GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Vorkurs Mathematik für Mathematikstudierende

Tag 5

Dr. Johannes Horn
horn@math.uni-frankfurt.de

09. - 13. Oktober 2023, 10.15 - 11.45 Uhr,
Hörsaal H11

Wiederholung

Eigenschaften von Abbildungen

Sei $f : M \to N$ eine Abbildung. Dann ist f

injektiv	$\Leftrightarrow$	Alle $n \in N$ haben höchstens ein Urbild unter f.
surjektiv	$\Leftrightarrow$	Alle $n \in N$ haben mindestens ein Urbild unter f.
bijektiv	$\Leftrightarrow$	Alle $n \in N$ haben genau ein Urbild unter f.

Quantoren

$\forall\, m \in M : A(m)$	„Für alle $m \in M$ gilt $A(m)$."
$\exists\, m \in M : A(m)$	„Es existiert ein $m \in M$, sodass $A(m)$ gilt."
$\exists!\, m \in M : A(m)$	„Es existiert genau ein $m \in M$, sodass $A(m)$ gilt."

Plan für heute

i) Mächtigkeit von Mengen
ii) Kartesisches Produkt
iii) Potenzmenge
iv) Anwendung des Modulo rechnen: Fehlerkorrektur.

Mächtigkeit endlicher Mengen

Definition 42

Sei M eine endliche Menge. Dann ist die Mächtigkeit (oder Kardinalität) der Menge $|M|$ definiert als die Anzahl der Elemente von M.

Beispiele:

i) $|\varnothing| = 0$ und die leere Menge ist die einzige Menge mit dieser Eigenschaft.

ii) $|\{1, 2, 3, 4\}| = 4$.

iii) $|\{\varnothing, \{\varnothing, \{\varnothing\}\}\}| = 2$.

Satz 43

i) *Seien M, N endliche Mengen, dann ist $|M \cup N| = |M| + |N| - |M \cap N|$.*

ii) *Seien $M_1, \ldots, M_k$ endliche Mengen, sodass für alle $1 \leq i, j \leq k$ mit $i \neq j$ gilt $M_i \cap M_j = \varnothing$, dann ist*

$$|M_1 \cup M_2 \cup \cdots \cup M_k| = |M_1| + \cdots + |M_k|. \tag{1}$$

Beweis von Satz 43 i).

Nach Vorraussetzung ist $M \cap N \subset N$ endlich, also können wir die Elemente von $M \cap N$ nummerieren, sodass

$$M \cap N = \{x_1, \ldots, x_k\}$$

mit $k = |M \cap N|$. Dann können wir die beiden Mengen M und N schreiben als

$$M = \{x_1, \ldots, x_k, m_{k+1}, \ldots, m_l\}$$
$$N = \{x_1, \ldots, x_k, n_{k+1}, \ldots, n_j\},$$

wobei $l = |M|$ und $j = |N|$. Dann ist

$$\begin{aligned} |M \cup N| &= |\{x_1, \ldots, x_k, m_{k+1}, \ldots, m_l, n_{k+1}, \ldots, n_j\}| \\ &= l + j - k = |M| + |N| - |M \cap N|. \end{aligned}$$

□

Beweis von Satz 43 ii).

Beweis mit Induktion über k.
IA: Für $k = 1$ ist nichts zu zeigen: $|M_1| = |M_1|$.
IV: Sei $k \in \mathbb{N}$ fest, sodass für alle endlichen paarweise disjunkten Mengen $M_1, \dots, M_k$ die Gleichung (1) gilt.
IS: Seien $M_1, \dots, M_{k+1}$ endliche, paarweise disjunkte Mengen. Dann ist $N = M_1 \cup \dots \cup M_k$ eine Menge mit

$$N \cap M_{k+1} = (M_1 \cup \dots \cup M_k) \cap M_{k+1}$$
$$\overset{\text{Blatt 1 A4}}{=} (M_1 \cap M_{k+1}) \cup \dots \cup (M_k \cap M_{k+1}) = \varnothing.$$

