§ 19. Grundbegriffe der Gruppentheorie

In: Otakar Borůvka (author): Grundlagen der Gruppoid- und Gruppentheorie. (German). Berlin: VEB Deutscher Verlag der Wissenschaften, 1960. pp. [131]--139.

Persistent URL: http://dml.cz/dmlcz/401511

III. GRUPPEN

§ 19. Grundbegriffe der Gruppentheorie

1. Die Gruppenaxiome. Gegenstand unserer weiteren Ausführungen bilden die Gruppen. Den Gruppenbegriff haben wir bereits in § 18, Nr. 5, 1 entwickelt. Wir haben gesehen, daß man unter einer *Gruppe* eine assoziative Quasigruppe versteht. Ausführlicher kann eine Gruppe in folgender Weise erklärt werden:

Ein Gruppoid $\mathfrak{G}$ heißt *Gruppe*, wenn die folgenden Axiome, die sogenannten *Gruppenaxiome*, erfüllt sind:

1. Für beliebige Elemente $a, b, c \in \mathfrak{G}$ *gilt* $a(bc) = (ab)c$.

2. Zu beliebigen Elementen $a, b \in \mathfrak{G}$ *gibt es genau eine Lösung* $x \in \mathfrak{G}$ *der Gleichung* $ax = b$ *und ebenfalls genau eine Lösung* $y \in \mathfrak{G}$ *der Gleichung* $ya = b$.

Diese Axiome werden das *Assoziativgesetz* und das *Axiom der eindeutigen Division* für Gruppen genannt. In § 18, Nr. 5, 1 haben wir gezeigt, daß diese Axiome stets die Existenz des Einselements $\underline{1} \in \mathfrak{G}$ mit sich bringen; $\underline{1}$ ist durch die für alle Elemente $a \in \mathfrak{G}$ bestehenden Gleichheiten $\underline{1}a = a\underline{1} = a$ charakterisiert. Der Kürze halber sprechen wir im allgemeinen von der Einheit anstatt vom Einselement. *Jede Gruppe besitzt also die Einheit.*

Im folgenden soll das Symbol $\mathfrak{G}$ stets eine Gruppe bezeichnen.

2. Inverse Elemente. Die Inversion. Da $\mathfrak{G}$ eine Quasigruppe mit Einheit darstellt, gibt es zu jedem Element $a \in \mathfrak{G}$ genau ein der Gleichung $ax = \underline{1}$ genügendes Element $x \in \mathfrak{G}$ und ebenfalls genau ein der Gleichung $ya = \underline{1}$ genügendes Element $y \in \mathfrak{G}$; das Symbol $\underline{1}$ bezeichnet hier (und stets im folgenden) die Einheit von $\mathfrak{G}$.

Es ist leicht zu zeigen, daß *aus der Gültigkeit des Assoziativgesetzes die Gleichheit der beiden Elemente* x, y *folgt*. Wenn wir nämlich das Produkt aus y und $ax (= \underline{1})$ bilden, so erhalten wir $y(ax) = y\underline{1} = y$ und ferner (in Hinblick auf die Gültigkeit des Assoziativgesetzes) $y(ax) = (ya)x = \underline{1}x = x$, so daß sich tatsächlich $x = y$ ergibt.

Zu jedem Element $a \in \mathfrak{G}$ gibt es also genau ein Element, das man im allgemeinen mit a^{-1} bezeichnet und für das $aa^{-1} = a^{-1}a = \underline{1}$ ist. Dieses Element a^{-1} heißt *invers in bezug auf* a; wir sagen auch, das Element a^{-1} sei *invers zu* a. Nach dieser Definition stellt also a^{-1} die einzige Lösung der Gleichung $ax = \underline{1}$ und zugleich die einzige Lösung der Gleichung $ya = \underline{1}$ dar. Da ferner die Gleichung $a^{-1}x = \underline{1}$ durch a erfüllt wird, ist a das inverse Element in bezug auf a^{-1}, also $(a^{-1})^{-1} = a$. Wegen dieser Symmetrie nennen wir die Elemente a, a^{-1} *zueinander invers*. Wir wollen beachten, daß das zu a inverse Element a^{-1} wiederum a sein kann, so daß $a^{-1} = a$ gilt; z. B. haben wir $\underline{1}^{-1} = \underline{1}$.

Auf der Gruppe $\mathfrak{G}$ gibt es also eine ausgezeichnete Zerlegung, deren Elemente teils je von einem zu sich selbst inversen Punkt, teils je von zwei zueinander inversen Punkten gebildet werden.

So stellt z. B. im Fall der Gruppe $\mathfrak{Z}$ die Zahl 0 die Einheit von $\mathfrak{Z}$ dar, und die erwähnte ausgezeichnete Zerlegung auf $\mathfrak{Z}$ besteht aus den Elementen $\{0\}, \{1, -1\}, \{2, -2\}, \ldots$.

