Diskrete Mathematik

Woche 7: Zahlentheorie und die Geburt der Algebra

Shivram Sambhus (cs.shivi.io)

ETH Zürich

Heutige Agenda

1. **Admin & Wiederholung**
2. **Überblick:** Von Zahlen zu abstrakten Strukturen
3. **Teil 1: Zahlentheorie - Die Grundlagen**
   - Teilbarkeit, gcd und der Euklidische Algorithmus
   - Ideale, Primzahlen, gcd & lcm aus der Primfaktorzerlegung
4. **Teil 2: Modulare Arithmetik**
   - Kongruenzen und das Rechnen in "Restklassen"
   - Der Chinesische Restsatz (CRT)
   - Anwendung: Diffie-Hellman Schlüsselaustausch
5. **Teil 3: Einführung in die Algebra**
   - Was ist Algebra? Strukturen wie Gruppen, Ringe, Körper
6. **Übungsteil & Vorschau**

Admin & Wiederholung

- **Korrekturen:** Die Korrekturen sind noch nicht draussen!
- **Nächste Woche:** Wahrscheinlich Vertretung durch einen substitution TA. Falls nicht, schreiben ich oder die Head-TAs euch.
- **Offene Fragen zu Funktionen oder Abzählbarkeit?**

Überblick: Von Zahlen zu abstrakten Strukturen

Wir starten bei den ganzen Zahlen $\mathbb{Z}$.

1. **Zahlentheorie:** Wir untersuchen ihre fundamentalen Regeln: Wie funktioniert Teilung? Was ist der grösste gemeinsame Teiler?
2. **Modulare Arithmetik:** Wir entdecken, dass das Rechnen mit Resten (wie auf einer Uhr) eigene, konsistente Strukturen bildet.
3. **Algebraische Strukturen:** Wir erkennen, dass diese Strukturen – und viele andere in der Mathematik – gemeinsamen Mustern folgen. Diese nennen wir **algebraische Strukturen** (Gruppen, Ringe, Körper).

Ziel: Zu verstehen, warum Kryptographie wie RSA oder Diffie-Hellman funktioniert, indem wir die zugrundeliegende Struktur verstehen.

Teil 1: Zahlentheorie - Die Grundlagen

Teilbarkeit und Division mit Rest

- **Teilbarkeit:** $d \mid a$ ("d teilt a"), falls $a = k \cdot d$ für ein $k \in \mathbb{Z}$.
- **Satz 4.1 (Division mit Rest):** Für $a, d \in \mathbb{Z}$ mit $d \neq 0$ existieren *eindeutige* $q, r \in \mathbb{Z}$, sodass:

$$a = q \cdot d + r \quad \text{und} \quad 0 \leq r < |d|$$

- **Beispiel:** Für $a = -27, d = 5$: $-27 = (-6) \cdot 5 + 3$. Der Rest r ist immer ≥ 0!

Der grösste gemeinsame Teiler (gcd - ggT - greatest common divisor)

- **Intuition:** Der grösste "gemeinsame Baustein" zweier Zahlen.
- **Definition 4.2:** Der gcd von a und b ist die grösste positive ganze Zahl d, die sowohl a als auch b teilt. ("Grösste" bezüglich der Teilbarkeitsrelation: d teilt jeden anderen gemeinsamen Teiler.)
- **Die Schlüsseleigenschaft (Lemma 4.2):**

$$\gcd(a, b) = \gcd(b, a \pmod b)$$

- **Warum?** Jeder gemeinsame Teiler von a und b muss auch $a - q \cdot b$ (also den Rest) teilen. Die Menge der gemeinsamen Teiler ändert sich durch diesen Schritt nicht.

Walk-through: Der Euklidische Algorithmus

Ziel: Berechne $\gcd(252, 198)$.

1. $\gcd(252, 198) \quad \rightarrow \quad 252 = 1 \cdot 198 + \mathbf{54}$
2. $\gcd(198, 54) \quad \rightarrow \quad 198 = 3 \cdot 54 + \mathbf{36}$
3. $\gcd(54, 36) \quad \rightarrow \quad 54 = 1 \cdot 36 + \mathbf{18}$
4. $\gcd(36, 18) \quad \rightarrow \quad 36 = 2 \cdot 18 + \mathbf{0}$

Ergebnis: Der letzte Rest ungleich Null ist der gcd. $\gcd(252, 198) = 18$.

Der *Erweiterte* Euklidische Algorithmus & Bézouts Identität

- **Satz (Bézouts Identität, Korollar 4.5):** Für $a, b \in \mathbb{Z}$ (nicht beide 0) existieren $x, y \in \mathbb{Z}$, sodass:

$$\gcd(a, b) = a \cdot x + b \cdot y$$

- **Wie?** Wir substituieren die Reste aus dem Euklidischen Algorithmus rückwärts.

Walk-through: $\gcd(252, 198) = 18$

1. **Gleichungen der Reste:**
   - $54 = 252 - 1 \cdot 198$
   - $36 = 198 - 3 \cdot 54$
   - $18 = 54 - 1 \cdot 36$
2. **Rückwärtssubstitution:**
   - $18 = 54 - 1 \cdot \mathbf{36}$
   - $18 = 54 - 1 \cdot (198 - 3 \cdot \mathbf{54}) = 4 \cdot \mathbf{54} - 1 \cdot 198$
   - $18 = 4 \cdot (252 - 1 \cdot 198) - 198 = 4 \cdot 252 - 5 \cdot 198$

Ergebnis: $x = 4$ und $y = -5$.

