Diskrete Mathematik

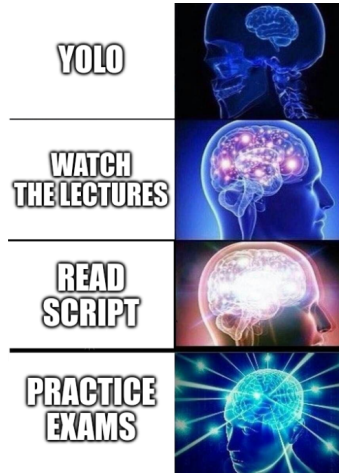
Finale: Repetition, Exam Prep & Survival Guide (Woche 13)

Shivram Sambhus (cs.shivi.io)

ETH Zürich

Willkommen zum Finale!

- **Thema:** Der grosse Rückblick (Kapitel 1-6).
- **Ziel:** Fit für die Prüfung (6.0 Mission).
- **Agenda:**
  1. **The Big Picture:** Alle Konzepte im Schnelldurchlauf.
  2. **Strategy:** Schritt-für-Schritt Strategien.
  3. **Topics:** Aufgaben nach Typ sortiert (3-4 Beispiele pro Typ).
  4. **Hard(er) Mode:** Härtere (mid-hard) problems.
  5. **Survival Guide:** How to survive BP1.



Teil 1: The Big Picture (TL;DR)

Kapitel 1 & 2: Das Fundament

Worum geht's? Mathematische Strenge, Logik und Beweismethoden.

- **Aussagenlogik:** Negation, Implikation ($A \to B \equiv \neg A \vee B$), Kontraposition.
- **Beweismethoden:**
  - *Direkt:* Definitionen einsetzen.
  - *Widerspruch (Reductio ad absurdum):* Nehme $\neg A$ an, leite Widerspruch ($\perp$) her.
  - *Schubfachprinzip (Pigeonhole):* $n+1$ Tauben, n Fächer $\implies$ Ein Fach voll.
- **Induktion:** Der Goldstandard für $\mathbb{N}$.
  1. **Basis:** Zeige für n_0.
  2. **Annahme (IA):** Gelte für n.
  3. **Schritt (IS):** Zeige für $n+1$ unter Verwendung der IA.

Kapitel 3: Die Sprache der Mathematik

Worum geht's? Mengen, Relationen und wie wir Dinge zählen.

- **Mengen:** $\mathcal{P}(A)$ (Potenzmenge), $|A| < |\mathcal{P}(A)|$.
- **Relationen:**
  - *Äquivalenzrelation:* Reflexiv, Symmetrisch, Transitiv. $\rightarrow$ **Partitionen**.
  - *Ordnungsrelation (Poset):* Reflexiv, Antisymmetrisch, Transitiv. $\rightarrow$ **Hasse-Diagramme**.
- **Funktionen:**
  - *Injektiv:* Verschiedene Inputs $\rightarrow$ Verschiedene Outputs. ($f(x) = f(y) \implies x = y$)
  - *Surjektiv:* Alles wird getroffen. (Gleichung $f(x) = y$ immer lösbar)
  - *Bijektiv:* Beides $\implies$ Umkehrfunktion existiert.
- **Abzählbarkeit:**
  - Abzählbar: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.
  - überabzählbar: $\mathbb{R}, \{0,1\}^{\mathbb{N}}$. **Diagonalargument!**

Kapitel 4: Zahlentheorie

Worum geht's? Die Struktur von $\mathbb{Z}$ und Kryptographie.

- **Euklidischer Algorithmus:**
  - $\gcd(a, b)$ berechnen.
  - *Erweiterter Euklid:* $\gcd(a, b) = sa + tb$. (Wichtig für Inverse!)
- **Modulare Arithmetik:**
  - Rechnen in $\mathbb{Z}_n$.
  - Inverses a^{-1} existiert $\iff \gcd(a, n) = 1$.
- **Die grossen Theoreme:**
  - *Kleiner Fermat:* $a^{p-1} \equiv 1 \pmod{p}$ (für Primzahl p).
  - *Satz von Euler:* $a^{\phi(n)} \equiv 1 \pmod{n}$. ($\phi(n) =$ Anzahl teilerfremder Zahlen).
  - *CRT (Chinesischer Restsatz):* Kongrünzsysteme lösen (wenn Moduli teilerfremd).

Kapitel 5: Algebra

Worum geht's? Abstrakte Strukturen und Symmetrien.