Es seien $a, b \in \mathfrak{G}$ beliebige Elemente. Aus $aa^{-1} = \underline{1}$ und wegen des Assoziativgesetzes erhalten wir $a(a^{-1}b) = (aa^{-1})b = \underline{1}b = b$; wir sehen, daß das Element $a^{-1}b$ die (einzige) Lösung der Gleichung $ax = b$ darstellt. Analog stellt ba^{-1} die (einzige) Lösung der Gleichung $ya = b$ dar. Ferner ist leicht festzustellen, daß $b^{-1}a^{-1}$ *das zu dem Produkt* ab *inverse Element ist.* Zu diesem Zweck genügt es zu zeigen, daß das Element $b^{-1}a^{-1}$ die Lösung x der Gleichung $(ab)x = \underline{1}$ darstellt; dies folgt jedoch aus

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(\underline{1}a^{-1}) = aa^{-1} = \underline{1}.$$

Ähnlich kann das allgemeinere Resultat hergeleitet werden, daß $a_n^{-1} \ldots a_2^{-1}a_1^{-1}$ *das zu dem Produktelement* $a_1a_2 \ldots a_n$ *einer beliebigen* $n(\geqq 2)$*-gliedrigen Folge von Elementen* $a_1, a_2, \ldots, a_n \in \mathfrak{G}$ *inverse Element ist.*

Zu dem Begriff des inversen Elements wollen wir noch die folgende Bemerkung hinzufügen. Wie wir gesehen haben, ist die Existenz des inversen Elements in bezug auf ein beliebiges Element eine Folgerung der charakteristischen Gruppeneigenschaften. Wir betrachten nun umgekehrt ein assoziatives Gruppoid $\mathfrak{G}$ mit der Einheit $\underline{1}$ und setzen voraus, daß es in $\mathfrak{G}$ zu jedem Element $a \in \mathfrak{G}$ ein inverses, d. h. den Gleichungen $aa^{-1} = a^{-1}a = \underline{1}$ genügendes Element a^{-1} gibt. In diesem Fall stellt das Gruppoid $\mathfrak{G}$ eine Quasigruppe und folglich (da es assoziativ ist) eine Gruppe dar. Das folgt daraus, daß für je zwei Elemente $a, b \in \mathfrak{G}$ die Produkte $x = a^{-1}b$, $y = ba^{-1}$ Lösungen der Gleichungen $ax = b$, $ya = b$ darstellen und diese Lösungen offenbar eindeutig bestimmt sind. Somit kommen wir zu der Erkenntnis, daß *unter allen assoziativen Gruppoiden mit Einheit die Gruppen durch die Existenz von inversen Elementen charakterisiert sind.*

Die Existenz von inversen Elementen in der Gruppe $\mathfrak{G}$ gibt zur Einführung einer ausgezeichneten schlichten Abbildung der Gruppe $\mathfrak{G}$ auf sich Anlaß.

Wenn man jedem Element $a \in \mathfrak{G}$ *das inverse Element* $a^{-1} \in \mathfrak{G}$ *zuordnet, so erhält man eine schlichte Abbildung der Gruppe* $\mathfrak{G}$ *auf sich, also eine Permutation der Gruppe* $\mathfrak{G}$. *Diese Permutation ist durch* $\mathfrak{G}$ *eindeutig bestimmt.* Wir wollen sie die *Inversion* der Gruppe $\mathfrak{G}$ nennen und mit $\boldsymbol{n}$ bezeichnen. Die Inversion der Gruppe $\mathfrak{G}$ ist offenbar eine involutorische Abbildung (§ 6, Nr. 7).

3. Potenzen von Elementen. Es sei $a \in \mathfrak{G}$ ein beliebiges Element und n eine natürliche Zahl. Da die Gruppe $\mathfrak{G}$ ein assoziatives Gruppoid darstellt, gibt es nur ein Produktelement $\underbrace{aa \ldots a}_{n}$. Dieses Element heißt die *n-te Potenz* von a und wird mit a^n bezeichnet. Ähnlich heißt das Element $\underbrace{a^{-1}a^{-1} \ldots a^{-1}}_{n}$ die $(-n)$*-te Potenz* von a; wir bezeichnen dieses Element mit a^{-n}. Es gelten also die Formeln $a^{-n} = (a^{-1})^n$, $a^{-n} = (a^n)^{-1}$.

Somit haben wir die positiven und die negativen Potenzen von a definiert. Es ist zweckmäßig, auch die nullte Potenz a^0 von a zu definieren, und zwar verstehen wir unter a^0 die Einheit $\underline{1}$ der Gruppe $\mathfrak{G}$, also $a^0 = \underline{1}$. Auf diese Weise haben wir jedem Element $a \in \mathfrak{G}$ unendlich viele Potenzen von a mit den Exponenten $\ldots, -2, -1, 0, 1, 2, \ldots$ zugeordnet:

$$\ldots, a^{-2}\, a^{-1}, a^0, a^1, a^2, \ldots, \qquad (a^1 = a);$$

einige (eventuell auch alle) von diesen Elementen können natürlich zusammenfallen.

