Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 20 (1947)

Artikel: Das "schiefe" Produkt in der Gruppentheorie.
Autor: Rédei, L.
DOI: https://doi.org/10.5169/seals-18060

Das „schiefe Produkt" in der Gruppentheorie

mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören

Von L. RÉDEI, Szeged (Ungarn)

§ 1. Einleitung

In dieser Arbeit führe ich ein sehr einfaches Prinzip ein, mit dessen Hilfe man aus einer Gruppe G und einem Ring R weitere Gruppen konstruieren kann. Diese Gruppen werden im allgemeinen auch dann nicht kommutativ sein, wenn G und R kommutativ sind, und deshalb nenne ich jede dieser Gruppen ein *schiefes Produkt* von G, R. In der Tat werde ich dreierlei Konstruktionen verwenden, entsprechend bezeichne ich das schiefe Produkt mit GR, $G(+)R$, $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$, und nenne es ein schiefes Produkt vom ersten, zweiten, dritten Typ. Jeder Typ umfaßt bei gegebenen G, R im allgemeinen mehrere Gruppen, da sich die zu verwendenden Konstruktionen auf mehrere Arten ausführen lassen. Es wird sich am hier zu besprechenden Beispiel zeigen, daß sich unser schiefes Produkt sehr gut zur Darstellung gewisser (endlicher) Gruppen gebrauchen läßt.

Es sei irgendeine Eigenschaft vorgelegt, von der wir annehmen, daß sie unter anderem auch der Einheitsgruppe (d. h. der Gruppe mit nur einem Element) zukommt. Dann können wir jeder endlichen Gruppe G eine bestimmte Stufenzahl n $(\geqq 0)$ beilegen, so daß $n = 0$ ist dann und nur dann, wenn G von der genannten Eigenschaft ist, für ein sonstiges G soll aber n um 1 größer sein als das Maximum der Stufenzahlen derjenigen Untergruppen von G, die kleiner als G sind. Nachher sei die vorgelegte Eigenschaft die Kommutativität. Als Anwendung des schiefen Produktes bestimmen wir die Gruppen 1-ter Stufe (genauer könnte man über 1-stufig nichtkommutative Gruppen sprechen), die also diejenigen endlichen nichtkommutativen Gruppen sind, die lauter kommutative echte Untergruppen haben. Diese Gruppen sind wichtig, da jede endliche nichtkommutative Gruppe wenigstens eine solche Untergruppe enthält.

Mit ihnen haben sich *Miller* und *Moreno*[1]), weiter auch *Schmidt*[2]), beschäftigt. Sie haben bewiesen, daß die Ordnung der Gruppen 1-ter Stufe höchstens durch zwei verschiedene Primzahlen teilbar ist (die Gruppen selbst also auflösbar sind), haben auch die vorkommenden Ordnungen genau angegeben, aber die Struktur dieser Gruppen nicht restlos bestimmt, und so blieb unter anderem unbeantwortet, wie viele Gruppen 1-ter Stufe zu einer festen Ordnung gehören[3]). Ich bestimme diese Gruppen vollständig und entwickle ihre Eigenschaften ausführlich. Für die Ordnungszahlen stellt sich heraus, daß zu einer Ordnung $p^u q^v$ (p, q verschiedene Primzahlen) höchstens zwei Gruppen 1-ter Stufe gehören, und zwar genau soviel wie die Anzahl der richtigen Aussagen unter „u, v ist die kleinste natürliche Zahl mit $q \mid p^u - 1$ bzw. $p \mid q^v - 1$". Unter 10^4 sind nur 12, 56, 80, 351, 992, 2025, 3875, 4352, 5103, 8125 solche Ordnungszahlen mit zwei Gruppen 1-ter Stufe. Zu einer Ordnung p^e gehört nur im Fall $e \geqq 3$ eine Gruppe 1-ter Stufe, und dann ist ihre genaue Zahl $e - 2 + \left[\frac{e-1}{2}\right]$, wobei $[x]$ die größte ganze Zahl $\leqq x$ bezeichnet.

Alle diese Gruppen teile ich auf Grund ihrer näheren Eigenschaften in vier Typen ein, und zwar in den ersten Typ die Gruppen 1-ter Stufe von einer Ordnung $p^u q^v$, in die übrigen drei Typen die p-Gruppen 1-ter Stufe. In den vierten Typ gehört die Quaternionengruppe (von der Ordnung 8) allein. Die Gruppen 1-ter Stufe von den drei ersten Typen lassen sich überraschend einfach und elegant als je ein schiefes Produkt GR, $G(+)R$, $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$ darstellen. Das ist um so mehr zu würdigen, als insbesondere die Gruppen 1-ter Stufe von dem ersten Typ als „abstrakte Gruppen" von ziemlich komplizierter Struktur sind, als schiefes Produkt GR entstehen sie aber als äußerst einfacher Spezialfall so, daß man für G und R eine zyklische Gruppe von Primzahlpotenzordnung bzw. einen endlichen (also kommutativen) Körper einsetzt (dessen Elementenzahl bekanntlich ebenfalls eine Primzahlpotenz ist). Für die Gruppen 1-ter Stufe von dem zweiten und dritten Typ kommt man ähnlich einfach aus, man braucht

[1]) *G.A.Miller* and *H.C.Moreno*, Non-abelian groups in which every subgroup is abelian, Transactions Amer. Math. Soc. 4 (1903), 398—404.

[2]) *O.Schmidt*, Über Gruppen, deren sämtliche Teiler spezielle Gruppen sind (russisch mit deutscher Zusammenfassung), Receuil Math. de la Soc. Math. d. Moscou 31 (1924), 367—372. Dabei wird eine endliche Gruppe „speziell" genannt, wenn sie ein direktes Produkt von p-Gruppen ist. In unserer obigen Terminologie handelt es (allgemeiner als bei uns) von den „1-stufig nichtspeziellen" Gruppen.

[3]) Die Verfasser der Arbeiten [1]), [2]) meinten irrtümlich, alle Fragen über die Gruppen erster Stufe restlos erledigt zu haben. Noch weniger wurden die 1-stufig nichtspeziellen Gruppen in der Arbeit[2]) vollkommen bestimmt. Auf diese Frage hoffe ich zurückzukommen.

in allen drei Fällen nur die allereinfachsten kommutativen Strukturen G, R zu Hilfe zu nehmen. Diese Erscheinung läßt sich nach zwei Richtungen auswerten, einerseits als Beleg für die Brauchbarkeit des schiefen Produktes aller drei Typen, anderseits als begründete Hoffnung, daß nach den so „einfach" gewordenen Gruppen 1-ter Stufe sich auch die Gruppen 2-ter Stufe mit Erfolg untersuchen lassen. Es ist zu vermuten, daß die letztere Frage zwangsläufig zu einer Verallgemeinerung unserer schiefen Produkte führen wird.

Die Resultate über die Gruppen 1-ter Stufe haben auch zwei interessante Folgerungen betreffend die (endlichen) kommutativen Gruppen.

In der einen handelt es sich um einen neulich von *Szép*[4]) gewonnenen schönen Satz, der eine hinreichende Bedingung ausspricht, damit eine Gruppe kommutativ sei. Ich werde diesen Satz wiedergewinnen und zugleich wesentlich verschärfen.

Als zweite Folgerung gebe ich alle Ordnungen an, zu denen nur kommutative Gruppen gehören. Das sind diejenigen

$$n = p_1 \ldots p_i q_1^2 \ldots q_j^2$$

mit verschiedenen Primzahlen $p_1, \ldots, q_j$, die zu

$$(p_1 - 1) \ldots (p_i - 1)(q_1^2 - 1) \ldots (q_j^2 - 1)$$

prim sind. Nach *Dirichlets* Satz über die arithmetische Progression gibt es zu jedem Paar i, j unendlich viele n mit der genannten Eigenschaft.

Ich teile meine Arbeit so ein: In den §§ 2—4 definiere ich die drei Typen schiefes Produkt allgemein (Sätze 1—3). In den §§ 5—8 gebe ich alle Gruppen 1-ter Stufe in vier verschiedenen Formen (Sätze 4—7) an. Den Beweis beende ich aber erst in den §§ 9—11, in denen ich nämlich zeige, daß alle Gruppen 1-ter Stufe unter den vorher angegebenen wirklich vorkommen und verschieden sind. Im § 12 entwickle ich die Eigenschaften der Gruppen 1-ter Stufe ausführlich. In den §§ 13, 14 beschäftige ich mich mit den angekündigten zwei Folgerungen betreffend die kommutativen Gruppen. Im § 15, der auch unmittelbar nach § 4 zu lesen ist, verweise ich auf die Beziehungen unserer schiefen Produkte mit der Literatur[5]).

---

[4]) Siehe die vorstehende Arbeit von *J. Szép:* On finite groups which are necessarily commutative.

[5]) Ich erwähne noch, daß ich schon im Jahre 1924 alle Gruppen erster Stufe bestimmt habe, und erst nachher von der Arbeit von *Miller* und *Moreno*[1]) Kenntnis nahm. Wegen dieser Arbeit habe ich meine Resultate nicht publiziert, zumal aus dem Grunde, daß ich mit meinen, damals noch komplizierten Resultaten nicht ganz zufrieden war. Erst die Sätze von Herrn *Szép*, von denen ich durch seine freundliche Mitteilung Kenntnis nahm, haben meine Aufmerksamkeit wieder auf diese Frage gelenkt, und so merkte ich, daß sich die Gruppen erster Stufe sehr durchsichtig als schiefes Produkt darstellen lassen.

§ 2. Das schiefe Produkt GR

Die hier folgenden Vorbereitungen betreffen teils auch schon die §§ 3, 4. G sei eine beliebige Gruppe mit den Elementen $\alpha, \beta, \ldots$ und dem Einselement ε, R ein beliebiger (nicht notwendig kommutativer) Ring, R^+ die additive (kommutative) Gruppe (aller Elemente) von R. Das Einselement in R bezeichnen wir mit 1, aber die Existenz setzen wir im allgemeinen nicht voraus. Entsprechend den zwei Grundoperationen in R, das sind die Multiplikation und Addition, läßt sich G im allgemeinen auf zwei Arten in R homomorph abbilden. Und zwar nennen wir eine eindeutige Abbildung $\overline{\alpha}$ oder α' ($\alpha \in G$; $\overline{\alpha}, \alpha' \in R$) von G in R (d. h. auf eine Teilmenge von R) eine Homomorphie, wenn unbeschränkt die „Homomorphieeigenschaft"

$$\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta} \tag{1}$$

mit $\overline{\varepsilon} = 1$, bzw.

$$(\alpha\beta)' = \alpha' + \beta' \tag{2}$$

gilt; im ersten Fall ist offenbar immer $\overline{\alpha} \neq 0$, im zweiten Fall braucht das Einselement 1 nicht zu existieren und muß notwendig $\varepsilon' = 0$ sein. Wir nennen diese Homomorphien multiplikativ bzw. additiv. Bekanntlich bilden die verschiedenen Bilder $\overline{\alpha}$ bzw. α' eine multiplikative bzw. additive Gruppe in R, die beidesmal das homomorphe Bild von G genannt wird. Bezeichnet N die Gruppe der α mit $\overline{\alpha} = 1$ bzw. $\alpha' = 0$, so ist N eine normale Untergruppe von G, und die Faktorgruppe G/N ist isomorph zu der Gruppe der $\overline{\alpha}$ bzw. α'. Wir nennen N den Kern der Homomorphie. Umgekehrt wenn man irgendeine normale Untergruppe N von G angibt, so daß eine zu G/N isomorphe multiplikative oder additive Gruppe H in R existiert, so läßt sich immer wenigstens eine Homomorphie $\overline{\alpha}$ bzw. α' mit dem Kern N konstruieren, die G auf H abbildet.

Zu den hier und in den folgenden §§ 3, 4 zu definierenden schiefen Produkten von G, R werden wir eine multiplikative bzw. additive bzw. zwei additive Homomorphien zu Hilfe nehmen, so daß also in den entsprechenden (schon in der Einleitung erwähnten) Bezeichnungen GR, $G(+)R$, $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$ die Anzahl der verwendeten „+"-Zeichen angibt, wie viel additive Homomorphien zur Konstruktion benötigt werden.

Die Definition von GR ist enthalten im folgenden:

Satz 1. *Es sei G eine Gruppe, R ein Ring mit Einselement, $\overline{\alpha}$ eine multiplikative homomorphe Abbildung von G in R. Die Menge aller (α, a) ($\alpha \in G$, $a \in R$) bildet nach der Produktregel*

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + \overline{\alpha}b) \tag{3}$$

eine Gruppe, die wir mit GR bezeichnen und ein schiefes Produkt (vom ersten Typ) von G, R nennen. Das Einselement ist $(\varepsilon, 0)$. *Wird*

$$A = (\alpha, a) \ , \qquad B = (\beta, b) \tag{4}$$

gesetzt, so ist das Inverse von A

$$A^{-1} = (\alpha^{-1}, -\overline{\alpha}^{-1}a) \ , \tag{5}$$

wobei $\overline{\alpha}^{-1}$ *das Inverse von* $\overline{\alpha}$ *in der Gruppe der* $\overline{\alpha}$ *bezeichnet; weiter ist*

$$B^{-1}AB = \left(\beta^{-1}\alpha\beta, \overline{\beta}^{-1}(a - b + \overline{\alpha}b)\right) \ , \tag{6}$$

$$A^{-1}B^{-1}AB = \left(\alpha^{-1}\beta^{-1}\alpha\beta, \overline{\alpha}^{-1}\overline{\beta}^{-1}\left((\overline{\alpha} - 1)\, b - (\overline{\beta} - 1)\, a\right)\right) , \tag{7}$$

$$A^n = \left(\alpha^n, (1 + \overline{\alpha} + \overline{\alpha}^2 + \cdots + \overline{\alpha}^{n-1})a\right) \quad (n \geqq 0) \ . \tag{8}$$

Wird nämlich $C = (\gamma, c)$ gesetzt, so gilt nach (3):

$$AB \cdot C = (\alpha\beta, a + \overline{\alpha}b)(\gamma, c) = (\alpha\beta\gamma, a + \overline{\alpha}b + \overline{\alpha\beta}\, c) \ ,$$

$$A \cdot BC = (\alpha, a)(\beta\gamma, b + \overline{\beta}c) = \left(\alpha\beta\gamma, a + \overline{\alpha}(b + \overline{\beta}c)\right) \ .$$

Beide Produkte sind wegen $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$ gleich. Offenbar gilt

$$(\alpha, a)(\varepsilon, 0) = (\alpha, a)$$

und wegen $\overline{\alpha}\,\overline{\alpha}^{-1} = 1$ auch

$$(\alpha, a)(\alpha^{-1}, -\overline{\alpha}^{-1}a) = (\varepsilon, a - \overline{\alpha}\,\overline{\alpha}^{-1}a) = (\varepsilon, 0) \ .$$

Alles dies beweist, daß GR eine Gruppe ist. Die übrigen Behauptungen beweist man mit einfacher Rechnung, insbesondere (8) mit einem Schluß von n auf $n + 1$.

