Mathematik 1

Manfred Jäger-Ambrożewicz
www.mathfred.de
www.mathstat.de
10. Oktober 2025

Das Skript ist teilweise fragmentarisch und hat bestimmt etliche Mängel/Fehler. Über Hinweise würde ich mich freuen; z.B. per Email an jaegera ät htw-berlin punkt de

Das Skript genügt (noch?) nicht den Anforderungen, die an eine wissenschaftliche Arbeit gestellt werden, denn die Quellen zu vielen Aussagen werden (noch) nicht vor Ort angegeben.

Inhaltsverzeichnis

1 Logik

Man kann Logik als eigenständiges Fach betrachten. Wir konzentrieren uns aber auf die für die Mathematik nützlichen Aspekte bzw. Konzepte. Logik ist dabei ein *Hilfsmittel*, um Erkenntnisse zu gewinnen.[1] Wir sind nur so formal und nur so umfassend wie nötig. Mehr kann man hier nachlesen: `https://www.logicmatters.net/`. Gut sind auch Lee [3], Rosen [4] und Epp [1].

Aussagen, Verknüpfungen und Aussageformen

1.1 Definition: Wir definieren

i.) Eine **Aussage** ist ein *Satz*, der

[1] Wenn ich ein Wort kursiv schreibe wird, dann möchte ich verdeutlichen, dass etwas *ambivalentes sage*.

$$w = \text{“wahr”}$$

oder

$$f = \text{“falsch”}$$

sein kann. w bzw. f heißen **Wahrheitswerte**.

Für Aussagen verwenden wir die Buchstaben A, B, C, $A_1, A_2, ..., B_1, B_2, ...$ Also große Buchstaben vom Anfang des Alphabets; unter Umständen mit einem Index.

ii.) Wir **verknüpfen** Aussagen (insbesondere Aussagenatome) zu neuen Aussagen. Die Wahrheitswerte dieser neuen Aussagen haben dann Wahrheitswerte, die sich gemäß entsprechender Tafeln berechnen lassen (folgt).

▶ Ich hoffe, sie können auf Basis dieser Definition erkennen, wann eine Aussage vorliegt und wann nicht. Die Definition erfüllt nur bedingt die Anforderungen, die wir (Mathematiker*innen) an eine Definition stellen. Ehrlich gesagt, habe ich gar nicht vor, zu definieren, was ein `Satz` ist und was `wahr` und `falsch` bedeutet.

Aber: **Ich definiere mathematisch sorgfälig, wie man mit Aussagen umgeht.** `Satz, wahr, falsch` sind **undefinierte Grundbegriffe**.[2].

[2] So wie `Punkt` in der Geometrie und Menge in der Mengenlehre

Es gibt Aussagen, da weiß jeder, dass sie wahr sind: 7 ist eine Primzahl. Es gibt Aussagen, da weiß jeder, dass sie falsch sind: 3 ist ein Teiler von 8. Es gibt Aussagen, da wissen nur manche, dass sie wahr sind: Es gibt unendlich viele Primzahlen. Das der große Satz von Fermat wahr ist, dass wissen wir erst seit einigen Jahren. Für den Nachweis benötigten *wir* 350 Jahre.[3]

Jetzt erläutere ich Ihnen wie man Aussagen (bzw. mit Aussageformen) umgeht/rechnet.[4]

1.2 Definition: Aussagen kann man verknüpfen und erhält neue Aussagen. Den Wahrheitswert der durch **Verknüpfung(en)** erhaltenen Aussage erhält man durch Anwendung der folgenden Regeln.

i.) Wahrheitstafel für $\neg$ ("nicht")

A	$\neg A$
w	f
f	w

ii.) Wahrheitstafel für $\wedge$ (und)

[3] https://de.wikipedia.org/wiki/Grosser_Fermatscher_Satz

[4] Ich rechne, also bin ich.

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

iii.) Wahrheitstafel für $\vee$ (“oder”)

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

iv.) Wahrheitstafel für $\rightarrow$ (“impliziert”)

A	B	$A \rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

v.) Wahrheitstafel für $\leftrightarrow$ (“genau dann wenn”)

A	B	$A \leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

1.3 Definition: Logische Formeln/Aussageformeln/Aussageform

entstehen im ersten Schritt durch syntaktisch zulässige Verknüpfung von **Aussageatomen**, die wir mit $A, B, C, A_1, A_2, ...$ bezeichnen; Aussageatome lassen sich nicht zerlegen. Weitere logische Formeln können wir dann weiter mit Aussageatomen oder mit schon definierten Formeln erzeugen. Damit der Vorrang ersichtlich bleibt, verwenden wir **Klammern**. Für solche zusammengesetzten Formeln verwenden wir $F, F_1, F_2, ...$

Beispiel:

$$F_1 = (A \vee B) \to (C \wedge (A \to B))$$
$$F_1 = A \vee (B \to C) \wedge (A \to B)$$

Für jede **Belegung** der Aussageatome mit Wahrheitswerten können wir dann (u.U. mühsam) den Wahrheitswert von F bestimmen. Wenn Sie Lust haben, dann schreiben sie ein Programm.[5]

[5] https://de.wikipedia.org/wiki/Ada_Lovelace

1.4 Bemerkung: Was ist der Unterschied zwischen Aussagen und Aussageformen? Wir überlegen uns, was der Unterschied zwischen $3 \cdot 4 + 3$ und dem Term $x \cdot y + x$ ist. .....

Aussageformen sind Formeln/Terme in die man Aussagen einsetzen kann. Das (einsetzen) haben wir aber zunächst gar nicht vor. Wir interessieren uns vorwiegend, wie man mit den Aussageformen/Termen umgeht/rechnet. Später, wie man mit Aussageformen valide Argumente erhält.

- Aussagen haben eine *echte sachliche* Bedeutung.
- Aussageformeln sind nützlich, um valide Argumentationsformen/Beweisprinzipien zu erhalten. Das wird sich im folgenden zeigen.

1.5 Bemerkung: Die Wahrheitstafel für die Implikation ist:

A	B	$A \to B$
w	w	w
w	f	f
f	w	w
f	f	w

Wie überprüft man $W(A \to B) = w$?

Man muss nachweisen, dass:

$$W(A) = w \text{ und } W(B) = f$$

nicht eintreten kann.

- Sollte $W(A) = w$ sein, dann darf $W(B) = f$ nicht sein.
- Sollte $W(B) = f$ sein, dann darf $W(A) = w$ nicht sein.
- Für den Fall $W(A) = f$ muss man nichts prüfen !!!!

1.6 Bemerkung: Die folgende Aufgabe heißt **Wasons Auswahlaufgabe**[6]. Auf dem Tisch liegen vier Karten. Auf der einen Seite jeder Karte steht eine Zahl und die andere Seite ist braun oder rot.

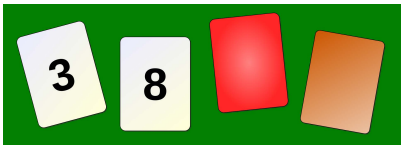


Abbildung 1.1: https://en.wikipedia.org/wiki/Wason_selection_task

Jetzt die Aufgabe:

[6] https://en.wikipedia.org/wiki/Wason_selection_task

Wie überprüft man, ob *"Wenn auf der Vorderseite eine gerade Zahl steht, dann ist die Rückseite rot"* wahr ist? Welche der Karten **muss** man dafür umdrehen?

A = Auf der Vorderseite steht eine gerade Zahl,

B = Die Rückseite ist rot.

Gilt $A \to B$?

Folgendes darf **nicht sein**: $W(A) = w$ **und** $W(B) = f$.

1.7 Bemerkung: Die Wahrheitstafel für die Implikation ist **gemäß Definition**:[7]

A	B	$A \to B$
w	w	w
w	f	f
f	w	w
f	f	w

Die beiden letzten Zeilen provozieren Fragen? Warum definiert man für die Fälle mit $W(A) = f$, dass $W(A \to B) = w$

[7] Siehe Smith in Introduction to formal Logic, Kapitel 18 https://www.logicmatters.net/ und die nächste Folie!

ist? Die folgenden Bemerkungen sind vielleicht verwirrend. Sie kann für unsere Zwecke ohne Schaden übersprungen werden.

