XXVII.

Über Gruppen, deren sämtliche Teiler Normalteiler sind.

[Mathematische Annalen, Bd. 48, S. 548—561 (1897).]

Die vorliegende Untersuchung, welche ich in den ersten Herbstwochen des Jahres 1895 begonnen und beendet habe, ist durch die Frage nach allen denjenigen endlichen Zahlenkörpern veranlaßt, deren sämtliche Divisoren Normalkörper sind. Ist R die Gruppe aller Permutationen φ eines Normalkörpers Ω, so gehört bekanntlich zu jeder Gruppe S, welche ein Teiler von R ist, ein bestimmter Körper Ω', nämlich der Inbegriff aller derjenigen Zahlen in Ω, welche durch jede Permutation der Gruppe S in sich selbst übergehen, und umgekehrt gehört jeder Divisor von Ω, d. h. jeder in Ω enthaltene Körper Ω' zu einer bestimmten in R als Teiler enthaltenen Gruppe S; die Bedingung aber, daß Ω' wieder ein Normalkörper ist, besteht darin, daß S ein Normalteiler*) von R, also immer

$$\varphi^{-1} S \varphi = S, \qquad S\varphi = \varphi S \tag{1}$$

ist, wo φ jedes beliebige Element der Gruppe R bedeutet. Der auf die Gruppentheorie bezügliche Teil der obigen Frage kommt daher auf die Aufgabe zurück, die allgemeinste Form einer Gruppe R zu finden, deren sämtliche Teiler S Normalteiler von R sind.

Zu diesen Gruppen R gehören offenbar alle Abelschen, d. h. diejenigen Gruppen, deren Elemente sämtlich miteinander permutabel

*) Diese Benennung, welche H. Weber in seinem Lehrbuch der Algebra (Bd. I, 1895, S. 511) eingeführt hat, scheint mir aus mehreren Gründen zweckmäßiger als die sonst gebräuchlichen eines ausgezeichneten oder invarianten oder eigentlichen Teilers, welche letztere Bezeichnung ich in meinen Göttinger Vorlesungen (1857—1858) im Anschluß an eine Ausdrucksweise von Galois benutzt habe. Sind R, S irgend zwei verwandte, d. h. solche Gruppen, die ein gemeinsames Multiplum besitzen, und bedeutet φ jedes Element von R, so empfiehlt es sich aus algebraischen Gründen, den größten gemeinsamen Teiler aller Gruppen $\varphi^{-1} S \varphi$ die Norm von S in bezug auf R zu nennen.

www.rcin.org.pl

sind; ihr Bau darf als hinreichend bekannt vorausgesetzt werden, und es handelt sich daher nur noch um die Form der nicht Abelschen Gruppen R, welche ich im folgenden Hamiltonsche Gruppen nennen werde. Die einfachste oder kleinste solche Gruppe R ist nämlich diejenige Gruppe achten Grades, welche sechs verschiedene Elemente vierten Grades enthält und welche wegen ihrer innigen Beziehungen zu Hamiltons berühmter Zahlenschöpfung die Quaterniongruppe Q heißen mag. Sodann ergibt sich das durch seine enge Umgrenzung überraschende Resultat, daß die allgemeinste Hamiltonsche Gruppe die Form

$$R = PQ \tag{2}$$

besitzt, wo P die Abelsche Gruppe aller derjenigen Elemente in R bedeutet, welche mit jedem Element von R permutabel sind; diese Gruppe P unterliegt nur den beiden Bedingungen, daß sie kein einziges Element vierten Grades, wohl aber das in der Quaterniongruppe Q befindliche Element zweiten Grades enthält.

§ 1.

Die Quaterniongruppe Q.

Man kann dieselbe (wie in der Einleitung) als Gruppe achten Grades definieren, welche sechs verschiedene Elemente vierten Grades enthält; die letzteren bilden offenbar drei Paare von je zwei reziproken Elementen und mögen mit $\alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}$ bezeichnet werden; außer dem Hauptelemente 1 muß Q endlich noch ein Element ε vom zweiten Grade enthalten. Es ist also

$$\varepsilon^2 = 1, \tag{3}$$

$$\alpha^2 = \alpha^{-2} = \beta^2 = \beta^{-2} = \gamma^2 = \gamma^{-2} = \varepsilon, \tag{4}$$

$$\varepsilon\alpha = \alpha\varepsilon = \alpha^{-1}, \quad \varepsilon\beta = \beta\varepsilon = \beta^{-1}, \quad \varepsilon\gamma = \gamma\varepsilon = \gamma^{-1}, \tag{5}$$

$$\varepsilon\alpha^{-1} = \alpha^{-1}\varepsilon = \alpha, \quad \varepsilon\beta^{-1} = \beta^{-1}\varepsilon = \beta, \quad \varepsilon\gamma^{-1} = \gamma^{-1}\varepsilon = \gamma. \tag{6}$$

Da nun das Produkt $\beta\gamma$ keine Potenz von β oder γ sein kann (weil sonst $\gamma = \beta^{\pm 1}$ wäre), so muß es mit einem der beiden übrigen Elemente $\alpha^{\pm 1}$ identisch sein. Offenbar dürfen wir die Bezeichnung der Elemente von Q so wählen, daß $\beta\gamma = \alpha$ wird; da hieraus $\beta\gamma\alpha = \alpha^2 = \beta^2$ und $\alpha\beta\gamma = \alpha^2 = \gamma^2$ folgt, so ergibt sich

$$\beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma. \tag{7}$$

www.rcin.org.pl

Aus $(\beta\gamma)(\gamma\beta) = \beta(\gamma^2)\beta = \beta(\beta^2)\beta = \beta^4 = 1$ folgt ferner, daß $\beta\gamma$ und $\gamma\beta$ reziproke Elemente sind; aus (7) ergibt sich daher