Die Potenzen jedes Elements $a \in \mathfrak{G}$ genügen für alle ganzzahligen Werte der Exponenten m, n den Formeln

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}. \tag{1}$$

Wir begnügen uns hier mit dem Beweis der ersten Formel und wollen es dem Leser überlassen, sich von der Gültigkeit der zweiten zu überzeugen.

Sind eine oder beide Zahlen m, n gleich 0, so ist die erwähnte Formel offenbar richtig. Sind beide Zahlen m, n positiv, so gilt

$$a^m a^n = \underbrace{(a \ldots a)}_{m}\,\underbrace{(a \ldots a)}_{n} = \underbrace{(a \ldots a)}_{m+n} = a^{m+n}.$$

Sind beide Zahlen m, n negativ, so sind $m' = -m$, $n' = -n$ positiv, und es ist

$$a^m a^n = a^{-m'} a^{-n'} = \underbrace{(a^{-1} \ldots a^{-1})}_{m'}\,\underbrace{(a^{-1} \ldots a^{-1})}_{n'} = \underbrace{(a^{-1} \ldots a^{-1})}_{m'+n'} = a^{-(m'+n')}$$
$$= a^{-m'-n'} = a^{m+n}.$$

Es ist also nur noch der Fall zu untersuchen, daß eine der Zahlen m, n positiv und die andere negativ ist. Ist m positiv und n negativ, so sind m, $n' = -n$ positiv, und es gilt

$$a^m a^n = a^m a^{-n'} = \underbrace{(a \ldots a)}_{m}\,\underbrace{(a^{-1} \ldots a^{-1})}_{n'}$$
$$= \begin{cases} \underbrace{(a \ldots a)}_{m-n'} = a^{m-n'} = a^{m+n} & \text{für} \quad m > n'; \\ \underline{1} = a^0 = a^{m-n'} = a^{m+n} & \text{für} \quad m = n'; \\ \underbrace{(a^{-1} \ldots a^{-1})}_{n'-m} = a^{-(n'-m)} = a^{m+n} & \text{für} \quad m < n'. \end{cases}$$

Wenn schließlich m negativ und n positiv ist, so sind $m' = -m$, n positiv, und wir erhalten

$$a^m a^n = a^{-m'} a^n = (a^{-1})^{m'} \big((a^{-1})^{-1}\big)^n = (a^{-1})^{m'} (a^{-1})^{-n} = (a^{-1})^{m'-n} = a^{-(m'-n)}$$
$$= a^{-m'+n} = a^{m+n}.$$

Damit ist die erste Formel (1) bewiesen.

Ist zum Beispiel a ein beliebiges Element in der Gruppe $\mathfrak{Z}$, so sind $\ldots, -2a, -a, 0, a, 2a, \ldots$ die Potenzen von a; für $a = 1$ haben wir ins-

besondere $\ldots, -2, -1, 0, 1, 2, \ldots$, und wir sehen, daß die von den einzelnen Potenzen der Zahl $1 \in \mathfrak{Z}$ gebildete Menge das Feld von $\mathfrak{Z}$ darstellt.

4. Untergruppen und Obergruppen. 1. *Definition.* Es sei $\mathfrak{A}$ ein beliebiges Untergruppoid in $\mathfrak{G}$. Nach § 12, Nr. 9,8 ist das Gruppoid $\mathfrak{A}$ assoziativ. Wenn es überdies eine (Quasigruppe, also eine) Gruppe ist, so sagen wir, $\mathfrak{A}(\mathfrak{G})$ sei eine *Untergruppe in* $\mathfrak{G}$ (eine *Obergruppe auf der Gruppe* $\mathfrak{A}$), und drücken diese Beziehung wie üblich durch $\mathfrak{A} \subset \mathfrak{G}$ oder $\mathfrak{G} \supset \mathfrak{A}$ aus. Die Untergruppe $\mathfrak{A}$ in $\mathfrak{G}$ wird *echt* genannt, wenn sie ein echtes Untergruppoid in $\mathfrak{G}$ darstellt, d. h. wenn das Feld A von $\mathfrak{A}$ in $\mathfrak{G}$ echt ist. In diesem Fall sagen wir, $\mathfrak{G}$ sei *echte Obergruppe* auf $\mathfrak{A}$. In der Gruppe $\mathfrak{G}$ gibt es stets die mit $\mathfrak{G}$ identische *größte Untergruppe* und die von dem einzigen Element $\underline{1}$ gebildete *kleinste Untergruppe* $\{\underline{1}\}$. Diese stellen die *extremen* Untergruppen in $\mathfrak{G}$ dar.

Für beliebige Gruppen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{G}$ gelten offenbar die folgenden Aussagen:

Ist $\mathfrak{B}$ *eine Untergruppe in* $\mathfrak{A}$ *und* $\mathfrak{A}$ *eine solche in* $\mathfrak{G}$, *so ist auch* $\mathfrak{B}$ *eine Untergruppe in* $\mathfrak{G}$.

Sind $\mathfrak{A}$, $\mathfrak{B}$ *Untergruppen in* $\mathfrak{G}$ *und besteht für ihre Felder* A, B *die Beziehung* $B \subset A$, *so ist* $\mathfrak{B}$ *eine Untergruppe in* $\mathfrak{A}$.

