

$$[(x_1, y_1)]_{\sim} * [(y_1, x_1)]_{\sim} = [(x_1 \circ y_1, x_1 \circ y_1)]_{\sim} = [(e, e)]_{\sim}, \text{ denn } x_1 \circ y_1 \circ e = e \circ x_1 \circ y_1$$

d)  $f : A \rightarrow B, x \mapsto [(x, e)]_{\sim}$  ist die gesuchte Abb.

## 0.3 Übung 2, 15.11.2004

### 0.3.1 Aufgabe 1

$(A, \circ)$  endliche Gruppe,  $e$  neutr. Element;  $x \in A$  fest

a) z.Z.: Es gibt ein kleinstes  $k \in \mathbb{N}$  mit  $x^k = e$ .

**Beweis:**  $B := \{x, x^2, \dots, x^n, x^{n+1}\} \subset A$  mit  $|A| = n$

$$\Rightarrow |B| \leq n$$

$$\Rightarrow \exists i, j \in \{1, \dots, n+1\} : i < j \quad \text{und} \quad x^i = x^j = x^i \circ x^{j-1}$$

$$\Rightarrow x^{j-1} = e \quad \text{und} \quad 1 \leq j-1 \leq n$$

Damit ist  $M := \{m \in \mathbb{N} | x^m = e\} \neq \emptyset$ . Da  $(j-1) \in M$  ex. außerdem  $k = \min M$ . □

b) z.Z.:  $B := \{x, x^2, \dots, x^n\}$  ist eine Untergruppe von  $A$

**Beweis:**

•  $B \neq \emptyset$ , da  $x \in B$

• Seien  $y, z \in B$ . Dann  $\exists i, j \in \{1, \dots, k\}$  mit  $y = x^i$  und  $z = x^j$

$$y \circ z^{-1} = x^i \circ x^{k-j} = x^{i+k-j} = \begin{cases} x^{k+i-j}, & \text{falls } i \leq j \\ x^{i-j}, & \text{falls } i > j \end{cases}$$

In beiden Fällen  $y \circ z^{-1} \in B$ .

• Seien  $y, z \in B$ . Dann  $\exists i, j \in \{1, \dots, k\}, y = x^i, z = x^j$

$$y \circ z = x^i \circ x^j = x^{i+j} = x^{j+i} = z \circ y$$

□

z.Z.: Ann.:  $|B| < k$ . Dann  $\exists i, j \in \{1, \dots, k\}$  mit  $i < j$  und  $x^i = x^j$

$$\Rightarrow x^{j-1} = e \quad \text{und} \quad 1 \leq j-1 < k$$

$$\Rightarrow |B| = k$$

### 0.3.2 Aufgabe 3

a) z.Z.: Die Menge  $\{Ba | a \in A\}$  (mit  $Ba = \{b \circ a | b \in B\}$ ) bildet eine Partition von  $A$ .

**Beweis:** Für alle  $a \in A$  gilt  $a \in Ba$ , da  $e \in B$  und somit  $e \circ a \in Ba$  ist.

Damit gilt:  $Ba \neq \emptyset$  für alle  $a \in A$  und  $\bigcap_{a \in A} Ba = a$ .

Sei  $a, a' \in A$  und  $Ba \cap Ba' \neq \emptyset$ . Dann ex.  $Ba \cap Ba'$  und es gibt  $b, b' \in B$  mit  $x = b \circ a$  und  $x = b' \circ a' \Rightarrow a = \underbrace{b^{-1} \circ b'}_{\in B} \circ a'$  und  $a' = \underbrace{b'^{-1} \circ b}_{\in B} \circ a$

$$\Rightarrow a \in Ba' \text{ und } a' \in Ba$$

$$\Rightarrow Ba \subset Ba' \Rightarrow Ba = Ba'.$$

□

b) z.Z.:  $|B|$  teilt  $|A|$

**Beweis:**

(1) Wir zeigen:  $|Ba| = |B|$  für alle  $a \in A$

$h : B \rightarrow Ba, h \mapsto b \circ a$  ist bijektiv denn  $h^{-1} : Ba \rightarrow B, x \mapsto x \circ a^{-1}$  ist ihre Umkehrabbildung.

$\Rightarrow |Ba| = |B|$  für alle  $a \in A$

(2) z.Z.:  $\exists m \in \mathbb{N} : m|B| = |A|$

Wir zeigen aus a), dass  $A = \bigcup_{a \in A} Ba$

Wir definieren  $m := |\{Ba | a \in A\}|$  (die Anzahl der verschiedenen Nebenklassen)

Dann gilt  $|A| = m|B|$ .

□

c) z.Z.  $\forall a \in A : a^{|A|} = e$

**Beweis:** Sei  $k$  die Ordnung von  $a$

$B := \{a, a^2, \dots, a^k\}$

Wir wissen aus Aufgabe 1:  $B$  ist Untergruppe von  $A$ . Dann ex. wegen b) ein  $m \in \mathbb{N}$  mit  $|A| = mk$ .

Somit:  $a^{|A|} = a^{mk} = a^{k^n} = e^m = e$

□

d) z.Z.:  $|A| \geq Z : |A|$  ist Primzahl  $\Leftrightarrow \{e\}, A$  sind die einzigen Untergruppen von  $A$

**Beweis:**

„ $\Rightarrow$ “ Wegen b) gilt für jede Untergruppe  $B$ , dass  $|B|$  teilt  $|A|$ .

„ $\Leftarrow$ “ Wegen  $|A| \geq 2$  gibt es  $x \in A \setminus \{e\}$ . Also ist die Ordnung  $k$  von  $x$  echt größer 1.

$\{e\} \subsetneq \{a, a^k\} = A$  (nach Vor.) und  $k = |A|$

Falls:  $|A|$  keine Primzahl ist, so ex.  $m \neq 1 \neq n$  mit  $|A| = mn = e$ .

$\{a^n, a^{2n}, a^{3n}, \dots, a^{nm}\}$  ist Untergruppe von  $A$  und  $1|\{a^n, \dots, a^{nm}\}| = m < k$  ist Widerspruch zur Vor.

Also gilt:  $|A|$  ist Primzahl

□

### 0.3.3 Aufgabe 2

b)

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 5 & 4 & 8 & 6 & 2 & 1 \end{pmatrix} \\ \Leftrightarrow \tau^{(1,8)} \circ \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 5 & 4 & 1 & 6 & 2 & 8 \end{pmatrix} \\ \Leftrightarrow \tau^{(2,7)} \circ \tau^{(1,8)} \circ \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 4 & 1 & 6 & 7 & 8 \end{pmatrix} \\ &\dots \\ \Leftrightarrow id &= \tau^{(1,2)} \circ \tau^{(1,3)} \circ \tau^{(1,5)} \circ \tau^{(2,7)} \circ \tau^{(1,8)} \circ \pi \\ \Leftrightarrow \pi &= \tau^{(1,8)} \circ \tau^{(2,7)} \circ \tau^{(1,5)} \circ \tau^{(1,3)} \circ \tau^{(1,2)} \end{aligned}$$