M. Künzer, J. Marhenke

Lineare Algebra für Informatiker, WS 03/04

Lösung 2

Aufgabe 5. $\sigma = (1,7,5,3)$ ist von Ordnung 4, $\varepsilon_\sigma = -1$; $\tau = (2,3)(5,6)$ ist von Ordnung 2, $\varepsilon_\tau = 1$; $\sigma^{-1} = (1,3,5,7)$ ist von Ordnung 4, $\varepsilon_{\sigma^{-1}} = -1$; $\tau^{-1} = \tau$; $\sigma \circ \tau = (1,7,5,6,3,2)$ und damit ist $(\sigma\circ\tau)^2 = (1,5,3)(2,7,6)$ von Ordnung 3, und hat das Signum $\varepsilon_{(\sigma\circ\tau)^2} = 1$.

Es ist $\tau^m = 1$, wenn $m = 2k$ für ein $k \in \mathbf{Z}$ ist. Außerdem ist $\sigma^n = 1$, wenn $n = 4k$ für ein $k \in \mathbf{Z}$ ist. Also lässt sich die folgende Tabelle anlegen (lies: $\tau^m \circ \sigma^n$; Ordnung; Signum).

$\tau^m \circ \sigma^n$	$m = 2k$	$m = 2k+1$
$n = 4k$	1; 1; 1	$(2,3)(5,6)$; 2; 1
$n = 4k+1$	$(1,7,5,3)$; 4; -1	$(1,7,6,5,2,3)$; 6; -1
$n = 4k+2$	$(1,5)(3,7)$; 2; 1	$(1,6,5)(2,3,7)$; 3; 1
$n = 4k+3$	$(1,3,5,7)$; 4; -1	$(1,2,3,6,5,7)$; 6; -1

Beachte, daß $\varepsilon_{\tau^m\circ\sigma^n} = \varepsilon_\tau^m \varepsilon_\sigma^n$.

Aufgabe 6.

(1) Die Verknüpfungstafel hat folgende Gestalt.

($\circ$)	1	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)	(1,2,3)	(2,4,3)	(1,4,2)	(1,3,4)	(1,3,2)	(1,4,3)	(2,3,4)	(1,2,4)
1	1	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)	(1,2,3)	(2,4,3)	(1,4,2)	(1,3,4)	(1,3,2)	(1,4,3)	(2,3,4)	(1,2,4)
(1,2)(3,4)	(1,2)(3,4)	1	(1,4)(2,3)	(1,3)(2,4)	(2,4,3)	(1,2,3)	(1,3,4)	(1,4,2)	(1,4,3)	(1,3,2)	(1,2,4)	(2,3,4)
(1,3)(2,4)	(1,3)(2,4)	(1,4)(2,3)	1	(1,2)(3,4)	(1,4,2)	(1,3,4)	(1,2,3)	(2,4,3)	(2,3,4)	(1,2,4)	(1,3,2)	(1,4,3)
(1,4)(2,3)	(1,4)(2,3)	(1,3)(2,4)	(1,2)(3,4)	1	(1,3,4)	(1,4,2)	(2,4,3)	(1,2,3)	(1,2,4)	(2,3,4)	(1,4,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,4)	(2,4,3)	(1,4,2)	(1,3,2)	(1,2,4)	(1,4,3)	(2,3,4)	1	(1,4)(2,3)	(1,2)(3,4)	(1,3)(2,4)
(2,4,3)	(2,4,3)	(1,4,2)	(1,2,3)	(1,3,4)	(1,4,3)	(2,3,4)	(1,3,2)	(1,2,4)	(1,2)(3,4)	(1,3)(2,4)	1	(1,4)(2,3)
(1,4,2)	(1,4,2)	(2,4,3)	(1,3,4)	(1,2,3)	(2,3,4)	(1,4,3)	(1,2,4)	(1,3,2)	(1,3)(2,4)	(1,2)(3,4)	(1,4)(2,3)	1
(1,3,4)	(1,3,4)	(1,2,3)	(1,4,2)	(2,4,3)	(1,2,4)	(1,3,2)	(2,3,4)	(1,4,3)	(1,4)(2,3)	1	(1,3)(2,4)	(1,2)(3,4)
(1,3,2)	(1,3,2)	(2,3,4)	(1,2,4)	(1,4,3)	1	(1,3)(2,4)	(1,4)(2,3)	(1,2)(3,4)	(1,2,3)	(1,4,2)	(1,3,4)	(2,4,3)
(1,4,3)	(1,4,3)	(1,2,4)	(2,3,4)	(1,3,2)	(1,2)(3,4)	(1,4)(2,3)	(1,3)(2,4)	1	(2,4,3)	(1,3,4)	(1,4,2)	(1,2,3)
(2,3,4)	(2,3,4)	(1,3,2)	(1,4,3)	(1,2,4)	(1,3)(2,4)	1	(1,2)(3,4)	(1,4)(2,3)	(1,4,2)	(1,2,3)	(2,4,3)	(1,3,4)
(1,2,4)	(1,2,4)	(1,4,3)	(1,3,2)	(2,3,4)	(1,4)(2,3)	(1,2)(3,4)	1	(1,3)(2,4)	(1,3,4)	(2,4,3)	(1,2,3)	(1,4,2)