Ideale: Die Struktur hinter dem ggT

- **Intuition:** Ein Ideal ist eine Teilmenge eines Rings, die "Vielfache absorbiert". Für ganze Zahlen ist es einfach die Menge aller Linearkombinationen.
- **Definition 4.4 (für $\mathbb{Z}$):** Das von a und b erzeugte **Ideal** ist die Menge:

$$(a, b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$$

- **Satz:** In $\mathbb{Z}$ ist jedes Ideal (a, b) gleich dem Ideal, das vom gcd erzeugt wird: $(a, b) = (\gcd(a, b))$.
- **Verbindung:** Da $\gcd(a, b)$ selbst im Ideal (a, b) liegt, *muss* es eine Linearkombination von a und b sein. Das ist der tiefere Grund für Bézouts Identität!

Primzahlen & Fundamentalsatz der Arithmetik

- **Definition 4.6:** Eine ganze Zahl $p > 1$ heisst **Primzahl**, wenn ihre einzigen positiven Teiler 1 und p sind.
- **Satz 4.6 (Fundamentalsatz der Arithmetik):** Jede ganze Zahl $n > 1$ kann *eindeutig* (bis auf Reihenfolge) als Produkt von Primzahlen geschrieben werden.

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

gcd & lcm aus der Primfaktorzerlegung

Der Fundamentalsatz gibt uns eine alternative Methode zur Berechnung von gcd und lcm (kleinstes gemeinsames Vielfaches).

- **Definition 4.5 (lcm):** Das lcm (kgV - kleinstes gemeinsames Vielfaches - least common multiple) von a, b ist die kleinste positive ganze Zahl l, die sowohl von a als auch von b ein Vielfaches ist. ("Kleinste" bezüglich der Teilbarkeitsrelation: jeder andere gemeinsame Vielfache teilt l.)
- **Formeln:** Seien $a = \prod_i p_i^{e_i}$ und $b = \prod_i p_i^{f_i}$.
  - $\gcd(a, b) = \prod_i p_i^{\min(e_i, f_i)}$ (nimm die *kleineren* Exponenten)
  - $\mathrm{lcm}(a, b) = \prod_i p_i^{\max(e_i, f_i)}$ (nimm die *grösseren* Exponenten)

gcd & lcm aus der Primfaktorzerlegung (Forts.)

- **Beispiel:** $a = 504 = 2^3 \cdot 3^2 \cdot 7^1$ und $b = 450 = 2^1 \cdot 3^2 \cdot 5^2$.
  - $\gcd(504, 450) = 2^{\min(3,1)} \cdot 3^{\min(2,2)} \cdot 5^{\min(0,2)} \cdot 7^{\min(1,0)} = 2^1 \cdot 3^2 = 18.$
  - $\mathsf{lcm}(504, 450) = 2^{\max(3,1)} \cdot 3^{\max(2,2)} \cdot 5^{\max(0,2)} \cdot 7^{\max(1,0)} = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 12600.$
- **Wichtige Identität:** $\gcd(a, b) \cdot \mathsf{lcm}(a, b) = |a \cdot b|$.
  - **Warum?** Weil $\min(e, f) + \max(e, f) = e + f$ für alle Exponenten e, f.

Teil 2: Modulare Arithmetik

Motivation: Diophantische Gleichungen

Frage: Haben Gleichungen ganzzahlige Lösungen? Modulare Arithmetik ist ein mächtiges Werkzeug, um "Nein" zu beweisen.

- **Beispiel 1:** $x^2 + x^3 = y^4 + y + 1$.
  - **Analyse (mod 2):** Betrachte die Parität (Gerade/Ungerade).
    - LHS $x^2 + x^3$: Wenn x gerade, beide Terme gerade $\rightarrow$ LHS gerade. Wenn x ungerade, beide ungerade $\rightarrow$ LHS gerade.
    - RHS $y^4 + y + 1$: Immer ungerade (prüfe für y gerade und ungerade).
    - LHS immer gerade, RHS immer ungerade $\rightarrow$ keine Lösung!
- **Beispiel 2:** $x^3 - x - 1 = y^2$.
  - **Analyse (mod 3):** Betrachte mögliche Reste.
    - LHS $x^3 - x - 1$: Für $x \equiv 0, 1, 2 \pmod 3$: immer $\equiv 2$.
    - RHS y^2: Kann 0 oder $1 \pmod 3$ sein, nie 2.
    - LHS immer $\equiv 2$, RHS nie $\equiv 2 \rightarrow$ keine Lösung!

Kongruenzen

- **Definition 4.8:** a, b sind **kongruent modulo** m, wenn sie bei Division durch m den gleichen Rest lassen.

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad m \mid (a - b)$$

- **Rechnen in $\mathbb{Z}_m$:** Die Menge der Reste $\{0, 1, \ldots, m-1\}$ bildet mit $\oplus$ (Addition mod m) und $\odot$ (Multiplikation mod m) den Ring $\mathbb{Z}_m$.

