Skript zur Vorlesung

Diskrete Strukturen

Universität Kassel

Andreas Bley

SoSe 2021

Inhaltsverzeichnis

Einleitung

Inhalte der Vorlesung

- **Primzahlen und modulare Arithmetik**

  Teilbarkeitsstruktur der ganzen Zahlen, Primzahlen, modulare Arithmetik, endliche Zahlenkörper

- **Grundelemente der Kryptographie und Codierung**

  RSA, Kanalcodierung

- **Graphentheorie**

  Darstellung und elementare Eigenschaften endlicher Graphen, Wege, Bäume, Eulersche Touren, Paarungen und Knotenüberdeckungen, Plättbarkeit von Graphen, Knotenfärbungen

Literaturempfehlungen

- G. Teschl, S. Teschl: Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra. Springer
- A. Steger: Diskrete Strukturen. Springer
- M. Aigner: Diskrete Mathematik. Springer
- A. Beutelspacher, M.-A. Zschiegner: Diskrete Mathematik für Einsteiger. Springer

Ergänzende und weiterführende Literatur

- E. Weitz: Konkrete Mathematik (nicht nur) für Informatiker. Springer
  (mit vielen Code-Beispielen in Python)
- R. Schulze-Pillot: Elementare Algebra und Zahlentheorie. Springer
- U. Knauer, K. Knauer: Diskrete und algebraische Strukturen – kurz gefasst. Springer

1. Primzahlen und modulare Arithmetik

Literaturempfehlung:

- Kapitel 3 in G. Teschl, S. Teschl: Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra.
- Kapitel 3 in A. Steger: Diskrete Strukturen.

Weitere Literaturempfehlungen:

- Kapitel 5 – 7 in A. Beutelspacher, M.A. Zschiegner: Diskrete Mathematik für Einsteiger.
- Kapitel 13 – 14 in M. Aigner: Diskrete Mathematik.
- Kapitel 3 – 7 in E. Weitz: Konkrete Mathematik (nicht nur) für Informatiker.
- Anhang A dieses Skriptes.

1.1. Teilbarkeit und Primzahlen

Zunächst befassen wir uns mit der Menge der ganzen Zahlen und ihrer Teilbarkeitsstruktur.

Definition 1.1.1 Seien $x, y \in \mathbb{Z}$. Wir sagen x **teilt** y, geschrieben $x|y$, wenn ein $q \in \mathbb{Z}$ existiert, so dass $y = q \cdot x$.

Bemerkung

- Auf $\mathbb{Z}$ ist die Relation $|$ („x teilt y “) reflexiv und transitiv.
- Auf $\mathbb{N}$ ist die Relation $|$ außerdem antisymmetrisch.
- Also definiert $|$ auf $\mathbb{N}$ eine partielle Ordnung.

Definition 1.1.2 Seien $x, y \in \mathbb{Z}$.

(i) $T(y) := \{t \in \mathbb{N} \mid t|y\}$ bezeichnet die **Menge aller positiven Teiler** von y.

(ii) $T(x, y) := T(x) \cap T(y)$ bezeichnet die Menge aller **positiven gemeinsamen Teiler** von x und y.

(iii) Für $x, y \neq 0$ heißt $ggT(x, y) := \max\{t \mid t \in T(x, y)\}$ **größter gemeinsamer Teiler** von x und y.

Bemerkung

- $T(0) = \mathbb{N}$
  $T(x, 0) = T(x)$ für alle $x \in \mathbb{N}$
- Gilt $x \neq 0$, so ist $t \leq |x|$ für alle $t \in T(x)$. Also ist dann $|T(x)| < \infty$.
  Somit ist $T(x, y)$ für $x, y \neq 0$ endlich und $ggT(x, y)$ daher wohldefiniert.
- Nach Definition gilt $ggT(x, y) = ggT(y, x)$ für alle $x, y \in \mathbb{Z}$.

Beispiel 1.1.3

$T(12) = \{1, 2, 3, 4, 6, 12\}$

$T(18) = \{1, 2, 3, 6, 9, 18\}$

$T(12, 18) = \{1, 2, 3, 6\}$, $ggT(12, 18) = 6$

Definition 1.1.4 Zwei ganze Zahlen $x, y \in \mathbb{Z}$ heißen **teilerfremd** (auch **coprim**), wenn $T(x, y) = \{1\}$.

Bemerkung
Für zwei ganze Zahlen $x, y \in \mathbb{Z}$ gilt immer $1 \in T(x, y)$.
Folglich ist $T(x, y) = \{1\}$ äquivalent zu $ggT(x, y) = 1$.
Also sind x und y genau dann teilerfremd, wenn $ggT(x, y) = 1$.

Beispiel 1.1.5

12 und 18 sind nicht teilerfremd, da $T(12, 18) = \{1, 2, 3, 6\}$ *(und somit* $ggT(12, 18) = 6$*).*

12 und 25 sind teilerfremd, da $T(12) = \{1, 2, 3, 4, 6, 12\}$, $T(25) = \{1, 5, 25\}$ *und somit* $T(12, 25) = \{1\}$.

Ein Verfahren zur effizienten Berechnung des ggT zweier Zahlen, den Euklidischen Algorithmus, lernen wir später in Kapitel 1.3 kennen. Zunächst widmen wir uns besonderen Zahlen, den sogenannten Primzahlen.

Definition 1.1.6 Eine Zahl $p \in \mathbb{N}$ heißt **prim** (oder **Primzahl**), wenn $|T(p)| = 2$ (d.h. $p \geq 2$ und $T(p) = \{1, p\}$).

Bemerkung Eine Primzahl ist eine natürlich Zahl mit **genau** zwei (voneinander verschiedenen) Teilern. 1 ist somit keine Primzahl.

Primzahlen sind die „Grundbausteine“ der multiplikativen Darstellung ganzer Zahlen.

Satz 1.1.7 (Fundamentalsatz der Arithmetik)

Jede natürliche Zahl $n \in \mathbb{N}$, $n \geq 2$, *lässt sich auf eindeutige Weise als Produkt von Primzahlen*

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

darstellen, wobei $p_1 < p_2 < \ldots < p_k$ *Primzahlen und* $k, e_1, e_2, \ldots, e_k \in \mathbb{N}$ *sind.*

Die Zahlen $p_1, \ldots, p_k$ *heißen* ***Primfaktoren*** *von* n.

Beweis. Siehe z.B. A. Steger: Diskrete Strukturen, Kapitel 3.1. □

Hat man die Primfaktorzerlegung zweier Zahlen, kann man bequem deren ggT und kgV (= kleinstes gemeinsames Vielfaches) ablesen:

Folgerung 1.1.8 *Seien $x, y \in \mathbb{N}$, so dass*

$$x = \prod_{i=1}^{k} p_i^{e_i} \quad \textit{und} \quad y = \prod_{i=1}^{k} p_i^{f_i}$$

für Primzahlen $p_1 < \ldots < p_k$ und $e_1, \ldots, e_k, f_1, \ldots, f_k \in \mathbb{N}_0$.

(D.h. $\{p_1, \ldots, p_k\}$ enthält mindestens alle Primzahlen, die in wenigstens einer der Faktorisierungen von x und y vorkommen, und $x = \prod_{i=1}^{k} p_i^{e_i}$ und $y = \prod_{i=1}^{k} p_i^{f_i}$ sind die Faktorisierungen von x und y, jeweils ergänzt um p_i^0 für diejenigen Primzahlen p_i, die nicht in der jeweiligen Faktorisierung vorkommen.)

Dann gilt

(i) *Es gilt $x|y$ genau dann, wenn $e_i \leq f_i$ für alle $i = 1, \ldots, k$.*

(ii) $ggT(x, y) = \prod_{i=1}^{k} p_i^{\min\{e_i, f_i\}}$

(iii) $kgV(x, y) = \prod_{i=1}^{k} p_i^{\max\{e_i, f_i\}}$

Beispiel 1.1.9

$ggT(1000, 210) = ggT(2^3 \cdot 3^0 \cdot 5^3 \cdot 7^0,\ 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1) = 2^1 5^1 = 10$

$kgV(1000, 210) = kgV(2^3 \cdot 3^0 \cdot 5^3 \cdot 7^0,\ 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1) = 2^3 \cdot 3^1 \cdot 5^3 \cdot 7^1 = 21000$

Bemerkung 1.1.10 Die Berechnung des $ggT(x, y)$ zweier Zahlen x, y auf diesem Wege ist jedoch sehr ineffizient, da bereits die Faktorisierung der einzelnen Zahlen x und y im Allgemeinen rechnerisch sehr aufwendig ist. Die Faktorisierung von Zahlen ist der Kern vieler kryptographischer Verfahren. Der in Kapitel 1.3 vorgestellte Euklidische Algorithmus ist deutlich effizienter zum Bestimmen des ggT.

Wir werden in Kapitel 1.3 sehen, dass Primzahlen spezielle und für das praktische Rechnen oft sehr nützliche Teilbarkeitseigenschaften haben. Vorher überlegen wir uns jedoch noch, wie viele dieser besonderen Zahlen es überhaupt gibt.

Definition 1.1.11 Seien $\mathbb{P} := \{p \in \mathbb{N} \mid p \text{ ist Primzahl}\}$ die Menge aller Primzahlen und $\pi(n) := |\{p \in \mathbb{P} \mid p \leq n\}|$ die Anzahl der Primzahlen kleiner oder gleich $n \in \mathbb{N}$.

Satz 1.1.12 *Es gibt unendlich viele Primzahlen, d.h.* $|\mathbb{P}| = \infty$.

Beweis. Widerspruchsbeweis:

- Angenommen $\mathbb{P} = \{p_1, \ldots, p_k\}$ ist endlich.
- Betrachte Zahl $m = p_1 \cdots p_k + 1$.
- Offenbar lässt m bei Division durch jede der Primzahlen p_i jeweils den Rest 1. Da alle p_i als Primzahlen 2 oder größer sind, ist m also durch keine der Zahlen p_i teilbar.
- Also ist m selbst eine neue Primzahl (nämlich falls $T(m) = \{1, m\}$) oder m hat einen Primteiler q, der eine neue Primzahl sein muss (da kein p_i Teiler von m ist).
- Beides widerspricht Annahme, dass $\mathbb{P}$ alle Primzahlen enthält. □

Eine exakte und effiziente Bestimmung der nächstgrößeren Primzahl zu einer gegebenen Zahl ist mit den bekannten mathematischen Techniken nicht möglich. Der folgende Satz liefert jedoch eine (ziemlich genaue) Abschätzung, wie viele Primzahlen es im Bereich $1, \ldots, n$ gibt, und damit eine Aussage zum erwarteten Abstand zwischen zwei aufeinanderfolgenden Primzahlen in einem gegebenen Zahlenbereich.

Satz 1.1.13 (Primzahlsatz) $\lim_{n \to \infty} \frac{\pi(n)}{n/\log(n)} = 1.$

Beweis. Geht deutlich über die hier behandelten Techniken hinaus. Bei Interesse in einem Lehrbuch zur Zahlentheorie nachlesen. □

1.2. Modulare Arithmetik

In diesem Kapitel beschäftigen wir uns mit dem Rechnen in Zahlenräumen endlicher Größe.

Hat man nur k Bits zum Speichern ganzer Zahlen zur Verfügung, so kann man damit in der üblichen Binärcodierung nur die $m = 2^k$ Zahlen von 0 bis $2^k - 1$ darstellen. Größere Zahlen würden mehr als k Bit zur Codierung benötigen. Schneidet man in der Binärcodierung einer größeren Zahl a (bzw. irgendeiner Zahl) einfach die zu den höherwertigen Stellen gehörenden Bits ab, so ergibt die in den verbliebenen k Bits beschriebene Zahl a' genau den Rest, den a bei der Division durch $m = 2^k$ lässt. Rechnen wir also nur mit den k kleinsten Bits aller Zahlen, so entspricht dies mathematisch genau dem Rechnen mit den Resten, die diese Zahlen bei Division durch m lassen.

Diese Technik, das Rechnen den Resten alle Zahlen bei Division durch eine feste Zahl m, ist das Grundelement aller ganzzahligen arithmetischen Operationen in modernen Rechnern. Mathematisch funktioniert das nicht nur für Zweierpotenzen $m = 2^k$, sondern für alle ganzen Zahlen m.

Grundlage für das Rechnen mit Resten ist natürlich, dass die Division durch m immer einen eindeutigen Rest liefert.

Satz 1.2.1 (Division mit Rest) *Seien $a \in \mathbb{Z}$ und $m \in \mathbb{N}$, $m \neq 0$. Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $0 \leq r < m$, so dass $a = q \cdot m + r$.*

*Wir nennen r den **Rest von a bei Division durch** m, geschrieben $Rest(a : m)$.*

Aus Sicht des Rechnens mit den Resten bei der Division durch m sind zwei Zahlen nicht mehr unterscheidbar und somit gleichwertig, wenn sie den gleichen Rest liefern. Dies wird durch die folgende Kongruenzrelation mathematisch formal beschrieben.

Definition 1.2.2 Sei $m \in \mathbb{N}$, $m \neq 0$ fest. Für $a, b \in \mathbb{Z}$ sagen wir a **ist kongruent zu** b **modulo m**, geschrieben

$$a \equiv b \mod m \qquad \text{oder} \qquad a \equiv_m b$$

wenn $b - a$ durch m teilbar ist. Wir nennen die Zahl m den gewählten **Modul**.

Beobachtung 1.2.3

Für jeden Modul $m \in \mathbb{N}$, $m \neq 0$, ist die in 1.2.2 definierte Relation $\equiv_m$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. Weisen Sie als Übung selbst nach, dass $\equiv_m$ die Eigenschaften einer Äquivalenzrelation erfüllt! □

Wollen wir komplizierterer Ausdrücke modulo m berechnen, also ihren Rest bei Division durch m, ist die folgende Beobachtung hilfreich. Sie erlaubt es uns, Multiplikationen und Additionen direkt mit den Resten der Summanden bzw. der Faktoren modulo m durchzuführen und so lediglich mit kleinen Zahlen (nämlich den Resten) rechnen zu müssen.

Beobachtung 1.2.4 *Seien $m \in \mathbb{N}$, $m \neq 0$, ein fest gewählter Modul und $a, a', b, b' \in \mathbb{Z}$. **Wenn***

$$a \equiv a' \mod m \qquad \textit{und} \qquad b \equiv b' \mod m$$

*gelten, **dann** folgen auch*

$$a + b \equiv a' + b' \mod m \qquad \textit{und} \qquad a \cdot b \equiv a' \cdot b' \mod m\ .$$

Beweis. Siehe z.B. A. Steger: Diskrete Strukturen, Kapitel 3.1. □

Beispiel 1.2.5

$10017 + 315 \equiv 7 + 5 \equiv 12 \equiv 2 \mod 10$

$6 \cdot 8 \equiv (-1) \cdot 1 \equiv -1 \equiv 6 \mod 7$

$41^{10} \equiv (-1)^{10} \equiv 1 \mod 7$

Mit den Regeln in Beobachtung 1.2.4 lassen sich viele Berechnungen modulo m stark vereinfachen. Zudem können Summen immer – genau wie beim Rechnen mit ganzen Zahlen in $\mathbb{Z}$ – durch das Subtrahieren/Entfernen gemeinsamer Summanden vereinfacht werden:

Beobachtung 1.2.6 *Seien $m \in \mathbb{N}$, $m \neq 0$, ein fest gewählter Modul und $a, a', c \in \mathbb{Z}$. Wenn*

$$a + c \equiv a' + c \mod m$$

gilt, dann folgt auch

$$a \equiv a' \mod m\ .$$

Warnung: Die Umkehrung der Multiplikationsregel in Beobachtung 1.2.4 gilt jedoch im Allgemeinen nicht! Sind die Faktoren und der Modul nicht teilerfremd, so kann man in Produkten nicht einfach kürzen, wie das folgende Beispiel zeigt.

Beispiel 1.2.7 *Es gilt*

$$2 \cdot 9 \equiv 4 \cdot 9 \mod 6,$$

aber

$$2 \not\equiv 4 \mod 6.$$

Kürzen ist nur möglich, wenn der zu kürzende Faktor und der Modul teilerfremd sind.

Beobachtung 1.2.8 *Sei $m \in \mathbb{N}$, $m \geq 2$ ein fest gewählter Modul. Für alle $a, b, c \in \mathbb{Z}$ mit $ggT(c, m) = 1$ gilt*

$$a \cdot c \equiv b \cdot c \mod m \quad \Rightarrow \quad a \equiv b \mod m \ .$$

Beweis. Siehe z.B. A. Steger: Diskrete Strukturen, Kapitel 3.1. □

Beispiel 1.2.9 *Wegen $ggT(9, 8) = 1$ folgt aus $\underbrace{2 \cdot 9}_{\equiv 2} \equiv \underbrace{10 \cdot 9}_{\equiv 2} \mod 8$ auch*

$2 \equiv 10 \mod 8$.

Wir werden später in diesem Kapitel sehen, wieso die Subtraktion gemeinsamer Summanden aus Summen immer, das Kürzen gemeinsamer Faktoren aus Produkten beim Rechnen modulo m nur bei zu m teilerfremden Faktoren möglich ist.

Zuvor führen wir aber den „Zahlenraum“ ein, in dem wir beim Rechnen modulo m eigentlich operieren.

Für einen festen Modul $m \in N$ ist $\equiv_m$ eine Äquivalenzrelation auf der Menge $\mathbb{Z}$ aller ganzen Zahlen. Sie zerlegt diese folglich in Äquvalenzklassen, welche wir Restklassen nennen.

Definition 1.2.10 Sei $m \in \mathbb{N}$, $m \neq 0$ ein fest gewählter Modul.

(i) Wir nennen die Menge

$$[a]_m := \{b \in \mathbb{Z} \mid a \equiv b \mod m\}$$

die **Restklasse** von a modulo m. Ist klar, welcher Modul m gewählt wurde, schreiben wir auch oft nur $[a]$ für $[a]_m$.

(ii) Wir bezeichnen die Menge aller Vielfachen von m, also die Restklasse von 0 modulo m, mit

$$m\mathbb{Z} := [0]_m = \{k \cdot m \mid k \in \mathbb{Z}\} \ .$$

(iii) Wir bezeichnen die Menge aller Restklassen modulo m mit

$$\mathbb{Z}/m\mathbb{Z} := \{[a]_m \mid a \in \mathbb{Z}\} \ .$$

Bemerkung In der Literatur ist es auch üblich, $(a \mod m)$ oder einfach nur a für die Restklasse $[a]_m$ zu schreiben. Um Verwechslungen zu vermeiden, verwenden wir im Folgenden immer $[a]_m$ oder abkürzend $[a]$ für die Restklasse des Repräsentanten $a \in \mathbb{Z}$.

Im eingangs beschriebenen Beispiel des Rechnens mit nur k Bit langen Zahlen entsprechen die Restklassen $\mathbb{Z}/m\mathbb{Z}$ mit $m = 2^k$ gerade den k-Bit-Zahlen, die man durch das Abschneiden aller

höherwertigen Bits erhält. Für $k = 2$ sind die ganzen Zahlen $a = 1 = (001)_b$ und $a' = 5 = (101)_b$ kongruent modulo $m = 2^k = 4$. Sie liegen folglich in der gleichen Restklasse $[1]_4 = [5]_4$, welche durch $1 = (01)_b$ repräsentiert werden kann – die letzten beiden in beiden Zahlen identischen Bits.

Die Rechenoperationen Addition und Multiplikation übertragen sich auf kanonische Weise von den ganzen Zahlen auf die Menge der Restklassen modulo m. Damit erhalten wir auf der Menge $\mathbb{Z}/m\mathbb{Z}$ die im Folgenden definierte Addition und Multiplikation.

Definition 1.2.11 Sei $m \in \mathbb{N}$, $m \neq 0$ ein fest gewählter Modul. Wir definieren auf $\mathbb{Z}/m\mathbb{Z}$ die Verknüpfungen

$$+ : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})$$
$$\cdot : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})$$

durch

$$[x]_m \underbrace{+}_{+ \text{ auf } \mathbb{Z}/m\mathbb{Z}} [y]_m := [x \underbrace{+}_{+ \text{ auf } \mathbb{Z}} y]_m \ ,$$
$$[x]_m \underbrace{\cdot}_{\cdot \text{ auf } \mathbb{Z}/m\mathbb{Z}} [y]_m := [x \underbrace{\cdot}_{\cdot \text{ auf } \mathbb{Z}} y]_m \ .$$

Bemerkung

$+$ ist auf $\mathbb{Z}/m\mathbb{Z}$ ist wohldefiniert, d.h. unabhängig von der Wahl der Repräsentanten x und y der jeweiligen Äquivalenzklassen:

- Seien $x, x' \in [x]_m$ und $y, y' \in [y]_m$.
- Dann gilt $x \equiv_m x'$ und $y \equiv_m y'$, also auch $x + y \equiv_m x' + y'$.
- Somit $[x + y]_m = \{z \in \mathbb{Z} \mid z \equiv_m x + y\} = \{z \in \mathbb{Z} \mid z \equiv_m x' + y'\} = [x' + y']$.

Analog zeigt man, dass $\cdot$ auf $\mathbb{Z}/m\mathbb{Z}$ wohldefiniert ist.

Damit können wir im endlichen Zahlenraum der Restklassen $\mathbb{Z}/m\mathbb{Z}$ rechnen. Aufgrund von Definition 1.2.11 und Beobachtung 1.2.4 wissen wir, dass wir zur Berechnung von $[a] + [b]$ einfach nur die Restklasse $[a + b]$ bestimmen müssen – wir also alternativ auch erst mal mit den Repräsentanten rechnen und dann die Restklasse nehmen können – und dass es dabei egal ist, welche Repräsentanten a und b der Restklassen $[a]$ und $[b]$ wir verwenden.

Beispiel 1.2.12
$[1]_6 + [0]_6 = [1 + 0]_6 = [1]_6$, *oder mit anderen Repräsentanten (und unnötig komplex)*
$[1]_6 + [0]_6 = [25]_6 + [666]_6 = [25 + 666]_6 = [691]_6 = [1]_6$

Da es sich bei $\mathbb{Z}/m\mathbb{Z}$ um eine endliche Menge (von Restklassen) handelt, kann man die beiden Verknüpfungen $+$ und $\cdot$ auch leicht durch ihre sogenannten **Verknüpfungstafeln** darstellen. Die Verknüpfungstafeln für $+$ und $\cdot$ über $\mathbb{Z}/6\mathbb{Z}$ sind beispielsweise:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Man kann leicht ablesen: $[3] + [4] = [1]$ oder $[3] \cdot [4] = [0]$.

Gruppen, Ringe und Körper

Um zu verstehen, wieso wir beim Rechnen mit den Restklassen immer aus Summen subtrahieren, aber nur in speziellen Fällen aus Produkten kürzen dürfen, müssen wir uns einige der dem Rechnen – auch in $\mathbb{Z}/m\mathbb{Z}$ – zu Grunde liegenden algebraischen Grundkonzepte und Begriffe etwas genauer ansehen. (Eine etwas ausführlichere Einführung in diese Konzepte findet sich u.A. im Anhang A dieses Skriptes.)

Grundsätzlich kann man jede Menge X mit einer beliebigen Verknüpfung $* : X \times X \to X$ versehen, die man sich auch als zweistelligen Operation bzw. Funktion mit zwei Argumenten $a, b \in X$ und Ergebnis $a * b \in X$ vorstellen kann. Ist X endlich, kann man so eine Verknüpfung $*$ einfach durch das Angeben der Verknüpfungstafel definieren.

Vernünftig mathematisch „rechnen“ kann man mit solchen Verknüpfungen allerdings nur, wenn sie einige zusätzliche Eigenschaften erfüllen.

Zunächst betrachten wir nur eine einzelne Verknüpfung.

Definition 1.2.13 Sei X eine Menge und $* : X \times X \to X$ eine **Verknüpfung auf** X.

(i) Wir nennen das Paar $(X, *)$ eine **Gruppe**, wenn gilt:

a) $*$ ist **assoziativ**, d.h. es gilt

$$\forall x, y, z \in X : \; x * (y * z) = (x * y) * z$$

b) Es existiert ein sogenanntes **neutrales Element** $e \in X$, für das gilt

$$\forall x \in X : \; e * x = x * e = x \; .$$

c) Für jedes Element $x \in X$ existiert ein zugehöriges **inverses Element** $i(x) \in X$, so dass gilt

$$x * i(x) = i(x) * x = e \; .$$

(ii) Ist $*$ zusätzlich **kommutativ**, d.h. gilt

$$\forall x, y \in X : \; x * y = y * x \; ,$$

so nennen wir die Gruppe $(X, *)$ **kommutativ** oder **abelsch**.

(iii) Die Anzahl der Elemente von X nennen wir $ord(X) := |X|$ die **Ordnung** von $(X, *)$.

Ist $ord(X)$ endlich, so sprechen wir von einer endlichen Gruppe.

Bemerkung

- Ist klar, um welche Verknüpfung $*$ es geht, schreibt man oft X statt $(X, *)$.
- Heißt die Verknüpfung $*$,$\cdot$, $\circ$, etc. (**Multiplikative Notation**), so
  - schreibt man oft abkürzend xy statt $x * y$,
  - bezeichnet man das neutrale Element oft mit e oder 1,
  - bezeichnet man das inverse Element zu x mit x^{-1}
- Heißt die Verknüpfung $+$ etc. (**Additive Notation**), so
  - kürzt man $x + y$ nie ab,
  - bezeichnet man das neutrale Element oft mit 0,
  - bezeichnet man das inverse Element zu x mit $-x$.

Eine wesentliche Eigenschaft von Gruppen ist, dass zu jedem Element ein eindeutiges Inverses existiert.

- Damit kann man in Ausdrücken „kürzen“, also gleiche Faktoren auf der linken und der rechten Seite von Produktgleichungen bzw. gleiche Summanden auf der linken und der rechten Seite einer Summengleichung weglassen.
- Damit kann man einfache Gleichung nach einer Unbekannten auflösen.

Satz 1.2.14 (Kürzungsregel) *Sei $(X, *)$ eine Gruppe. Für alle „Variablen“ $x, y \in X$ und alle „Parameter“ $a, b \in X$ gilt*

(i) $a * x = a * y \quad \Rightarrow \quad x = y$
$x * a = y * a \quad \Rightarrow \quad x = y$

(ii) *$a * x = b$ hat eine eindeutige Lösung, nämlich $x = a^{-1} * b$.*
$x * a = b$ hat eine eindeutige Lösung, nämlich $x = b * a^{-1}$.

Beweis.

(i) $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$

(ii) analog □

Beispiel 1.2.15

a) Die ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Addition $+$ bilden eine Gruppe.

Das neutrale Element ist die Zahl 0, da $x + 0 = 0 + x = x$ für alle $x \in \mathbb{Z}$ gilt.

Zu jeder Zahl $x \in \mathbb{Z}$ existiert auch ein (bzgl. der Operation $+$) inverses Element, nämlich genau $-x$, so dass $x + (-x) = (-x) + x = 0$.

b) Die ganzen Zahlen $\mathbb{Z}$ zusammen mit der üblichen Multiplikation $\cdot$ bilden keine Gruppe. Es existiert zwar ein neutrales Element, die Zahl 1 mit $x \cdot 1 = 1 \cdot x = x$ für alle $x \in \mathbb{Z}$, aber nicht zu jedem $x \in \mathbb{Z}$ existiert ein (bzgl. der Operation $\cdot$) inverses Element: Für $x = 2$ existiert z.B. keine Zahl $y \in \mathbb{Z}$, so dass $2 \cdot y = 1$ gilt.

c) Für festes $m \in \mathbb{Z}$, $m \geq 2$, bilden die Restklassen $\mathbb{Z}/m\mathbb{Z}$ zusammen mit der in Definition 1.2.11 erklärten Addition eine Gruppe.

Das neutrale Element ist die Restklasse $[0]$, da $[x] + [0] = [0] + [x] = [x]$ für alle $[x] \in Z/m\mathbb{Z}$ gilt.

Zu jeder Restklasse $[x] \in \mathbb{Z}/m\mathbb{Z}$ existiert auch eine (bzgl. der Operation $+$) inverse Restklasse, nämlich genau $[-x] = [m - x]$, so dass $[x] + [-x] = [-x] + [x] = [0]$.

d) Für festes $m \in \mathbb{Z}$, $m \geq 2$, bilden die Restklassen $\mathbb{Z}/m\mathbb{Z}$ zusammen mit der in Definition 1.2.11 erklärten Multiplikation keine Gruppe.

Das neutrale Element ist die Restklasse $[1]$, da $[x] \cdot [1] = [1] \cdot [x] = [x]$ für alle $[x] \in Z/m\mathbb{Z}$ gilt.

Nicht zu jeder Restklasse $[x] \in \mathbb{Z}/m\mathbb{Z}$ existiert auch eine (bzgl. der Operation $\cdot$) inverse Restklasse: So gibt es zur Restklasse $[0]$ keine inverse Restklasse $[y]$ mit $[0] \cdot [y] = [1]$.

Komplexere Strukturen ergeben sich, wenn man zwei verschiedene Verknüpfungen auf einer Menge X gleichzeitig betrachtet.

Definition 1.2.16 Sei R eine Menge mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$.

(i) Das Tripel $(R, +, \cdot)$ heißt **Ring**, wenn

a) $(R, +)$ ist eine kommutative Gruppe.

- Das neutrale Element bzgl. $+$ heißt **Nullelement** $0 \in R$.
- Das zu $a \in R$ inverses Element bzgl. $+$ bezeichnen wir $-a$.

b) Die Verknüpfung $\cdot$ ist assoziativ, d.h.

$$\forall a, b, c \in R : \ a \cdot (b \cdot c) = (a \cdot b) \cdot c \ .$$

c) Es gelten die **Distributivgesetze**, d.h.

$$\begin{aligned} \forall a, b, c \in R : &\quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \ , \\ \forall a, b, c \in R : &\quad (a + b) \cdot c = (a \cdot c) + (b \cdot c) \ . \end{aligned}$$

(ii) Falls zusätzlich die Verknüpfung $\cdot$ kommutativ ist, also

$$\forall a, b \in R : \ a \cdot b = b \cdot a,$$

so nennt man $(R, +, \cdot)$ einen **kommutativen Ring**.

(iii) Falls es ein neutrales Element für die Multiplikation gibt, also ein $e \in R$, so dass

$$\forall a \in R : \ e \cdot a = a \cdot e = a \ ,$$

so nennt man $(R, +, \cdot)$ einen **Ring mit Eins**.

Man bezeichnet das neutrale Element der Multiplikation dann mit e oder mit 1.

(iv) Ist sogar $(R \setminus \{0\}, \cdot)$ eine kommutative Gruppe, so nennt man $(R, +, \cdot)$ einen **Körper**.

Bemerkung

- Wir schreiben nur R, wenn $+$ und $\cdot$ klar sind.
- Wir schreiben $ab := a \cdot b$ sowie $a - b := a + (-b)$.
- Wir vereinbaren „Punktrechnung vor Strichrechnung“.
- Die in der Definition eines Körpers (iv) gestellte zusätzliche Forderung, dass $(R \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist, bedeutet insbesondere, dass es zu jedem Element a außer 0, dem neutralen Element der Addition, tatsächlich ein inverses Element a^{-1} für die Multiplikation geben muss.

Beispiel 1.2.17

(a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *sind jeweils kommutativer Ring mit Einselement.*

(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *und* $(\mathbb{C}, +, \cdot)$ *sind sogar Körper,* $(\mathbb{Z}, +, \cdot)$ *hingegen nicht.*

(c) Die reellen, quadratischen $n \times n$*-Matrizen* $\mathbb{R}^{n,n}$ *bilden zusammen mit der Matrixaddition* $+$ *und der Matrixmultiplikation* $\cdot$ *einen Ring. Dieser ist aber nicht kommutativ, da die Matrixmultiplikation nicht kommutativ ist.*

(d) $\mathbb{F}_2 = \{0, 1\}$ *ist mit folgenden Verknüpfungen kommutativer Ring:*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(e) $\mathbb{C}[x] := \{f(x) = \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in \mathbb{C}\}$ *ist Menge der komplexen Polynome.*

Mit der üblichen Addition

$$(\sum_{i=0}^{n} a_i x^i) + (\sum_{i=0}^{n} b_i x^i) := \sum_{i=0}^{n} (a_i + b_i) x^i$$

und Multiplikation

$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) := \sum_{i=0}^{n} c_i x^i \quad \text{mit } c_i := \sum_{k=0}^{i} a_k b_{i-k}$$

wird $\mathbb{C}[x]$ *zum Polynom-Ring.*

Nullelement: $f(x) = 0$ *Einselement:* $f(x) = 1$

Man prüft leicht nach, dass für jedes feste $m \in \mathbb{N}$, $m \geq 2$, die Menge $\mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m zusammen mit den in Definition 1.2.11 erklärten Verknüpfungen der Addition $(+)$ und der Multiplikation $(\cdot)$ einen kommutativen Ring mit Einselement bilden.

Beobachtung 1.2.18 *Für jedes feste* $m \in \mathbb{N}$, $m \geq 2$, *ist* $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ *ein kommutativer Ring mit Nullelement* $[0]$ *und Einselement* $[1]$.

Das bedeutet insbesondere:

(i) $\mathbb{Z}/m\mathbb{Z}$ bildet zusammen mit der Addition $+$ eine kommutative Gruppe:

a) Kommutativ- und Assoziativgesetz gelten für die Addition:

$$\forall [x], [y] \in \mathbb{Z}/m\mathbb{Z} : \ [x] + [y] = [y] + [x]$$
$$\forall [x], [y], [z] \in \mathbb{Z}/m\mathbb{Z} : \ ([x] + [y]) + [z] = [x] + ([y] + [z])$$

b) Es gibt mit $[0]$ ein neutrales Element bezüglich der Addition:

$$\forall [x] \in \mathbb{Z}/m\mathbb{Z} : \ [0] + [x] = [x] = [x] + [0]$$

c) Es gibt zu jedem $[a]$ mit $[-a]$ ein (eindeutiges) Inverses bezüglich der Addition:

$$\forall [a] \in \mathbb{Z}/m\mathbb{Z} \ \exists (-[a]) = [-a] \in \mathbb{Z}/m\mathbb{Z} : \ [a] + [-a] = [0] = [-a] + [a]$$

(ii) $\mathbb{Z}/m\mathbb{Z}$ bildet zusammen mit der Multiplikation $\cdot$ ein kommutatives Monoid:

a) Kommutativ- und Assoziativgesetz gelten für die Multiplikation.

$$\forall [x], [y] \in \mathbb{Z}/m\mathbb{Z} : \ [x] \cdot [y] = [y] \cdot [x]$$
$$\forall [x], [y], [z] \in \mathbb{Z}/m\mathbb{Z} : \ ([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$$

b) Es gibt mit $[1]$ ein neutrales Element bezüglich der Multiplikation.

$$\forall [x] \in \mathbb{Z}/m\mathbb{Z} : \ [1] \cdot [x] = [x] = [x] \cdot [1]$$

(iii) Es gelten die Distributivgesetze:

$$\forall [x], [y], [z] \in \mathbb{Z}/m\mathbb{Z} : \ [x] \cdot ([y] + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$$
$$\forall [x], [y], [z] \in \mathbb{Z}/m\mathbb{Z} : \ ([x] + [y]) \cdot [z] = ([x] \cdot [z]) + ([y] \cdot [z])$$

Die unter (i) genannten Eigenschaften bedeuten, dass Summanden beim Rechnen in $\mathbb{Z}/m\mathbb{Z}$ beliebig vertauscht und zusammengefasst werden dürfen, dass die Addition von $[0]$ alle Werte unverändert lässt und dass es zu jeder Restklasse $[a]$ modulo m auch tatsächlich genau eine **additiv inverse** Restklasse, nämlich gerade $[-a] = [m - a]$ gibt, so dass die Summe $[a] + [-a]$ gerade die additiv neutrale Restklasse $[0]$ ergibt.