2. *Charakteristische Eigenschaft der Untergruppen.* Wir betrachten eine beliebige Untergruppe $\mathfrak{A}$ in $\mathfrak{G}$, und j sei die Einheit von $\mathfrak{A}$. Gibt es irgendwelche Beziehungen zwischen der Einheit $\underline{1}$ von $\mathfrak{G}$ und der Einheit j von $\mathfrak{A}$? Nach Definition von j haben wir für jedes Element $a \in \mathfrak{A}$ die Gleichung $a = ja$, und zugleich gilt natürlich $a = \underline{1}a$. Daraus folgt in Hinblick auf Nr. 1,2 die Gleichung $j = \underline{1}$. Wir sehen, daß *die Einheit* $\underline{1}$ *von* $\mathfrak{G}$ *zugleich die Einheit von* $\mathfrak{A}$ *darstellt.* Daraus schließen wir, daß das zu einem beliebigen Element $a \in \mathfrak{A}$ inverse Element in der Untergruppe $\mathfrak{A}$ mit a^{-1} zusammenfällt, also das inverse Element zu a in der Gruppe $\mathfrak{G}$ darstellt.

Wenn also ein Untergruppoid in $\mathfrak{G}$ *eine Untergruppe in* $\mathfrak{G}$ *darstellt, so enthält es die Einheit von* $\mathfrak{G}$ *und mit jedem Element* a *zugleich das Element* a^{-1}; *wenn umgekehrt ein Untergruppoid in* $\mathfrak{G}$ *diese Eigenschaft besitzt, so stellt es eine Untergruppe in* $\mathfrak{G}$ *dar.*

Mit Hilfe dieses Ergebnisses wollen wir eine Eigenschaft von Untergruppen in $\mathfrak{G}$ herleiten, die diese letzteren unter allen Untergruppoiden in $\mathfrak{G}$ charakterisiert. Wie wir gesehen haben, enthält die Untergruppe $\mathfrak{A}$ mit jedem Element a zugleich das Element a^{-1}, also auch mit je zwei Elementen a, b das Element ab^{-1}. Wir nehmen nun an, daß ein Untergruppoid $\mathfrak{A}$ in $\mathfrak{G}$ die Eigenschaft besitzt, mit je zwei Elementen a, b zugleich das Element ab^{-1} zu enthalten. Sodann kommt in $\mathfrak{A}$ die Einheit $\underline{1}$ von $\mathfrak{G}$ vor (es genügt, $b = a$ zu wählen) und desgleichen das Element $b^{-1}(a = \underline{1})$, so daß nach dem obigen Resultat das Untergruppoid $\mathfrak{A}$ eine Untergruppe in $\mathfrak{G}$ darstellt. Somit haben wir die folgende charakteristische Eigenschaft der Untergruppe erhalten: *Unter allen Untergruppoiden in* $\mathfrak{G}$ *sind die Untergruppen dadurch charakterisiert, daß sie mit je zwei Elementen* a, b *stets auch das Element* ab^{-1} *enthalten.*

Übrigens wollen wir beachten, daß eine beliebige nicht leere Untermenge $A \subset \mathfrak{G}$, in der mit je zwei Elementen a, b zugleich das Element ab^{-1} vor-

kommt, gruppoidal ist und folglich das Feld einer Untergruppe in $\mathfrak{G}$ darstellt. Offenbar erhält man analoge Ergebnisse, wenn man statt ab^{-1} das Element $a^{-1}b$ betrachtet.

3. *Beispiel.* Wir betrachten wiederum die Gruppe $\mathfrak{Z}$. Es sei $\mathfrak{A}$ eine beliebige Untergruppe in $\mathfrak{Z}$, Da diese Untergruppe $\mathfrak{A}$ mit jedem Element b zugleich das inverse Element b^{-1} besitzt, enthält sie entweder nur die Zahl 0 oder neben negativen auch positive Zahlen. Im ersten Fall stellt $\mathfrak{A}$ die kleinste Untergruppe in $\mathfrak{Z}$ dar. Im zweiten Fall sei a die kleinste, als Element in $\mathfrak{A}$ enthaltene positive Zahl. In der Untergruppe $\mathfrak{A}$ kommen natürlich alle Potenzen von a, d. h. alle ganzzahligen Vielfachen der Zahl a vor:

$$\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots .$$

Es sei b ein beliebiges Element in $\mathfrak{A}$. Sodann gibt es ganze Zahlen q, r derart, daß $b = qa + r$, $0 \leqq r \leqq a - 1$ ist. Da die Untergruppe $\mathfrak{A}$ die Zahlen b, qa enthält, gilt dasselbe auch von der Zahl $b - qa = r$; da sie ferner keine kleineren positiven Zahlen als a enthält, ist $r = 0$. Wir haben also $b = qa$ und sehen, daß die Untergruppe $\mathfrak{A}$ außer den ganzzahligen Vielfachen der Zahl a keine anderen Elemente besitzt. Somit ist gezeigt, daß die Untergruppe $\mathfrak{A}$ in den beiden erwähnten Fällen von allen ganzzahligen Vielfachen einer nichtnegativen ganzen Zahl gebildet wird. Umgekehrt ist es klar, daß die Menge aller ganzzahligen Vielfachen einer nichtnegativen ganzen Zahl mit der entsprechenden Multiplikation eine Untergruppe in $\mathfrak{Z}$ darstellt.

