

Mathematik III

(für IF, ET, Ph)

Oliver Ernst

Professur Numerische Mathematik

Wintersemester 2018/19

Studiengänge: B Angewandte Informatik, B Informatik,
M Informatik für Geistes- und Sozialwissenschaftler, B Biomedizinische Technik,
B Regenerative Energietechnik, B Elektromobilität, B Elektrotechnik,
B Computational Science, B Physik



Mathematik!
TU Chemnitz

8 Potenz- und Fourier-Reihen

8.1 Konvergenz von Funktionenfolgen

8.2 Potenzreihen

8.3 Fourier-Reihen

- Begriff, Konvergenz, und Darstellbarkeit von Funktionen
- Funktionen mit beliebiger Periode
- Konvergenz, Gliedweise Differentiation und Integration
- Komplexe Darstellung

9 Differentialrechnung in mehreren Variablen

9.1 Vektorfolgen und ihre Grenzwerte

9.2 Grenzwerte von Funktionen und Stetigkeit

9.3 Darstellungsfragen, Anwendungen und Systematisierungsversuch zu Funktionen mehrerer Variablen

9.4 Differenzierbarkeit bei mehreren Variablen

9.5 Differentiation vektorwertiger Funktionen

9.6 Extrema von Funktionen mehrerer Variablen

10 Integralrechnung in mehreren Variablen

10.1 Das Riemann-Integral im \mathbb{R}^n

10.2 Kurven und Kurvenintegrale

10.3 Oberflächen und Oberflächenintegrale

⑪ Integraltransformationen

11.1 Allgemeines

11.2 Fourier-Transformation

11.3 Laplace-Transformationen

⑫ Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

- Die bekanntesten algebraische Strukturen kennen wir für Zahlenmengen wie die natürlichen Zahlen \mathbb{N} , die ganzen Zahlen \mathbb{Z} , die rationalen Zahlen \mathbb{Q} , die reellen Zahlen \mathbb{R} und die komplexen Zahlen \mathbb{C} .
- Weitere Strukturen, den **Vektorraum** bzw. **Innenproduktraum** oder auch **Hilbert-Raum** haben wir ebenfalls schon kennengelernt. Dabei haben wir festgestellt, dass mehrere konkrete Ausprägungen auf diese abstrakte Strukturen passen.
- Sind mathematische Eigenschaften einer algebraischen Struktur einmal ermittelt, so gelten sie natürlich sofort für jedes konkrete Beispiel dieser Struktur.
- Nicht unähnlich: abstrakte Datentypen, abstrakte Objekte in der Informatik.

Definition 12.1

Eine **binäre Operation** auf einer nichtleeren Menge A ist eine Abbildung $\circ : A \times A \rightarrow A$. Das Bild eines Elementepaares $(a, b) \in A \times A$ wird mit $a \circ b$ bezeichnet. Das Paar (A, \circ) heißt dann **binäre algebraische Struktur** oder auch **Gruppoid**.

Bekannte Zahlenmengen bilden mit den binären Operationen Addition und Multiplikation eine algebraische Struktur:

$$\begin{array}{ccccc} (\mathbb{N}, +), & (\mathbb{Z}, +), & (\mathbb{Q}, +), & (\mathbb{R}, +), & (\mathbb{C}, +), \\ (\mathbb{N}, \cdot), & (\mathbb{Z}, \cdot), & (\mathbb{Q}, \cdot), & (\mathbb{R}, \cdot), & (\mathbb{C}, \cdot). \end{array}$$

Die Eigenschaft, dass das Ergebnis einer binären Operation auf einer Menge wieder in dieser Menge enthalten ist, nennt man **Abgeschlossenheit**. So ist etwa \mathbb{N} nicht abgeschlossen bezüglich der Subtraktion.

Bildet $A = \mathbb{N}$ zusammen mit $a \circ b := a^b$ eine algebraische Struktur?

Wichtig sind folgende Eigenschaften algebraischer Strukturen (vgl. Kapitel 1).

Definition 12.2

Sei (A, \circ) eine algebraische Struktur.

- a Assoziativgesetz:** für alle $a, b, c \in A$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.
- b Kommutativgesetz:** für alle $a, b \in A$ gilt $a \circ b = b \circ a$.
- c Existenz eines neutralen Elements:** Es gibt ein Element $e \in A$ mit der Eigenschaft

$$e \circ a = a \circ e = a \quad \text{für alle } a \in A.$$

- d Existenz inverser Elemente:** Zu jedem $a \in A$ gibt es ein $a' \in A$ mit der Eigenschaft

$$a \circ a' = a' \circ a = e.$$

Wird speziell die binäre Operation als Addition (+) oder Multiplikation (·) geschrieben, so bezeichnet man ein inverses Element zu a oft als $-a$ bzw. a^{-1} .

Beispiele:

- ① $(\mathbb{N}, +)$: assoziativ, kommutativ.
- ② $(\mathbb{N}_0, +)$: assoziativ, kommutativ, neutrales Element $e = 0$; nur die Null besitzt ein inverses Element $e' = e$.
- ③ $(\mathbb{Z}, +)$: alle Eigenschaften (a)-(d) gelten.
- ④ (\mathbb{Z}, \cdot) : assoziativ, kommutativ, neutrales Element $e = 1$, inverse Elemente besitzen nur ± 1 .
- ⑤ (\mathbb{Q}, \cdot) : assoziativ, kommutativ, neutrales Element $e = 1$, inverse Elemente besitzen alle Elemente von \mathbb{Q} außer 0.
- ⑥ $(\mathbb{Q} \setminus \{0\}, \cdot)$: alle Eigenschaften (a)-(d) gelten.

Satz 12.3

- a *In einer algebraischen Struktur gibt es höchstens ein neutrales Element.*
- b *In einer assoziativen algebraischen Struktur gibt es zu jedem Element höchstens ein inverses Element.*

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

Definition 12.4

Eine algebraische Struktur heißt

- a **Halbgruppe**, wenn sie assoziativ ist,
- b **Monoid**, wenn wenn sie assoziativ ist und ein neutrales Element besitzt,
- c **Gruppe**, wenn sie assoziativ ist, ein neutrales Element besitzt und jedes Element ein inverses Element besitzt.

Gilt in einer Halbgruppe, einem Monoid oder einer Gruppe zusätzlich das Kommutativgesetz, so heißt die entsprechende algebraische Struktur **kommutative** Halbgruppe, Monoid oder Gruppe.

Kommutative Gruppen werden auch **abelsche Gruppen** genannt.

