P 31. Werteschreibweise versus Zykelschreibweise

Sei $n \in \mathbb{N}$ und $E_n := \{1, \ldots, n\}$. Die symmetrische Gruppe $(S_n, \circ)$ ist gegeben als Menge der Permutationen: $S_n := \{f : E_n \to E_n \mid f \text{ bijektiv }\}$ zusammen mit der Komposition (Hintereinanderausführung) $\circ$ als Verknüpfung. Die Komposition $(f \circ g)(x) := f(g(x)), x \in E_n$ wird auch als Produkt der beiden Permutationen bezeichnet und man setzt: $g^k := \underbrace{g \circ g \circ \ldots \circ g}_{k \text{ mal}}$.

Die Elemente $f \in S_n$ lassen sich darstellen in **Werteschreibweise** als: $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$ oder als **Produkt von Zykeln**, wobei ein k–Zykel $(x_1 x_2 \ldots x_k), k \leq n$ diejenige Permutation $g \in S_n$ ist mit $g(x_1) = x_2,\ g(x_2) = x_3,\ \ldots,\ g(x_{k-1}) = x_k,\ g(x_k) = x_1$ sowie $g(x) = x\ \forall x \in E_n \backslash \{x_1, x_2, \ldots, x_k\}$.

Sei nun $f \in S_8$ in Zykelschreibweise als $f = (1\ 3\ 6) \circ (5\ 2\ 3) \circ (6\ 1) \circ (8\ 3\ 4) \circ (1\ 7)$ gegeben.

1. Geben Sie für f das Ergebnis in Werteschreibweise an.
2. Zwei Zykel $(x_1\ x_2 \ldots x_k)$, $(y_1\ y_2 \ldots y_l)$ heißen elementfremd, wenn $\{x_1, x_2, \ldots, x_k\} \cap \{y_1, y_2, \ldots, y_l\} = \emptyset$. Geben Sie ein Verfahren an, wie man von der Werteschreibweise einer Permutation auf eine elementfremde Zykelschreibweise kommt. Lassen sich elementfremde Zykel vertauschen ?
   Geben Sie das Ergebnis von f als Produkt elementfremder Zykel an.
3. Zeigen Sie : Für einen k–Zykel g gilt $g^k = id$ und $\forall j < k : g^j \neq id$. Bestimmen Sie damit f^{2007}.
4. Stellen Sie f als Produkt von 2–Zykeln (Transpositionen) dar und bestimmen Sie das Signum von f.

1) $f = (1\ 3\ 6) \circ (5\ 2\ 3) \circ (6\ 1) \circ (8\ 3\ 4) \circ (1\ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 8 & 2 & 3 & 1 & 5 \end{pmatrix}$

$f(1)$ $f(2)$ $f(7)$

2) Jede Permutation lässt sich in Werteschreibweise angeben.
Bilde einen Zykel mit 1 beginnend : $(1\ f(1)\ f(f(1)) \ldots)$ wobei f solange iteriert angewendet wird, bis sich wieder 1 einstellt.
Dabei wird das Element $f(f(\ldots f(1))) = 1$ nicht nochmals in den Zykel aufgenommen.
Bilde einen neuen Zykel beginnend mit einem Element aus E_n, welches noch nicht im vorangegangenen Zykel auftritt und vervollständige diesen Zykel nach obigem Schema.
Erstelle weitere Zykel bis alle Elemente aus E_n verwendet wurden.
Einelementige Zykel können (als Identität) weggelassen/weggestrichen werden.
→ Die Zykellänge ist höchstens n und damit endlich
→ konstruktives Verfahren zur Gewinnung paarweise elementfremder Zykel.

Verfahren „bricht ab"

Bem: Da die Zahlen $1, \ldots, n \in E_n$ in beiden Zeilen jeweils genau einmal vorkommen und bei der Zykelbildung jeweils paarweise (oben und unten) „weggestrichen" werden, bleiben in keiner der beiden Zeilen Zahlen übrig.