(8) $$\gamma\beta = \alpha^{-1}, \quad \alpha\gamma = \beta^{-1}, \quad \beta\alpha = \gamma^{-1}.$$

Aus (7) und (8) folgen auch die Produkte der reziproken Elemente

(9) $$\gamma^{-1}\beta^{-1} = \alpha^{-1}, \quad \alpha^{-1}\gamma^{-1} = \beta^{-1}, \quad \beta^{-1}\alpha^{-1} = \gamma^{-1},$$

(10) $$\beta^{-1}\gamma^{-1} = \alpha, \quad \gamma^{-1}\alpha^{-1} = \beta, \quad \alpha^{-1}\beta^{-1} = \gamma.$$

Da ferner

(11) $$\alpha\alpha^{-1} = \alpha^{-1}\alpha = \beta\beta^{-1} = \beta^{-1}\beta = \gamma\gamma^{-1} = \gamma^{-1}\gamma = 1,$$

so ergeben sich aus den vorhergehenden Gleichungen auch die Produkte

(12) $$\gamma\beta^{-1} = \gamma^{-1}\beta = \alpha, \quad \beta\gamma^{-1} = \beta^{-1}\gamma = \alpha^{-1},$$

(13) $$\alpha\gamma^{-1} = \alpha^{-1}\gamma = \beta, \quad \gamma\alpha^{-1} = \gamma^{-1}\alpha = \beta^{-1},$$

(14) $$\beta\alpha^{-1} = \beta^{-1}\alpha = \gamma, \quad \alpha\beta^{-1} = \alpha^{-1}\beta = \gamma^{-1}.$$

Die Kompositionstabelle der Quaterniongruppe ist daher die folgende:

	1	ε	α^{-1}	α	β^{-1}	β	γ^{-1}	γ
1	1	ε	α^{-1}	α	β^{-1}	β	γ^{-1}	γ
ε	ε	1	α	α^{-1}	β	β^{-1}	γ	γ^{-1}
α	α	α^{-1}	1	ε	γ^{-1}	γ	β	β^{-1}
α^{-1}	α^{-1}	α	ε	1	γ	γ^{-1}	β^{-1}	β
β	β	β^{-1}	γ	γ^{-1}	1	ε	α^{-1}	α
β^{-1}	β^{-1}	β	γ^{-1}	γ	ε	1	α	α^{-1}
γ	γ	γ^{-1}	β^{-1}	β	α	α^{-1}	1	ε
γ^{-1}	γ^{-1}	γ	β	β^{-1}	α^{-1}	α	ε	1

wo das durch die Zeile φ und Spalte ψ bestimmte Feld das Produkt $\varphi\psi$ enthält.

Statt von der obigen Definition der Quaterniongruppe Q kann man auch von der folgenden ausgehen: die Gruppe Q wird durch zwei nicht permutable Elemente α, β erzeugt, welche den Bedingungen

(15) $$\beta\alpha\beta = \alpha, \quad \alpha\beta\alpha = \beta$$

genügen. Führt man nämlich das dritte Element $\gamma = \alpha\beta$ ein, so nehmen diese Bedingungen die Form (7) an, woraus alle anderen

www.rcin.org.pl

Relationen leicht folgen. Durch Multiplikation der ersten Gleichung (7) mit α ergibt sich zunächst $\alpha^2 = \beta\gamma\alpha = \alpha\beta\gamma$; mit Rücksicht auf die zweite und dritte Gleichung (7) kann man daher das vierte Element ε durch

$$\varepsilon = \alpha^2 = \beta^2 = \gamma^2$$

einführen, welches folglich mit α, β, γ permutabel ist; die aus (7) folgende Gleichung

$$(\beta\gamma)\,(\gamma\alpha)\,(\alpha\beta) = \alpha\beta\gamma$$

ist daher identisch mit $\varepsilon^3 = \varepsilon$, also mit (3), und hieraus folgen offenbar die übrigen Gleichungen, also alle Kompositionen der Tabelle. Da wir ferner angenommen haben, daß die beiden erzeugenden Elemente α, β nicht permutabel sind, so ist $\gamma = \alpha\beta$ verschieden von $\gamma^{-1} = \beta\alpha$, mithin $\varepsilon = \gamma^2$ verschieden von 1, d. h. ε ist vom zweiten, und α, β, γ, α^{-1}, β^{-1}, γ^{-1} sind vom vierten Grade; man überzeugt sich auch leicht, daß alle diese Elemente voneinander verschieden sind.

Mag man aber von der einen oder der anderen Definition ausgehen und so zu der obigen Tabelle gelangen, so ist hiermit die Existenz der Gruppe Q noch nicht vollständig erwiesen; es muß bekanntlich noch gezeigt werden, daß sowohl aus $\varphi\psi = \varphi\chi$ wie aus $\psi\varphi = \chi\varphi$ immer $\psi = \chi$ folgt, und daß außerdem das Assoziationsgesetz $(\varphi\psi)\chi = \varphi(\psi\chi)$ gilt. Die erstere Eigenschaft ergibt sich zwar leicht aus dem Anblick der Tabelle, welche in jeder Zeile wie in jeder Spalte lauter verschiedene Elemente enthält; aber die Verifikation des Assoziationsgesetzes, wenn sie sich auch auf manche Art abkürzen läßt, würde doch schon ziemlich lästig sein. In solchen Fällen pflegt das einfachste Verfahren, um die Existenz einer durch erzeugende Elemente definierten Gruppe nachzuweisen, darin zu bestehen, daß man dieselbe als Teiler einer schon bekannten Gruppe G darstellt, weil dann die beiden obigen Gesetze von selbst erfüllt sind. Für unser Beispiel genügt es, die symmetrische Gruppe G aller $\Pi(8)$ Versetzungen von acht verschiedenen Dingen a, b, c, d, a', b', c', d' zu betrachten; benutzt man die bekannte Bezeichnung der Zyklen und setzt

$$(16)\qquad \begin{cases} \alpha = (d\,a\,d'\,a')(c\,b\,c'\,b'), \\ \beta = (d\,b\,d'\,b')(a\,c\,a'\,c'), \\ \gamma = (d\,c\,d'\,c')(b\,a\,b'\,a'), \\ \varepsilon = (a\,a')(b\,b')(c\,c')(d\,d'), \end{cases}$$

www.rcin.org.pl

so erfüllen die beiden nicht permutablen Elemente α, β der Gruppe G wirklich die beiden Bedingungen (15), und folglich muß die von ihnen erzeugte Gruppe, welche ein Teiler von G ist, mit unserem System Q der acht verschiedenen Elemente $1, \varepsilon, \alpha, \beta, \gamma, \alpha^{-1}, \beta^{-1}, \gamma^{-1}$ identisch sein.