Bemerkungen. Die Elemente A, B sind nach (3) dann und nur dann vertauschbar, wenn

$$\alpha\beta = \beta\alpha \ , \qquad (\overline{\alpha} - 1)\, b = (\overline{\beta} - 1)\, a$$

ist. Sind insbesondere G und R kommutativ, so lautet diese Bedingung einfach als

$$\begin{vmatrix} \overline{\alpha} - 1 & a \\ \overline{\beta} - 1 & b \end{vmatrix} = 0 \ . \tag{9}$$

Da diese Bedingung nur ganz selten identisch erfüllt wird, ist es berechtigt, daß wir GR ein „schiefes" Produkt nennen.

Wegen $(\alpha, 0)(\beta, 0) = (\alpha\beta, 0)$, $(\varepsilon, a)(\varepsilon, b) = (\varepsilon, a + b)$ bilden die Elemente $(\alpha, 0)$ bzw. (ε, a) je eine zu G bzw. R^+ isomorphe Untergruppe von GR. Bezeichnen wir diese Gruppen mit (G) und (R^+), so gilt auch

$$GR = (G)(R^+) = (R^+)(G) \ , \tag{10}$$

wobei die zwei letzten Produkte im gewöhnlichen Sinn zu deuten sind, d. h. das schiefe Produkt GR ist gleich dem Produkt seiner (zu G und R^+ isomorphen) Untergruppen (G), (R^+), und dabei kommt es auf die Reihenfolge der Faktoren nicht an. Zum Beweis von (10) berechnen wir

$$(\alpha, 0)(\varepsilon, a) = (\alpha, \overline{\alpha}a) \ , \qquad (\varepsilon, a)(\alpha, 0) = (\alpha, a) \ .$$

Indem nun α, a die Elemente von G bzw. R durchlaufen, werden durch $(\alpha, \overline{\alpha}a)$ bzw. (α, a) alle Elemente von GR in der Tat genau einmal dargestellt. Insbesondere für $(\alpha, \overline{\alpha}a)$ folgt dies nämlich daraus, daß $\overline{\alpha}$ sein Inverses $\overline{\alpha}^{-1}$ hat. Hiermit ist (10) richtig.

Wegen (10) ist es berechtigt, daß wir GR ein (schiefes) „Produkt" von G, R nennen. (Es wäre vielleicht richtiger, wenn wir GR wegen (10) ein schiefes Produkt von G, R^+ nannten, das tun wir aber deshalb nicht, da an der Konstruktion von GR nicht nur die Addition, sondern auch die Multiplikation in R teilnimmt.) Endlich bemerken wir hierzu noch, daß (3) für die „triviale" Abbildung $\overline{\alpha} = 1$ in die „direkte" Multiplikation

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + b)$$

übergeht. Somit umfaßt das schiefe Produkt GR das bekannte direkte Produkt von G, R^+ als trivialen Spezialfall.

§ 3. Das schiefe Produkt $G(+)R$

Im Ring R setzen wir jetzt die Existenz des Einselementes nicht voraus und definieren das schiefe Produkt $G(+)R$ im folgenden:

Satz 2. *Es sei G eine Gruppe, R ein Ring, α' eine additive homomorphe Abbildung von G in R mit der weiteren Eigenschaft*

$$\alpha'\beta' = 0 \ . \tag{11}$$

Die Menge aller (α, a) $(\alpha \in G, a \in R)$ bildet nach der Produktregel

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + b + \alpha' b) \tag{12}$$

eine Gruppe, die wir mit $G(+)R$ bezeichnen und ein schiefes Produkt (vom zweiten Typ) von G, R nennen. Das Einselement ist $(\varepsilon, 0)$. Wird

$$A = (\alpha, a), \qquad B = (\beta, b) \tag{13}$$

gesetzt, so ist das Inverse von A

$$A^{-1} = (\alpha^{-1}, -a + \alpha' a), \tag{14}$$

weiter ist

$$B^{-1}AB = (\beta^{-1}\alpha\beta, a + \alpha' b - \beta' a), \tag{15}$$

$$A^{-1}B^{-1}AB = (\alpha^{-1}\beta^{-1}\alpha\beta, \alpha' b - \beta' a), \tag{16}$$

$$A^n = (\alpha^n, na + \binom{n}{2} \alpha' a). \tag{17}$$

Wird nämlich $C = (\gamma, c)$ gesetzt, so gilt nach (12)

$$AB \cdot C = (\alpha\beta, a + b + \alpha' b)(\gamma, c) = (\alpha\beta\gamma, a + b + \alpha' b + c + (\alpha\beta)' c)$$

$$A \cdot BC = (\alpha, a)(\beta\gamma, b + c + \beta' c) = (\alpha\beta\gamma, a + b + c + \beta' c + \alpha'(b + c + \beta' c)).$$

Beide Produkte sind wegen $(\alpha\beta)' = \alpha' + \beta', \alpha'\beta' = 0$ gleich. Offenbar gilt

$$(\alpha, a)(\varepsilon, 0) = (\alpha, a)$$

und wegen des Spezialfalls $\alpha'^2 = 0$ von (11) auch

$$(\alpha, a)(\alpha^{-1}, -a + \alpha' a) = (\varepsilon, a - a + \alpha' a + \alpha'(-a + \alpha' a)) = (\varepsilon, 0).$$

Alles dies beweist, daß $G(+)R$ eine Gruppe ist. Auch die übrigen Behauptungen beweist man mit einfacher Rechnung.

Bemerkungen. Nach (12) lautet jetzt die Bedingung der Vertauschbarkeit von A, B einfach

$$\alpha\beta = \beta\alpha, \qquad \alpha' b = \beta' a,$$

insbesondere im Falle kommutativer G, R aber

$$\begin{vmatrix} \alpha' & a \\ \beta' & b \end{vmatrix} = 0. \tag{18}$$

Wieder gilt $(\alpha, 0)(\beta, 0) = (\alpha\beta, 0)$, $(\varepsilon, a)(\varepsilon, b) = (\varepsilon, a + b)$, und so bilden die $(\alpha, 0)$ bzw. (ε, a) je eine zu G und R^+ isomorphe Untergruppe (G) bzw. (R^+), für die dann wieder

$$G(+)R = (G)(R^+) = (R^+)(G) \tag{19}$$

gilt. Es ist nämlich

$$(\alpha, 0)(\varepsilon, a) = (\alpha, a + \alpha' a) , \qquad (\varepsilon, a)(\alpha, 0) = (\alpha, a) ,$$

und so besagt (19), daß durch $(\alpha, a + \alpha' a)$ bzw. $(\alpha, a)(\alpha \in G, a \in R)$ jedes Element von $G(+)R$ genau einmal dargestellt wird. Für das zweite ist das klar, für das erste müssen wir zeigen, daß $x + \alpha' x = a$ für festes α und a genau eine Lösung x in R hat. Eine Lösung ist $x = a - \alpha' a$. Ist aber y eine weitere Lösung, so ist $x + \alpha' x = y + \alpha' y$; nach Multiplikation mit α' folgt $\alpha' x = \alpha' y$, also auch $x = y$, womit (19) bewiesen ist.

Für die „triviale" Abbildung $\alpha' = 0$ ist $G(+)R$ nach (12) ein direktes Produkt. Hat R insbesondere keine Nullteiler, so folgt aus (11), daß unbeschränkt $\alpha' = 0$ gelten muß. Also gibt zu einem, vom direkten Produkt verschiedenen schiefen Produkt $G(+)R$ nur ein Ring R mit Nullteilern Anlaß. Bekanntlich schließt diese Einschränkung insbesondere für endliche Ringe nur die (endlichen) Körper aus.

Endlich bemerken wir, daß wenn in R das Einselement existiert, so ist $G(+)R$ nur ein Spezialfall von GR. In der Tat setzen wir $\overline{\alpha} = 1 + \alpha'$. Dann gilt wegen (11)

$$\overline{\alpha\beta} = 1 + (\alpha\beta)' = 1 + \alpha' + \beta' = (1 + \alpha')(1 + \beta') = \overline{\alpha}\,\overline{\beta} ,$$

also ist $\overline{\alpha}$ eine multiplikative homomorphe Abbildung von G in R. Weiter geht (12) wegen $b + \alpha' b = (1 + \alpha')b = \overline{\alpha} b$ in (3) über, und das beweist die Behauptung.

§ 4. Das schiefe Produkt $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$

Auch jetzt nehmen wir in R die Existenz des Einselementes nicht an und definieren das schiefe Produkt $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$ im folgenden:

Satz 3. *Es seien G eine Gruppe, R ein Ring, α', α'' zwei additive homomorphe Abbildungen von G in R. Die Menge aller (α, a) $(\alpha \in G, a \in R)$ bildet nach der Produktregel*

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + b + \alpha'\beta'') \tag{20}$$

eine Gruppe, die wir mit $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$ bezeichnen und ein schiefes Produkt (vom dritten Typ) von G, R nennen. Das Einselement ist $(\varepsilon, 0)$. Wird

$$A = (\alpha, a) , \qquad B = (\beta, b) \tag{21}$$

gesetzt, so ist das Inverse von A

$$A^{-1} = (\alpha^{-1}, -a + \alpha'\alpha'') \ , \tag{22}$$

weiter ist

$$B^{-1}AB = (\beta^{-1}\alpha\beta, a + \alpha'\beta'' - \beta'\alpha'') \ , \tag{23}$$

$$A^{-1}B^{-1}AB = (\alpha^{-1}\beta^{-1}\alpha\beta, \alpha'\beta'' - \beta'\alpha'') \ , \tag{24}$$

$$A^n = (\alpha^n, n\alpha + \binom{n}{2}\alpha'\alpha'') \ . \tag{25}$$

Wird nämlich $C = (\gamma, c)$ gesetzt, so gilt nach (20)

$$AB \cdot C = (\alpha\beta, a + b + \alpha'\beta'')(\gamma, c) = (\alpha\beta\gamma, a + b + \alpha'\beta'' + c + (\alpha\beta)'\gamma''),$$
$$A \cdot BC = (\alpha, a)(\beta\gamma, b + c + \beta'\gamma'') = (\alpha\beta\gamma, a + b + c + \beta'\gamma'' + \alpha'(\beta\gamma)''),$$

und so sind beide Produkte wegen $(\alpha\beta)' = \alpha' + \beta'$, $(\beta\gamma)'' = \beta'' + \gamma''$ gleich. Offenbar gilt $(\alpha, a)(\varepsilon, 0) = (\alpha, a)$ und wegen $(\alpha^{-1})'' = -\alpha''$ auch

$$(\alpha, a)(\alpha^{-1}, -a + \alpha'\alpha'') = (\varepsilon, a - a + \alpha'\alpha'' - \alpha'\alpha'') = (\varepsilon, 0) \ .$$

Alles dies beweist, daß $G(\overset{+}{+})R$ eine Gruppe ist. Die übrigen Behauptungen beweist man mit einfacher Rechnung.

Bemerkungen. Nach (20) lautet die Bedingung der Vertauschbarkeit von A, B: $\alpha\beta = \beta\alpha$, $\alpha'\beta'' = \beta'\alpha''$,

insbesondere für kommutative G, R:

$$\begin{vmatrix} \alpha' & \alpha'' \\ \beta' & \beta'' \end{vmatrix} = 0 \ . \tag{26}$$

Wohl gelten auch jetzt die (10) und (19) entsprechenden Zerlegungen

$$G(\overset{+}{+})R = (G)(R^+) = (R^+)(G) \ , \tag{27}$$

wobei (G) und (R^+) wieder die Menge aller $(\alpha, 0)$ bzw. (ε, a) bezeichnen, und (R^+) eine zu R^+ isomorphe Untergruppe von $G(\overset{+}{+})R$ ist, aber (G) ist diesmal im allgemeinen keine Gruppe mehr. Zunächst folgt nämlich die Richtigkeit von (27) aus $(\alpha, 0)(\varepsilon, a) = (\varepsilon, a)(\alpha, 0) = (\alpha, a)$. Wegen $(\varepsilon, a)(\varepsilon, b) = (\varepsilon, a + b)$ ist (R^+) eine zu R^+ isomorphe Untergruppe von $G(\overset{+}{+})R$. Endlich ist $(\alpha, 0)(\beta, 0) = (\alpha\beta, \alpha'\beta'')$, und so sehen wir, daß (G) nur dann eine Gruppe ist, wenn unbeschränkt $\alpha'\beta'' = 0$ gilt. In diesem (uninteressanten) Falle ist $G(\overset{+}{+})R$ nach (20) nichts anderes als das direkte Produkt von G, R^+.

§ 5. Die vier Typen der Gruppen 1-ter Stufe

Unten im Satz 4 geben wir alle Gruppen 1-ter Stufe in begrifflich einfachster Weise als Spezialfälle der schiefen Produkte an (bis auf die Quaternionengruppe). Die Konstruktionen dieser Gruppen führen wir dann in den Sätzen 5, 6, 7 in drei weiteren Formen explicit aus. Insbesondere drückt Satz 7 die Gruppen 1-ter Stufe als „abstrakte" Gruppen aus. Die Darstellungen in den Sätzen 5, 6 weichen voneinander nur wenig ab. Unter allen vier Darstellungen ist die zweite, im Satz 5 angegebene für die formal einfachste anzurechnen.

Wir führen noch ein paar Bezeichnungen ein:

p, q sind verschiedene positive Primzahlen.

$O(x)$ ist die Ordnung von x für eine endliche Gruppe x oder für ein Gruppenelement x von endlicher Ordnung.

$G(P_1, \ldots, P_i)$ ist die endliche kommutative Gruppe mit den Invarianten $P_1, \ldots, P_i$, die also notwendig Primzahlpotenzen sind, und es gilt $O\big(G(P_1, \ldots, P_i)\big) = P_1 \ldots P_i$. Insbesondere ist $G(P)$ die zyklische Gruppe von der Primzahlpotenzordnung P.

R^* ist für einen endlichen Ring R die (multiplikative) Gruppe aller von 0 und den Nullteilern von R verschiedenen Elemente von R, kurz die multiplikative Gruppe von R.

$k(P)$ ist der endliche (kommutative) Körper mit P-Elementen, wobei also P eine beliebige Primzahlpotenz ist. Bekanntlich ist $k(P)^+$ ein $G(p, \ldots, p)$ von der Ordnung P und $k(P)^*$ eine zyklische Gruppe von der Ordnung $P - 1$.

$R(m)$ ist der Restklassenring $\bmod m$, d. h. der Ring der (aus den ganzen Zahlen gebildeten) Restklassen $\bmod m$. $R(m)^+$ ist zyklisch von der Ordnung m, $R(m)^*$ ist von der Ordnung $\varphi(m)$ und ist für eine Primzahlpotenz m zyklisch, wobei φ das Eulersche Zeichen bedeutet. Insbesondere ist $R(p)$ gleich $k(p)$.

$O\big(q(\bmod p)\big)$ ist die Ordnung der Restklasse $q \pmod p$ (in der Gruppe $R(p)^*$), d. h. die kleinste natürliche Zahl n mit $q^n \equiv 1 \pmod p$.