- **Gruppen** $(G, \star)$**:** Abgeschlossen, Assoziativ, Neutrales e, Inverse.
  - *Ordnung:* Kleinste k mit $g^k = e$. Teilt immer $|G|$ (Lagrange).
  - *Zyklisch:* Ein Generator erzeugt alles.
  - *Homomorphismus:* $\phi(a \star b) = \phi(a) \circ \phi(b)$. (Strukturerhaltend).
- **Ringe & Körper:**
  - Ring: Gruppe bzgl $+$, Monoid bzgl $\cdot$, Distributiv.
  - Körper (Field): Ring wo fast alles (ausser 0) multiplikativ invertierbar ist. $(\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p)$.
- **Polynome:**
  - Rechnen mit $P(x)$ in Körpern. Irreduzibilitut = "Primzahlen der Polynome".

Kapitel 6: Logik-Kalküle

Worum geht's? Automatisiertes Schliessen und Grenzen der Beweisbarkeit.

- **Aussagenlogik:**
  - Erfüllbarkeit (SAT) vs. Allgemeingultigkeit (Tautologie).
  - CNF (Konjunktive Normalform) & DNF.
- **Resolution:**
  - Ein *korrekter* und *vollstundiger* Kalkül für Unerfüllbarkeit.
  - Regel: $\{L, A\}, \{\neg L, B\} \vdash \{A, B\}$. Ziel: Leere Klausel $\square$.
- **Prädikatenlogik:**
  - Quantoren $\forall, \exists$.
  - **PNF (Prenex Normal Form):** Alle Quantoren nach vorne.
  - **Skolemisierung:** $\exists$ eliminieren durch Funktionen.
  - **Theorem 6.12:** Die Mutter aller Paradoxa (Russell, Cantor, Halteproblem).

Teil 2: Topic Buckets (Aufgaben nach Typ)

Bucket A: Induktion & Beweise

A1. Induktion

Aufgabe: Zeige mittels vollständiger Induktion: Für alle $n \geq 1$ gilt: $6 \mid (n^3 - n)$.

Lösung A1

- **Basis ($n = 1$):** $1^3 - 1 = 0,\ 6 \mid 0.$ ✓
- **Schritt ($n \to n+1$):** $(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1$
  $= (n^3 - n) + 3n(n+1).$
- Erster Term $(n^3 - n)$ ist durch 6 teilbar (IA).
- Zweiter Term $3n(n+1)$:
  - $n(n+1)$ ist Produkt zweier aufeinanderfolgender Zahlen $\implies$ gerade ($\mid 2$).
  - Also ist $3 \cdot n(n+1)$ teilbar durch $3 \cdot 2 = 6$.
- Summe zweier durch 6 teilbarer Zahlen ist teilbar durch 6. $\square$

A2. Pigeonhole Principle

Aufgabe: Seien $a_1, \ldots, a_n$ ganze Zahlen. Beweise: Es gibt eine Teilfolge $a_i, \ldots, a_j$ $(1 \leq i \leq j \leq n)$, deren Summe durch n teilbar ist.

Hinweis: Betrachte die Partialsummen $s_k = a_1 + \cdots + a_k$.

Lösung A2

Strategie: Schubfachprinzip (Pigeonhole Principle)

1. **Definitionen:**
   - **Tauben:** Die n Partialsummen $s_k = a_1 + \cdots + a_k$ für $k = 1, \ldots, n$.
   - **Fächer:** Die möglichen Reste modulo n: $\{0, 1, \ldots, n-1\}$.
2. **Fallunterscheidung:**
   - **Fall 1:** Einer der Reste ist 0 (d.h. $s_k \equiv 0 \pmod{n}$).
     - Dann ist die Summe s_k bereits durch n teilbar. Fertig.
   - **Fall 2:** Keiner der Reste ist 0.
     - Verfügbare Fächer: $\{1, \ldots, n-1\}$ (Anzahl: $n-1$).
     - Anzahl Tauben: n.
     - **PHP:** Da $n > n-1$, müssen zwei verschiedene Summen s_i und s_j $(i < j)$ im gleichen Fach landen.
3. **Schlussfolgerung:**
   - $s_j \equiv s_i \pmod{n} \implies s_j - s_i \equiv 0 \pmod{n}$.
   - Die Differenz ist $s_j - s_i = a_{i+1} + \cdots + a_j$.
   - Diese Teilsumme ist durch n teilbar. $\square$

A3. Summenformel

Aufgabe: Sei $S = \{1, 2, \ldots, 9\}$. Beweise: Jede Teilmenge $A \subseteq S$ mit $|A| = 6$ enthält mindestens zwei verschiedene Elemente x, y mit $x + y = 10$.

