Diskrete Mathematik

Woche 9: Algebraische Strukturen (Vertiefung)

Shivram Sambhus (cs.shivi.io)

ETH Zürich

Heutige Agenda

1. **Admin & Kurze Wiederholung (Gruppen, Untergruppen, Homomorphismen)**
2. **Teil 1: Vertiefung Gruppen**
   - Zyklische Gruppen & Generatoren
   - Die Gruppe $\mathbb{Z}_m^*$ und Eulersche Phi-Funktion
   - Lagrange's Theorem & Korollare
   - Anwendung: RSA-Kryptosystem
   - Übungen
3. **Teil 2: Ringe und Körper**
   - Definition und Struktur
   - Einheiten und die multiplikative Gruppe
   - Nullteiler und Integritätsbereiche
   - Körper
   - Übungen

Admin & Organisatorisches

- **Korrekturen:** W6 sollte in den nächsten Tagen raus kommen.
- **Letzte Woche (W8):** Substitution TA hat Gruppen, Untergruppen, Homomorphismen abgedeckt. Wir wiederholen das Wichtigste heute kurz.
- **Fragen vor dem Start?**

Kurze Wiederholung: Was ist eine Gruppe?

Definition 5.7: Eine Gruppe ist eine Algebra $\langle G; *, \hat{}, e \rangle$ mit den folgenden vier Axiomen:

1. **Abgeschlossenheit:** Für alle $a, b \in G$ gilt $a * b \in G$.
   - Das Ergebnis der Operation bleibt in der Menge.
2. **Assoziativität:** Für alle $a, b, c \in G$ gilt $(a * b) * c = a * (b * c)$.
   - Die Reihenfolge von mehreren Operationen ist egal (Klammern sind egal).
3. **Identitätselement:** Es existiert ein $e \in G$ mit $a * e = e * a = a$ für alle $a \in G$.
   - Es gibt ein neutrales Element, das nichts ändert.
4. **Inverses Element:** Für jedes $a \in G$ existiert ein $\hat{a} \in G$ mit $a * \hat{a} = \hat{a} * a = e$.
   - Jede Operation kann rückgängig gemacht werden.

Gruppe: Intuition & Beispiele

Intuition: Eine Gruppe ist eine Menge mit einer Operation, wo man...

- ...immer in der Menge bleibt (Abgeschlossenheit)
- ...jede Operation rückgängig machen kann (Inverses)
- ...Klammern beliebig setzen darf (Assoziativität)

Gute Beispiele (Sind Gruppen):

- $(\mathbb{Z}, +)$: Ganze Zahlen mit Addition.
- $(\mathbb{Z}_n, \oplus)$: Restklassen modulo n mit modularer Addition.
- $(\mathbb{R} \setminus \{0\}, \cdot)$: Reelle Zahlen ohne Null mit Multiplikation.

Gegenbeispiele (Sind keine Gruppen):

- $(\mathbb{N}, +)$: Natürliche Zahlen mit Addition. **Keine Inverse!** (z.B. hat 5 kein Inverses in $\mathbb{N}$)
- $(\mathbb{Z}, \cdot)$: Ganze Zahlen mit Multiplikation. **Nicht alle Elemente haben Inverse!** (z.B. hat 2 kein Inverses in $\mathbb{Z}$)

Schnelle Wiederholung: Untergruppen

Definition 5.11: $H \subseteq G$ ist eine **Untergruppe** von G, wenn H mit der von G geerbten Operation selbst eine Gruppe ist.

Untergruppen-Test (3-Punkte-Checkliste): Eine nichtleere Teilmenge $H \subseteq G$ ist eine Untergruppe, wenn:

1. **Abgeschlossenheit:** Für alle $a, b \in H$ ist $a * b \in H$.
2. **Inverses:** Für alle $a \in H$ ist auch das Inverse $\hat{a} \in H$.

Anmerkung: Die Identität e muss nicht separat geprüft werden. Wenn $a \in H$, dann ist auch $\hat{a} \in H$, und somit ist $e = a * \hat{a} \in H$ aufgrund der Abgeschlossenheit.

Untergruppen: Beispiele

Intuition: Eine Untergruppe ist eine “Gruppe in der Gruppe”, die für sich allein überleben kann.

Beispiel: Die geraden Zahlen $(2\mathbb{Z}, +)$ sind eine Untergruppe von $(\mathbb{Z}, +)$.

1. a, b gerade $\Rightarrow a + b$ ist gerade (abgeschlossen). ✓
2. a gerade $\Rightarrow -a$ ist gerade (invers). ✓

Gegenbeispiel: Die ungeraden Zahlen U sind **keine** Untergruppe von $(\mathbb{Z}, +)$.

- **Nicht abgeschlossen:** $1 \in U, 3 \in U$, aber $1 + 3 = 4 \notin U$. (X)
- **Keine Identität:** Das neutrale Element der Addition, 0, ist nicht ungerade. (X)

Definition: Ordnung eines Elements (Def 5.13)

Definition 5.13: Die **Ordnung** von $a \in G$, geschrieben ord(a), ist:

- Die kleinste positive Zahl m mit $a^m = e$, falls sie existiert
- Ansonsten ord$(a) = \infty$

Beispiele:

- In $\mathbb{Z}_6$: ord$(2) = 3$ weil $2^3 = 6 \equiv 0 \pmod 6$ ($2^3 \sim 2 + 2 + 2$)
- In $\mathbb{Z}_{12}$: ord$(3) = 4$ weil $3^4 = 12 \equiv 0$
- In $(\mathbb{Z}, +)$: ord$(5) = \infty$ (man kann nie zu 0 zurück)

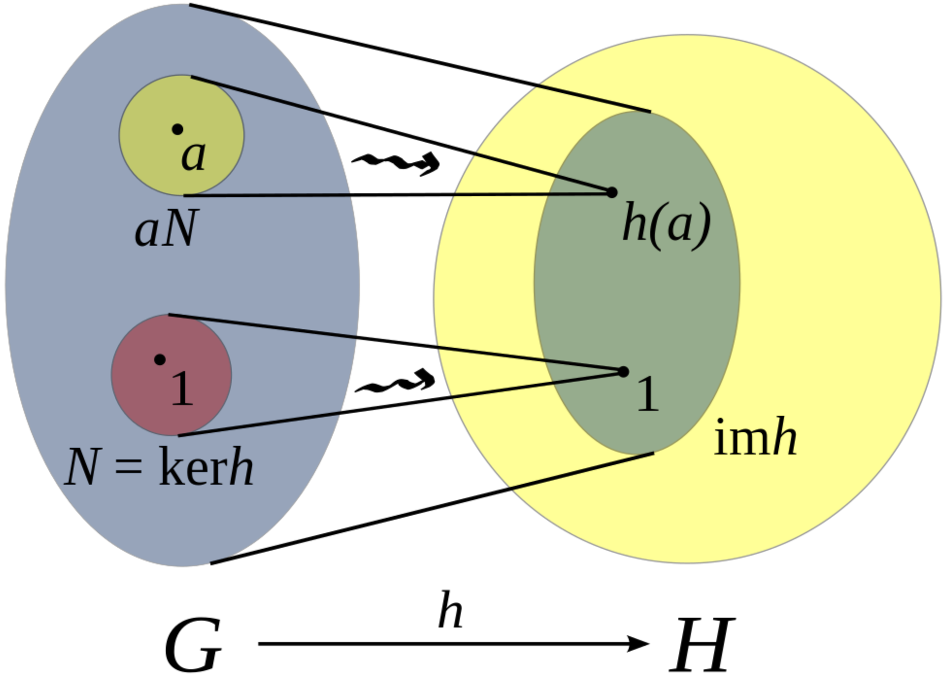
Schnelle Wiederholung: Homomorphismen & Isomorphismen