Multiplikative Inverse

- **Frage:** Wann können wir in $\mathbb{Z}_m$ "dividieren"?
- **Definition:** a^{-1} ist das Inverse von a modulo m, wenn $a \cdot a^{-1} \equiv 1 \pmod{m}$.
- **Satz (Lemma 4.18):** Ein Inverses $a^{-1} \pmod{m}$ existiert **genau dann, wenn** $\gcd(a, m) = 1$.
- **Wie findet man es?** Mit dem Erweiterten Euklidischen Algorithmus! Aus $1 = ax + my$ folgt $ax \equiv 1 \pmod{m}$.

Regeln für Modulare Arithmetik

Kongruenz ist eine Äquivalenzrelation:

- Reflexiv: $a \equiv a \pmod{m}$
- Symmetrisch: $a \equiv b \implies b \equiv a \pmod{m}$
- Transitiv: $a \equiv b, b \equiv c \implies a \equiv c \pmod{m}$

Rechenregeln (für Addition und Multiplikation):

- $a \equiv b \pmod{m} \implies a + c \equiv b + c \pmod{m}$
- $a \equiv b \pmod{m} \implies a \cdot c \equiv b \cdot c \pmod{m}$
- $a \equiv b, c \equiv d \pmod{m} \implies a + c \equiv b + d, a \cdot c \equiv b \cdot d \pmod{m}$

Potenzen und Inverse: Wenn $a \cdot a^{-1} \equiv 1 \pmod{m}$, dann existiert das Inverse genau dann, wenn $\gcd(a, m) = 1$.

Der Chinesische Restsatz (CRT): Die Methode

Satz 4.19: Seien $m_1, \dots, m_r$ paarweise teilerfremd. Das System

$$x \equiv a_i \pmod{m_i} \quad \text{für } i = 1, \dots, r$$

hat eine eindeutige Lösung modulo $M = m_1 \cdots m_r$.

Der konstruktive Algorithmus (aus dem Skript):

1. Berechne $M = m_1 \cdot m_2 \cdots m_r$.
2. Für jedes i, berechne $M_i = M/m_i$. (Das Produkt aller *anderen* Moduli).
3. Für jedes i, finde das Inverse N_i, sodass $M_i N_i \equiv 1 \pmod{m_i}$.
4. Die Lösung ist die Summe der "isolierten" Lösungen:

$$x = \sum_{i=1}^{r} a_i M_i N_i \pmod{M}$$

Warum funktioniert die CRT-Konstruktion?

Die Summe: $x = \underbrace{a_1 M_1 N_1}_{\text{für } i=1} + \underbrace{a_2 M_2 N_2}_{\text{für } i=2} + \cdots + \underbrace{a_r M_r N_r}_{\text{für } i=r} \pmod{M}$

Betrachte $x \pmod{m_j}$ **für ein festes** j**:**

- Für $i \neq j$: M_i ist durch m_j teilbar, also $\underbrace{M_i N_i \equiv 0 \pmod{m_j}}_{\text{verschwindet}}$. Somit $\underbrace{a_i M_i N_i \equiv 0 \pmod{m_j}}_{0 \bmod m_j}$.
- Für $i = j$: $\underbrace{M_j N_j \equiv 1 \pmod{m_j}}_{\text{Inverse}}$, also $\underbrace{a_j M_j N_j \equiv a_j \pmod{m_j}}_{\text{gleich } a_j}$.

Ergebnis: $\underbrace{\text{Alle anderen Terme verschwinden}}_{0 \bmod m_j}$, nur der j-te bleibt als a_j. Also erfüllt x jede Kongruenz!

CRT Walk-through: Ein komplexeres Beispiel

Ziel: Löse das System $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$.

Schritt 1 & 2: Berechne M und die M_i

- $m_1 = 3, m_2 = 5, m_3 = 7$. Sie sind paarweise teilerfremd.
- $M = 3 \cdot 5 \cdot 7 = 105$.
- $M_1 = M/3 = 35$.
- $M_2 = M/5 = 21$.
- $M_3 = M/7 = 15$.

CRT Walk-through: Schritt 3 (Inverse finden)

Ziel: Finde die Inversen N_i, sodass $M_i N_i \equiv 1 \pmod{m_i}$.

- **Für N_1:** Löse $35N_1 \equiv 1 \pmod{3}$.
  - $35 \equiv 2 \pmod{3}$. Die Gleichung wird zu $2N_1 \equiv 1 \pmod{3}$.
  - Das Inverse von $2 \pmod{3}$ ist 2 (da $2 \cdot 2 = 4 \equiv 1$).
  - Also ist $N_1 = 2$.
- **Für N_2:** Löse $21N_2 \equiv 1 \pmod{5}$.
  - $21 \equiv 1 \pmod{5}$. Die Gleichung wird zu $1N_2 \equiv 1 \pmod{5}$.
  - Also ist $N_2 = 1$.
- **Für N_3:** Löse $15N_3 \equiv 1 \pmod{7}$.
  - $15 \equiv 1 \pmod{7}$. Die Gleichung wird zu $1N_3 \equiv 1 \pmod{7}$.
  - Also ist $N_3 = 1$.

CRT Walk-through: Schritt 4 & 5 (Zusammensetzen)

Ziel: Berechne die endgültige Lösung mit $x = \sum a_i M_i N_i \pmod{M}$.