Nunmehr sprechen wir folgenden Satz aus:

Satz 4. *Die Gruppen 1-ter Stufe verteilen sich auf vier Typen, von denen die zu den ersten drei Typen gehörenden Spezialfälle der schiefen Produkte GR, $G(+)R$ bzw. $G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R$ sind. In diesen ist gemeinsam, daß die jedesmal zu verwendenden Homomorphien $\overline{\alpha}$, α' bzw. α', α'' einen Kern vom Index p in G haben, weiter sind die im letzten Fall zu den α', α'' gehörenden Kerne verschieden. Dies vorausgeschickt, sind die vier Typen die folgenden:*

Erster Typ. *Bei gegebenen* p, q, u $(u \geqq 1)$

$$G_I(p, q, u) = GR \quad \big(G = G(p^u),\ R = k(q^v),\ v = O\big(q(\mathrm{mod}\ p)\big)\big) \ . \tag{28}$$

Es ist

$$O\big(G_I(p, q, u)\big) = p^u q^v \ . \tag{29}$$

Zweiter Typ. *Bei gegebenen* p, u, v $(u \geqq 1, v \geqq 2)$

$$G_{II}(p, u, v) = G(+)R \quad \big(G = G(p^u),\ R = R(p^v)\big) \ . \tag{30}$$

Es ist

$$O\big(G_{II}(p, u, v)\big) = p^{u+v} \ . \tag{31}$$

Dritter Typ. *Bei gegebenen* p, u, v $(u \geqq v \geqq 1)$

$$G_{III}(p, u, v) = G\left(\begin{smallmatrix}+\\+\end{smallmatrix}\right)R \quad \big(G = G(p^u, p^v),\ R = R(p)\big) \ . \tag{32}$$

Es ist

$$O\big(G_{III}(p, u, v)\big) = p^{u+v+1} \ . \tag{33}$$

Vierter Typ. *Die Quaternionengruppe von der Ordnung* 8.

Diese Gruppen hängen von der speziellen Wahl der Homomorphien $\bar{\alpha}$, α', α'' *nicht ab, sondern sind durch die jedesmal angegebenen* p, q, u, v *eindeutig bestimmt und sind verschieden mit der einzigen Ausnahme, daß die zwei Gruppen* $G_{II}(2, 1, 2)$, $G_{III}(2, 1, 1)$ *von 8-ter Ordnung gleich sind. (Die so entstandene „Lücke" wird durch die Quaternionengruppe von derselben Ordnung „ersetzt".) Zu einer Ordnung* $p^u q^v$ $(u, v \geqq 1)$ *gehören also zwei, eine oder keine Gruppen 1-ter Stufe, je nachdem von den Bedingungen*

$$u = O\big(p(\mathrm{mod}\ q)\big) \ , \qquad v = O\big(q(\mathrm{mod}\ p)\big)$$

zwei, eine oder keine erfüllt sind. Zu einer Ordnung p^e $(e \geqq 3)$ *gehören* $e-2$ *bzw.* $\left[\frac{e-1}{2}\right]$ *Gruppen 1-ter Stufe vom zweiten bzw. dritten Typ, insgesamt also* $e - 2 + \left[\frac{e-1}{2}\right]$ *Gruppen.*

Bemerkung. Es läßt sich leicht zeigen, daß die Quaternionengruppe kein schiefes Produkt ist.

Wir beweisen zuerst, daß die Gruppen (kurz) G_I, G_{II}, G_{III} existieren und von den $\bar{\alpha}$, α', α'' unabhängig sind. Wir fangen es mit G_I an. Da $G = G(p^u)$ zyklisch von der Ordnung p^u ist, enthält G eine einzige normale Untergruppe vom Index p. Andererseits ist $R^* = k(q^v)^*$ zyklisch

von der Ordnung $q^v - 1$ $(\equiv 0 \pmod p)$, und somit enthält R^* eine einzige zyklische Untergruppe p-ter Ordnung. Also existiert eine gewünschte Homomorphie $\overline{\alpha}$, zugleich auch wenigstens ein G_I. Weiter aber ist klar, daß sich jede weitere solche Homomorphie in der Form $\overline{\alpha}^i$ $(p \nmid i)$ annehmen läßt. Die zugehörigen zwei Gruppen G_I, G_I' bestehen aus denselben Elementen (α, a) und weichen nur darin ab, daß man in ihnen bzw. nach den Regeln (vgl. (3)).

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + \overline{\alpha}b) \ , \qquad (\alpha, a) \circ (\beta, b) = (\alpha\beta, a + \overline{\alpha}^i b) \quad (34)$$

multipliziert. Es genügt also, zu zeigen, daß es eine (eindeutige) Abbildung S der Menge aller (α, a) auf sich gibt, für die die Homomorphieeigenschaft

$$S\big((\alpha, a) \circ (\beta, b)\big) = S(\alpha, a)\, S(\beta, b) \quad (35)$$

gilt, denn dann sind beide Gruppen G_I, G_I' isomorph. Ein solches S läßt sich durch $S(\alpha, a) = (\alpha^i, a)$ angeben. Wegen $p \nmid i$ durchläuft nämlich α^i gleichzeitig mit α alle Elemente von G, und so ist nur noch (35) zu beweisen. Die linke und rechte Seite ist nach (34) bzw.

$$S(\alpha\beta, a + \overline{\alpha}^i b) = \big((\alpha\beta)^i, \ a + \overline{\alpha}^i b\big) = (\alpha^i\beta^i, \ a + \overline{\alpha}^i b) \ ,$$
$$(\alpha^i, a)(\beta^i, b) = (\alpha^i\beta^i, \ a + \overline{\alpha^i} b) = (\alpha^i\beta^i, \ a + \overline{\alpha}^i b) \ .$$

Beide sind gleich, woraus die Behauptung folgt.

Der Fall von G_{II} ist sehr ähnlich. Statt des vorigen R^* kommt jetzt $R^+ = R(p^v)^+$ in Betracht. Da diese additive Gruppe zyklisch von der Ordnung p^v ist, so hat sie eine einzige zyklische Untergruppe p-ter Ordnung. Eine gewünschte Homomorphie α' existiert also auch jetzt, für die nämlich wegen $v \geqq 2$ offenbar auch (11) gilt, und alle weiteren lassen sich in der Form $i\alpha'$ angeben. Alles übrige geht genau so wie im vorigen Fall, mit (demselben S aber) dem einzigen Unterschied, daß man überall $i\alpha'$ statt $\overline{\alpha}^i$ einzusetzen hat, und so ist die Behauptung auch jetzt richtig.

Im Fall G_{III} hat $G = G(p^u, p^v)$ mehrere (insgesamt $p + 1$) normale Untergruppen vom Index p, weiter ist $R^+ = R(p)^+$ selbst von der Ordnung p, und so existieren die gewünschten Homomorphien α', α'', zugleich also existiert auch wenigstens ein G_{III}. Für das übrige verfahren wir anders als in den vorigen zwei Fällen, und zwar zeigen wir direkt, daß G_{III} von der speziellen Wahl der α', α'' unabhängig ist. Hierzu führen wir eine Basis ϱ, σ für G ein mit $O(\varrho) = p^u$, $O(\sigma) = p^v$. Zwei beliebige Elemente von G lassen sich in der Form

$$\alpha = \varrho^i \sigma^j,\ \beta = \varrho^k \sigma^l \quad (i, k = 0, \ldots, p^u - 1;\ j, l = 0, \ldots, p^v - 1) \tag{36}$$

annehmen, und so erscheint die Produktregel für G_{III} nach (20) in der Form

$$(\varrho^i \sigma^j, a)(\varrho^k \sigma^l, b) = \left(\varrho^{i+k} \sigma^{j+l},\ a + b + (i\varrho' + j\sigma')(k\varrho'' + l\sigma'')\right), \tag{37}$$

wobei nämlich $\alpha' = i\varrho' + j\sigma'$, $\beta'' = k\varrho'' + l\sigma''$ berücksichtigt wurde. Der Kern der Homomorphie α' besteht aus den α mit $\alpha' = 0$, d. h. $i\varrho' + j\sigma' = 0$. Da beide Homomorphien α', α'' verschiedene Kerne haben, dürfen die Lösungen i, j der Gleichungen $i\varrho' + j\sigma' = 0$, $i\varrho'' + j\sigma'' = 0$ nicht übereinstimmen, und das hat

$$d = \begin{vmatrix} \varrho' & \sigma' \\ \varrho'' & \sigma'' \end{vmatrix} \neq 0 \tag{38}$$

zur Folge. Nunmehr setzen wir

$$A = (\varrho, 0), \qquad B = (\sigma, 0), \qquad C = (\varepsilon, d)\ . \tag{39}$$

Es ist nach (37) klar, daß

$$AC = CA\ , \qquad BC = CB \tag{40}$$

ist. Weiter ist nach (37) offenbar $A^i B^j = (\varrho^i \sigma^j, a_{ij})$, wobei a_{ij} irgendein Element von R ist, also nach (39) und (37) $A^i B^j C^m = (\varrho^i \sigma^j, a_{ij} + md)$. Damit haben wir gezeigt, daß sich alle Elemente von G_{III} in der Form $A^i B^j C^m$ schreiben lassen. Da insbesondere

$$A^k = (\varrho^k, x)\ , \qquad B^j = (\sigma^j, y)$$

gilt mit irgendwelchen Elementen x, y (ϵR), so folgt aus (24) wegen $\varrho\sigma = \sigma\varrho$ mit Rücksicht auf (38):

$$A^{-k} B^{-j} A^k B^j = \left(\varepsilon, jk\,(\varrho'\sigma'' - \sigma'\varrho'')\right) = (\varepsilon, jkd)\ .$$

Die rechte Seite ist nach (39), (37) offenbar C^{jk}, also ist

$$A^k B^j = B^j A^k C^{jk}\ .$$

Dies ergibt wegen (40)

$$A^i B^j C^m \cdot A^k B^l C^n = A^{i+k} B^{j+l} C^{m+n-jk}\ .$$

Diese neue Form der Produktregel in G_{III} ist von α', α'' unabhängig, und das zeigt die Richtigkeit unserer Behauptung.

Jetzt wollen wir zeigen, daß die Gruppen von allen vier Typen im Satz 4 von der 1-ten Stufe sind. Hier genügt es zu zeigen, daß alle diese Gruppen ein nichtvertauschbares Elementenpaar haben und durch ein beliebiges solches Paar auch erzeugt werden. Das tun wir zuerst für G_I. Ein Elementenpaar

$$A = (\alpha, a) \ , \qquad B = (\beta, b) \qquad (\alpha, \beta \in G(p^u) \, ; \ \ a, b \in k(q^v)) \tag{41}$$

ist nach (9) dann und nur dann nichtvertauschbar, wenn

$$d = \begin{vmatrix} \overline{\alpha} - 1 & a \\ \overline{\beta} - 1 & b \end{vmatrix} \neq 0 \tag{42}$$

ist. Dies findet sicher statt, wenn α ein Basiselement von $G(p^u)$, also $\overline{\alpha} \neq 1$, weiter $a = 0$, $\beta = \varepsilon$, also $\overline{\beta} = 1$ und $b \neq 0$ ist. Betrachten wir nunmehr ein nichtvertauschbares Paar A, B, wofür also (42) gilt. Dann kann nicht $\overline{\alpha} = \overline{\beta} = 1$ sein. Wir dürfen annehmen, daß eben $\overline{\alpha} \neq 1$ ist. Einerseits ist dann α ein Basiselement von $G(p^u)$, andererseits ist $\overline{\alpha}$ ein Element p-ter Ordnung von $k(q^v)^*$, also $\overline{\alpha}^p = 1$ und somit

$$\frac{\overline{\alpha}^p - 1}{\overline{\alpha} - 1} = 0 \ . \tag{43}$$

Ziehen wir jetzt den in $k(q^v)$ enthaltenen Primkörper $k(q)$ heran. In diesem zerfällt das Polynom

$$\frac{x^p - 1}{x - 1}$$

wegen $v = O\,(q \pmod p)$ in lauter irreduzible Faktoren v-ten Grades, und so ist $\overline{\alpha}$ wegen (43) ein Element v-ten Grades von $k(q^v)$ über $k(q)$. Dies vorausgeschickt, bestimmen wir nach (7), (8) (und $\alpha\beta = \beta\alpha$, $\overline{\alpha^n} = \overline{\alpha}^n$) den Kommutator

$$C_n = A^{-n} B^{-1} A^n B =$$

$$\left(\varepsilon, \overline{\alpha}^{-n} \overline{\beta}^{-1} \left((\overline{\alpha}^n - 1)\, b - (\overline{\beta} - 1)(1 + \overline{\alpha} + \cdots + \overline{\alpha}^{n-1})\, a \right)\right) \quad (n \geqq 0) \ .$$

Die rechte Seite ist nach (42) offenbar

$$\left(\varepsilon, \overline{\alpha}^{-n} \overline{\beta}^{-1} (1 + \overline{\alpha} + \cdots + \overline{\alpha}^{n-1})\, d\right) \ .$$

Also ist

$$C_n = \left(\varepsilon, (c^{n-1} + \cdots + c + 1)\, d_1\right) \ ,$$

wobei $d_1 = \overline{\alpha}^{-1} \overline{\beta}^{-1} d \neq 0$ und von n unabhängig, weiter $c = \overline{\alpha}^{-1}$, also (mit $\overline{\alpha}$ zusammen) ein Element v-ten Grades von $k(q^v)$ über $k(q)$ ist.

Irgendein Element (ε, x) $(x \neq 0)$ von G_I ist wegen $(\varepsilon, x)^q = (\varepsilon, qx) = (\varepsilon, 0)$ von der Ordnung q. Das trifft für die C_n $(n = 1, \ldots, v)$ offenbar zu. Dabei sind sie auch miteinander vertauschbar. Wir zeigen, daß sie eine Gruppe q^v-ter Ordnung erzeugen. Hierzu ist genug zu zeigen, daß die $C_1, \ldots, C_v$ unabhängig sind. Diese Behauptung ist äquivalent mit der Unabhängigkeit der Elemente

$$C_1' = C_1, \quad C_n' = C_n C_{n-1}^{-1} \qquad (n = 2, \ldots, v) \ .$$

Da $C_n' = (\varepsilon, c^{n-1} d_1)$ und c ein Element v-ten Grades von $k(q^v)$ über $k(q)$ ist, kann

$$C_v'^{i_v} \ldots C_1'^{i_1} = \left(\varepsilon, (i_v c^{v-1} + \cdots + i_2 c + i_1) d_1\right) = (\varepsilon, 0)$$

nur für $q \mid i_n$ $(n = 1, \ldots, v)$ bestehen, und das zeigt die Richtigkeit unserer letzten Behauptung. Hiernach enthält die durch die Elemente A, B erzeugte Gruppe eine Untergruppe q^v-ter Ordnung. Sie enthält auch das Element $A = (\alpha, a)$, dessen Ordnung nach (8) eine Vielfache der Ordnung p^u von α ist (in der Wirklichkeit ist $O(A) = O(\alpha) = p^u$). Folglicherweise erzeugen A, B eine Untergruppe mit einer durch $p^u q^v$ teilbaren Ordnung. Diese Gruppe muß wegen (29) selbst G_I sein, womit die Behauptung für diesen Fall bewiesen ist.

