Lösungshinweise zur Aufgabensammlung zur Vorlesung "Diskrete Algebraische Strukturen" im Sommersemester 2010 bei Dr. M. Junker

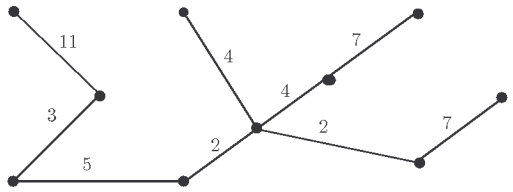
19. 07. 2010

---

1. Man kann an den Graphen ablesen:

Graph Nr.	1	2	3	4	5
Baum	Ja	Nein	Nein	Nein	Nein
Wald	Ja	Nein	Ja	Nein	Ja
bipartit	Ja	Nein	Ja	Ja	Ja
3-färbbar	Ja	Nein	Ja	Ja	Ja
zusammenhängend	Ja	Ja	Nein	Ja	Nein

2. Ein minimal aufspannender Baum ist gegeben durch:



3. Sind m und n teilerfremd, so folgt $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ aus dem chinesischen Restsatz (Satz 10.5).

   Andererseits falls ein Isomorphismus $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ existiert, so bezeichnen wir das Bild von $[1]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ mit $([g]_m, [h]_n) \in \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Nach Satz 9.4 und dessen Beweis ist dann $([g]_m, [h]_n)$ ein Erzeuger von $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Nehmen wir nun an, dass $\mathrm{ggT}(n, m) = k > 1$ gilt, so folgt für die natürliche Zahl $\frac{mn}{k} < mn$ bereits:

$$([g]_m, [h]_n)^{\frac{mn}{k}} = ([m\frac{n}{k}g]_m, [n\frac{m}{k}h]_n) = ([1]_m, [1]_m).$$

   Dies ist ein Widerspruch.

4. Seien $(G, \circ), (H, \circ)$ zwei Gruppen, e_H das neutrale Element von H und $\varphi : G \to H$ ein Gruppenhomomorphismus. Bezeichne mit e_G das neutrale Element von G. Dann gilt:

   - $\ker \varphi$ ist eine Untergruppe:
     DENN:
     - $\varphi(e_G) = e_H \quad \Rightarrow \quad e_G \in \ker \varphi$
     - Seien $g, h \in \ker \varphi$ beliebig, d.h. $\varphi(g) = e_H = \varphi(h) \quad \Rightarrow \quad \varphi(g \circ h) = \varphi(g) \circ \varphi(h) = e_H \circ e_H = e_H$, also gilt $g \circ h \in \ker \varphi$
     - Sei $g \in \ker \varphi$ beliebig, d.h. $\varphi(g) = e_H \quad \Rightarrow \quad \varphi(g^{-1}) = \varphi(g)^{-1} = e_H$, also $g^{-1} \in \ker \varphi$

- $\operatorname{im}\varphi$ ist eine Untergruppe:
  DENN:
  - $\varphi(e_G) = e_H \quad \Rightarrow \quad e_H \in \operatorname{im}\varphi$
  - Seien $h_1, h_2 \in \operatorname{im}\varphi$ beliebig, d.h. ex. $g_1, g_2 \in G$ mit $\varphi(g_i) = h_i$, $i = 1, 2$,
    $\Rightarrow \quad h_1 \circ h_2 = \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \circ g_2) \in \operatorname{im}\varphi$
  - Sei $h \in \operatorname{im}\varphi$ beliebig, d.h. ex. $g \in G$ mit $\varphi(g) = h$,
    $\Rightarrow \quad h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \operatorname{im}\varphi$

5. Sei $(G, \circ)$ eine Gruppe. Der Zentralisator von G ist gegeben durch $Z(G) = \{h \in G \mid h \circ g = g \circ h \quad \forall\, g \in G\}$. Das neutrale Element von G wird mit e bezeichnet.

   Es gilt:

   - $e \in Z(G)$.
   - Seien $g_1, g_2 \in Z(G)$ beliebig $\quad \Rightarrow \quad g_1 \circ g_2 \circ h = g_1 \circ h \circ g_2 = h \circ g_1 \circ g_2 \quad \forall\, h \in G$, also gilt $g_1 \circ g_2 \in Z(G)$
   - Sei $g \in Z(G)$ beliebig, so gilt für beliebiges $h \in G$: $g \circ h = h \circ g \quad \Rightarrow \quad h = g^{-1} \circ h \circ g \quad \Rightarrow$ $h \circ g^{-1} = g^{-1} \circ h$. Somit gilt $g^{-1} \in Z(G)$.

