§ 27. Zyklische Gruppen

In: Otakar Borůvka (author): Grundlagen der Gruppoid- und Gruppentheorie. (German). Berlin: VEB Deutscher Verlag der Wissenschaften, 1960. pp. 182--187.

Persistent URL: http://dml.cz/dmlcz/401519

2. Ist eine Gruppentafel einer endlichen Gruppe $\mathfrak{G}$ gegeben, so erhält man Symbole der linksseitigen Translationen auf $\mathfrak{G}$, wenn man den horizontalen Eingang und je eine Zeile der Multiplikationstabelle herausgreift. Ähnlich erhält man aus dem vertikalen Eingang und den einzelnen Spalten der Gruppentafel Symbole der rechtsseitigen Translationen auf $\mathfrak{G}$.

3. Ein reguläres Oktaeder hat 13 Symmetrieachsen (3 gehen durch je zwei gegenüberliegende Ecken, 6 durch die Mittelpunkte von je zwei gegenüberliegenden Kanten und 4 durch die Mittelpunkte von je zwei gegenüberliegenden Seitenflächen). Alle Drehungen des Oktaeders um die Symmetrieachsen, die das Oktaeder in sich selbst überführen, bilden eine Gruppe von der Ordnung 24, die sogenannte *Oktaedergruppe* (dabei werden gleichachsige Drehungen um Winkel, die sich nur um ganzzahlige Vielfache von 360° unterscheiden, als gleich angesehen); wir wollen die erwähnte Gruppe mit $\mathfrak{O}$ bezeichnen. Einer Drehung, die ein Element in $\mathfrak{O}$ darstellt, entspricht stets eine Permutation der aus den drei durch je zwei gegenüberliegende Ecken des Oktaeders gehenden Symmetrieachsen bestehenden Menge. Wenn man jedem Element der Gruppe $\mathfrak{O}$ die entsprechende Permutation zuordnet, so erhält man eine Deformation von $\mathfrak{O}$ auf die symmetrische Permutationsgruppe $\mathfrak{S}_3$. Der Leser möge diese Deformation benutzen und mit Hilfe des ersten und dritten Isomorphiesatzes für Gruppen die Tatsache beweisen, daß in $\mathfrak{O}$ invariante Untergruppen der Ordnungen 4 und 12 enthalten sind.

§ 27. Zyklische Gruppen

1. Definition. Eine Gruppe $\mathfrak{G}$, die aus den Potenzen eines einzigen Elements a besteht, nennt man *zyklisch*. Das Element a heißt das *erzeugende Element* von $\mathfrak{G}$. Eine zyklische Gruppe mit dem erzeugenden Element a wird im allgemeinen mit (a) bezeichnet.

Aus der ersten Formel (1) in § 19, Nr. 3 sehen wir, daß *jede zyklische Gruppe abelsch ist.*

2. Ordnung einer zyklischen Gruppe. Wir betrachten eine zyklische Gruppe (a). Wenn die Potenzen a^i, a^j mit zwei verschiedenen Exponenten i, j stets voneinander verschieden sind, so ist die Ordnung der Gruppe (a) gleich 0, da in diesem Fall in der Gruppe (a) unendlich viele voneinander verschiedene Elemente auftreten:

$$\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \tag{1}$$

Da jedes Element in (a) eine Potenz von a ist, gibt es in der Gruppe (a) außer den Elementen (1) keine weiteren Elemente, und wir sehen, daß die Gruppe (a) genau von den Elementen (1) gebildet wird.