Beispiel Sei $m = 9$. Die zu $[4]$ additiv inverse Restklasse ist dann $[-4] = [5]$, da $[4]+[5] = [9] = [0]$. (Oder anders: da $4 + 5 \equiv 0 \mod 9$.)

Die unter (ii) genannten Eigenschaften bedeuten, dass Produkte beim Rechnen in $\mathbb{Z}/m\mathbb{Z}$ beliebig vertauscht und zusammengefasst werden dürfen und dass die Multiplikation mit $[1]$ alle Werte unverändert lässt. Die unter (iii) genannten Distributivgesetze sind selbsterklärend.

Wir hatten in Beobachtung 1.2.8 jedoch bereits festgestellt, dass wir beim Rechnen modulo m nicht ohne Weiteres aus Produkten kürzen können. Der Grund dafür ist, dass es bei der Multiplikation im Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ nicht zu jedem Wert $[a]$ ein multiplikatives Inverses $[a]^{-1}$ geben muss, so dass $[a] \cdot [a]^{-1} = [1]$ ist.

Auch die ganzen Zahlen $\mathbb{Z}$ bilden zusammen mit der Addition und der Multiplikation einen kommutativen Ring mit Einselement. Auch im Ring der ganzen Zahlen gibt es lediglich für die beiden Zahlen -1 und 1 multiplikative Inverse (nämlich -1 und 1), für alle Zahlen $x \in \mathbb{Z} \setminus \{-1, 1\}$ existiert kein Zahl $y \in \mathbb{Z}$ mit $x \cdot y = 1$.

Im Gegensatz zu den ganzen Zahlen $\mathbb{Z}$ kann es im endlichen Ring $\mathbb{Z}/m\mathbb{Z}$ aber mehr Elemente als die $[1]$ oder $[-1]$ geben, für die es multiplikative Inverse gibt. Diese nennen wir Einheiten.

Definition 1.2.19 Sei R ein kommutativer Ring mit Einselement.

(i) $a \in R$ heißt **Einheit**, falls es ein $a^{-1} \in R$ mit $a^{-1}a = aa^{-1} = 1$ gibt.

(ii) $R^* := \{a \in R \mid a \text{ ist Einheit}\}$ heißt **Einheitengruppe** von R.

Entsprechend dieser Definition ist ein kommutativer Ring R mit Einselement genau dann ein Körper, wenn $|R| \geq 2$ und seine Einheitengruppe gerade $R^* = R \setminus \{0\}$ ist, d.h. alle Elemente außer 0 sind Einheiten.

Man prüft leicht nach, dass die Menge der Einheiten unter der multiplikativen Verknüpfung $\cdot$ immer abgeschlossen ist, d.h. für alle $a, b \in R^*$ gilt immer auch $a \cdot b \in R^*$ und $a^{-1}, b^{-1} \in R^*$. Sie bilden daher zusammen mit der Multiplikation die Gruppe $(R^*, \cdot)$.

Beispiel 1.2.20 *In $\mathbb{Z}/10\mathbb{Z}$ sind die Elemente $[1], [3], [7], [9]$ Einheiten. Die zugehörigen Inversen sind*

$[1]^{-1} = [1]$, *da* $[1] \cdot [1] = [1]$, *bzw.* $1 \cdot 1 \equiv 1 \mod 10$

$[3]^{-1} = [7]$, *das* $[3] \cdot [7] = [21] = [1]$

$[7]^{-1} = [3]$, *das* $[7] \cdot [3] = [21] = [1]$

$[9]^{-1} = [9]$, *das* $[9] \cdot [9] = [81] = [1]$

Für alle anderen Restklassen in $\mathbb{Z}/10\mathbb{Z}$ gibt es keine multiplikativen Inversen.

Folglich ist die Einheitengruppe $(\mathbb{Z}/10\mathbb{Z})^* = \{[1], [3], [7], [9]\}$.

Man prüfe selbst nach, dass auch alle Produkte von $\{[1], [3], [7], [9]\}$ wieder in $\{[1], [3], [7], [9]\}$ liegen.

In $\mathbb{Z}/m\mathbb{Z}$ können wir leicht charakterisieren, welche Elemente $[a]$ tatsächlich Einheiten sind.

Satz 1.2.21 *Sei $m \in \mathbb{N}$, $m \geq 2$. $[a] \in \mathbb{Z}/m\mathbb{Z}$ ist genau dann eine Einheit, also modulo m invertierbar, wenn $ggT(a, m) = 1$.*

Beweis. Übung! □

Bemerkung Man erkennt die Einheiten in $\mathbb{Z}/m\mathbb{Z}$ sehr leicht in der Verknüpfungstafel der Multiplikation: $[a]$ ist eine Einheit in $\mathbb{Z}/m\mathbb{Z}$, wenn in der zu $[a]$ gehörenden Zeile in einer der Ergebnisspalten die $[1]$ vorkommt. Ist $[b]$ die entprechende Spalte, so gilt dann nämlich $[a]\cdot[b] = [1]$, also $[a]^{-1} = [b]$.

Diese Bestimmung des multiplikativen Inversen $[a]^{-1}$ für gegebenes $[a]$ über die Verknüpfungstabelle erfordert allerdings im schlimmsten Fall die Berechnung der kompletten Zeile von $[a]$, also aller m Ergebnisse $[a] \cdot [b]$ mit $[b] \in \mathbb{Z}/m\mathbb{Z}$. Dies ist sehr ineffizient. Eine effizientere Berechnung ist mit dem Euklidischen Algorithmus möglich und wird in Kapitel 1.3 vorgestellt.

Im Vergleich zum unendlich großen Ring der ganzen Zahlen $\mathbb{Z}$ gibt es eine weitere Besonderheit im endlichen Restklassenring $\mathbb{Z}/m\mathbb{Z}$: Beim Rechnen mit ganzen Zahlen folgt für $a, b \in \mathbb{Z}$ aus der Gleichung $a \cdot b = 0$ sofort $a = 0$ oder $b = 0$, d.h. ein Produkt kann nur dann 0 sein, wenn wenigstens einer der Faktoren bereits 0 ist. Dies gilt in $\mathbb{Z}/m\mathbb{Z}$ nicht mehr: Beispielsweise gilt im Ring der Restklassen modulo 6 zwar $[2] \cdot [3] = [0]$, aber auch $[2] \neq [0]$ und $[3] \neq [0]$. Es ist also in bestimmten Fällen möglich, aus Faktoren ungleich $[0]$ das Produkt $[0]$ zu erhalten. Diese Faktoren sind also beim Rechnen modulo m Teiler der $[0]$.

Definition 1.2.22 Sei R ein kommutativer Ring.

(i) $a \in R$ heißt **Nullteiler**, wenn es $b \in R \setminus \{0\}$ mit $b \cdot a = 0$ bzw. $a \cdot b = 0$ gibt.

(ii) R heißt **nullteilerfrei**, wenn es außer 0 keine Nullteiler gibt.

Für $\mathbb{Z}/m\mathbb{Z}$ können wir wieder sehr leicht charakterisieren, welche Elemente $[a]$ Nullteiler sind.

Satz 1.2.23 *Sei $m \in \mathbb{N}$, $m \geq 2$. $[a] \in \mathbb{Z}/m\mathbb{Z}$ ist genau dann Nullteiler wenn $ggT(a, m) \neq 1$.*

Beweis. Übung! □

Bemerkung Man erkennt die Nullteiler in $\mathbb{Z}/m\mathbb{Z}$ sehr leicht in der Verknüpfungstafel der Multiplikation: $[a]$ ist ein Nullteiler in $\mathbb{Z}/m\mathbb{Z}$, wenn in der zu $[a]$ gehörenden Zeile in einer der Ergebnisspalten, welche nicht zur Spalte $[0]$ gehören, die $[0]$ vorkommt. Ist $[b] \neq [0]$ die entprechende Spalte, so gilt dann nämlich $[a] \cdot [b] = [0]$.

Diese Bestimmung der Nullteiler über die Verknüpfungstabelle erfordert allerdings im schlimmsten Fall wieder die Berechnung vieler Ergebnisse $[a] \cdot [b]$ und ist sehr ineffizient. Eine Bestimmung der Teiler von m und anschließend aller Zahlen $a < m$ mit $ggT(a, m) \neq 1$ ist wesentlich effizienter.

Als direkte Folgerung der Sätze 1.2.21 und 1.2.23 sehen wir, dass jedes $[a] \in \mathbb{Z}/m\mathbb{Z}$ entweder ein Nullteiler oder eine Einheit von $\mathbb{Z}/m\mathbb{Z}$ ist.

Folglich ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper (d.h. alle Elemente außer $[0]$ sind Einheiten), wenn m eine Primzahl ist und somit keine Zahlen $a < m$ mit $ggT(a, m) \neq 1$ existieren.

Folgerung 1.2.24 *$\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beispiel 1.2.25

a) Wir betrachten $\mathbb{Z}/6\mathbb{Z}$. Da 6 keine Primzahl ist, muss es Nullteiler ungleich $[0]$ geben. Offenbar gilt

$$[2] \cdot [3] = [6] = [0], \quad \text{also sind } [2] \text{ und } [3] \text{ Teiler von } [0].$$

Die Einheitengruppe von $\mathbb{Z}/6\mathbb{Z}$ ist $(\mathbb{Z}/6\mathbb{Z})^* = \{[1], [5]\}$.

Die Verknüpfungstafel der Multiplikation ist:

$\cdot$	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*
[0]	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*
[1]	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*
[2]	*[0]*	*[2]*	*[4]*	*[0]*	*[2]*	*[4]*
[3]	*[0]*	*[3]*	*[0]*	*[3]*	*[0]*	*[3]*
[4]	*[0]*	*[4]*	*[2]*	*[0]*	*[4]*	*[2]*
[5]	*[0]*	*[5]*	*[4]*	*[3]*	*[2]*	*[1]*

Man erkennt die Nullteiler und Einheiten leicht in der Verknüpfungstafel:

- *Das Nullelement $[0]$ ist immer Nullteiler, da alle Produkte mit $[0]$ wieder $[0]$ sind.*
- *Ein Element ist (linker) Nullteiler, wenn in der zugehörigen Zeile in einer nicht zu $[0]$ gehörenden Spalte das Ergebnis $[0]$ auftritt.*

  Im Beispiel sind also $[2], [3], [4]$ Nullteiler.
- *Ein Element ist Einheit, wenn in der zugehörigen Zeile und Spalte die $[1]$ auftritt. Im Beispiel sind also $[1], [5]$ die Einheiten.*

b) $\mathbb{Z}/5\mathbb{Z}$ ist ein Körper, da 5 eine Primzahl ist und es somit keine Nullteiler ungleich $[0]$ geben kann. (Zur Übung mit Verknüpfungstafel selbst prüfen.)

Die folgende Beobachtung fasst noch einmal die wichtigsten Vereinfachungs- und Lösungsregeln für modulares Rechnen zusammen.

Beobachtung 1.2.26 *Seien $m \in \mathbb{N}$, $m \geq 2$, $[x], [y] \in \mathbb{Z}/m\mathbb{Z}$ Variablen und $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$ gegebene Parameter.*

(i) Summen können Sie immer durch Addition von additiven Inversen vereinfachen oder auflösen:

a) $[a] + [x] = [a] + [y] \quad \Rightarrow \quad [x] = [y]$
$[x] + [a] = [y] + [a] \quad \Rightarrow \quad [x] = [y]$

b) $[a] + [x] = b$ hat eine eindeutige Lösung, nämlich $[x] = [-a] + [b]$.
$[x] + [a] = [b]$ hat eine eindeutige Lösung, nämlich $[x] = [b] + [-a]$.

(ii) Produkte können Sie nur dann durch Multiplikation mit multiplikativen Inversen vereinfachen oder auflösen, wenn diese existieren, also wenn im Folgenden $ggT(a,m) = 1$ *gilt:*

a) Wenn $ggT(a,m) = 1$*, so folgt aus* $[a] \cdot [x] = [a] \cdot [y]$ *auch* $[x] = [y]$.
Wenn $ggT(a,m) = 1$*, so folgt aus* $[x] \cdot [a] = [y] \cdot [a]$ *auch* $[x] = [y]$.

b) Wenn $ggT(a,m) = 1$*, so hat* $[a] \cdot [x] = [b]$ *die eindeutige Lösung* $[x] = [a]^{-1} \cdot [b]$.
Wenn $ggT(a,m) = 1$*, so hat* $[x] \cdot [a] = [b]$ *die eindeutige Lösung* $[x] = [b] \cdot [a]^{-1}$.

Falls $ggT(a,m) \neq 1$*, so sind die Folgerungen in a) falsch und die Gleichungen in b) können mehrere oder gar keine Lösungen haben (aber sie haben definitiv keine eindeutigen Lösungen).*

1.3. Der Euklidische Algorithmus

Wie berechnet man den ggT zweier Zahlen?

- Reduziere die Zahlen mit folgender Beobachtung, bis der ggT offensichtlich ist.

Lemma 1.3.1 *Seien $x, y \in \mathbb{Z}$, $y \neq 0$. Seien $q, r \in \mathbb{Z}$ so, dass*

$$x = qy + r. \tag{*}$$

(Division mit Rest: Man kann sogar $0 \leq r < |y|$ fordern.) Dann gilt

(i) $T(x, y) = T(y, r)$ *und*

(ii) $ggT(x, y) = ggT(y, r)$.

Beweis. Wir zeigen (i), (ii) folgt direkt aus (i).

$\subseteq$ Sei $t \in T(x, y)$.

Dann gilt $t|x$ und $t|y$.

Dann folgt $t|qy$ und somit auch $t|(x - qy)$.

Wegen $r = x - qy$ heißt das also $t|r$.

Somit $t \in T(y, r)$.

$\supseteq$ Analog. □

Wiederholtes Anwenden von Lemma 1.3.1 ist Kern des Euklidischen Algorithmus:

Satz 1.3.2 (Euklidischer Algorithmus)

Seien $x, y \in \mathbb{Z}$, $y \neq 0$. Durch wiederholte Division mit Rest erhält man

$$\begin{array}{rll}
(1) & x = q_1 y + r_1 & \text{mit } 0 < r_1 < |y| \\
(2) & y = q_2 r_1 + r_2 & \text{mit } 0 < r_2 < r_1 \\
(3) & r_1 = q_3 r_2 + r_3 & \text{mit } 0 < r_3 < r_2 \\
 & \vdots & \\
(n) & r_{n-2} = q_n r_{n-1} + r_n & \text{mit } 0 < r_n < r_{n-1} \\
(n+1) & r_{n-1} = q_{n+1} r_n + 0 &
\end{array}$$

Dann gilt $ggT(x, y) = ggT(r_n, 0) = r_n$.

Beweis. Wiederholtes Anwenden von Lemma 1.3.1 liefert:
$ggT(x, y) = ggT(y, r_1) = \cdots = ggT(r_n, 0) = r_n$. □

Bemerkung

- Die Zeilen entsprechen den Iterationen des Algorithmus.

  Die Kette endet, sobald der Rest 0 auftritt.

  Die Anzahl der Iterationen ist endlich, da die Reste streng monoton fallend und nichtnegativ sind.

- Setzt man die Gleichungen in dieser Reihenfolge wieder ineinander ein, so erhält man auch eine Darstellung $ggT(x, y) = r_n = ax + by$ mit $a, b \in \mathbb{Z}$.

  Dabei stellt man zunächst alle Gleichungen nach r_i um, setzt dann jeweils den dabei entstehenden Ausdruck für „$r_i = \dots$“ in die (nach r_{i+1} umgestellte) Gleichung $(i + 1)$ ein, und fasst am Ende die Koeffizienten vor x und y zusammen. (Dabei dürfen die Produkte mit den r_i nicht ausmultipliziert, sondern nur die Koeffizienten davor zusammengefasst werden!)

  Da $q_i, r_i \in \mathbb{Z}$ für alle i, erhält man automatisch auch $a, b \in \mathbb{Z}$.

  Dieses Verfahren zur Bestimmung von $a, b \in \mathbb{Z}$ mit $ggT(x, y) = ax + by$ nennt man den **erweiterten Euklidischen Algorithmus**.

Beispiel 1.3.3

Bestimme $ggT(456, 210)$ *und* $a, b \in \mathbb{Z}$ *mit* $ggT(456, 210) = a \cdot 456 + b \cdot 210$.

$$\begin{aligned}
(1) \quad & 456 = 2 \cdot 210 + 36 \\
(2) \quad & 210 = 5 \cdot 36 + 30 \\
(3) \quad & 36 = 1 \cdot 30 + 6 \\
(4) \quad & 30 = 5 \cdot 6 + 0
\end{aligned}$$

Also $ggT(456, 210) = 6$.

Auflösen nach Resten:

$$\begin{aligned}
(3) \quad & 6 = 1 \cdot 36 - 1 \cdot 30 \\
(2) \quad & 30 = 1 \cdot 210 - 5 \cdot 36 \\
(1) \quad & 36 = 1 \cdot 456 - 2 \cdot 210
\end{aligned}$$

Iterativ einsetzen:

$$\begin{aligned}
\textit{setze (2) in (3) ein} \quad & 6 = 1 \cdot 36 - 1 \cdot (1 \cdot 210 - 5 \cdot 36) \\
\textit{ergibt } (*) \quad & 6 = 6 \cdot 36 - 1 \cdot 210 \\
\textit{setze (1) in } (*) \textit{ ein} \quad & 6 = 6 \cdot (1 \cdot 456 - 2 \cdot 210) - 1 \cdot 210 \\
& = \underbrace{6}_{a} \cdot 456 \ \underbrace{-13}_{b} \cdot 210
\end{aligned}$$

Folgerung 1.3.4 (Lemma von Bezout)

Seien $x, y \in \mathbb{Z}$ mit $y \neq 0$. Dann gibt es $a, b \in \mathbb{Z}$, so dass $ggT(x, y) = ax + by$.

*($ggT(x, y)$ ist eine $\mathbb{Z}$-Linearkombination (d.h. ganzzahlige Linearkombination) von x und y. a, b heißen auch **Bezout-Koeffizienten**.)*

Beweis.

Der Satz folgt als Nebenprodukt aus erweitertem Euklidischen Algo 1.3.2, siehe oben. □

Folgerung 1.3.5 *Seien $x, y \in \mathbb{Z}$, $y \neq 0$ und $g = ggT(x, y)$. Für alle $t \in T(x, y)$ gilt $t|g$.*

Primzahlen haben spezielle Teilbarkeitseigenschaften:

Lemma 1.3.6 *Ist p eine Primzahl, so gilt für alle $x, y \in \mathbb{Z}$:* $p|xy \Rightarrow (p|x$ *oder* $p|y)$

Bemerkung Diese Eigenschaft gilt tatsächlich nur, wenn p eine Primzahl ist (oder $p \in \{-1, 1\}$)! Für $p = 6$ und $x = 9$, $y = 4$ gilt beispielsweise $6|9 \cdot 4$, aber $6 \nmid 9$ und $6 \nmid 4$.

Beweis.

- Indirekter Beweis: Angenommen, $p \nmid x$ und $p \nmid y$.
- Wegen $p|xy$: $\exists q \in \mathbb{Z}$ mit $pq = xy$.
- $p \nmid x \Rightarrow ggT(p, x) = 1$ (da p prim, also $T(p) = \{1, p\}$)
  $p \nmid y \Rightarrow ggT(p, y) = 1$ (da p prim, also $T(p) = \{1, p\}$)
- Mit Satz 1.3.4 folgt:
  $\exists a, b \in \mathbb{Z} : \ ap + bx = 1$
  $\exists a', b' \in \mathbb{Z} : \ a'p + b'y = 1$
- Multiplikation der Gleichungen liefert

$$1 = (ap + bx)(a'p + b'y) = \underbrace{aa'p^2 + ab'py + ba'px}_{=r \cdot p \text{ mit } r \in \mathbb{Z}} + \underbrace{bb'xy}_{=(bb'q)p}$$

  Also $1 = (r + bb'q) \cdot p$ mit $(r + bb'q) \in \mathbb{Z}$.
- Widerspruch zu $p \geq 2$. □

Folgerung 1.3.7

Für Primzahlen $p, p_1, \ldots, p_n$ gilt: $p | \prod_{i=1}^{n} p_i \Rightarrow \exists i \in \{1, \ldots, n\} : p = p_i$.

Wegen dieser speziellen Teilbarkeits eigenschaften kann man jede natürliche Zahl eindeutig in ihre Primfaktoren zerlegen (faktorisieren), vergleiche Satz 1.1.7.

Bestimmung von Einheiten und Nullteilern in $\mathbb{Z}/k\mathbb{Z}$

Man kann mit dem Euklidischen Algorithmus leicht die Einheiten und deren multiplikative Inverse in $\mathbb{Z}/k\mathbb{Z}$ bestimmen.

Zur Erinnerung:

- $\mathbb{Z}/k\mathbb{Z} = \{[0], [1], \ldots, [k-1]\}$ ist Ring mit Operationen

$$[x] + [y] = [x + y] = [Rest((x + y) : k)]$$
$$[x] \cdot [y] = [x \cdot y] = [Rest((x \cdot y) : k)]$$

- $[x]$ ist Einheit in $\mathbb{Z}/k\mathbb{Z} \Leftrightarrow \exists [y] \in \mathbb{Z}/k\mathbb{Z} : \ [x][y] = [1]$, d.h. $xy \equiv 1 \mod k$
- $[x]$ ist Nullteiler in $\mathbb{Z}/k\mathbb{Z} \Leftrightarrow \exists [0] \neq [y] \in \mathbb{Z}/k\mathbb{Z} : \ [x][y] = [0]$, d.h. $xy \equiv 0 \mod k$

Beobachtung 1.3.8 *(Wiederholung)*

(i) $[x]$ *ist Einheit* $\Leftrightarrow$ $[1]$ *taucht in* $[x]$*-Zeile der Verknüpfungstabelle von* $\cdot$ *auf.*
$\Leftrightarrow$ *Alle* $[j]$ *tauchen in* $[x]$*-Zeile der Verknüpfungstabelle von* $\cdot$ *auf.*

(ii) $[x]$ *ist Nullteiler* $\Leftrightarrow$ $[0]$ *taucht in* $[x]$*-Zeile der Tabelle von* $\cdot|_{(\mathbb{Z}/k\mathbb{Z})\setminus\{[0]\}}$ *auf.*

Für große x und k ist die Berechnung der Tabellen zu aufwendig.

Satz 1.3.9 *Für $k \in \mathbb{N}$ und $x \in \mathbb{Z} \setminus \{0\}$ gilt:*

(i) $[x]$ *ist Einheit in* $\mathbb{Z}/k\mathbb{Z}$ *genau dann, wenn* $ggT(x, k) = 1$.

(ii) $[x]$ *ist Nullteiler in* $\mathbb{Z}/k\mathbb{Z}$ *genau dann, wenn* $ggT(x, k) \neq 1$.

Beweis. (Nur Teil (i).) Sei $g := ggT(x, k)$.

$\Rightarrow$
- Angenommen $[x]$ ist Einheit.
  - Dann gibt es $[y] \in \mathbb{Z}/k\mathbb{Z}$ mit $[x][y] = [1]$, d.h. $xy \equiv 1 \mod k$.
  - Also $k|(xy - 1)$, d.h. $1 = xy - ak$ für ein $a \in \mathbb{Z}$.

- Wegen $g|x$ und $g|k$ folgt $g|1$. Also $g = 1$

$\Leftarrow$
- Angenommen $g = 1$.
- Dann gibt es $a, b \in \mathbb{Z}$ mit $1 = ax + bk$.
- Also $k|(1 - ax)$, d.h. $1 \equiv ax \mod k$.
- Also $[1] = [a][x]$, d.h. $[x]^{-1} = [a]$ □

Man kann mit dem Euklidischen Algorithmus zur Berechnung des ggT also leicht prüfen, welche $[x]$ Einheiten und welche $[x]$ Nullteiler in $\mathbb{Z}/k\mathbb{Z}$ sind. Ist $[x]$ eine Einheit, so liefert der erweiterte Euklidische Algorithmus über die Bezout-Koeffizienten dabei automatisch das multiplikative Inverse.

Algorithmus 1.3.10 [Einheiten und multi. Inverse oder Nullteiler in $\mathbb{Z}/k\mathbb{Z}$]

Input: $x \in \mathbb{Z} \setminus \{0\}$, $k \in \mathbb{N}$

Output: Angabe, ob $[x]$ Einheit oder Nullteiler ist.
$[x]^{-1} \in \mathbb{Z}/k\mathbb{Z}$, falls $[x]$ eine Einheit ist.

(1) Berechne $g = ggT(x, k)$ und $a, b \in \mathbb{Z}$ mit $g = ax + bk$ (mit erweitertem Euklidischen Algorithmus).

(2) Falls $g \neq 1$: „$[x]$ ist keine Einheit“ „$[x]$ ist Nullteiler mit $[q][x] = [0]$“ für $q = k/g$.

(3) Falls $g = 1$: „$[x]$ ist Einheit und $[x]^{-1} := [a]$“ „$[x]$ ist kein Nullteiler“

Folgerung 1.3.11 (zu Satz 1.3.9) *Für $k \in \mathbb{N}$, $k \geq 2$ gilt: $\mathbb{Z}/k\mathbb{Z}$ ist Körper genau dann, wenn k eine Primzahl ist.*

Beispiel 1.3.12

$[13]$ *ist eine Einheit in* $\mathbb{Z}/1000\mathbb{Z}$, *denn* $ggT(13, 1000) = 1$.

Mit Erw. Eukl. Algo findet man $1 = 77 \cdot 13 - 1 \cdot 1000$. *Also* $[13]^{-1} = [77]$ *in* $\mathbb{Z}/1000\mathbb{Z}$.

$[600]$ *ist ein Nullteiler in* $\mathbb{Z}/1000\mathbb{Z}$, *denn* $ggT(600, 1000) = 200$. *Mit Erw. Eukl. Algo findet man* $200 = 2 \cdot 600 - 1 \cdot 1000$. *Also* $[\frac{1000}{200}][600] = [5][600] = [0]$ *in* $\mathbb{Z}/1000\mathbb{Z}$.

$\mathbb{Z}/1000\mathbb{Z}$ *ist kein Körper, da* 1000 *keine Primzahl. Beispielsweise sind* $[5]$ *und* $[600]$ *Nullteiler.*

1.4. Der Chinesische Restsatz

Motivation:

Im endlichen Zahlenraum $\mathbb{Z}/m\mathbb{Z}$ können wir nur bis auf Vielfache von m genau rechnen.

Führen wir die gleiche Rechnung jedoch parallel in mehreren endlichen Zahlenräumen $\mathbb{Z}/m_1\mathbb{Z}$, $\ldots$, $\mathbb{Z}/m_k\mathbb{Z}$, so erhalten wir – bei geschickter Wahl der $m_1, \ldots, m_k$ – insgesamt eine Genauigkeit, die größer als die Genauigkeit in jedem einzelnen Zahlenraum ist. Im besten Fall können wir so insgesamt bis auf Vielfache von $M = m_1 \cdot \ldots \cdot m_k$ genau rechnen (obwohl wir in jedem einzelnen Zahlenraum $\mathbb{Z}/m_i\mathbb{Z}$ nur bis auf Vielfache von m_i genau rechnen müssen und dazu nur mit kleinen Zahlen von 0 bis m_i operieren müssen!). Außerdem können wir die jeweiligen Rechnungen in den einzelnen Zahlenräumen $\mathbb{Z}/m_1\mathbb{Z}$, $\ldots$, $\mathbb{Z}/m_k\mathbb{Z}$ unabhängig voneinander, also auch computertechnisch parallel durchführen; lediglich bei der Rekonstruktion des Endergebnisses mit der Gesamtgenauigkeit bis auf Vielfache von M werden die Ergebnisse aller einzelnen Rechnungen benötigt.

Satz 1.4.1 *Seien R_1, $\ldots$, R_k Ringe mit Einselementen. In jedem dieser Ringe $(R_i, +, \cdot)$ bezeichne $+$ die Addition, $\cdot$ die Multiplikation, 0_{R_i} das Nullelement (neutrales Element der Addition) und 1_{R_i} das Einselement (neutrales Element der Multiplikation).*

Dann wird das kartesische Produkt $R_1 \times \ldots \times R_k$ mit den Verknüpfungen

$$(x_1, \ldots, x_k) \cdot (y_1, \ldots, y_k) := (x_1 \cdot y_1, \ldots, x_k \cdot y_k)$$
$$(x_1, \ldots, x_k) + (y_1, \ldots, y_k) := (x_1 + y_1, \ldots, x_k + y_k)$$

zu einem Ring mit 0-Element $(0_{R_1}, \ldots, 0_{R_k})$, 1-Element $(1_{R_1}, \ldots, 1_{R_k})$ und Einheitengruppe $(R_1 \times \cdots \times R_k)^* = R_1^* \times \cdots \times R_k^*$.

Beweis. Übung / selbst. □

Arithmetik mit mehreren endlichen Ringen:

Für $m_1, \ldots, m_k \in \mathbb{N}$, $m_1, \ldots, m_k \geq 2$ betrachten wir nun die Ringe $\mathbb{Z}/m_1\mathbb{Z}$, $\ldots$, $\mathbb{Z}/m_k\mathbb{Z}$.

Nach obigem Satz ist das kartesische Produkt $P := (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$ ein Ring.

Für $M := m_1 \cdot \ldots \cdot m_k$ ist außerdem $P' := \mathbb{Z}/M\mathbb{Z}$ ein Ring.

Frage(n):

- Was ist die Beziehung zwischen diesen Ringen?
- Wann können Ergebnisse für Rechnungen in $\mathbb{Z}/M\mathbb{Z}$ aus den Ergebnissen der entsprechenden Rechnungen in $(\mathbb{Z}/m_1\mathbb{Z})$, $\ldots$, $(\mathbb{Z}/m_k\mathbb{Z})$ abgeleitet werden?

Diese Fragen führt uns direkt zum mathematischen Begriff des Homomorphismus.

Betrachten wir dazu zunächst den etwas einfacheren Fall von Gruppen, also von Mengen mit nur einer Verknüpfung. Hat man zwei Gruppen $(G, *)$ und $(H, \cdot)$, eine bestehen aus der Menge G mit der Verknüpfung $*$ und eine aus der Menge H mit der Verknüpfung $\cdot$, stellt sich die Frage, ob die beiden Gruppen nicht „eigentlich gleich“ sind, also dass man $(H, \cdot)$ aus $(G, *)$ einfach durch eine Umbenennung der Elemente und der Verknüpfung erhält. Ist dies der Fall, so genügt es

natürlich, eine der Gruppen zu verstehen. Eine etwas schwächere Frage ist, ob die Gruppe $(H, \cdot)$ nicht „eigentlich“ eine Untergruppe von $(G, *)$ ist, deren Elemente und Verknüpfung lediglich umbenannt wurden. Wenn dies so sein sollte, dann muss es ein Abbildung ϕ von G nach H geben, die gerade der „Umbenennung der Elemente“ entspricht, und die mit den Verknüpfungen in den beiden Gruppen kompatibel ist. Kompatibel heißt, dass es egal sein muss, ob wir die „umbenannte“ Verknüpfung $\cdot$ auf den „umbenannten“ Element $\phi(a)$ und $\phi(b)$ für $a, b \in G$ ausführen oder ob wir die Verknüpfung $*$ direkt auf den Elementen $a, b \in G$ ausführen und dann das Ergebnis zu $\phi(a * b)$ umbenennen. Solche Abbildungen ϕ nennen wir (Gruppen-)Homomorphismen.

Ist die Abbildung ϕ nicht nur kompatibel mit den Verknüpfungen $*$ und $\cdot$, sondern außerdem auch noch bijektiv, also invertierbar, so funktioniert diese „Umbenennung“ natürlich auch in der entgegengesetzten Richtung. In diesem Fall sind die Gruppen tatsächlich bis auf Umbenennung der Elemente und der Verknüpfung identisch und wir nennen ϕ einen (Gruppen-)Isomorphismus.

Ist die Abbldung ϕ zwar kompatibel mit den Verknüpfungen $*$ und $\cdot$, aber nicht bijektiv, so erhalten offenbar (mindestens) zwei verschiedene Elemente $a, b \in G$ bei der „Umbenennung“ die gleiche Bezeichnung $\phi(a) = \phi(b) \in H$ (ansonsten wäre ϕ ja invertierbar). In diesem Fall entspricht H einer Untergruppe von G.

Definition 1.4.2 Seien $(G, *)$ und $(H, \cdot)$ Gruppen.

(i) Eine Abbildung $\phi : G \to H$ heißt **Gruppenhomomorphismus**, falls gilt

$$\forall a, b \in G : \ \phi(a * b) = \phi(a) \cdot \phi(b).$$

(ii) Ist ϕ außerdem bijektiv, so heißt ϕ **Gruppenisomorphismus**.
G und H heißen dann **isomorph**, geschrieben $G \simeq H$.

(iii) Die Menge $\ker(\phi) := \phi^{-1}(\{e_H\}) = \{x \in G \mid \phi(x) = e_H\}$ heißt **Kern** von ϕ.

Bemerkung

- morphe: Gestalt, Form homo-: gleich, ähnlich iso-: gleich, identisch
- Isomorphe Gruppen „verhalten“ sich identisch, d.h. sie unterscheiden sich nur in der Bezeichnung der Elemente und der Bezeichnung der Verknüpfung.

Beobachtung 1.4.3 *Ist $\phi : G \to H$ Gruppenhomomorphismus, so gilt*

(i) $\phi(e_G) = e_H$

(ii) $\phi(a^{-1}) = (\phi(a))^{-1}$ *für alle* $a \in G$

(iii) Ist ϕ bijektiv, so ist auch $\phi^{-1} : H \to G$ ein Gruppenisomorphismus.

Beweis. Siehe Anhang. □

Beispiele für Gruppenisomorphismen finden sich im Anhang A dieses Skriptes (Beispiel A.1.32).

Stellt man sich die Fragen nach der Einbettbarkeit oder Gleichheit bis auf die Umbenennung der Element und Verknüpfungen für Ringe, also Mengen mit jeweils zwei Verknüpfungen, führt das auf den Begriff von Ring-Homomorphismen oder Ring-Isomorphismen. Ring-Homomorphismen sind Abbildungen zwischen zwei Ringen, die mit jeweils beiden Verknüpfungen kompatibel sind; Ring-Isomorphismen sind bijektive Ring-Homomorphismen.