Lösung A3

Strategie: Schubfachprinzip mit Partitionen

1. **Fächer (Partitionierung von S):** Wir bilden Paare, die sich zu 10 addieren:
   - $P_1 = \{1, 9\}$
   - $P_2 = \{2, 8\}$
   - $P_3 = \{3, 7\}$
   - $P_4 = \{4, 6\}$
   - $R = \{5\}$ (Rest) Insgesamt gibt es 5 "Fächer" (4 Paare + 1 Einzelgänger).
2. **Tauben:** Wir wählen 6 Elemente aus S (unsere Menge A).
3. **Anwendung PHP:**
   - Selbst im "schlimmsten" Fall wählen wir die 5 als Erstes.
   - Es verbleiben 5 weitere Elemente, die wir auf die 4 Paare $P_1, \ldots, P_4$ verteilen müssen.
   - Nach PHP muss mindestens ein Paar P_k vollständig in A enthalten sein (da $5 > 4$).
4. **Ergebnis:**
   - Ein vollständig gewähltes Paar $\{x, y\}$ erfüllt $x + y = 10$. $\square$

Bucket B: Relationen & Mengen

B1. Äquivalenzrelation

Aufgabe: Sei ρ eine reflexive Relation auf A mit der Eigenschaft:

$$a\rho b \wedge b\rho c \implies c\rho a$$

Beweise, dass ρ eine Äquivalenzrelation ist.

Lösung B1

Zu zeigen: Reflexiv, Symmetrisch, Transitiv.

1. **Reflexiv:** Gegeben in der Aufgabenstellung. ✓
2. **Symmetrisch:** $(a\rho b \implies b\rho a)$
   - Wir wissen: $a\rho a$ (Reflexivität).
   - Setze in der Bedingung $b = a$ und $c = b$: $a\rho a \wedge a\rho b \implies b\rho a$.
   - Da $a\rho a$ wahr ist, vereinfacht sich dies zu $a\rho b \implies b\rho a$. ✓
3. **Transitiv:** $(a\rho b \wedge b\rho c \implies a\rho c)$
   - Gegeben ist: $a\rho b \wedge b\rho c \implies c\rho a$.
   - Aus (2) wissen wir, dass ρ symmetrisch ist.
   - Also $c\rho a \implies a\rho c$.
   - Kombiniert: $a\rho b \wedge b\rho c \implies c\rho a \implies a\rho c$. ✓

B2. Komposition von Relationen

Aufgabe: Seien ρ und σ zwei Äquivalenzrelationen auf einer Menge A. Beweise: Wenn $\rho \circ \sigma = \sigma \circ \rho$, dann ist $\rho \circ \sigma$ eine Äquivalenzrelation. (Zeige hier nur die Symmetrie).

Lösung B2

Symmetrie: Zu zeigen: Wenn $(x, y) \in \rho \circ \sigma$, dann $(y, x) \in \rho \circ \sigma$.

- Sei $(x, y) \in \rho \circ \sigma$.
- Da $\rho \circ \sigma = \sigma \circ \rho$, gilt $(x, y) \in \sigma \circ \rho$.
- Das heisst, es existiert ein z, sodass $(x, z) \in \sigma$ und $(z, y) \in \rho$.
- Da σ und ρ symmetrisch sind (Äquivalenzrelationen), gilt $(z, x) \in \sigma$ und $(y, z) \in \rho$.
- Also $(y, z) \in \rho$ und $(z, x) \in \sigma \implies (y, x) \in \rho \circ \sigma$. ✓

B3. Partielle Ordnung

Aufgabe: Betrachte $\preceq$ auf $\mathbb{N}^2$: $(a,b) \preceq (c,d) \iff (a,b) = (c,d) \vee (a < c \wedge a + d \leq b + c)$.
Zeige: $\preceq$ ist eine partielle Ordnung (Antisymmetrie).

Lösung B3

Antisymmetrie: Sei $(a, b) \preceq (c, d)$ und $(c, d) \preceq (a, b)$. Zu zeigen: $(a, b) = (c, d)$.