(2) Die Untergruppen sind $\{1\}$; $\{1,(1,2)(3,4)\}$; $\{1,(1,3)(2,4)\}$; $\{1,(1,4)(2,3)\}$; $\{1,(1,2,3),(1,3,2)\}$; $\{1,(1,2,4),(1,4,2)\}$; $\{1,(1,3,4),(1,4,3)\}$; $\{1,(2,3,4),(2,4,3)\}$; $\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$; $\mathcal{A}_4$. Alle Untergruppen mit Ausnahme von $\mathcal{A}_4$ sind abelsch.

Aufgabe 7.

(1) Die Produktschreibweise in $(1,2)$, $(2,3)$ und $(3,4)$ liefert die folgenden Bilder.

1	$= 1$	$\mapsto 1$	$(1,2,4,3)$	$= (1,2)\circ(3,4)\circ(2,3)$	$\mapsto (2,3)$
$(1,2)$	$= (1,2)$	$\mapsto (1,2)$	$(2,4)$	$= (2,3)\circ(3,4)\circ(2,3)$	$\mapsto (1,3)$
$(2,3)$	$= (2,3)$	$\mapsto (2,3)$	$(1,4,3,2)$	$= (3,4)\circ(2,3)\circ(1,2)$	$\mapsto (1,3)$
$(3,4)$	$= (3,4)$	$\mapsto (1,2)$	$(1,3,4)$	$= (1,2)\circ(2,3)\circ(1,2)\circ(3,4)$	$\mapsto (1,2,3)$
$(1,2,3)$	$= (1,2)\circ(2,3)$	$\mapsto (1,2,3)$	$(1,2,4)$	$= (1,2)\circ(2,3)\circ(3,4)\circ(2,3)$	$\mapsto (1,3,2)$
$(1,3,2)$	$= (2,3)\circ(1,2)$	$\mapsto (1,3,2)$	$(1,3)(2,4)$	$= (2,3)\circ(1,2)\circ(3,4)\circ(2,3)$	$\mapsto 1$
$(1,2)(3,4)$	$= (1,2)\circ(3,4)$	$\mapsto 1$	$(1,4,3)$	$= (1,2)\circ(3,4)\circ(2,3)\circ(1,2)$	$\mapsto (1,3,2)$
$(2,3,4)$	$= (2,3)\circ(3,4)$	$\mapsto (1,3,2)$	$(1,4,2)$	$= (2,3)\circ(3,4)\circ(2,3)\circ(1,2)$	$\mapsto (1,2,3)$
$(2,4,3)$	$= (3,4)\circ(2,3)$	$\mapsto (1,2,3)$	$(1,3,2,4)$	$= (1,2)\circ(2,3)\circ(1,2)\circ(3,4)\circ(2,3)$	$\mapsto (1,2)$
$(1,3)$	$= (1,2)\circ(2,3)\circ(1,2)$	$\mapsto (1,3)$	$(1,4)$	$= (1,2)\circ(2,3)\circ(3,4)\circ(2,3)\circ(1,2)$	$\mapsto (2,3)$
$(1,2,3,4)$	$= (1,2)\circ(2,3)\circ(3,4)$	$\mapsto (1,3)$	$(1,4,2,3)$	$= (2,3)\circ(1,2)\circ(3,4)\circ(2,3)\circ(1,2)$	$\mapsto (1,2)$
$(1,3,4,2)$	$= (2,3)\circ(1,2)\circ(3,4)$	$\mapsto (2,3)$	$(1,4)(2,3)$	$= (1,2)\circ(2,3)\circ(1,2)\circ(3,4)\circ(2,3)\circ(1,2)$	$\mapsto 1$