Definition 1.4.4

Seien $(R, +, \cdot)$ und $(S, \oplus, \odot)$ Ringe. Eine Abbildung $\phi: R \to S$ heißt **Ring-Homomorphismus**, wenn

(i) $\forall a, b \in R: \ \phi(a + b) = \phi(a) \oplus \phi(b)$

(ii) $\forall a, b \in R: \ \phi(a \cdot b) = \phi(a) \odot \phi(b)$

Ist ϕ bijektiv, so heißt ϕ **Ring-Isomorphismus**.

Die Ringe $(R, +, \cdot)$ und $(S, \oplus, \odot)$ heißen dann **isomorph**, geschrieben $(R, +, \cdot) \simeq (S, \oplus, \odot)$ oder kurz $R \simeq S$.

Bemerkung Sind R und S Ringe mit Einselement, so fordern einige Autoren zusätzlich auch noch $\phi(1_R) = 1_S$ für Ring-Homomorphismen $\phi : R \to S$.

Satz 1.4.5 *Sei $\phi : R \to S$ ein Ring-Homomorphismus. Ist ϕ ein Ring-Isomorphismus (also bijektiv), so ist auch ϕ^{-1} ein Ring-Isomorphismus.*

Sind $(R, +, \cdot)$ und $(S, \oplus, \odot)$ zwei Ringe und ist $\phi : R \to S$ eine Ring-Isomorphismus, so ist also $(S, \oplus, \odot)$ lediglich eine Umbenennung der Elemente in R und der Verknüpfungen $+$ und $\cdot$ und umgekehrt. Um einen beliebigen Ausdruck in R mit den Operationen/Verknüpfungen $+$ und $\cdot$ auf den Elementen $a_1, \ldots, a_k$ zu berechnen, können wir also alternativ auch den entsprechenden Ausdruck in S mit den entsprechend umbenannten Operationen/Verknüpfungen $\oplus$ und $\odot$ auf den umbenannten Elementen $\phi(a_1), \ldots, \phi(a_k)$ berechnen, und dessen Ergebnis $z \in S$ wieder zu $\phi^{-1}(s) \in R$ zurück übersetzen.

Dies bringt uns nun schließlich wieder zurück zu unserer Frage vom Anfang:

- In welcher Beziehung stehen die beiden Ringe $P := (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$ (mit Addition und Multiplikation wie in Definition 1.4.1) und $P' := \mathbb{Z}/M\mathbb{Z}$ mit $M := m_1 \cdot \ldots \cdot m_k$.

Beobachtung 1.4.6

Die Abbildung $\phi : P' \to P, \ [x]_M \mapsto ([x]_{m_1}, \ldots, [x]_{m_k})$ ist ein Ring-Homomorphismus.

(D.h. es gilt $\phi(x + y) = \phi(x) + \phi(y)$ und $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ für alle $x, y \in P'$.)

Beispiel 1.4.7 *Betrachte* $P = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ *und* $P' = \mathbb{Z}/6\mathbb{Z}$.

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$\phi(x)$	$([0],[0])$	$([1],[1])$	$([0],[2])$	$([1],[0])$	$([0],[1])$	$([1],[2])$

$$\begin{aligned}([0]_2,[1]_3) &= \phi([4]_6) = \phi([1]_6 + [3]_6) = \phi([1]_6) + \phi([3]_6) \\ &= ([1]_2,[1]_3) + ([1]_2,[0]_3) = ([1]_2 + [1]_2, [1]_3 + [0]_3) = ([0]_2,[1]_3)\end{aligned}$$

Da ϕ ein Homomorphismus ist, können die Ergebnisse von Additionen und Multiplikationen in den einzelnen Ringen $(\mathbb{Z}/m_k\mathbb{Z})$ immer aus den Ergebnissen der entsprechenden Additionen und Multiplikationen im Produktring $(\mathbb{Z}/M\mathbb{Z})$ rekonstruiert werden: Man wende nach der Rechnung in $(\mathbb{Z}/M\mathbb{Z})$ einfach ϕ an, das liefert die Ergebnisse in allen einzelnen Ringen $(\mathbb{Z}/m_k\mathbb{Z})$. (Das sollte Sie nicht überraschen. Wenn Sie modulo 6 rechnen, können Sie aus dem Ergebnis der Rechnung modulo 6 natürlich auch den Rest des Ergebnisses modulo 2 und der Rest des Ergebnisses modulo 3 rekonstruieren, da 2 und 3 beides Teiler der 6 sind.)

Im konkreten Fall des vorigen Beispiels ist ϕ offenbar sogar bijektiv: Jedes Paar $([i],[j])$ taucht in der Abbildungstabelle von ϕ genau einmal als Ergebnis auf. Das heißt, man kann auch umgekehrt die Ergebnisse von Additionen und Multiplikationen in $\mathbb{Z}/M\mathbb{Z}$ aus denen der Rechnungen in *allen* einzelnen Ringen $\mathbb{Z}/m_k\mathbb{Z}$ rekonstruieren. Der Ring $\mathbb{Z}/6\mathbb{Z}$ und der Produktring $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ sind isomorph.

Der Chinesische Restsatz besagt, dass das genau dann der Fall ist, wenn die m_i paarweise teilerfremd sind.

Satz 1.4.8 (Chinesischer Restsatz, Basisversion für 2 Ringe)
Seien $m_1, m_2 \in \mathbb{N}$ *mit* $ggT(m_1, m_2) = 1$ *und* $M = m_1 \cdot m_2$. *Dann gilt*

$$\mathbb{Z}/M\mathbb{Z} \simeq (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}).$$

(Daraus folgt insbesondere auch $(\mathbb{Z}/M\mathbb{Z})^* \simeq (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$*.)*

Beweis.

- Wir zeigen zunächst, dass ϕ aus 1.4.6 injektiv ist:
  - Seien $[x]_M \neq [y]_M$ in P'. Zu zeigen: $\phi([x]_M) \neq \phi([y]_M)$.
  - Angenommen $\phi([x]_M) = \phi([y]_M)$, d.h. $[x]_{m_1} = [y]_{m_1}$ und $[x]_{m_2} = [y]_{m_2}$.
  - Dann folgt $m_1|(x-y)$ und $m_2|(x-y)$.
  - Daraus folgt sofort $kgV(m_1, m_2)|(x-y)$.
  - Wegen $ggT(m_1, m_2) = 1$ folgt $kgV(m_1, m_2) = m_1 m_2 = M$, also dann $M|(x-y)$.
  - Das heißt aber $[x]_M = [y]_M$, Widerspruch.
- Da $|\mathbb{Z}/M\mathbb{Z}| = m_1 m_2 = |(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z})|$, ist ϕ auch surjektiv. □

Wir können obigen Satz leicht auf das Produkt von mehreren Ringen verallgemeinern:

Folgerung 1.4.9 (Chinesischer Restsatz, allgemeine Version)
Seien $m_1, \ldots, m_k \in \mathbb{N}$ mit $ggT(m_i, m_j) = 1$ für alle $i \neq j$ und $M = m_1 \cdot \ldots \cdot m_k$. Dann gilt

$$\mathbb{Z}/M\mathbb{Z} \simeq (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z}) \ .$$

(Daraus folgt wieder $(\mathbb{Z}/M\mathbb{Z})^* \simeq (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^*$.)

Eine klassische Anwendung des Chinesischen Restsatzes ist das Lösen von Systemen simultaner Kongruenzen, beschrieben im folgenden Satz 1.4.10. Dies entspricht genau der zu Beginn des Kapitels angesprochenen Aufgabe, das Ergebnis einer Rechnung in einem großen Zahlenraum $\mathbb{Z}/M\mathbb{Z}$ aus allen Lösungen der entsprechenden Rechnung in den kleineren Zahlenräumen $\mathbb{Z}/m_1\mathbb{Z}$, $\ldots$, $\mathbb{Z}/m_k\mathbb{Z}$ zu rekonstruieren.

Satz 1.4.10 (Chinesischer Restsatz, klassische Version)
Seien $k \in \mathbb{N}$, $m_1, \ldots, m_k \in \mathbb{N}$ mit $ggT(m_i, m_j) = 1$ für alle $i \neq j$ und $M := m_1 \cdot \ldots \cdot m_k$. Für alle $a_1, \ldots, a_k \in \mathbb{Z}$ hat das System simultaner Kongruenzen

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned} \tag{K}$$

eine Lösung $x' \in \{0, \ldots, M-1\}$. Die Menge aller ganzzahligen Lösungen von (K) ist $\mathbb{L}(K) = x' + M \cdot \mathbb{Z}$.

Das folgende Beispiel zeigt, wie man solche Systeme praktisch löst:

Beispiel 1.4.11 *Bestimme alle Lösungen $x \in \mathbb{Z}$ von*

$$\begin{aligned} x &\equiv 1 \ (= a_1) \mod 3 \ (= m_1) \\ x &\equiv 3 \ (= a_2) \mod 4 \ (= m_2) \\ x &\equiv 2 \ (= a_3) \mod 5 \ (= m_3) \end{aligned} \tag{K}$$

(1) Berechne $M = m_1 \cdot \ldots \cdot m_k$ sowie alle $\bar{m}_i = \frac{M}{m_i}$. Also hier

$$M = 3 \cdot 4 \cdot 5 = 60 \qquad \bar{m}_1 = 4 \cdot 5 = 20,$$
$$\bar{m}_2 = 3 \cdot 5 = 15, \qquad \bar{m}_3 = 3 \cdot 4 = 12.$$

(2) Bestimme jeweils Inverses $[c_i]$ *zu* $[\bar{m}_i]$ *in* $(\mathbb{Z}/m_i\mathbb{Z})$ *(mit Algo. 1.3.10).*

(⇔ Finde c_i*, so dass* $c_i \cdot \bar{m}_i \equiv 1 \mod m_i$*.):*

$$\begin{aligned} c_1 &= 2 && \text{denn } 2 \cdot 20 \equiv 2 \cdot 2 \equiv 1 \mod 3 \\ c_2 &= 3 && \text{denn } 3 \cdot 15 \equiv 3 \cdot 3 \equiv 1 \mod 4 \\ c_3 &= 3 && \text{denn } 3 \cdot 12 \equiv 3 \cdot 2 \equiv 1 \mod 5 \end{aligned}$$

(3) Eine Lösung ist

$$x'' = \bar{m}_1(c_1a_1) + \bar{m}_2(c_2a_2) + \cdots + \bar{m}_k(c_ka_k) \ .$$

Hier: $x'' = 20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 2 = 247$

x'' *ist eine Lösung von (K), denn für alle* $i = 1, \ldots, k$ *gilt*

$$\begin{aligned} x'' &\equiv \underbrace{\bar{m}_1}_{m_2 \cdots m_k} c_1a_1 + \underbrace{\bar{m}_2}_{m_1m_3 \cdots m_k} c_2a_2 \cdots + \underbrace{\bar{m}_k}_{m_1 \cdots m_{k-1}} c_ka_k \mod m_i \\ &\equiv \underbrace{(\bar{m}_ic_i)}_{\equiv 1} a_i \mod m_i \end{aligned}$$

(4) Lösungsmenge $\mathbb{L}(K) = x'' + M\mathbb{Z}$*, also hier* $\mathbb{L}(K) = 247 + 60\mathbb{Z}$*.*
(Die Lösung ist also bis auf Vielfache von 60 eindeutig.)

$x' := Rest(x'' : M) = 7$ *ist Lösung wie in Satz 1.4.10.*

Also $\mathbb{L}(K) = 7 + 60\mathbb{Z}$

Wir haben hier also $[x]_{60} \in \mathbb{Z}/60\mathbb{Z}$ *aus* $[x]_3 = [1]_3$*,* $[x]_4 = [3]_4$ *und* $[x]_5 = [2]_5$ *rekonstruiert.*

1.5. Die Eulersche φ-Funktion, Primzahlen und der kleine Fermat

Die Eulersche φ-Funktion

Frage: Wie viele Einheiten hat $\mathbb{Z}/k\mathbb{Z}$?

Definition 1.5.1 Für $k \in \mathbb{N}$ heißt

$$\begin{aligned}\varphi(k) := |(\mathbb{Z}/k\mathbb{Z})^*| &= \text{Anzahl der Einheiten in } \mathbb{Z}/k\mathbb{Z} \\ &= \text{Anzahl der zu } k \text{ teilerfremden Zahlen in } \{1, \ldots, k\}\end{aligned}$$

die **Eulersche φ-Funktion** von k.

Beispiel 1.5.2

$(\mathbb{Z}/10\mathbb{Z})^* = \{[1], [3], [7], [9]\}, \quad \varphi(10) = 4$

$(\mathbb{Z}/17\mathbb{Z})^* = \{[1], [2], \ldots, [16]\}, \quad \varphi(17) = 16$

Berechnung von $\varphi(k)$:

- Falls k prim: $\varphi(k) = k - 1$. (Alle $[i]$ außer $[0]$ sind Einheiten.)
- Naive Methode sonst:
  Zähle alle $i \in \{1, \ldots, k-1\}$ mit $ggT(i, k) = 1$. $\rightsquigarrow$ Sehr aufwendig. Eine effizientere Berechnung von $\varphi(k)$ ist mit den folgenden Methoden möglich:

Satz 1.5.3 *Ist p eine Primzahl und $e \in \mathbb{N}$, so gilt $\varphi(p^e) = p^{e-1}(p-1)$.*

Beweis.

- Betrachte $X := \{1, \ldots, p^e\}$.
- Die durch p teilbaren Zahlen in X sind $1p$, $2p$, $\ldots$, $p^{e-1}p$.
  Das sind p^{e-1} viele.
- Alle nicht durch p teilbaren Zahlen in X sind auch zu p^e teilerfremd, da p eine Primzahl ist.
  Das sind insgesamt also $|X| - p^{e-1} = p^e - p^{e-1} = p^{e-1}(p-1)$ viele. □

Beispiel 1.5.4

(a) $\varphi(1024) = \varphi(2^{10}) = 2^9(2-1) = 512$.
$\mathbb{Z}/1024\mathbb{Z}$ *hat also 512 Einheiten (und 512 Nullteiler).*

(b) $\varphi(\underbrace{101}_{prim}) = 101^0(101-1) = 100$.
$\mathbb{Z}/101\mathbb{Z}$ *hat also 100 Einheiten (und den trivialen Nullteiler* $[0]$*).*

Mit Hilfe des Chinesischen Restsatzes können wir φ zunächst für Produkte teilerfremder Zahlen berechnen:

Satz 1.5.5 *Sind $m_1, \ldots, m_k \in \mathbb{N}$, $m_i \geq 2$, mit $ggT(m_i, m_j) = 1$, so gilt*

$$\varphi(m_1 \cdot \ldots \cdot m_k) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k).$$

Beweis. Sei $M := m_1 \cdot \ldots \cdot m_k$. Nach Chin. Restsatz ist

$$(\mathbb{Z}/M\mathbb{Z})^* \simeq (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^*,$$

also gilt

$$\begin{aligned}\varphi(m_1 \cdot \ldots \cdot m_k) = |(\mathbb{Z}/M\mathbb{Z})^*| &= |(\mathbb{Z}/m_1\mathbb{Z})^*| \cdot \ldots \cdot |(\mathbb{Z}/m_k\mathbb{Z})^*| \\ &= \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)\ .\end{aligned}$$

□

Mit Hilfe der Primfaktorzerlegung erhalten wir damit eine Möglichkeit zur Berechung von φ für beliebige natürliche Zahlen:

Folgerung 1.5.6 *Sind $p_1 < \cdots < p_k$ Primzahlen und $e_1, \ldots, e_k \in \mathbb{N}$, so gilt*

$$\varphi(p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}) = p_1^{e_1-1}(p_1 - 1) \cdot \ldots \cdot p_k^{e_k-1}(p_k - 1)\ .$$

(Man kann also $\varphi(n)$ für $n \in \mathbb{N}$ aus der Primfaktorzerlegung von n berechnen.)

Beweis. Folgt direkt aus 1.5.3 und 1.5.5. □

Beispiel 1.5.7 *Wie viele Einheiten hat $\mathbb{Z}/1000\mathbb{Z}$?*
$\varphi(1000) = \varphi(2^3 5^3) = 2^2(2-1)5^2(5-1) = 400$
D.h. 400 der Zahlen in $\{1, \ldots, 999\}$ sind zu 1000 teilerfremd.

Wir betrachte nun die Einheitengruppe $(\mathbb{Z}/k\mathbb{Z})^*$ noch einmal etwas etwas genauer.

Definition 1.5.8 Für $[x] \in (\mathbb{Z}/k\mathbb{Z})^*$ seien

$$\langle [x] \rangle = [x]^{\mathbb{N}} := \{[x]^n = \underbrace{[x] \cdot \ldots \cdot [x]}_{n \text{ mal}} \mid n \in \mathbb{N}\}$$

die Menge der verschiedenen Potenzen von $[x]$ in $(\mathbb{Z}/k\mathbb{Z})^*$ und

$$\mathrm{ord}([x]) = |\langle [x] \rangle|$$

die Anzahl der verschiedenen Potenzen von $[x]$ in $(\mathbb{Z}/k\mathbb{Z})^*$.

Bemerkung

- Da $(\mathbb{Z}/k\mathbb{Z})^*$ endlich und jedes $[x] \in (\mathbb{Z}/k\mathbb{Z})^*$ eine Einheit ist, ist jedes $\langle [x] \rangle$ eine endliche Gruppe, welche auch immer alle Potenzen $[x]^{-n} = ([x]^{-1})^n$ des multiplikativ Inversen $[x]^{-1}$ sowie $[x]^0 = [1]$ enthält. Daher findet man auch häufig die Schreibweise $[x]^{\mathbb{Z}}$ für $[x]^{\mathbb{N}} = \langle [x] \rangle$.
- Man nennt Gruppen, die von einem einzelnen Element $[x]$ durch beliebige Potenzen dieses Elements erzeugt werden, auch **zyklische Gruppen**. Ist die zu Grunde liegende Gruppe endlich, wie hier $\mathbb{Z}/k\mathbb{Z}$ für $k \geq 2$, so bilden die von $[x]$ erzeugten Potenzen immer einen Zyklus der Form

$$[1] = [x]^0, \quad [x]^1, \quad [x]^2, \quad \dots \quad [x]^{k-1} = [x]^{-1}, \quad [x]^k = [1], \quad [x]^{k+1} = [x]^k \cdot [x] = [x], \dots,$$

  wobei $k = \operatorname{ord}([x])$ die kleinste Potenz (ungleich 0) von $[x]$ mit $[x]^k = [1]$ und damit die Länge des Zyklus ist (siehe Beobachtung 1.5.10).

Beispiel 1.5.9 *Für* $(\mathbb{Z}/10\mathbb{Z})^* = \{[1], [3], [7], [9]\}$ *sind* $|(\mathbb{Z}/10\mathbb{Z})^*| = 4$ *und*

$\langle [1] \rangle = \{[1]\}$, $\operatorname{ord}([1]) = 1$, $\langle [3] \rangle = \{[1], [3], [9], [7]\}$, $\operatorname{ord}([3]) = 4$
$\langle [7] \rangle = \{[1], [7], [9], [3]\}$, $\operatorname{ord}([7]) = 4$, $\langle [9] \rangle = \{[1], [9]\}$, $\operatorname{ord}([9]) = 2$

Beobachtung 1.5.10

(i) $\langle [x] \rangle$ *ist endliche, zyklische Untergruppe von* $((\mathbb{Z}/k\mathbb{Z})^*, \cdot)$, *erzeugt von* $[x]$.

(ii) $\operatorname{ord}([x]) = \min\{k \geq 1 \mid [x]^k = [1]\}$ *und* $\langle [x] \rangle = \{[1], [x], [x]^2, \dots, [x]^{ord(x)-1}\}$

(iii) $[x]^{|(\mathbb{Z}/k\mathbb{Z})^*|} = [1]$

Beweis.

- Da $\langle x \rangle \subseteq (\mathbb{Z}/k\mathbb{Z})^*$ und $|(\mathbb{Z}/k\mathbb{Z})^*| < \infty$, muss es $n, m \in \mathbb{N}$ mit $n < m$ und $[x]^n = [x]^m$ geben.

  Für $k = m - n > 0$ gilt dann $[x]^n = [x]^m = [x]^n[x]^k$, also $[x]^k = [1]$.

  Daraus folgt bereits (i).
- Sei $k \geq 1$ die kleinste Zahl mit $[x]^k = [1]$.

  Für $n \in \mathbb{N}$ und $q, r \in \mathbb{N}$ gemäß Division durch k mit Rest gewählt, also $n = qk + r$, $0 \leq r < k$, gilt dann

$$[x]^n = [x]^{qk+r} = ([x]^k)^q [x]^r = [x]^r$$

  Also $[x]^n \in \{[x]^0, [x]^1, \dots, [x]^{k-1}\}$.
- Gäbe es $0 \leq r < s < k$ mit $[x]^r = [x]^s$, so wäre $[x]^{s-r} = 1$ mit $s - r < k$. Das Widerspricht der Wahl von k.

  Also sind alle $[x]^r$ mit $0 \leq r < k$ auch paarweise verschieden.

  Daraus folgt (ii).

- Da $\langle [x] \rangle$ eine Untergruppe von $(\mathbb{Z}/k\mathbb{Z})^*$ und $[x]^{\mathrm{ord}(x)} = [1]$, folgt mit dem Satz von Lagrange (siehe A.1.42), dass $\mathrm{ord}(x)$ ein Teiler von $|(\mathbb{Z}/k\mathbb{Z})^*|$ ist, also $|(\mathbb{Z}/k\mathbb{Z})^*| = q \cdot \mathrm{ord}(x)$ mit $q \in \mathbb{N}$.

  Damit folgt auch $[x]^{|(\mathbb{Z}/k\mathbb{Z})^*|} = ([x]^{\mathrm{ord}(x)})^q = [1]^q = [1]$. □

Primzahlen und der kleine Fermat

Frage: Wie erzeugt man große Primzahlen? (z.B. für kryptographische Verfahren)

- Es ist kein Algorithmus bekannt, um einzelne große Primzahlen gezielt zu berechnen.
- **Alternative:** Teste viele Zahlen in einem gewünschten Bereich:
  - Satz 1.1.12 sagt:
    Im Schnitt ist von $\{1, \ldots, n\}$ jede $c \cdot \log(n)$-te Zahl prim. Man beachte, dass c eine Konstante ist und $\log(n)$ viel, viel langsamer als n wächst. Man findet also mit relativ wenigen (sinnvollen) Test ab einem Startwert eine Primzahl. („relativ“ im Verhältnis zur Größe der Startzahl.)
  - Für Primzahlen in der Größenordnung 2^{1024} gilt:

    Mehr als jede 1000-te Zahl ist prim.

    Nach relativ wenigen Tests der ungeraden Zahlen ab 2^{1024} findet man also eine Primzahl.

Frage: Wie testet man, ob eine Zahl p prim ist?

Naiv: Sieb des Erathostenes/Probedivision:

- Erzeuge und Prüfe alle Primzahlen $< \sqrt{p}$. $\quad \rightsquigarrow$ Extrem aufwendig.

Theoretisch effizient: AKS-Algorithmus (Agrawal, Kayal, Saxena)

- Laufzeit wächst nur polynomiell in $\log(n)$ = Codierungslänge der Zahl n.
- Liefert immer exakte Antwort.

  (Die Existenz eines polynomiellen Primzahltests war bis 2002 ein offenes Problem.)

Praktisch effizient: Randomisierte Tests auf Basis des „kleinen Satz von Fermat“ (z.B. Solovay-Strassen-Test oder Miller-Rabin-Test)

- Antwortet Algo „keine Primzahl“, dann ist p mit Sicherheit keine Primzahl.
- Antwortet Algo „Primzahl“, dann ist p nur wahrscheinlich eine Primzahl.

Satz 1.5.11 (Kleiner Satz von Fermat)
Sei $p \in \mathbb{P}$. Dann gilt für alle $x \in \mathbb{N}$

$$x^p \equiv x \mod p \ .$$

Bemerkung

Ist x ein Vielfaches von p, so ist die Aussage trivial.

Andernsfalls ist $ggT(x,p) = 1$, da p prim. Obige Kongruenz ist dann äquivalent zu $x^{p-1} \equiv 1 \mod p$.

Beweis.
Version 1: Per Induktion über x.

Version 2: Die Aussage $x^{p-1} \equiv 1 \mod p$ folgt wegen $\varphi(p) = p - 1$ aus dem folgenden, allgemeineren Satz von Euler. □

Satz 1.5.12 (Satz von Euler)
Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt für alle $x \in \mathbb{N}$ mit $ggT(x,n) = 1$

$$x^{\varphi(n)} \equiv 1 \mod n \ .$$

Beweis.

- Wegen $ggT(x,n) = 1$ ist $[x]$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$, also $[x] \in (\mathbb{Z}/n\mathbb{Z})^*$.
- Damit folgt nach Satz 1.5.10 (iii) sofort $[x]^{|(\mathbb{Z}/n\mathbb{Z})^*|} = [1]$.
- Nach Definition ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.
  Also gilt $[x]^{\varphi(n)} = [1]$, d.h. $x^{\varphi(n)} \equiv 1 \mod n$. □

Bemerkung

- Einfacher **Fermatscher Primzahltest**-Algorithmus (auf Basis von Satz 1.5.11):

  Eingabe: $p \in \mathbb{N}$, $p \geq 3$

  (1) Wähle $a \in \mathbb{N}$ mit $1 < a < p$.

  (2) Wenn $ggT(a,p) \neq 1$, dann „p keine Primzahl".

  (3) Wenn $a^{p-1} \not\equiv 1 \mod p$, dann „$p$ keine Primzahl".

  (4) „Keine Ahnung", gehe zu (1) und wähle anderes a.

  Endet Test nach mehreren Versuchen für verschiedene a mit „Keine Ahnung", so interpretiert man das als „p ist wahrscheinlich Primzahl".

- Es gibt Zahlen $p \notin \mathbb{P}$, so dass trotzdem $x^{p-1} \equiv 1 \mod p$ für alle x mit $ggT(x,p) = 1$ gilt. (sog. Carmichael Pseudoprimzahlen: 561, 1105, ...)
- Satz 1.5.12 ist Grundlage vieler asymmetrischer Verschlüsselungsverfahren wie RSA.

2. Grundzüge der Kryptographie und Codierung

Literatur:

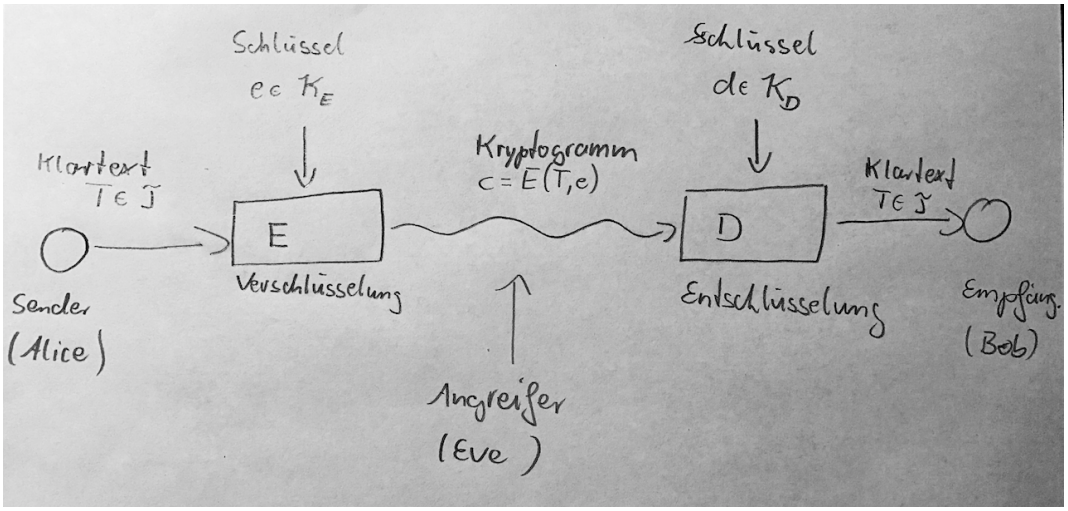
- A. Beutelspacher, M.A. Zschiegner. Diskrete Mathematik für Einsteiger. Springer-Spektrum, Kap. 5 - 7
- M. Aigner: Diskrete Mathematik, Kap. 13 & 14

2.1. Grundzüge der Kryptographie

Literaturempfehlung:

- Kapitel 7 in A. Beutelspacher, M.A. Zschiegner: Diskrete Mathematik für Einsteiger
- Kapitel 14 in M. Aigner: Diskrete Mathematik
- Kapitel 3.5 in A. Steger: Diskrete Strukturen.
- Kapitel 3.3.1 in G. Teschl, S. Teschl: Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra.

Verschlüsselte Datenübertragung (schematische Darstellung):



Definition 2.1.1 Ein **kryptographisches System** besteht aus

- der Menge $\mathcal{T}$ aller möglichen Klartextnachrichten,
- der Menge $\mathcal{C}$ aller möglichen Kryptogramme,
- den Mengen $\mathcal{K}_E$, $\mathcal{K}_D$ aller möglichen Schlüssel zu Ver- bzw. Entschlüsseln und
- den Abbildungen zum Ver- und Entschlüsseln:

$$E : \mathcal{T} \times \mathcal{K}_E \to \mathcal{C} \qquad \text{und} \qquad D : \mathcal{C} \times \mathcal{K}_D \to \mathcal{T},$$

so dass gilt

$$\forall\, e \in \mathcal{K}_E \;\; \exists\, d = d(e) \in \mathcal{K}_D \;\; \forall\, T \in \mathcal{T} : \quad D(E(T,e),d) = T$$

(d.h. für jeden Verschlüsselungsschlüssel existiert ein Entschlüsselungsschlüssel, mit dem sich alle Texte nach Verschlüsseln auch wieder entschlüsseln lassen.)

I.d.R. sind $\mathcal{T}$ und $\mathcal{C}$ die Mengen aller Texte $T \in A^*$ über einem Alphabet A oder die Mengen aller Zahlen in $x \in \mathbb{Z}/k\mathbb{Z}$. (Man verwendet dabei die Zahlen $x \in \{0, \ldots, k-1\}$ als Representanten der Restklassen $[x]$.)

Definition 2.1.2

Ein Kryptosystem heißt **symmetrisch**, wenn $\mathcal{K}_E = \mathcal{K}_D$ und $d(e) = e$ (oder $d(e)$ sehr leicht aus e berechenbar) ist.

Ein Kryptosystem heißt **asymmetrisch**, wenn $d(e)$ in der Praxis nicht oder nur mit extrem großen Aufwand aus e berechnet werden kann.

„Historische“ Kryptosysteme sind symmetrisch und basieren darauf, dass nur Sender und Empfänger den gemeinsamen Schlüssel $e = d$ oder die Abbildungsvorschriften von E und D kennen.

Beispiel 2.1.3

(a) „Caesar-Code“ (auch als `rotN` bekannt)

- *Kodiere Buchstaben A–Z durch Zahlen 1 bis 26.*

  Jeder Buchstabe des Klartextes wird einzeln ver- und entschlüsselt, d.h. es werden eigentlich viele einzelne Klartexte aus $\mathcal{T} = (\mathbb{Z}/26\mathbb{Z})$ verschlüsselt verschickt.

  Der Schlüssel (das `N` in `rotN`) ist ebenfalls eine (für den ganzen Text fest) gewählte Zahl k zwischen 0 und 25. Um diese werden beim Verschlüsseln alle Klartextzahlen erhöht, beim Entschlüsseln alle Zahlen des Kryptogramms wieder verringert.

- *Schlüsselraum:* $\mathcal{K}_E = \mathcal{K}_D = \{0, \ldots, 25\}$

  Verschlüsselung $E : T \mapsto (T + k \mod 26)$

  Entschlüsselung $D : C \mapsto (C - k \mod 26)$

  (Anschließend werden die Zahlen 1 bis 26 wieder zu Buchstaben dekodiert.)

- *Sehr leicht zu knacken:*
  - *viel zu wenige mögliche Schlüssel $\rightsquigarrow$ durch brute-force Attacke knackbar: Einfach alle 26 Schlüssel ausprobieren, bis sinnvoll erscheinender Klartext gefunden wurde.*
  - *Durch Verwendung der gleichen Abbildung von Klartextbuchstabe zu Chiffrebuchstabe für gesamten Text ist das Verfahren außerdem durch* statistische Analyse *sehr leicht knackbar: Die häufigsten Buchstaben in Chiffre sind mit recht großer Wahrscheinlichkeit auch häufigste Buchstaben in der Klartextsprache, im Deutschen also ’e’ und ’n’. Nutzt man diese Tatsache aus und probiert zunächst die vielversprechenden Schlüssel (die häufige Klartextbuchstaben auch auf häufige Chiffre-Buchstaben abbilden), findet man den richtigen Schlüssel oft noch viel schneller.*

(b) Verbesserung: Vigenère-Code

- *Idee: Verwende verschiedene Schlüssel, in Abhängigkeit von der Position der Zeichen in Klartext/Chiffre.*

$\rightsquigarrow$ *Abbildung Klartextbuchstabe zu Chiffrebuchstabe ist nicht mehr für gesamten Text fest.*

$\rightsquigarrow$ *Statistische Analyse wird deutlich schwerer.*

- *Verwende „Schlüsselworte" der Länge m: $\mathcal{K}_E = \mathcal{K}_D = \{0, \ldots, 25\}^m$*

  1. Zahl des Schlüsselwortes für 1., m+1., 2m+1., ... Buchstaben des Klartextes 2. Zahl des Schlüsselwortes für 2., m+2., 2m+2., ... Buchstaben des Klartextes ...

- *Wenn Schlüsselwort zu kurz im Vergleich zu Nachricht, trotzdem mit statistischer Analyse knackbar.*

(c) Unknackbare One-Time-Pads:

- *Wähle* zufälliges *„Schlüsselwort" $e = d \in \{0,1\}^m$ für Nachricht $T \in \{0,1\}^m$.*
- *$E : T_i \mapsto (T_i \text{ xor } e_i)$ für alle $i = 1, \ldots, m$*

  $D : C_i \mapsto (C_i \text{ xor } e_i)$ für alle $i = 1, \ldots, m$

  $\Rightarrow D(E(T, e), e) = T$
- *Entscheidend dafür, dass Kryptosystem unknackbar wird:*
  - *Schlüssel e muss wirklich an allen Positionen des Klartextes zufällig sein*

    $\rightsquigarrow$ Chiffre sieht statistisch absolut zufällig aus.
  - *Schlüssel darf nicht wiederverwendet werden.*

    Man muss für jede Nachricht einen neuen Schlüssel verwenden. (One-Time-Pad)
- *Verwendung bei allerhöchsten Sicherheitsanforderungen (u.A. Militär)*
- *Problem:*
  - *Schlüsselaustausch (im Voraus) ist extrem aufwendig.*
- *Schwächere Alternative:*
  - *Erzeugung möglichst guter Folge von Pseudozufallszahlen aus wenigen Startparametern sowohl bei Sender und Empfänger.*

    $\rightsquigarrow$ Beide können gleiche Folge scheinbar zufälliger Zahlen aus wenigen Startparametern unabhängig voneinander zum Ver- bzw. Entschlüsseln als Ersatz für One-Time-Pad erzeugen.
  - *Sicherheit steht und fällt hier mit Qualität des Zufallszahlengenerator.*

    (So hat Enigma funktioniert.)