Für G_{II} kommen wir schnell zum Ziel. Ein beliebiges Elementenpaar ist jetzt

$$A = (\alpha, a) \ , \qquad B = (\beta, b) \qquad \left(\alpha, \beta \in G(p^u); \ a, b \in R(p^v)\right)$$

und die Bedingung der Nichtvertauschbarkeit lautet nach (18) so:

$$d = \begin{vmatrix} \alpha' & a \\ \beta' & b \end{vmatrix} \neq 0 \ .$$

Dies trifft z. B. zu, wenn α ein Basiselement von $G(p^u)$, also $\alpha' \neq 0$ und $a = 0$, $\beta = \varepsilon$, $b = 1$ ist. Wenn nun A, B nichtvertauschbar sind, so kann vor allem nicht $\alpha' = \beta' = 0$ sein. Wir dürfen $\alpha' \neq 0$ annehmen, und dann ist α ein Basiselement von $G(p^u)$. Hieraus folgt, daß β eine Potenz α^n von α ist. Offenbar erzeugen A, B und $A, A^{-n}B$ dieselbe Gruppe. Dabei ist $A^{-n}B$ wegen $\beta = \alpha^n$ von der Form (ε, x). Ersetzen wir also B durch $A^{-n}B$, was ja gestattet ist, so hat das zur Folgerung, daß man von vornherein $\beta = \varepsilon$ annehmen darf. Da $\varepsilon' = 0$ und auch die „neuen" A, B nichtvertauschbar sind, muß $\alpha' b \neq 0$ sein. Es fällt aber α' in die Untergruppe p-ter Ordnung der zyklischen Gruppe $R(p^v)^+$, und so folgt weiter, daß b ein Basiselement von $R(p^v)^+$ ist. Nun ist nach (16)

$$C = A^{-1} B^{-1} A B = (\varepsilon, d) \ ,$$

weiter ist wegen $d \neq 0$ jedes Bildelement ω' $(\omega \in G(p^u))$ ein Vielfaches von d. Letzteres hat nach (17), (12) (und $\beta = \varepsilon$) zur Folgerung, daß

$$A^i B^j = (\alpha^i,\ ia + jb + nd)$$

gilt, wobei n irgendeine, von i, j abhängende ganze Zahl ist. Wegen $C^{-n} = (\varepsilon,\ -nd)$ ist dann

$$A^i B^j C^{-n} = (\alpha^i,\ ia + jb)\ .$$

Da α und b je ein Basiselement von $G(p^u)$ bzw. $R(p^v)^+$ ist, erzeugt die rechte Seite alle Elemente von G_{II}, woraus die Richtigkeit der Behauptung folgt.

Noch leichter wird der Fall von G_{III} sein. Da wir oben schon gesehen haben, daß G_{III} nichtkommutativ ist, brauchen wir nur noch zu zeigen, daß G_{III} durch jedes nichtvertauschbare Elementenpaar

$$A = (\alpha, a),\quad B = (\beta, b) \qquad (\alpha, \beta \in G(p^u, p^v);\ \ a, b \in R(p))$$

erzeugt wird. Nach (26) gilt

$$d = \begin{vmatrix} \alpha' & \alpha'' \\ \beta' & \beta'' \end{vmatrix} \neq 0\ .$$

Wir drücken α, β wieder in der Form (36) durch die Basis ϱ, σ von $G(p^u, p^v)$ aus. Dann ist

$$d = \begin{vmatrix} i\varrho' + j\sigma' & i\varrho'' + j\sigma'' \\ k\varrho' + l\sigma' & k\varrho'' + l\sigma'' \end{vmatrix} = \begin{vmatrix} i & j \\ k & l \end{vmatrix} \begin{vmatrix} \varrho' & \varrho'' \\ \sigma' & \sigma'' \end{vmatrix} \neq 0\ ,$$

also auch $\begin{vmatrix} i & j \\ k & l \end{vmatrix} \neq 0$. Hieraus folgt nach (36), daß α, β die Gruppe $G(p^u, p^v)$ erzeugen. Nach (20) kommt also in den durch A, B erzeugten Elementen (ω, x) jedes Element ω von $G(p^u, p^v)$ wenigstens einmal vor. Da aber insbesondere $(\varepsilon, 0)$ und nach (24) auch noch

$$A^{-1}B^{-1}AB = (\varepsilon, d)$$

Elemente der durch A, B erzeugten Untergruppe sind, so ist die Ordnung dieser Gruppe $> p^{u+v}$. Wegen (33) kann dann die Ordnung nur p^{u+v+1} sein, und das war die Behauptung.

Endlich ist die Quaternionengruppe auch von 1-ter Stufe, da sie nichtkommutativ ist und die echten Untergruppen höchstens von 4-ter Ordnung sind.

Die restlichen Behauptungen des Satzes, daß er nämlich alle Gruppen 1-ter Stufe umfaßt, und zwar jede solche nur einmal, beweisen wir später.

§ 6. Die zweite Darstellung der Gruppen 1-ter Stufe

Die Gruppen 1-ter Stufe drücken wir hier und in den §§ 7, 8 in den Sätzen 5, 6, 7 in drei weiteren Formen aus. Der volle Beweis dieser Sätze wird mit dem des Satzes 4 zusammen später erfolgen.

Wir haben schon bewiesen, daß die Gruppen im Satz 4 unabhängig davon sind, wie man die zur Konstruktion nötigen Homomorphien $\overline{\alpha}$, α', α'' wählt. Indem wir diese Homomorphien geeignet wählen, kommen wir nach (3), (12), (20) unmittelbar zum folgenden:

Satz 5. *Die ersten drei Typen G_I, G_{II}, G_{III} der Gruppen 1-ter Stufe lassen sich auch so angeben:*

Erster Typ. *Man nehme ein erzeugendes Element ϱ von $G(p^u)$ $(u \geqq 1)$, ein Element r von der Ordnung p von $k(q^v)^*$ $\left(\text{mit } v = O\,(q \pmod p)\right)$ und multipliziere die*

$$(\varrho^i, a) \qquad \left(i = 0, \ldots, p^u - 1\,;\ \ a \in k(q^v)\right)$$

nach der Regel

$$(\varrho^i, a)(\varrho^k, b) = (\varrho^{i+k}, a + r^i b)\ . \tag{44}$$

Zweiter Typ. *Man behalte das vorige ϱ und multipliziere die*

$$(\varrho^i, a) \qquad \left(i = 0, \ldots, p^u - 1\,;\ \ a \in R(p^v)\right)\ ; \qquad (v \geqq 2)$$

nach der Regel

$$(\varrho^i, a)(\varrho^k, b) = (\varrho^{i+k}, a + b + p^{v-1} ib)\ . \tag{45}$$

Dritter Typ. *Man nehme eine Basis ϱ, σ von $G(p^u, p^v)$ $(u \geqq v \geqq 1)$ mit $O(\varrho) = p^u$, $O(\sigma) = p^v$ und multipliziere die*

$$(\varrho^i \sigma^j, a) \qquad \left(i = 0, \ldots, p^u - 1\,;\ \ j = 0, \ldots, p^v - 1\,;\ \ a \in R(p)\right)$$

nach der Regel

$$(\varrho^i \sigma^j, a)(\varrho^k \sigma^l, b) = (\varrho^{i+k} \sigma^{j+l}, a + b + il)\ , \tag{46}$$

wobei man das Glied il als das Element $il \cdot 1$ von $R(p)$ aufzufassen hat.

§ 7. Die dritte Darstellung der Gruppen 1-ter Stufe

Satz 6. *Die vier Typen (G_I, G_{II}, G_{III} und die Quaternionengruppe) der Gruppen 1-ter Stufe lassen sich auch so angeben:*

Erster Typ. *Bei gegebenen* p, q, u $(u \geqq 1)$ *bezeichne man mit* $\Psi(x)$ *einen (gleichgültig welchen)* mod q *irreduziblen Faktor von* $\dfrac{x^p - 1}{x - 1}$ *mit dem Leitkoeffizienten* 1, *mit* v *den Grad von* $\Psi(x)$, *der (bekanntlich) durch* p, q *bestimmt, und zwar* $v = O\,(q \pmod p)$ *ist, bilde die Paare* $(i, f(x))$ *aller ganzen Zahlen* i *und ganzzahligen Polynome* $f(x)$, *definiere für sie eine Gleichheit*

$$(i, f(x)) = (k, g(x)) \qquad (i \equiv k \pmod{p^u},\ f(x) \equiv g(x) \pmod{q,\ \Psi(x)})$$

und das Produkt

$$(i, f(x))\,(k, g(x)) = (i + k,\ f(x) + x^i g(x)) \ . \tag{47}$$

Zweiter Typ. *Bei gegebenen* p, u, v $(u \geqq 1\,;\ v \geqq 2)$ *bilde man die Paare* (i, j) *aller ganzen Zahlen* i, j, *definiere für sie eine Gleichheit*

$$(i, j) = (k, l) \qquad (i \equiv k \pmod{p^u},\ j \equiv l \pmod{p^v})$$

und das Produkt

$$(i, j)(k, l) = (i + k,\ j + l + p^{v-1} i l) \ . \tag{48}$$

Dritter Typ. *Bei gegebenen* p, u, v $(u \geqq v \geqq 1)$ *bilde man die Tripel* (i, j, m) *aller ganzen Zahlen* i, j, m, *definiere für sie eine Gleichheit*

$$(i, j, m) = (k, l, n) \qquad (i \equiv k \pmod{p^u},\ j \equiv l \pmod{p^v},\ m \equiv n \pmod{p})$$

und das Produkt

$$(i, j, m)\,(k, l, n) = (i + k,\ j + l,\ m + n + il) \ . \tag{49}$$

Vierter Typ. *Man bilde die Paare* (i, j) *aller ganzen Zahlen* i, j, *definiere für sie eine Gleichheit*

$$(i, j) = (k, l) \quad (i \equiv k,\ j \equiv l \pmod 4 \text{ oder } i \equiv k + 2,\ j \equiv l + 2 \pmod 4)$$

und das Produkt

$$(i, j)(k, l) = \left(i + k,\ j + (-1)^i l\right) \ . \tag{50}$$

Bezeichne nämlich Γ den Ring der ganzen Zahlen, $\Gamma(x)$ den Ring der Polynome von x über Γ, M den Modul der Elemente

$$q f(x) + \Psi(x) g(x) \qquad (f(x), g(x) \in \Gamma(x)) \ .$$

Bekanntlich ist dann $k(q^v)$ eben der Restklassenring von $\Gamma(x)$ nach M (das gälte auch für irgendein mod$q$ irreduzibles Polynom $\Psi(x)$ vom

Grade v). Wir zeigen weiter, daß die Restklasse $x \pmod M$ ein Element p-ter Ordnung in $k(q^v)^*$ ist. Da nämlich $\Psi(x)$ ein Faktor von $\frac{x^p-1}{x-1}$ mod q ist, so gilt

$$\frac{x^p-1}{x-1} \equiv 0 \ (\mathrm{mod}\, q\,,\ \Psi(x))\,,$$

d. h. $(\mathrm{mod}\, M)$. Also ist $x^p \equiv 1 \pmod M$, und somit kann die Ordnung der Restklasse $x \pmod M$ in $k(q^v)^*$ nur p oder 1 sein. Letzteres ist unmöglich, da dann $x \equiv 1 \ (\mathrm{mod}\, q, \Psi(x))$ also $\Psi(x) \equiv x-1 \pmod q$, und somit $\Psi(x)$ ein mehrfacher Faktor mod q von $x^p - 1$ wäre, wobei doch der Differentialquotient px^{p-1} den Faktor $x - 1 \bmod q$ nicht enthält. In der Tat ist die Restklasse $x \pmod M$ von der Ordnung p, und somit ein Basiselement für die Untergruppe p-ter Ordnung von $k(q^v)^*$. Repräsentiert man also $k(q^v)$ — wie gesagt — durch den Restklassenring von $\Gamma(x)$ nach M, so kann man in (44) die Restklasse $x \pmod M$ für r einsetzen. Offenbar darf in (44) auch jedes ϱ^n durch n ersetzt werden, und so entsteht die Produktregel (47), wie behauptet wurde.

Es ist klar, daß auch (48), (49) bloß andere Formen von (45), (46) sind.

Es bleibt nur noch übrig, (50) zu beweisen. Die Quaternionengruppe wird durch zwei Elemente 4-ter Ordnung A, B erzeugt, für die außer $A^4 = B^4 = 1$ noch $A^2 = B^2$ und $B^{-1}AB = A^{-1}$ ist. Man sieht leicht, daß allgemein

$$A^jB^i \cdot A^lB^k = A^{j+(-1)^{il}}B^{i+k}$$

gilt. Diese Produktregel stimmt im wesentlichen mit (50) überein, womit Satz 6 bewiesen wurde.

§ 8. Die vierte Darstellung der Gruppen 1-ter Stufe

Satz 7. *Die vier Typen (G_I, G_{II}, G_{III} und die Quaternionengruppe) der Gruppen 1-ter Stufe lassen sich als „abstrakte" Gruppen durch folgende Gleichungen definieren:*

Erster Typ.

$$\left.\begin{aligned} &A^{p^u} = B_0^q = B_1^q = \cdots = B_{v-1}^q = 1\,,\ B_r B_s = B_s B_r \ (0 \leqq r < s \leqq v-1)\,, \\ &A^{-1}B_r A = B_{r+1} \qquad\qquad (r = 0, \ldots, v-2)\,, \\ &A^{-1}B_{v-1}A = B_0^{c_0} \ldots B_{v-1}^{c_{v-1}}\,, \end{aligned}\right\} \quad (51)$$

wobei p, q, u $(u \geqq 1)$ gegeben sind, $v = O\,(q \pmod p)$ ist und die c_r die

Koeffizienten eines (irreduziblen) Faktors $x^v - c_{v-1}x^{v-1} - \cdots - c_0$ *von* $\frac{x^p-1}{x-1} \bmod q$ *liefern. (Es ist gleichgültig, welcher dieser Faktoren gewählt wird.)*

Zweiter Typ.

$$A^{p^u} = B^{p^v} = 1\ , \qquad A^{-1}BA = B^{1+p^{v-1}}\ , \tag{52}$$

wobei p, u, v $(u \geqq 1, v \geqq 2)$ *gegeben sind.*

Dritter Typ.

$$A^{p^u} = B^{p^v} = C^p = 1,\ AC = CA,\ BC = CB,\ A^{-1}BA = BC, \tag{53}$$

wobei p, u, v $(u \geqq v \geqq 1)$ *gegeben sind.*

Vierter Typ.

$$A^4 = 1, \quad A^2 = B^2, \quad A^{-1}BA = B^{-1}\ . \tag{54}$$

Wir beweisen diesen Satz mit Hilfe des Satzes 6.