Wir nehmen nun an, daß Potenzen a^i, a^j für gewisse voneinander verschiedene Exponenten i, j zusammenfallen, also $a^i = a^j$ für $i \neq j$ ist. Aus dieser Gleichheit erhalten wir $a^{-j}a^i = a^{-j}a^j$, also $a^{i-j} = \underline{1}$. Da eine der ganzen Zahlen $i-j$, $j-i$ positiv ist und die mit diesen Exponenten gebildeten Potenzen von a mit dem Einselement $\underline{1}$ identisch sind, sehen wir, daß die Gleichung $a^x = \underline{1}$ Lösungen x in natürlichen Zahlen zuläßt. Unter diesen Lösungen gibt es eine kleinste Lösung n; n ist also eine natürliche Zahl, und

es gilt $a^n = \underline{1}$, während alle Potenzen von a mit kleineren natürlichen Exponenten, soweit es solche gibt, vom Einselement $\underline{1}$ verschieden sind. Wir betrachten nun die folgenden Elemente der Gruppe (a):

$$\underline{1},\ a,\ a^2,\ \ldots,\ a^{n-1}. \tag{2}$$

Zunächst ist leicht einzusehen, daß je zwei dieser Potenzen mit verschiedenen Exponenten verschiedene Elemente darstellen. Aus dem Bestehen der Gleichheit $a^i = a^j (i \neq j;\ 0 \leqq i, j \leqq n-1)$ folgt nämlich, daß eine der beiden ganzen Zahlen $i - j$, $j - i$ positiv und kleiner als n ist und zugleich eine Lösung der Gleichung $a^x = \underline{1}$ darstellt; dies widerspricht jedoch der Definition der Zahl n. Die Gruppe (a) besteht also aus wenigstens n Elementen (2), so daß ihre Ordnung gleich 0 oder mindestens gleich n ist. Ferner zeigen wir, daß in der Gruppe (a) keine anderen als die in (2) auftretenden Elemente vorkommen, so daß die Ordnung von (a) gleich n ist. Zu diesem Zweck betrachten wir ein beliebiges Element $a^x \in (a)$. Es sei q bzw. r der Quotient bzw. Rest von x bei der Division durch n, also $x = qn + r$, $0 \leqq r \leqq n-1$, so daß a^r mit einem der Elemente (2) identisch ist. Nach den Formeln (1) aus § 19, Nr. 3 gilt

$$a^x = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = \underline{1}^q \cdot a^r = \underline{1} \cdot a^r = a^r,$$

so daß das Element a^x mit a^r übereinstimmt. Damit ist gezeigt, daß die Gruppe (a) genau aus den Elementen (2) besteht und folglich von der Ordnung n ist. Ferner sehen wir, daß das Produkt $a^i \cdot a^j (= a^{i+j})$ aus beliebigen Elementen $a^i, a^j \in (a)$ mit dem Element a^k identisch ist, wobei k den Rest der Zahl $i + j$ bei der Division durch n darstellt.

Wir fassen unsere Resultate zusammen:

Die Ordnung n einer zyklischen Gruppe (a) ist entweder gleich Null, also $n = 0$, und in diesem Fall besteht die Gruppe (a) aus den Elementen (1); oder die Ordnung von (a) ist größer als Null, also $n > 0$, und dann wird die Gruppe (a) von den Elementen (2) gebildet. Das Produkt $a^i \cdot a^j$ aus beliebigen Elementen $a^i, a^j \in (a)$ wird im ersten Fall durch a^{i+j} und im zweiten durch a^k dargestellt, wobei k den Rest der Zahl $i + j$ bei der Division durch n bedeutet. Im zweiten Fall ist n die kleinste natürliche Lösung der Gleichung $a^x = \underline{1}$.

Wir wollen beachten, daß in beiden Fällen die Potenz a^{n-i} das inverse Element von a^i darstellt.