Beispiele:

- 1 $(\mathbb{N}, +)$ ist eine (kommutative) Halbgruppe.
 $(\mathbb{N}_0, +)$ und (\mathbb{Z}, \cdot) sind (kommutative) Monoide, aber keine Gruppen.
- 2 Sei \mathcal{A} eine endliche Menge von Zeichen (Alphabet) sowie $A = \mathcal{A}^*$ die Menge aller endlichen Wörter über \mathcal{A} , d.h. alle endlichen Folgen $(x_1 x_2 \cdots x_k)$, $x_j \in \mathcal{A}$, sowie das leere Wort e . Als binäre Operation auf A sei die Konkatenation zweier Wörter $w_1 = x_1 \cdots x_k$ und $y_1 \cdots y_\ell$ definiert durch $w_1 \circ w_2 = x_1 \cdots x_k y_1 \cdots y_\ell$. Dann ist (A, \circ) ein Monoid.
- 3 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R}, +), (\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen.
- 4 $A = \mathbb{R}^{n \times n}$, $n \in \mathbb{N}$ bildet zusammen mit der Matrizenaddition eine abelsche Gruppe. Die invertierbaren Matrizen aus $\mathbb{R}^{n \times n}$ bilden bezüglich der Matrizenmultiplikation eine Gruppe, die jedoch nicht abelsch ist.
- 5 Die Menge aller Teilmengen einer festen Grundmenge M bildet bezüglich der **symmetrischen Mengendifferenz**

$$A \Delta B := (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

eine abelsche Gruppe.

Satz 12.5

Sei (A, \circ) eine Gruppe sowie $a, b \in A$ sowie a' das inverse Element von a . Dann ist $a' \circ b$ die eindeutig bestimmte Lösung der Gleichung $a \circ x = b$.

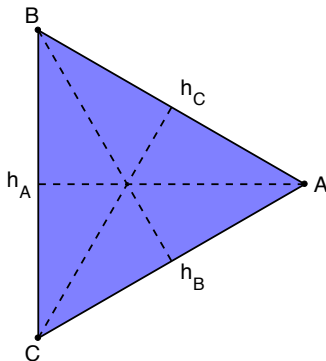
- Eine bijektive Abbildung π der Menge $\{1, 2, \dots, n\}$ in sich ($n \in \mathbb{N}$) wird als **Permutation** bezeichnet.
- Es gibt genau $n!$ verschiedene Permutationen von n Objekten.
- Zusammen mit der binären Operation der Hintereinanderausführung (Komposition, Verkettung) bilden die Permutationen von n Zahlen (Objekten) eine Gruppe, die als **symmetrische Gruppe** S_n bezeichnet wird.
- S_n ist (bis auf $n = 1, 2$) nicht abelsch.
- Darstellung:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

- Neutrales Element: identische Abbildung ($\pi(j) = j$, $j = 1, \dots, n$).
- Inversen: Umkehrabbildung (Bijektionen!).

Gruppen

Symmetriegruppe eines gleichseitigen Dreiecks



- Die Menge aller Isometrien (winkel- und längentreue Abbildungen) der Ebene, welche ein gleichseitiges Dreieck auf sich selbst abbilden, bilden bezüglich Komposition die **symmetrische Gruppe** des Dreiecks.
- Entspricht hier der Menge aller Permutationen der Eckpunkte.

Gruppen

Verknüpfungstabellen

Bei (kleinen) algebraischen Strukturen kann man alle möglichen binären Operationen in einer **Verknüpfungstafel** (*engl.* Cayley table) darstellen. In Zeile a und Spalte b steht jeweils das Element ab . Die Tafeln zu allen Gruppen mit bis zu drei Elementen lauten somit (e bezeichne das neutrale Element)

\circ	e
e	e

\circ	e	a_1
e	e	a_1
a_1	a_1	e

\circ	e	a_1	a_2
e	e	a_1	a_2
a_1	a_1	a_2	e
a_2	a_2	e	a_1

- Man zeige: In jeder Zeile/Spalte tritt jedes Element genau einmal auf.
- Wie sieht die Tafel einer abelschen Gruppe aus?
- Wieviele Vierergruppen gibt es?

Systematische Konstruktion: zuerst inverse Paare festlegen; bei der Anordnung der Elemente, mit e beginnend, zuerst die Selbstinversen aufzählen; danach unter Beachtung der Permutationsregel ergänzen.

Definition 12.6

Sei (G, \circ) eine Gruppe und U eine (nichtleere) Teilmenge von G .

Ist (U, \circ) ebenfalls eine Gruppe, so heißt U **Untergruppe** von (G, \circ) , geschrieben $(U, \circ) \leq (G, \circ)$.

Beispiel:

- 1 Triviale Untergruppen: $U = G$ bzw. $U = \{e\}$.
- 2 Die Mengen $n\mathbb{Z} := \{0, \pm n, \pm 2n, \pm 3n \dots\}$ bilden für $n \in \mathbb{N}$ Untergruppen von $(\mathbb{Z}, +)$.

Welche Gruppeneigenschaften sind noch nachzuprüfen, um festzustellen ob $(\emptyset \neq) U \subset G$ eine Untergruppe einer Gruppe (G, \circ) bildet?

Definition 12.7

Sei (G, \circ) eine Gruppe mit Untergruppe U sowie $a \in G$. Dann heien

$$\begin{array}{ll} a \circ U := \{a \circ u : u \in U\} & \text{von } a \text{ erzeugte \textcolor{red}{Linksnebenklasse} von } U \text{ in } G \text{ und} \\ U \circ a := \{u \circ a : u \in U\} & \text{von } a \text{ erzeugte \textcolor{red}{Rechtsnebenklasse} von } U \text{ in } G. \end{array}$$

Die Relation $a \sim b :\Leftrightarrow a \circ U = b \circ U$, $a, b \in G$, ist eine quivalenzrelation. Die zugehrige Partition von G besteht aus den entsprechenden Linksnebenklassen. (Analog fr Rechtsnebenklassen.)

Definition 12.8

Sei (G, \circ) eine endliche Gruppe mit Untergruppe U . Die Anzahl der Links- bzw. Rechtsnebenklassen von U in G wird als **Index** $|G : U|$ von G nach U bezeichnet. Die Anzahl $|G|$ der Elemente von G wird als **Ordnung** der Gruppe G bezeichnet.

Satz 12.9 (Satz von Lagrange)

Fr eine endliche Gruppe (G, \circ) mit Untergruppe U teilt die Ordnung $|U|$ von U stets die von G und es gilt $|G : U| = |G|/|U|$.

Definition 12.10

Für ein Element a einer Gruppe (G, \circ) mit neutralem Element e definieren wir die **Potenzen** $a^k, k \in \mathbb{Z}$ von a wie folgt^a:

$$a^0 := e, \quad a^1 := a, \quad a^k := a^{k-1} \circ a \text{ rekursiv für } k > 1, \quad (a^{-1})^{-k} \text{ für } k < 0.$$

^aWird $+$ als Operationssymbol verwendet, schreibt man auch ka anstelle von a^k

Man zeige:

- $a^{m+n} = a^m \circ a^n, \quad m, n \in \mathbb{Z}.$
- $(a^m)^n = a^{mn}, \quad m, n \in \mathbb{Z}.$
- Folgern Sie aus der ersten Beziehung, dass die Menge $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$ eine Untergruppe von G bildet, die stets kommutativ ist, auch wenn G selbst es nicht ist.

Die o.g. Gruppe $\langle a \rangle$ wird **von a erzeugte Untergruppe** von G genannt.