Wir werden regelmäßig **zulässig** (deshalb grün) so argumentieren (das Argument heißt (**Modus Tollens**)):

> a.) Wenn A, dann B. B gilt nicht. **Also** gilt A nicht.

und so kann man **nicht argumentieren** (deshalb rot):

> b.) Wenn A, dann B. B gilt. **Also** gilt A.

Man sagt: Die Argumentationsform a.) ist gültig/valide. Argumentationsform b.) ist nicht gültig/invalide!

Dann sehen wir

- Die **vierte Zeile** der Tabelle für $\rightarrow$ ist passend definiert: Das sieht man an der zulässigen Argumentation a.). Die einzige Zeile mit $W(A \rightarrow B) = w$ und $W(B) = f$ ist die vierte Zeile. In dieser Zeile ist wie *gewünscht* $W(A) = f$. Wenn wir die vierte Zeile ändern, dann könnten wir $W(A) = f$ nicht ermitteln.

- Die **dritte Zeile** ist auch passend definiert. Das sieht man an b.). Denn: Es gibt zwei Zeilen mit $W(A \rightarrow B) = w$ und $W(B) = w$ [die dritte und die erste]. A

kann den Wert w oder den Wert f haben. Wir können also den Wahrheitswert nicht ermitteln und so soll es auch sein, denn die rote Argumentationsform ist invalide. Wenn man die dritte Zeile ändert, dann wäre b.) zulässig und man könnte merkwürdigerweise $W(A) = w$ ermitteln.

▶ Eine *brauchbare* Definition Verknüpfung der Implikation $\rightarrow$ muss also so sein, wie sie ist. (siehe auch Epp [1, Seite 68] zum Thema valide versus invalide Argumente)

1.8 Aufgabe 1.1: Bestimmen sie die Wahrheitswerte für

a.) $(A \wedge (A \rightarrow B)) \rightarrow B$

b.) $(A \vee B) \rightarrow (C \wedge (A \rightarrow B))$

1.9 Definition: Aussageformen F_1 und F_2 heißen **gleichwertig**, wenn sie für jede Belegung der Atomen, den gleichen Wert haben.

1.10 Aufgabe 1.2: Überprüfen Sie:

a.) $A \rightarrow B$ ist gleichwertig zu $\neg B \rightarrow \neg A$

b.) $A \rightarrow B$ glw $A \vee B$

c.) $A \to B$ glw $A \vee \neg B$

d.) $A \to B$ glw $\neg A \vee B$

▶ Wir benötigen regelmäßig die folgenden Gleichwertigkeiten. Die Gleichwertigkeiten sollte man *auswendig* können und zwar auch dann, wenn **man nachts geweckt wird**.

1.11 Satz: Es gilt

i.) $A \to B$ ist gleichwertig zu $\neg B \to \neg A$.

ii.) $A \to B$ ist gleichwertig zu $\neg A \vee B$.

iii.) $A \to B \wedge B \to A$ ist gleichwertig zu $A \leftrightarrow B$.

iv.) $\neg(A \vee B)$ ist gleichwertig zu $\neg A \wedge \neg B$ (**De Morgansche**[8] **Regel**).

v.) $\neg(A \wedge B)$ ist gleichwertig zu $\neg A \vee \neg B$ (**De Morgansche Regel**).

1.12 Aufgabe 1.3: Beweisen Sie alle Gleichwertigkeiten aus dem vorherigen Satz.

1.13 Bemerkung:

[8] https://de.wikipedia.org/wiki/Ada_Lovelace

- Wenn man die Gleichwertigkeit zweier Formeln verifizieren will, dann kann man die **Wahrheitstafel** für beide Formeln bestimmen. Dann sieht man gegebenenfalls, dass die beiden Formeln immer (bei jeder Belegung der Atome) den gleichen Wert haben.

- Es geht aber auch *verbal*.

  - $A \to B$ sei wahr. Kann dann $\neg B \to \neg A$ falsch sein? Wir nehmen an, dass $\neg B \to \neg A$ falsch ist. $\neg B \to \neg A$ falsch, bedeutet: $\neg B$ ist wahr, aber $\neg A$ ist falsch. Also A wahr und B falsch. Dann wäre aber $A \to B$ falsch. Wir erhalten einen Widerspruch: Die Voraussetzung $W(A \to B) = w$ ist also unvereinbar mit $W(\neg B \to \neg A) = f$. Also: Wenn $W(A \to B) = w$, dann $W(\neg B \to \neg A) = w$

  - $\neg B \to \neg A$ ... DIY

Prädikate

▶ Mathematik ohne x ist ni$x$.

1.14 Definition: $A(x)$ heißt **Prädikat**, wenn $A(x)$ für jede zulässige konkrete Einsetzungen von x eine Aussage/Aussageform ist. Die zulässigen Einsetzung x sind Elemente der Menge $\mathcal{U}$,

dem sogenannten **Universum**.

x ist ein *Platzhalter*. Dort kann man etwas einsetzen. Wenn man etwas zulässiges einsetzet, dann erhält man eine Aussage.

Beispiel:

$A(x) = x$ ist eine Primzahl.

Die Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3...\}$ ist die Menge der möglichen zulässigen Einsetzungen, d.h. $\mathcal{U} = \mathbb{N}$. Wenn wir z.B. 7 einsetzen, dann erhalten wir die wahre Aussage

7 ist eine Primzahl.

Wenn wir 4 einsetzen (das ist zulässig), dann erhalten wir die falsche Aussage

4 ist eine Primzahl.

1.15 Definition:

- $\forall$ für *für alle*
- $\exists$ für *es gibt*

▶ Auch die folgenden Regeln sollte man auswendig können

und natürlich verstanden haben.

1.16 Satz: Es gelten die folgenden Formeln der **Prädikatenlogik**

- $\neg(\forall x : A(x))$ ist gleichwertig zu $\exists\, x : \neg A(x)$
- $\neg(\exists x : A(x))$ ist gleichwertig zu $\forall\, x : \neg A(x)$

Aussageformen, Validität und Beweisprinzipien

1.17 Definition: Eine **Argumentationsform** ist eine Folge von Aussageformen (die wir gerne untereinander schreiben). Alle Aussageformen bis auf die letzte heißen **Hypothesen**. Die letzte Aussageformen der Argumentationsform heißt **Konklusion**.

Eine Argumentationsform heißt **valide bzw. gültig**, wenn für alle Belegungen in denen alle Hypothesen wahr sind, auch die Konklusion wahr ist.

Wir nennen eine gültige Argumentationsform auch **Beweisprinzip**.

1.18 Bemerkung: Das **Beweisprinzip** des **direkten Be-**

weises beruht auf der folgenden Beobachtung (siehe Epp [1, Seite 68]).

i.) Finde die Zeilen in denen gilt:

$W(A) = w$ (Zeile 1 und 2) **und**

$W(A \to B) = w$ (Zeile 1 und 3 und 4)

A	B	$A \to B$	A	B
w	w	w	w	w
w	f	f		
f	w	w		
f	f	w		

ii.) Nur die Zeile 1 erfüllt $W(A) = w$ und $W(A \to B) = w$. Dort ist $W(B) = w$. Also ist B wahr.

iii.) Diese gültige Argumentsform ist (**Modus Ponens**):

$$\begin{array}{l} W(A) = w \\ W(A \to B) = w \\ \hline \therefore \;\; W(B) = w \end{array}$$

$\therefore$ steht für **Also**

Man gibt die Argumentationsform Modus Ponens regelmäßig so an

$$\begin{array}{l} A \\ A \to B \\ \hline \therefore \;\; B \end{array}$$

1.19 Beispiel: Wir betrachten

$$\begin{array}{ll} & A \to (B \vee \neg C) \\ & B \to (A \wedge C) \\ \hline \therefore & A \to C \end{array}$$

1.20 Bemerkung: Eine Tautologie ist immer (für jede Belegung) wahr[9]. Der folgenden Tabelle entnehmen wir, dass $A \wedge (A \to B) \to B$ eine Tautologie ist.

A	B	$A \to B$	$A \wedge (A \to B)$	$A \wedge (A \to B) \to B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

Die Tautologie $A \wedge (A \to B) \to B$ *gehört* zu Modus Ponens.