- Wir haben:
  - $a_1 = 2, M_1 = 35, N_1 = 2$
  - $a_2 = 3, M_2 = 21, N_2 = 1$
  - $a_3 = 2, M_3 = 15, N_3 = 1$
- **Summe:**

$$x = (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (2 \cdot 15 \cdot 1)$$

$$x = 140 + 63 + 30 = 233$$

- **Finale Reduktion:**

$$x \equiv 233 \pmod{105}$$

$$233 = 2 \cdot 105 + 23 \implies x = 23$$

Lösung: $x = 23$. **Probe:** $23 \equiv 2 \pmod{3}$, $23 \equiv 3 \pmod{5}$, $23 \equiv 2 \pmod{7}$.

Anwendung: Diffie-Hellman Schlüsselaustausch

Problem: Alice und Bob wollen einen geheimen Schlüssel über einen öffentlichen Kanal (den Eve abhört) vereinbaren. Dies war vor 1976 ein ungelöstes Problem.

Die Lösung: Nutze eine **Einwegfunktion**, die auf einem **rechenintensiven Problem** basiert.

- **Die Funktion:** Modulare Exponentiation, $x \mapsto g^x \pmod{p}$.
- **Das Problem:** Das **Diskrete Logarithmus Problem (DLP)** – finde x aus g, p und $g^x \pmod{p}$. Für grosse Primzahlen p ist dies extrem schwer.

Die Rolle der Zyklischen Gruppe & des Generators

- Diffie-Hellman funktioniert in einer **endlichen zyklischen Gruppe**. Das Standardbeispiel ist die multiplikative Gruppe $(\mathbb{Z}_p^*, \odot)$ für eine grosse Primzahl p.
- Diese Gruppe ist zyklisch (Thm. 5.15), d.h. es gibt ein Element g, den **Generator**, sodass jede Zahl in $\{1, \ldots, p-1\}$ als eine Potenz $g^k \pmod p$ geschrieben werden kann.
- **Warum ist das wichtig?** Der Generator g spannt den gesamten möglichen "Raum" für die Schlüssel auf. Alice und Bob wählen ihre geheimen Exponenten a, b aus $\{1, \ldots, p-1\}$, und die Potenzen g^a, g^b sind dann ebenfalls im Raum.

Das Diffie-Hellman Protokoll

Ablauf:

1. **Öffentlich:** Wähle grosse Primzahl p und Generator g für $\mathbb{Z}_p^*$.
2. **Privat:**
   - Alice wählt geheimes $a \in \{1, \ldots, p-1\}$.
   - Bob wählt geheimes $b \in \{1, \ldots, p-1\}$.
3. **Austausch:**
   - Alice sendet $A = g^a \pmod{p}$.
   - Bob sendet $B = g^b \pmod{p}$.
4. **Geheimer Schlüssel:**
   - Alice berechnet $S = B^a \pmod{p}$.
   - Bob berechnet $S = A^b \pmod{p}$.

Sicherheit: Eve sieht nur p, g, A, B. Um S zu finden, muss sie a oder b aus $A = g^a$ bestimmen (DLP).

Diffie-Hellman Beispiel

Beispiel ($p = 13, g = 2$):

1. Öffentlich: $p = 13, g = 2$.
2. Privat: Alice $a = 5$, Bob $b = 8$.
3. Austausch:
   - $A = 2^5 \pmod{13} = 6$
   - $B = 2^8 \pmod{13} = 9$
4. Geheimer Schlüssel:
   - $S = 9^5 \pmod{13} = 3$
   - $S = 6^8 \pmod{13} = 3$

Ergebnis: Beide haben $S = 3$. Eve müsste DLP lösen.

Übungsteil

1. **Diophantine Equations (5 Min):** Zeige, dass die Gleichung $x^2 - 7y^2 = 3$ keine ganzzahligen Lösungen hat.
2. **Extended Euclidean + Ideal (5 Min):** Berechne $\gcd(100, 75)$ mit dem erweiterten Euklidischen Algorithmus. Erstelle das Ideal $(100, 75)$.
3. **CRT (5 Min):** Löse das System $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 7 \end{cases}$.
4. **Diffie-Hellman (5 Min):** Mit $p = 23, g = 5, a = 6, b = 15$, berechne den gemeinsamen Schlüssel S.

Lösung 1

- **Strategie:** Wir betrachten die Gleichung modulo einer geschickt gewählten Zahl. Da der Term $7y^2$ vorkommt, ist Modulo 7 eine gute Wahl.
- **Gleichung reduzieren:** Wir nehmen die gesamte Gleichung modulo 7:

$$x^2 - 7y^2 \equiv 3 \pmod{7}$$

Da $7y^2$ immer ein Vielfaches von 7 ist, gilt $7y^2 \equiv 0 \pmod{7}$. Die Gleichung vereinfacht sich zu:

$$x^2 \equiv 3 \pmod{7}$$

- **Mögliche Quadrate mod 7:** Wir prüfen, welche Reste eine Quadratzahl bei Division durch 7 haben kann. Wir müssen nur die Reste $\{0, 1, 2, 3, 4, 5, 6\}$ überprüfen:
  - $0^2 \equiv 0 \pmod 7$
  - $1^2 \equiv 1 \pmod 7$
  - $2^2 \equiv 4 \pmod 7$
  - $3^2 = 9 \equiv 2 \pmod 7$
  - $4^2 = 16 \equiv 2 \pmod 7$
  - $5^2 = 25 \equiv 4 \pmod 7$
  - $6^2 = 36 \equiv 1 \pmod 7$
- **Widerspruch:** Die Menge der möglichen Werte für $x^2 \pmod 7$ ist $\{0, 1, 2, 4\}$. Der Wert 3 kommt in dieser Menge nicht vor.
- **Fazit:** Da die Bedingung $x^2 \equiv 3 \pmod 7$ für keine ganze Zahl x erfüllbar ist, kann die ursprüngliche Gleichung keine ganzzahligen Lösungen haben.