- Sind alle Potenzen $a^k, k \in \mathbb{Z}$ paarweise verschieden, so kann man die entstehende Untergruppe von G als Kopie der ganzen Zahlen ansehen (identifiziere $a^k \in \langle a \rangle \subset G$ mit $k \in \mathbb{Z}$.)
- Ist dies nicht der Fall, d.h. gilt $a^m = a^n$ für $m, n \in \mathbb{Z}, m < n$, so folgt durch Multiplikation mit a^{-m} sofort $a^{n-m} = e$. Es gibt also $k \in \mathbb{Z}$ mit $a^k = e$.

Definition 12.11

Sei (G, \circ) eine Gruppe und $a \in G$. Sind alle Potenzen $a^k, k \in \mathbb{Z}$ verschieden, so besitzt a **unendliche Ordnung**, geschrieben $\text{ord}_G(a) = \infty$. Andernfalls besitzt a die **endliche Ordnung**

$$\text{ord}_G(a) = \min\{k > 0 : a^k = e\}.$$

- Ist $\text{ord}_G(a) = \infty$, so ist auch die von a erzeugte Untergruppe unendlich.
- Ist $\text{ord}_G(a) < \infty$ so ist $\langle a \rangle = \{a^k : 0 \leq k < \text{ord}_G(a)\}$ die von a erzeugte Untergruppe, da die Potenzen sich wegen $a^{n+\text{ord}_G(a)} = a^n$ zyklisch wiederholen.
- In allen Fällen ist $|\langle a \rangle| = \text{ord}_G(a)$.
- Insbesondere teilt $\text{ord}_G(a)$ die Gruppenordnung $|G|$.

Satz 12.12 (kleiner Satz von Fermat)

Ist (G, \circ) eine endliche Gruppe, so gilt $a^{|G|} = e$ für alle $a \in G$.

Eine Gruppe G wird als **zyklische Gruppe** bezeichnet, wenn es ein $a \in G$ gibt mit $\langle a \rangle = G$, d.h. wenn G von a erzeugt wird.

Definition 12.13

Eine Untergruppe N einer Gruppe (G, \circ) heit **Normalteiler**, wenn die zugehrigen Links- und Rechtsnebenklassen bereinstimmen. Schreibweise: $N \trianglelefteq G$.

- Bei abelschen Gruppen ist jede Untergruppe Normalteiler.
- Ebenso ist jede Untergruppe mit Index $|G : N| = 2$ Normalteiler, denn in diesem Fall gibt es nur zwei Links- und Rechtsnebenklassen. Eine hiervon ist $e \circ N = N \circ e = N$, die andere $G \setminus N$.
- Sind $a_1 \in a \circ N = N \circ a$ sowie $b_1 \in b \circ N = N \circ b$, so gilt $a_1 \circ b_1 \in (a \circ N) \circ (b \circ N)$. Aufgrund der Normalteilereigenschaft gilt aber auch

$$\begin{aligned}(a \circ N) \circ (b \circ N) &= (N \circ a) \circ (b \circ N) = N \circ (a \circ b) \circ N \\ &= (a \circ b) \circ (N \circ N) = (a \circ b) \circ N,\end{aligned}$$

d.h. $a_1 \circ b_1 \in (a \circ b) \circ N$ und die Nebenklasse $(a \circ b) \circ N$ hngt nicht von der Wahl von a_1, b_1 ab.

Aufgrund der letzten Eigenschaft kann man eine Gruppenoperation auf der Menge der Nebenklassen definieren:

Definition 12.14

Sei N Normalteiler einer Gruppe (G, \circ) und bezeichne G/N die Menge der Nebenklassen von G nach N . Dann wird durch die Operation

$$(a \circ N) \circ (b \circ N) := (a \circ b) \circ N$$

eine Gruppenoperation auf G/N definiert. Die entstehende Gruppe $(G/N, \circ)$ wird als **Faktorgruppe** von G nach N bezeichnet.

Weisen Sie die Gruppeneigenschaften für die Faktorgruppe nach. Wie lauten neutrales Element und Inverse?

Beispiel: $(\mathbb{Z}, +)$ mit Normalteiler $N = m\mathbb{Z}$ ($m \in \mathbb{N}$).

- Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z} =: \mathbb{Z}_m$ besteht aus den m Nebenklassen

$$[0] := 0 + m\mathbb{Z} = m\mathbb{Z}, \quad [1] := 1 + m\mathbb{Z}, \dots, [m-1] := (m-1) + m\mathbb{Z}.$$

- Addition in \mathbb{Z}_m ist also Addition modulo m . Die Äquivalenzklassen bezüglich \mathbb{Z}_m werden daher auch als **Restklassen** bezeichnet.
- $(\mathbb{Z}_m, +)$ ist eine zyklische Gruppe und wird erzeugt von $[1] = 1 + m\mathbb{Z}$.

Definition 12.15

Eine Abbildung $\phi : G \rightarrow H$ zwischen zwei Gruppen (G, \circ) und $(H, *)$ heit **Homomorphismus** (oder **Gruppenhomomorphismus**), wenn

$$\phi(a \circ b) = \phi(a) * \phi(b) \quad \forall a, b \in G.$$

Ist ϕ bijektiv, so heit ϕ **Isomorphismus**. In diesem Fall ist die Umkehrabbildung $\phi^{-1} : H \rightarrow G$ ebenfalls ein Isomorphismus. Zwei Gruppen, zwischen denen ein Isomorphismus existiert, heien **isomorph**, geschrieben $G \cong H$.

Beispiel: Sei (G, \circ) eine Gruppe und $a \in G$ fest. Die Abbildung

$$\phi : \mathbb{Z} \rightarrow \langle a \rangle, \quad k \mapsto a^k$$

ist ein Homomorphismus zwischen den Gruppen $(\mathbb{Z}, +)$ und $(\langle a \rangle, \circ)$. Sind alle Potenzen von a verschieden, so ist ϕ bijektiv und damit $\mathbb{Z} \cong \langle a \rangle$.

Satz 12.16

Bei einem Gruppenhomomorphismus $\phi : G \rightarrow H$ wird das neutrale Element e_G von G auf das neutrale Element e_H von H abgebildet. Ebenso gilt für alle $a \in G$: $\phi(a^{-1}) = \phi(a)^{-1}$.

Definition 12.17

Ist $\phi : G \rightarrow H$ ein Gruppenhomomorphismus, so wird die Menge aller Elemente von G , welche durch ϕ auf das neutrale Element e_H von H abgebildet werden, als **Kern** von ϕ bezeichnet:

$$\ker \phi = \phi^{-1}(e_H) = \{a \in G : \phi(a) = e_H\}.$$

Als **Bild** von G unter ϕ bezeichnet man die Menge aller Bilder von ϕ :

$$\phi(G) = \{\phi(a) : a \in G\} = \{b \in H : \exists a \in G, \phi(a) = b\}.$$

Satz 12.18

Bei einem Gruppenhomomorphismus $\phi : G \rightarrow H$ ist $\ker \phi$ ein Normalteiler von G und $\phi(G)$ eine Untergruppe von H .

Satz 12.19 (Homomorphiesatz)

Sei $\phi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist die Faktorgruppe $G/\ker \phi$ isomorph zum Bild $\phi(G)$:

$$G/\ker \phi \cong \phi(G).$$

Einem Element $\phi(a)$ von $\phi(G)$ entspricht dabei die Nebenklasse $a \circ \ker \phi \in G/\ker \phi$.