Definition 5.10: $\psi : G \to H$ ist ein **Gruppenhomomorphismus**, wenn die Struktur erhalten bleibt:

$$\psi(a * b) = \psi(a) \star \psi(b)$$

Intuition (Basis-Wechsel mit Nullraum): Homomorphismen sind wie Koordinaten-Transformationen in der linearen Algebra:

- sie bewahren die "Beziehungen" zwischen Elementen
- sie können aber Information "verlieren" (wenn nicht injektiv)
- Der **Kern** $\ker(\psi) = \{g \in G \mid \psi(g) = e_H\}$ ist wie der Nullraum – er sagt, welche Elemente zur gleichen Stelle abgebildet werden
- Ein Homomorphismus ist **injektiv genau dann wenn** $\ker(\psi) = \{e_G\}$ (wie in LA: Injektivität $\Leftrightarrow$ Nullraum $= \{0\}$)



a
aN
h(a)
1
N = ker h
1
im h
h
G
H

Isomorphismen und Homomorphismen

Isomorphismen: Ein **Isomorphismus** ist ein Homomorphismus, der eine Bijektion ist ($G \cong H$):

- Beide Richtungen funktionieren perfekt
- $\ker(\psi) = \{e_G\}$ (injektiv) und $\mathrm{im}(\psi) = H$ (surjektiv)
- Die beiden Gruppen haben "gleiche Struktur"

Was Homomorphismen bewahren:

- $\psi(e_G) = e_H$ (Identität $\rightarrow$ Identität)
- $\psi(a^{-1}) = \psi(a)^{-1}$ (Inverses $\rightarrow$ Inverses)

Steps to Prove an Isomorphism

To rigorously prove that two groups G and H are isomorphic, follow these steps:

1. **Define a Candidate Map**: Identify a function $\phi : G \to H$ that you suspect to be an isomorphism.
2. **Verify the Map is Well-Defined**: Ensure that the proposed map is unambiguous and consistent. That is, for any $g \in G$, $\phi(g)$ is uniquely determined.
3. **Verify the Map is Totally Defined**: Confirm that the map is defined for all elements of G (i.e., ϕ applies to every element of G).
4. **Verify the Map Maps to the Codomain**: Ensure that $\phi(g) \in H$ for all $g \in G$, so that the image of ϕ lies entirely within H.
5. **Check the Homomorphism Property**: Verify that $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for all $g_1, g_2 \in G$. This ensures the map preserves the group operation.
6. **Check Injectivity**: Prove that ϕ is one-to-one by showing that if $\phi(g_1) = \phi(g_2)$, then $g_1 = g_2$.
7. **Check Surjectivity**: Prove that ϕ is onto by demonstrating that for every $h \in H$, there exists $g \in G$ such that $\phi(g) = h$.
8. **Conclude Isomorphism**: If the map satisfies the homomorphism property, is well-defined, maps to the codomain, and is bijective, then ϕ is an isomorphism, and $G \simeq H$.

Exam-Beispiel: Isomorphismus Beweisen

Aufgabe: Zeige, dass $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Lösung (Schritt-für-Schritt Prozedur):

Schritt 1: Definiere die Abbildung Wir brauchen eine Abbildung $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$.
Wir verwenden den CRT als Inspiration:

$$\phi(n) = (R_2(n), R_3(n))$$

wobei $R_k(n)$ der Rest bei Division von n durch k ist (also $n \pmod{k}$).

Beispiele:

- $\phi(4) = (4 \pmod 2, 4 \pmod 3) = (0, 1)$
- $\phi(5) = (5 \pmod 2, 5 \pmod 3) = (1, 2)$

Exam-Beispiel: Homomorphismus-Eigenschaft

Schritt 2: Zeige Homomorphismus-Eigenschaft Für $a, b \in \mathbb{Z}_6$ müssen wir $\phi(a \oplus_6 b) = \phi(a) \oplus \phi(b)$ zeigen.

$$\begin{aligned}
\phi(a \oplus_6 b) &= (R_2(a+b), R_3(a+b)) \\
&= (R_2(a) \oplus_2 R_2(b), R_3(a) \oplus_3 R_3(b)) \\
&= (R_2(a), R_3(a)) \oplus (R_2(b), R_3(b)) \\
&= \phi(a) \oplus \phi(b)
\end{aligned}$$

- **Erklärung des 2. Schritts:** Die Eigenschaft der modularen Arithmetik, dass $R_k(a+b) = R_k(R_k(a) + R_k(b))$, wurde hier verwendet.
- **Erklärung des 3. Schritts:** Die Operation $\oplus$ im Produktraum $\mathbb{Z}_2 \times \mathbb{Z}_3$ ist **komponentenweise** definiert: $(x_1, y_1) \oplus (x_2, y_2) = (x_1 \oplus_2 x_2, y_1 \oplus_3 y_2)$

Schritt 3: Injektivität Wenn $\phi(a) = \phi(b)$, dann $R_2(a) = R_2(b)$ und $R_3(a) = R_3(b)$. Nach Chinesischen Restsatz (da $\gcd(2, 3) = 1$): $a \equiv b \pmod 6$, also $a = b$ ✓

Schritt 4: Surjektivität Für $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ existiert (nach CRT) ein $z \in \mathbb{Z}_6$ mit $z \equiv x \pmod 2$ und $z \equiv y \pmod 3$. Daher $\phi(z) = (x, y)$ ✓

Fazit: ϕ ist bijektiv und ein Homomorphismus, also ein Isomorphismus. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

Teil 1: Vertiefung Gruppen – Zyklische Gruppen & RSA

Definition & Intuition: Zyklische Gruppen

Definition 5.14-5.15: Für $a \in G$ ist die von a **erzeugte Untergruppe**:

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} = \{e, a, a^2, a^3, \ldots\}$$

Eine Gruppe $G = \langle g \rangle$ heisst **zyklisch**, wenn sie von einem einzigen Element g erzeugt wird.