(d) Variante „visuelle Verschlüsselung":

- *Klartext ist s/w-Bild mit $m \times m$ Pixeln.*
- *Schlüssel ist Bild mit $2m \times 2m$ Pixeln, gruppiert in 2×2 Quadrate.*

  In jedem Quadrat sind genau 2 zufällige Pixel schwarz und 2 weiß.

  Das Schlüsselbild erscheint also wie „zufälliges graues Rauschen".
- *Teile jedes Pixel eines Klartextbildes in 2×2 Unterpixel, so dass $2m \times 2m$ Klartextbild entsteht.*
- *Verschlüsselung: Überlagere Klartextbild und Schlüsselbild mit „xor":*

- *Ist 2×2 Quadrat weiß, färbe die beiden schwarzen Pixel des Schlüsselbildes schwarz.*
- *Ist 2×2 Quadrat schwarz, färbe die anderen beiden Pixel schwarz.*

Das Kryptogramm-Bild erscheint dann auch wie „zufälliges graues Rauschen".

- *Enschlüsselung: Überlagere Kryptogrammbild und Schlüsselbild mit „xor".*

Problem symmetrischer Kryptosysteme:

- Gemeinsame Schlüssel müssen vor Kommunikation ausgetauscht werden.
- Schlüsselverwaltung ist zu aufwendig.

  Alle Paare von Kommunikationspartnern müssen individuellen, geheimen Schlüssel für ihre jeweilige Kommunikation austauschen.

  Wollen n Parteien alle miteinander kommunizieren können, so muss jede Partei $n-1$ viele verschieden Schlüssel (einen je Partner) verwalten.

Public-Key-Kryptographie – RSA

Frage (Diffie und Hellmann): (Wie) kann man eine geheime Nachricht an jemanden schicken, mit dem man keinen gemeinsamen geheimen Schlüssel hat?

Idee: Asymmetrisches Kryptosystem mit sog. Einweg- oder Trapdoor-Funktionen, bei dem **verschiedene Schlüssel zum Ver- bzw. Entschlüsseln** genutzt werden.

- Empfänger (= einzig legaler Entschlüsseler)
  - stellt **öffentlichen Schlüssel** $e \in \mathcal{K}_E$ **zur Verschlüsselung** aller an ihn gerichteten Nachrichten öffentlich bereit,
  - behält **privaten Schlüssel** $d \in \mathcal{K}_D$ **zur Entschlüsselung** aller an ihn gerichteten Nachrichten geheim.
- Anforderungen:
  - Entschlüsselung soll beim Empfänger möglich sein:

    $$D(E(T, e), d) = T$$

  - Entschlüsselung soll bei Angreifern nicht möglich sein:

    Aus dem öffentlichen Schlüssel e, einer Klartextnachricht T oder einem abgefangenen oder selbst erzeugten Kryptogramm $E(T, e)$ (oder allem davon) kann man d oder $D(E(T, e), d)$ praktisch nicht berechnen. Der Aufwand zur Berechnung von d aus diesen Informationen muss so groß sein, dass d nicht so schnell bestimmt werden kann, dass der Angreifer noch Nutzen aus der Berechnung und dem Knacken der Nachrichten ziehen kann (z.B. weil die Information dann bereits veraltet ist).
  - Effizienz:

    $E(T, e)$ und $D(C, d)$ sollen im Gegensatz dazu möglichst leicht berechenbar sein, damit die legale Ver- und Entschlüsselung schnell durchgeführt werden kann.

- Solche Kryptosysteme nennt man Public-Key-Kryptosysteme.

Das bekannteste Public-Key-System basiert auf dem Satz von Euler:

Algorithmus 2.1.4 (RSA-Verschlüsselung (Rivest, Shamir, Adleman))

- **Initialisierung** (Einmalig, für alle künftigen Nachrichten an Empfänger)
  - Empfänger wählt zwei *zufällige, große* ($> 100^{300}$) Primzahlen $p \neq q$.
  - Empfänger berechnet

$$N = pq$$
$$\varphi = \varphi(N) = (p-1)(q-1)$$

  - Empfänger wählt zufälliges $e > 1$ mit $ggT(e, \varphi) = 1$.
  - Empfänger berechnet d mit $ed \equiv 1 \mod \varphi$. (erw. Eukl. Alg.)

    Öffentlicher Schlüssel (für Verschlüsselung): (N, e)

    Privater Schlüssel (für Entschlüsselung): (d, p, q, φ)

- **Verschlüsselung** (beim Sender, je Nachricht an Empfänger)
  - Codiere Nachricht T als Zahl $x \in (\mathbb{Z}/N\mathbb{Z})$.
    (Falls T zu groß, als Folge von Zahlen.)
  - Berechne und sende Kryptogramm $E(x, e) = y = (x^e \mod N)$.

- **Entschlüsselung** (beim Empfänger, je Nachricht)
  - Für empfangenes $y = E(x, e)$ berechne $x' = (y^d \mod N)$.
  - Decodiere Zahl x' wieder zu $T' = D(E(T, e), d)$.

Satz 2.1.5 *Für alle $x \in \mathbb{Z}/N\mathbb{Z}$ und x' wie in Algorithmus 2.1.4 berechnet gilt $x' = x$. (Also auch $T = T'$.)*

Beweis. Nach Wahl von e und d gibt es $k \in \mathbb{Z}$ mit $ed = k\varphi + 1$.
Nach Satz von Fermat/Euler gilt somit

$$x' \equiv y^d \equiv (x^e)^d = x^{ed} = x^{k\varphi+1} = (x^\varphi)^k \cdot x \equiv 1^k \cdot x \equiv x \mod N.$$

Analyse der Sicherheit

- Jeder Angreifer kennt e und N.
  d, p, q und φ kennt er nicht.
- Berechnung von d aus e, N:
  Angreifer muss $[e]$ in $\mathbb{Z}/\varphi\mathbb{Z}$ invertieren. Das geht nicht, ohne φ zu kennen.

- Berechnung von φ aus N:

  Wegen $\varphi = (p-1)(q-1)$ ist die Berechnung von φ aus N äquivalent dazu, N in $N = pq$ zu faktorisieren:

Satz 2.1.6 *Sei $N = pq$ mit p, q prim. Die Berechnung von $\varphi(N)$ ist genau so schwer wie die Faktorisierung von N.*

Beweis. Aus der Faktorisierung $N = pq$ erhält man sofort $\varphi(N) = (p-1)(q-1)$.

Für bekannte N und $\varphi(N)$ erhält man aus den Gleichungen

$$\begin{aligned} \varphi(N) &= (p-1)(q-1) \\ N &= pq \end{aligned}$$

leicht p und q. □

Bemerkung Die Sicherheit von RSA basiert auf der Hypothese, dass es keinen praktisch ausreichend schnellen Algorithmus zur Faktorisierung großer Primzahlprodukte gibt.

(Es ist aber mathematisch bisher nicht bewiesen, dass das nicht doch geht!!!)

Mit dem der RSA-Verschlüsselung zugrunde liegenden Prinzip kann man auch Nachrichten signieren, da die Reihenfolge der Anwendung von öffentlichem und privaten Schlüssel für die Entschlüsselungseigenschaft keine Rolle spielt, aber nur der Sender einer Nachricht nur dann in der Lage ist, diese auch mit dem privaten Schlüssel des angeblichen Senders zu verschlüsseln, wenn er tatsächlich im Besitz dieses privaten Schlüssels ist.

Algorithmus 2.1.7 (RSA Signierungsverfahren)

- **Initialisierung**
  - *Sender* erzeugt Schlüsselpaar wie oben.
- **Sender**
  - Berechne Signatur $y_s = x^d$ aus Nachricht x und privatem Schlüssel d des Senders.
  - Sende y_s gemeinsam mit Nachricht x ab.
- **Empfänger**
  - Erhält Nachricht x zusammen mit Signatur y_s.
  - Berechne Nachricht $x' = y_s^e$ aus Signatur und öffentlichem Schlüssel e des Senders.
  - Ist $x' = x$, so ist Nachricht tatsächlich vom Sender.

    (Denn niemand außer Besitzer von d kann y_s passend berechnen.)

2.2. Kanalcodierung und Fehlererkennung

Literaturempfehlung:

- Kapitel 6 in A. Beutelspacher, M.A. Zschiegner: Diskrete Mathematik für Einsteiger
- Kapitel 13 in M. Aigner: Diskrete Mathematik
- Kapitel 5.4.4 in A. Steger: Diskrete Strukturen.
- Kapitel 3.2.1 in G. Teschl, S. Teschl: Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra.

Situation:

- Nachrichten werden über einen Kanal schickt (oder in einem Medium gespeichert), der sie evtl. verfälscht.

Ziel:

- Erkennung und Korrektur von (wichtigsten Typen von) Fehlern.

Grundidee:

- **Füge** bei der Datenübertragung/-speicherung so viele von den eigentlichen „Nutzdaten“ abhängige **redundante Daten** (Kopien, Prüfsummen, ...) **hinzu**, dass ein Kanalfehler nicht alle Nutz- und redundanten Daten auf konsistente Weise verändern kann.

  $\rightsquigarrow$ Fehler können erkannt (und ggf. sogar korrigiert) werden.

Beispiel 2.2.1

(a) Paritätscode:

Füge zu Bitvektor $x = (x_1, \ldots, x_s)$ *Paritätsbit* $x_{s+1} \equiv \sum_{i=0}^{s} x_i \mod 2$ *hinzu.*

Sende Codewort $c = c(x) = (x_1, \ldots, x_s, x_{s+1})$.

Für jedes so konstruierte Codewort c *gilt* $\sum_{i=1}^{s+1} c_i \equiv 0 \mod 2$.

Verändert ein Fehler (nur) ein Bit, so erhält man Wort $\tilde{c}$ *mit* $\sum_{i=1}^{s+1} \tilde{c}_i \equiv 1 \mod 2$.

$\rightsquigarrow$ *Einzelfehler wird erkannt. (Kann aber nicht korrigiert werden, da Fehlerstelle unklar bleibt.)*

(b) ISBN-10-Code: Funktioniert ähnlich

Nutzdaten: Neun Ziffern $z_1, \ldots, z_9$ *zwischen* 0 *und* 9.

Füge Prüfziffer z_{10} *zwischen* 0 *und* $X = 11$ *hinzu, so dass* $z_{10} \equiv \sum_{i=1}^{9} i \cdot c_i \mod 11$

$\rightsquigarrow$ *Einzelfehler und Vertauschungen benachbarter Ziffern werden erkannt.*

(c) Triple-Rep-Code:

Nutzdaten: Einzelnes Bit x (Geht analog für Bitvektoren.)

Sende Codewort $c = (x, x, x)$.

Jedes so konstruierte Codewort c erfüllt $\sum_{i=1}^{2} c_i \equiv 0 \mod 3$.

Ändert ein Fehler ein oder zwei Bits, erhält man $\tilde{c} = (\tilde{x}, \tilde{y}, \tilde{z})$ mit $\tilde{x} + \tilde{y} + \tilde{z} \not\equiv 0 \mod 3$.

$\rightsquigarrow$ *Einzel- und Doppelfehler werden erkannt.*

Mit der Entschlüsselung/Kontrollfunktion

$$x = \begin{cases} 0 & \text{falls } \tilde{x} + \tilde{y} + \tilde{z} \in \{0, 1\} \\ 1 & \text{falls } \tilde{x} + \tilde{y} + \tilde{z} \in \{2, 3\} \end{cases}$$

kann man Einzelfehler sogar korrigieren!

Wir beschränken uns im Folgenden auf (blockweise) Kanalcodierung von Bitvektoren:

- „Nutzinformation“: Vektoren (Blöcke) $(x_1, \ldots, x_s) \in \mathbb{F}_2^s$ aus s Bits.
- Über fehleranfälligen Kanal übertragen werden Vektoren (Blöcke) $(y_1, \ldots, y_k) \in \mathbb{F}_2^k$ aus $k = s + t$ Bits.

  Viele einfache Verfahren fügen dazu einfach t aus $(x_1, \ldots, x_s)$ berechnete „Kontrollbits“ $(x_{s+1}, \ldots, x_{s+t}) = f(x_1, \ldots, x_s)$ hinzu, so dass $y = (x, f(x))$.

Sowohl für die Nutzinformation x als auch für die übertragene Daten y sind dabei nur bestimmte Teilmengen von $\mathbb{F}_2^s$ bzw. $\mathbb{F}_2^k$ zulässig.

Definition 2.2.2

(i) Ein **binärer Blockcode** der Länge $k \in \mathbb{N}$ ist eine Teilmenge $\mathcal{C} \subseteq \mathbb{F}_2^k$.

Die Vektoren $x \in \mathcal{C}$ sind die (legalen) **Codeworte** des Codes.

(ii) Seien $\mathcal{B} \subseteq \mathbb{F}_2^s$ und $\mathcal{C} \subseteq \mathbb{F}_2^k$ binäre Blockcodes.

Eine Bijektion $K : \mathcal{B} \to \mathcal{C}$ heißt **Kanalcodierung**.

Bemerkung

(i) Analogie:

- $\mathcal{C}$ ist Wörterbuch aller legalen/echten Worte
- $x \in \mathcal{C}$ ist legales und korrektes Wort
- $x \notin \mathcal{C}$ ist ein fehlerhaftes Wort (oder einfach nur unverständlicher Quatsch)

(ii) Robustheit der Kanalcodierung K entspricht Fehlertoleranz des Codes $\mathcal{C}$.

$\mathcal{B}$ ist nur Quellencodierung. (Kann man auch als „Datenformat“ der Nutzdaten interpretieren.)

Ein wichtiges Maß für die Robustheit von Codes ist die Anzahl tolerierbarer Einzelfehler:

Definition 2.2.3 Für $k \in \mathbb{N}$ heißt $\triangle : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{N}_0$ mit

$$\triangle(x, y) = |\{i \mid x_i \neq y_i\}| \quad (= \|x - y\|_1)$$

die **Hamming-Distanz** (auch Manhattan-Distanz) von x und y.

Bemerkung 2.2.4 Die Hamming-Distanz ist eine Metrik. Für alle $x, y, z \in \mathbb{F}_2^k$ gilt

(i) $\triangle(x, y) \geq 0$ und $\triangle(x, y) = 0$ gdw. $x = y$

(ii) $\triangle(x, y) = \triangle(y, x)$

(iii) $\triangle(x, z) \leq \triangle(x, y) + \triangle(y, z)$

Situation: Wir übertragen (oder speichern) die kodierte Information nun über einen fehleranfälligen Kanal (oder in einem fehleranfälligen Speicher), der die Daten möglicherweise verändert.

$$\underbrace{x \in \mathcal{C}}_{\text{legales Wort}} \subseteq \mathbb{F}_2^k \xrightarrow{\text{fehlerhafter Kanal } g} \underbrace{y \in g(x) \subseteq \mathbb{F}_2^k}_{y=x?}$$

$g(x) \subseteq \mathbb{F}_2^k$: Menge aller möglichen Bitvektoren, die aus x durch die betrachteten Fehler entstehen könnten.

Beobachtung 2.2.5

- *Man kann einen Fehler erkennen, wenn er nicht auf ein (anderes) legales Codewort führt:*

  Falls $y \notin \mathcal{C}$, so muss $x \neq y$ gelten.
- *Man kann einen Fehler korrigieren, wenn nicht auch ein anderes legales Codewort bei der Übertragung zum gleichen (verfälschten) Bitvektor führen kann:*

  Falls $y \notin g(\tilde{x})$ für alle $\tilde{x} \in \mathcal{C} \setminus \{x\}$, so muss $y \in g(x)$ gelten.

Definition 2.2.6 Für $x \in \mathbb{F}_2^k$ und $f \in \mathbb{N}_0$ heißt

$$B_f(x) := \{y \in \mathbb{F}_2^k \mid \triangle(x, y) \leq f\}$$

die **Kugel um x mit Radius f**.

Sei $\mathcal{C} \subseteq \mathbb{F}_2^k$ ein Code.

(i) $\mathcal{C}$ heißt **f-fehlerentdeckend** wenn $B_f(x) \cap \mathcal{C} = \{x\}$ für alle $x \in \mathcal{C}$

(ii) $\mathcal{C}$ heißt **f-fehlerkorrigierend** wenn $B_f(x) \cap B_f(y) = \emptyset$ für alle $x, y \in \mathcal{C}$ mit $x \neq y$.

Beobachtung 2.2.7

(i) $\Leftrightarrow \triangle(x, y) \geq f + 1$ *für alle* $x, y \in \mathcal{C}$ *mit* $x \neq y$.

(ii) $\Leftrightarrow \triangle(x, y) \geq 2f + 1$ *für alle* $x, y \in \mathcal{C}$ *mit* $x \neq y$.

Beispiel 2.2.8

(a) Paritätscode: $\mathcal{C} := \{(x_1, \ldots, x_s, x_{s+1}) \in \mathbb{F}_2^{s+1} \mid \sum_{i=1}^{s+1} x_i \equiv 0 \mod 2\}$

$\Rightarrow \triangle(x, y) \geq 2$ *für alle* $x, y \in \mathcal{C}$ *mit* $x \neq y$

$\Rightarrow \mathcal{C}$ *ist 1-fehlerentdeckend und 0-fehlerkorrigierend*

(b) Triple-Rep-Code: $\mathcal{C} := \{(x, y, z) \in \mathbb{F}_2^{3s} \mid x = y = z \in \mathbb{F}_2^s\}$

$\Rightarrow \triangle(x, y) \geq 3$ *für alle* $x, y \in \mathcal{C}$ *mit* $x \neq y$

$\Rightarrow \mathcal{C}$ *ist 2-fehlerentdeckend und 1-fehlerkorrigierend*

Frage: Wie viel Overhead braucht man für eine gewünschte Robustheit?

Oder genauer: Wie viel Nutzinformation kann man in einem f-fehlerentdeckenden oder f-fehlerkorrigierenden Code der Länge k maximal unterbringen? (=**Informationsrate**)

Definition 2.2.9 Für einen Code $\mathcal{C} \subseteq \mathbb{F}_2^k$ sei

$$d(\mathcal{C}) := \min\{\triangle(x, y) \mid x, y \in \mathcal{C},\ x \neq y\} \ . \quad \text{(min Abstand zwischen Codeworten)}$$

Für $d, k \in \mathbb{N}_0$ sei

$$M(k, d) := \max\{|\mathcal{C}| \mid \mathcal{C} \subseteq \mathbb{F}_2^k \mid d(\mathcal{C}) \geq d\} \ . \quad \text{(max \#Codeworte bei Minimalabstand } d\text{)}$$

Satz 2.2.10 (Hamming-Schranke) *Sei* $d = 2t + 1$ *für* $t \in \mathbb{N}_0$. *Dann gilt*

$$M(k, d) \leq \frac{1}{\sum_{i=0}^{t} \binom{k}{i}} 2^k \ .$$

Beweis.

- Sei $\mathcal{C} \subseteq \mathbb{F}_2^k$ mit $d(\mathcal{C}) \geq 2t+1$.
- Dann gilt $B_t(x) \cap B_t(y) = \emptyset$ für alle $x, y \in \mathcal{C}$ mit $x \neq y$.
- Größe von $B_t(x)$:
  Für $x \in \mathcal{C}$ und $i \in \{0, \ldots, t\}$ viele Fehler: Genau $\binom{k}{i}$ Möglichkeiten, i Fehler auf k Bits zu verteilen.
  $\Rightarrow \quad |B_t(x)| = \sum_{i=0}^{t} \binom{k}{i}$
- $|\mathcal{C}| \cdot \sum_{i=0}^{t} \binom{k}{i} = \dot{\bigcup_{x \in \mathcal{C}}} |B_t(x)| \leq |\mathbb{F}_2^k| = 2^k$ □

Praxis: Lineare Codes (Vektoren x, c im Folgenden immer als Zeilenvektoren)

- Kontrollbits werden durch lineare Funktion (über Körper $\mathbb{F}_2$) gebildet:

$$(x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+t}) := (x_1, \ldots, x_s) \cdot G \quad \text{mit} \quad G = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & P \\ 0 & & 1 & \end{array}\right) \in \mathbb{F}_2^{s,s+t}$$

  (Aus Nutzinformation $x \in \mathbb{F}_2^s$ wird $c(x) = xG \in \mathbb{F}_2^{s+t}$.)
  G heißt **Generatormatrix** des Codes.
  Formal: Code $\mathcal{C}$ ist Zeilenraum von G.
- **Kontrollmatrix** des Codes ist

$$H = \left(\begin{array}{c|ccc} & 1 & & 0 \\ P^T & & \ddots & \\ & 0 & & 1 \end{array}\right) \in \mathbb{F}_2^{t,s+t}.$$

  Es gilt $HG^T = 0$. Insbesondere: $Hc^T = 0$
- Decodierung von (evtl. verfälschtem) $\tilde{c} \in \mathbb{F}_2^{s+t}$:
  - Berechne **Syndrom** $H\tilde{c}^T$.
  - Falls $H\tilde{c}^T = 0$: (Kein Fehler erkannt.)
    Decodiere Codewort $\tilde{c} = c(x) = (x_1, \ldots, x_{s+t}) \to x = (x_1, \ldots, x_s)$
  - Falls $H\tilde{c}^T \neq 0$: (Fehler. Decodierte das nächstgelegene Codewort)
    Finde Vektor e mit minimaler Anzahl Einsen und $He^T = H\tilde{c}$.
    Nächstgelegenes Codewort ist dann $\tilde{c} + e$.
    Annahme $\tilde{c} + e = c(x)$. Dekodierte $\tilde{c} + e = c(x) = (x_1, \ldots, x_{s+t}) \to x = (x_1, \ldots, x_s)$

Beispiel 2.2.11 ((7, 4)-Hammincode ($s = 4$, $t = 3$))

- *Erzeugenden-Matrix und Kontroll-Matrix:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{4,7} \qquad H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

- *Codeworte: Linearkombinationen (über Körper $\mathbb{F}_2$) der Zeilen von G.*
  Hamming-Distanz zwischen Codeworten ≥ 3
- *Codierung:* $x = (1,1,1,0) \longrightarrow c(x) = xG = (\underbrace{1,1,1,0}_{x}, \underbrace{0,0,0}_{Kontrollbits})$
- *Empfange verfälschtes* $\tilde{c} = (1,1,0,0,\ 0,0,0)$. *(Genau ein Fehler.)*
  Syndrom $H\tilde{c}^T = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} (1,1,0,0,\ 0,0,0)^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, *also Fehler.*
  Für $e = (0,0,1,0,0,0,0)$ *ist* $He^T = H\tilde{c}^T$. *(Nur eine Eins nötig, da nur ein Fehler in* $\tilde{c}$*!)*
  Das nächstgelegene Codewort ist also $\tilde{c} + e = (1,1,1,0,\ 0,0,0) = c(x)$.
  Decodiere $c(x)$ *wieder zu* $x = (1,1,1,0)$.

3. Graphentheorie

Literatur:

- Kapitel 2 in A. Steger: Diskrete Strukturen.
- Kapitel 8 in A. Beutelspacher, M.A. Zschiegner: Diskrete Mathematik für Einsteiger.
- Kapitel 6–8 in M. Aigner: Diskrete Mathematik.
- Kapitel 15–17 in G. Teschl, S. Teschl: Mathematik für Informatiker, Band 1: Diskrete Mathematik und Lineare Algebra.
- sehr viele weitere Lehrbücher „Graphentheorie“

3.1. Grundbegriffe

Graphen werden verwendet, um reale Netze, wie z.B. Straßen oder Computernetze, oder abstrakte Netzwerke aus Objekten und deren Beziehungen untereinander, wie z.B. Datentypen und Interfaces sowie deren Ableitungshierarchien und möglichen Umwandlungen zu beschreiben. Je nach Anwendungsfall stehen dabei strukturelle Fragen, wie zum Beispiel ob und wie stark ein Netz zusammenhängend ist, oder Optimierungsfragen, wie zum Beispiel die Suche nach einem kürzesten Weg in einem Netz, im Fokus. In diesem Kapitel geben wir einen (kleinen) Einblick in dieses Gebiet.

Im Folgenden bezeichnen wir mit $\binom{V}{2}$ oder $\mathcal{P}_2(V)$ die Menge aller ungeordneten Paare $\{u, v\}$ mit $u, v \in V$ und $u \neq v$, d.h.

$$\binom{V}{2} := \mathcal{P}_2(V) = \{\{u, v\} \mid u, v \in V,\ u \neq v\}\,.$$

(Das ist genau die Menge aller zweielementigen Teilmengen von V.)

Definition 3.1.1 Ein (einfacher, endlicher, ungerichteter) **Graph** ist ein Paar $G = (V, E)$ aus einer endlichen **Knotenmenge** V und einer **Kantenmenge** $E \subseteq \binom{V}{2}$.

Begriffe und Notation:

- $v \in V$ heißt **Ecke** oder **Knoten** (vertex, node).
- $e = \{u, v\} \in E$ heißt **Kante** (edge).

  Schreibweisen: $e = \{u, v\}$ oder $e = uv$
- Jede Kante $e = uv \in E$ hat zwei **Endknoten** u, v.

  Die Kante $e = uv$ **verbindet** u und v.

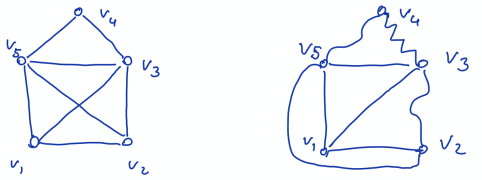
  Ein Knoten u heißt **inzident** zur Kante e, wenn u einer der Endknoten von e ist, also $e = uv$.

  Zwei Knoten u, v heißen **adjazent**, wenn $e = uv \in E$.
- Anzahl der Knoten: $|G| = |V(G)| = |V|$.
- Anzahl der Kanten: $\|G\| = |E(G)| = |E|$.

Bemerkung

- Typische Visualisierung von Graphen in der Ebene:
  - Knoten $v \in V \rightsquigarrow$ (paarweise verschiedene) Punkte
  - Kanten $uv \in E \rightsquigarrow$ Strecken (oder allgemeiner Jordan-Kurven) zwischen den zugehörigen Punkten u und v

    (Diese Darstellung ist nicht eindeutig. Das Finden einer Darstellung mit minimaler Anzahl Kreuzungen ist beweisbar schwer!)



    Beide Darstellungen zeigen den gleichen Graphen.

- Die in Definition 3.1.1 nur in Klammern genannten Eigenschaften bedeuten:
  - **endlich:** Die Knotenmenge (und damit auch die Kantenmenge) ist endlich, d.h. $|V| < \infty$.
  - **ungerichtet:** Die Kanten sind ungeordnete Paare $\{u, v\}$ von Knoten $u, v \in V$, d.h. uv und vu sind die gleiche Kante $e = uv$, die man sich als ungerichtete Verbindung u–v zwischen den Knoten u und v vorstellen kann.

    Im Gegensatz dazu sind in sogenannten **gerichteten Graphen**, auch **Digraphen** genannt, die Kanten geordnete Paare (u, v) von Knoten $u, v \in V$, die man sich auch als gerichtete Verbindung $u \to v$ zwischen den Knoten u und v vorstellen kann. In einem gerichteten Graphen sind (u, v) und (v, u) verschiedene Kanten. Man nennt gerichtete Kanten dann auch **Bögen**.
  - **einfach:** Ein Graph $G = (V, E)$ heißt einfach, wenn gilt:
    - Es gibt keine Schleifen, d.h. $u \neq v$ für alle $\{u, v\} \in E$.
    - Für je zwei Knoten $u, v \in V$ existiert höchstens eine Kante $e = uv \in E$.

    Beide Eigenschaften werden in Definition 3.1.1 bereits durch $E \subseteq \binom{V}{2}$ erzwungen.

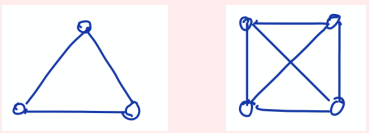
    Eine allgemeinere Definition sind sogenannte nicht-einfache Graphen, auch **Multigraphen** genannt. In Multigraphen
    - sind mehrere **parallele Kanten** $e_1, e_2, \ldots$ zwischen $u, v \in V$ möglich und
    - **Schleifen** $e = uu$ mit $u \in V$ möglich.

    In der Definition eines Multigraphen muss die Einschränkung $E \subseteq \binom{V}{2}$ aufgegeben und dafür eine zusätzliche Inzidenzabbildung $\text{inz} : E \to \binom{V}{2}$ eingeführt werden, um verschiedene parallele Kanten in E sowohl unterscheiden zu können als auch die Endknoten korrekt zu den Kanten zuordnen zu können.

Wir werden im Folgenden ausschließlich Graphen betrachten, die entsprechend der obigen Begriffsdefinition 3.1.1 einfach, endlich und ungerichtet sind. Aus diesem Grund werden wir diese Attribute im Weiteren immer weglassen. Beachten Sie, dass sich viele der folgenden Resultate *nicht* problemlos auf Multigraphen, unendliche Graphen oder gerichtete Graphen übertragen lassen.

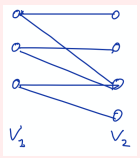
Beispiel 3.1.2 (Wichtige Graphen und Graphenklassen)

- ***Vollständiger Graph:*** $K_n = (V, E)$
  - $V = \{v_1, \ldots, v_n\}$ *und* $E = \binom{V}{2}$



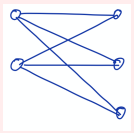
Die Graphen K_3 *und* K_4.

- ***Bipartiter Graph***
  - $V := V_1 \dot\cup V_2$ *und* $E \subseteq \{uv \mid u \in V_1,\ v \in V_2\}$



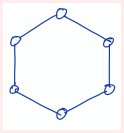
Ein bipartiter Graph mit Knoten-Partition in V_1 *und* V_2.

- ***Vollständiger bipartiter Graph:*** $K_{n,k} = (V, E)$
  - $V = (V_1 \dot\cup V_2)$ *und* $E = \{uv \mid u \in V_1,\ v \in V_2\}$ *mit* $|V_1| = n$ *und* $|V_2| = k$



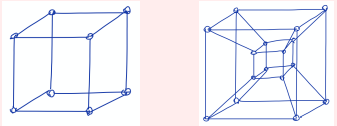
Der vollständige bipartite Graph $K_{2,3}$.

- ***Kreis auf*** n ***Knoten:*** $C_n = (V, E)$
  - $V = \{v_1, \ldots, v_n\}$ *und* $E = \{v_1v_2,\ v_2v_3, \ldots, v_{n-1}v_n,\ v_nv_1\}$



Der Kreis C_6.

- d***-Hyperwürfel:*** $Q_d = (V, E)$
  - *Gittergraph des* d*-dimensionalen Hyperwürfels, d.h.*
    $V = \{0,1\}^d$ *und* $uv \in E \Leftrightarrow \triangle(u, v) = 1$



Die Graphen Q_3 *und* Q_4.

Nachbarn und Knotengrade

Definition 3.1.3 Für einen Graphen $G = (V, E)$ und $v \in V$ heißen

- $\delta(v) := \{\{v, w\} \mid \{v, w\} \in E\} = \{e \in E \mid |e \cap \{v\}| = 1\}$ der **von v induzierte Schnitt** (oder der Schnitt um v),
- $N(v) := \Gamma(v) := \{w \in V \mid \{v, w\} \in \delta(v)\}$ die **Nachbarschaft von v** und
- $\deg(v) := |\delta(v)|$ der **Grad von v**.

Bemerkung: Der von v induzierte *Schnitt ist die Menge der Kanten*, die zum Knoten v inzident sind, die *Nachbarschaft von v ist die Menge der Knoten*, die adjazent zu v sind, und der *Grad von v ist die Anzahl* der zu v inzidenten Kanten.

Beobachtung 3.1.4 *In jedem Graphen $G = (V, E)$ gilt* $\sum_{v \in V} deg(v) = 2 \cdot |E|$.

Beweis. In der Graphentheorie gibt es einige elementare Beweistechniken, die sehr vielseitig einsetzbar und – in angepasster Form – für verschiedenen Herleitungen und Beweise nützlich sind. Eine dieser Standardtechniken ist das sogenannte *doppelte Abzählen*, bei dem eine bestimmte Menge auf verschiedene Weise gezählt wird.

In diesem Beweis zählen wir die Anzahl k der Knoten-Kanten-Inzidenzen (also der „Enden von Kanten“).

- Zählung über die Kanten:

  Jede Kante hat genau zwei Enden, also gilt $k = 2 \cdot |E|$.

- Zählung über die Knoten:

  An Knoten v sind genau $\deg(v)$ Kanten inzidenz (anliegende Kantenenden), also gilt $k = \sum_{v \in V} \deg(v)$

Damit folgt $\sum_{v \in V} \deg(v) = k = 2|E|$ □

Folgerung 3.1.5 *In jedem Graphen ist die Anzahl der Knoten mit ungeradem Grad gerade.*

Beweis. In diesem Satz verwenden wir das gerade gezeigt Resultat, dass die Summe aller Knotengrade gerade ist, zusammen mit einem einfachen Paritätsargument: Eine Summe von zwei ungeraden Zahlen ist genau dann gerade, wenn die Summe eine gerade Anzahl von Summanden enthält. Auch dies ist ein *Standatdargument* in der Graphentheorie.

- Setze $U := \{v \in V \mid \deg(u) \text{ ungerade}\}$ und $W := V \setminus U$.

- Offenbar ist dann $V = U \mathbin{\mathring{\cup}} W$ und somit
$$2|E| = \sum_{v \in V} \deg(v) = \sum_{v \in U} \deg(v) + \sum_{v \in W} \deg(v) \ .$$
Dies ist äquivalent zu
$$\sum_{v \in U} \underbrace{\deg(v)}_{ungerade} = \underbrace{2|E|}_{gerade} - \sum_{v \in W} \underbrace{\deg(v)}_{gerade}.$$
- Da die rechte Seite gerade ist, muss $|U|$ gerade sein. □

Definition 3.1.6 Ein Graph $G = (V, E)$ heißt **k-regulär**, falls $\deg(v) = k$ für alle $v \in V$.

Beispiel 3.1.7

(a) Der vollständige Graph K_n ist $(n-1)$-regulär.

(b) Jeder Kreis C_n ist 2-regulär.

(c) Der Gittergraph Q_d des d-dimensionalen Hyperwürfels ist d-regulär.

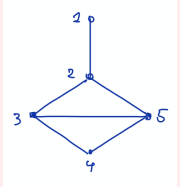
Graphenisomorphie und Teilgraphen

Graphen, die sich lediglich durch die Bezeichnung der Knoten und Kanten, jedoch nicht ihren intrinsischen Inzidenz- und Adjazenzbeziehungen untercheiden nennen wir isomorph oder äquivalent.