Somit sind wir zu dem Ergebnis gekommen, daß *alle Untergruppen in* $\mathfrak{Z}$ *von den ganzzahligen Vielfachen der einzelnen nichtnegativen ganzen Zahlen gebildet werden.* Wir wollen beachten, daß alle positiven ganzzahligen Vielfachen einer natürlichen Zahl ein Untergruppoid, nicht aber eine Untergruppe in $\mathfrak{Z}$ bilden. Es kann also in Gruppen Untergruppoide geben, die keine Untergruppen sind.

Eine weitere Bemerkung, die an die obigen Überlegungen anknüpft, ist folgende: Es ist uns gelungen, alle Untergruppen der Gruppe $\mathfrak{Z}$ zu bestimmen. Ein ähnlicher Erfolg kann in komplizierteren Fällen im allgemeinen nicht erwartet werden, da die Frage nach der Bestimmung aller Untergruppen einer beliebigen Gruppe bisher unbeantwortet blieb.

5. Durchschnitt und Produkt von Untergruppen. 1. *Durchschnitt von Untergruppen.* Wir betrachten beliebige Untergruppen $\mathfrak{A}, \mathfrak{B} \subset \mathfrak{G}$. Da die beiden Untergruppen das Element $1 \in \mathfrak{G}$ enthalten, ist der Durchschnitt $\mathfrak{A} \cap \mathfrak{B}$ von $\mathfrak{A}$ und $\mathfrak{B}$ definiert (§ 12, Nr. 6). Es ist leicht zu zeigen, daß dieser wiederum eine Untergruppe in $\mathfrak{G}$ darstellt. In der Tat, offenbar stellt $\mathfrak{A} \cap \mathfrak{B}$ ein assoziatives Untergruppoid in $\mathfrak{G}$ mit Einheit dar; wir haben also festzustellen, daß in $\mathfrak{A} \cap \mathfrak{B}$ mit jedem Element a zugleich das in $\mathfrak{G}$ enthaltene inverse Element a^{-1} vorkommt. Für $a \in \mathfrak{A} \cap \mathfrak{B}$ haben wir $a \in \mathfrak{A}$, $a \in \mathfrak{B}$ und ferner, da $\mathfrak{A}$, $\mathfrak{B}$ Untergruppen in $\mathfrak{G}$ sind, $a^{-1} \in \mathfrak{A}$, $a^{-1} \in \mathfrak{B}$, also $a^{-1} \in \mathfrak{A} \cap \mathfrak{B}$; damit ist der Beweis beendet. Wir sehen, daß *je zwei Untergruppen in* $\mathfrak{G}$ *stets einen Durchschnitt haben, der wiederum eine Untergruppe in* $\mathfrak{G}$ *ist.* Er stellt offenbar eine Untergruppe in jeder dieser Untergruppen dar. Dieses Resultat kann

ohne Schwierigkeiten auf eine beliebige (sogar unendliche) Anzahl von Untergruppen in $\mathfrak{G}$ erweitert werden.

2. *Produkt von Untergruppen.* Wir nehmen an, daß die Untergruppen $\mathfrak{A}$, $\mathfrak{B}$ miteinander vertauschbar sind; es gilt also $AB = BA$, wobei natürlich $A(B)$ das Feld von $\mathfrak{A}(\mathfrak{B})$ bedeutet. *In dieser Situation existiert das Produkt* $\mathfrak{A}\mathfrak{B}$ *aus* $\mathfrak{A}$ *und* $\mathfrak{B}$ (§ 12, Nr. 9,9), und es ist leicht einzusehen, daß $\mathfrak{A}\mathfrak{B}$ *wiederum eine Untergruppe in* $\mathfrak{G}$ *darstellt.* In der Tat, das Gruppoid $\mathfrak{A}\mathfrak{B}$ ist offenbar assoziativ und enthält die Einheit $\underline{1}$ von $\mathfrak{G}$, wie aus den Beziehungen $\underline{1} \in \mathfrak{A}$, $\underline{1} \in \mathfrak{B}$, $\underline{1} = \underline{1}\,\underline{1} \in \mathfrak{A}\mathfrak{B}$ hervorgeht. Ferner ist jedes Element in $\mathfrak{A}\mathfrak{B}$ das Produkt ab aus einem Element $a \in \mathfrak{A}$ mit einem Element $b \in \mathfrak{B}$; das zu ab inverse Element ist $b^{-1}a^{-1}$, und dieses Element ist wegen $BA = AB$ in $\mathfrak{A}\mathfrak{B}$ enthalten. Somit haben wir gezeigt, daß das Produkt $\mathfrak{A}\mathfrak{B}$ eine Untergruppe in $\mathfrak{G}$ ist. Wir wollen auch den in § 19, Nr. 7, 6 beschriebenen Sachverhalt beachten. Ferner haben wir $\mathfrak{A}\mathfrak{B} \supset \mathfrak{A}$, $\mathfrak{A}\mathfrak{B} \supset \mathfrak{B}$. Insbesondere stellt das Quadrat $\mathfrak{A}^2$ von $\mathfrak{A}$, d. h. das Produkt $\mathfrak{A}\mathfrak{A}$, die Untergruppe $\mathfrak{A}$ in $\mathfrak{G}$ dar. Schließlich weisen wir darauf hin, daß in jeder abelschen Gruppe (je zwei Untergruppen miteinander vertauschbar sind, also) das Produkt von je zwei Untergruppen existiert und wiederum eine Gruppe darstellt.