Intuition: Zyklische Gruppen sind die "einfachsten" Gruppen. Alle Elemente entstehen durch wiederholte Anwendung einer einzigen Operation auf ein Element g.

Beispiele:

- $(\mathbb{Z}, +)$: Zyklisch, erzeugt von 1. Potenzen sind $k \cdot 1 = k$.
- $(\mathbb{Z}_n, \oplus)$: Zyklisch, erzeugt von 1. Es ist $\langle 1 \rangle = \{0, 1, 2, \ldots, n-1\}$.
- $(\mathbb{Z}_{12}, \oplus)$: Auch $\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$ erzeugt die ganze Gruppe (weil $\gcd(5, 12) = 1$).

Satz 5.7: Struktur zyklischer Gruppen

Satz 5.7: Jede zyklische Gruppe der Ordnung n ist **isomorph zu** $\mathbb{Z}_n$.

Wichtigkeit: Diese Isomorphie sagt: **Alle zyklischen Gruppen der gleichen Ordnung sind strukturell identisch!**

- sie unterscheiden sich nur darin, wie man die Elemente nennt.
- Die abstrakte Struktur ist immer dieselbe wie $\mathbb{Z}_n$.
- Um eine beliebige zyklische Gruppe zu verstehen, genügt es, $\mathbb{Z}_n$ zu verstehen.

Beweis-Idee: Die Abbildung ϕ

Sei $G = \langle g \rangle$ eine zyklische Gruppe mit $|G| = n$. Wir wollen zeigen, dass G isomorph zu $\mathbb{Z}_n$ ist.

Schritt 1: Definiere die Abbildung

Wir definieren eine Abbildung $\phi : \mathbb{Z}_n \to G$ durch:

$$\phi(k) = g^k$$

Beweis-Idee: Homomorphismus-Eigenschaft

Schritt 2: Zeige Homomorphismus-Eigenschaft

Wir müssen zeigen, dass ϕ die Gruppenstruktur erhält:

$$\phi(i \oplus_n j) = \phi(i) * \phi(j)$$

Beweis:

$$\begin{aligned} \phi(i \oplus_n j) &= g^{i+j} \quad \text{(nach Definition von } \phi) \\ &= g^i * g^j \quad \text{(Potenzgesetz in } G) \\ &= \phi(i) * \phi(j) \quad \text{(nach Definition von } \phi) \end{aligned}$$

Die Struktur der Addition in $\mathbb{Z}_n$ wird auf die Struktur der Multiplikation in G abgebildet.

Beweis-Idee: Injektivität von ϕ

Schritt 3a: Zeige Injektivität

Wir müssen zeigen: wenn $\phi(i) = \phi(j)$, dann $i = j$.

- Sei $\phi(i) = \phi(j)$ für $i, j \in \{0, \dots, n-1\}$.
- Das heisst $g^i = g^j$, woraus $g^{i-j} = e$ folgt.
- Nach Definition der Ordnung muss gelten: $\text{ord}(g) \mid (i-j)$.
- Da G von g erzeugt wird und $|G| = n$, ist $\text{ord}(g) = n$.
- Also: $n \mid (i-j)$.
- Da $i, j \in \{0, \dots, n-1\}$, liegt $i - j$ im Bereich $-(n-1)$ bis $(n-1)$.
- Das einzige Vielfache von n in diesem Bereich ist 0.
- Also muss $i - j = 0$ sein, woraus $i = j$ folgt. ✓

Beweis-Idee: Surjektivität & Fazit

Schritt 3b: Zeige Surjektivität

Wir müssen zeigen, dass jedes Element in G das Bild von ϕ ist.

- Per Definition ist $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.
- Genauer gesagt, da die Ordnung von g endlich ist (n), können wir uns auf Exponenten $k \in \{0, \dots, n-1\}$ beschränken.
- Jedes Element von G ist also von der Form g^k für ein solches k.
- Nach Definition von ϕ ist dieses Element genau $\phi(k)$.
- Also ist ϕ surjektiv. ✓

Fazit: ϕ ist ein bijektiver Homomorphismus und damit ein Isomorphismus. $G \cong \mathbb{Z}_n$.

Generatoren: Wer spannt die ganze Gruppe auf?

Frage: Welche Elemente g können die ganze Gruppe $\mathbb{Z}_n$ erzeugen?

Antwort: g erzeugt $\mathbb{Z}_n$ genau dann, wenn ord$(g) = n$, also:

$$\gcd(g, n) = 1$$

Intuition: Ein Generator "springt" in grösseren Schritten und besucht alle n Elemente, bevor er zum Start zurückkehrt. Wenn $\gcd(g, n) > 1$, dann springt g in kleineren Schritten und besucht nur einen Teil der Gruppe.

Beispiel: $\mathbb{Z}_{12}$

- Generatoren: $1, 5, 7, 11$ (alle teilerfremd zu 12)
  - $\langle 1 \rangle = \{0, 1, 2, \ldots, 11\}$ (alle 12!)
  - $\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$ (auch alle 12, nur andere Reihenfolge)
- Keine Generatoren: $2, 3, 4, 6, 8, 9, 10$ (nicht teilerfremd zu 12)
  - $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$ (nur 6 Elemente)
  - $\langle 4 \rangle = \{0, 4, 8\}$ (nur 3 Elemente)

Folge: Es gibt genau $\phi(n)$ Generatoren von $\mathbb{Z}_n$ (die zu n teilerfremden Zahlen)

Die multiplikative Gruppe $\mathbb{Z}_m^*$

Definition 5.16: $\mathbb{Z}_m^*$ ist die Menge der zu m teilerfremden Zahlen modulo m:

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$$

Beispiel:

- $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ (alle ausser 0 sind teilerfremd zu 5)
- $\mathbb{Z}_6^* = \{1, 5\}$ (nur 1 und 5 sind teilerfremd zu 6)
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Satz: $(\mathbb{Z}_m^*, \odot)$ ist eine **abelsche Gruppe** unter Multiplikation modulo m.

Wichtig: Die Multiplikation modulo m ist:

- Abgeschlossen: Wenn $\gcd(a, m) = 1$ und $\gcd(b, m) = 1$, dann $\gcd(ab, m) = 1$ ✓
- Hat Identität: $1 \in \mathbb{Z}_m^*$ ✓
- Hat Inverse: Erweiterter Euklidischer Algorithmus findet a^{-1} ✓

Eulersche Phi-Funktion: $\phi(m)$

Definition 5.17 (Phi-Funktion): $\phi(m) = |\mathbb{Z}_m^*|$ = Anzahl der zu m teilerfremden Zahlen in $\{1, \ldots, m\}$.