(2) Es ist $\operatorname{Kern} f = \{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$. Da $\operatorname{Kern} f \neq \{1\}$, ist f nicht injektiv. Dagegen ist f surjektiv.

Aufgabe 8.

(1) Seien (x,y), (x',y'), $(x'',y'') \in G$.

(G1) Assoziativität folgt mit

$$\begin{aligned}((x,y)\cdot(x',y'))\cdot(x'',y'') &= (x+yx',yy')\cdot(x'',y'') = (x+yx'+yy'x'',yy'y'') \\ &= (x+y(x'+y'x''),yy'y'') = (x,y)\cdot(x'+y'x'',y'y'') \\ &= (x,y)\cdot((x',y')\cdot(x'',y''))\end{aligned}$$

(G2) Es ist $1_G = (0,1)$, da $(x,y)\cdot(0,1) = (x+y\cdot 0, y\cdot 1) = (x,y)$ und $(0,1)\cdot(x,y) = (0+1\cdot x, 1\cdot y) = (x,y)$.

(G3) Es ist $(x,y)^{-1} = (-xy^{-1}, y^{-1})$, da

$$\begin{aligned}(-xy^{-1},y^{-1})(x,y) &= (-xy^{-1}+y^{-1}x, y^{-1}y) &= (0,1)\ , \qquad \text{und} \\ (x,y)(-xy^{-1},y^{-1}) &= (x+y(-xy^{-1}), yy^{-1}) &= (0,1)\ .\end{aligned}$$

(2) Zunächst ist $U \neq \emptyset$. Seien $x = (a,1), y = (b,1) \in U$. Dann ist $xy^{-1} = (a,1)\cdot(-b,1) = (a+1\cdot(-b),1) \in U$. Damit ist $U \leq G$.

Zunächst ist $V \neq \emptyset$. Seien $x = (0,a), y = (0,b) \in V$. Dann ist $xy^{-1} = (0,a)\cdot(0,b^{-1}) = (0,ab^{-1}) \in V$. Damit ist $V \leq G$.

Aufgabe 9.

(1) Aussage trifft zu. Wegen $f(1) = 1 \in V$ ist $f^{-1}(V) \neq \emptyset$. Seien $x,y \in f^{-1}(V)$. Dann ist $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} \in V$ wegen $V \leq H$. Also ist $xy^{-1} \in f^{-1}(V)$. Damit folgt $f^{-1}(V) \leq G$.

(2) Gegenbeispiel: Betrachte den Gruppenmorphismus $\varepsilon : \mathcal{S}_3 \to \{\pm 1\}$. Dann hat $\sigma = (1,2,3)$ die Ordnung 3, aber die Ordnung von $\varepsilon_\sigma = 1$ ist 1.

Bemerkung: Die Ordnung von $f(g)$ ist aber sehr wohl ein Teiler der Ordnung von g.