Diese Gruppe Q, deren Existenz hiermit gesichert ist, verdient den Namen der Quaterniongruppe zunächst wegen der augenscheinlichen Analogie zwischen der Komposition der drei Elemente vierten Grades α, β, γ und der Multiplikation der drei Hamiltonschen imaginären Einheiten i, j, k; es findet aber, wie ich schon im Februar 1886 erkannt habe, eine noch tiefer liegende Beziehung zwischen der Gruppe Q und Hamiltons Quaternionen statt, von welcher demnächst an einem anderen Orte gehandelt werden soll. Damals habe ich auch schon Normalkörper gebildet, deren Permutationsgruppe mit Q identisch ist; ein einfaches Beispiel, welches unendlich viele Spezialfälle umfaßt, liefert die Gleichung

$$\omega^2 = r(2+\sqrt{2})(3+\sqrt{6}),$$

wo r irgendeine von Null verschiedene rationale Zahl bedeutet; jede Wurzel ω einer solchen Gleichung erzeugt einen Quaternionkörper, d. h. einen Normalkörper achten Grades mit der Gruppe Q, und man kann beweisen, daß auf diese Weise jeder Quaternionkörper entsteht, der die Quadratwurzeln aus 2 und 3 enthält.

Daß aber diese Gruppe Q, welche außerdem schon in ganz anderen Untersuchungen aufgetreten ist, die in der Einleitung angegebene wichtige Bedeutung für alle Hamiltonschen Gruppen besitzt, habe ich erst im Herbste 1895 erkannt, und die Darlegung dieser Bedeutung bildet den ausschließlichen Gegenstand der vorliegenden Abhandlung.

Man überzeugt sich zunächst leicht, daß Q keine anderen Teiler als Normalteiler besitzt. Bezeichnet man der Kürze halber die durch irgendwelche Elemente $\varphi, \psi, \chi \cdots$ erzeugte Gruppe mit dem Symbol $[\varphi, \psi, \chi, \cdots]$, so daß z. B. $[\varphi]$ die aus allen Potenzen von φ bestehende zyklische oder reguläre Gruppe oder Periode bedeutet, so hat Q offenbar nur die folgenden sechs Teiler

$$(17) \qquad [1],\ [\varepsilon],\ [\alpha],\ [\beta],\ [\gamma],\ [\alpha, \beta] = Q;$$

www.rcin.org.pl

daß $[1]$ und Q Normalteiler von Q sind, ist eine allgemeine Eigenschaft aller Gruppen; dasselbe gilt von $[\varepsilon]$, weil ε mit allen Elementen von Q permutabel ist, und auch z. B. von $[\alpha]$, weil

$$Q = [\alpha] + [\alpha]\beta \tag{18}$$

und

$$\beta^{-1}[\alpha]\beta = [\alpha^{-1}] = [\alpha] \tag{19}$$

ist. Also ist Q im Sinne der Einleitung wirklich eine Hamiltonsche Gruppe.

§ 2.

Kennzeichen der Hamiltonschen Gruppen.

Um die allgemeine Form aller Hamiltonschen Gruppen zu finden, ist es zweckmäßig, aus ihrer Definition, wie sie in der Einleitung gegeben ist, einfachere charakteristische Kennzeichen abzuleiten, welche in den folgenden Sätzen enthalten sind; daß dieselben auch für die Abelschen Gruppen gelten, welche also, wenn auch nur vorläufig, als ein spezieller Fall der Hamiltonschen Gruppen anzusehen sind, braucht kaum bemerkt zu werden*).

I. Die erforderliche und hinreichende Bedingung dafür, daß R eine Hamiltonsche Gruppe ist, besteht darin, daß, wenn φ, ψ irgendwelche Elemente von R bedeuten, das Element $\varphi^{-1}\psi\varphi$ eine Potenz von ψ, also in der Periode $[\psi]$ enthalten ist.

Denn wenn R eine Hamiltonsche (oder Abelsche) Gruppe ist, so muß $\varphi^{-1}[\psi]\varphi = [\psi]$, also $\varphi^{-1}\psi\varphi$ eine Potenz von ψ sein. Umgekehrt, wenn diese Bedingung durch alle Elemente φ, ψ einer Gruppe R erfüllt wird, und S irgendeine in R enthaltene Gruppe bedeutet, so wird, wenn ψ alle Elemente von S durchläuft, $\varphi^{-1}\psi\varphi$ als Potenz von ψ ebenfalls in S enthalten sein; mithin ist die aus den Elementen $\varphi^{-1}\psi\varphi$ bestehende Gruppe $\varphi^{-1}S\varphi$ ein Teiler von S und folglich $= S$, w. z. b. w.