- Annahme $(a, b) \neq (c, d)$.
- Dann gilt aus der Definition:
  1. $a < c \wedge a + d \leq b + c$
  2. $c < a \wedge c + b \leq d + a$
- $a < c$ und $c < a$ ist ein direkter Widerspruch!
- Daher muss die Annahme falsch sein.
- Es bleibt nur $(a, b) = (c, d)$. ✓

Bucket C: Zahlentheorie

C1. CRT-System

Aufgabe: Finde alle Lösungen x mit $0 \leq x < 180$ für:

$$x \equiv 2 \pmod{15}$$

$$x \equiv 8 \pmod{12}$$

Lösung C1

Strategie: Zerlegen in Primzahlpotenzen & CRT

1. **Analyse der Moduli:** $15 = 3 \cdot 5$ und $12 = 3 \cdot 4$. Da $\gcd(15, 12) = 3 \neq 1$, können wir CRT nicht direkt anwenden.
2. **Aufspalten der Gleichungen:**
   - $x \equiv 2 \pmod{15} \iff \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}$
   - $x \equiv 8 \pmod{12} \iff \begin{cases} x \equiv 8 \equiv 2 \pmod{3} \\ x \equiv 8 \equiv 0 \pmod{4} \end{cases}$
3. **Konsistenzprüfung:** Beide Gleichungen fordern $x \equiv 2 \pmod{3}$. Das ist konsistent! Wir fassen das System zusammen zu:

   3.1 $x \equiv 0 \pmod{4}$
   3.2 $x \equiv 2 \pmod{5}$
   3.3 $x \equiv 2 \pmod{3}$

4. **Schrittweises Lösen:**

   - **Schritt A (Mod 4 & 5):** Suche Zahl, die durch 4 teilbar ist und Rest 2 bei Division durch 5 lässt. Kandidaten (Vielfache von 4): $0, 4, 8, 12, \ldots$ $12 \equiv 2 \pmod 5$. ✓ $\implies x \equiv 12 \pmod{20}$ (da kgV$(4, 5) = 20$).
   - **Schritt B (Mod 20 & 3):** Wir haben $x = 20k + 12$. Einsetzen in $x \equiv 2 \pmod 3$: $20k + 12 \equiv 2 \pmod 3$ $2k + 0 \equiv 2 \pmod 3$ $2k \equiv 2 \pmod 3$ $\implies k \equiv 1 \pmod 3$.

5. **Gesamtlösung:** Setze $k = 3j + 1$ in $x = 20k + 12$ ein:
   $x = 20(3j + 1) + 12 = 60j + 20 + 12 = 60j + 32.$ $\implies x \equiv 32 \pmod{60}$.

   Lösungen in $[0, 180)$**:** $32, 92, 152$.

C2. RSA Key Calculation

Aufgabe: Gegeben RSA Public Key $(n, e) = (77, 7)$. Berechne den Secret Key d.

Lösung C2

1. **Parameter bestimmen:**
   - $n = 77 = 7 \cdot 11 \implies p = 7, q = 11.$
   - $\phi(n) = (p-1)(q-1) = 6 \cdot 10 = 60.$
2. **Ziel:** Finde d mit $e \cdot d \equiv 1 \pmod{\phi(n)}$, also $7d \equiv 1 \pmod{60}$.
3. **Erweiterter Euklidischer Algorithmus (EEA):** Wir stellen 1 als Linearkombination von 60 und 7 dar.

Gleichung	Umformung
$60 = 8 \cdot 7 + 4$	$4 = 60 - 8 \cdot 7$
$7 = 1 \cdot 4 + 3$	$3 = 7 - 1 \cdot 4$
$4 = 1 \cdot 3 + 1$	$1 = 4 - 1 \cdot 3$

- **Rückwärts einsetzen:**

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) \\ &= 2 \cdot 4 - 1 \cdot 7 \\ &= 2 \cdot (60 - 8 \cdot 7) - 1 \cdot 7 \\ &= 2 \cdot 60 - 16 \cdot 7 - 1 \cdot 7 \\ &= 2 \cdot 60 - 17 \cdot 7 \end{aligned}$$

4. **Ergebnis:** $-17 \cdot 7 \equiv 1 \pmod{60}$. $d \equiv -17 \equiv 43 \pmod{60}$.

   Antwort: $d = 43$.

C3. Teilbarkeits-Beweis

Aufgabe: Beweise: $\forall a, b, c \in \mathbb{Z} \setminus \{0\}$: Wenn $a \mid bc$ und $\gcd(a, b) = 1$, dann $a \mid c$.

Lösung C3

Zu zeigen: $a \mid bc \land \gcd(a,b) = 1 \implies a \mid c$.

1. **Bézout's Identity:** $\gcd(a,b) = 1 \implies \exists u, v \in \mathbb{Z} : ua + vb = 1$.
2. **Multipliziere mit c:** $c(ua + vb) = c \implies uac + vbc = c \quad (0)$.
3. **Teilbarkeit prüfen:**
   - $a \mid uac$ ist klar, da a ein Faktor ist. (1)
   - $a \mid vbc$ gilt, da $a \mid bc$ (Voraussetzung). (2)
4. **Kombinieren:**
   - Aus (1) und (2) folgt: a teilt die Summe $(uac + vbc)$.
   - Wegen (0) ist die Summe gleich c.
   - $\implies a \mid c$. $\square$

Bucket D: Algebra

D1. Injektiver Homomorphismus

Aufgabe: Existiert ein injektiver Homomorphismus $\psi : \mathbb{Z}_{14}^* \to \mathbb{Z}_{14}$?

