LXI.

Aus den Gruppen-Studien (1855—1858).

Komposition.

Ist m eine positive Zahl, so fragt sich, wie viele verschiedene Arten Gruppen M von m Objekten gibt es? —

Ist θ irgendein in M enthaltenes Objekt, so ist die Ordnung n von θ jedenfalls ein Divisor von m.

Umgekehrt, ist n irgendein Divisor von m, so fragt sich, wie viele Objekte θ von der Ordnung n sind in M enthalten? — Satz: Diese Anzahl ist jedenfalls ein Multiplum $\psi(n)\,\varphi(n)$ von der zahlentheoretischen Funktion $\varphi(n)$; (wo $\psi(n)$ auch $= 0$ sein kann, und im allgemeinen nicht eine vollständig bestimmte Funktion von n (wie $\varphi(n)$) bedeutet, sondern wesentlich von der Natur der Gruppe M abhängt). ...

Anwendbar auf Drehungen. Quaternions:

... III) $m = 8$; $1 + \psi(2) + 2\,\psi(4) + 4\,\psi(8) = 8$; da $\psi(8)$ wieder $= 0$ sein soll*), so bleibt $\psi(2) + 2\,\psi(4) = 7$; also a priori folgende Fälle:

1. $\psi(4) = 0$; $\psi(2) = 7$
2. $\psi(4) = 1$; $\psi(2) = 5$
3. $\psi(4) = 2$; $\psi(2) = 3$
4. $\psi(4) = 3$; $\psi(2) = 1$

... 4) $\psi(4) = 3$; $\psi(2) = 1$; es seien wieder θ, θ_1 zwei primitive Objekte 4ter Ordnung aus verschiedenen Systemen.

$$M = 1 + \theta + \theta^2 + \theta^3 + \theta_1 + \theta\,\theta_1 + \theta^2\,\theta_1 + \theta^3\,\theta_1$$

und also θ, θ^3, θ_1, $\theta\,\theta_1$, $\theta^2\,\theta_1$, $\theta^3\,\theta_1$ sämtlich von der vierten Ordnung, also

$$\theta_1^2 = \theta\,\theta_1\,\theta\,\theta_1 = \theta^2\,\theta_1\,\theta^2\,\theta_1 = \theta^3\,\theta_1\,\theta^3\,\theta_1 = \theta^2.$$

*) [D. h. der zyklische Fall soll ausgeschlossen sein. E. N.]

Also

$$\theta_1 = \theta\,\theta_1\,\theta = \theta^2\,\theta_1\,\theta^2 = \theta^3\,\theta_1\,\theta^3$$
$$\theta_1\,\theta = \theta^3\,\theta_1 \quad \text{und} \quad \theta_1^2 = \theta^2.$$

Dann lautet das Schema:

$$\begin{array}{cccccccccccccccc}
1 & + & \theta & + & \theta^2 & + & \theta^3 & + & \theta_1 & + & \theta\,\theta_1 & + & \theta^2\,\theta_1 & + & \theta^3\,\theta_1 \\
\theta & + & \theta^2 & + & \theta^3 & + & 1 & + & \theta^3\,\theta_1 & + & \theta_1 & + & \theta\,\theta_1 & + & \theta^2\,\theta_1 \\
\theta^2 & + & \theta^3 & + & 1 & + & \theta & + & \theta^2\,\theta_1 & + & \theta^3\,\theta_1 & + & \theta_1 & + & \theta\,\theta_1 \\
\theta^3 & + & 1 & + & \theta & + & \theta^2 & + & \theta\,\theta_1 & + & \theta^2\,\theta_1 & + & \theta^3\,\theta_1 & + & \theta_1 \\
\theta_1 & + & \theta\,\theta_1 & + & \theta^2\,\theta_1 & + & \theta^3\,\theta_1 & + & \theta^2 & + & \theta^3 & + & 1 & + & \theta \\
\theta\,\theta_1 & + & \theta^2\,\theta_1 & + & \theta^3\,\theta_1 & + & \theta_1 & + & \theta & + & \theta^2 & + & \theta^3 & + & 1 \\
\theta^2\,\theta_1 & + & \theta^3\,\theta_1 & + & \theta_1 & + & \theta\,\theta_1 & + & 1 & + & \theta & + & \theta^2 & + & \theta^3 \\
\theta^3\,\theta_1 & + & \theta_1 & + & \theta\,\theta_1 & + & \theta^2\,\theta_1 & + & \theta^3 & + & 1 & + & \theta & + & \theta^2.
\end{array}$$

Äquivalenz von Gruppen.