3. Untergruppen in zyklischen Gruppen. Wir betrachten eine Untergruppe $\mathfrak{A} \subset (a)$ einer zyklischen Gruppe (a). Wenn $\mathfrak{A}$ aus dem einzigen Element $\underline{1}$ besteht, so ist $\mathfrak{A}$ zyklisch und wird von dem Einselement $\underline{1}$ erzeugt, also $\mathfrak{A} = (\underline{1})$. Wir wollen also annehmen, daß die Untergruppe $\mathfrak{A}$ außer dem Einselement $\underline{1}$ ein Element a^i besitzt, wobei $i \neq 0$ ist. Da in $\mathfrak{A}$ zugleich das inverse Element a^{-i} vorkommt und entweder i oder $-i$ eine natürliche Zahl ist, treten in $\mathfrak{A}$ Potenzen von a mit natürlichen Exponenten auf. Unter diesen Exponenten ist einer, den wir mit m bezeichnen wollen, der kleinste. Es gilt also $a^m \in \mathfrak{A}$, während alle Potenzen von a, deren Exponenten natürliche Zahlen und kleiner als m sind, in der Untergruppe $\mathfrak{A}$ nicht auftreten. Es sei nun $a^x \in \mathfrak{A}$ ein beliebiges Element in $\mathfrak{A}$. Wir bezeichnen mit q bzw. r den

Quotienten bzw. Rest der Zahl x bei der Division durch m, so daß $x = qm + r$, $0 \leqq r \leqq m - 1$ ist. Nach den Formeln (1) aus § 19, Nr. 3 gilt $a^x = a^{qm+r} = a^{qm} \cdot a^r$, und man sieht, daß das Element a^r mit dem Produkt aus a^{-qm} und a^x identisch ist. Da nun a^{-qm} das inverse Element von $(a^m)^q$ ist und $(a^m)^q$ als Potenz von a^m ebenfalls in der Untergruppe $\mathfrak{A}$ auftritt, liegt das Element a^r in $\mathfrak{A}$. Daraus folgt mit Rücksicht auf $0 \leqq r \leqq m - 1$ und auf die Definition der Zahl m die Beziehung $r = 0$, und es ergibt sich $a^x = (a^m)^q$. Jedes Element von $\mathfrak{A}$ ist also eine Potenz von a^m, und wir kommen zu der Erkenntnis, daß die Untergruppe $\mathfrak{A}$ zyklisch ist und von dem Element a^m erzeugt wird. Diese Überlegung führt also zu dem Resultat, daß *jede Untergruppe der zyklischen Gruppe* (a) *ebenfalls zyklisch ist.*

Wir wollen beachten, daß jede Untergruppe einer zyklischen Gruppe (a) in (a) invariant ist, da (a) eine abelsche Gruppe darstellt.

4. Erzeugende Elemente. Gibt es in der zyklischen Gruppe (a) außer dem Element a noch weitere erzeugende Elemente der Gruppe (a)? Es sei n die Ordnung der Gruppe (a) und a^ν ein erzeugendes Element von (a). Dann ist insbesondere das Element a eine Potenz von a^ν, und wir erhalten $a = a^{\nu q}$, wobei q eine ganze Zahl bedeutet. Ist $n = 0$, so folgt aus der letzten Gleichheit die Beziehung $\nu q = 1$, da in diesem Fall zwei Potenzen von a mit verschiedenen Exponenten voneinander verschieden sind. Wir haben also $\nu = q = 1$ oder $\nu = q = -1$. Wir sehen, daß außer dem Element a nur das zu ihm inverse Element a^{-1} erzeugend sein kann und ferner tatsächlich jedes Element $a^i \in (a)$ die $(-i)$-te Potenz von a^{-1} ist. Im Fall $n = 0$ hat also die Gruppe (a) genau zwei erzeugende Elemente, nämlich a, a^{-1}. Wir wollen beachten, daß dies die einzigen Elemente in der Gruppe (a) sind, deren Exponenten zu der Ordnung $n(= 0)$ der Gruppe (a) relativ prim sind. Wir wollen nun den Fall $n > 0$ betrachten. In diesem Fall besteht die zyklische Gruppe (a) aus den Elementen $\underline{1}, a, a^2, \ldots, a^{n-1}$. Ist r der Rest der Zahl νq bei der Division durch n, gilt also $\nu q = nq' + r$, wobei q' den Quotienten bedeutet und $0 \leqq r \leqq n - 1$ ist, so haben wir $a^{\nu q} = a^r = a$. Aus diesen Beziehungen folgt $r = 1$, da a, a^r der Reihe $\underline{1}, a, a^2, \ldots, a^{n-1}$ angehören, in der zwei Potenzen mit verschiedenen Exponenten voneinander verschieden sind. Es gilt also $\nu q - nq' = 1$, und wir sehen, daß die Zahlen ν, n zueinander relativ prim sind. Wenn umgekehrt ν zu n relativ prim ist, so gibt es bekanntlich ganze Zahlen q, q' für die $\nu q - nq' = 1$ ist. Daraus folgt für jede ganze Zahl i die Beziehung $i = \nu(qi) - n(q'i)$, und wir haben $a^i = (a^\nu)^{qi}$. Wir sehen, daß das Element a^ν für die Gruppe (a) erzeugend ist. Im Fall $n > 0$ stellen also genau diejenigen Potenzen von a, deren Exponenten zu der Ordnung n der Gruppe (a) relativ prim sind, erzeugende Elemente der Gruppe (a) dar. Wir haben oben gesehen, daß dasselbe Resultat auch im Fall $n = 0$ gültig bleibt.