Dieses Kennzeichen läßt sich in einer für unseren Zweck noch bequemeren Form ausdrücken, wenn man das durch die Bedingung

$$\psi\varphi = \varphi\psi\varepsilon \tag{20}$$

definierte Element

$$\varepsilon = (\psi^{-1}\varphi^{-1}\psi)\varphi = \psi^{-1}(\varphi^{-1}\psi\varphi) \tag{21}$$

*) Man könnte vielleicht beide Arten von Gruppen unter dem gemeinsamen Namen von Normalgruppen zusammenfassen.

www.rcin.org.pl

einführt, welches wir der Kürze halber den Kommutator der Elemente φ, ψ nennen wollen*); der vorige Satz geht dann, weil

$$[\varphi^{-1}]\varphi = [\varphi]\varphi = [\varphi] \quad \text{und} \quad \psi^{-1}[\psi] = [\psi]$$

ist, offenbar in den folgenden über:

II. Die erforderliche und hinreichende Bedingung dafür, daß R eine Hamiltonsche Gruppe ist, besteht darin, daß der Kommutator ε von je zwei in R enthaltenen Elementen φ, ψ ein gemeinsames Element ihrer Perioden $[\varphi]$, $[\psi]$ und folglich auch mit allen Elementen der durch φ und ψ erzeugten Gruppe $[\varphi, \psi]$ permutabel ist.

Die nächsten Folgerungen, welche sich hieraus mit Zuziehung der bekannten, für je zwei Elemente ϱ, σ einer beliebigen Gruppe und für jede ganze rationale Zahl s gültigen Identität

$$\varrho^{-1}\sigma^s\varrho = (\varrho^{-1}\sigma\varrho)^s \tag{22}$$

ergeben, bilden den folgenden Satz:

III. Ist ε der Kommutator der Elemente φ, ψ einer Hamiltonschen Gruppe, so ist

$$\psi^n\varphi^m = \varphi^m\psi^n\varepsilon^{mn}, \tag{23}$$

$$(\varphi^m\psi^n)^t = \varphi^{mt}\psi^{nt}\varepsilon^{\frac{1}{2}mnt(t-1)}, \tag{24}$$

und die durch φ und ψ erzeugte Gruppe ist

$$[\varphi, \psi] = [\varphi][\psi] = [\psi][\varphi]. \tag{25}$$

Setzt man ferner

$$\varphi_1 = \varphi^m\psi^n, \quad \psi_1 = \varphi^r\psi^s, \tag{26}$$

so ist

$$\varepsilon_1 = \varepsilon^{ms-nr} \tag{27}$$

der Kommutator der Elemente φ_1, ψ_1.

Wendet man nämlich die Identität (22) auf das Beispiel $\varrho = \varphi$, $\sigma = \psi$, $s = n$ an, so wird $\varrho^{-1}\sigma\varrho = \varphi^{-1}\psi\varphi = \psi\varepsilon$, und weil ψ zufolge II mit ε permutabel ist, so erhält man

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

also

$$\psi^{-n}\varphi^{-1}\psi^n = \varepsilon^n\varphi^{-1};$$

*) Ohne auf die Bedeutung dieses Begriffes für die allgemeine Gruppentheorie näher einzugehen, will ich nur den Satz erwähnen, daß der größte in einem Normalkörper von der Gruppe G enthaltene Abelsche Körper zu derjenigen Gruppe gehört, welche durch alle in G enthaltenen Kommutatoren erzeugt wird.

www.rcin.org.pl

setzt man daher in (22) jetzt $\varrho = \psi^n$, $\sigma = \varphi^{-1}$, $s = m$, so wird $\varrho^{-1}\sigma\varrho = \varepsilon^n\varphi^{-1}$, und weil ε^n mit φ^{-1} permutabel ist, so erhält man

$$\psi^{-n}\varphi^{-m}\psi^n = (\varepsilon^n\varphi^{-1})^m = \varepsilon^{mn}\varphi^{-m},$$

also die Gleichung (23), und hieraus folgt leicht durch vollständige Induktion der Satz (24); denn wenn derselbe für eine bestimmte ganze rationale Zahl t gilt (wie z. B. für $t = 0$), so folgt durch Multiplikation mit $\varphi^m\psi^n$ oder mit dem reziproken Element $\psi^{-n}\varphi^{-m}$ unter Zuziehung von (23), daß er auch für die beiden benachbarten Zahlen $t \pm 1$ gilt. Aus (23) und (26) folgt ferner

$$\varphi_1\psi_1 = \varphi^m(\psi^n\varphi^r)\psi^s = \varphi^{m+r}\psi^{n+s}\varepsilon^{nr},$$
$$\psi_1\varphi_1 = \varphi^r(\psi^s\varphi^m)\psi^n = \varphi^{m+r}\psi^{n+s}\varepsilon^{ms},$$

und da ε Potenz von ψ ist, so sind alle Produkte $\varphi_1\psi_1$ von je zwei in dem Komplex $[\varphi][\psi]$ enthaltenen Elementen φ_1, ψ_1 in demselben Komplex enthalten, woraus (25) folgt; zugleich ergibt sich aus den beiden vorstehenden Gleichungen auch der Kommutator ε_1 in der Form (27), w. z. b. w.

§ 3.

Eigenschaften zweier nicht permutablen Elemente einer Hamiltonschen Gruppe.

Die zuletzt erhaltenen Resultate sind offenbar nur dann von Interesse, wenn die beiden Elemente φ, ψ nicht permutabel sind, was wir im folgenden annehmen; ihr Kommutator ε ist dann verschieden von dem Hauptelement 1 der Hamiltonschen Gruppe R; bedeutet daher e den Grad des Elementes ε und der Periode $[\varepsilon]$, so ist

$$e > 1, \quad \varepsilon^e = 1. \tag{28}$$

Wählt man nun die Exponenten m, n des Elementes φ_1 in (26) so, daß m, n, e keinen gemeinsamen Teiler haben, so kann man die Exponenten r, s des anderen Elementes ψ_1 so bestimmen, daß $ms - nr \equiv 1 \pmod{e}$ wird; nach (27) folgt hieraus $\varepsilon_1 = \varepsilon$, und da der Kommutator ε_1 der Elemente φ_1, ψ_1 nach Satz II eine Potenz von φ_1 ist, so ergibt sich nach (24) die Existenz einer ganzen Zahl t, welche der Bedingung

$$\varphi^{mt}\psi^{nt}\varepsilon^{\frac{1}{2}mnt(t-1)} = \varepsilon \tag{29}$$

genügt.