Verfahren „geht auf"

oder direkt als Produkt der Zykel aus Angabe

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 8 & 2 & 3 & 1 & 5 \end{pmatrix} = (17)\circ(263485) = (263485)\circ(17)$

$[f(1)=7,\ f(7)=1]$ und $[f(2)=6,\ f(6)=3,\ f(3)=4,\ f(4)=8,\ f(8)=5,\ f(5)=2]$

Nach Definition eines k-Zykels $g=(x_1,\dots,x_k)$ gilt $\forall x \in E_n \setminus \{x_1,\dots,x_k\}$:
$g(x)=x$ $\Rightarrow$ elementfremde Zykel können vertauscht werden.

3) g ist aus k paarweise verschiedenen Elementen aufgebaut (*) $\Rightarrow$

$g = (x\ g(x)\ g(g(x))=g^2(x)\ g^3(x)\ \dots\ g^{k-2}(x)\ g^{k-1}(x))$

Nach Definition eines k-Zykels gilt: $g(g^{k-1}(x)) = g^k(x) = x$

D.h.: $\forall$ Zykelelemente $y = g^i(x)$, $i=1,\dots,k-1$ gilt:

$$g^k(y) = g^k(g^i(x)) = g^{k+i}(x) = g^{i+k}(x) = g^i(g^k(x)) = g^i(x) = y$$

$\forall$ nicht-Zykelelemente ist g nach Definition die Identität, also auch g^k. $\Rightarrow$

$\Rightarrow g^k = id.$ und $g^j \neq id$ für $j<k$ nach (*), vgl. Definition.

$(2007 = 334\cdot 6 + 3)$

$$f^{2007} = [(17)\circ(263485)]^{2007} = \underbrace{(17)\circ(263485)\circ\dots\circ(17)(263485)}_{2007 \text{ mal}} =$$

$$\overset{2)}{=} (17)^{2007}\circ(263485)^{2007} \overset{3)}{=} (17)^{2007 \bmod 2}\circ(263485)^{2007 \bmod 6} =$$

$$= (17)\circ(263485)^3 = (17)(263485)(263485)(263485) = \underline{(17)(24)(35)(68)}$$

Hier erweist sich das Rechnen mit Zykeln als vorteilhaft!

Beachte: $(263485)^5 = (258436) = (263485)^{-1}$ ($f^5(2)$)

4) k-Zykel $(x_1\ x_2\ x_3\ \dots\ x_k) = \underbrace{(x_1x_2)\circ(x_2x_3)\circ(x_3x_4)\circ\dots\circ(x_{k-1}x_k)}_{k-1 \text{ Transpositionen}}$

$\Rightarrow f = \underbrace{(17)(26)(63)(34)(48)(85)}_{6 \text{ Transpositionen}} \Rightarrow sign(f) = (-1)^6 = 1$

Zusatz

Mit Hilfe von Fehlständen $F(f)$, d.h. der Anzahl der Paare (i,j), $i,j \in E_n$ mit $i<j$ und $f(i)>f(j)$: $sign(f) = (-1)^{|F(f)|} = (-1)^{20} = 1$

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 8 & 2 & 3 & 1 & 5 \end{pmatrix} \Rightarrow$

$F(f) = \{(1,2), (1,3), (1,5), (1,6), (1,7), (1,8), (2,3), (2,5), (2,6), (2,7), (2,8),$
$(3,5), (3,6), (3,7), (4,5), (4,6), (4,7), (4,8), (5,7), (6,7)\}$

P 32. Seien $\pi_1, \pi_2 \in S_6$ mit $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$ und $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}$

a) Berechnen Sie $\pi_2 \circ \pi_1$, π_1^{-1}, π_2^{-1}, π_2^{27}, π_1^8 und geben Sie das Ergebnis in Werte- und Zykelschreibweise an.

b) Finden Sie die Lösungen $x \in S_6$ der Gleichung $\pi_1 \circ x \circ \pi_2 = \pi_2 \circ \pi_1$.

