

Prof. Dr. J. Ziegenbalg
Institut für Mathematik und Informatik
Pädagogische Hochschule Karlsruhe

email: ziegenbalg@ph-karlsruhe.de
homepage: <http://www.ph-karlsruhe.de/~ziegenbalg>

Zum Begriff der Gruppe, dem Satz von Lagrange und den Sätzen von Fermat und Euler

Definitionen, Grundbegriffe, Beispiele

Definition: Eine *Gruppe* ist ein Tripel (G, \circ, e) bestehend aus einer Menge G , einer zweistelligen Verknüpfung $\circ: G \times G \rightarrow G$ und einem speziellen Element $e \in G$ mit den folgenden Eigenschaften:

- (i) Die Verknüpfung \circ ist *assoziativ*; d.h., für alle $a, b, c \in G$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$.
- (ii) Für alle $x \in G$ gilt $x \circ e = e \circ x = x$.
- (iii) Zu jedem Element $x \in G$ gibt es ein Element $y \in G$ mit der Eigenschaft $x \circ y = y \circ x = e$.

Definitionen:

- (i) Falls für alle $a, b \in G$ stets $a \circ b = b \circ a$ gilt, so heißt die Gruppe *kommutativ* oder auch *Abelsche*¹ Gruppe.
- (ii) Falls G eine endliche Menge ist, so heißt (G, \circ, e) *endliche* Gruppe; andernfalls *unendliche* Gruppe.
- (iii) Die Mächtigkeit (d.h. im Falle einer endlichen Gruppe die Elementzahl) der Gruppe G heißt die *Ordnung* von G .

Im Zeichen: $|G| = \text{Ordnung von } G$.

Bemerkungen:

- (i) Die Menge G wird auch als die *Trägermenge* der Gruppe bezeichnet. Wenn keine Verwechslungsgefahr besteht, spricht man oft auch kurz von der Gruppe G .
- (ii) Als Verknüpfungssymbol für die (zweistellige) Verknüpfung wird auch das gewöhnliche Multiplikationszeichen (\cdot) und das Additionszeichen $(+)$ verwendet; letzteres meist bei kommutativen Gruppen. Das Multiplikationszeichen wird gelegentlich auch

¹ Niels Henrik Abel (1802-1829), norwegischer Mathematiker

weggelassen, wenn keine Verwechslungsgefahr besteht. An Stelle von $a \circ b$ wird also auch $a \cdot b$, $a + b$ oder ab geschrieben.

- (iii) Das spezielle Element $e \in G$ heißt *neutrales Element*. Wird die Gruppe multiplikativ geschrieben, so verwendet man auch das Symbol 1 für das neutrale Element; wird die Gruppe additiv geschrieben, so verwendet man meist das Symbol 0 für das neutrale Element.
- (iv) Sind $x, y \in G$ mit $x \circ y = y \circ x = e$, so heißen x und y zueinander *invers*.

Beispiele:

1. Die Menge D_3 der Deckabbildungen eines gleichseitigen Dreiecks mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung und der identischen Abbildung als neutralem Element. Gruppenelemente sind: 3 Drehungen (um 120, 240 und 360 Grad) um den Schwerpunkt; 3 Achsenspiegelungen an den (ortsfesten) Mittelsenkrechten. Neutrales Element: Die Drehung um 360 Grad (= 0 Grad), also die *identische Abbildung*.

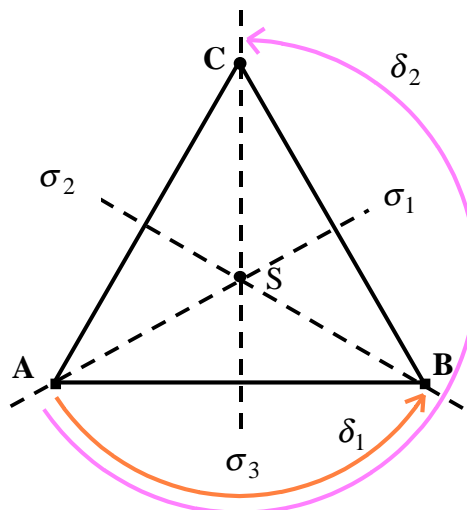
Etwas genauer:

In der folgenden Abbildung seien A, B und C (ortsfeste) Punkte in der Ebene, die ein gleichseitiges Dreieck bestimmen. S sei der Schwerpunkt dieses Dreiecks. Weiterhin seien:

- δ_1 die Drehung um S (entgegen dem Uhrzeigersinn) um 120 Grad,
 δ_2 die Drehung um S um 240 Grad, und
 δ_0 die Drehung um S um 360 Grad (= 0 Grad).