www.rcin.org.pl

Um diesen Existenzsatz für unseren Zweck zu verwerten, wird es nötig, die Perioden $[\varphi]$, $[\psi]$ und deren größten gemeinsamen Teiler D, welcher bekanntlich selbst eine Periode ist, genauer zu betrachten. Da die Periode $[\varepsilon]$ nach Satz II ein gemeinsamer Teiler von $[\varphi]$, $[\psi]$, also auch ein Teiler von D ist, so ist der Grad von D teilbar durch e, also von der Form de. Da ferner jedes Element in D von der Form φ^m und zugleich eine Potenz von ψ, also auch mit ψ permutabel ist, so folgt aus (23), wenn man dort $n = 1$ setzt, daß $\varepsilon^m = 1$, also m durch e teilbar sein muß; alle Elemente von D sind daher Potenzen von φ^e, und da offenbar auf dieselbe Weise folgt, daß sie auch Potenzen von ψ^e sein müssen, so ist der größte gemeinsame Teiler D der Perioden $[\varphi]$, $[\psi]$ zugleich derjenige der Perioden $[\varphi^e]$, $[\psi^e]$; bezeichnet man daher die Grade der letzteren, weil sie durch den von D teilbar sein müssen, mit ade, bde, so sind ade^2, bde^2 die Grade von $[\varphi]$, $[\psi]$, und zufolge (25) ist nach einem bekannten Satze $abde^3$ der Grad von $[\varphi, \psi]$, woraus beiläufig folgt, daß der Grad einer Hamiltonschen Gruppe nicht kleiner als acht sein kann. Zugleich ergeben sich folgende Darstellungen unserer Gruppen:

$$[\varepsilon] = [\varphi^{ade}] = [\psi^{bde}], \tag{30}$$

$$\begin{aligned} D &= [\varphi^{ae}] = [\psi^{be}] \\ &= [\varepsilon](1 + \varphi^{ae} + \varphi^{2ae} + \cdots + \varphi^{(d-1)ae}) \\ &= [\varepsilon](1 + \psi^{be} + \psi^{2be} + \cdots + \psi^{(d-1)be}), \end{aligned} \tag{31}$$

$$[\varphi] = D(1 + \varphi + \varphi^2 + \cdots + \varphi^{ae-1}), \tag{32}$$

$$[\psi] = D(1 + \psi + \psi^2 + \cdots + \psi^{be-1}), \tag{33}$$

$$\begin{aligned} [\varphi, \psi] &= [\varphi][\psi] = [\psi][\varphi] \\ &= [\varphi](1 + \psi + \psi^2 + \cdots + \psi^{be-1}) \\ &= [\psi](1 + \varphi + \varphi^2 + \cdots + \varphi^{ae-1}) \end{aligned} \tag{34}$$

und aus den beiden ersten Darstellungen von D folgt die Existenz von zwei ganzen Zahlen h, k, welche den Bedingungen

$$\varphi^{ae} = \psi^{bek}, \quad \psi^{be} = \varphi^{aeh}, \quad hk \equiv 1 \pmod{de} \tag{35}$$

genügen.

Wir wenden uns nun dazu, den Existenzsatz (29) zur Geltung zu bringen; statt dies in voller Allgemeinheit durchzuführen, ziehen wir es vor, ihn auf zwei spezielle Beispiele von Zahlenpaaren m, n anzuwenden, was bequemer und ebenso erfolgreich ist.

www.rcin.org.pl

Erstes Beispiel. Bedeutet c den größten gemeinsamen Teiler der beiden Zahlen

$$a = ca', \qquad b = cb', \tag{36}$$

so setzen wir

$$m = -ha', \qquad n = b';$$

dann haben die Zahlen m, n, e zufolge (35), (36) keinen gemeinsamen Teiler, und es gibt daher zufolge (29) eine ganze Zahl t, welche der Bedingung

$$\varphi^{-ha't}\psi^{b't}\varepsilon^{-\frac{1}{2}ha'b't(t-1)} = \varepsilon$$

genügt. Da ε Potenz von φ ist, so muß $\psi^{b't}$ in D enthalten, also $b't$ zufolge (31) teilbar sein durch $be = b'ce$; mithin wird $t = ceu$, wo u eine ganze Zahl bedeutet, und da nach (35), (36) hieraus

$$\psi^{b't} = \psi^{beu} = \varphi^{aehu} = \varphi^{ha't}$$

folgt, so geht die obige Bedingung für t in

$$\varepsilon^{-\frac{1}{2}ha'b'ceu(ceu-1)} = \varepsilon,$$

also in die Kongruenz

$$-\tfrac{1}{2}ha'b'ceu(ceu-1) \equiv 1 \pmod{e}$$

über. Da unter den Faktoren der linken Seite sich auch die Zahl e befindet, so ergibt sich durch Multiplikation mit 2 das Resultat

$$2 \equiv 0 \pmod{e},$$

also zufolge (28)

$$e = 2, \quad \varepsilon^2 = 1, \tag{37}$$

und hierdurch geht die vorstehende Kongruenz in

$$ha'b'cu \equiv 1 \pmod{2}$$

über, woraus mit Rücksicht auf (36) auch

$$1 \equiv h \equiv a' \equiv b' \equiv c \equiv a \equiv b \pmod{2} \tag{38}$$

folgt. Die Grade von $[\varphi]$, $[\psi]$ sind $4ad$, $4bd$, und zufolge (30) ist

$$\varepsilon = \varphi^{2ad} = \psi^{2bd}. \tag{39}$$

Der Grad der Gruppe $[\varphi, \psi]$ ist $= 8abd$.

