Matrikelnummer:

Prof. Dr. Stephan Kreutzer
FG Logik und Semantik
Technische Universität Berlin

SoSe 2025

Schriftlicher Test Diskrete Strukturen

Aufgabe:	1	2	3
Punkte:			

Summe:

Punkte: Insgesamt sind in dieser Teilleistung 200 Testpunkte zu erreichen. 4 Testpunkte entsprechen einem Portfoliopunkt. Es können maximal 50 Portfoliopunkte erarbeitet werden.
Bearbeitungszeit: Die Bearbeitungszeit beträgt 60 Minuten.

Alle Antworten sind zu begründen, es sei denn, dies wird **explizit** ausgeschlossen.

Aufgabe 1 $20 + 20 + 25 + 15 = 80$ Punkte

(i) Zeigen Sie $3 \mid a(a^2 - 1)$ für alle $a \in \mathbb{Z}$.

(ii) Sei $\text{ggT}(a, b) = 1$ und $c \mid (a + b)$. Zeigen Sie, dass a und c teilerfremd sind.

(iii) Geben Sie alle $(a, b) \in \mathbb{Z}_{31} \times \mathbb{Z}$ an, sodass $11a + 31b = 1$.

(iv) Sei $l = 7$ und $k = 7$. Finden Sie ein n, sodass (l, n) und (k, n) ein gültiges RSA-Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel sind. Begründen sie, dass es sich um ein gültiges Schlüsselpaar handelt.

Lösung zu Aufgabe 1

(i) Wir machen eine Fallunterscheidung bezüglich $a \mod 3$ und zeigen dass in allen drei Fällen $3 \mid a$ oder $3 \mid (a^2 - 1)$ gilt.

- Für $a = 3k$ folgt direkt $3|a$.
- Für $a = 3k + 1$ gilt $a^2 - 1 = 9k^2 + 6k + 1 - 1 = 3(3k^2 + 2k)$ und somit $3 \mid (a^2 - 1)$.
- Für $a = 3k + 2$ gilt $a^2 - 1 = 9k^2 + 12k + 4 - 1 = 3(3k^2 + 4k + 1)$ und somit $3 \mid (a^2 - 1)$.

Alternativ kann auch der kleine Satz von Fermat genutzt werden.

(ii) Sei d ein gemeinsamer Teiler von a und c, d.h. $d \mid a$ und $d \mid c$. Dann gilt wegen $c \mid (a + b)$ auch $d \mid (a + b)$. Es folgt $d \mid a + b - a$, also $d \mid b$ wegen $d \mid a$. Da $\text{ggT}(a, b) = 1$ ist, folgt $d = 1$.

(iii) Wir bestimmen mit dem erweiterten euklidschen Algorithmus a' und b' sodass $11a' + 31b' = 1$. Dies ist möglich da $\text{ggT}(11, 31) = 1$ ist.

$$
\begin{aligned}
31 - 2 \cdot 11 &= 9 \\
11 - 1 \cdot 9 &= 2 \\
9 - 4 \cdot 2 &= 1 \\
1 &= 9 - 4 \cdot 2 \\
1 &= 9 - 4 \cdot (11 - 1 \cdot 9) = -4 \cdot 11 + 5 \cdot 9 \\
1 &= -4 \cdot 11 + 5 \cdot (31 - 2 \cdot 11) = 5 \cdot 31 - 14 \cdot 11
\end{aligned}
$$

Also $a' = -14$ und $b' = 5$. Es folgt dass $a = a' + 31 = 17$ und $b' = b - 11 = -6$ die gesuchte Lösung ist. Nach Satz aus der VL ist $a = 17 \in \mathbb{Z}_{31}$ eine eindeutige Lösung für die Gleichung $11a \equiv 1 \pmod{31}$. Durch a ist auch b und somit die gesamte Lösung eindeutig bestimmt.

