Fachrichtung Mathematik • Institut für Algebra • Prof. Baumann, Dr. Noack

Mathematische Methoden für Informatiker INF-120-2
Wintersemester 2019/20

15. Übungsblatt für die Woche 21.10. - 27.10.2019

Algebraische Strukturen: Halbgruppen, Monoide, Gruppen, Permutationen

Ü85 (a) Zeigen Sie:

- Für jede Teilmenge $U \neq \emptyset$ einer Halbgruppe $(H, \circ)$ gilt:

$$(\,\forall\, a, b \in U :\; a \circ b \in U\,) \quad \Rightarrow \quad (U, \circ) \text{ ist eine Halbgruppe.}$$

- Für jede Teilmenge $U \neq \emptyset$ einer Gruppe $(G, \circ)$ gilt:

$$(\,\forall\, a, b \in U :\; a^{-1} \circ b \in U\,) \quad \Rightarrow \quad (U, \circ) \text{ ist eine Gruppe.}$$

(b) Es sei $(H, \circ)$ ein Monoid mit neutralem Element e. Zeigen Sie, dass die Menge der invertierbaren Elemente H^* von H mit der Operation $\circ$ eine Gruppe bildet.

(c) Zeigen Sie, dass für jede endliche Gruppe gilt: In der Gruppentafel tritt in jeder Zeile und in jeder Spalte jedes Element der Gruppe genau einmal auf.

Ü86 Gegeben sind die Mengen $A := \{a, b, c\}$ und $M := \{f \mid f\colon A \to A\}$, sowie die Abbildungen

$$f\colon A \to A \text{ mit } f(a) = a, f(b) = f(c) = b \quad \text{und}$$
$$g\colon A \to A \text{ mit } g(a) = b,\, g(b) = g(c) = a.$$

Zeigen Sie, dass die Teilmenge $U := \{f, g\}$ von M mit der Hintereinanderausführung $\circ$ ein Monoid bildet. Handelt es sich um ein Untermonoid des Monoids $(M, \circ)$? Ist $(U, \circ)$ eine Gruppe?

Ü87 In der symmetrischen Gruppe $(S_9, \circ)$ werden folgende Permutationen betrachtet:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 3 & 6 & 4 & 5 & 7 & 2 & 1 \end{pmatrix} \quad \text{und} \quad \beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 7 & 8 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}.$$

(a) Bestimmen Sie α, β, α^{-1}, β^{-1}, $\alpha \circ \beta$ und $\beta \circ \alpha$ in Zyklenschreibweise.

(b) Welche Ordnung haben α und β?

(c) Geben Sie β^{2019} in Zyklenschreibweise an.

(d) Ist die von der Menge $\{\alpha, \beta\}$ erzeugte Untergruppe von $(S_9, \circ)$ abelsch?

(e) Bestimmen Sie die Untergruppen $\langle\alpha\rangle$ und $\langle\beta\rangle$ von S_9. Vergleichen Sie beide Untergruppen.

(f) Welche Ordnung haben die Permutationen β^4, β^5 und β^9?

H88 $\boxed{\textbf{A}}$ In der symmetrischen Gruppe $(S_{11}, \circ)$ ist die Permutation

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 4 & 3 & 2 & 6 & 8 & 5 & 10 & 1 & 7 & 9 \end{pmatrix}$$

gegeben.

(a) Bestimmen Sie α, α^{-1} α^2 und α^{423} in Zyklenschreibweise.

(b) Berechnen Sie die Ordnung von α und von α^9.

(c) Zeigen Sie, dass $H := \{\sigma \in S_{11} \mid \sigma(3) = 3\}$ eine Untergruppe von $(S_{11}, \circ)$ ist.

H89 Untersuchen Sie, ob die folgenden Mengen M mit den angegebenen Operationen Halbgruppen, Monoide bzw. Gruppen sind. Welche der Operationen sind kommutativ?

(a) $M = \mathbb{Z}, \quad \forall x, y \in M: \ x \circ y := x + y - x \cdot y,$
(mit der üblichen Multiplikation $\cdot$ und Addition $+$ der reellen Zahlen)

(b) $M = (\mathbb{R} \setminus \{0\}) \times \mathbb{R}, \quad \forall (r_1, \varphi_1), (r_2, \varphi_2) \in M: \ (r_1, \varphi_1) \circ (r_2, \varphi_2) = (r_1 \cdot r_2, \varphi_1 + \varphi_2),$
(mit der üblichen Multiplikation $\cdot$ und Addition $+$ der reellen Zahlen)

H90 Es bezeichne U die Menge aller Lösungen der Gleichung $z^6 = 1$ in der Gruppe $(\mathbb{C} \setminus \{0\}, \cdot)$.

(a) Geben Sie alle Elemente von U konkret an.