Zweites Beispiel. Setzen wir

$$m = a(d-h), \qquad n = b,$$

so haben die Zahlen m, n, e zufolge (37), (38) keinen gemeinsamen Teiler, und außerdem ist zufolge (38) das Produkt

$$mn \equiv d-1 \pmod{2};$$

www.rcin.org.pl

es gibt daher zufolge (29) eine ganze Zahl t, welche der Bedingung

$$\varphi^{a(d-h)t}\psi^{bt}\varepsilon^{\frac{1}{2}(d-1)t(t-1)} = \varepsilon$$

genügt. Da ε Potenz von φ ist, so muß ψ^{bt} in D enthalten, also bt zufolge (31) teilbar sein durch $be = 2b$; mithin wird $t = 2u$, wo u wieder eine ganze Zahl bedeutet, also $\frac{1}{2}t(t-1) \equiv u \pmod 2$; mit Rücksicht auf (35), (39) wird zugleich

$$\psi^{bt} = \psi^{2bu} = \varphi^{2ahu} = \varphi^{aht},$$
$$\varphi^{a(d-h)t}\psi^{bt} = \varphi^{adt} = \varphi^{2adu} = \varepsilon^{u},$$

mithin kommt die obige Bedingung für t auf

$$\varepsilon^{du} = \varepsilon$$

zurück, woraus

(40) $$d \equiv 1 \pmod 2$$

folgt.

Die in (37), (38), (39), (40) gewonnenen fundamentalen Resultate fassen wir zusammen in den folgenden Satz:

IV. Die Grade von je zwei nicht permutablen Elementen φ, ψ einer Hamiltonschen Gruppe sind $\equiv 4 \pmod 8$; bezeichnet man dieselben bzw. mit $8r+4$, $8s+4$, so ist der durch $\psi\varphi = \varphi\psi\varepsilon$ definierte Kommutator

(41) $$\varepsilon = \varphi^{4r+2} = \psi^{4s+2},$$

also vom Grade zwei.

§ 4.

Allgemeine Form der Hamiltonschen Gruppen.

Mit Hilfe der eben gewonnenen Grundlage gelingt es nun ohne Schwierigkeit, die allgemeine Form aller Hamiltonschen (nicht Abelschen) Gruppen R zu finden.

Diejenigen Elemente π einer solchen (oder auch jeder anderen) Gruppe R, welche mit jedem Element ω von R permutabel sind, bilden bekanntlich eine Gruppe, weil aus $\pi'\omega = \omega\pi'$ und $\pi''\omega = \omega\pi''$ auch $(\pi'\pi'')\omega = \omega(\pi'\pi'')$ folgt; diese, offenbar Abelsche Gruppe soll im folgenden durchweg mit P bezeichnet werden. Da R eine Hamiltonsche, also nicht Abelsche Gruppe ist, so muß P ein echter Teiler von R, d. h. verschieden von R sein, und es gibt mindestens zwei Elemente φ, ψ, welche nicht miteinander permutabel

www.rcin.org.pl

und folglich auch nicht in P enthalten sind. Behalten wir für diese Elemente die Bezeichnungen unseres letzten Satzes IV bei, und setzen wir

$$\alpha = \varphi^{2r+1}, \quad \beta = \psi^{2s+1},$$

so ist

$$\alpha^4 = \beta^4 = 1,$$

und für den Kommutator ε der Elemente φ, ψ, welcher vom zweiten Grade ist, ergibt sich

$$\varepsilon = \alpha^2 = \beta^2, \quad \varepsilon^2 = 1;$$

wendet man ferner den Satz (23) auf das Beispiel $m = 2r + 1$, $n = 2s + 1$ an, so folgt

$$\beta\alpha = \alpha\beta\varepsilon,$$

d. h. ε ist auch der Kommutator der Elemente α, β, welche folglich nicht miteinander, wohl aber mit ε permutabel sind. Da nun aus der letzten Gleichung auch

$$\begin{aligned} \beta\alpha\beta &= \alpha\beta\varepsilon\beta = \alpha\beta^2\varepsilon = \alpha\varepsilon^2 = \alpha, \\ \alpha\beta\alpha &= \alpha^2\beta\varepsilon = \varepsilon\beta\varepsilon = \beta\varepsilon^2 = \beta \end{aligned}$$

folgt, so ergibt sich aus dem Vergleiche mit (15) in § 1, daß α, β die erzeugenden Elemente einer Quaterniongruppe Q sind. Es gilt daher der folgende Satz:

V. In jeder Hamiltonschen Gruppe R ist mindestens eine Quaterniongruppe Q als Teiler enthalten.

Wir untersuchen nun im folgenden die Beziehungen zwischen den beiden in R enthaltenen Gruppen P, Q, wobei wir für die letztere alle in § 1 benutzten Bezeichnungen beibehalten, und gelangen so zu der folgenden Reihe von Sätzen.

VI. Der Grad jedes nicht in P enthaltenen Elementes φ von R ist $\equiv 4$ (mod. 8).

Dies folgt unmittelbar aus IV, weil es mindestens ein mit φ nicht permutables Element ψ in R gibt.

VII. Das Quadrat jedes Elementes ω von R ist in P enthalten.

Denn wenn ω in P enthalten ist, so gilt dasselbe auch von ω^2, weil P eine Gruppe ist. Wenn aber das Element ω nicht in P enthalten ist, so ist nach VI sein Grad $\equiv 4$ (mod. 8), also der seines Quadrates $\equiv 2$ (mod. 4), woraus nach VI folgt, daß ω^2 in P enthalten ist, w. z. b. w.

www.rcin.org.pl

VIII. Jedes Element ω der Gruppe R ist permutabel mit wenigstens einem der drei Elemente α, β, γ der Gruppe Q, und zwar entweder nur mit einem einzigen oder mit allen dreien.