Lösung D1

Strategie: Vergleich der Elementordnungen

1. **Ordnung der Gruppe $\mathbb{Z}_{14}^*$:**
   - $\mathbb{Z}_{14}^* = \{x \in \mathbb{Z}_{14} \mid \gcd(x, 14) = 1\} = \{1, 3, 5, 9, 11, 13\}$.
   - Die Gruppenordnung ist $|\mathbb{Z}_{14}^*| = \phi(14) = \phi(2)\phi(7) = 1 \cdot 6 = 6$.
   - Das Element $3 \in \mathbb{Z}_{14}^*$ hat Ordnung 6 ($3^1 = 3, 3^2 = 9, 3^3 = 27 \equiv 13, \ldots, 3^6 \equiv 1$).
2. **Eigenschaft von Homomorphismen:**
   - Ein injektiver Homomorphismus ψ muss die Ordnung von Elementen erhalten: $\mathsf{ord}(\psi(x)) = \mathsf{ord}(x)$.
   - Also müsste $\psi(3)$ in der Zielgruppe $(\mathbb{Z}_{14}, +)$ ein Element der Ordnung 6 sein.
3. **Analyse der Zielgruppe $(\mathbb{Z}_{14}, +)$:**
   - Die Ordnung eines Elements $y \in \mathbb{Z}_{14}$ ist $k = \frac{14}{\gcd(y,14)}$.
   - Dies ist immer ein Teiler von 14.
   - 6 ist *kein* Teiler von 14.
4. **Fazit:** Es gibt kein Element der Ordnung 6 in $\mathbb{Z}_{14}$. Daher kann kein solcher Homomorphismus existieren.

D2. Polynome & Körper

Aufgabe: Bestimme alle Nullstellen von $2x^2 + 3x + 1$ in $\mathbb{Z}_5$.

Lösung D2

Strategie: Einsetzen aller Elemente (Brute Force)

Da der Körper $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ klein ist, testen wir alle Werte:

x	$2x^2 + 3x + 1 \pmod 5$	Ergebnis
0	$0 + 0 + 1 = 1$	$\neq 0$
1	$2(1) + 3(1) + 1 = 6 \equiv 1$	$\neq 0$
2	$2(4) + 3(2) + 1 =$ $8 + 6 + 1 = 15 \equiv 0$	**Nullstelle**
3	$2(9) + 3(3) + 1 =$ $18 + 9 + 1 = 28 \equiv 3$	$\neq 0$
4	$2(16) + 3(4) + 1 =$ $32 + 12 + 1 = 45 \equiv 0$	**Nullstelle**

Antwort: Die Nullstellen sind $x_1 = 2$ und $x_2 = 4$.

D3. Isomorphie-Check

Aufgabe: Beweise, dass $\mathbb{Z}_{12}^*$ und $\mathbb{Z}_4$ nicht isomorph sind.

Lösung D3

Strategie: Struktureller Vergleich (Zyklizität)

1. **Gruppe 1:** $(\mathbb{Z}_4, +)$
   - Elemente: $\{0, 1, 2, 3\}$.
   - Das Element 1 ist ein Generator, da $\langle 1 \rangle = \{1, 2, 3, 0\} = \mathbb{Z}_4$.
   - $\implies$ $\mathbb{Z}_4$ ist **zyklisch**.
2. **Gruppe 2:** $(\mathbb{Z}_{12}^*, \cdot)$
   - Elemente: $\{1, 5, 7, 11\}$. (Ordnung 4).
   - Wir prüfen die Ordnung aller Elemente:
     - $1^1 = 1$ (Ordnung 1)
     - $5^2 = 25 \equiv 1$ (Ordnung 2)
     - $7^2 = 49 \equiv 1$ (Ordnung 2)
     - $11^2 = 121 \equiv 1$ (Ordnung 2)
   - Es gibt kein Element der Ordnung 4.
   - $\implies$ $\mathbb{Z}_{12}^*$ ist **nicht zyklisch** (isomorph zur Kleinschen Vierergruppe V_4).
3. **Fazit:** Da eine Gruppe zyklisch ist und die andere nicht, können sie nicht isomorph sein. $\square$