1.21 Bemerkung: Die folgenden **Beweisprinzipien**[10] werden wir später oder in Übungen nutzen. Wir wollen jeweils beweisen, dass B wahr ist.

- **Modus Tollens**:
  $W(A) = w$ und $W(\neg B \to \neg A) = w$.
  Also: $W(B) = w$

[9] https://de.wikipedia.org/wiki/Clara_Immerwahr

[10] In Epp [1, Seite 66ff] werden diese Techniken **Rules of Inference** oder **Valide Argumente** genannt. Das ist vielleicht auch besser.

- **Widerspruchsbeweis**/Reductio ad absurdum[11] :
  $W(A) = w$ und $W(A \wedge \neg B \rightarrow f) = w$.
  Also: $W(B) = w$

- **Widerspruchsbeweis**/Reductio ad absurdum:
  $W(\neg B) = w$ und $W(\neg B \rightarrow A \wedge \neg A) = w$.
  Also: $W(B) = w$

- **Fallunterscheidung**:
  $W(A1 \vee A2) = w$ und $W(A1 \rightarrow B) = w$ und $W(A2 \rightarrow B) = w$.
  Also: $W(B) = w$

- **Ersetzung**:
  $W(A \vee B) = w$ und $W(A) = f$.
  Also: $W(B) = w$

Beweis(e): Siehe Epp [1, Seite 66ff].

1.22 Bemerkung: Mathematische Beweise bestehen aus Sequenzen solcher valider Argumente.

1.23 Bemerkung: Warum funktioniert Modus Tollens?

- $\neg B \rightarrow \neg A$ und $A \rightarrow B$ sind gleichwertig.

[11] Rosen S. 90f erläutert dieses Beweisprinzip und gibt Beispiele an. Nützlich sind auch die Erläuterungen in Lee [3] und natürlich Epp [1, Seite 66ff]

Warum funktioniert Reductio ad absurdum?

- $A \wedge \neg B \to f$ und $A \to B$ sind gleichwertig.

2 Mengenlehre

2.1 Beschreibende Definition: Eine **Menge** M ist die Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.

2.2 Bemerkung: Die obige (beschreibende) Definition stammt von Georg Cantor[1].

2.3 Bemerkung: Die Mengenlehre ist die **Lingua franca** (**Verkehrssprache**) der Mathematik. Wir werden nicht definieren, was eine Menge ist. Wir lernen also *nur* wie man mathematisch mit Mengen **umgeht**. Wir werden *nur* bestimmte **Beziehungen** zwischen Mengen definieren und **Konstruktionsprinzipien** für neue Mengen definieren. `Mengen` und `ist Element von` bleiben **undefinierte Grundbegriffe**.

[1] `https://de.wikipedia.org/wiki/Georg_Cantor`

2.4 Bemerkung: Für Mengen verwenden wir typischerweise (das ist also eine Konvention) die Buchstaben M, N bzw. meistens A, B, C bzw. $A_1, A_2, ...$ und für Elemente x, y, z bzw. $x_1, x_2, ...$ Wenn ein *Objekt* x ein Element von A ist, dann schreiben wir

$$x \in A.$$

Wenn ein *Objekt* x **nicht** Element von A ist, dann schreiben wir

$$x \notin A.$$

2.5 Bemerkung: Wir geben Mengen gelegentlich durch Aufzählung der Elemente an, die dann in **geschweiften** Klammern eingeschlossen werden. Die Menge der natürlichen Zahlen ist z.B.

$$\mathbb{N} := \{1, 2, 3, 4, ...\}.$$

"..." verwenden wir nur, wenn die Fortsetzung eindeutig ist.

Wir können Mengen auch durch eine Beschreibung so angeben:

$$\mathbb{N} = \{x \mid x \text{ ist eine natürliche Zahl}\}$$

2.6 Bemerkung (Axiomatik): Seit Euklid verwenden Mathematiker die sogenannte **axiomatische Methode**. Ein **Axiom** ist eine **unbewiesen als wahr angenommen Aussage**. Ausgehend von den Axiomen werden dann Aussagen

deduktiv abgeleitet.

Ein Axiomensystem sollte:

- widerspruchsfrei sein,
- kurz und einfach sein,
- logisch unabhängige Aussagen enthalten.

2.7 Axiom: Dass zwei Mengen A bzw. B gleich sind, bedeutet:

i.) Jedes Element, das ein Element von A ist, ist auch ein Element von B und

ii.) jedes Element, das ein Element von B ist, ist auch ein Element von A.

$A = B$ bedeutet also:

$$x \in A \text{ gdw. } x \in B.$$

2.8 Beispiel:

$A = \{n \in \mathbb{N} \,|\, n \neq 1 \text{ und } n \text{ ist nur durch sich und 1 teilbar}\}$
$B = \{n \in \mathbb{N} \,|\, n \text{ hat genau 2 Teiler }\}$

Es gilt $A = B$. Wie beweist man das?

2.9 Bemerkung: Wichtige Mengen

- $\mathbb{N}$ bezeichnet die Menge der natürlichen Zahlen. $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$.
  Wir beachten, dass 0 keine natürliche Zahl ist.
  $\mathbb{P} = \{p \in \mathbb{N} | p \text{ ist eine Primzahl}\}$.

- $\mathbb{Z}$ bezeichnet die Menge der ganzen Zahlen. $\mathbb{Z} = \{0, -1, 1, -2, 2, -3,$

- $\mathbb{Q}$ bezeichnet die Menge der rationalen Zahlen. $\mathbb{Q} = \{\frac{a}{b} \,|\, a, b \in \mathbb{Z} \text{ und } b \neq 0\}$.

- $\mathbb{R}$ bezeichnet die Menge der reellen Zahlen. $\mathbb{R} = ...?$

2.10 Definition: Es seien A und B Mengen. Wenn für jedes $x \in A$ auch $x \in B$ gilt, dann schreiben wir $A \subset B$. Wir sagen in diesem Fall, dass A eine **Teilmenge** von B ist.

2.11 Definition (Verknüpfungen): Es seien A und B Mengen.

i.) Wir definieren

$$A \cap B := \{x \,|\, x \in A \text{ und } x \in B\}.$$

Wir nennen $A \cap B$ den **Durchschnitt** von A und B.

ii.) Wir definieren

$$A \cup B := \{x \,|x \in A \text{ oder } x \in B\}.$$

Wir nennen $A \cup B$ den **Vereinigung** von A und B.

iii.) Wir definieren

$$A \setminus B := \{x \,|x \in A \text{ und } x \notin B\}.$$

Wir nennen $A \setminus B$ die **Differenzmenge** von A und B.

2.12 Satz: Es seien A, B, C Mengen. Dann gelten die folgenden *Gesetze*:

- Kommutativ-Gesetz: $A \cup B = B \cup A$
- Kommutativ-Gesetz: $A \cap B = B \cap A$
- Assoziativ-Gesetz: $(A \cup B) \cup C = A \cup (B \cup C)$
- Assoziativ-Gesetz: $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributivgesetz: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Distributivgesetz: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

2.13 Definition:: Es sei A eine Menge. Wir definieren

$$\mathcal{P}(A) := \{B \,|B \subset A\}.$$

$\mathcal{P}(A)$ heißt die **Potenzmenge** von A.

2.14 Definition: Es sei G eine Menge und $A \subset G$. Wir definieren

$$A^c := \{x \in G \,|\, x \notin A\}.$$

A^c heißt das **Komplement** von A (in G). G heißt in diesem Zusammenhang **Grundmenge**.

2.15 Satz: A, B, G seien Mengen und $A, B \subset G$. Dann gilt

- i.) $A \setminus B = A \cap B^c$
- ii.) $(A \cup B)^c = A^c \cap B^c$
- iii.) $(A \cap B)^c = A^c \cup B^c$
- iv.) $(A^c)^c = A$
- v.) $A \subset B$ impliziert $B^c \subset A^c$

2.16 Definition: Es seien A, B Mengen. Wir definieren

$$A \times B := \{(x, y) \,|\, x \in A \text{ und } y \in B\}.$$

$A \times B$ heißt das **kartesisches Produkt** von A und B. Die Elemente von $A \times B$ sind **geordnete Paare** von Elementen aus A bzw. B.