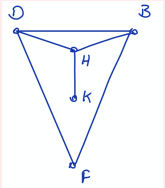
Definition 3.1.8 Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ heißen **isomorph** (oder äquivalent), wenn es eine bijektive Abbildung $\phi : V \to V'$ gibt, so dass
$$\{u, v\} \in E \quad \Leftrightarrow \quad \{\phi(u), \phi(v)\} \in E'.$$

Zwei Graphen G und G' heißen also genau dann isomorph, wenn es eine „eins-zu-eins“ zwischen den Knoten gibt, so dass auch die Kanten von G „eins-zu-eins“ auf die Kanten von G' abgebildet werden.

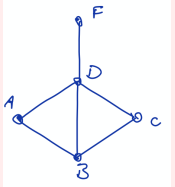
Beispiel 3.1.9



Graph G.



Graph G'.



Graph G''.

Die beiden Graphen G und G' sind isomorph. Eine Bijektion ϕ mit den in 3.1.8 geforderten Eigenschaften ist:

v	$\phi(v)$
1	K
2	H
3	B
4	F
5	D

Beachte, dass es - wie hier - auch mehrere solche Bijektionen geben kann.

Die Graphen G' und G'' sind nicht isomorph. G enthält 3 Knoten mit Grad 3, G'' nur einen Knoten mit Grad 3.

Teilmengen der Knoten und Kanten eines Graphen können sogenannte Teil- oder Untergraphen bilden.

Definition 3.1.10 Sei $G = (V, E)$ ein Graph. Für Teilmengen $V' \subseteq V$ und $E' \subseteq E$ definieren wir

$$E(V') := E \cap \binom{V'}{2} = \{uv \in E \mid u, v \in V'\}$$

$$V(E') := \{v \in V \mid v, w \in E' \text{ für ein } w \in V\}$$

Definition 3.1.11 (Teilgraph)

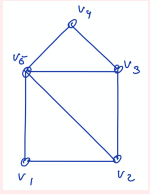
(i) Sind $G = (V, E)$ und $G' = (V', E')$ zwei Graphen mit $V' \subseteq V$ und $E' \subseteq E$, so heißt G' ein (schwacher) **Teilgraph** (oder Untergraph) von G.

(ii) Falls zusätzlich $E' = E \cap \binom{V'}{2}$ gilt, so heißt der Teilgraph G' der von V' **induzierte Teilgraph** von G.

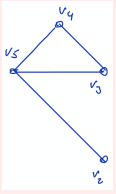
Wir schreiben dann auch $G' = G[V']$.

(iii) Ist $G' = (V', E')$ ein Teilgraph von $G = (V, E)$ und gilt $V' = V$, so heißt G' **(auf-)spannender Teilgraph** von G.

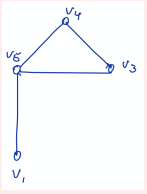
Beispiel 3.1.12 *Wir betrachten den dargestellten Graph $G = (E, V)$ und seine beiden Teilgraphen $G' = (V', E')$ und $G'' = (V'', E'')$:*



Graph G.



Graph G'.



Graph G''.

Beide Graphen G' und G'' sind offenbar (schwache) Teilgraphen von G, da $V' \subset V$, $E' \subset E$ und $V'' \subset V$, $E'' \subset E$.

Der Graph G' ist jedoch kein induzierter Teilgraph von G, auf der zu G' gehörenden Knoten-Teilmenge V' enthält G mehr Kanten als G', es gilt also $E' \subsetneq E(V')$. (Die Kante v_2v_3 fehlt in G'.)

Der Graph G'' ist ein induzierter Teilgraph von G, da er tatsächlich alle in G zwischen den Knoten in V'' verlaufenden Kanten enthält.

Wichtige elementare Konstruktionen für einen Graphen $G = (V, E)$ sind:

Löschen und Hinzufügen von Kanten oder Knoten:

- Löschen eines Knoten v und aller mit v inzidenter Kanten:
  $G - v := G[V \setminus \{v\}]$, für $v \in V$, ist der von $V \setminus \{v\}$ induzierte Teilgraph von G,
- Löschen eine Kante e
  $G - e := (V, E \setminus \{e\})$, für $e \in E$,
- Hinzufügen einer noch nicht vorhandenen Kante:
  $G + e := (V, E \cup \{e\})$, für $e \in \binom{V}{2} \setminus E$,
- Hinzufügen eines neuen Knotens:
  $G + v := (V \cup \{v\}, E)$, für $v \notin V$.

Mit diesen Operationen kann man jeden Graphen sukzessive aus dem leeren Graphen $(\emptyset, \emptyset)$ konstruieren oder ihn auf den leeren Graphen reduzieren. Sie spielen daher in vielen Induktionsbeweisen der Graphentheorie eine große Rolle.

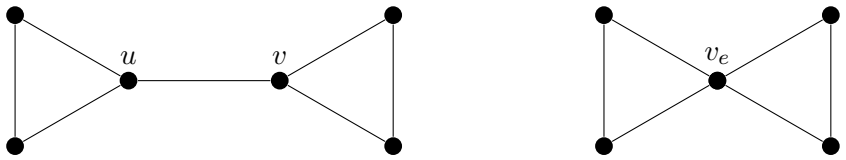
Eine weiter wichtige Operation ist die

Kontraktion von Kanten

- Für $xy = e \in E$ ist $G/e = (V \setminus \{x, y\} \cup \{v_e\}, E')$ mit

$$E' := \{f \in E \mid f \cap e = \emptyset\} \cup \{uv_e \mid ux \in E \text{ oder } uy \in E\},$$

  d. h., die Knoten x, y werden durch den Knoten v_e ersetzt, der mit allen Nachbarn von x oder y verbunden wird.



Beobachtung 3.1.13 *Wenn man aus einem gegebenen Graphen $G = (V, E)$ beliebige Kanten oder Knoten (und deren inzidente Kanten) löscht, so erhält man einen (schwachen) Teilgraphen von G.*

Um einen induzierten Teilgraphen von G zu erhalten, darf man nicht einzelne Kanten löschen, sondern nur Knoten und deren inzidente Kanten.

Graphen G', die man durch wiederholtes Löschen von Knoten oder Löschen oder Kontrahieren von Kanten aus G erhält nennt man Minoren von G (vgl. Def. 3.6.2). Mit der Minorenbildung werden wir uns später noch einmal befassen. Im Gegensatz zu den Lösch-Operationen bei der Teilgraphenbildung erlaubt es die Minorenbildung, große Graphen auf kleiner Graphen zu reduzieren, ohne dabei Zusammenhangs- und Verbindungseigenschaften zwischen nur mittelbar verbundenen Knoten durch das Löschen von Kanten „opfern“ zu müssen.

Speicherung von Graphen

Endliche, einfache Graphen lassen sich auf einfache Weise als Matrizen mit Einträgen in $\{0,1\}$ darstellen und speichern.

Definition 3.1.14 Sei $G=(V,E)$ ein Graph mit $V=\{v_1,\dots,v_n\}$, $E=\{e_1,\dots,e_m\}$.

- Die Matrix $Adj(G) := A = (a_{vw})_{v,w\in V} \in \{0,1\}^{n\times n}$ mit Einträgen

$$a_{vw} = \begin{cases} 1, & vw \in E, \\ 0, & \text{sonst} \end{cases}$$

  heißt **Adjazenzmatrix** von G.

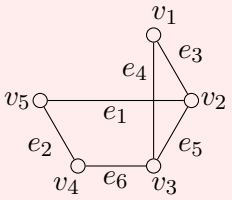
  (Offenbar gilt damit immer $Adj(G) = Adj(G)^T$, d.h. $Adj(G)$ ist symmetrisch.)

- Die Matrix $Inz(G) := B = (b_{ve})_{v\in V, e\in E} \in \{0,1\}^{n\times m}$ mit Einträgen

$$b_{ve} = \begin{cases} 1, & v \in e, \\ 0, & \text{sonst} \end{cases}$$

  heißt **(Knoten-Kanten-) Inzidenzmatrix** von G.

Beispiel 3.1.15 *Für den abgebildeten Graphen $G=(V,E)$ mit $V=(v_1,\dots,v_5)$ und $E=(e_1,\dots,e_6)$ mit $e_1=v_2v_5$, $e_2=v_4v_5$, $e_3=v_1v_2$, $e_4=v_1v_3$, $e_5=v_2v_3$, $e_6=v_3v_4$*



ist die Adjazenzmatrix

$$Adj(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

und die Inzidenzmatrix

$$Inz(G) = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Bemerkung: Wir indizieren in beiden Matrizen sowohl die Zeilen als auch die Spalten direkt mit den Knoten bzw. Kanten. Der Eintrag in der 3-ten Zeile und 4-ten Spalte der Inzidenzmatrix $Inz(G) = (b)$ im vorherigen Beispiel gehört also zum Knoten v_3 und zur Kante e_4: $b_{v_3,e_4} = 1$, da im Graphen G die Kante $e_4 = v_1v_3$ inzident zu Knoten v_3 ist. Andererseits ist $b_{v_3,e_3} = 0$, da die Kante $e_3 = v_1v_2$ nicht inzident zu Knoten v_3 ist. Das genaue Aussehen der Matrizen hängt also von der Reihenfolge der Knoten und Kanten ab, welche zuvor festgelegt werden muss.

Eine Alternative zur Darstellung endlicher Graphen als Inzidenz- oder Adjazenzmatrizen ist deren Speicherung als Inzidenz- oder Adjazenzlisten. (Datentechnisch entspricht dies im Wesentlichen der Speicherung der Inzidenz- bzw. Adjazenzmatrizen als Sparse-Matrix, wobei nur die Indizes der Nicht-Null-Einträge tatsächlich gespeichert werden müssen.)

Wie auch bei der Speicherung von Graphen $G = (V, E)$ als Matrizen wird dabei davon ausgegangen, dass die Knoten bereits als $V = \{v_1, \ldots, v_n\}$ (oder $V = \{1, \ldots, n\}$) und die Kanten bereits als $E = \{e_1, \ldots, e_m\}$ (oder $E = \{1, \ldots, m\}$) indiziert (oder nummeriert) sind. Für jeden Knoten $v \in V$ wird dann anstelle der kompletten Zeile der Adjazenz- oder Inzidenzmatrix lediglich eine verkettete Liste (oder ein Array oder Vektor entsprechender Länge) mit den Indizes der zu v adjazenten Knoten oder inzidenten Kanten gespeichert. Die Startelemente / Schlüssel-Indizes dieser Listen, also die Knoten $v \in V$, werden dabei meist in einem Array/Vektor der Länge $|V|$ gespeichert.

Beispiel 3.1.16 *Für den im vorigen Beispiel abgebildeten Graphen $G = (V, E)$ ist die Darstellung über Adjazenliste(n)*

Array der Startelemente	*jeweilige Adjazenzliste*
v_1	$\to v_2 \to v_3$
v_2	$\to v_1 \to v_3 \to v_5$
v_3	$\to v_1 \to v_2 \to v_4$
v_4	$\to v_3 \to v_5$
v_5	$\to v_2 \to v_4$

und als Inzidenzliste(n)

Array der Startelemente	*jeweilige Inzidenzliste*
v_1	$\to e_3 \to e_4$
v_2	$\to e_1 \to e_3 \to e_5$
v_3	$\to e_4 \to e_5 \to e_6$
v_4	$\to e_2 \to e_6$
v_5	$\to e_1 \to e_2$

Beide Darstellungen haben Vor- und Nachteile. Die Darstellungen als Adjazenz- bzw. Inzidenzmatrix benötigen für einen Graphen $G = (V, E)$ immer $O(|V|^2)$ bzw. $O(|V| \cdot \|E|)$ viel Speicherplatz. Dafür lassen sich Abfragen wie „Ist v zu e inzident?“ in konstanter Laufzeit $O(1)$ realisieren. Bei der Darstellung als Adjazenz- oder Inzidenzliste wird dagegen nur $O(|V| + |E|)$ viel Speicherplatz benötigt. Dafür erfordern einfache Abfragen wie „Ist v zu e inzident?“ mehr Laufzeit: Es muss jeweils die Liste oder Tabelle des Knotens v durchsucht werden, was bei einer linearen Suche einen Aufwand von $O(deg(v))$ ergäbe.

3.2. Wege, Kreise, Zusammenhang und Schnitte

Definition 3.2.1 Sei $G = (V, E)$ ein Graph.

(i) Eine Folge $P = (v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$, in der Knoten $v_0, \ldots, v_n \in V$ und Kanten $e_1, \ldots, e_n \in E$ im Wechsel vorkommen, beginnend und endend jeweils mit einem Knoten, so dass

$$e_1 = v_0v_1,\ e_2 = v_1v_2,\ \ldots,\ e_n = v_{n-1}v_n$$

gilt, heißt **Kantenzug** oder **Pfad** (genauer: $v_0 - v_n$-Pfad) (engl: **walk**).

(ii) Sind alle Knoten $v_0, v_1, \ldots, v_n$ paarweise verschieden, so heißt P ein (einfacher) v_0v_n**-Weg**. (engl: **path**)

(iii) Ist $n \geq 3$, $v_0 = v_n$ und sind die Knoten $v_0, v_1, \ldots, v_{n-1}$ paarweise verschieden, so heißt P ein (einfacher) **Kreis**.

(iv) Die Anzahl der Kanten $\ell(P) := n$ nennen wir die **(kombinatorische) Länge** von P.

Bemerkung

- **Achtung:** Die Begriffe *Pfad* und *Weg* werden in der deutschsprachigen Literatur nicht einheitlich verwendet. In der Regel werden die Begriffe wie in diesem Skript, also *Weg* für einen einfachen Weg ohne Knotenwiederholungen und *Pfad* für einen beliebigen Kantenzug, der auch Knotenwiederholungen enthalten darf, verwendet. (In A. Steger: *Diskrete Strukturen* werden die Begriffe jedoch genau mit umgekehrter Bedeutung verwendet.) Lesen Sie daher immer zunächst nach, welcher Begriff in der jeweiligen Quelle mit welcher Bedeutung verwendet wird. Unmissverständlich sind die Begriffe *Kantenzug* (immer mit erlaubten Knotenwiederholungen) und *einfacher Weg* (immer ohne Knotenwiederholungen).
- Die Attribute „einfach“ in den Begriffen Weg und Kreis lassen wir im Folgenden weg. Wege und Kreise sind nach obiger Definition immer einfach, d.h. ohne Knotenwiederholungen (bis auf den Startknoten beim Kreis) und somit auch ohne Kantenwiederholungen.
- Wir nennen auch jeden Pfad $P = (v_0)$ der Länge 0, d.h. ohne Kanten mit Start- und Endknoten v_0, einen v_0v_0-Weg.

  Ein Kreis enthält dagegen immer mindestens drei Knoten (und somit auch mindestens drei Kanten).
- Zur Vereinfachung identifiziert man den Pfad P oft nur mit der Teilfolge seinen Knoten $(v_0, \ldots, v_n)$ oder nur mit der Teilfolge seiner Kanten $(e_1, \ldots, e_n)$. Aus jeder dieser Teilfolgen kann man (in einem *einfachen* Graphen) die wechselnde Folge aller Knoten und Kanten des Pfades leicht rekonstruieren.
- Ist bei einem Weg die Wahl zwischen Start- und Endknoten (d.h. die Richtung) bzw. bei einem Kreis die Wahl des Start- und Endknotens und die Richtung des Durchlaufens des Kreises irrelevant, so kann man den Weg bzw. den Kreis sogar nur mit der entsprechenden Kanten*menge* $P = \{e_1, \ldots, e_n\}$ (also ohne der Reihenfolge, die durch eine Kanten*folge* gegeben wäre,) identifizieren.

Definition 3.2.2

(i) Ein Graph $G = (V, E)$ heißt **zusammenhängend**, wenn es für jedes Paar $s, t \in V$ einen s-t-Weg in G gibt.

(ii) Die **Zusammenhangskomponenten von** G sind die maximalen zusammenhängenden Teilgraphen von G.

(Diese sind über ihre Knotenmengen identifizierbar.)

Bemerkung

- Die Relation

$$\sim_R \subseteq V \times V \quad \text{mit } s \sim_R t :\Leftrightarrow \text{Es gibt einen } s\text{-}t\text{-Weg in } G$$

  ist Äquivalenzrelation auf V.
- Die Knotenmengen der Zusammenhangskomponenten von G sind die Äquivalenzklassen $V/\sim_R$.

Zum Nachweis, dass $\sim_R$ tatsächlich eine Äquivalenzrelation auf V definiert, ist das folgende Lemma hilfreich:

Lemma 3.2.3 *Existiert ein $s-t$-Kantenzug P (möglicherweise mit Knotenwiederholungen) in G, so existiert auch ein $s-t$-Weg P' in G.*

Beweis. Übung. □

Definition 3.2.4 Sei $G = (V, E)$ ein Graph.

(i) Ein Knoten $v \in V$ heißt **Artikulationsknoten** von G, falls $G - v$ mehr Zusammenhangskomponenten als G hat.

(ii) Eine Kante $e \in E$ heißt **Brücke** von G, falls $G - e$ mehr Zusammenhangskomponenten als G hat.

Die Artikulationsknoten und die Brücken sind also die kritischen Knoten und Kanten hinsichtlich der Zusammenhangsbeziehungen in einem Graphen: Entfernt man einen Artikulationsknoten oder eine Brücke, so zerfallen einige der Zusammenhangskomponenten von G in kleinere Zusammenhangskomponenten: Einige Knoten, die in G noch über Wege verbunden waren, sind anschließend nicht mehr über Wege verbunden.

Lemma 3.2.5 *Ein Graph $G = (V, E)$ hat mindestens $|V| - |E|$ viele Zusammenhangskomponenten.*

Beweis. Eine weitere wichtige Beweistechnik in der Graphentheorie ist die Induktion, häufig über die Anzahl der Knoten oder über die Anzahl der Kanten der Graphen geführt.

Hier führen wir einen Induktionsbeweis über die Anzahl $m = |E|$ der Kanten des Graphen.

- IAnf $m = 0$:

  D.h. G hat keine Kanten, also ist jeder Knoten eine eigene Zush.-komp.

  Also $|V| - |E|$ viele Zush.-komp.
- ISchritt $m \to m + 1$:

  Sei $G = (V, E)$ mit $|E| = m + 1$.

  Entferne beliebige Kante $e = uv$ aus G

  Der resultierende Teilgraph $G' := G - e$ hat nur noch m Kanten.

  Nach IVor. hat G' also mindestens $|V| - m$ Zush-komp.

  Fügt man $e = uv$ wieder zu G' hinzu, sind zwei Fälle zu unterscheiden:
  - Anzahl Zush.-komp. nimmt um 1 ab, falls u und v in verschiedenen Zush-komp. von G'
  - Anzahl Zush.-komp. bleibt gleich, falls u und v in gleicher Zush-komp. von G'

  Also hat G mindestesn $|V| - m - 1 = |V| - |E|$ Zush-komp. □

Folgerung 3.2.6 *Ist $G = (V, E)$ ein* zusammenhängender *Graph, so gilt $|E| \geq |V| - 1$.*

Beobachtung 3.2.7 *Ist $G = (V, E)$ ein zusammenhängender Graph und $C \subseteq E$ die Kantenmenge eines Kreises, so ist für jedes $e \in C$ auch $G - e$ zusammenhängend.*

Beweis. Selbst / Übung. □

Definition 3.2.8 Seien $G = (V, E)$ ein Graph und $S, T \subseteq V$.

(i) $[S, T] := \{e \in E \mid |e \cap S| = 1 \text{ und } |e \cap T| = 1\}$

(ii) $\delta(S) := [S, V \setminus S]$ heißt der **von S induzierte Schnitt**.

(iii) Eine Kantenmenge $F \subseteq E$ heißt **Schnitt**, falls $F = \delta(S)$ für ein $\emptyset \neq S \subsetneq V$.

Lemma 3.2.9 *Ein Graph $G = (V, E)$ ist genau dann zusammenhängend, wenn für alle $\emptyset \neq S \subsetneq V$ gilt $\delta(S) \neq \emptyset$.*

Beweis.

„⇒“
- Sei $\emptyset \neq S \subsetneq V$ beliebig.
- Wähle $s \in S$, $t \in V \setminus S$.
- Angenommen $P = (sv_1, \ldots, v_k t)$ wäre die Kantenfolge eines (s,t)-Weges in G. Dann gäbe es eine Kante $v_i v_{i+1} \in P$ mit $v_i \in S$, $v_{i+1} \notin S$, also $\delta(S) \neq \emptyset$.

„⇐“
- Angenommen es gäbe $s, t \in V$, so dass kein (s,t)-Weg existiert.
- Sei $S := \{v \in V \mid \text{es existiert } (s,v)\text{-Weg}\}$.
- Dann ist $\delta(S) = \emptyset$, $s \in S$ und $t \notin S$, also $\emptyset \neq S \subsetneq V$. □

3.3. Bäume und Wälder

Eine wichtige Klasse von Graphen sind sogenannte Bäume.

Definition 3.3.1

(i) Ein Graph $G = (V, E)$ heißt **Wald**, wenn er keinen Kreis als Teilgraphen enthält.

(ii) Ein Wald $G = (V, E)$ heißt **Baum**, wenn er zusammenhängend ist.

(iii) Ist $G = (V, E)$ ein Wald und $v \in V$ ein Knoten mit $\deg(v) = 1$, so heißt v ein **Blatt** von G.

Bemerkung

- Wir nennen auch eine Kantenmenge $W \subseteq E$ eines Graphen $G = (V, E)$ einen Wald bzw. Baum, wenn der Teilgraph $(V(W), W)$ von G ein Wald bzw. Baum ist.

Beobachtung 3.3.2 *Jeder Baum $T = (V, E)$ mit $|V| \geq 2$ enthält mindestens 2 Blätter.*

Beweis. Wir zeigen, wie man 2 verschiedene Blätter findet.

- Wähle eine Kante $e = uv \in E$. (Mindestens eine Kante muss existieren, da T wegen $|V| \geq 2$ sonst nicht zusammenhängend sein kann.)
- Setze Kante e startend bei u zu einem Pfad $P_1 = (u, e, v, \dots)$ so weit fort wie möglich, ohne dabei Kanten mehrfach zu verwenden.

  Da T ein Baum ist, gibt es keine Kreise.

  P_1 kann also auch keine Knoten wiederholen, ist also einfacher Weg.

  Da G endlich ist, ist auch $P_1 = (u, e, v, \dots, f, w)$ endlich.

  Da P_1 an w nicht fortgesetzt werden konnte, ist f die einzige Kante in $\delta(w)$.

  Also ist w Blatt.
- Setze Kante e startend bei v zu Pfad $P_2 = (v, e, u, \dots, f', w')$ so weit fort, wie möglich.

  Analog wie oben sieht man: w' ist Blatt.
- Außerdem muss $w \neq w'$ gelten, da sonst P_1 und $P_2 - e$ zusammen einen geschlossenen Kantenzug bilden würden und dieser (und somit auch T) folglich einen Kreis enthalten müsste. □

Beobachtung 3.3.3 *Ist $T = (V, E)$ ein Baum mit $|V| \geq 2$ und $v \in V$ ein Blatt, so ist auch $T - v$ ein Baum.*

Beweis. Selbst / Übung. □

Bäume lassen sich auf viele verschiedene Arten charakterisieren (oder definieren), die jedoch alle äquivalent zueinander sind. Die wichtigsten Charakterisierungen werden im folgenden Satz zusammengefasst.

Satz 3.3.4 *Sei $G = (V, E)$ ein Graph. Folgende Aussagen sind äquivalent:*

(i) *G ist ein Baum.*

(ii) *G ist kreisfrei und $|E| = |V| - 1$.*

(iii) *G ist zusammenhängend und $|E| = |V| - 1$.*

(iv) *G ist minimal zusammenhängend*
(d.h. G ist zusammenhängend und jedes $e \in E$ ist eine Brücke).

(v) *G ist minimal mit $\delta(S) \neq \emptyset$ für alle $\emptyset \neq S \subsetneq V$*
(d. h. es gilt $\delta(S) \neq \emptyset$ für alle $\emptyset \neq S \subsetneq V$, aber für jedes $e \in E$ gibt es eine Menge $\emptyset \neq S \subsetneq V$, so dass $\delta(S) \setminus \{e\} = \emptyset$).

(vi) *G ist maximal kreisfrei*
(d.h. G ist kreisfrei, aber für alle $u, v \in V$ mit $u \neq v$ und $uv \notin E$ enthält $G + uv$ einen Kreis).

(vii) *Für alle $s, t \in V$ enthält G genau einen (s, t)-Weg.*

Bemerkung Die Begriffe „minimal“ und „maximal“ beziehen sich, wie im obigen Satz, bei Graphen immer auf die Inklusionsrelation bezüglich der Kantenmenge. G ist minimal bzw. maximal mit Eigenschaft X heißt also, dass der Graph $G = (V, E)$ die Eigenschaft X besitzt, aber alle Graphen, die man aus G durch Entfernen bzw. Hinzufügen einer einzigen Kante erhält, die Eigenschaft X nicht mehr besitzen.

Beweis. (Skizze für (1) ⇔ (4) ⇔ (7))

(1)⇒(7): Gäbe es zwei verschiedene (s, t)-Wege P_1 und P_2, so enthielte die Vereinigung der Kanten von P_1 und P_2 einen Kreis.

(7)⇒(4): Zusammenhängend ist klar.

Wäre $e = (s, t) \in E$ keine Brücke, so enthielte $G - e$ einen (s, t)-Weg P_1. Mit $P_2 = (s, e, t)$ gäbe es dann aber einen zweiten (s, t)-Weg $P_2 \neq P_1$.

(4)⇒(1): Zusammenhängend ist klar. Enthielte G einen Kreis C, so wäre $e \in C$ keine Brücke in G. □

Definition 3.3.5 Ein Teilgraph $T = (U, F)$ eines Graphen $G = (V, E)$ heißt **aufspannender Baum** oder **Spannbaum**, falls T ein Baum ist und $U = V$ (also T aufspannend in G ist).

Bemerkung

- Wir bezeichnen auch allein die Kantenmenge $F \subseteq E$ eines Spannbaumes (V, F) von $G = (V, E)$ wieder als Spannbaum von G.

Beobachtung 3.3.6 *Jeder zusammenhängende Graph G besitzt einen Spannbaum.*

Beweis.

- Wähle einen minimal zusammenhängenden Teilgraph T von G.
- Mit Satz 3.3.4 (iv $\rightarrow$ i) folgt sofort, dass T ein Baum ist. □

Praktisch finden kann man einen Spannbaum leicht mit Hilfe der Tiefen- oder Breitensuche im Graphen G.

Das etwas allgemeinere Problem, einen (sogar kardinalitäts-) maximalen Wald in (einem nicht notwendigerweise zusammenhängenden) Graphen G zu finden, kann man mit den folgenden Algorithmen lösen:

Algorithmus 3.3.7 (Greedy-In)

Eingabe: Graph $G = (V, E)$ mit $E = \{e_1, \ldots, e_m\}$

Ausgabe: maximaler Wald $W \subseteq E$
(Ist G zusammenhängend, so ist W ein Spannbaum (vgl. Satz 3.3.4))

1: $W = \emptyset$
2: **for** $i = 1, \ldots, |E|$ **do**
3: **if** $|W| = |V| - 1$ **then**
4: **return** W
5: **if** $(V, W \cup \{e_i\})$ enthält keinen Kreis **then**
6: $W \leftarrow W \cup \{e_i\}$
7: **return** W

Greedy-In startet mit einer leeren und somit kreisfreien Kantenmenge W und fügt dann sukzessive diejenigen Kanten zu W hinzu, deren Hinzufügen die Kreisfreiheit von W nicht zerstört. Man erhält damit einen inklusionsmaximalen kreisfreien Teilgraphen.

Satz 3.3.8 *Algorithmus Greedy-In arbeitet korrekt (liefert also für jeden Graphen $G = (V, E)$ tatsächlich immer einen maximalen Wald W) und kann so implementiert werden, dass seine Laufzeit $\mathcal{O}(|V|^2)$ beträgt.*

Bemerkung Die $\mathcal{O}()$-Notation dient üblicherweise zur asymptotischen Abschätzung von Laufzeit- und Speicherbedarfsfunktionen von Algorithmen in Abhängigkeit von der Größe der Eingabedaten.

Faktisch werden dadurch für eine Funktion $f : \mathbb{N} \to \mathbb{N}$ nur noch die für $n \to \infty$ dominanten Terme betrachtet.

Formal ist für eine Funktion $f : \mathbb{N} \to \mathbb{N}$:

$$\mathcal{O}(f) := \{g : \mathbb{N} \to \mathbb{N} \mid \exists n_0, c \in \mathbb{N}\ \forall n \geq n_0 :\ g(n) \leq c \cdot f(n)\}$$

die Menge alle Funktionen $g : \mathbb{N} \to \mathbb{N}$, die sich ab einer (von g abhängigen) Konstanten n_0 für alle größeren $n \geq n_0$ durch $g(n) \leq c \cdot f(n)$ abschätzen lassen, wobei c auch eine (von g abhängige) Konstante ist.

Mehr Details dazu in den Vorlesungen der Theoretischen Informatik.

Beweis.

Korrektheit: Folgt direkt aus Schritt 5: Jede vom Algorithmus nicht zu W hinzugefügte Kante $e \in E \setminus W$ bildet einen Kreis mit den Kanten in W. (Sonst wäre sie in Schritt 5 hinzugefügt worden.) Also ist W eine (inklusions-)maximal kreisfreie Kantenteilmenge aus G, d.h. ein (inklusions-)maximaler Wald.

Für jede Zusammenhangskomponente $G_i = (V_i, E_i)$ von G ist die Kantenmenge $W \cap E_i$ ein aufspannender Baum von G_i, da sie in G_i (inklusions-)maximal kreisfrei ist. Folglich enthält W auch genau $|V_i| - 1$ viele Kanten aus der Zusammenhangskomponente G_i, d.h. $|W \cap E_i| = |V_i| - 1$.

Da jede kreisfreie Kantenmenge maximal $|V_i| - 1$ Kanten in der Zusammenhangskomponente G_i enthält, ist W somit auch kardinalitätsmaxial unter allen kreisfreien Kantenmengen in G.

Abschätzung der Laufzeit: (Skizze)

- Speichere für jeden Knoten $v \in V$ während des gesamten Algorithmus die Nummer $k(v)$ derjenigen Zusammenhangskomponente in (V, W), die den Knoten v enthält. (Als Abbildung $k \colon V \to \{1, \ldots, n\}$ oder, äquivalent, als Vektor $k \in \{1, \ldots, n\}^V$.)

  Starte mit $k(v_i) = i$ für $V = \{v_1, \ldots, v_n\}$.
- Laufzeit: maximal $|E| = m \leq n^2$ Iterationen der for-Schleife
  - Der Test, ob $e_i = uv$ mit W einen Kreis bildet, ist äquivalent zum Test, ob u und v in der gleichen Zusammenhangskomponente von (V, W) liegen.

    Dazu genügt es, $k(u) = k(v)$ zu testen. $\rightsquigarrow$ konstanter Aufwand $\mathcal{O}(1)$
  - Wird e_i nicht zu W hinzugefügt: $\rightsquigarrow$ kein Aufwand $\mathcal{O}(1)$
  - Wird e_i zu W hinzugefügt:

    aktualisiere Zusammenhangskomponenten von (V, W_{neu}):

    $$k_{neu}(w) := \begin{cases} k(u), & \text{falls } k(w) = k(v), \\ k(w), & \text{sonst.} \end{cases} \qquad \text{für alle } w \in V$$

    $\rightsquigarrow$ Aufwand: n Knoten, je 1 Test und ≤ 1 Zuweisung, insgesamt $\mathcal{O}(n)$.
- Maximal $n - 1$ mal wird eine Kante hinzugefügt. $\rightsquigarrow$ Aufwand $\mathcal{O}(n \cdot n)$

  Maximal m mal wird eine Kante nicht hinzugefügt: $\rightsquigarrow$ Aufwand $\mathcal{O}(m \cdot 1)$.
- Insgesamt: Aufwand $\mathcal{O}(n^2 + m) = \mathcal{O}(n^2)$. □

Algorithmus 3.3.9 (Greedy-Out)

Eingabe: zusammenhängender Graph $G = (V, E)$ mit $E = \{e_1, \ldots, e_m\}$

Ausgabe: Spannbaum $W \subseteq E$ von G

1: $W = E$
2: **for** $i = 1, \ldots, |E|$ **do**
3: **if** $(V, W \setminus \{e_i\})$ ist zusammenhängend **then**
4: $W \leftarrow W \setminus \{e_i\}$
5: **if** $|W| = |V| - 1$ **then**
6: **return** W
7: **return** W

Greedy-Out startet mit der kompletten und somit zusammenhängenden und aufspannenden Kantenmenge $W = E$ und entfernt dann sukzessive diejenigen Kanten aus W, deren Entfernen den Zusammenhang von W nicht zerstört. Man erhält damit einen inklusionsminimalen zusammenhängenden und aufspannenden Teilgraphen.

Folgerung 3.3.10 *Algorithmus Greedy-Out arbeitet korrekt (d.h. W ist ein Spannbaum von G) und kann so implementiert werden, dass seine Laufzeit $\mathcal{O}(n^4)$ beträgt.*

Bemerkung Mit Varianten von Greedy-In und Greedy-Out kann man auch längen- bzw. kostenmaximale Wälder oder längen- bzw. kostenminimale Spannbäume in einem Graphen $G = (V, E)$ mit Kantenlängen c_e, $e \in E$, berechnen. Mehr Details dazu können Sie in einer Vorlesung zur „Kombinatorischen Optimierung“ erfahren.

3.4. Paarungen / Matchings

Ein in vielen praktischen Anwendungen sehr wichtiges Konstrukt in Graphen sind sogenannte Matchings oder Paarungen, bei denen Knoten entsprechen der existierenden Kanten zu Paaren zusammengefasst werden sollen. Da ein Paar von Knoten nichts anderes als eine Kante im Graphen ist, lassen sich solche Paarungen gut als spezielle Teilmengen der Kanten eines Graphen beschreiben.

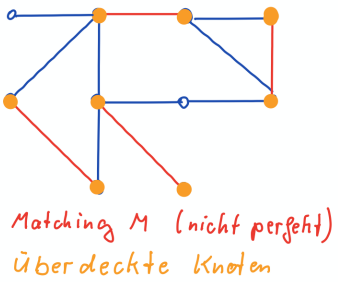
Definition 3.4.1

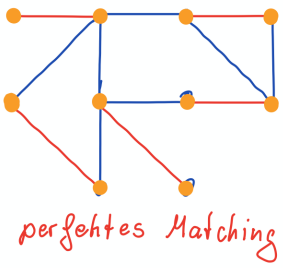
(i) Eine **Paarung** oder ein **Matching** in einem Graphen $G = (V, E)$ ist eine Kantenteilmenge $M \subseteq E$ mit $|M \cap \delta(v)| \leq 1 \quad$ für alle $v \in V$.

(ii) Ein Matching $M \subseteq E$ heißt **perfekt**, wenn $|M \cap \delta(v)| = 1 \quad$ für alle $v \in V$.

(iii) Ein Knoten $v \in V$ heißt von Matching M **überdeckt**, falls $v \in e$ für ein $e \in M$.