Bucket E: Logik

E1. Prenex Normal Form

Aufgabe: Finde eine äquivalente Formel in PNF für:

$$\neg\forall x(P(x) \vee \neg Q(y)) \wedge \exists y(P(x) \vee Q(y))$$

Lösung E1

Strategie: Schrittweise Transformation

1. **Variablen bereinigen (Bound Variable Renaming):** Wir zerlegen die Formel in zwei Teile:

$$\underbrace{\neg\forall x(P(x) \vee \neg Q(y))}_{L} \wedge \underbrace{\exists y(P(x) \vee Q(y))}_{R}$$

- In L ist x gebunden. Wir benennen es um zu u: $L' = L[x/u] = \neg\forall u(P(u) \vee \neg Q(y))$.
- In R ist y gebunden. Wir benennen es um zu v: $R' = R[y/v] = \exists v(P(x) \vee Q(v))$.

Neue Formel: $\neg\forall u(P(u) \vee \neg Q(y)) \wedge \exists v(P(x) \vee Q(v))$.

2. **Negation nach innen ziehen:**
   - $\neg\forall u(\dots) \equiv \exists u\neg(\dots)$
   - $\exists u\neg(P(u) \vee \neg Q(y)) \wedge \exists v(P(x) \vee Q(v))$
   - De Morgan: $\exists u(\neg P(u) \wedge Q(y)) \wedge \exists v(P(x) \vee Q(v))$
3. **Quantoren nach vorne ziehen (Prenexing):**
   - Da u nicht im zweiten Teil und v nicht im ersten Teil vorkommt, können wir sie ganz nach vorne ziehen.
   - $\exists u\exists v((\neg P(u) \wedge Q(y)) \wedge (P(x) \vee Q(v)))$

E2. Modell finden

Aufgabe: Finde ein Modell für die Formel $\forall x P(f(x), y)$ der Prädikatenlogik.

Lösung E2

Strategie: Konstruktion eines minimalen Modells

Wir definieren eine Struktur $\mathcal{A} = (U, P^{\mathcal{A}}, f^{\mathcal{A}}, y^{\mathcal{A}})$, die die Formel wahr macht.

1. **Universum:** Wähle $U = \{0\}$ (ein einziges Element reicht oft).
2. **Konstante** y**:** Setze $y^{\mathcal{A}} = 0$.
3. **Funktion** f**:** Setze $f^{\mathcal{A}}(0) = 0$.
4. **Prädikat** P**:**
   - Die Formel verlangt: Für alle $x \in U$ gilt $P(f(x), y)$.
   - Hier: $P(f(0), 0) \implies P(0, 0)$.
   - Wir definieren $P^{\mathcal{A}} = \{(0, 0)\}$ (d.h. P ist immer wahr).

Überprüfung: $\forall x \in \{0\} : P^{\mathcal{A}}(f^{\mathcal{A}}(x), y^{\mathcal{A}}) \iff P^{\mathcal{A}}(0, 0) \iff$ Wahr. ✓

Teil 4: Hard(er) Mode

H1: Isomorphie

Aufgabe: Sind $(\mathbb{Z}_4, +)$ und $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ isomorph?

Lösung H1

Antwort: Nein.

Begründung über Elementordnungen:

1. **Gruppe $(\mathbb{Z}_4, +)$:**
   - Elemente: $\{0, 1, 2, 3\}$.
   - Ordnung von 1: $1 \to 2 \to 3 \to 0$. (Ordnung 4).
   - Ordnung von 3: $3 \to 2 \to 1 \to 0$. (Ordnung 4).
   - Es gibt Elemente der Ordnung 4.
2. **Gruppe $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$:**
   - Elemente: $\{(0,0), (0,1), (1,0), (1,1)\}$.
   - Addition ist komponentenweise modulo 2.
   - Für jedes Element $x \in V_4$ gilt $x + x = (0,0)$.
   - Das bedeutet: Jedes Element (außer dem neutralen) hat Ordnung 2.
3. **Schlussfolgerung:** Ein Isomorphismus müsste die Ordnung von Elementen erhalten. Da $\mathbb{Z}_4$ Elemente der Ordnung 4 hat, V_4 aber nicht, können sie nicht isomorph sein.

H2: Zahlentheorie Beweis

Aufgabe: Seien $a, b, c, d \in \mathbb{N}_{\geq 1}$. Beweise: $ab = cd \implies a + b + c + d$ ist nicht prim.