Schließlich seien

- σ_1 die (Achsen-) Spiegelung an der (ortsfesten) Achse AS,
 σ_2 die Spiegelung an der Achse BS, und
 σ_3 die Spiegelung an der Achse CS.



Bei endlichen Gruppen lässt sich die Wirkung der Verknüpfung vollständig in einer tabellenartigen Form, der sogenannten *Verknüpfungstafel* darstellen. Die im folgenden dargestellte Verknüpfungstafel zur Gruppe D_3 ist folgendermaßen zu lesen: Das Ergebnis des Produkts

Spalten-Element *mal* Zeilen-Element

ist im „Kreuzungspunkt“ dargestellt. Dabei ist zuerst die Abbildung in der (linken) Spalte und dann die Abbildung in der (oberen) Zeile auszuführen.

Beispiel: $\delta_1 \circ \sigma_2 = \sigma_3$

\circ	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_0	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_1	δ_1	δ_2	δ_0	σ_2	σ_3	σ_1
δ_2	δ_2	δ_0	δ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	δ_0	δ_2	δ_1
σ_2	σ_2	σ_1	σ_3	δ_1	δ_0	δ_2
σ_3	σ_3	σ_2	σ_1	δ_2	δ_1	δ_0

- Die Menge \mathbb{Z} der ganzen Zahlen mit der gewöhnlichen Addition von ganzen Zahlen als Gruppenverknüpfung und der Zahl Null (0) als neutralem Element.
- Die Menge \mathbb{B} der Brüche (d.h. der positiven rationalen Zahlen) mit der gewöhnlichen Multiplikation von Brüchen als Gruppenverknüpfung und der Zahl Eins (1) als neutralem Element.
- Ist M eine Menge, so ist die Menge der *Permutationen* von M eine Gruppe mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung und der identischen Abbildung als neutralem Element.

Permutationen endlicher Mengen können in der Form von Zuordnungstabellen dargestellt werden; die Permutation σ z.B. in der Form

$$\sigma = \begin{pmatrix} a & b & c & d & e & f & g & h & j & k \\ f & e & c & k & b & g & j & h & a & d \end{pmatrix}$$

Dabei ist $\sigma(a) = f$, $\sigma(b) = e$, $\sigma(c) = c$, ..., $\sigma(k) = d$

Zyklenschreibweise der Permutation σ : $(a, f, g, j)(b, e)(c)(d, k)(h)$

Zyklen der Länge 2 heißen *Transpositionen*. Zyklen der Länge 1 werden meist weggelassen; d.h. $\sigma = (a, f, g, j)(b, e)(d, k)$. Ein Element x mit $\sigma(x) = x$ heißt *Fixpunkt* der Permutation σ . Permutationen ohne Fixpunkte heißen *fixpunktfrei*.

Mit S_n wird die Gruppe aller Permutationen der Menge $\{1, 2, 3, \dots, n\}$ bezeichnet. Sie heißt die *symmetrische Gruppe* über der Menge $\{1, 2, 3, \dots, n\}$.

Satz: $|S_n| = n!$ (Beweis: Übung)

Satz: Die Gruppe D_3 ist strukturgleich zur Gruppe S_3 .

Aufgabe: Auch wenn bisher keine formale Definition des Begriffs „strukturgleich“ gegeben wurde, erläutern Sie, was damit gemeint sein könnte und beweisen Sie den Satz.

5. Die Menge $\mathbb{Z}/n\mathbb{Z}$ (vgl. [Zbg 2001]) der Restklassen modulo n bildet zusammen mit der Restklassenaddition eine endliche, kommutative Gruppe mit neutralem Element $\bar{0}$.