6. Es gilt $(\mathbb{Z}/15\mathbb{Z})^* = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$.

   Aus $[1]_{15}^1 = [2]_{15}^4 = [4]_{15}^2 = [7]_{15}^4 = [8]_{15}^4 = [11]_{15}^2 = [13]_{15}^4 = [14]_{15}^2 = [1]_{15}$ können wir jedoch ablesen, dass keines der Elemente Ordnung $8 = \operatorname{ord}((\mathbb{Z}/15\mathbb{Z})^*)$ besitzt. Also kann keines der Elemente die Gruppe erzeugen und daher die Gruppe nicht zyklisch sein.

7.

	5	6	7	8	9	10	11	12
$\varphi(\,\cdot\,)$	4	2	6	4	6	4	10	4

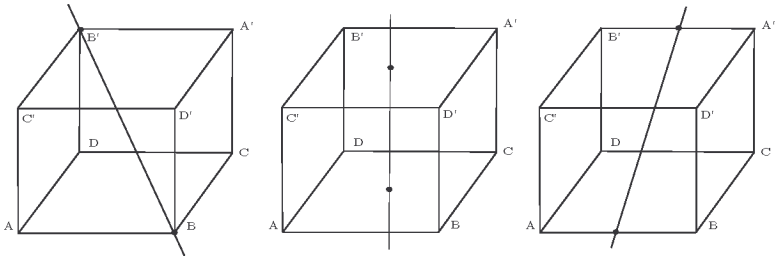
8. Seien $p \neq q$ zwei Primzahlen und φ die Eulersche φ-Funktion.

$$\begin{aligned}
\varphi(p^2q^2) &= |\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, p^2q^2) = 1\}| \\
&= p^2q^2 - |\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, p^2q^2) > 1\}| \\
&= p^2q^2 - |\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, p^2) > 1\} \cup \{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, q^2) > 1\}| \\
&= p^2q^2 - \Big(|\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, p^2) > 1\}| + |\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, q^2) > 1\}| \\
&\qquad\qquad - |\{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, p^2) > 1\} \cap \{a \mid 1 \le a \le p^2q^2;\ \mathrm{ggT}(a, q^2) > 1\}|\Big) \\
&= p^2q^2 - (pq^2 + p^2q - pq) = pq(pq - q - p + 1) = pq(p-1)(q-1) = (p^2 - p)(q^2 - q)
\end{aligned}$$

   Hierbei folgt die vierte Gleichung aus der Siebformel.

9. Seien die Ecken des Würfels mit $A, A', B, B', C, C', D, D'$ bezeichnet. Die Menge der Hauptachsen sei durch $\{A, A'\}, \{B, B'\}, \{C, C'\}, \{D, D'\}$ gegeben (vgl. Bild). Weiterhin bezeichne $D(W)$ die Drehgruppe des Würfels. Wir betrachten die Abbildung $G : D(W) \to S_4$, die einer Drehung die zugehörigen Permutation der 4 Hauptachsen des

Würfels (als Menge, also ohne Richtung betrachtet) zuordnet und werden zeigen, dass diese Abbildung bijektiv ist.



1. Injektivität: Wir zeigen, dass ausschließlich die Identität alle Hauptachsen fest lässt. Dazu betrachten wir eine beliebige Drehung φ des Würfels, so dass die Mengen $\{A, A'\}, \{B, B'\}, \{C, C'\}, \{D, D'\}$ jeweils auf sich abgebildet werden. Insbesondere gilt also $\varphi(A) = A$ oder $\varphi(A) = A'$. Betrachten wir zunächst den zweiten Fall, so können wir am Bild ablesen, dass dann auch $\varphi(B) = B'$, $\varphi(C') = C$ und $\varphi(D) = D'$ gilt. Dann muss aber auch $\varphi(A') = A$, $\varphi(B') = B$, $\varphi(C) = C'$ und $\varphi(D') = D$ gelten. Also gilt $\varphi = -\mathrm{id}$ und ist keine Drehung. Dieser Fall kann also nicht auftreten. Im ersten Fall zeigt man analog, dass dann tatsächlich $\varphi = \mathrm{id}$ gilt.

