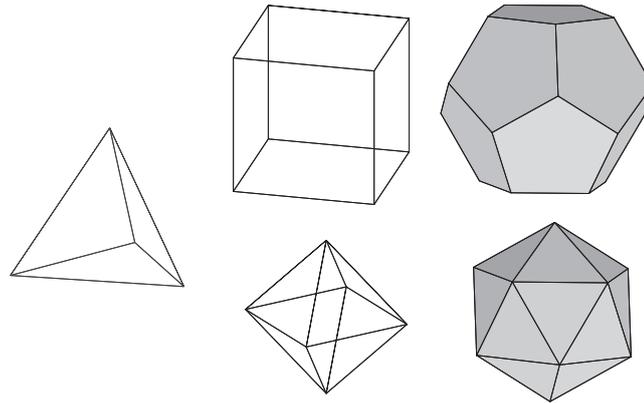


Mathematik für Informatiker  
Algebraische Strukturen  
Übungsblatt 6

**Abgabetermin Samstag, den 09.12.2023 bis 23:59 in OpenOlat.**

1. Basteln Sie Papiermodelle der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder (bitte in die Übung mitbringen).



2. Sei  $G$  eine Menge zusammen mit einer Verknüpfung  $\circ$ , die folgende Axiome erfüllt:

(G1) Assoziativität:  $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$ .

(G2') Es existiert ein linksneutrales Element, d.h. ein  $e \in G$  mit  $e \circ a = a \quad \forall a \in G$ .

(G3') Existenz des Linksinversen, d.h.  $\forall a \in G \exists a^{-1} \in G$  mit  $a^{-1} \circ a = e$ .

Zeigen Sie:

- (a) Für  $a, b \in G$  gilt: Ist  $a \circ b = e$ , dann ist auch  $b \circ a = e$ .
  - (b) Es ist  $a \circ e = a \quad \forall a \in G$ .
  - (c) Das neutrale Element ist eindeutig.
  - (d) Die Inversen sind eindeutig.
  - (e) Für  $a, b \in G$  ist  $(ab)^{-1} = b^{-1}a^{-1}$ .
  - (f) Für  $a \in G$  ist  $(a^{-1})^{-1} = a$ .
3. (a) Berechnen Sie für

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 6 & 4 & 3 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 2 & 5 & 7 & 6 \end{pmatrix},$$

die Permutationen  $\sigma^2$ ,  $\tau^2$ ,  $\sigma \circ \tau$  und  $\tau \circ \sigma$ .

- (b) Bestimmen Sie alle Transpositionen der symmetrischen Gruppe  $S_4$ .
4. Implementieren Sie (auch in Form von Pseudocode)
- (a) das Sieb des Eratosthenes und
  - (b) die Faktorisierung von ganzen Zahlen mittels Probedivision.
  - (c) Bestimmen Sie die Primfaktorzerlegung von 116338867864982351.

5. (4 Zusatzpunkte) Schreiben Sie (z.B. mit Hilfe Ihrer Implementierung des erweiterten Euklidischen Algorithmus oder der MAPLE-Funktion `igcdex`) eine Prozedur, die die Lösungsmenge der simultanen Kongruenzen

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

für  $a_1, a_2 \in \mathbb{Z}$  und  $n_1, n_2 \in \mathbb{Z}_{>0}$  mit  $\text{ggT}(n_1, n_2) = 1$  bestimmt.

Erweitern Sie die Funktionalität Ihrer Implementierung so, dass sie auch im Fall nicht teilerfremder  $n_1, n_2$  korrekt funktioniert.