Es sei M eine Gruppe von m Objekten; jedem in M enthaltenen Objekt θ entspreche ein Objekt θ_1 in der Weise, daß jedem Produkt $\theta\,\varphi\,\psi\,..\,\lambda$ aus Objekten θ, φ, ψ, ..., λ, welche in M enthalten sind, das Produkt $\theta_1\,\varphi_1\,\psi_1\,..\,\lambda_1$ aus den entsprechenden Objekten θ_1, φ_1, ψ_1, .., λ_1 entspreche. Der Komplex der m_1 voneinander verschiedenen Objekte θ_1 werde mit M_1 bezeichnet.

Satz 1: Der Komplex M_1 ist eine Gruppe. — Beweis. Sind θ_1, φ_1 in M_1 enthalten, so gibt es in M (mindestens) ein θ, welchem θ_1, ferner (mindestens) ein φ, welchem φ_1 entspricht; dem $\theta\,\varphi$ entspricht $\theta_1\,\varphi_1$; folglich ist $\theta_1\,\varphi_1$ in M_1 enthalten.

Satz 2: Es sei θ irgendein Objekt der Gruppe M, welchem das Objekt θ_1 der Gruppe M_1 entspricht; alle n Objekte der Gruppe M, welchen ein und dasselbe θ_1 entspricht, können in die Form $\theta\,\varphi$ oder $\psi\,\theta$ gebracht werden, wo φ und ψ stets Objekte der Gruppe M sind. Dem $\theta\,\varphi$ entspricht nun $\theta_1\,\varphi_1 = \theta_1$, also ist $\varphi_1 = 1$; ebenso entspricht jedem $\psi\,\theta$ ein Objekt $\psi_1\,\theta_1 = \theta_1$, also ist auch $\psi_1 = 1$. Also entspricht sämtlichen n Objekten φ, sowie sämtlichen n Objekten ψ das Objekt 1 der Gruppe M_1. Umgekehrt ist φ ein Objekt von M, dem das Objekt 1 entspricht, so entspricht θ_1 sowohl $\theta\,\varphi$ als auch $\varphi\,\theta$. Der Komplex aller der n in M enthaltenen Objekte φ, denen das Objekt 1 entspricht, bildet eine Gruppe, und zwar einen eigentlichen Divisor von M; dann ist $m = m_1\,n$.

Satz 3: Man bezeichne mit N die Gruppe aller n in M enthaltenen Objekte, denen das Objekt 1 entspricht; so kann man

$$M = N + N\theta' + N\theta'' + \cdots + N\theta^{(m_1-1)}$$

setzen. Allen in einem Komplex $N\theta = \theta N$ enthaltenen n Objekten entspricht ein und dasselbe Objekt θ_1 der Gruppe M_1. Die m_1 Komplexe N, N', N'', .., $N^{(m_1-1)}$ gestatten bekanntlich wieder eine Komposition $N^{(p)} N^{(q)} = N^{(r)}$. Diese m_1 Komplexe bilden daher eine Gruppe von m_1 Objekten, und offenbar entspricht jedem Komplex $N^{(p)}$ ein Objekt $\theta_1^{(p)}$ der Gruppe M_1 in der Weise, daß jedem Produkte $N^{(p)} N^{(q)}$ das Objekt $\theta_1^{(p)} \theta_1^{(q)}$ der Gruppe M_1 entspricht. Und jedem Objekte θ_1 der Gruppe M_1 entspricht ein Komplex $N\theta = \theta N$, aber auch nur einer.

Definitionen: Von zwei Gruppen wie M und M_1 wollen wir sagen: die Art von M_1 ist unter der Art von M enthalten, die Art von M enthält die Art von M_1. — Ist daher N ein eigentlicher Divisor von $M = N + N' + \cdots$, so ist die Art der Gruppe der Komplexe N, N', etc. unter der Art von M enthalten. — Enthalten die Arten zweier Gruppen M und M_1 sich gegenseitig, so sollen diese beiden Gruppen äquivalent oder von derselben Art heißen. — Zwei äquivalente Gruppen haben stets denselben Grad; jedem Divisor der einen entspricht ein äquivalenter Divisor der andern. Sind zwei Gruppen einer dritten äquivalent, so sind sie untereinander äquivalent. — Sind M und M_1 äquivalent, so entspricht jedem in M enthaltenen Objekt θ ein in M_1 enthaltenes Objekt θ_1 auf die angegebene Weise; wir sagen, daß M durch die Substitution $S = \begin{pmatrix} 1, & \theta, & \theta', & \cdots \\ 1, & \theta_1, & \theta_1', & \cdots \end{pmatrix}$ in M_1 übergeht. Durch wieviel verschiedene Substitutionen geht M in M_1 über? Es sei T_1 das Symbol für alle Substitutionen, durch welche M_1 in sich selbst übergeht, S eine bestimmte Substitution, durch welche M in M_1 übergeht, so geht M durch sämtliche Substitutionen ST_1 in M_1 über; ebenso durch TS. Umgekehrt jede Substitution, durch welche M in M_1 übergeht, ist sowohl in der Form ST_1 als in der Form TS enthalten; denn bringt man, was immer und (für ein bestimmtes S) nur auf eine einzige Weise möglich ist, eine solche Substitution auf die Formen ST_1' und $T'S$, so folgt, daß M_1 durch T_1' in M_1, M durch T' in M übergeht. — Es fragt sich also, durch wieviel Substitutionen T geht eine Gruppe M in sich selbst über?

