L. A. Kaloujnine, V. U. Suščanskij

Transformationen und Permutationen

Eine Einführung in die Gruppentheorie

1986 Deutscher Verlag der Wissenschaften Berlin
MSB: Nr. 124
Abschrift und LaTex-Satz: 2022 https://mathematikalpha.de

Vorwort zur deutschen Ausgabe

Vom VEB Deutscher Verlag der Wissenschaften, mit dem mich während meiner Tätigkeit an der Humboldt-Universität viele gemeinsame Anliegen verbanden, und von meinem alten Freund Dr. Ludwig Boll wurde ich gebeten, für die vorliegende Übersetzung ein Vorwort zu schreiben. Dieser Bitte bin ich gern nachgekommen.

Unser Büchlein ist für Schüler der oberen Klassen gedacht; es dürfte aber auch für Studienanfänger in Mathematik bzw. Informatik von Nutzen sein. Die erste, vor einigen Jahren in ukrainischer Sprache erschienene Ausgabe war nämlich hauptsächlich aus der Arbeit der Verfasser in Schülerarbeitsgemeinschaften an der "Spezialschule für Mathematik und Physik", die der Universität Kiew angegliedert ist, entstanden.

Die Resonanz und der Erfolg machten eine erweiterte Neuauflage erforderlich - sie erschien in russischer Sprache. Nun liegt eine Übersetzung in die deutsche Sprache vor, von der wir hoffen, dass sie unseren jungen Lesern im deutschen Sprachgebiet Wissen und Anregung vermitteln wird.

Die Entwicklung des hier behandelten Gegenstandes begann vor etwa 200 Jahren in Frankreich mit J. L. Lagrange (1736-1813). Er untersuchte Permutationen der Lösungen ("Wurzeln") algebraischer Gleichungen mit dem Ziel herauszufinden, wann sich diese Lösungen durch "Radikale" ausdrücken lassen.
Die ersten hundert Jahre der Entwicklung der Theorie der Permutationen und der aus solchen Permutationen bestehenden "Gruppen" stehen ganz im Zeichen hervorragender französischer Mathematiker: J. L. Lagrange, A. Cauchy (1789-1857), E. Galois (1811-1832), O. Jordan (1838-1922). Schon als Schüler hat Galois die Arbeiten Lagranges studiert, und von ihnen ausgehend hat er die Bedeutung des Begriffs einer Permutationsgruppe der Wurzeln für die Auflösbarkeit algebraischer Gleichungen in Radikalen erkannt. Dies kann als die Geburtsstunde der sogenannten modernen Algebra angesehen werden.

Vom Ende des 19. Jahrhunderts an hat dann der Gruppenbegriff größte Bedeutung in der gesamten Mathematik, aber auch in der Physik erlangt. Diese Entwicklung vollzog sich in der Hauptsache an den Universitäten in Deutschland, vor allem in Leipzig, Berlin und Göttingen. Die Namen S. Lie (1842-1899; Theorie der kontinuierlichen Transformationsgruppen), F. Klein (1849-1925; Erlanger Programm), H. Minkowski (1864-1909 ; vierdimensionale pseudoeuklidische Geometrie) seien hier stellvertretend für viele andere genannt.

Alles dies mündete in Anwendungen in der theoretischen Physik, u. a. in der Relativitätstheorie bei A. Einstein (1879-1955) und in der Quantentheorie bei M. Planck (1858-1947) und W. Heisenberg (1901-1976). Die dazu notwendigen mathematischen Begriffsbildungen sind in großer Allgemeinheit von H. Weyl (1895-1955) weiterentwickelt worden. Andere Anwendungen fand die Gruppentheorie in der Kristallographie ("Raumgruppen", A. Schoenflies (1853-1928) und E. S. Federov (1853-1919)).

Im ersten Jahrzehnt des 20. Jahrhunderts entstand in Kiew in dem Seminar von D. Grave (1863-1939) eine gruppentheoretische Schule, die in den folgenden Jahrzehnten zur

Wiege der sowjetischen Gruppentheorie wurde. Hier ist an erster Stelle O. Ju. Schmidt (1891-1956) zu nennen, ein unwahrscheinlich vielseitiger Gelehrter und Organisator.
Ihm folgten später in Moskau und Leningrad, aber auch an anderen Universitäten der Sowjetunion heute weltbekannte Gelehrte und Kollektive. Genannt seien hier nur A. Kuros (1908-1971) und D. K. Faddeev (geb. 1907). Von ihnen wurden höchst wichtige Resultate erzielt. So hat sich, ausgehend von Galois, der Gruppenbegriff zu einem zentralen Begriff der Mathematik entwickelt.

Darüber muss heute jeder Mathematiker Näheres wissen - als Einführung soll ihm unser Büchlein behilflich sein.
Es ist jedoch noch auf eine andere Entwicklungsrichtung hinzuweisen, die hier kurz gestreift werden soll. Permutationen endlicher Mengen gehören zum Bereich der Kombinatorik, und die damit zusammenhängenden Eigenschaften werden heute wichtig auch unabhängig vom Gruppenbegriff. Innerhalb der Mathematik spielt die Kombinatorik eine Rolle in der Wahrscheinlichkeitsrechnung und in der mathematischen Logik; wichtige außermathematische Anwendungen findet sie in der Informatik und neuerdings in der organischen Chemie.

Kombinatorische Eigenschaften der Permutationen wurden z. T. auch schon von Galois, so z. B. Cauchy und dann von dem irischen Mathematiker T. P. Kirkman (1806-1895) studiert. Wir möchten hoffen, dass unser Büchlein seinen Lesern auch einen Zugang zu diesem wichtigen Problemkreis eröffnet.

Kiew, den 27. 9. 1984 L. A. Kaloujnine

Inhaltsverzeichnis

1 Superposition von Funktionen

Die Superposition von Funktionen besitzt eine Reihe interessanter Eigenschaften und viele wichtige Anwendungen. Wir erinnern an die Definition und die einfachsten Eigenschaften der Superposition von Funktionen einer reellen Veränderlichen (Funktionen, deren Definitions- und Wertebereich Teilmengen der Menge der reellen Zahlen sind).

Es seien f und g beliebige Funktionen einer reellen Veränderlichen x. Eine Funktion h heißt Superposition dieser Funktionen (und zwar in der angegebenen Reihenfolge), wenn folgendes gilt:

a) Der Definitionsbereich von h besteht aus allen denjenigen Zahlen zu des Definitionsbereiches von f, für die $f(x_0)$ im Definitionsbereich der Funktion g liegt,

b) der Wert der Funktion h in jedem Punkt x_0 ihres Definitionsbereiches hängt mit den Werten von f und von g durch die Beziehung

$$h(x_0) = g(f(x_0))$$

zusammen.
Somit muss man, um den Wert der Funktion h im Punkt x_0 zu bestimmen, $f(x_0) = y_0$ und dann $g(y_0)$ bestimmen. Die Zahl $g(y_0)$ ist dann der Wert der Funktion h im Punkt x_0.
Dass eine Funktion u im Punkt x_0 den Wert u_0 annimmt, drücken wir wie folgt aus:

$$x_0 \overset{u}{\to} u(x_0) = u_0$$

Wir sagen auch, "die Funktion u ordnet dem Punkt x_0 den Wert u_0 zu" oder "der Punkt u_0 ist das Bild des Punktes x_0 unter der Funktion u". Die Superposition h der Funktionen $y = f(x)$ und $z = g(x)$ können wir folgendermaßen schreiben:

$$\begin{array}{ccccc} x_0 & \xrightarrow{f} & y_0 & \xrightarrow{g} & z_0 \\ \llcorner & & h & & \uparrow \end{array}$$

Dies besagt: Ordnet die Funktion f dem Punkt x_0 den Punkt y_0 zu und die Funktion g dem Punkt y_0 den Punkt z_0, so ordnet die Funktion h dem Punkt x_0 den Punkt z_0 zu.

Beispiel. Es seien $f(x) = x^2$ und $g(x) = \sin x$. Um den Wert der Superposition h dieser Funktionen in einem Punkt x_0 zu bestimmen, muss man zu ins Quadrat erheben,

$$x_0 \xrightarrow{f} y_0 = x_0^2$$

und den Wert von g im Punkt y_0 bestimmen:

$$y_0 \xrightarrow{f} y_0 = x_0^2 \xrightarrow{g} \sin(x_0^2)$$

Durch Zusammensetzung erhält man

$$x_0 \xrightarrow{f} y_0 = x_0^2 \xrightarrow{g} \sin(x_0^2)$$

Somit ordnet die Funktion h jedem Punkt x_0 die Zahl $\sin(x_0^2)$ zu, mit anderen Worten, h kann durch die Formel

$$h(x) = \sin(x^2)$$

angegeben werden.
Wir betrachten jetzt die Superposition h_1 der Funktionen $g(x) = \sin x$ und $f(x) = x^2$, d. h. die Superposition derselben Funktionen wie im oben betrachteten Beispiel, aber in umgekehrter Reihenfolge. Jetzt erhalten wir

$$\begin{array}{ccccc} x_0 & \xrightarrow{\sin} & \sin x_0 & \xrightarrow{(\ldots)^2} & (\sin x_0)^2 \\ \llcorner & & h_1 & & \uparrow \end{array}$$

Das bedeutet, dass die Superposition der Funktionen $g(x) = \sin x$ und $f(x) = x^2$ die Funktion

$$h_1(x) = (\sin x)^2 = \sin^2 x$$

ist. Somit hängt die Superposition von Funktionen von der Reihenfolge ab, in der die Funktionen superponiert werden.

Die Superposition der Funktionen $y = f(x)$ und $z = g(x)$ werden wir mit $(f \circ g)(x)$ bezeichnen, und wir erhalten die Darstellung

$$\begin{array}{ccccc} x & \xrightarrow{f} & y = f(x) & \xrightarrow{g} & z = g(y) \\ \llcorner & & f \circ g & & \uparrow \end{array}$$

Es ist also

$$(f \circ g)(x) = g(f(x))$$

Eine besondere Rolle in Bezug auf die Superposition spielt die Funktion $y = x$, die wir mit e bezeichnen wollen. Für jede Zahl x_0 schreiben wir also

$$x_0 \xrightarrow{e} x_0$$

Offenbar gelten für jede Funktion $y = f(x)$ die Gleichungen

$$(f \circ e)(x) = (e \circ f)(x) = f(x)$$

oder schematisch

$$\begin{array}{ccccc} x_0 & \xrightarrow{f} & y_0 = f(x_0) & \xrightarrow{e} & y_0 \\ \llcorner & & f \circ e & & \uparrow \end{array}$$

$$\begin{array}{ccccc} x_0 & \xrightarrow{e} & x_0 & \xrightarrow{f} & y_0 = f(x_0) \\ \llcorner & & e \circ f & & \uparrow \end{array}$$

Auch für die Funktion $y = -x$ führen wir eine besondere Bezeichnung ein, nämlich e'. Nun betrachten wir die Menge derjenigen Funktionen, welche die folgende Eigenschaft besitzen:

$$\begin{array}{ccc} \llcorner & h & \uparrow \end{array}$$

Gehören die Funktionen f und g einer gegebenen Funktionenmenge an, so gehört auch die Superposition $f \circ g$ dieser Funktionen zu dieser Menge.

Von einer solchen Menge sagt man, sie sei bezüglich der Superposition von Funktionen abgeschlossen oder auch, die Superposition sei für diese Menge eine innere Operation.

Als Beispiel bestimmen wir die Superposition zweier linearer Funktionen. Es sei $f(x) = 2x + 5$, $g(x) = 3x + 1$. Für eine beliebige Zahl x_0 erhalten wir

$$x_0 \xrightarrow{f} 2x_0 + 5 = y_0 \xrightarrow{g} 3y_0 + 1 = 3(2x_0 + 5 + 1)$$

d.h.

$$x_0 \xrightarrow{f \circ g} 3(2x_0 + 5) + 1 = 6x_0 + 16$$

daher ist $(f \circ g)(x) = 6x + 16$. Hieraus geht hervor, dass die Superposition dieser beiden linearen Funktionen wieder eine lineare Funktion ist.

Man kann leicht beweisen, dass dies auch für den allgemeinen Fall gilt: Ist $f(x) = ax+b$ und $g(x) = cx + d$, so ist

$$(f \circ g)(x) = c(ax + b) + d = acx + be + d = a_1x + b_1$$

also wieder eine lineare Funktion. Dabei lassen sich die Koeffizienten dieser Funktion durch die Koeffizienten der Funktionen f und g mit Hilfe der Gleichungen

$$a_1 = ae \qquad , \qquad b_1 = bc + d$$

ausdrücken. Folglich enthält die Menge aller linearen Funktionen mit je zwei Funktionen auch deren Superposition, d. h., die Superposition ist für die Menge aller linearen Funktionen eine innere Operation.

Auch das Ergebnis der Superposition linearer Funktionen hängt im allgemeinen von der Reihenfolge ab, in der sie superponiert werden. Ist etwa $f(x) = 2x + 3$ und $g(x) = 3x+2$, so ist $(f \circ g)(x)$ die Funktion ax_1+b_1, wobei $a_1 = 2 \cdot 3 = 6$ und $b_1 = 3 \cdot 3+2 = 11$ ist, während $(g \circ f)(x)$ die Funktion $a_2x + b_2$ mit $a_2 = 3 \cdot 2 = 6$ und $b_2 = 2 \cdot 2 + 3 = 7$ ist.
Somit ist $(f \circ g)(x) = 6x + 11$, aber $(g \circ f)(x) = 6x + 7$, d. h., für die gegebenen Funktionen gilt $f \circ g \neq g \circ f$.

Ein weiteres Beispiel für eine bezüglich der Superposition abgeschlossene Menge von Funktionen ist die Menge aller Polynome der Gestalt

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$

mit ganzzahligen Koeffizienten. Sind nämlich

$$f(x) = c_0x^k + c_1x^{k-1} + ... + c_{k-1}x + c_k, \qquad g(x) = b_0x^m + b_1x^{m-1} + ... + b_{k-1}x + b_k$$

zwei solche Polynome, so ist die Superposition $(f \circ g)(x)$ (wovon man sich leicht überzeugen kann) ein Ausdruck der Gestalt

$$b_0(c_0x^k + c_1x^{k-1} + ... + c_k)^m + b_1(c_0x^k + c_1x^{k-1} + ... + c_k)^{m-1} + ... + b_m$$

Das ist ein Polynom mk-ten Grades:

$$d_0x^{mk} + d_1x^{mk-1} + ... + d_{mk-1}x + d_{mk}$$

Dabei lassen sich die Koeffizienten $d_0, d_1, ..., d_{mk}$ in bestimmter Weise durch die Koeffizienten von f und g ausdrücken.

Die allgemeine Regel zur Bestimmung der Zahlen $d_0, d_1, ..., d_{mk}$ durch die bekannten Koeffizienten $c_0, ...c_k$, $b_0, ..., b_m$ ist ziemlich kompliziert; in jedem konkreten Fall gelingt es jedoch, die Koeffizienten ohne besondere Schwierigkeiten zu berechnen. Ist beispielsweise

$$f(x) = x^2 + 2x + 2 \qquad \text{und} \qquad g(x) = 2x^2 + x + 2$$

so gilt

$$(f \circ g)(x) = 2(x^2 + 2x + 2)^2 + (x^2 + 2x + 2) + 2 = 2x^4 + 8x^3 + 17x^2 + 18x + 12;$$
$$(g \circ f)(x) = (2x^2 + x + 2)^2 + 2(2x^2 + x + 2) + 2 = 4x^4 + 4x^3 + 13x^2 + 6x + 10$$

also wieder $f \circ g \neq g \circ f$.

In diesen Beispielen waren die bezüglich der Superposition abgeschlossenen Funktionenmengen unendlich. Eine solche Menge kann jedoch auch abgeschlossen sein, wenn sie nur aus endlich vielen Elementen besteht.
Für die nur aus den beiden Funktionen $y = x$ und $y = -x$ (die wir mit e bzw. e' bezeichnet haben) bestehende Menge ist die Superposition ebenfalls eine innere Operation. In der Tat ist

$$(e \circ e)(x) = (e' \circ e')(x) = e(x)$$
$$(e \circ e')(x) = (e' \circ e)(x) = e'(x)$$

d. h., die Bedingung für die Abgeschlossenheit ist erfüllt.

Schon aus diesen Beispielen geht hervor, dass Mengen, in denen die Superposition eine innere Operation ist, von ganz verschiedener Struktur sein können. Im weiteren betrachten wir die Struktur solcher Mengen für Funktionen, die auf endlichen Mengen definiert sind.

Aufgaben

1. Man bestimme die Superpositionen $f \circ g$ und $g \circ f$ für die Funktionen $y = f(x)$ und $y = g(x)$ in den Fällen

a) $y = 2x + 3$, $y = 3x + 4$;

b) $y = x^3 + 5x^2$, $y = x^2 + 3$;

c) $y = x^2 + 2$, $y = x^3 + x + 1$;

d) $y = \frac{2x+3}{3x+2}$, $y = \frac{x+4}{x-1}$

2. Sind folgende Funktionenmengen bezüglich der Superposition abgeschlossen?

a) die Menge aller Funktionen der Gestalt $y = ax$, wobei a eine beliebige reelle Zahl ist;

b) die Menge aller Funktionen der Gestalt $y = x + a$, wobei a eine beliebige rationale Zahl ist;

c) die Menge der vier Funktionen $y = x$, $y = 1/x$, $y = -1/x$, $y = -x$, von denen jede auf der Menge der von 0 verschiedenen reellen Zahlen betrachtet wird;

d) die Menge der Polynome höchstens dritten Grades;

e) die Menge der sechs Funktionen $y = \frac{1}{1-x}$, $y = \frac{x-1}{x}$, $y = 1 - x$, $y = \frac{1}{x}$, $y = \frac{x}{x-1}$, $y = x$.

2 Transformationen

Unter einer Abbildung einer Menge A in eine Menge B wollen wir eine Zuordnung verstehen, bei der jedem Element a der Menge A ein eindeutig bestimmtes Element b der Menge B entspricht; das Element b wird das Bild des Elementes a genannt, das Element a seinerseits heißt ein Urbild des Elementes b.

Abbildungen einer Menge in eine andere bezeichnen wir mit kleinen griechischen Buchstaben. Ist eine Abbildung φ einer Menge A in eine Menge B gegeben, so lässt sich dies durch eine der folgenden Schreibweisen zum Ausdruck bringen:

$$\varphi : A \to B \qquad , \qquad A \overset{\varphi}{\to} B$$

Das Bild eines Elementes $a \in A$ bei der Abbildung φ werden wir mit $(a)\varphi$ bezeichnen (das Zeichen für die Abbildung wird rechts hinter das Symbol des Elementes gesetzt).

Eine Abbildung einer Menge in eine andere kann angegeben werden durch die Vorschrift, nach welcher jedem Element der Menge A sein Bild aus der Menge B zugeordnet wird, aber auch durch Tabellen, durch graphische Darstellungen oder durch Pfeildiagramme.

Auf diese Arten, Abbildungen beliebiger Mengen anzugeben (die sowohl aus Zahlen als auch aus Elementen anderer Art bestehen können), gehen wir noch etwas ausführlicher ein.
Die Tabelle einer Abbildung $\varphi : A \to B$ stellt man auf, indem man alle möglichen Paare der Gestalt $(a, (a)\varphi)$, $a \in A$, aufschreibt:

x	a_1	a_2	...	a_n
$(x)\varphi$	$(a_1)\varphi$	$(a_2)\varphi$	...	$(a_n)\varphi$

Eine solche Tabelle beschreibt die Abbildung nur dann vollständig, wenn die Menge A endlich ist und aus den Elementen $a_1, ..., a_n$ besteht.

Graphische Darstellungen für Abbildungen von Mengen A, B, deren Elemente keine Zahlen sind, haben eine etwas andere Gestalt als graphische Darstellungen numerischer Funktionen, mit denen der Leser gut vertraut ist. Man realisiert sie auf folgende Weise: Es werden zwei senkrecht aufeinanderstehende Strahlen gezogen, die in einem Punkt entspringen. Dies sind die "Koordinatenachsen".

Auf dem horizontalen Strahl werden willkürlich (z. B. in gleichen Abständen) Punkte markiert, die den Elementen der Menge A entsprechen, und auf dem vertikalen Strahl Punkte, die den Elementen der Menge B entsprechen. Durch diese Punkte zieht man horizontale bzw. vertikale Geraden, so dass ein rechtwinkliges Netz (Gitter) entsteht.

Um eine graphische Darstellung der Abbildung $\varphi : A \to B$ zu gewinnen, markiert man diejenigen Gitterpunkte, deren "Koordinaten" alle möglichen Paare der Gestalt $(a, (a)\varphi)$ sind, wobei a ein beliebiges Element der Menge A ist.

Beispiel 1. Es sei A die Menge $\{n, i, x, e\}$ und B die Menge $\{1, 2, 3, 4, 5, 6, 7\}$, ferner $\varphi : A \to B$ die Abbildung, durch die jedem Buchstaben aus A diejenige Zahl zugeordnet wird, welche besagt, an wievielter Stelle in dem Wort Lexikon er steht.

Die graphische Darstellung dieser Abbildung ist in Abb. 1 angegeben.

Mit Hilfe von Pfeildiagrammen oder, wie man auch sagt, von Graphen, lassen sich Abbildungen von Mengen folgendermaßen angeben:
Den Elementen der Mengen A und B werden verschiedene Punkte der Ebene zugeordnet (für die Menge A links und für die Menge B rechts), und jeden der Punkte, welche Elemente von A kennzeichnen, verbindet man durch einen Pfeil von links nach rechts mit dem Punkt, der das entsprechende Element von B kennzeichnet.

Beispiel 2. Es sei A die Menge $\{3, 2, 6, 7\}$ und B die Menge $\{28, 12, 4, 5, 11\}$, ferner $\varphi : A \to B$ die Abbildung, die jeder Zahl aus A das kleinste gemeinsame Vielfache dieser Zahl und der Zahl 4 zuordnet.

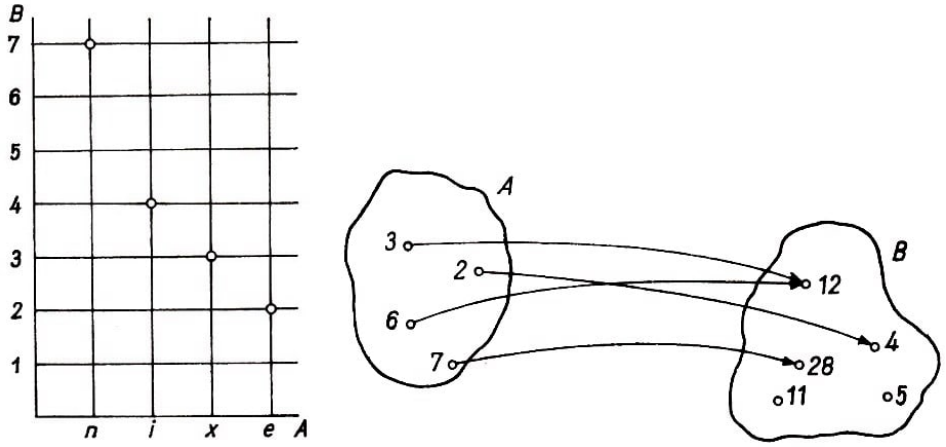


Abb. 1, 2

Diese Abbildung wird vollständig durch das Pfeildiagramm beschrieben, das in Abb. 2 dargestellt ist. Folglich erhält man $(3)\varphi = 12$, $(2)\varphi = 4$, $(6)\varphi = 12$, $(7)\varphi = 28$.

Wir werden im folgenden die Anzahl der Elemente einer endlichen Menge A mit $|A|$ bezeichnen. Beispielsweise ist $|\{a, b, c, f\}| = 4$, $|\{1, 7, 10\}| = 3$ usw.
Es seien A und B endliche Mengen mit $|A| = m$, $|B| = n$. Offenbar existieren nur endlich viele verschiedene Abbildungen von A in B, wenn als verschieden solche Abbildungen angesehen werden, welche auf mindestens ein Element der Menge A in verschiedener Weise wirken.

Unter Benutzung der Tatsache, dass jede Abbildung von A in B vollständig durch ihre Wertetabelle beschrieben wird, wollen wir jetzt berechnen, wieviel verschiedene Abbildungen der Menge A in die Menge B es gibt.

Wir bezeichnen die Elemente von A mit $a_1, a_2, ..., a_m$. Dann können wir jede Abbildung φ von A in B wie folgt als Tabelle schreiben:

x	a_1	a_2	...	a_m
$(x)\varphi$	b_1	b_2	...	b_m

wobei $b_1, b_2, ..., b_m$ gewisse nicht notwendig voneinander verschiedene Elemente der Menge B bezeichnen. Die obere Reihe der Tabelle ist für alle Abbildungen von A in B identisch, während die untere Reihe sich ändert, da verschiedenen Abbildungen verschiedene Tabellen entsprechen.

Dabei gibt es soviel verschiedene Abbildungen, wie es verschiedene Arten gibt, die zweite Reihe der betrachteten Tabelle auszufüllen.

In jedes Kästchen der zweiten Tabellenzeile kann man den Namen jedes einzelnen Elementes der Menge B schreiben. Somit kann man jedes der m Kästchen der unteren Tabellenzeile auf n verschiedene Arten füllen, unabhängig davon, was in den anderen Kästchen steht. Das bedeutet, dass man in der Tabelle der Abbildungen insgesamt

$$\underbrace{n \cdot n \cdot \ldots \cdot n}_{m} = n^m$$

verschiedene untere Zeilen bilden kann. Folglich existieren n^m verschiedene Abbildungen von A in B.

Wir heben nun einige wichtige Klassen von Abbildungen einer Menge in eine andere hervor und untersuchen sie gesondert.

1. Die Abbildung "auf".
Eine Abbildung $\varphi : A \to B$ heißt Abbildung auf die ganze Menge B oder Surjektion, wenn zu jedem Element $b \in B$ ein Element $a \in A$ existiert derart, dass $(a)\varphi = b$ gilt.

Beispiele.
3. Es seien $A = \mathbb{R}$ die Menge aller reellen Zahlen und $B = \mathbb{R}^+$ die Menge aller positiven reellen Zahlen. Wir geben eine Abbildung $\varphi : \mathbb{R} \to \mathbb{R}^+$ vor, indem wir $(x)\varphi = x^2$ für jedes $x \in \mathbb{R}$ setzen.
Dann ist φ eine Surjektion, weil zu jedem $y \in \mathbb{R}^+$ mindestens eine Zahl $x \in \mathbb{R}$ existiert derart, dass $(x)\varphi = y$ gilt. Es genügt, wenn wir $x = \sqrt{y}$ setzen. Wir erhalten sogar mehr: Zu jedem $y \in \mathbb{R}^+$ existieren genau zwei Urbilder, nämlich $\sqrt{y}$ und $-\sqrt{y}$.

4. Es sei $A = T$ die Menge aller rechtwinkligen Dreiecke in der Ebene und $B = \mathbb{R}^+$. Wir definieren die Abbildung $\varphi : T \to \mathbb{R}^+$ folgendermaßen:
Jedem rechtwinkligen Dreieck aus T ordnen wir die Zahl zu, die bei festgelegter Maßeinheit gleich seinem Flächeninhalt ist; φ ist eine Surjektion, weil zu jedem $x \in \mathbb{R}^+$ ein rechtwinkliges Dreieck (mit den Katheten $\sqrt{x}$ und $2\sqrt{x}$) existiert, das den Flächeninhalt x besitzt.

Es existieren sogar unendlich viele rechtwinklige Dreiecke, die den Flächeninhalt x besitzen (z. B. die Dreiecke mit den Katheten $\sqrt{2}/k$, $2k\sqrt{x}$, $k = 1, 2, 3, \ldots$). Folglich hat hier jedes Element $x \in \mathbb{R}^+$ unendlich viele Urbilder.

5. Es sei S die Menge aller dreistelligen Primzahlen und L die Menge aller Ziffern. Die Abbildung $\varphi : S \to L$ definieren wir wie folgt:
Wir ordnen jeder dreistelligen Primzahl ihre zweite Ziffer zu. Zum Beispiel

$$(179)\varphi = 7, \qquad (821)\varphi = 2, \qquad \varphi(907)\varphi = 0$$

Man kann sich unmittelbar davon überzeugen, dass φ eine Surjektion ist, d. h., dass zu jeder Ziffer eine dreistellige Primzahl existiert, in der diese Ziffer in der Mitte steht. Hier sind die Mengen S und L endlich, und zu jedem Element aus L gibt es nur endlich viele Elemente aus S, welche auf dieses Element abgebildet werden.

Sind die Mengen A und B endlich und ist $\varphi : A \to B$ eine Surjektion, so kommen in der unteren Zeile der Wertetabelle von φ alle Elemente von B vor. Auf jeder horizontalen Geraden der graphischen Darstellung einer Surjektion ist notwendigerweise ein Gitterpunkt markiert.
Im Pfeildiagramm einer Surjektion führt zu jedem Punkt, der ein Element von B bezeichnet, mindestens ein Pfeil.

Unter den Abbildungen einer endlichen Menge A auf eine Menge B braucht keine Surjektion zu existieren. Für die Existenz einer Surjektion ist offenbar notwendig, dass die Menge B ebenfalls endlich und die Ungleichung $|A| \geq |B|$ erfüllt ist.

2. Die umkehrbar eindeutige Abbildung.
Eine Abbildung $\varphi : A \to B$ wird umkehrbar eindeutig oder eine Injektion genannt, wenn voneinander verschiedene Elemente der Menge A durch diese Abbildung in voneinander verschiedene Elemente der Menge B übergeführt werden, d. h., wenn für beliebige Elemente x_1, x_2 aus A mit $x_1 \neq x_2$ auch $(x_1)\varphi \neq (x_2)\varphi$ gilt.

Beispiele.
6. Eine Abbildung φ der Menge $\mathbb{Z}$ der ganzen Zahlen in die Menge $2\mathbb{Z}$ aller geraden Zahlen sei folgendermaßen definiert: Für jedes $z \in \mathbb{Z}$ sei $(z)\varphi = 6z$. Dies ist eine Injektion; denn aus $x_1 \neq x_2$ folgt $6z_1 \neq 6z_2$.

7. Es sei A die Menge aller zweielementigen Teilmengen der Menge der reellen Zahlen $\mathbb{R}$ und B die Menge der auf die Normalform reduzierten quadratischen Gleichungen. Jedem Element $\{a, b\}$ aus A ordnen wir diejenige Gleichung aus B zu, für welche die Zahlen a und b Lösungen sind. Wie aus dem Vietaschen Wurzelsatz folgt, ist diese Abbildung injektiv.

In der unteren Zeile der Tabelle einer injektiven Abbildung $\varphi : A \to B$ tritt im Unterschied zu den Tabellen beliebiger Abbildungen jedes Element von B nur einmal auf. Folglich wird auf jeder horizontalen Geraden der graphischen Darstellung einer Injektion höchstens ein Gitterpunkt markiert, und in dem Pfeildiagramm geht zu jedem Punkt, der ein Element der Menge B bezeichnet, höchstens ein Pfeil.

Sind die Mengen A und B endlich und existiert eine Injektion der Menge A in die Menge B, so gilt offenbar die Ungleichung $|A| \leq |B|$.

3. Die umkehrbar eindeutige Abbildung "auf". Ist eine Abbildung einer Menge A in eine Menge B gleichzeitig injektiv und surjektiv, so wird sie eine umkehrbar eindeutige (bijektive) Abbildung von A auf B oder eine Bijektion von A auf B genannt.

Beispiele.
8. Es sei $A = B = \Pi$ die Menge aller Punkte der Ebene. Dann ist jede der folgenden aus dem Geometrieunterricht in der Schule bekannten Abbildungen der Menge Π auf sich eine Bijektion: die Spiegelung bezüglich eines festen Punktes, die Spiegelung bezüglich einer festen Geraden, die Parallelverschiebung, die Drehung um einen festen Punkt, die zentrische Streckung.

9. Die Abbildung $\varphi : x \to 2x$ für $x \in \mathbb{Z}$ ist offenbar eine Bijektion der Menge $\mathbb{Z}$ auf

die Menge $2\mathbb{Z}$ der geraden Zahlen.

Existiert eine Bijektion einer endlichen Menge A auf eine endliche Menge B, so müssen die Ungleichungen $|A| \geq |B|$ und $|A| \geq |B|$ gelten. Folglich existiert für endliche Mengen A und B eine Bijektion von A auf B dann und nur dann, wenn die Gleichung $|A| = |B|$ besteht.

Wir berechnen nun, wieviel verschiedene Bijektionen von $A = \{a_1, a_2, ..., a_n\}$ auf $B = \{b_1, b_2, ..., b_n\}$ existieren.
Jede Bijektion $\varphi : A \to B$ lässt sich vollständig durch eine Wertetabelle beschreiben:

x	a_1	a_2	...	a_n
$(x)\varphi$	b_1	b_2	...	b_n

Die obere Reihe der Tabelle ändert sich nicht, während in der unteren Reihe die notwendigerweise voneinander verschiedenen Elemente der Menge B in beliebiger Anordnung stehen können.
Folglich kann man das erste Kästchen (z. B. von links) der unteren Reihe der Tabelle auf n verschiedene Arten füllen. Ist das erste Kästchen bereits gefüllt, so kann man unabhängig davon, welches Element es enthält, in das zweite Kästchen jedes beliebige der übriggebliebenen Elemente von B einsetzen.
Analog ist es mit dem dritten Kästchen; unabhängig davon, welche Elemente in die ersten beiden Kästchen eingesetzt wurden, kann man es auf $n-2$ Arten ausfüllen usw.

Das vorletzte Kästchen kann nur noch auf zwei mögliche Weisen gefüllt werden, das letzte lediglich noch auf eine. Da für jedes Kästchen die Anzahl der Möglichkeiten seiner Belegung unabhängig von der Belegung der übrigen ist, existieren

$$n(n-1) \cdot (n-2) \cdot 2 \cdot 1 = n!$$

verschiedene Arten, die Kästchen gleichzeitig zu füllen. Folglich kann man $n!$ verschiedene solcher Tabellen aufstellen, d. h., es existieren $n!$ verschiedene Bijektionen von A auf B.

Sehr oft hat man Abbildungen einer gewissen Menge M in sich zu betrachten. Solche Abbildungen heißen Transformationen der Menge M. Dem Leser sind z. B. die verschiedenen Typen geometrischer Transformationen gut bekannt, die bereits in Beispiel 8 genannt wurden.

Als Transformationen einer beliebigen Menge können auch die oben eingeführten Klassen von Abbildungen, die Injektionen, Bijektionen und Surjektionen angesehen werden. Wie man leicht sieht, stimmen aber diese drei Transformationsklassen für endliche Mengen überein, d.h., jede Injektion einer endlichen Menge in sich ist auch eine Surjektion, und jede Surjektion ist gleichzeitig auch Injektion. Daher lässt sich für endliche Mengen nur die Klasse der bijektiven Transformationen hervorheben.

Bei der Untersuchung von Transformationen einer endlichen Menge ist es zweckmäßig, sich an bestimmte Standardbezeichnungen zu halten. Die Natur der Elemente einer Menge M ist beim Studium ihrer Transformationen unwesentlich.

Folglich können wir alle Elemente von M nummerieren und nicht mit den Elementen selbst, sondern mit ihren Nummern operieren. Daher werden wir uns bei der Untersuchung von Transformationen endlicher Mengen künftig die Menge $M = \{1, 2, ..., n\}$ der natürlichen Zahlen $1, 2, ..., n$ vorstellen. Wenn wir die Transformationen mit Hilfe von Tabellen vorgeben, schreiben wir sie in der folgenden vereinfachten Gestalt:

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix}$$

Offenbar charakterisiert diese Bezeichnung die Transformation eindeutig und führt nicht zu Missverständnissen. Ist beispielsweise $M = \{1, 2, 3, 4, 5\}$, so sind

$$a) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 2 & 5 \end{pmatrix}, \qquad b) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}, \qquad c) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Tabellen für verschiedene Transformationen auf der Menge M. Zu lesen ist eine solche Tabelle (etwa a)) folgendermaßen:
"Die Transformation φ, die durch die Tabelle a) gegeben wird, führt

1 in 2, 2 in 2, 3 in 4, 4 in 2, 5 in 5

über.
Es ist unwesentlich, in welcher Reihenfolge man die Elemente der oberen Zeile einer solchen Tabelle aufschreibt. Zum Beispiel kann man die durch Tabelle b) gegebene Transformation mit Hilfe folgender Tabellen beschreiben:

$$\begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 5 & 4 & 1 & 2 & 3 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

Da jede Transformation einer endlichen Menge durch ihre Tabelle vollständig beschrieben wird, werden wir oft die Transformation und ihre Tabelle mit demselben Symbol bezeichnen.

Einige Transformationen der Menge M haben spezielle Namen:
a) Die identische Transformation. Dies ist die Transformation s, die alle Elemente aus M fest lässt, für die also (a) $\varepsilon = a$ für jedes $a \in M$ gilt. Ist M eine endliche Menge, so besitzt diese Transformation die Tabelle

$$\begin{pmatrix} 1 & 2 & 3 & ... & n-1 & n \\ 1 & 2 & 3 & ... & n-1 & n \end{pmatrix}$$

b) Die konstante Transformation. Eine Transformation wird konstant genannt, wenn sie jedem Element aus M ein bestimmtes festgehaltenes Element derselben Menge zuordnet.
Ist M eine endliche Menge, so wird die konstante Transformation durch eine Tabelle der Form

$$\begin{pmatrix} 1 & 2 & 3 & ... & n-1 & n \\ a & a & a & ... & a & a \end{pmatrix}$$

charakterisiert, wobei a zu M gehört.

c) Permutation. Unter einer Permutation versteht man eine Bijektion einer endlichen Menge auf sich. Folglich ist φ dann und nur dann eine Permutation von M, wenn für beliebige Elemente a, b aus M mit $a \in b$ auch $(a)\varphi \neq (b)\varphi$ gilt. Das bedeutet, dass eine Permutation durch eine Tabelle der Gestalt

$$\begin{pmatrix} 1 & 2 & 3 & ... & n-1 & n \\ a_1 & a_2 & a_3 & ... & a_{n-1} & a_n \end{pmatrix}$$

beschrieben wird, wobei $a_1, a_2, a_3, ..., a_n$ die voneinander verschiedenen Elemente aus M sind.