Es gilt also der folgende

Satz. *Die erzeugenden Elemente einer zyklischen Gruppe* (a) *von der Ordnung* $n \geqq 0$ *sind genau die Potenzen von* a, *deren Exponenten zu der Ordnung* n *relativ prim sind.*

Im Fall $n = 0$ besitzt also die zyklische Gruppe (a) genau zwei erzeugende Elemente a, a^{-1}, während es im Fall $n > 0$ so viele Elemente gibt, als in der Folge $1, 2, \ldots, n$ zu n teilerfremde Zahlen vorhanden sind.

5. Bestimmung aller zyklischen Gruppen. 1. Ein wichtiges Beispiel einer zyklischen Gruppe von der Ordnung 0 stellt die Gruppe $\mathfrak{Z}$ dar, und es gilt offenbar $\mathfrak{Z} = (1)$. Jede Untergruppe von $\mathfrak{Z}$ wird von den ganzzahligen Vielfachen einer nichtnegativen ganzen Zahl n gebildet (§ 19, Nr. 4, 3) und ist folglich nach dem obigen Resultat die zyklische Gruppe (n). Es sei $n \geqq 0$. Wir betrachten die Faktorgruppe $\mathfrak{Z}/(n)$. Zunächst wollen wir daran erinnern, daß die Faktorgruppe $\mathfrak{Z}/(n)$ im Fall $n = 0$ aus den Mengen $\bar{a}_i = \{i\}$, wobei i die Zahlen $\ldots, -2, -1, 0, 1, 2, \ldots$ durchläuft, besteht, während sie im Fall $n > 0$ von den Elementen $\bar{a}_0, \ldots, \bar{a}_{n-1}$ gebildet wird, wobei jedes Element $\bar{a}_j$ aus allen in $\mathfrak{Z}$ enthaltenen Zahlen besteht, die sich von der Zahl j um ein ganzzahliges Vielfaches der Zahl n unterscheiden; in beiden Fällen ist die Ordnung der Faktorgruppe $\mathfrak{Z}/(n)$ gleich n. Nun ist leicht zu zeigen, daß die Faktorgruppe $\mathfrak{Z}/(n)$ zyklisch ist und von dem Element $\bar{a}_1$ erzeugt wird. In der Tat, nach Definition der Multiplikation in $\mathfrak{Z}/(n)$ stimmt die i-te Potenz jedes Elements $\bar{a}_k \in \mathfrak{Z}/(n)$ mit dem die Zahl ik enthaltenden Element von $\mathfrak{Z}/(n)$ überein; folglich gilt insbesondere $\bar{a}_j = \bar{a}_1^j$. Damit ist unsere Behauptung bewiesen. Gleichzeitig haben wir die Existenz von zyklischen Gruppen von beliebiger Ordnung $n (\geqq 0)$ nachgewiesen.