Ist nämlich ω nicht permutabel mit α, so muß das von α verschiedene Element $\omega^{-1}\alpha\omega = \alpha^{-1}$ sein, weil es bekanntlich denselben Grad 4 wie α hat und außerdem nach Satz I (in § 2) eine Potenz von α ist; ebenso muß, wenn dasselbe Element ω auch mit β nicht permutabel ist, $\omega^{-1}\beta\omega = \beta^{-1}$ sein; da nun $\gamma = \alpha\beta$ ist, so folgt hieraus

$$\omega^{-1}\gamma\omega = \omega^{-1}\alpha\beta\omega = \omega^{-1}\alpha\omega \cdot \omega^{-1}\beta\omega = \alpha^{-1}\beta^{-1} = \gamma,$$

also $\gamma\omega = \omega\gamma$, d. h. ω ist mit wenigstens einem der drei Elemente α, β, γ permutabel. Ist aber ω mit zweien von ihnen, z. B. mit α und mit β permutabel, so ist es auch mit deren Produkt γ, also mit allen dreien permutabel, w. z. b. w.

IX. Der Grad eines mit α, β, γ permutablen Elementes ω kann nicht durch vier teilbar sein, und der Inbegriff aller dieser Elemente ω ist die Gruppe P.

Den ersten Teil dieses Satzes beweisen wir auf indirektem Wege, indem wir annehmen, der Grad eines mit α, β (also auch mit γ) permutablen Elementes ω sei teilbar durch vier. Dann gibt es unter den Potenzen von ω, welche alle ebenfalls mit α, β permutabel sind, auch zwei Elemente vierten Grades ϱ (und ϱ^{-1}); nach der Fundamentaleigenschaft I der Hamiltonschen Gruppe R ist nun $\beta^{-1}(\varrho\alpha)\beta$ eine Potenz $(\varrho\alpha)^n$ von $\varrho\alpha$; weil aber ϱ permutabel mit β ist, so folgt $\beta^{-1}(\varrho\alpha)\beta = \varrho\beta^{-1}\alpha\beta = \varrho\alpha^{-1}$, und weil ϱ permutabel mit α ist, so folgt $(\varrho\alpha)^n = \varrho^n\alpha^n$; mithin ist $\varrho\alpha^{-1} = \varrho^n\alpha^n$, also $\varrho^{1-n} = \alpha^{1+n}$. Daß dies aber unmöglich ist, ergibt sich, wenn man die vier Fälle $n \equiv 0, 1, 2, 3 \pmod 4$ durchgeht; im ersten und dritten Falle wäre nämlich $\varrho = \alpha$, was dem Umstande widerspricht, daß β mit ϱ, aber nicht mit α permutabel ist; im zweiten oder vierten Fall wäre $1 = \alpha^2$ oder $\varrho^2 = 1$, während doch α und ϱ vom vierten Grade sind. Unsere obige Annahme führt daher zu einem Widerspruch, und folglich ist der erste Teil des Satzes bewiesen. Es muß daher jedes mit α, β, γ permutable Element ω in der Gruppe P enthalten sein, weil nach Satz VI der Grad eines jeden, in P nicht enthaltenen Elementes durch vier teilbar ist, und da

www.rcin.org.pl

umgekehrt jedes Element der Gruppe P zufolge ihrer Definition mit α, β, γ permutabel ist, so ergibt sich auch der zweite Teil des Satzes, w. z. b. w.

X. Der Inbegriff aller derjenigen Elemente ω, welche nur mit α, nicht mit β, γ permutabel sind, ist der Komplex $P\alpha$.

Der Grad eines solchen Elementes ω, welches nicht mit β permutabel, also auch nicht in der Gruppe P enthalten ist, hat nach Satz IV die Form $8p + 4$, und zufolge (41) wird der Kommutator der beiden Elemente ω, β durch die Potenzen

$$\omega^{4p+2} = \beta^2 = \varepsilon = \alpha^2$$

dargestellt; wenn ferner ω mit α, also auch mit α^{-1} permutabel ist, so folgt hieraus

$$(\omega\alpha^{-1})^{4p+2} = \omega^{4p+2}\alpha^{-(4p+2)} = \alpha^2\alpha^{-2} = 1;$$

mithin ist der Grad des Elementes $\omega\alpha^{-1}$ nicht teilbar durch vier, und hieraus folgt nach Satz VI, daß dieses Element in P, also ω in dem Komplex $P\alpha$ enthalten ist. Umgekehrt, wenn $\omega = \pi\alpha$ irgendein Element in $P\alpha$, also π mit allen Elementen permutabel ist, so ist $\omega\alpha = \pi\alpha^2 = \alpha\omega$, ferner $\omega\beta = \pi\alpha\beta$, und

$$\beta\omega = \beta\pi\alpha = \pi\beta\alpha = \pi\alpha\beta\varepsilon = \omega\beta\varepsilon;$$

mithin ist jedes Element ω in $P\alpha$ permutabel mit α, aber nicht permutabel mit β, w. z. b. w.

XI. Jede Hamiltonsche Gruppe R ist von der Form

$$R = PQ = P + P\alpha + P\beta + P\gamma, \tag{42}$$

wo Q eine in R enthaltene Quaterniongruppe

$$Q = (1 + \varepsilon)(1 + \alpha + \beta + \gamma), \tag{43}$$

und P die Abelsche Gruppe der mit allen Elementen von R permutablen Elemente bedeutet; diese Gruppe P enthält kein einziges Element vierten Grades, wohl aber das in Q befindliche Element zweiten Grades ε, welches zugleich der Kommutator von je zwei nicht permutablen Elementen der Gruppe R ist.