Aufgaben

1. Man konstruiere die graphischen Darstellungen und Pfeildiagramme für die Abbildungen der Menge $\{1, 2, 3, 4, 5\}$ in die Menge $\{a, b, c, d\}$, die durch die folgenden Tabellen gegeben sind:

$$a) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & b & a \end{pmatrix}, \qquad b) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & a & a & c & a \end{pmatrix}, \qquad c) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & a & b & c \end{pmatrix}$$

2. Es seien A und B endliche Mengen mit $|A| = m$, $|B| = n$. Wieviel verschiedene Injektionen von A in B gibt es?

3. Unter Benutzung der Lösung von Aufgabe 2 ist zu ermitteln, wieviel m-elementige Teilmengen einer n-elementigen Menge es gibt.

4. Gibt es eine surjektive Abbildung $\varphi : S \to L$ aus der Menge S der Wörter der russischen Sprache in die Menge L der Buchstaben des russischen Alphabets, die jedem Wort seinen ersten Buchstaben zuordnet?

5. Welche Eigenschaften unterscheiden die graphischen Darstellungen und die Pfeildiagramme einer Bijektion von den graphischen Darstellungen und den Pfeildiagrammen beliebiger Abbildungen?

6. Auf wieviel Arten kann man n Türme derselben Farbe auf einem Schachbrett mit n^2 Feldern so aufstellen, dass niemals zwei einander schlagen können?

7. Wieviel verschiedene Permutationen auf der Menge $M = \{1, 2, 3, 4, 5\}$ existieren, die kein Element aus M festlassen (d. h., für die $(a)\varphi \neq a$ für jedes $a \in M$ gilt)?

8. Auf wieviel verschiedene Arten kann man auf einem Schachbrett acht Türme derselben Farbe so aufstellen, dass keiner von ihnen auf der weißen Diagonale steht und dass niemals zwei einander schlagen können?

9. Wieviel verschiedene sechsstellige Zahlen kann man aus den Ziffern 0, 1, 2, 3, 4, 7, 9 bilden?

10. Wieviel verschiedene Permutationen φ der Menge $\{1, 2, 3, ..., n\}$ existieren, für welche $(1)\varphi - (2)\varphi > 1$ gilt?

11. Man zeige, dass für $n \geq 4$ eine Permutation φ der Menge $M = \{1, 2, ..., n\}$ existiert, für die bei beliebigen $i, j \in M$ die Bedingung $|(i)\varphi - (j)\varphi| = |i - j|$ erfüllt ist.

12. Man zeige, dass für $n \geq 4$ eine Anordnung von n Damen derselben Farbe auf einem Schachbrett mit n^2 Feldern existiert, bei der keine zwei Damen einander schlagen können.

13. Auf wieviel Arten kann man acht Damen derselben Farbe auf einem Schachbrett so anordnen, dass keine zwei von ihnen einander schlagen können?

3 Multiplikation von Transformationen

In Abschnitt 1 haben wir die Bildung der Superposition von Funktionen betrachtet, die auf der Menge der reellen Zahlen definiert sind. Analog kann man aus zwei gegebenen Transformationen eine neue Transformation konstruieren, und zwar für beliebige Mengen.

Es seien M eine beliebige Menge, φ und ψ gewisse Transformationen dieser Menge. Unter dem Produkt (der Hintereinanderausführung) der Transformationen φ und ψ versteht man die Transformation ω, die auf jedes Element $a \in M$ so wirkt, dass

$$(a)\omega = ((a)\varphi)\psi \tag{1}$$

gilt; um das Bild eines beliebigen Elementes a aus M bei der Transformation ω zu bestimmen, muss man zuerst das Bild b von a bei der Transformation φ finden und danach das Bild c des Elementes b vermöge der Transformation ψ.
Das Element c ist dann das Bild von a vermöge der Transformation ω.

In einem Pfeildiagramm kann man die Wirkung der Transformation ω auf $a \in M$ folgendermaßen ausdrücken:

$$\begin{array}{ccccc} a & \xrightarrow{\varphi} & b & \xrightarrow{\psi} & c \\ \llcorner & & \omega & & \uparrow \end{array}$$

Das Produkt der Transformationen φ und ψ wird im weiteren mit $\varphi \circ \psi$ bezeichnet.

Beispiele
1. Es sei M die Menge der Menschen, die irgendwann auf der Erde lebten, φ sei diejenige Transformation von M, die jedem Menschen seinen Vater zuordnet, und ψ die Transformation von M, die jedem Menschen seine Mutter zuordnet. Dann ist

a) $\varphi\circ\psi$ die Transformation von M, die jedem Menschen die Großmutter väterlicherseits zuordnet;
b) $\varphi\circ\varphi$ die Transformation von M, die jedem Menschen den Großvater väterlicherseits zuordnet;
c) $\psi \circ \varphi$ die Transformation von M, die jedem Menschen seinen Großvater mütterlicherseits zuordnet;
d) $\psi \circ \psi$ die Transformation von M, die jedem Menschen seine Großmutter mütterlicherseits zuordnet.

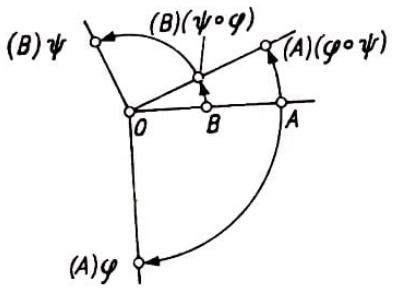


Abb. 3

2. Es sei $M = \Pi$ die Menge der Punkte der Ebene, φ die Drehung der Ebene um einen festen Punkt O um den Winkel $\pi/2$ im Uhrzeigersinn, ψ die Drehung der Ebene um diesen Punkt um den Winkel $2\pi/3$ im Gegenzeigersinn. Dann sind sowohl $\varphi \circ \psi$ als auch $\psi \circ \varphi$ Drehungen um den Winkel $\pi/6$ im Gegenzeigersinn (vgl. Abb. 3).

3. Es sei $\varphi : x \to x + 3$ die Transformation der Menge der reellen Zahlen $\mathbb{R}$, die jeder Zahl x die Zahl $x + 3$ zuordnet, und $\psi : x \to x + 2$ die Transformation derselben Menge, die jede Zahl x in die Zahl $x + 2$ überführt.
Dann ist $\varphi \circ \psi = \psi \circ \varphi$ die Transformation, die jede Zahl x in die Zahl $x + 5$ überführt (vgl. Abb. 4).

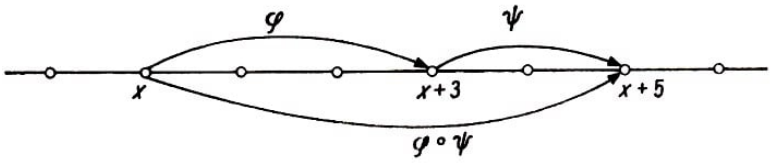


Abb. 4

Sehr leicht ist das Produkt zweier durch Pfeildiagramme gegebener Transformationen zu bilden. Wir erläutern dies an einem Beispiel.

Es seien $varphi$ und ψ Transformationen der Menge $M = \{a, b, c, d, 1\}$, deren Pfeildiagramme in Abb. 5 dargestellt sind.
Um das Pfeildiagramm der Transformation $\varphi \circ \psi$ zu konstruieren, muss man diejenigen Punkte der rechten Seite des Diagramms von φ und der linken Seite des Diagramms von ψ miteinander verbinden, welche dieselben Elemente von M kennzeichnen (in Abb. 5 sind diese Pfeile durch gestrichelte Linien dargestellt).

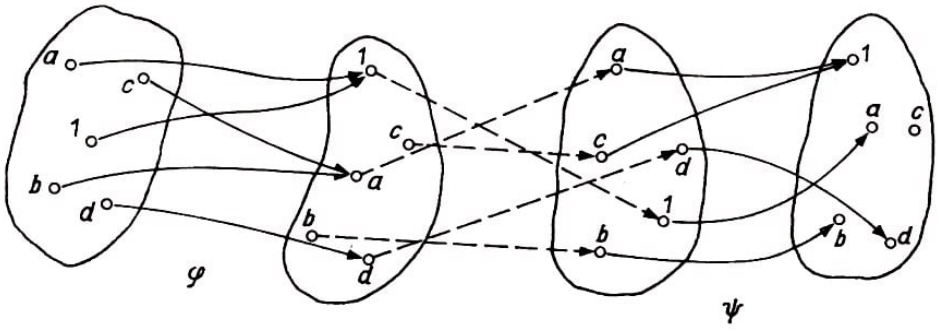


Abb. 5

Wir erhalten ein eindeutiges Schema, mit dessen Hilfe wir das Bild jedes Elementes aus M bei der Transformation $\varphi \circ \psi$ auf folgende Weise finden: Von jedem Punkt der linken Seite des Pfeildiagramms von 99 gehen wir längs der Pfeile bis zu dem entsprechenden Punkt der rechten Seite des Pfeildiagramms von ψ. Somit ist

$$(a)(\varphi \circ \psi) = a, \quad (b)(\varphi \circ \psi) = 1, \quad (c)(\varphi \circ \psi) = 1, \quad (d)(\varphi \circ \psi) = d, \quad (e)(\varphi \circ \psi) = a$$

Folglich besitzt die Transformation $\varphi \circ \psi$ das in Abb. 6 dargestellte Pfeildiagramm.

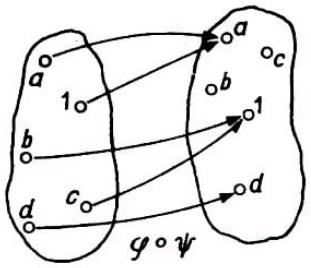


Abb. 6

Die Tabelle des Produktes der Permutationen

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \qquad , \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ j_1 & j_2 & j_3 & \dots & j_n \end{pmatrix}$$

findet man mit Hilfe einer ebenso bequemen Regel:

a) Die Spalten der Tabelle von ψ werden so umgestellt, dass ihre obere Zeile mit der unteren Zeile der Tabelle von φ übereinstimmt; man erhält dann

$$\psi' = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ k_1 & k_2 & k_3 & \dots & k_n \end{pmatrix}$$

b) man konstruiert eine neue Tabelle, deren erste Zeile gleich der ersten Zeile der Tabelle von φ und deren zweite Zeile gleich der zweiten Zeile von ψ' ist.
Diese Tabelle ist dann die Tabelle der Transformation $\varphi \circ \psi$.

28 3. Multiplikation von Transformationen Beispiel 4. Es seien

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}, \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

dann ist

$$\begin{aligned} \varphi \circ \psi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 1 & 6 & 2 & 5 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} \end{aligned}$$

Im vorangegangenen Abschnitt betrachteten wir die drei Klassen von Transformationen einer beliebigen Menge: Injektionen, Surjektionen und Bijektionen.
Es wird sich zeigen, dass jede dieser drei Klassen bezüglich der Multiplikation von Transformationen abgeschlossen ist, d. h., dass das Produkt von Injektionen wieder eine Injektion, das Produkt von Surjektionen eine Surjektion und schließlich das Produkt von Bijektionen wieder eine Bijektion ist.

Sind nämlich φ und ψ Injektionen der Menge M in sich und ist $\omega = \varphi \circ \psi$, so gilt für jedes Paar von verschiedenen Elementen a, b aus M

$$(a)\varphi \neq (b)\varphi, \qquad (a)\psi \neq (b)\psi$$

Nun lassen wir die Transformation ω auf a und b einwirken. Nach Definition des Produkts von Transformationen ist

$$(a)\omega = ((a)\varphi)\psi = (a_1)\psi, \qquad (b)\omega = ((b)\varphi)\psi = (b_1)\psi$$

mit $a_1 = (a)\varphi$, $b_1 = (b)\varphi$. Da φ eine Injektion ist, gilt $a_1 \neq b_1$. Da ψ seinerseits eine Injektion ist, gilt $(a_1)\psi \neq (b_1)\psi$. Folglich gilt für jedes Paar $a, b \in M$ mit $a \neq b$ die Beziehung $(a)\omega \neq= (b)\omega$; somit ist ω eine Injektion.

Nun seien die Transformationen φ und ψ Surjektionen.
Wir überzeugen uns davon, dass es zu jedem Element a aus M ein Element $b \in M$ gibt, für welches $(b)\omega = a$ gilt. Da ψ eine Surjektion ist, lässt sich ein Element $c \in M$ finden, für welches $(c)\psi = a$ ist, und aus der Surjektivität von φ folgt, dass ein Element b aus M existiert, für welches $(b)\varphi = c$ gilt.
Das Element b ist das gesuchte:

$$(b)\omega = ((b)\varphi)\psi = (c)\psi = a$$

Folglich ist die Transformation ω eine Surjektion.

Hieraus ergibt sich aber sofort, dass das Produkt bijektiver Transformationen eine bijektive Transformation ist. Insbesondere stimmen für endliche Mengen alle drei Transformationsklassen überein, d. h., das Produkt zweier beliebiger Permutationen einer Menge M ist wieder eine Permutation von M. Dies folgt auch aus unserer Regel zur Bestimmung des Produktes von Permutationen.

Bekanntlich lassen sich die Grundrechenarten Addition und Multiplikation von Zahlen durch eine Reihe von Eigenschaften charakterisieren. Zum Beispiel kommen der Addition von Zahlen (und zwar der Operation Addition und nicht den Zahlen selbst) die folgenden Eigenschaften zu:

a) Assoziativität. Für je drei Zahlen a, b, c gilt die Identität

$$a + (b + c) = (a + b) + c$$

b) Kommutativität. Für je zwei Zahlen a und b gilt die Identität

$$a + b = b + a$$

c) Es existiert ein neutrales Element (die Null) derart, dass für jede Zahl a

$$a + 0 = 0 + a = a$$

gilt.

d) Zu jeder Zahl a existiert eine entgegengesetzte Zahl $-a$ derart, dass

$$a + (-a) = 0$$

gilt.

Wir untersuchen nun, ob diese Eigenschaften auch für die Multiplikation von Transformationen einer beliebigen Menge M zutreffen.

a) Die Multiplikation von Transformationen einer beliebigen Menge M ist assoziativ. Das bedeutet: Für je drei Transformationen α, β, γ der Menge M besteht die Identität

$$(\alpha \circ \beta) \cdot \gamma = \alpha \circ (\beta \circ \gamma) \tag{2}$$

Sie besagt, dass die Transformationen $\varphi = (\alpha \circ \beta) \circ \gamma$ und $\psi = \alpha \circ (\beta \circ \gamma)$ auf jedes Element a aus M in gleicher Weise wirken:

$$(a)((\alpha \circ \beta) \circ \gamma) = (a)(\alpha \circ (\beta \circ \gamma)) \tag{3}$$

Wählen wir willkürlich ein Element a aus M und ist $(a)\alpha = b$, $(b)\beta = c$, $(c)\gamma = d$, so ist nach Definition (1)

$$(a)\varphi = ((a)(\alpha \circ \beta))\gamma = (((a)\alpha)\beta)\gamma = ((b)\beta)\gamma = (c)\gamma = d$$
$$(a)\psi = ((a)\alpha)(\beta \circ \gamma) = (b)(\beta \circ \gamma) = ((b)\beta)\gamma = (c)\gamma = d$$

Somit gilt die Identität (3) für beliebiges $a \in M$; folglich ist auch die Identität (2) richtig.

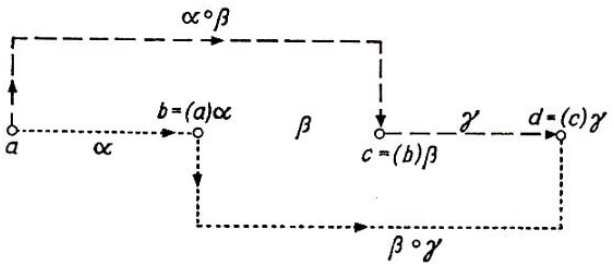


Abb. 7

In Abb. 7 ist die Wirkung des Produktes von Transformationen auf ein Element a schematisch dargestellt. Dem Produkt $\alpha \circ (\beta \circ \gamma)$ entspricht der Weg, der durch die punktierte Linie angedeutet ist, und dem Produkt $(\alpha \circ \beta)\gamma$ der Weg, den die gestrichelte Linie angibt. Beide Linien enden in dem Punkt, der dem Element d aus M entspricht, d. h., die Transformationen φ und ψ wirken in gleicher Weise auf das Element a. Folglich ist die Multiplikation von Transformationen einer Menge M assoziativ.

b) Die Multiplikation von Transformationen einer beliebigen Menge ist nicht kommutativ. Das bedeutet, dass Transformationen φ und ψ einer gegebenen Menge existieren, für die

$$\varphi \circ \psi \neq \psi \circ \varphi$$

gilt.
Solche Transformationen auf den entsprechenden Mengen sind die in den Beispielen 1 und 4 angegebenen Transformationen φ und ψ.

Man darf jedoch nicht glauben, dass das Produkt von Transformationen immer von der Reihenfolge der Faktoren abhängt. Beispielsweise hängt das Produkt der in den

Beispielen 2 und 3 definierten Transformationen nicht von der Reihenfolge der Faktoren ab. Das Produkt der Permutationen

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix} \qquad \text{und} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}$$

hängt ebenfalls nicht davon ab, in welcher Reihenfolge sie aufgeschrieben werden:

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

c) Eine besondere Rolle bei der Multiplikation von Transformationen spielen die identische Transformation ε und die konstante Transformation δ_x für $x \in M$ (wir erinnern daran, dass $(a)\varepsilon = a$ und $(a)\delta_x = x$ für jedes $a \in M$ ist). Die Transformation ε spielt für die Multiplikation von Transformationen dieselbe Rolle, wie die Eins bei der Multiplikation von Zahlen (oder die Null bei der Addition von Zahlen), d.h., für jede Transformation φ der Menge M gilt

$$\varphi \circ \varepsilon = \varepsilon \circ \varphi = \varphi \tag{4}$$

Setzen wir nämlich $(a)\varphi = b$, so ist nach Definition (1) des Produktes für jedes $a \in M$

$$(a)(\varphi \circ \varepsilon) = ((a)\varphi)\varepsilon = (b)\varepsilon = b$$
$$(a)(\varepsilon \circ \varphi) = ((a)\varepsilon)\varphi = (a)\varphi = b$$

Dies besagt gerade, dass die Gleichung (4) erfüllt ist.
Es ist leicht einzusehen, dass ε die einzige Transformation ist, für welche die Gleichungen (4) gelten. Nehmen wir nämlich an, es existiere eine Transformation $\varepsilon' \neq \varepsilon$ derart, dass für jedes φ

$$\varepsilon' \circ \varphi = \varphi \circ \varepsilon' = \varphi$$

gilt. Dann muss das Produkt $\varepsilon \circ \varepsilon' = \varepsilon' \circ \varepsilon$ einerseits gleich ε' sein (wenn ε' die Rolle der Eins spielt). Folglich gilt

$$\varepsilon = \varepsilon \circ \varepsilon' = \varepsilon'$$

also $\varepsilon = \varepsilon'$; wir haben einen Widerspruch erhalten, der davon zeugt, dass unsere Annahme falsch war.

Die Transformationen δ_x (davon gibt es ebensoviel, wie die Menge M Elemente besitzt) spielen für die Multiplikation die Rolle der "Null", d. h., für jede Transformation φ gilt

$$\varphi \circ \delta_x = \delta_x$$

Es ist aber $\delta_x \circ \varphi = \delta_{(x)\varphi}$. Dies möge der Leser selbst nachprüfen.

Beispiel 5. Es sei

$$M = \{1, 2, 3, 4, 5\} \qquad , \qquad \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Dann ist

$$\varphi \circ \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix}$$
$$\delta_2 \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 \end{pmatrix}$$

(hier ist $4 = (2)\varphi$).
Folglich erhält man, wenn man eine beliebige Transformation von rechts mit "Null" multipliziert, wieder dieselbe "Null", multipliziert man aber von links, so wird die "Null" eine andere.

d) Unter einer Inversen der Transformation α einer beliebigen Menge M versteht man eine Transformation β dieser Menge, welche die Gleichung

$$\alpha \circ \beta = \beta \circ \alpha = \varepsilon$$

erfüllt.
Diese Transformation spielt dieselbe Rolle wie die entgegengesetzte Zahl bei der Addition von Zahlen bzw. die Reziproke bei der Multiplikation von Zahlen. Ebenso wie die reziproke Zahl a^{-1} (die nur für $a \neq 0$ existiert) braucht eine inverse Transformation nicht immer zu existieren. Zum Beispiel ist die zu $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ inverse Transformation die Transformation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$; zu den konstanten Transformationen existieren jedoch keine Inversen. In denjenigen Fällen jedoch, in denen eine inverse Transformation existiert, ist sie eindeutig bestimmt.

Nehmen wir nämlich an, zu einer Transformation φ der Menge M würden zwei inverse Transformationen φ_1 und φ_2 ($\varphi_1 \neq \varphi_2$) existieren, welche gleichzeitig den Gleichungen

$$\varphi \circ \varphi_1 = \varphi_1 \circ \varphi = \varepsilon \qquad , \qquad \varphi \circ \varphi_2 = \varphi_2 \circ \varphi = \varepsilon$$

genügen, dann würden wir aus den Gleichungen und der Assoziativität der Multiplikation von Transformationen

$$\varphi_1 = \varphi_1 \circ \varepsilon = \varphi_1 \circ (\varphi \circ \varphi_2) = (\varphi_1 \circ \varphi) \circ \varphi_2 = \varepsilon \circ \varphi_2 = \varphi_2$$

erhalten und kämen zu einem Widerspruch, der bestätigt, dass unsere Annahme falsch war.

Die eindeutig bestimmte Transformation, die zur Transformation α invers ist, werden wir im folgenden mit φ^{-1} bezeichnen.
Wann existiert nun die inverse Transformation? Der folgende Satz gibt uns auf diese Frage eine erschöpfende Antwort.

Satz. Zu einer Transformation α der Menge M existiert dann und nur dann die inverse Transformation, wenn α eine Bijektion der Menge M ist.

Beweis. Notwendigkeit. Es existiere die zu α inverse Transformation β, d. h., es sei $\alpha \circ \beta = \beta \circ \alpha = \varepsilon$. Dann gelten für jedes $y \in M$ die Beziehungen

$$y = (y)\varepsilon = (y)(\beta \circ \alpha) = ((y)\beta)\alpha = (z)\alpha$$

mit $z = (y)\beta$. Folglich existiert zu jedem $y \in M$ ein Element $z \in M$ derart, dass $(z)\alpha = y$ ist. Somit ist α eine Surjektion.

Wir zeigen nun, dass die Transformation α auch eine Injektion ist. Nehmen wir an, dies sei nicht der Fall, dann lassen sich verschiedene Elemente $a, b \in M$ finden, für welche $(a)\alpha = (b)\alpha = c$ gilt. Daraus ergibt sich

$$((a)\alpha)\beta = ((b)\alpha)\beta = (c)\beta \qquad \text{oder} \qquad (a)(\alpha \circ \beta) = (b)(\alpha \circ \beta) = (c)\beta$$

und hieraus $(a)\varepsilon = (b)\varepsilon$, also $a = b$. Dies ist ein Widerspruch, der beweist, dass α eine Injektion ist.

Hinlänglichkeit. Es sei α eine bijektive Transformation.
Dann existiert zu jedem $x \in M$ ein eindeutig bestimmtes Urbild, d. h. ein Element y aus M mit $(y)\alpha = x$. Daher kann man eine Transformation β der Menge M bestimmen, die jedem Element an aus M sein Urbild y vermöge der Transformation α zuordnet:

$$\text{Wenn } y \xrightarrow{\alpha} x, \text{ so } x \xrightarrow{\beta} y.$$

β ist wirklich eine Transformation; denn da α eine Surjektion ist, ist β für jedes Element von M definiert. Aus der Definition von β folgt, dass die Gleichungen

$$((x)\alpha)\beta = x \qquad \text{und} \qquad ((x)\beta)\alpha = x$$

für jedes $x \in M$ erfüllt sind. Somit ist $\alpha \circ \beta = \beta \circ \alpha = \varepsilon$, also β die zu α inverse Transformation.
Damit ist der Satz bewiesen.

Mit Hilfe dieses Satzes ist das Problem, wann eine inverse Funktion existiert, leicht zu lösen. Eine Funktion g heißt Inverse oder Umkehrfunktion der Funktion f, wenn $(f \circ g)(x) = (g \circ f)(x) = x$ ist.
Für die Existenz der Inversen einer Funktion f ist notwendig und hinreichend, dass f eine bijektive Abbildung ihres Definitionsbereiches auf die Menge ihrer Werte darstellt.

Offenbar sind die Transformationen α und α^{-1} zueinander invers, d. h., jede von ihnen ist die Inverse der anderen. Folglich gilt $(\alpha^{-1})^{-1} = \alpha$.

Beispiele.
6. Es sei φ die Drehung der Ebene um den Winkel $2\pi/3$ entgegen dem Uhrzeigersinn um den Punkt 0. Da φ eine Bijektion ist, existiert φ^{-1}. Es ist leicht zu sehen, dass φ^{-1} die Drehung der Ebene um den Winkel $2\pi/3$ im Uhrzeigersinn um den Punkt 0 ist.

7. Die Funktionen $y = 2x + 3$, $y = x^3$ sind bijektive Transformationen

$$x \to 2x + 3, \qquad x \to x^3$$

der Menge $\mathbb{R}$ der reellen Zahlen auf sich. Daher existieren die zu ihnen inversen Transformationen, nämlich

$$x \to \frac{x-3}{2}, \qquad x \to \sqrt[3]{x} \text{ für } x \geq 0, \qquad x \to -\sqrt[3]{-x} \text{ für } x < 0$$

Folglich sind die Funktionen

$$y = \frac{x-3}{2} \qquad \text{und} \qquad y = \begin{cases} \sqrt[3]{x} & \text{für } x \geq 0 \\ -\sqrt[3]{-x} & \text{für } x < 0 \end{cases}$$

die Inversen zu den Funktionen $y = 2x + 3$ bzw. $y = x^3$.
Die Funktionen $y = x^2$, $y = \sin x$ sind Transformationen

$$x \to x^2 \qquad , \qquad x \to \sin x$$

der Menge $\mathbb{R}$, die nicht bijektiv sind. Daher existieren zu ihnen keine Inversen. Man kann jedoch die Einschränkung der Funktion $y = x^2$ auf die Menge $\mathbb{R}^+ \cup \{0\}$ der nichtnegativen reellen Zahlen betrachten. Dies ist eine Funktion, deren Definitionsbereich die Menge $\mathbb{R}^+ \cup \{0\}$ ist, wobei sie in allen Punkten des Definitionsbereiches mit der Funktion $y = x^2$ übereinstimmt.

Diese Einschränkung ist eine bijektive Transformation der Menge $\mathbb{R}^+ \cup \{0\}$, d. h., zu ihr existiert die inverse Transformation $x \to \sqrt{x}$. Somit ist die Funktion $y = \sqrt{x}$ invers zur Einschränkung der Funktion $y = x^2$ auf $\mathbb{R}^+ \cup \{0\}$ (und nicht, wie man oft sagt, zur Funktion $y = x^2$).

Völlig analog kann man die Einschränkung der Funktion $y = \sin x$ auf das Intervall $[-\pi/2, \pi/2]$ betrachten. Diese Einschränkung ist eine bijektive Abbildung der Menge $[-\pi/2, \pi/2]$ auf die Menge $[-1, 1]$.
Folglich existiert zu ihr die Inverse, und das ist die Funktion $y = \arcsin x$.

8. Die Transformation φ der Punkte der Ebene sei durch eine Parallelverschiebung in einer gegebenen Richtung um den Abstand d gegeben. Offenbar ist φ eine bijektive Transformation; daher existiert ihre Inverse. Diese ist ebenfalls eine Parallelverschiebung um denselben Abstand, aber in entgegengesetzter Richtung.

Zu einer Transformation einer endlichen Menge M existiert die inverse Transformation dann und nur dann, wenn sie eine Permutation ist.
Es sei die Permutation

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

gegeben; dann ist ihre Inverse, wie sich aus der Multiplikationsregel für Permutationen ergibt, die folgende Permutation:

$$\varphi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Deren Spalten kann man so umordnen, dass die Zahlen in der oberen Reihe wachsend angeordnet sind. Beispielsweise ist die Inverse der Permutation

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

die Permutation

$$\varphi^{-1} = \begin{pmatrix} 4 & 2 & 1 & 5 & 7 & 6 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 1 & 4 & 6 & 5 \end{pmatrix}$$

Für Transformationen einer beliebigen Menge kann man Gleichungen aufstellen und lösen. Als Beispiel betrachten wir Gleichungen ersten Grades. Es seien φ und ψ beliebige Transformationen einer Menge M. Existieren Transformationen x und y dieser Menge, für welche die Gleichungen

$$\varphi \circ x = \psi \qquad , \qquad y \circ \varphi = \psi \tag{5,6}$$

erfüllt sind? Wenn solche Transformationen existieren, sind sie dann eindeutig bestimmt? Wir betonen, dass man beide Gleichungen betrachten muss, da die Multiplikation von Transformationen nicht kommutativ ist, diese Gleichungen also verschiedene Lösungen haben können.

Es ist ziemlich leicht, die Frage nach Existenz und eindeutiger Bestimmtheit von Lösungen der Gleichungen (5) und (6) zu beantworten, in denen der "Koeffizient" φ eine Permutation ist. In diesem Fall existieren Lösungen für beide Gleichungen und sind eindeutig bestimmt.
Man beweist diese Tatsache folgendermaßen.

Weil φ eine Bijektion ist, existiert ihre inverse Transformation φ^{-1}. Daher kann man die Transformationen $\varphi^{-1} \circ \psi$ und $\psi \circ \varphi^{-1}$ betrachten (wir merken an, dass im allgemeinen $\varphi^{-1} \circ \psi \neq \psi \circ \varphi^{-1}$ gilt, da die Multiplikation von Transformationen nicht kommutativ ist).
Wir zeigen nun, dass $\varphi^{-1} \circ \psi$ Lösung der Gleichung (5) ist. Zu diesem Zweck berechnen wir das Produkt $\varphi \circ (\varphi^{-1} \circ \psi)$. Benutzen wir die Assoziativität der Multiplikation von Transformationen und die Definition der inversen Transformation, so erhalten wir

$$\varphi \circ (\varphi^{-1} \circ \psi) = (\varphi \circ \varphi^{-1}) \circ \psi = \varepsilon \circ \psi = \psi$$

Dies bedeutet aber, dass $\varphi^{-1} \circ \psi$ Lösung der Gleichung (5) ist. Analog zeigt man, dass die Transformation $\psi \circ \varphi^{-1}$ Lösung der Gleichung (6) ist.

Jetzt beweisen wir, dass die angegebenen Lösungen von (5) und (6) die einzigen sind. Sind nämlich die Transformationen α und β Lösungen der Gleichungen (5) bzw. (6), d. h., gilt

$$\varphi \circ \alpha = \psi \qquad \text{bzw.} \qquad \beta \circ \varphi = \psi \tag{7,8}$$

so erhalten wir, wenn wir die Gleichung (7) von links und die Gleichung (8) von rechts mit φ^{-1} multiplizieren,

$$\varphi^{-1} \circ (\varphi \circ \alpha) = \varphi^{-1} \circ \psi \qquad \text{bzw.} \qquad (\beta \circ \varphi) \circ \varphi^{-1} = \psi \circ \varphi^{-1}$$

d. h.

$$(\varphi^{-1} \circ \varphi) \circ \alpha) = \varphi^{-1} \circ \psi \qquad \text{bzw.} \qquad \beta \circ (\varphi) \circ \varphi^{-1}) = \psi \circ \varphi^{-1}$$

oder

$$\varepsilon \circ \alpha = \varphi^{-1} \circ \psi, \qquad \alpha = \varphi^{-1} \circ \psi$$
$$\beta \circ \varepsilon = \psi \circ \varphi^{-1}, \qquad \beta = \psi \circ \varphi^{-1}$$

Diese Identitäten besagen, dass die Gleichungen (5) und (6) außer den bereits erwähnten keine weiteren Lösungen besitzen.

Beispiel 9. Es sei $M = \{1, 2, 3, 4\}$,

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad , \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Dann ist leicht nachzuprüfen, dass die Permutation

$$\varphi^{-1} \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Lösung der Gleichung (5) und die Permutation

$$\psi \circ \varphi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \qquad (\neq \varphi^{-1} \circ \psi)$$

Lösung der Gleichung (6) ist.
Ist die Transformation φ in den Gleichungen (5) und (6) keine Permutation, so brauchen diese Gleichungen keine Lösung zu besitzen (vgl. Aufgabe 8 bis 11).

Aufgaben 1. Man zeige, dass das Produkt von Parallelverschiebungen wieder eine Parallelverschiebung ist.

2. Man stelle die nachstehend durch Tabellen gegebenen Transformationen mit Hilfe von Pfeildiagrammen dar und bilde das Produkt dieser Transformationen:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 2 & 4 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 1 & 2 \end{pmatrix}$

b) $\begin{pmatrix} a & b & c & d & e \\ a & b & a & b & c \end{pmatrix}$; $\begin{pmatrix} a & b & c & d & e \\ c & d & c & a & b \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 2 & 1 & 2 \end{pmatrix}$; $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 2 & 1 & 6 \end{pmatrix}$

3. Man zeige, dass das Produkt von Spiegelungen bezüglich sich schneidender Geraden eine Drehung ist.

4. Die Transformation φ und ψ seien durch graphische Darstellungen gegeben. Man gebe eine Regel zur Bestimmung der graphischen Darstellung von $\varphi \circ \psi$ an.

5. Man beweise: Ist das Produkt $\varphi \circ \psi$ der Transformationen φ und ψ einer endlichen Menge M eine Permutation, so sind auch φ und ψ Permutationen.

6. Man beweise: Existiert zu einer gegebenen Transformation φ eine Zahl n derart, dass

φ^n die identische Transformation ist, so ist φ eine Bijektion (zur Definition von φ^n vgl. Abschnitt 6).

7. Man löse die folgenden Gleichungen:

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

$$b) \quad x \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

8. Welche Lösungen besitzen die nachstehenden Gleichungen und wieviel Lösungen gibt es?

$$a) \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

$$b) \quad x \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 2 \end{pmatrix}$$

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

$$d) \quad x \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}$$

9. Es sei M eine beliebige Menge und $\varphi : M \to M$ eine Transformation von M. Unter einer Rechts- (bzw. Links-)inversen von φ versteht man eine Transformation α von M mit $\varphi \circ \alpha = \varepsilon$ (bzw. $\alpha \circ \varepsilon = \varepsilon$).
Man beweise, dass die Transformation φ dann und nur dann eine Rechts- (bzw. Links-)inverse besitzt, wenn ε injektiv (bzw. surjektiv) ist.

10. Ist φ eine Injektion (bzw. eine Surjektion), so besitzt die Gleichung (5) (bzw. (6)) für jede Transformation ψ eine Lösung (im allgemeinen aber nicht nur eine). Man beweise dies unter Benutzung von Aufgabe 9.

11. Es sei φ eine Surjektion (bzw. Injektion). Man beweise: Besitzt die Gleichung (5) (bzw. (6)) eine Lösung, so ist sie eindeutig bestimmt.

12. $2n$ Sportler stellen sich in eine Einerreihe auf. Durch Abzählen "1-2" bilden sie eine Zweier-Reihe. Diejenigen, die in der zweiten Reihe stehen, nehmen, an der linken Flanke beginnend, ein "Umgehungsmanöver" vor und wechseln so an den rechten Rand, dass die linke Flanke zur rechten wird (vgl. Abb. 8).

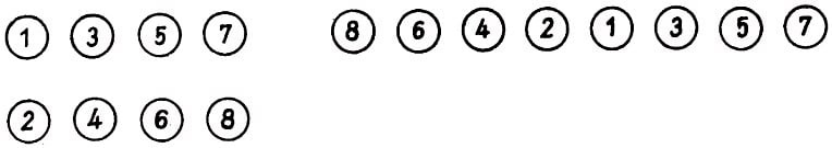


Abb. 8

Man bestimme die Permutation, welche die Aufstellung der Sportler in einer Reihe nach dreimaliger Umgruppierung charakterisiert, wenn man annimmt, dass die Nummern auf den Hemden der Sportler vor der Umgruppierung ihrem Platz in der Reihe entsprechen.

4 Gruppen von Permutationen und Halbgruppen von Transformationen

Wie bereits festgestellt wurde, besitzt die Multiplikation von Transformationen einer beliebigen Menge M eine Reihe von Eigenschaften, die nicht von der Natur der Elemente von M abhängen. Diese Eigenschaften können für verschiedene Mengen von Transformationen von M verschieden sein.
Beispielsweise existiert in der Menge aller Transformationen nicht zu jeder Transformation eine Inverse, während dies in der Menge aller bijektiven Transformationen der Fall ist. Die Multiplikation beliebiger Transformationen ist nicht kommutativ, während die Multiplikation (Hintereinanderausführung) von Parallelverschiebungen in der Ebene kommutativ ist. Man muss sehr oft die Eigenschaften einzelner Transformationsklassen in Bezug auf die Multiplikation studieren ; daher ist es zweckmäßig, für das Studium dieser Eigenschaften ein bestimmtes allgemeines Schema zu erarbeiten. .