2. Surjektivität: Um die Surjektivität zu zeigen, müssen wir uns nun nur noch überlegen, dass die Mächtigkeit von $D(W)$ mindestens $|S_4| = 24$ beträgt. Hierzu listen wir 24 Drehungen auf (vgl. Bild):

- die Identität
- die Drehungen um die Hauptdiagonalen (4×2 verschiedene Drehungen)
- die Drehungen um die Achsen durch die Mittelpunkte zweier gegenüberliegender Seiten (3×3 verschiedene Drehungen)
- die Drehungen um die Achsen durch die Mittelpunkte zweier gegenüberliegender Kanten (6 verschiedene Drehungen).

10. (a) Wir nehmen an, dass 9 eine Primzahl ist. Mit dem kleinen Satz von Fermat folgt nun für $p = 9$ und $a = 2$, dass $2^8 \equiv 1 (\mathrm{mod}\, 9)$ ist. Eine kleine Rechnung zeigt jedoch $2^8 = 256 \not\equiv 1 (\mathrm{mod}\, 9)$ und wir erhalten einen Widerspruch.

    (b) Da 2011 eine Primzahl ist, kann man den kleinen Satz von Fermat ausnutzen. Dazu zerlegt man $2013 = 2010 + 3$. Da $2011 \not| 1764$ kann man nun berechnen

$$\begin{aligned} 1764^{2013} (\mathrm{mod}\, 2011) &\equiv (1764^{2010} \cdot 1764^3) (\mathrm{mod}\, 2011) \equiv 1764^3 (\mathrm{mod}\, 2011) \\ &\equiv (1764^2 \cdot 1764) (\mathrm{mod}\, 2011) \equiv (679 \cdot 1764) (\mathrm{mod}\, 2011) \\ &\equiv 1211 (\mathrm{mod}\, 2011) \end{aligned}$$

11. Da $\varphi(pq)$ und 1331 teilerfremd sind, existieren ganze Zahlen a und b, so dass

$$1 = \mathrm{ggT}(\varphi(pq), 1331) = a \cdot \varphi(pq) + b \cdot 1331.$$

Bilden wir nun die Restklassen bzgl. mod $\varphi(pq)$, so erhalten wir

$$[1]_{\varphi(pq)} = [a\varphi(pq)]_{\varphi(pq)} + [b]_{\varphi(pq)} \cdot [1331]_{\varphi(pq)} = [b]_{\varphi(pq)} \cdot [1331]_{\varphi(pq)}.$$

$[b]_{\varphi(pq)}$ ist also das gesuchte Inverse.

Daher bestimmen wir nun mit dem Euklidischen Algorithmus zunächst b:

$$\begin{aligned} 12000000 &= 9015 \cdot 1331 + 1035 \\ 1331 &= 1035 + 296 \\ 1035 &= 3 \cdot 296 + 147 \\ 296 &= 2 \cdot 147 + 2 \\ 14773 &\cdot 2 + 1 \end{aligned}$$

Also gilt

$$\begin{aligned} 1 &= 147 - 73 \cdot 2 \\ &= 147 - 73(296 - 2 \cdot 147) = 147 \cdot 147 - 73 \cdot 296 \\ &= 147(1035 - 3 \cdot 296) - 73 \cdot 296 = 147 \cdot 1035 - 514 \cdot 296 \\ &= 147 \cdot 1035 - 514(1331 - 1035) = 661 \cdot 1035 - 514 \cdot 1331 \\ &= 661 \cdot (12000000 - 9015 \cdot 1331) - 514 \cdot 1331 = 661 \cdot 12000000 - 5959429 \cdot 1331. \end{aligned}$$

Nun gilt $[b]_{\varphi(pq)} = [-5959429]_{\varphi(pq)} = [6040571]_{\varphi(pq)}$.