Formeln:

- **Ist p Primzahl:** $\phi(p) = p - 1$ (alle Zahlen ausser 0 sind teilerfremd zu p)
- **Ist p^k Primzahlpotenz:** $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
- **Allgemein (Multiplikativität):** Für $n = p_1^{e_1} \cdots p_r^{e_r}$ ist:

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{e_i}) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1})$$

Beispiele:

- $\phi(5) = 5 - 1 = 4$ ✓
- $\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = (2-1)(3-1) = 1 \cdot 2 = 2$ ✓
- $\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = (4-2)(3-1) = 2 \cdot 2 = 4$ ✓
- $\phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ ✓

Theorem 5.8 (Lagrange) - Das zentrale Theorem

Theorem 5.8 (Lagrange): Ist G eine endliche Gruppe und H eine Untergruppe, dann teilt die Ordnung von H die Ordnung von G:

$$|H| \mid |G|$$

Beweis-Idee (Partition durch Nebenklassen):

- Die Linksnebenklassen $gH = \{gh \mid h \in H\}$ bilden eine Partition von G.
- Das heisst, jede Nebenklasse ist nicht-leer, zwei Nebenklassen sind entweder identisch oder disjunkt, und die Vereinigung aller Nebenklassen ist G.
- Man kann zeigen, dass jede Nebenklasse gH genau $|H|$ Elemente hat.
- Wenn es k Nebenklassen gibt, dann ist $|G| = k \cdot |H|$.
- Also teilt die Ordnung der Untergruppe $|H|$ die Ordnung der Gruppe $|G|$.

Wichtige Korollare zum Satz von Lagrange

1. **Ordnung von Elementen:** Für jedes Element $a \in G$ gilt: $\text{ord}(a) \mid |G|$.
   - *Warum?* Die von a erzeugte zyklische Untergruppe $\langle a \rangle$ hat die Ordnung $\text{ord}(a)$. Nach Lagrange muss $\text{ord}(a)$ ein Teiler von $|G|$ sein.
2. **Gruppen von Primordnung:** Jede Gruppe G mit Primzahl-Ordnung $|G| = p$ ist zyklisch.
   - *Warum?* Für jedes $a \neq e$ ist $\text{ord}(a) > 1$. Da $\text{ord}(a)$ aber $|G| = p$ teilen muss, bleibt nur $\text{ord}(a) = p$. Also erzeugt a die ganze Gruppe.

Warnung: Die Umkehrung von Lagrange gilt NICHT!

- Wenn d ein Teiler von $|G|$ ist, heisst das **nicht**, dass es immer eine Untergruppe der Ordnung d gibt.
- **Gegenbeispiel:** Die Gruppe A_4 hat Ordnung 12, aber keine Untergruppe der Ordnung 6.
- Die Umkehrung gilt aber für **endliche zyklische Gruppen**.

Korollar 5.10: Satz von Euler

Korollar 5.10 (Euler): Für alle $a \in \mathbb{Z}_m^*$ gilt:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Beweis (mit Lagrange):

- $(\mathbb{Z}_m^*, \odot)$ ist eine endliche Gruppe der Ordnung $\phi(m)$
- Die Untergruppe $\langle a \rangle$ hat Ordnung $\mathrm{ord}(a)$
- Nach Lagrange: $\mathrm{ord}(a) \mid \phi(m)$, also $\phi(m) = k \cdot \mathrm{ord}(a)$ für ein k
- Daher: $a^{\phi(m)} = (a^{\mathrm{ord}(a)})^k = 1^k = 1$ ✓

Intuition: Lagrange garantiert: jedes Element zykliert mit Periode die $\phi(m)$ teilt. Nach $\phi(m)$ Schritten sind wir garantiert zurück bei 1!

Spezialfall - Fermat's Little Theorem: Für Primzahl p ist $\phi(p) = p - 1$:

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{für alle } a \not\equiv 0 \pmod{p}$$

Praktischer Trick: Exponent Reduktion

Problem: Wie berechnet man $a^{\text{großer Exponent}} \pmod{m}$ effizient?

Lösung: Nutze Euler: Reduziere den Exponenten modulo $\phi(m)$:

$$a^e \equiv a^{e \bmod \phi(m)} \pmod{m}$$

Beispiel: Berechne $7^{100} \pmod{13}$

- $\phi(13) = 12$ (13 ist Primzahl)
- $100 \bmod 12 = 4$ (denn $100 = 8 \cdot 12 + 4$)
- Also: $7^{100} \equiv 7^4 \pmod{13}$
- $7^2 = 49 \equiv 10 \pmod{13}$
- $7^4 = 10^2 = 100 \equiv 9 \pmod{13}$ ✓
- **Resultat:** Statt 100 Multiplikationen nur 2 Quadrierungen!

Korollar 5.11: Gruppen von Primordnung

Korollar 5.11: Jede Gruppe von **Primordnung** p ist:

1. Zyklisch
2. Jedes nicht-neutrale Element ist ein Generator

Beweis-Skizze:

- Sei $|G| = p$ (Primzahl) und $a \neq e$
- Nach Lagrange: $\text{ord}(a) \mid p$
- Da p prim: $\text{ord}(a) \in \{1, p\}$
- $a \neq e$ bedeutet $\text{ord}(a) \neq 1$, also $\text{ord}(a) = p$
- Daher $\langle a \rangle = G$ ✓

Fazit: Primordnung $\Rightarrow$ zyklisch, aber zyklisch $\not\Rightarrow$ Primordnung

Anwendung 1: Das RSA-Kryptosystem

Die zentrale Idee:

1. Einfach: Nachricht m mit öffentlichem Exponenten e zu m^e erheben
2. Schwierig: Aus $m^e \pmod{n}$ das m ohne den geheimen d zu finden
3. Dies basiert darauf, dass n faktorisieren schwer ist

RSA-Schlüsselerzeugung (Step-by-Step):

1. **Wähle Primzahlen:** Alice wählt zwei grosse, verschiedene Primzahlen p und q geheim
2. **Berechne n:** $n = p \cdot q$ (öffentlich)
3. **Berechne $\phi(n)$:** $\phi(n) = (p-1)(q-1)$ (geheim – nur Alice kennt es!)
4. **Wähle e:** Öffentlicher Exponent mit $\gcd(e, \phi(n)) = 1$
5. **Berechne d:** Privater Exponent als Inverses: $d \cdot e \equiv 1 \pmod{\phi(n)}$ (Erweiterter Euklid!)

Öffentlicher Schlüssel: (n, e) – wird überall verteilt
Privater Schlüssel: d – wird geheim gehalten (evtl. auch p, q)

RSA: Verschlüsselung und Entschlüsselung

Verschlüsselung (Bob hat Alice's öffentlichen Schlüssel (n, e)):

- Bob hat Nachricht $m \in \{1, \dots, n-1\}$
- Bob berechnet: $c \equiv m^e \pmod{n}$
- Bob sendet c (das Chiffrat) an Alice

Entschlüsselung (nur Alice mit (n, e, d)):

- Alice hat c erhalten
- Alice berechnet: $m \equiv c^d \pmod{n}$
- Alice hat die Original-Nachricht zurück!