Lösung 2

Euklidischer Algorithmus:

- $100 = 1 \cdot 75 + 25$
- $75 = 3 \cdot 25 + 0$
- $\gcd(100, 75) = 25$

Erweiterter Euklid:

- $25 = 100 - 1 \cdot 75$

Ideal: $(100, 75) = (25)$, da 25 alle Linearkombinationen erzeugt.

Lösung 3

System: $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 7 \end{cases}$

- $M = 3 \cdot 5 \cdot 7 = 105$
- $M_1 = 105/3 = 35$, Inverse von $35 \pmod 3$: $35 \equiv 2$, $2^{-1} \equiv 2$ (da $2 \cdot 2 = 4 \equiv 1$)
- $M_2 = 105/5 = 21$, $21 \equiv 1 \pmod 5$, Inverse 1
- $M_3 = 105/7 = 15$, $15 \equiv 1 \pmod 7$, Inverse 1
- $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 1 \cdot 15 \cdot 1 = 140 + 63 + 15 = 218$
- $218 \div 105 = 2 \cdot 105 = 210$, Rest $218 - 210 = 8$

Lösung: $x \equiv 8 \pmod{105}$

Lösung 4

Parameter: $p = 23, g = 5, a = 6, b = 15$

Berechne A:

- $A = 5^6 \pmod{23}$
- $5^2 = 25 \equiv 2$
- $5^4 = 2^2 = 4$
- $5^6 = 4 \cdot 2 = 8$

Berechne B:

- $B = 5^{15} \pmod{23}$
- $5^1 = 5$, $5^2 = 25 \equiv 2$, $5^4 = 4$, $5^8 = 16$
- $5^{12} = 16 \cdot 4 = 64 \equiv 18$
- $5^{15} = 18 \cdot 125 \pmod{23} \equiv 18 \cdot 10 = 180 \equiv 19$

Berechne S:

- $S = A^{15} = 8^{15} \pmod{23}$
- $8^2 = 64 \equiv 18$, $8^4 = 18^2 \equiv 2$, $8^8 = 4$
- $8^{12} = 4 \cdot 2 = 8$, $8^{15} = 8 \cdot 512 \pmod{23} \equiv 8 \cdot 6 = 48 \equiv 2$

Gemeinsamer Schlüssel: $S = 2$

Teil 3: Einführung in die Algebra

Was ist Abstrakte Algebra?

Die Idee: Statt einzelne Objekte (wie Zahlen oder Matrizen) zu studieren, studieren wir die *Systeme und Regeln*, denen sie folgen. Es ist die Lehre von algebraischen Strukturen.

- **Analogie zu OOP (Objektorientierte Programmierung):**
  - Eine **algebraische Struktur** wie eine **Gruppe** ist wie eine abstrakte Klasse oder ein Interface.
  - **Properties/Axiome:** Sie definiert, welche Eigenschaften gelten müssen (z.B. Assoziativität, Inverse).
  - **Instanzen:** Objekte, die dieses Interface implementieren, sind z.B. $\langle \mathbb{Z}, + \rangle$, die Symmetrien eines Quadrats, oder $\langle \mathbb{Z}_p^*, \odot \rangle$.
- **Vorteil:** Ein Satz, der für die abstrakte Klasse "Gruppe" bewiesen wird, gilt automatisch für *alle* ihre Instanzen. Das ist extrem mächtig und effizient!

Unsere Reise durch die Algebra (Kapitel 5)

Was wir heute behandeln:

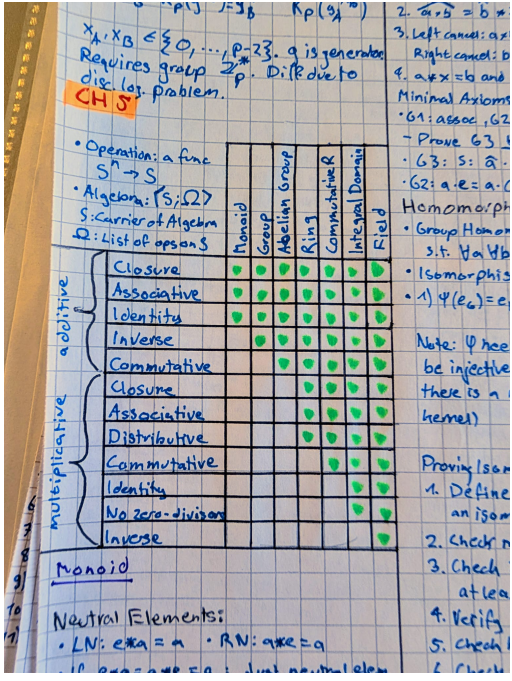
- **Algebraische Strukturen (Def. 5.1, 5.2):** Was ist eine "Algebra"? (Menge + Operationen)
- **Wichtige Eigenschaften (Axiome):** Assoziativität, Neutrales & Inverses Element.
- **Monoiden (Def. 5.5):** Eine erste einfache Struktur.
- **Gruppen (Def. 5.7):** Die wichtigste Struktur der Algebra. Wir betrachten die Axiome und auch eine minimale Version davon.