3. *Beispiel.* In der Gruppe $\mathfrak{Z}$ besitzen je zwei Untergruppen sowohl den Durchschnitt als auch das Produkt. Wir wollen diese Gebilde z. B. für die beiden auf den Feldern

$$\ldots, \quad -8, -4, 0, 4, \quad 8, \ldots,$$
$$\ldots, -14, -7, 0, 7, 14, \ldots$$

bestehenden Untergruppen $\mathfrak{A}$, $\mathfrak{B}$ von $\mathfrak{Z}$ bestimmen. Jede in dem Durchschnitt $\mathfrak{A} \cap \mathfrak{B}$ enthaltene Zahl ist ein ganzzahliges Vielfaches der beiden Zahlen 4 und 7 und folglich auch ein ganzzahliges Vielfaches des kleinsten gemeinsamen Vielfachen dieser Zahlen, d. h. der Zahl 28. Der Durchschnitt $\mathfrak{A} \cap \mathfrak{B}$ besteht also aus den Zahlen

$$\ldots, -56, -28, 0, 28, 56, \ldots.$$

Das Produkt $\mathfrak{A}\mathfrak{B}$ enthält offenbar die Zahl $4 + 7 = 11$, und da es eine Untergruppe in $\mathfrak{Z}$ ist, besteht es aus allen ganzzahligen Vielfachen einer gewissen nichtnegativen ganzen Zahl a (Nr. 4,3). Insbesondere ist also die Zahl 11 ein solches Vielfaches, woraus $a = 1$ oder $a = 11$ folgt. Da ferner in $\mathfrak{A}\mathfrak{B}$ z. B. auch die Zahl 4 vorkommt, ist $a = 1$, da 4 kein ganzzahliges Vielfaches von 11 ist. Wir sehen, daß die Untergruppe $\mathfrak{A}\mathfrak{B}$ von allen ganzzahligen Vielfachen der Zahl 1 gebildet wird und folglich mit der Gruppe $\mathfrak{Z}$ zusammenfällt.

6. Bemerkungen über Multiplikationstabellen endlicher Gruppen. 1. *Charakteristische Eigenschaften der Multiplikationstabellen.* Wir betrachten eine endliche Gruppe $\mathfrak{G}$ und die zugehörige Multiplikationstabelle. Da für die Gruppe $\mathfrak{G}$ die Kürzungsregeln gelten (§ 18, Nr. 3,1), kommen in der Tabelle in jeder Zeile und Spalte rechts vom vertikalen bzw. unter dem horizontalen

Eingang die Symbole aller Elemente der Gruppe $\mathfrak{G}$, also insbesondere das Symbol für das Einselement und mit jedem weiteren Symbol auch dasjenige des entsprechenden inversen Elements vor. Offenbar sind diese Eigenschaften für die Multiplikationstabelle einer endlichen Gruppe charakteristisch, wenn auch das Assoziativgesetz erfüllt ist. So sind z. B. die Multiplikationstabellen für Gruppen von der Ordnung 1, 2, 3 mit den Elementen $\underline{1}, a, b$ die folgenden:

	$\underline{1}$
$\underline{1}$	$\underline{1}$

	$\underline{1}$	a
$\underline{1}$	$\underline{1}$	a
a	a	$\underline{1}$

	$\underline{1}$	a	b
$\underline{1}$	$\underline{1}$	a	b
a	a	b	$\underline{1}$
b	b	$\underline{1}$	a

Für Gruppen von der Ordnung 4 mit den Elementen $\underline{1}, a, b, c$ sind zwei verschiedene Multiplikationstabellen möglich:

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	a	$\underline{1}$
c	c	b	$\underline{1}$	a

	$\underline{1}$	a	b	c
$\underline{1}$	$\underline{1}$	a	b	c
a	a	$\underline{1}$	c	b
b	b	c	$\underline{1}$	a
c	c	b	a	$\underline{1}$

Diese Tabellen findet man, wenn man für je zwei (gleiche oder verschiedene) Elemente das entsprechende Produkt wählt, unter Berücksichtigung aller Möglichkeiten, und zum Schluß die Gültigkeit des Assoziativgesetzes nachweist; bei der Wahl des Produkts bedient man sich der Tatsache, daß in jeder Zeile und Spalte rechts vom vertikalen bzw. unter dem horizontalen Eingang die Symbole aller Elemente der Gruppe auftreten, und zwar jedes Symbol genau einmal. Diese Methode zur Ermittlung der Multiplikationstabellen für endliche Gruppen ist für höhere Ordnungen im allgemeinen sehr langwierig und praktisch undurchführbar. Die Frage nach den Multiplikationstabellen aller endlichen Gruppen ist für spezielle Ordnungen gelöst, bleibt aber im allgemeinen ein offenes Problem.