- Beachte unbedingt: $\{1, 2\} = \{2, 1\}$. Aber $(1, 2) \neq (2, 1)$.
- ... man muss also die Form der Klammern beachten.

3 Relationen und Abbildungen

3.1 Definition: Es seien A, B Mengen. Eine Teilmenge $R \subset A \times B$ heißt **Relation** auf A kreuz B bzw. von A auf B.

Wenn $A = B$ ist, dann heißt $R \subset A \times A$ **Relation** auf A.

Wenn $(x, y) \in R$, dann schreiben wir $x\,R\,y$ und sagen, dass die Relation R zwischen x und y gilt. Oder wir sagen dann, dass x und y zueinander in der Relation R stehen.

3.2 Bemerkung: Wir können (jedenfalls manche) Relationen anschaulich mittels **gerichteter Graphen** oder mittels einer **Inzidenzmatrix** darstellen.

3.3 Definition: Sei R eine Relation auf einer Menge A. Wir definieren:

- R ist **reflexiv**, falls:
  für alle $x \in A$ gilt: $x\,R\,x$.

- R ist **symmetrisch**, falls:
  für alle $x, y \in A$ gilt: Gilt $x\,R\,y$, so gilt auch $y\,R\,x$.

- R ist **transitiv**, falls:
  für alle $x, y, z \in A$ gilt: Gilt $x\,R\,y$ und $y\,R\,z$, so gilt auch $x\,R\,z$.

Eine Relation R auf A, die reflexiv, symmetrisch und transitiv ist, heißt **Äquivalenzrelation**.

Es sei R eine Äquivalenzrelation auf A und $x \in A$. Dann heißt die Menge

$$[x] = \{b \in A |\, bRx\,\}$$

die **Äquivalenzklasse zum Repräsentanten** x. $[x]$ beinhaltet also alle x, die zu b in Relation stehen.

3.4 Definition: Es sei R eine Relation auf einer Menge A. Wir definieren:

- R ist **anti-symmetrisch**, falls:
  für alle $x, y \in A$ gilt: $x\,R\,y$ und $y\,R\,x$ impliziert $x = y$.

- R ist **vollständig**, falls:

für alle $x, y \in A$ gilt: $x\,R\,y$ oder $y\,R\,x$.

3.5 Bemerkung: Manchmal ist eine äquivalente Charakterisierung für die Eigenschaft anti-symmetrisch bequemer. R ist genau dann **anti-symmetrisch**, wenn $x \not R\, y$ oder $y \not R\, x$ für alle x, y mit $x \neq y$ gilt

3.6 Definition: Eine Relation R auf A heißt **partielle Ordnung**, falls R reflexiv, transitiv und anti-symmetrisch ist.

Ist R eine partielle Ordnung und zudem vollständig, dann heißt R eine **vollständige Ordnung**.

3.7 Definition: Es seien A und B Mengen. Eine **Abbildung** f wird durch

- die Angabe der Mengen A und B sowie
- einer **Zuweisungsregel**, die jedem $x \in A$ genau ein Element $y \in B$ zuweist,

definiert.

Symbolisch geben wir eine Abbildung so an:

$$f : A \to B, x \mapsto f(x)$$

Wir verwenden die folgenden Begriffe:

- A heißt **Definitionsbereich** von f.
- B heißt **Zielmenge**.
- x heißt das **Argument** von $f(x)$.
- Ist $y = f(x)$, dann heißt y das **Bild** von x und x ein **Urbild** von y.
- $f(A) := \{f(x) \,|x \in A\}$ heißt das Bild oder der Wertebereich von f.
- Für $V \subset B$ heißt $f^{-1}(V) = \{x \in A \,|f(x) \in V\}$ das **Urbild** von V.
- Für $U \subset A$ heißt $\{f(x) \,|x \in U\}$ das **Bild** von U.

3.8 Definition: Es seien $f : A \to B$ und $g : B \to C$ Abbildungen. Dann heißt die Abbildung

$$g \circ f : A \to C, x \mapsto g(f(x))$$

die **Hintereinanderausführung** von g nach f.

3.9 Definition: Es sei $f : A \to B$ eine Abbildung.

- f heißt **injektiv**, falls: Für alle $x, y, x \neq y, x, y \in A$ gilt $f(x) \neq f(y)$.
  Unterschiedliche Elemente des Definitionsbereichs ha-

ben unterschiedliche Bilder.

- f heißt **surjektiv**, falls: Für alle $y \in B$ gibt es ein $x \in A$ mit $f(x) = y$.
  Jedes Element der Zielmenge wird *erreicht*.

- f heißt **bijektiv**, falls f injektiv und surjektiv ist.

3.10 Definition: **Definition:** Es sei $f : A \to B$ eine bijektive Abbildung. Die Abbildung

$$g : B \to A \text{ mit } g(y) = x \text{ falls } f(x) = y$$

heißt **Umkehrabbildung (oder Inverse)** von f. Wir bezeichnen die Umkehrabbildung mit f^{-1}. Das x mit $g(y) = x$ ist für jedes y eindeutig bestimmt [denn f ist bijektiv.]

3.11 Bemerkung: i.) Wir benötigen die Injektivität, da wir sonst nicht wüssten, welchen Wert wir für $g(y)$ nehmen sollen. ii.) Wir benötigen die Surjektivität, damit f^{-1} auf ganz B definiert werden kann. Wäre f nur injektiv, dann könnte man die Umkehrabbildung *immerhin* auf Bild(f) definieren.

3.12 Satz: Es sei $f : A \to B$ eine Abbildung. f ist genau dann bijektiv, wenn es eine Abbildung $g : B \to A$ gibt, so

dass

$$g \circ f = \mathrm{id}_A \text{ und } f \circ g = \mathrm{id}_B.$$

In diesem Fall ist $f^{-1} = g$.

Dieser Satz eignet sich zum Überprüfen der Bijektivität.

3.13 Definition: i.) Zwei Mengen A und B heißen **gleich mächtig**, wenn es eine Bijektion zwischen A und B gibt.

ii.) $A \neq \emptyset$ heißt **endlich**, falls es ein $k \in \mathbb{N}$ gilt, so dass: Es gibt eine Bijektion zwischen A und $\{1, ..., k\}$.

iii.) Eine Menge A heißt **abzählbar unendlich**, falls es eine Bijektion $f : A \to \mathbb{N}$ gibt.

4 Vollständige Induktion

4.1 Bemerkung (Axiomatik): Seit Euklid verwenden Mathematiker die sogenannte **axiomatische Methode**. Ein **Axiom** ist eine **unbewiesen als wahr angenommen Aussage**. Ausgehend von den Axiomen werden dann Aussagen deduktiv abgeleitet.

Ein Axiomensystem sollte:

- widerspruchsfrei sein,
- kurz und einfach sein,
- logisch unabhängige Aussagen enthalten.

4.2 Bemerkung: Natürliche Zahlen $\mathbb{N}$ – Axiomensystem von Giuseppe Peano[1]

A1: 1 ist eine natürliche Zahl.

[1] https://de.wikipedia.org/wiki/Giuseppe_Peano

A2: Jede natürliche Zahl hat genau einen von 1 verschiedenen Nachfolger, der eine natürliche Zahl ist.

A3: Verschiedene natürliche Zahlen haben verschiedene Nachfolger.

A4: Für jede Teilmenge $M \subset \mathbb{N}$ mit

- $1 \in M$
- Ist k ein Element von M, so ist auch der Nachfolger von k ein Element von M

gilt: $M = \mathbb{N}$

4.3 Bemerkung: Vollständige Induktion – Beweisprinzip

- Es sei $A(n)$ eine Aussage über die natürliche Zahl n.
  - **Induktionsanfang (IA)**: $A(1)$ ist wahr.
  - **Induktionsschluss (IS)**: Für alle $k \geq 1$ gilt: Wenn $A(k)$ wahr ist, dann ist auch $A(k+1)$ wahr.
- Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Die Teil "Wenn $A(k)$ wahr ist" heißt **Induktionsvoraussetzung (IV)**

5 Zahlentheorie

5.1 Definition: Die Menge $\{1, 2, 3, 4, ...\}$ heißt Menge der **natürlichen Zahlen**. Wir bezeichnen die Menge der natürlichen Zahlen mit $\mathbb{N}$, also

$$\mathbb{N} = \{1, 2, 3, 4, ...\}$$

Wenn k eine natürliche Zahl bezeichnen soll, dann schreiben wir $k \in \mathbb{N}$.