Next time:

- **Ringe & Körper:** Haben wir in der Übersicht gesehen, sind aber komplexere Strukturen mit zwei Operationen.
- **Homomorphismen & Isomorphismen:** Das sind "struktur-erhaltende" Abbildungen zwischen Algebren. Sie erlauben uns zu sagen, wann zwei Strukturen "im Grunde gleich" sind (isomorph).
- **Weiterführende Themen:** Galoistheorie, Lie-Algebren, etc.

Die Bausteine: Menge und Operation

- **Definition 5.1 (Operation):** Eine **Operation** auf einer Menge S ist eine Funktion $f : S^n \to S$. Die Zahl n heisst **Stelligkeit** (Arity).
  - **Binär ($n = 2$):** Nimmt zwei Elemente, gibt eines zurück. Bsp: $a + b$, $a \cdot b$.
  - **Unär ($n = 1$):** Nimmt ein Element, gibt eines zurück. Bsp: $-a$ (Negation).
  - **Nullär ($n = 0$):** Nimmt null Elemente, gibt also immer dasselbe Element zurück. Dies ist eine **Konstante**. Bsp: $0, 1 \in \mathbb{Z}$.
- **Definition 5.2 (Algebra):** Eine **Algebra** ist ein Paar $\langle S; \Omega \rangle$, bestehend aus:
  - einer Trägermenge S (z.B. $\mathbb{Z}$, $\mathbb{R}$, $\{\text{true}, \text{false}\}$).
  - einer Liste von Operationen Ω auf S (z.B. $\{+, \cdot, -, 0, 1\}$).



$x_A \cdot x_B \in \{0, \dots, p-2\}$. g is generator.
Requires group $\mathbb{Z}_p^*$. Diffie to
disc. log. problem.

CHS

- Operation: a func $S^n \to S$
- Algebra: $\langle S; \Omega \rangle$
  S: Carrier of Algebra
  Ω: List of opers on S

	Monoid	Group	Abelian Group	Ring	Commutative R	Integral Domain	Field
Closure	●	●	●	●	●	●	●
Associative	●	●	●	●	●	●	●
Identity	●	●	●	●	●	●	●
Inverse		●	●	●	●	●	●
Commutative			●	●	●	●	●
Closure				●	●	●	●
Associative				●	●	●	●
Distributive				●	●	●	●
Commutative					●	●	●
Identity						●	●
No zero-divisors						●	●
Inverse							●

additive

multiplicative

Monoid

Neutral Elements:
- LN: $e \circ a = a$
- RN: $a \circ e = a$

2. $a \cdot 5 = b$ ...
3. Left cancel: $a \cdot x = b$ ...
   Right cancel: b
4. $a \cdot x = b$ and ...

Minimal Axioms
- G1: assoc, G2
- Prove G3 ...
- G3: $\exists$ ...
- G2: $a \cdot e = a$ ...

Homomorph...
- Group Homom...
  s.t. $\forall a \forall b$ ...
- Isomorphis...
- 1) $\varphi(e_G) = e$ ...

Note: φ nee...
be injective
there is n...
kernel)

Proving Isom...
1. Define ... an isom...
2. Check ...
3. Check ... at lea...
4. Verify ...
5. Check ...
6. Check ...

Wichtige Eigenschaften von Operationen (Axiome)

Wir können Operationen nach bestimmten "Verhaltensregeln" oder Axiomen klassifizieren.

1. **Assoziativität (Def. 5.4):** $(a * b) * c = a * (b * c)$
   - **Wichtig:** Erlaubt uns, Klammern wegzulassen ($a * b * c$). Gilt für $+$ und $\cdot$ auf $\mathbb{Z}$.
   - **Gegenbeispiel:** Subtraktion auf $\mathbb{Z}$ ist nicht assoziativ: $(5 - 3) - 2 = 0$, aber $5 - (3 - 2) = 4$.
2. **Neutrales Element (Def. 5.3):** Ein Element e, sodass $a * e = e * a = a$.
   - Für $(\mathbb{Z}, +)$ ist es 0. Für $(\mathbb{Z}, \cdot)$ ist es 1.
   - **Satz (Lemma 5.1):** Wenn ein links-neutrales und ein rechts-neutrales Element existieren, sind sie identisch. Es gibt also **höchstens ein** neutrales Element.
3. **Inverses Element (Def. 5.6):** Zu einem Element a gibt es ein a^{-1} mit $a * a^{-1} = a^{-1} * a = e$.
   - Für a in $(\mathbb{Z}, +)$ ist das Inverse $-a$.
   - Für a in $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist das Inverse $1/a$.

Die erste Struktur: Das Monoid

Ein Monoid ist eine der einfachsten, aber nützlichsten algebraischen Strukturen.