Lösung H2

Strategie: Parametrisierung der Gleichung $ab = cd$

1. **Setze:** $g = \gcd(a, c)$.
   - Wir können schreiben: $a = g \cdot x$ und $c = g \cdot y$, wobei $\gcd(x, y) = 1$.
2. **Einsetzen in $ab = cd$:**
   - $(gx)b = (gy)d \implies xb = yd$.
   - Da $\gcd(x, y) = 1$, muss x ein Teiler von d sein ($x \mid d$).
   - Also existiert ein $z \in \mathbb{N}$, sodass $d = x \cdot z$.
   - Daraus folgt auch $b = y \cdot z$.
3. **Summe berechnen:**
   - $a + b + c + d = gx + yz + gy + xz$.
4. **Faktorisieren:**
   - Gruppiere Terme: $g(x + y) + z(y + x)$.
   - Klammere aus: $(g + z)(x + y)$.
5. **Prüfung auf Primzahl:**
   - Da $a, b, c, d \geq 1$, sind $g, x, y, z \geq 1$.
   - Damit sind beide Faktoren $(g + z) \geq 2$ und $(x + y) \geq 2$.
   - Eine Zahl, die in zwei Faktoren > 1 zerlegt werden kann, ist **zusammengesetzt** (nicht prim).

□

H3: Satz von Cantor

Aufgabe: Beweise $|\mathcal{P}(A)| > |A|$ für jede Menge A.

Lösung H3

Beweis durch Widerspruch (Diagonalargument):

1. **Annahme:** Es existiert eine Surjektion $f : A \to \mathcal{P}(A)$. (D.h. jedes Element der Potenzmenge wird von f getroffen).
2. **Konstruktion der "bösen" Menge D:** Wir definieren $D = \{x \in A \mid x \notin f(x)\}$. (Dies ist die Menge aller Elemente, die *nicht* in ihrem eigenen Bild enthalten sind). Da $D \subseteq A$, ist $D \in \mathcal{P}(A)$.
3. **Der Widerspruch:**
   - Da f surjektiv ist, muss es ein Urbild $a \in A$ geben mit $f(a) = D$.
   - Frage: Ist $a \in D$?
   - **Fall 1:** $a \in D$. $\implies$ Nach Def. von D gilt $a \notin f(a)$. $\implies$ Da $f(a) = D$, heisst das $a \notin D$. (Widerspruch!)
   - **Fall 2:** $a \notin D$. $\implies$ Nach Def. von D gilt $a \in f(a)$. $\implies$ Da $f(a) = D$, heisst das $a \in D$. (Widerspruch!)
4. **Fazit:** Die Annahme war falsch. Es gibt keine Surjektion. Da $|A| \leq |\mathcal{P}(A)|$ trivial ist, folgt $|A| < |\mathcal{P}(A)|$. $\square$

H4: Zigzag Funktion

Aufgabe: Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ heisst "Zigzag", wenn sie immer abwechselnd grösser/kleiner wird (z.B. $f(0) < f(1) > f(2) < f(3)$...). Ist die Menge aller Zigzag-Funktionen abzählbar?

Lösung H4

Antwort: Nein, überabzählbar.

Strategie: Injektion von $\{0,1\}^{\mathbb{N}}$ (Menge aller Binärfolgen) Wir zeigen, dass wir jede unendliche Binärfolge $b = (b_0, b_1, b_2, \dots)$ eindeutig in eine Zigzag-Funktion kodieren können. Da die Menge der Binärfolgen überabzählbar ist (Cantor), muss auch die Menge der Zigzag-Funktionen überabzählbar sein.

1. Konstruktion: Wir definieren $f_b(n)$ rekursiv, sodass die Schrittweite $|f(n) - f(n-1)|$ das Bit b_{n-1} kodiert.

- **Kodierung:**
  - Bit $0 \to$ Schrittweite 1.
  - Bit $1 \to$ Schrittweite 2.
- **Zigzag-Bedingung:**
  - n ungerade $(1, 3, \dots)$: Wir müssen **hoch** $(f(n) > f(n-1))$.
  - n gerade $(2, 4, \dots)$: Wir müssen **runter** $(f(n) < f(n-1))$.

2. Beispiel: Sei die Folge $b = (0, 1, 0, \dots)$. Startwert $f(0) = 10$.

- $n = 1$ **(Bit $b_0 = 0$):** Wir müssen **hoch**.
  - Bit $0 \implies$ Schrittweite 1.
  - $f(1) = f(0) + 1 = 11$.
- $n = 2$ **(Bit $b_1 = 1$):** Wir müssen **runter**.
  - Bit $1 \implies$ Schrittweite 2.
  - $f(2) = f(1) - 2 = 9$.
- $n = 3$ **(Bit $b_2 = 0$):** Wir müssen **hoch**.
  - Bit $0 \implies$ Schrittweite 1.
  - $f(3) = f(2) + 1 = 10$.