Wir wollen auch bemerken, daß bei den Gruppen die Multiplikationstabellen gelegentlich auch *Gruppentafeln* genannt werden.

2. *Normale Multiplikationstabellen.* Eine Multiplikationstabelle für eine endliche Gruppe von beliebiger Ordnung kann zunächst so vereinfacht werden, daß man ihre beiden Eingänge wegläßt. Ferner kann die Tabelle umgeformt werden, indem man als die erste, zweite, dritte usw. Zeile diejenige Zeile der ursprünglichen Tabelle aufschreibt, in der das Einselement auf der ersten, zweiten, dritten usw. Stelle vorkommt. Eine Multiplikationstabelle dieser Art heißt *normal.* In einer normalen Multiplikationstabelle steht also in der Hauptdiagonale stets das Einselement. Offenbar gibt es für jede endliche Gruppe im wesentlichen (d. h. abgesehen von der Bezeichnung der Elemente) genau eine normale Multiplikationstabelle. So haben z. B. die normalen

Multiplikationstabellen der Gruppen von der Ordnung 1, 2, 3, 4, deren Elemente mit $\underline{1}, a, b, c$ bezeichnet wurden, die folgende Form:

$\underline{1}$	$\underline{1}\ a$ $a\ \underline{1}$	$\underline{1}\ a\ b$ $b\ \underline{1}\ a$ $a\ b\ \underline{1}$

$\underline{1}\ a\ b\ c$ $a\ \underline{1}\ c\ b$ $c\ b\ \underline{1}\ a$ $b\ c\ a\ \underline{1}$	$\underline{1}\ a\ b\ c$ $a\ \underline{1}\ c\ b$ $b\ c\ \underline{1}\ a$ $c\ b\ a\ \underline{1}$

3. Die *Rechtecksregel.* In einer normalen Multiplikationstabelle steht in der Hauptdiagonale, wie wir wissen, stets das Einselement $\underline{1}$. Wir betrachten die normale Multiplikationstabelle einer endlichen Gruppe. Das Symbol des Produkts aus einem Element a mit einem Element b steht natürlich im Schnittpunkt der mit a beginnenden Zeile und der mit b beginnenden Spalte. Wenn a und b in der Tabelle in bezug auf die Hauptdiagonale symmetrisch liegen, so gilt $ab = \underline{1}$, so daß die Elemente a, b zueinander invers sind. In der ersten Zeile der Tabelle treten also von links nach rechts die Symbole von Elementen auf, die zu den in der ersten Spalte von oben nach unten aufeinanderfolgenden Elementen invers sind.

Wir betrachten beliebige Elemente x, y, z, deren Symbole zusammen mit $\underline{1}$ in der Multiplikationstabelle die Eckpunkte eines Rechtecks bilden. Wir nehmen z. B. an, daß x in derselben Spalte und y in derselben Zeile wie $\underline{1}$ enthalten ist, so daß z in derselben Zeile wie x und in derselben Spalte wie y auftritt. Es seien a, b die Anfangsbuchstaben der die Symbole $\underline{1}, x$ enthaltenden Zeilen und ähnlich c, d diejenigen der die Symbole $\underline{1}, y$ enthaltenden Spalten. Zum Beispiel steht dann x im Schnittpunkt der mit b und c beginnenden Zeile bzw. Spalte, und wir haben $x = bc$; ähnlich erhalten wir $y = ad$, $z = bd$, $\underline{1} = ac$. Aus der letzten Gleichung sehen wir, daß die Elemente a, c zueinander invers sind, so daß gleichzeitig $ca = \underline{1}$ gilt. Folglich haben wir $xy = (bc)(ad) = b(ca)d = b\underline{1}d = bd = z$, also $xy = z$. Auf diese Weise haben wir die *Rechtecksregel für normale Multiplikationstabellen* erhalten:

Wenn in einer normalen Multiplikationstabelle die Symbole von vier beliebigen Elementen, unter denen $\underline{1}$ vorkommt, die Eckpunkte eines Rechtecks bilden, so stellt das zu $\underline{1}$ gegenüberliegende Element das Produkt xy dar, wobei x (y) das in derselben Spalte (Zeile) wie $\underline{1}$ liegende Element des Rechtecks bedeutet.

