C) \wedge 1]$

$= (\neg B \vee \neg A) \vee (B \vee C)$

$= (\neg B \vee B) \vee \neg A \vee C$

$= 1 \vee \neg A \vee C$

$= 1$

$(A_1 \vee A_2 \vee A_3) \wedge (B_1 \vee B_2 \vee B_3)$

$= (A_1 \wedge B_1) \vee (A_1 \wedge B_2) \vee \ldots \vee (A_3 \wedge B_3)$

1.12 Vollständige Induktion

Für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$ sei eine Aussage $A(n)$ gegeben,

gilt:

1) Induktionsanfang: $A(1)$ ist wahr

2) Induktionsschluß: $[A(n) \Rightarrow A(n+1)]$ ist wahr

Dann gelten die Aussagen $A(n)$ für alle $n \in \mathbb{N}_{\geq 1}$.

1.13 Bsp.:

Beweis von Satz 1.5

Betrachte die Behauptung

$A(n)$: Eine Menge von n Elementen hat 2^n Teilmengen.

Beweis mit Induktion nach n

I.A.: $n = 1$: Es sei o.E.d.A. $M = \{1\}$ (OE)

$$2^M = \{\emptyset, \{1\}\}, \quad |2^{\{1\}}| = 2 \overset{!}{=} 2^1 \quad \text{ok.}$$

Induktionsschritt: $n \to n+1$

o.E.d.A $M = \{1, 2, \ldots, n+1\}$

$$2^M = \{A \mid A \subset M\} = \{A \subset M \mid (n+1) \in A\} \cup \{A \subset M \mid (n+1) \notin A\}$$ disjunkt!?

$$= \{A \mid A = A' \cup \{n+1\}\} \cup \{A \mid A \subset \{1, \ldots, n\}\}$$
und $A' \subset \{1, \ldots n\}$

$$|2^M| = |\{A \mid A = A' \cup \{n+1\}, A' \subset \{1, \ldots, n\}\}| + |\{A \mid A \subset \{1, \ldots,$$

Induktionsvoraussetzung (die Aussage $A(n)$)

$$= 2^n + 2^n = 2 \cdot 2^n = 2^1 \cdot 2^n = 2^{n+1}$$

die Behauptung für $n+1$.

Damit ist Satz 1.5 bewiesen ∎

Vollständige Induktion wird oft bei Beweisen von Summen- und Produktformeln verwendet.

1.14 Summen- und Produktzeichen

$a_m, a_{m+1}, \dots, a_n \in \mathbb{R}$ seien reelle Zahlen

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \dots + a_n$$

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \dots \cdot a_n$$

falls $m \leq n$.

Für $m > n$ setzen wir

$$\sum_{k=m}^{m-1} a_k = 0$$

$$\prod_{k=m}^{m-1} a_k = 1$$

Dann gilt die Rekursionsformel

$$\sum_{k=m}^{n+1} a_k = \sum_{k=m}^{n} a_k + a_{n+1}$$

$$\prod_{k=m}^{n+1} a_k = \left(\prod_{k=m}^{n} a_k \right) \cdot a_{n+1}$$

1.15 Bsp.:

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

Beweis mit vollständiger Induktion

I.A $n = 1$

$$\sum_{k=1}^{1} k = 1 \stackrel{!}{=} \frac{1(1+1)}{2} = 1 \quad \text{ok.}$$

I.S. $n \to n+1$

$$\sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k \right) + n+1 \overset{\text{Ind.V.}}{=} \frac{n(n+1)}{2} + (n+1) = (n+1) \cdot \left(\frac{n}{2} + \right.$$

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

die Verhaupteke Formel für n+1.

Gauss

$$\begin{array}{ccccccc} 1 & + & 2 & + & 3 & + \ldots + & n \\ n & + & (n-1) & + & (n-3) & & \end{array} \Big\} 2\times$$

$$\underbrace{(n+1) \quad (n+1) \quad (n+1)}_{= n\cdot(n+1) : 2}$$

1.16 Bsp.

Sei $q \in \mathbb{R}$, $q \neq 1$

$$\sum_{k=0}^{n} q^k \quad (= q^0 + q^1 + \ldots + q^n)$$

$$= 1 + q + q^2 + \ldots + q^n$$

$$= \frac{1 - q^{n+1}}{1-q}$$

Beweis: Induktion

I. A. $(n=0)$

$$\sum_{k=0}^{0} q^k = 1 \overset{!}{=} \frac{1-q^1}{1-q} = 1 \quad \text{gilt}$$

I. S $n \to n+1$

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1}$$

$$\overset{\text{I.V.}}{=} \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1} + \overbrace{q^{n+1} - q^{n+2}}^{\text{H. N.}}}{1-q}$$

$$= \frac{1-q^{n+2}}{1-q}$$

1.17 Def.

Die Anzahl der k-elementigen Teilmengen einer Menge mit n Elementen bezeichnen wir mit

$\binom{n}{k}$ n über k

$$:= |\{A \subset \{1,\dots,n\} \mid |A| = k\}|$$

Dann ist $\binom{n}{k} = 0$ für $k > n$ und $k < 0$

1.18 Lemma Es gilt:

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

Beweis:

Für $k = 0$ und $k = n$ ist die Aussage richtig

da $1 = 1 + 0$ bzw. $1 = 0 + 1$

Sei nun $1 \le k \le n-1$

$$\{A \subset \{1,\dots,n\} \mid |A| = k\} = \{A \subset \{1,\dots,n-1\} \mid |A| = k\}$$
$$\cup \{A \mid A = A' \cup \{n\},$$
$$A' \subset \{1,\dots,n-1\},$$
$$|A'| = k-1\}$$

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

da die Vereinigung disjunkt ist.

1.19 Satz

Für $0 \le k \le n$ gilt

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

Dabei ist $m! = \prod_{k=1}^{m} k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot m$

Insbesondere: $0! = 1$

$1! = 1$

Beweis: Induktion nach n.

I.A. $n = 0$

$$\binom{0}{0} = |\{A \subset \emptyset \mid |A| = 0\}| = |\{\emptyset\}| = 1$$

$$\frac{0!}{0! \cdot 0!} = 1$$

I.S. $n \to n+1$

Für $k = 0$

$$\binom{n+1}{0} = 1 = \frac{(n+1)!}{0!\,(n+1)!} = 1 \quad \text{gilt}$$

Sei $k \geq 1$ nach Lemma 1.18

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

$$\overset{\text{I.V.}}{=} \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!}$$

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

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

□

Unmittelbar aus der Def. ist klar, daß

$$+ \sum_{k=0}^{n} \binom{n}{k} = \left|2^{\{1,\dots n\}}\right| = 2^n$$

Ferner

$$* \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Für ungerades n ist dies klar: $2^{\{1,2,\dots n\}} \ni A \mapsto \bar{A}$

$$k = |A|, \quad |\bar{A}| = n - k$$

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

$$(-1)^k = (-1)^n \cdot (-1)^{n-k} = -(-1)^{n-k} \quad \text{falls } n \text{ ungerade ist}$$

