Matrikelnummer:

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

SoSe 2024

Schriftlicher Test Diskrete Strukturen

Aufgabe:	1	2	3
Punkte:			

Summe:

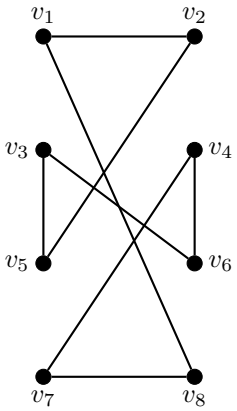
Punkte: Insgesamt sind in dieser Teilleistung 200 Testpunkte zu erreichen. 4 Testpunkte entsprechen einem Portfoliopunkt. Es können maximal 50 Portfoliopunkte erarbeitet werden.

Bearbeitungszeit: Die Bearbeitungszeit beträgt 60 Minuten. Zudem gibt es 15 Minuten Einlesezeit.

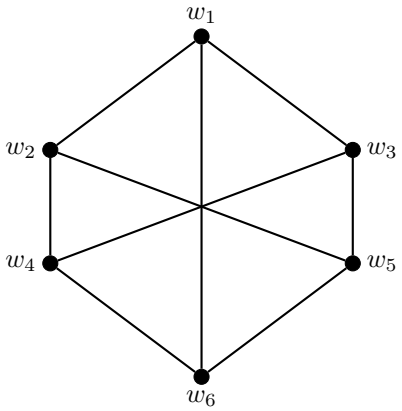
Alle Antworten sind zu begründen, es sei denn, dies wird **explizit** ausgeschlossen.

Aufgabe 1 18 + 10 + 12 + 20 = 60 Punkte

G_1 :



G_2 :



Sei $G_3 = (V_3, E_3)$ mit

$$V_3 = \{0, 1, 2, 3, 4\}$$
$$E_3 = \{\{x, y\} \mid x, y \in V_3, |x - y| = 1\} \cup \{\{0, 4\}\}.$$

Wir definieren $\mathcal{P}$ als die Menge der planaren Graphen. Zudem definieren wir die 2-stellige Relation $\lhd$ auf $\mathcal{P}$ wie folgt:

$$G \lhd G', \text{ falls } \chi(G) < \chi(G')$$

Hinweis: In dieser Aufgabe werden nur Graphen mit nichtleerer Knotenmenge betrachtet.

(i) Bestimmen Sie für $(G_1, G_3), (G_2, G_3)$ und (G_3, G_1), ob sie in $\lhd$ sind. Die Antworten sind zu begründen.

(ii) Geben Sie 2 planare Graphen H und I an, für die gilt, dass $|E(H)| \neq |E(I)|$ und $(H, I), (I, H) \notin \lhd$. Begründen Sie ihre Wahl.

(iii) Begründen Sie, dass $(P, \lhd)$ eine strikte partielle Ordnung ist. (Eine strikte partielle Ordnung ist irreflexiv, transitiv und antisymmetrisch)

Sei $\trianglelefteq$ die minimale partielle Ordnung über $\mathcal{P}$, die $\lhd$ enthält.

(iv) Geben Sie für $(\mathcal{P}, \trianglelefteq)$ eine Kette maximaler Länge an und geben sie eine Überdeckung minimaler Größe von $(\mathcal{P}, \trianglelefteq)$ durch Antiketten an. Begründen Sie kurz warum ihre Überdeckung $\mathcal{P}$ überdeckt und warum es keine Überdeckung kleinerer Größe gibt.

Lösung zu Aufgabe 1

(i) Da G_2 nicht planar ist, ist (G_2, G_3) nicht in $\lhd$. G_1 und G_3 sind beide planar. Da $\chi(G_1) = 2 < 3 = \chi(G_3)$, ist (G_1, G_3) in $\lhd$ und (G_3, G_1) nicht.

(ii) Für die Pfade P_2 und P_3 mit 2 bzw. 3 Knoten gilt $|E(P_2)| = 1 < 2 = |E(P_3)$ und $\chi(P_2) = 2 = \chi(P_3)$. Da nicht 2 nicht kleiner als 2 ist erfüllen sie die Aufgabe.