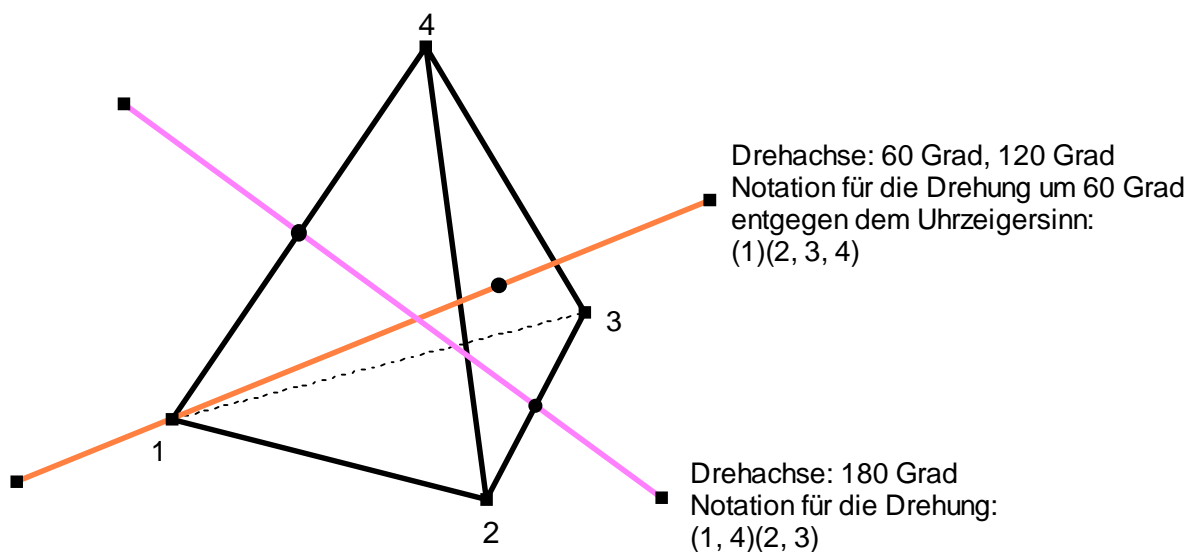
Beispiel: $n = 6$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

6. Die Menge T der Deckabbildungen eines (regelmäßigen) Tetraeders, zusammen mit der Hintereinanderausführung von Abbildungen als Gruppenverknüpfung. T besitzt die folgenden 12 Elemente:

- * Drehungen jeweils um die Achse durch eine Ecke und den Schwerpunkt der gegenüberliegenden Seite um 60 bzw. 120 Grad. Dies sind 8 ($= 4 \cdot 2$) Drehungen (eine davon ist in der Abbildung anhand der roten Achse dargestellt).
- * Drehungen jeweils um die Achse durch die Seitenmitten zweier gegenüberliegender Seiten um 180 Grad. Dies sind 3 Drehungen (eine davon ist in der Abbildung anhand der blauen Achse dargestellt).
- * die identische Abbildung (neutrales Element).

(Die Gruppe T wird auch als *Tetraedergruppe* bezeichnet.)



Die Eindeutigkeit der inversen Elemente

Satz (Eindeutigkeit des inversen Elements): Sei $x \in G$. Ist y ein zu x inverses Element und z ein Element von G mit der Eigenschaft $x \circ z = e$, so ist $y = z$.

Beweis: $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$.

Bemerkung: Sei $x \in G$. Ein zu x inverses Element y ist also eindeutig bestimmt. Es heißt *das* Inverse von x und wird (in funktionaler Schreibweise) in der Form x^{-1} geschrieben. Es gilt also $x \circ x^{-1} = x^{-1} \circ x = e$.

Im Falle der additiven Schreibweise wird für das Inverse von x in der Form $-x$ geschrieben. Es gilt dann $x + (-x) = (-x) + x = 0$.

Definition: (aggregierende Schreibweisen)

(i) multiplikative Schreibweise – Potenzierung

$$x^1 = x, x^2 = x \circ x, x^3 = x \circ x \circ x, \dots, x^n = x \circ x^{n-1}, \dots$$

$$x^0 = e$$

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

Hinweis: Permanenzprinzip von Hermann Hankel; siehe:

<http://www.ph-karlsruhe.de/~ziegenbalg/PermSig.pdf>

(ii) additive Schreibweise – Vervielfachung

$$1 \cdot x = x, 2 \cdot x = x + x, 3 \cdot x = x + x + x, \dots, n \cdot x = x + (n-1) \cdot x, \dots$$

$$0 \cdot x = 0$$

$$(-2) \cdot x = (-x) + (-x), (-3) \cdot x = (-x) + (-x) + (-x), \dots, (-k) \cdot x = (-x) + (-(k-1))x, \dots$$

Die Links-Multiplikation

Definition: Sei $a \in G$. Die Abbildung $l_a : G \rightarrow G$ mit $l_a(x) = a \circ x$ heißt *Links-Multiplikation* (genauer eigentlich: *Links-Verknüpfung*) mit dem Element a .