Für den ersten Typ sind nach Satz 6 die $(-1, 0)$, $(0, x^r)$ $(r = 0, \ldots, v-1)$ offenbar erzeugende Elemente der Gruppe G_I. Nach (47) gilt

$$O\big((-1,0)\big) = p^u, \quad O\big((0,x^r)\big) = q, \quad (0,x^r)(0,x^s) = (0,x^s)(0,x^r)\ ,$$

weiter gilt $(-1,0)(1,0) = (0,0)$, d. h. $(-1,0)^{-1} = (1,0)$ und somit

$$(-1,0)^{-1}(0,x^r)(-1,0) = (1,0)(-1,x^r) = (0,x^{r+1})\ ,$$

insbesondere also mit der Bezeichnung $\Psi(x) = x^v - c_{v-1}x^{v-1} - \cdots - c_0$

$$(-1,0)^{-1}(0,x^{v-1})(-1,0) = (0,x^v) = \big(0, x^v - \Psi(x)\big) =$$
$$= (0, c_{v-1}x^{v-1} + \cdots + c_0) = (0,1)^{c_0} \ldots (0,x^{v-1})^{c_{v-1}}\ .$$

Mit der Bezeichnung $A = (-1,0)$, $B_r = (0,x^r)$ entstehen aus allen diesen eben die Gleichungen (51).

Für den zweiten Typ sind nach Satz 6 die $(-1,0)$, $(0,1)$ erzeugende Elemente der Gruppe G_{II}. Nach (48) gilt

$$O\big((-1,0)\big) = p^u\ , \qquad O\big((0,1)\big) = p^v\ ,$$

weiter gilt $(-1,0)(1,0) = (0,0)$, d. h. $(-1,0)^{-1} = (1,0)^{-1}$ und somit

$$(-1,0)^{-1}(0,1)(-1,0) = (1,0)(-1,1) = (0,p^{v-1}) = (0,1)^{p^{v-1}} .$$

Mit der Bezeichnung $A = (-1,0)$, $B = (0,1)$ entstehen hieraus die Gleichungen (52).

Für den dritten Typ sind nach Satz 6 die $(-1,0,0)$, $(0,1,0)$, $(0,0,1)$ erzeugende Elemente der Gruppe G_{III}. Nach (49) gilt

$$O\big((-1,0,0)\big) = p^u,\quad O\big((0,1,0)\big) = p^v,\quad O\big((0,0,1)\big) = p ,$$
$$(-1,0,0)(0,0,1) = (0,0,1)(-1,0,0) ,$$
$$(0,1,0)(0,0,1) = (0,0,1)(0,1,0) ,$$

weiter gilt $(-1,0,0)(1,0,0) = (0,0,0)$, d. h. $(-1,0,0)^{-1} = (1,0,0)$ und somit

$$(-1,0,0)^{-1}(0,1,0)(-1,0,0) = (1,0,0)\ (-1,1,0) =$$
$$= (0,1,1) = (0,1,0)(0,0,1) .$$

Mit der Bezeichnung $A = (-1,0,0)$, $B = (0,1,0)$, $C = (0,0,1)$ entstehen hieraus die Gleichungen (53).

In diesen drei Fällen reichen die Gleichungen (51), (52), (53) augenscheinlich auch aus, um die betreffenden Gruppen zu definieren.

Für den vierten Typ haben wir schon erwähnt, daß (54) die Quaternionengruppe definiert. Satz 7 ist richtig.

Bemerkungen. Ohne Zweifel spiegelt Satz 4 die wahre Natur der Gruppen 1-ter Stufe am klarsten, wogegen die „expliziten" Darstellungen in den Sätzen 5, 6, 7 natürlich auch ihren Vorteil haben. Insbesondere ist die „abstrakte" Form von G_I im Satz 7 den übrigen Darstellungen gegenüber sehr kompliziert, von der unmittelbar nicht mehr abzulesen ist, daß es sich in der Wirklichkeit um ein schiefes Produkt handelt. Eben darin erblicken wir die Brauchbarkeit des „schiefen Produktes", daß man mit seiner Hilfe z. B. das Gleichungssystem (51) in der einzigen Gleichung (3) zusammenfassen kann. *Miller* und *Moreno*[1]) und auch *Schmidt*[2]) haben die G_I in der Form (51) angegeben, haben aber die Exponenten $c_0, \ldots, c_{v-1}$ nicht bestimmt.

§ 9. Die Auflösbarkeit der Gruppen 1-ter Stufe

Von nun an bezeichne G_1 eine beliebige Gruppe 1-ter Stufe. Im vorliegenden und in den folgenden §§ 10, 11 bringen wir den Beweis des Satzes 4 zum Schluß, indem wir zeigen, daß alle G_1 unter den im Satz 4

angeführten Gruppen wirklich vorkommen und letztere verschieden sind. Als ersten Schritt beweisen wir hier, daß jedes G_1 auflösbar ist.

Hierzu zeigen wir zuerst, daß G_1 nicht einfach ist. Bezeichne H eine maximale Untergruppe[6]) und A ein Element von G_1 außerhalb H. Da $O(G_1)$ weder 1 noch eine Primzahl ist, existiert H (und mit ihm auch A), und es ist $O(H)>1$. Ist $A^{-1}HA = H$, so ist H normal, und dann sind wir fertig. Es sei deshalb $A^{-1}HA \neq H$; bezeichne D den Durchschnitt beider Gruppen. Da diese kommutativ sind und G_1 erzeugen, so ist D eine normale Untergruppe von ihnen, also auch von G_1. Im Falle $O(D)>1$ sind wir fertig. Es steht also nur noch der Fall aus, daß H mit keinem Element außerhalb H vertauschbar ist und mit keiner Konjugierten ein Element außer 1 (dem Einselement) gemein hat. Nach *Frobenius*[7]) bilden dann die Elemente von G_1 außerhalb von H und seiner Konjugierten mit 1 zusammen eine (echte) normale Untergruppe von G_1. Wir haben bewiesen, daß G_1 nicht einfach ist.

Bezeichne N eine echte normale Untergruppe von G_1 von maximaler Ordnung. Dann ist G_1/N einfach und somit nicht von der 1-ten Stufe. Von höherer Stufe kann G_1/N auch nicht sein, denn dann hätte es und mit ihm auch G_1 eine nichtkommutative Untergruppe, das unmöglich ist. Folglich ist G_1/N kommutativ und einfach, also von Primzahlordnung. Andererseits ist N kommutativ, also auflösbar. Beide ergeben die Richtigkeit der Behauptung, daß G_1 auflösbar ist.

§ 10. Die Gruppen 1-ter Stufe, die keine p-Gruppen sind

Vorläufig betrachten wir eine beliebige Gruppe G_1 von der 1-ten Stufe. Das Zentrum und die Kommutatorgruppe bezeichnen wir mit Z bzw. K. Sind A, B irgendwelche nichtvertauschbare Elemente von G_1, so ist offenbar $G_1 = \{A, B\}$[8]). Setzen wir

$$C = B^{-1}A^{-1}BA \ . \tag{55}$$

Offenbar ist dann und nur dann $AC = CA$, $BC = CB$, wenn $C \in Z$ ist. Ist dies der Fall, so folgt aus (55) $BC = A^{-1}BA$, $B^jC^j = A^{-1}B^jA$, $B^jC^{kj} = A^{-k}B^jA^k$. Hieraus sieht man folgendes ein:

---

[6]) Maximal nennen wir eine Untergruppe $\mathfrak{U}$ von einer Gruppe $\mathfrak{G}$, wenn $\mathfrak{U} \neq \mathfrak{G}$ und es zwischen $\mathfrak{U}$ und $\mathfrak{G}$ keine weitere Gruppe gibt.

[7]) Siehe z. B. *A. Speiser*, Theorie der Gruppen von endlicher Ordnung, 3. Aufl., Berlin 1937, S. 202, Satz 180.

[8]) Wir verstehen darunter die Gruppe, die durch die eingeklammerten Elemente erzeugt wird.

Ist in (55) $C \in Z$, so ist

$$C^{jk} = B^{-k}A^{-j}B^kA^j \ , \tag{56}$$

also auch $\{C\} = K \subseteqq Z$.

Sind A, B wieder beliebige nichtvertauschbare Elemente von G_1, so kann man sie durch je eine passende Potenz ersetzen, so daß die Nichtvertauschbarkeit erhalten bleibt und dabei $O(A)$, $O(B)$ Potenzen von Primzahlen p, q sind, und auch $A^pB = BA^p$, $AB^q = B^qA$ gilt (hier brauchen p, q nicht verschieden zu sein).

Im vorliegenden Paragraphen wollen wir beweisen, daß jede Gruppe G_1, die keine p-Gruppe (d. h. $O(G_1)$ keine Primzahlpotenz) ist, im Satz 4 genau einmal vorkommt.

Wir betrachten eine solche Gruppe G_1 und zeigen zuerst, daß K keine Untergruppe von Z ist. Wenn nämlich $K \subseteqq Z$ ist, so wählen wir ein Elementenpaar A, B wie eben vordem. Für C in (55) gilt dann $C \in K$, also $C \in Z$, und so ist jetzt (56) in Geltung. Dies ergibt wegen $A^pB = BA^p$, $AB^q = B^qA$ offenbar $C^p = C^q = 1$, woraus $O(C) = p = q$ folgt. Da $O(A)$, $O(B)$, $O(C)$ alle die Potenzen derselben Primzahl p sind, ist G_1 wegen $C \in K$ und (56) eine p-Gruppe. Dieser Widerspruch beweist die Behauptung.

Nunmehr bezeichne N eine normale Untergruppe von G_1 von einem Primzahlindex p, die wegen der Auflösbarkeit von G_1 sicher existiert. Bezeichne A ein Element von G_1 außerhalb N und von Primzahlpotenzordnung. Da $A^p \in N$ ist, muß

$$O(A) = p^u \qquad (u \geqq 1) \tag{57}$$

sein. Da weiter N kommutativ und $G = \{N, A\}$ ist, muß N ein mit A nicht vertauschbares Element B haben. Dabei sei B von minimaler Ordnung, woraus gleich folgt, daß $O(B)$ die Potenz einer Primzahl q ist (von der wir erst später beweisen, daß sie $\neq p$ ist). Wir zeigen, daß

$$O(B) = q \tag{58}$$

ist. Hierzu nehmen wir C in (55) zu Hilfe. Da $B \in N$ und N normal ist, ist auch $C \in N$. Andererseits ist N kommutativ, und so ist wegen $BC = A^{-1}BA$ offenbar $B^qC^q = A^{-1}B^qA$. Wegen der Minimaleigenschaft von B ist $AB^q = B^qA$, und so folgt $C^q = 1$, $O(C) = q$. Endlich kann C mit A nicht vertauschbar sein, denn dann folgte nach dem Schluß bei (56), daß $K \subseteqq Z$ ist, und wir haben doch bewiesen, daß das nicht gilt. Nach diesem hat C alle Eigenschaften, die wir von B verlangt haben,

darunter auch $(q =) O(C) \leqq O(B)$, und so muß hier wegen der Minimaleigenschaft von B das Zeichen „=“ gelten. Damit haben wir (58) bewiesen.

Wir setzen

$$B_i = A^{-i} B A^i \qquad (i = 0, 1, \ldots) \; . \tag{59}$$

Es ist $B_i \in N$, insbesondere $B_0 = B$. Nach (58) ist

$$O(B_i) = q \qquad (i = 0, 1, \ldots) \; . \tag{60}$$

Aus (59) folgt

$$B_{i+j} = A^{-i} B_j A^i \qquad (i, j = 0, 1, \ldots) \; . \tag{61}$$

Wegen $A^p \in N$ ergibt sich hieraus

$$B_i = B_j \qquad \left(i \equiv j \pmod p\right) \; . \tag{62}$$

Alle B_i erzeugen eine Untergruppe N_0 von N. Wir wählen B so, daß das kleinste v mit

$$N_0 = \{B_0, \ldots, B_{v-1}\} \tag{63}$$

möglichst klein ausfällt. Wegen (40) ist sicher

$$1 \leqq v \leqq p \; , \tag{64}$$

weiter muß $B_v \in N_0$, d. h. eine Gleichung

$$B_v B_{v-1}^{c_{v-1}} \ldots B_0^{c_0} = 1 \tag{65}$$

gelten.

Die $B_0, \ldots, B_{v-1}$ müssen unabhängig sein, denn sonst wäre für ein $v' (< v)$ $B_{v'} \in N_0'$, wobei $N_0' = \{B_0, \ldots, B_{v'-1}\}$ ist. Hieraus folgt nach (61) $B_{v'+1} \in \{B_1, \ldots, B_{v'}\}$, also $B_{v'+1} \in N_0'$, und mit wiederholtem Schluß $B_{v'}, B_{v'+1}, B_{v'+2}, \ldots \in N_0'$, d. h. $N_0' = N_0$. Dies widerspricht der Minimaleigenschaft von v, womit die Behauptung bewiesen ist.

Hieraus folgt nach (63)

$$O(N_0) = q^v \; . \tag{66}$$

Dabei ist N_0 ein $G(q, \ldots, q)$ (die Anzahl dieser q ist v).

Im folgenden verwenden wir Polynome $f(x), \Psi(x), \ldots$ der Unbestimmten x mit ganzen Koeffizienten, die wir aber als Elemente des Primkörpers $k(q)$ auffassen, so daß also $0, 1, 2, \ldots, q - 1$ alle verschiedenen

Elemente und zwei ganze Zahlen i, j mit $i \equiv j \pmod q$ gleiche Elemente von $k(q)$ bezeichnen. Nach dieser Vereinbarung sind $f(x), \Psi(x), \ldots$ Polynome über $k(q)$.

Ist nun

$$f(x) = a_n x^n + \cdots + a_0$$

irgendein solches Polynom, so setzen wir

$$(f(x)) = B_n^{a_n} \ldots B_0^{a_0} \ .$$

Hierdurch haben wir jedem $f(x)$ ein Element der Gruppe N_0 zugeordnet, und diese Zuordnung ist eindeutig, denn zu gleichen Polynomen gehört nach (60) dasselbe Element von N_0. Umgekehrt ist klar, daß jedes Element von N_0 (sogar mehrmals) unter den $(f(x))$ vorkommt.