Außer mit der Multiplikation von Transformationen hat man es auch mit anderen Operationen zu tun, die auf verschiedenartigen Mengen vorgegeben sind. Beispielsweise betrachtet man die Addition reeller Zahlen, die Multiplikation in der Menge der rationalen Zahlen, das Potenzieren in der Menge der ganzen Zahlen usw.

Dies legt den Gedanken nahe, den allgemeinen Begriff der Operation zu betrachten. Aus den angeführten Beispielen ist ersichtlich, dass eine auf irgendeiner Menge D gegebene Operation jedem Paar von Elementen aus D ein bestimmtes Element aus D zuordnet (das Ergebnis der Anwendung der Operation).
So ordnet beispielsweise die Addition ganzer Zahlen dem Paar $(2, 3)$ die Zahl 5 und dem Paar $(-2, 1)$ die Zahl -1 zu; die Multiplikation von Permutationen auf der Menge $\{1, 2, 3\}$ ordnet dem Paar

$$\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right)$$

die Permutation $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ zu usw.
Daher liegt folgende Definition nahe:

Eine Zuordnung, durch die jedem Paar von Elementen der Menge D ein bestimmtes Element ebendieser Menge zugeordnet wird, nennt man eine Operation auf D.
Operationen werden mit verschiedenen Symbolen gekennzeichnet, wie etwa $+$, $\times$, $\cdot$, $\circ$, $*$ usw. Wird eine Operation auf der Menge D mit dem Symbol $*$ bezeichnet und ordnet sie dem Paar (a, b) von Elementen aus D das Element c zu, so schreibt man kurz

$$a * b = c$$

Das Element c wird das Kompositum oder (öfter) das Produkt der Elemente a, b genannt, die Operation * nennt man in diesem Fall Multiplikation (dies ist dadurch gerechtfertigt, dass die Operation * sehr oft als Multiplikation von Permutationen aufgefasst wird).

Beispiele für Mengen mit Operationen sind die Menge der ganzen Zahlen mit ihrer Addition, die Menge der Parallelverschiebungen in der Ebene mit ihrer Hintereinanderausführung, die Menge der positiven reellen Zahlen mit der Operation des Potenzierens (dem Paar (a, b) positiver Zahlen wird die Zahl a^b zugeordnet), die Menge der Permutationen der ersten 100 natürlichen Zahlen mit der Multiplikation von Permutationen.

Man betrachtet Mengen mit Operationen, die bestimmte Eigenschaften besitzen. Aus dem im vorhergehenden Abschnitt Gesagten folgt, dass sich in natürlicher Weise zwei Gesamtheiten von Transformationen herausheben:
Die Menge aller Transformationen und die Menge der Permutationen. Wir schreiben nun die Eigenschaften der Operationen Multiplikation von beliebigen Transformationen einer Menge M und Multiplikation von Permutationen einer Menge M gesondert auf. Die Gesamtheit aller Transformationen der Menge M wollen wir mit $P(M)$ und die Gesamtheit aller Permutationen dieser Menge mit $S(M)$ bezeichnen.

A. Eigenschaften der Multiplikation von Transformationen aus $P(M)$

A_1. Das Produkt zweier Transformationen der Menge M ist wieder eine Transformation derselben Menge:
Gilt $\varphi, \psi \in P(M)$, so auch $\varphi \circ \psi \in P(M)$.

Oder anders ausgedrückt: Die Menge $P(M)$ ist bezüglich der Multiplikation von Transformationen abgeschlossen.

A_2. Die Multiplikation von Transformationen ist assoziativ, d. h., für alle $\varphi, \psi, \omega \in P(M)$ gilt die Beziehung

$$(\varphi \circ \psi) \circ \omega = \varphi \circ (\psi \circ \omega)$$

A_3. Es existiert eine einzige Transformation $\varepsilon \in P(M)$ mit der Eigenschaft, dass für jedes $\varphi \in P(M)$

$$\varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi$$

gilt.

B. Eigenschaften der Multiplikation von Permutationen aus $S(M)$.

B_1. Gilt $\varphi, \psi \in S(M)$, so auch $\varphi \circ \psi \in S(M)$.

B_2. Die Multiplikation von Permutationen ist assoziativ.

B_3. Es existiert eine einzige Permutation $\varepsilon \in S(M)$ derart, dass für jede Permutation $\varphi \in S(M)$

$$\varepsilon \circ \varphi = \varphi \circ \varepsilon = \varphi$$

gilt.

B_4. Zu jeder Permutation $\varphi \in S(M)$ existiert eine Permutation $\psi \in S(M)$ mit

$$\varphi \circ \psi = \psi \circ \varphi = \varepsilon$$

Jedes allgemeine Schema, nach dem Gesamtheiten von Transformationen mit der Operation Multiplikation studiert werden, muss die Liste der Eigenschaften unter A bzw.

unter B irgendwie berücksichtigen. Dies wird erreicht durch Einführung der grundlegenden Begriffe Gruppe und Halbgruppe.

Definition. Eine beliebige Menge D mit einer auf ihr erklärten Operation * wird Halbgruppe genannt, wenn folgendes gilt:

a) für alle $a, b \in D$ liegt das Produkt $a * b$ in D;

b) für je drei Elemente $a, b, c \in D$ gilt die Identität

$$(a * b) * c = a * (b * c) \tag{1}$$

d. h., die auf D gegebene Multiplikation ist assoziativ;

c) es existiert ein Element e aus D derart, dass für jedes $a \in D$

$$a * e = e * a = a$$

gilt; dieses Element e heißt neutrales Element für die Operation *.

Beispiele.
1. Die Menge $\mathbb{Z}$ aller ganzen Zahlen ist bezüglich der Operation Addition eine Halbgruppe.
Die Summe ganzer Zahlen ist nämlich eine ganze Zahl. Die Addition ganzer Zahlen ist assoziativ. Neutrales Element für die Addition ganzer Zahlen ist die Zahl 0; denn für jedes $a \in \mathbb{Z}$ gilt

$$a + 0 = 0 + a = a$$

2. Die Menge $\mathbb{Q}^+$ aller positiven rationalen Zahlen ist bezüglich der Operation Multiplikation eine Halbgruppe.
3. Die Menge $P(M)$ der Transformationen ist bezüglich der Hintereinanderausführung von Transformationen eine Halbgruppe.

Die Menge $\mathbb{R}^+$ der positiven reellen Zahlen mit der auf ihr erklärten Operation $a*b = a^b$ ist keine Halbgruppe, da diese Operation nicht assoziativ ist; denn nicht für alle Zahlen aus $\mathbb{R}^+$ besteht die Beziehung (1). So gilt beispielsweise

$$(2 * 3) * 2 \neq 2 * (3 * 2)$$

es ist nämlich $(2^3)^2 = 64$, aber $2^{3^2} = 512$.

Definition. Eine Menge D mit einer auf ihr erklärten Operation * wird eine Gruppe genannt, wenn die Forderungen a) bis c) der Definition einer Halbgruppe und außerdem die folgende Bedingung erfüllt sind:
d) zu jedem Element a aus D existiert ein Element b aus D derart, dass $a*b = b*a = e$ gilt.

Ebenso wie für Transformationen kann man beweisen, dass durch Bedingung d) das Element b eindeutig bestimmt ist; es heißt inverses Element von a und wird - analog - mit a^{-1} bezeichnet.

Beispiele.
4. Die Menge $\mathbb{Z}$ aller ganzen Zahlen ist bezüglich der Addition eine Gruppe.
In Beispiel 1 haben wir bereits geprüft, dass die Forderungen a) bis c) erfüllt sind. Außerdem existiert zu jeder Zahl a aus $\mathbb{Z}$ eine Zahl $b \in \mathbb{Z}$ (die zu a entgegengesetzte Zahl) mit $a+b = b+a = 0$. Daher ist auch die letzte Forderung der Gruppendefinition erfüllt.

5. Die Menge $\mathbb{R}^+$ der positiven reellen Zahlen ist bezüglich der Multiplikation eine Gruppe.
In der Tat ist das Produkt positiver Zahlen wieder eine positive Zahl; die Multiplikation von Zahlen ist assoziativ; neutrales Element ist die Zahl 1; zu jeder Zahl $a \in \mathbb{R}^+$ existiert die zu ihr inverse a^{-1}.

6. Die Menge aller Drehungen der Ebene um einen festen Punkt um beliebige Winkel ist bezüglich der Hintereinanderausführung von Drehungen eine Gruppe.
In der Tat ist das Produkt von Drehungen der Ebene um den Punkt O um die Winkel α bzw. β wieder eine Drehung um diesen Punkt um den Winkel $\alpha + \beta$ (oder um den Winkel $\alpha + \beta \pm 2\pi$); die Multiplikation von Drehungen ist assoziativ, weil sie der Multiplikation beliebiger Transformationen gleichkommt; neutrales Element ist die identische Transformation der Ebene, die man als Drehung um den Punkt O um den Winkel vom Bogenmaß 0 betrachten kann; Inverse zur Drehung um den Winkel α ist die Drehung um den Winkel $-\alpha$.

Die Gesamtheit $S(M)$ aller Permutationen auf der Menge $M = \{1, 2, 3, ..., n\}$ bildet bezüglich der Multiplikation von Permutationen eine Gruppe. Diese Gruppe wird die symmetrische Gruppe der Permutationen der Menge M genannt. Dass alle Forderungen der Gruppendefinition erfüllt sind, folgt aus den Eigenschaften B1 bis B4.

Jede Gruppe ist auch Halbgruppe; die Umkehrung gilt jedoch nicht. Beispielsweise ist die Menge der nichtnegativen ganzen Zahlen bezüglich der Addition eine Halbgruppe, aber keine Gruppe.

Addition und Multiplikation von Zahlen sind kommutativ, jedoch wird die Kommutativität in den Definitionen einer Gruppe und einer Halbgruppe nicht gefordert. Dies erklärt sich dadurch, dass die Multiplikation von Transformationen nicht kommutativ ist und historisch der Gruppenbegriff gerade auf der Grundlage des Studiums der Eigenschaften der Multiplikation von Permutationen endlicher Mengen entstand (der Begriff Halbgruppe entstand erheblich später).

Gruppen, bei denen die Gruppenoperation kommutativ ist, werden gesondert untersucht. Man nennt sie abelsche Gruppen (zu Ehren des norwegischen Mathematikers Niels Henrik Abel (1802 bis 1829), der die Bedeutung dieser Gruppen für die Theorie der Auflösbarkeit algebraischer Gleichungen in Radikalen erkannte).

Dass eine Menge mit einer gegebenen Operation alle Gruppeneigenschaften besitzt, ist oft gar nicht so leicht nachzuweisen.
Ist die Menge endlich, so kann man für die Überprüfung die sogenannte Multiplikationstabelle für Gruppen (auch Gruppentafel genannt) benutzen. Eine solche Tabelle

wird ähnlich wie eine Multiplikationstabelle für ganze Zahlen aufgestellt, und zwar folgendermaßen:
Es seien $g_1, g_2, ..., g_n$ alle Elemente einer Gruppe G. Wir schreiben sie in die erste Zeile und in die erste Spalte der vorbereiteten Tabelle.
Dann füllen wir die Felder der Tabelle aus, indem wir die Produkte der entsprechenden Elemente aus der ersten Spalte und der ersten Zeile (in dieser Reihenfolge) eintragen. Als Ergebnis erhalten wir die Tabelle

	g_1	g_2	...	g_n
g_1	$g_1 * g_1$	$g_1 * g_2$	...	$g_1 * g_n$
g_2	$g_2 * g_1$	$g_2 * g_2$	...	$g_2 * g_n$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
g_n	$g_n * g_1$	$g_n * g_2$	...	$g_n * g_n$

Beispiele.
7. Es sei G die Menge der Permutationen

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Durch unmittelbares Ausmultiplizieren überzeugt man sich leicht davon, dass die Multiplikationstabelle der Elemente aus G folgende Gestalt hat:

	α_1	α_2	α_3
α_1	α_1	α_2	α_3
α_2	α_2	α_3	α_1
α_3	α_3	α_1	α_2

8. Es sei H die Menge der Transformationen

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \end{pmatrix}, \qquad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}$$

Wenn man diese Transformationen miteinander multipliziert, erhält man die folgende Tabelle:

	ε	α	β	γ
ε	ε	α	β	γ
α	α	α	β	γ
β	β	α	β	γ
γ	γ	α	β	γ

Mit Hilfe der letzten beiden Tabellen überzeugt man sich leicht davon, dass die Mengen G und H bezüglich der Multiplikation von Transformationen eine Gruppe bzw. eine Halbgruppe bilden.
Wir überzeugen uns beispielsweise davon, dass G eine Gruppe ist. Da alle Felder der ersten Tabelle nur die Symbole $\alpha_1, \alpha_2, \alpha_3$ enthalten, ist die Menge G bezüglich der Multiplikation der gegebenen Permutationen abgeschlossen.

Dass die Multiplikation der Elemente aus G assoziativ ist, ergibt sich automatisch, weil dies für die Multiplikation beliebiger Transformationen zutrifft. Die Permutation α_1 ist das neutrale Element der Gruppe. Aus der Tabelle geht auch hervor, dass jedes der Elemente $\alpha_1, \alpha_2, \alpha_3$ ein inverses besitzt, nämlich $\alpha_1^{-1} = \alpha_1$, $\alpha_2^{-1} = \alpha_3$, $\alpha_3^{-1} = \alpha_2$.

Aufgaben

1. Bilden folgende Mengen mit den angegebenen Operationen Halbgruppen:
a) die Menge der positiven natürlichen Zahlen mit der Operation, die jedem Zahlenpaar seinen größten gemeinsamen Teiler zuordnet;
b) die Menge aller Polynome beliebigen von 0 verschiedenen Grades bezüglich der Superposition von Polynomen;
c) die Menge der ungeraden ganzen Zahlen bezüglich der Multiplikation?

2. Sind folgende Mengen bezüglich der auf ihnen gegebenen Operationen Gruppen?
a) Die Menge der reellen Zahlen bezüglich der Multiplikation;
b) das System der Funktionen $y = x$, $y = -x$, $y = 1/x$, $y = -1/x$, die auf der Menge der reellen Zahlen ohne die Zahl Null definiert sind, bezüglich der Superposition von Funktionen;
c) die Menge der Funktionen $y = x$, $y = -x$ bezüglich der Superposition von Funktionen;
d) die Mengen aus Aufgabe 1 bezüglich der entsprechenden Operationen?

3. Man zeige, dass in jeder Zeile und in jeder Spalte einer Multiplikationstabelle von Permutationsgruppen das Symbol jeder Permutation genau zweimal vorkommt.

4. Welche Eigenschaft der Multiplikationstabelle einer abelschen Gruppe besitzen die Multiplikationstabellen nichtabelscher Gruppen nicht?

5. Man stelle die Multiplikationstabelle auf für
a) die Gruppe $S(M)$ mit $M = \{1, 2, 3\}$;
b) die Gruppe aus Aufgabe 2b);
c) die Halbgruppe $P(M)$ für $M = \{1, 2\}$.

6. Wieviel verschiedene Multiplikationstabellen, welche Gruppentafeln sind, kann man für vierelementige Mengen von Permutationen aufstellen?

5 Graphen von Transformationen. Orbits. Zyklenschreibweise für Permutationen

Pfeildiagramme von Transformationen einer gegebenen Menge M, sogenannte Graphen, kann man anders aufbauen als entsprechende Diagramme für beliebige Abbildungen. Wir markieren dazu jedes Element von M durch einen Punkt der Ebene, und zwar so, dass verschiedenen Elementen verschiedene Punkte entsprechen. Die Punkte bezeichnen wir mit denselben Symbolen wie die entsprechenden Elemente von M.

Zwei Punkte verbinden wir dann und nur dann durch einen Pfeil in Richtung von a nach b, wenn für a und b die Bedingung $(a)\varphi = b$ gilt. So erhalten wir den Graphen der Transformation φ.
Offenbar bestimmt dieser Graph die Transformation eindeutig. Sieht man von der Gestalt der Pfeile und der Lage der Punkte in der Ebene ab, so entspricht auch jeder Transformation ein ganz bestimmter Graph.

Beispiele.
1. Es sei eine Transformation φ der Menge $M = \{1, 2, 3, 4, 5, 6\}$ durch die Tabelle

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 6 & 2 \end{pmatrix}$$

gegeben. Wir kennzeichnen jede Zahl von M durch einen Punkt der Ebene (z. B. so wie in Abb. 9). Da $(1)\varphi = 3$ ist, verbinden wir die Punkte 1 und 3 durch einen Pfeil in Richtung vom Punkt 1 zum Punkt 3. Analog konstruieren wir die Pfeile, die von den Punkten 2, 3, 4, 5, 6 ausgehen (vgl. Abb. 10). Dies ist dann gerade der Graph der Transformation φ.

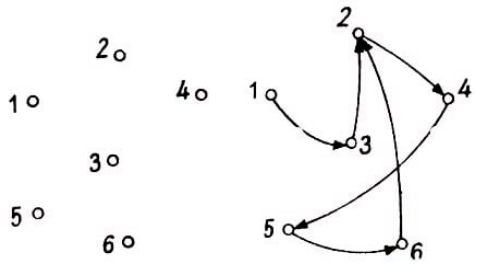


Abb. 9,10

2. Es sei $\varphi = \varepsilon$ die identische Transformation der Menge $M = \{1, 2, 3, ..., n\}$. Nach Definition gilt für jedes $a \in M$ die Beziehung $(a)\varepsilon = a$. Daher hat der Graph der Transformation ε die in Abb. 11 angegebene Gestalt.

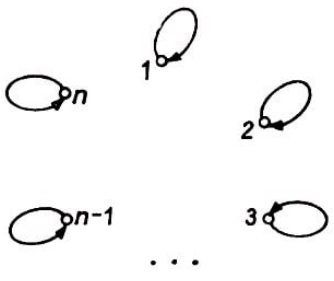


Abb. 11

3. Es sei $\varphi = \delta_a$ die konstante Transformation der Menge $M = \{1, 2, 3, ..., n\}$, welche jedem Element b aus M das feste Element a aus M zuordnet, d. h., für jedes $b \in M$ gilt

$$(b)\delta_a = a$$

In diesem Fall wird jeder Punkt b auf dem Graphen der Transformation φ durch einen Pfeil mit dem festen Punkt a verbunden, der in a endet (vgl. Abb. 12).

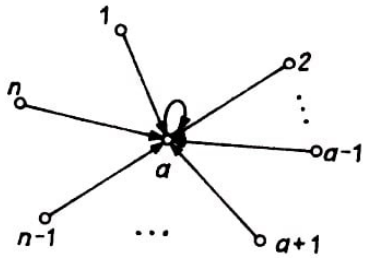


Abb. 12

4. Es sei $M = \mathbb{Z}$ und φ die Transformation der Menge $\mathbb{Z}$, die jeder ganzen Zahl x die Zahl $x + 3$ zuordnet: $(x)\varphi = x + 3$.
In diesem Fall gelingt es nicht, den Graphen der Transformation vollständig zu konstruieren; man kann aber einen bestimmten Teil so darstellen, dass die Struktur des Graphen insgesamt begreiflich wird (vgl. Abb. 13).

Abb. 13

5: Ist M eine endliche Menge und die Transformation φ eine Permutation von M, so geht von jedem Knotenpunkt des Graphen von φ genau ein Pfeil aus, und in jedem Knotenpunkt endet notwendigerweise ein und nur ein Pfeil.
Ist insbesondere $M = \{1, 2, 3, 4, 5, 6, 7\}$ und φ die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 3 & 6 & 5 & 7 \end{pmatrix}$$

von M, so hat ihr Graph die in Abb. 14 angegebene Gestalt.

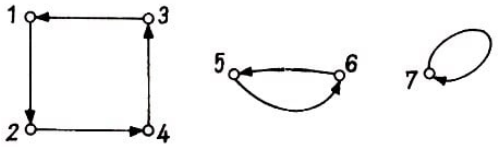


Abb. 14

Der Graph einer beliebigen Transformation 99 besteht aus einem einzigen Stück (vgl. Abb. 10, 12) oder aus mehreren nicht miteinander zusammenhängenden Teilen (vgl. Abb. 14), von denen jeder ein einziges Ganzes bildet. Dabei kann ein einzelner zusammenhängender Teil des Graphen von φ aus einem einzigen Punkt mit einer "Schleife" bestehen, d. h. aus einem Pfeil, der in diesem Punkt beginnt und wieder in ihm endet. Ist a ein solcher Punkt, so gilt für das entsprechende Element a der Menge M die Beziehung $(a)\varphi = a$. Derartige Elemente werden Fixpunkte der Transformation φ genannt. Erfüllt ein Element a aus M die Bedingung

$$(a)\varphi \neq a$$

so heißt a beweglicher Punkt der Transformation φ. Im Graphen sind die beweglichen Punkte die Punkte ohne Schleife.
Beispielsweise sind in Abb. 14 die Punkte 1, 2, 3, 4, 5, 6 bewegliche Punkte, 7 dagegen ist ein Fixpunkt von φ.

Die Anzahl der beweglichen Punkte einer Transformation ist eine ihrer wichtigen Charakteristiken, sie wird Grad dieser Transformation genannt. Die einzige Transformation vom Grad 0 ist die identische Transformation. Eine konstante Transformation einer n-elementigen Menge besitzt den Grad $n-1$.

Es sei φ eine Transformation der Menge M und a ein beliebiges Element von M. Die Folge

$$a_0 = a, (a)\varphi = a_1, (a_1)\varphi = a_2, ..., (a_n)\varphi = a_{n+1} \tag{1}$$

von Elementen aus M wird Orbit des Elementes a bezüglich der Transformation φ genannt. Die Menge

$$O(a, \varphi) = \{x_0, x_1, ..., x_n, ...\}$$

der Elemente des Orbits (1) ist stets eine Teilmenge von M. Insbesondere kann es vorkommen, dass $O(a, \varphi) = M$ gilt.

Wir untersuchen nun die Struktur eines Orbits etwas näher, wenn M eine endliche Menge, $O(a, \varphi) = M$ und $|M| = m$ ist.
Offenbar werden sich in diesem Fall Elemente der Folge (1) von einer gewissen Stelle an wiederholen. Es sei k die kleinste Zahl, für welche $(a_k)\varphi = a_l$ mit $l < k$ ist.

Natürlich kommen die Elemente $a_{k+1}, a_{k+2}, ...$ ebenfalls unter den Elementen $a_0, a_1, a_2, ..., a_k$ vor. Daher ist $k = m - 1$, und es ist leicht einzusehen, dass der Graph der Transformation φ die in Abb. 15 dargestellte Gestalt hat.

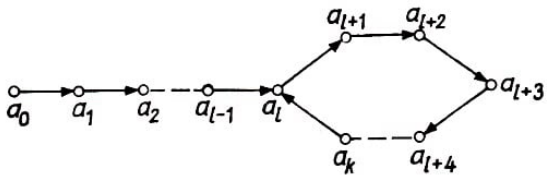


Abb. 15

Für $l \neq 0$ ist die Transformation φ keine Permutation, weil im Punkt a, zwei Pfeile enden. Für $l = 0$ besitzt die Transformation einen Graphen, der Zyklus genannt wird (vgl. Abb. 16), und in diesem Fall ist φ offensichtlich eine Permutation.

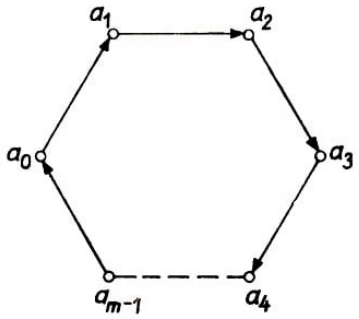


Abb. 16

Diese wirkt auf die Elemente von M folgendermaßen:

$$\varphi(a_0) = a_1, \varphi(a_1) = a_2, ..., \varphi(a_{m-2}) = a_{m-1}, \varphi(a_{m-1}) = a_0$$

Eine solche Permutation wird zyklisch oder einfach Zyklus genannt und mit

$$\varphi = (a_0, a_1, a_2, ..., a_{m-1})$$

bezeichnet. Die Zahl m ist die Länge des Zyklus. Zyklen der Länge 2 nennt man Transpositionen.

Wenn die Elemente des Orbits $O(a, \varphi)$ nicht die ganze Menge M ausschöpfen, charakterisieren die Graphen in den Abb. 15 und 16 die Transformation nicht vollständig. Dann muss man die Orbits der anderen Elemente betrachten, die nicht in $O(a, \varphi)$ liegen. Verschiedene Orbits bezüglich einer gegebenen Transformation können gemeinsame Knotenpunkte besitzen (vgl. Abb. 12), aber für eine Permutation beschreiben verschiedene Orbits nicht zusammenhängende Teile ihres Graphen.

In der Tat, es seien $O_1 = \{a_1, a_2, ..., a_m\}$ und $O_2 = \{b_1, b_2, ..., b_n\}$ verschiedene Orbits der Permutation φ. Wir nehmen an, O_1 und O_2 hätten gemeinsame Elemente. In der nach wachsenden Indizes geordneten Folge wählen wir das erste Element $a_k \in O_1$, das mit einem bestimmten Element b_l aus O_2 übereinstimmt.
Dann wäre $a_{k-1} \neq b_{l-1}$, aber $(a_{k-1})\varphi = a_k = b_l = (b_{l-1})\varphi$, also die Transformation φ keine Permutation. Wir erhalten einen Widerspruch, und damit ist unsere Behauptung bewiesen.

Nun kann man die Graphen von Permutationen auf einer endlichen Menge M genauer charakterisieren. In diesem Fall lässt sich die Menge M in einzelne Teilmengen ohne gemeinsame Elemente zerlegen. Auf jeder dieser Teilmengen bildet die Permutation φ einen Zyklus. Daher besteht der Graph jeder Permutation aus einer bestimmten Anzahl nicht miteinander zusammenhängender Zyklen.

Da der Graph einer Permutation in einzelne nicht miteinander zusammenhängende Zyklen zerfällt, ist es zweckmäßig, die Permutationen einer endlichen Menge so aufzuschreiben, dass man mit Hilfe dieser Schreibweise sofort die einzelnen Teile des Graphen - die Zyklen - konstruieren kann. Diese Schreibweise für Permutationen wird Zyklenschreibweise genannt. Ehe wir näher darauf eingehen, machen wir einige allgemeine Bemerkungen.

Es sei φ eine beliebige Permutation einer Menge M und P eine Teilmenge von M mit der Eigenschaft, dass für jedes Element $a \in P$ auch $(a)\varphi$ zu P gehört.
Vermöge der Permutation φ von M kann man eine Transformation ψ von P definieren, indem man für jedes $b \in P$

$$(b)\psi = (b)\varphi \quad ((b)\varphi \in P)$$

setzt. Offenbar ist ψ eine Permutation von P. Wir wollen sie die Einschränkung der Permutation φ auf die Teilmenge P der Menge M nennen.

Beispiel 6. Es sei $M = \{1, 2, 3, 4, 5, 6\}$, $P = \{1, 2, 3, 4\}$ und

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$$

Man sieht sofort, dass $(a)\varphi \in P$ für jedes $a \in P$ gilt; daher kann man die Einschränkung von φ auf P betrachten. Dies ist die Permutation

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Haben wir umgekehrt eine Permutation ψ der Menge $P \subset M$, so können wir eine Permutation φ von M definieren, indem wir für jedes Element a aus M

$$(a)\varphi = \begin{cases} (a)\psi & \text{für } a \in P \\ a & \text{für } a \notin P \end{cases}$$

setzen. Dann wirkt die Permutation φ auf die Elemente aus P ebenso wie die Permutation ψ, während alle übrigen Elemente von M ungeändert bleiben. Wir wollen φ eine Erweiterung von ψ auf die Menge M nennen.

Beispiel 7. Es sei $P = \{1, 2, 3, 4, 5\}$, $M = \{1, 2, 3, 4, 5, 6, 7, 8\}$ und

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Dann ist die Permutation $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 6 & 7 & 8 \end{pmatrix}$ eine Erweiterung von φ auf M.

Wir nennen zwei Permutationen einer Menge M elementefremd (oder disjunkt), wenn die Mengen ihrer beweglichen Punkte keine gemeinsamen Elemente besitzen.
Elementefremd sind z. B. die Permutationen

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 5 & 6 & 7 & 8 \end{pmatrix} \quad \text{und} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 7 & 6 & 8 \end{pmatrix}$$

denn die Mengen der beweglichen Punkte von φ bzw. ψ sind $\{1, 2, 3, 4\}$ bzw. $\{6, 7\}$.

Im Unterschied zu den Permutationen allgemeiner Form hängt das Produkt elementefremder Permutationen nicht von der Reihenfolge der Faktoren ab.

In der Tat, es seien φ und ψ elementefremde Permutationen, und a sei ein beliebiges Element von M. Ist a ein beweglicher Punkt der Permutation φ, so setzen wir $(a)\varphi = b$; die Elemente a und b sind Fixpunkte von ψ, da $(a)\varphi \neq a$ und $(b)\varphi \neq b$ gilt. Daher erhalten wir

$$(a)(\varphi \circ \psi) = ((a)\varphi)\psi = (b)\psi = b, \quad (a)(\psi \circ \varphi) = ((a)\psi)\varphi = (a)\varphi = b$$

d. h., in diesem Fall ist $(a)(\varphi \circ \psi) = (a)(\psi \circ \varphi)$.

Ist a ein Fixpunkt der Permutation φ, so setzen wir $(a)\psi = c$ $(= a$, falls a auch Fixpunkt von ψ ist), und analog erhalten wir, dass sich die Elemente a und c bei der Permutation φ nicht ändern. Daher ist

$$(a)(\varphi \circ \psi) = ((a)\varphi)\psi = (a)\psi = c, \quad (a)(\psi \circ \varphi) \qquad = ((a)\psi)\varphi = (c)\varphi = c$$

d. h., auch in diesem Fall wirken die Permutationen $\varphi \circ \psi$ und $\psi \circ \varphi$ auf das Element a von M in gleicher Weise; dies bedeutet aber $\varphi \circ \psi = \psi \circ \varphi$.

Die Tabelle für das Produkt zweier elementefremder Permutationen φ und ψ ist sehr einfach aufzustellen. Zu diesem Zweck muss man in der zweiten Reihe der Tabelle für $\varphi \circ \psi$ alle beweglichen Punkte der Permutationen φ bzw. ψ an ihrer Stelle belassen (d. h. an den Stellen, an denen sie in den Tabellen für φ bzw. ψ stehen), die übrigen Stellen sind mit den (gemeinsamen) Fixpunkten zu besetzen.

Beispiel.

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

Nun sei φ eine beliebige Permutation einer Menge M. Wir zerlegen M in die verschiedensten Teilmengen $M_1, M_2, ..., M_s$, von denen jede Orbit eines gewissen Elementes von M ist.
Diese Zerlegung hat folgende Eigenschaften:

a) Jedes Element von M gehört zu einer der Teilmengen M_i $(i = 1, 2, ..., s)$;
b) ist $i \neq j$, so haben M_i und M_j keine Elemente gemeinsam;
c) für jedes $a \in M_i$ (i ist dabei einer der Indizes 1, 2, ..., 8) gehört auch das Element $(a)\varphi$ zu M_i.

Nach der letzten Eigenschaft kann man die Einschränkungen φ_i der Permutation φ auf jede der Teilmengen M_i betrachten. Sie sind durch die Permutation φ eindeutig bestimmt.

Jedes φ_i kann man seinerseits auf die gesamte Menge M erweitern. Wir bezeichnen diese Erweiterung mit $\overline{\varphi_i}$ $(i = 1, 2, ..., 8)$. Im folgenden werden wir solche Permutationen ebenfalls zyklisch nennen und sie wie gewöhnliche Zyklen bezeichnen. Folglich ist eine Permutation in diesem Sinne genau dann zyklisch, wenn sie einen Graphen besitzt, wie er in Abb. 17 dargestellt ist.

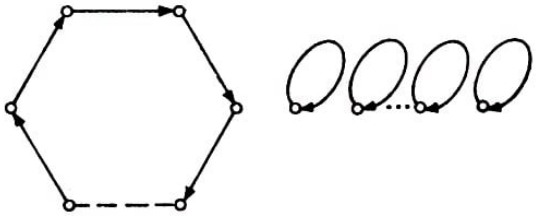


Abb. 17

Offenbar stimmt die Menge der beweglichen Punkte jede der Permutationen $\overline{\varphi_i}$ mit der Menge M_i überein; nach Eigenschaft b) sind die Permutationen $\overline{\varphi_i}$ und $\overline{\varphi_j}$ für $i \neq j$ elementefremd.

Wenn wir die weiter oben angegebene Regel für die Multiplikation elementefremder Permutationen anwenden, erhalten wir

$$\varphi = \overline{\varphi}_1 \circ \overline{\varphi}_2 \circ ... \circ \overline{\varphi}_s$$

Da die Permutationen $\overline{\varphi}_1, \overline{\varphi}_2, ..., \overline{\varphi}_s$ paarweise elementefremd sind, hängt dieses Produkt nicht von der Reihenfolge der Faktoren ab. Somit haben wir folgenden Satz bewiesen:

Satz. Jede Permutation einer endlichen Menge M kann in ein Produkt elementefremder Zyklen zerlegt werden, wobei diese Zerlegung bis auf die Reihenfolge der Faktoren eindeutig ist.

Das System der Zahlen $k_1, k_2, ..., k_s$, welche die Längen der Zyklen angeben, in welche die gegebene Permutation zerlegt wurde, heißt ihr Typ und wird mit $\langle k_1, k_2, ..., k_s \rangle$ bezeichnet.

Beispiel 8. Man zerlege die Permutation

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

in ein Produkt von Zyklen.
Wir ermitteln die verschiedenen Orbits für φ. Es ist

$$\varphi(1) = 2, \varphi(2) = 3, \varphi(3) = 1, \varphi(4) = 6, \varphi(5) = 4, \varphi(6) = 7, \varphi(7) = 5, \varphi(8) = 8$$

Demnach bestimmen die Orbits die Teilmengen $\{1, 2, 3\}$, $\{4, 6\}$, $\{5, 7\}$, $\{8\}$. Als Einschränkungen der Permutation φ auf diese Mengen ergeben sich die Permutationen

$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix}, \quad \varphi_3 = \begin{pmatrix} 5 & 7 \\ 7 & 5 \end{pmatrix}, \quad \varphi_4 = \begin{pmatrix} 8 \\ 8 \end{pmatrix}$$

Erweiterungen dieser Permutationen auf die Menge M sind die Permutationen

$$\overline{\varphi}_1 = (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}, \quad \overline{\varphi}_2 = (4, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 6 & 5 & 4 & 7 & 8 \end{pmatrix}$$

$$\overline{\varphi}_3 = (5, 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 6 & 8 \end{pmatrix}, \quad \overline{\varphi}_4 = (8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \varepsilon$$

Daher gilt

$$\varphi = \overline{\varphi}_1 \circ \overline{\varphi}_2 \circ \overline{\varphi}_3 \circ \overline{\varphi}_4 = (1, 2, 3) \circ (4, 6) \circ (5, 7) \circ (8) = (1, 2, 3) \circ (4, 6) \circ (5, 7)$$

Die letzte Schreibweise bestimmt die Permutation nur dann eindeutig, wenn bekannt ist, auf welcher Menge sie wirkt.

Aufgaben
1. Kann jeder Graph der Graph einer Transformation sein?

2. Eine Permutation sei durch einen Graphen gegeben. Wie ist der Graph der inversen Permutation zu konstruieren?

3. Man gebe eine Regel zur Bestimmung des Graphen für das Produkt von Transformationen an, von denen jede durch ihren Graphen gegeben ist, ohne dass man die Tabellen dieser Transformationen konstruiert.

4. Man konstruiere die Graphen der durch folgende Tabellen gegebenen Transformationen:

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 8 & 3 & 7 & 2 & 4 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 5 & 4 & 3 & 7 & 1 & 3 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 3 & 7 & 5 & 1 & 2 \end{pmatrix}$ d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 8 & 4 & 3 & 4 & 9 & 9 \end{pmatrix}$

5. Man beweise: Jede Permutation, deren Graph zusammenhängend ist, ist zyklisch.

6. Unter der Länge eines Orbits versteht man die Anzahl seiner Elemente. Für die Transformationen einer n-elementigen Menge bestimme man den größten und den kleinsten Wert der Summen der Längen ihrer verschiedenen Orbits.

7. Man beweise: Eine Transformation φ einer Menge M ist dann und nur dann eine Permutation, wenn die Summe der Längen ihrer verschiedenen Orbits gleich $|M|$ ist.

8. Man beweise: Ist φ eine beliebige Transformation der Menge M, so existieren eine Menge $P \subseteq M$ und eine natürliche Zahl k derart, dass $(a)\varphi^k \in P$ für jedes $a \in P$ gilt und die Einschränkung von φ^k auf P eine Permutation ist.

9. Man zerlege folgende Permutationen in ein Produkt elementefremder Zyklen und bestimme die Typen dieser Permutationen:

$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 3 & 2 \end{pmatrix},$$
$$\varphi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 3 & 1 & 5 & 8 & 4 & 2 & 6 \end{pmatrix}$$

10. Man beschreibe die allgemeine Form des Graphen einer beliebigen Transformation (so wie wir es für Permutationen getan haben).

11. Wieviel Permutationen vom vorgegebenen Typ $\langle n_1, n_2, ..., n_k \rangle$ mit $n_1 < n_2 < ...n_k$ existieren auf einer m-elementigen Menge (wobei natürlich $n_1 + n_2 + ... + n_k = m$ ist)?

12. In der Gruppe $S_4 = S(\{1, 2, 3, 4\})$ bestimme man die Anzahl der Permutationen jedes möglichen Typs.

13. Man bestimme den Typ derjenigen Permutation, welche die Aufstellung von 30 Sportlern (vgl. Aufgabe 12 von Abschnitt 3) nach zweimaliger Umgruppierung charakterisiert.