(iv) Es muss gelten

$$
\begin{aligned}
l \cdot k &\equiv 1 \pmod{\varphi(n)} \\
7 \cdot 7 &\equiv 1 \pmod{\varphi(n)} \\
49 &\equiv 1 \pmod{\varphi(n)} \\
48 &\equiv 0 \pmod{\varphi(n)}
\end{aligned}
$$

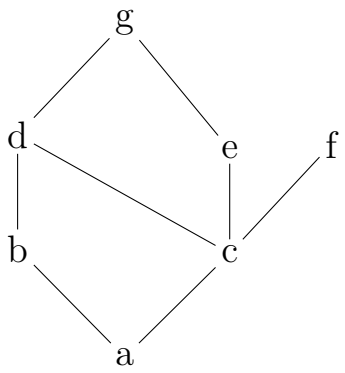
Zudem muss gelten, dass $\varphi(n) = (p - 1) \cdot (q - 1)$. Somit müssen $p - 1$ und $q - 1$ Teiler von 48 sein. Eine mögliche Wahl ist $p - 1 = 12$ und $q - 1 = 4$, da 13 und 5 Primzahlen sind. Dann gilt $n = 65$ und $\varphi(n) = 48$ was ein korrekter Schlüssel ist, da p und q Primzahlen sind und $49 \equiv 1 \pmod{48}$ ist.

Aufgabe 2 12 + 8 + 27 + 18 = 65 Punkte

Sei R eine partielle Ordnung auf einer nicht-leeren Menge M. Wir definieren den Unvergleichbarkeitsgraphen G_R durch:

$$V(G_R) := M,$$
$$E(G_R) := \{\{u, v\} \in \mathcal{P}_2(M) \mid (u, v) \notin R \text{ und } (v, u) \notin R\}.$$

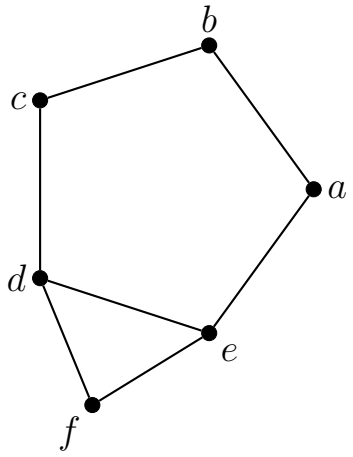
(i) Zeichnen Sie den Unvergleichbarkeitsgraphen für die zu folgendem Hasse Diagramm gehörende partielle Ordnung.



(ii) Sei R eine partielle Ordnung auf einer nicht-leeren Menge M. Zeigen Sie, dass der induzierte Teilgraph jeder Kette von R eine unabhängige Menge in G_R ist.

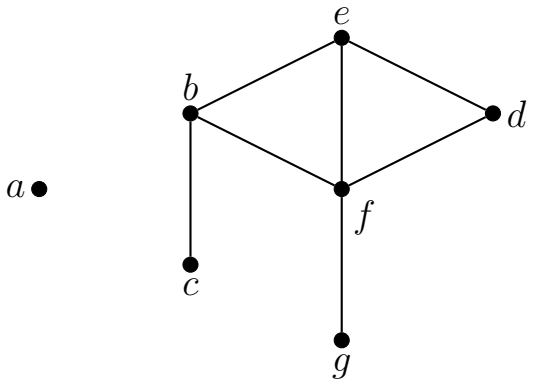
(iii) Zeigen Sie, dass für jeden Unvergleichbarkeitsgraphen die chromatische Zahl gleich der maximalen Größe eines vollständigen Untergraphen ist.

(iv) Ist der folgende Graph der Unvergleichbarkeitsgraph einer partiellen Ordnung?



Lösung zu Aufgabe 2

(i) Für den zugehörigen Unvergleichbarkeitsgraphen erhält man



(ii) Sei S eine Kette. Dann gilt nach Definition für alle $a \neq b$ aus S entweder $(a, b) \in R$ oder $(b, a) \in R$. Nach Definition des Unvergleichbarkeitsgraphen gibt es dann zwischen den Knoten a und b keine Kante. Also ist S eine unabhängige Menge in G_R.

(iii) Sei G ein Unvergleichbarkeitsgraph und k die Größe des größten vollständigen Untergraphen. Es gilt offensichtlich $k \leq \chi(G)$. Nach Definition des Unvergleichbarkeitsgraphen stimmt k mit der maximalen Größe einer Antikette überein. Nach dem Satz von Dilworth existiert also eine Überdeckung durch k Ketten. Färbt man alle Knoten einer Kette mit einer Farbe, so bekommt man eine valide k-Färbung denn nach der ii) bilden alle Ketten unabhängige Mengen in G.