Beispiel: $(G, \circ) = (\mathbb{Z}, +)$,

$$H = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}, \quad \zeta_m = e^{2\pi i/m} \quad (m \in \mathbb{N})$$

mit der Multiplikation (endliche multiplikative Gruppe der m -ten Einheitswurzeln). Hier ist

$$\phi : G \rightarrow H, \quad k \mapsto \zeta_m^k$$

ein surjektiver Homomorphismus mit $\ker \phi = m\mathbb{Z}$. Nach dem Homomorphiesatz gilt $\mathbb{Z}/m\mathbb{Z} \cong H = \langle \zeta_m \rangle$. Die Restklasse $[k]$ entspricht ζ_m^k .

Gruppen

Beispiel Gruppenhomomorphismen: symmetrische Gruppe

Für jedes Element der symmetrischen Gruppe S_n bestehend aus allen bijektiven Abbildungen $\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ definieren wir das **Signum** (Vorzeichen) durch

$$\operatorname{sgn} \pi := \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

- Da π bijektiv treten in Zähler und Nenner bis auf Reihenfolge und Vorzeichen dieselben Faktoren auf, daher gilt $\pi(j) \in \{-1, 1\}$ für alle j .
- Für

$$\pi_{\text{id}} := \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} \quad \text{bzw.} \quad \pi_{1,2} := \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix}$$

gilt beispielsweise $\operatorname{sgn} \pi_{\text{id}} = 1$ und $\operatorname{sgn} \pi_{1,2} = -1$.

- Bezeichnungen: $\pi \in S_n$ **gerade** bzw. **ungerade** je nachdem ob $\operatorname{sgn} \pi = 1$ bzw. $\operatorname{sgn} \pi = -1$.

- Für $\pi, \sigma \in S_n$ gilt stets

$$\begin{aligned}\operatorname{sgn}(\pi \circ \sigma) &= \prod_{1 \leq i < j \leq n} \frac{(\pi \circ \sigma)(i) - (\pi \circ \sigma)(j)}{i - j} \\ &= \prod_{1 \leq i < j \leq n} \frac{(\pi \circ \sigma)(i) - (\pi \circ \sigma)(j)}{\sigma(i) - \sigma(j)} \cdot \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= (\operatorname{sgn} \pi) \cdot (\operatorname{sgn} \sigma).\end{aligned}$$

- Damit ist sgn ein Gruppenhomomorphismus zwischen der symmetrischen Gruppe (S_n, \circ) und der zweielementigen Gruppe $(\{-1, 1\}, \cdot)$.
- Der Kern $\ker \operatorname{sgn} = \{\pi \in S_n : \operatorname{sgn} \pi = 1\}$ von sgn umfasst alle geraden Permutationen und wird auch mit A_n (alternierende Permutationen) bezeichnet.
- Homomorphiesatz \Rightarrow Nebenklassenzerlegung von S_n ($n \geq 2$) besteht aus zwei Klassen, A_n und $S_n \setminus A_n$ (ungeraden Permutationen).

Gruppen

Beispiel Gruppenhomomorphismen: symmetrische Gruppe

- Damit ist A_n eine Untergruppe vom Index $|S_n : A_n| = 2$ und beide Nebenklassen bestehen aus $n!/2$ Permutationen.
- Insbesondere gibt es ebensoviele gerade wie ungerade Permutationen.

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

- Die ganzen Zahlen \mathbb{Z} bilden sowohl mit der Addition als auch der Multiplikation eine algebraische Struktur, nämlich die abelsche Gruppe $(\mathbb{Z}, +)$ bzw. Monoid (\mathbb{Z}, \cdot) .
- Ein **Ring** ist eine algebraische Struktur mit **zwei** binären Operationen, welche mit $+$ und \cdot bezeichnet werden (aber nicht zwingend mit Addition und Multiplikation übereinstimmen müssen).
- Das **Distributivgesetz**

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

verbindet die beiden Operationen.

- Das neutrale Element der Addition wird, falls es existiert, mit 0 (Null), das der Multiplikation mit 1 (Eins) bezeichnet.
- Das additive inverse Element zu a wird mit $-a$, das multiplikative mit a^{-1} bezeichnet.
- Die Vorrangregel, Multiplikation vor Addition auszuführen wenn diese nebeneinanderstehen („Punkt vor Strich“), spart Klammern.

Definition 12.20

Eine algebraische Struktur $(R, +, \cdot)$ mit zwei binären Operationen heißt **Ring**, wenn folgende drei Eigenschaften gegeben sind

- i $(R, +)$ ist eine kommutative Gruppe (mit neutralem Element 0),
- ii (R, \cdot) ist eine Halbgruppe, und
- iii es gelten die **Distributivgesetze**

$$\begin{array}{ll} \text{für alle } a, b, c \in R \text{ gilt} & a \cdot (b + c) = a \cdot b + a \cdot c \\ \text{ sowie} & (a + b) \cdot c = a \cdot c + b \cdot c. \end{array}$$

Besitzt R ein neutrales Element bezüglich \cdot , so nennt man R **Ring mit Eins**.
Ist R kommutativ bezüglich \cdot , so nennt man R einen **kommutativen Ring**.

Beispiele:

- 1 $(\mathbb{Z}, +, \cdot)$ sowie $(\mathbb{Z}_m, +, \cdot)$ ($m \in \mathbb{N}$) sind kommutative Ringe mit Eins.
- 2 Die Menge $R^{n \times n}$ aller $(n \times n)$ -Matrizen M mit Einträgen $m_{i,j}$ aus einem Ring R bilden bezüglich Matrizenaddition und -multiplikation wieder einen Ring.
- 3 Polynome in der Variablen x über einem Ring R sind formale Summen

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k.$$

mit Koeffizienten $a_0, \dots, a_k \in R$. Für zwei Polynome $p(x) = \sum_{j=0}^k a_jx^j$ und $q(x) = \sum_{j=0}^{\ell} b_jx^j$ definieren wir

$$p(x) + q(x) = \sum_{j=0}^{\max\{k,\ell\}} (a_j + b_j)x^j, \quad p(x) \cdot q(x) = \sum_{j=0}^{k+\ell} \left(\sum_{i=\max\{0, j-\ell\}}^{\min\{j, k\}} a_i b_{j-i} \right) x^j.$$

Die Menge $R[x]$ aller solcher Polynome bildet mit dieser Addition und Multiplikation den **Polynomring über R** : $(R[x], +, \cdot)$.

- In jedem Ring gilt die Rechenregel $a \cdot 0 = 0 \cdot a = 0$.
- In einem Ring kann ein Produkt jedoch durchaus Null sein, obwohl beide Faktoren von Null verschieden sind:
Im Ring $(\mathbb{Z}_6, +, \cdot)$ gilt etwa $[2] \neq [0]$ sowie $[3] \neq [0]$, aber $[2] \cdot [3] = [6] = [0]$.
- Man nennt ein Element $a \neq 0$ eines Ringes R einen **Nullteiler**, wenn es ein $b \neq 0$ aus R gibt mit der Eigenschaft $a \cdot b = 0$ oder $b \cdot a = 0$. (In diesem Fall ist natürlich b ebenfalls ein Nullteiler.)