Beispiele:

Gruppe: $(\mathbb{B}, \text{gewöhnliche Multiplikation}, 1)$: $l_2(x) = 2 \cdot x$

Gruppe: $(\mathbb{Z}, +, 0)$: $l_{17}(x) = 17 + x$

Satz: Die Links-Multiplikation ist bijektiv.

Beweis: Die Umkehrabbildung von l_a ist die durch das Inverse von a gegebene Links-Multiplikation $l_{a^{-1}}$. Für alle $x \in G$ gilt also $l_a(l_{a^{-1}}(x)) = l_{a^{-1}}(l_a(x)) = x$.

Untergruppen

Definition: Sei (G, \circ, e) eine Gruppe und U eine Teilmenge von G mit den Eigenschaften:

- (i) $e \in U$
- (ii) Für alle $a, b \in U$ gilt $a \circ b \in U$.
- (iii) Für alle $a \in U$ ist $a^{-1} \in U$.

Dann heißt U *Untergruppe* von G .

Im Zeichen: $U \leq G$.

Bemerkungen:

- (i) Die Menge U ist also eine Untergruppe von G , wenn sie das neutrale Element von G enthält und bezüglich der Gruppenverknüpfung von G und der Inversenbildung abgeschlossen ist.
- (ii) Mit anderen Worten: Ist (U, \circ, e) mit der auf U eingeschränkten Verknüpfung von G und mit dem neutralen Element $e \in G$ ebenfalls eine Gruppe, so ist U eine *Untergruppe* von G .

Beispiele: Wir betrachten die Gruppe D_3 der Deckabbildungen eines gleichseitigen Dreiecks (siehe Definition des Gruppenbegriffs: Beispiel 1). Ihrer Gruppentafel entnehmen wir die folgenden Untergruppen:

- die „trivialen“ Untergruppen: $\{\delta_0\}$ und D_3 selbst,
- die Untergruppen der Ordnung 2: $\{\sigma_1, \delta_0\}$, $\{\sigma_2, \delta_0\}$ und $\{\sigma_3, \delta_0\}$,
- die Untergruppe der Ordnung 3: $\{\delta_1, \delta_2, \delta_0\}$.

\circ	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_0	δ_0	δ_1	δ_2	σ_1	σ_2	σ_3
δ_1	δ_1	δ_2	δ_0	σ_2	σ_3	σ_1
δ_2	δ_2	δ_0	δ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	δ_0	δ_2	δ_1
σ_2	σ_2	σ_1	σ_3	δ_1	δ_0	δ_2
σ_3	σ_3	σ_2	σ_1	δ_2	δ_1	δ_0

Aufgabe: Zeigen Sie, dass dies alle Untergruppen von D_3 sind. (Hinweis: Nehmen Sie an, dass ein beliebiges Element x in einer Untergruppe U von D_3 enthalten ist und ziehen Sie Schlüsse daraus, welche weiteren Elemente noch in U enthalten sein müssen, damit die Untergruppenkriterien erfüllt sind.)

Aufgabe:

- (i) Ermitteln Sie alle Untergruppen der Tetraedergruppe T (siehe Beispiel 6).
- (ii) Ermitteln Sie alle Untergruppen der Restklassengruppen $\mathbb{Z}/n\mathbb{Z}$ für $n=5, 6, 8$ und 12 .

Nebenklassen

Definition: Es sei G eine Gruppe, U eine Untergruppe von G und a ein beliebiges Element von G . Dann heißt die Menge

$$a \circ U := \{a \circ x / x \in U\}$$

die durch a gegebene *Links-Nebenklasse* von U .

Bei multiplikativ geschriebenen Gruppen schreibt man meist kurz aU an Stelle von $a \circ U$.

(Entsprechend ist der Begriff der Rechts-Nebenklasse definiert durch: $Ua := \{x \circ a / x \in U\}$.)

Bemerkung: Offensichtlich ist: $aU = l_a(U)$.