Die Menge $\{0, -1, 1, -2, 2, -3, 3, ...\}$ heißt Menge der **ganzen Zahlen**. Die Menge der ganzen Zahlen bezeichnen wir mit $\mathbb{Z}$. Wenn k eine ganze Zahl bezeichnen soll, dann schreiben wir $k \in \mathbb{Z}$.

▶ Zahlentheorie beschäftigt sich mit $\mathbb{Z}$.

5.2 Definition: Es seien $a, b \in \mathbb{Z}, b \neq 0$. b heißt **Teiler** von a, wenn es ein $q \in \mathbb{Z}$ gibt mit $bq = a$. In diesem Fall schreiben

wir $b|a$ und sagen b teilt a. Wir sagen dann auch, dass a ein (ganzzahliges) **Vielfaches** von b ist.

▶ Die 0 ist speziell: 0 ist Teiler keiner Zahl (sie wird bei der Definition ausgeschlossen), wird aber von jeder Zahl geteilt.

5.3 Satz: i.) Wenn $c|b$ und $b|a$, dann $c|a$.
ii.) Wenn $b_1|a_1$, $b_2|a_2$, dann $b_1b_2|a_1a_2$.
iii.) Wenn $b|a_1$, $b|a_2$ und $\alpha, \beta \in \mathbb{Z}$, dann $b|(\alpha a_1 + \beta a_2)$.
iv.) Wenn $b|a$ und $a|b$, dann $a = b$ oder $a = -b$.

▶ Zwei Fälle von iii.) sind besonders wichtig.

1. Wenn $b|a_1$, $b|a_2$, dann $b|(a_1 + a_2)$. [das ist der Fall $\alpha = 1, \beta = 1$]

2. Wenn $b|a_1$, $b|a_2$, dann $b|(a_1 - a_2)$. [das ist der Fall $\alpha = 1, \beta = -1$]

5.4 Satz (Division mit Rest): Es sei $a, b \in \mathbb{Z}, b \neq 0$. Dann gibt es genau eine Darstellung

$$a = bq + r \text{ mit } q, r \in \mathbb{Z}, 0 \leq r < |b|.$$

Man nennt

- a Dividend

- b Divisor
- q Quotient
- $r = r_{a/b}$ **Rest** [bei Division von a durch b]

5.5 Definition: Es seien $a, b \in \mathbb{Z}$. Eine ganze Zahl $d \in \mathbb{Z}, d \neq 0$ heißt ein gemeinsamer Teiler von a und b, falls $d|a$ und $d|b$. Den **größten gemeinsamen Teiler** von a, b bezeichnet man mit $\mathrm{ggT}(a, b)$.

5.6 Satz: Es seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gilt

$$\mathrm{ggT}(a,b) = \begin{cases} |b| & \text{falls } r_{a/b} = 0 \\ \mathrm{ggT}(b, r_{a/b}) & \text{sonst} \end{cases}$$

5.7 Bemerkung: Der Satz zeigt, wie man den ggT bestimmen kann. Das Verfahren heißt **Euklid'scher Algorithmus**.

Mit dem **erweiterten euklid'schen Algorithmus** kann man auch immer $\alpha, \beta \in \mathbb{Z}$ bestimmen, so dass

$$\mathrm{ggT}(a,b) = \alpha \cdot a + \beta \cdot b.$$

5.8 Satz (Bezout's Theorem): Es seien a, b, ganze Zahlen. Dann gibt es $\alpha, \beta \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a,b) = \alpha \cdot a + \beta \cdot b.$$

5.9 Bemerkung: Es gibt 10 Typen von Menschen. Diejenigen, die die **binären Zahlen** kennen, und die Anderen. Gemeint war also

$$(10)_2 = 1 \cdot 2^1 + 0 \cdot 2^0 = (2)_{10} = 2 \cdot 10^0 = 2\mathrm{E}$$

5.10 Satz: Es sei $b > 1$ eine natürliche Zahl (wird in diesem Zusammenhang **Basis** genannt). Dann lässt sich jede natürliche Zahl n eindeutig in der Form

$$\begin{aligned} n &= a_m b^m + a_{m-1} b^{m-1} + ... + a_1 b + a_0 \\ &= (a_m\, a_{m-1} \,...\, a_1\, a_0)_b \end{aligned}$$

darstellen, wobei $m \in \mathbb{N}_0, a_i \in \{0, 1, 2, ..., b-1\}, a_m \neq 0$. Die Menge $\{0, 1, 2, ..., b-1\}$ heißt **Ziffernmenge**.

5.11 Bemerkung: Praktisch relevant sind besonders $b = 10$ (**Dezimalzahlensystem**), $b = 2$ (**Binärzahlen**), $b = 16$ (**Hexadezimalsystem**).

Für $b = 16$ benötigt man *neue* Symbole für Ziffern, denn: $(1\,1\,1\,1)_{16}, (11\,1\,1)_{16}, (11\,11)_{16}$? Das ist missverständlich!
Die Ziffermenge ist dann $\{0, 1, 2, ..., 8, 9, A, B, C, D, E, F\}$

6 Algebraische Strukturen

6.1 Definition: Es sei $m \in \mathbb{N}$ das sogenannte **Modul** und $a, b \in \mathbb{Z}$.

- a heißt **kongruent zu** b modulo m, falls $m|(a-b)$ gilt.
- In diesem Fall schreiben wir

$$a \equiv b \bmod m$$

  oder einfach $a \equiv b$, wenn das **Modul** m aus dem Zusammenhang hervorgeht.

Also: $a \equiv b \bmod m$ gdw $a - b = k \cdot m$ für ein geeignetes $k \in \mathbb{Z}$.

6.2 Satz: Es sei $m \in \mathbb{N}$. Es seien $a, b \in \mathbb{Z}$, r_a sei der Rest bei Division von a durch m und r_b der Rest bei Division von

b durch m. Dann gilt:

$$a \equiv b \quad \Leftrightarrow \quad r_a = r_b$$

6.3 Satz: Es sei $m \in \mathbb{N}$ das Modul für $\equiv$. $\equiv$ definiert eine Äquivalenzrelation auf $\mathbb{Z}$.

6.4 Definition: Es sei $m \in \mathbb{N}$ das Modul. Für $a \in \mathbb{Z}$ definieren wir

$$[a]_m := \{b | b \equiv a\}.$$

$[a]_m$ heißt **Restklasse** von a. Wenn das Modul m aus dem Zusammenhang hervorgeht, dannn schreiben wir nur $[a]$.

6.5 Satz Es sei $m \in \mathbb{N}$ das Modul. Es seien $a, b \in \mathbb{Z}$ und r der Rest bei Division von a durch m. Es gilt

i.) $[a] = [b] \Leftrightarrow a \equiv b$

ii.) $[a] = [r]$

6.6 Satz Es gibt m Restklassen: $[0], [1], ..., [m-1]$.

6.7 Restklassen und deren Arithmetik (Kreisarithmetik Modulararithmetik)

- **Satz:** Es sei $m \in \mathbb{N}$ das Modul.

$$[a] = [a'], [b] = [b'], \text{ dann } [a+b] = [a'+b']$$
$$[a] = [a'], [b] = [b'], \text{ dann } [a \cdot b] = [a' \cdot b']$$

- **Definition:** Es sei $m \in \mathbb{N}$.

$$\mathbb{Z}_m := \{[a] | a \in \mathbb{Z}\} = \{[0], [1], ..., [m-1]\}$$

- **Definition:** Es sei $m \in \mathbb{N}$ das Modul. Es seien $a, b \in \mathbb{Z}$. Wir definieren zwei **Verknüpfungen** auf $\mathbb{Z}_m$:

$$[a] \oplus [b] = [a+b]$$
$$[a] \odot [b] = [a \cdot b]$$

6.8 Definition (Inverse bezüglich $\oplus$:) Es sei $[a] \in \mathbb{Z}_m$ eine Restklasse. Eine Restklasse $[b]$ mit

$$[a] \oplus [b] = [0]$$

heißt **Inverses** von $[a]$ bezüglich $\oplus$. Man nennt $[0]$ das neutrale Element von $\mathbb{Z}_m$ bezüglich $\oplus$.