Damit folgt aus i), dass $|N \cup M_{k+1}| = |N| + |M_{k+1}|$. Also gilt

$$|M_1 \cup \dots \cup M_{k+1}| = |N \cup M_{k+1}| = |N| + |M_{k+1}|$$
$$= |M_1 \cup \dots \cup M_k| + |M_{k+1}| \overset{IV}{=} |M_1| + \dots + |M_k| + |M_{k+1}|.$$

□

Mächtigkeit von Mengen und Abbildungen

Satz 44

Seien M, N endliche Mengen und $f : M \to N$ eine Abbildung.

i) *Wenn f injektiv ist, dann gilt $|M| \leq |N|$.*

ii) *Wenn f surjektiv ist, dann gilt $|M| \geq |N|$.*

iii) *Wenn f bijektiv ist, dann gilt $|M| = |N|$.*

Beweis.

Sei $k = |N|$ und $N = \{n_1, \ldots, n_k\}$. Wir können M wie folgt zerlegen:

$$M = f^{-1}(N) = f^{-1}(\{n_1\} \cup \{n_2\} \cup \cdots \cup \{n_k\})$$
$$\overset{\text{Blatt5}}{=} f^{-1}(\{n_1\}) \cup f^{-1}(\{n_2\}) \cup \cdots \cup f^{-1}(\{n_k\}).$$

Dabei gilt für $1 \leq i, j \leq k$ mit $i \neq j$

$$f^{-1}(\{n_i\}) \cap f^{-1}(\{n_j\}) \overset{\text{Blatt5}}{=} f^{-1}(\{n_i\} \cap \{n_j\}) = f^{-1}(\varnothing) = \varnothing.$$

Beweis.

Also gilt nach Satz 43

$$|M| = |f^{-1}(\{n_1\})| + |f^{-1}(\{n_2\}| + \cdots + |f^{-1}(\{n_k\})|. \tag{2}$$

Zu i): Falls f injektiv ist, dann hat jedes $n_i \in N$ höchstens ein Urbild. Damit gilt $\forall\, i : |f^{-1}(\{n_i\})| \leq 1$. Also ist nach Gleichung (2)

$$|M| = |f^{-1}(\{n_1\})| + |f^{-1}(\{n_2\}| + \cdots + |f^{-1}(\{n_k\})| \leq \underbrace{1 + 1 + \cdots + 1}_{k \text{ viele}} = |N|.$$

Zu ii): Falls f surjektiv ist, dann hat jedes $n_i \in N$ mindestens ein Urbild. Damit gilt $\forall\, i : |f^{-1}(\{n_i\})| \geq 1$. Also ist nach Gleichung (2)

$$|M| = |f^{-1}(\{n_1\})| + |f^{-1}(\{n_2\})| + \cdots + |f^{-1}(\{n_k\})| \geq \underbrace{1 + 1 + \cdots + 1}_{k \text{ viele}} = |N|.$$

Zu iii): Falls f bijektiv ist, dann ist f injektiv und surjektiv. Also gilt $|M| \leq |N|$ und $|M| \geq |N|$. Folglich ist $|M| = |N|$. □

Kartesisches Produkt

Definition 45

Seien M und N Mengen. Eine Tupel ist ein geordnetes Paar (m, n) mit $m \in M$ und $n \in N$.

Das kartesische Produkt $M \times N$, gesprochen „M kreuz N“, ist definiert als

$$M \times N = \{(m, n) \mid m \in M \wedge n \in N\}.$$

Achtung: Die Ordnung ist entscheidend. Sei $M = N = \mathbb{Z}$. Dann ist $(2, 1) \neq (1, 2)$.