Warum funktioniert Entschlüsselung?

Nach Konstruktion ist $ed \equiv 1 \pmod{\phi(n)}$, also $ed = k \cdot \phi(n) + 1$ für ein k.

$$c^d \equiv (m^e)^d = m^{ed} = m^{k\phi(n)+1} = (m^{\phi(n)})^k \cdot m$$

Nach Euler's Korollar (für $\gcd(m, n) = 1$): $m^{\phi(n)} \equiv 1 \pmod{n}$

$$\Rightarrow c^d \equiv 1^k \cdot m = m \pmod{n} \checkmark$$

RSA: Sicherheit

Warum ist RSA sicher?
Um den privaten Schlüssel d zu berechnen, muss ein Angreifer:

1. $\phi(n)$ kennen
2. Aber $\phi(n) = (p-1)(q-1)$, also müsste man p und q kennen
3. Das bedeutet: n faktorisieren!

Für $n = p \cdot q$ mit p, q Primzahlen von ~300 Dezimalstellen:

- Faktorisierung mit heutigen Verfahren: nicht praktikabel (~100+ Jahre auf einem einzelnen Computer)
- Dies ist das **Faktorisierungsproblem** (vermutlich schwer)

Korollar: RSA ist nur so sicher wie die Schwierigkeit der Faktorisierung!

Anwendung 2: Diffie-Hellman Schlüsselaustausch

Das Problem: Wie können Alice und Bob über einen öffentlichen Kanal, den Angreiferin Eve mithört, einen gemeinsamen geheimen Schlüssel vereinbaren?

Die Kernidee (Diffie & Hellman, 1976): Eine "Einwegfunktion" verwenden. Eine mathematische Operation, die in eine Richtung einfach, aber in die andere Richtung sehr schwer umzukehren ist.

Die gewählte Einwegfunktion: Modulares Potenzieren in einer zyklischen Gruppe.

- **Einfach:** $g^x \pmod p$ berechnen.
- **Schwer:** Aus $y = g^x \pmod p$, den Exponenten x zurückrechnen. Dies ist das **Diskrete Logarithmus Problem (DLP)**.

Übungsteil 1: Gruppen

Übung 1.1: Generatoren & Zyklizität

Frage:

a) Finde alle Generatoren der additiven Gruppe $(\mathbb{Z}_{10}, \oplus)$.

b) Ist die multiplikative Gruppe $(\mathbb{Z}_{12}^*, \odot)$ zyklisch? Begründe deine Antwort.

Lösung 1.1

a) Generatoren von $\mathbb{Z}_{10}$: Die Generatoren von $\mathbb{Z}_n$ sind die Zahlen $k \in \{1, \dots, n-1\}$, für die $\gcd(k, n) = 1$ gilt. Für $n = 10$ sind das die Zahlen, die teilerfremd zu 10 sind:

$$\{1, 3, 7, 9\}$$

Es gibt $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$ Generatoren.

b) Ist $\mathbb{Z}_{12}^*$ zyklisch? Die Gruppe ist $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. ihre Ordnung ist $|\mathbb{Z}_{12}^*| = \phi(12) = 4$. Damit die Gruppe zyklisch ist, muss es ein Element der Ordnung 4 geben. Wir prüfen die Ordnungen:

- $\text{ord}(1) = 1$
- $5^2 \equiv 25 \equiv 1 \pmod{12} \implies \text{ord}(5) = 2$
- $7^2 \equiv 49 \equiv 1 \pmod{12} \implies \text{ord}(7) = 2$
- $11^2 \equiv (-1)^2 \equiv 1 \pmod{12} \implies \text{ord}(11) = 2$

Kein Element hat die Ordnung 4. **Also ist $\mathbb{Z}_{12}^*$ nicht zyklisch.** (sie ist isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}_2$, der Klein'schen Vierergruppe).

Übung 1.2: Anwendung von Eulers Satz

Frage:

Berechne $3^{2023} \pmod{100}$.

Lösung 1.2

Ziel: Berechne $3^{2023} \pmod{100}$. Wir verwenden Eulers Satz: $a^{\phi(n)} \equiv 1 \pmod{n}$ für $\gcd(a, n) = 1$.

1. **Prüfe Bedingung:** $\gcd(3, 100) = 1$. ✓
2. **Berechne $\phi(100)$:** $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2)$
   $= (2^2 - 2^1)(5^2 - 5^1) = (4 - 2)(25 - 5) = 2 \cdot 20 = 40.$
3. **Reduziere den Exponenten:** Wir müssen den Exponenten 2023 modulo $\phi(100) = 40$ reduzieren. $2023 = 50 \cdot 40 + 23$. Also $2023 \equiv 23 \pmod{40}$.
4. **Berechne die Potenz:**
   - $3^{2023} \equiv 3^{23} \pmod{100}$.
   - $3^1 = 3$
   - $3^2 = 9$
   - $3^4 = 81 \equiv -19$
   - $3^5 = 81 \cdot 3 = 243 \equiv 43$
   - $3^{10} \equiv 43^2 = 1849 \equiv 49$
   - $3^{20} \equiv 49^2 = 2401 \equiv 1$
   - $3^{23} = 3^{20} \cdot 3^3 \equiv 1 \cdot 27 = 27 \pmod{100}$.

Antwort: $3^{2023} \equiv 27 \pmod{100}$.

Übung 1.3: RSA Secret Key (Exam HS18)

Frage:

Der öffentliche RSA-Schlüssel von Alice ist $(n, e) = (77, 7)$. Berechne ihren geheimen Schlüssel d.

Lösung 1.3

Ziel: Finde d, sodass $e \cdot d \equiv 1 \pmod{\phi(n)}$.

1. **Faktorisiere n:** $n = 77 = 7 \cdot 11$. Also $p = 7, q = 11$.
2. **Berechne $\phi(n)$:** $\phi(77) = (p-1)(q-1) = (7-1)(11-1) = 6 \cdot 10 = 60$.
3. **Löse die Kongruenz:** Wir suchen d mit $7d \equiv 1 \pmod{60}$. Wir verwenden den Erweiterten Euklidischen Algorithmus für $\gcd(60, 7)$:
   - $60 = 8 \cdot 7 + 4$
   - $7 = 1 \cdot 4 + 3$
   - $4 = 1 \cdot 3 + 1$

   Jetzt rückwärts einsetzen:
   - $1 = 4 - 1 \cdot 3$
   - $1 = 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7$
   - $1 = 2 \cdot (60 - 8 \cdot 7) - 1 \cdot 7 = 2 \cdot 60 - 16 \cdot 7 - 1 \cdot 7 = 2 \cdot 60 - 17 \cdot 7$

   Wir haben also $2 \cdot 60 - 17 \cdot 7 = 1$. Modulo 60 ergibt das: $-17 \cdot 7 \equiv 1 \pmod{60}$.
4. **Finde positives d:** $d \equiv -17 \equiv -17 + 60 \equiv 43 \pmod{60}$.