- **Definition 5.5:** Ein **Monoid** $\langle M; *, e \rangle$ ist eine Algebra, die nur zwei Regeln befolgen muss:
  1. Die Operation $*$ ist **assoziativ**.
  2. Es gibt ein **neutrales Element** e.
- **Beispiele:**
  - $\langle \mathbb{N}_0, +, 0 \rangle$: Natürliche Zahlen mit Addition.
  - $\langle \mathbb{Z}, \cdot, 1 \rangle$: Ganze Zahlen mit Multiplikation.
  - $\langle \text{Strings}, \text{Konkatenation}, "" \rangle$: Die Menge aller Zeichenketten mit dem Anhängen als Operation und der leeren Zeichenkette als neutralem Element.
- **Sanity Check:** Warum ist $\langle \mathbb{N}_0, +, 0 \rangle$ ein Monoid, aber keine Gruppe?
  - Weil für die meisten Elemente (ausser 0) kein additives Inverses in $\mathbb{N}_0$ existiert (z.B. gibt es kein $x \in \mathbb{N}_0$ mit $3 + x = 0$).

Die wichtigste Struktur: Die Gruppe

Eine Gruppe ist ein Monoid, in dem wir jede Operation "rückgängig" machen können.

- **Definition 5.7:** Eine **Gruppe** $\langle G, *, ^{-1}, e\rangle$ ist eine Algebra, die drei Axiome erfüllt:
  1. **Assoziativität:** $(a * b) * c = a * (b * c)$.
  2. **Neutrales Element:** Es gibt ein e mit $a * e = e * a = a$.
  3. **Inverses Element:** Zu jedem a gibt es ein a^{-1} mit $a * a^{-1} = a^{-1} * a = e$.
- Wenn zusätzlich $a * b = b * a$ gilt, heisst die Gruppe **abelsch** (kommutativ).
- **Beispiele:** $\langle \mathbb{Z}, +\rangle$, $\langle \mathbb{Q} \setminus \{0\}, \cdot\rangle$, $\langle \mathbb{Z}_n, \oplus\rangle$, $\langle \mathbb{Z}_p^*, \odot\rangle$, Symmetrien eines Quadrats.

Minimale Gruppenaxiome

Die Standard-Axiome für Gruppen sind leicht redundant. Man kann zeigen, dass schwächere Axiome ausreichen.

- Man kann nur ein **rechts-neutrales Element** und nur ein **rechts-inverses Element** fordern. Die "linken" Eigenschaften folgen dann automatisch aus der Assoziativität.
- **Minimale Axiome:**
  1. **Assoziativität:** $(a * b) * c = a * (b * c)$.
  2. **Rechts-neutrales Element (G2'):** Es gibt ein e, sodass $a * e = a$ für alle a.
  3. **Rechts-inverses Element (G3'):** Zu jedem a gibt es ein $\bar{a}$ mit $a * \bar{a} = e$.
- **Resultat:** Aus diesen drei Axiomen allein kann man beweisen (siehe Skript, S. 95), dass auch $e * a = a$ und $\bar{a} * a = e$ gelten. Man braucht sie also nicht extra zu fordern.

Übungsteil

Übung 1: Strukturen identifizieren (5 Min)

Welche der folgenden Strukturen sind Monoide, welche sind Gruppen, und welche sind keines von beidem? Begründe kurz.

a) Die ganzen Zahlen mit der Subtraktion, $\langle \mathbb{Z}, - \rangle$.
b) Die geraden ganzen Zahlen mit der Addition, $\langle 2\mathbb{Z}, + \rangle$.
c) Die natürlichen Zahlen mit dem Maximum-Operator, $\langle \mathbb{N}_0, \max \rangle$.

Lösung 1

a) $\langle \mathbb{Z}, - \rangle$: **Keines von beidem.**

- **Nicht assoziativ:** $(8-4)-2=2$, aber $8-(4-2)=6$. Da die Assoziativität fehlt, kann es weder ein Monoid noch eine Gruppe sein.

b) $\langle 2\mathbb{Z}, + \rangle$: **Eine abelsche Gruppe.**

- **Assoziativ:** Addition ist assoziativ.
- **Neutrales Element:** 0 ist eine gerade Zahl.
- **Inverses Element:** Wenn x gerade ist, ist auch $-x$ gerade.
- (Kommutativität wird von $\mathbb{Z}$ geerbt).

c) $\langle \mathbb{N}_0, \max \rangle$: **Ein kommutatives Monoid.**

- **Assoziativ:** $\max(\max(a,b),c) = \max(a,\max(b,c))$.
- **Neutrales Element:** 0, da $\max(a,0)=a$ für alle $a \in \mathbb{N}_0$.
- **Keine Gruppe:** Für jedes Element $a > 0$ gibt es kein Inverses. Es gibt kein $x \in \mathbb{N}_0$ mit $\max(a,x)=0$.

Übung 2: Invertierbare Matrizen (5 Min)

Betrachte die Menge G aller invertierbaren 2×2 Matrizen mit reellen Einträgen und der Matrizenmultiplikation als Operation.

a) Warum bildet dies eine Gruppe? (Nenne die Elemente der Gruppenstruktur).

b) Ist diese Gruppe abelsch? Begründe mit einem Gegenbeispiel.

Lösung 2

a) **Es ist eine Gruppe:**

- **Assoziativität:** Matrizenmultiplikation ist assoziativ.
- **Neutrales Element:** Die Einheitsmatrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- **Inverses Element:** Per Definition besteht die Menge nur aus *invertierbaren* Matrizen, also hat jedes Element eine Inverse. Das Produkt zweier invertierbarer Matrizen ist wieder invertierbar (Abgeschlossenheit).

b) **Die Gruppe ist nicht abelsch.** Wir brauchen ein Gegenbeispiel:

- Sei $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- $A \cdot B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$.
- $B \cdot A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$.
- Da $A \cdot B \neq B \cdot A$, ist die Gruppe nicht kommutativ.