Beispiel: $M = \{1, 2, 3\}$, $N = \{a, b\}$. Dann ist

$$M \times N = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Definition 46 (Reelle Ebene)

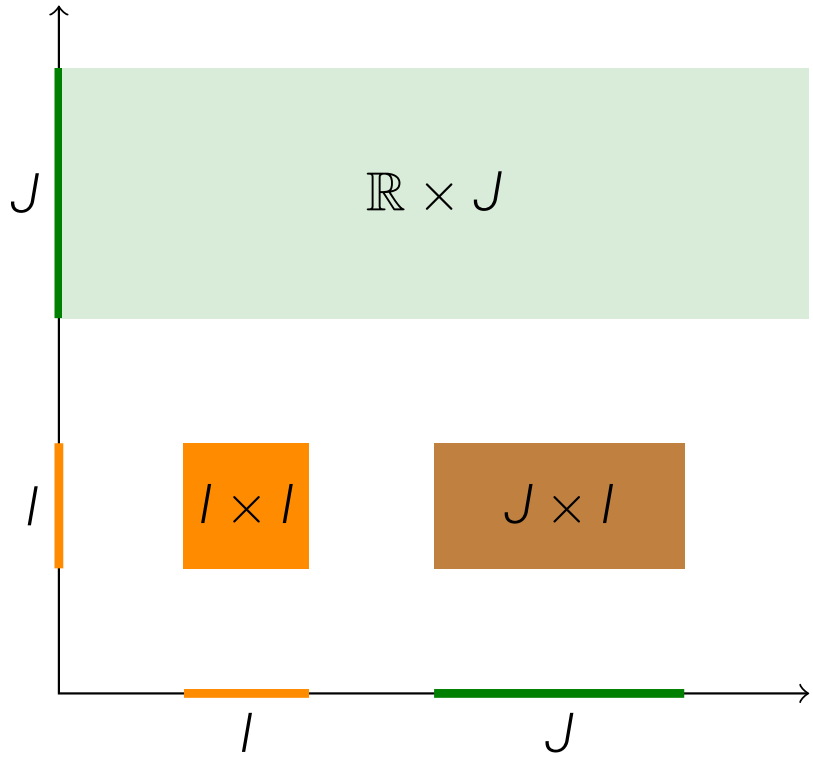
Sei nun $M = N = \mathbb{R}$. Dann ist

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

die reelle Ebene.

Sei $I = [1, 2] = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$
und $J = [3, 5] = \{x \in \mathbb{R} \mid 3 \leq x \leq 5\}$.
Dann ist

$$I \times I = \{(x, y) \in \mathbb{R}^2 \mid 1 \leq x, y \leq 2\},$$
$$\mathbb{R} \times J = \{(x, y) \in \mathbb{R}^2 \mid 1 \leq y \leq 2\},$$
$$J \times I = \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; \begin{array}{l} 3 \leq x \leq 5 \\ 1 \leq y \leq 2 \end{array} \right\}.$$



n-faches kartesisches Produkt

Definition 47

Sei M eine Menge. Dann ist ein n-Tupel mit Werten in M eine geordnete Folge $(m_1, \ldots, m_n)$ mit $m_i \in M$. Das n-te kartesische Produkt M^n ist definiert als

$$M^n = \{(m_1, \ldots, m_n) \mid m_i \in M\}.$$

Beispiel:

i) $\mathbb{R}^3$ „der drei-dimensionale Raum“: Tripel (x, y, z) mit $x, y, z \in \mathbb{R}$.

ii) Sei $M = \{0, 1\}$. Dann ist

$$\begin{aligned} M^3 = \{&(0,0,0), (1,0,0), (0,1,0), (0,0,1), \\ &(1,1,0), (1,0,1), (0,1,1), (1,1,1)\}. \end{aligned}$$

Mächtigkeit des kartesischen Produkts

Satz 48

Seien M, N endliche Mengen und n eine natürliche Zahl. Dann ist

i) $|M \times N| = |M| \cdot |N|$.

ii) $|M^n| = |M|^n$.

Beweis.