6 Ordnung einer Permutation

Für jede Transformation φ kann man ihre Potenzen betrachten, wobei unter der n-ten Potenz einer Transformation φ das Produkt

$$\underbrace{\varphi \circ \varphi \circ \varphi \circ ... \circ \varphi}_{n}$$

verstanden wird ($n > 0$ eine natürliche Zahl). Im folgenden werden wir sie mit φ^n bezeichnen.
Aus der Definition der Potenz einer Transformation folgen die Gleichungen

a) $\varphi^n \circ \varphi^m = \varphi^{n+m}$, b) $(\varphi^n)^m = \varphi^{nm}$

Wir erweitern die Definition und setzen $\varphi^0 = \varepsilon$.
Für Permutationen (beliebige Bijektionen) kann man den Begriff der Potenz auch auf den Fall ganzer negativer Zahlen verallgemeinern, indem man

$$\varphi^{-n} = \underbrace{\varphi^{-1} \circ \varphi^{-1} \circ \varphi^{-1} \circ ... \circ \varphi^{-1}}_{n} = (\varphi^{-1})^n = (\varphi^n)^{-1}$$

setzt. Die Gleichungen a) und b) gelten dann für beliebige ganze Exponenten.

Ist φ eine Permutation auf der Menge M und $|M| < \infty$, so ist φ^n für jedes ganze n ebenfalls eine Permutation auf M. Es gibt nur endlich viele solche Permutationen, d. h., in der Folge $\varphi^1, \varphi^2, \varphi^3, ...$, können nicht alle Permutationen voneinander verschieden sein.

Für bestimmte natürliche Zahlen k und l ($k < l$) gelte die Gleichung $\varphi^k = \varphi^l$. Dann ist

$$(\varphi^k)^{-1} = \varphi^{-k}, \qquad (\varphi^k)^{-1} \circ \varphi^k = (\varphi^k)^{-1} \circ \varphi^l$$

und hieraus folgt $\varphi^{l-k} = \varepsilon$. Zu jeder Permutation ε einer endlichen Menge M gibt es also mindestens eine natürliche Zahl s, für welche $\varphi^s = \varepsilon$ ist. Die kleinste dieser natürlichen Zahlen wird die Ordnung der Permutation ε genannt und mit Ord φ bezeichnet.

Die Potenz einer zyklischen Permutation $(a_1, a_2, ..., a_n)$ ergibt sich aus der Formel

$$\begin{pmatrix} a_1 & a_2 & ... & a_{n-1} & a_n \\ a_2 & a_3 & ... & a_n & a_1 \end{pmatrix}^k = \begin{pmatrix} a_1 & a_2 & ... & a_{n-1} & a_n \\ a_{k+1} & a_{k+2} & ... & k-1 & a_k \end{pmatrix}$$

Diese Gleichung kann man wie folgt interpretieren: Wenn sich ein Zahnrad mit n Zähnen um einen Mittelpunkt dreht, kann man seine Drehungen eindeutig durch Permutationen auf der Menge $\{1, 2, ..., n\}$ beschreiben, wenn man die Zähne mit den Zahlen $1, 2, ..., n$ nummeriert und eine Anfangsstellung der Zähne fixiert. Die zyklische Permutation

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ 2 & 3 & ... & n & 1 \end{pmatrix}$$

beschreibt offenbar die Drehung um den Winkel $2\pi/n$ (der Zahn mit der Nummer 1 wird an die Stelle des Zahnes mit der Nummer 2 gerückt usw.).

Ohne Beschränkung der Allgemeinheit wollen wir annehmen, das Zahnrad drehe sich im Uhrzeigersinn. Damit es sich um den Winkel $2\pi k/n$ dreht, muss man die Drehung um den Winkel $2\pi/n$ in derselben Richtung k-mal ausführen, so dass die Permutation α^k, $k > 0$, derjenigen Stellung des Zahnrades entspricht, bei der an der Stelle des ersten Zahnes der $(k+1)$-te steht, an der Stelle des zweiten der $(k+2)$-te usw. Dreht sich das Zahnrad n-mal um den Winkel $2\pi/n$ um seinen Mittelpunkt, so nimmt es wieder die Ausgangsstellung ein. Somit gilt für jeden Zyklus $(a_1, a_2, ..., a_n)$ die Gleichung

$$(a_1, a_2, ..., a_n)^n = \varepsilon$$

Für natürliche Zahlen, die kleiner als n sind, kann diese Gleichung nicht erfüllt sein. Für $k < 0$ beschreiben die Permutationen α^k Zahnradbewegungen um den Winkel $2\pi k/n$ entgegen dem Uhrzeigersinn.

Wie im vorhergehenden Abschnitt bewiesen wurde, kann man jede Permutation in ein Produkt paarweise elementefremder Zyklen zerlegen:

$$\varphi = \varphi_1 \circ \varphi_2 \circ ... \circ \varphi_s$$

Für keine zwei der Indizes i, j hängt das Produkt der Permutationen φ_i, φ_j von der Reihenfolge der Faktoren ab. Benutzt man diese Tatsache, so kann man die i-te Potenz der Permutation φ für jedes ganze n folgendermaßen beschreiben:

$$\begin{aligned}\varphi^n &= \underbrace{(\varphi_1 \circ \varphi_2 \circ ... \circ \varphi_s) \circ ... \circ (\varphi_1 \circ \varphi_2 \circ ... \circ \varphi_s)}_{n} \\ &= \underbrace{(\varphi_1 \circ \varphi_1 \circ ... \circ \varphi_1)}_{n} \circ \underbrace{(\varphi_2 \circ \varphi_2 \circ ... \circ \varphi_2)}_{n} \circ ... \circ \underbrace{(\varphi_s \circ \varphi_s \circ ... \circ \varphi_s)}_{n} \\ &= \varphi_1^n \circ \varphi_2^n \circ ... \circ \varphi_s^n \end{aligned} \tag{1}$$

Diese Gleichung lässt ebenfalls eine mechanische Interpretation zu:
Da die Zyklen $\varphi_1, \varphi_2, ..., \varphi_s$ paarweise elementefremd sind, beschreiben ihre Potenzen Drehbewegungen um die Mittelpunkte von s Zahnrädern mit jeweils entsprechender Anzahl von Zähnen, wobei die Zahnräder nicht miteinander zusammenhängen. Somit beschreiben die Potenzen der Permutation φ Drehungen des ganzen Systems der Zahnräder. Die Zähne aller Zahnräder kann man so nummerieren, dass sämtliche Bewegungen in einer Richtung ausgeführt werden.

Die Ordnung ist ein sehr wichtiges Charakteristikum einer Permutation. Zu jeder Permutation φ existieren viele Zahlen n. mit $\varphi^n = \varepsilon$, aber alle diese Zahlen sind durch die Ordnung der Permutation teilbar.

Wir beweisen dies indirekt, nehmen also an, es existiere eine natürliche Zahl k derart, dass die Gleichung $\varphi^k = \varepsilon$ gilt, ohne dass k durch die Ordnung r von φ teilbar ist. Nach Definition der Ordnung einer Permutation gilt $k > r$, daher ist $k = lr + s$, $0 < s < r$. Daraus folgt

$$\varphi^k = \varphi^{lr+s} = \varphi^{lr} \circ \varphi^s$$

wegen $\varphi^{lr} = (\varphi^r)^l = \varepsilon^l = \varepsilon$ also

$$\varepsilon = \varphi^k = \varphi^s$$

im Widerspruch zu $0 < s < r$. Damit ist die Behauptung bewiesen.

Wir leiten jetzt eine Regel zur Bestimmung der Ordnung einer beliebigen Permutation her. Zunächst merken wir an, dass das Produkt mehrerer elementefremder Permutationen nur dann gleich der identischen Permutation sein kann, wenn jede dieser Permutationen die identische Permutation ist. Dies folgt daraus, dass das Produkt φ der elementefremden Permutationen $\varphi_1, \varphi_2, ..., \varphi_s$ auf jeden seiner beweglichen Punkte ebenso wirkt wie auf ihn diejenige Permutation φ_i, für welche dieser Punkt beweglicher Punkt ist. Daher ergibt sich aus Gleichung (1), dass $\varphi^n = \varepsilon$ dann und nur dann gilt, wenn gleichzeitig die Beziehungen

$$\varphi_1^n = \varepsilon, \varphi_2^n = \varepsilon, ..., \varphi_s^n = \varepsilon \tag{2}$$

bestehen.
Sind die Permutationen $\varphi_1, \varphi_2, ..., \varphi_s$ Zyklen der Länge $k_1, k_2, ..., k_s$, d. h., besitzen sie die Ordnungen $k_1, k_2, ..., k_s$, so ist die kleinste Zahl n, für welche gleichzeitig alle Gleichungen (2) erfüllt sind, das kleinste gemeinsame Vielfache der Zahlen $k_1, k_2, ..., k_s$. Somit haben wir bewiesen, dass die Ordnung einer Permutation φ, die in ein Produkt von Zyklen der Längen $k_1, k_2, ..., k_s$ zerlegbar ist, gleich dem kleinsten gemeinsamen Vielfachen der Zahlen $k_1, k_2, ..., k_s$ ist:

$$\mathrm{Ord}\varphi = \mathrm{kgV}(\mathrm{Ord}\varphi_1, \mathrm{Ord}\varphi_2, ..., \mathrm{Ord}\varphi_s)$$

Beispiel. Es sei

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

Wir zerlegen φ in ein Produkt von Zyklen:

$$\varphi = (1, 3, 4) \circ (2, 6, 7) \circ (5, 8)$$

Daher ist Ord $\varphi = \mathrm{kgV}(3, 3, 2) = 6$.

Aufgaben
1. Man bestimme die Ordnung jeder der Permutationen
a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 9 & 6 & 8 & 1 & 2 & 4 \end{pmatrix}$; b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 7 & 8 & 9 & 2 & 1 & 10 \end{pmatrix}$.

2. Man bestimme die Ordnungen aller Permutationen auf einer 6elementigen Menge.

3. Welche höchste Ordnung können die Permutationen auf einer 10elementigen Menge besitzen?

4. Man bestimme die zum Zyklus $(a_1, a_2, ..., a_n)$ inverse Permutation.

5. Hängt das Produkt der Permutationen φ und ψ nicht von der Reihenfolge dieser Faktoren ab, so ist die Ordnung von $\varphi \circ \psi$ Teiler des kleinsten gemeinsamen Vielfachen der Ordnungen von φ und ψ. Im allgemeinen Fall kann man nicht behaupten, es sei Ord $(\varphi \circ \psi) =$ kgV (Ord φ, Ord ψ). Man gebe Beispiele dafür an.

6. Wieviel Permutationen der Ordnung 15 existieren auf einer 8elementigen Menge?

7. Man leite eine Formel zur Bestimmung der Ordnung einer Permutation her, indem man die mechanische Interpretation des Potenzierens benutzt.

8. Man beweise: Ist n eine Primzahl, dann ist die Permutation $(a_1, a_2, ..., a_n)$ für jedes k, $0 < k < n$, ein Zyklus der Länge n. Ist n eine zusammengesetzte Zahl, so ist diese Permutation für die Zahlen k, die zu n teilerfremd sind, ein Zyklus, und für alle anderen k ein Produkt von Zyklen ein und derselben Länge.

9. Man zeige: Für jede Permutation φ, die in ein Produkt von l elementefremden Zyklen der gleichen Länge s zerlegbar ist, lassen sich ein Zyklus ψ der Länge ls und eine natürliche Zahl k bestimmen derart, dass $\varphi = \psi^k$ gilt. Ist dieser Zyklus eindeutig bestimmt?

10. Zwölf Kinder werfen verschiedenfarbige Bälle hin und her, jedes Kind wirft seinen Ball immer ein und demselben Partner zu, alle Bälle werden gleichzeitig geworfen, und niemals werfen zwei Kinder den Ball zu ein und demselben Spieler. Nach welcher kleinsten Anzahl von Würfen befinden sich alle Bälle in den Händen derselben Kinder wie am Anfang?

11. Ein Spiel aus 36 Karten wird folgendermaßen gemischt: Das Spiel wird mit der Bildseite nach unten in die linke Hand genommen; dann werden die Karten einzeln von oben in die rechte Hand gelegt, wobei sie dort abwechselnd auf bzw. unter diejenigen Karten gelegt werden, die sich in diesem Augenblick schon in der rechten Hand befinden. Wie oft muss man diese Permutation durchführen, damit im Spiel die anfängliche Reihenfolge wiederhergestellt wird?

12. Welche kleinste Anzahl von Umgruppierungen für 30 Sportler (vgl. Aufgabe 12 von Abschnitt 3) muss durchgeführt werden, damit in der Reihe die anfängliche Reihenfolge wieder hergestellt wird? Welche Antwort erhält man in dem Fall, dass es sich um 36 Sportler handelt?

7 Erzeugende der symmetrischen Gruppe

Aufgabe. An den Wänden eines runden Saales einer Gemäldegalerie hingen Bilder. Einmal wurde beschlossen, sie in anderer Anordnung aufzuhängen. Beim Umhängen sollten aber nur die Plätze nebeneinander hängender Bilder vertauscht werden. Kann man mit Hilfe solcher Vertauschungen die Bilder immer so umverteilen, wie man es sich gedacht hatte?

Lösung. Wir nummerieren die Bilder in der ursprünglichen Anordnung mit Hilfe der Zahlen $1, 2, ..., n$, An dem Platz des ersten Bildes soll das Bild mit der Nummer i_1 aufgehängt werden, an dem Platz des zweiten Bildes das Bild mit der Nummer i_2 usw., schließlich an dem Platz des n-ten Bildes das Bild mit der Nummer i_n ($i_1, i_2, ..., i_n$ sind verschiedene Zahlen aus der Menge $\{1, 2, ..., n\}$).
Indem man ein Bild längs der Wand auf die bezeichnete Weise in ein und derselben Richtung vertauscht, nimmt es nacheinander alle Plätze ein, an denen Bilder hängen. Daher kann man das Bild mit der Nummer 131 an den Platz des ersten Bildes hängen (vgl. Abb. 18).

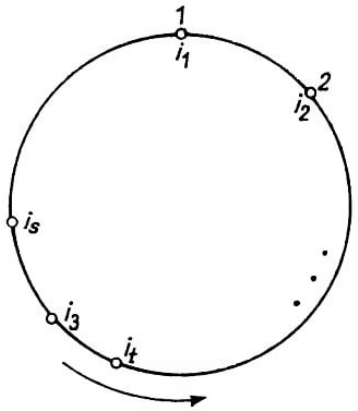


Abb. 18

Wählt man die Vertauschungsrichtung des Bildes mit der Nummer i_2 so, dass das Bild mit der Nummer i_1 nicht bewegt wird, so kann man das Bild i_2 an den Platz des zweiten Bildes hängen. Analog kann man das Bild i_3 an den Platz des dritten Bildes hängen, wenn man die Vertauschungsrichtung so wählt, dass die Bilder $_1$ und i_2 nicht bewegt werden. Führt man diesen Prozess weiter, so kann man jedes Bild an den gewünschten Platz hängen. Folglich ist die in der Aufgabe gestellte Frage mit "ja" zu beantworten.

Wir formulieren diese Aufgabe jetzt in der Sprache der Permutationen. Dazu nummerieren wir die Plätze, an denen Bilder hängen, so, dass die Bezeichnung der Plätze mit der Nummerierung der Bilder in der ursprünglichen Anordnung übereinstimmt. Die Anordnung der Bilder, bei der das Bild mit der Nummer i_1 auf dem ersten Platz, das Bild mit der Nummer i_2 auf dem zweiten Platz usw., das Bild mit der Nummer i_n auf dem n-ten Platz hängt, wird eindeutig durch die Permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i_1 & i_2 & i_3 & ... & i_n \end{pmatrix} \tag{1}$$

beschrieben; insbesondere wird die ursprüngliche Anordnung der Bilder durch die identische Permutation charakterisiert.

Ändern sich in der Anordnung, welche die Permutation (1) beschreibt, die Plätze der Bilder, die sich auf dem k-ten und dem $(k+1)$-ten Platz befinden $(1 \leq k \leq n)$, so entsteht die Permutation α_1, die diese neue Anordnung charakterisiert, durch Multiplikation der Permutation α mit der Transposition $(k, k+1)$ von links:

$$\begin{pmatrix} 1 & 2 & ... & k-1 & k & k+1 & k+2 & ... & n \\ i_1 & i_2 & ... & i_{k-1} & i_{k+1} & i_k & i_{k+2} & ... & i_n \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & ... & k-1 & k & k+1 & k+2 & ... & n \\ 1 & 2 & ... & k-1 & k+1 & k & k+2 & ... & n \end{pmatrix}$$
$$\circ \begin{pmatrix} 1 & 2 & ... & k-1 & k & k+1 & k+2 & ... & n \\ i_1 & i_2 & ... & i_{k-1} & i_k & i_{k+1} & i_{k+2} & ... & i_n \end{pmatrix}$$

Wenn der Übergang von der ursprünglichen zur gewünschten Anordnung, dem die Permutation φ entspricht, in s Schritten realisiert wird, gilt

$$\delta_s \circ ... \circ \delta_1 \circ \delta_1 \circ \varepsilon = \varphi$$

wobei $\delta_1, \delta_2, ..., \delta_s$ gewisse Transpositionen sind. Folglich kann man die Aufgabenstellung so formulieren:
Lässt sich jede Permutation in ein Produkt von Transpositionen zerlegen?

Es ist interessant, analoge Probleme nicht nur für Transpositionen, sondern auch für beliebige Mengen von Permutationen zu lösen.

Definition. Eine Teilmenge T der Menge aller Permutationen heißt Erzeugendensystem der gegebenen symmetrischen Gruppe S, wenn sich jede Permutation aus S in ein Produkt von Permutationen aus T zerlegen lässt.

In Abschnitt 5 wurde bewiesen, dass die Gesamtheit aller möglichen Zyklen ein Erzeugendensystem ist. Jeder Zyklus $(a_1, a_2, ..., a_s)$ kann in ein Produkt von Transpositionen zerlegt werden:

$$(a_1, a_2, ..., a_s) = (a_1, a_2) \circ (a_1, a_3) \circ ... \circ (a_1, a_s)$$

(Der Leser verifiziere dies!) Unter Benutzung dieser Tatsache kann man jede Permutation, indem man sie zuerst in ein Produkt von Zyklen zerlegt, als Produkt von Transpositionen darstellen.

Beispiel 1. Man zerlege die Permutation

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

in ein Produkt von Transpositionen.
Wir zerlegen φ in ein Produkt von Zyklen:

$$\varphi = (1, 8, 4) \circ (2, 7, 3) \circ (5, 6)$$

Weiter ist

$$(1, 8, 4) = (1, 8) \circ (1, 4) \qquad , \qquad (2, 7, 3) = (2, 7) \circ (2, 3)$$

Somit ist $\varphi = (1,8) \circ (1,4) \circ (2,7) \circ (2,3) \circ (5,6)$.
Aus diesem Beispiel ersieht man, dass bei der Zerlegung von Permutationen in ein Produkt von Transpositionen die Reihenfolge der Faktoren wesentlich ist.

Im weiteren werden wir die symmetrische Gruppe der Permutationen der Menge $M = \{1, 2, ..., n\}$ mit S_n bezeichnen.
In dieser Gruppe werden wir Erzeugendensysteme herausheben, die nur aus Transpositionen einer bestimmten Form bestehen. Beispielsweise sind die Folgen der Transpositionen

$$\begin{array}{ll} I & (1,2), (2,3), (3,4), ..., (n-1,n) \\ II & (1,2), (1,3), (1,4), ..., (1,n) \end{array}$$

wie man sich leicht überzeugt, Erzeugendensysteme für S_n. Man kann nämlich die Permutation (i,j) in ein Produkt von Transpositionen des Systems II folgendermaßen zerlegen:

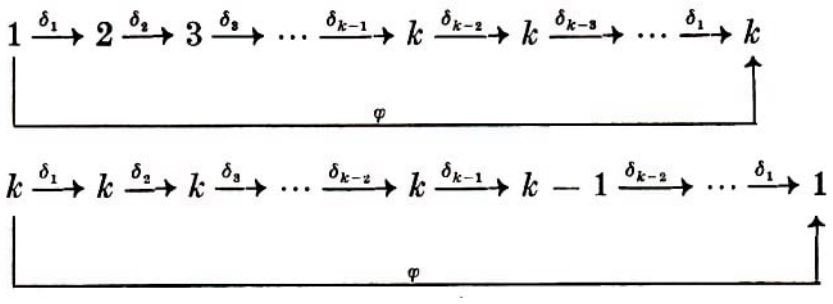
$$(i,j) = (1,i) \circ (1,j) \circ (1,i) \tag{2}$$

(Man überzeuge sich davon, dass die Permutationen, die rechts und links in dieser Gleichung stehen, auf jedes Element von M in gleicher Weise wirken.)
Da man jede beliebige Permutation φ in ein Produkt von Transpositionen der Gestalt (i,j) zerlegen kann, erhält man, wenn in dieser Zerlegung alle Transpositionen gemäß Gleichung (2) ersetzt werden, eine Zerlegung von φ in ein Produkt von Transpositionen des Systems II.

Andererseits kann man jede Transposition aus der Folge II in ein Produkt von Permutationen des Systems I zerlegen, und zwar mit Hilfe der Gleichung

$$(1,k) = (1,2) \circ (2,3) \circ ... \circ (k-1,k) \circ (k-1,k-2) \circ ... \circ (2,1) \tag{3}$$

Wir wollen Gleichung (3) verifizieren. Es sei $\delta_i = (i, i+1)$. Die Permutation $\varphi = \delta_1 \circ \delta_2 \circ ... \circ \delta_{k-1} \circ \delta_{k-2} \circ ... \circ \delta_1$ wirkt auf die Elemente 1 und k in folgender Weise:



Die übrigen Elemente der Menge sind Fixpunkte von φ Folglich ist die Reihe I ebenfalls ein Erzeugendensystem für S_n.

Die interessantesten Erzeugendensysteme sind diejenigen, bei denen es nicht möglich ist, auch nur ein einziges Element zu streichen, ohne dass das System aufhört, ein

Erzeugendensystem zu sein. Solche Systeme nennt man irreduzibel. Sie können unterschiedlich viele Permutationen enthalten, aus denen sie bestehen. Insbesondere existieren Erzeugendensysteme, die aus zwei Permutationen bestehen (solche Systeme sind immer irreduzibel). Beispielsweise ist

$$III \quad \alpha = (1,2), \quad \beta = (1,2,3,...,n)$$

ein solches System. Für $1 \leq j \leq n-2$ ist nämlich

$$\beta^j(1) = j+1 \qquad , \qquad \beta^j(2) = j+2$$

und somit

$$(\beta^j)^{-1} \circ \alpha \circ \beta^j = (j+1, j+2)$$

Daher lässt sich jede Permutation des Systems I in ein Produkt der Permutationen α und β zerlegen, weil das Element β^j eine endliche Ordnung, etwa l, besitzt, und somit $(\beta^j)^{-1} = (\beta^j)^{l-1}$ gilt.

Aufgaben

1. Man zerlege die Permutationen

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 7 & 5 & 6 & 1 & 8 \end{pmatrix}$; b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 2 & 1 & 4 & 3 & 5 \end{pmatrix}$; c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$

in Produkte von Elementen der Systeme I, II, III.

2. Sind die Erzeugendensysteme I und II irreduzibel?

3. Man zeige, dass alle Zyklen der Länge 3 zusammen mit irgendeiner Transposition ein Erzeugendensystem der symmetrischen Gruppe S_n bilden.

4. Bilden die Permutationen $(1,2,3)$, $(1,2,3,...,9)$ ein Erzeugendensystem der symmetrischen Gruppe S_9?

5. Man beweise: Jede Teilmenge von S_n, die aus mehr als $n!/2$ Elementen besteht, bildet ein Erzeugendensystem für S_n.

8 Untergruppen der symmetrischen Gruppe

Wie wir bereits an Beispielen gesehen haben, bilden einige Teilmengen von S_n selbst eine Gruppe bezüglich der Multiplikation von Permutationen. Solche Teilmengen spielen beim Studium der Struktur der Gruppe S_n eine wichtige Rolle.

Definition. Eine Teilmenge T der Menge S_n heißt Untergruppe der Gruppe S_n, wenn sie bezüglich der Multiplikation von Permutationen eine Gruppe ist.

Oft, wenn dies kein Missverständnis hervorruft, nennt man die Untergruppen der symmetrischen Gruppe S_n einfach Permutationsgruppen der Menge $\{1, 2, 3, ..., n\}$. Insbesondere ist auch die Menge S_n selbst Untergruppe von sich, eine sogenannte uneigentliche Untergruppe. Außerdem ist die Menge, die nur aus dem Element ε besteht, ebenfalls eine Untergruppe, wie aus den Gleichungen

$$\varepsilon \circ \varepsilon = \varepsilon, \qquad \varepsilon^{-1} = \varepsilon$$

folgt. Sie wird die triviale Untergruppe der Gruppe S_n genannt. Jede andere Untergruppe G von S_n erfüllt offenbar die Ungleichungen

$$1 < |G| < n!$$

Die Anzahl der Elemente einer (endlichen) Gruppe wird Ordnung der Gruppe genannt.

Für jede Teilmenge der Menge S_n, welche Untergruppe ist, müssen alle Bedingungen der Gruppendefinition erfüllt sein. Es ist aber nicht notwendig, dies für alle Bedingungen zu verifizieren. Genauer gesagt, es gilt folgender

Satz. Eine Teilmenge T der Gruppe S_n, die wenigstens eine Permutation enthält, ist genau dann Untergruppe der Gruppe S_n, wenn folgende Bedingungen erfüllt sind :
1. Mit je zwei Elementen α, β gehört auch ihr Produkt $\alpha \circ \beta$ zu T.
2. Aus $\alpha \in T$ folgt $\alpha^{-1} \in T$.

Ist nämlich T eine Untergruppe von S_n, so ist sie bezüglich der Multiplikation von Permutationen in T abgeschlossen, d. h., die Bedingung 1 ist erfüllt. Jedes Element aus T besitzt ein Inverses, folglich ist auch Bedingung 2 erfüllt.

Umgekehrt seien für eine Menge T von Permutationen die Bedingungen 1 und 2 erfüllt. Wir prüfen, ob die Menge T alle Gruppeneigenschaften besitzt. Bedingung 1 bedeutet, dass die Menge T bezüglich der Multiplikation ihrer Elemente abgeschlossen ist; folglich genügt sie der ersten Forderung der Gruppendefinition. Die Assoziativität der Multiplikation von Permutationen gilt, weil die Multiplikation beliebiger Permutationen (insbesondere auch derjenigen, die in T liegen) diese Eigenschaft besitzt.

Die identische Permutation muss ebenfalls zu T gehören. Denn T enthält wenigstens eine Permutation, sagen wir α, und dann gehört nach Bedingung 2 auch α^{-1} zu T. Daher liegt nach Bedingung 1 die Permutation $\alpha \circ \alpha^{-1} = \varepsilon$ in T. Schließlich zeigt Bedingung 2, dass jedes Element aus T ein inverses besitzt, das ebenfalls zu T gehört. Folglich ist T eine Untergruppe der Gruppe S_n.

Beispiele.
1. Es sei H die Menge der Permutationen

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Wir prüfen nach, ob H eine Untergruppe der Gruppe S_4 ist. Wegen $\alpha^{-1} = \alpha$, $\beta^{-1} = \beta$, $\gamma^{-1} = \gamma$ gilt für die Menge H die Bedingung 2 des soeben bewiesenen Satzes. Außerdem haben wir

$$\alpha \circ \beta = \beta \circ \alpha = \gamma, \quad \alpha \circ \gamma = \gamma \circ \alpha = \beta, \quad \beta \circ \gamma = \gamma \circ \beta = \alpha, \quad \alpha^2 = \beta^2 = \gamma^2 = \varepsilon,$$
$$\alpha \circ \varepsilon = \alpha, \quad \beta \circ \varepsilon = \beta, \quad \gamma \circ \varepsilon = \gamma$$

(man prüfe dies nach !). Somit ist das Produkt je zweier Elemente aus H ein Element ebendieser Menge, d. h., für H gilt auch Bedingung 1 des erwähnten Satzes. Aus den oben aufgeschriebenen Gleichungen folgt, dass die Gruppe H abelsch ist.

2. Es sei G die Menge der Permutationen

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix},$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

Dann ist $\alpha^{-1} = \delta$, $\beta^{-1} = \gamma$, $\delta^{-1} = \alpha$, $\gamma^{-1} = \beta$, also die Bedingung 2 des Satzes über Untergruppen von S_n erfüllt. Außerdem gelten die Gleichungen

$$\alpha \circ \beta = \beta \circ \alpha = \gamma, \quad \alpha \circ \gamma = \gamma \circ \alpha = \delta, \quad \alpha \circ \delta = \delta \circ \alpha = \varepsilon, \quad \beta \circ \gamma = \gamma \circ \beta = \varepsilon,$$
$$\beta \circ \delta = \delta \circ \beta = \alpha, \quad \gamma \circ \delta = \delta \circ \gamma = \beta, \quad \alpha^2 = \alpha, \quad \beta^2 = \delta, \quad \gamma^2 = \alpha, \quad \delta^2 = \gamma$$

(Man prüfe dies nach!) Wie wir sehen, liegt das Produkt je zweier Elemente von G wieder in G, folglich ist auch Bedingung 1 erfüllt. Daher bildet die Menge G eine Untergruppe der Gruppe S_5, wobei aus den angegebenen Gleichungen folgt, dass G abelsch ist.

3. Es sei T die Menge der Permutationen

$$\varepsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Diese Menge ist keine Untergruppe der Gruppe S_4, weil für sie keine der Bedingungen 1 und 2 erfüllt ist. Es ist nämlich

$$\gamma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \notin T, \qquad \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \notin T$$

Die symmetrische Gruppe S_n besitzt viele verschiedene Untergruppen, und ihre Anzahl wächst mit zunehmendem n sehr rasch.

Beispiele bringen wir im folgenden Abschnitt. Alle Untergruppen der Gruppe S_n zu beschreiben gelingt nur für kleinere n, für größere n studiert man nur die allgemeinen Eigenschaften solcher Untergruppen.

Aufgabe. Man beschreibe alle Untergruppen der symmetrischen Gruppe S_3.

Lösung. 1. Wir beschreiben zuerst die aus zwei Elementen bestehenden Untergruppen. Ist H eine solche Untergruppe, so gehört zu ihr das Element ε und noch irgendein anderes Element α. Das zu α inverse Element kann nicht mit ε übereinstimmen; daher ist $\alpha^{-1} = \alpha$. Diese Gleichung kann man auch folgendermaßen schreiben: $\alpha^2 = \varepsilon$.
Folglich ist α eine Permutation der Ordnung 2, d. h. ein Zyklus der Länge 2. Somit existieren nicht mehr als drei Untergruppen von S_3 der Ordnung 2. Das sind folgende Teilmengen der Menge S_3:

$$A = \{\varepsilon, (1,2)\}, \quad B = \{\varepsilon, (2,3)\}, \quad C = \{\varepsilon, (1,3)\}$$

Durch Anwendung des oben formulierten Satzes überzeugt man sich jetzt leicht davon, dass die Teilmengen A, B und C wirklich Untergruppen sind, weil für jede von ihnen die Bedingungen 1 und 2 dieses Satzes erfüllt sind.

2. Jetzt beschreiben wir die aus drei Elementen bestehenden Untergruppen. Ist $G = \{\varepsilon, \alpha, \beta\}$ eine solche Untergruppe, so müssen die Elemente α und β die Ordnung 3 haben.
Hätte nämlich eines von ihnen, etwa α, die Ordnung 2, so wäre $\alpha = \alpha^{-1}$; da aber jedes Element nur ein inverses besitzt, wäre aus $\beta^{-1} = \beta$, also $\beta^2 = \varepsilon$.
Es ist jedoch leicht unmittelbar nachzuprüfen, dass S_3 das Produkt zweier voneinander verschiedener Elemente der Ordnung 2 ein Element der Ordnung 3 ist. Hieraus ergibt sich, dass das Produkt $\alpha \circ \beta$ nicht in G liegen würde, und G wäre keine Untergruppe.

Wir betrachten jetzt den Fall, dass die Permutationen α und β beide die Ordnung 3 besitzen, also $G = \{\varepsilon, (1,2,3), (1,3,2)\}$ ist. Dann gilt

$$\alpha^{-1} = \beta, \quad \beta^{-1} = \alpha, \quad \alpha \circ \beta = \beta \circ \alpha = \varepsilon, \quad \alpha^2 = \beta, \quad \beta^2 = \alpha$$

d. h., die Teilmenge G der Menge S_3 ist wirklich eine Untergruppe der Gruppe S_3.

Man kann sich leicht davon überzeugen, dass die Teilmengen der Menge S_3, welche vier oder fünf Elemente enthalten, keine Untergruppen bilden. Dies möge der Leser selbständig tun.

Somit besitzt die symmetrische Gruppe s_3 sechs verschiedene Untergruppen.

Nun betrachten wir noch ein allgemeines Beispiel einer Gruppe von Permutationen. Es sei $\alpha \neq \varepsilon$ eine Permutation aus S_n der Ordnung k. Dann sind die Permutationen

$$\alpha, \alpha^2, \alpha^3, ..., \alpha^{k-1}, \alpha^k = \varepsilon$$

voneinander verschieden. Wir zeigen nun, dass die Menge C dieser Permutationen eine Gruppe bildet. In der Tat gilt nach Definition der Multiplikation für beliebige

Permutationen $\alpha^i, \alpha^j \in C$

$$\alpha^i \circ \alpha^j = \begin{cases} \alpha^{i+j} & \text{für } i+j < k \\ \alpha^{i+j-k} & \text{für } i+j \geq k \end{cases}$$

Die zu α^i inverse Permutation ist α^{k-i} wegen $\alpha^i \circ \alpha^{k-i} = \alpha^k = \varepsilon$. Somit ist das Produkt je zweier Permutationen aus der Menge C wieder ein Element der Menge C, und die zu einer beliebigen Permutation aus C inverse Permutation liegt ebenfalls in C. Folglich ist C eine Gruppe. Solche Gruppen heißen zyklische Gruppen.

Die Untergruppe in Beispiel 2 ist zyklisch; jede Untergruppe der Gruppe S_3 ist ebenfalls zyklisch. Die Untergruppe in Beispiel 1 ist jedoch keine zyklische Untergruppe.

Aufgaben
1. Man beschreibe alle Untergruppen der Gruppe S_4, die aus drei Elementen bestehen. Wieviel sind es?

2. Wieviel Untergruppen der Ordnung 2 besitzt die Gruppe S_5?

3. Man beweise, dass die Menge aller Elemente der Gruppe S_n, die eine bestimmte Zahl k unverändert lassen, eine Gruppe ist.

4. Man sagt, die Permutationen α und β seien vertauschbar, wenn $\alpha \circ \beta = \beta \circ \alpha$ gilt. Die Menge aller Elemente einer beliebigen Gruppe, die mit jedem ihrer Elemente vertauschbar sind, wird das Zentrum der Gruppe genannt. Man bestimme das Zentrum der Gruppe S_4.

5. Welche größte Ordnung kann eine zyklische Untergruppe der Gruppe S_9 haben?

6. Man beweise, dass eine Teilmenge K der Menge S_n eine Untergruppe bildet, wenn das Produkt je zweier Elemente aus K zu K gehört.

9 Symmetriegruppen

Eines der am häufigsten benutzten Beispiele für Gruppen und insbesondere für Permutationsgruppen sind Gruppen, welche die Symmetrie ebener bzw. räumlicher geometrischer Figuren "messen". In diesem Abschnitt führen wir entsprechende Beispiele an.

Zunächst betrachten wir die Symmetrie ebener Figuren.
Eine ebene Figur kann eine oder mehrere Symmetrieachsen besitzen; eine Symmetrieachse ist eine Gerade, die die Figur in zwei Teile teilt (vgl. Abb. 19), von denen jeder Spiegelbild des anderen ist. In diesem Fall nennt man die Figur symmetrisch bezüglich der gegebenen Geraden.

Ein anderer Typ von Symmetrie ist die Symmetrie bezüglich eines Punktes (vgl. Abb. 20), des sogenannten Symmetriezentrums; die Figur wird dann zentralsymmetrisch genannt.

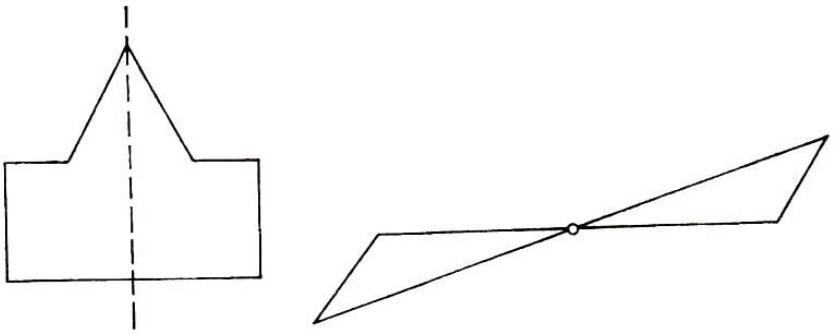


Abb. 19,20

Dieser Begriff lässt sich auf natürliche Weise verallgemeinern; und zwar werden wir sagen, ein Punkt O sei ein Symmetriezentrum der Ordnung n für die Figur M, wenn die Figur M bei Drehungen um Winkel, welche Vielfache von $2\pi/n$ sind, mit sich zur Deckung gebracht wird. Als Beispiel ist in Abb. 21 eine Figur dargestellt, die ein Symmetriezentrum der Ordnung 3 besitzt.