denn $(-1)^{2n} = 1$, $(-1)^{2k} = 1$

Pascalsche Dreieck

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5  10  10   5   1
```

1.20 Satz (Binomische Formel)

Für $a, b \in \mathbb{R}$ gilt:

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

Bem.: Der Fall $a = b = 1$ gibt (+)

$a = 1,\ b = -1$ gibt (+)

Beweis: Induktion nach n, $n = 1$

$$(a+b)^1 = a + b \overset{!}{=} \sum_{k=0}^{1} \binom{1}{k} a^{1-k} \cdot b^k = a+b \text{ gil}$$

$$1 \cdot a^1 \cdot b^0 + 1 \cdot a^0 \cdot b^1 = a + b$$

$n \to n+1$

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b)$$

$$\overset{\text{I.V.}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k \right) \cdot (a+b)$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^{k+1}$$

($k \to k-1$ in der zweiten Summe)

Kommutativ- u. Distributivgesetz in $\mathbb{R}$

Index schieben!

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} \cdot b^k$$

$$= \binom{n}{0} a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n+1-k} b^k + \underbrace{\binom{n}{n} a^0 \cdot b^{n+1}}_{\binom{n+1}{n+1} b^{n+1}}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k$$

§2 Abbildungen

2.1. Def.:

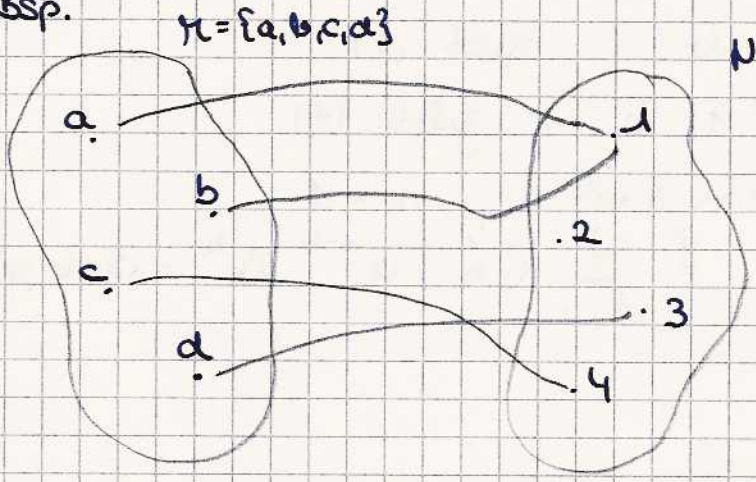
Eine Abbildung zwischen zwei Mengen M und N ist eine Vorschrift

$$f: M \to N,$$

die jedem Element x von M ein Element $f(x) \in N$ zuordnet.

Schreibweise $x \mapsto f(x)$

Bsp.



Also $a \mapsto f(a) = 1$

Für eine Teilmenge $A \subset M$ heißt $f(A) = \{ f(x) \mid x \in A \} \subset N$ das Bild von A.

Für $B \subset N$ heißt $f^{-1}(B) = \{x \in M \mid f(x) \in B\}$ das Urbild von B

Im Bsp.

$f(\{a, b\}) = \{1\}$ $\quad$ $f(\{a, c\}) = \{1, 3\}$

$f^{-1}(\{2\}) = \{\}$

Speziell: Hat B nur ein Element $B = \{y\}$, dann $f^{-1}(y) = f^{-1}(\{y\})$

$f^{-1}(1) = \{a, b\}$

Ist $f: M \to N$ eine Abbildung, $A \subset M$

$f|_A : A \to N$, $A \ni x \mapsto f(a)$

heißt Einschränkung von f auf A.

2.2. Def.

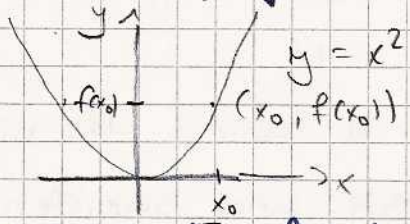
Die Menge

$$\Gamma_f = \{(x,y) \in M \times N \mid y = f(x)\}$$

heißt Graph von f.

Bsp.: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$

c)



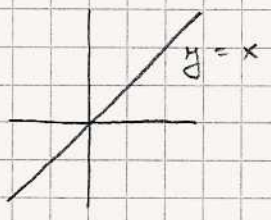
Aus dem Graphen Γ_f läßt sich f zurückgewinnen.
Zu $x_0 \in M$ ist $y_0 = f(x_0)$ der eindeutig bestimmte Punkt, so daß

$$\Gamma_f \cap (\{x_0\} \times N) = \{(x_0, y_0)\} \subset M \times N$$

2.3. Die wichtigsten Abbildungen sind reelle Funktionen $f: D \to \mathbb{R}$, $D \subset \mathbb{R}$ nicht leere Teilmenge, der Definitionsbereich

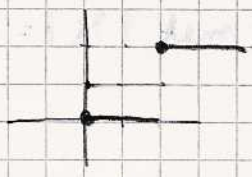
2.4. Bsp.:

a) $id_{\mathbb{R}}: \mathbb{R} \to \mathbb{R}$, $x \mapsto x$

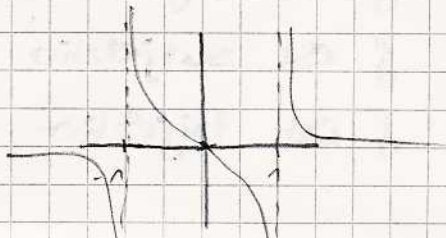


b) entier: $\mathbb{R} \to \mathbb{Z} \subset \mathbb{R}$ $\lfloor x \rfloor$

entier(x) = größte ganze Zahl $\leq x$



d) $y = \frac{x}{x^2-1}$, $D = \mathbb{R} \setminus \{\pm 1\}$



Zwei Eigenschaften von Abbildungen verdienen Namen

2.5 Def

$f: M \to N$ (eine Abbildung) heißt

injektiv, wenn $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

äquivalent: $(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$

surjektiv, wenn für alle $y \in N$ ein $x \in M$ existiert, mit $f(x) = y$

$\Leftrightarrow f(M) = N$

jedes Element in N kommt als Bildpunkt vor

bijektiv, wenn f injektiv und surjektiv ist.

Ist f bijektiv, dann heißt die Abbildung

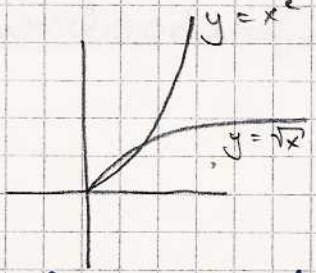
$f^{-1}: N \to M$, $y \mapsto x$, wobei $y = f(x)$,

die Umkehrabbildung.

Bsp.:

Betrachte $f: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2 = f(x)$

Umkehrabbildung $f^{-1}(y) = \sqrt{x}$



Ist $f: M \to N$ bijektiv, dann gilt

$|M| = |N|$

Umgekehrt gilt

2.6 Satz

Ist $f: M \to N$ eine Abbildung zwischen endlichen Mengen, dann sind äquivalent (mit $|M| = |N|$)

(a) f ist injektiv

(b) f ist surjektiv

(c) f ist bijektiv

Beweis

(1) $\Rightarrow$ a) $\wedge$ b) nach Def.

Bleibt a $\Leftrightarrow$ b zu zeigen

zu b $\Rightarrow$ a:

Sei f surjektiv. Dann gilt

$$|\mathbb{R}| = \sum_{n \in N} |f^{-1}(n)| \geq \sum_{n \in N} 1 = |N|$$

Da $|\mathbb{R}| = |N|$, muß $|f^{-1}(n)| = 1$

für alle n gelten. $\Rightarrow$ f ist injektiv

a) $\Rightarrow$ b): f injektiv $\Rightarrow$

$|f^{-1}(n)| \leq 1$ für alle $n \in N$

also

$$|\mathbb{R}| = \sum_{n \in N} |f^{-1}(n)| \leq \sum_{n \in N} 1 = |N|$$

und $|\mathbb{R}| = |N|$ gibt $|f^{-1}(n)| = 1$ für alle n.

d.h. f ist surjektiv

2.7 Korollar 1 (aus dem Beweis)

Ist $f: \mathbb{R} \to N$ injektiv, dann gilt

$|\mathbb{R}| \leq |N|$

Ist $f: \mathbb{R} \to N$ surjektiv, dann gilt

$|\mathbb{R}| \geq |N|$

Korollar 2 (Schubfachprinzip)

Eine Abbildung $f: \mathbb{R} \to N$ mit $|\mathbb{R}| > |N|$

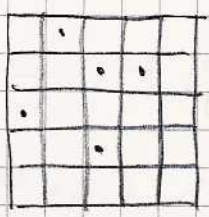
ist nicht injektiv.

2.8 Bsp.:

Für beliebige n^2+1 viele Punkte in dem Quadrat

$Q = \{(x,y) \mid 0 < x < n,\ 0 < y < n\}$

gibt es zwei mit Abstand $\leq \sqrt{2}$



Betrachte die n^2 Teilquadrate

$$Q_{ij} = \{(x,y) \mid i-1 \leq x < i, \quad j-1 \leq y < j\}$$

Nach dem Schubfachprinzip müssen in einem der n^2- Fächer zwei Punkte liegen ∎

2.10. Weitere Notation zu Abbildung

Def.

$$N^M = \{ f : M \to N \}$$

bezeichnet die Menge aller Abbildungen.

Sind M und N endlich, dann gilt

$$|N^M| = |N|^{|M|}$$

Diese Notation ist mit der Notation für die Potenzmenge verträglich.

$$\chi : 2^M \longrightarrow \{0,1\}^M$$

die Abbildung, die einer Teilmenge $A \subseteq M$ ihre char. Funktion zuordnet.

$$A \mapsto \chi_A \quad \text{mit}$$

$$\chi_A : M \to \{0,1\}$$

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

ist eine Bijektion

$$A = \chi_A^{-1}(1)$$

2.11 Def

Seien $f : M \to N$ und $g : N \to K$ Abbildungen.

Dann ist die Komposition von f und g

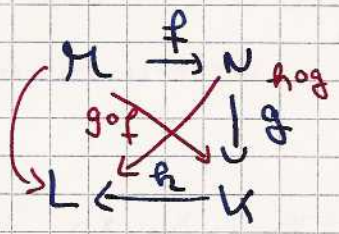
$$g \circ f : M \to K \qquad (g \text{ Kringel } f)$$

durch $(g \circ f)(m) = g(f(m))$ für $m \in M$ definiert.

Komposition von Abbildungen ist assoziativ

$f: M \to N$, $g: N \to K$, $h: K \to L$

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



denn für alle $m \in M$ gilt:

$$\begin{aligned}(h \circ (g \circ f))(m) &= h((g \circ f)(m)) \\ &= h(g(f(m))) \\ &= (h \circ g)(f(m)) \\ &= ((h \circ g) \circ f)(m)\end{aligned}$$

2.12 Existent und Allquantor

Die Phrasen "es existiert ein" und "für alle" tauchen häufig auf. Wir schreiben

$\exists$ "es existiert ein"

$\forall$ "für alle"

$\square$ Ende eines Beweises q.e.d.

Bsp.:

$f: M \to N$ ist surjektiv

$\Leftrightarrow \forall n \in N \; \exists m \in M: f(m) = n$

"mit"

Bei Negationen von logischen Aussagen vertauschen sich $\forall$, $\exists$-Quantor. (de Morgan für $\exists, \forall$)

Bsp.:

f ist nicht surjektiv

$\Leftrightarrow \neg(\forall n \in N \; \exists m \in M: f(m) = n)$

$= \exists n \in N: \neg(\exists m \in M: f(m) = n)$

$= \exists n \in N \; \forall m \in M: \neg(f(m) = n)$

$= \exists n \in \mathbb{N}\ \forall m \in \mathbb{N} : f(m) \neq n$

§3 Äquivalentrelationen und Kongruenzen

3.1 Sei $\mathbb{M}$ eine Menge. Wir wollen den Begriff von Gleichheit von Elementen zu einem Begriff von „ähnlich" oder „äquivalent" abschwächen.

Bsp.:

$f: \mathbb{M} \to N$ eine Abbildung, x_1, x_2 sind äquivalent ($x_1 \sim x_2$), wenn $f(x_1) = f(x_2)$

3.2. Def

Eine Teilmenge $R \subset M \times M$ heißt Äquivalentrelation, wenn folgendes gilt: [Schreibe $a \sim b$ für $(a,b) \in R$]

(1) Reflexivität: $a \sim a \quad \forall a \in M$

(2) Symmetrie: $a \sim b \Rightarrow b \sim a \quad \forall a, b \in M$