Insbesondere setzen wir

$$\Psi(x) = x^v + c_{v-1} x^{v-1} + \cdots + c_0 \ . \tag{67}$$

Nach (65) gilt

$$(\Psi(x)) = 1 \ . \tag{68}$$

Weiter ist nach (62) $B_p B_0^{-1} = 1$, also

$$(x^p - 1) = 1 \ . \tag{69}$$

Wegen der Kommutativität von N_0 ist

$$(f(x) + g(x)) = (f(x))(g(x)) \ . \tag{70}$$

Offenbar gelten noch

$$(0) = 1 \ , \qquad (-f(x)) = (f(x))^{-1} \tag{71}$$

und allgemeiner

$$(c\, f(x)) = (f(x))^c \qquad (c = 0, \pm 1, \ldots) \ , \tag{72}$$

die sich auch aus (70) ableiten lassen. Endlich ergibt (61) leicht

$$A^{-i}(f(x))\ A^i = (x^i f(x)) \qquad (i = 0, 1, \ldots) \ , \tag{73}$$

und so gilt nach (71) auch

$$(f(x))^{-1} A^{-i} (f(x)) A^i = ((x^i - 1) f(x)) \qquad (i = 0, 1, \ldots) \ , \tag{74}$$

insbesondere

$$(f(x))^{-1} A^{-1} (f(x)) A = ((x - 1) f(x)) \ . \tag{75}$$

Aus (68), (73) folgt $(x^i\Psi(x)) = 1$, und weiter hieraus nach (72) und (70)

$$(f(x)\Psi(x)) = 1 \ . \tag{76}$$

Andererseits folgt aus der Unabhängigkeit der $B_0, \ldots, B_{v-1}$, daß die Polynome $f(x)$ vom Grade $\leqq v-1$ lauter verschiedene $(f(x))$ darstellen. Also ist dann und nur dann $(f(x)) = (g(x))$, wenn

$$f(x) \equiv g(x) \qquad (\mathrm{mod}\ \Psi(x)) \ . \tag{77}$$

Wir beweisen

$$\Psi(x) \neq (x-1)^v \ . \tag{78}$$

Nehmen wir hierzu $\Psi(x) = (x-1)^v$ an. Für ein beliebiges Element $D = D_0$ in N_0 setzen wir $D_{i+1} = D_i^{-1}A^{-1}D_iA$ $(i = 0, 1, \ldots)$. Allgemein ist D_i mit A dann und nur dann vertauschbar, wenn $D_{i+1} = 1$ ist, weiter sind alle D_i in N_0, also miteinander vertauschbar. Wir betrachten zuerst den Fall $v \geqq 2$ und setzen insbesondere $D_0 = ((x-1)^{v-2})$. Nach (75) ist dann $D_1 = ((x-1)^{v-1}) \neq 1$, $D_2 = ((x-1)^v) = 1$. Nach der vorausgeschickten Bemerkung und dem Schluß bei (56) (angewendet auf den Fall $B = D_0$, $C = D_1$) folgt, daß $(G = \{A, D_0\}, \{D_1\} =) K \subseteqq Z$ ist. Da dies aber nicht gilt, ist (78) für $v \geqq 2$ bewiesen. Im übriggebliebenen Fall $v = 1$ setzen wir $D_0 = (1) = B_0$. Nach (75) ist dann $D_1 = (x-1) = 1$, d. h. $B_0 (= B)$ mit A vertauschbar. Da dies falsch ist, so ist (78) in allen Fällen richtig.

Nach (69), (71) ist $(x^p - 1) = (0) (= 1)$. Hieraus folgt nach (77)

$$\Psi(x) \mid x^p - 1 \ . \tag{79}$$

Dies ergibt vor allem

$$p \neq q \ . \tag{80}$$

Denn im Fall $p = q$ wäre (79) nichts anderes als $\Psi(x) \mid (x-1)^q$, und das ist ein Widerspruch mit (78).

Nunmehr zeigen wir, daß $\Psi(x)$ irreduzibel ist. Sonst gibt es nämlich nach (78) eine Zerlegung

$$\Psi(x) = \Psi'(x)\, f(x) \qquad (x - 1 \nmid \Psi'(x)) \ ,$$

wobei rechts die Faktoren nichtkonstant sind und den Leitkoeffizienten 1 haben. Dann ist $\Psi(x) \nmid (x-1)\, f(x)$, und das bedeutet nach (75), daß

das Element $B' = (f(x))$ mit A nicht vertauschbar ist. Dabei ist $(B' \in N_0)$ $O(B') = q$. Setzen wir andererseits

$$\Psi'(x) = x^{v'} + c'_{v'-1}x^{v'-1} + \cdots + c'_0 ,$$
$$B'_i = A^{-i}B'A^i = (x^i f(x)) \qquad (i = 0, 1, \ldots)$$

und berechnen nach (72) und (70):

$$B'_{v'} B'^{c'_{v'-1}}_{v'-1} \ldots B'^{c'_0}_0 = (x^{v'} f(x))\,(x^{v'-1} f(x))^{c'_{v'-1}} \ldots (f(x))^{c'_0} =$$
$$= (\Psi'(x) f(x)) = (\Psi(x)) = 1 .$$

Da aber offenbar $v' < v$ und sonst B' ein mit B gleichberechtigtes Element ist, so sind wir mit der Minimaleigenschaft von v zu einem Widerspruch gekommen. Dies beweist die Irreduzibilität von $\Psi(x)$.

Hieraus und aus (78), (79) folgt sogleich auch

$$\Psi(x) \Big| \frac{x^p - 1}{x - 1} . \tag{81}$$

Wie schon erwähnt, sind wegen (80) alle irreduziblen Faktoren der rechten Seite von (81) vom Grade

$$v = O\,(q (\mathrm{mod}\ p)) . \tag{82}$$

Da $G_1 = \{A, B\} = \{A, N_0\}$ ist, und N_0 aus allen Elementen $(f(x))$ besteht, so folgt aus (73), daß sich alle Elemente von G_1 in der Form $A^i(f(x))$ schreiben lassen. Wegen (57) und (77) genügt es, wenn man i auf $0, \ldots, p^u - 1$ und $f(x)$ auf die Polynome vom Grade $\leqq v - 1$ beschränkt. Die verbliebenen $p^u q^v$ Elemente $A^i(f(x))$ müssen auch schon alle verschiedenen Elemente von G_1 sein, denn G_1 enthält die Untergruppen $\{A\}$, N_0 von der Ordnung p^u bzw. q^v, muß also wenigstens $p^u q^v$ Elemente enthalten.

Aus (73) folgt, daß in G_1 die Produktregel

$$A^i(f(x)) \cdot A^j(g(x)) = A^{i+j}(x^j f(x) + g(x)) \tag{83}$$

gilt. Wir schreiben jetzt $(i, f(x))$ für $A^i(f(x))$. Die Bedingung (77) ist dann für diese neue Schreibweise äquivalent mit folgender „Gleichheitsdefinition“:

$$(i, f(x)) = (j, g(x)) \quad (i \equiv j (\mathrm{mod}\ p^u), f(x) \equiv g(x) (\mathrm{mod}\ q, \Psi(x))) . \tag{84}$$

Dabei haben wir nämlich berücksichtigt, daß $f(x)$, $g(x)$, $\Psi(x)$ in (77) Polynome mit ganzen Koeffizienten sind, die man als Elemente in $k(q)$ aufzufassen hat. Das kommt aber auf dasselbe hinaus, daß man die ganzzahligen Polynome einfach mod q betrachtet, und so ließ sich (77) mit $f(x) \equiv g(x) \pmod{q, \Psi(x)}$ ersetzen. Selbst (83) schreibt sich jetzt so

$$(i, f(x))\,(j, g(x)) = (i + j,\ x^j g(x) + f(x)) \ .$$

Bekanntlich geht jede Gruppe in eine gleiche Gruppe über, wenn man in ihr die „transponierte" Multiplikation $a \circ b = ba$ statt ab anwendet. Dann gilt

$$(i, f(x)) \circ (j, g(x)) = (j, g(x))\,(i, f(x)) = (j + i,\ x^i g(x) + f(x)) = \\ = (i + j,\ f(x) + x^i g(x)) \ .$$

Dies ist nichts anderes als (47). Mit Rücksicht auf (84), (82), (81) und auf die Irreduzibilität von $\Psi(x)$ haben wir bewiesen, daß jede Gruppe G_1 von der 1-ten Stufe, die keine p-Gruppe ist, unter den Gruppen G_I (des Satzes 6, also auch) des Satzes 4 wirklich vorkommt.

Daß nun diese Gruppen G_I auch wirklich verschieden sind, ergibt sich sehr leicht. Wir haben nämlich schon im § 5 bei (35) bewiesen, daß $G_I = G_I(p, q, u)$ nur von p, q, u abhängt (d. h. von der Homomorphie $\overline{\alpha}$ unabhängig ist). Hieraus folgt nach (28), daß im Satz 4 zu einer Ordnung $p^u q^v$ $(u, v \geqq 1)$ nur dann zwei Gruppen angegeben werden, wenn gegenseitig $v = O\ (q \pmod p)$, $u = O\ (p \pmod q)$ ist. Es kann nicht $u = v = 1$ sein, und so dürfen wir $u > 1$ annehmen. Die erste der entsprechenden zwei Gruppen $G_I(p, q, u)$, $G_I(q, p, v)$ enthält nach (57) eine Sylow-Gruppe $G(p^u)$ und eine Sylow-Gruppe von der Form $G(q, \ldots, q)$ und der Ordnung q^v. Entsprechend enthält $G_I(q, p, v)$ eine Sylow-Gruppe $G(p, \ldots, p)$. Da wegen $u > 1$ $G(p^u)$ und $G(p, \ldots, p)$ sicher verschieden und andererseits die zur selben Ordnung gehörenden Sylow-Gruppen einer Gruppe konjugiert sind, ist klar, daß die Gruppen $G_I(p, q, u)$, $G_I(q, p, v)$ verschieden sind.

§ 11. Die p-Gruppen 1-ter Stufe

Wir betrachten jetzt den noch übriggebliebenen Fall, in dem die angegebene Gruppe G_1 von der 1-ten Stufe zugleich eine p-Gruppe ist, um zu zeigen, daß G_1 auch dann unter den Gruppen des Satzes 4 genau einmal vorkommt (mit der genannten Ausnahme $G_{II}(2,1,2) = G_{III}(2,1,1)$).

Zuerst zeigen wir, daß

$$K \subseteqq Z \tag{85}$$

ist. Da G_1 eine nichtzyklische p-Gruppe ist, so enthält sie zwei verschiedene normale Untergruppen N_1, N_2 vom Index p[9]). Die Faktorgruppen G_1/N_i $(i = 1, 2)$ sind kommutativ, und hieraus folgt $K \subseteqq N_1, N_2$, also $K \subseteqq N$, wobei N den Durchschnitt von N_1 und N_2 bezeichnet. Andererseits ist $G_1 = \{N_1, N_2\}$, woraus wegen der Kommutativität von N_1, N_2 folgt, daß die Elemente von N mit allen Elementen von G_1 vertauschbar sind, d. h. $N \subseteqq Z$ ist. Mit dem vorigen zusammen ergibt das den Beweis von (85).

Sind A, B irgend zwei nichtvertauschbare Elemente von G_1, und wird

$$C = B^{-1}A^{-1}BA \tag{86}$$

gesetzt, so gilt wegen (85) $C \in Z$, und dies hat nach (56) zur Folge, daß

$$B^j A^k = A^k B^j C^{jk} \tag{87}$$

und

$$K = \{C\} \tag{88}$$

ist. Zugleich folgt aus $G_1 = \{A, B\}$, daß sich alle Elemente von G_1 in der Form $A^i B^j C^m$ schreiben lassen, und nach (87) gilt

$$A^i B^j C^m \cdot A^k B^l C^n = A^{i+k} B^{j+l} C^{m+n+jk} \ . \tag{89}$$

Durch vollständige Induktion folgt hieraus noch

$$(A^i B^j C^m)^n = A^{ni} B^{nj} C^{nm + \binom{n}{2} ij} \tag{90}$$

zunächst für $n \geqq 0$, dann aber auch für jedes n. Wir setzen

$$O(A) = p^u, \quad O(B) = p^v \qquad (u, v \geqq 1) \tag{91}$$

und wählen A, B fest so, daß $O(A)O(B)$, d. h. auch $u + v$ minimal ausfällt. Dann ist $A^p B = BA^p$, und so ist nach (87) $C^p = 1$, also

$$O(C) = p \ . \tag{92}$$

Jetzt schließen wir den Fall aus, daß G_1 die Quaternionengruppe ist. Dann zeigen wir, daß $\{A\}$, $\{B\}$ nach geeigneter Wahl von A, B kein gemeinsames Element außer 1 haben. Sonst besteht nämlich eine Gleichung

$$A^{p^{u'}} = B^{p^{v'} z} \qquad (0 < u' < u\,;\ 0 < v' < v\,;\ p \nmid z) \ . \tag{93}$$

---

[9]) Siehe z. B. *A. Speiser*, l. c. S. 70, Satz 84.

Aus Symmetriegründen dürfen wir $u' \leqq v'$ annehmen. Wir setzen

$$A' = AB^{-p^{v'-u'}z} . \tag{94}$$

Nach (90), (93) ist dann

$$A'^{p^{u'}} = C^{-\binom{p^{u'}}{2} p^{v'-u'} z} . \tag{95}$$

Wegen (94) sind A', B nicht vertauschbar, und so folgt aus der Minimaleigenschaft von $u + v$, daß

$$O(A') \geqq O(A) \tag{96}$$

ist. Dies ergibt wegen $u' < u$ und (91) $O(A') > p^{u'}$, also ist die rechte Seite von (95) $\neq 1$ und wegen (92) der Exponent von C nicht durch p teilbar.

Hieraus folgt

$$p = 2, \quad u' = v' = 1 , \tag{97}$$

und wegen (92) auch

$$A'^2 = C , \tag{98}$$

$A'^4 = 1$, $O(A') = 4$. Nach (96) ist also $O(A) \leqq 4$. Andererseits ist wegen (93) $u \geqq 2$, d. h. wegen (91) $O(A) \geqq 4$, und so muß $O(A) = 4$ sein. Nach (97), (93) ist dann $A^2 = B^2$, $O(B) = 4$. Wenn also unsere Behauptung falsch ist, so müssen irgend zwei nichtvertauschbare Elemente 4-ter Ordnung von G_1 gleiches Quadrat haben. Da auch A', B ein solches Paar ist, so folgt aus (98) $B^2 = C$, also nach (86) $B^2 = B^{-1}A^{-1}BA$, $A^{-1}BA = B^{-1}$. Wir erkennen, daß $G_1 = \{A, B\}$ die Quaternionengruppe ist, da wir aber diesen Fall ausgeschlossen haben, so ist die Behauptung richtig.

Hieraus folgt nach (91), daß alle $A^i B^j$ ($i = 0, \ldots, p^u - 1$; $j = 0, \ldots, p^v - 1$) verschieden sind. Andererseits — wenn man hierzu auch (92) berücksichtigt — lassen sich nach obiger Bemerkung alle Elemente von G_1 in der Form

$$A^i B^j C^m \ (i = 0, \ldots, p^u - 1 ; j = 0, \ldots, p^v - 1 ; m = 0, \ldots, p - 1) \tag{99}$$

schreiben. Folglich ist

$$O(G_1) = p^{u+v} \quad \text{oder} \quad p^{u+v+1} , \tag{100}$$

je nachdem es unter den Elementen (99) auch gleiche gibt oder sie alle verschieden sind. Wir betrachten beide Fälle gesondert.

Im ersten Fall liefert (100) mit $m = 0$ schon alle verschiedenen Ele-

mente von G_1, also muß C von der Form A^iB^j sein. Wegen $C \in Z$ muß hier $p \mid i,j$ sein, und wegen (91), (92) sogar $p^{u-1} \mid i, p^{v-1} \mid j$ gelten. Wir setzen

$$C = A^{p^{u-1}x} B^{p^{v-1}y} \qquad (p \mid p^{u-1}x, p^{v-1}y) \tag{101}$$

und zeigen, daß man durch passende Wahl von A, B erreichen kann, daß $p \mid x$ oder $p \mid y$ ist, d. h. C in $\{A\}$ oder $\{B\}$ gehört.