Achtung: Die Begriffe Matching oder Paarung bezeichnen immer die gesamte Menge M in der vorherigen Definition, also die Menge aller durch M beschriebenen Knotenpaare. Zwei Knoten u, v mit $uv \in M$ heißen in M gepaart oder eine Paar in M.





Das Entscheidungsproblem, für einem gegebenen Graphen zu entscheiden, ob ein Matching eine bestimten Mindestgröße (oder ein perfektes Matching) existiert, und das Optimierungsproblem, in einem gegebenen Graphen ein Matching maximaler Kardinalität zu bestimmen, treten in vielen praktischen Anwendungen auf, beispielsweise beim Bilden von 2er-Übungsgruppen, beim Bilden von Tanzpaaren, bei der Zuordnungen von Aufgaben zu Servern, etc.

Problem 3.4.2 (Maximum-Matching-Problem)
Instanz: Graph $G = (V, E)$
Aufgabe: Bestimme ein Matching $M \subseteq E$ mit maximaler Kardinalität $|M|$ in G.

Wir wollen im Folgenden sowohl Methoden kennen lernen, mit denen einerseits die Größe des maximalen Matchings abgeschätzt und somit die Optimalität eines irgendwie geratenen oder bestimmten Matchings leicht nachgewiesen werden kann, als auch Methoden, mit denen ein kardinalitätsmaximales Matching tatsächlich effizient bestimmt werden kann.

Die folgende Abschätzungen und Beobachtungen sind offensichtlich, da zu jedem Knoten des Graphen nur eine Kante eines Matchings inzident sein darf:

Beobachtung 3.4.3 *Sei $G = (V, E)$ ein Graph.*

(i) Für jedes Matching $M \subseteq E$ gilt $|M| \leq \lfloor \frac{|V|}{2} \rfloor$.

(ii) Ein Matching $M \subseteq E$ ist perfekt genau dann, wenn $|M| = \frac{|V|}{2}$.

Zunächst überlegen wir uns, wann ein Matching kardinalitätsmaximal ist und wie man kardinalitätsmaximale Matchings algorithmisch konstruieren kann.

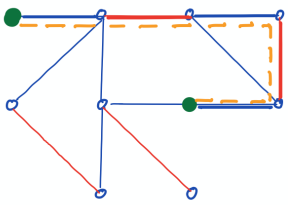
Definition 3.4.4 Sei $G = (V, E)$ ein Graph und $M \subseteq E$ ein Matching in G.

(i) Ein Knoten $v \in V$ heißt **M-exponiert**, wenn $v \notin V(M)$ gilt.
(Ein Knoten ist also M-exponiert genau dann, wenn er nicht von M überdeckt ist.)
Die Menge aller M-exponierten Knoten bezeichnen wir mit $X_M \subseteq V$.

(ii) Ein Weg P in G mit Kantenfolge $(e_1, \ldots, e_\ell)$ heißt **M-alternierend**, wenn

$$|\{e_i, e_{i+1}\} \cap M| = 1 \quad \text{für alle } i \in [\ell - 1] \text{ gilt.}$$

(D.h. P enthält abwechselnd Kanten aus M und aus $E \setminus M$.)

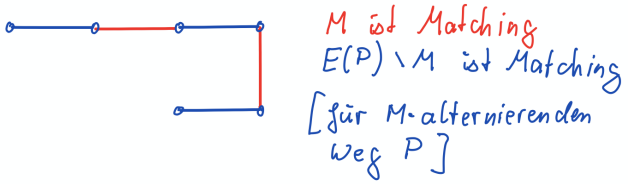


M-exponierte Knoten
M-alternierender Weg
(auch M-augmentierend)

Alternierende Wege sind der Schlüssel zur Verbesserung von nicht bereits maximalen Matchings. Findet man zu einem gegebenen Matching M einen M-alternierenden Weg P, dessen Start- und End-Knoten nicht von M überdeckt sind, so kann man ein neues, größeres Matching M' (mit $|M'| = |M| + 1$) konstruieren. Die folgenden Definitionen und der Satz von Berge beschreiben diese Grundidee mathematisch präzise:

Beobachtung 3.4.5 *Sei $G = (V, E)$ ein Graph, $M \subseteq E$ ein Matching und P ein (einfacher) Weg in G. P ist M-alternierend genau dann, wenn auch $E(P) \setminus M$ ein Matching ist.*

($E(P) \cap M$ ist als Teilmenge von M natürlich auch ein Matching.)



Definition 3.4.6 Sei $G = (V, E)$ ein Graph und $M \subseteq E$ ein Matching. Ein M-alternierender Weg P, dessen Endknoten v_0 und v_ℓ beide M-exponiert sind, heißt **M-augmentierend**.

Definition 3.4.7 Für zwei Mengen A und B bezeichnet

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

die sogenannte **symmetrische Differenz** von A und B.

Satz 3.4.8 (Berge) *Sei $G = (V, E)$ ein Graph. Ein Matching $M \subseteq E$ in G ist genau dann kardinalitätsmaximal, wenn es keinen M-augmentierenden Weg in G gibt.*

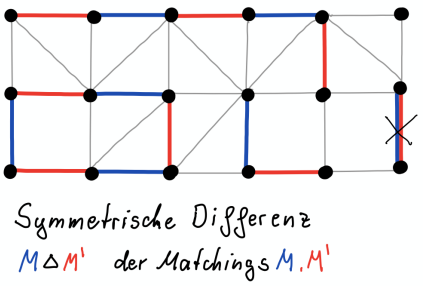
Beweis.

„⇒“: Angenommen es existiert ein M-augmentierender Weg P, so ist auch

$$M' := M \triangle E(P) := (M \setminus E(P)) \cup (E(P) \setminus M)$$

ein Matching. Da für einen M-augmentierenden Weg P aber $|E(P) \setminus M| = |M \cap E(P)| + 1$ gilt, ist die Kardinalität von M' folglich $|M'| = |M| + 1$, also war M nicht kardinalitätsmaximal.

„⇐“: Angenommen es existiert ein Matching M' mit $|M'| > |M|$. Betrachte den Graphen $H = (V, M \triangle M')$.



Da M und M' Matchings sind, hat jeder Knoten in H einen Grad von maximal 2. (Jeder Knoten kann nur zu jeweils maximal einer Kante aus M und einer aus M' inzident sein.)

Damit ist H eine Vereinigung von knotendisjunkten Kreisen $C_1, \ldots, C_k$ und Wegen $P_1, \ldots, P_l$. (Das folgt für jeden Graph, dessen Knotengrade maximal 2 sind.)

Da jeder Knoten nur zu jeweils maximal einer Kante aus M und einer aus M' inzident ist, kommen auf jedem dieser Kreise und Wege abwechselnd eine Kante aus M und eine Kante aus M' vor, d.h. aller Kreise und Wege sind M-alternierend.

Damit folgt sofort, dass jeder Kreis C_i gerade Länge hat und genau so viele Kanten aus M wie aus M' enthält.

Da insgesamt jedoch $|M'| > |M|$ gilt, muss mindestens einer der Wege P_j mehr Kanten aus M' als aus M enthalten.

Da P_j M-alternierend ist, ist das nur möglich, wenn die erste und die letzte Kante von P_j Kanten aus M' sind. Damit aber automatisch die beiden Endknoten von P_j M-exponiert. (Sonst wäre P_j Teil einer echt größeren Zusammenhangskomponente von H.) Also ist P_j auch ein M-augmentierender Weg. □

Der Satz von Berge liefert unmittelbar den folgenden Algorithmischen Ansatz zur Berechnung eines Matchings maximaler Kardinalität.

Algorithmus 3.4.9 (Maximum-Matching)

Eingabe: Graph $G = (V, E)$
Ausgabe: Matching $M \subseteq E$ in G mit maximaler Kardinalität $|M|$

1: Starte mit beliebigem Matching $M \subseteq E$. (z. B. $M = \emptyset$)
2: **repeat**
3: Suche beliebigen M-augmentierenden Weg P in G.
4: **if** (M-augmentierender Weg P gefunden) **then**
5: Ersetze M durch $M \triangle E(P)$.
6: **until** (kein M-augmentierenden Weg gefunden)
7: **return** M

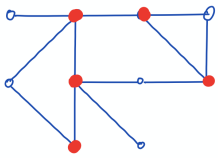
Offensichtlich wird mit jedem gefundenen M-augmentierenden Weg die Kardinalität von M um genau 1 erhöht. Da die Kardinalität eines Matchings nicht größer als $\frac{|V|}{2}$ sein kann, werden also höchstens $\frac{|V|}{2}$ Iterationen der Schleife 2-6 durchgeführt.

Der kritische Teilschritt des Algorithmus ist Schritt 3. In diesem Schritt muss ein M-augmentierender Weg P in G gefunden werden, falls es einen gibt (oder korrekt verifiziert werden, dass es keinen M-augmentierender Weg P in G mehr gibt). Es gibt effiziente Algorithmen für Schritt 3 (vgl. Vorlesung Kombinatorische Optimierung). Für den Fall, dass G bipartit ist, sind diese auch noch relativ einfach, für allgemeine (nicht-bipartite) Graphen G sind sie deutlich komplexer.

Im Folgenden beschäftigen wir uns mit Methoden, die maximale Kardinalität eines Matchings in einem Graphen $G = (V, E)$ wesentlich präziser als durch $\lfloor \frac{|V|}{2} \rfloor$ nach oben abzuschätzen. Dafür führen wir eine zweites, auf den ersten Blick völlig neues und in keiner Beziehung zum Matching stehendes Konzept (und Optimierungsproblem) ein.

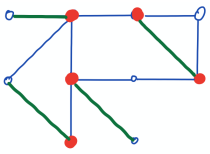
Definition 3.4.10 Eine **Knotenüberdeckung (Vertex Cover)** eines Graphen $G = (V, E)$ ist eine Knotenteilmenge $W \subseteq V$ mit

$$\{u, v\} \cap W \neq \emptyset \quad \text{für alle } e = uv \in E.$$



Matchings und Knotenüberdeckungen stehen in einer sehr einfachen und sehr bedeutsamen Beziehung zueinander:

Satz 3.4.11 *Seien $G = (V, E)$ ein Graph, $M \subseteq E$ ein beliebiges Matching und $W \subseteq V$ eine beliebige Knotenüberdeckung in G. Dann gilt $|M| \leq |W|$.*



Beweis.

- Für $uv = e \in M$ sei $W_e := \{u, v\} \cap W$.
- Da W eine Knotenüberdeckung, gilt $|W_e| \geq 1$ für alle $e \in M$.
- Da M ein Matching ist, gilt $W_e \cap W_f = \emptyset$ für alle $e, f \in M$, $e \neq f$.
- Folglich ist $|M| \cdot 1 \leq \sum_{e \in M} |W_e| = |\dot{\bigcup}_{e \in M} W_e| \leq |W|$. □

Satz 3.4.11 liefert direkt die folgende Folgerung, die als **schwache Dualität** zwischen Matchings und Knotenübeckungen bezeichnet wird.

Folgerung 3.4.12 *Sei $G = (V, E)$ ein Graph. Dann gilt*

$$\max \{|M| \mid M \subseteq E \text{ ist Matching in } G\} \leq \min \{|W| \mid W \subseteq V \text{ ist Knotenüberdeckung von } G\}.$$

Mit Hilfe von Satz 3.4.12 kann man in vielen Fällen die Maximalität eines gegebenen, irgendwie bestimmten (oder geratenen) Matchings M^* nachweisen, indem man einfach eine geeignete Knotenüberdeckung W^* des Graphen mit $|M^*| = |W^*|$ findet und angibt. Da nach dem Satz

jedes Matching M die Bedingung $|M| \leq |W^*|$ erfüllt, folgt sofort auch für jedes Matching M die Bedingung $|M| \leq |M^*|$ und somit die Maximalität von M^*.

Frage: Geht das immer? Anders gefragt: Gilt in 3.4.12 im Allgemeinen oder in Spezialfällen sogar die Gleichheit (sogenannte **starke Dualität**)?

Beobachtung 3.4.13 *Im Allgemeinen gilt in 3.4.12 keine Gleichheit.*
Für Kreise $G = C_n$ mit n ungerade gilt beispielsweise

$$\begin{aligned} &\max\{|M| \mid M \text{ ist Matching in } G\} = \lfloor \frac{n}{2} \rfloor \\ &< \lceil \frac{n}{2} \rceil = \min\{|W| \mid W \text{ ist Knotenüberdeckung von } G\}. \end{aligned}$$

Für den Spezialfall **bipartitier Graphen** gilt die **starke Dualität** zwischen Matchings und Knotenübeckungen.

Satz 3.4.14 (Satz von König) *In einem bipartiten Graphen $G = (V, E)$ gilt*

$$\begin{aligned} &\max\{|M| \mid M \subseteq E \text{ ist Matching in } G\} \\ &\qquad = \min\{|W| \mid W \subseteq V \text{ ist Knotenüberdeckung von } G\}. \end{aligned}$$

Beweis.

- Sei $G = (V, E)$ der gegebene bipartite Graph und $V = A \dot\cup B$ die Bipartition der Knotenmenge, so dass $E \subseteq \{uv \mid u \in A, v \in B\}$.

  Sei M eine Paarung maximaler Kardinalität.

  Nach 3.4.12 gilt $|W| \geq |M|$ für jede Knotenüberdeckung W von G.

  Wir konstruieren nun eine Knotenüberdeckungen $U \subseteq V$ mit genau $|M|$ Knoten, deren Existenz dann den Satz beweist.

- Sei $ab \in M$ eine Kante mit $a \in A$ und $b \in B$.

  Wir müssen entscheiden, ob $a \in U$ oder $b \in U$. Setze

  $$F := \{ab \in M \mid a \in A, b \in B, \text{ in } ab \text{ endet ein in } A - V(M) \text{ beginnender } M\text{-alt. Weg}\},$$

  sowie

  $$U := \{b \in B \mid ab \in F\} \cup \{a \in A \mid ab \in M \setminus F\}.$$

  Offenbar ist $|U| = |M|$.

  Es bleibt zu zeigen, dass U eine Knotenüberdeckung von G ist.

- Angenommen nein, dann exisitierte eine Kante $a'b' \in E$, $a' \in A$, $b' \in B$, mit $a', b' \notin U$. Wir unterscheiden vier Fälle:

  (1.) $a' \cap V(M) = b' \cap V(M) = \emptyset$.

  Dann ist $\{a'b'\} \cup M$ ein größeres Matching, Widerspruch.

(2.) $\exists e \in M : a' \in e, b' \cap V(M) = \emptyset$.

Dann ist $e = a'\bar{b}$ für ein $\bar{b} \in B \setminus \{b'\}$.

Wegen Annahme $a' \notin U$, existiert M-alt. Weg der Form $(P, \bar{b}, a')$ mit Start in $A - V(M)$

$\Rightarrow (P, \bar{b}, a', b')$ ist M-verbessernder Weg.

$\Rightarrow M$ ist nicht maximal. Widerspruch.

(3.) $a' \cap V(M) = \emptyset$, $\exists e \in M : b' \in e$.

Dann ist $e = \bar{a}b'$ für ein $\bar{a} \in A \setminus \{a'\}$.

$\Rightarrow P = (a', b', \bar{a})$ ist M-alt. Weg mit Start in $A - V(M)$, der in e endet.

$\Rightarrow b' \in U$. Widerspruch.

(4.) $\exists e, f \in M : e \neq f, a' \in e, b' \in f$.

Dann sind $e = a'\bar{b}, \bar{b} \in B \setminus \{b'\}$ und $f = \bar{a}b', \bar{a} \in A \setminus \{a'\}$.

Wegen $a', b' \notin U$ und $e, f \in M$ sind dann $\bar{a}, \bar{b} \in U$.

Also existiert nach Wahl von U ein M-alternierender Weg der Form $(P, \bar{b}, a')$ mit Start in $A - V(M)$.

Dieser Weg kann b' (und somit auch $\bar{a}$) nicht enthalten, sonst wäre $b' \in U$.

Dann ist aber $(P, a', b', \bar{a}$ ein M-alternierender Weg mit Start in $A - V(M)$, der in $\bar{a}b'$ endet, erneut ein Widerspruch zu $b' \notin U$. □

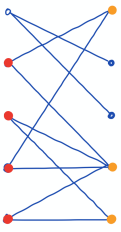
Für bipartite Graphen kann man auch die Bedingungen, unter denen maximale oder sogar perfekte Matchings existieren, relativ einfach beschreiben.

Satz 3.4.15 (Satz von Hall, Heiratssatz) *Sei $G = (V, E)$ ein bipartiter Graph mit Bipartition $V = V_1 \dot{\cup} V_2$. Es gibt genau dann ein Matching $M \subset E$ in G, welches alle Knoten von V_1 überdeckt, wenn*

$$|N(X)| \geq |X| \text{ für alle } X \subseteq V_1. \tag{H}$$

(Man sagt auch, dass X die Hall-Bedingung (H) erfüllt*.)*

Ist die Hall-Bedingung verletzt, d.h. gibt es für irgendeine Teilmenge X der Knoten in V_1 nicht genug mögliche Partner $N(X)$ in V_2, so kann es offensichtlich kein Matching geben, das alle Knoten aus X mit den Knoten aus $N(X)$ paart. Also kann auch kein Matching existieren, dass alle Knoten aus V_1 paart.



Verletzte Hall-Bedingung:
$|N(X)| < |X|$

Beweis.

„⇒ “: Falls ein V_1-überdeckendes Matching M existiert, so ist

$$|N(X)| \geq |\{xy \in M \mid x \in X, y \in V_2\}| \geq |X| \text{ für alle } X \subseteq V_1.$$

„⇐“: Ang. G enthält kein V_1-überdeckendes Matching. Dann ist die Kardinalität einer minimalen Knotenüberdeckung kleiner als $|V_1|$. Sei U eine Knotenüberdeckung für G mit $U_1 := U \cap V_1, U_2 := U \cap V_2$ und $|U_1| + |U_2| < |V_1|$.

Da auch alle Kanten in $\delta(V_1 \setminus U_1)$ von der Knotenüberdeckung U überdeckt werden müssen und dafür nur die Knoten aus U_2 in Frage kommen, gilt $|N(V_1 \setminus U_1)| \leq |U_2|$.

Damit folgt gilt:

$$|N(V_1 \setminus U_1)| \leq |U_2| < |V_1| - |U_1| = |V_1 \setminus U_1|\,.$$

Damit wird die Hall-Bedingung für $V_1 \setminus U_1$ verletzt. □

Der Satz 3.4.15 erlaubt es uns, in beiden möglichen Fällen einen algorithmisch effizient (hier sogar in linearer Zeit) prüfbaren Beweis – ein sogenanntes Zertifikat – anzugeben:

- Existiert ein Matching M, das alle Knoten in V_1 überdeckt, so kann man das Matching M selbst angeben.

  (Das Prüfen der Matching-Eigenschaft und der Behauptung, dass alle Knoten in V_1 überdeckt werden, geht algorithmisch sehr einfach durch Zählen, wie oft jeder Knoten in M vorkommt.)

- Existiert kein Matching, das alle Knoten in V_1 überdeckt, so kann man eine Knotenmenge $X \subseteq V_1$ mit $|N(X)| < |X|$ angeben.

  (Das Prüfen, dass $X \subseteq V_1$ und dass $|N(X)| < |X|$, geht algorithmisch sehr einfach durch Markieren und Zählen der entsprechenden Knoten.)

Dieses Konzept effizient verifizierbarer Lösungen ist wichtig in der Komplexitätstheorie in der Theoretischen Informatik.

Aus dem Satz von Hall erhält man leicht die folgende Existenzaussage für perfekte Matchings in bipartiten Graphen.

Folgerung 3.4.16 (Satz von Frobenius) *Sei $G = (V, E)$ ein bipartiter Graph mit Bipartition $V = V_1 \dot\cup V_2$ und $|V_1| = |V_2|$. Es gibt genau dann ein perfektes Matching in G, wenn $|N(X)| \geq |X|$ für alle $X \subseteq V_1$.*

3.5. Eulertouren

In verschiedenen Anwendungen treten Probleme auf, in denen eine Graph auf eine bestimmte Art und Weise durchlaufen werden muss. Ein sehr bekanntes Beispiel ist das Problem des Handlungsreisenden (Travelling Salesman Problem), bei dem alle Knoten eines gegeben Graphen auf einem Kreis so durchlaufen werden sollen, dass dabei jeder Knoten genau einmal besucht wird (und die Summe der Kantenlängen des Kreises so kurz wie möglich sein soll). Dieses Problem tritt nicht nur bei der Planung von Touren in der Logistik auf, sondern u. A. auch beim Scheduling von Jobs auf Prozessoren/Maschinen. Diese Problem ist im Allgemeinen NP-vollständig. Es ist kein polynomieller Algorithmus bekannt, mit dem sich in einem beliebigen Graphen entscheiden lässt, ob überhaupt ein solcher sogenannter Hamilton-Kreis existiert.

In diesem Unterkapitel befassen wir uns mit dem deutlich einfacheren Problem, einen Graphen so auf einem Kreis (oder auf einem Weg) zu druchlaufen, dass dabei jede Kante genau einmal durchlaufen wird. Diese Problem ist auch als Königsberger Brückenproblem bekannt und geht auf Leonhard Euler zurück.

Definition 3.5.1 Sei $G = (V, E)$ ein zusammenhängender Graph. Ein Pfad $W = (v_0, e_1, v_1, \ldots, e_m, v_m)$ in G, so dass jede Kante $e \in E$ **genau einmal** in W vorkommt (d.h. $E(W) = E$ und $m = |E|$), heißt

(i) (offener) **Euler-Zug** in G, falls $v_0 \neq v_m$,

(ii) **Euler-Tour** (oder geschlossener Euler-Zug) in G, falls $v_0 = v_m$.

(iii) Ein Graph G heißt **Eulersch**, wenn eine *Euler-Tour* in G existiert.

Bemerkung

- In Euler-Touren und -zügen
  - dürfen sich Knoten beliebig wiederholen, aber
  - jede Kante $e \in E$ muss *genau* einmal enthalten sein.
- Ein Graph ist Eulersch, wenn man seine Kanten „in einem Zug zeichen“ kann

  $\rightsquigarrow$ Haus vom Nikolaus.

Fragen:

- Für welche Graphen G existieren Euler-Touren bzw. offene Euler-Züge?

  $\rightsquigarrow$ Offensichtlich muss G zusammenhängend sein.

  (Das allein reicht aber noch nicht.)
- Wie findet man Euler-Touren bzw. offene Euler-Züge effizient?

Läuft man eine Euler-Tour ab, so betritt man jeden Knoten genau so oft, wie man ihn verlässt. Bei einem Euler-Zug gilt dies an allen Knoten außer am Start- und am Endknoten, welche man genau einmal mehr verlässt bzw. betritt. Da jede Kante des Graphen in einem Euler-Zug oder einer Euler-Tour genau einmal enthalten ist, liefert uns dies die folgende Beobachtung.

Beobachtung 3.5.2 *Sei G ein zusammenhängender Graph.*

(i) Existiert eine Euler-Tour in G, so gilt

$$deg(v) \equiv 0 \mod 2 \text{ für alle } v \in V.$$

(ii) Ist $W = (v_0, e_1, v_1, \ldots, e_m, v_m)$ ein offener Euler-Zug in G, so gilt

$$deg(v) \equiv 0 \mod 2 \text{ für alle } v \in V \setminus \{v_0, v_m\} \text{ und}$$

$$deg(v_0) \equiv deg(v_m) \equiv 1 \mod 2.$$

Verbindet man den Endknoten eines Euler-Zuges wieder mit dem Startknoten (durch Hinzufügen einer zusätzlichen Kante), erhält man offenbar eine Euler-Tour.

Beobachtung 3.5.3 *Der Pfad $W = (v_0, e_1, v_1, \ldots, e_m, v_m)$ ist ein offener Euler-Zug in G genau dann, wenn $(W, v_m v_0, v_0)$ eine geschlossene Euler-Tour in $G + v_m v_0$ ist.*

Bemerkung Es genügt also, Euler-Touren genauer zu untersuchen:

- Falls G genau zwei Knoten $u \neq v$ mit ungeradem Grad hat, so kann man die Existenz und das Finden eines Euler-Zuges in G auf die Existenz und das Finden einer Euler-Tour in $G + uv$ zurückführen.
- Andernfalls kann G wegen 3.5.2 keinen Euler-Zug enthalten.

Beobachtung 3.5.2 liefert uns dafür, dass in einem Graphen G überhaupt eine Euler-Tour existieren kann, das notwendige Kriterium, dass alle Knoten einen geraden Grad haben müssen. Im Folgenden zeigen wir, dass diese Kriterium in zusammenhängenden Graphen auch hinreichend ist. Dazu werden wir zeigen, wie man eine Euler-Tour algorithmisch effizient finden kann.

Lemma 3.5.4 *Sei $G = (V, E)$ ein Graph mit $E \neq \emptyset$ und $deg(v) \equiv 0 \mod 2$ für alle $v \in V$. Für jedes $e \in E$ existiert dann in G ein Kreis C mit $e \in C$.*

Beweis. Übung / Hausaufgabe □

Satz 3.5.5 (Euler) *Sei $G = (V, E)$ ein zusammenhängender Graph mit $|V| \geq 2$.*

G ist Eulersch genau dann, wenn jeder Knoten $v \in V$ geraden Grad hat.

Bemerkung Satz 3.5.5 gilt auch für Multigraphen. Schleifen $e = vv$ zählen dann doppelt zum Grad von v.

Beweis.

$\Rightarrow$ Ist G Eulersch, so existiert eine Eulertour W in G.

Nach 3.5.2 (i) sind dann alle Knotengrade gerade.

$\Leftarrow$ Da G zusammenhängend und $|V| \geq 2$ ist, folgt $E \neq \emptyset$.

Da $\deg(v) \equiv 0 \mod 2$ für alle $v \in V$ gilt, enthält G nach 3.5.4 wenigstens einen Kreis. Also enthält G auch einen geschlossenen Kantenzug mit paarweise verschiedenen Kanten. (Jeder Kreis ist so ein Kantenzug.)

Wir wählen einen geschlossenen Kantenzug $W = (v_0, e_1, v_1, \ldots, e_l, v_l = v_0)$ mit paarweise verschiedenen Kanten und l maximal.

Ist $E(W) = E$, so ist W eine Euler-Tour und der Beweis fertig.

Wie zeigen daher nun, dass $E(W) \neq E$ im Widerspruch zur Wahl von W mit maximalem l steht.

Dazu betrachten wir den Restgraphen $G' = (V, F)$ mit $F = E \setminus E(W)$.

Für die Knotengrade im Restgraphen G' gilt offenbar für alle $v \in V$

$$\deg_{G'}(v) := |\delta_G(v) \cap F| = \underbrace{|\delta_G(v)|}_{\text{gerade}} - \underbrace{|\delta_G(v) \cap E(W)|}_{\text{gerade}} \equiv 0 \mod 2.$$

Wegen $E(W) \subsetneq E$ ist außerdem $F \neq \emptyset$.

Da G zusammenhängend ist, gibt es auch einen Knoten $u \in W$, so dass $\deg_F(u) > 0$ gilt. (Sonst wäre $\delta(V(W))$ ein Schnitt, der G in zwei Zusammenhangskomponenten trennt.)

Also gibt es nach Lemma 3.5.4 in $G' = (V, F)$ einen Kreis C positiver Länge mit $u \in C$. (Wähle $e \in \delta'_G(u)$ und wende Lemma 3.5.4 an.)
Dieser ist ein geschlossener Kantenzug $C = (u, e, u_1 \ldots, f, u_k = u)$ mit paarweise verschiedenen Kanten.

Fügt man C an der Stelle des ersten Vorkommens von u in W in den geschlossenen Kantenzug W ein, so erhält man den längeren geschlossenen Kantenzug

$$W' = (\underbrace{v_0, e_1, v_1, \ldots, u}_{W, \text{ erster Teil}} = \underbrace{u, e, u_1, \ldots, f, u_k}_{C} = \underbrace{u, \ldots, e_l, v_l = v_0}_{W, \text{ zweiter Teil}})$$

mit paarweise verschiedenen Kanten.

Das ist wegen $|E(W')| > |E(W)|$ ein Widerspruch zur Maximalität von W. □

Die im Beweis verwendete Konstruktion führt direkt auf den folgenden Algorithmus.

Algorithmus 3.5.6 (Hierholzer-/Zwiebelschalen-Algorithmus)
Eingabe: Eulerscher Graph $G = (V, E)$.
Ausgabe: Euler-Tour W.

(1) Wähle Knoten $v_0 \in V$ beliebig.

(2) Konstruiere beliebigen geschlossenen Pfad $W = (v_0, e_1, v_1, \ldots, e_l, v_l)$ mit $v_0 = v_l$ und paarweise verschiedenen Kanten.

(3) Ist $E(W) = E$:

Fertig. Gib W aus.

(4) Wähle $v_i \in V(W)$ mit $W \cap \delta(v_i) \neq \delta(v_i)$ und $e = v_i u$ mit $e \in \delta(v_i) \setminus W$.

(5) Konstruiere geschlossenen Kantenzug $W' = (v_i, e, u, \ldots, v_i)$ mit paarweise verschiedenen Kanten in $G' = (V, E \setminus E(W))$.

(6) Füge W' an erster Position von v_i in W ein.

Gehe zu (3)

Die Schritt 2 und 5 lassen sich algorithmisch sehr einfach und ähnlich einer Tiefensuche durchführen: Man startet bei v_0 bzw. v_i, läuft von dort über eine unmarkierte Kante e und markiert diese. Den dabei erreichten Knoten verlässt man wieder über eine unmarkierte Kante, die man anschließend markiert, u.s.w. Da alle Knoten in G bzw. G' einen gerade Grad haben, kann man jeden Knoten, den man dabei betritt, auch wieder verlassen – bis auf den Startknoten v_0 bzw. v_i. Diese Tiefensuche endet also zwangsläufig wieder im Startknoten und liefert somit einen geschlossenen Kantenzug mit paarweise verschiedenen Kanten.

3.6. Planare Graphen

Ein einfacher Graph ist durch seine Knoten- und Kantenmenge formal vollständig beschrieben. In vielen Fällen ist die graphische Darstellung des Graphen als Zeichnung in der Ebene jedoch zur Erkennung struktureller Eigenschaften sehr nützlich. Darüber hinaus gibt es auch zahlreiche Anwendungen wie z.B. im Leiterplatten oder Chipdesign, bei denen praxisrelevante Aspekte wie etwa Kreuzungen von Leitungen erst durch die Beschreibung der Einbettung des Graphen in die Eben erfasst werden können.

Besonders interessant sind dabei ebene Darstellungen, bei denen sich die Kanten eines Graphen überhaupt nicht kreuzen. Graphen, für die dies möglich ist, haben spezielle Eigenschaften.

Definition 3.6.1 Sei $G = (V, E)$ ein Graph.

(i) Das Tupel $\bar{G} = (V, E, p, (c_e)_{e \in E})$ heißt **ebener Graph** (oder **ebene Darstellung**) von G, wenn

- $p : V \to \mathbb{R}^2$ injektiv und
- $c_e : [0, 1] \to \mathbb{R}^2$ für jede Kante $e \in E$ ein injektiver Polygonzug

mit

(a) $\{c_e(0), c_e(1)\} = \{p(u), p(v)\}$ für alle $e = uv \in E$ (Kanten enden in Knoten)

(b) $c_e(]0, 1[) \cap p(V) = \emptyset$ (keine Knoten im Inneren)

(c) $c_e(]0, 1[) \cap c_f(]0, 1[) = \emptyset$ für alle $e, f \in E$, $e \neq f$ (keine Kreuzungen)

(Die Abbildungen p und c_e, $e \in E$, beschreiben eine „kreuzungsfreie Zeichnung von G in der Ebene“.)

(ii) G heißt **planar** (oder **plättbar**), wenn es eine planare Darstellung $\bar{G} = (V, E, p, (c_e)_{e \in E})$ gibt.

Bemerkung Die Planarität von G kann äquivalent wie folgt definiert werden:

- G hat eine kreuzungsfreie Darstellung mit geradlinigen Verbindungsstrecken für die Kanten (statt Polygonzügen)
- G hat eine kreuzungsfreie Darstellung mit allgemeinen Jordankurven für die Kanten (statt Polygonzügen)
- G hat eine kreuzungsfreie Darstellung auf der Kugeloberfläche (statt in der Ebene)
- G ist Minor eines $k \times k$-Gittergraphen (V, E) mit $V = \{1, \ldots, k\}^2 \subset \mathbb{R}^2$, $E = \{uv \mid u, v \in V,\ \|u - v\| = 1\}$

Ein Minor von G ist ein Graph, den man durch Löschen von Knoten oder Kanten oder Kontrahieren von Kanten aus G erhält. Ist G planar, so ist (leicht nachzuprüfen) auch jeder Minor von G planar.

Definition 3.6.2 Seien G und H Graphen. H heißt **Minor** von G, wenn man H durch wiederholtes

- Entfernen von Kanten oder Knoten oder
- Kontrahieren von Kanten

aus G erhält.

Definition 3.6.3 Eine ebene Darstellung eines Graphen zerlegt die Ebene in zusammenhängende **Gebiete**, wobei es genau ein unbeschränktes **äußeres Gebiet** gibt.

Bemerkung Man sieht leicht:

(i) Eine ebene Darstellung von G zerlegt die Ebene genau dann in mindestens 2 Gebiete (davon also mind. ein beschränktes inneres Gebiet), wenn G einen Kreis enthält.

(ii) Jeder Wald ist planar.

Jede ebene Darstellung eines Waldes hat nur ein, nämlich das äußere Gebiet.

Satz 3.6.4 (Eulersche Polyederformel) *Sei $G = (V, E)$ ein zusammenhängender planarer Graph, $\bar{G} = (V, E, p, (c_e)_{e \in E})$ eine beliebige ebene Darstellung von G und F die Anzahl der Gebiete dieser Darstellung. Dann gilt*

$$|F| - |E| + |V| = 2 \ .$$

(Daraus folgt insbesondere, dass jede ebene Darstellung von G die gleiche Anzahl F von Gebieten hat.)

Beweis. Induktion über $|F|$.

IAnf: $|F| = 1$.

$\Rightarrow$ nur 1 (äußeres) Gebiet

$\Rightarrow$ G ist Baum (da zusammenhängend und nach Vorüberlegung kreisfrei).

$\Rightarrow$ $|E| = |V| - 1$

$\Rightarrow$ $|F| - |E| + |V| = 1 - (|V| - 1) + V = 2$ gilt

ISchritt: Sei $G = (V, E)$ mit $|F| \geq 2$.

$\Rightarrow$ Es gibt ein inneres Gebiet.

$\Rightarrow$ G enthält einen Kreis C

Wähle $e \in C$. Offenbar trennt e zwei verschiedene Gebiete F_1 und F_2 der planaren Darstellung von G.

Betrachte $G' := G - e$ und $\bar{G}' := \bar{G} - e$, d.h. entferne e aus G und aus der ebenen Darstellung von G.

Die entstehende Darstellung $\bar{G}'$ von G'

- ist immer noch planar (Löschen von e kann keine Kreuzungen erzeugen)
- hat ein Gebiet weniger als die planare Darstellung $\bar{G}$ von G (da die Gebiete F_1 und F_2 zu einem zusammenhängendem Gebiet verschmelzen)
- hat eine Kante weniger als G.