(3) Transitivität: $(a \sim b) \wedge (b \sim c) \Rightarrow a \sim c \quad \forall a, b, c \in M$

Bsp.:

1) Sei $M = \mathbb{Z}$ und $d \in \mathbb{Z}_{>1}$. a und b heißen kongruent modulo d ($a \equiv b \bmod d$), wenn $a - b$ durch d teilbar ist.

$\equiv \bmod d$ ist eine Äquivalentrelation

(1) • $a - a = 0 = 0 \cdot d$

(2) • $a \equiv b \bmod d$, also $a - b = \alpha \cdot d$, $\alpha \in \mathbb{Z}$

$\Rightarrow b - a = (-\alpha) d \Rightarrow b \equiv a \bmod d$

(3) • $a \equiv b$, $b \equiv c \bmod d$, also

$a - b = \alpha \cdot d$, $b - c = \beta \cdot d$, $\alpha, \beta \in \mathbb{Z}$

$\Rightarrow a - c = (a - b) + (b - c) = (\alpha + \beta) d$

$\Rightarrow \alpha \equiv c \bmod d$

2) $\mathcal{H} = \mathbb{Z}$ und die Relation $\leq$

$\leq$ ist keine Äquivalentrelation, da die Symmetrie nicht erfüllt ist.

3.3 Def und Satz

Sei $\sim$ eine Äquivalentrelation auf eine Menge $\mathcal{H}$.

Zu $a \in \mathcal{H}$ heißt

$[a] = \{ b \in \mathcal{H} \mid b \sim a \}$ die Äquivalentklasse von

Jedes Element $b \in [a]$ nennen wir einen Repräsentanten der Äquivalentklasse.

Je 2 Äquivalentklassen $[a]$ und $[b]$ sind entweder gleich oder disjunkt.

Bsp.:

$\sim$ Sei $\equiv \mod 3$

$[0] = \{ \ldots, -6, -3, 0, 3, 6, 9, \ldots \}$

$[1] = \{ \ldots, -5, -2, 1, 4, 7, 10, \ldots \}$

$[2] = \{ \ldots, -4, -1, 2, 5, 8, 11, \ldots \}$

die Restklassen bei Division mit Rest nach 3

Beweis:

Sei $[a] \cap [b] \neq \emptyset$. Dann müssen wir $[a] = [b]$ zeigen. Sei etwa $c \in [a] \cap [b]$

Dann: $c \sim a$ und $c \sim b$

Symmetrie $\Rightarrow a \sim c$, trans. $\Rightarrow a \sim b$

$\Rightarrow a \in [b]$.

Sei nun $d \in [a]$ beliebig, also $d \sim a$, $a \sim b$

$\Rightarrow d \sim b \Rightarrow d \in [b]$

Damit ist $[a] \subset [b]$ gezeigt.

Die andere Inklusion zeigt man genauso!

3.4. Def.

Sei $\sim$ eine Äquivalenzrelation auf M. Dann bezeichnet

$M/_\sim = \{ [a] \mid a \in M \} \subset 2^M$ (= Teilmenge der Potenzmenge von M)

die Menge der Äquivalenzklassen.

$\pi : M \to M/_\sim, \; a \mapsto \pi(a) = [a]$

heißt kanonische Äquivalenzklassenabbildung

kanonisch wenn keine weitere Information gegeben.

Im Bsp. $\equiv \bmod 3$

$\mathbb{Z} \to \{ [0], [1], [2] \}$

$n \mapsto$ Rest bei Division nach 3

Die Abbildung π gibt die Äquivalenzrelation zurück.

$$\pi(a) = \pi(b) \iff [a] = [b]$$

und

$$[a] = \pi^{-1}([a]) \subset M$$

$[a]$: Teilmenge von M; $[a]$: Element von $M/_\sim$

3.5 Bsp.

Konstruiere die rationalen Zahlen $\mathbb{Q} = \{ \frac{a}{b} \}$ aus den ganzen Zahlen.

Betrachte $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ und auf M die folgende Äquivalenzrelation:

$$(p_1, q_1) \sim (p_2, q_2) \iff q_2 \cdot p_1 = q_1 \cdot p_2$$

Die Äquivalenzklasse von $(p, q) \in M$ wird üblicherweise mit $p/q = [(p, q)]$ bezeichnet

$\sim$ ist in der Tat eine Äquivalentrelation:

(1) $(p,q) \sim (p,q)$ ist klar, da
$q \cdot p = p \cdot q$

(2) $(p_1,q_1) \sim (p_2,q_2)$
$\Leftrightarrow q_2 \cdot p_1 = q_1 \cdot p_2$
$\Leftrightarrow q_1 \cdot p_2 = q_2 \cdot p_1$
$\Leftrightarrow (p_2,q_2) \sim (p_1,q_1)$

(3) transitiv:
$(p_1,q_1) \sim (p_2,q_2) \sim (p_3,q_3)$
$\Rightarrow q_2 \cdot p_1 = q_1 \cdot p_2 \;,\; q_3 \cdot p_2 = q_2 \cdot p_3$

$\Rightarrow q_3 q_2 p_1 = q_3 q_2 p_2 = q_1 q_3 p_2 = q_1 q_2 p_3$
$\Rightarrow q_2 (q_3 p_1 - q_1 p_3) = 0 \quad \wedge \; q_3 (q_2 p_2 - q_1 p_2) = 0$

Da $q_2 \in \mathbb{Z} \setminus \{0\} \Rightarrow q_3 p_1 - q_1 p_3 = 0$
$\Rightarrow (p_1,q_1) \sim (p_3,q_3)$

(1) $q_2 = \frac{q_1 p_2}{p_1}$ (1) $p_2 = \frac{q_2 \cdot p_3}{q_3}$

(2) $q_2 = \frac{q_3 p_2}{p_3}$ (2) $p_2 = \frac{q_2 p_1}{q_1}$

$\Rightarrow \frac{q_1 p_2}{p_1} = \frac{q_3 p_2}{p_3}$ $\Rightarrow \frac{q_2 p_3}{q_3} = \frac{q_2 p_1}{q_1}$

$\Rightarrow q_1 p_2 p_3 = q_3 p_2 p_1$ $\Rightarrow q_2 p_3 q_1 = q_2 p_1 q_3$

Addition und Multiplikation auf $\mathbb{Q}$ definieren wir Repräsentanten weise

$$\frac{p}{q} + \frac{r}{s} := \frac{ps + qr}{qs} \quad ;$$

$$\frac{p}{q} \cdot \frac{r}{s} := \frac{pr}{qs}$$

Also wenn $\frac{p}{q} = \frac{p_1}{q_1}$, d.h. $(p,q) \sim (p_1, q_1)$, dann müssen wir zeigen, daß

$$(ps + qr,\ qs) \sim (p_1 s + q_1 r,\ q_1 s)$$

Man sagt, wir müssen zeigen, daß die Addition wohldefiniert ist.

Wir setzen voraus $q_1 p = q \cdot p_1$

und sollen

$$q_1 s(ps + qr) = qs(p_1 s + q_1 r)$$

zeigen.

$$\Leftrightarrow s^2 \cdot \underbrace{(q_1 p - q p_1)}_{=0} + sr \underbrace{(q_1 q - q q_1)}_{=0} = 0$$

ist erfüllt.

Genauso geht man bei anderen

$$(r_1, s_1) \in \frac{r}{s}$$

und bei der Multiplikation vor.

Also haben Abbildungen

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \quad , \quad \cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$$

$\mathbb{Z} \to \mathbb{Q}$ diese Abbildung ist injektiv.

$n \to \frac{n}{1}$ und respektiert $+, \cdot$

Also $\mathbb{Z} \hookrightarrow \mathbb{Q}$ $\hookrightarrow$ Inklusion

Bem.: In $\mathbb{Q}$ hat jeder Bruch $\frac{a}{b}$ einen eindeutig bestimmten Repräsentanten mit $b > 0$ und

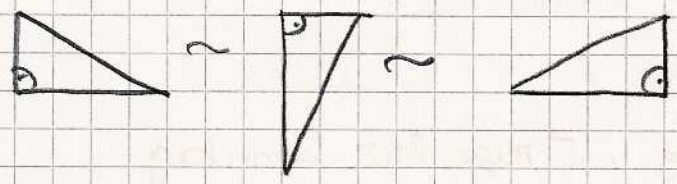
$$ggT(a,b) = 1$$

I.a. gibt es keine ausgezeichnete Repräsentanten.

Bsp.:

$\mathcal{M}$ = { Dreiecke in der Ebene }

Zwei Dreiecke sind äquivalent, wenn sie durch eine Bewegung der Ebene ineinander überführt werden (Ineinander Bewegung ≠ Spiegelung)



3.6. Wir studieren die Äquivalentrelation

$\equiv \bmod n$ genauer.

Für $\mathbb{Z}/(\equiv \bmod n)$ schreiben wir kurz $\mathbb{Z}/n$

Die Äquivalentklassen aus $\mathbb{Z}/n$ bestehen aus den Zahlen mit gleichem Rest bei Division durch n.

$\bar{i} = [i]$ ist gebräuchl.

$$\mathbb{Z}/n = \{ \bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1} \}$$

Auf $\mathbb{Z}/n$ kann man addieren und multiplizieren.

$$\bar{i} + \bar{j} = \overline{i+j}$$
$$\bar{i} \cdot \bar{j} = \overline{i \cdot j}$$

$\mathbb{Z}/n$ hat n Elemente.

$$\mathbb{Z} \to \mathbb{Z}/n$$
$$j \mapsto \bar{j}$$

Restklassenabbildung

Betrachte zwei verschiedene natürliche Zahlen $n, m > 1$ und zwei Werte a, b und frage

→ Hat die Simultane Kongruent

$$x \equiv a \bmod n$$
$$x \equiv b \bmod m$$

eine Lösung $x \in \mathbb{Z}$?

Diese Frage taucht in der Kalenderrechnung auf:
In wieviel Tagen fällt Vollmond auf einen Sonntag?

Vollmond alle 30 Tage
Sonntag alle 7 Tage

Heute ist 29.10.

letzter Vollmond 21.10.

Wollen $x \equiv 30 - 8 \mod 30$

$x \equiv 5 \mod 7$ lösen

↑ Dienstag, 5 Tage bis Sonntag

Bsp. Zahnräder

Notwendig für die Lösung des simultanen Kongruenz

$x \equiv a \mod n$

$x \equiv b \mod m$

ist $a \equiv b \mod ggT(n,m)$

Wie berechnet man den ggT?

$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ p_i Primzahlen, paarweise verschieden

$m = p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}$ und $e_i \geq 0$, $f_i \geq 0$

$\Rightarrow ggT(n,m) = \prod_{i=1}^{r} p_i^{\min(e_i, f_i)}$

3.7. Satz Euklid. Alg.

Seien $a, b \in \mathbb{Z}$. Setze $x_1 = a$, $x_2 = b$

und für $i \geq 2$ falls $x_i \neq 0$

$x_{i+1} = x_{i-1} - c_i x_i$

mit $c_i \in \mathbb{Z}$, $0 \leq x_{i+1} < |x_i|$

d. h. x_{i+1} ist der Rest von x_{i-1} bei Division durch x_i.

Dann existiert ein $n \in \mathbb{N}$, so daß $x_n \neq 0$ und $x_{n+1} = 0$ und es gilt

$d = x_n = ggT(a,b)$ ist der größte gemeinsame Teiler von a, b

(Engl. gcd greatest common divisor)

Ferner sei $u_1 = 1$, $u_2 = 0$ und $v_1 = 0$, $v_2 = 1$

und induktiv