Die Funktion ist $10, 11, 9, 10, \dots$ (Zigzag erfüllt).

3. Eindeutigkeit (Injektivität): Aus der Funktion können wir die Folge b rekonstruieren: $b_{n-1} = |f(n) - f(n-1)| - 1$. Unterschiedliche Folgen erzeugen unterschiedliche Funktionen. $\square$

H5: Logik Folgerung

Aufgabe: Beweise oder widerlege: $(\forall x F) \vee G \models \forall x (F \vee G)$.

Lösung H5

Beweis: Es gilt.

Wir müssen zeigen: Jedes Modell $\mathcal{A}$, das die Prämisse $(\forall x F) \vee G$ wahr macht, macht auch die Konklusion $\forall x(F \vee G)$ wahr.

Sei $\mathcal{A}$ ein beliebiges Modell mit $\mathcal{A} \vDash (\forall x F) \vee G$. Das bedeutet, mindestens einer der beiden Teile ist wahr:

1. **Fall 1:** $\mathcal{A} \vDash G$**.**
   - Dann ist G wahr (unabhängig von x).
   - Damit ist auch die Disjunktion $(F \vee G)$ für jedes x wahr.
   - Also gilt $\forall x(F \vee G)$.
2. **Fall 2:** $\mathcal{A} \vDash \forall x F$**.**
   - Das bedeutet: Für alle $d \in U$ gilt $F[x/d]$.
   - Wenn F wahr ist, ist auch $(F \vee G)$ wahr (Einführung der Disjunktion).
   - Also gilt für alle x: $(F \vee G)$.
   - Also gilt $\forall x(F \vee G)$.

In beiden Fällen folgt die Konklusion. $\square$

Teil 5: Survival Guide

General Learning Principles

1. **Intensity $\gg$ Duration**
   - Lerne nicht 10 Stunden "halbwach". Lerne 4 Stunden mit **voller Intensität**.
   - Deep Work: Handy weg, Fokus an. Qualität der Stunden schlägt Quantität.
2. **Sleep is Part of the Job**
   - Schlaf ist keine Zeitverschwendung.
   - Im Schlaf passiert **Memory Consolidation**. Wer nicht schläft, speichert nicht.
3. **The Feynman Technique**
   - Erkläre das Konzept einem Freund, mach dir ein eigenes Cheatsheet (!).
   - Wenn du stockst oder Fachbegriffe als "Black Box" benutzt, hast du eine Wissenslücke.

Exam Strategy: Think RL

1. **Reinforcement Learning Loop**
   - Dein Gehirn lernt wie ein RL-Agent: **Action** $\rightarrow$ **Feedback** $\rightarrow$ **Update**.
   - Löse Aufgaben und hole dir *sofort* Feedback (Lösung vergleichen).
   - Ohne Feedback kein Lernen.
2. **Quantity + Quality**
   - **Quantity:** Löse viele Aufgaben, um Mustererkennung (Pattern Matching) aufzubauen.
   - **Quality:** Verstehe bei jeder Aufgabe das *Warum*. "Warum dieser Schritt?"
3. **Simulation**
   - Löse alte Prüfungen unter **Realbedingungen** (Timer, keine Musik, nur erlaubte Hilfsmittel).

DM Specifics: The 80/20 Rule

Der High-Value-Cluster (Punktegaranten):

- ✓ **Induktion**
- ✓ **Äquivalenz/POSETs**
- ✓ **Number Theory Restrechnungen**
- ✓ **Euclid+Inverse**
- ✓ **Resolution**
- ✓ **Definitionen Anwenden**
- ✓ ...

Fokussiere dich auf diese Basics, wenn du sicher bestehen willst.

One Last Thing...

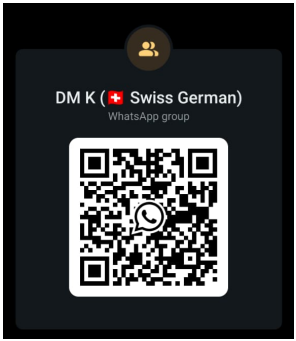
ETH ist hart.

- Es ist normal, sich manchmal überfordert zu fühlen.
- Jeder kämpft hier – auch die, bei denen es “einfach” aussieht.
- Lass dich nicht von schlechten Tagen oder schwierigen Phasen entmutigen.

Danke, dass ihr dabei wart!

- Es hat mir unglaublich viel Spass gemacht, diese Übungsstunde zu halten.
- Falls ihr Fragen (Diskmat, zu den anderen Fächern, oder Generell) feel free to reach out :D

Viel Erfolg bei der Prüfung! Ihr schafft das.


DM K (Swiss German)
WhatsApp group