Antwort: Der geheime Schlüssel ist $d = 43$.

Übung 1.4: Isomorphismus (Exam HS22)

Frage:

Beweise oder widerlege: Die Gruppen $(\mathbb{Z}_{12}^*, \odot)$ und $(\mathbb{Z}_4, \oplus)$ sind isomorph.

Lösung 1.4

Ziel: Prüfen, ob $\mathbb{Z}_{12}^* \cong \mathbb{Z}_4$.

Strategie: Isomorphe Gruppen müssen dieselben strukturellen Eigenschaften haben. Wir vergleichen einige davon:

1. **Ordnung der Gruppen:**
   - $|\mathbb{Z}_{12}^*| = \phi(12) = 4$.
   - $|\mathbb{Z}_4| = 4$. Die Ordnungen stimmen überein. Das schliesst einen Isomorphismus nicht aus.
2. **Ist die Gruppe zyklisch?**
   - $(\mathbb{Z}_4, \oplus)$ ist zyklisch, da sie von 1 (und 3) erzeugt wird. ord$(1) = 4$.
   - Ist $(\mathbb{Z}_{12}^*, \odot)$ zyklisch? Wie in Übung 1.1 gesehen, sind die Ordnungen der Elemente $\{1, 5, 7, 11\}$:
     - ord$(1) = 1$, ord$(5) = 2$, ord$(7) = 2$, ord$(11) = 2$.
     - Es gibt kein Element der Ordnung 4. Also ist $\mathbb{Z}_{12}^*$ **nicht zyklisch**.

Fazit: Da $\mathbb{Z}_4$ zyklisch ist, aber $\mathbb{Z}_{12}^*$ nicht, können sie **nicht isomorph** sein. Isomorphismen erhalten die Eigenschaft, zyklisch zu sein.

Teil 2: Ringe und Körper

Von Gruppen zu Ringen

Warum eine zweite Operation?

- Gruppen sind Strukturen mit **einer** Operation (z.B. Addition ODER Multiplikation).
- Die Zahlensysteme, die wir kennen $(\mathbb{Z}, \mathbb{Q}, \mathbb{R})$, haben aber **zwei** Operationen: Addition und Multiplikation.
- **Ringe** sind die Abstraktion davon. sie modellieren Mengen, auf denen man "sinnvoll" addieren und multiplizieren kann.
- Die entscheidende Verbindung zwischen den beiden Operationen ist das **Distributivgesetz**: $a \cdot (b + c) = a \cdot b + a \cdot c$

Was sind Ringe? Intuition & Definition

Intuition: Ein Ring ist eine Struktur, die sich “fast” wie die ganzen Zahlen $\mathbb{Z}$ verhält.

- Man kann immer addieren, subtrahieren und multiplizieren.
- Die Addition ist “schön” (kommutativ, assoziativ).
- Die Multiplikation ist assoziativ.
- Addition und Multiplikation sind durch das Distributivgesetz verträglich.

Achtung: Division ist nicht immer möglich!

Definition: Ring

Definition 5.18: Ein **Ring** ist eine Algebra $\langle R; +, -, 0, \cdot, 1\rangle$ wobei:

1. $\langle R; +, -, 0\rangle$ eine **abelsche Gruppe** ist (für die Addition).
   - *Wir wollen, dass Addition und Subtraktion immer funktionieren und kommutativ sind.*
2. $\langle R; \cdot, 1\rangle$ ein **Monoid** ist (für die Multiplikation).
   - *Multiplikation ist assoziativ und hat ein neutrales Element, die 1.*
3. **Distributivgesetze** gelten, die Addition und Multiplikation verbinden.
   - $a \cdot (b + c) = ab + ac$ und $(b + c)a = ba + ca$.

Ein Ring heisst **kommutativ**, wenn die Multiplikation kommutativ ist ($ab = ba$).

Ringe: Erste Beispiele

Kommutative Ringe (Regelfall für uns):

- $(\mathbb{Z}, +, \cdot)$: Der Prototyp eines Rings.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$: Ebenfalls kommutative Ringe.
- $(\mathbb{Z}_m, \oplus, \odot)$: Der Ring der Restklassen modulo m. Sehr wichtig in der Informatik!

Nicht-kommutativer Ring:

- Der Ring der $n \times n$ Matrizen $M_n(\mathbb{R})$ mit Matrixaddition und -multiplikation.
- Hier gilt im Allgemeinen $A \cdot B \neq B \cdot A$.

“Division” in einem Ring: Einheiten

In $\mathbb{Q}$ oder $\mathbb{R}$ können wir durch jede Zahl $x \neq 0$ dividieren. Division durch x ist dasselbe wie Multiplikation mit dem Inversen x^{-1}.

Frage: Welche Elemente in einem allgemeinen Ring R haben ein multiplikatives Inverses?

Definition 5.20: Ein Element $u \in R$ heisst **Einheit**, wenn es ein multiplikatives Inverses $v \in R$ gibt, sodass:

$$u \cdot v = v \cdot u = 1$$

Die Menge aller Einheiten in R wird mit R^* bezeichnet.

Einheiten: Beispiele & Struktur

Beispiele für Einheiten-Mengen R^*:

- Für die ganzen Zahlen $\mathbb{Z}$ ist $\mathbb{Z}^* = \{1, -1\}$. Nur diese haben ein Inverses in $\mathbb{Z}$.
- Für einen Körper wie $\mathbb{Q}$ ist $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
- Für den Restklassenring $\mathbb{Z}_m$ ist $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$. (Das kennen wir schon!)

Satz: Die Menge der Einheiten $(R^*, \cdot)$ ist immer eine **Gruppe**!

- sie erbt die Assoziativität von R.
- sie ist abgeschlossen, da $(uv)^{-1} = v^{-1}u^{-1}$.
- sie enthält die 1 und per Definition alle Inversen.

Ein Problem: Die Kürzungsregel

In der Schule lernen wir: Wenn $a \cdot b = a \cdot c$ und $a \neq 0$, dann dürfen wir a kürzen und folgern $b = c$.

Frage: Gilt das in jedem Ring?

Antwort: **Nein!** Schauen wir uns $\mathbb{Z}_6$ an:

- $2 \cdot 1 = 2$
- $2 \cdot 4 = 8 \equiv 2 \pmod 6$
- Also haben wir $2 \cdot 1 \equiv 2 \cdot 4 \pmod 6$.
- Aber $1 \neq 4$! Wir können die 2 nicht einfach kürzen.