Also gilt nach IVor für G' und $\bar{G}'$: $(|F|-1)-(|E|-1)+|V|=2$
$\Rightarrow |F|-|E|+|V|=2$ □

Aus der Eulerschen Formel erhält man viele wichtige Aussagen über planare Graphen.

Folgerung 3.6.5 *Ist $G=(V,E)$ ein planarer Graph mit $|V|\geq 3$, so existiert ein Knoten $u\in V$ mit $deg(u)\leq 5$.*

Beweis. Wir können im Beweis annehmen, dass G zusammenhängend ist. Falls G nicht zusammenhängend ist, so betrachte man eine beliebige Zusammenhangskomponente $(V_i, E(V_i))$ von G und zeige für den zugehörigen (immer noch planaren) Teilgraphen, dass eine Knoten $u\in V_i$ mit $\deg(u)\leq 5$ existiert.

Sei also G zusammenhängend.

Sei F_i die Anzahl der Gebiete, die genau i angrenzende Kanten haben, und V_i die Anzahl der Knoten mit i Nachbarn. (Jede Kante e hat zwei angrenzende Gebiete, eins auf jeder Seite. Liegt auf beiden Seiten einer Kante das gleiche Gebiet, so zählt die Kante doppelt als angrenzende Kante des Gebietes.)

Wir zählen nun die Gebiets-Kanten-Inzidenzen und die Knoten-Kanten-Inzidenzen jeweils doppelt ab:

Jedes Gebiet hat mind. 3 angrenzende Kanten, also gilt

$$|F| = |F_3| + |F_4| + \dots$$

Jede Kante wird von beiden Nachbargebieten gezählt:

$$\Rightarrow \quad 2|E| = 3|F_3| + 4|F_4| + \dots$$

Damit folgt $2|E|-3|F|\geq 0$.

Angenommen, es gilt $\deg(u)\geq 6$ für alle $u\in V$, also

$$|V| = |V_6| + |V_7| + \dots$$

Jede Kante hat genau zwei Endknoten, also gilt :

$$\Rightarrow \quad 2|E| = 6|V_6| + 7|V_7| + \dots$$

Damit folgt $2|E|-6|V|\geq 0$.

Zusammen erhält man

$$6(|E|-|V|+|F|) = 2(2|E|-3|F|) + (2|E|-6|V|) \geq 0$$

also $|E\geq |V|+|F|$. Das ist ein Widerspruch zur Euler-Formel. □

Folgerung 3.6.6 *Ist $G = (V, E)$ ein planarer Graph mit $|V| \geq 3$, so gilt $|E| \leq 3|V| - 6$*

Beweis. Wie im Beweis zuvor genügt es, die Behauptung für zusammenhängende Graphen zu zeigen.

Wie im Beweis zuvor erhält man $2|E| - 3|F| \geq 0$.

Mit der Euler-Formel $|F| - |E| + |V| = 2$ erhält man daraus

$$3|V| - 6 = 3(|V| - 2) = 3(|E| - |F|) = \underbrace{2|E| - 3|F|}_{\geq 0} + |E| \geq |E|$$

Der folgende Satz liefert eine vollständige Charakterisierung der planaren Graphen.

Satz 3.6.7 (Kuratowski) *Ein Graph $G = (V, E)$ ist genau dann planar, wenn er weder den Graphen K_5 noch den Graphen $K_{3,3}$ als Minor enthält.*

Bemerkung

- K_5 und $K_{3,3}$ sind die kleinsten nicht-planaren Graphen.
- K_5 verletzt 3.6.6 $\Rightarrow$ nicht planar
- Nachweis, dass $K_{3,3}$ nicht planar, etwas komplizierter

3.7. Knotenfärbungen

Eines der bekanntesten Resultate der Graphentheorie ist der sogenannte 4-Farben-Satz, der besagt, dass die Knoten eines planaren Graphen (bzw. jede Landkarte ohne Exklaven) so mit 4 Farben gefärbt werden können, dass dabei benachbarte Knoten (bzw. Länder mit einer gemeinsamen Grenze) verschiedene Farben haben.

Viele praktische Anwendungsprobleme, bei denen es um die konfliktfreie Nutzung gemeinsamer Ressourcen geht, lassen sich als Knotenfärbungproblem in Graphen modellieren. Typische Beispiele sind die Zuweisung von Funkkanälen zu verschiedenen, sich möglicherweise gegenseitig störenden Sendern in Mobilfunk-Netzen, die Zuweisung von Variablen auf Register in einer CPU oder die Zuweisung von Räumen, Zeiten und Lehrpersonen bei der Stundenplanung an Schulen.

Die „Farben“ werden bei diesen Färbungsproblemen i.d.R. einfach von 1 bis k durchnummeriert. Eine Knotenfärbung ist somit nichts anderes als eine Abbildung $c : V \to \{1, \ldots, k\}$. Typischerweise sucht man nach der kleinsten Anzahl von Farben, also dem minimalen k, so dass ein gegebener Graph mit diesen k Farben konfliktfrei färbbar ist.

Definition 3.7.1 Sei $G = (V, E)$ ein Graph.

(i) Ein **(Knoten-) k-Färbung** von G ist eine Abbildung $c : V \to [k] = \{1, \ldots, k\}$ mit $c(u) \neq c(v)$ für alle $uv \in E$.

(ii) Die Zahl $\chi(G) := \min\{k \in \mathbb{N} \mid G \text{ hat } k\text{-Färbung}\}$ heißt **chromatische Zahl** von G.

(iii) G heißt **k-färbbar**, wenn $\chi(G) \leq k$.

Die chromatische Zahl, also die Anzahl der mindestens benötigten Farben, lässt sich für einige einfache Graphen leicht bestimmen. Für kompliziertere Graphen erhält man mit den gleichen Überlegungen immerhin noch Abschätzungen für die chromatische Zahl.

Beobachtung 3.7.2 *Sei $G = (V, E)$.*

(i) Triviale Schranke: $\chi(G) \leq |V|$.

Bessere Schranke: $\chi(G) \leq \max\{deg(v) \mid v \in V\} + 1$

(ii) Für den vollständigen Graphen K_n mit n Knoten gilt $\chi(K_n) = n$.

(iii) $\chi(G) \leq \frac{1}{2} + \sqrt{2|E| + \frac{1}{4}}$

(iv) Für den Kreis C_n mit n Knoten gilt $\chi(C_n) = \begin{cases} 2 & \text{falls } n \text{ gerade} \\ 3 & \text{sonst} \end{cases}$ *für* $n \geq 3$

(v) $\chi(G) \geq \max\{|C| \mid C \subseteq V \text{ ist eine Clique}\}$

*$C \subseteq V$ heißt **Clique** wenn $uv \in E$ für alle $u, v \in C$, $u \neq v$.*

Beweis.

(i) (Bessere Schranke): Induktion über $|V|$:

Anfang: Für $|V| = 1$ klar.

Schritt: Wähle $u \in V$ und betrachte $G' = G - u$.

Nach Indunktionsvor. kann G' mit $\max\{\deg_{G'}(v) \mid v \in V\} + 1 \leq \max\{\deg_G(v) \mid v \in V\} + 1$ Farben gefärbt werden.

Da u nur $\deg(u)$ viele Nachbarn hat, ist eine der Farben $\{1, \ldots, \max\{\deg_G(v) \mid v \in V\} + 1\}$ von den Nachbarn von u nicht benutzt. Damit kann dann u gefärbt werden.

(ii) Offensichtlich.

(iii) Sei c eine k-Färbung mit minimalem k.

Für eine Farbe $a \in [k]$ ist $V[a] := \{v \in V \mid c(v) = a\}$ die Menge aller Knoten mit Farbe a (*Farbklasse* zu a).

Für je zwei verschiedene Farben $a \neq b$ existiert mindestens eine Kante $uv \in E$ mit $u \in V[a]$ und $v \in V[b]$, sonst wäre c keine Färbung mit minimaler Farbzahl. (Sonst könnte man alle Knoten in $V[a]$ und $V[b]$ gleich färben und würde eine Farbe sparen.)

Also: $|E| \geq \binom{k}{2} = \frac{k(k-1)}{2}$

(iv) Offensichtlich.

(v) Eine Clique $C \subseteq V$ ist ein induzierter Teilgraph $K_{|C|}$ in G.

Außerdem induziert jede beliebige Färbung c von G auch eine Färbung $c\,|_C$ auf dem Teilgraphen $K_{|C|}$.

Da nach (ii) jede Färbung von $K_{|C|}$ genau $|C|$ Farben benötigt, benötigt auch jede Färbung von G mindesten $|C|$ Farben. □

Satz 3.7.3 (Vierfarbensatz, Appel und Haken 1977) *Ist G planar, so existiert für G eine Knotenfärbung mit 4 Farben.*

Beweis. Extrem schwierig, verwendet Computerprogramm zur Verifikation sehr vieler Fälle!□

Folgerung 3.7.4 *Man kann jede Landkarte, in der die Länder zusammenhängend sind (d.h. keine Exklaven haben), mit höchstens 4 Farben so färben, dass benachbarte Länder verschiedene Farben haben.*

Beweis. Eine Färbung der Gebiete einer Landkarte entspricht einer Knotenfärbung des Graphen $G = (V, E)$ mit

- Land $u \rightsquigarrow$ Knoten $u \in V$
- gemeinsame Grenze zwischen Ländern u und $v \rightsquigarrow$ Kante $uv \in E$

Existieren keine Exklaven, so ist G planar.

Nach dem Vierfarbensatz existiert eine 4-Färbung der Knoten von G. Diese überträgt sich direkt auf eine 4-Färbung der Länder der Landkarte. □

Für die wesentlich schwächer Aussage, dass für jeden planare Graph eine 6-Färbung existiert, liefert die Euler-Formel für planare Graphen einen einfachen, konstruktiven Beweis, d.h. einen Algorithmus, der eine 6-Färbung bestimmt.

Satz 3.7.5 („Sechsfarbensatz“) *Ist G planar, so existiert für G eine Knotenfärbung mit maximal 6 Farben.*

Beweis. Basierend auf 3.6.5 kann man rekursiv eine 6 Färbung von G bestimmen:

Skizze des Induktionsbeweises über $n = |V|$, der auch einen rekursiven 6-Färbungsalgorithmus für $G = (V, E)$ liefert:

Induktionsanfang/Rekursionsende:

(1) Ist $|V| \leq 6$, färbe alle Knoten verschieden. Ende.

Induktions-/Rekursionsschritt:

(2) Wähle Knoten $u \in V$ mit $\deg(u) \leq 5$

(existiert nach 3.6.5)

(3) Färbe $G' = G - u$ mit den verfügbaren 6 Farben.

(Nach Induktionsvoraussetzung möglich, da G' auch planar ist und weniger Knoten als G enthält.)

(4) Wähle für u eine der 6 Farben, die keiner der 5 Nachbarn von u hat.

(Wegen $\deg(u) \leq 5$ ist mindestens eine der 6 Farben zulässig für u.) □

Bemerkung

- Der 6-Färbungsalgorithmus funktioniert ohne Ändern der Teilfärbung in G'.
- Mit zusätzlichem Umfärben findet man sogar Algorithmus für 5-Färbung.

A. Algebraische Grundbegriffe

Dieser Anhang enthält eine kompakte Einführung in wesentliche algebraische Grundbegriffe und -konzepte.

Literatur:

- A. Steger. Diskrete Strukturen, Kapitel 5
- T. Glosauer. Elementar(st)e Gruppentheorie

Ergänzung / Wiederholung:

- A. Beutelspacher. Mathe-Basics zum Studienbeginn, Kap. 4, 8
- R. Schulze-Pillot. Elementare Algebra und Zahlentheorie.
- Knauer, Knauer. Diskrete und algebraische Strukturen – kurz gefasst.

A.1. Gruppen

Grundlegende Begriffe und Resultate

Zunächst befassen wir uns mit einzelnen „zweistellige Rechenoperationen“ auf Mengen, sogenannten Verknüpfungen. Das sind Abbildungen ähnlich der Addition oder Multiplikation, die zwei Operanden aus der Menge auf ein Ergebnis aus der gleichen Menge abbilden. Mathematisch und algorithmisch interessant werden solche Verknüpfungen, wenn sie bestimmte Eigenschaften erfüllen, die es uns erlauben, damit zu „rechen“, also komplexere Ausdrücke aus diesen Verknüpfungen umzustellen und zu vereinfachen.

Definition A.1.1 Sei X eine Menge. Eine **Verknüpfung auf** X ist eine Abbildung $* : X \times X \to X$.

(i) $*$ heißt **assoziativ**, wenn

$$\forall x, y, z \in X : \; x * (y * z) = (x * y) * z$$

(ii) $*$ heißt **kommutativ**, wenn

$$\forall x, y, z \in X : \; x * (y * z) = (x * y) * z$$

(iii) $e \in X$ heißt **linksneutral** (bzw. **rechtsneutral**) bezüglich $*$, wenn

$$\forall x \in X : \; e * x = x \quad (\text{bzw. } \forall x \in X : \; x * e = x)$$

(iv) $e \in X$ heißt **neutral** bezüglich $*$, wenn e links- und rechtsneutral ist.

Bemerkung A.1.2 Es gibt höchstens ein neutrales Element $e \in X$ bzgl. $*$.

Beweis. Seien $e_1, e_2 \in X$ beides neutrale Elemente.

Dann folgt $\underbrace{e_1 = e_1 * e_2}_{\text{da } e_2 \text{ recht-neutal}} = \underbrace{e_1 * e_2 = e_2}_{\text{da } e_1 \text{ links-neutal}}$ □

Definition A.1.3 Sei X eine Menge mit einer Verknüpfung $*$ auf X. Das Paar $(X, *)$ heißt

(i) **Halbgruppe**, wenn $*$ assoziativ ist.

(ii) **Monoid**, wenn $*$ assoziativ ist und es ein neutrales Element $e \in X$ gibt.

Beispiel A.1.4

(a) $(\mathbb{N}_0, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ *und* $(\mathbb{C}, +)$ *sind kommutative Monoide.*

(Neutrales Element: 0*)*

(b) $(\mathbb{N}, +)$ *ist kommutative Halbgruppe, aber kein Monoid.*

(kein neutrales Element in $\mathbb{N}$*)*

(c) $(Abb(M, M), \circ)$ *ist Monoid mit neutralem Element* Id_M*.*

(Hierbei ist M *eine Menge mit* $|M| \geq 3$*,* $Abb(M, M) := \{f : M \to M\}$ *die Menge aller Abbildungen von* M *nach* M *und* $\circ$ *die Verknüpfung von Abbildungen.)*

(d) Auf $X = \{1, 2, 3\}$ *betrachten wir die Verknüpfung* $*$*, die durch die folgende* ***Verknüpfungstafel*** *definiert ist:*

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	3

(Wert für $x * y$ *steht in Zeile* x *und Spalte* y*.)*

Offensichtlich ist 1 *neutrales Element (die 1. Ergebnisspalte der Tafel entspricht genau der Spalte der linksseitigen Argumente und 1. Ergebniszeile der Tafel entspricht genau der Zeile der rechtsseitigen Argument)*

Offensichtlich ist $*$ *kommutativ (Symmetrie der Tabelle bzgl. Hauptdiag.)*

Assoziativität ist nicht offensichtlich in Verknüpfungstabelle erkennbar, diese muss immer explizit überprüft werden!

Man findet: $1 = 2 * 3 = 2 * (3 * 3) \neq (2 * 3) * 3 = 1 * 3 = 3$.

Also ist $*$ *nicht assoziativ.*

Bemerkung

- Ist klar, um welche Verknüpfung $*$ es geht, schreibt man oft X statt $(X, *)$.
- Heißt die Verknüpfung $*, \cdot, \circ$, etc. (**Multiplikative Notation**), so
  - schreibt man oft abkürzend xy statt $x * y$,
  - nennt man das neutrale Element oft e oder 1.
- Heißt die Verknüpfung $+$ etc. (**Additive Notation**), so
  - kürzt man $x + y$ nie ab,
  - nennt man das neutrale Element oft 0.

Definition A.1.5 Sei $(X, *)$ ein Monoid mit neutralem Element e. Ferner sei $x \in X$.

(i) Falls ein Element $y \in X$ mit $y * x = e$ (bzw. $x * y = e$) existiert, so nennt man y **linksinvers** (bzw. **rechtsinvers**) zu x bzgl. $*$.

(ii) Ist y links- und rechtsinvers zu x, so heißt es **invers** zu x und wird bezeichnet als $\left\{ \begin{array}{c} y = x^{-1} \\ y = (-x) \end{array} \right\}$ bei einem Monoid in $\left\{ \begin{array}{c} \text{multiplikativer} \\ \text{additiver} \end{array} \right\}$ Notation.

Bemerkung A.1.6

(i) Es gibt nicht immer zu jedem Element ein links- oder rechtsinverses Element.

(ii) Es gibt zu jedem $x \in X$ höchstens ein inverses Element y.

Beweis.

(i) Siehe Beispiel A.1.7

(ii) Seien $y_1, y_2 \in X$ beides inverse Elemente zu x.
Dann folgt $\underbrace{y_1 = y_1 * e = y_1 * (x * y_2)}_{\text{da } e \text{ neutal, } y_2 \text{ invers zu } x} = \underbrace{(y_1 * x) * y_2 = e * y_2 = y_2}_{\text{da } e \text{ neutal, } y_1 \text{ invers zu } x}$. □

Beispiel A.1.7
*Auf $X = \{1, 2, 3\}$ sei $*_{\max}$ definiert durch die **Verknüpfungstabelle***

$*_{\max}$	*1*	*2*	*3*
1	*1*	*2*	*3*
2	*2*	*2*	*3*
3	*3*	*3*	*3*

1 *ist neutrales Element (vgl. 1. Spalte/1. Zeile)*

$*_{\max}$ *kommutativ (Symmetrie der Tabelle bzgl. Hauptdiag.)*

Assoziativität gilt auch.

Welche Elemente haben ein inverses bzgl. $\max$*?*

1: ja, $1^{-1} = 1$

2,3: nein (keine 1 *in entsprechenden Zeilen/Spalten)*

Definition A.1.8

(i) Ein Monoid $(X, *)$ heißt **Gruppe**, wenn es zu jedem $x \in X$ ein inverses Element $y \in X$ gibt.

(ii) Eine Gruppe heißt **abelsch** oder **kommutative Gruppe**, wenn sie kommutativ ist.

Bemerkung A.1.9 $(X, *)$ ist also genau dann eine Gruppe, wenn

- $*$ assoziativ ist,
- es ein neutrales Element $e \in X$ gibt, und
- es zu jedem $x \in X$ ein inverses Element $x^{-1} \in X$ gibt.

Beispiel A.1.10

(a) $(\mathbb{N}_0, +)$ *ist keine Gruppe. Kein Element außer* 0 *hat ein Inverses.*

$(\mathbb{Z}, \cdot)$ *ist keine Gruppe. Kein Element außer* $1, -1$ *hat ein Inverses.*

(b) $(\mathbb{Z}, +)$ *ist Gruppe mit neutr. Element* 0*. Jedes Element hat Inverses.*

$(\mathbb{Q} \setminus \{0\}, \cdot)$ *ist Gruppe mit neutr. Element* 1*. Jedes Element hat Inverses.*

Für eine Menge M sei

$$S(M) := \underbrace{\{\sigma : M \to M \mid \sigma \text{ is bijektiv}\}}_{\text{Menge der Permutationen auf } M} .$$

Dann ist

$$\circ : \underbrace{S(M) \times S(M) \to S(M),\ (\sigma, \eta) \mapsto \sigma \circ \eta}_{\text{Hintereinanderausführung der Abbildungen}}$$

eine Verknüpfung auf $S(M)$.

Satz A.1.11 *$(S(M), \circ)$ ist eine Gruppe, genannt die **symmetrische Gruppe** auf M.*

Beweis.

- Assoziativ: (Vgl. FGI Abbildungen)

  Es gilt für alle (passend verknüpfbaren) Abbildungen $f \circ (g \circ h) = (f \circ g) \circ h$.
- Neutrales Element:

  $Id_M : x \mapsto x$ ist neutrales Element, denn $Id_M \circ \sigma = \sigma = \sigma \circ Id_M$ für alle $\sigma \in S(M)$
- Inverse Elemente:

  Sei $\sigma \in S(M)$ beliebig.

  Da $\sigma : M \to M$ bijektiv ist, existiert auch eine Umkehrabbildung $\eta : M \to M$, so dass $\forall x \in M : \ \eta(\sigma(x)) = x = \sigma(\eta(x))$.

  Also $\eta \circ \sigma = Id_M = \sigma \circ \eta$.

  Außerdem ist auch η bijektiv, somit hat σ das Inverse $\eta \in S(M)$. □

Bemerkung A.1.12

- Für $n \in \mathbb{N}$ schreibt man $S_n := S(\{1, \dots, n\})$.

  Dies ist eine Gruppe mit $|S_n| = n!$ vielen Elementen.

  Die Elemente von S_n sind die Permutationen von $\{1, \dots, n\}$.
- Für $n \geq 3$ ist $(S_n, \circ)$ nicht kommutativ:

  Betrachte $\sigma = (1\ 2\ 3)$ und $\tau = (1\ 2)$.

  Dann ist $\sigma \circ \tau \neq \tau \circ \sigma$, denn

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

Beispiel A.1.13 *$GL(2) := \{A \in \mathbb{R}^{2,2} \mid \det A \neq 0\}$ bildet zusammen mit der Matrixmultiplikation $\cdot$ die Gruppe $(GL(2), \cdot)$.*

- *Assoziativität: folgt aus Assoz. der Matrixmultiplikation*
- *Neutrales Element: Einheitsmatrix* $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- *Inverses Element zu $A \in GL(2)$: Inverse Matrix A^{-1}*

  (wegen $\det A \neq 0$ sind alle $A \in GL(2)$ invertierbar)

  Offenbar gilt $A^{-1} \in GL(2)$ und $AA^{-1} = E = A^{-1}A$
- *Aber: Matrix-Multiplikation ist nicht kommutativ, also keine abelsche Gruppe*

Eine wesentliche Eigenschaft von Gruppen ist, dass zu jedem Element ein eindeutiges Inverses existiert.

- Damit kann man in Ausdrücken „kürzen“.
- Damit kann man einfache Gleichung auflösen.

Satz A.1.14 (Kürzungsregel) *Sei $(X, *)$ eine Gruppe. Für alle „Variablen“ $x, y \in X$ und alle „Parameter“ $a, b \in X$ gilt*

(i) $a * x = a * y \quad \Rightarrow \quad x = y$
$x * a = y * a \quad \Rightarrow \quad x = y$

(ii) *$a * x = b$ hat eine eindeutige Lösung, nämlich $x = a^{-1} * b$.*
$x * a = b$ hat eine eindeutige Lösung, nämlich $x = b * a^{-1}$.

Beweis.

(i) $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$

(ii) Geht analog. □

Bemerkung A.1.15

(i) Der Satz besagt, dass für jedes $a \in X$ die folgenden Abbildungen bijektiv sind:

$$\tau_{l,a} : X \to X,\ x \mapsto a * x \qquad \text{(Linkstranslation um } a\text{)}$$
$$\tau_{r,a} : X \to X,\ x \mapsto x * a \qquad \text{(Rechtstranslation um } a\text{)}$$

(ii) Eine endliche Halbgruppe $(X, *)$ ist genau dann eine Gruppe, wenn die Kürzungsregeln gelten.

(D.h. wenn jedes Element von X in jeder Zeile und in jeder Spalte der Verknüpfungstafel jeweils genau einmal vorkommt.)

Satz A.1.16 *Sei $(X, *)$ eine (multiplikative) Gruppe und seien $a, b \in X$. Dann gilt*

(i) $(a^{-1})^{-1} = a$

(ii) $(ab)^{-1} = b^{-1}a^{-1}$

Beweis. Zur Übung selbst machen. □

Untergruppen

Innerhalb einer Gruppe $(G, *)$ kann es Teilmengen $H \subseteq G$ geben, die bezüglich Verknüpfung $*$ in sich abgeschlossen sind, d.h. invertiert oder verknüpft man beliebige Elemente aus H miteinander,

so erhält man als Ergebnis auch wieder nur Elemente aus H. Zum Beispiel bilden die geraden Zahlen innerhalb der Gruppe $(\mathbb{Z}, +)$ eine solche bezüglich der Addition $+$ in sich abgeschlossen Menge: Summen und Inverse (hier also Negative) von geraden Zahlen sind wieder gerade Zahlen. Die geraden Zahlen bilden mit der von den ganzen Zahlen „vererbten“ Verknüpfung der Addition ein (kleinere) Gruppe, eine sogenannte Untergruppe von $(\mathbb{Z}, +)$.

Definition A.1.17 Sei $(G, *)$ eine Gruppe.

$H \subseteq G$ heißt **Untergruppe** von G, falls H zusammen mit der Verknüpfung $*$ selbst wieder eine (bzgl. * abgeschlossene) Gruppe ist.

Man schreibt $H \leq G$ bzw. $H < G$.

Bemerkung Genauer: $(H, * |_{H \times H})$ muss selbst eine Gruppe sein, wobei

$$* |_{H \times H} \colon H \times H \to G, (a, b) \mapsto a * b$$

die Einschränkung der auf G definierten Abbildung $*$ auf H ist. Dazu muss das Bild von $H \times H$ unter der Verknüpfung $*$ wieder in H liegen, also ist $* |_{H \times H}$ tatsächlich eine Abbildung nach $H \subseteq G$.

Beispiel A.1.18

(a) $(\mathbb{Z}, +)$ *und* $(\mathbb{Q}, +)$ *sind Untergruppen von* $(\mathbb{R}, +)$

(b) $(\mathbb{N}, +)$ *ist keine Untergruppe von* $(\mathbb{Z}, +)$*: Für* $2 \in \mathbb{N}$ *liegt das Inverse* -2 *nicht in* $\mathbb{N}$.

Satz A.1.19 *Sei* $(G, *)$ *eine Gruppe.* $H \subseteq G$ *ist genau dann eine Untergruppe von* G*, wenn*

(i) $H \neq \emptyset$

(ii) $a * b \in H$ *für alle* $a, b \in H$

(iii) $a^{-1} \in H$ *für alle* $a \in H$

Beweis.

$\Rightarrow$ Zeige: Wenn H Untergruppe, dann gelten (i)-(iii)

- Da H mit $*|_{H \times H}$ eine Gruppe ist, gilt insbesondere $* |_{H \times H} \colon H \times H \to H$ statt $* |_{H \times H} \colon H \times H \to G$.

  Also $a * b \in H$ für alle $a, b \in H$ d.h. (ii) gilt.

- H hat als Gruppe neutrales Element.

  Also $e_H \in H$ und $H \neq \emptyset$, d.h. (i) gilt.

– Wir zeigen zunächst $e_H = e$, d.h. e_H ist das neutrale Element von G:

Wegen $H \subseteq G$ gilt $e_H \in G$.

Also hat e_H Inverses $e_H^{-1} \in G$.

Es gilt $e_H = e * e_H = (e_H^{-1} * e_H) * e_H = e_H^{-1} * \underbrace{(e_H * e_H)}_{=e_H, \text{ da } e_H \text{ neutral}} = e_H^{-1} * e_H = e$

– Sei nun $a \in H$.

a hat Inverses $a_H \in H$.

Da in G $a_H * a = e_H = e$ gilt, folgt $a_H = a^{-1}$ (Eindeutigkeit des Inversen in G!)

Also $a^{-1} \in H$, d.h. (iii) gilt.

$\Leftarrow$ Zeige: Wenn (i)-(iii) gelten, dann ist H Untergruppe.

– Wegen (ii) ist auf H die Verknüpfung $* : H \times H \to H, (a, b) \mapsto a * b$ wohldefiniert.

Die Assoziativität vererbt sich von $*$ auf G.

– Wegen (i) gibt es ein $a \in H$.

Also gilt wegen (iii) $a^{-1} \in H$ und wegen (ii) $a^{-1} * a = e \in H$.

Da e bereits in G neutrales Element ist, ist e auch in H neutral.

– Wegen (iii) hat jedes $a \in H$ Inverses in H. $\square$

Beispiel A.1.20

(a) *Für* $k \in \mathbb{N}$ *ist* $k\mathbb{Z} := \{kn \mid n \in \mathbb{Z}\}$ *(alle Vielfachen von* k*) Untergruppe von* $(\mathbb{Z}, +)$.
Man prüft (i)-(iii) leicht nach: ...

(b) *Betrachte* $\mathbb{Z} + i\mathbb{Z} := \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ ***(ganze Gaußsche Zahlen)***
Mit Addition ist $(\mathbb{Z} + i\mathbb{Z}, +)$ *Untergruppe von* $(\mathbb{C}, +)$

(c) *Betrachte* $A_n := \{\sigma \in S_n \mid sign(\sigma) = 1\}$ ***(alternierende Gruppe)***
(=Menge der Permutationen mit gerader Anzahl von Transpositionen)
Mit Komposition $\circ$ *ist* $(A_n, \circ)$ *eine Untergruppe von* $(S_n, \circ)$

(d) $GL(n) := \{A \in \mathbb{R}^{n,n} \mid \det A \neq 0\}$ ***(allgemeine lineare Gruppe)***
$O(n) := \{A \in GL(n) \mid$ *A ist orthogonal*$\}$ ***(orthogonale Gruppe)***
(im $\mathbb{R}^3$ *entsprechen die orthogonalen Matrizen den Drehungen und Drehspiegelungen mit Achsen durch* 0*-Punkt)*
$SO(n) := \{A \in O(n) \mid \det(A) = 1\}$ ***(spezielle orthogonale Gruppe)***
(im $\mathbb{R}^3$ *entsprechen die speziellen orthogonalen Matrizen den Drehungen um Achsen durch* 0*-Punkt)*
Mit Matrixmultiplikation als Verknüpfung gilt $SO(n) < O(n) < GL(n)$

Alternative Charakterisierung von Untergruppen:

Satz A.1.21 *Sei* $(G, *)$ *eine Gruppe.* $\emptyset \neq H \subseteq G$ *ist genau dann eine Untergruppe von* G*, wenn für alle* $a, b \in H$ *auch* $a * b^{-1} \in H$ *gilt.*

Beweis. Übung. Benutze Satz A.1.19. □

Satz A.1.22 *Seien* H_i*,* $i \in I$*, Untergruppen von* $(G, *)$*. Dann ist auch* $\left(\bigcap_{i \in I} H_i\right)$ *eine Untergruppe von* G*.*

Beweis. Benutze Satz A.1.21. □

Beispiel A.1.23

$H_1 := \{x \in \mathbb{C} \mid |x| = 1\}$ *ist UG von* $(\mathbb{C} \setminus \{0\}, \cdot)$
$H_2 := \{a + bi \in \mathbb{C} \setminus \{0\} \mid a = 0$ *oder* $b = 0\}$ *ist UG von* $(\mathbb{C} \setminus \{0\}, \cdot)$
(Nachweise in Übung!)
Also ist auch $H_1 \cap H_2 = \{1, -1, i, -i\}$ *eine Untergruppe von* $(\mathbb{C} \setminus \{0\}, \cdot)$.

Definition A.1.24 Sei G eine Gruppe. Für $M \subseteq G$ ist

$$< M >= Erz(M) := \bigcap_{H \leq G:\, M \subseteq H} H$$

eine Untergruppe von G, genannt die **von M erzeugte Gruppe**.

Satz A.1.25 *Für $M \subseteq G$ ist*

$$< M >= \left\{ a = b_1 * \ldots * b_n \mid n \in \mathbb{N} \text{ und } (b_i \in M \text{ oder } b_i^{-1} \in M) \right\}.$$

($< M >$ ist Menge aller a, die sich als endliches Produkt von Elementen oder Inversen von Elementen aus M schreiben lassen.)

Definition A.1.26 Eine Gruppe G heißt

(i) **endlich erzeugt**, wenn es $M \subset G$ mit $|M| < \infty$ und $G =< M >$ gibt,

(ii) **zyklische Gruppe**, wenn es ein $a \in G$ mit $G =< \{a\} >$ gibt.

Definition A.1.27 Sei G eine Gruppe.

(i) $ord(G) := |G|$ heißt die **Ordnung der Gruppe** G.

(ii) Für $a \in G$ heißt $ord(a) := ord(< \{a\} >)$ die **Ordnung des Elements** a.

Beispiel A.1.28

(a) Für $(\mathbb{Z}, +)$ und $5 \in \mathbb{Z}$ ist

$$< \{5\} >:= \{k5 \mid k \in \mathbb{Z}\} = \{\ldots, -10, 5, 0, 5, 10, \ldots\}$$

die von 5 erzeugte Untergruppe von $(\mathbb{Z}, +)$.

$< \{5\} >$ ist endlich erzeugt und zyklische Gruppe.

(b) Für $(\mathbb{Z}, +)$ und $\{6, 8\} \in \mathbb{Z}$ ist

$$< \{6, 8\} >:= \{k6 + l8 \mid k, l \in \mathbb{Z}\} = \{\ldots, -4, 2, 0, 2, 4, \ldots\}$$

die von $\{6, 8\}$ erzeugte Untergruppe von $(\mathbb{Z}, +)$.

$< \{6, 8\} >$ ist endlich erzeugt und zyklische Gruppe, denn $< \{6, 8\} >=< \{2\} >$.

(c) Für $(\mathbb{Z}+i\mathbb{Z},+)$ und $\{6+2i, 8+2i\} \subset \mathbb{Z}+i\mathbb{Z}$ ist

$$< \{6+2i, 8+2i\} >:= \{k(6+2i)+l(8+2i) \mid k,l \in \mathbb{Z}\}$$

eine endlich erzeugte Untergruppe, aber nicht zyklisch.

$< \{6+2i, 8+2i\} >=< \{2, 2i\} >$ *ist ein Teilgitter der ganzen Gaußschen Zahlen.*

(d) Für $n \in \mathbb{N}$ sei σ die Permutation $\sigma = (1\ 2\ \ldots n)$ und

$$Z_n := \{Id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\} \subseteq S_n.$$

$(Z_n, \circ)$ ist Untergruppe von $(S_n, \circ)$.

*$(Z_n, \circ)$ heißt **zyklische Gruppe der Ordnung** n.*

Z_n entspricht den Drehsymmetrien eines regulären n-Ecks.

Satz A.1.29 *Alle Untergruppen von $(\mathbb{Z},+)$ sind zyklisch.*
Anders ausgedrückt: Für jede Untergruppe $U \leq \mathbb{Z}$ existiert ein $k \in \mathbb{N}_0$, so dass $U = k\mathbb{Z}$.

Beweis.