Denn aus den drei vorhergehenden Sätzen folgt, daß jedes Element ω der Gruppe R in einem, und nur in einem der vier Komplexe P, $P\alpha$, $P\beta$, $P\gamma$ enthalten ist; die Behauptungen über P folgen aus IX und VII, weil $\varepsilon = \alpha^2$ ist. Da endlich die Elemente

www.rcin.org.pl

von P mit allen Elementen von R, ferner die Elemente von $P\alpha$ nach X mit α und folglich auch mit allen Elementen desselben Komplexes $P\alpha$ permutabel sind, so gehören zwei nicht permutable Elemente auch zwei verschiedenen der drei Komplexe $P\alpha$, $P\beta$, $P\gamma$ an; wählt man nun z. B. aus $P\alpha$, $P\beta$ nach Belieben die beiden Elemente $\varphi' = \pi'\alpha$, $\varphi'' = \pi''\beta$, wo also π', π'' in P enthalten sind, so ergibt sich

$$\varphi'\varphi'' = \pi'\pi''\alpha\beta, \quad \varphi''\varphi' = \pi'\pi''\beta\alpha = \pi'\pi''\alpha\beta\varepsilon = \varphi'\varphi''\varepsilon,$$

mithin sind diese Elemente φ', φ'' nicht permutabel, und ihr Kommutator ist $= \varepsilon$, w. z. b. w.

XII. Wenn in einer Gruppe G eine Quaterniongruppe Q und eine Abelsche Gruppe P enthalten ist, deren Elemente mit denen von Q permutabel sind, wenn ferner P das in Q befindliche Element zweiten Grades ε, aber kein einziges Element vierten Grades enthält, so ist das Produkt PQ eine Hamiltonsche Gruppe R.

Aus der Permutabilität der Elemente von P mit denen von Q folgt zunächst, daß PQ eine Gruppe R ist; wählt man für Q wieder die bisherige Bezeichnung (43), so ist R von der Form (42), weil die Periode $[\varepsilon] = 1 + \varepsilon$ der größte gemeinsame Teiler von P, Q ist. Daß R keine Abelsche Gruppe ist, folgt daraus, daß ihre Elemente α, β nicht permutabel sind. Um zu zeigen, daß R eine Hamiltonsche Gruppe ist, haben wir nach Satz I in § 2 für je zwei Elemente φ, ψ nachzuweisen, daß $\varphi^{-1}\psi\varphi$ eine Potenz von ψ ist. Wenn nun wenigstens eins dieser beiden Elemente in P enthalten ist, oder wenn sie beide demselben Komplex $P\alpha$ oder $P\beta$ oder $P\gamma$ angehören, so sind sie permutabel, und folglich ist $\varphi^{-1}\psi\varphi = \psi$. Wenn aber z. B. $\psi = \pi\alpha$ in $P\alpha$, und $\varphi = \pi'\beta$ in $P\beta$ enthalten ist, so wird

$$\varphi^{-1}\psi\varphi = \beta^{-1}\pi\alpha\beta = \pi\beta^{-1}\alpha\beta = \pi\alpha^{-1};$$

da nun der Grad von π nicht durch vier teilbar ist, weil sonst unter den (in P enthaltenen) Potenzen von π auch zwei Elemente vierten Grades wären, so ist der Grad von π^2 eine ungerade Zahl $2m+1$, also $\pi^{-(4m+1)} = \pi$, mithin $\varphi^{-1}\psi\varphi = \pi\alpha^{-1} = \psi^{-(4m+1)}$, w. z. b. w.

Hiermit ist das am Schlusse der Einleitung ausgesprochene Resultat der Untersuchung in allen Teilen begründet.

Braunschweig, 9. August 1896.

---

www.rcin.org.pl

Erläuterungen zur vorstehenden Abhandlung.

Weitere Untersuchungen über die Struktur der Hamiltonschen Gruppen verdankt man G. A. Miller (Comptes rendus, Paris **126** (1898), S. 1406—1408; Bull. Amer. Math. Soc. **4** (1898), S. 510—515; **5** (1899), S. 292—296) und d'Alessandro (Giorn. di Matematica **37**). In anderer Weise hat E. Wendt einige der Millerschen Resultate abgeleitet (Math. Ann. **59** (1904), S. 187—192; **60** (1905), S. 319—320). Verallgemeinerungen der Hamiltonschen Gruppen studierten Miller (Math. Ann. **60** (1905), S. 597—606; Arch. d. Math. u. Phys. (3) **11** (1907), S. 76—79; Transactions Amer. Math. Soc. **8** (1907), S. 25—29) und Wendt (Math. Ann. **62** (1906), S. 381—400).

Die wichtigsten Eigenschaften der Kommutatoren und Kommutatorgruppen hat Dedekind schon 1880 erkannt und brieflich an Frobenius mitgeteilt. (Man vergleiche die Abhandlung von Frobenius, Sitzungsber. d. Berl. Akad. 1896, S. 1343—1382, § 2.) Publiziert ist aber der Satz in der Fußnote S. 93 zuerst von G. A. Miller (Quarterly Journ. of Math. **28** (1896), S. 232—284).

Über die auf S. 91 erwähnte Beziehung zwischen Quaternionen und Quaternionengruppen hat Dedekind nichts weiteres plubliziert. Die Bemerkung bezieht sich, wie aus den im Nachlaß veröffentlichten Briefen an Frobenius klar hervorgeht, auf die im Februar 1886 entdeckte Gruppendeterminante und ihre Zerlegung, die Dedekind im Quaternionenfall vollständig durchgeführt hatte. Auch die Konstruktion der Quaternionkörper wird im Nachlaß gebracht (XXXIX).

Die Bestimmung aller Gleichungen mit Quaternionengruppe ist von Mertens. und zwar für beliebige Grundkörper durchgeführt worden (Sitzungsber. d. Wien. Akad. **111** (1902), Abt. IIa, S. 17—37; **125** (1916), Abt. IIa, S. 735—740; **130** (1921), Abt. IIa, S. 69—90). Man vgl. auch die Abhandlung von G. Bucht (Ark. för Math. Astr. och Phys. **6** (1911), Nr. 30).

Ore.

www.rcin.org.pl