Warum? Das Phänomen der **Nullteiler** ist schuld.

Nullteiler

Definition 5.23: Ein Element $a \neq 0$ in einem kommutativen Ring R heisst **Nullteiler**, wenn es ein $b \neq 0$ gibt, sodass:

$a \cdot b = 0$

Beispiel $\mathbb{Z}_6$:

- $2 \cdot 3 = 6 \equiv 0$. Also sind 2 und 3 Nullteiler.
- $4 \cdot 3 = 12 \equiv 0$. Also ist auch 4 ein Nullteiler.
- Die Nullteiler in $\mathbb{Z}_m$ sind genau die Zahlen, die nicht teilerfremd zu m sind.

Die Kürzungsregel schlägt fehl, weil $a(b-c) = 0$ nicht mehr $b - c = 0$ impliziert!

Integritätsbereiche: Ringe ohne Nullteiler

Um die guten Eigenschaften wie die Kürzungsregel zu retten, definieren wir eine speziellere Klasse von Ringen.

Definition 5.24: Ein **Integritätsbereich** ist ein kommutativer, nicht-trivialer Ring $(1 \neq 0)$, der **keine Nullteiler** hat.

$\forall a, b \in D : ab = 0 \implies a = 0$ oder $b = 0$

Warum wichtig?

- In Integritätsbereichen funktioniert die Kürzungsregel wie gewohnt.
- sie verhalten sich "integer" (wie die ganzen Zahlen $\mathbb{Z}$).

Beispiele:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sind Integritätsbereiche.
- $\mathbb{Z}_m$ ist ein Integritätsbereich $\iff$ m eine Primzahl ist.

Körper: Die "perfekten" Ringe

Definition 5.26: Ein **Körper** (engl. *Field*) ist ein kommutativer Ring, in dem jedes Element ausser 0 eine Einheit ist. - Äquivalent: $F^* = F \setminus \{0\}$.

Warum wichtig?

- In einem Körper kann man addieren, subtrahieren, multiplizieren und durch **jedes** nicht-null Element dividieren.
- Körper sind die fundamentalen Strukturen, um lineare Algebra zu betreiben und Gleichungssysteme zu lösen.

Beispiele:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.
- $\mathbb{Z}_p$ ist ein Körper, wenn p eine Primzahl ist.
- $\mathbb{Z}$ ist **kein** Körper, da z.B. 2 kein multiplikatives Inverses hat.

Die Hierarchie der Algebraischen Strukturen

Gruppen $\subset$ **Ringe** $\subset$ **Körper** (grob gesagt)

Eine verfeinerte Sicht für kommutative Ringe:

Körper $\implies$ Integritätsbereich $\implies$ Kommutativer Ring

- Jeder Körper ist ein Integritätsbereich.
  - *Beweis-Idee:* Wenn $a \neq 0$ ein Inverses a^{-1} hat, kann es kein Nullteiler sein. Wenn $ab = 0$, dann ist $a^{-1}ab = 0 \Rightarrow b = 0$.
- Aber nicht jeder Integritätsbereich ist ein Körper (z.B. $\mathbb{Z}$).

Charakteristik eines Ringes

Definition 5.19: Die **Charakteristik** char(R) eines Ringes R ist die kleinste positive ganze Zahl n, sodass:

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ mal}} = 0$$

Falls es keine solche Zahl gibt, ist die Charakteristik 0.

Intuition: Wie oft muss man die 1 aufaddieren, um zur 0 zurückzukehren? **Beispiele:**

- char$(\mathbb{Z}) = 0$, char$(\mathbb{Q}) = 0$, char$(\mathbb{R}) = 0$.
- char$(\mathbb{Z}_m) = m$.
- Wenn ein Ring Charakteristik p (Primzahl) hat, gilt oft $(a + b)^p = a^p + b^p$ ("Freshman's Dream").

$\ldots K_p(g \ldots) = y_B \quad K_p(g_A^{x_B})$

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

CH 5

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

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

Monoid

Neutral Elements:

- LN: $e * a = a$ • RN: $a * e = a$
- If $e * a = a * e = a$: Just neutral elem...

2. $\widehat{a * b} = b * \ldots$
3. Left cancel: $a * \ldots$
   Right cancel: $b \ldots$
4. $a * x = b$ and ...

Minimal Axioms
- G1: assoc, G2 ...
- → Prove G3 ...
- G3: S: $\hat{a} \cdot \ldots$
- G2: $a \cdot e = a \cdot \ldots$

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

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

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

Übungsteil 2: Ringe & Körper

Übung 2.1: Einheiten & Nullteiler (Exam HS18)

Frage:

Finde alle Einheiten und alle Nullteiler im Ring $\mathbb{Z}_{12}$.

Lösung 2.1

Der Ring ist $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$.

Einheiten in $\mathbb{Z}_{12}$: Die Einheiten sind die Elemente u, für die $\gcd(u, 12) = 1$ gilt.

- $\gcd(1, 12) = 1 \implies 1$ ist eine Einheit.
- $\gcd(5, 12) = 1 \implies 5$ ist eine Einheit.
- $\gcd(7, 12) = 1 \implies 7$ ist eine Einheit.
- $\gcd(11, 12) = 1 \implies 11$ ist eine Einheit.
- Die Einheiten sind $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.

Nullteiler in $\mathbb{Z}_{12}$: Die Nullteiler sind die von Null verschiedenen Elemente a, für die es ein $b \neq 0$ gibt mit $ab \equiv 0 \pmod{12}$. Das sind genau die Elemente, die nicht teilerfremd zu 12 sind (und nicht 0 sind).

- $2 \cdot 6 = 12 \equiv 0 \implies 2, 6$ sind Nullteiler.
- $3 \cdot 4 = 12 \equiv 0 \implies 3, 4$ sind Nullteiler.
- $8 \cdot 3 = 24 \equiv 0 \implies 8$ ist Nullteiler.
- $9 \cdot 4 = 36 \equiv 0 \implies 9$ ist Nullteiler.
- $10 \cdot 6 = 60 \equiv 0 \implies 10$ ist Nullteiler.

Die Nullteiler sind $\{2, 3, 4, 6, 8, 9, 10\}$.

Übung 2.2: Ringaxiome (Exam HS20)

Frage:

Sei $\langle R; +, -, 0, \cdot, 1 \rangle$ ein Ring. Beweise nur mit den Ringaxiomen, dass für alle $a, b \in R$ gilt:

$$(-a)b = -(ab)$$

(Hinweis: $-(ab)$ ist das additive Inverse von ab. Du musst zeigen, dass $(-a)b + ab = 0$.)

Lösung 2.2

Ziel: Zeige $(-a)b = -(ab)$. Per Definition des additiven Inversen müssen wir also zeigen, dass $(-a)b + ab = 0$.