Beispiele: Wir betrachten die Gruppe D_3 der Deckabbildungen eines gleichseitigen Dreiecks.

Die Links-Nebenklassen der Untergruppe $U := \{\sigma_1, \delta_0\}$ sind:

- $\delta_0 \circ \{\sigma_1, \delta_0\} = \{\sigma_1, \delta_0\}$
- $\delta_1 \circ \{\sigma_1, \delta_0\} = \{\sigma_2, \delta_1\}$
- $\delta_2 \circ \{\sigma_1, \delta_0\} = \{\sigma_3, \delta_2\}$
- $\sigma_1 \circ \{\sigma_1, \delta_0\} = \{\sigma_1, \delta_0\} \quad (= \delta_0 \circ U = U)$
- $\sigma_2 \circ \{\sigma_1, \delta_0\} = \{\delta_1, \sigma_2\} \quad (= \delta_1 \circ U)$
- $\sigma_3 \circ \{\sigma_1, \delta_0\} = \{\delta_2, \sigma_3\} \quad (= \delta_2 \circ U)$

Es gibt also drei Links-Nebenklassen zur Untergruppe $U = \{\sigma_1, \delta_0\}$ von D_3 .

Aufgabe: Geben Sie die Links-Nebenklassen der restlichen Untergruppen von D_3 an.

Aufgabe:

- (i) Ermitteln Sie die Links-Nebenklassen aller Untergruppen der Tetraedergruppe T (siehe Beispiel 6).
- (ii) Ermitteln Sie die Links-Nebenklassen aller Untergruppen der Restklassengruppen $\mathbb{Z}/n\mathbb{Z}$ für $n=5, 6, 8$ und 12 .
- (iii) Führen Sie entsprechendes für die Rechts-Nebenklassen durch

Satz: (Eigenschaften von Nebenklassen)

Es sei G eine Gruppe und U eine Untergruppe von G . Dann gilt

- (i) Für alle $x \in G$ gilt: $x \in U \Leftrightarrow xU = U$.
- (ii) xU ist stets gleichmächtig zu U .
- (iii) Für alle $x, y \in G$ gilt: $xU = yU \Leftrightarrow y^{-1}x \in U$.
- (iv) Für alle $y \in G \setminus U$ gilt: $yU \cap U = \emptyset$.
- (v) $G = \bigcup_{x \in G} xU$

Beweis:

- (i) " \Rightarrow ": Es sei $x \in U$. Dann ist (wegen der Abgeschlossenheitseigenschaft von U) $xU = \{x \circ u / u \in U\} \subseteq U$. Weiterhin kann jedes Element $t \in U$ in der Form $t = x \circ u$ (mit einem geeigneten Element $u \in U$) geschrieben werden. Man verwende dazu $u := x^{-1} \circ t$. Also ist $xU = U$.
" \Leftarrow ": Es sei nun $xU = U$. Dann ist insbesondere $x \circ e \in U$, also $x \in U$.
- (ii) Dies folgt aus der Tatsache, dass die Links-Multiplikation als Abbildung bijektiv ist.
- (iii) Übung
- (iv) (Beweis durch Widerspruch) Angenommen $yU \cap U \neq \emptyset$. Dann gibt es ein Element x mit $x \in yU \cap U$. Daraus folgt: Es gibt ein $t \in U$ mit der Eigenschaft $y \circ t = x$. Daraus folgt $y = x \circ t^{-1} \in U$ – im Widerspruch zur Annahme $y \notin U$.
- (v) Für jedes $x \in G$ gilt $x \in xU$.

Bemerkung: Die Eigenschaften (iv) besagt, dass verschiedene Nebenklassen von U *disjunkt* sind.

Die Eigenschaften (iv) und (v) besagen, dass die Gesamtheit der Nebenklassen von U eine *Zerlegung* von G darstellt.

Der Index einer Untergruppe

Definition: Es sei G eine Gruppe und U eine Untergruppe von G . Die Anzahl der Links-Nebenklassen von U in G heißt der *Index* von U in G .

Im Zeichen: $|G : U| = \text{Index von } U \text{ in } G$.

Beispiel: Die additive Gruppe $\mathbb{Z}_{12} := \mathbb{Z}/_{12}\mathbb{Z}$ der Restklassen modulo 12. (Der Einfachheit halber sind die Restklassen im folgenden Beispiel durch Fettschrift an Stelle der Überstreichung gekennzeichnet.)