$$u_{i+1} = u_{i-1} - c_i \cdot u_i$$

$$v_{i+1} = v_{i-1} - c_i \cdot v_i$$

definiert.

Dann gilt für $u = u_n$ und $v = v_n$

die Gleichung

$$d = ua + vb$$

Bsp.: $a = 1517$ $b = 1221$

$x_1 = 1517$

$x_2 = 1221$

$x_3 = 1517 - (1) 1221 = 296$ $c_2 = 1$

$x_4 = 1221 - (4) \cdot 296 = 37$ $c_3 = 4$

$x_5 = 296 - (8)\ 37 = 0$ $c_4 = 8$

$\Rightarrow n = 4 \Rightarrow 37 = ggT(a,b)$

$u_1 = 1$ $v_1 = 0$ $u_3 = u_1 - u_2 \cdot c_2 = 1 - 0 \cdot 1$

$u_2 = 0$ $v_2 = 1$ $v_3 = v_1 - v_2 \cdot c_2 = 0 - 1 \cdot 1$

$u_3 = 1$ $v_3 = -1$

$u_4 = 0 - 4 \cdot 1$ $v_4 = 1 - 4 \cdot (-1)$

$= -4$ $= 5$

$37 = (-4) \cdot 1517 + 5 \cdot 1221 = -6068 + 6105 = 37$ ok

Def:

$d, a \in \mathbb{Z}$

$d \mid a$ heißt "d teilt a"

Beweis:

Da $|x_2| > x_3 > x_4 > \ldots \geq 0$

bricht das Verfahren nach endlich vielem Schritten ab.

d.h. $\exists\, n$ sodaß $x_n \neq 0$ und $x_{n+1} = 0$

Dann gilt:

$d \mid x_{n-1}$, denn $x_{n-1} = c_n \cdot \underbrace{x_n}_{=d} + \underbrace{x_{n+1}}_{=0}$

Induktio mit absteigender Induktion folgt aus der Gleichung

$$x_{i-1} = c_i x_i + x_{i+1}$$

und der Ind. Vor. $d \mid x_{i+1}$, $d \mid x_i$ auch $d \mid x_{i-1}$

also $d \mid x_1 = a$ und $d \mid x_2 = b$,

d.h. d ist ein gemeinsamer Teiler von a und b.

Sei e ein weiterer Teiler. Dann gilt $e \mid x_1$ und $e \mid x_2$ und Induktio folgt $e \mid x_{i+1}$,

also $e \mid x_n = d$, d.h. d ist der größte gemeinsame Teiler.

Bleibt die Formel zu beweisen.

Wir zeigen mit Induktion

$$x_i = u_i \cdot a + v_i \cdot b$$

I.A. Für $i = 1$ und 2 ist die Formel nach Wahl von u_1, u_2, v_1, v_2 richtig

I.S. $i-1,\ i \rightsquigarrow i+1$

$$x_{i+1} = x_{i-1} - c_i x_i \overset{\text{I.V.}}{=} u_{i-1} a + v_{i-1} b - c_i (u_i a + v_i b)$$

$$= (u_{i-1} - c_i u_i) a + (v_{i-1} - c_i v_i) b$$

$$\overset{\text{Def}}{=} u_{i+1} \cdot a + v_{i+1} \cdot b$$

Also $d = x_n = u_n a + v_n \cdot b = ua + vb$ ∎

3.8. Korollar

Sei $p \in \mathbb{Z}_{>1}$. Dann sind folgende Aussagen äquivalent:

(1) p ist eine Primzahl

(2) wenn $d \mid p$ gilt und $d > 0$ gilt, dann ist $d \in \{1, p\}$

(3) Es gilt: $(p \mid a \cdot b \Rightarrow p \mid a$ oder $p \mid b)$ $\forall a, b \in$

Beweis:

(1) $\Leftrightarrow$ (2) ist die Def. von Primzahlen

(3) $\Rightarrow$ (2)

Sei (2) nicht erfüllt. Dann existiert ein Teiler a von p mit $1 < a < p$, etwa $a \cdot b = p$.

Also gilt: $p \mid a \cdot b$ und $p \nmid a$ und $p \nmid b$, da $1 < a, b < p$ gilt. Also (3) ist nicht erfüllt.

(2) $\Rightarrow$ (3)

Sei (2) erfüllt und $a, b \in \mathbb{Z}$ zwei Zahlen mit $p \mid a \cdot b$. Angenommen $p \nmid a$. Wir müssen dann $p \mid b$ zeigen. Nach Voraussetzung (2) für p gilt dann $1 = ggT(a, p) = u \cdot a + v \cdot p$ für gewisse $u, v \in \mathbb{Z}$ nach Euklid. Algorithmen. Dann gilt: $p \mid uab \Rightarrow p \mid (uab + vpb) = 1b = b$,

also $p \mid b$ ∎

3.9 Satz Fundamentalsatz der Arithmetik

Sei $n \in \mathbb{Z}$, $n \neq 0$. Dann existiert $\varepsilon \in \{1, -1\}$ und nicht notwendig verschiedene Primzahlen $p_1, \dots, p_r$, so daß

$$n = \varepsilon \cdot p_1 \cdot \dots \cdot p_r = \varepsilon \cdot \prod_{i=1}^{r} p_i$$

Die Darstellung ist eindeutig bis auf Reihenfolge von $p_1, \dots, p_r$.

Beweis:

Ist $n = 1$ dann können wir $\varepsilon = 1$ und $r = 0$ wählen.

Allgemein zeigen wir die Existenz mit Induktion nach $|n|$

Der Anfang ist klar

Ind. schritt: OE sei $n > 0$. Ist n eine Primzahl, also $n = p$, dann können wir $\varepsilon = 1$, $r = 1$ und $p_1 = p$ wählen.

Ist n keine Primzahl, dann ist $n = a \cdot b$ mit $1 < a, b < n$. Die Ind. Vor. gibt Darstellungen

$$a = p_1 \cdot \dots \cdot p_{r_a} = \prod_{i=1}^{r_a} p_i, \quad b = \prod_{j=1}^{r_b} q_j$$

Dann ist $r = r_a + r_b$ und $n = p_1 \cdot \dots \cdot p_{r_a} \cdot q_1 \cdot \dots \cdot q_{r_b}$

Zur Eindeutigkeit

OE $n > 0$

Angenommen

$$n = p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s$$

für $r, s \in \mathbb{N}$ und p_i, q_j Primzahlen.

Wir müssen $r = s$ zeigen und daß die Faktoren bis auf die Reihenfolge gleich sind.

Induktion nach r.

Für $r = 0$, also $n = 1$, muß auch $s = 0$ gelten.

Sei die Behauptung für $r-1$ schon gezeigt.

Da $p_r \mid n = q_1 \cdot \ldots \cdot q_s$

gilt $p_r \mid q_j$ für ein j (nach 3.8 (31) mit Induktion verallgemeinert.

Da q_j Primzahl ist, gilt: $q_j = p_r$

Nach Umnummerieren von $q_1, \ldots, q_s$ dürfen wir $j = s$ annehmen.

Also: $n = p_1 \cdot \ldots \cdot p_{r-1} \cdot p_r = q_1 \cdot \ldots \cdot q_{s-1} \cdot p_r$

da $q_s = p_r$

$\Rightarrow$ $p_1 \cdot \ldots \cdot p_{r-1} = q_1 \cdot \ldots \cdot q_{s-1}$

Division mit p_r

Ind. Vor. $\Rightarrow$ $r-1 = s-1$, d.h. $r = s$ und $p_1, \ldots, p_{r-1}$ und $q_1, \ldots, q_{s-1}$ sind gleich bis auf Reihenfolge

Bem.: Satz 3.9 gilt nicht in bel. Zahlbereichen

z.B. $R = \mathbb{Z}[\sqrt{-5}] = \{(a + b\sqrt{-5}) \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$

$(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3 \cdot 3$ ☒

3.10 Def. und Satz

Seien $a, b \in \mathbb{Z}_{>0}$. Dann bezeichnet

$kgV(a,b)$ das kleinste gemeinsame Vielfache von a und b (Engl.: lcm (a,b) lowest common multiple)

Das kgV existiert und

$$kgV(a,b) = \frac{a \cdot b}{ggT(a,b)}$$

Beweis:

da $\frac{a}{ggT(a,b)} \in \mathbb{Z}$ ist $l = \frac{a \cdot b}{ggT(a,b)}$ Vielfaches von b

Analog: l ist Vielfaches von a.

Sei k ein weiteres Vielfaches von a und b,

etwa $k = a \cdot n = b \cdot m$ für $m, n \in \mathbb{Z}$

Sei $d = ggT(a,b) = u \cdot a + v \cdot b$

$$\Rightarrow d \cdot k = (u \cdot a + vb)\, k$$
$$= (u \cdot m + vn)\, ab$$
$$\Rightarrow k = (u \cdot m + vn) \cdot \frac{ab}{d} = (\underbrace{um \cdot vn}) \cdot l$$

ein Vielfaches von l.

3.11 Satz Chinesischer Restsatz

Seien $n, m \in \mathbb{Z}_{>0}$. Die Kongruenten

$$x \equiv a \bmod n$$
$$x \equiv b \bmod m$$

seien haben eine gemeinsame Lösung $x \in \mathbb{Z}$

bei vorgegebenen a und $b \in \mathbb{Z}$, genau dann wenn

$$a \equiv b \bmod ggT(n,m)$$

Die Lösung $x \in \mathbb{Z}$ ist bis auf ein Vielfaches von $kgV(n,m)$ eindeutig bestimmt.

Beweis

Notwendigkeit der Bedingung ist klar. Existiert x, dann gelt $x \equiv a \bmod ggT(n,m)$

$$x \equiv b \bmod ggT(n,m)$$
$$\Rightarrow a \equiv b \bmod ggT(n,m)$$

Existent: Seien a und b gegeben. und $a \equiv b \bmod ggT(n,m) = d$

etwa $a = b + k \cdot d$

Ist $d = u \cdot n + v \cdot m$, dann ist

$x = a + k \cdot u \cdot n$ eine Lösung

$x \equiv a \bmod n$

$x = a + k \cdot u \cdot n = a + k(d \cdot vm) = b - kvm$

$\equiv b \bmod m$

Ist y eine weitere Lösung, also

$y \equiv a \bmod n$

$y \equiv b \bmod m$

$\Rightarrow x - y \equiv 0 \bmod n$

$x - y \equiv 0 \bmod m$

$\Rightarrow x - y$ ist Vielfaches von $kgV(n, m)$

Wir wollen die Kongruent

$x \equiv 30 - 14 = 16 \bmod 30$

$x \equiv 5 \bmod 7$

Notwendig: $16 \equiv 5 \bmod ggT(30, 7)$ $\quad m \;\; m$ $\quad = 1 = u \cdot n + v$

$16 + k \cdot 1 = 5$, $\quad k = -11$

Eine Lösung ist

$x = 16 + k \cdot u \cdot n = 16 - 11 \cdot u \cdot 30$

Bestimme u:

$x_1 = 30$

$x_2 = 7$

$x_3 = 30 - 4 \cdot 7 = 2 \qquad c_2 = 4$

$x_4 = 7 - 3 \cdot 2 = 1 \qquad c_3 = 3$

$x_5 = 2 - 2 \cdot 1 = 0$

$u_1 = 1 \qquad u_2 = 0 \qquad u_3 = u_1 - c_2 u_2$

$= 1 - 0 = 1$

$u_4 = 0 - 3 \cdot 1 = -3$

$x_4 = u_4 \cdot n + v_4 \cdot m$

$16 + 990 = 1006$

Alle Lösungen $1006 + i \cdot 210$

Kleinste positive Lösung : 166