Definition 12.21

Ein kommutativer Ring mit Eins ohne Nullteiler heißt **Integritätsbereich** (oder auch **Integritätsring**).

Beispiele: $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich, hingegen besitzt $(\mathbb{Z}_m, +, \cdot)$ genau dann Nullteiler, wenn m keine Primzahl ist, ist also in diesen Fällen kein Integritätsbereich.

Der Polynomring $R[x]$ über einem Integritätsbereich R ist selbst Integritätsbereich.

- In einem Integritätsbereich kann man kürzen: Ist $a \neq 0$ und $a \cdot b = a \cdot c$, so folgt $a \cdot (b - c) = 0$, also $b - c = 0$ und somit $b = c$.
- In einem beliebigen Ring R kann man stets durch Elemente $a \in R$ kürzen, die ein multiplikatives Inverses a^{-1} besitzen. Solche Elemente heißen auch **Einheiten**. Es ist direkt nachzurechnen, dass die Menge R^* aller Einheiten von R eine (multiplikative) Gruppe bildet, die so genannte **Einheitengruppe** von R . Beispielsweise ist $\mathbb{Z}^* = \{-1, 1\}$.

Definition 12.22

Ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $a \neq 0$ eine Einheit ist, also ein multiplikatives Inverses besitzt, heißt ein **Körper**.

Eine algebraische Struktur $(K, +, \cdot)$ ist also genau dann ein Körper, wenn $(K, +)$ und $(K \setminus \{0\}, \cdot)$ kommutative Gruppen sind und die Distributivgesetze gelten.

Beispiele: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

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

$(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich, aber kein Körper.

Satz 12.23

Jeder Körper ist ein Integritätsbereich, und jeder endliche Integritätsbereich ist ein Körper.

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

Definition 12.24 (Teilbarkeit, ggT, kgV)

Seien $a, b \in \mathbb{Z}$.

- a** Man sagt b **teilt** a , in Zeichen $b|a$, wenn es eine ganze Zahl c gibt mit $a = bc$.
- b** Eine Zahl $g \in \mathbb{Z}$ heißt **größter gemeinsamer Teiler** von a und b , geschrieben $g = \text{ggT}(a, b)$, wenn folgende zwei Bedingungen erfüllt sind:
 - i** g teilt sowohl a als auch b , d.h. $g|a$ und $g|b$.
 - ii** Für jeden weiteren Teiler t von a und b gilt $t|g$.
- c** a und b heißen **teilerfremd**, wenn $\text{ggT}(a, b) = 1$.
- d** Eine Zahl $k \in \mathbb{Z}$ heißt **kleinstes gemeinsames Vielfaches** von a und b , geschrieben $k = \text{kgV}(a, b)$, wenn folgende zwei Bedingungen erfüllt sind:
 - i** k ist ein Vielfaches von sowohl a als auch b , d.h. $a|k$ und $b|k$.
 - ii** Für jedes weitere Vielfache v von a und b gilt $k|v$.

Bemerkung: Mit g ist auch $-g$ größter gemeinsamer Teiler zweier Zahlen. Mit der Festlegung, dass dieser stets positiv ist, wird der größte gemeinsame Teiler eindeutig bestimmt. Analog verfährt man beim kleinsten gemeinsamen Vielfachen.

Satz 12.25 (Division mit Rest)

Es seien $a, b \in \mathbb{Z}$ und $b > 0$. Dann gibt es Zahlen $q, r \in \mathbb{Z}$ mit

$$a = bq + r \quad \text{und} \quad 0 \leq r < b.$$

Satz 12.26 (Euklidischer Algorithmus)

Führt man zu $a, b \in \mathbb{Z}$, $b > 0$, die folgende Kette von Divisionen mit Rest durch,

$$\begin{array}{ll} a = bq_0 + r_0, & 0 < r_0 < b, \\ b = r_0q_1 + r_1, & 0 < r_1 < r_0, \\ r_0 = r_1q_2 + r_2, & 0 < r_2 < r_1, \\ \vdots & \\ r_{k-2} = r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1}, \\ r_{k-1} = r_kq_{k+1} + 0, & \end{array}$$

so muss diese wegen $b > r_0 > r_1 > \dots \geq 0$ nach endlich vielen Schritten mit einem verschwindenden Rest abbrechen. Für den zuletzt berechneten Rest gilt $r_k = \text{ggT}(a, b)$.

Bemerkung: Die Anzahl der Divisionsschritte ist (auf den ersten Blick) durch b beschränkt. Tatsächlich ist der Algorithmus viel schneller:

Aus $r_{k-2} \geq r_k + r_{k-1} \geq 2r_k$ folgt

$$r_k \leq \frac{1}{2} r_{k-2}.$$

Der Euklidische Algorithmus terminiert also nach wenigen Schritten. Genauer gilt: $r_k \leq b \cdot 2^{-\lfloor k/2 \rfloor}$. Der Algorithmus bricht also spätestens nach $2(\log b / \log 2) + 1$ Schritten ab.

Satz 12.27

Ist $d = \text{ggT}(a, b)$, $a, b \in \mathbb{Z} \setminus \{0\}$, so gibt es ganze Zahlen e, f mit

$$d = ea + fb.$$

Diese können mit dem Euklidischen Algorithmus berechnet werden.

Definition 12.28

Eine natürliche Zahl $p > 1$ heißt **Primzahl**, wenn die einzigen Teiler von p die Zahlen ± 1 und $\pm p$ sind. Die Menge der Primzahlen wird mit \mathbb{P} bezeichnet.

Satz 12.29

Teilt eine Primzahl p ein Produkt ganzer Zahlen a_1, \dots, a_r , also $p \mid a_1 a_2 \cdots a_r$, dann teilt sie wenigstens einen der Faktoren, also $p \mid a_j$ für ein $j \in \{1, \dots, r\}$.

Satz 12.30 (Fundamentalsatz der Zahlentheorie)

Jede natürliche Zahl $a \geq 2$ lässt sich als Produkt von Primzahlen darstellen:

$$a = p_1 \cdot p_2 \cdots p_r \quad \text{mit } p_1, \dots, p_r \in \mathbb{P}$$

wobei die Darstellung bis auf die Reihenfolge eindeutig ist.

Satz 12.31

Es gibt unendlich viele Primzahlen.

Für eine natürliche Zahl a und eine Primzahl p schreibt man $\nu_p(a) = k$, falls gilt $p^k | a$, aber $p^{k+1} \nmid a$. Aus dem Fundamentalsatz erhält man dann durch Zusammenfassung der entsprechenden Primzahlteiler zu Primzahlpotenzen die sogenannte Primfaktorenzerlegung von a als

$$a = 2^{\nu_2(a)} \cdot 3^{\nu_3(a)} \cdot 5^{\nu_5(a)} \dots = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}.$$

Satz 12.32

Es seien $\prod_{p \in \mathbb{P}} p^{\nu_p(a)}$ und $\prod_{p \in \mathbb{P}} p^{\nu_p(b)}$ die Primfaktorenzerlegungen von $a, b \in \mathbb{N}$. Dann gilt:

$$\text{ggT}(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{\nu_p(a), \nu_p(b)\}} \quad \text{und} \quad \text{kgV}(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{\nu_p(a), \nu_p(b)\}}.$$

Insbesondere gilt auch

$$\text{ggT}(a, b) \cdot \text{kgV}(a, b) = ab.$$

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

Erinnerung: In Kapitel 2 der Vorlesung hatten wir den Begriff einer **Relation** R auf einer Menge M definiert als Teilmenge von $M \times M$, und eine **Äquivalenzrelation** als eine solche, welche die drei folgenden Eigenschaften besitzt:

- a Reflexivität.** $\forall x \in M : (x, x) \in R$.
- b Symmetrie.** $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$.
- c Transitivität.** $\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$.