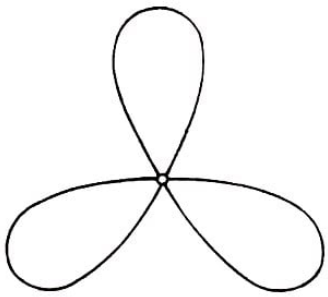


Abb. 21

Jedem Symmetrietyp entspricht eine Symmetrie-Transformation - die Transformation der Menge der Punkte der Ebene, die durch diesen Typ bestimmt wird. Ist etwa O ein Symmetriezentrum der Ordnung n, so ist die entsprechende Transformation eine Drehung aller Punkte der Ebene um den Punkt O um den Winkel $2\pi/n$ (vgl. Abschnitt 2, Beispiel 8).

Der Bestimmtheit halber werden wir annehmen, die Drehung verlaufe entgegen dem Uhrzeigersinn. Symmetrie einer Figur bedeutet, dass die Figur bei einer entsprechenden

Symmetrie-Transformation mit sich selbst zur Deckung kommt. (Solche Transformationen nennt man Deckoperationen.)
Somit ist die Aufzählung aller gegebenen Symmetrien einer Figur gleichwertig mit der Aufzählung aller derjenigen Transformationen der Ebene, bei denen die Figur mit sich zur Deckung kommt.

Natürlich sind diese Transformationen Bijektionen. Daher bildet die Menge aller dieser Transformationen bezüglich der Multiplikation von Transformationen eine Gruppe, die gleichsam ein Maß für den Grad der Symmetrie der gegebenen Figuren ist. Die Symmetrie-Transformationen vieler ebener Figuren lassen sich in natürlicher Weise mit Hilfe von Permutationen beschreiben, d. h., der Grad ihrer Symmetrie lässt sich durch bestimmte Permutationsgruppen "messen".
Wir beschreiben diese Gruppen für den Fall, dass die betrachtete Figur ein regelmäßiges Vieleck ist.

1. Die Symmetriegruppe des gleichseitigen Dreiecks.

Wir nummerieren die Ecken eines gleichseitigen Dreiecks mit den Zahlen 1, 2, 3 (vgl. Abb. 22) und charakterisieren jede seiner Deckoperationen φ durch eine Permutation der Menge der Ecken des Dreiecks; sagen wir

$$\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix}$$

wobei $i_k = (k)\varphi$ die Nummer der Stelle ist, welche nach Ausführung der Transformation φ von der Ecke k belegt wird, $k = 1, 2, 3$.

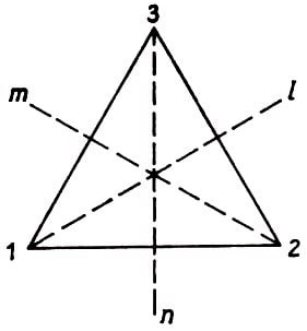


Abb. 22

Der Mittelpunkt O des gleichseitigen Dreiecks ist ein Symmetriezentrum der Ordnung 3, d. h., die Drehungen $\varphi_0 = \varepsilon$, φ_1, φ_2 um die Winkel 0, $2\pi/3$ bzw. $4\pi/3$ um den Punkt O entgegen dem Uhrzeigersinn bringen das Dreieck mit sich zur Deckung.

Außerdem gibt es die drei Achsensymmetrien $\varphi_3, \varphi_4, \varphi_5$, welche durch die drei Symmetrieachsen l, m, n definiert werden, die durch die Ecken des gleichseitigen Dreiecks und die Mittelpunkte der ihnen gegenüberliegenden Seiten führen (vgl. Abb. 22). Unsere Zuordnung zwischen den Deckoperationen des Dreiecks und den Permutationen der

Eckpunkte des Dreiecks liefert

$$\varphi_0 \sim \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \varphi_1 \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$$
$$\varphi_2 \sim \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2), \qquad \varphi_3 \sim \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$$
$$\varphi_4 \sim \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3), \qquad \varphi_5 \sim \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$$

Somit ist die Symmetriegruppe des gleichseitigen Dreiecks die symmetrische Gruppe S_3.

2. Die Symmetriegruppe des Quadrates.

Die Deckoperationen des Quadrates sind die Drehungen $\alpha_0 = \varepsilon$, α_1, α_2, α_3 um die Winkel 0, $\pi/2$, π, $3\pi/2$ um den Mittelpunkt des Quadrates und die Spiegelungen α_4, α_5, α_6, α_7 bezüglich der Achsen k, l, m, n, die durch die Mittelpunkte gegenüberliegender Seiten bzw. durch gegenüberliegende Eckpunkte führen (vgl. Abb. 23).

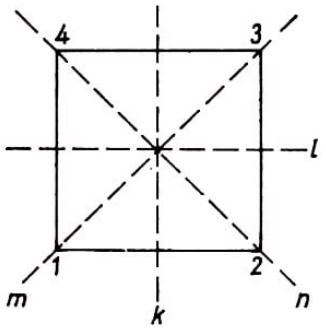


Abb. 23

Die Zuordnung zwischen den Deckoperationen des Quadrates und den Permutationen der Menge der Eckpunkte bei der in Abb. 23 angenommenen Nummerierung seiner Eckpunkte liefert

$\alpha_1 \sim (1,2,3,4)$, $\alpha_2 \sim (1,3) \circ (2,4)$, $\alpha_3 \sim (1,4,3,2)$, $\alpha_4 \sim (1,2) \circ (3,4)$,
$\alpha_5 \sim (1,4) \circ (2,3)$, $\alpha_6 \sim (2,4)$, $\alpha_7 \sim (1,3)$

Somit ist die Symmetriegruppe des Quadrates eine echte Untergruppe der symmetrischen Gruppe S_4. Sie wird mit D_4 bezeichnet.

3. Die Symmetriegruppe des regelmäßigen n-Ecks

besteht aus den n Drehungen um die Winkel 0, $2\pi/n$, $4\pi/n$, ..., $2(n-1)\pi/n$ um den Mittelpunkt des n-Ecks und n Spiegelungen bezüglich gewisser Geraden. Die Lage der Symmetrieachsen hängt davon ab, ob die Zahl n gerade oder ungerade ist.
Bei geradem n hat man $n/2$ Symmetrieachsen, die durch die Mittelpunkte der einander gegenüberliegenden Seiten, und $n/2$ Achsen, die durch die einander gegenüberliegenden Eckpunkte (und den Mittelpunkt) des Vielecks führen.

Bei ungeradem n sind die Symmetrieachsen die Geraden, die durch die Eckpunkte (und

den Mittelpunkt) des n-Ecks und die Mittelpunkte der ihnen gegenüberliegenden Seiten führen.
Somit besteht die Symmetriegruppe des regelmäßigen n-Ecks aus $2n$ Transformationen.

Werden diese Transformationen durch Permutationen der Menge der Eckpunkte des regelmäßigen n-Ecks beschrieben, so ist die entsprechende Permutationsgruppe eine Untergruppe der symmetrischen Gruppe S_n. Diese Permutationsgruppe wird Diedergruppe genannt und mit D_n bezeichnet.

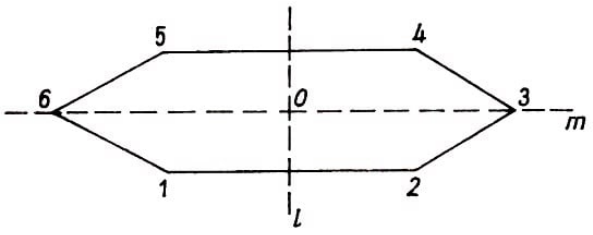


Abb. 24

4. Die Symmetriegruppe des in Abb. 24 dargestellten Vielecks besteht aus der identischen Transformation $\alpha_0 = \varepsilon$, den Spiegelungen α_1 und α_2 bezüglich der Achsen l und m und der Spiegelung α_3 bezüglich des Zentrums O.
Sie lassen sich durch die folgenden Permutationen der Menge $\{1, 2, 3, 4, 5, 6\}$ beschreiben:

$$\alpha_1 \sim (1,2) \circ (3,6) \circ (4,5), \qquad \alpha_2 \sim (1,5) \circ (2,4), \qquad \alpha_3 \sim (1,4) \circ (2,5) \circ (3,6)$$

Bei räumlichen Körpern kann man von folgenden Symmetrietypen sprechen:

a) Spiegelsymmetrie (Symmetrie bezüglich gewisser Ebenen);
b) Achsensymmetrie (Symmetrie bezüglich gewisser Geraden);
c) Zentralsymmetrie (Symmetrie bezüglich eines Punktes).

In Analogie zur Ebene kann man den Begriff der Achsensymmetrie in natürlicher Weise verallgemeinern. Eine Gerade wird Symmetrieachse der Ordnung n genannt, wenn der Körper bei Drehungen um diese Gerade um Winkel, welche Vielfache von $2\pi/n$ sind, mit sich zur Deckung kommt. Jedem Symmetrietyp entspricht seine Transformation des Raumes, und dass ein Körper eine Symmetrie besitzt, bedeutet, dass er bei entsprechenden räumlichen Transformationen mit sich selbst zur Deckung kommt. Die Menge aller solcher Transformationen, durch die der Körper mit sich selbst zur Deckung gebracht wird (die Menge der Deckoperationen des Körpers), bildet die Symmetriegruppe des gegebenen Körpers.

Die Symmetrie von Polyedern und von gewissen anderen Körpern lässt sich durch Permutationen der Menge ihrer Eckpunkte charakterisieren. In diesem Fall ist die Symmetriegruppe auch eine gewisse Permutationsgruppe. Wir führen ein Beispiel für eine solche Beschreibung an.

5.Die Symmetriegruppe des Tetraeders.

Das Tetraeder (Abb. 25) besitzt die vier Symmetrieachsen l_1, l_2, l_3, l_4 der Ordnung 3,

die durch die Eckpunkte 1, 2, 3, 4 und die Mittelpunkte O_1, O_2, O_3, O_4 der gegenüberliegenden Seitenflächen führen. Um jede Achse sind außer der identischen noch zwei Drehungen möglich, denen folgende Permutationen entsprechen:

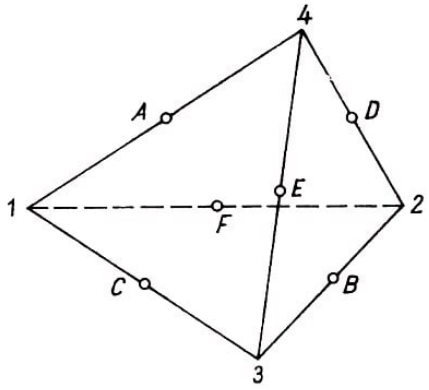


Abb. 25

Um die Achse l_1 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$

um die Achse l_2 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

um die Achse l_3 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

um die Achse l_2 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Außerdem gibt es drei Symmetrieachsen der Ordnung 2, die durch die Mittelpunkte A, B, C, D, E, F der windschiefen Kanten führen. Daher gibt es noch drei (entsprechend der Anzahl der Paare windschiefer Kanten) nichtidentische Transformationen, die den Permutationen

um die Achse AB $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

um die Achse CD $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

um die Achse EF $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ entsprechen.

Somit erhalten wir zusammen mit der identischen Transformation zwölf Permutationen. Die Symmetriegruppe des Tetraeders ist mit dieser Beschreibung eine Untergruppe der Gruppe S_4.

Analog kann man auch die Symmetriegruppen anderer, nicht notwendig regelmäßiger Vielecke und Vielflache bestimmen. Sie sind Untergruppen entsprechender symmetrischer Gruppen. Daraus ist bereits ersichtlich, dass die symmetrischen Gruppen sehr reich an Untergruppen sind. Überdies gilt folgende wichtige Tatsache.

Jede endliche Gruppe ist im Grunde Untergruppe der symmetrischen Gruppe S_n bei passendem n. Auf den Beweis dieser Aussage werden wir jedoch nicht eingehen.

Aufgaben

1. Man bestimme die Ordnung aller Elemente der Gruppe D_8.

2. Sind die Gruppen D_n abelsch?

3. Den Begriff des Erzeugendensystems kann man für beliebige Permutationsgruppen betrachten, und zwar wird eine Teilmenge T der Permutationsgruppe G ein Erzeugendensystem genannt, wenn man jede Permutation aus G als Produkt von Permutationen aus T schreiben kann. Analog definiert man auch die irreduziblen Erzeugendensysteme. Man gebe ein irreduzibles Erzeugendensystem der Gruppe D_n an. Gibt es ein irreduzibles Erzeugendensystem der Gruppe D_n, das aus Permutationen der Ordnung 2 besteht? Existieren irreduzible Erzeugendensysteme, die aus einer verschiedenen Anzahl von Permutationen bestehen?

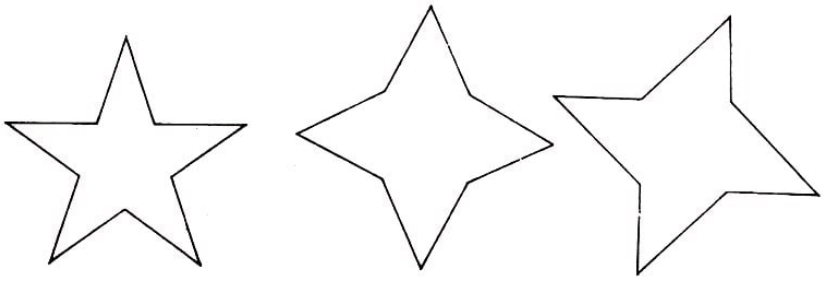


Abb. 26,27

4. Man beschreibe die Symmetriegruppe des in Abb. 26 dargestellten Sterne. Welche Ordnung hat diese Gruppe?

5. Man beweise, dass die Symmetriegruppe des Würfels aus 48 Permutationen besteht.

6. Man beschreibe alle Drehungen des Würfels um alle möglichen Symmetrieachsen. Wieviel sind es?

7. Unterscheiden sich die Symmetriegruppen der in Abb. 27 dargestellten ebenen Figuren?

10 Der Satz von Lagrange

Es seien G und H Gruppen von Permutationen und $H \subset G$, mit anderen Worten, H sei Untergruppe von G. Einer der ersten Sätze der Gruppentheorie ist der Satz, der den Zusammenhang zwischen den Ordnungen der Gruppen G und H wiedergibt und bereits Ende des 18. Jahrhunderts von Lagrange, allerdings in anderer Terminologie, bewiesen wurde. Dieser in Bezug auf die Beweisidee einfache Satz wird oft benutzt, sowohl in der Gruppentheorie selbst als auch bei allen Anwendungen. Eine davon betrachten wir weiter unten.

Satz von Lagrange. Ist H Untergruppe der Gruppe G, so ist die Ordnung von H ein Teiler der Ordnung von G.

Beweis. Es seien ε, α_2, α_2, ..., α_{n-1} alle in G enthaltenen Permutationen, $\beta_0 = \varepsilon$, β_1, β_2, ..., β_{m-1} alle Permutationen aus H (dabei ist $m \leq n$).
Für $H = G$ ist die Behauptung des Satzes richtig, daher setzen wir $H \neq G$ voraus (H sei also eine echte Untergruppe von G). Auf Grund dieser Voraussetzung existiert eine Permutation $\gamma_1 \in G$, für welche $\gamma_1 \notin H$ gilt. Wir betrachten die Folge der Permutationen

$$\beta_0 \circ \gamma_1 = \gamma_1, \quad \beta_1 \circ \gamma_1, \quad ..., \qquad \beta_{m-1} \circ \gamma_1$$

Alle Permutationen dieser Folge sind voneinander verschieden:
Würde nämlich für irgendwelche i, j die Gleichung $\beta_i \circ \gamma_1 = \beta_j \circ \gamma$ gelten, so erhielten wir, wenn wir ihre rechte und ihre linke Seite mit γ^{-1} multiplizieren, die Beziehung $\beta_i = \beta_j$.
Außerdem ist keine dieser Permutationen in der Untergruppe H enthalten; denn würde für irgendeinen Index i die Beziehung $\beta_i \circ \gamma_1 \in H$ gelten, so hieße das, dass $\beta_i \circ \gamma_1 = \beta_j$ für irgendein j gilt. Aus dieser Gleichung erhielten wir $\gamma_1 = \beta_i^{-1} \circ \beta_j$; da aber H eine Gruppe von Permutationen ist, läge γ_1 in H, und das widerspräche der obigen Auswahl von γ_1.

Wenn die Permutationen der Gruppe H und die Folge (1) alle Permutationen von G ausschöpfen, dann gilt $|G| = 2|H|$, und alles ist bewiesen. Andererenfalls lässt sich eine Permutation $\gamma_2 \in G$ finden derart, dass $\gamma_2 \notin H$ gilt und γ_2 auch nicht in der Folge (1) enthalten ist. Nun definieren wir die Permutationen

$$\beta_0 \circ \gamma_2 = \gamma_2, \beta_1 \circ \gamma_2, ..., \beta_{m-1} \circ \gamma_2 \tag{2}$$

Wie oben lässt sich zeigen: a) Alle Permutationen aus (2) sind voneinander verschieden; b) keine davon gehört zu H; c) keine von ihnen kommt unter den Permutationen der Folge (1) vor.

Wenn die Permutationen aus der Untergruppe H und den Folgen (1) und (2) alle Elemente von G ausschöpfen, ist $|G| = 3|H|$, und alles ist bewiesen.
Anderenfalls führen wir den Prozess der Auswahl von Permutationen γ_3 und der Konstruktion von Folgen der Gestalt (1) und (2) weiter fort. Da G endlich ist, werden bei irgendeinem, etwa beim k-ten Schritt alle Permutationen aus G erfasst sein. Mit

anderen Worten, man kann sie alle in einer Tabelle der folgenden Gestalt anordnen:

$$\begin{aligned}
&\beta_0, \beta_1, ..., \beta_{m-1} \\
&\beta_0 \circ \gamma_1, \beta_1 \circ \gamma_1, ..., \beta_{m-1} \circ \gamma_1 \\
&\beta_0 \circ \gamma_2, \beta_1 \circ \gamma_2, ..., \beta_{m-1} \circ \gamma_2 \\
&... \\
&\beta_0 \circ \gamma_k, \beta_1 \circ \gamma_k, ..., \beta_{m-1} \circ \gamma_k
\end{aligned} \tag{3}$$

wobei alle Permutationen in jeder Zeile dieser Tabelle voneinander verschieden sind und je zwei verschiedene Zeilen keine gemeinsamen Elemente besitzen. Da die Gesamtzahl der Elemente in der Tabelle gleich n (der Ordnung der Gruppe G) und die Anzahl der Elemente in jeder Zeile gleich m (der Ordnung der (Unter-) Gruppe H) ist, erhalten wir die Gleichung $n = mk$, mit anderen Worten, m ist Teiler von n. Damit ist der Satz bewiesen.

Die Zahl k nennt man den Index der Untergruppe H in der Gruppe G; sie wird mit $[G : H]$ bezeichnet. Hiernach folgt aus dem Beweis des Satzes von Lagrange die Gleichung

$$|G| = |H| \cdot [G : H]$$

Da die Ordnung der zyklischen Untergruppe, die von der Permutation $\alpha \in G$ erzeugt wird, mit der Ordnung der Permutation α übereinstimmt, ergibt sich aus dem Satz von Lagrange, dass die Ordnung jeder Permutation aus G ein Teiler von $|G|$ ist.

Der Satz von Lagrange erlaubt es auch, die Lösung der Aufgabe, alle Untergruppen einer gegebenen Gruppe zu beschreiben, wesentlich zu vereinfachen. Ist z. B. die Ordnung $|G|$ von G eine Primzahl, so hat G nach diesem Satz keine echten Untergruppen.

Echte Untergruppen von S_3 können aus zwei oder drei Permutationen bestehen (Teiler von $3! = 6$); daher kann man auf die Nachprüfung, von der als Aufgabe in Abschnitt 8 die Rede ist (ob es Untergruppen der Ordnungen 4 und 5 gibt), verzichten.
Dieses Nachprüfen ist übrigens recht umständlich, weil es $\binom{6}{4}+\binom{6}{5} = 21$ Teilmengen von S_3 gibt, die aus vier bzw. fünf Elementen bestehen. Schon an diesen beiden Beispielen ist zu erkennen, wie wichtig es sein kann, den Satz von Lagrange zu benutzen.

Aufgaben
1. Die Mengen von Permutationen, die in den Zeilen von Tabelle (3) stehen, werden Rechtsnebenklassen genannt (da von rechts mit γ_i multipliziert wird); Tabelle (3) selbst wird natürlich die Tabelle der Zerlegung der Gruppe G in Rechtsnebenklassen nach der Untergruppe H genannt. Ganz analog kann man die Tabelle für die Zerlegung von G in Linksnebenklassen nach der Untergruppe H aufstellen.
Man konstruiere die Tabellen für die Zerlegung der Gruppe S_3 sowohl in Rechts- als auch in Linksnebenklassen nach der Untergruppe $A = \{\varepsilon, (1, 2)\}$ und nach der Untergruppe $B = \{\varepsilon, (1, 2, 3), (1, 3, 2)\}$.

2. Mein zeige, dass die Drehungen des regelmäßigen Sechsecks um seinen Mittelpunkt um Winkel, welche Vielfache von $\pi/3$ sind, eine Untergruppe seiner Symmetriegruppe bilden. Man stelle die Tabellen für die Zerlegung in Rechts- bzw. Linksnebenklassen

der Symmetriegruppe des Sechsecks nach der Untergruppe aller Drehungen auf. Man verallgemeinere dies auf den Fall des regelmäßigen n-Ecks.

3. Man beweise: Ist H eine Untergruppe vom Index 2 in der Gruppe G, so stimmen die Rechts- und die Linksnebenklassen nach dieser Untergruppe überein.

4. Man beweise: Ist das System $k_1, k_2, ..., k_n$ natürlicher Zahlen k_i; eine Lösung der Gleichung $x_1 + x_2 + ... + x_n = m$ (für eine beliebige natürliche Zahl m), so ist das Produkt $k_1! \cdot k_2! \cdot ...k_n!$ Teiler von $m!$

5. Man schreibe alle Zahlen auf, die nach dem Satz von Lagrange Ordnungen der Elemente der Gruppe D_{12} sein können. Existieren in D_{12} Permutationen dieser Ordnungen?

6. Man beantworte dieselbe Frage für die Gruppe S_4.

11 Orbits einer Permutationsgruppe. Das Lemma von Burnside

Bei der Untersuchung von Permutationsgruppen haben wir uns auf das Studium ihrer Wirkungsweise auf die Elemente einer Menge beschränkt. Sobald aber eine solche Wirkungsweise definiert ist, "verschieben" die Permutationen auch Teilmengen der gegebenen Menge elementweise.
Beim Studium von Eigenschaften der Wirkungen auf Teilmengen besteht der erste Schritt natürlich darin, diejenigen Teilmengen zu beschreiben, welche die gegebene Transformationsgruppe im ganzen nicht verschiebt. In diesem Zusammenhang entsteht der Begriff des Orbits einer Permutationsgruppe auf einer gegebenen Menge.

Es sei G eine Permutationsgruppe der Menge $M = \{1, 2, ..., n\}$. Eine Teilmenge $O \subset M$ wird Orbit der Gruppe G genannt, wenn folgendes gilt:

a) $\alpha(a) \in O$ für jedes $\alpha \in G$ und jedes $a \in O$; d. h., die Wirkung der Permutationen aus G auf Elemente von O führt nicht aus O heraus;
b) je zwei Elemente von O können durch eine Permutation aus G ineinander übergeführt werden.

Jede Permutationsgruppe $G = \{\varepsilon = \alpha_0, \alpha_1, ..., \alpha_{k-1}\}$ besitzt Orbits. Zum Beweis greifen wir ein willkürliches Element $a \in M$ heraus und betrachten die Menge

$$O(a) = \{a = (a)\alpha_0, (a)\alpha_1, ..., (a)\alpha_{k-1}\}$$

Das ist ein Orbit der Gruppe G, denn:

a) Ist $\alpha_i \in G$ und $b = (a)\alpha_j \in O(a)$, so gehört auch $(b)\alpha_i = (a)(\alpha_j \circ \alpha_i)$ zu $O(a)$ wegen $\alpha_j \circ \alpha_i \in G$ (da G eine Gruppe ist);

b) sind $b = (a)\alpha_i$ und $c = (a)\alpha_j$ beliebige Elemente von $O(a)$, so gilt

$$b = (a)\alpha_i = (a)(\varepsilon \circ \alpha_i) = (a)(\alpha_j \circ \alpha_j^{-1} \circ \alpha_i) = (c)\alpha_j^{-1} \circ \alpha_i$$

dabei ist $\alpha_j^{-1} \circ \alpha_i \in G$, da G eine Gruppe ist.

Es zeigt sich, dass sich durch Orbits dieser Gestalt alle Typen von Orbits erschöpfen. Genauer: Ist O ein Orbit von G und gilt $a \in O$, so ist $O = O(a)$. Die Richtigkeit dieser Behauptung folgt unmittelbar aus der Definition des Orbits einer Gruppe.

Offenbar stimmen zwei beliebige Orbits $O(a)$ und $O(b)$ völlig überein (im Fall $b \in O(a)$), oder sie haben keine gemeinsamen Elemente (im Fall $b \notin O(a)$).
Daraus folgt (fast ebenso wie beim Beweis des Satzes von Lagrange), dass sich die Menge M als Vereinigung elementefremder Teilmengen - den Orbits der Gruppe G - darstellen lässt. Insbesondere kann es vorkommen, dass der einzige Orbit von G die Menge M selbst ist, wie das für die Gruppen D_n der Fall ist (man prüfe dies nach).

Gruppen mit dieser Eigenschaft nennt man transitiv. So ist eine Permutationsgruppe G auf der Menge M transitiv, wenn man jedes Element $a \in M$ durch Anwendung einer

passend gewählten Permutation $\alpha \in G$ aus jedem anderen Element $b \in M$ erhalten kann, d. h., wenn $(b)\alpha = a$ gilt. Alle anderen Gruppen von Permutationen heißen intransitiv.

Im Zusammenhang mit der Zerlegung einer Menge M in Orbits einer Permutationsgruppe G erheben sich die beiden folgenden Fragen:

1. Wieviel Orbits besitzt die Gruppe G auf M?
2. Welche Länge hat jeder dieser Orbits, d.h., aus wieviel Elementen besteht er?

Wir formulieren zuerst eine Aussage, die es erlaubt, auf die zweite Frage eine Antwort zu geben. Sie wird unter Benutzung des Begriffs Stabilisator eines Elementes a von M formuliert.
Man kann nämlich für jedes Element $a \in M$ die Menge G_a aller Permutationen aus G betrachten, für die der Punkt a Fixpunkt ist. Diese Menge ist offenbar eine Gruppe (hier haben wir eine weitere Methode zur Erzeugung von Permutationsgruppen), welche Stabilisator des Punktes a genannt wird.

Satz. Die Länge des Orbits $O(a)$ ist gleich dem Index des Stabilisators G_a in der Gruppe G, in Zeichen

$$|O(a)| = [G : G_a] = |G| : |G_a|$$

Beweis. Es sei $G = \{\alpha_0 = \varepsilon, \alpha_1, ..., \alpha_{k-1}\}$, $G_a = \{\beta_0 = \varepsilon, \beta_1, ..., \beta s - 1\}$. Zur Berechnung der verschiedenen Elemente der Folge $a, (a)\alpha_1$, ..., $(a)\alpha_{k-1}$ ist es zweckmäßig, die Elemente der Gruppe G in bestimmter Weise in einer Folge anzuordnen.
Zu diesem Zweck erinnern wir uns der beim Beweis des Satzes von Lagrange angewandten Zerlegung der Gruppe G in Rechtsnebenklassen nach der Untergruppe G_a. Es existieren Permutationen $\gamma_0 = \varepsilon$, γ_1, ..., γ_{l-1} aus G derart, dass alle Permutationen der Folge

$$\begin{aligned}
&\alpha_0 = \beta_0 \circ \gamma_0 = \varepsilon, \alpha_1 = \beta_1 \circ \gamma_0, ..., \alpha_{s-1} = \beta_{s-1} \circ \gamma_0, \\
&\alpha_s = \beta_0 \circ \gamma_1, \alpha_{s+1} = \beta_1 \circ \gamma_1, ..., \alpha_{2s-1} = \beta_{s-1} \circ \gamma_1 \\
&... \\
&\alpha_{(l-1)s} = \beta_0 \circ \gamma_{l-1}, \alpha_{(l-1)s+1} = \beta_1 \circ \gamma_{l-1}, ..., \alpha_{ls-1} = \beta_{s-1} \circ \gamma_{l-1} \qquad (1)
\end{aligned}$$

paarweise verschieden sind und die ganze Gruppe G ausschöpfen.
Für jedes $i = 0, ..., l-1$ ergibt die Anwendung der s Permutationen α_{is}, α_{is+1}, ..., $\alpha_{(i+1)s-1}$, welche die i-te Zeile der Tabelle (1) bilden, auf das Element a ein und dasselbe Element $(a)\gamma_i$.
Alle l Elemente $(a)\gamma_i$ sind paarweise verschieden. Wäre nämlich $(a)\gamma_i = (a)\gamma_j$ für gewisse $i \neq j$, so wäre $(a)\gamma_j \circ \alpha_i^{-1} = a$, so dass die Permutation $\gamma_j \circ \gamma_i^{-1}$ zu G_a gehören würde. Das ist aber nur dann möglich, wenn γ_i und γ_j in ein und derselben Rechtsnebenklasse von G nach der Untergruppe G_a enthalten sind, was nicht der Fall ist.

Somit ist die Länge des Orbits $O(a)$ gleich l, d. h. gleich der Anzahl der Zeilen in der Tabelle (1). Diese Zahl hatten wir aber in Abschnitt 10 Index der Untergruppe in der Gruppe genannt.

Wir veranschaulichen den Begriff des Orbits einer Gruppe und den soeben bewiesenen Satz am Beispiel 4 aus Abschnitt 9, in welchem die Permutationsgruppe $G = \{\varepsilon, \alpha_1, \alpha_2, \alpha_3\}$ betrachtet wurde, die auf der Menge $M = \{1, 2, 3, 4, 5, 6\}$ wirkt.
Es ist $(1)\varepsilon = 1$, $(1)\alpha_1 = 2$, $(1)\alpha_2 = 5$, $(1)\alpha_3 = 4$, also $O(1) = \{1, 2, 4, 5\}$. Wählen wir irgendein Element aus M, das nicht in $O(1)$ liegt, sagen wir 6, so erhalten wir $(6)\varepsilon = 6$, $(6)\alpha_1 = 3$, $(6)\alpha_2 = 6$, $(6)\alpha_3 = 3$, also $O(6) = \{3, 6\}$. Somit besitzt die Permutationsgruppe G der Menge M die beiden Orbits und ist demzufolge intransitiv.

Der Stabilisator G_1 des Punktes 1 aus $O(1)$ besteht aus einer einzigen Permutation, nämlich ε. Daher ist $[G : G_1] = 4 = |O(1)|$.
Der Stabilisator G_6 des Punktes 6 aus $O(6)$ besteht aus den Permutationen ε und α_2. Die Zerlegung der Gruppe G in Rechtsnebenklassen nach der Untergruppe $G_6 = \{\varepsilon, \alpha_2\}$ lautet

$$\varepsilon, \alpha_2, \varepsilon \circ \alpha_1 = \alpha_1, \alpha \circ \alpha_1 = \alpha_3$$

daher ist $[G : G_6] = 2 = |O(6)|$.

Wir beweisen jetzt eine Aussage, die aus historischen Gründen Lemma von Burnside genannt wird (nach dem englischen Algebraiker W. Burnside (1852-1927), der anscheinend als erster den Beweis in seinem Buch über die Theorie der endlichen Gruppen (1911) veröffentlichte). Diese einfache Aussage ist die Grundlage der Abzähltheorie, die von G. Polya und einigen anderen Mathematikern ausgearbeitet wurde, einer Theorie, welche vielfache Anwendungen in der Kybernetik, der Technik, der organischen Chemie, der Biologie usw. findet.

Es sei $\chi(\alpha)$ die Anzahl der Fixpunkte der Permutation α und $t(G)$ die Anzahl der Orbits der Permutationsgruppe $G = \{\alpha_0 = \varepsilon, \alpha_1, ..., \alpha_{k-1}\}$, die auf der Menge $M = \{1, 2, ..., n\}$ wirkt.

Lemma von Burnside. Für jede Permutationsgruppe gilt die Beziehung

$$t(G) = \frac{1}{|G|} \sum_{\alpha \in G} \chi(\alpha)$$

Beweis. Wir betrachten die Relation "Die Permutation α lässt das Element m fest" zwischen den Permutationen der Gruppe G und den Elementen der Menge M.

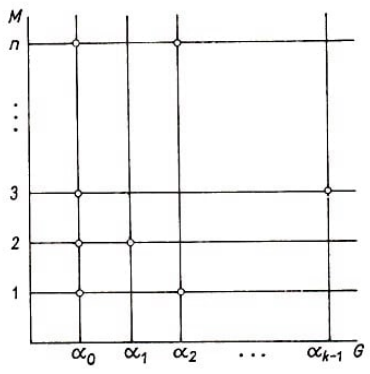


Abb. 28

Dann ordnen wir den Paaren (α, m), $\alpha \in G$, $m \in M$, die Gitterpunkte eines rechtwinkligen Netzes zu und markieren diejenigen von ihnen, für welche sich das entsprechende

Paar (α, m) in der genannten Relation befindet, d. h., für welche $(m)\alpha = m$ ist (vgl. Abb. 28). Mit anderen Worten, wir konstruieren eine graphische Darstellung dieser Relation.

Nun lässt sich die Anzahl der markierten Punkte (der Punkte, die zu der graphischen Darstellung gehören) auf zwei Arten berechnen: Man bestimmt die Anzahl der markierten Punkte auf jeder Vertikalen und addiert die erhaltenen Zahlen, oder man bestimmt die Anzahl dieser Punkte auf jeder Horizontalen und bildet danach ihre Summe.

Nach Definition der Relation sind auf jeder Vertikalen alle Punkte markiert, die von der Permutation α festgelassen werden, welche dieser Vertikalen entspricht. Ihre Anzahl, ist gleich $\chi(\alpha)$. Daher ist die Anzahl aller markierten Punkte der graphischen Darstellung gleich

$$\chi(\alpha_0) + \chi(\alpha_1) + ... + \chi(\alpha_{k-1}) = \sum_{\alpha \in G} \chi(\alpha)$$

Andererseits sind auf jeder Horizontalen alle Permutationen markiert, die das Element $m \in M$ festlassen, das dieser Horizontalen entspricht. Wir wissen, dass sie die Gruppe G_m den Stabilisator des Elementes m, bilden und dass die Anzahl $|G_m|$ dieser Permutationen nach dem vorhergehenden Satz gleich $|G| : |O(m)|$ ist.
Daher erhalten wir, wenn wir die Anzahl der markierten Punkte der graphischen Darstellung der betrachteten Relation auf die zweite Art berechnen, den Ausdruck

$$|G_1| + |G_2| + ... + |G_n| = \sum_{m \in M} |G_m| \tag{2}$$

Gehören jedoch die Elemente i, j aus M zu ein und demselben Orbit, so gilt $O(i) = O(j)$; daher ist $|G_i| = |G| : |O(i)| = |G| : |O(j)| = |G_j|$.
Es seien $O_1, O_2, ..., O_t$ alle Orbits der Gruppe G, und zwar seien in der Vereinigung $M = O_1 \cup O_2 \cup ... \cup O_t$ die Glieder elementefremd. Wir zerlegen die Summe (2) so in Teile, dass innerhalb jedes der Teile die Summierung über die Elemente eines bestimmen Orbits vorgenommen wird:

$$\sum_{m \in M} |G_m| = \sum_{m \in O_1} |G_m| + \sum_{m \in O_2} |G_m| + ... + \sum_{m \in O_t} |G_m|$$

Jedes der t Glieder auf der rechten Seite dieser Gleichung kann man folgendermaßen umformen:

$$\sum_{m \in O} |G_m| = \sum_{m \in O} \frac{|G|}{|O_m|} = \frac{|G|}{|O|} \sum_{m \in O} 1 = \frac{|G|}{|O|} |O| = |G|$$

Daher ist

$$\sum_{m \in M} |G_m| = \underbrace{|G| + ... + |G|}_{t} = t|G|$$

Somit haben wir bei der zweiten Art der Berechnung $t|G|$ markierte Punkte in der graphischen Darstellung. Da die bei beiden Arten erhaltenen Zahlen einander gleich sind, ergibt sich

$$t|G| = \sum_{\alpha \in G} \chi(\alpha) \qquad \text{d.h.} \qquad t = t(G) = \frac{1}{|G|} \sum_{\alpha \in G} \chi(\alpha)$$

Damit ist das Lemma bewiesen.

Ist insbesondere die Gruppe G transitiv, gilt also $t(G) = 1$, so ist nach dem Lemma von Burnside

$$|G| = \sum_{\alpha \in G} \chi(\alpha)$$

Aufgaben
1. Es sei G die Symmetriegruppe des Würfels. Man bestimme die Ordnung des Stabilisators eines Eckpunktes in dieser Gruppe. Welche Permutationen enthält er?

2. Man prüfe die Richtigkeit der Aussage des Lemmas von Burnside am Beispiel der Gruppe G von Beispiel 4 in Abschnitt 9 nach.

3. Permutationen α und β aus G heißen in G konjugierte Permutationen, wenn man in G eine Permutation γ finden kann derart, dass $\gamma^{-1} \circ \alpha \circ \gamma = \beta$ ist. Man beweise folgende Aussagen:
a) Jede Permutation ist zu sich selbst konjugiert;
b) ist α zu β konjugiert, so ist auch β zu α konjugiert;
c) ist α zu β konjugiert und β zu γ konjugiert, so ist α zu γ konjugiert.

