

Diedergruppe D_5

Gruppe der ebenen Isometrien (längenerhaltenden Abbildungen), die ein regelmäßiges Fünfeck invariant lassen.

$$a \quad \text{Drehung um } 72^\circ \quad a^5 = e$$

$$b \quad \text{Spiegelung an fester Achse} \quad b^2 = e$$

$$b \circ a = a^{-1} \circ b$$

$$\implies D_5 = \{e, a, a^2, a^3, a^4, b, a \circ b, a^2 \circ b, a^3 \circ b, a^4 \circ b\}$$

$$d_i := \begin{cases} a^i & 0 \leq i \leq 4 \\ a^{i-5} \circ b & 5 \leq i \leq 9 \end{cases} \implies D_5 = \{d_0, d_1, \dots, d_9\}.$$

$$r(k) := k \text{ modulo } 5 \text{ in } \{0, 1, \dots, 4\}$$

Verknüpfung

$$d_i \circ d_j = a^i \circ a^j = a^{i+j} = a^{r(i+j)} = d_{r(i+j)} \quad (0 \leq i \leq 4, 0 \leq j \leq 4)$$

$$\begin{aligned} d_i \circ d_j &= a^i \circ a^{j-5} \circ b \\ &= a^{i+j-5} \circ b = a^{r(i+j)} \circ b = d_{5+r(i+j)} \quad (0 \leq i \leq 4, 5 \leq j \leq 9) \end{aligned}$$

Diedergruppe D_5 - Fortsetzung

Erinnerung

$$a^5 = e, \quad b^2 = e, \quad b \circ a = a^{-1} \circ b$$

$$d_i = \begin{cases} a^i & 0 \leq i \leq 4 \\ a^{i-5} \circ b & 5 \leq i \leq 9 \end{cases}$$

$$r(k) = \text{Rest modulo 5 in } \{0, 1, \dots, 4\}$$

Restliche Fälle

$$\begin{aligned} d_i \circ d_j &= a^{i-5} \circ b \circ a^j \\ &= a^{i-5} \circ a^{-j} \circ b \\ &= a^{i-j-5} \circ b = a^{r(i-j)} \circ b = d_{5+r(i-j)} \quad (5 \leq i \leq 9, 0 \leq j \leq 4) \end{aligned}$$

$$\begin{aligned} d_i \circ d_j &= a^{i-5} \circ b \circ a^{j-5} \circ b \\ &= a^{i-5} \circ a^{5-j} \circ b \circ b \\ &= a^{i-j} = a^{r(i-j)} = d_{r(i-j)} \quad (5 \leq i \leq 9, 5 \leq j \leq 9) \end{aligned}$$

- Für positive Werte i lässt sich $r(i)$ mit dem %-Operator realisieren. Für negative Werte ist die Wirkung des %-Operators implementierungsdefiniert.

Prüfziffer

Betrachte Ziffernfolge $z_1 \dots z_{K-1}$ und füge Prüfziffer hinzu. Die einfachsten Prüfverfahren erkennen fehlerhafte Ziffernfolgen, bei denen genau eine Ziffer falsch ist.

1. Finde Prüfziffer z_K so, dass *eine* falsche Ziffer erkannt wird.

$$\text{Ansatz: } d_{z_1} \circ d_{z_2} \circ \dots \circ d_{z_{K-1}} \circ d_{z_K} = e$$

$$\begin{aligned} D_5 \text{ Gruppe} &\implies d_{z_K} \text{ eindeutig bestimmt} \\ &\implies z_K \text{ eindeutig bestimmt.} \end{aligned}$$

Unterscheiden sich zwei Ziffernfolgen an genau einer Stelle, so haben die Produktausdrücke unterschiedliche Werte. (Wären sie gleich, $K - 1$ Faktoren "kürzen", dann restliche Faktoren gleich)

Prüfziffer - Fortsetzung

2. Erkenne Vertauschung aufeinanderfolgender Ziffern:

Ansatz: Betrachte Permutation $\pi : \{0, \dots, 9\} \rightarrow \{0, \dots, 9\}$
Bestimme Prüfziffer aus Gleichung

$$d_{\pi(z_1)} \circ d_{\pi^2(z_2)} \cdots d_{\pi^{K-1}(z_{K-1})} \circ d_{z_K} = e$$

- ▶ Erkennt offenbar auch *eine* fehlerhafte Ziffer
- ▶ Erfüllt die Permutation

$$d_i \circ d_{\pi(j)} \neq d_j \circ d_{\pi(i)} \quad (\forall i \neq j)$$

dann gilt (mit den Ersetzungen $i \rightarrow \pi^k(i), j \rightarrow \pi^k(j)$)

$$d_{\pi^k(i)} \circ d_{\pi^{k+1}(j)} \neq d_{\pi^k(j)} \circ d_{\pi^{k+1}(i)} \quad (\forall i \neq j, k)$$

insbesondere (mit den Ersetzungen $i \rightarrow z_k, j \rightarrow z_{k+1}$)

$$d_{\pi^k(z_k)} \circ d_{\pi^{k+1}(z_{k+1})} \neq d_{\pi^k(z_{k+1})} \circ d_{\pi^{k+1}(z_k)} \quad (\forall z_k \neq z_{k+1}, k < K-1)$$

Hinweise zum Programm

- ▶ Klasse `dieder` für Gruppenverknüpfung anlegen, Konstruktor mit `int`-Argument versehen
- ▶ Operatorfunktion für Typumwandlung `dieder` \rightarrow `int` anlegen oder Ausgabeoperator überladen
- ▶ Vorsicht bei der Auswertung von $r(k)$ für $k < 0$
- ▶ Bereichsüberschreitungen im Konstruktor und bei der Multiplikation evtl. mit Exceptions behandeln
- ▶ Funktion `perm` zur Berechnung von $\pi^k(i)$ sinnvoll
- ▶ Funktion zur Umwandlung Zeichenkette \rightarrow Ziffernkette nützlich
- ▶ Assoziativer Vektor für Abbildung Ortsbuchstaben \rightarrow Ziffer und `'0'` \rightarrow `0`, `'1'` \rightarrow `1`, ..., `'9'` \rightarrow `9`
- ▶ Auflösen der Prüfziffergleichung entweder explizit oder durch systematisches Durchgehen aller Fälle
- ▶ Testbeispiele: Vierte Banknotenserie (BBK3) unter http://de.wikipedia.org/wiki/Bargeld_der_Deutschen_Mark