(b) Zeigen Sie, dass U eine Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$ bildet. Stellen Sie dazu die Gruppentafel auf, und geben Sie zu jedem Element sein Inverses an.

(c) Bestimmen Sie für jedes Element von U seine Ordnung.

(d) Ist U zyklisch?

(e) Vergleichen Sie $(U, \cdot)$ mit den Gruppen $(\mathbb{Z}_6, +)$, $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ und $(\mathbb{Z}_{14}^*, \cdot)$.

$(H, \circ)$

1) $\circ: H \times H \to H$ (abgeschlossen) } Halbgruppe
2) $\circ$. assoziativ.
3) neutrales Element: $\exists e \in H : \forall a \in H \quad a \circ e = e \circ a = a$
4) Inverse: $\forall a \in H . \exists b \in H, \ a \circ b = b \circ a = e$
(Bezeichen: $b = a^{-1}$) } Gruppe

Monoid.

85

a) Sei $U \neq \emptyset$, $U \subseteq H$ und $(H, \circ)$ ist Halbgruppe.
$\underbrace{\forall a, b \in U. \ a \circ b \in U}_{(*)} \Rightarrow (U, \circ)$ ist Halbgruppe.

Beweis.
1) wegen $(*)$
2) da $U \subseteq H$ und H Halbgruppe $\square$

Sei $U \neq \emptyset$, $U \subseteq G$, und $(G, \circ)$ Gruppe
$\underbrace{\forall a, b \in U, \ a^{-1} \circ b \in U}_{(E) \text{ Untergruppenkriterium}} \Rightarrow (U, \circ)$ ist Gruppe

Beweis.
Sei $U \neq \emptyset$, $U \subseteq G$ mit Eigenschaft (E)
zu 3): $U \neq \emptyset \Rightarrow$ existiert $u \in U$.
Eig (E) mit: $a := u$, $b := u \Rightarrow u^{-1} \circ u = e \in U$

Zu 4): Eig(E) mit $a \in U$, $b = e \Rightarrow a^{-1} \circ e = a^{-1} \in U$

Zu 1): Seien $x, y \in U$ bel., nach 4) ist $x^{-1} \in U$
Eig(E) mit $a = x^{-1}$, $b = y$ $\quad (x^{-1})^{-1} \circ y = x \circ y \in U$

Assoziativität wird geerbt

b) Sei $(H, \circ)$ ein Monoid.
z.zg.: $H^* := \{ a \in H \mid \exists a^{-1} \in H \}$ ist eine Gruppe mit $\circ$.

Beweis

1 Weg: Eigenschaft (E) nachweisen. d.h.
$\forall a, b \in H^* : a^{-1} \circ b \in H^*$, d.h. $(a^{-1} \circ b)^{-1} \in H$.
Inverse raten oder $(a^{-1} \circ b) \circ y = e$

2 Weg: Eigenschaften 1) – 4) zeigen.

mit 1 Weg: $(a^{-1} \circ b) \circ y = e$

$$\overset{\text{asso.}}{\Longleftrightarrow} \quad a^{-1} \circ (b \circ y) = e \quad \mid a \circ .$$

$$(a \circ a^{-1}) \circ (b \circ y) = a \circ e$$

$$\overset{\text{inves}}{\Longleftrightarrow} \quad e \circ (b \circ y) = a \circ e$$

$$\overset{\text{neut}}{\Longleftrightarrow} \quad b \circ y = a \quad \mid b^{-1} \circ .., \ b^{-1} \text{ existiert, da } b \in H^*$$

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

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

und es gibt: $y \circ (a^{-1} \circ b) \overset{\text{asso}}{=} b^{-1} \circ (a \circ a^{-1}) \circ b = b^{-1} \circ b = e$

mit (a) folgt: $(U, \circ)$ ist eine Gruppe.

$$(AB)^{-1} = B^{-1} A^{-1}$$

c) 1) z.zg: in jeder Zeile (Spalte) der Gruppentafel einer endlichen Gruppe sind alle Elemente verschieden, d.h. $\forall a, b, c \in G : a \circ b \neq a \circ c$
$b \neq c$

Beweis Angenommen: $\exists a \in G,\ b, c \in G$ mit $b \neq c$.

$$a \circ b = a \circ c.$$

a^{-1} existiert in G: $a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$

$$\overset{\text{asso}}{\Longrightarrow} (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$$

$$\overset{\text{neu.}}{\Longrightarrow} \quad b = c \qquad \lightning$$

2) jedes Element kommt in jede Zeile (Spalte) vor.