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Eine der Untergruppen von Z_{12} ist $U := \{0, 3, 6, 9\}$. Die Links-Nebenklassen von U sind:

$$0+U = \{0, 3, 6, 9\} = U, \quad 1+U = \{1, 4, 7, 10\} \quad \text{und} \quad 2+U = \{2, 5, 8, 11\}$$

Man beachte: Es gibt 3 Links-Nebenklassen zu je 4 Elementen; $3 \cdot 4 = 12$.

$$Z_{12} = U \cup (1+U) \cup (2+U) \quad (\text{disjunkte Vereinigung; „Zerlegung“})$$

*Satz von Lagrange*²: Es sei G eine *endliche* Gruppe und U eine Untergruppe von G . Dann gilt:
 $|G| = |G:U| \cdot |U|$.

Beweis: Für jede Gruppe G gilt $G = \bigcup_{x \in G} xU$. Da G eine endliche Gruppe ist, gibt es nur endlich

viele verschiedene Links-Nebenklassen von U ; diese seien mit g_1U, g_2U, \dots, g_kU bezeichnet. Also ist (wegen der Disjunktheits-Eigenschaft der Links-Nebenklassen)

$|G| = |g_1U \cup g_2U \cup \dots \cup g_kU| = |g_1U| + |g_2U| + \dots + |g_kU|$. Da alle Links-Nebenklassen von U gleichmächtig sind, folgt daraus: $|G| = k \cdot |U|$. Da k als die Anzahl der Links-Neben-

klassen von U (also als der Index von U in G) definiert war, folgt $|G| = |G:U| \cdot |U|$.

Folgerung und Bemerkung zur und Motivation der Bezeichnungsweise: $|G:U| = \frac{|G|}{|U|}$.

Erzeugende Elemente und zyklische Gruppen

Satz (Durchschnittsbildung und Untergruppen):

- (i) Der Durchschnitt zweier Untergruppen einer Gruppe G ist eine Untergruppe von G .

² Joseph Louis Lagrange (1736–1813); italienisch-französischer Mathematiker

- (ii) Der Durchschnitt beliebig vieler Untergruppen einer Gruppe G ist eine Untergruppe von G .

Beweis: Übung

Definitionen: Es sei G eine Gruppe und M eine Teilmenge von G . Es sei $D := \bigcap_{M \subseteq U \leq G} U$ der

Durchschnitt aller Untergruppen von G , welche die Menge M enthalten. Dann ist D ebenfalls eine Untergruppe von G ; sie wird als die von der Menge M erzeugte Untergruppe bezeichnet.

Im Zeichen: $\langle M \rangle :=$ die von M erzeugte Untergruppe von G .

Besteht die Menge M nur aus einem Element x , ist also $M = \{x\}$, so schreibt man auch kurz $\langle x \rangle$ an Stelle von $\langle \{x\} \rangle$ und bezeichnet $\langle x \rangle$ als die von dem Element x erzeugte Untergruppe.

Gruppen, die von einem Element x erzeugt werden können, heißen *zyklische* Gruppen.

Bemerkung: Es sei G eine zyklische Gruppe; etwa $G = \langle x \rangle$. Aufgrund der Abgeschlossenheit von G , muss G alle Produkte der Form $x, x \circ x, x \circ x \circ x, \dots, x^n, \dots, x^{-1}, x^{-1} \circ x^{-1}, x^{-1} \circ x^{-1} \circ x^{-1}, \dots, x^{-k}, \dots$ sowie das neutrale Element e enthalten.

Beispiele:

- Die Menge der rationalen Zahlen (mit der gewöhnlichen Multiplikation) enthält die zyklische Gruppe $\langle 2 \rangle := \{2^x / x \in \mathbb{Z}\}$; m.a.W.: die (multiplikativ geschriebene) zyklische Gruppe $\langle 2 \rangle$ besteht aus den Elementen $2, 2^2, 2^3, \dots, 2^n, \dots$ sowie $2^{-1}, 2^{-2}, \dots, 2^{-k}, \dots$ und dem neutralen Element 1.
- Die Menge der ganzen Zahlen (mit der gewöhnlichen Addition) enthält die zyklische Gruppe $\langle 6 \rangle$ der durch 6 teilbaren ganzen Zahlen; m.a.W.: die (additiv geschriebene) zyklische Gruppe $\langle 6 \rangle$ besteht aus den Elementen $6, 12, 18, \dots, n \cdot 6, \dots$, sowie $-6, -12, -18, \dots, -k \cdot 6, \dots$ und dem neutralen Element 0.
- Die zyklische Gruppe der ebenen Drehungen eines regelmäßigen 8-Ecks besteht aus den 8 folgenden Drehungen (etwa im Uhrzeigersinn):
 - $\delta_1 =$ Drehung um 45 Grad
 - $\delta_2 =$ Drehung um 90 Grad
 - $\delta_3 =$ Drehung um 135 Grad
 - ...
 - $\delta_6 =$ Drehung um 270 Grad
 - $\delta_7 =$ Drehung um 315 Grad
 - $\delta_8 =$ Drehung um 360 Grad $= \delta_0 =$ Drehung um 0 Grad (dies ist das neutrale Element bzw. die identische Abbildung)

4. Die (additive) Gruppe $\mathbb{Z}/n\mathbb{Z}$ der Restklassen modulo n ist eine zyklische Gruppe, die z.B. von dem Element (der Restklasse) $\bar{1}$ erzeugt wird.

Für $n = 6$ ist z.B.: $\mathbb{Z}/n\mathbb{Z} = \{\bar{1}, \bar{1}+\bar{1}, \bar{1}+\bar{1}+\bar{1}, \bar{1}+\bar{1}+\bar{1}+\bar{1}, \bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}, \bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}\}$

bzw. $\mathbb{Z}/n\mathbb{Z} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

Dabei ist $\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1} = \bar{6} = \bar{0}$.

Bemerkung: Es sei G eine endliche zyklische Gruppe der Ordnung n ; etwa $G = \langle x \rangle$. Dann gilt

$$G = \{x, x^2, x^3, \dots, x^n\}. \text{ Insbesondere gilt } x^n = e \text{ und } x^{-1} = x^{n-1}.$$

Denn die Elemente x, x^2, x^3, \dots, x^n müssen alle verschieden sein, da sonst die Elementezahl von G nicht erreicht würde. Eines dieser Elemente muss das neutrale Element e von G sein. Dies ist nur im Falle $x^n = e$ möglich (sonst wäre wieder die Ordnungs-Bedingung verletzt). Aus $x \circ x^{n-1} = x^n = e$ folgt schließlich $x^{n-1} = x^{-1}$.

Definition: Sei G eine Gruppe und $x \in G$. Als Ordnung des Elements x (im Zeichen: $\text{ord}(x)$)

wird die kleinste positive natürliche Zahl n bezeichnet, für die die Gleichung $x^n = e$ gilt.

Mit anderen Worten: Die Ordnung des Elements x ist gleich der Ordnung der Untergruppe $\langle x \rangle$ von G .

Im Zeichen: $\text{ord}(x) = |\langle x \rangle|$

Satz (Ordnung von Gruppenelementen):

Sei G eine endliche Gruppe der Ordnung n und x ein beliebiges Element von G .

(i) Die Ordnung des Elements x ein Teiler der Gruppenordnung: $\text{ord}(x) \mid n$.

(ii) $x^n = e$

Beweis:

(i) Dies ist eine unmittelbare Folgerung aus dem Satz von Lagrange.

(ii) Es sei k der Index der Untergruppe $\langle x \rangle$ in G und r die Ordnung von x .

Nach dem Satz von Lagrange gilt $|G| = |G : \langle x \rangle| \cdot \text{ord}(x)$ bzw. $n = k \cdot r$. Mit diesen Bezeichnungen gilt: $x^n = x^{k \cdot r} = x^{r \cdot k} = (x^r)^k = e^k = e$.

Satz: Jede zyklische Gruppe ist kommutativ.

Beweis: Übung

Satz: Jede Gruppe von Primzahlordnung ist zyklisch.