Aber es ist nicht nur jede Faktorgruppe der Gruppe $\mathfrak{Z}$ zyklisch, sondern umgekehrt ist auch jede zyklische Gruppe isomorph einer Faktorgruppe auf $\mathfrak{Z}$. In der Tat es sei (a) eine zyklische Gruppe. Dann gibt es zu jedem Element $x \in (a)$ wenigstens eine ganze Zahl ξ, für die $a^\xi = x$ ist; umgekehrt stellt für jede ganze Zahl ξ die Potenz a^ξ ein Element der Gruppe (a) dar. Wenn wir also jeder Zahl $\xi \in \mathfrak{Z}$ das Element $a^\xi \in (a)$ zuordnen, so erhalten wir eine Abbildung $\boldsymbol{d}$ der Gruppe $\mathfrak{Z}$ auf die Gruppe (a). Für beliebige Zahlen $\xi, \eta \in \mathfrak{Z}$ und die zugeordneten Elemente $\boldsymbol{d}\xi = x$, $\boldsymbol{d}\eta = y$ von (a) erhalten wir die Beziehungen $x = a^\xi$, $y = a^\eta$ und folglich $xy = a^\xi a^\eta = a^{\xi+\eta}$, woraus $\boldsymbol{d}(\xi + \eta) = xy = \boldsymbol{d}\xi\,\boldsymbol{d}\eta$ folgt. Wir sehen, daß die Abbildung $\boldsymbol{d}$ eine Deformation darstellt. Damit ist zunächst gezeigt, daß die zyklische Gruppe (a) der Gruppe $\mathfrak{Z}$ homomorph ist. Nach dem ersten Isomorphiesatz für Gruppen (§ 26, Nr. 3, 1) bildet die Menge aller $\boldsymbol{d}$-Urbilder des Einselements von (a) eine (in $\mathfrak{Z}$ invariante) Untergruppe $\mathfrak{A}$, und die durch $\mathfrak{A}$ bestimmte Faktorgruppe $\mathfrak{Z}/\mathfrak{A}$ auf $\mathfrak{Z}$ ist der Gruppe (a) isomorph, also $\mathfrak{Z}/\mathfrak{A} \simeq (a)$. Es sei $n (\geqq 0)$ die Ordnung der zyklischen Gruppe (a). Dann hat auch die Faktorgruppe $\mathfrak{Z}/\mathfrak{A}$ die Ordnung n, und wir sehen, daß die Untergruppe $\mathfrak{A}$ von allen ganzzahligen Vielfachen der Zahl n gebildet wird. So ergibt sich die Tatsache, daß die zyklische Gruppe (a) von der Ordnung n der durch die Untergruppe (n) der Gruppe $\mathfrak{Z}$ bestimmten Faktorgruppe $\mathfrak{Z}/(n)$ isomorph ist. Insbesondere ist also jede zyklische Gruppe von der Ordnung 0 der Gruppe $\mathfrak{Z}/(0)$, also auch der Gruppe $\mathfrak{Z}$ isomorph.

Offenbar ist jede einer zyklischen Gruppe von der Ordnung $n (\geqq 0)$ isomorphe Gruppe wiederum zyklisch und hat die Ordnung n.

Unsere Überlegung führt also zu dem folgenden Resultat:

Alle zyklischen Gruppen von der Ordnung $n \geqq 0$ werden durch die Faktorgruppe $\mathfrak{Z}/(n)$ repräsentiert, und zwar so, daß jede zyklische Gruppe von der Ordnung n der Faktorgruppe $\mathfrak{Z}/(n)$ isomorph ist und umgekehrt jede mit dieser Faktorgruppe isomorphe Gruppe zyklisch ist und die Ordnung n hat.