Beweis: Wir starten mit dem Ausdruck $(-a)b + ab$.

1. **Distributivgesetz anwenden:** Wir können b ausklammern (rechtsdistributiv):
$$(-a)b + ab = (-a + a)b$$
2. **Additives Inverses nutzen:** Nach Definition des additiven Inversen in der Gruppe $(R, +)$ ist $-a + a = 0$.
$$(-a + a)b = 0 \cdot b$$
3. **Eigenschaft des Nullelements:** In jedem Ring gilt, dass die Multiplikation mit dem Nullelement immer Null ergibt ($0 \cdot x = 0$). (Dies kann man separat aus den Axiomen beweisen, indem man $0 \cdot b = (0 + 0)b = 0b + 0b$ betrachtet und dann kürzt). $0 \cdot b = 0$

Zusammenfassung: $(-a)b + ab = (-a + a)b = 0 \cdot b = 0$.

Da $(-a)b + ab = 0$, ist $(-a)b$ per Definition das additive Inverse von ab. **Also gilt $(-a)b = -(ab)$.** ✓

Übung 2.3: Ringeigenschaften (Exam HS19)

Frage:

Sei $\langle R; +, \cdot \rangle$ ein Ring, in dem für alle $a \in R$ gilt: $a \cdot a = a$. Beweise, dass der Ring kommutativ ist (d.h. $ab = ba$ für alle $a, b \in R$).

Tipp: Zeige zuerst, dass $a + a = 0$ für alle $a \in R$ gilt.

Lösung 2.3 (Teil 1: $a + a = 0$)

Ziel 1: Zeige $a + a = 0$ für alle $a \in R$.

- Sei $a \in R$. Wir verwenden die Eigenschaft $x^2 = x$ für $x = a + a$.
  - $(a + a)^2 = a + a$
- Mit dem Distributivgesetz ausmultiplizieren:
  - $(a + a)(a + a) = a(a + a) + a(a + a) = a^2 + a^2 + a^2 + a^2$
- Da $a^2 = a$ gilt:
  - $a + a + a + a = a + a$
- Da $(R, +)$ eine abelsche Gruppe ist, können wir auf beiden Seiten $-(a + a)$ addieren:
  - $(a + a + a + a) - (a + a) = (a + a) - (a + a)$
- $a + a = 0$

Dies bedeutet, jedes Element ist sein eigenes additives Inverses ($a = -a$). ✓

Lösung 2.3 (Teil 2: $ab = ba$)

Ziel 2: Zeige $ab = ba$ für alle $a, b \in R$.

- Wir verwenden wieder $x^2 = x$, diesmal für $x = a + b$.
  - $(a+b)^2 = a + b$
  - $(a+b)(a+b) = a^2 + ab + ba + b^2$
- Da $a^2 = a$ und $b^2 = b$:
  - $a + ab + ba + b = a + b$
- Wir addieren $-(a+b)$ auf beiden Seiten:
  - $ab + ba = 0$
  - Das heisst $ab = -(ba)$.
- Aus Teil 1 wissen wir, dass jedes Element sein eigenes additives Inverses ist, also $x = -x$.
- Für $x = ba$ gilt also $ba = -(ba)$.
- Somit können wir in der Gleichung $ab = -(ba)$ den Term $-(ba)$ durch ba ersetzen:
  - $ab = ba$

Der Ring ist kommutativ. ✓

Übung 2.4: Endliche Integritätsbereiche

Frage:

Beweise den Satz: Jeder endliche Integritätsbereich ist ein Körper.

Lösung 2.4

Satz: Jeder endliche Integritätsbereich D ist ein Körper.

Beweis: Sei D ein endlicher Integritätsbereich. Wir müssen zeigen, dass jedes Element $a \in D, a \neq 0$ ein multiplikatives Inverses hat.

1. Sei $a \in D$ mit $a \neq 0$. Betrachte die Abbildung $f_a : D \to D$ definiert durch Multiplikation mit a:
$$f_a(x) = ax$$
2. **Wir zeigen, dass f_a injektiv ist.** Angenommen $f_a(x) = f_a(y)$ für $x, y \in D$. Dann ist $ax = ay$, was $ax - ay = 0$ oder $a(x - y) = 0$ bedeutet. Da D ein Integritätsbereich ist, hat er keine Nullteiler. Weil $a \neq 0$ ist, muss also $x - y = 0$ gelten, woraus $x = y$ folgt. Also ist f_a injektiv.

Lösung 2.4 (Cont.)

3. **Schubfachprinzip (Pigeonhole Principle):** Die Abbildung f_a ist eine injektive Funktion von einer endlichen Menge D in sich selbst. Nach dem Schubfachprinzip muss eine solche Abbildung auch **surjektiv** sein.
4. **Existenz des Inversen:** Da f_a surjektiv ist, gibt es für jedes Element in D ein Urbild. Insbesondere für das Einselement $1 \in D$ muss es ein $b \in D$ geben, sodass:

$$f_a(b) = 1$$

   Das bedeutet $ab = 1$. Dieses b ist das gesuchte multiplikative Inverse von a.

Fazit: Da jedes von Null verschiedene Element a ein Inverses hat, ist D per Definition ein Körper. ✓

Lösung 2.4: Warum "endlich"?

Frage: Warum funktioniert dieser Beweis nur für **endliche** Integritätsbereiche?

Antwort: Der entscheidende Schritt ist die Anwendung des **Schubfachprinzips**:

> *Eine injektive Funktion von einer* ***endlichen*** *Menge in sich selbst ist automatisch auch surjektiv.*

Dies gilt **nicht** für unendliche Mengen!

Gegenbeispiel: Der unendliche Integritätsbereich $\mathbb{Z}$

- Nehmen wir $a = 2 \in \mathbb{Z}$.
- Die Abbildung ist $f_2(x) = 2x$.
- **Injektiv?** Ja, denn wenn $2x = 2y$, dann ist $x = y$.
- **Surjektiv?** Nein! Das Bild von f_2 ist die Menge der geraden Zahlen. Ungerade Zahlen wie z.B. 1 werden nie erreicht.
- Da 1 nicht im Bild von f_2 liegt, gibt es kein $b \in \mathbb{Z}$ mit $f_2(b) = 2b = 1$.
- Folglich hat $a = 2$ kein multiplikatives Inverses in $\mathbb{Z}$.

Fazit: Für unendliche Mengen kann eine injektive Abbildung "Löcher" im Zielbereich lassen. Der Beweis, dass das Inverse existiert, scheitert, weil wir nicht garantieren können, dass die 1 getroffen wird.

Offene Fragen & Feedback

- Feedback zur heutigen Session? (https://forms.gle/LPrQfoZNsAHVeKoM9)
- E-Mail: dm@shivi.io

Schöne Pause und bis nächste Woche!

DM K (🇨🇭 Swiss German)

WhatsApp group