Beweis: Übung

Gruppen primer Restklassen

Satz (Gruppe der primen Restklassen in $\mathbb{Z}/n\mathbb{Z}$)

Bezeichnungen und Basiswissen: siehe [Zbg 2001]

- (i) Es sei $R_n := \mathbb{Z}/n\mathbb{Z}$ die Menge der Restklassen modulo n . Die Menge $G_n \subseteq R_n$ sei wie folgt definiert: $G_n = \{\bar{x} \in R_n \mid \text{GGT}(x, n) = 1\}$. G_n enthält also genau die Restklassen, deren Repräsentant teilerfremd zu n ist. Dann bildet G_n mit der Restklassenmultiplikation eine Gruppe. Sie wird als die Gruppe der *primen Restklassen* modulo n bezeichnet.
- (ii) Die Gruppe der *primen Restklassen* modulo n hat die Ordnung $\varphi(n)$, wo φ die Eulersche Funktion („Totientenfunktion“) ist.
- (iii) Ist $n = p$ eine Primzahl, so hat die Gruppe der primen Restklassen modulo p die Ordnung $p - 1$.

Beweis:

- (i) *Zum neutralen Element:* Das neutrale Element $\bar{1}$ ist offensichtlich in G_n enthalten.

Zur multiplikativen Abgeschlossenheit: Es ist zu zeigen: Sind \bar{a} und \bar{b} Elemente von G_n , dann ist auch $\overline{a \cdot b}$ ein Element von G_n . Dazu ist zu zeigen: Ist $\text{GGT}(a, n) = 1$ und $\text{GGT}(b, n) = 1$, dann ist auch $\text{GGT}(a \cdot b, n) = 1$. Dies folgt unmittelbar aus dem Satz von der eindeutigen Primfaktorzerlegung.

Zur Abgeschlossenheit bezüglich der Inversenbildung: Zu zeigen: Jedes Element $\bar{a} \in G_n$ besitzt ein Inverses. Sei also $\text{GGT}(a, n) = 1$. Dann gibt es nach dem Satz von der Vielfachendarstellung ganze Zahlen x und y mit der Eigenschaft $1 = x \cdot a + y \cdot n$. Man findet diese ganzen Zahlen x und y mit Hilfe des erweiterten Euklidischen Algorithmus (Berlekamp Algorithmus). Modulo n betrachtet (also in R_n) bedeutet dies $\bar{1} = \bar{x} \cdot \bar{a}$. Das mit dem Berlekamp Algorithmus zu findende Element \bar{x} ist also das Inverse von \bar{a} .

- (ii) und (iii): Dies sind nur direkte Umsetzungen der Definition der Eulerschen Totientenfunktion [siehe Zbg 2001].

Die Sätze von Fermat und Euler

Satz (Fermat³): Es sei p eine Primzahl und a eine ganze Zahl, die nicht von p geteilt wird. Dann gilt $a^{p-1} \equiv 1 \pmod{p}$.

³ Pierre de Fermat (1601-1665), französischer Mathematiker

Satz (Euler⁴): Es sei n eine ganze Zahl und a eine zu n teilerfremde ganze Zahl. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Beweis: Die beiden letzten Sätze folgen unmittelbar aus dem Satz von Lagrange (bzw. dem Satz über die Ordnung von Gruppenelementen), angewandt auf die Gruppe der primen Restklassen.

⁴ Leonhard Euler (1707-1783), Schweizer Mathematiker

Literaturhinweise

- [Baum 1964] Baumgartner L.: Gruppentheorie; Walter de Gruyter & Co., Sammlung Götschen, Berlin 1964
- [B-C 1968] Baumslag G. and Chandler B.: Theory and Problems of Group Theory; Schaum's Outline Series, McGraw-Hill, 1968
- [Bud 1972] Budden F. J.: The Fascination of Groups; Cambridge University Press 1972
- [Bur 1955] Burnside W.: Theory of groups of finite order; Dover Publications, 1955 (2nd ed.)
- [Gor 1968] Gorenstein D.: Finite Groups; Harper & Row Publishers, New York 1968
- [Hup 1967] Huppert B.: Endliche Gruppen I; Springer Verlag, Berlin 1967
- [Koch 1966] Kochendörffer R.: Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen; Akademische Verlagsgesellschaft, Leipzig 1966
- [Led 1973] Ledermann: Introduction to Group Theory; Oliver & Boyd, Edinburgh 1973
- [Mar 1961] Hall M.: The theory of groups; The Macmillan Company, New York 1961 (2nd ed.)
- [Zbg 2001] Ziegenbalg J.: Basiswissen Zahlentheorie, Hochschulsript Pädagogische Hochschule Karlsruhe, 2001