6.9 Satz: $[-a]$ ist ein Inverses von $[a]$.

6.10 Definition (Inverse bezüglich $\odot$): Es sei $[a] \in \mathbb{Z}_m, [a] \neq$

$[0]$ eine Restklasse $\neq [0]$. Eine Restklasse $[b]$ mit

$$[a] \odot [b] = [1]$$

heißt **Inverses** von $[a]$ bezüglich $\odot$. Man nennt $[1]$ das neutrale Element von $\mathbb{Z}_m$ bezüglich $\odot$.

6.11 Kürzen und Inverse bezüglich $\odot$ in $\mathbb{Z}_m$

- **Satz (Inverses in $\mathbb{Z}_m$):** $[k] \in \mathbb{Z}_m \setminus \{[0]\}$ hat genau dann ein Inverses bezüglich $\odot$, falls $\text{ggT}(k, m) = 1$.

- Betrachte: Wenn der ggT 1 ist, dann gibt es $\alpha, \beta \in \mathbb{Z}$ mit $1 = \alpha k + \beta m$. Man bestimmt α und β mit dem erweiterten euklidischen Algorithmus.
  Also $[1] = [\alpha k + \beta m] = [\alpha k] = [\alpha][k]$. Also ist $[\alpha]$ das Inverse von $[k]$.

- Wenn m eine Primzahl ist, dann gibt es für alle $[k] \neq [0]$ ein Inverses.

- **Satz (Kürzen in $\mathbb{Z}_m$):** Es sei $m \in \mathbb{N}$ das Modul und $k \neq 0$ und $\text{ggT}(k, m) = 1$. Wenn $[k] \odot [a] = [k] \odot [b]$, dann $[a] = [b]$.

6.12 Notation/Konvention

- Es sei $m \in \mathbb{N}$ das Modul. Wenn wir ein festes Modul

betrachten und Missverständnisse ausgeschlossen sind, dann

- schreiben wir a anstatt $[a]_m$ bzw. $[a]$.
- Anstatt $\oplus$ schreiben wir oft auch einfach $+$. Also $a+b$ anstatt $[a] \oplus [b]$
- Anstatt $\odot$ schreiben wir oft auch einfach $\cdot$. Also $a\dot{b}$ anstatt $[a] \cdot [b]$

6.13 Definition (Gruppe): Eine Menge G zusammen mit einer Verknüpfung

$$\circledast : G \times G \to G, (a,b) \mapsto a \circledast b$$

heißt **Gruppe**, falls:

- Es gibt ein $e \in G$ mit $e \circledast a = a = a \circledast e$ für alle $a \in G$. e heißt das bezüglich $\circledast$ **neutrale Element**.
- Für alle $a \in G$ gibt es ein eindeutig bestimmtes $b \in G$ mit $b \circledast a = a \circledast b = e$. b heißt das **bezüglich** $\circledast$ zu a **inverse Element.**
- Für alle $a, b, c \in G$ gilt $(a \circledast b) \circledast c = a \circledast (b \circledast c)$. [**Assoziativität**]

Beachte, dass $a \circledast b \in G$ gelten muss. Die Eigenschaft nennt

man die **Abgeschlossenheit** von $\circledast$.

Ist G zusammen $\circledast$ eine Gruppe und gilt $a \circledast b = b \circledast a$, dann heißt die Gruppe **kommutativ**.

6.14 Definition (Körper): Eine Menge K zusammen mit **zwei Verknüpfungen**

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

heißt **Körper**, falls:

- K zusammen **mit** $\oplus$ ist eine **kommutative Gruppe**. Das neutrale bezüglich $\oplus$ bezeichnen wir mit 0. [die Null]
- $K^* = K \setminus \{0\}$ zusammen **mit** $\odot$ ist eine **kommutative Gruppe**. Das neutrale Element bezeichnen wir mit 1. [die Eins]
- Für alle $a, b, c \in R$ gilt:

$$a \odot (b \oplus c) = a \odot b \oplus a \odot c \quad [\textbf{Distributivgesetz}]$$

6.15 Satz: i.) $\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m \setminus \{[0] \mid \text{ggT}(k, m) = 1\}$ zusammen mit $\odot$ bilden eine kommutative Gruppe. Das neutrale Element ist [1].

ii.) $\mathbb{Z}_m$ mit $\oplus$ und $\odot$ ist genau dann ein Körper, falls m eine Primzahl ist.

Die Notation $GF(p) = \mathbb{Z}_p$ ist dann üblich; GF steht für **Galois-Field** (**Galois-Körper**).

6.16 Satz (der kleine Satz von Fermat): Wenn p eine Primzahl ist, dann gilt für jedes $a \in \mathbb{Z}, p \not| a$

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

▶ Man kann den Satz auch äquivalent so formulieren:

6.17 Satz (der kleine Satz von Fermat): Es sei p eine Primzahl. Für jedes $a \in \mathrm{GF}(p), a \neq 0$ gilt

$$a^{p-1} = 1 \quad [\text{in } \mathbb{Z}_p = \mathrm{GF}(p)]$$

Beweis: Wir betrachten für $a \neq 0$ die Elemente $a \odot 1, ..., a \odot (p-1)$ des GF(p). Diese Elemente müssen alle verschieden sein [denn man kann in $\mathrm{GF}(p)$ das a kürzen].

Dann gilt

$$\{1, ..., p-1\} = \{a \odot 1, ..., a \odot (p-1)\}.$$

Dann folgt

$$\begin{aligned} 1 \odot ... \odot (p-1) &= (a \odot 1) \odot (a \odot 2) \odot ... \odot (a \odot (p-1)) \\ &= a^{p-1} \odot 1 \odot 2 \odot ... \odot (p-1). \end{aligned}$$

Kürzen:

$$1 = a^{p-1}.$$

6.18 Bemerkung: Mit dem kleinen Satz von Fermat sieht man, dass a^{p-2} das Inverse von $a \in \mathrm{GF}(p), a \neq 0$ ist. [denn: $a^{p-2}a = a^{p-1} = 1$ in $\mathbb{Z}_p$.]

6.19 Bemerkung (RSA Verschlüsselung):

- Es gibt zwei Schlüssel, die zusammengehören:
  - einen öffentlichen Schlüssel, den der Absender (Alice) zum verschlüsseln verwendet.
  - einen privaten Schlüssel, den nur der Empfänger (Bob) kennt und zum Entschlüsseln verwendet.
- Bob generiert das Schlüsselpaar und übermittelt den öffentlichen Schlüssel an Alice. Bei dieser Übermittlung muss der Alice sicher sein, dass ihm der öffentliche Schlüssel wirklich von Bob geschickt wurde.
- Ferner muss es praktisch unmöglich sein, den privaten

Schlüssel auf Basis des öffentlichen Schlüssels (und der verschlüsselten Nachricht) zu ermitteln.

- https://de.wikipedia.org/wiki/RSA-Kryptosystem

6.20 RSA Verschlüsselung

- Zu einem RSA gehören ein öffentlicher Schlüssel (e, n) und ein privater Schlüssel (d, n) mit
  - p, q sehr große Primzahlen, $n = pq$.
  - Wähle e teilerfremd zu $(p-1)(q-1)$.
  - Bestimme d mit $d \cdot e \equiv 1 \mod (p-1)(q-1)$. [$d$ ist das Inverse von e in $\mathbb{Z}^*_{(p-1)(q-1)}$; mit dem erweiterten euklidischen Algorithmus]
- Die Nachricht N wird mit (e, n) verschlüsselt: $S = N^e \mod n$. Versendet wird dann S.
- Die Nachricht N wird mit dem privaten Schlüssel (d, n) entschlüsselt: $N = S^d \mod n$.
- Wir müssen beweisen (mit dem kl. Fermat), dass die Schlüssel funktionieren:

$$N = (N^e)^d = N^{ed} \mod n$$

- Es ist nach aktuellem Ermessen für sehr große Primzahlen p, q praktisch unmöglich, die Faktorisierung pq von n auf Basis von e (und n) zu berechnen.
- Nach aktuellen Wissen benötigt man diese Faktorisierung, um d zu bestimmen.
- Hartmann, Seite 136ff, `https://de.wikipedia.org/wiki/RSA-Kryptosystem`

6.21 Beispiel: $p = 3, q = 5$. $n = 15$. $(p-1)(q-1) = 8$. $e = 3$. $d = 3$ (bestimmt man mit dem erweiterte euklidischen Algorithmus).