a1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix}$

$\pi_2(1)$ $\pi_1(2)$ $\pi_2 \circ \pi_1(2) = \pi_2(\pi_1(2)) = \pi_2(1) = 3$

bzw in Zykelschreibweise mit $\pi := \pi_2 \circ \pi_1$

$\pi(2)$ $\pi(3)$ $\pi(6)$ $\pi(5)$ $\pi(4)=2$

$(1\,3\,5\,4) \circ (1\,4\,2) \circ (3\,6) = (2\,3\,6\,5\,4)$

direkt $\pi(2) = (1\,3\,5\,4) \circ (1\,4\,2)(3\,6)\,\underline{(2)} = (1\,3\,5\,4) \circ (1\,4\,2)\,\underline{(2)} = (1\,3\,5\,4)\,\underline{(1)} = 3$

a2) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} \Rightarrow \pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix}$

$\pi_1(1) = 4 \Rightarrow \pi_1^{-1}(4) = 1$ analog $\pi_1(2) = 1 \Rightarrow \pi_1^{-1}(1) = 2$, ...

π_1^{-1} entsteht aus π_1 durch Sortieren der Spalten nach der zweiten Zeile und anschließender Vertauschen der Zeilen

a3) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} \Rightarrow \pi_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 3 & 6 \end{pmatrix}$

bzw in Zykelschreibweise (umgekehrte Reihenfolge)

$\pi_1 = (1\,4\,2) \circ (3\,6) \Rightarrow \pi_1^{-1} = (2\,4\,1)(6\,3) = (1\,2\,4)(3\,6)$

$\pi_2 = (1\,3\,5\,4) \Rightarrow \pi_2^{-1} = (4\,5\,3\,1) = (1\,4\,5\,3)$

a4) Zur Berechnung von π^k ist Zykelschreibweise günstiger:

$\pi_2^{27} = (1\,3\,5\,4)^{27} = (1\,3\,5\,4)^{(27 \bmod 4)} = (1\,3\,5\,4)^3 = (1\,3\,5\,4)^{-1} = \pi_2^{-1}$

k fache Anwendung einer k Zykels ist die Identität!

a5) $\pi_1^8 = ((1\,4\,2) \circ (3\,6))^8 = (1\,4\,2)^8 \circ (3\,6)^8 = (1\,4\,2)^2 = (1\,2\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

elementfremde Zykel vertauschbar!

b) Multiplikation der Gleichung von links mit π_1^{-1} und von rechts mit π_2^{-1} liefert:

$x = \pi_1^{-1} \circ \pi_2 \circ \pi_1 \circ \pi_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 2 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 3 & 6 \end{pmatrix}$

$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 3 & 5 \end{pmatrix}$ oder als Zykel $x = (1\,4) \circ (2\,6\,5\,3)$

P 33. Gruppe der Einheiten

Seien $(R, \oplus, \cdot)$ ein Ring mit Einselement und $M \subseteq R$ die Menge aller invertierbaren Elemente von R bezüglich der Multiplikation $\odot$.

1. Zeigen Sie, dass $(M, \odot)$ eine Gruppe (die *Einheitengruppe* von R) ist. Ist $(M, \oplus, \odot)$ ein Körper ?
2. Bestimmen Sie die Einheitengruppe von $\mathbb{Z}_{10}$.

1) Aus Vorlesung: $(R, \oplus, \odot)$ ist Ring mit Einselement 1

(i) $(R, \oplus)$ ist kommutative (abelsche) Gruppe (Addition)

(ii) Multiplikation $\odot$ ist abgeschlossen, assoziativ und distributiv

(iii) $\exists\, 1 \in R$ mit $1 \odot a = a \quad \forall\, a \in R$

Sei M die Menge der invertierbaren Elemente von R bzgl $\odot$

Es gilt: $a \in R$ liegt in $M \Leftrightarrow \exists\, a^{-1} \in R : a^{-1} \circ a = 1$

Zu zeigen: $(M, \odot)$ ist Gruppe

- neutrales Element / Einselement: $1 \cdot 1 = 1 \Rightarrow 1^{-1} = 1 \in M$
- Abgeschlossenheit: $\forall\, a, b \in M : (a \circ b)^{-1} = b^{-1} \circ a^{-1} \in R$, da
  $(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ 1 \circ b = b^{-1} \circ b = 1$
  $\Rightarrow a \circ b \in M$.
- inverses Element: Mit a gehört wegen $(a^{-1})^{-1} = a$ auch a^{-1} zu M !
- Assoziativität erbt $M \subseteq R$ von $(R, \odot)$, vgl. Ringaxiome.