Ist nämlich $p \nmid x,y$, so muß vor allem $u, v \geqq 2$ sein. Wegen Symmetriegründe dürfen wir $u \geqq v (\geqq 2)$ annehmen. Bestimmen wir z aus

$$yz \equiv x \pmod{p} \tag{102}$$

und setzen

$$B' = A^{p^{u-v}z} B \ . \tag{103}$$

Da A, B' nichtvertauschbar sind, muß $O(B') \geqq O(B)$ sein. Andererseits ist nach (90), (91) und (103) wegen $v \geqq 2$, $B'^{p^v} = 1$, d. h. $O(B') \leqq p^v = O(B)$. Folglich ist $O(B') = O(B)$, und da A, B' nichtvertauschbar sind, so dürfen wir von vornherein B' statt B nehmen. Dabei bleibt C nach (86), (103) ungeändert. Nach (90), (103), (102) und (101) ist

$$B'^{p^{v-1}y} = C C^{\binom{p^{v-1}y}{2} p^{u-v} z} \ .$$

Ist der zweite Faktor rechts gleich 1, so ist die Behauptung richtig. Im übriggebliebenen Fall muß wegen (92) $p = 2$, $u = v = 2$ sein. Dann ist $O(A) = O(B) = 4$ und nach (101) $C = A^2B^2 = B^2A^2$, also nach (86) $B^{-1}A^{-1}BA = B^2A^2$, $A^{-1}B = B^3A$. Dies ergibt

$$(A^{-1}B)^2 = A^{-1}B \cdot B^3A = 1 \ .$$

Wir haben ein mit A nichtvertauschbares Element $A^{-1}B$ von 2-ter Ordnung gefunden. Dieser Widerspruch beweist die Behauptung.

Da nach (88) $\{C\}$ nur von G_1 abhängt, so können wir nach Vertauschung von A, B erreichen, daß eben $C \in \{B\}$ ist. Ersetzen wir dann A durch eine passende Potenz von ihm, so wird $C = B^{p^{v-1}}$, und nach (86)

$$A^{-1}BA = B^{1+p^{v-1}} \ .$$

Zugleich muß $v \geqq 2$ sein, und so haben wir für diesen Fall gefunden, daß G_1 die durch (52) definierte Gruppe ist.

Im übriggebliebenen zweiten Fall von (100) ist C nicht von der Form A^iB^j. Das bleibt auch dann erhalten, wenn A, B vertauscht werden,

denn sonst müßte wieder der vorige Fall entstehen, was unmöglich ist. Durch diese Vertauschung können wir immer $u \geqq v$ erreichen. Wir haben gewonnen, daß G_1 im vorliegenden Fall eine durch (53) definierte Gruppe ist. Das hat den Beweis beendet, daß die Gruppen von den vier Typen im Satz 4 alle Gruppen 1-ter Stufe erschöpfen.

Jetzt endlich bringen wir den Beweis des Satzes 4 (mithin auch der Sätze 5, 6, 7) zum Schluß, indem wir zeigen, daß auch die dort angegebenen p-Gruppen 1-ter Stufe verschieden sind, abgesehen von der genannten Ausnahme $G_{II}(2, 1, 2) = G_{III}(2, 1, 1)$.

Zuerst zeigen wir die Gleichheit dieser zwei Gruppen 8-ter Ordnung. Sie lassen sich bzw. durch

$$A^2 = B^4 = 1\,, \qquad BA = AB^3\,,$$
$$A^2 = B^2 = C^2 = 1\,, \quad AC = CA\,, \quad BC = CB\,, \quad BA = ABC$$

definieren. Setzen wir für die letztere Gruppe $B_1 = AB$. Dann ist $B_1^2 = = ABAB = C$, woraus folgt

$$B_1^4 = 1\,, \quad B_1 A = ABA = AABC = AB_1^3\,.$$

Diese zwei Gleichungen und $A^2 = 1$ beweisen, daß beide Gruppen gleich sind.

Im folgenden dürfen wir $G_{II}(2, 1, 2)$ ausschließen, und so beweisen wir, daß die übriggebliebenen Gruppen wirklich verschieden sind. Das zeigen wir vor allem für zwei Gruppen, die verschiedenen Typen angehören. Hierzu betrachten wir eine beliebige dieser Gruppen G_1 und bezeichnen mit P das Minimum des Produktes der Ordnungen zweier erzeugender (d. h. nichtvertauschbarer) Elemente. Aus (91), (100) und den darauffolgenden sehen wir, daß $P = O(G_1)$ oder $P < O(G_1)$ ist, je nachdem $G_1 = G_{II}$ oder $G_1 = G_{III}$; weiter ist $P > O(G_1)$, wenn G_1 die Quaternionengruppe ist (dann gilt nämlich $P = 16$, $O(G_1) = 8$). Das beweist unsere letzte Behauptung.

Wir müssen noch zeigen, daß alle Gruppen $G_{II}(p, u, v)$ und desgleichen auch alle Gruppen $G_{III}(p, u, v)$ untereinander verschieden sind. Nehmen wir zuerst $G_{II}(p, u, v) = G_{II}(p, u', v')$ an. Wegen der Gleichheit der Ordnungen muß vor allem $u + v = u' + v'$ sein. Wenn wir auch noch $v = v'$ zeigen, so sind wir mit dem Beweis für diesen Fall fertig. Hierzu nehmen wir für die Gruppe $G_{II}(p, u, v)$ wieder das Elementenpaar A, B in (91) zu Hilfe. Wie gezeigt worden ist, ist dann $K = \{B^{p^{v-1}}\}$. Andererseits sind die $A^i B^j$ alle Gruppenelemente. Die p^v-te

Potenz ist nach (90) wegen $v \geqq 2$ eine Potenz von A, also kein erzeugendes Element von K. Folglich ist v invariant durch $G_{II}(p, u, v)$ bestimmt, woraus $v = v'$ folgt, wie behauptet wurde.

Zweitens nehmen wir $G_{III}(p, u, v) = G_{III}(p, u', v')$ an. Wie eher folgt $u + v = u' + v'$. Andererseits ist p^u nach (90) wegen $u \geqq v \geqq 1$ das Maximum der Ordnungen der Elemente von $G_{III}(p, u, v)$, ausgenommen wenn $p = 2$, $u = 1$ ist. In diesem Ausnahmefall ist $u = v = u' = v' = 1$ unmittelbar klar, sonst aber folgt zuerst $p^u = p^{u'}$, $u = u'$, also auch $v = v'$. Dies beendet unseren Beweis.

§ 12. Weitere Eigenschaften der Gruppen 1-ter Stufe

Im folgenden Satz 8 stellen wir die strukturellen Eigenschaften der Gruppen 1-ter Stufe zusammen. Es wird am bequemsten, wenn wir dabei die Gruppen $G_I(p, q, u)$ in ihrer dritten Darstellung (Satz 6), die übrigen aber als abstrakte Gruppen (Satz 4) annehmen. Bei den Gruppen $G_{II}(p, u, v)$ vergrößern wir den Parameter v um 1, werden also $G_{II}(p, u, v + 1)$ betrachten. Dann wird diese Gruppe und die Gruppe $G_{III}(p, u, v)$ von gleicher Ordnung.

Außer den bisherigen Bezeichnungen Z (= Zentrum), K (= Kommutatorgruppe), $O(x)$ (= „Ordnung") bezeichne noch $\nu(x)$ die Anzahl der Konjugierten eines Gruppenelementes x, N eine echte normale Untergruppe, U eine maximale Untergruppe. Da in unserem Falle alle U kommutativ sind, werden durch die Angabe aller U auch schon sämtliche Untergruppen bekannt.

Satz 8. *Die Gruppen 1-ter Stufe (mit Ausnahme der Quaternionengruppe) sind die folgenden:*

Erster Typ. $G_I = G_I(p, q, u) (u \geqq 1)$. *Es ist* $O(G_I) = p^u q^v$ *mit* $v = O(q \pmod p)$. *Bezeichne* $\Psi(x)$ *einen (gleichgültig welchen) mod q irreduziblen Faktor von* $\dfrac{x^p - 1}{x - 1}$. *Die Elemente von* G_I *sind die Paare* $(i, f(x))$ *(i ganze Zahl, $f(x)$ Polynom mit ganzen Koeffizienten), wobei i und $f(x)$ nur mod p^u bzw. mod $(q, \Psi(x))$ zu berücksichtigen sind. Die Produktregel lautet:*

$$(i, f(x))\,(j, g(x)) = (i + j, f(x) + x^i g(x)) .$$

Es gilt

$$(i, f(x))^n = \left(ni, \frac{x^{ni} - 1}{x^i - 1} f(x)\right) \qquad (n \geqq 0) ,$$

insbesondere

$$(i, f(x))^p = \begin{cases} (pi, pf(x)) & (p \mid i) , \\ (pi, 0) & (p \nmid i) . \end{cases}$$

Für das Element $A = (i, f(x))$ *ist*

	$p \nmid i$	$i = p^{u'} i' \quad (u' > 0 ; p \nmid i')$	
		$f(x) \not\equiv 0 \pmod{q, \Psi(x)}$	$f(x) \equiv 0 \pmod{q, \Psi(x)}$
$O(A)$	p^u	$p^{u-u'} q$	$p^{u-u'}$
$v(A)$	q^v	p	1

Z und K bestehen aus den Elementen $(pi, 0)$ *bzw.* $(0, f(x))$, *sie haben nur das Einselement* $(0,0)$ *gemeinsam, es ist* $O(Z) = p^{u-1}$, $O(K) = q^v$.

Die Sylow-Gruppen sind K und die q^v *konjugierten zyklischen Gruppen* $\{(i, f(x))\}$ $(p \nmid i)$ *von der Ordnung* p^u. *Letztere enthalten Z.*

Die N sind alle Z' *und* KZ' $(Z' \subseteq Z)$.

Die U sind die zyklischen Sylow-Gruppen und ZK; letztere Gruppe hat die Ordnung $p^{u-1} q^v$ *und die Invarianten* $p^{u-1}, q, \ldots, q$.

Ein erzeugendes Elementenpaar ist $(1, 0)$, $(0, 1)$ *(die Ordnung ist* p^u *bzw.* q*), jedes weitere gleichberechtigte Paar ist* $(n, a(x))$, $(0, b(x))$, *wobei* $p \nmid n$, $b(x) \not\equiv 0 \pmod{q, \Psi(x)}$ *ist. Entsprechend sind alle Automorphismen:*

$$(i, f(x))' = \left(ni \, , \; a(x) \frac{x^{ni} - 1}{x^i - 1} + b(x) f(x^n) \right) .$$

Die Faktorgruppe G_I/Z *ist ein* $G_I(p, q, 1)$ *(ohne Zentrum).*

Zweiter Typ. $G_{II} = G_{II}(p, u, v+1)$ $(u, v \geqq 1)$. *Es ist* $O(G_{II}) = p^{u+v+1}$. *Als abstrakte Gruppe besteht* G_{II} *aus den Elementen* $A^i B^j$ *mit* $O(A) = p^u$, $O(B) = p^{v+1}$ *und der Produktregel*

$$A^i B^j \cdot A^k B^l = A^{i+k} B^{j+l+p^v jk} .$$

Es gilt

$$(A^i B^j)^n = A^{ni} B^{nj + p^v \binom{n}{2} ij}$$

und $O(A^i B^j)$ *ist das größere von* $O(A^i)$, $O(B^j)$.

Es ist $Z = \{A^p, B^p\}$, $K = \{B^{p^v}\}$ *mit* $O(Z) = p^{u+v-1}$, $O(K) = p$, $K \subseteq Z$. *Die Elemente außerhalb Z haben je p Konjugierte.*

Die U sind die Gruppen zwischen Z und G_{II}, *d. h.* $\{AB^i, B^p\}$ $(i = 0, \ldots, p-1)$ *und* $\{A^p, B\}$. *Es ist* $O(U) = p^{u+v}$ *und die Anzahl der U gleich* $p + 1$.

Die N sind die Z' ($\subseteq Z$) und die Untergruppen von U, die K enthalten. Insbesondere ist jedes U ein N.

Alle dem A, B gleichberechtigten (erzeugenden) Elementenpaare sind $A^\alpha B^\beta$, $A^\gamma B^\delta$ mit

$$\begin{aligned} &p \mid \alpha - 1, \quad p^{v+1} \mid p^u \beta, \quad p^u \mid p^{v+1}\gamma && (u \neq v+1), \\ &\delta \equiv \alpha\delta - \beta\gamma \not\equiv 0 \pmod{p} && (u = v+1) \end{aligned}$$

ausgenommen den folgenden Fall:

$$2 \nmid \alpha, \quad 2 \mid \gamma, \quad 2 \nmid \delta \qquad (u = v+1 = 2, \; p = 2).$$

Entsprechend sind alle Automorphismen:

$$(A^i B^j)' = A^{\alpha i + \gamma i} B^{\beta i + \delta j + p^v\left(\alpha\beta\binom{i}{2} + \gamma\delta\binom{j}{2} + \beta\gamma ij\right)}.$$

Dritter Typ. *$G_{III} = G_{III}(p, u, v)$ $(u \geqq v \geqq 1)$. Es ist $O(G_{III}) = p^{u+v+1}$. Als abstrakte Gruppe besteht G_{III} aus den Elementen $A^i B^j C^m$ mit $O(A) = p^u$, $O(B) = p^v$, $O(C) = p$ und der Produktregel*

$$A^i B^j C^m \cdot A^k B^l C^n = A^{i+k} B^{j+l} C^{m+n+jk}.$$

Es gilt

$$(A^i B^j C^m)^n = A^{ni} B^{nj} C^{nm + \binom{n}{2} ij}.$$

Wie auch schon im Satz 4 erwähnt, ist $G_{III}(2, 1, 1)$ gleich $G_{II}(2, 1, 2)$. Im folgenden schließen wir $G_{III}(2, 1, 1)$ aus.

$O(A^i B^j C^m)$ ist das größte von $O(A^i)$, $O(B^j)$, $O(C)$.

Es ist $Z = \{A^p, B^p, C\}$, $K = \{C\}$ mit $O(Z) = p^{u+v-1}$, $O(K) = p$, $K \subseteq Z$. Die Elemente außerhalb Z haben je p Konjugierte.

Die U sind die Gruppen zwischen Z und G_{III}, d. h. $\{AB^i, B^p, C\}$ $(i = 0, \ldots, p-1)$ und $\{A^p, B, C\}$. Es ist $O(U) = p^{u+v}$ und die Anzahl der U gleich $p + 1$.

Für die N gilt alles wörtlich wie im Fall G_{II}.