Die Nachricht ist $N = 7$. Dann $13 = 7^3 \mod 15$. Übertragen wird 13. Entschlüsselt: $7 = 13^3 \mod 15$.

6.22 Beispiel: $p = 11, q = 13$. $n = 143$. $(p-1)(q-1) = 120$. $e = 23$. $d = 47$ bestimmt mit dem erweiterte euklidischen Algorithmus.

- Die Nachricht ist $N = 7$. Dann $2 = 7^{23} \mod 143$. Übertragen wird 2. Entschlüsselt: $7 = 2^{47} \mod 143$
- Vorsicht: die Zahlen werden so groß, dass selbst gute Software bei unvorsichtiger Anwendung falsche Ergebnisse liefern.

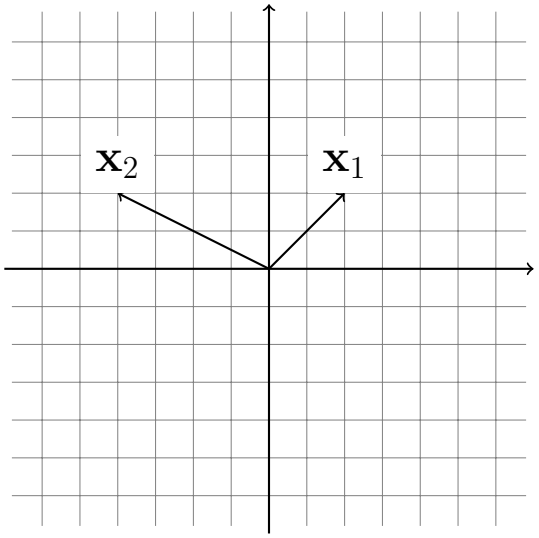
7 Vektoren und lineare Gleichungssysteme

7.1 Vektoren des $\mathbb{R}^n$: Eine **Spalte** von reellen Zahlen der Länge n

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

nennen wir **Vektor** des $\mathbb{R}^n$ und schreiben $\mathbf{x} \in \mathbb{R}^n$.

7.2 Vektoren im $\mathbb{R}^2$: $\mathbf{x}_1 = (1,1)^T$, $\mathbf{x}_2 = (-2,1)^T$ grafisch darstellen

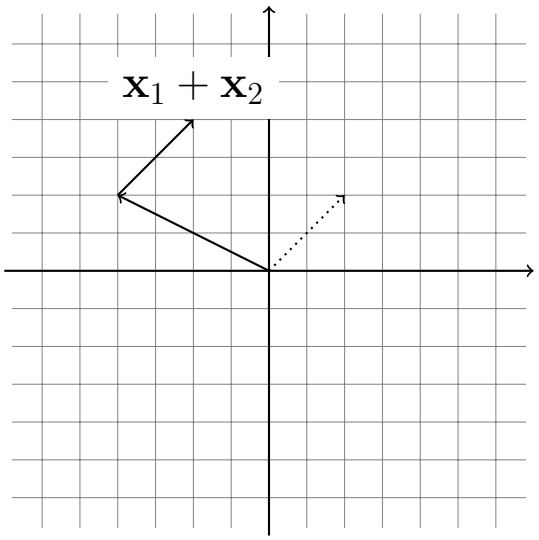


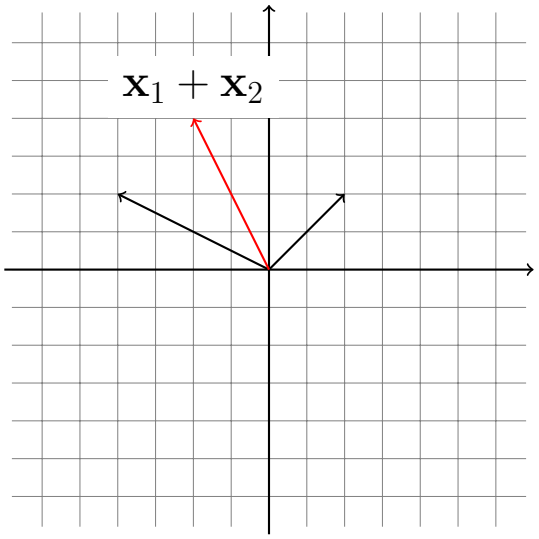
7.3 Definition (Vektoren im $\mathbb{R}^2$) addieren: Zwei Vektoren

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

addieren wir elementweise

$$\mathbf{x} + \mathbf{y} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

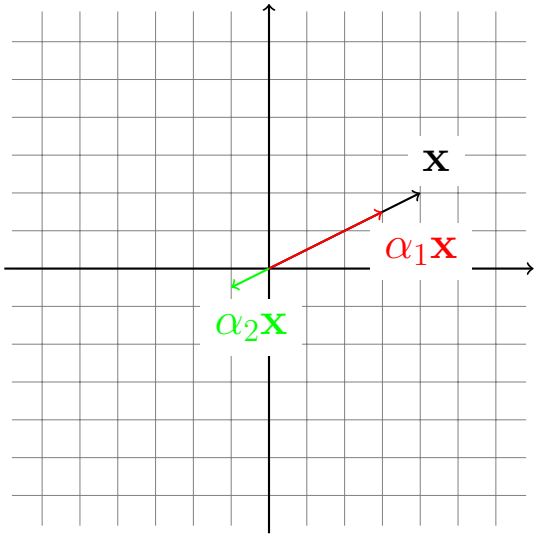




7.4 Definition (Vektoren mit einen Skalar multiplizieren): Einen Vektor $\mathbf{x}$ kann man mit einem Skalar $\lambda \in \mathbb{R}$ multiplizieren:

$$\lambda \mathbf{x} = \lambda \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

Skalieren ($\alpha_1 = 0.75$, $\alpha_2 = -0.25$)



7.5 Definitionen (Linearkombination): Wenn zwei Vektoren $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ und zwei Skalare $\alpha, \beta \in \mathbb{R}$ gegeben sind, dann können wir die **Linearkombinationen** bilden

$$\alpha\mathbf{x} + \beta\mathbf{y} = \alpha \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \beta \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 + \beta y_1 \\ \alpha x_2 + \beta y_2 \\ \vdots \\ \alpha x_n + \beta y_n \end{pmatrix}.$$

7.6 Definition (Vektorräume): Eine nichtleere Menge V mit zwei Verknüpfungen

$$+ : V \times V \to V, (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} + \mathbf{w}$$
$$\cdot : \mathbb{R} \times V \to V, (\lambda, \mathbf{v}) \mapsto \lambda \cdot \mathbf{v}$$

heißt **Vektorraum**, falls

- $(V, +)$ ist eine kommutative Gruppe.
- Für alle $\mathbf{v}, \mathbf{w}, \alpha, \beta$ gilt
  - $1 \cdot \mathbf{v} = \mathbf{v}$
  - $\alpha \cdot (\beta \cdot \mathbf{v}) = (\alpha\beta) \cdot \mathbf{v}$
  - $\alpha \cdot (\mathbf{v} + \mathbf{w}) = \alpha \cdot \mathbf{v} + \alpha \cdot \mathbf{w}$
  - $(\alpha + \beta) \cdot \mathbf{v} = \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v}$

▶ $\mathbb{R}^n$ ist ein Vektorraum.

7.7 Definitionen: Ein rechteckiges Schema

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n-1} & a_{m,n} \end{pmatrix}$$

mit reellen Werten $a_{i,j} \in \mathbb{R}, m, n \in \mathbb{N}$ heißt $m \times n$ **Matrix**. Für die Menge der $m \times n$ Matrizen schreiben wir $\mathbb{R}^{m \times n}$ oder $M(m, n; \mathbb{R})$.