Zu i): Für jedes $m \in M$ existieren $|N|$ Paare von der Form (m, n). Also existieren insgesamt $|M| \cdot |N|$ viele Paare in $M \times N$.
Zu ii): Beweis mit Induktion über n.
IA: $n = 1$ ist die Aussage offensichtlich erfüllt.
IV: Sei $n \in \mathbb{N}$ fest, sodass $|M^n| = |M|^n$.
IS: Es gilt $M^{n+1} = M^n \times M$. Das heißt nach i) gilt

$$|M^{n+1}| = |M^n \times M| \overset{i)}{=} |M^n| \cdot |M| \overset{IV}{=} |M|^n \cdot |M| = |M|^{n+1}.$$

Potenzmenge

Definition 49

Sei M eine Menge. Dann ist die Potenzmenge $\mathcal{P}(M)$ die Menge aller Teilmengen von M.

Beispiele:

i) Sei $M = \{1, 2\}$, dann ist $\mathcal{P}(M) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

ii) Sei $M = \varnothing$. Dann ist $\mathcal{P}(M) = \{\varnothing\}$.

Satz 50

Sei M eine Menge mit Mächtigkeit $|M|$. Dann hat die Potenzmenge die Mächtigkeit $|\mathcal{P}(M)| = 2^{|M|}$.

Erster Beweis von Satz 50 mit Induktion.

Induktion über die Mächtigkeit $k = |M|$.
IA: Für $k = 1$ ist $M = \{m\}$. Dann ist $\mathcal{P}(M) = \{\varnothing, \{m\}\}$. Damit stimmt die Aussage.
IV: Sei $k \in \mathbb{N}$ fest, sodass für jede endliche Menge M mit $|M| = k$ gilt $|\mathcal{P}(M)| = 2^k$.
IS: Sei M eine Menge mit $|M| = k + 1$. Sei $m \in M$. Dann ist $|M \setminus \{m\}| = k$.
Sei $N \subset M$ eine Teilmenge. Dann ist entweder $m \in N$ oder $m \notin N$. Falls $m \notin N$, dann ist $N \subset M \setminus \{m\}$. Nach Induktionsvorraussetzung existieren 2^k dieser Teilmengen. Falls $m \in N$, dann existiert eine Teilmenge $N' \subset M \setminus \{m\}$, sodass $N = N' \cup \{m\}$. Nach Induktionsvorraussetzung existieren auch 2^k solcher Teilmengen N. Also gibt es insgesamt $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ Teilmengen von M. □

Zweiter Beweis von Satz 50 Teil 1.

Sei $|M| = n$. Dann nummerieren wir die Elemente von M mit den Zifferen $1, \ldots, n$. Das heißt

$$M = \{m_1, m_2, \ldots, m_n\}.$$

Nun können wir für jede Teilmenge $N \subset M$ ein n-Tupel

$$(x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$$

definieren, sodass $x_i = 1$, wenn $m_i \in N$ und $x_i = 0$, wenn $m_i \notin\in N$. Dies definiert eine Abbildung

$$F : \mathcal{P}(M) \to \{0, 1\}^n, \quad N \mapsto (x_1, x_2, \ldots, x_n).$$

Als nächstes zeigen wir, dass die Abbildung F bijektiv ist.
Injektivität: Seien $N_1, N_2 \subset M$ zwei Teilmengen mit $F(N_1) = (x_1, \ldots, x_n), F(N_2) = (y_1, \ldots, y_n)$ und $F(N_1) = F(N_2)$. Dann ist $x_i = 1$ genau dann, wenn $y_i = 1$. Das heißt $m_i \in N_1$ genau dann, wenn $m_i \in N_2$. Also gilt $N_1 = N_2$.

Zweiter Beweis von Satz 50 Teil 2.

Surjektivität: Sei $(x_1, \ldots, x_n) \in \{0,1\}^n$. Definiere die Teilmenge

$$N = \{m_i \in M \mid x_i = 1\} \subset M.$$

Dann gilt offensichtlich $F(N) = (x_1, \ldots, x_n)$. Damit ist F surjektiv. Insgesamt ist $F : \mathcal{P}(M) \to \{0,1\}^n$ also bijektiv. Damit gilt nach Satz 44 $|\mathcal{P}(M)| = |\{0,1\}^n|$ und nach Satz 48 gilt $|\{0,1\}^n| = 2^n = 2^{|M|}$. □

Fehlerprüfung durch Modulo Rechnen

Problem:

i) Bei der Übermittlung von Zahlencodes werden einzelne Ziffern falsch übergeben oder gehen verloren.

ii) Menschen neigen zu Tippfehlern oder Zahlendreher bei Zahlencodes.