(iii) $\lhd$ ist irrflexiv, da für alle Graphen gilt, dass $\chi(G) \not< \chi(G)$. $\lhd$ ist transitiv, da wenn $\chi(G) < \chi(G')$ und $\chi(G') < \chi(G'')$ auch $\chi(G) < \chi(G'')$. $\lhd$ ist antisymmetrisch, da die chromatischen Zahlen von zwei Graphen nicht größer und kleiner als die andere sein können.

(iv) Eine längste Kette bilden die vollständigen Graphen K_1, K_2, K_3 und K_4. Eine Zerlegung in Antiketten von $(\mathcal{P}, \trianglelefteq)$ sind die Antiketten $C_i = \{G | \chi(G) = i$ für $i \in \{1, 2, 3, 4\}$. Es kann keine kleinere Zerlegung geben, da es eine Kette der Länge 4 gibt und sie überdeckt alle planaren Graphen, da alle planaren Graphen 4-färbbar sind.

Aufgabe 2 12 + 20 + 18 + 20 = 70 Punkte

(i) Berechnen Sie 5^{27} mod 13 ohne explizit eine Zahl größer als 13^2 zu nutzen.

(ii) Geben Sie alle ganzen Zahlen x an, die die folgende Gleichung erfüllen:

$$(14 \cdot x) \bmod 15 = 13$$

Begründen Sie ihr Ergebnis.

(iii) Sei $l = 9$ und $k = 5$. 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.

(iv) Sei $a \cdot b \equiv 21 \pmod{840}$ und $\text{ggt}(a, 840) = 1$. Bestimmen Sie $\text{ggt}(b, 840)$ oder zeigen Sie, dass $\text{ggt}(b, 840)$ nicht eindeutig bestimmt werden kann.

Lösung zu Aufgabe 2

(i) Es gilt:

$$\begin{aligned} 5^2 &\equiv 12 \pmod{13} \\ 5^4 \equiv (5^2)^2 &\equiv 1 \pmod{13} \\ 5^8 \equiv (5^4)^2 &\equiv 1 \pmod{13} \\ 5^{16} \equiv (5^8)^2 &\equiv 1 \pmod{13} \\ 5^{27} \equiv 5^{16} \cdot 5^8 \cdot 5^2 \cdot 5 \equiv 5^3 &\equiv 8 \pmod{13} \end{aligned}$$

(ii) $x = 2$ erfüllt die Gleichung. Alle Lösungen haben die Form $x = 2 + k \cdot 15$ für $k \in \mathbb{Z}$. Diese Lösungen erfüllen die Gleichung da $a \bmod 15 = 2$ und es sind alle Lösungen, da für jede Lösung gelten muss, dass $9 \cdot (a-2)$ durch 15 teilbar ist und da 14 teilerfremd zu 15 ist und somit $a-2$ durch 15 teilbar sein muss.

(iii) Es muss gelten

$$l \cdot k \equiv 1 \pmod{\varphi(n)) 9 \cdot 5 \equiv 1 \pmod{\varphi(n))} 45 \equiv 1 \pmod{\varphi(n))} 44 \equiv 0 \pmod{\varphi(n))}$$

Zudem muss gelten, dass $\varphi(n) = (p-1) \cdot (q-1)$. Somit müssen $p-1$ und $q-1$ teiler von 44 sein. Eine mögliche Wahl ist $p-1 = 22$ und $q-1 = 2$, da 23 und 3 Primzahlen sind. Dann gilt $n = 69$ und $\varphi(n) = 44$ was ein korrekter Schlüssel ist, da p und q Primzahlen sind und $45 \equiv 1 \pmod{44}$ ist.

(iv) 21 teilt 840. Da $a \cdot b = 21 + k \cdot 840 = 21 \cdot (1 + k \cdot 40)$ ist, ist $a \cdot b$ durch 21 teilbar. Da $\text{ggt}(a, 840) = 1$ ist, folgt, dass b durch 21 teilbar ist. Wäre $\text{ggt}(b, 840) = x > 21$, dann würde gelten, dass x Teiler von 21 ist, da x $a \cdot b$ und $k \cdot 840$ teilt.