Anstelle von $(x, y) \in R$ schreiben wir im Folgenden einfacher $x \sim_R y$ oder, wenn die Relation R aus dem Kontext klar ist, $x \sim y$.

Definition 12.33

Sei R eine Äquivalenzrelation auf der Menge M . Für $x \in M$ heißt die Menge

$$[x] := \{y \in M : x \sim y\}$$

die von x erzeugte **Äquivalenzklasse**.

Beachte: Aufgrund der Reflexivitätseigenschaft ist $[x] \neq \emptyset$ für alle $x \in M$.

Satz 12.34

- a *Sei R eine Äquivalenzrelation auf der Menge M . Dann bilden die (verschiedenen) Äquivalenzklassen der Elemente von M eine Partition von M .*
- b *Ist Umgekehrt $\mathcal{P} = \{M_j\}_{j \in J}$ eine Partition der Menge M und bezeichne $[x]$ jene Teilmenge aus \mathcal{P} , welche x enthält. Definiert man nun $x \sim y$ genau dann, wenn $[x] = [y]$, so ist hierdurch eine Äquivalenzrelation auf M definiert.*

Corollary 12.35

Sei R eine Äquivalenzrelation auf der Menge M und $x \in M$. Gilt $y \in [x]$, so folgt $[x] = [y]$, d.h. die Äquivalenzklasse ist unabhängig von der Auswahl des Repräsentanten.

Definition 12.36

Sei R eine Äquivalenzrelation auf der Menge M . Sei ferner \circ eine binäre Operation auf M . Wir sagen, die binäre Operation \circ **respektiert** die Relation R , falls für alle $x, x', y, y' \in M$ gilt

$$x' \sim x \wedge y' \sim y \Rightarrow x' \circ y' \sim x \circ y.$$

Satz 12.37

Sei R eine Äquivalenzrelation auf der Menge M , sowie \circ eine binäre Operation auf M , welche die Relation R respektiert. Dann wird durch die Vorschrift

$$[x] \circ [y] := [x \circ y]$$

eine binäre Operation auf der Menge M_R aller Äquivalenzklassen von R auf M erklärt.

Definition 12.38

Sei $m \in \mathbb{N}$ fest. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **kongruent modulo m** , falls m ein Teiler von $b - a$ ist. Man schreibt hierfür auch kurz $a \equiv b \pmod{m}$.

Satz 12.39

Sei $m \in \mathbb{N}$ fest. Durch die Beziehung

$$a \sim b :\Leftrightarrow a \equiv b \pmod{m}, \quad a, b \in \mathbb{Z},$$

wird eine Äquivalenzrelation erklärt. Die Menge aller Äquivalenzklassen $[a] = [a]_m$ wird mit \mathbb{Z}_m bezeichnet. Es gilt

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

Bemerkung: Die Äquivalenzklassen der Kongruenz modulo m werden auch **Restklassen** genannt, da sie genau aus den ganzen Zahlen bestehen, welche bei der Division durch m denselben Rest ergeben.

- Für $m \in \mathbb{N}$ ist $m\mathbb{Z}$ ein Normalteiler der Gruppe $(\mathbb{Z}, +)$.
- $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ ist die zugehörige Faktorgruppe.
- Die Abbildung

$$\phi : \mathbb{Z} \rightarrow \{0, 1, \dots, m-1\}, \quad k \mapsto k \bmod m$$

ist ein Gruppenhomomorphismus mit $\ker \phi = m\mathbb{Z}$.

- Die endliche Gruppe $(\mathbb{Z}_m, +)$ ist zyklisch und wird von $[1] = 1 + m\mathbb{Z}$ erzeugt.

Satz 12.40

Sei $m \in \mathbb{N}$ fest. Die binären Operationen Addition und Multiplikation auf der Menge \mathbb{Z} respektieren die Kongruenzrelation modulo m . Diese sind somit auch binäre Operationen auf \mathbb{Z}_m .

Beispiel: Verknüpfungstafel der Addition in \mathbb{Z}_5 :

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

Beispiel: Verknüpfungstafel der Multiplikation in \mathbb{Z}_4 . (Wenn die Restklassenmenge klar ist, kann die Restklassenklammer auch weggelassen werden.)

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Satz 12.41

Eine Restklasse $[a] \in \mathbb{Z}_m$ besitzt genau dann eine multiplikativ inverse Restklasse, wenn $\text{ggT}(a, m) = 1$ ist.

- Insbesondere ist $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ für $p \in \mathbb{P}$ eine abelsche Gruppe.

Man bestimme in \mathbb{Z}_{17} die inverse Restklasse zu $[15]$.

Man zeige: die Quersumme einer Zahl $n \in \mathbb{N}$ ist genau dann durch 9 teilbar, wenn n es ist.

Satz 12.42

$(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit Eins.

*$(\mathbb{Z}_m, +, \cdot)$ ist genau dann auch ein Integritätsbereich, wenn m eine Primzahl ist.
In diesem Fall bildet $(\mathbb{Z}_m, +, \cdot)$ auch einen Körper.*

Prüfziffern dienen der Erkennung von Übertragungsfehlern bei Artikelnummern, Sozialversicherungsnummern, Bankkontonummern usw.

Ein Beispiel ist die **Internationale Standard-Buchnummer** (ISBN), mit Format

$$\text{ISBN } a_1 - a_2 a_3 a_4 - a_5 a_6 a_7 a_8 a_9 - p$$

Ziffern a_1 bis a_9 beschreiben Gruppe, Verlag und Titel des Buches. Die letzte Ziffer p ist die Prüfziffer, mit der Eigenschaft

$$10a_1 + 9a_2 + 8a_3 + \cdots + 3a_8 + 2a_9 + p \equiv 0 \pmod{11}. \quad (12.1)$$

Damit besitzt p die Darstellung

$$p \equiv a_1 + 2a_2 + \cdots + 9a_9 \pmod{11}, \quad p \in 0, 1, 2, \dots, 9, X,$$

wobei X für die „Ziffer“ 10 steht.

Ist ISBN 3–211–82084–1 eine korrekte ISBN-Nummer?

Mit Hilfe des ISBN-Codes können sowohl Einzelfehler als auch Vertauschungsfehler an zwei beliebigen Stellen erkannt werden, eine Fehlerkorrektur ist allerdings i. Allg. nicht möglich.

Satz 12.43

Jeder Fehler in einer Ziffer sowie alle Vertauschungen zweier Ziffern werden vom ISBN-Code erkannt.