(iv) Nein, der Graph ist kein Unvergleichbarkeitsgraph. Wir geben hier zwei alternative Beweise an. Sei jeweils angenommen, dass es eine partielle Ordnung $\sqsubseteq$ gegebenem Graphen als Unvergleichbarkeitsgraphen gibt.

a) Wenn $\sqsubseteq$ eine partielle Ordnung auf S ist, dann folgt aus der Definition, dass auch $\sqsubseteq$ eingeschränkt auf $S \setminus \{f\}$ eine partielle Ordnung ist. Der Unvergleichbarkeitsgraph von dieser Ordnung wäre der Kreis mit fünf Knoten, was nach der iii) aber kein Unvergleichbarkeitsgraph sein kann.

b) Nach Definition sind a und c vergleichbar. Sei also o.B.d.A. $a \sqsubseteq c$. Da auch a und d vergleichbar sind aber c und d unvergleichbar sind, folgt wegen der Transitivität $a \sqsubseteq d$. Weiter ist d mit b vergleichbar aber a nicht mit b. Somit folgt wegen der Transitivität $b \sqsubseteq d$. Analog folgt $e \sqsubseteq c$. Nun sind aber auch d und e vergleichbar, aber aus $d \sqsubseteq e$ folgt mit der Transitivität $d \sqsubseteq c$ was ein Widerspruch zur Unvergleichbarkeit von c und d ist. Analoges Argument gilt für $e \sqsubseteq d$.

Aufgabe 3 15 + 25 + 15 = 55 Punkte

Wir definieren $\mathcal{P}_\infty(\mathbb{N})$ als die Menge aller unendlich großen Teilmengen von $\mathbb{N}$, d.h.

$$\mathcal{P}_\infty(\mathbb{N}) := \{A \subseteq \mathbb{N} : |A| = \infty\}.$$

(i) Zeigen oder widerlegen Sie: $(\mathcal{P}_\infty(\mathbb{N}), \cap)$ ist ein Monoid.

Für zwei Mengen A und B definieren wir die symmetrische Differenz durch

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

Sie dürfen ohne Beweis die Assoziativität der symmetrischen Differenz annehmen.

(ii) Zeigen Sie, dass $(\mathcal{P}(\mathbb{N}), \Delta)$ eine Gruppe ist.

(iii) Sei $a +_2 b := a + b \pmod 2$. Es ist bekannt, dass $(\{0,1\}, +_2)$ eine Gruppe ist. Geben sie ohne Begründung einen Homomorphismus h von $(\mathcal{P}(\mathbb{N}), \Delta)$ nach $(\{0,1\}, +_2)$ an für den mindestens eine Menge $A \in \mathcal{P}(\mathbb{N})$ mit $h(A) = 1$ existiert.

Lösung zu Aufgabe 3

(i) $(\mathcal{P}_\infty(\mathbb{N}), \cap)$ ist kein Monoid. Der Grund dafür ist die Abgeschlossenheit. Sei A die Menge aller geraden Zahlen und B die Menge aller ungeraden Zahlen. Dann ist $A \cap B$ die leere Menge und somit nicht in $\mathcal{P}_\infty(\mathbb{N})$ enthalten.

(ii) Wir zeigen alle Eigenschaften einer Gruppe.

- Die Abgeschlossenheit folgt aus der Definition da die Potenzmenge jede Teilmenge enthält.
- Die Assoziativität darf angenommen werden.
- Die leere Menge ist das neutrale Element, denn es gilt $A \Delta \emptyset = \emptyset \Delta A = (\emptyset \setminus A) \cup (A \setminus \emptyset) = A$.
- Jede Element ist zu sich selbst invers, denn $A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset$.

(iii) Für eine beliebige Zahl $n \in \mathbb{N}$ definieren wir

$$h_n(A) \coloneqq \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A. \end{cases}$$

Dies ist ein Homomorphismus, da $h_n(A \Delta B) = 1$ genau dann wenn n in genau einer der beiden Mengen A oder B enthalten ist. Dies ist genau der Fall in dem $h_n(A) +_2 h_n(B) = 1$ gilt.