Aufgabe 3 $6 + 6 + 13 + 25 + 14 + 6 = 70$ Punkte

Wir definieren die Menge $F := \{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ ist eine Funktion}\}$.

Die Relation $R \subseteq F \times F$ sei definiert durch $(f_1, f_2) \in R$, falls $f_1(1) = f_2(1)$ für $f_1, f_2 \in F$.

(i) Geben Sie ohne Begründung zwei verschiedene Elemente $g_1, g_2 \in F$ an, für die $(g_1, g_2) \notin R$ gilt.

(ii) Geben Sie ohne Begründung zwei verschiedene Elemente $g_1, g_2 \in F$ an, für die $(g_1, g_2) \in R$ gilt.

(iii) Zeigen Sie, dass R eine Äquivalenzrelation ist.

Weiter sei die Verknüpfung $+_F$ auf F, die Funktionen f_1 und f_2 zur Funktion $(f_1 +_F f_2)$ verknüpft, definiert durch

$$(f_1 +_F f_2)(z) := f_1(z) + f_2(z)$$

für $f_1, f_2 \in F$ und $z \in \mathbb{Z}$, wobei $+$ die normale Addition ganzer Zahlen bezeichnet.

Hinweis: Für Funktionen $f_1, f_2 \in F$ gilt $f_1 = f_2$ genau dann, wenn $f_1(z) = f_2(z)$ für alle $z \in \mathbb{Z}$ gilt.

(iv) Zeigen Sie, dass $(F, +_F)$ eine Gruppe ist.

Weiter definieren wir die Menge $H := \{h : \mathbb{Z} \to \mathbb{Z} \mid h \text{ ist ein Homomorphismus von } (\mathbb{Z}, +) \text{ nach } (\mathbb{Z}, +)\}$.

(v) Zeigen Sie, dass H eine Unteralgebra von $(F, +_F)$ erzeugt.

(vi) Geben Sie ohne Begründung einen Homomorphismus φ von $(H, +_F)$ nach $(F, +_F)$ an.

Lösung zu Aufgabe 3

(i) Beispielsweise für

$$\begin{aligned} g_1 : \mathbb{Z} &\to \mathbb{Z} \\ z &\mapsto 1 \end{aligned}$$

und

$$\begin{aligned} g_2 : \mathbb{Z} &\to \mathbb{Z} \\ z &\mapsto 2 \end{aligned}$$

gilt $(g_1, g_2) \notin R$.

(ii) Beispielsweise für

$$\begin{aligned} g_1 : \mathbb{Z} &\to \mathbb{Z} \\ z &\mapsto 1 \end{aligned}$$

und

$$\begin{aligned} g_2 : \mathbb{Z} &\to \mathbb{Z} \\ z &\mapsto z \end{aligned}$$

gilt $(g_1, g_2) \in R$.

(iii) Um zu zeigen, dass R eine Äquivalenzrelation ist, muss die Reflexivität, die Symmetrie und die Transitivität von R gezeigt werden.

- **Reflexivität:** Sei $f \in F$ beliebig. Es gilt $f(1) = f(1)$ und damit $(f, f) \in R$.
- **Symmetrie:** Seien $f_1, f_2 \in F$ beliebig mit $(f_1, f_2) \in R$. Dann gilt $f_1(1) = f_2(1)$ nach der Definition von R. Da die Gleichheitsrelation auf den ganzen Zahlen symmetrisch ist, folgt $f_2(1) = f_1(1)$ und weiter $(f_2, f_1) \in R$.
- **Transitivität:** Seien $f_1, f_2, f_3 \in F$ beliebig mit $(f_1, f_2), (f_2, f_3) \in R$. Dann gilt $f_1(1) = f_2(1)$ und $f_2(1) = f_3(1)$ nach der Definition von R. Da die Gleichheitsrelation auf den ganzen Zahlen transitiv ist, folgt $f_1(1) = f_3(1)$ und weiter $(f_1, f_3) \in R$.