Die A, B sind Erzeugende. Alle gleichberechtigten Paare sind $A^\alpha B^\beta C^\mu$, $A^\gamma B^\delta C^\nu$ mit

$$\begin{aligned} &p \nmid \alpha, \quad p^{u-v} \mid \gamma, \quad p \mid \delta && (u > v), \\ &p \nmid \alpha\delta - \beta\gamma && (u = v). \end{aligned}$$

Entsprechend sind alle Automorphismen

$$(A^i\ B^j\ C^m)' = A^{\alpha i+\gamma j}\ B^{\beta i+\delta j}\ C^{(\alpha\delta-\beta\gamma)m+\alpha\beta\binom{i}{2}+\gamma\delta\binom{j}{2}+\beta\gamma ij}.$$

Dieser Satz ist teils eine Wiederholung voriger Tatsachen, teils eine Reihe einfacher rechnerischer Folgerungen, deren Beweis wir uns ersparen dürfen.

Bemerkung. Aus diesem Satz entnehmen wir, daß eine endliche kommutative Gruppe dann und nur dann in wenigstens einer Gruppe 1-ter Stufe enthalten ist, wenn sie ein $G(p^r)$, $G(p^r,p^s)$, $G(p^r,p^s,p)$, $G(p,p,\ldots,p)$ oder $G(p,p,\ldots,p,q^r)$ ist, wobei im letzteren die Anzahl der Invarianten p höchstens nur $O(p(\mathrm{mod}\,q))$ sein darf. Es ist auffallend, wie wenig Typen der (kommutativen) Gruppen durch die Gruppen 1-ter Stufe umfaßt werden.

Unter allen Gruppen 1-ter Stufe sind die $G_I(p,q,u)$ und vor allem insbesondere die $G_I(p,q,1)$ am interessantesten. Letztere Gruppe ist von der Ordnung pq^v mit $v = O(q(\mathrm{mod}\,p))$, alle Gruppenelemente $(\neq 1)$ sind von Primzahlordnung, irgend zwei Sylow-Gruppen sind gleich oder fremd, es gibt unter ihnen insgesamt q^v Gruppen $G(p)$ und eine Gruppe $G(q,\ldots,q)$ von der Ordnung q^v.

Wir haben gesehen, daß allgemein die $G_I = G_I(p,q,v)$ im engsten Zusammenhang mit den endlichen Körpern stehen. In ähnlich starker Beziehung sind die p-Gruppen 1-ter Stufe und bekanntlich auch die endlichen kommutativen Gruppen mit den Restklassenringen. Das läßt vermuten, daß sich auch weitere Gruppen mit Hilfe endlicher Körper und Restklassenringe (eventuell sonstiger endlicher Ringe) gut beschreiben lassen.

§ 13. Die Verschärfung des Satzes von Szép

Bezeichne n in diesem und dem folgenden Paragraphen eine natürliche Zahl. Wir zerlegen sie in paarweise teilerfremde Primzahlpotenzfaktoren:

$$n = P_1 \ldots P_k$$

und definieren

$$\Phi(n) = (P_1 - 1)\ldots(P_k - 1)$$

mit der Ergänzung $\Phi(1) = 1$. Enthält n keine mehrfachen Primfaktoren, so fällt $\Phi(n)$ mit der Eulerschen Funktion $\varphi(n)$ zusammen.

Als einfache Anwendung des Satzes 4 beweisen wir folgenden

Satz 9. *Wenn für eine Gruppe G von der Ordnung n jedes $\Phi(d)$ $(d \mid n)$ zu n prim ist, und alle Sylow-Gruppen von G kommutativ sind, so ist G selbst kommutativ. Enthält n höchstens nur zweifache Primfaktoren, so folgt die Kommutativität von G schon aus der einzigen Bedingung, daß $\Phi(n)$ zu n prim ist.*

Diesen Satz fand und bewies *Szép*[4]) unter der weiteren Annahme, daß G auflösbar ist. Diese Forderung ist in seinem Beweise wesentlich. Wenn aber insbesondere n quadratfrei ist, so ist die Auflösbarkeit von selbst erfüllt, und so ist Satz 9 für diesen Fall nicht allgemeiner als der von *Szép*.

Zum Beweis nehmen wir an, daß G nicht kommutativ ist. Dann ist G von positiver Stufe und enthält somit eine Untergruppe G_1 von 1-ter Stufe und einer Ordnung $d(d \mid n)$. Wegen der Annahme ist G_1 keine p-Gruppe, und so folgt aus Satz 4 $d = p^u q^v$ $(u, v \geqq 1\,;\, p \neq q)$ mit $p \mid q^v - 1$ oder $q \mid p^u - 1$. Dann ist $\Phi(d)$ zu n nicht prim, und dieser Widerspruch beweist die erste Hälfte von Satz 9. Die zweite Hälfte ist auch richtig, da zu den Ordnungen p, p^2 nur kommutative Gruppen gehören, und jetzt jedes $\Phi(d)$ $(d \mid n)$ ein Teiler von $\Phi(n)$ ist.

§ 14. Die Ordnungen, zu denen nur kommutative Gruppen gehören

Satz 10. *Alle natürlichen Zahlen n, für die es nur kommutative Gruppen n-ter Ordnung gibt, sind diejenigen, die höchstens nur zweifache Primfaktoren enthalten und zu $\Phi(n)$ prim sind.*

Dieser Satz ist die Umkehrung der zweiten Hälfte von Satz 9, deshalb genügt es, zu beweisen, daß es wenigstens eine nichtkommutative Gruppe n-ter Ordnung gibt, wenn eine Primzahl p vorhanden ist, für die $p^3 \mid n$ oder $p \mid n$, $\Phi(n)$ ist. Im zweiten Fall gibt es eine Primzahl $q(\neq p)$ mit $q \mid n$, $p \mid q - 1$ oder $q^2 \mid n$, $p \mid q^2 - 1$. In allen Fällen gibt es nach Satz 4 eine nichtkommutative Gruppe bzw. von der Ordnung $d = p^3$, pq, pq^2, und dabei ist jedesmal $d \mid n$. Dann gibt es offenbar eine nichtkommutative Gruppe auch von der n-ten Ordnung. Satz 10 ist richtig.

§ 15. Schlußbemerkungen

Es wäre vorteilhafter gewesen, das Produkt in GR statt (3) durch

$$(\alpha, a)(\beta, b) = (\alpha\beta, \bar{\beta}a + b) \tag{104}$$

zu definieren, denn dann gilt $(\alpha, a) = (\alpha, 0)(\varepsilon, a)$. (Nach (3) gilt weniger elegant $(\alpha, a) = (\varepsilon, a)(\alpha, 0)$.) Natürlich weichen (3) und (104) nur

formal ab. Eine andere Variante wäre, wenn man (a, α) statt (α, a) nimmt, und man nach

$$(a, \alpha)(b, \beta) = (a + \bar{\alpha} b, \alpha\beta) \tag{105}$$

multipliziert. (Dann gilt $(a, \alpha) = (a, \varepsilon)(0, \alpha)$.)

Nach einer mündlichen Bemerkung von Herrn *B.v.Sz.Nagy* braucht man bei der Definition von GR nur die Moduleigenschaft von R zu fordern, so daß man G als Operatorenbereich für R auffaßt. Das erlaubt, daß man R multiplikativ schreibt und (als weitere wesentliche Verallgemeinerung) keine Kommutativität mehr fordert. Das führt zu folgender Definition. Es seien G, H zwei (multiplikative) Gruppen mit den Elementen $\alpha, \beta, \ldots$ bzw. $a, b, \ldots$, und dabei sei das Produkt αa erklärt so, daß αa ein Element von H ist und unbeschränkt

$$\alpha(ab) = \alpha a \cdot \alpha b\,, \qquad \alpha\beta a = \alpha(\beta a)\,, \qquad \varepsilon a = a$$

gilt, wobei ε das Einselement von G ist. Dann bilden die Paare (α, a) mit der Produktregel

$$(\alpha, a)(\beta, b) = (\alpha\beta, a \cdot \alpha b) \tag{106}$$

eine Gruppe, die wir das (verallgemeinerte) schiefe Produkt GH nennen können.

Murray und *Neumann*[10]) verwenden in einem interessanten Spezialfall eine mit unserem schiefen Produkt identische Konstruktion, um mit geistvoller Leichtigkeit abzählbare Gruppen anzugeben, in denen jede Klasse konjugierter Elemente (außer der Klasse von 1) unendlich ist, gleichzeitig wird die Existenz solcher Gruppen zum ersten Male ausgewiesen. Dazu nehmen sie eine beliebige abzählbare Gruppe G, die Menge M aller endlichen Teilmengen von G, definieren in M eine Addition so, daß für irgend zwei Elemente a, b von M die Summe $a + b$ die Menge derjenigen Elemente von a und b bedeutet, die nur in a oder b (aber nicht in beiden) vorkommen — dann ist M eine ebenfalls abzählbare, kommutative Gruppe, in der alle Elemente $(\neq 1)$ von der 2-ten Ordnung sind — und setzen

$$(\alpha, a)(\beta, b) = (\alpha\beta, \beta a + b) \qquad (\alpha, \beta \in G;\ a, b \in M)\,,$$

wobei βa die gewöhnliche „Gruppenelement mal Komplex"-Multiplikation bedeutet, also G als Operatorenbereich für M aufgefaßt wird. Dann

[10]) *F. J. Murray* and *J. v. Neumann:* On rings of operators IV, Annals of Math. 44 (1943), 716—808, insbesondere S. 796—797.

ist dieses schiefe Produkt GM eine gewünschte Gruppe (wie auch die Ausgangsgruppe G gewählt wurde). Der einfachste Fall tritt ein, wenn G (unendlich) zyklisch ist, aber auch dann stünde man vor einer schweren Aufgabe, wollte man GM auf andere Weise, nicht als schiefes Produkt definieren.

Merkwürdig ist es, wie unser $G_I(p, q, u) = G(p^u)k(q^v)$ und dieses GM von *Murray* und *Neumann* als zwei extreme Fälle von nichtkommutativen Gruppen einander gegenüberstehen. Das erste ist nämlich eine (endliche) Gruppe, die am „schwächsten" nichtkommutativ ist, das zweite ist dagegen eine (unendliche) „sehr stark" nichtkommutative Gruppe. In der Tat, das schiefe Produkt (vom ersten Typ) ist fähig, sehr verschiedenartige Gruppen zu repräsentieren.

Murray und *Neumann* bemerken über ihr Beispiel GM, daß es „die einfachste Kombination von G und M ist, abgesehen vom direkten Produkt".

Obige Verallgemeinerung von GR enthält das schiefe Produkt $G(+)R$ vom zweiten Typ als Spezialfall (was jetzt schon offenbar auch aus der Bemerkung im § 3 folgt). Um dies unmittelbar einzusehen, definiere man nämlich $\alpha a = a + \alpha' a$, wobei die α wieder als Operatoren anzusehen sind.

Auch $G(\dagger)R$ läßt sich wie folgt verallgemeinern. Hierzu schreiben wir (20) in der Form

$$(\alpha, a)(\beta, b) = (\alpha\beta, a + b + \alpha\beta') \ ,$$

wobei β' (wie bisher) eine additive homomorphe Abbildung von G in R, dagegen α in einem Produkt αx $(x \in R)$ als Operator aufzufassen ist mit $\alpha(x + y) = \alpha x + \alpha y$, $\alpha\beta x = \alpha x + \beta x$. Dann ist von R wieder nur die Moduleigenschaft zu fordern. Schreibt man R als multiplikative (kommutative) Gruppe H, so lautet die Produktregel

$$(\alpha, a)(\beta, b) = (\alpha\beta, ab \cdot \alpha\overline{\beta}) \ , \tag{107}$$

wobei $\overline{\beta}$ eine (multiplikative) homomorphe Abbildung von G in H und α in einem Produkt $\alpha x (x \in H)$ ein Operator ist mit $\alpha(xy) = \alpha x \cdot \alpha y$, $\alpha\beta x = \alpha x \cdot \beta x$. (Dann muß $\alpha^n x = \alpha x^n = (\alpha x)^n$, $\varepsilon x = \alpha 1 = 1$ gelten, wobei 1 das Einselement von H ist.)

Noch allgemeiner multipliziere man statt (107) nach der Regel

$$(\alpha, a)(\beta, b) = (\alpha\beta, ab C_{\alpha,\beta}) \ , \tag{108}$$

wobei $C_{\alpha,\beta}$ in H ist, fordere Assoziativität, die mit

$$C_{\alpha,\beta} C_{\alpha\beta,\gamma} = C_{\alpha,\beta\gamma} C_{\beta,\gamma} \tag{109}$$

gleichkommt, und schreibe auch vor, daß $C_{\varepsilon,\varepsilon}$ das Einselement von H ist. Dann bilden die (α, a) eine Gruppe. Diese ist im wesentlichen ein Spezialfall der Erweiterung von H mit der Faktorgruppe G im Sinne von *O. Schreier*[11]), in der nämlich H im Zentrum ist, und die $C_{\alpha,\beta}$ ein „Faktorsystem" bilden. Diese „zentrale" Erweiterung verwendet *Eckmann*[12]) in der Topologie. Einen weiteren Zusammenhang mit der Algebra findet man bei *Witt*[13]) und *Teichmüller*[14]).

Diese Berührungen unserer schiefen Produkte mit den hier angeführten Arbeiten wurden mir erst bekannt, als ich meine Arbeit schon fertig hatte. Übrigens haben diese Arbeiten mit den Gruppen 1-ter Stufe nichts gemein und ermöglichen eine Verkürzung unserer Arbeit nicht.

Verwendet man, wie oben besprochen, eine Operatorenkonstruktion, so tritt für unsere Gruppen G_I, G_{II}, G_{III} die prinzipielle Vereinfachung ein, daß sie bzw. als ein (verallgemeinertes) schiefes Produkt $G(p^u)G(q^v)$, $G(p^u)G(p^v)$, $G(p^u, p^v)G(p)$ erscheinen, indem man den ersten Faktor passend zu einem Operatorenbereich für den zweiten Faktor macht (aber im dritten Fall ist auch die Verwendung einer Homomorphie nötig). In der Tat bleibt aber die auf der ursprünglichen Definition der schiefen Produkte (§§ 2—4) beruhende Konstruktion im Satz 4 die einfachste, wobei eben die Ringeigenschaft des zweiten Faktors weit ausgenutzt wurde.

(Eingegangen den 5. Januar 1947.)

---

[11]) Siehe z. B. *H. Zassenhaus*, Lehrbuch der Gruppentheorie, Leipzig und Berlin 1937, S. 89.

[12]) *B. Eckmann*, Der Cohomologie-Ring einer beliebigen Gruppe, diese Commentarii 18 (1945/46), S. 232—282. Hier auf S. 238 sind die zweiten Glieder beider Seiten von (2) miteinander zu vertauschen. Nach dieser Berichtigung kommt man im wesentlichen zu obigem (109).

[13]) *E. Witt*, Der Existenzsatz für abelsche Funktionenkörper, Journ. f. d. reine u. angew. Math. 173 (1935), 43—51.

[14]) *O. Teichmüller*, Über die sogenannte nichtkommutative Galoische Theorie und die Relation $\xi_{\lambda,\mu,\pi}\,\xi_{\lambda,\mu\nu,\pi}\,\xi^{\lambda}_{\mu,\nu,\pi} = \xi_{\lambda,\mu,\nu\pi}\,\xi_{\lambda\mu,\nu,\pi}$. Deutsche Math. 5 (1940), 138 bis 149.