- Sei $U < \mathbb{Z}$ eine UG.
- Gilt $U = \{0\}$, so ist $U = 0\mathbb{Z}$.
- Sei also $U \neq \{0\}$.
  Setze $k := \min\{u \in U \mid u > 0\}$.
- **Beh:** $U = k\mathbb{Z}$
- $\supseteq$: klar
- $\subseteq$: Sei $u \in U$.
  Dann $u = qk + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < k$. (Division mit Rest)
  Also $r = u - qk = \underbrace{u}_{\in U} + \overbrace{\underbrace{(-k)}_{\in U} + \cdots + \underbrace{(-k)}_{\in U}}^{q \text{ mal}} \in U$.
  Wegen $0 \leq r < k$ und Minimalität von k folgt $r = 0$, also $u = qk \in k\mathbb{Z}$. □

Bemerkung

Satz A.1.29 gilt nicht nur für Untergruppen von $(\mathbb{Z},+)$, sondern allgemein für alle Untergruppen einer zyklischen Gruppe. Er lautet dann wie folgt:

Ist U eine Untergruppe einer zyklischen Gruppe G, so ist U auch zyklisch.

Beweisen kann man die allgemeine Form mit Hilfe der Techniken des folgenden Kapitels.

Gruppen-Homomorphismen

Hat man zwei Gruppen, eine bestehen aus der Menge G mit der Verknüpfung $*$ und eine aus der Menge H mit der Verknüpfung $\cdot$, stellt sich in einigen Situationen die Frage, ob die beiden Gruppen nicht „eigentlich gleich“ sind, und zwar in dem Sinne, dass lediglich die Elemente und die Verknüpfung umbenannt wurden. Dann genügt es natürlich, die Strukturen einer der Gruppen zu verstehen, um beide verstanden zu haben. Eine etwas schwächere Frage ist, ob eine Gruppe nicht „eigentlich“ eine Untergruppe der anderen ist, also die Elemente und die Verknüpfung wieder einfach umbenannt werden können, um diese als Untergruppe in der zweiten Gruppe wiederzufinden. Der Schlüssel zur Beantwortung dieser Fragen sind Abbildungen zwischen den Gruppen, die mit jeweiligen Verknüpfungen „kompatibel“ sind, sogenannte Homomorphismen.

Definition A.1.30 Seien $(G, *)$ und $(H, \cdot)$ Gruppen.

(i) Eine Abbildung $\phi : G \to H$ heißt **Gruppenhomomorphismus**, falls gilt

$$\forall a, b \in G : \ \phi(a * b) = \phi(a) \cdot \phi(b).$$

(ii) Ist ϕ außerdem bijektiv, so heißt ϕ **Gruppenisomorphismus**.
G und H heißen dann **isomorph**, geschrieben $G \simeq H$.

(iii) Die Menge $\ker(\phi) := \phi^{-1}(\{e_H\}) = \{x \in G \mid \phi(x) = e_H\}$ heißt **Kern** von ϕ.

Bemerkung

- morphe: Gestalt, Form homo-: gleich, ähnlich iso-: gleich, identisch
- Isomorphe Gruppen „verhalten“ sich identisch, d.h. sie unterscheiden sich nur in der Bezeichnung der Elemente und der Verknüpfung.

Beobachtung A.1.31 *Ist $\phi : G \to H$ Gruppenhomomorphismus, so gilt*

(i) $\phi(e_G) = e_H$

(ii) $\phi(a^{-1}) = (\phi(a))^{-1}$ *für alle* $a \in G$

(iii) Ist ϕ bijektiv, so ist auch $\phi^{-1} : H \to G$ ein Gruppenisomorphismus.

Beweis.

(i) Es gilt $\phi(e_G) = \phi(\underbrace{e_G * e_G}_{=e_G, \text{ da } e_G \text{ neutral}}) = \phi(e_G) \cdot \phi(e_G)$.

Damit folgt $\phi(e_G) = \underbrace{\phi(e_G)^{-1} \cdot \phi(e_G)}_{=e_h} \cdot \phi(e_G) = \phi(e_G)^{-1} \cdot \underbrace{\phi(e_G)}_{=\phi(e_G)\cdot\phi(e_G)} = e_H$.

(ii) Ähnlich.

(iii) Bijektiv: offensichtlich. Homo-Eigenschaft: Einsetzen von $a' = \phi(a)$ und $b' = \phi(b)$. □

Beispiel A.1.32

(a) $\phi : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$ *ist ein Gruppenhomomorphismus von* $(\mathbb{Z}, +)$ *nach* $(\mathbb{Z}, +)$*, denn*

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b) \qquad \forall a, b \in \mathbb{Z}$$

(b) $exp : \mathbb{R} \to \mathbb{R}_{>0}, x \mapsto e^x$ *ist ein Gruppenisomorphismus zwischen den Gruppen* $(\mathbb{R}, +)$ *und* $(\mathbb{R}_{>0}, \cdot)$*, denn exp ist bijektiv und*

$$exp(x + y) = e^{x+y} = e^x \cdot e^y = exp(x) \cdot exp(y) \quad \forall x, y \in \mathbb{R}$$

Der Kern ist $\ker(exp) = \{x \in \mathbb{R} \mid e^x = 1\} = \{0\}$.

(c) $\|.\| : \mathbb{C} \setminus \{0\} \to \mathbb{R} \setminus \{0\}, x \mapsto \|x\|$ *ist ein Gruppenhomomorphismus zwischen den Gruppen* $(\mathbb{C} \setminus \{0\}, \cdot)$ *und* $(\mathbb{R} \setminus \{0\}, \cdot)$*, denn*

$$\|x \cdot y\| = \|x\| \cdot \|y\|.$$

Der Kern ist $\ker(\phi) = \{x \in \mathbb{C} \mid \|x\| = 1\}$.

(d) Für $n \in \mathbb{N}$ hatten wir die zyklische Gruppe $(Z_n, \circ) \leq S_n$ definiert.

Alternativ betrachten wir $[n]' = \{0, \ldots, n-1\}$ mit der Verknüpfung

$$+ : [n]' \times [n]' \to [n]', (a, b) \mapsto \text{„Rest von } a + b \text{ bei Division durch } n\text{“}$$

Dann sind $(Z_n, \circ)$ und $([n]', +)$ isomorph:

Der kanonischen Isomorphismus ist $\phi : Z_n \to [n]', \sigma^k \mapsto k$.

($\sigma^k \in Z_n$ entspricht $k \in [n]'$, $\circ$ entspricht $+$)

$\ker(\phi) = \{\rho \in Z_n \mid \phi(\rho) = 0\} = \{Id\}$

(e) Wir betrachten die Gruppen $G = H = \mathbb{R}^2$ zusammen mit der Vektoraddition $+$

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 + x_2 \\ 0 \end{pmatrix}$$

f ist Gruppenhomomorphismus (nachrechnen!)

Bild$(f) = \{\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{R}^2 \mid z_2 = 0 \in\} = \{\begin{pmatrix} z \\ 0 \end{pmatrix} \mid z \in \mathbb{R}\}$ *ist offenbar Untergruppe (und Untervektorraum) von* $\mathbb{R}^2$

$\ker(f) = \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \mid x_1 + x_2 = 0\}$ *ist offenbar Untergruppe (und Untervektorraum) von* $\mathbb{R}^2$

Satz A.1.33 *Seien $(G, *)$, $(H, \cdot)$ Gruppen und $\phi : G \to H$ ein Gruppenhomomorphismus.*

(i) U Untergruppe von G $\Rightarrow$ $\phi(U)$ Untergruppe von H

(ii) V Untergruppe von H $\Rightarrow$ $\phi^{-1}(V)$ Untergruppe von G

Beweis.

(i) Wegen $e_G \in U$ folgt $e_H = \phi(e_G) \in \phi(U)$, also $\phi(U) \neq \emptyset$.

Für alle $a, b \in \phi(U)$ existieren $c, d \in U$ mit $\phi(c) = a$ und $\phi(d) = b$.

Wegen Homomorphie-Eigenschaft gilt dann auch

$a \cdot b = \phi(c) \cdot \phi(d) = \phi(\underbrace{c * d}_{\in U}) \in \phi(U)$ und $a^{-1} = \phi(c)^{-1} = \phi(\underbrace{c^{-1}}_{\in U}) \in \phi(U)$.

Also ist $\phi(U)$ in H abgeschlossen bzgl. $\cdot$.

(ii) analog. □

Folgerung A.1.34 *Seien $(G, *)$, $(H, \cdot)$ Gruppen und $\phi : G \to H$ ein Gruppenhomomorphismus.*

(i) Bild(ϕ) ist Untergruppe von H.

(ii) $\ker(\phi)$ ist Untergruppe von G.

Kongruenzen und Faktorgruppen

In Kapitel 1.2 haben wir Restklassen modulo m eingeführt, indem wir zunächst die Äquivalenzrelation der Kongruenz modulo m ($\equiv_m$) auf der Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen definiert und dann die Menge der entstehenden Äquivalenzklassen zusammen mit der von den ganzen Zahlen

auf diese Klassen „vererbten“ Addition betrachtet haben. Wir haben gesehen, dass wir so eine neue Gruppe erhalten haben. Die Elemente der Äquivalenzklasse $[0]_m$ des neutralen Elements 0 bezüglich der betrachteten Verknüpfung $+$ haben dabei außerdem ein Untergruppe der zu Grunde liegenden Gruppe $(\mathbb{Z}, +)$ gebildet.

Diese Konstruktion lässt sich leicht verallgemeinern. Dazu definiert man die Äquivalenzrelation „kongruent“ auf einer beliebigen Gruppe G von vornherein auf Basis einer Untergruppe U von G.

Definition A.1.35 Sei $(G, +)$ eine Gruppe, U eine Untergruppe von G und $x, y \in G$. Wir nennen x **kongruent zu** y **modulo U**, geschrieben $x \equiv_U y$, falls $x + (-y) \in U$.

Die zugehörige Relation $\equiv_U \subseteq G \times G$

$$x \equiv_U y \quad :\Leftrightarrow \quad x + (-y) \in U \qquad x, y \in G$$

heißt **Kongruenzrelation modulo** U.

Bemerkung Alternative Schreibweisen sind

$$x \equiv y \mod U \quad \text{oder} \quad x \equiv y \ (U)$$

Für $G = \mathbb{Z}$ und $U = k\mathbb{Z}$ schreibt man oft einfach $x \equiv y \mod k$ (statt $\mod k\mathbb{Z}$).

Beispiel A.1.36

(a) $5 \equiv 47 \mod 7$, *da* $5 - 47 = -42 = -6 \cdot 7$ *Alternative Sicht:* $Rest(5:7) = 5 = Rest(47:7)$

(b) $5 \not\equiv 15 \mod 7$, *da* $5 - 15 = -10 \notin 7\mathbb{Z}$

Konvention

Als Ergebnisse bei Kongruenzen modulo $k\mathbb{Z}$ werden meist Zahlen $r \in \{0, 1 \ldots, k-1\}$ angegeben, nämlich genau Rest$(Ergebnis : k)$. $10017 + 315 \equiv 10332 \mod 10$ stimmt zwar, besser ist aber $10017 + 315 \equiv 2 \mod 10$.

Beim Rechnen mit Kongruenzen kann es jedoch sinnvoll sein, statt mit betragsmäßig relativ großen Resten mit den äquivalenten, aber betragsmäßig kleineren negativen Resten zu rechnen, also z.B. mit -1 anstelle von $k - 1$ (siehe weiter unten). Dies geht, da die Kongruenz modulo $k\mathbb{Z}$ eine Äquivalenzrelation ist.

Satz A.1.37 *Sei $(G, +)$ eine Gruppe und U eine UG von G.*

(i) *$\equiv_U$ ist eine Äquivalenzrelation.*

(ii) *Ist G kommutativ, so gilt*

$$\forall x, x', y, y' \in G: \ (x \equiv_U x' \ \wedge \ y \equiv_U y') \ \Rightarrow \ x + y \equiv_U x' + y' \ .$$

Beweis.

(i)
- Reflexivität:

  Offensichtlich gilt für alle $x \in G$ $x + (-x) = 0 \in U$, also $x \equiv_u x$
- Symmetrie:

  Für alle $x, y \in G$ gilt: $x \equiv_U y \Leftrightarrow x + (-y) \in U \Leftrightarrow -(x + (-y)) \in U \Leftrightarrow y + (-x) \in U \Leftrightarrow y \equiv_U x$
- Transitivität:

  Für alle $x, y, z \in G$ mit $x \equiv_U y$ und $y \equiv_U z$ gilt: $x + (-y) \in U$, $y + (-z) \in U \Rightarrow x + (-y) + (y) + (-z) = x + (-z) \in U \Rightarrow x \equiv_U z$

(ii) Einsetzen! □

Definition A.1.38 Sei $(G, +)$ eine kommutative Gruppe und U eine Untergruppe von G.

Für $x \in G$ bezeichnen wir mit

$$[x] = [x]_U := \{y \in G \mid x \equiv_U y\} = \{y \in G \mid x + (-y) \in U\} = U + x$$

die Äquivalenzklasse von x bezüglich $\equiv_U$.

Die Menge

$$G/U \ := \ G/\equiv_U \ = \ \{[x]_U \mid x \in G\}$$

heißt die **Faktormenge** von G und U.

Wir definieren auf G/U die Verknüpfung $+ : G/U \times G/U \to G/U$ durch

$$[x]_U \underbrace{+}_{+ \text{ auf } G/U} [y]_U := [x \underbrace{+}_{+ \text{ auf } G} y]_U \ . \qquad (*)$$

Bemerkung

$+$ auf G/U ist wohldefiniert, d.h. unabhängig von der Wahl der Repräsentanten der Äquivalenzklassen:

Seien $x, x' \in [x]$ und $y, y' \in [y]$.

Dann gilt $x \equiv_U x'$ und $y \equiv_U y'$, also auch $x + y \equiv_U x' + y'$.

Somit $[x + y] = \{z \in G \mid z \equiv_U x + y\} = \{z \in G \mid z \equiv_U x' + y'\} = [x' + y']$.

Satz A.1.39 *Sei $(G, +)$ eine kommutative Gruppe und U eine UG von G. Dann ist auch $(G/U, +)$ eine kommutative Gruppe, genannt* ***Faktorgruppe von G nach U****.*

(Das neutrale Element ist $[0]_U$. Das inverse Element zu $[x]_U$ ist $[-x]_U$.)

Beweis. Einfach Gruppenaxiome mit Hilfe von (*) nachrechnen! □

Beispiel A.1.40 *Für $k \in \mathbb{N}$ haben wir mit genau diesem Vorgehen die kommutative Gruppe $(\mathbb{Z}/k\mathbb{Z}, +)$ der Restklassen bei Division durch k definiert.*

$(\mathbb{Z}/k\mathbb{Z}, +)$ ist zyklische Gruppe mit $\mathbb{Z}/k\mathbb{Z} =< [1]_{k\mathbb{Z}} >$.

Für $k = 3$: $(\mathbb{Z}/3\mathbb{Z}) = \{[0], [1], [2]\}$

Verknüpfungstafel:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Bemerkung A.1.41

Für nicht-kommutative Gruppen $(G, +)$ wird alles etwas komplizierter:

- $x + U := \{x + u \mid u \in U\}$ heißt **Linksnebenklasse** von x zu U. $U + x := \{u + x \mid u \in U\}$ heißt **Rechtsnebenklasse** von x zu U.
- U heißt **Normalteiler**, wenn für alle $x \in G$ gilt $x + U = U + x$.

  (Ist G kommutativ, so ist jede Untergruppe U automatisch ein Normalteiler.)
- $x \equiv_U y$ bleibt defininiert durch $x \equiv_U y \Leftrightarrow x + (-y) \in U$.

  Es gilt trotzdem $x \equiv_U y \;\Leftrightarrow\; y \equiv_U x$.

  Äquivalenzklassen $[x]_U = U + x$ sind (nur) Rechtsnebenklassen.
- $U \setminus G$ ist dann die Menge der Rechtsnebenklassen bzgl. U. G/U ist dann die Menge der Linksnebenklassen bzgl. U.
- Die Verknüpfung $+$ auf der Faktorgruppe G/U wird wie bisher definiert, aber nur noch für die Normalteiler U von G.

Der folgende Satz von Lagrange ermöglicht es uns festzustellen, welche Teilmengen einer endlichen Gruppe $(G, +)$ allein aufgrund ihrer Größe (=Ordnung) überhaupt als Untergruppen von $(G, +)$ in Frage kommen.

Satz A.1.42 (Satz von Lagrange) *Sei $(G, +)$ eine endliche Gruppe und U eine Untergruppe von G. Dann gilt*

$$|G| = |G/U| \cdot |U| \ .$$

Insbesondere ist $|G|$ durch $|U|$ teilbar.

Beweis. (Beweis nur für den Sonderfall, dass G kommutativ.)

Nach Satz A.1.37 ist $\equiv_U$ eine Äquivalenzrelation.

Somit gilt $|G| = \sum_{M \in G/U} |M|$.

Für jede Äquivalenzklasse $M \in G/U$ ist von Form

$$M = [x]_U = \{y \in G \mid y \equiv_U x\} = \{y \mid y - x \in U\} = U + x \quad \text{für ein festes } x \in M.$$

Also $|M| = |U|$ für alle $M \in G/U$.

Also $|G| = \sum_{M \in G/U} |M| = \sum_{M \in G/U} |U| = |G/U| \cdot |U|$. □

Beispiel A.1.43

Frage: Welche Untergruppen hat $(\mathbb{Z}/7\mathbb{Z}, +)$?

Wegen des Satzes von Lagrange gilt für jede Untergruppe $U < \mathbb{Z}/7\mathbb{Z}$ dass $|U|$ ein Teiler von $|\mathbb{Z}/7\mathbb{Z}| = 7$ ist.

Da 7 eine Primzahl ist, sind nur Untergruppen der Ordnung 1 und 7 möglich. Die einzigen möglichen Untergruppen dieser Größen sind die beiden Gruppen $\{[0]\}$ und $\mathbb{Z}/7\mathbb{Z}$.

Der folgende Isomorphiesatz besagt – vereinfacht formuliert – dass sich jeder Gruppenhomomorphismus f zwischen zwei Gruppen G und H zerlegen lässt in $f = f_2 \circ f_1$, wobei f_1 eine Abbildung von G in die Faktorgruppe $G/ker(f)$ ist, bei der jedes $x \in G$ auf seine Äquivalenzklasse in $G/ker(f)$ projiziert wird (d.h. der „nicht injektive“ Kern von f herausfaktorisiert wird), und f_2 eine injektive Abbildung von der Faktorgruppe $G/ker(f)$ nach H. Schränkt man den Wertebereich der zweiten Abbildung f_2 zusätzlich auf den Bereich der tatsächlich angenommenen Werte $Bild(f) = Bild(f_2)$ ein, so ist die durch diese Einschränkung entstehende Abbildung $\bar{f}$ sogar bijektiv.

Satz A.1.44 (Isomorphiesatz) *Seien $(G, +)$ und $(H, \oplus)$ Gruppen und $f : G \to H$ ein Gruppenhomomorphismus. Dann ist*

$$\bar{f} : G/\ker(f) \to Bild(f),\ [x]_{\ker(f)} = x + \ker(f) \mapsto f(x)$$

ein Gruppenisomorphismus. Insbesondere ist $G/ker(f) \simeq f(G)$.

Beispiel A.1.45

(a) Fortsetzung Bsp A.1.32 (e):

$$Bild(f) = \{\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{R}^2 \mid z_2 = 0\} = \{\begin{pmatrix} z \\ 0 \end{pmatrix} \mid z \in \mathbb{R}\}$$

$$\ker(f) = \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 \mid x_1 + x_2 = 0\} =: U$$

$$\begin{aligned}\mathbb{R}^2/\ker(f) =& \{[x]_U \mid x \in \mathbb{R}^2\} = \{(U+x) \mid x \in \mathbb{R}^2\} = \{(U+n) \mid n \in \mathbb{R}^2, n \perp U\} \\ =& \{(U + \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix}) \mid \lambda \in \mathbb{R}\}\end{aligned}$$

Die Verknüpfung $\oplus$ *auf* $\mathbb{R}^2/U$ *wird von* $+$ *auf* $\mathbb{R}^2$ *„geerbt“, also*

$$(U+x) \oplus (U+y) := (U + (x+y)) \ .$$

Damit ist $(\mathbb{R}^2/\ker(f), \oplus) \simeq (\mathbb{R}, +) \simeq (Bild(f), +)$

(b) *G: Symmetrische Gruppe* $(S_n, \circ)$ *H:* $R^* = (\mathbb{R} \setminus \{0\}, \cdot)$ $f : G \to H, \sigma \mapsto sign(\sigma)$

Bild$(f) = \{-1, 1\}$ *ist eine Untergruppe von* $\mathbb{R}^*$.

$\ker(f) = \{\sigma \in S_n \mid sign(\sigma) = 1\} = A_n$ *ist gerade die alternierende Gruppe.*

$S_n/A_n = \{ \underbrace{A_n}_{\text{alle } \sigma \text{ mit } sign(\sigma)=1} , \underbrace{A_n \circ \tau}_{\text{alle } \sigma \text{ mit } sign(\sigma)=-1} \}$ *für eine beliebige, aber feste Transposition* τ

Die Verknüpfung $\bar{\circ}$ *auf* S_n/A_n *wird wieder von* $\circ$ *auf* S_n *„geerbt“. Damit ergibt sich*

$\bar{\circ}$	A_n	$A_n \circ \tau$
A_n	A_n	$A_n \circ \tau$
$A_n \circ \tau$	$A_n \circ \tau$	A_n

$\bar{f} : S_n/A_n \to \{-1, 1\}$ *mit* $\bar{f}(A_n) = 1$ *und* $\bar{f}(A_n \circ \tau) = -1$ *ist ein Isomorphismus, d.h.* $(S_n/A_n, \bar{\circ}) \simeq (\{-1, 1\}, \cdot)$.

A.2. Ringe und Körper

Grundbegriffe

Ringe und Körper sind Mengen mit zwei verschiedenen Verknüpfungen.

Definition A.2.1 Das Tripel $(R, +, \cdot)$ aus einer Menge R und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ heißt **Ring**, wenn

(i) $(R, +)$ ist abelsche Gruppe.

- Neutrales Element bzgl. $+$ heißt **Nullelement** $0 \in R$.
- Inverses Element bzgl. $+$ zu $a \in R$ bezeichnen wir $-a$.

(ii) $(R, \cdot)$ ist Halbgruppe.

(iii) Es gelten die **Distributivgesetze**

$$\forall a, b, c \in R: \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Falls $(R, \cdot)$ sogar **Monoid** ist, so heißt $(R, +, \cdot)$ **Ring mit Eins**.

- Neutrales Element bzgl. $\cdot$ heißt dann **Einselement** $1 \in R$.

$(R, +, \cdot)$ heißt **kommutativ**, wenn $(R, \cdot)$ kommutativ ist.

Bemerkung

- Wir schreiben nur R, wenn $+$ und $\cdot$ klar.
- Wir schreiben $ab := a \cdot b$ sowie $a - b := a + (-b)$.
- Wir vereinbaren „Punktrechnung vor Strichrechnung“.

Beispiel A.2.2

(a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *sind kommutative Ringe.*

(b) $(\mathbb{R}^{n,n}, +, \cdot)$ *ist Ring, aber nicht kommutativ.*

(c) $\mathbb{F}_2 = \{0, 1\}$ *ist mit folgenden Verknüpfungen kommutativer Ring:*

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(d) $\mathbb{C}[x] := \{f(x) = \sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N}_0, a_i \in \mathbb{C}\}$ *ist Menge der komplexen Polynome.*
Mit der üblichen Addition

$$(\sum_{i=0}^{n} a_i x^i) + (\sum_{i=0}^{n} b_i x^i) := \sum_{i=0}^{n} (a_i + b_i) x^i$$

und Multiplikation

$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) := \sum_{i=0}^{n} c_i x^i \qquad \textit{mit } c_i := \sum_{k=0}^{i} a_k b_{i-k}$$

wird $\mathbb{C}[x]$ *zum Polynom-Ring.*

Nullelement: $f(x) = 0$ *Einselement:* $f(x) = 1$

Bemerkung A.2.3 Ist R ein Ring, so gilt automatisch

(i) $a0 = 0a = 0 \quad \forall a \in R$

(ii) $(-a)b = a(-b) = -(ab) \quad \forall a, b \in R$

$(-a)(-b) = ab \quad \forall a, b \in R$

(iii) $1 = 0 \quad \Leftrightarrow \quad R = \{0\}$

Beweis.

(i) $a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \quad \underbrace{\Rightarrow}_{\text{Kürzungsregel in } (R,+)} \quad 0 = a \cdot 0$

(ii)-(iii) Übung. □

Ideale und Faktorringe

Die Konzepte von Untergruppen, Homomorphismen zwischen Gruppen und der Bildung von Faktorgruppen lassen sich – mit kleinen Ergänzungen – von Gruppen mit nur einer Verknüpfung auf Ringe mit zwei Verknüpfungen übertragen.

Definition A.2.4 Sei R ein Ring. Eine Teilmenge $\emptyset \neq I \subseteq R$ heißt **Ideal**, wenn

(i) $(I, +)$ ist Untergruppe von $(R, +)$ und

(ii) $\forall a \in R,\ i \in I :\ a \cdot i \in I \ \wedge\ i \cdot a \in I.$

Die sehr starke Bedingung (ii) in der Definition eines Ideals (Beachte: Obwohl der Faktor a nicht aus dem Ideal I zu sein braucht, müssen die Produkte ai und ia beide wieder im Ideal liegen.) ist nötig, damit auch die Multiplikation vernünftig – also insbesondere wohldefiniert – in die Faktormenge R/I „vererbt“ werden kann (siehe Satz A.2.8).

Beispiel A.2.5

(a) In $\mathbb{Z}$ ist jede Untergruppe (automatisch von der Form $k\mathbb{Z}$ mit $k \in \mathbb{N}_0$) auch Ideal:

$$\forall a \in Z,\ i = kb \in k\mathbb{Z} :\ a \cdot kb = kb \cdot a = k(ab) \in k\mathbb{Z}$$

(b) Für ein gegebenes Polynom $\tilde{p}(x) = (x - b)$ ist

$$I := \{f(x) \in \mathbb{C}[x] \mid f(x) = q(x) \cdot \tilde{p}(x) \text{ mit } q(x) \in \mathbb{C}[x]\}$$

ein Ideal in $\mathbb{C}[x]$. *(I enthält alle Polynome, die b als Nullstelle haben.)*

Ring- und Körper-Homomorphismen

Wie bei Gruppen interessiert man sich auch bei Ringen für Homomorphismen zwischen Ringen und deren Wirkung auf Ideale:

Definition A.2.6

Seien R, S Ringe. Eine Abbildung $f : R \to S$ heißt **Ring-Homomorphismus**, wenn

(i) $\forall a, b \in R :\ f(a + b) = f(a) + f(b)$
(f ist Gruppen-Homomorphismus von $(R, +)$ nach $(S, +)$),

(ii) $\forall a, b \in R :\ f(ab) = f(a) \cdot f(b)$
(f ist Halbgruppen-Homomorphismus von $(R, \cdot)$ nach $(S, \cdot)$),

Ist f bijektiv, so heißt f **Ring-Isomorphismus**.

Bemerkung Sind R und S Ringe mit Einselement, so fordern einige Autoren zusätzlich auch noch $f(1_R) = 1_S$ für Ring-Homomorphismen $f : R \to S$.

Satz A.2.7 *Sei $f : R \to S$ ein Ring-Homomorphismus.*

(i) Ist f ein Ring-Isomorphismus (also bijektiv), so ist auch f^{-1} ein Ring-Isomorphismus.

(ii) Ist I ein Ideal in S, so ist $f^{-1}(I)$ ein Ideal in R.
Insbesondere ist $\ker(f) = f^{-1}(\{0\})$ *ein Ideal in R.*

Beweis. Lassen wir aus ... □

Analog zu Gruppen können wir Ideale (also auch Kerne von Homomorphismen) aus Ringen heraus faktorisieren:

Satz A.2.8 *Sei $(R, +, \cdot)$ ein Ring und I ein Ideal in R.*

(i) Die Faktorgruppe $(R/I, +)$ wird mit der durch

$$[a] \cdot [b] := [a \cdot b]$$

auf $(R/I, +)$ definierten Multiplikation zu einem (neuen) Ring, genannt ***Faktorring oder Restklassenring von R modulo I.***

Das Nullelement ist $[0]$.

Ist R ein Ring mit Einselement 1 ist, so ist auch R/I ein Ring mit Einselement $[1]$.

Ist R kommutativ, so ist auch R/I kommutativ.

(ii) $\pi : R \to R/I$, $a \mapsto [a] = a + I$ ist ein Ring-Homomorphismus und heißt ***kanonischer (Faktor-)Homomorphismus****.*

(iii) Durch $a \equiv_I b \ :\Leftrightarrow \ a + (-b) \in I$ wird eine Kongruenzrelation $\equiv_I$ auf R definiert.

Beweis. Analog Gruppen. □

Beispiel A.2.9

(a) Für jedes $k \in \mathbb{N}$ ist $k\mathbb{Z}$ ein Ideal in $\mathbb{Z}$.

Der Restklassenring ist $\mathbb{Z}/k\mathbb{Z} := \{[0], [1], \ldots, [k-1]\}$.

Addition: $[i] + [j] = [i + j]$ (ist wohldefiniert nach Bemerkung zu Def. A.1.38)

Multiplikation: $[i] \cdot [j] = [i \cdot j]$ (ist wohldefiniert nach Satz A.2.8)

(b) Sei $I \subseteq \mathbb{C}[x]$ das vom Polynom $\tilde{p} = (x - b)$ in $\mathbb{C}[x]$ definierte Ideal (vgl. Beispiel A.2.5).

Die Faktorgruppe $\mathbb{C}[x]/I$ bildet mit der von den Polynomen geerbeten Multiplikation den Restklassenring der Polynomdivision durch das Polynom $\tilde{p}$.

Für $f \in \mathbb{C}[x]$ ist die Restklasse (Äquivalenzklasse modulo I)

$$[f]_I = \{q(x) \cdot \tilde{p}(x) + f(x) \mid q(x) \in P\} = f + \tilde{p} \cdot \mathbb{C}[x] \ .$$

Der kanonische Repräsentant von der Restklasse $[f]$ ist das Polynom $r(x)$ mit $f(x) = q(x) \cdot \tilde{p}(x) + r(x)$, wobei $q(x), r(x) \in \mathbb{C}[x]$ und $\deg(r) < \deg(\tilde{p})$. (Rest bei Polynomdivision)

Nullteiler, Einheiten und Körper

Definition A.2.10 Sei R ein Ring.

(i) $a \in R$ heißt (rechter bzw. linker) **Nullteiler**, wenn es $b \in R \setminus \{0\}$ mit $b \cdot a = 0$ bzw. $a \cdot b = 0$ gibt.

(ii) R heißt **nullteilerfrei**, wenn es außer 0 keine Nullteiler gibt.

(iii) R heißt **Integritätsring**, wenn R ein Einselement enthält und nullteilerfrei und kommutativ ist.

Bemerkung A.2.11 Ist R ein Ring mit Einselement, dann sind äquivalent:

(i) R ist nullteilerfrei.

(ii) $R \setminus \{0\}$ ist abgeschlossen bzgl. der Multiplikation $\cdot$.

(iii) In R gelten die Kürzungsregeln für die Multiplikation $\cdot$:
Für alle $a, b, x \in R$ mit $x \neq 0$ gilt

$$ax = bx \;\Rightarrow\; a = b \qquad \text{und} \qquad xa = xb \;\Rightarrow\; a = b$$

Definition A.2.12 Sei R ein Ring mit Einselement.

(i) $a \in R$ heißt **Einheit**, falls es ein $a^{-1} \in R$ mit $a^{-1}a = aa^{-1} = 1$ gibt.

(ii) $R^* := \{a \in R \mid a \text{ ist Einheit}\}$ heißt **Einheitengruppe** von R.

(iii) R heißt **Körper**, wenn R kommutativ, $|R| \geq 2$ und $R^* = R \setminus \{0\}$ ist (d.h. alle Elemente außer 0 sind Einheiten).

Beispiel A.2.13

(a) $\mathbb{R}$ *ist Integritätsring.*

Einheitengruppe ist $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. *(Alle außer* 0 *haben multiplikatives Inverses.)*

Also ist $\mathbb{R}$ *ein Körper.*

(b) $\mathbb{Z}$ *ist Integritätsring.*

Einheitengruppe ist $\mathbb{Z}^* = \{1, -1\}$. *(Andere* $a \in \mathbb{Z}$ *haben keine mult. Inversen.)*

Also ist $\mathbb{Z}$ *kein Körper.*

(c) $\mathbb{R}^{2,2}$ *ist kein Integritätsring, da nicht nullteilerfrei. Beispielsweise ist*

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}}_{\neq Nullmatrix} \cdot \underbrace{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\neq Nullmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Einheitengruppe von $\mathbb{R}^2$ *ist* $GL(2, \mathbb{R}) = \{A \in \mathbb{R}^{2,2} \mid A \text{ regulär}\}$.
(Vgl. Dimensionssatz für lineare Abbildungen)

(d) $\mathbb{Z}/6\mathbb{Z}$ *ist kein Integritätsring, da nicht nullteilerfrei:*

$$[2] \cdot [3] = [6] = [0], \quad \textit{also sind } [2] \textit{ und } [3] \textit{ Teiler von } [0].$$

Die Einheitengruppe von $\mathbb{Z}/6\mathbb{Z}$ *ist* $(\mathbb{Z}/6\mathbb{Z})^* = \{[1], [5]\}$.

Verknüpfungstafel:

$\cdot$	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*
[0]	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*	*[0]*
[1]	*[0]*	*[1]*	*[2]*	*[3]*	*[4]*	*[5]*
[2]	*[0]*	*[2]*	*[4]*	*[0]*	*[2]*	*[4]*
[3]	*[0]*	*[3]*	*[0]*	*[3]*	*[0]*	*[3]*
[4]	*[0]*	*[4]*	*[2]*	*[0]*	*[4]*	*[2]*
[5]	*[0]*	*[5]*	*[4]*	*[3]*	*[2]*	*[1]*

Man erkennt die Nullteiler und Einheiten leicht in der Verknüpfungstafel:

- *Das Nullelement (*$[0]$*) ist immer Nullteiler, da alle Produkte mit 0 wieder sind.*
- *Ein Element ist linker Nullteiler, wenn in der zugehörigen Zeile in einer nicht zu 0 gehörenden Spalte das Ergebnis 0 auftritt. (Analog findet man rechte Nullteiler durch eine 0 in der zugehörigen Spalte.)*

  Im Beispiel sind also $[2], [3], [4]$ *Nullteiler.*
- *Ein Element ist Einheit, wenn in der zugehörigen Zeile und Spalte die 1 auftritt. Im Beispiel sind also* $[1], [5]$ *die Einheiten.*

(e) $\mathbb{Z}/5\mathbb{Z}$ *ist Körper.* *(Zur Übung selbst prüfen.)*

(f) $\mathbb{C}[x]$ *ist kein Körper, da* $\mathbb{C}[x]^* = \{f(x) = a \mid a \neq 0\} \neq \mathbb{C}[n] \setminus \{f(x) = 0\}$.

Satz A.2.14 *Sei* R *ein kommutativer Ring und* $a \in R$ *beliebig.*

(i) Wenn a *ein Nullteiler ist, dann ist* a *keine Einheit.*

(ii) Wenn $|R| < \infty$*, dann ist* a *entweder Einheit oder Nullteiler.*