Nächster Vollmond (bei 166 Tagen) = 20. April 2003

§4 Gruppen und Symmetrien

4.1 Def

Eine Menge G zusammen mit einer Verknüpfung $\circ$,

d.h. eine Abbildung

$$G \times G \to G$$

$$(a, b) \mapsto a \circ b$$

heißt Gruppe, wenn folgende Axiome erfüllt sind:

(G1) Die Verknüpfung ist assoziativ

$$(a \circ b) \circ c = a \circ (b \circ c) \quad \forall\, a, b, c \in G$$

(G2) Es existiert ein neutrales Element

$e \in G$ mit $a \circ e = a \quad \forall\, a \in G$

(G3) Zu jedem $a \in G$ existiert ein Element $a' \in G$

mit $a \circ a' = e$

Gilt darüberhinaus

(G4) Die Verknüpfung ist kommutativ

$$a \circ b = b \circ a \quad \forall\, a, b \in G,$$

dann heißt die Gruppe abelsch

[N.H. Abel 1802 - 1827]

Bsp.: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind Gruppen

4.2. Bemerkungen

Sei $(G, \circ)$ eine Gruppe. Dann gilt

(1) $e \circ a = a \quad \forall\, a$

(2) e ist durch die Eigenschaft $a \circ e = a \ \forall\, a \in G$

eindeutig bestimmt

(3) Für das a' mit $a \cdot a' = e$ gilt auch $a' \cdot a = e$

(4) a' ist durch die Eigenschaft $a \cdot a' = e$ eindeutig bestimmt.

a' heißt das zu a inverse Element

Schreibweise: $a^{-1} = a'$

Bsp.:

Sei M eine Menge. Dann ist $S(M) = \{\sigma : M \to M \mid \sigma \text{ ist bijektiv}\}$ mit Komposition als Verknüpfung eine Gruppe.

Neutrales Element $e = id_M$ Ident. Abbildung

Inverses Element zu $\sigma \in S(M)$ ist die Umkehrabbildung $\sigma^{-1} : M \to M$

Speziell: Ist $M = \{1, \dots, n\}$.

dann schreiben wir $S_n := S(\{1, \dots, n\})$

und nennen S_n die symm. Gruppe auf n Elementen

$\sigma \in S_n$, so geben wir σ häufig in Tabellenform an

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & & n \\ \sigma(1) & \sigma(2) & \sigma(3) & & \sigma(n) \end{pmatrix}$$

Bsp:

$S_3 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

S_3 ist nicht abelsch.

Allgemein für beliebiges n gilt

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = n!$$

Bsp: S_3 hat 6 Elemente

$S_3 = \{\sigma, \tau, \sigma\circ\tau, \underbrace{\tau\circ\sigma}_{\text{invers zueinander}}, e = id = \sigma^2 = \tau^2\}$ und $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Herleitung von (1),... (4) aus den Axiomen (G_1), (G_2), (G_3)

Zunächst (3). Wir wissen $a \cdot a' = e$

Wir wenden $(G3)$ auf a' an. Also existiert ein Element a'', sodass $a' \cdot a'' = e$

$$a' \cdot a = (a' \cdot a) \cdot e \overset{G_1}{=} a' \cdot (a \cdot e) \overset{G_3}{=} a'(a(a' \cdot a''))$$
$$= a' \cdot ((a \cdot a') \cdot a'') = a' \cdot (e \cdot a'') = (a' \cdot e) \cdot a''$$
$$= a' \cdot a'' = e$$

zu (1)

$$e \cdot a = (a \cdot a') \cdot a = a \cdot (a' \cdot a) \overset{(3)}{=} a \cdot e = a$$

zu (2) Sei e' ein weiteres neutrales Element.

$$e \overset{\text{def. Eigenschaft von } e'}{=} e \cdot e \overset{(4)}{=} e' \quad \text{also } e = e'$$

zu (4) Sei a'' ein weiteres inverses Element $a \cdot a'' = e$

$$\overset{\text{mit (2)}}{\Longrightarrow} a'' \cdot a = e \text{. Dann gilt } a'' = a'' \cdot e = a''(a \cdot a')$$
$$= (a'' \cdot a) \cdot a' = e \cdot a' \overset{(1)}{=} a'$$

4.3 Weitere Beispiele

- $(G_1, \circ)$, $(G_2, \circ)$ seien Gruppen. Dann ist

  $G_1 \times G_2$ mit der Verknüpfung

  $(a_1, a_2) \circ (b_1, b_2) = (a_1 \circ b_1, a_2 \circ b_2)$

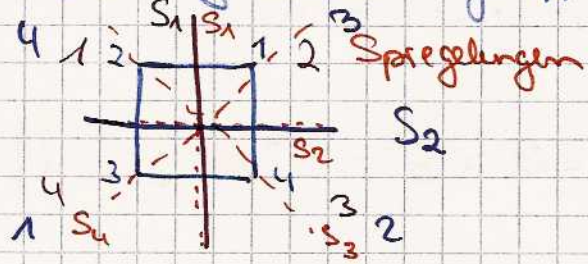
  ebenfalls eine Gruppe

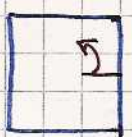
- $(\mathbb{Z}/n, +)$ ist eine Gruppe mit n Elementen

  $\mathbb{Z}/2 \times \mathbb{Z}/2$ ist Gruppe mit 4 Elementen

  $\mathbb{Z}/4$ ebenfalls

- Die Symmetrie Gruppe des Quadrats





Drehungen

90°

180°

270°

id

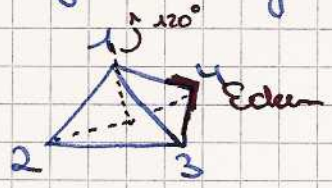
D_4 hat 8 Elemente

$D_4 \supset \mathbb{Z}/4$

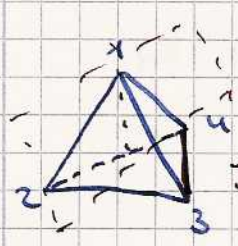
$\cup$

$\mathbb{Z}/2 \times \mathbb{Z}/2 = \{e, s_1, s_2, d_{180°}\}$

• Symmetriegruppe vom Tetraeder

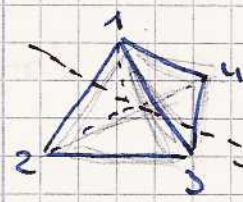


Ecken $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$



Spiegelung an Ebene

Kanten $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$



$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ gegenüberliegende Seiten

Wie viele Elemente bisher : 18

id = e , $\circlearrowright 120°$, Spiegelung , $\circlearrowright 180°$

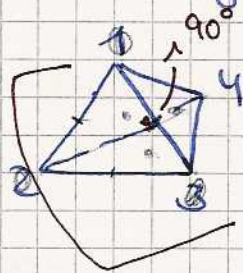
1 + 4·2 + 6 + 3

Also: $Sym(\text{Tetraeder}) \subset S_4$

$|S_4| = 24$

Fehlt z.B.: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Drehspiegelung 3 · 2 (Drei Achsen, 2 Richtungen)



Zusammen: 24

3 Ecken 4 Seiten

44. Häufig treten Gruppen als Untergruppen von $S(M)$ für eine Menge M auf.

Bsp.:

$M = \mathbb{R}^2$ die Ebene

$SO(2) = \{$ Drehung in $\mathbb{R}^2$ um $0\} \subset S(\mathbb{R}^2)$

Spezielle orthogonale Gruppe

4.5 Def

Sei M eine Menge, G eine Gruppe

Eine Operation von G (von links) auf M ist eine Abbildung

$$G \times M \to M, \quad (g, m) \mapsto g \cdot m$$

mit folgenden Eigenschaften:

(O1) $g(h \cdot m) = (g \cdot h) m \quad \forall g, h \in G, \forall m \in M$

(O2) $e \cdot m = m \quad \forall m \in M$

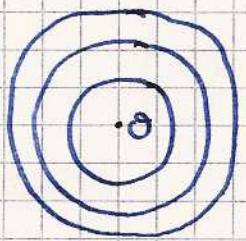
4.6. Ist eine Operation $G \times M \to M$ und $m \in M$

Heißt $G \cdot m = \{g \cdot m \mid g \in G\} \subset M$

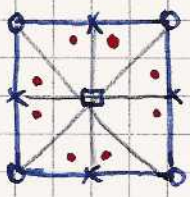
die Bahn von M (Orbit)

Bsp.:

$SO(2)$ operiert auf $\mathbb{R}^2$ und hat die Bahn



Die Symmetriegruppe D_4 des Quadrats operiert auf dem Quadrat. Einige Bahnen:



(neun 8 Punkte hat sie sonst, da D_4 8 Elemente)

Punkte auf Diagonalen: 4

Bahnen der Ordnung 1, 4, 8

4.7. Def

Sei $G \times M \to M$ eine Operation, $m \in M$.

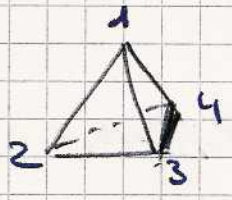
Dann heißt

$$Stab(m) = \{ g \in G \mid g \cdot m = m \}$$

der Stabilisator von m.

Bsp.:

$T \cong S_4$ Tetraedergruppe



Stab (1) hat 6 Elemente

$Stab(m) \subset G$ ist eine Untergruppe

4.8 Satz und Def.

Sei $H \subset G$, nicht leer.

H heißt Untergruppe, wenn

$$a, b \in H \Rightarrow a \cdot b^{-1} \in H \quad \forall a, b \in H$$

Für eine Untergruppe hat das Bild von

$\circ|_{H \times H}$ Werte in H.

Also $(H, \circ|_{H \times H} : H \times H \to H)$

ist eine Gruppe

Beweis:

$H \neq \emptyset \quad \exists a \in H \Rightarrow e = a \cdot a^{-1} \in H$,

H hat ein neutrales Element.

Weiter mit $b \in H$ gilt $e \cdot b^{-1} = b^{-1} \in H$,

d. h. in H gibt es Inverse,

und $g, h \in H \Rightarrow g, h^{-1} \in H \Rightarrow g(h^{-1})^{-1} = g \cdot h \in$

4.9 Satz

Stab (m) ist eine Untergruppe

Beweis:

1) $a, b \in \text{Stab}(m) \Rightarrow a \cdot m = m$ und $b \cdot m = m$

$\Rightarrow (ab)m = a \cdot (bm) = a \cdot m = m$

$\Rightarrow a \cdot b \in \text{Stab}(m)$

2) $m = e \cdot m = b^{-1} \cdot b \cdot m = b^{-1} \cdot (b \cdot m) = b^{-1} \cdot m$

$\Rightarrow b^{-1} \in \text{Stab}(m)$

1) und 2) $a, b \in \text{Stab}(m) \Rightarrow ab^{-1} \in \text{Stab}(m)$

4.10 Jede Operation $G \times M \to M$ definiert eine Äquivalentrelation auf M:

$m \sim n \Leftrightarrow \exists\, g \in G \quad g \cdot m = n$

($\Leftrightarrow$ m, n liegen in der gleichen Bahn)

deren Äquivalentklassen gerade die Bahn sind.

In der Tat: $m \sim n$, da

(r) $e \cdot m = m$

(s) $m \sim n \Rightarrow g \cdot m = n \Rightarrow m = e \cdot m = g^{-1} \cdot g \cdot m = g^{-1} n$, also $n \sim m$

(t) $m \sim n \sim k$ etwa $g \cdot m = n$, $h \cdot n = k$

$\Rightarrow (hg)m = h(gm) = h \cdot n = k$ also $m \sim k$.

Mit $G\backslash M := M/\sim = \{ G \cdot m \mid m \in M \} \subset 2^M$