2. *Beispiel.* Als Beispiel einer zyklischen Gruppe von der Ordnung $n > 0$ wollen wir die aus den Wurzeln der Gleichung $x^n = 1$ bestehende Gruppe angeben, in der die Multiplikation als die arithmetische Multiplikation erklärt wird. Die Wurzeln der genannten Gleichung sind

$$\varepsilon_0 = 1, \quad \varepsilon_1 = e^{\frac{2\pi i}{n}}, \quad \varepsilon_2 = e^{\frac{4\pi i}{n}}, \quad \ldots, \quad \varepsilon_{n-1} = e^{\frac{2(n-1)\pi i}{n}};$$

sie bilden offenbar die zyklische Gruppe $\left(e^{\frac{2\pi i}{n}}\right)$. Die in einer Ebene liegenden Punkte, deren Koordinaten aus dem Real- und dem Imaginärteil je einer dieser Wurzeln bestehen, bilden die Eckpunkte eines regulären n-Ecks. Für $n = 6$ erhalten wir z. B. die Eckpunkte eines regulären Sechsecks. Die erzeugenden Elemente dieser zyklischen Gruppe sechster Ordnung sind durch die Wurzeln $e^{\frac{2\pi i}{6}}$, $e^{\frac{10\pi i}{6}}$ bestimmt.

6. Der Fermatsche Satz für Gruppen. Der Begriff einer zyklischen Gruppe ist auch für Gruppen, die nicht zyklisch zu sein brauchen, von besonderer Wichtigkeit.

Wie betrachten eine Gruppe $\mathfrak{G}$ und ein beliebiges Element $a \in \mathfrak{G}$. Die Potenzen von a bilden eine zyklische Untergruppe (a) in $\mathfrak{G}$.

Unter der *Ordnung des Elementes a* verstehen wir die Ordnung der zyklischen Untergruppe (a). Jedes Element $a \in \mathfrak{G}$ hat also stets eine Ordnung n, die entweder gleich 0 oder durch die kleinste natürliche Lösung x der Gleichung $a^x = \underline{1}$ gegeben ist; in jedem Fall gilt also die Beziehung $a^n = \underline{1}$.

Es ist leicht festzustellen, daß *die Ordnung n jedes Elementes $a \in \mathfrak{G}$ einen Teiler der Ordnung N der Gruppe $\mathfrak{G}$ darstellt*, so daß also $N = nd$ gilt, wobei d eine ganze Zahl bedeutet. Die Gültigkeit dieser Beziehung ist zunächst klar, wenn $N = 0$ ist. Im Fall $N > 0$ folgt sie aus der Tatsache, daß die Ordnung einer Untergruppe in $\mathfrak{G}$ ein Teiler der Zahl N ist.

Aus $N = nd$ folgt $a^N = a^{nd} = (a^n)^d = \underline{1}^d = \underline{1}$; diese Beziehungen enthalten den sogenannten *Fermatschen Satz für Gruppen:*

In jeder Gruppe von beliebiger Ordnung N stimmt die N-te Potenz jedes Elements mit dem Einselement der Gruppe überein.

7. Erzeugung der Translationen auf endlichen Gruppen mit Hilfe echter zyklischer Permutationen. Wir wollen unsere Überlegungen mit einer Bemerkung über (beispielsweise) linksseitige Translationen auf einer endlichen Gruppe abschließen.