12 Algebraische Strukturen

12.1 Gruppen

12.2 Ringe und Körper

12.3 Elementare Zahlentheorie

12.4 Äquivalenzrelationen und Äquivalenzklassen

12.5 Zahlentheorie und Kryptographie

Satz 12.44

Ist p eine Primzahl, so gilt $p \mid \binom{p}{k}$ für alle $k = 1, 2, \dots, p-1$.

Satz 12.45

Ist p eine Primzahl und $a, b \in \mathbb{Z}_p$, so gilt $(a+b)^p = a^p + b^p$.

Mit anderen Worten: für alle $a, b \in \mathbb{Z}$ gilt $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Corollary 12.46

Ist p eine Primzahl sowie $a_1, \dots, a_n \in \mathbb{Z}_p$, so gilt $(a_1 + \dots + a_n)^p = a_1^p + \dots + a_n^p$.

Mit anderen Worten: für alle $a_1, \dots, a_n \in \mathbb{Z}$ gilt

$$(a_1 + \dots + a_n)^p \equiv a_1^p + \dots + a_n^p \pmod{p}.$$

Satz 12.47 (Kleiner Satz von Fermat)

Ist p eine Primzahl und $a \in \mathbb{Z}$ mit $\text{ggT}(a, p) = 1$, so gilt $a^{p-1} \equiv 1 \pmod{p}$.

- Selbstverständlich haben wir diesen Satz schon einmal in abstrakterem Kontext bewiesen, und zwar im gleich bezeichneten Satz 12.12.
- Man muss lediglich feststellen, dass $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ für $p \in \mathbb{P}$ eine $p - 1$ -elementige (insbesondere endliche) Gruppe bildet und dass $[1]$ das neutrale Element der Multiplikation in \mathbb{Z}_p darstellt.

Definition 12.48

Die **Eulersche φ -Funktion** $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ ist definiert durch

$$\varphi(m) = |\{a \in \mathbb{Z} : 1 \leq a \leq m, \text{ggT}(a, m) = 1\}|.$$

Bemerkung: Für einen Ring R hatten wir mit R^* die multiplikative Gruppe derjenigen Elemente von R bezeichnet, welche eine multiplikative Inverse besitzen. Nach Satz 12.42 bilden die Restklassen $\mathbb{Z}_m, m \in \mathbb{N}$, einen Ring (mit Eins).

Für $m > 1$ gibt, im Anbetracht von Satz 12.41, der Wert $\varphi(m)$ somit die Anzahl der invertierbaren Elemente der Restklassen modulo m an, d.h. $\varphi(m) = |\mathbb{Z}_m^*|$.

- 1 Man bestimme $\varphi(m)$ für $m = 1, 2, \dots, 12$.
- 2 Man zeige: für Primzahlen p gilt $\varphi(p) = p - 1$.

Satz 12.49

Sei p eine Primzahl und $n \in \mathbb{N}$. Dann gilt $\varphi(p^n) = p^{n-1}(p - 1)$.

Angesichts der Primfaktorenzerlegung beliebiger natürlicher Zahlen

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}, \quad n \in \mathbb{N},$$

können wir die φ -Funktion für beliebige n dann ausrechnen, wenn wir ihr Verhalten für das Produkt teilerfremder Zahlen kennen. Genauer gesagt: es gilt

$$m, n \in \mathbb{N}, \quad \text{ggT}(m, n) = 1 \quad \Rightarrow \quad \varphi(mn) = \varphi(m)\varphi(n).$$

Hierzu benötigen wir einen einfachen Spezialfall des **Chinesischen Restsatzes**:

Satz 12.50

Seien $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$ sowie $a, b \in \mathbb{Z}$ beliebig. Dann besitzt das Gleichungssystem

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$$

genau eine Lösung modulo $m \cdot n$.

Für den Beweis der Multiplikativität der φ -Funktion genügt es zu zeigen, dass $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*|$. Dies kann durch Angabe einer Bijektion zwischen beiden Mengen gezeigt werden.

Satz 12.51

Seien $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$. Dann gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

Satz 12.52

Sei $m \in \mathbb{N}$ mit Primfaktorenzerlegung $m = p_1^{\nu_1} \cdot p_2^{\nu_2} \cdots p_r^{\nu_r}$. Dann gilt

$$\varphi(m) = \prod_{j=1}^r p_j^{\nu_j-1} (p_j - 1) = m \prod_{j=1}^r \left(1 - \frac{1}{p_j}\right).$$

Satz 12.53 (Euler)

Sei $n \in \mathbb{N}$ beliebig sowie $k \in \mathbb{Z}$ mit $\text{ggT}(k, n) = 1$. Dann gilt $k^{\varphi(n)} \equiv 1 \pmod{n}$.

Den Beweis der expliziten Darstellung der Eulerschen φ -Funktion in Satz 12.52 kann man mit Hilfe der folgenden kombinatorischen Tatsache auf die Funktionswerte von Primzahlpotenzen zurückführen. Es handelt sich dabei um die Verallgemeinerung der Formel für die Mächtigkeit der Vereinigung zweier endlicher Mengen und ist als **Inklusions-/Exklusions-Prinzip** bekannt.

Satz 12.54 (Inklusions-/Exklusions-Prinzip)

Für ein System n endlicher Mengen A_1, A_2, \dots, A_n gilt

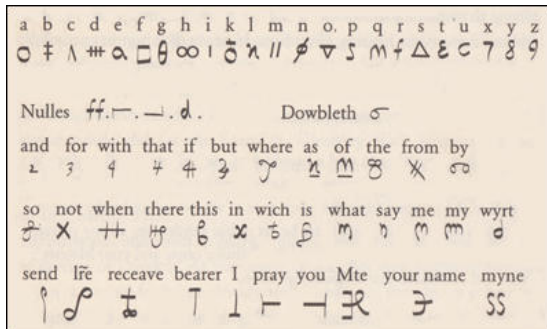
$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq 1} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad - + \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n| \\ &= \sum_{\emptyset \neq I \subset \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|. \end{aligned}$$

- Im Gegensatz zur Erkennung von Übertragungsfehlern besteht das Ziel der **Kryptographie** (Verschlüsselung) darin, Nachrichten an einen designierten Empfänger für Dritte unzugänglich zu halten.
- Neben klassischen Anwendungen in Diplomatie, Nachrichtendiensten und Militär ließen elektronischer Geldverkehr und Handel die Bedeutung sicherer Verschlüsselungstechniken seit Ende des 20. JH noch weiter steigen.
- Grundidee: Nachrichten werden in Zahlen kodiert, Ver- und Entschlüsselung bestehen in der Anwendung einer Bijektion $v : \mathbb{N} \rightarrow \mathbb{N}$ bzw. ihrer Umkehrabbildung v^{-1} auf die (Bestandteile der) Nachricht.
- Ein **Schlüssel** kann als Parametrisierung von v angesehen werden, sodass Kenntnis des Schlüssels auch die von v und v^{-1} bedeutet.
- Seit Entwicklung der **public key cryptography** (Verschlüsselung mit öffentlichem Schlüssel) ist es nicht mehr nötig, mit jedem Kommunikationspartner vorher einen geheimen Schlüssel auszutauschen.