heißt Quotient von M nach G oder Bahnenraum

M/G verwendet man bei Operationen von rechts

Bsp.

Sei $H \subset G$ eine Untergruppe. Dann liefert die Verknüpfung eine Operation

$$H \times G \to G, (h, g) \mapsto h \cdot g$$

nach links.

Analog $G \times H \to G$ Operation nach rechts

$H \backslash G = \{ H \cdot g \mid g \in G \}$ von links $\subset 2^G$

$G / H = \{ g \cdot H \mid g \in G \}$ von rechts

dabei $Hg = \{ h \cdot g \mid h \in H \}$ bzw. $g \cdot H = \{ g \cdot h \mid h \in H \}$

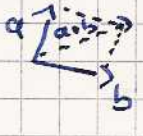
$g \cdot H$ bzw. Hg heißen linke bzw. rechte Nebenklasse von H.

Bsp.

$G = (\mathbb{Z}, +)$, $H = d \cdot \mathbb{Z} = \{ d \cdot k \mid k \in \mathbb{Z} \}$

$H \backslash G = \{ i + d\mathbb{Z} \mid i = 0, 1, \ldots, d-1 \}$ die Restklassen

$(\mathbb{R}^2, +)$ Vektoraddition



L Gerade durch $0 \in \mathbb{R}^2$

$(L, +)$ ist Untergruppe

$L \backslash \mathbb{R}^2$ = Menge der Parallelen

4.11 Satz

Sei G eine endliche Gruppe, $H \subset G$ eine Untergruppe.

Dann gilt

$$|_H \backslash G| = |G / H| = \frac{|G|}{|H|}$$

Insbesondere ist $|H|$ ein Teiler von G.

Def.

Man nennt $[G : H] := |G / H|$ den Index von H in G.

$|G|$ heißt Ordnung von G.

Beweis:

Wir zeigen, daß zwei Nebenklassen

$H \cdot a$ und $H \cdot b$ gleich viele Elemente haben.

In der Tat

$H \to H \cdot a$, $h \mapsto h \cdot a$ ist eine Bijektion

mit Umkehrabbildung

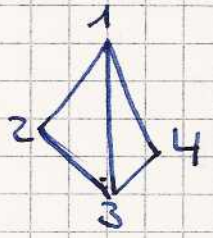
$$\begin{array}{ccc} Ha & \longrightarrow & H \\ \downarrow & & \\ g & \longmapsto & g \cdot a^{-1} \end{array}$$

Da die Bahnen disjunkt sind folgt:

$$|G| = \sum_{Hg \in H\backslash G} |H \cdot g|$$

$$= \sum_{Hg \in H\backslash G} |H| = |H| \cdot \left|H\backslash G\right| \qquad \square$$

Bsp.: $T \cong S_4 \supset \mathrm{Stab}(4) \cong S_3$



$|S_4| = 4! = 24$, $|S_3| = 3! = 6$

4.12 Def

Sei G eine Gruppe, $g \in G$. Dann bezeichnet

$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$ (dabei $g^{-k} = (g^{-1})^k$)

die von g erzeugte Untergruppe

$$\mathrm{ord}(g) = |\langle g \rangle| = \begin{cases} \infty, & \text{falls } \{k>0 \mid g^k = e\} = \emptyset \\ \min\{k>0 \mid g^k = e\} \end{cases}$$

heißt Ordnung von G.

Nach der Indexformel ist $\mathrm{ord}(g)$ ein Teiler von $|G|$

Bsp:

In $G = S_4$ gibt es Elemente der Ordnung $1, 2, 3, 4$. Die Teiler $6, 8, 12$ tauchen nicht auf (von 24)

4.13 Lemma

Sei $G \times M \to M$ eine Operation, $m \in M$.

$$G/\mathrm{Stab}(m) \to G \cdot m \qquad H \ \mathrm{Stab}(m)$$

$$g \cdot \mathrm{Stab}(m) \mapsto g \cdot m$$

ist eine Bijektion

Beweis:

Surjektiv ist klar. Nicht so klar ist, daß die Abbildung wohldefiniert ist, d.h. $g_1 \cdot H = g_2 \cdot H$

$\Rightarrow g_1 \cdot m = g_2 \cdot m$ ist zu zeigen

Ist $g_2 = g_1 \cdot h$, dann ist in der Tat

$g_2 \cdot m = (g_1 \cdot h)\, m = g_1 \cdot (h \cdot m) = g_1 \cdot m$,

da $h \in H = \mathrm{Stab}(m)$

Injektiv: Ann.: $g_1 \cdot m = g_2 \cdot m$

z.z.: $g_1 H = g_2 \cdot H$

$g_1 \cdot m = g_2 \cdot m \Rightarrow g_2^{-1} \cdot g_1 m = g_2^{-1} \cdot g_2 \cdot m = e m = m$

$\Rightarrow g_2^{-1} g_1 \in H$.

$g_1 = g_2 \cdot (g_2^{-1} \cdot g_1) \in g_2 H \Rightarrow g_1 H = g_2 H$

4.14 Satz (Bahnengleichung)

Sei $G \times M \to M$ eine Operation auf einer endl. Menge. Dann gilt:

$$|M| = \sum_{G m \in G\backslash M} |G m| = \sum_{g m \in G\backslash M} |G/\mathrm{Stab}(m)|$$

Beweis:

Die Bahnen sind disjunkt und $|G \cdot m| = |G / Stab(m)|$

4.15 Def.:

Ein Graph $G = (V, E)$ von einer endlichen Menge V von Knoten (= vertices) und Kanten E (= edges)

$$E \subset V \times V$$

Ist E symmetrisch und disjunkt von den Diagonalen, dann ist G ein ungerichteter Graph ohne Schleifen.

Bsp.:

Graph mit 4 Knoten und 4 Kanten

Zwei Graphen $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ sind isomorph, wenn es eine Bijektion gibt

$$\varphi : V_1 \to V_2$$

die eine Bijektion $E_1 \to E_2$ induziert.

Bsp. 

Frage: Wieviele verschiedene Typen von Graphen mit 4 Knoten gibt es?

$V = \{1, 2, 3, 4\}$, $G = (V, E)$

$M = \{ G \mid G = (V, E) \text{ mit 4 Knoten} \}$

$|M| = 2^6 = 64$

1) 

2) 

3) 

4) 

5) 

6) 

7) 

8) 

9) 

10) 

$G=(V,E)$									
$\mathrm{Stab}(V,E)$	S_4	$\mathbb{Z}_2\times\mathbb{Z}_2$	D_4 $\lvert D_4\rvert=8$	$\mathbb{Z}_2$	$\mathbb{Z}_2$	S_3	D_4	$\mathbb{Z}_2$	$\mathbb{Z}_2\times\mathbb{Z}_2$
$\lvert\text{Bahn}\rvert$	1	$24/4=6$	3	12	12	$24/6=4$	3	12	6

Betrachte Operation $S_4 \times \mathcal{H} \to \mathcal{H}$

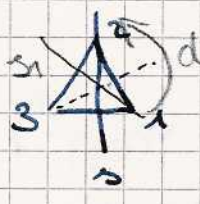
$\sum \lvert\text{Bahnen}\rvert = 60$

Fehlt: 

S_3

4

Bsp.: $G = S_3$ Symmetriegruppe des Dreiecks



$\mathcal{H} = \langle s \rangle = \{e, s\}$, da $s^2 = e$

$s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

g	$g\mathcal{H}$
id	$H = \langle id, s \rangle$
s	$sH = H$
s_1	$s_1 H = \{s_1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = d\}$
d	$d \cdot H = \{d, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s_1\}$
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = d^2$	$d^2 \cdot H = \{d^2, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\}$

$G/\mathcal{H} = \{H, d\cdot\mathcal{H}, d^2\cdot\mathcal{H}\}$

Es gibt also 3 Nebenklassen

4.16 Def

Seien $(G, \circ)$, $(H, *)$ zwei Gruppen.

Ein (Gruppen-) Homomorphismus ist eine Abbildung

$\varphi : G \to H$,

die $\varphi(a \circ b) = \varphi(a) * \varphi(b) \quad \forall a, b \in G$

erfüllt.

Bem.

Gruppenhomomorphismen erfüllen außerdem

- $\varphi(e_G) = e_H$ $\quad e_G \in G$ neutrales Element von G, $e_H \in H$ " " von H
- $\varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G$

Mit anderen Worten: φ respektiert die Verknüpfungs-Strukturen.

Beweis:

1) $\varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G)$

$e_H = \varphi(e_G) * \varphi(e_G)^{-1} = \varphi(e_G) * (\varphi(e_G) * \varphi(e_G)^{-1})$

$= \varphi(e_G) * e_H = \varphi(e_G)$

2) $e = \varphi(e) = \varphi(a \circ a^{-1}) = \varphi(a) * \varphi(a^{-1})$

$\Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$, da das Inverse von $\varphi(a)$ durch obige Gleichung bestimmt ist.

4.17 Def

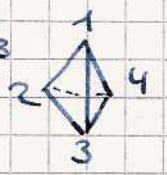
Einen injektiven, surjektiven bzw. bijektiven Gruppenhomomorphismus nennen wir einen Monomorphismus, Epimorphismus bzw. Isomorphismus.

Zwei Gruppen G und H, zwischen denen es einen Isomorphismus gibt, nennt man isomorph

Schreibweise $G \cong H$

Bsp.: T Tetraedergruppe

$T \cong S_4$, $\mathrm{Stab}(4) \cong S_3$



$S_3 \to S_4$

ist Monomorphismus

$(\mathbb{Z}, +)$ $\quad g \in \mathcal{G}$

$\mathcal{U} = \langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \}$

$\mathbb{Z} \xrightarrow{\varphi} \mathcal{U}$

$k \mapsto g^k$

ist Gruppenhomomorphismus, da

$g^{k+l} = g^k \cdot g^l \qquad k, l \in \mathbb{Z}$

φ ist ein Epimorphismus

$\mathbb{Z} \to \langle g \rangle$ ist ein Isomorphismus $\Leftrightarrow \mathrm{ord}(g) = \infty$

4.18 Def + Satz

Sei $\varphi : \mathcal{G} \to \mathcal{H}$ ein Gruppenhomomorphismus.

Dann heißt

$$\ker \varphi = \{ a \in \mathcal{G} \mid \varphi(a) = e \} = \varphi^{-1}(e)$$

Kern von φ

und $\mathrm{Im}\,\varphi = \varphi(\mathcal{G}) = \{ \varphi(a) \mid a \in \mathcal{G} \} \subset \mathcal{H}$

heißt Bild von φ (image)

$\ker \varphi$ und $\mathrm{Im}\,\varphi$ sind Untergruppen von

$\mathcal{G}$ bzw. $\mathcal{H}$.

Bsp.:

Sei $g \in \mathcal{G}$ ein Element der Ordnung $\mathrm{ord}(g) = d < \infty$