4. Aus den Eigenschaften a), b) und c) von Aufgabe 3 folgt, dass sich die Menge G als Vereinigung durchschnittsfremder Teilmengen von Permutationen schreiben lässt, die paarweise zueinander konjugiert sind und die man Klassen konjugierter Elemente von Permutationen aus der Gruppe G nennt. Man beweise dies.

5. Sind die Permutationen α und β konjugiert, so gilt $\chi(\alpha) = \chi(\beta)$ d. h., die Funktion χ ist auf den Klassen konjugierter Elemente von G konstant.

6. Unter Benutzung von Aufgabe 5 zeige man, dass die Formel zur Bestimmung der Anzahl der Orbits einer Gruppe G in der Gestalt

$$t(G) = \frac{1}{|G|} \sum_{i=1}^{s} \chi_i \psi_i$$

geschrieben werden kann, wobei χ_i der gemeinsame Wert von $\chi(\alpha)$ für die Permutationen der i-ten Klasse konjugierter Permutationen, ψ_i die Anzahl der Permutationen in der i-ten Klasse von konjugierten Permutationen und s die Anzahl der Klassen konjugierter Permutationen ist.

7. Man beweise, dass konjugierte Permutationen den gleichen Typ besitzen.

8. Unter der Drehgruppe des Würfels verstehen wir diejenige Untergruppe seiner Symmetriegruppe, die aus allen möglichen Drehungen des Würfels um den Mittelpunkt oder die Symmetrieachsen besteht. Man zeige, dass sie transitiv ist, und bestimme mit Hilfe des Lemmas von Burnside ihre Ordnung.

9. Die Drehgruppe des Würfels definiert auf natürliche Weise eine Gruppe von Permutationen auf der Menge seiner Kanten. Man bestimme den Typ aller Permutationen dieser Gruppe.

10. Jede Drehung des Würfels permutiert auf natürliche Weise seine Seiten, d. h., die Drehgruppe des Würfels definiert eine Gruppe von Permutationen der Menge seiner Seiten. Man beweise, dass diese Gruppe transitiv ist. Man bestimme den Stabilisator eines der Punkte (einer Seite des Würfels) in dieser Gruppe.

12 Kombinatorische Aufgaben

Wir betrachten zwei einfache Beispiele, welche die Möglichkeiten der Anwendung des Lemmas von Burnside bei der Lösung kombinatorischer Abzählungsaufgaben verdeutlichen. Andere Beispiele findet der Leser in den Aufgaben zu diesem Abschnitt.

1. Färben der Eckpunkte eines Würfels. Auf wieviel Arten kann man die Eckpunkte eines Würfels mit drei Farben (etwa rot, blau und grün) färben?

Auf den ersten Blick könnte es scheinen, die Aufgabe sei ganz einfach. Da jeder der acht Eckpunkte auf dreierlei Weise gefärbt werden kann, unabhängig davon, wie die anderen Eckpunkte gefärbt sind, kann die Menge aller Eckpunkte des Würfels auf $3^8 = 6561$ verschiedene Arten gefärbt werden.
Bei diesem Herangehen an die Lösung der Aufgabe wird jedoch stillschweigend vorausgesetzt, man könne die Eckpunkte des Würfels vor dem Färben unterscheiden, d. h. beispielsweise, der Würfel sei starr befestigt oder seine Eckpunkte seien nummeriert.

Unter diesen Annahmen kann man die Antwort folgendermaßen interpretieren: Man kann die Ecken von 3^8 absolut gleichen, starr befestigten Würfeln so färben, dass sich sämtliche Würfel voneinander unterscheiden. Bei $3^8 + 1$ Würfeln geht dies schon nicht mehr.

Die Situation ändert sich wesentlich, wenn man auf die Voraussetzung verzichtet, die Würfel seien starr befestigt, weil man dann verschieden gefärbte Würfel so drehen kann, dass die Färbungen in der neuen Stellung übereinstimmen (vgl. Abb. 29).

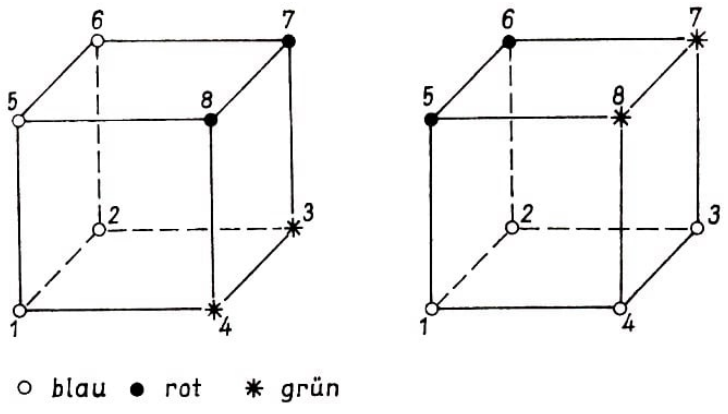


Abb. 29

Natürlich wird man zwei Würfel als in gleicher Weise gefärbt ansehen, wenn ihre Färbungen bis auf die Lage der Würfel im Raum, d. h. bis auf eine bestimmte Drehung eines der Würfel, übereinstimmen. Wir sagen, solche Färbungen der Würfel seien geometrisch nicht unterscheidbar. Daher ist die folgende Aufgabe eine natürliche Präzisierung der ursprünglichen Aufgabe:
Auf wieviel geometrisch verschiedene Arten kann man die Eckpunkte eines Würfels mit drei Farben färben?

Wir formulieren nun diese Aufgabe so um, dass ihr Zusammenhang mit dem Lemma von Burnside deutlich wird. Es sei M die Menge aller verschieden gefärbten gleichgroßen

Würfel deren Lage im Raum fixiert ist, also $|M| = 3^8$, und G die Gruppe aller Drehungen des Würfels, die aus 24 Permutationen besteht.
Die Gruppe G bestimmt auf natürliche Weise eine Gruppe von Permutationen auf der Menge M: Ist $\alpha \in G$ eine Drehung, so kann man jedem Würfel aus M einen bestimmten, im allgemeinen anderen Würfel zuordnen, der sich aus dem ersten durch die Drehung α ergibt. Diese Zuordnung ist offenbar eine Permutation auf der Menge M, die wir mit $\tilde{\alpha}$ bezeichnen.

Die Gruppe aller dieser Permutationen von M, welche durch Permutationen aus G bestimmt werden, wollen wir mit $\tilde{G}$ bezeichnen.
Offenbar ist $|G| = |\tilde{G}|$.

Dass zwei Würfel K_1 und K_2 aus M geometrisch gleich gefärbt sind, bedeutet dann, dass man einen von ihnen durch eine Drehung in eine Lage überführen kann, in der die Würfel nicht mehr verschieden sind.
Mit anderen Worten, es existiert eine Permutation $\tilde{\alpha} \in \tilde{G}$ derart, dass $(K_1)\tilde{\alpha} = K_2$ ist, d. h., K_1 und K_2 gehören zu ein und demselben Orbit der Gruppe $\tilde{G}$, die auf der Menge M wirkt. Somit muss man die Anzahl der Orbits der Gruppe $\tilde{G}$ auf M bestimmen, um die Anzahl der geometrisch verschiedenen Färbungen der Ecken des Würfels zu finden.

Wir nehmen an, die Eckpunkte der Würfel seien durch die Ziffern 1, 2, 3, 4, 5, 6, 7, 8 nummeriert; dann kann man jeden der 3^8 Würfel durch ein "Wort" aus acht Buchstaben eindeutig charakterisieren, von denen jeder entweder r oder b oder g ist.
Dass der i-te Buchstabe des Wortes r (bzw. b bzw. g) ist, bedeutet, dass der i-te Eckpunkt bei der gewählten Nummerierung rot (bzw. blau bzw. grün) gefärbt ist.

Beispielsweise erhalten wir für die in Abb. 29 dargestellten Würfel die Folgen $bbggbbrr$ bzw. $bbbbrrgg$. Die Permutationen aus der Gruppe $\tilde{G}$ permutieren diese Folgen.
Ist etwa $\alpha = (l, 2, 3, 4) \circ (5, 6, 7, 8) \in G$, so führt die Permutation $\tilde{\alpha}$ das Wort $bbbbbbbg$ in $bbbbgbbb$ und das Wort $bbggbbrr$ in $gbbgrbbr$ über, während die Wörter $bbbbbbbb$, $rrrrrrrr$, $gggggggg$ unverändert bleiben usw.
Es wäre sehr schwierig, die ganze Wertetabelle für die Permutation $\tilde{\alpha}$ aufzuschreiben, da sie aus 3^8 Zeilen besteht!

Um das Lemma von Burnside anwenden zu können, ist es notwendig, die Anzahl der Fixpunkte jeder Permutation aus $\tilde{G}$ zu bestimmen. Die Buchstabenfolge r, b, g wird für die Permutation $\tilde{\alpha} \in \tilde{G}$ dann und nur dann unverändert bleiben, wenn bei Zerlegung der entsprechenden Permutationen $\alpha \in G$ in ein Produkt von Zyklen die Würfelpunkte, deren Nummern in ein und demselben Zyklus stehen, mit ein und derselben Farbe gefärbt sind.

Ist etwa $\alpha = (1, 2, 3, 4) \circ (5, 6, 7, 8)$, so werden diejenigen Wörter bezüglich $\tilde{\alpha}$ unverändert bleiben, die ganz aus einem einzigen Buchstaben bestehen, sowie diejenigen Wörter, die aus zwei verschiedenen Buchstaben bestehen, wobei der eine an den ersten vier Stellen und der andere an den folgenden vier Stellen des Wortes steht.
Daher gibt es neun Fixpunkte der Permutation $\tilde{\alpha}$ auf der Menge M. An diesem Beispiel sieht man schon, dass die Berechnung der Anzahl der Fixpunkte der Permutationen aus $\tilde{G}$ stark vereinfacht wird, wenn die Zerlegungen der entsprechenden Permutationen aus

G in ein Produkt von Zyklen bekannt sind.

Wenn die Permutation $\alpha \in G$ in ein Produkt von k Zyklen zerlegt ist, so ist die Anzahl ihrer Fixpunkte gleich 3^k $(1 \le k \le 8)$. Daher beschreiben wir zunächst für alle Permutationen aus der Gruppe G der Drehungen des Würfels die Zerlegungen in ein Zyklenprodukt.

a) Um jede der drei Achsen, welche Mittelpunkte gegenüberliegender Seiten verbinden, existieren drei nichtidentische Drehungen um die Winkel $\pi/2$, π, $3\pi/2$. Ihnen entsprechen die Permutationen

$$(1,5,8,4)\circ(2,6,7,3),\quad (1,4,3,2)\circ(5,8,7,6),\quad (1,8)\circ(2,7)\circ(3,6)\circ(4,5),$$
$$(1,3)\circ(2,4)\circ(5,7)\circ(6,8),\quad (1,4,8,5)\circ(2,3,7,6),\quad (1,2,3,4)\circ(5,6,7,8),$$
$$(1,5,6,2)\circ(3,4,8,7),\quad (1,6)\circ(2,5)\circ(3,8)\circ(4,7),\quad (1,2,6,5)\circ(3,7,8,4)$$

b) Um jede der vier Diagonalen, d. h. der Achsen, welche gegenüberliegende Eckpunkte des Würfels verbinden, existieren zwei nichttriviale Drehungen. Ihnen entsprechen die Permutationen

$$(1)\circ(2,5,4)\circ(3,6,8)\circ(7),\quad (1)\circ(2,4,5)\circ(3,8,6)\circ(7),$$
$$(2)\circ(1,3,6)\circ(4,7,5)\circ(8),\quad (2)\circ(1,6,3)\circ(4,5,7)\circ(8),$$
$$(3)\circ(1,6,8)\circ(2,7,4)\circ(5),\quad (3)\circ(1,8,6)\circ(2,4,7)\circ(5),$$
$$(4)\circ(1,3,8)\circ(2,7,5)\circ(6),\quad (4)\circ(1,8,3)\circ(2,5,7)\circ(6)$$

c) Um jede der sechs Achsen, welche die Mittelpunkte gegenüberliegender Kanten verbinden, existiert eine einzige nichttriviale Drehung. Diesen Drehungen entsprechen die Permutationen

$$(1,5)\circ(2,8)\circ(3,7)\circ(4,6),\quad (1,7)\circ(2,6)\circ(3,5)\circ(4,8),$$
$$(1,2)\circ(3,5)\circ(4,6)\circ(7,8),\quad (1,7)\circ(2,8)\circ(3,4)\circ(5,6),$$
$$(1,7)\circ(2,3)\circ(4,6)\circ(5,8),\quad (1,4)\circ(2,8)\circ(3,5)\circ(6,7)$$

Zusammen mit der identischen Permutationen erhalten wir 24 Permutationen, und das sind alle Elemente der Gruppe G. Somit existieren in der Gruppe G der Drehungen des Würfels

eine Permutation vom Typ $\langle 1,1,1,1,1,1,1,1\rangle$,
sechs Permutationen vom Typ $\langle 4,4\rangle$,
neun Permutationen vom Typ $\langle 2,2,2,2\rangle$,
acht Permutationen vom Typ $\langle 1,1,3,3\rangle$.

Die Permutation vom ersten Typ hat 3^8 Fixpunkte, jede des zweiten Typs 3^2, jede des dritten und des vierten Typs 3^4 Fixpunkte. Daher erhalten wir nach dem Lemma von Burnside

$$t(\tilde{G}) = \frac{1}{24}(3^8 + 6\cdot 3^2 + 9\cdot 3^4 + 8\cdot 3^4) = 333$$

Somit gibt es 333 geometrisch verschiedene Arten des Färbens der Würfeleckpunkte mit drei Farben.

2. Zusammenstellung eines Armbands. Wieviel verschiedene Armbänder aus sieben

Glasperlen kann man aus roten und blauen Perlen zusammenstellen?

Um die Analogie dieser Aufgabe zu der vorhergehenden deutlich werden zu lassen, formulieren wir sie auf folgende äquivalente Weise um: Auf wieviel geometrisch verschiedene Arten kann man die Eckpunkte eines regelmäßigen Siebenecks mit zwei Farben färben?

Hier sind zwei Färbungsarten nicht unterscheidbar, wenn man die eine aus der anderen erhalten kann, indem man auf das Siebeneck Drehungen bzw. Spiegelungen bezüglich der Achsen, d. h. die Permutationen aus der Diedergruppe D_7 wirken lässt.
Wenn man die Eckpunkte des Siebenecks nummeriert, erhält man $2^7 = 128$ verschiedene Varianten ihrer Färbung, da man jeden Eckpunkt unabhängig von den anderen auf zwei Arten färben kann.

Wieder beschreiben wir die Färbung durch Wörter der Länge 7, die aus den Buchstaben r (rot gefärbte Ecke) und b (blau gefärbte Ecke) bestehen. Auf die Menge N aller solcher Wörter wirkt die Gruppe $\tilde{D}_7$ der Permutationen, die durch Permutationen aus D_7 gegeben sind.
Ist beispielsweise $\alpha = (1, 2, 3, 4, 5, 6, 7)$, so führt die Permutation α den letzten Buchstaben jedes Wortes in den Anfangsbuchstaben über, während alle anderen Buchstaben unverändert bleiben.

Um die Anzahl der Orbits der Gruppe $\tilde{D}_7$ auf der Menge N zu bestimmen, ist es notwendig, die Typen der Permutationen aus D_7 zu finden.
Diese Aufgabe ist viel einfacher als das analoge Problem für die Gruppe G aus Beispiel 1. Die Gruppe D_7 besteht aus den 14 Permutationen der Menge $\{1, 2, 3, 4, 5, 6, 7\}$, die sich nach den möglichen Typen folgendermaßen verteilen:

eine Permutation vom Typ $\langle 1, 1, 1, 1, 1, 1, 1\rangle$,
sechs Permutationen vom Typ $\langle 7\rangle$,
sieben Permutationen vom Typ $\langle 1, 2, 2, 2\rangle$.

Ein Wort ist bezüglich der Permutation $\tilde{\alpha} \in \tilde{D}_7$ dann und nur dann unveränderlich, wenn die Buchstaben, die an den Stellen mit den Nummern aus einem Zyklus in der Permutation es stehen, übereinstimmen. Daher hat die identische Permutation 2^7 Fixpunkte auf N, die Permutationen des zweiten Typs haben 2, die Permutationen des dritten Typs 2^4 Fixpunkte.
Wenden wir das Lemma von Burnside an, so erhalten wir

$$t(\tilde{D}_7) = \frac{1}{14}(2^7 + 6 \cdot 2 + 7 \cdot 2^4) = 18$$

Somit kann man aus Glasperlen zweier Farben 18 Armbänder zu je sieben Perlen zusammenstellen.

Aufgaben
1. Die Seiten eines Würfels kann man färben: a) alle weiß, b) alle schwarz, c) einen Teil weiß und die übrigen schwarz. Wieviel verschiedene Färbungsmöglichkeiten gibt es?

2. Wieviel verschiedene Armbänder kann man aus zwei blauen, zwei weißen und zwei

roten Perlen zusammenstellen?

3. Auf wieviel geometrisch verschiedene Arten können sich drei absolut gleiche Fliegen in die Ecken eines regelmäßigen Fünfecks setzen?

4. Der bereits früher benutzte Begriff des Graphen ist einer der Grundbegriffe der modernen angewandten Mathematik. In einer genügend allgemeinen Situation kann man einen (gerichteten) Graphen als System von Punkten der Ebene definieren, von denen einige durch Pfeile verbunden sind.
Die Punkte heißen die Knotenpunkte und die Pfeile die Bögen des Graphen. Es werden auch nichtorientierte Graphen betrachtet, d. h. Graphen, deren Bögen keinen Richtungssinn besitzen. Wieviel orientierte Graphen mit drei Knotenpunkten gibt es?

5. Wieviel verschiedene nichtorientierte Graphen mit vier Knotenpunkten gibt es?

6. Auf wieviel Arten kann man die Ecken eines Würfels mit zwei Farben so färben, dass gleichviel Ecken jeder Farbe vorhanden sind?

7. Auf wieviel verschiedene Arten kann man die Seiten eines Würfels mit vier Farben färben?

13 Wirkung von Permutationen auf Polynome

Wir erinnern daran, dass ein Polynom eine Summe von Monomen ist. Kommen in allen Monomen eines Polynoms f nur die Symbole $x_1, x_2, ..., x_n$ vor, so bezeichnet man das Polynom mit $f(x_1, x_2, ..., x_n)$ und nennt es ein Polynom in n Veränderlichen.
Beispielsweise ist

$$f(x_1, x_2) = x_1^2 x_2 + 2x_1 x_2 + 5x_1$$

ein Polynom in zwei Veränderlichen und

$$g(x_1, x_2, x_3) = 2x_1^2 x_2 x_3^3 + 5x_1^2 x_2 + 6x_3$$

ein Polynom in drei Veränderlichen.

Es sei $f(x_1, x_2, ..., x_n)$ ein Polynom in n Veränderlichen und $M = \{1, 2, ..., n\}$ die Menge der Indizes der Veränderlichen.
Für eine beliebige Permutation $\sigma \in S_n$ definieren wir die Wirkung von σ auf $f(x_1, x_2, ..., x_n)$, indem wir

$$(f(x_1, x_2, ..., x_n))^\sigma = f^\sigma(x_1, x_2, ..., x_n) = f(x_{(1)\sigma}, x_{(2)\sigma}, ..., x_{(n)\sigma})$$

setzen.

Beispiel 1. a) Ist

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 x_4^2 + x_1^2 x_2 x_3 x_4 + x_1 + x_2 + 1$$

und

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

so ist

$$f^\sigma(x_1, x_2, x_3, x_4) = x_2 x_3 x_1 x_4^2 + x_2^2 x_3 x_1 x_4 + x_2 + x_3 + 1$$

b) Für das Polynom

$$g(x_1, x_2, x_3, x_4) = x_1^3 x_2 x_3 x_4 + x_1 x_2^3 x_3 x_4 + x_1 x_2 x_3^3 x_4$$

und die Permutation σ aus Beispiel a) ist

$$g^\sigma(x_1, x_2, x_3, x_4) = x_2^3 x_3 x_1 x_4 + x_2 x_3^3 x_1 x_4 + x_2 x_3 x_1^3 x_4 = g(x_1, x_2, x_3, x_4)$$

Aus diesem Beispiel ersieht man, dass sich das Polynom $f^\sigma(x_1, x_2, ..., x_n)$ von $f(x_1, x_2, ..., x_n)$ unterscheiden, aber auch mit ihm übereinstimmen kann.

Ist $f^\sigma(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$, so sagt man, das Polynom f ändere sich unter Einwirkung der Permutation σ nicht, oder es sei bezüglich der Operation σ invariant. Selbstverständlich ist jedes Polynom in n Variablen bezüglich der identischen Permutation invariant:

$$f^\varepsilon(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$$

Da die Multiplikation zweier Permutationen ihre Hintereinanderausführung bedeutet, gilt für jedes Polynom $f(x_1, x_2, ..., x_n)$ und beliebige Permutationen σ, τ die Beziehung

$$((f^{\varepsilon}(x_1, x_2, ..., x_n))^{\sigma})\tau = f^{\sigma\circ\tau}(x_1, x_2, ..., x_n)$$

Somit ist ein Polynom $f(x_1, x_2, ..., x_n)$, das sich unter Einwirkung von τ und von σ nicht ändert, auch bezüglich des Produktes $\sigma \circ \tau$ invariant. Außerdem ist jedes Polynom $f(x_1, x_2, ..., x_n)$, das bezüglich σ invariant ist, auch bezüglich der Permutation σ^{-1} invariant.
Daher bildet die Menge aller Permutationen, die ein gegebenes Polynom $f(x_1, x_2, ..., x_n)$ nicht ändern, eine Gruppe, diese Gruppe wird die Trägheitsgruppe des Polynoms $f(x_1, x_2, ..., x_n)$ genannt.

Beispiel 2. Wir bestimmen die Trägheitsgruppe des Polynoms

$$A(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

Es ist

$$\begin{aligned}
A^{(1,2)}(x_1, x_2, x_3) &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -A(x_1, x_2, x_3)\\
A^{(2,3)}(x_1, x_2, x_3) &= (x_1 - x_3)(x_1 - x_2)(x_3 - x_2) = -A(x_1, x_2, x_3)\\
A^{(1,3)}(x_1, x_2, x_3) &= (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = -A(x_1, x_2, x_3)\\
A^{(1,2,3)}(x_1, x_2, x_3) &= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = A(x_1, x_2, x_3)\\
A^{(1,3,2)}(x_1, x_2, x_3) &= (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = A(x_1, x_2, x_3)
\end{aligned}$$

Die Trägheitsgruppe des Polynoms $A(x_1, x_2, x_3)$ ist somit die Menge $\{\varepsilon, (1, 2, 3), (1, 3, 2)\}$.

An diesem Beispiel ist zu erkennen, dass das Polynom $A(x_1, x_2, x_3)$ unter Einwirkung einer beliebigen Transposition sein Vorzeichen ändert. Dieses Ergebnis lässt sich auf Polynome dieser Gestalt mit mehr als drei Veränderlichen verallgemeinern.

Das Polynom $A(x_1, x_2, x_3)$ ist ein Produkt von Differenzen $x_i - x_j$ für $i < j$, $i, j = 1, 2, 3$. Daher hat ein derartiges Polynom in n Veränderlichen die Gestalt

$$\begin{aligned}
A(x_1, x_2, ..., x_n) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)...(x_1 - x_n)\\
\cdot (x_2 - x_3)(x_2 - x_4)...(x_2 - x_n)\\
\cdot (x_3 - x_4)...(x_3 - x_n) \cdot ... \cdot (x_{n-1} - x_n)
\end{aligned}$$

Es enthält $(n-1) + (n-2) + ... + 1 = n(n-1)/2$ Faktoren. Es sei (i, j), $i < j$, eine beliebige Transposition. Sie wirkt nur auf diejenigen Faktoren $x_k - x_l$, $k < l$, in denen wenigstens einer der Indizes k, l mit i oder j übereinstimmt.
Unter Einwirkung der Transposition (i, j) kehrt sich das Vorzeichen des Faktors $x_i - x_j$ um:

$$(x_i - x_j)^{(i,j)} = x_j - x_i = -(x_i - x_j)$$

Für die anderen Faktoren, die sich unter Einwirkung der Transposition (i, j) ändern, gilt:

a) Für $i, j < k$ wird $x_i - x_k$ in $x_j - x_k$ übergeführt und umgekehrt, ohne dass sich das Vorzeichen ändert;

b) für $i, j > k$ wird $x_k - x_i$ in $x_k - x_j$ übergeführt und umgekehrt, ohne dass sich das Vorzeichen ändert;

c) für $i < k < j$ wird $x_i - x_k$ in $x_j - x_k = -(x_k - x_j)$ und $x_k - x_j$ in $x_k - x_i = -(x_i - x_k)$ übergeführt, d. h., das Produkt $(x_i - x_k)(x_k - x_j)$ ändert unter Einwirkung der Transposition (i, j) sein Vorzeichen nicht.

Folglich ändert das Produkt aller von $x_i - x_j$ verschiedenen Faktoren des Polynoms $A(x_1, x_2, ..., x_n)$ unter Einwirkung der Transposition (i, j) das Vorzeichen nicht, während der Faktor $x_i - x_j$ sein Vorzeichen umkehrt. Daher ändert auch das Produkt aller Faktoren - das Polynom $A(x_1, x_2, ..., x_n)$ - das Vorzeichen:

$$A^{(i,j)}(x_1, x_2, ..., x_n) = -A(x_1, x_2, ..., x_n)$$

Weil jede Permutation in ein Produkt von Transpositionen zerlegbar ist, kann das Polynom $A(x_1, x_2, ..., x_n)$ unter Einwirkung einer beliebigen Permutation höchstens das Vorzeichen ändern. Daher nennt man dieses Polynom das alternierende Polynom in n Veränderlichen.

Es sei $f(x_1, x_2, ..., x_n)$ ein Polynom. Wenn wir auf dieses Polynom alle möglichen Permutationen aus S_n einwirken lassen, erhalten wir im allgemeinen ein System verschiedener Polynome:

$$f_1(x_1, x_2, ..., x - n), f_2(x_1, x_2, ..., x - n), ..., f_s(x_1, x_2, ..., x - n)$$

Das Polynom $f(x_1, x_2, ..., x_n)$ selbst kommt natürlich in dieser Folge vor, da $f^\varepsilon = f$ gilt.
Das Polynom

$$f_1(x_1, x_2, ..., x - n) + f_2(x_1, x_2, ..., x - n) + ... + f_s(x_1, x_2, ..., x - n)$$

wollen wir das Orbitalpolynom von $f(x_1, x_2, ..., x_n)$ nennen. Das Orbitalpolynom ist, wie man leicht sieht, bezüglich jeder Permutation aus S_n invariant.

Beispiel 3. a) Für das Monom x_1^k ist das Orbitalpolynom in n Veränderlichen das Polynom

$$s_k = x_1^k + x_2^k + ... + x_n^k$$

Solche Polynome werden Potenzsummen in n Veränderlichen genannt. Insbesondere sind die Polynome

$$s_1 = x_1 + x_2, \quad s_2 = x_1^2 + x_2^2, \quad s_3 = x_1^3 + x_2^3$$

Potenzsummen in zwei Veränderlichen.

b) Für das Monom $x_1^2 x_2^3 x_3$ erhält man als Orbitalpolynom in drei Veränderlichen das Polynom

$$x_1^2 x_2^3 x_3 + x_1^2 x_2 x_3^3 + x_1^3 x_2^2 x_3 + x_1 x_2^3 x_3^2 + x_1^3 x_2 x_3^2 + x_1 x_2^2 x_3^3$$

Das Orbitalpolynom in n Veränderlichen für das Monom $x_1^{l_1}x_2^{l_2}...x_s^{l_s}$ bezeichnen wir mit $o_n(x_1^{l_1}x_2^{l_2}...x_s^{l_s})$. Beispielsweise ist

$$o_2(x_1x_2^2) = x_1x_2^2 + x_1^2x_2$$
$$o_3(x_1x_2^2) = x_1x_2^2 + x_1x_3^2 + x_1^2x_2 + x_1^2x_3 + x_2x_3^2 + x_2^2x_3$$

Man kann sich leicht davon überzeugen, dass für jedes n das Polynom $o_n(x_1^kx_2^l)$ durch Potenzsummen ausgedrückt werden kann. Wir verifizieren dies für den Fall $n = 3$.
Es ist

$$\begin{aligned} s_ks_l &= (x_1^k + x_2^k + x_3^k)(x_1^l + x_2^l + x_3^l) \\ &= (x_1^{k+l} + x_2^{k+l} + x_3^{k+l} + x_1^kx_2^l + x_1^kx_3^l + x_1^lx_2^k + x_2^kx_3^l + x_1^lx_3^k + x_2^lx_3k \\ &= s_{k+l} + o_3(x_1^kx_2^l) \end{aligned}$$

Somit ist $o_3(x_1^lx_2^l) = s_ks_l - s_{k+l}$.
Interessant ist das Problem, die Anzahl der Glieder in einem Orbitalpolynom zu bestimmen. Offenbar kann die Anzahl der Monome im Polynom $o_n(x_1^{l_1}x_2^{l_2}...x_s^{l_s})$ die Zahl $n!$ nicht übertreffen. Die maximale Anzahl von Monomen wird nur dann erreicht, wenn alle Veränderlichen in jedem Monom mit verschiedenen Exponenten vorkommen; wenn jedoch Exponenten der Veränderlichen in einem Monom übereinstimmen, wird ihre Anzahl kleiner als die Maximalzahl sein.

Aufgaben

1. Es sei $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ und f eines der Polynome

a) $x_1x_2^2x_3x_4^2 + 2x_1^2x_2xs_3x_4 + 3x_1x_2^2$;
b) $x_1^2x_2^2x_3x_4 + x_1^2 + x_3$;
c) $x_1^2 + x_2^2 + x_3 + x_4$.
Man bestimme f^σ.

2. Man bestimme die Trägheitsgruppe des Polynoms

$$f(x_1, x_2, x_3, x_4) = x_1^3x_2x_3^2x_4 + 2x_1^2x_2x_3^3x_4 + 5x_1 + 3x_2 + 1$$

3. Aus wieviel Permutationen besteht die Trägheitsgruppe des Polynoms $A(x_1, x_2, x_3, x_4)$?

4. Man beweise: Zu jeder Gruppe von Permutationen existiert ein Polynom, für welches diese Gruppe Trägheitsgruppe ist.

5. Wieviel Monome enthält das Polynom $o_4(x_1^2x_2x_3^2x_4)$? Man schreibe dieses Polynom auf.

6. Man beweise, dass sich das Polynom $o_n(x^kx^l)$ für jedes n durch Potenzsummen ausdrücken lässt.

7. Wieviel Monome enthält ein Polynom der Gestalt $o_n(x_1x_2...x_l)$ für verschiedene n und l?

14 Gerade und ungerade Permutationen. Die alternierende Gruppe

Die Zerlegung von Permutationen aus S_n in ein Produkt von Transpositionen ist im allgemeinen nicht eindeutig; so gilt beispielsweise

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

Trotzdem kann man eine bestimmte Eigenschaft angeben, die für jede dieser Zerlegungen dieselbe ist. Diese Eigenschaft ist die Parität der Anzahl der Faktoren in der Zerlegung, d. h., die Tatsache, dass die Anzahl der Faktoren bei allen Zerlegungen entweder immer eine gerade oder immer eine ungerade Zahl ist.
Es gilt nämlich folgender wichtiger Satz:

Satz. Sind $\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_s$ und $\beta_1 \circ \beta_2 \circ ... \circ \beta_t$ Zerlegungen einer Permutation in ein Produkt von Transpositionen, so haben die Zahlen s und t die gleiche Parität, d. h., sie sind beide gerade oder beide ungerade.

Beweis. Es sei φ eine Permutation der Menge $M = \{1, 2, ..., n\}$, und $\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_s$ sowie $\beta_1 \circ \beta_2 \circ ... \circ \beta_t$ seien Zerlegungen von φ in ein Produkt von Transpositionen.
Wir lassen φ auf das alternierende Polynom $A(x_1, x_2, ..., x_n)$ einwirken. Wie im vorhergehenden Abschnitt bewiesen wurde, können sich A und A^φ nur um das Vorzeichen unterscheiden, wobei für jede Transposition α die Beziehung $A^\alpha = -A$ gilt. Wir betrachten die beiden Polynomfolgen

$$A, A^{\alpha_1} = F_1, F_1^{\alpha_2} = F_2, ..., F_{s-1}^{\alpha_s} = F_s$$
$$A, A^{\beta_1} = G_1, G_1^{\beta_2} = G_2, ..., G_{t-1}^{\beta_t} = G_t$$

In jeder dieser Folgen unterscheiden sich zwei benachbarte Ausdrücke nur durch das Vorzeichen ; daher gilt

$$F_s = (-1)^s A \qquad , \qquad G_t = (-1)^t A$$

Andererseits ist $F_s = G_t = A^\varphi$, also $(-1)^s A = (-1)^t A$, d. h. aber, s und t sind Zahlen gleicher Parität.
Jetzt können wir folgende Definition aussprechen:

Eine Permutation heißt gerade, wenn sie sich in ein Produkt einer geraden Anzahl von Transpositionen zerlegen lässt. Andernfalls heißt die Permutation ungerade.

Somit sind genau diejenigen Permutationen gerade, die das alternierende Polynom $A(x_1, x_2, ..., x_n)$ unverändert lassen. Wir bezeichnen nun die Menge aller geraden Permutationen aus S_n mit A_n und die Menge aller ungeraden Permutationen aus S_n mit B_n. Nach dem soeben bewiesenen Satz liegt jede Permutation $\varphi \in S_n$ in genau einer dieser Mengen, so dass A_n und B_n keine gemeinsamen Elemente besitzen.

Nun zeigen wir, dass die Mengen A_n und B_n aus der gleichen Anzahl von Permutationen bestehen, d. h., dass

$$|A_n| = |B_n| \tag{1}$$

gilt. Zu diesem Zweck konstruieren wir eine eineindeutige Abbildung Ψ von A_n auf B_n. Wir greifen eine gewisse Transposition α heraus und ordnen jedem Element $\omega \in A_n$ die Permutation $\omega \circ \alpha$ zu:

$$\Psi : \omega \to \omega \circ \alpha$$

Die Permutationen ω und $\omega \circ \alpha$ sind von verschiedener Parität (d. h. nicht beide zugleich gerade bzw. ungerade), d.h., $\omega \circ \alpha$ gehört zu B_n, und die Abbildung Ψ ist korrekt definiert.

Jetzt überzeugen wir uns davon, dass Ψ bijektiv ist. Gehören β, γ zu A_n und ist $\beta \neg \gamma$, so ist auch $\beta \circ \alpha \neq \gamma \circ \alpha$, weil die Gleichung $\beta \circ \alpha = \gamma \circ \alpha$ durch α gekürzt werden könnte und demnach entgegen der Annahme $\beta = \gamma$ wäre.

Zu jeder Permutation $\beta \in B_n$ existiert eine Permutation $\alpha \in A_n$, nämlich $\gamma = \beta \circ \alpha^{-1} = \beta \circ \alpha$ derart, dass $\Psi(\gamma) = \beta$ ist.
Folglich ist die Abbildung Ψ sowohl injektiv als auch surjektiv. Daraus folgt, dass die Gleichheit (1) besteht.

Jede Transposition ist eine ungerade Permutation. Die Zerlegung eines Zyklus in ein Produkt von Transpositionen zeigt, dass ein Zyklus ungerader Länge eine gerade Permutation ist. Die identische Permutation ist ebenfalls gerade. Offenbar ist das Produkt gerader Permutationen eine gerade Permutation; das Produkt zweier ungerader Permutationen ist ebenfalls gerade, während das Produkt einer geraden und einer ungeraden Permutation (bzw. einer ungeraden und einer geraden) ungerade ist.

Ist eine Permutation φ in ein Produkt von Transpositionen zerlegt,

$$\varphi = \delta_1 \circ \delta_2 \circ ... \circ \delta_{s-1} \circ \delta_s$$

so besitzt die Inverse von φ die Gestalt

$$\varphi^{-1} = \delta_s \circ \delta_{s-1} \circ ... \circ \delta_2 \circ \delta_1$$

denn aus der Gleichung

$$(\delta_1 \circ \delta_2 \circ ... \circ \delta_{s-1} \circ \delta_s) \circ (\delta_s \circ \delta_{s-1} \circ ... \circ \delta_2 \circ \delta_1) = \varepsilon$$

folgt

$$\varphi^{-1} = \delta_s^{-1} \circ \delta_{s-1}^{-1} \circ ... \circ \delta_2^{-1} \circ \delta_1^{-1}$$

und für Transpositionen gilt $\delta_i^{-1} = \delta_i$.

Daraus ergibt sich, dass die Menge A_n eine Untergruppe der Gruppe S_n bildet. Diese Untergruppe wird alternierende Gruppe von Permutationen genannt. Sie spielt in der Theorie der Permutationsgruppen und ihren Anwendungen eine wichtige Rolle.

Wir weisen darauf hin, dass man die Parität von Permutationen auch bestimmen kann, ohne die Permutation in ein Produkt von Transpositionen zu zerlegen. Es genügt, die Permutation in ein Produkt von Zyklen zu zerlegen und die Anzahl der Zyklen gerader Länge zu bestimmen. Ist diese Anzahl gerade, so ist die Permutation gerade,

anderenfalls ist sie ungerade (vgl. Aufgabe 11).

Aufgaben 1. Welche charakteristische Besonderheit besitzt der Graph einer geraden Permutation?

2. Welche höchste Ordnung können Elemente der Gruppe A_5 haben?

3. Man stelle die Multiplikationstabelle der Gruppe A_4 auf.

4. Welche der von uns in Abschnitt 8 beschriebenen Untergruppen von S_3 ist die alternierende?

5. Man bestimme das Zentrum der Gruppe A_n (vgl. Abschnitt 8, Aufgabe 4).

6. Man beweise, dass A_n eine von S_n verschiedene maximale Untergruppe von S_n ist, d. h., dass jede Untergruppe, die A_n enthält, entweder mit A_n oder mit S_n übereinstimmt.