Algebraische Strukturen

Beispiele zu Verschlüsselung

Verschlüsselte Verschwörungsnachricht von Anthony Babington an Mary Queen of Scots in Hausarrest, später entschlüsselt durch Sir Francis Walsingham.



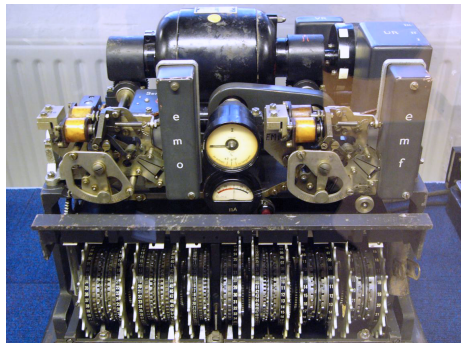
Klartext: *We ... will undertake the delivery of your royal persons from the hands of your enemies ... For the dispatch of the usurper (Elizabeth)... six noble gentlemen, who, for the zeal they have to the Catholic cause... will undertake that tragical execution.*

Algebraische Strukturen

Beispiele zu Verschlüsselung



Chiffriergerät **Enigma**, ab ca. 1920.



Chiffriergerät **Lorenz SZ40**, ab ca. 1941.

- Die **RSA-Verschlüsselung** war die erste praktikable **asymmetrische** Verschlüsselungstechnik, d.h. Ver- und Entschlüsselung geschehen durch unterschiedliche Schlüssel.
- Prinzipielle Idee von **Diffie, Hellman und Merkle** (Stanford University, 1976).
- Mathematische Umsetzung dann durch **Rivest, Shamir und Adleman** (MIT, 1977).
- Aus Geheimhaltungsgründen wurden ähnliche Ideen von **Ellis, Cocks und Williamson** (≈ 1970 , Government Communications Headquarters (GCHQ), Cheltenham, UK) erst 1997 veröffentlicht.

Satz 12.55

Seien $p \neq q$ zwei ungerade Primzahlen, $m = pq$ und $v = \text{kgV}(p-1, q-1)$. Dann gilt für beliebige Zahlen $a, k \in \mathbb{Z}$

$$a^{kv+1} \equiv a \pmod{m}.$$

- Insbesondere: für $e, d \in \mathbb{Z}$ mit $ed \equiv 1 \pmod{v}$ gilt für alle $a \in \mathbb{Z}$

$$(a^e)^d \equiv a \pmod{m}.$$

- Zum Empfang verschlüsselter Nachrichten multipliziert A zwei (große) Primzahlen p, q und veröffentlicht $m := pq$ sowie eine zu $v = \text{kgV}(p-1, q-1)$ teilerfremde Zahl e .
- Um an A verschlüsselte Nachrichten zu versenden (die nur A lesen kann) zerlegt B die Nachricht in Blöcke a_1, a_2, \dots , die durch ganze Zahlen im Bereich $0, 1, \dots, m-1$ dargestellt werden können, und sendet die verschlüsselten Zahlen

$$b_j := v(a_j) = a_j^e \pmod{m}.$$

- Nach Empfang kann A die Entschlüsselung vornehmen durch

$$a_j = v^{-1}(b_j) = b_j^d \pmod{m}.$$

- $d = e^{-1} \pmod{v}$ kann nur mit Hilfe von $v = \text{kgV}(p-1, q-1)$ berechnet werden, wofür die Primfaktorenzerlegung von $m = pq$ erforderlich ist.

Beispiel:

- Die zu versendende Nachricht laute allekreterluegen.
- Als Vorkehrung gegen statistische Textanalyse, bei welcher anhand von Häufigkeiten Rückschlüsse die Verschlüsselung einzelner Buchstaben gezogen werden könnte, wenden wir die Verschlüsselungsabbildung auf Buchstabenpaare (hier Paare) anstelle einzelner Buchstaben an.
- Wir ordnen jedem Buchstaben seine Ordnungszahl d_x zwischen 1 und 26 zu.
- Jedem Buchstabenpaar (x, y) ordnen wir die Zahl $(d_x - 1) \cdot 26 + d_y$ zu. Zu deren Verschlüsselung sind mindestens $m > 26^2 = 676$ nötig, wir wählen etwa $m = 5893$ und als Exponent $e = 17$.
- Für unsere Beispielnachricht erhalten wir zunächst

$$\begin{array}{llll} \text{al} \mapsto 12 & \text{le} \mapsto 291 & \text{kr} \mapsto 278 & \text{et} \mapsto 124 \\ \text{er} \mapsto 122 & \text{lu} \mapsto 307 & \text{eg} \mapsto 111 & \text{en} \mapsto 118 \end{array}$$

- Die zugehörigen Verschlüsselungen lauten

$$\begin{aligned}v(12) &= 4492 & v(291) &= 985 & v(278) &= 1618 & v(124) &= 5323 \\v(122) &= 2579 & v(307) &= 1943 & v(111) &= 5542 & v(118) &= 738\end{aligned}$$

- Die Umkehrabbildung ist gegeben durch

$$x = v(x)^d \pmod{m}, \quad 0 \leq v(x) < m \quad \text{mit } d = 1013.$$

Im Beispiel:

$$\begin{aligned}4492^{1013} &\equiv 12 \pmod{5893}, & 985^{1013} &\equiv 291 \pmod{5893}, \\1618^{1013} &\equiv 278 \pmod{5893}, & 5323^{1013} &\equiv 124 \pmod{5893}, \\2579^{1013} &\equiv 122 \pmod{5893}, & 1943^{1013} &\equiv 307 \pmod{5893}, \\5542^{1013} &\equiv 111 \pmod{5893}, & 738^{1013} &\equiv 118 \pmod{5893}.\end{aligned}$$

- **Fazit:** Einziges geheim zu haltendes Datum ist der 'Schlüssel' d .
- Der Schlüssel d ist so zu wählen, dass $0 < d < \varphi(n)$ mit

$$[e]_{\varphi(m)} \cdot [d]_{\varphi(m)} = [1]_{\varphi(m)} \quad \text{d.h.} \quad e \cdot d \equiv 1 \pmod{\varphi(m)},$$

d.h. d ist das multiplikativ inverse Element von e in $\mathbb{Z}_{\varphi(n)}$.

- Die multiplikativ Inverse d zu e kann man mit dem Euklidischen Algorithmus bestimmen.
- Die Schwierigkeit bei der Entschlüsselung besteht in der Berechnung von $\varphi(m)$ ohne die Primfaktorenzerlegung von m zu kennen.

Ziele erreicht?

Sie sollten nun (bzw. nach Abschluss der Übungen/Selbststudium):

- die algebraischen Strukturen Halbgruppe, Monoid und Gruppe unterscheiden und Beispiele angeben können;
- wichtige Begriffe elementarer Gruppentheorie wie Untergruppe, Nebenklassen, Normalteiler, Faktorgruppe und Gruppenhomomorphiesatz verstanden haben;
- die Rechenregeln der Restklassenarithmetik kennen;
- den Euklidischen Algorithmus zur Berechnung des ggT von Hand durchführen können;
- die Rolle der Restklassenarithmetik bei der RSA-Verschlüsselung erklären können.