Dann ist für $\varphi : \mathbb{Z} \to \langle g \rangle$, $k \mapsto g^k$

$\ker \varphi = d\mathbb{Z} = \{ d \cdot k \mid k \in \mathbb{Z} \} \subset \mathbb{Z}$.

Beweis:

1) $a, b \in \ker \varphi$

$e = \varphi(e) = \varphi(b \cdot b^{-1}) = \varphi(b) \cdot \varphi(b^{-1})$

$= e \cdot \varphi(b^{-1}) = \varphi(b^{-1}) \Rightarrow b^{-1} \in \ker \varphi$

Wollen $ab^{-1} \in \ker \varphi$ zeigen.

$\varphi(ab^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = e \cdot e = e$ o.k.

2) Ähnlich aber einfacher ∎

4.19 Satz

Sei $\varphi: G \to \mathcal{H}$ ein Hom. Dann ist φ injektiv, genau dann, wenn $\ker \varphi = \{e\}$

Beweis:

Da $\ker \varphi = \varphi^{-1}(e_H) \ni e$ ist $\ker \varphi = \{e\}$ notwendig für die Injektivität.

Sei nun $a, b \in G$ mit $\varphi(a) = \varphi(b)$ und die Voraussetzung $\ker \varphi = \{e\}$ erfüllt.

Dann gilt:

$\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = e$

da $\varphi(a) = \varphi(b)$. Also $a \cdot b^{-1} \in \ker \varphi = \{e\}$

$\Rightarrow a \cdot b^{-1} = e \Rightarrow a = b$ ∎

Der Kern eines Gruppenhomomorphismus $\varphi: G \to \mathcal{H}$ hat eine besondere Eigenschaft:

$a \in \ker \varphi$, $g \in G \Rightarrow g \cdot a \cdot g^{-1} \in \ker \varphi$

denn $\varphi(gag^{-1}) = \varphi(g) \cdot \varphi(a) \cdot \varphi(g^{-1})$

$= \varphi(g) \cdot \varphi(g^{-1}) = e$

4.20 Def.

Eine Untergruppe $N \subset G$ heißt Normalteiler, wenn $g \cdot N \cdot g^{-1} = N$, d.h.

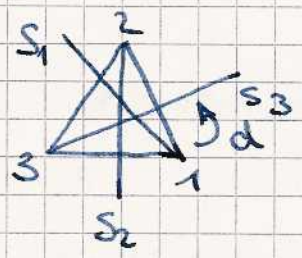
$\{ gag^{-1} \mid a \in N \} = N$ oder

$gN = \{ g \cdot a \mid a \in N \} = \{ a \cdot g \mid a \in N \} = N \cdot g$.

Der Kern eines Gruppenhomomorphismus ist ein Normalteiler.

Bsp.:

S_3



Untergruppen $\{e\}$

$\mathcal{H}_1 = \{ e, s_1 \}$, $\mathcal{H}_2$ $\mathcal{H}_3 = \{ e, s_3 \}$

diese sind isomorph zu $\mathbb{Z}/2$

$A_3 = \{ 1, d, d^2 \}$, S_3

Normalteiler: $\{e\}$, S_3

$$s_1 d s_1^{-1} = s_1 d s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = d^2$$

$$s_2 s_1 s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = s_3 \notin \mathcal{H}_1$$

Bsp.:

Ker φ, $\varphi : G \to \mathcal{H}$ ist ein Normalteiler

Unser nächstes Ziel ist zu zeigen, daß jeder Normalteiler $N \subset G$ als Kern eines geeigneten Gruppenhom. auftaucht. Die Idee ist dabei, die Menge der Nebenklassen

$G/N = \{ g \cdot N \mid g \in G \}$

die Struktur einer Gruppe zu geben,

so daß die Klassenabbildung

$\pi : G \to G/N$ ein gruppenhom. ist.

Wir definieren eine Verknüpfung $\circ$ auf G/N repräsentantenweise.

$$g \cdot N \circ h \cdot N := (g \cdot h) N$$

Wir müssen zeigen, daß diese Def. wohldefiniert ist, d.h. $g_1 \in gN$, $h_1 \in hN$, dann ist

$$(g_1 h_1) \cdot N = (g \cdot h) N$$

zu zeigen.

Hierfür benötigen wir die Normalteilereigenschaft.

Sei etwa $g_1 = g \cdot n$, $h_1 = h \cdot m$, $n, m \in N$

$$\begin{aligned} g_1 h_1 \cdot N = g \cdot n \cdot h \cdot m \cdot N &= \{ g n h m a \mid a \in N \} \\ &= \{ g n h b \mid b \in N \} \\ &= g n h \cdot N \\ &= g \cdot n \cdot N \cdot h = \{ g \cdot n \cdot a \cdot h \mid a \in N \}, \\ &= g \cdot N \cdot h \quad , \text{da } n \in N \\ &= g \cdot h \cdot N \quad , \text{da } N \text{ Normalteiler} \end{aligned}$$

da $hN = Nh$ ($N \trianglelefteq$)

Also:

$\circ : G/N \times G/N \to G/N$ ist wohldefiniert

und $\pi(g \cdot h) = \pi(g) \circ \pi(h)$

Assoziativ für $\circ$ ist klar, da dies in G gilt.

Neutrales Element $N = eN \in G/N$

Inverses zu gN ist $g^{-1}N$.

Also haben wir gezeigt

4.21 Satz

Ist $N \subset G$ ein Normalteiler, dann trägt G/N die Struktur einer Gruppe, so daß $\pi : G \to G/N$ ein Gruppenhomomorphismus ist. Und $\ker \pi = N$.

4.22 Wortgruppen bzw. Gruppen definiert über Erzeuger und Relationen

Enthält eine Gruppe G Elemente a, b, c, dann sind auch alle Ausdrücke der Gestalt

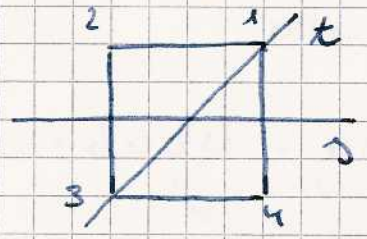
$$a b a a c a^{-1} b \in G$$

Die Verknüpfung solcher Ausdrücke entspricht hintereinanderschreiben, wenn man noch $a^{-1} \cdot a = e$ etc. beachtet.

$$(a b c^{-1})^{-1} = c \cdot b^{-1} \cdot a^{-1}$$

Bsp.:

D_4 Symmetriegruppe des Quadrats



$s^2 = e, \quad t^2 = e$

$s \circ t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ = Drehung um 90°

↑ zuerst t anwenden!

$D_4 = \{ e, s, t, s \circ t, t \circ s, s \cdot t \cdot s, tst, \ldots, \underbrace{tststst}_{= (ts)^4} \}$

Wissen auch noch $(ts)^4 = tstststs = e$

$D_4 = \langle s, t \mid s^2 = t^2 = (ts)^4 = e \rangle$

Erzeuger

Def:

Sei $A = \{a, b, \ldots x\}$ eine Candidate / Menge.

Dann besteht die freie Wortgruppe über A aus allen Wörtern w mit Buchstaben $a, b, \ldots, x, a^{-1}, b^{-1}, \ldots, x^{-1}$

und der Regel $aa^{-1} = e$, ... , $x \cdot x^{-1} = e$
mit Verknüpfung Hintereinanderschreiben.

$G = \langle a, b, \dots, x \rangle$

Sind nun $w_1, \dots, w_k$ Wörter in G, dann bezeichnet

$\langle a, \dots x \mid w_1 = w_2 = \dots = w_k = e \rangle = G/N$

wobei $N \subset G = \langle a, \dots x \rangle$ der kleinste Normalteiler ist, der $w_1, \dots, w_k$ enthält.

Also $w w_1 w^{-1} = e \Leftrightarrow w \cdot w_1 = w$

$\Rightarrow w \cdot w_1 \cdot v = w \cdot v$

I. A. ist $w \cdot N = v \cdot N$ schwierig zu entscheiden

($\Leftrightarrow v^{-1} \cdot w \cdot N = N$ bzw. $v^{-1} w \in N$)

Bsp.:

$G = \langle ab \mid a^2 = e, \; b^3 = e, \; aba^x = ba b^{xx} \rangle$

Frage: Was ist das für eine Gruppe

↳ Grund I $ab^2a \cdot aba^x = a^2 \cdot a^2 \cdot b^3 = e \cdot e \cdot e = e$

II $ab^2a \cdot bab = ab^2a \cdot aba =$ wie I

da $bab = aba$

$aba = bab \rightarrow aba^2 = ba\,ba = bbab = b^3ab$

$aba^2 = ab$; $ba\,ba = bab$

$ab = b^2ab \rightarrow e = b^2 = b^3 \Rightarrow b = e$,

$e \cdot a^2 = a$

↳ da $ab = b^2 \cdot ab \mid \cdot x^{-1}$

4.22 Satz Homomorphiesatz

Sei $\varphi : G \to \mathcal{H}$ ein Homomorphismus.
Dann ist

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

vermöge dem Isomorphismus

$$g \cdot \ker\varphi \mapsto \varphi(g)$$

Bsp.:

$$\varphi : \mathbb{Z} \to G, \quad k \mapsto g^k$$

$\operatorname{Im}\varphi = \langle g \rangle$, $\ker\varphi = d\cdot\mathbb{Z}$, $d = \operatorname{ord}(g)$
Nach dem Satz gilt:

$$\mathbb{Z}/d\mathbb{Z} \cong \langle g \rangle \qquad (= \mathbb{Z}/(d))$$

Beweis:
Zu zeigen ist zunächst, daß

$$\overline{\Phi} : G/\ker\varphi \to \operatorname{Im}\varphi$$

$$\overline{\Phi}(g\ker\varphi) = \varphi(g)$$

wohldefiniert ist.

Sei $g_1 \in g\ker\varphi$ ein anderer Repräsentant, etwa $g_1 = g\cdot a$, $a \in \ker\varphi$
Dann

$$\varphi(g_1) = \varphi(g\cdot a) = \varphi(g)\cdot\varphi(a) = \varphi(g)\cdot e = \varphi(g)$$

Also ist $\overline{\Phi}$ ist wohldefiniert.
Surjektiv ist klar. Für injektiv betrachten wir

$$\ker\overline{\Phi} = \{ g\ker\varphi \mid \overline{\Phi}(g\ker\varphi) = e \}$$
$$= \{ g\ker\varphi \mid \varphi(g) = e \}$$
$$= \{ g\ker\varphi \mid g \in \ker\varphi \} = \{\ker\varphi\}$$

also nur das neutrale Element von $G/\ker\varphi$ $\Rightarrow$ injektiv

4.23 Bahnenschreibweise für Permutation

S_n operiert auf $\{1,\dots,n\}$ nach Def. Sei $\sigma \in S_n$.
$\langle \sigma \rangle \cong \mathbb{Z}/d$, $d = \mathrm{ord}(\sigma)$ und $\{1,\dots,n\}$ zerlegt sich unter Operation von $\langle \sigma \rangle$ in endlich viele zyklische Bahnen.

Bsp.:

$S_4 \ni \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \sigma \qquad \sigma^2 = \mathrm{id}$