(3) Aussage trifft zu. Sei $y = f(x) \in f(Z(G))$ mit $x \in Z(G)$ und sei $h \in H$. Zu zeigen: $hy = yh$. Da f surjektiv ist, existiert ein $g \in G$ mit $f(g) = h$. Dann ist

$$yh = f(x)f(g) = f(xg) = f(gx) = f(g)f(x) = hy\ .$$

(4) Gegenbeispiel: Die Gruppe $\{1,(1,2,3,4),(1,4,3,2),(1,3)(2,4),(2,4),(1,2)(3,4),(1,4)(2,3),(1,3)\} \leq \mathcal{S}_4$ ist nicht abelsch, ihr Zentrum ist $\{1,(1,3)(2,4)\} \neq \{1\}$.

(5) Aussage trifft zu. Sei $(\sim)$ die Äquivalenzrelation auf M, die durch

$$(g_1,g_2,\ldots,g_p) \sim (g_1',g_2',\ldots,g_p') \qquad \Longleftrightarrow \qquad \exists\, h \in G\ (g_1',g_2',\ldots,g_p') = (h^{-1}g_1,g_2,\ldots,g_{p-1},g_ph)$$

erklärt ist. Gegeben $(g_1,g_2,\ldots,g_p) \in M$, so gibt es eine Bijektion

$$G \xrightarrow{\sim} \overline{(g_1,g_2,\ldots,g_p)}\ , \qquad h \longmapsto (h^{-1}g_1,g_2,\ldots,g_{p-1},g_ph)$$

von G in seine Äquivalenzklasse, wobei insbesondere zu beachten ist, dass für jedes $h \in G$ in der Tat $(h^{-1}g_1,g_2,\ldots,g_{p-1},g_ph) \in M$ liegt wegen $h^{-1}g_1g_2\cdots g_{p-1}g_ph = h^{-1}h = 1$. Damit haben alle Äquivalenzklassen bezüglich $(\sim)$ genau $\#G$ Elemente. Mit der disjunkten Zerlegung in Äquivalenzklassen folgt, dass $\#G$ die Anzahl $\#M$ teilt.

Sei $(g_1,g_2,\ldots,g_p) \in M$. Wegen

$$g_2\cdots g_{p-1}g_pg_1 = g_1^{-1}g_1g_2\cdots g_{p-1}g_pg_1 = g_1^{-1}g_1 = 1$$

ist auch sein um einen Schritt zyklisch vertauschtes Element $(g_2,\ldots,g_p,g_1)$ in M. Erklären wir nun eine zweite Äquivalenzrelation $(\approx)$ der *zyklischen Vertauschbarkeit* auf M vermittels

$$(g_1,g_2,\ldots,g_p) \approx (g_1',g_2',\ldots,g_p') \Longleftrightarrow \exists\, i \in [1,p]\ (g_1',g_2',\ldots,g_p') = (g_i,g_{i+1},\ldots,g_p,g_1,\ldots,g_{i-1})\ ,$$

so enthält wegen p prim die Äquivalenzklasse von $(g_1,g_2,\ldots,g_p) \in M$ genau p Elemente, falls nicht $g_1 = g_2 = \cdots = g_p$; sie enthält 1 Element, falls $g_1 = g_2 = \cdots = g_p$. Sei u die Anzahl der Äquivalenzklassen mit p Elementen, sei v die Anzahl der Äquivalenzklassen mit 1 Element. Es teilt p die Anzahl $\#G$, welche wiederum $\#M = pu + v$ teilt. Also teilt p die Anzahl v der konstanten Tupel in M.

Da $(1,\ldots,1) \in M$, muss es also ein $g \in G \smallsetminus \{1\}$ geben mit $(g,\ldots,g) \in M$, d.h. mit $g^p = 1$. Da $g \neq 1$, und da p prim, hat g die Ordnung p.

Bemerkung: Wir sehen sogar, dass die Anzahl der Elemente von G von Ordnung p kongruent zu -1 modulo p ist.