Da die Gruppe endlich ist, $(|G| = n)$ und auf n Plätze genau n El. passen und alle mit 1) verschieden sind.
(Sudokuprinzip)

8b) $A = \{a, b, c\}$, $\quad M = \{f : A \to A\}$

$$h = \begin{pmatrix} a & b & c \\ \downarrow & \downarrow & \downarrow \\ a\,b\,c & c & c \end{pmatrix} \quad h \in M.$$

$|M| = 3^3 = 27$

$U = \{f, g\}$ $\quad f = \begin{pmatrix} a & b & c \\ a & b & b \end{pmatrix}$ $\quad g = \begin{pmatrix} a & b & c \\ b & a & a \end{pmatrix}$

z.zg. $(U, \circ)$ ist Monoid.

$\circ$ Hintereinanderausführung: $(f_1 \circ f_2)(x) = f_1(f_2(x))$ für alle $x \in A$.

$(M, \circ)$ ist ein Monoid.

- abgeschlossen
- assoziativ
- $e_M = id$.

$\forall x \in A: \ id(x) = x$.

Abgeschlossenheit von U:

	f	g	$f \circ f$	$f \circ g$	$g \circ f$	$g \circ g$
a	a	b	a	b	b	a
b	b	a	b	a	a	b
c	b	a	b	a	a	b

$$\left.\begin{array}{l} f \circ g = g \circ f = g \\ f \circ f = g \circ g = f. \end{array}\right\} \text{abgeschlossen}$$

$\overset{\text{ass(a)}}{\Longrightarrow}$ $(U, \circ)$ ist Halbgruppe.

$e_U = f \Rightarrow (U, \circ)$ Monoid.

Da $e_U \neq e_M$ ist U kein Untermonoid von M.

$\circ$	f	g
f	f	g
g	g	f

$\cong$

$+$	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, +)$

Hintereinanderausf. ist assoziativ. Seien $f_1, f_2, f_3 \in M$ beliebig.

z.zg. $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$

d.h. $\forall x \in A.\ (f_1 \circ (f_2 \circ f_3))(x) = ((f_1 \circ f_2) \circ f_3)(x)$

$\iff f_1((f_2 \circ f_3)(x)) \qquad (f_1 \circ f_2)(f_3(x))$

$\iff f_1(f_2(f_3(x))) = f_1(f_2(f_3(x)))$ w.A.

87. $S_9 = \{\sigma\ \{1, \dots, 9\} \to \{1, \dots, 9\} \mid \sigma \text{ bijektiv}\}$
Permutation

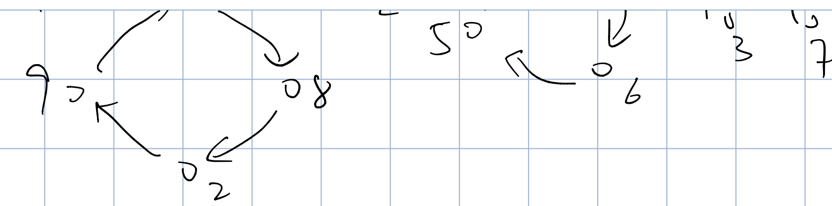
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 3 & 6 & 4 & 5 & 7 & 2 & 1 \end{pmatrix},$$

$3 \to 7 \to 7$
$7 \to 3 \to 3$
$5 \to 1 \to 8$
$8 \to 6 \to 5$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 7 & 8 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}$$

a) in Zyklenschreibweise.

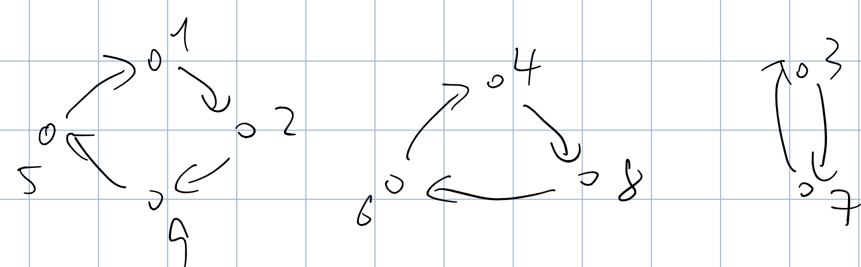
$\alpha = (\underbrace{1\ 8\ 2\ 9}_{21})(\underbrace{4\ 6\ 5}_{2_1})$ $\to 0^1$ 4



$$\alpha^{-1} = (9\ 2\ 8\ 1)\ (5\ 6\ 4)$$

$$\beta = (\underbrace{1\ 2\ 9\ 5}_{\beta_1})\ (\underbrace{3\ 7}_{\beta_2})\ (\underbrace{4\ 8\ 6}_{\beta_3})$$

$$\beta^{-1} = (5\ 9\ 2\ 1)\ (7\ 3)\ (6\ 8\ 4)$$



$$\alpha \circ \beta = (1\ 9\ 4\ 2)\ (3\ 7)\ (5\ 8)$$

$$\beta \circ \alpha = (1\ 6)\ (2\ 5\ 8\ 9)\ (3\ 7)$$

zu d) Da $\alpha \circ \beta \neq \beta \circ \alpha$, ist die von $\{\alpha, \beta\}$ erzeugte UG nicht abelsch.