So bilden z. B. in der obigen zweiten normalen Multiplikationstabelle der Gruppe vierter Ordnung die Elemente $\underline{1}, c$ in der zweiten und b, a in der vierten Zeile die Eckpunkte eines Rechtecks. Folglich gilt nach der Rechtecksregel die Gleichung $bc = a$; sie ist richtig, da sich die mit b beginnende Zeile und die mit c beginnende Spalte in a schneiden.

7. Übungsaufgaben.

1. Das auf dem von allen euklidischen Bewegungen auf der Geraden $f[\alpha]$, $g[a]$ oder von denjenigen in der Ebene $f[\alpha; a, b]$, $g[\alpha; a, b]$ gebildeten Feld bestehende Gruppoid, dessen Multiplikation mit Hilfe der Zusammensetzung von Bewegungen definiert ist (vgl. § 11, Nr. 5, 1), stellt eine Gruppe, die sogenannte *vollständige Gruppe euklidischer Bewegungen auf der Geraden* bzw. *in der Ebene dar*. In dieser Gruppe bilden die euklidischen Bewegungen $f[a]$ bzw. $f[\alpha; a, b]$ eine Untergruppe. Der Leser möge etwaige weitere Untergruppen angeben.

Bemerkung. Die euklidische Geometrie beschreibt bekanntlich die Eigenschaften von Figuren, die von Punkten und Geraden gebildet werden, wie z. B. verschiedene aus Punkten und Geraden bestehende Konfigurationen, Dreiecke, Kegelschnitte usw. Diese Geometrie beruht auf dem Begriff der vollständigen Gruppe euklidischer Bewegungen, indem zwei Figuren als kongruent erklärt werden, wenn sie mittels einer euklidischen Bewegung ineinander übergeführt werden können.

2. Das Gruppoid, dessen Feld von den in § 8, Nr. 8, 4 beschriebenen $2n$ ($n \geqq 3$) Permutationen der Eckenmenge eines regulären ebenen n-Ecks gebildet und in dem die Multiplikation mit Hilfe der Zusammensetzung von Permutationen erklärt wird, stellt eine Gruppe, die sogenannte *diëdrische Permutationsgruppe* von der Ordnung $2n$ dar. Diese Gruppe enthält neben der kleinsten Untergruppe weitere echte Untergruppen: die Untergruppe von der Ordnung n, die von allen den Drehungen der Eckpunkte um den Mittelpunkt des n-Ecks entsprechenden Elementen gebildet wird; n Untergruppen zweiter Ordnung, von denen jede von der identischen Permutation und einer weiteren, durch die symmetrische Abbildung der Eckpunkte in bezug auf eine Achse des n-Ecks definierten Permutation gebildet wird.

3. Die Anzahl der zu sich selbst inversen Elemente ist für jede endliche Gruppe gerader (ungerader) Ordnung gerade (ungerade).

4. Die Inversion einer abelschen Gruppe stellt einen Automorphismus auf dieser Gruppe dar.

5. In jeder abelschen Gruppe bilden die zu sich selbst inversen Elemente eine Untergruppe.

6. Es seien $\mathfrak{A}$, $\mathfrak{B}$ Untergruppen in $\mathfrak{G}$. Wenn das aus den Feldern A, B gebildete Produkt AB das Feld einer Untergruppe in $\mathfrak{G}$ darstellt, so sind die Untergruppen $\mathfrak{A}$, $\mathfrak{B}$ miteinander vertauschbar.

7. Es seien $\mathfrak{A} \subset \mathfrak{B}$ Untergruppen in $\mathfrak{G}$. Dann gilt $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{B}$, $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{A}$. Wenn die Untergruppe $\mathfrak{C}$ in $\mathfrak{G}$ mit $\mathfrak{A}$ vertauschbar ist, so ist auch die Untergruppe $\mathfrak{C} \cap \mathfrak{B}$ mit $\mathfrak{A}$ vertauschbar.

8. Jede Gruppe hat ein Zentrum.

9. Es sei $p \in \mathfrak{G}$ ein beliebiges Element der Gruppe $\mathfrak{G}$. Wir definieren in der Gruppe $\mathfrak{G}$ eine neue Multiplikation mit dem Produktzeichen $\circ$ auf folgende Weise: Für beliebige Elemente $x, y \in \mathfrak{G}$ wird das Produkt $x \circ y$ durch das Element $xp^{-1}y$ dargestellt, also $x \circ y = xp^{-1}y$. Sodann gilt: a) Das aus dem Feld G der Gruppe $\mathfrak{G}$ und aus der Multiplikation $\circ$ bestehende Gruppoid $\overset{\circ}{\mathfrak{G}}$ ist eine Gruppe; b) das Einselement von $\overset{\circ}{\mathfrak{G}}$ ist durch p und das zu einem beliebigen Element $x \in \overset{\circ}{\mathfrak{G}}$ inverse Element in $\overset{\circ}{\mathfrak{G}}$ durch $px^{-1}p$ dargestellt.

Bemerkung. Wir wollen die Gruppe $\overset{\circ}{\mathfrak{G}}$ die *mit der Gruppe* $\mathfrak{G}$ *assoziierte* (p)*-Gruppe* nennen.