$(M, \oplus, \odot)$ ist kein Körper, da $0 \notin M$ (Neutrales Element der Addition)

selbst $(M \cup \{0\}, \oplus, \odot)$ ist im allgemeinen kein Körper, da $M \cup \{0\}$ bzgl. Addition im allgemeinen nicht mehr abgeschlossen ist, vgl. 2).

Wenn $(R, \oplus, \odot)$ schon ein Körper ist, dann ist auch $(M \cup \{0\}, \oplus, \odot)$ wieder ein Körper (trivial!, da $M = R \setminus \{0\}$)

---

2) $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ Einselement $1 \in M$ (siehe oben!)

Nullelement 0 ist sicher nicht invertierbar.

Zu $2, 4, 6, 8$ $\nexists\, k \in \mathbb{Z}_{10} : 2k, 4k, 6k, 8k = 1 \bmod 10$ (Ergebnis gerade!)

Bleiben $3, 5, 7, 9$ übrig. Es gilt $5k = \begin{cases} 0 \bmod 10 & \text{für } k = 0, 2, 4, 6, 8 \\ 5 \bmod 10 & \text{für } k = 1, 3, 5, 7, 9 \end{cases}$

$3 \cdot 7 = 1 \bmod 10$ und $9 \cdot 9 = 1 \bmod 10 \Rightarrow \underline{M = \{1, 3, 7, 9\}}$

Z 34. Nebenklassen, Quotientengruppe, Isomorphie und Äquivalenz

Gegeben sei die Abbildung $f : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_3$ mit $x \mapsto x \mod 3$ zwischen den Gruppen $(\mathbb{Z}_{12}, \oplus_{12})$ und $(\mathbb{Z}_3, \oplus_3)$.

1. Zeigen Sie, dass f ein Epimorphismus ist, und geben Sie $Kern(f)$ an.
2. Geben Sie die Elemente von $\mathbb{Z}_{12}/Kern(f)$ an. Um welche Mengen handelt es sich dabei?
3. Beweisen Sie, dass $\mathbb{Z}_{12}/Kern(f)$ isomorph zu $\mathbb{Z}_3$ ist $(\mathbb{Z}_{12}/Kern(f) \cong \mathbb{Z}_3)$.
4. Zeigen Sie, dass $a \sim b :\leftrightarrow a \ominus_{12} b \in Kern(f)$ auf $\mathbb{Z}_{12}$ eine Äquivalenzrelation definiert.
5. Zeigen Sie: $[a]_\sim = [a]_{Kern(f)}, \forall a \in \mathbb{Z}_{12}$.

Vorbemerkung: Wegen 3 teilt 12 gilt: $(x \bmod 12) \bmod 3 = x \bmod 3 \quad \forall x \in \mathbb{Z}$

Wir zeigen allgemein:

Für $u, v \in \mathbb{N}\setminus\{0\}$ mit v teilt u gilt: $(x \bmod u) \bmod v = x \bmod v \quad \forall x \in \mathbb{Z}$

Beweis: Nach Division mit Rest gilt:

$\left.\begin{array}{l} \forall x \in \mathbb{Z}, \exists q \in \mathbb{Z}, r \in \mathbb{N}: \; x = q \cdot u + r \text{ mit } 0 \le r < u \\ \text{Wegen } v \text{ teilt } u \; \exists m \in \mathbb{N}: \; u = v \cdot m \end{array}\right\} \Rightarrow$

$(x \bmod u) \bmod v = [(q \cdot u + r) \bmod u] \bmod v = r \bmod v$ und

$x \bmod v = (q \cdot v \cdot m + r) \bmod v = r \bmod v$ ∎

Achtung: $(15 \bmod 12) \bmod 5 = 3 \bmod 5$ aber $15 \bmod 5 = 0$!