(iv) Um zu zeigen, dass $(F, +_F)$ eine Gruppe ist, muss die Abgeschlossenheit, die Assoziativiät, die Existenz eines neutralen Elementes und die Existenz von inversen Elementen gezeigt werden.

- **Abgeschlossenheit:** Seien $f_1, f_2 \in F$ und $x \in \mathbb{Z}$ beliebig. Dann ist $(f_1 +_F f_2)(x) = f_1(x) + f_2(x)$ ein eindeutig definiertes Element von $\mathbb{Z}$, da f_1 und f_2 Funktionen sind und somit ist $f_1 +_F f_2$ eine Funktion von $\mathbb{Z}$ nach $\mathbb{Z}$.
- **Assoziativität:** Seien $f_1, f_2, f_3 \in F$ und $z \in \mathbb{Z}$ beliebig. Es gilt

$$\begin{aligned} ((f_1 +_F f_2) +_F f_3)(z) &= (f_1 +_F f_2) + f_3(z) \\ &= f_1(z) + f_2(z) + f_3(z) \\ &= f_1(z) + (f_2 +_F f_3)(z) \\ &= (f_1 +_F (f_2 +_F f_3))(z) \end{aligned}$$

- **Neutrales Element:** Die Funktion

$$\begin{aligned} f_0 : \mathbb{Z} &\to \mathbb{Z} \\ z &\mapsto 0 \end{aligned}$$

ist das neutrale Element bezüglich $+_F$. Da f_0 eine Funktion ist, gilt $f_0 \in F$. Für $f \in F$ und $z \in \mathbb{Z}$ beliebig gilt

$$\begin{aligned}(f_0 +_F f)(z) &= f_0(z) + f(z)\\ &= 0 + f(z)\\ &= f(z)\end{aligned}$$

und

$$\begin{aligned}(f +_F f_0)(z) &= f(z) + f_0(z)\\ &= f(z) + 0\\ &= f(z)\end{aligned}$$

- **Inverse Elemente:** Sei $f \in F$ beliebig. Dann ist

$$\begin{aligned}g : \mathbb{Z} &\to \mathbb{Z}\\ z &\mapsto -f(z)\end{aligned}$$

das inverse Element für f bezütlich $+_F$, denn es gilt für alle $z \in \mathbb{Z}$

$$\begin{aligned}(f +_F g)(z) &= f(z) + g(z)\\ &= f(z) + (-f(z))\\ &= 0\\ &= f_0(z)\end{aligned}$$

und

$$\begin{aligned}(g +_F f)(z) &= g(z) + f(z)\\ &= (-f(z)) + f(z)\\ &= 0\\ &= f_0(z)\end{aligned}$$

Da g eine Funktion ist, gilt $g \in F$.

(v) Um zu zeigen, dass H eine Unteralgebra von $(F, +_F)$ erzeugt, muss $H \subseteq F$ und die Abgeschlossenheit von H unter $+_F$ gezeigt werden.
Sei $h \in H$, dann ist h ein Homomorphismus von $\mathbb{Z}$ nach $\mathbb{Z}$ und somit insbesondere auch eine Abbildung von $\mathbb{Z}$ nach $\mathbb{Z}$ und damit gilt $h \in F$ und weiter $H \subseteq F$.

Seien $h_1, h_2 \in H$ und $x, y \in \mathbb{Z}$. Dann gilt

$$\begin{aligned}(h_1 +_F h_2)(x + y) &= h_1(x + y) + h_2(x + y) && \mid \text{Definition von } +_F\\ &= h_1(x) + h_1(y) + h_2(x) + h_2(y) && \mid \text{Homomorphie von } h_1, h_2\\ &= h_1(x) + h_2(x) + h_1(y) + h_2(y) && \mid \text{Kommutativität von } +\\ &= (h_1 +_F h_2)(x) + (h_1 +_F h_2)(y) && \mid \text{Definition von } +_F\end{aligned}$$

(vi) Beispielsweise

$$\begin{aligned}\varphi : H &\to F\\ h &\mapsto h\end{aligned}$$

ist ein Homomorphismus.