Es sei $\mathfrak{G}$ eine endliche Gruppe und $a \in \mathfrak{G}$ ein beliebiges Element. Wie wir in § 26, Nr. 2, 1 gezeigt haben, ist die linksseitige Translation ${}_a\boldsymbol{t}$ auf der Gruppe $\mathfrak{G}$ eine Permutation von $\mathfrak{G}$. Folglich wird ${}_a\boldsymbol{t}$ durch endlich viele echte zyklische

Permutationen erzeugt; d. h., es gibt eine Zerlegung $\bar{G} = \{\bar{a}, \bar{b}, \ldots, \bar{m}\}$ der Gruppe $\mathfrak{G}$ derart, daß jedes Element $\bar{a}, \bar{b}, \ldots, \bar{m}$ bei der Permutation ${}_a\boldsymbol{t}$ invariant bleibt und die partiellen Abbildungen ${}_a\boldsymbol{t}\bar{a}, {}_a\boldsymbol{t}\bar{b}, \ldots, {}_a\boldsymbol{t}\bar{m}$ echte zyklische Permutationen der Elemente $\bar{a}, \bar{b}, \ldots, \bar{m}$ darstellen (§ 8, Nr. 5). Ein beliebiges Element $\bar{x} \in \bar{G}$ besteht aus den Elementen des Zyklus x, ${}_a\boldsymbol{t}x$, $({}_a\boldsymbol{t})^2x, \ldots,$ $({}_a\boldsymbol{t})^{k-1}x$, wobei x einen beliebigen Punkt in $\bar{x}$ und k die kleinste natürliche, der Beziehung $({}_a\boldsymbol{t})^k x = x$ genügende Zahl bedeutet. Nach Definition von ${}_a\boldsymbol{t}$ gelten die Formeln ${}_a\boldsymbol{t}x = ax$, $({}_a\boldsymbol{t})^2x = a^2x, \ldots, ({}_a\boldsymbol{t})^{k-1}x = a^{k-1}x$, und aus $({}_a\boldsymbol{t})^k x = a^k x = x$ folgt $a^k = \underline{1}$. Daraus schließen wir, daß der Zyklus mit der Folge $x, ax, a^2x, \ldots, a^{k-1}x$ zusammenfällt. Ferner sehen wir, daß die Menge $\{\underline{1}, a, a^2, \ldots, a^{k-1}\}$ das Feld der zyklischen Untergruppe (a) in $\mathfrak{G}$ darstellt. Das Element $\bar{x}$ stimmt also mit der rechtsseitigen Nebenklasse des Punktes x in bezug auf die zyklische Untergruppe (a) überein. Daraus folgt weiter, daß $\bar{G}$ die rechtsseitige Nebenklassenzerlegung der Gruppe $\mathfrak{G}$ in bezug auf die zyklische Untergruppe (a) ist.

Durch diese Überlegung kommen wir also zu dem Resultat, daß *jede linksseitige Translation* ${}_a\boldsymbol{t}$ *auf einer endlichen Gruppe* $\mathfrak{G}$ *durch echte zyklische Permutationen erzeugt wird, deren Zyklen von denselben Elementen wie die rechtsseitigen Nebenklassen der Gruppe* $\mathfrak{G}$ *in bezug auf die zyklische Untergruppe* (a) *gebildet werden.*

8. Übungsaufgaben.

1. Ein Element $a \neq \underline{1}$ in einer beliebigen Gruppe hat dann und nur dann die Ordnung 2, wenn es zu sich selbst invers ist.

2. In einer endlichen Gruppe von gerader Ordnung gibt es stets Elemente von der Ordnung 2.

3. Hat ein Element $a \in \mathfrak{G}$ einer Gruppe $\mathfrak{G}$ die Ordnung n, so ist die Ordnung jedes Elements der zyklischen Untergruppe $(a) \subset \mathfrak{G}$ ein Teiler von n.

4. Jede Gruppe von einer Primzahlordnung ist zyklisch.

5. Die Ordnung eines Elements $\bar{a}$ einer Faktorgruppe auf einer endlichen Gruppe $\mathfrak{G}$ ist ein Teiler der Ordnung jedes in $\bar{a}$ enthaltenen Punktes. Wenn die Ordnung von $\bar{a}$ eine Potenz einer Primzahl p ist, so gibt es in $\bar{a}$ einen Punkt a, dessen Ordnung ebenfalls eine Potenz von p ist.