1) $f: \begin{cases} \mathbb{Z}_{12} \to \mathbb{Z}_3 = \{0,1,2\} \quad ; \quad \mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\} \\ x \mapsto f(x) = x \bmod 3 \end{cases} \Rightarrow Kern(f) = \{x \in \mathbb{Z}_{12} \mid f(x) = 0\} = \{0,3,6,9\}$

f ist Epimorphismus $\Leftrightarrow$ f ist Homomorphismus und surjektiv.

a) f ist surjektiv, da $f(0) = 0, \; f(1) = 1, \; f(2) = 2$

b) f ist Homomorphismus (strukturerhaltend), da

$$f(x \oplus_{12} y) = (x \oplus_{12} y) \bmod 3 = [(x+y) \bmod 12] \bmod 3 =$$
$$= (x+y) \bmod 3 = x \bmod 3 \oplus_3 y \bmod 3 = f(x) \oplus_3 f(y)$$

Bemerkung: $Kern(f)$ ist eine Untergruppe von $(\mathbb{Z}_{12}, \oplus_{12})$.

Bemerkung: Für $\bar{f}: \mathbb{Z}_{12} \to \mathbb{Z}_5$ mit $x \mapsto x \bmod 5$ ist $\bar{f}$ kein Homomorphismus,

da $f(6 \oplus_{12} 6) = f(0) = 0 \bmod 5 = 0 \; \wedge \; f(6) \oplus_5 f(6) = 6 \bmod 5 \oplus_5 6 \bmod 5 = 2$

Ferner gilt: $Kern(\bar{f}) = \{x \in \mathbb{Z}_{12} \mid \bar{f}(x) = 0\} = \{0,5,10\}$ ist keine Untergruppe von $(\mathbb{Z}_{12}, \oplus_{12})$

2) $\mathbb{Z}_{12}/Kern(f) = \{[a]_{Kern(f)} \mid a \in \mathbb{Z}_{12}\}$ mit $[a]_{Kern(f)} := \{a \oplus_{12} x \in \mathbb{Z}_{12} \mid x \in Kern(f)\}$

$= \{\underbrace{[0]_{Kern(f)}}_{=\{0,3,6,9\}}, \underbrace{[1]_{Kern(f)}}_{=\{1,4,7,10\}}, \underbrace{[2]_{Kern(f)}}_{=\{2,5,8,11\}}\}$

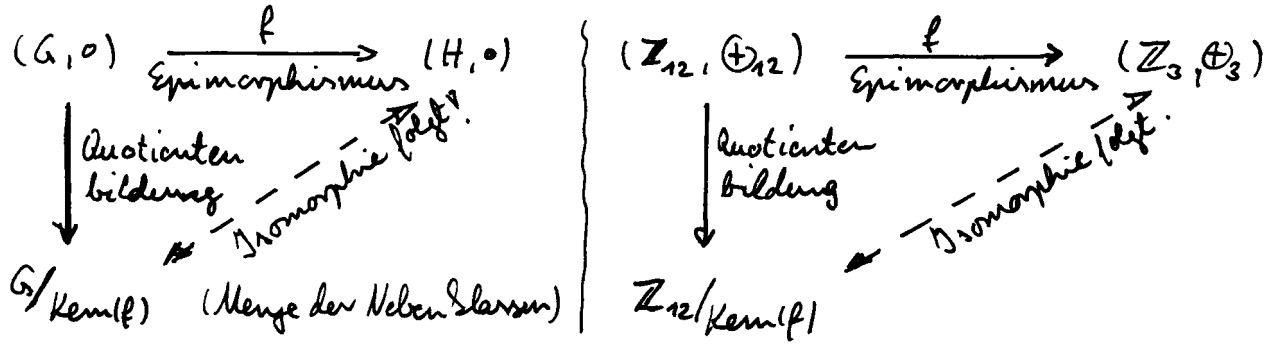
Untergruppe! da f homomorph

Partition von $\mathbb{Z}_{12}$ in 3 Nebenklassen mit je 4 Elementen

Da $\mathbb{Z}_{12}$ kommutativ: Linksnebenklassen ≡ Rechtsnebenklassen

3) $\mathbb{Z}_{12}/_{Kern(f)} \cong \mathbb{Z}_3$ lässt sich wie folgt zeigen:

a) mit Hilfe des Isomorphiesatzes für Gruppen $(G,\circ), (H,\bullet)$



b) durch direkte Angabe eines Isomorphismus (bijektiver Homomorphismus)

z.B.: $g: \begin{cases} \mathbb{Z}_{12}/_{Kern(f)} \to \mathbb{Z}_3 \\ [x]_{Kern(f)} \mapsto x \bmod 3 \end{cases}$ bleibt zu zeigen:

- g ist bijektiv, da surjektiv (betrachte $x=0,1,2$) und injektiv, da

$g([x]_{Kern(f)}) = g([y]_{Kern(f)}) \overset{\text{Vorbem.}}{\Leftrightarrow} x \bmod 3 = y \bmod 3 \Leftrightarrow (x-y) \bmod 3 = 0 \Leftrightarrow$

$\Leftrightarrow [(x-y) \bmod 12] \bmod 3 = 0 \Leftrightarrow (x \ominus_{12} y) \bmod 3 = 0 \Leftrightarrow x \ominus_{12} y \in Kern(f) \Leftrightarrow$

$\Leftrightarrow [x]_{Kern(f)} = [y]_{Kern(f)}$

- g ist Homomorphismus (strukturtreu), da

$g([x]_{Kern(f)} + [y]_{Kern(f)}) = g([x \oplus_{12} y]_{Kern(f)}) = (x \oplus_{12} y) \bmod 3 =$

$= [(x+y) \bmod 12] \bmod 3 \overset{\text{Vorbem.}}{=} (x+y) \bmod 3 = x \bmod 3 \oplus_3 y \bmod 3 = g([x]_{Kern(f)}) \oplus_3 g([y]_{Kern(f)})$

4) $a \sim b :\Leftrightarrow a \ominus_{12} b \in Kern(f)$ ist Äquivalenzrelation, da $\sim$:

<u>reflexiv</u>: $a \sim a \Leftrightarrow a \ominus_{12} a = 0 \in Kern(f)$ ✓

<u>symmetrisch</u>: $a \sim b$, o.E. $a \neq b \Leftrightarrow (a \ominus_{12} b) \bmod 3 = 0$

$\Rightarrow (b \ominus_{12} a) \bmod 3 \overset{\text{Inversenbildung in } \mathbb{Z}_{12}}{=} [12 - (a \ominus_{12} b)] \bmod 3 = \underbrace{12 \bmod 3}_{=0} \ominus_3 \underbrace{(a \ominus_{12} b) \bmod 3}_{=0 \text{ nach Voraus.}} = 0 \Leftrightarrow b \sim a$

<u>transitiv</u>: $a \sim b \wedge b \sim c \Leftrightarrow (a \ominus_{12} b) \bmod 3 = 0 \wedge (b \ominus_{12} c) \bmod 3 = 0$

$\Rightarrow (a \ominus_{12} c) \bmod 3 = [(a \ominus_{12} b) \oplus_{12} (b \ominus_{12} c)] \bmod 3 = \left([(a \ominus_{12} b) + (b \ominus_{12} c)] \bmod 12\right) \bmod 3 =$

$\overset{\text{Vorbem.}}{=} [(a \ominus_{12} b) + (b \ominus_{12} c)] \bmod 3 = \underbrace{(a \ominus_{12} b) \bmod 3}_{=0} \oplus_3 \underbrace{(b \ominus c) \bmod 3}_{=0} = 0 \Leftrightarrow a \sim c$

5) $[a]_\sim := \{x \in \mathbb{Z}_{12} \mid x \sim a\} = \{x \in \mathbb{Z}_{12} \mid (x \ominus_{12} a) \in Kern(f)\} = \{a \oplus_{12} y \in \mathbb{Z}_{12} \mid y \in Kern(f)\} = [a]_{Kern(f)}$

o.E. $x = a \oplus_{12} y$ mit $y \in Kern(f)$, da $(\mathbb{Z}_{12}, \oplus_{12})$ Gruppe

<u>alternativ</u>: $b \in [a]_{Kern(f)} \Leftrightarrow \exists\, x \in Kern(f)$ mit $b = a \oplus_{12} x \Leftrightarrow$

$\Leftrightarrow b \ominus_{12} a = x \in Kern(f) \Leftrightarrow b \sim a \Leftrightarrow b \in [a]_\sim$ □