7. Man beweise, dass sich jede gerade Permutation in ein Produkt von Zyklen der Länge 3 zerlegen lässt.

8. Kann man jede gerade Permutation aus S_n für ungerades n in ein Produkt der Zyklen $(1,2,3)$, $(1,4,5)$, ..., $(1,n-1,n)$ zerlegen?

9. Man sagt, das Zahlenpaar i,j bilde eine Inversion, wenn $i>j$ ist. Man beweise, dass die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$$

dann und nur dann gerade ist, wenn die Anzahl der Inversionen, welche von Elementen der zweiten Zeile gebildet werden, gerade ist.

10. Wieviel Permutationen aus S_{10} gibt es, in denen die Elemente der zweiten Zeile genau sechs Inversionen bilden?

11. Es sei $\langle k_1, k_2, ..., k_s\rangle$ der Typ einer Permutation $\varphi \in S_n$. Die Differenz $n-s$ wird Dekrement dieser Permutation genannt. Man beweise, dass die Parität einer Permutation mit der ihres Dekrementes übereinstimmt (d. h., dass die Permutation und das Dekrement zugleich gerade bzw. ungerade sind).

15 Symmetrische und geradsymmetrische Polynome

Ein Polynom $f(x_1, x_2, ..., x_n)$ heißt symmetrisch, wenn es bezüglich der Einwirkung jeder Permutation aus S_n invariant ist, d. h., wenn die Trägheitsgruppe dieses Polynoms die gesamte symmetrische Gruppe S_n ist.

Beispielsweise sind folgende Polynome in n Veränderlichen symmetrisch:

$$\begin{aligned}
\sigma_1(x_1, x_2, ..., x_n) &= x_1 + x_2 + ... + x_n \\
\sigma_2(x_1, x_2, ..., x_n) &= x_1x_2 + x_1x_3 + ... + x_{n-1}x_n \\
\sigma_3(x_1, x_2, ..., x_n) &= x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n \\
&... \\
\sigma_n(x_1, x_2, ..., x_n) &= x_1x_2...x_n
\end{aligned}$$

Das Orbitalpolynom jedes Monoms ist nämlich symmetrisch, und es ist

$$\begin{aligned}
\sigma_1(x_1, x_2, ..., x_n) &= o_n(x_1) \\
\sigma_2(x_1, x_2, ..., x_n) &= o_n(x_1x_2) \\
&... \\
\sigma_n(x_1, x_2, ..., x_n) &= o_n(x_1x_2...x_n)
\end{aligned}$$

Die Polynome $\sigma_1, \sigma_2, ..., \sigma_n$ werden elementarsymmetrische Polynome genannt. Wir schreiben sie für $n = 2$ und $n = 3$ vollständig auf:

$$\begin{aligned}
\sigma_1(x_1, x_2) &= x_1 + x_2, \qquad \sigma_2(x_1, x_2) = x_1x_2 \\
\sigma_1(x_1, x_2, x_3) &= x_1 + x_2 + x_3, \qquad \sigma_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3, \\
\sigma_3(x_1, x_2, x_3) &= x_1x_2x_3
\end{aligned}$$

Man sieht unmittelbar, dass a) die Summe von symmetrischen Polynomen wieder ein symmetrisches Polynom und b) das Produkt symmetrischer Polynome ebenfalls ein symmetrisches Polynom ist.
Daher erhalten wir, wenn wir in ein beliebiges Polynom $g(y_1, y_2, ..., y_n)$ in n Veränderlichen anstelle von y_1, y_2, ..., y_n die elementarsymmetrischen Polynome $\sigma_1, \sigma_2, ..., \sigma_n$ einsetzen, ein Polynom in $x_1, x_2, ..., x_n$ das symmetrisch ist.
Wenn beispielsweise

$$g(y_1, y_2) = y_1^2y_2 + 5y_2 + 2$$

ist, ergibt sich

$$g(\sigma_1, \sigma_2) = (x_1 + x_2)^2x_1x_2 + 5x_1x_2 + 2 = x_1^3x_2 + 2x_1x_2 + x_1x_2^3 + 5x_1x_2 + 2$$

und das ist ein symmetrisches Polynom.

Man kann zeigen, dass man jedes symmetrische Polynom auf diese Weise erhalten kann.

Satz. Jedes symmetrische Polynom ist ein Polynom in elementarsymmetrischen Polynomen.

Das ist der sogenannte Hauptsatz über symmetrische Polynome. Wir beweisen ihn nur für Polynome in drei Veränderlichen. An diesem Spezialfall können wir die einzelnen Schritte des Beweises im allgemeinen Fall erkennen.
Offenbar ist jedes symmetrische Polynom in beliebig vielen Veränderlichen die Summe von Orbitalpolynomen. Daher genügt es für den Beweis des Satzes im Fall $n = 3$, sich davon zu überzeugen, dass die Polynome der Gestalt $o_3(x_1^k)$, $o_3(x_1^k x_2^l)$, $o_3(x_1^k x_2^l x_3^m)$ als Polynome in $\sigma_1, \sigma_2, \sigma_3$ dargestellt werden können.

1. Wir überzeugen uns mit Hilfe vollständiger Induktion über k davon, dass sich jede Potenzsumme $s_k := x_1^k + x_2^k + x_3^k$ durch elementarsymmetrische Polynome ausdrücken lässt:
$s_1 = x_1 + x_2 + x_3$ stimmt mit σ_1 überein,

$$s_2 = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2$$
$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

Wir drücken nun s_k für ein beliebiges k durch Polynome s_i, $i < k$, aus. Es ist

$$\sigma_1 s_{k-1} = (x_1 + x_2 + x_3)(x_1^{k-1} + x_2^{k-1} + x_3^{k-1}) = s_k + o_3(x^{k-1}x_2)$$

Daraus folgt

$$s_k = \sigma_1 s_{k-1} - o_3(x_1^{k-1}x_2)$$

Analog ist

$$\sigma_2 s_{k-2} = o_3(x_1^{k-1}x_2) + o_3(x_1^{k-2}x_2x_3) \qquad , \qquad \sigma_3 s_{k-3} = o_3(x_1^{k-2}x_2x_3)$$

Wenn wir aus den letzten beiden Gleichungen das Polynom $o_3(x_1^{k-1}x_2)$ bestimmen und es in die vorhergehende einsetzen, erhalten wir

$$s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2} + \sigma_3 s_{k-3}$$

Nach Induktionsannahme lassen sich die Potenzsummen $s_{k-1}, s_{k-2}, s_{k-3}$ als Polynome in elementarsymmetrischen Polynomen schreiben; daher kann man auch die Summe s_k mit ihrer Hilfe ausdrücken.

2. In Abschnitt 13 wurde bewiesen, dass jedes Orbitalpolynom der Gestalt $o_3(x_1^k x_2^l)$ durch eine Potenzsumme ausgedrückt werden kann. Nach dem soeben Bewiesenen kann man also $o_3(x_1^k x_2^l)$ in Gestalt eines Polynoms in elementarsymmetrischen Polynomen darstellen.

3. Es sei $o_3(x_1^k x_2^l x_3^m)$ ein Orbitalpolynom und etwa m die kleinste der Zahlen k, l, m. Dann ist

$$o_3(x_1^k x_2^l x_3^m) = x_1^m x_2^m x_3^m (x_1^{k-m} x_2^{l-m}) = \sigma_3^m o_3(x_1^{k-m} x_2^{l-m})$$

Nun ist aber $o_3(x_1^{k-m} x_2^{l-m})$ Orbitalpolynom eines Monoms mit einer kleineren Anzahl von Veränderlichen, d.h., dieser Fall reduziert sich auf den vorhergehenden.

Der Hauptsatz über symmetrische Polynome ist damit für $n = 3$ bewiesen. Für $n = 2$

ist der Beweis ganz analog, aber bedeutend einfacher. Wir schlagen dem Leser vor, diesen Beweis selbständig zu führen.

Wir betrachten einige Beispiele für die Anwendung des Hauptsatzes über symmetrische Polynome.

1. Man bestimme die Lösungen des Systems

$$x + xy + y = 7 \qquad , \qquad x^2 + xy + y^2 = 13 \tag{1}$$

Wir drücken die symmetrischen Polynome auf den linken Seiten dieser Gleichungen durch $\sigma_1 = x + y$ und $\sigma_2 = xy$ aus und führen die neuen Unbekannten $u = x + y$, $v = xy$ ein. Dann erhalten wir das Hilfssystem

$$u + v = 7 \qquad , \qquad u^2 - v = 13$$

dieses besitzt die beiden Lösungen $u = -5, v = 12$; $u = 4, v = 3$.
Das bedeutet, dass die Lösungsmenge des Ausgangssystems (1) die Vereinigung der Lösungsmengen der folgenden beiden Systeme ist:

$$\begin{aligned} x + y &= -5 \qquad , \qquad xy = 12 \\ x + y &= 4 \qquad , \qquad xy = 3 \end{aligned}$$

Die Lösungsmenge des ersten Systems ist leer, die des zweiten besteht aus $(1; 3)$, $(3; 1)$. Folglich ist Lösungsmenge des Ausgangssystems (1)

$$\varnothing \cup \{(1; 3), (3; 1)\} = \{(1; 3), (3; 1)\}$$

2. Man zeige, dass für $a + b + c = 0$ die Identität

$$a^3 + b^3 + c^3 = 3abc$$

gilt.
Wir drücken das symmetrische Polynom $a^3 + b^3 + c^3 - 3abc$ durch die elementarsymmetrischen Polynome $\sigma_1 = a + b + c$, $\sigma_2 = ab + ac + bc$, $\sigma_3 = abc$ aus.

Wie schon beim Beweis des Satzes über symmetrische Polynome hergeleitet wurde, ist das Polynom von $\sigma_1, \sigma_2, \sigma_3$, welches mit der Summe $s_3 = a^3 + b^3 + c^3$ übereinstimmt, das Polynom $\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Daher erhalten wir

$$a^3 + b^3 + c^3 - 3abc = \sigma_1^3 + 3\sigma_1\sigma_2 + 3\sigma_3 - 3\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2$$

Da nach Voraussetzung $\sigma_1 = 0$ gilt, ist auch $a^3 + b^3 + c^3 - 3abc$ gleich 0, woraus die Richtigkeit der zu beweisenden Identität folgt.

3. Man stelle eine quadratische Gleichung mit den Wurzeln x_1, x_2 auf, wenn

$$x_1 + x_2 = 2 \qquad , \qquad x_1^4 + x_2^4 = 82$$

gilt.

Eine solche Gleichung lässt sich unter Benutzung des Vietaschen Wurzelsatzes aufstellen. Zu diesem Zweck muss man feststellen, welchen Wert das Produkt der Wurzeln hat.

Wenn man $x_1^4+x_2^4=s_4$ durch elementarsymmetrische Polynome ausdrückt, ergibt sich $s_4=\sigma_1^4-4\sigma_1^2\sigma_2+2\sigma_2^2$. Setzt man in diese Gleichung die Werte von s_4 und σ_1 ein, so erhält man eine quadratische Gleichung für σ_2:

$$2\sigma_2^2-16\sigma_2+66=0$$

Daraus folgt $\sigma_2^{(1)}=11$, $\sigma_2^{(2)}=-3$. Folglich leisten die Gleichungen

$$x^2-2x+11=0 \qquad , \qquad x^2-2x-3=0$$

das Gewünschte.

Außer mit symmetrischen Polynomen hat man es oft mit geradsymmetrischen Polynomen zu tun. Polynome werden geradsymmetrisch genannt, wenn sie bezüglich aller geraden Permutationen invariant sind.
Folglich muss die Trägheitsgruppe eines geradsymmetrischen Polynoms die alternierende Gruppe enthalten. Da in der symmetrischen Gruppe S_2 nur die identische Permutation gerade ist, ist jedes Polynom in zwei Veränderlichen geradsymmetrisch, d. h., in diesem Fall ist der Begriff Geradsymmetrie überflüssig.

Doch schon unter den Polynomen mit drei Veränderlichen gibt es solche, die nicht geradsymmetrisch sind, etwa $x_1+2x_2+3x_3$ (die Trägheitsgruppe dieses Polynoms ist die nur aus dem neutralen Element bestehende Gruppe).

Offenbar ist jedes symmetrische Polynom geradsymmetrisch, doch gilt das Umgekehrte nicht. Beispielsweise ist das alternierende Polynom $A(x_1,x_2,...,x_n)$ für jedes n geradsymmetrisch, aber nicht symmetrisch.
Insbesondere ist jedes Polynom, das unter Einwirkung irgendeiner Transposition das Vorzeichen wechselt, geradsymmetrisch. Polynome mit dieser Eigenschaft werden antisymmetrisch genannt.

Wie in Abschnitt 13 bewiesen wurde, ist das Polynom $A(x_1,x_2,...,x_n)$ antisymmetrisch. Ganz klar ist auch, dass das Produkt eines symmetrischen Polynoms mit einem beliebigen antisymmetrischen Polynom wieder ein antisymmetrisches Polynom ist. Insbesondere sind Polynome der Gestalt

$$p(x_1,x_2,...,x_n)A(x_1,x_2,...,x_n)$$

wobei $p(x_1,x_2,...,x_n)$ ein beliebiges symmetrisches Polynom ist, antisymmetrisch. Man kann zeigen, dass jedes antisymmetrische Polynom in dieser Gestalt geschrieben werden kann (vgl. Aufgabe 7). Offenbar ist das Produkt zweier antisymmetrischer Polynome ein symmetrisches Polynom.

Lemma. Jedes geradsymmetrische Polynom $f(x_1,x_2,...,x_n)$ wird durch ungerade Permutationen stets in ein und dasselbe Polynom übergeführt, d. h., für je zwei ungerade

Permutationen α und β gilt

$$f^{\alpha}(x_1, x_2, ..., x_n) = f^{\beta}(x_1, x_2, ...x_n)$$

In diesem Fall sind nämlich $\alpha \circ \alpha$ und $\beta \circ \alpha$ gerade Permutationen, so dass

$$f^{\alpha\circ\alpha} = f^{\beta\circ\alpha}$$

gilt. Wendet man auf beide Seiten dieser Gleichung die Permutation α^{-1} an, so erhält man

$$(f^{\alpha\circ\alpha})^{\alpha^{-1}} = (f^{\beta\circ\alpha})^{\alpha^{-1}}$$

Da $(f^{\sigma})^{\tau} = f^{\sigma\circ\tau}$ für beliebige Permutationen σ, τ gilt, ist

$$f^{(\alpha\circ\alpha)\circ\alpha^{-1}} = f^{(\beta\circ\alpha)\circ\alpha^{-1}}$$

Auf Grund der Assoziativität der Multiplikation von Permutationen erhalten wir

$$f^{\alpha\circ(\alpha\circ\alpha^{-1})} = f^{\beta\circ(\alpha\circ\alpha^{-1})}$$

Nach Definition der inversen Permutation ist also

$$f^{\alpha\circ\varepsilon} = f^{\beta\circ\varepsilon} \qquad \text{somit} \qquad f^{\alpha} = f^{\beta}$$

Satz. Jedes geradsymmetrische Polynom kann, und zwar in eindeutiger Weise, als Summe eines symmetrischen Polynoms und eines antisymmetrischen Polynoms dargestellt werden.

Beweis. Eindeutigkeit: Es sei ein gegebenes geradsymmetrisches Polynom f in der Gestalt

$$f = g + h \tag{1}$$

dargestellt, wobei g ein symmetrisches und h ein antisymmetrisches Polynom ist. Wenden wir auf beide Seiten dieser Gleichung eine ungerade Permutation α an, so ergibt sich

$$f^{\alpha} = g^{\alpha} + h^{\alpha}$$

Nach den Voraussetzungen über g und h gilt aber $9^{\alpha} = g$ und $h^{\alpha} = -h$, so dass wir

$$f^{\alpha} = g - h \tag{2}$$

erhalten. Durch Addition bzw. Subtraktion der Gleichungen (1) und (2) ergibt sich

$$g = \frac{f + f^{\alpha}}{2} \qquad , \qquad h = \frac{f - f^{\alpha}}{2} \tag{3}$$

Wir weisen darauf hin, dass sich nach dem oben bewiesenen Lemma die rechten Seiten der Gleichungen (3) nicht ändern, wenn wir anstelle von α irgendeine andere ungerade Permutation β nehmen.
Diese Überlegungen zeigen: Ist eine Zerlegung (1) möglich, so gelten für g und h die Formeln (3), d. h., existieren g und h, so sind sie eindeutig bestimmt.

Existenz: Für den Beweis der Existenz der Zerlegung (1) muss gezeigt werden:

1. Es gilt $f = \frac{f + f^\alpha}{2} + \frac{f - f^\alpha}{2}$, wobei α eine (gleichgültig welche) ungerade Permutation ist;
2. $G = \frac{f + f^\alpha}{2}$ ist ein symmetrisches Polynom;
3. $H = \frac{f - f^\alpha}{2}$ ist ein antisymmetrisches Polynom.

Die Beziehung 1. gilt trivialerweise, zum Beweis von 2. und 3. genügen folgende Bemerkungen.
Ist β eine gerade Permutation, so gilt $f^\beta = f$ und $(f^\alpha)^\beta = f^{\alpha\circ\beta} = f^\alpha$ nach dem Lemma, weil $\alpha \circ \beta$ eine ungerade Permutation ist. Daher ist $G^\beta = G$ und $H^\beta = H$.

Ist aber β eine ungerade Permutation, so gilt $f^\beta = f^\alpha$ nach dem Lemma und $(f^\alpha)^\beta = f^{\alpha\circ\beta} = f$, weil $\alpha \circ \beta$ eine gerade Permutation ist. Daher gilt

$$G^\beta = \frac{f^\alpha + f}{2} = G \qquad , \qquad H^\beta = \frac{f^\alpha - f}{2} = -H$$

und damit ist der Satz bewiesen.

Insbesondere ist jedes Polynom in zwei Veränderlichen die Summe eines symmetrischen und eines antisymmetrischen Polynoms.

Aufgaben
1. Man drücke die folgenden Polynome durch elementarsymmetrische Polynome aus:
a) $x_1^5 + x_2^5$; b) $x_1^4 + x_2^4 + x_3^4$; c) $o_3(x_1^2 x_2)$.

2. Man löse die Gleichungssysteme

a) $\sqrt{x}\sqrt{y} + 2 = \sqrt{xy}, \qquad x + y = 20.$

b) $x^2 + y^2 + 2x + 2y = 23, \qquad x^2 + y^2 + xy = 19$

c) $x + y = 4, \qquad x^4 + y^4 = 82.$

3. Man bestimme den Flächeninhalt eines Dreiecks, wenn man seinen Umfang, die Summe der Quadrate der Längen seiner Seiten und die Summe der Kuben der Längen seiner Seiten kennt.

4. Man beweise: Wird ein Polynom $f(y_1, y_2)$ gleich 0, wenn man y_1 durch $x_1 + x_2$ und y_2 durch $x_1 x_2$ ersetzt, so ist es identisch gleich 0.

5. Eindeutigkeitssatz: Zu jedem symmetrischen Polynom $f(x_1, x_2)$ existiert nur ein Polynom $g(y_1, y_2)$ derart, dass $f(x_1, x_2) = g(\sigma_1, \sigma_2)$ ist. Man beweise diese Behauptung unter Benutzung von Aufgabe 4.

6. Ist $f(x_1, x_2)$ ein antisymmetrisches Polynom, so ist $f(x_1, x_1) = 0$. Man beweise dies. Man formuliere und beweise eine analoge Behauptung für Polynome in drei Veränderlichen.

7. Unter Benutzung der vorhergehenden Aufgabe beweise man, dass jedes antisymme-

trische Polynom $f(x_1, x_2)$ in zwei Veränderlichen die Gestalt $(x_1 - x_2)g(x_1, x_2)$ besitzt, wobei $g(x_1, x_2)$ ein symmetrisches Polynom ist.

8. Eine Funktion $f(x_1, x_2, ..., x_n)$ von n Veränderlichen wird symmetrisch genannt, wenn sie bei keiner Permutation der Argumente ihren Wert ändert, d. h., wenn für jede Permutation $\sigma \in S_n$ die Beziehung

$$f(x_{(1)\sigma}, x_{(2)\sigma}, ..., x_{(n)\sigma} = f(x_1, x_2, ..., x_n)$$

Man beweise, dass die Funktion

$$f(x_1, x_2, x_3) = ||x_1 - x_2| + x_1 + x_2 - 2x_3| + |x_1 - x_2| + x_1 + x_2 + 2x_3$$

symmetrisch ist.

16 Auflösung algebraischer Gleichungen

1. Eine Gleichung der Gestalt

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n = 0$$

mit $a_0 \neq 0$ wird algebraische Gleichung n-ten Grades genannt.

Die einfachsten algebraischen Gleichungen - die Gleichungen ersten und zweiten Grades und sogar einige spezielle Gleichungen dritten Grades - konnten bereits die Mathematiker im alten Babylon vor ca. 4000 Jahren lösen. Allerdings kannten die Wissenschaftler in diesen fernen Zeiten die moderne mathematische Symbolik noch nicht und beschrieben sowohl die Gleichungen als auch den Prozess ihrer Auflösung in Worten und nicht in Formeln.

2. Jede Gleichung ersten Grades

$$ax + b = 0 \qquad (a \neq 0)$$

besitzt eine Lösung $x = -b/a$, und zwar genau eine.
In der Schule beweist man den folgenden Satz über die Auflösung einer beliebigen quadratischen Gleichung

$$ax^2 + bx + c = 0 \qquad (a \neq 0)$$

Ist $D = b^2 - 4ac > 0$, so besitzt die Gleichung genau zwei Lösungen, die durch die Formel

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}$$

gegeben werden.
Ist $D = 0$, so gibt es nur eine einzige Lösung, die Zahl $x = -\frac{b}{2a}$.
Ist aber $D < 0$, so existiert im. Bereich der reellen Zahlen keine Lösung.

Die Mathematiker sind immer bestrebt, solche Fallunterscheidungen zu vermeiden - ihre Zahl würde beim Übergang zu Gleichungen höheren Grades immer mehr wachsen. Wünschenswert wäre natürlich die Formulierung:
"Jede Gleichung zweiten Grades besitzt zwei Lösungen."

Man kann das erreichen, wenn man einerseits den Zahlbegriff so erweitert, dass es möglich ist, Quadratwurzeln aus negativen Zahlen zu ziehen, andererseits bestimmte "Lösungen" mehrfach zählt (d. h. den Begriff der Vielfachheit einer Lösung einführt). Sowohl das eine als auch das andere ist korrekt ausführbar.

3. Die allgemeine Gleichung dritten Grades besitzt die Gestalt

$$Ax^3 + Bx^2 + Cx + D = 0 \qquad (A \neq 0)$$

Dividiert man diese Gleichung durch den Koeffizienten A, wobei sich offenbar die Lösung nicht ändert, so gelangt man zu einer Gleichung der Gestalt

$$x^3 + ax^2 + bx + c = 0$$

Durch Einführung der neuen Unbekannten $z = x + \frac{a}{3}$ kann man den Summanden, der die Unbekannte in der zweiten Potenz enthält, eliminieren, d. h., die Gleichung auf die Gestalt

$$z^3 + pz + q = 0 \tag{1}$$

bringen, die man reduzierte Gleichung dritten Grades nennt.

Über die Geschichte der Entdeckung der Formeln für die Lösung einer kubischen Gleichung wissen wir nur wenig und nichts Genaues. Vermutlich hat Scipione del Ferro (1465 bis 1526), Professor an der Universität Bologna, als erster eine Methode zur Auflösung kubischer Gleichungen gefunden (etwa 1515).
Unabhängig von ihm (etwa 1535) entdeckte Niccolo Tartaglia (1500-1557) diese Methode. Der erste jedoch, der die Formel für die Lösung der kubischen Gleichung veröffentlichte, war Girolamo Cardano (1501-1576) (seine Arbeit erschien 1545). Daher wird diese Formel nach ihm benannt.
Wir merken an, dass Cardano möglicherweise die Arbeiten von Tartaglia und del Ferro kannte.

In heutiger Bezeichnungsweise besteht die Methode zur Auflösung der Gleichung (1) in folgendem:
Wir führen die beiden neuen Unbekannten u und v ein; setzen wir $z = u+v$, so erhalten wir

$$(u+v)^3 + p(u+v) + q = 0 \qquad , \qquad u^3 + v^3 + (u+v)(3uv+p)q = 0 \tag{2}$$

Genügen die Unbekannten u und v dem System

$$uv = -\frac{p}{3} \qquad , \qquad u^3 + v^3 = -q \tag{3}$$

so genügen sie auch der Gleichung (2). Das System (3) zu lösen ist sehr einfach. Wir erheben die erste Gleichung in die dritte Potenz und setzen anstelle von v^3 den sich aus der zweiten Gleichung ergebenden Ausdruck ein; dann genügt $u^3 = y$ der quadratischen Gleichung

$$y^2 + qy - \frac{p^3}{27} = 0$$

Folglich ist

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \qquad , \qquad v^3 = -\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

und schließlich

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{4}$$

Dies ist die Cardanosche Formel zur Lösung der reduzierten kubischen Gleichung (1). Sofort erheben sich folgende Fragen:

1. Was ist zu tun, wenn der Ausdruck $q^2/4 + p^3/27$ negativ ist?

2. Wieviel Lösungen besitzt eine kubische Gleichung?

3. Liefert die Cardanosche Formel (4) alle Lösungen der Gleichung (1)?

Diese Fragen hängen zusammen. Man sieht z. B. leicht, dass

$$x^3 - 19x + 30 = 0$$

die Lösungen -5, 2, 3 besitzt, aber in diesem Fall

$$\frac{q^2}{4} + \frac{p^3}{27} < 0$$

ist; daher verlieren die Quadratwurzeln in der Cardanoschen Formel ihren Sinn, so dass sich die drei erwähnten Lösungen nicht durch diese Formel ausdrücken lassen.

Alles spricht dafür, dass man hier noch weniger als im Fall der quadratischen Gleichungen die Einführung solcher "neuen Zahlen" umgehen kann, durch welche das Ziehen einer Quadratwurzel immer möglich ist.

Solche Zahlen wurden nach und nach in der Zeit vom 16. bis 19. Jahrhundert eingeführt. Man nennt sie komplexe Zahlen. Im Bereich der komplexen Zahlen hat jede algebraische Gleichung n-ten Grades genau n Lösungen.
Wir betrachten als Beispiel die Gleichung

$$x^n - 1 = 0 \tag{5}$$

Sie spielt in der Theorie eine wichtige Rolle, wir benötigen sie im weiteren. Im Bereich der komplexen Zahlen besitzt diese Gleichung n verschiedene Lösungen, welche n-te Einheitswurzeln genannt werden:

$$\begin{aligned} \rho_0 &= 1, \\ \rho_1 &= \cos(2\pi/n) + i\sin(2\pi/n), ..., \\ \rho_{n-1} &= \cos(2\pi(n-1)/n) + i\sin(2\pi(n-1)/n) \end{aligned} \tag{6}$$

Um die Lösungen einer kubischen Gleichung aufzuschreiben, braucht man die dritten Wurzeln aus 1. Gemäß den Formeln (6) sind das die folgenden komplexen Zahlen:

$$\begin{aligned} \rho_0 &= 1, \\ \rho_1 &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \\ \rho_2 &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \end{aligned}$$

Man kann zeigen, dass die drei Lösungen der reduzierten kubischen Gleichung $z^3 +$

$pz + q = 0$ die Zahlen

$$z_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$
$$z_2 = \rho\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \rho^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$
$$z_3 = \rho^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \rho\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

sind. Hier wird mit ρ die dritte Einheitswurzel ρ_1 bezeichnet, und wie man leicht sieht, ist ρ^2 gleich ρ_2. Dies sind dann die endgültigen Cardanoschen Formeln.
Dabei ist noch zu beachten, dass die dritten Wurzeln zur Bestimmung von u und v in $z_1 = u + v$ (vgl. auch (4)), für deren Festlegung man im Bereich der komplexen Zahlen jeweils drei Möglichkeiten hat, nicht unabhängig voneinander gewählt werden können, sondern gemäß (3) in der Beziehung $u \cdot v = -\frac{p}{3}$ stehen müssen.

4. Für die Gleichungen ersten, zweiten und dritten Grades sind uns Formeln bekannt, nach denen sich die Lösungen mit Hilfe der rationalen Operationen $+$, $-$, $\times$, :, der Operation Quadratwurzel $\sqrt{}$ (im Fall der quadratischen Gleichungen) bzw. der Quadratwurzel $\sqrt{}$ und der Kubikwurzel $\sqrt[3]{}$ (im Fall der kubischen Gleichung) ausgehend von den Koeffizienten der Gleichung ausdrücken lassen.

Ähnliche Regeln wurden auch für die Gleichungen vierten Grades von einem Schüler Cardanos, dem italienischen Algebraiker Ludovico Ferrari (1522-1565) aufgestellt. Darin werden ebenfalls nur die rationalen Operationen und die Operationen $\sqrt{}$ und $\sqrt[3]{}$ benutzt.
Alle Versuche im Laufe fast dreier Jahrhunderte (16.-18. Jh.), ähnliche Regeln (bei denen also nur rationale Operationen und Wurzeloperationen benutzt werden) für Gleichungen fünften und höheren Grades zu finden, waren nicht von Erfolg gekrönt.

Allmählich begann man zu vermuten, es sei im allgemeinen nicht möglich, die Lösungen einer Gleichung n-ten Grades für $n \geq 5$ aus den Koeffizienten ausschließlich mit Hilfe der Operationen $+$, $-$, $\times$, : und $\sqrt[m]{}$ (für beliebige natürliche Zahlen n) zu gewinnen, d. h., es sei nicht möglich, die Auflösung solcher Gleichungen auf rationale Operationen und die sukzessive Lösung der speziellen Gleichung $y^m = A$ zurückzuführen.

Die Lösungen einer Gleichung $y^m = A$, die man üblicherweise durch $\sqrt[m]{A}$ ausdrückt, werden Radikale genannt; daher nennt man das Problem, ob die Bestimmung der Lösungen einer beliebigen Gleichung auf die Bestimmung der Lösungen von Gleichungen der Gestalt $y^m = A$ zurückgeführt werden kann, das Problem der Darstellbarkeit der Lösungen einer Gleichung durch Radikale.

Versuche, diese Vermutung zu beweisen oder zu widerlegen, wiederholten sich insbesondere in der zweiten Hälfte des 18. Jahrhunderts und führten Anfang des 19. Jahrhunderts zum Beweis der Unmöglichkeit der Auflösung der allgemeinen Gleichung fünften und höheren Grades durch Radikale.

Unter den Arbeiten des 18. Jahrhunderts, die in die erwähnte Richtung zielten, zeichnete sich eine Abhandlung des bekannten französischen Mathematikers Joseph Louis Lagrange (1736 bis 1813) durch große Gedankenklarheit aus; sie trug den Titel "Überlegungen über die algebraische Lösung von Gleichungen" (1771/72).
Dort analysierte der Autor sorgfältig und ausführlich die bekannten Methoden zur Auflösung von Gleichungen zweiten, dritten und vierten Grades durch Radikale, um zu erläutern, wie und warum in diesen Fällen diese Auflösung gelingt. Dabei bemerkte er folgende Tatsache: In allen betrachteten Fällen gibt es Funktionen der Wurzeln, welche Gleichungen niedrigeren Grades genügen und von denen schon bekannt ist, dass sie mit Hilfe von Radikalen lösbar sind. Die Lösungen der Ausgangsgleichung ihrerseits können sukzessive aus diesen Zwischenfunktionen mit Hilfe von in Radikalen lösbaren Gleichungen bestimmt werden.

Weiterhin untersuchte Lagrange die Frage, auf welche Art und Weise man in den bekannten Fällen solche Funktionen der Wurzeln bestimmen kann.
Es zeigte sich, dass dies Polynome $\varphi(\xi_1, ..., \xi_n)$ in den Wurzeln $\xi_1, ..., \xi_n$ sind, die bei allen möglichen Permutationen der Wurzeln (deren Anzahl bekanntlich $n!$ ist) nicht $n!$, sondern eine kleinere Anzahl von Werten annehmen, die sogar kleiner als n ist (n ist dabei der Grad der betrachteten Gleichung).
Das ist dann der Fall, wenn sich $\varphi(\xi_1, ..., \xi_n)$ bei gewissen Permutationen der Wurzeln nicht ändert.

Auf diese Weise spielen die Permutationen bei der Auflösung von Gleichungen eine wichtige Rolle.

Wenn eine Funktion $\varphi(\xi_1, \xi_2, ..., \xi_n)$ der Wurzeln nur die k verschiedenen Werte $\varphi_1, ..., \varphi_k$ annimmt, müssen sich die Koeffizienten des Polynoms

$$(y - \varphi_1)...(y - \varphi_k) = y^k + b_1 y^{k-1} + ... + b_k$$

nach einem schon längst bekannten Satz, dem sogenannten Hauptsatz über symmetrische Funktionen, rational durch die Koeffizienten der untersuchten Gleichung

$$a_0 x^n + a_1 x^{n-1} + ... + a_0 = 0$$

ausdrücken lassen.
Wir führen Beispiele an:

1. Es sei $A(\xi_1, ..., \xi_n) = A$ die alternierende Funktion

$$\Delta = \prod_{l<m} (\xi_l - \xi_m)$$

der Lösungen einer Gleichung n-ten Grades. Sie nimmt bei allen möglichen Permutationen der Wurzeln nur die beiden Werte Δ bzw. $-\Delta$ an, je nachdem, ob die Permutation gerade oder ungerade ist.
Folglich ändert sich die Diskriminante $D = \Delta^2$ bei allen möglichen Permutationen nicht und lässt sich rational durch die Koeffizienten der betrachteten Gleichung ausdrücken.

Für die quadratische Gleichung $ax^2 + bx + c = 0$ ist

$$D = b^2 - 4ac$$

für die reduzierte kubische Gleichung $x^3 + px + q = 0$ gilt

$$D = -4p^3 - 27q^2$$

Die alternierende Funktion Δ der Wurzeln erfüllt die Gleichungen

$$y^2 - (b^2 - 4ac) = 0 \qquad \text{bzw.} \qquad y^2 + (4p^3 + 27q^2) = 0$$

Wir erkennen die Ausdrücke unter den Quadratwurzeln in der Lösungsformel für die quadratische Gleichung bzw. - bis auf einen konstanten Faktor - in der Cardanoschen Formel.

2. Ein anderes Beispiel tauchte in der oben erwähnten Arbeit von Lagrange auf. Dies sind die sogenannten Lagrangeschen Resolventen. Wir betrachten sie, wie es auch Lagrange selbst tat, für den Fall einer Gleichung dritten Grades. Mit Hilfe der kubischen Einheitswurzeln 1, ρ, ρ^2 werden sie folgendermaßen definiert:

$$\eta_0 = \xi_1 + \xi_2 + \xi_3, \qquad \eta_1 = \xi_1 + \rho\xi_2 + \rho^2\xi_3, \qquad \eta_2 = \xi_1 + \rho^2\xi_2 + \rho\xi_3 \qquad (7)$$

Hier sind ξ_1, ξ_2, ξ_3 die Lösungen der betrachteten kubischen Gleichung. Wir richten unsere Aufmerksamkeit auf die zweite und die dritte Resolvente.
Wie man leicht sieht, multiplizieren sie sich bei der zyklischen Permutation $(\xi_1, \xi_2, \xi_3) \to (\xi_2, \xi_3, \xi_1)$ der Lösungen nur mit ρ^2 bzw. mit ρ. Folglich bleiben η_1^3 und η_2^3 bei zyklischen Permutationen invariant, lassen sich daher rational durch die Koeffizienten der Gleichung und durch Δ ausdrücken. Die entsprechenden Darstellungen kann man berechnen.

Wenn man die dritten Wurzeln zieht, erhält man η_1 und η_2. Nach dem Satz von Vieta ist $\xi_1 + \xi_2 + \xi_3$ der Koeffizient von z^2 mit entgegengesetztem Vorzeichen, d. h., im Fall der reduzierten kubischen Gleichung ist $\eta_0 = 0$.
Kennt man η_0, η_1, η_2 aus dem System linearer Gleichungen (7), so kann man ξ_1, ξ_2, ξ_3 bestimmen. Durch Ausführung der erwähnten Rechnungen kann man sich davon überzeugen, dass sich ξ_1, ξ_2, ξ_3 nach den Cardanoschen Formeln berechnen lassen.

Analog, nur technisch komplizierter, kann man die Lösung einer Gleichung vierten Grades in Radikalen erhalten. Bei der Gleichung fünften Grades gelang es jedoch nicht, eine ähnliche Reduktion auf Gleichungen niedrigeren Grades zu bewerkstelligen. Allerdings schloss Lagrange nicht aus, dass eine solche Reduktion möglich sei.

Dass eine derartige Herabsetzung des Grades prinzipiell nicht durchführbar ist, zeigte im Jahre 1799 der italienische Mathematiker Paolo Ruffini (1765-1822) in seiner Arbeit "Allgemeine Theorie der Gleichungen, in der die Unmöglichkeit der algebraischen Lösung allgemeiner Gleichungen höheren als vierten Grades bewiesen wird".
Allerdings gab es in seinem Beweis Lücken, die er nicht ausfüllen konnte. Ein strenger Beweis wurde erst im Jahre 1826 in einer Arbeit des norwegischen Mathematikers Niels

Henrik Abel (1802-1829) gegeben ("Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen").