12. Das Verfahren ahmt den Euklidischen Algorithmus nach. Wir benennen den großen Krug mit G und den kleinen Krug mit K und schreiben die darin enthaltene Wassermenge in Klammern dahinter.

$$\begin{aligned} &G(9)K(0) \to G(2)K(7) \to G(2)K(0) \to G(0)K(2) \to G(9)K(2) \\ &\to G(4)K(7) \to G(4)K(0) \to G(0)K(4) \to G(9)K(4) \to G(6)K(7) \\ &\to G(6)K(0) \to G(0)K(6) \to G(9)K(6) \to G(8)K(7) \to G(8)K(0) \to G(1)K(7) \end{aligned}$$

13. In $\mathbb{F}_3$ gilt: $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

In $\mathbb{F}_5$ gilt: $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 2 \\ 1 & 3 & 0 \\ 3 & 1 & 4 \end{pmatrix}$.

14. (a) *alter Code*: Seien a_i und b_i die richtige und die falsche Ziffer (welche ist egal) und $a_i > b_i$. Wäre die Prüfsumme gleich, so würde folgen

$$\begin{aligned} & i \cdot a_i \equiv i \cdot b_i \bmod 11 \\ \iff\ & i \cdot (a_i - b_i) \equiv 0 \bmod 11. \end{aligned}$$

Dann müsste aber bereits $i = 11$ oder $a_i - b_i = 11$, da 11 eine Primzahl ist. Da $i \in \{1, \dots 10\}$ und $(a_i - b_i) \in \{1, \dots, 10\}$, folgt daraus, dass die Prüfsummen nicht gleich sein können.

neuer Code: Der Beweis funktioniert analog zu oben, wenn man bedenkt, dass $\mathrm{ggT}(3, 10) = 1 = \mathrm{ggT}(1, 10)$.

(b) Sei $i > j$. Und nehmen wir an, dass

$$\begin{aligned} i \cdot a_i + j \cdot a_j &\equiv i \cdot a_j + j \cdot a_i \bmod 11 \\ i(a_i - a_j) + j(a_j - a_i) &\equiv 0 \bmod 11 \\ (i-j)(a_i - a_j) &\equiv 0 \bmod 11. \end{aligned}$$

Nun sieht man wie oben ein, dass die Prüfsumme nicht gleich sein kann.

(c) Betrachte 1632487413457 und 6132487413457. Die Prüfsummen sind $[90]_{10} = [0]_{10}$ bzw. $[80]_{10} = [0]_{10}$.

15. Zunächst übersetzen wir den Text in ASCII-Code: S=19, I=09, C=03, H=08, E=05, R=18. Außerdem benötigen wir für die Rechnung die binäre Darstellung von 17: Es gilt $17 = 1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 2^4$ und somit folgt für beliebiges $z \in \mathbb{R}$:

$$z^{17} = (((z^2)^2)^2)^2 \cdot z.$$

Nun können wir für SI= 1909 berechnen:

$$\begin{aligned} 1909^2 \bmod 2773 &\equiv 559 \\ 559^2 \bmod 2773 &\equiv 1905 \\ 1905^2 \bmod 2773 &\equiv 1941 \\ 1941^2 \bmod 2773 &\equiv 1747 \\ 1747 \cdot 1909 \bmod 2773 &\equiv 1877 \end{aligned}$$

Also gilt $1909^{17} \bmod 2773 \equiv 1877$. Analog berechnet man $(0308)^{17} \bmod 2773 \equiv 1163$ und $(0518)^17 \bmod 2773 \equiv 1787$.

16. Wir nutzen das Verfahren aus der Vorlesung:

Finde zunächst b_1 mit $b_1 \equiv 3 \bmod 5$ und $b_1 \equiv 2 \bmod 4$:

$$\begin{aligned} -3 \cdot 5 + 4 \cdot 4 &= 1 \\ b_1 = 2 \cdot (-3) \cdot 5 + 3 \cdot 4 \cdot 4 &= 18. \end{aligned}$$

Bestimme nun $b = b_2$ mit $b_2 \equiv 18 \bmod 20$ und $b_2 \equiv 5 \bmod 7$:

$$\begin{aligned} -1 \cdot 20 + 3 \cdot 7 &= 1 \\ b_2 = 5 \cdot (-1) \cdot 20 + 18 \cdot 3 \cdot 7 &= 278. \end{aligned}$$

In $\mathbb{Z}/m\mathbb{Z}$ mit $m = 5 \cdot 4 \cdot 7 = 140$ gilt nun $278 \equiv 138 \bmod 140$. Daher ist 138 die gesuchte Zahl.