Übung 3: Die Herausforderung (Bonus, 7 Min)

Gegeben sei eine Struktur $\langle G, * \rangle$ mit nur drei **minimalen Axiomen**:

- **G1 (Assoziativität):** $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.
- **G2' (Rechts-neutrales Element):** Es existiert ein $e \in G$, sodass $a * e = a$ für alle $a \in G$.
- **G3' (Rechts-inverses Element):** Zu jedem $a \in G$ existiert ein $\bar{a} \in G$, sodass $a * \bar{a} = e$.

Die Aufgabe: Zeige, dass aus diesen schwachen Axiomen die vollen, zweiseitigen Gruppenaxiome folgen. Wir müssen also beweisen:

1. Das Rechts-Inverse ist auch ein Links-Inverses: $\bar{a} * a = e$.
2. Das Rechts-Neutrale ist auch ein Links-Neutrales: $e * a = a$.

Tipp: Beweise (1) zuerst. Das Resultat wird für den Beweis von (2) entscheidend sein.

Lösung 3a: Das Links-Inverse ($\bar{a} * a = e$)

Die Idee: Wir starten mit dem Ausdruck $\bar{a} * a$ und formen ihn geschickt um. Der Trick ist, das Rechts-Inverse des Rechts-Inversen zu benutzen. Da $\bar{a} \in G$, muss es nach (G3') selbst ein Rechts-Inverses haben, nennen wir es $\bar{\bar{a}}$, sodass $\bar{a} * \bar{\bar{a}} = e$.

Der Beweis Schritt für Schritt:

- $\bar{a} * a = (\bar{a} * a) * e$ (G2': Rechts-neutrales Element)
- $= (\bar{a} * a) * (\bar{a} * \bar{\bar{a}})$ (G3': e durch Inverse von $\bar{a}$)
- $= ((\bar{a} * a) * \bar{a}) * \bar{\bar{a}}$ (G1: Assoziativität)
- $= (\bar{a} * (a * \bar{a})) * \bar{\bar{a}}$ (G1: Assoziativität)
- $= (\bar{a} * e) * \bar{\bar{a}}$ (G3': $a * \bar{a} = e$)
- $= \bar{a} * \bar{\bar{a}}$ (G2': Rechts-neutral)
- $= e$ (G3': Definition von $\bar{\bar{a}}$) Wir haben somit gezeigt, dass das Rechts-Inverse auch als Links-Inverses fungiert.

Lösung 3b: Das Links-Neutrale ($e * a = a$)

Die Idee: Jetzt können wir das Resultat aus Teil (a), also $\bar{a} * a = e$, benutzen. Wir starten mit $e * a$ und ersetzen e geschickt.

Der Beweis Schritt für Schritt:

- $e * a = (a * \bar{a}) * a$ (G3': e durch $a * \bar{a}$)
- $= a * (\bar{a} * a)$ (G1: Assoziativität)
- $= a * e$ (Resultat aus (a): $\bar{a} * a = e$)
- $= a$ (G2': Rechts-neutral)

Fazit: Wir haben erfolgreich gezeigt, dass die schwachen, einseitigen Axiome (G1, G2', G3') ausreichen, um die vollen, zweiseitigen Gruppenaxiome zu garantieren. Dies zeigt die Eleganz und innere Konsistenz der Gruppenstruktur.

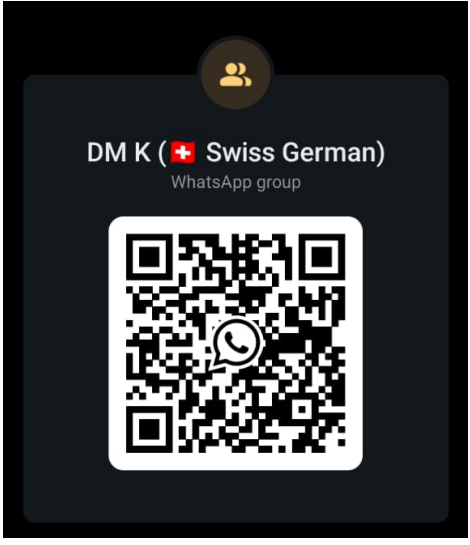
Keine Übung nächste Woche & Ausblick

- **Erinnerung:** Nächste Woche TA substitution.
- **Tipp für die Pause:**
  - Festigt die Konzepte von **Gruppen, Ringen und Körpern**. Was sind die Unterschiede? Könnt ihr für $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}_5, \mathbb{Z}_6$ bestimmen, was sie sind?
  - Der Euklidische Algorithmus ist zentral. Stellt sicher, dass ihr ihn sicher anwenden könnt.

Offene Fragen & Feedback

- Fragen zu Zahlentheorie oder den algebraischen Strukturen?
- Feedback zur heutigen Session? (https://forms.gle/LPrQfoZNsAHVeKoM9)
- E-Mail: dm@shivi.io

Schöne Pause und bis in zwei Wochen!


DM K (Swiss German)
WhatsApp group