Den wesentlichen Grund für die Tatsache, dass es keine Funktionen der Wurzeln gibt, welche Gleichungen niedrigeren als des betrachteten Grades genügen (eine Ausnahme bildet immer die alternierende Funktion, welche einer quadratischen Gleichung genügt), deckte der geniale französische Mathematiker Evariste Galois (1811-1832) auf. Er ordnete jeder algebraischen Gleichung die Gruppe derjenigen Permutationen ihrer Wurzeln zu, welche die Werte aller Polynome der Wurzeln mit Koeffizienten, die rational von den Koeffizienten der gegebenen Gleichung abhängen, unverändert lassen.
Diese Gruppe wird jetzt die Galoissche Gruppe der betrachteten Gleichung genannt.

Anhand der Eigenschaften dieser Gruppe kann man feststellen, ob die gegebene Gleichung in Radikalen auflösbar ist oder nicht. Dieses Kriterium enthält alle vorher bekannten Ergebnisse über die Auflösbarkeit bzw. Nichtauflösbarkeit algebraischer Gleichungen in Radikalen als Spezialfälle.

Es ist aber nicht ausgeschlossen, dass gewisse Gleichungen, deren Koeffizienten bestimmte Zahlen sind, in Radikalen lösbar sind. Ob dies möglich ist oder nicht, lässt sich wiederum auf Grund des von Galois gefundenen Kriteriums feststellen.

17 Das Fünfzehnerspiel

Die Theorie der Permutationen lässt sich auch bei der mathematischen Analyse vieler populärer Spiele anwenden. Beispielsweise war eine Zeitlang das heute fast vergessene Fünfzehnerspiel (auch unter dem Namen Sam Loyds Schiebepuzzle bekannt) sehr beliebt. "Schuld daran", dass es vergessen ist, sind die Mathematiker, weil sie streng bewiesen haben, dass nur bestimmte Ausgangsstellungen des Spiels zum Erfolg führen, alle übrigen aber nicht. Wir beweisen dies hier unter Benutzung der Theorie der Permutationen.

Zuerst beschreiben wir das Spiel. In einem flachen quadratischen Kästchen (Rähmchen) sind 15 gleichgroße quadratische Spielsteine untergebracht, so dass ein Feld frei bleibt. Die Steine sind mit den Zahlen von 1 bis 15 nummeriert und in irgendeiner Reihenfolge angeordnet (z. B. so wie in Abb. 30a). Das Spiel besteht darin, die Steine nach wachsenden Nummern zu ordnen (vgl. Abb. 30b), und zwar durch bloßes Verschieben je eines Steines auf das benachbarte freie Feld; kein Stein darf aus dem Kästchen herausgehoben werden.

Abb. 30a, b

9	6	3	13
1	5	7	2
14	4	8	11
10	15	12	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Diese Anordnung der Steine nach wachsenden Nummern wollen wir Standardanordnung nennen. Es hat sich gezeigt, dass die Standardanordnung nach der Spielregel nicht von jeder Ausgangsstellung aus erreichbar ist; es gibt tatsächlich Stellungen, von denen aus dieser Übergang niemals bewerkstelligt werden kann.
Wir vereinbaren, solche Anordnungen der Steine in dem Kästchen, bei denen das Feld in der rechten unteren Ecke frei bleibt, ausgezeichnete Stellungen zu nennen. Sonst sprechen wir einfach von Stellungen oder Anordnungen.

Mit jeder Anordnung der Steine in dem Kästchen kann man eine bestimmte Permutation der Menge $M = \{1, 2, 3, ..., 15, 16\}$ verknüpfen, wobei man annimmt, das freie Feld stelle einen fiktiven Spielstein mit der Nummer 16 dar.
Wir markieren die Felder mit Hilfe der Zahlen 1 bis 16 so, dass die Nummerierung mit der Standardanordnung der Spielsteine übereinstimmt.

Dann wird jede Anordnung der Spielsteine eindeutig durch eine Permutation der Menge M charakterisiert, deren erste Zeile die Nummer der Felder und deren zweite die Nummern der auf diesen Feldern stehenden Steine enthält. Beispielsweise wird die Anordnung der Spielsteine in Abb. 30a durch die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 9 & 6 & 3 & 13 & 1 & 5 & 7 & 2 & 14 & 4 & 8 & 11 & 10 & 15 & 12 & 16 \end{pmatrix}$$

beschrieben, die Anordnung der Spielsteine in Abb. 30b durch die identische Permutation.

Die ausgezeichneten Stellungen lassen sich eindeutig durch die Permutationen auf der Menge $M_1 = \{1, 2, 3, ..., 15\}$ beschreiben, weil für diese der fiktive Spielstein auf dem Feld Nummer 16 steht.
Der Übergang von einer Anordnung, die durch die Permutation φ charakterisiert wird, zu einer Anordnung, die durch die Permutation ψ charakterisiert wird, lässt sich, wenn er möglich ist, in einigen Zügen bewerkstelligen, wobei jeder Zug in der Verschiebung eines Spielsteins auf das benachbarte freie Feld besteht. Ist das i-te Feld frei und trägt der Spielstein, der verschoben wird, die Nummer a_j, und steht er auf dem j-ten Feld, so steht dieser Spielstein nach der Verschiebung auf dem i-ten Feld, und das j-te Feld ist frei. Das bedeutet, dass wir durch einen einzigen Zug von der Anordnung

$$\varphi = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & 16 \\ a_1 & a_2 & ... & 16 & ... & a_j & ... & a_{16} \end{pmatrix}$$

zu der Anordnung

$$\varphi = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & 16 \\ a_1 & a_2 & ... & a_j & ... & 16 & ... & a_{16} \end{pmatrix}$$

übergehen. Das heißt, wir multiplizieren die Permutation φ mit der Transposition

$$\delta_1 = (a_j, 16) = \varphi = \begin{pmatrix} 1 & 2 & ... & a_j & ... & 15 & 16 \\ 1 & 2 & ... & 16 & ... & 15 & a_j \end{pmatrix}$$

und erhalten die Gleichung

$$\varphi_1 = \varphi \circ \delta_1$$

Wenn man von einer durch die Permutation φ_1 beschriebenen Stellung durch einen einzigen Zug zu einer neuen übergehen kann, lässt sich eine Transposition δ_2 finden derart, dass die Permutation φ_2, welche der neuen Stellung entspricht, mit φ_1 durch die Gleichung

$$\varphi_2 = \varphi_1 \circ \delta_2$$

verknüpft ist.

Wir nehmen nun an, für den Übergang von der Stellung φ zur Stellung ψ seien k Züge nötig. Das bedeutet, dass Transpositionen $\delta_1, \delta_2, ..., \delta_k$ der Gestalt $(i, 16)$ existieren, für welche die Gleichung

$$\psi = \varphi \circ \delta_1 \circ \delta_2 \circ ... \circ \delta_k$$

gilt. Auf das freie Feld wird jedesmal ein benachbarter Stein geschoben, und dies erlegt dem Produkt $\delta_1 \circ \delta_2 \circ ... \circ \delta_k$ bestimmte Einschränkungen auf. Wenn es gelingt, von einer ausgezeichneten Stellung φ zur Standardanordnung überzugehen, kann man solche Transpositionen $\delta_1, \delta_2, ..., \delta_s$ der angegebenen Art wählen, dass die Gleichung

$$\varphi \circ \delta_1 \circ \delta_2 \circ ... \circ \delta_{s-1} \circ \delta_s = \varepsilon$$

erfüllt ist; daraus folgt

$$\varphi = \delta_s^{-1} \circ \delta_{s-1}^{-1} \circ ... \circ \delta_2^{-1} \circ \delta_1^{-1} = \delta_s \circ \delta_{s-1} \circ ... \circ \delta_2 \circ \delta_1$$

Dieses Produkt kann aber kein beliebiges Produkt sein, weil die Folge der Transpositionen $\delta_1, \delta_2, ..., \delta_s$ der Folge der Züge entspricht, bei denen jedesmal ein benachbarter Spielstein auf das freie Feld geschoben wird.

Wir beweisen zunächst folgendes: Kann man von einer ausgezeichneten Stellung φ zur Standardanordnung übergeben, so ist die Permutation φ gerade.

Wir nummerieren die Zeilen und Spalten, die aus Spielsteinen bestehen, in der Weise, wie Abb. 31 zeigt. Bei jeder Verschiebung eines Spielsteines auf das freie Feld (seiner Vertauschung mit dem fiktiven Spielstein) vergrößert oder verkleinert sich die Summe der Nummern der Zeile und der Spalte,

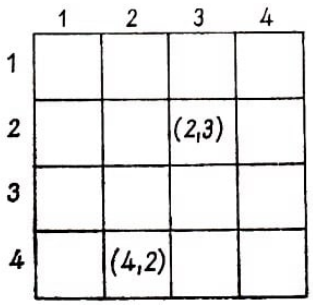


Abb. 31

in denen der fiktive Stein steht, um 1. Dies folgt so:
Das Feld jedes Steins ist eindeutig durch ein Zahlenpaar (i, j), $i, j = 1, 2, 3, 4$, charakterisiert. Steht der fiktive Stein auf dem Feld (i, j), so kann der nächste Zug einer der folgenden vier Züge sein:

$$\begin{aligned}
(i,j) &\to (i-1,j) \qquad (i \neq 1)\\
(i,j) &\to (i+1,j) \qquad (i \neq 4)\\
(i,j) &\to (i,j-1) \qquad (j \neq 1)\\
(i,j) &\to (i,j+1) \qquad (j \neq 4)
\end{aligned}$$

oder einer von drei bzw. von zwei dieser Möglichkeiten, wenn der fiktive Stein am Rand bzw. in einer Ecke des Kästchens steht. In jedem Fall wird die Summe $i + j$ durch $i + j + 1$ oder $i + j - 1$ ersetzt, d. h., sie erhöht oder verringert sich um 1.

Es sei nun eine ausgezeichnete Stellung φ gegeben. In dieser Stellung hat nach unserer Nummerierung das leere Feld die Nummer (4, 4). Sind wir nach einer gewissen Anzahl von Verschiebungen von Spielsteinen auf das jeweils freie Feld zur Standardanordnung gelangt, so hat der fiktive Spielstein auch diese Nummer. Da sich bei jedem Zug (bei jeder Transposition) die Parität der Summe aus den Nummern der Zeile und der Spalte, in denen sich der fiktive Stein befindet, ändert, kann man den fiktiven Stein nur durch eine gerade Anzahl von Zügen auf das Feld (4, 4) zurückbringen.

Somit kann die Permutation φ in ein Produkt einer geraden Anzahl von Transpositionen zerlegt werden, d. h., sie ist gerade.
Es zeigt sich, dass die Bedingung, die Permutation, welche eine ausgezeichnete Stellung der Spielsteine charakterisiert, sei gerade, auch hinreichend dafür ist, dass man von dieser Stellung zur Standardanordnung übergeben kann.

Es ist nicht notwendig, diese Behauptung für alle geraden Permutationen zu beweisen; wenn man nämlich von jeder der durch die Permutationen φ bzw. ψ beschriebenen Stellungen zur Standardanordnung gelangen kann, so ist dies, wie man leicht sieht, auch von der Stellung $\varphi \circ \psi$ aus möglich.
Daher braucht man sich davon nur für solche Permutationen zu überzeugen, in deren Produkt sich jede gerade Permutation zerlegen lässt.

Wir betrachten als Beispiel die Permutationen

$$(1,2,3),(1,2,4),(1,2,5),...,(1,2,15) \tag{1}$$

Alle Spielsteine in dem Kästchen, außer denen, die auf dem ersten und dem zweiten Feld stehen, kann man zu einer einzigen "Kette" verbinden, die so bewegt werden kann, dass sich die gegenseitige Lage ihrer Glieder nicht ändert (wenn man das freie Feld nicht berücksichtigt, das sich längs der Kette bewegen kann).

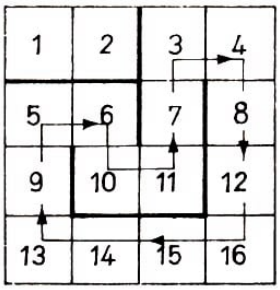


Abb. 32

Man braucht sich ja nur vorzustellen, im Inneren des Kästchens seien "Wände" aufgestellt, z. B. so wie in Abb. 32. Die Steine können längs der "Wände" im Uhrzeigersinn oder entgegen dem Uhrzeigersinn bewegt werden. Jeder Stein, der zur Kette gehört, kann nach einer bestimmten Anzahl von Zügen auf dem Feld mit der Nummer 3 stehen.

Eine Anordnung werde nunmehr durch den Zyklus $(1,2,k)$ charakterisiert, d. h., in dem Kästchen befindet sich der Stein mit der Nummer 2 auf dem ersten Feld, der Stein mit der Nummer Ja auf dem zweiten Feld, der Stein mit der Nummer 1 auf dem k-ten Feld $(3 \leq k \leq 15)$, und alle übrigen Steine befinden sich auf den Feldern ihrer Nummer. Nehmen wir eine bestimmte Anzahl von Verschiebungen der Kettenglieder vor, so können wir den Stein mit der Nummer 1 auf das dritte Feld bringen.

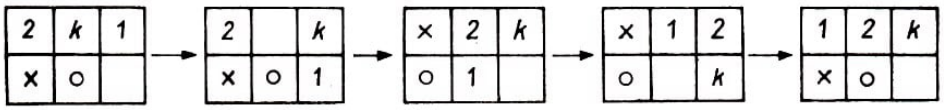


Abb. 33

Danach machen wir das Feld mit der Nummer 7 frei, indem wir den fiktiven Spielstein längs der Kette in der entgegengesetzten Richtung verschieben. Nun kann man, wenn man nur die Spielsteine auf den Feldern 1, 2, 3, 5, 6, 7 umstellt, erreichen, dass die Steine mit den Nummern 1 und 2 auf den entsprechenden Feldern 1, 2 stehen, der Stein mit der Nummer Ja auf dem dritten Feld steht und alle übrigen ihre Position nicht ändern.
Das ist aus dem in Abb. 33 dargestellten Schema, welches die aufeinanderfolgenden Verschiebungen der Steine zeigt, ersichtlich. In diesem Schema bedeuten $\circ$ und $\times$

Steine, deren Nummern für uns unwesentlich sind.

Im Ergebnis änderte sich die Anordnung von nur drei Steinen. Der Stein mit der Nummer k kann jetzt in die Kette eingegliedert werden. Verschieben wir ihn längs der Kette, so können wir ihn auf das Feld mit der Nummer k bringen. Dabei nehmen alle übrigen Steine in der Kette ihre anfängliche Stellung ein. Nun müssen wir nur noch den fiktiven Stein auf das letzte Feld bringen und erhalten die Standardanordnung.

Wir beweisen nun, dass jede gerade Permutation in ein Produkt von Zyklen der Folge (1) zerlegt werden kann. In der Tat, man kann jede gerade Permutation α in ein Produkt einer geraden Anzahl von Transpositionen zerlegen:

$$\alpha = \delta_1 \circ \delta_2 \circ ... \circ \delta_{2k-1} \circ \delta_{2k} \tag{2}$$

Ist $\sigma = (1, 2)$, so kann man aufgrund der Gleichung $\sigma^2 = \varepsilon$

$$\begin{aligned}\alpha &= \delta_1 \circ \sigma \circ \sigma \circ \delta_2 \circ \delta_3 \circ \sigma \circ \sigma \circ \delta_4 \circ ... \circ \delta_{2k-1} \circ \sigma \circ \sigma \circ \delta_{2k} \\ &= (\delta_1 \circ \sigma) \circ (\sigma \circ \delta_2) \circ (\delta_3 \circ \sigma) \circ (\sigma \circ \delta_4) \circ ... \circ (\delta_{2k-1} \circ \sigma) \circ (\sigma \circ \delta_{2k})\end{aligned}$$

schreiben. Um den Beweis zu vervollständigen, genügt es zu zeigen, dass man für jede Transposition (i, j) die beiden Produkte $(i, j) \circ (1, 2)$ und $(1, 2) \circ (i, j)$ in ein Produkt von Zyklen der Folge (1) zerlegen kann. Und dies gilt tatsächlich, wie folgende leicht nachzuprüfende Gleichungen zeigen:

$(1,2) \circ (i,j) = (i,j) \circ (1,2) = (1,2,j) \circ (1,2,i) \circ (1,2,i) \circ (1,2,j)$ für $i, j > 2$
$(1,2) \circ (1,j) = (2,j) \circ (1,2) = (1,2,j)$ für $j > 2$
$(1,2) \circ (2,j) = (1,j) \circ (1,2) = (1,2,j) \circ (1,2,j)$ für $j > 2$

Ist eines der δ_k in der Zerlegung (2) gleich (1, 2), so wird das entsprechende Produkt mit σ die identische Permutation und braucht nicht berücksichtigt zu werden.

Aufgaben
1. Wie kann man praktisch den Übergang zu der Standardstellung verwirklichen, ausgehend von Stellungen, die sich durch eine gerade Permutation charakterisieren lassen?

2. Man beweise, dass jede gerade Permutation der Menge $M = \{1, 2, ..., n\}$ in ein Produkt folgender Zyklen der Länge 3 zerlegt werden kann: $(1, 2, 3)$, $(2, 3, 4)$, ..., $(n-2, n-1, n)$.

3. Man zerlege die Permutationen

$$\varphi = (1, 2, 3) \circ (7, 5) \circ (4, 6, 9, 8) \quad , \quad \psi = (1, 2, 3, 4) \circ (8, 7, 5, 6)$$

in ein Produkt von Zyklen der Gestalt $(1, 2, k)$.

4. Kann man von den ausgezeichneten Stellungen, die durch die Permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 8 & 7 & 6 & 5 & 1 & 2 & 4 & 3 & 13 & 15 & 11 & 10 & 14 & 12 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 6 & 3 & 4 & 5 & 2 & 1 & 15 & 10 & 13 & 12 & 11 & 14 & 9 & 8 & 7 \end{pmatrix}$$

gegeben sind, zur Standardstellung übergehen?

5. Man beweise: Wird eine Anordnung durch eine ungerade Permutation charakterisiert, so kann man zu einer Anordnung übergehen, die sich von der Standardanordnung durch die Reihenfolge der letzten beiden Spielsteine unterscheidet.

6. Auf die Spielsteine des Fünfzehnerspiels können anstelle der Zahlen die Buchstaben f, ü, n, f, z, e, h, n, e, r, s, p, i, e, l geschrieben werden. Verschiebt man die Steine wie im Fünfzehnerspiel, so kann man von jeder Anordnung zu einer solchen übergehen, bei der die Buchstaben auf den Steinen das Wort Fünfzehnerspiel bilden. Man beweise dies.

7. Das Spiel "Kastanie" wird auf einer Tafel mit neun Feldern gespielt, die durch geradlinige Strecken verbunden sind (vgl. Abb. 34). Auf jedem der acht Spielsteine befindet sich einer der Buchstaben k, a, s, t, a, n, i, e.

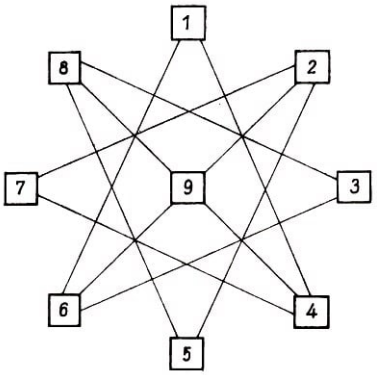


Abb. 34

Die Steine werden beliebig auf die Felder verteilt, die in den Ecken des Vielecks angeordnet sind. Das Mittelfeld bleibt zunächst leer.
Das Ziel des Spiels besteht darin, sie in die richtige Reihenfolge zu bringen, so dass sich beim Lesen im Uhrzeigersinn, wenn man beim ersten Feld beginnt, das Wort "Kastanie" ergibt.

Dabei sollen die Steine auf den Verbindungsgeraden verschoben werden. Man beweise, dass man von jeder Anfangsverteilung zur richtigen Anordnung der Steine gelangen kann.

8. Man zeige, dass die Theorie des Fünfzehnerspiels auch für das Achterspiel gültig bleibt, dessen Regeln dieselben sind, wobei aber nur acht Steine mit den Nummern 1, 2, 3, 4, 5, 6, 7, 8 in einem Quadrat mit neun Feldern verschoben werden.

9. Auf den Steinen des Kastanie-Spiels seien anstelle der Buchstaben die Zahlen 1 bis 8 geschrieben. Die Spielregeln bleiben die alten.
Man beweise, dass man auf diese Weise ein Spiel erhält, das mit dem Achterspiel übereinstimmt.

10. Analog zum Fünfzehnerspiel untersuche man das Vierundzwanzigerspiel.

18 Antworten, Hinweise, Lösungen

Abschnitt 1

1. a) $(f \circ g)(x) = 6x + 13$, $(g \circ f)(x) = 6x + 11$;

b) $(f \circ g)(x) = x^6 + 10x^5 + 25x^4 + 3$; $(g \circ f)(x) = x^6 + 14x^4 + 57x^2 + 72$;

c) $(f \circ g)(x) = x^6 + 6x^4 + 13x^2 + 11$; $(g \circ f)(x) = x^6 + 2x^4 + 2x^3 + x^2 + x + 3$

d) $(f \circ g)(x) = \begin{cases} (14x+11)/(1-x) & \text{für } x \neq -3/2, x \neq 1 \\ \text{nicht definiert für } x = -3/2 \text{ für } x = 1 \end{cases}$

$(g \circ f)(x) = \begin{cases} (x+1)/(x+2) & \text{für } x \neq -2, x \neq 1 \\ \text{nicht definiert für } x = -2/3 \text{ bzw. } x = 1 \end{cases}$

2. a) Abgeschlossen; b) abgeschlossen; c) abgeschlossen; d) nicht abgeschlossen; e) abgeschlossen.

Abschnitt 2

2. Für $m \leq n$ existieren $n(n-1)...(n-m+1)$ verschiedene Injektionen der Menge A in die Menge B.

3. Lösung. Es sei B eine n-elementige Menge. Wir wählen eine beliebige Menge A mit $|A| = m$.
Das Bild von A bei jeder injektiven Abbildung $A \to B$ ist eine m-elementige Teilmenge von B, wobei man jede m-elementige Teilmenge von B auf diese Weise erhalten kann. Die Menge A besitzt ein und dasselbe Bild $A' \subset B$ bei verschiedenen Injektionen dann und nur dann, wenn diese sich durch eine Bijektion der Menge A in sich voneinander unterscheiden.

Da $|A'| = |A| = m$ ist, existieren $m!$ verschiedene Bijektionen von A auf sich. Daher gibt es

$$\frac{n(n-1)...(n-m+1)}{m!} = \binom{n}{m}$$

verschiedene m-elementige Teilmengen von B.

5. Auf jeder vertikalen bzw. horizontalen Geraden der graphischen Darstellung einer Bijektion ist ein und nur ein Gitterpunkt markiert. Bei der Darstellung einer Bijektion $A \to$B durch ein Pfeildiagramm geht von jedem Punkt, durch den ein Element von A bezeichnet wird, genau ein Pfeil aus, und zu jedem Punkt, der ein Element von B bezeichnet, führt ein und nur ein Pfeil.

7. 44. Hinweis. Zuerst muss man die Anzahl der Permutationen bestimmen, die wenigstens ein Element der Menge M unverändert lassen.

9. $6 \cdot 7^5$.

10. Es seien G_1 und G_2 die Mengen der Permutationen φ, die den Bedingungen $\varphi(1) - \varphi(2) > 0$ bzw. $\varphi(1) - \varphi(2) < 0$ genügen. Offenbar ist jede Permutation

in einer dieser Mengen enthalten.
Da die Abbildung von G_1 auf G_2, durch welche jeder Permutation

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i_1 & i_2 & i_3 & ... & i_n \end{pmatrix}$$

aus G_1 die Permutation

$$\varphi' = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i_2 & i_1 & i_3 & ... & i_n \end{pmatrix}$$

aus G_2 zugeordnet wird, bijektiv ist (man beweise dies!), gilt $|G_1| = |G_2| = n!/2$. Für $(n-1)!$ Permutationen der Menge G_1 gilt (1) $\varphi - (2)\varphi = 1$. Folglich existieren $(n!/2) - (n-1)!$ Permutationen, welche die Voraussetzung der Aufgabe erfüllen.

Abschnitt 3

2) a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 1 & 1 \end{pmatrix}$; b) $\begin{pmatrix} a & b & c & d & e \\ c & d & c & d & c \end{pmatrix}$; c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 3 & 2 & 3 \end{pmatrix}$.

4. Die Ecke (a, b) eines Koordinatennetzes wird bei der Konstruktion der graphischen Darstellung der Transformationen $\varphi \circ \psi$ dann und nur dann markiert, wenn eine Zahl $c \in M$ existiert derart, dass auf der graphischen Darstellung der Transformationen φ die Ecke (a, c) und auf der graphischen Darstellung der Transformation ψ die Ecke (c, b) markiert ist.

5. Wir nehmen zunächst an, φ sei keine, Permutation. Dann gibt es Elemente $a, b \in M$, $a \neq b$, derart, dass $(a)\varphi = (b)\varphi$ ist. Für sie gilt

$$(a)(\varphi \circ \psi) = ((a)\varphi)\psi = ((b)\varphi)\psi = (b)(\varphi \circ \psi)$$

was der Bedingung der Aufgabe widerspricht. Ist ψ keine Permutation, so ist die Menge der Bilder der Elemente von M vermöge der Operation ψ eine echte Teilmenge von M. Folglich erschöpfen die Elemente der Gestalt $(a)(\varphi \circ \psi) = ((a)\varphi)\psi$, $a \in M$, nicht die ganze Menge M, d. h., die Transformation $\varphi \circ \psi$ ist nicht surjektiv, und das widerspricht der Annahme der Aufgabe.

6. Hinweis. Man benutze die in der vorhergehenden Aufgabe formulierte Aussage.

7. a) $x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 2 & 6 & 3 \end{pmatrix}$; b) $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$.

8. a) Die Gleichung besitzt keine Lösung; b) die Gleichung besitzt die vier Lösungen:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 2 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 3 \end{pmatrix}$$

c) Die Gleichung besitzt keine Lösung; d) die Gleichung besitzt die einzige Lösung

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 2 & 2 & 2 \end{pmatrix}$$

Abschnitt 4

1. a) Nein; b) ja; c) ja.

2. a) Nein; b) ja; c) ja; d) keine dieser Halbgruppen ist eine Gruppe.

4. Die Multiplikationstabelle einer abelschen Gruppe ist symmetrisch bezüglich der "Achse", die von der linken oberen zur rechten unteren Ecke führt.

Abschnitt 5

1. Nein. Wenn der Graph eine Transformation liefert, führt aus jedem seiner Knotenpunkte ein und nur ein Pfeil heraus.

3. Auf dem Graphen des Produkts $\varphi \circ \psi$ der Transformationen φ und ψ der Menge M lassen sich die Punkte, welche Bilder der Elemente a und b von M sind, dann und nur dann durch einen Pfeil in Richtung von a nach b verbinden, wenn ein Punkt c existiert derart, dass sich auf dem Graphen der Transformation φ die Punkte a und c durch einen Pfeil in Richtung von a nach c und auf dem Graphen der Transformation ψ die Punkte c und b durch einen Pfeil von c nach b verbinden lassen.

Abschnitt 6

1. a) 12; b) 9.

2. 1, 2, 3, 4, 5, 6.

3. 30.

4. $(a_n, a_{n-1}, ..., a_2, a_1)$.

5. Hinweis. Man betrachte die Permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

6. $8!/3 \cdot 5$. Hinweis. Man benutze die Lösung der Aufgabe 11 von Abschnitt 5.

9. Besitzt die Permutation φ die Zerlegung

$$\varphi = \underbrace{(a_1, ..., a_s) \cdot (b_1, ..., b_s) \circ ... \circ (c_1, ..., c_s)}_{l}$$

so leistet der Zyklus ψ

$$psi = (a_1, b_1, ..., c_1, a_2, b_2, ..., c_2, a_s, b_s, ..., c_s)$$

das Gewünschte. Man überzeuge sich von der Gültigkeit der Gleichung $\psi^l = \varphi$.

Abschnitt 7

1. a)

$$\begin{aligned}(1,3,4,7) &= (1,3)\circ(1,4)\circ(1,7)\\ &= (1,2)\circ(4,5)\circ(5,6)\circ(6,7)\circ(6,5)\circ(5,4)\circ(4,3)\circ(3,2)\circ(2,1)\\ &= (1,2)\circ(1,2,3,4,5,6,7)^{-3}\circ(1,2)\circ(1,2,3,4,5,6,7)^{-1}\circ(1,2)\\ &\circ(1,2,3,4,5,6,7)^{-1}\circ(1,2)\circ(1,2,3,4,5,6,7)^{-1}\circ(1,2)\circ(1,2,3,4,5,6,7)\\ &\circ(1,2,3,4,5,6,7)(1,2)\circ(1,2,3,4,5,6,7)\circ(1,2)\circ(1,2,3,4,5,6,7)\circ(1,2).\end{aligned}$$

2. Ja.

3. Aus der Gleichung $(i,j,k) = (i,j)\circ(i,k)$ folgt $(i,j) = (i,j,k)\circ(i,k)$. Bei festgehaltenen i,k ergibt sich, dass man die Transpositionen der Gestalt (i,j) (i fest, j beliebig) durch die angegebenen Permutationen ausdrücken kann. Man muss sich noch davon überzeugen, dass die Menge dieser Transpositionen ein Erzeugendensystem von S_n ist.

4. Nein.

Abschnitt 8

1. Die Gruppe S_4 enthält die vier 3elementigen Untergruppen

$$\{\varepsilon,(1,2,3),(1,3,2)\},\{\varepsilon,(1,2,4),(1,4,2)\},\{\varepsilon,(1,3,4),(1,4,3)\},\{\varepsilon,(2,3,4),(2,4,3)\}$$

2. $\binom{5}{2}+\binom{5}{2}\cdot\binom{3}{2}=40$

4. Das Zentrum von S_4 ist die triviale Untergruppe $\{\varepsilon\}$.

5. 20.

6. Hinweis. Zu jeder Permutation $\alpha\in K$ existiert eine natürliche Zahl l derart, dass $\alpha^l=\varepsilon$ ist (z. B. die Ordnung der Permutation α). Daher ist $\alpha^{-1}=\alpha^{l-1}$.

Abschnitt 13

2. Die Trägheitsgruppe des Polynoms $f(x_1,x_2,x_3,x_4)$ ist die zyklische Gruppe $\{\varepsilon,(2,4)\}$ der Ordnung 2.

3. Die Trägheitsgruppe des Polynoms $A(x_1,x_2,x_3,x_4)$ besteht aus 12 Permutationen.

4. Beweis. Wir betrachten das Polynom $f(x_1,x_2,...,x_n) = x_1+2x_2+...+nx_n$. Seine Trägheitsgruppe ist trivial. Außerdem gilt für jede von der identischen verschiedene Permutation $\sigma\in S_n$ die Beziehung $f^\sigma\neq f$; daher ist für jede Untergruppe $G=\{\alpha_1,\alpha_2,...,\alpha_k\}$ der Gruppe S_n das Polynom

$$f^{\alpha_1}f^{\alpha_2}...f^{\alpha_k}=h(x_1,x_2,...,x_n)$$

invariant bezüglich derjenigen Permutationen (und nur dieser), die zur Untergruppe G gehören.

5. $o_4(x_1^2x_2x_3^2x_4)$ enthält sechs Monome.

7. $o_n(x_1x_2...x_l)$, $l \leq n$, enthält $\binom{n}{l} = n!/l!(n-l)!$ Monome.

Abschnitt 14

2. Die Ordnung 5.

4. Die Untergruppe, die drei Elemente enthält.

5. Das Zentrum der Gruppe A_n ist die triviale Untergruppe $(n > 3)$.
Hinweis. Man beweise, dass jede gerade Permutation, die mit allen Zyklen der Länge 3 vertauschbar ist, die identische Permutation ist.

7. Hinweis. Man benutze die Gleichungen

$$(i,j,k) = (i,j) \circ (i,k), \qquad (i,j) \circ (k,l) = (i,l,k) \circ (i,j,k)$$

wobei i, j, k, l verschiedene Elemente der Menge $\{1, 2, ..., n\}$ sind.

8. Ja.

10. Hinweis. Man benutze die Tatsache, dass für die Anzahl T_n^k der Permutationen einer n-elementigen Menge, deren zweite Zeile genau k Inversionen enthält, die Beziehung

$$T_n^k = T_{n-1}^k + T_{n-1}^{k-1} + ... + T_{n-1}^{k-n-1}$$

gilt, wobei $T_n^j = 0$ für $j < 0$ bzw. $j > (n-1)/2$ ist.

9. Man beweise, dass sich bei Multiplikation einer Permutation mit einer Transposition die Anzahl der Inversionen in der zweiten Zeile um 1 vermehrt oder vermindert.

11. Hinweis. Man zerlege jeden Zyklus einer in Zyklenschreibweise angegebenen Permutation in ein Produkt von Transpositionen und bestimme deren Anzahl.

Abschnitt 15

1. a) $s_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$

b) $s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$

c) $o_3(x_1^2x_2) = \sigma_1\sigma_2 - 3\sigma_3$.

2. a) $\{(4;16)\text{fl}(16;4)\}$; b) $\{(2;3)\text{fl}(3;2)\text{fl}(2;-5)\text{fl}(-5;2)\}$; c) $\{(1;3),(3;1)\}$.

3. Hinweis. Man drücke die Produkte je zweier der Seitenlängen des Dreiecks und das Produkt der Längen aller seiner Seiten durch die gegebenen Zahlen aus und benutze die Tatsache, dass in der Heronschen Formel unter dem Wurzelzeichen ein symmetrisches Polynom steht.

4. Hinweis. Für das Polynom $f(x_1, x_2)$ betrachte man das Monom $ax_1^kx_2^l$, in welchem k der höchste Exponent ist. Wenn es mehrere solche Monome gibt, muss man dasjenige nehmen, in welchem l der höchste Exponent ist.

Man beweise, dass ein Monom mit diesen Eigenschaften beim Übergang von $f(x_1, x_2)$ zu $f(x_1 + x_2, x_1x_2)$ nicht verschwinden kann.

6. In der Tat, vertauscht man in dem Polynom $f(x_1, x_4)$ die Plätze von x_1 und x_4, so ändert sich natürlich das Vorzeichen nicht, obwohl es sich doch eigentlich umkehren sollte. Daher ist $f(x_1, x_1) = -f(x_1, x_1)$, also $f(x_1, x_1)$ identisch gleich 0.

8. Hinweis. Man beweise, dass $f(x_1, x_2, x_3) = 4\max(x_1, x_2, x_3)$ ist.

Abschnitt 17

4. a) Ja; b) nein.

5. Hinweis. Auf jeden Spielstein schreiben wir eine neue Nummer nach folgender Regel: Ist die alte Nummer 14 (15), so ist die neue Nummer 15 (bzw. 14). Auf allen anderen Steinen stimmt die neue Nummer mit der alten überein. Die Steine selbst werden wir nicht verschieben.
Die Anordnung der Steine mit den neuen Nummern wird durch eine gerade Permutation charakterisiert, daher kann man von dieser zur Standardanordnung bezüglich der neuen (!) Nummern übergehen. Die Standardanordnung bezüglich der neuen Nummern ist gerade die gewünschte Anordnung bezüglich der alten Nummern.

6. Hinweis. Man nummeriere die Buchstaben in der Reihenfolge, in der sie in dem Wort Fünfzehnerspiel stehen. Dabei berücksichtige man, dass manche Buchstaben (die Buchstaben e, f, n) mehrfach vorkommen und, benutze zur Lösung die vorhergehende Aufgabe.

19 Literatur

ALEXANDROFF, P. S., Einführung in die Gruppentheorie, 9. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1975 (Übersetzung aus dem Russischen).

BANDELOW, CH., Einführung in die Cubologie, Vieweg, Braunschweig - Wiesbaden 1981.

FLACHSMEYER, J., Kombinatorik - Eine Einführung in die mengentheoretische Denkweise, 3. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1972.

GROSSMAN, I., and W. MAGNUS, Groups and their graphs, New York 1964.

HINTZE, W., Die Verwandten des Zauberwürfels, VEB Deutscher Verlag der Wissenschaften, Berlin 1985.

KEMENY, J. G., J. L. SNELL and G. L. THOMPSON, Introduction to finite Mathematics, Prentice Hall, Englewood Cliffs (N.Y.) 1957.

KLOTZEK, B., U. LENGTAT, E. LETZEL und K. SCHRÖTER, kombinieren, parkettieren, färben, VEB Deutscher Verlag der Wissenschaften, Berlin 1985.

KUROSCH, A. G., Algebraische Gleichungen beliebigen Grades, 5.Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1969 (Übersetzung aus dem Russischen).

LOVASZ, L., J. PELIKAN und K. L. VESZTERGOMBI, Kombinatorik, BSE B. G. Teubner Verlagsgesellschaft, Leipzig 1977 (Übersetzung aus dem Ungarischen).

MARKUSCHEWITSCH, A. I., Komplexe Zahlen und konforme Abbildungen, 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1973 (Übersetzung aus dem Russischen).

MATHIAK, K., und P. STINGL, Gruppentheorie für Chemiker, Physiko-Chemiker, Mineralogen, 2. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1969.

OKUNJEW, L. J., Der Ring der Polynome und der Körper der rationalen Funktionen, in: Enzyklopädie der Elementarmathematik II, 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1967 (Übersetzung aus dem Russischen).

SEDLACEK, J., Einführung in die Graphentheorie, BSB B. G. Teubner Verlagsgesellschaft, Leipzig 1972 (Übersetzung aus dem Tschechischen).

PIEPER, H., Die komplexen Zahlen, VEB Deutscher Verlag der Wissenschaften, Berlin 1984.

SIEMON, H., Anwendungen der elementaren Gruppentheorie in Zahlentheorie und Kombinatorik, Klett Verlag, Stuttgart 1981.