Bahnen $\{1,2\}$, $\{3,4\}$

$S_4 \ni \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \tau$, $\{1,2,3\}$, $\{4\}$ Bahnen von τ

Def (in Bsp. zunächst)

$\sigma = (1\,2)(3\,4)$ ← kürzere Notation

$\tau = (1\,2\,3)$ → Konvention: da $\{4\}$ fest ist, wird es einfach weggelassen

Allgemein hat für $\sigma \in S_n$ die Gruppe $\langle \sigma \rangle$ die Bahnen $i_1 \to i_2 \to \dots i_k$, $j_1 \to \dots \to j_e, \dots$

$\sigma = (i_1, i_2, \dots i_k)\,(j_1, \dots, j_e)$

Bsp.:

$\underbrace{(1\,2\,5)(3\,4)}_{=\sigma} \in S_5$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad (1\,2\,5)$

"

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$

$\sigma_2 = (3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$

Dann $\sigma = \sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$

Bsp. Komposition

$(1\,2) = \sigma$, $(2\,3) = \tau$

$\sigma \circ \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3) = (\tau \circ \sigma \circ \sigma)$

4.24. Def

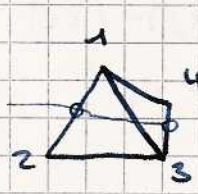
Eine Permutation σ, die nur zwei Elemente vertauscht

$\sigma(i,j)$ heißt Transposition.

Es ist klar, daß S_n von Transpositionen erzeugt wird

Bsp.:

$$(1\,2\,3) = (1\,2)\circ(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$



$S_4 \ni (1\,2\,3) = (1\,2)(2\,3)$

$(1\,2)(3\,4)$ gerade Drehung

ungeraden $(1\,2)$ Spiegelung

$(1\,2\,3\,4) = (1\,2)(2\,3)(3\,4)$ Drehspiegelung

4.25 Def

Sei $\sigma \in S_n$. Dann heißt die Signatur

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Dann gilt:

$$\operatorname{sgn}(\sigma) \in \{\pm 1\}$$

denn $\prod_{1 \le i < j \le n} |i - j| = \prod_{1 \le i < j \le n} |\sigma(j) - \sigma(i)|$

4.26 Satz

$\operatorname{sgn} : S_n \to (\{\pm 1\}, \cdot)$

ist Gruppenhomomorphismus.

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{falls } \sigma \text{ ein gerades Produkt von Transpositionen ist} \\ -1 & \text{falls } \sigma \text{ ungerades Produkt von Transpositionen ist} \end{cases}$$

Def:

$A_n = \ker(\mathrm{sgn}: S_n \to \{\pm 1\})$ heißt alternierende Gruppe.

Beweis:

$$\mathrm{sgn}(\sigma\circ\tau) = \prod_{1\le i<j\le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i}$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \frac{\tau(j)-\tau(i)}{j-i}$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)} \cdot \prod_{1\le i<j\le n} \frac{\tau(j)-\tau(i)}{j-i}$$

$$= \prod_{1\le i<j\le n} \frac{\sigma(j) - \sigma(i)}{j-i} \cdot \mathrm{sgn}(\tau)$$

denn wenn $\{i,j\}$ die 2-elementigen Teilmengen von $\{1,\dots,n\}$ durchläuft, durchläuft auch $\tau(i), \tau(j)$ die Menge der 2-elementigen Teilmengen.

$= \mathrm{sgn}(\sigma)\cdot\mathrm{sgn}(\tau)$

$$\mathrm{sgn}(\underbrace{12}_{\tau}) = \prod_{1\le i<j\le n} \frac{\tau(j)-\tau(i)}{j-i} = \prod_{3\le i<j\le n} \frac{j-i}{j-i} \cdot \prod_{3\le i<j\le n} \frac{j-i}{j-2}$$

$$\cdot \prod_{3\le j\le n} \frac{j-2}{j-1} \cdot \frac{1-2}{2-1} = -1$$

$i,j = 1,2$

$\mathrm{sgn}(kl) = ?$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & k & \dots & l & \dots \\ k & l & 3 & \dots & 1 & \dots & 2 & \dots \end{pmatrix}$$

$(kl) = \sigma(12)\sigma$

Es folgt

$$\begin{aligned} \operatorname{sgn}(\kappa\ell) &= \operatorname{sgn}(\beta(12)\beta) \\ &= \operatorname{sgn}(\beta)\cdot\operatorname{sgn}(12)\cdot\operatorname{sgn}(\beta) \\ &= (\operatorname{sgn}(\beta))^2\cdot(-1) = -1 \end{aligned}$$

Nun ist die zweite Aussage klar.

Da ein gerades Produkt von (-1)-en $(+1)$ ergibt

Bsp.:

$A_4 \subset S_4 \cong T$ ist die Untergruppe der Drehungen

$A_3 \subset S_3$: $A_3 \cong \mathbb{Z}/3$

Kapitel 2 : Die reellen Zahlen

§ 5 Die Körperaxiome

Def:

Ein Körper (engl. field) ist eine Menge K zusammen mit 2 Verknüpfungen

$$+ : K \times K \to K, \ (a,b) \mapsto a+b$$

$$\cdot : K \times K \to K, \ (a,b) \mapsto a\cdot b$$

die folgenden Axiomen genügt:

(K1) $(K,+)$ ist eine abelsche Gruppe

neutrales Element von $(K,+)$ ist $0 = 0_K$

Inverses Element von $a \in K$ bzgl. $+$ ist $-a$ (das N

(K2) $K^* = K \setminus \{0\}$, $(K^*,\cdot)$ ist eine abelsche Gruppe

mit neutralem Element $1 \in K$, Inverses zu $a = \frac{1}{a} = a^{-1}$

(K3) Es gelten die Distributivgesetze.

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

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

$\forall a,b,c \in K$

Bsp.:

$(\mathbb{Q}, +, \cdot)$ ist ein Körper

$(\mathbb{R}, +, \cdot)$ "

$(\mathbb{Z}, +, \cdot)$ ist kein Körper, da außer für ± 1 die Elemente $a \in \mathbb{Z} \setminus \{0\}$ kein mult. Inverses in $\mathbb{Z}$ haben

Bsp.:

$\mathbb{F}_2 = \{0, 1\}$ mit Verknüpfung

+	0	1
0	0	1
1	1	0

$1 + 1 = 0 \in \mathbb{F}_2$

·	0	1
0	0	0
1	0	1

5.1 Beispiele

Sei p eine Primzahl. Dann ist $\mathbb{F}_p = \mathbb{Z}/p = \{\bar{0}, \bar{1}, \dots \overline{p-1}\}$ mit repräsentantenweiser Addition und Multiplikation

$$\bar{i} + \bar{j} = \overline{i + j}$$

$$\bar{i} \cdot \bar{j} = \overline{(i \cdot j)}$$

Beweis:

Die Axiome sind klar, außer die Existenz eines Inversen.

Sei $\bar{i} \in \mathbb{F}_p^*$, $1 \le i \le p-1$

Da p eine Primzahl ist gilt:

$$ggT(p, i) = 1 = u \cdot p + v \cdot i$$

nach euklid Algorithmus

Es folgt $\bar{1} = \bar{v} \cdot \bar{i}$, d.h. $\bar{i}^{-1} = \bar{v}$

Das Inverse in $\mathbb{F}_p$ berechnen wir mit dem euklid. Algorithmus.

5.3 Folgerungen aus dem Axiom

1) $0 \in K$ und $1 \in K^*$ sind eindeutig bestimmt.

2) Zu $a \in K$ ist das Negative $-a$ eindeutig bestimmt.

3) Zu $a \in K$ ist das Inverse a^{-1} eindeutig bestimmt.

Dies gilt, da Eindeutigkeit von neutralen und inversen Elementen in Gruppen gilt.

4) $0 \cdot a = 0 \quad \forall\, a \in K$

denn $0 \cdot a = (0+0) \cdot a$

$= 0 \cdot a + 0 \cdot a$

$\Rightarrow 0 = 0 \cdot a$ (aus Distributivgesetz)

5) $1 \cdot a = a \quad \forall\, a \in K$

nach Def richtig für $a \in K^*$ für $a = 0$ vg. (4

(6) $(-1) \cdot a = -a \quad \forall\, a \in K$

Beweis: -1 ist das Negative von 1

Also $1 + (-1) = 0$. Multiplikation mit a

liefert $a \cdot (1 + (-1)) = a \cdot 0 = 0$

$= a \cdot 1 + a \cdot (-1) = 1 \cdot a + (-1) \cdot a)$

$(= a + (-a) = a - a = 0)$

Also $(-1) \cdot a$ ist ein Element, so daß $a + x = 0$ gilt

Andererseits $x = -a$ hat auch diese Eigenschaft.

Wegen (2) folgt $(-1) \cdot a = -a$

(7): $(-1) \cdot (-1) = 1 = -(-1) = 1$

denn nach (6) gilt $(-1) \cdot \underbrace{(-1)}_{a} = -(-1)$

Wissen: $(-1) + -(-1) = 0$. Andererseits

$(-1) + 1 = 0$. Wegen der Eindeutigkeit des Inversen

(2) gilt $-(-1) = 1$

(8) $(-a)(-b) = a \cdot b$

Bew.:

$(-a)(-b) = (-1) \cdot a \cdot (-1) \cdot b = (-1)^2 \cdot a \cdot b = 1 \cdot a \cdot b = a \cdot b$

Def:

Sei $a, b \in K$. Dann ist

$a - b := a + (-b)$

Ist $b \in K^*$. Dann

$a : b = a \cdot b^{-1} = \frac{a}{b}$

(9) Seien $a, b \in K$. Dann gilt: $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

Beweis:

Sei $a \cdot b = 0$ und $b \neq 0$. Wir müssen dann $a = 0$ zeigen.

$0 = a \cdot b \Rightarrow 0 = 0 \cdot b^{-1} = (a \cdot b) b^{-1}$

$= a \cdot (b \cdot b^{-1}) = a \cdot 1 = a$

Folgerung:

Ist n eine zusammengesetzte Zahl, Dann ist

$(\mathbb{Z}/n, +, \cdot)$ kein Körper.

Beweis:

Ist $n = p \cdot q$ $1 < p, q < n \Rightarrow \bar{p} \cdot \bar{q} = \bar{0} \in \mathbb{Z}/n$

aber $\bar{p}, \bar{q} \neq 0$ d.h. die Folgerung (9) ist nicht erfüllt.

Bem.

In einem Körper hat die Gleichung $ax + b = 0$ für geg. $a \in K^*$, $b \in K$ genau 1 Lösung nämlich $x = -\frac{b}{a}$