Ist $a_{i,j}$ ein Eintrag der Matrix $\mathbf{A}$, dann heißt i der **Zeilenindex** und j der **Spaltenindex** des Eintrags $a_{i,j}$. Der Zeilenindex steht also vorne und der Spaltenindex hinten. Manche Autoren machen zwischen i und j kein Komma. Wir nennen

das Paar (i, j) die **Stelle** des Eintrags $a_{i,j}$.

7.8 Definitionen (Matrix · Vektor): Ist $\mathbf{x} \in \mathbb{R}^n$ so eine Spalte der Länge n, dann definiert man das **Produkt** $\mathbf{Ax} \in \mathbb{R}^m$ durch

$$\mathbf{Ax} = \begin{pmatrix} a_{1,1}x_1 + ... + a_{1,n}x_n \\ a_{2,1}x_1 + ... + a_{2,n}x_n \\ ... \\ a_{m,1}x_1 + ... + a_{m,n}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{1,1} \\ a_{2,1} \\ ... \\ a_{m,1} \end{pmatrix} + ... + x_n \begin{pmatrix} a_{1,n} \\ a_{2,n} \\ ... \\ a_{m,n} \end{pmatrix}.$$

Ax ist also die **Linearkombination** der Spalten von **A** (aber man rechnet zeilenweise Zeile mal Spalte).

7.9 Definitionen (Lineare Gleichungen): Es seien $a_i, i = 1, ..., n$ und b reelle Zahlen. Dann heißt

$$a_1x_1 + ... + a_nx_n = b$$

eine **lineare Gleichung** mit den **Koeffizienten** a_i, den **Unbekannten** x_i und der **rechten Seite** b.

Sind $s_i, i = 1, ..., n$ reelle Zahlen, so dass

$$a_1s_1 + ... + a_ns_n = b$$

gilt, dann heißt $(s_1, ..., s_n)^T \in \mathbb{R}^n$ eine **Lösung** der linearen Gleichung.

7.10 Definiton: Es seien $a_{i,j}, i = 1, ..., m, j = 1, ..., n$ und $b_j, j = 1, ..., m$ reelle Zahlen. Dann heißt

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + ... + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + ... + a_{2,n}x_n &= b_2 \\ &..... \\ a_{m,1}x_1 + a_{m,2}x_2 + ... + a_{m,n}x_n &= b_m \end{aligned}$$

ein **lineares Gleichungssystem** oder **LGS** – mit m linearen Gleichungen, den n Unbekannten x_i, den Koeffizienten $a_{i,j}$ und den rechten Seiten b_j.

Löst ein Vektor $\mathbf{s} := (s_1, ..., s_n)^T \in \mathbb{R}^n$ **jede** der m linearen Gleichungen, dann heißt $\mathbf{s}$ eine **Lösung des linearen Gleichungssystems**.

Ein LGS

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + ... + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + ... + a_{2,n}x_n &= b_2 \\ &..... \\ a_{m,1}x_1 + a_{m,2}x_2 + ... + a_{m,n}x_n &= b_m \end{aligned}$$

kann man kompakt als

$$\mathbf{Ax = b}$$

schreiben.

Noch knapper repräsentiert die sogenannte **erweiterte Systemmatrix**

$$(\mathbf{A}\ \mathbf{b}) = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \dots & a_{m,n-1} & a_{m,n} & b_m \end{pmatrix}$$

das lineare Gleichungssystem.

7.11 Definiton: Die folgenden drei Operationen heißen **elementare Zeilenumformungen (Umformungsschritte)**:

- Das λ-fache der k-ten Zeile (Gleichung) zur l-ten Zeile (Gleichung) addieren. Dabei muss $k \neq l$ gelten.
- Die k-te Zeile (Gleichung) mit der l-ten Zeile (Gleichung) vertauschen. Dabei muss $k \neq l$ gelten.
- Eine Zeile (Gleichung) mit $\lambda \neq 0$ multiplizieren.

7.12 Satz: Die Lösungsmenge eines linearen Gleichungssystems $\mathbf{Ax} = \mathbf{b}$ ist invariant bezüglich auf die erweiterte Systemmatrix angewandte elementare Zeilenoperationen.

7.13 Bemerkung: Die Idee des sogenannten **Gauß'schen Eliminationsverfahren** besteht darin, das LGS durch ele-

mentare Zeilenoperation so zu vereinfachen, dass man die Lösung fast *ablesen* kann.

7.14 Definition (Zeilenstufenform): Der erste von Null verschiedene Eintrag einer Zeile heißt **Leitkoeffizient** der Zeile.

Eine Matrix ist in **Zeilenstufenform**, wenn jeder Leitkoeffizient – bis auf den Koeffizienten der obersten Zeile – rechts von Leitkoeffizienten der darüberstehenden Zeile steht und alle etwaigen Nullzeilen der Matrix unten stehen. Die Zahl der Leitkoeffizienten (also der Zahl der Nicht-Null-Zeilen) der Zeilenstufenform einer Matrix $\mathbf{A}$ heißt der **Rang** der Matrix $\mathbf{A}$.

7.15 Satz (Charakterisierung der Lösungsmenge): An einer Zeilenstufenform der erweiterten Systemmatrix kann man zunächst drei Fälle erkennen:

- Wenn in der letzten Spalte ein Leitkoeffizient steht, dann hat das LGS **keine Lösung**. Die Lösungsmenge ist **leer**.
- Steht in jeder der ersten n Spalten ein Leitkoeffizient und in der letzte Spalte kein Leitkoeffizient, dann gibt es **genau eine Lösung**.

- Steht in der letzten Spalte und in mindestens einer weiteren Spalte kein Leitkoeffizient, dann gibt es **unendlich viele Lösungen**.

7.16 Definition (Basisvariablen und freie Variablen): Wir betrachten ein lineares Gleichungssystem dessen Matrix in Zeilenstufenform ist. Die Variablen, die zu einer Spalte mit Leitkoeffizienten gehören heißen **Basisvariablen**. Die anderen Variablen heißen **freie Variablen**.

7.17 Bemerkung (Rückwärtssubstitution): Falls die Lösungsmenge nicht leer ist, so findet man die Lösungsmenge des LGS, indem man die Zeilen des reduzierten LGS von unten nach oben nach den Basisvariablen auflöst **(Rückwärtssubstitution)**.

Wenn es **keine freien** Variablen gibt, so findet man so auch die eindeutig bestimmte Lösung.

Wenn es $\mathbb{N} \ni q > 0$ **freie Variablen** gibt, dann erhält man für jede Wahl der freien Variablen $x_{l_1} = \lambda_1, ..., x_{l_q} = \lambda_q$ wieder mit Rückwärtssubstitution eine Lösung des LGS; $l_1 < ... < l_q$ sind die Indizes der freien Variablen. Die **allgemeine Lösung** hat dann (das müssen Sie an vielen Beispielen üben)

die Form:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} + \lambda_1 \begin{pmatrix} v_1^1 \\ v_2^1 \\ \vdots \\ v_n^1 \end{pmatrix} + ... + \lambda_q \begin{pmatrix} v_1^q \\ v_2^q \\ \vdots \\ v_n^q \end{pmatrix}, \lambda_1, ..., \lambda_q \in \mathbb{R}$$

Der Vektor $\mathbf{u} = (u_1, u_2, ..., u_n)^T \in \mathbb{R}^n$ heißt (eine) **spezielle Lösung**.

Die Vektoren $\mathbf{v}^k = (v_1^k, v_2^k, ..., v_n^k)^T \in \mathbb{R}^n, k = 1, ..., q$ bilden eine Basis des **Kerns** des LGS.

Literaturverzeichnis

[1] **Epp** Susanne, Discrete Mathematics, 5. ed

[2] **Hartmann**, Peter, Mathematik für Informatiker, https://link.springer.com/book/10.1007/978-3-658-26524-3

[3] **Lee**, John, Axiomatic Geometry

[4] **Rosen**, Kenneth, Discrete Mathematics