b) $\mathrm{Ord}(\alpha) = |\langle \alpha \rangle| = |\{\alpha, \alpha\circ\alpha, \alpha\circ\alpha\circ\alpha, \dots, id\}|$
$= \mathrm{kgV}(\mathrm{Ord}(\alpha_1), \mathrm{Ord}(\alpha_2))$

$$= \text{kgV}(4,3) = 12$$

$$\text{Ord}(\beta) = \text{kgV}(4, 2, 3) = 12$$

c) $$\beta^{2019} = \beta_1^{2019 \bmod 4} \circ \beta_2^{2019 \bmod 2} \circ \beta_3^{\bmod 3}$$

$$= \beta_1^{3} \circ \beta_2^{1} \circ \beta_2^{0} = \beta_1^{3} \circ \beta_2^{1}$$

H88 $\boxed{\text{A}}$ In der symmetrischen Gruppe $(S_{11}, \circ)$ ist die Permutation

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 4 & 3 & 2 & 6 & 8 & 5 & 10 & 1 & 7 & 9 \end{pmatrix}$$

gegeben.

(a) Bestimmen Sie $\alpha,\ \alpha^{-1}\ \alpha^2$ und α^{423} in Zyklenschreibweise.

(b) Berechnen Sie die Ordnung von α und von α^9.

(c) Zeigen Sie, dass $H := \{\sigma \in S_{11} \mid \sigma(3) = 3\}$ eine Untergruppe von $(S_{11}, \circ)$ ist.

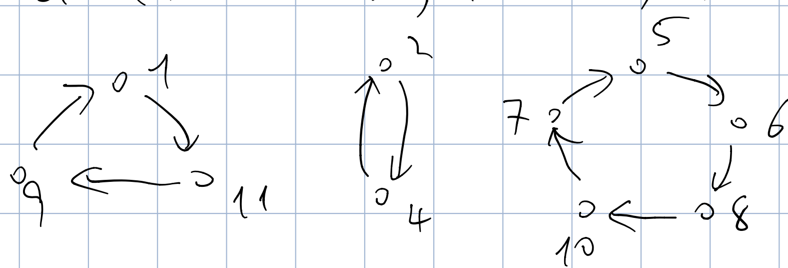
a)

$1 \to 11 \to 9 \to 1.$

$2 \to 4 \to 2$

$5 \to 6 \to 8 \to 10 \to 7 \to 5$

$\Rightarrow \alpha = (1\ 11\ 9)(2\ 4)(5\ 6\ 8\ 10\ 7)$



$\alpha^{-1} = (9\ 11\ 1)(4\ 2)(7\ 10\ 8\ 6\ 5)$

α^2

$1 \xrightarrow{2} 11 \xrightarrow{2} 9 \qquad 9 \to 1 \to 11$

$11 \to 9 \to 1$

$4 \to 2 \to 4$

$2 \to 4 \to 2.$

$7 \to 10 \to 8$

$8 \to 6 \to 5$

$5 \to 7 \to 10$

$10 \to 8 \to 6$

$6 \to 5 \to 7.$

$6 \to 3 \to 4$

$\alpha^2 = (1\ 9\ 11)(5\ 8\ 7\ 6\ 10)$

$\alpha^{423} = \alpha_1^{423 \bmod 3} \circ \alpha_2^{423 \bmod 2} \circ \alpha_3^{423 \bmod 5}$

$= \alpha_1^0 \circ \alpha_2^1 \circ \alpha_3^3 = \alpha_2^1 \circ \alpha_3^3$

b)

$\mathrm{Ord}(\alpha) = \mathrm{kgV}(\mathrm{Ord}(\alpha_1), \mathrm{Ord}(\alpha_2), \mathrm{Ord}(\alpha_3))$

$= \mathrm{kgV}(3, 2, 5)$

$= 30$

$\alpha^9 = \alpha_2^1 \circ \alpha_3^4$

$\mathrm{Ord}(\alpha^9) = \mathrm{kgV}(\mathrm{Ord}(\alpha_2), \mathrm{Ord}(\alpha_3^4))$

$= \mathrm{kgV}(\mathrm{Ord}(\alpha_2), \mathrm{Ord}(\alpha_3^{-1}))$

$= \mathrm{kgV}(2, 5) = 10$

c)

$H := \{\sigma \in S_{11} \mid \sigma(3) = 3\}$

$\sigma(3)_H = \sigma(3)_2 \Rightarrow (H, \circ)$ ist Untergruppe

Von $(S_{11}, 0)$