. Diese Fehler kann man durch das Hinzufügen von Prüfziffern zum Zahlencode feststellen. Hierbei wird oft das Modulo Rechnen verwendet.

Beispiel 51 (ISBN-10)

ISBN-10 (International Standard Book Number) wurde bis 2007 für die Identifizerung von Bücher verwendet. Eine ISBN-10 besteht aus 10 Ziffern

$$a_0\text{-}a_1a_2a_3\text{-}a_5a_6a_7a_8a_9\text{-}a_{10}$$

Hierbei sind $a_1, \ldots, a_9 \in \{0, \ldots, 9\}$ und die letzte Ziffer a_{10} kann zusätzlich den Wert X für 10 annehmen.

Fehlerprüfung bei der ISBN-10

Für eine gültige ISBN-10 gilt die Gleichung

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} = 0 \mod 11. \tag{3}$$

Angenommen ein Nutzer tippt eine Zahl falsch ein, dann kann diese Gleichung nicht mehr gelten.

Satz 52

Sei $a_1 \dots a_{10}$ eine gültige ISBN-10. Wenn wir genau eine Ziffer a_i ändern, ist Gleichung (3) *falsch.*

Beweis.

Angenommen der Fehler passiert an der Stelle i. D.h. wir ersetzen a_i durch $b_i \neq a_i$. Dann ist

$$\begin{aligned} &10a_1 + 9a_2 + \cdots + +(11-i)b_i + \cdots + a_{10} \\ =&a_1 + 2a_2 + \cdots + (11-i)b_i - (11-i)a_i + (11-i)a_i + \cdots + a_{10} \\ =&i(b_i - a_i) \mod 11. \end{aligned}$$

Da $i < 11$ und 11 eine Primzahl, ist dies nur gleich 0 modulo 11 teilbar, wenn $b_i - a_i$ durch 11 teilbar ist. Da aber

$$b_i - a_i \in \{-10, -9, \ldots, -2, -1, 1, 2, \ldots, 9, 10\}$$

ist dies nie der Fall. Also ist die Gleichung nicht erfüllt, wenn ein Tippfehler vorliegt. □

Auch Zahlendreher werden mit diesem Prüfverfahren zuverlässig erkannt (siehe Aufgabe). Seit 2007 wird die 13stellige Ziffernfolge ISBN-13 verwendet. Diese hat einen ähnlichen Prüfalgorithmus, der Tippfehler erkennt. Allerdings nicht alle Zahlendreher.

Fehlerprüfung bei der IBAN

Die IBAN (International Bank Account Number) besitzt einen sehr guten Prüfalgorithmus. Hier wird modulo 97 gerechnet und es werden Einzelfehler, Zahlendreher und Verschiebungen in der Ziffernfolge erkannt.
Für ein fiktives Bankkonto mit der IBAN

$$\text{DE}68210501700012345678$$

bei einer deutschen Bank funktioniert die Prüfung wie folgt:

i) Ersetze DE durch die Zahlen 1314:
$$131468210501700012345678$$

ii) Setze die ersten 6 Ziffern an das Ende der Nummer:
$$210501700012345678131468$$

iii) Berechne diese Zahl minus Eins modulo 97:
$$210501700012345678131467 \mod 97 = 0$$

Wenn das Ergebnis 0 ist, ist die Prüfung bestanden.

Tipps für das kommende Semester

1. **Suchen Sie sich eine Lerngruppe.**
2. **Reden Sie mit Ihren Kommoliton*innen über Mathematik.**
3. **Arbeiten Sie die Vorlesungen nach.**
4. **Lasst Sie sich nicht unterkriegen!**

Ende

Danke fürs Mitmachen und viel Erfolg im Studium!

Ich freue mich über weiteres Feedback:

horn@math.uni-frankfurt.de