Die Substitutionen T beziehen sich auf die m Objekte der Gruppe M (Permutationen), lassen aber alle das Objekt 1 ungeändert. Der Komplex aller Substitutionen T bildet eine Gruppe. Der Komplex aller Objekte der Gruppe M, welche durch sämtliche Substitutionen T ungeändert bleiben, bildet eine Gruppe. — Eine reguläre Gruppe vom Grade m ist auf $\varphi(m)$ Arten sich selbst äquivalent. —

Satz ?: Ist M eine Gruppe von m Objekten, und p eine in m aufgehende Primzahl, so enthält M jedenfalls ein Objekt $p$ter Ordnung. —

Versuch zu einem Beweise. Gesetzt der Satz wäre falsch, so muß es einen kleinsten Grad $m \geqq 6$ geben, für welchen er falsch ist, so daß er für alle Gruppen von kleinerm Grade als m richtig ist. Dann sei M eine Gruppe vom Grade m, welche kein Objekt p^{ter} Ordnung enthält, obgleich p eine in m aufgehende Primzahl ist. Man kann $m = p^{\omega}.n$ setzen, wo n nicht durch p teilbar ist; n kann nicht $= 1$ sein, weil die Richtigkeit des Satzes für $m = p^{\omega}$ einleuchtet.

Der Grad $k < m$ einer jeden Gruppe $K < M$, welche ein Divisor von M ist, muß ein Divisor von n sein; denn dieser Grad k ist jedenfalls ein Divisor von $m = p^{\omega}.n$, wäre er aber teilbar durch p, so wäre, da K auch kein Objekt p^{ter} Ordnung enthalten kann, der Satz auch für $k < m$ falsch. Die Ordnung eines jeden in M enthaltenen Objekts ist ein Divisor von n. Ist δ irgendein Divisor von n, $\psi(\delta)$ die Anzahl der regulären Gruppen vom Grade δ, so ist

$$\sum \psi(\delta)\varphi(\delta) = p^{\omega}.n; \quad \sum \varphi(\delta) = n.$$

Ist nun K irgendein Divisor von M (von einem Grade $1 < k < m$, solche gibt es), und H der Komplex aller in M enthaltenen Objekte φ, für welche $\varphi^{-1}K\varphi = K$ ist; so ist H eine Gruppe, Divisor von M, und eigentliches Multiplum von K; der Grad h von H ist entweder $= m$, wenn K eigentlicher Divisor von M, oder ein Divisor von n, wenn K uneigentlicher Divisor von M ist. Es sei $m = \mu h$, $h = \nu k$.

Ist nun 1) $K < M$ eigentlicher Divisor von M, also $h = m$, $\mu = 1$, ν teilbar durch p^{ω}; $m = \nu k$; so zerfällt M in ν Komplexe

$$M = K + K_1 + \cdots + K_{\nu-1},$$

welche kompositionsfähig sind ($K_\alpha K_\beta = K_\gamma$) und so eine Gruppe vom Grade ν bilden. Da $\nu < m$, so enthält diese Gruppe mindestens einen Komplex p^{ter} Ordnung $K_1 = K\varphi = \varphi K$, so daß $K_1^p = K$; es muß also φ^p die niedrigste Potenz von φ in K enthalten sein; dann ist die Ordnung von φ ein Multiplum von p; folglich enthielte M doch auch Objekte von der p^{ten} Ordnung.

Hieraus folgt, daß M außer 1 und sich selbst nur uneigentliche Divisoren enthalten kann.

Es ist also für jeden (von 1 und M verschiedenen) Divisor K von M:

$h \geqq k$ ein Divisor von n; μ teilbar durch p^ω; $\nu \geqq 1$; $\mu < m$.

Die Anzahl μ der voneinander verschiedenen mit K konjugierten Gruppen ist daher stets teilbar durch p^ω. Ist daher $\delta' > 1$ ein Divisor von n, so ist auch $\psi(\delta')$ teilbar durch p^ω. Also wäre

$$p^\omega . n = \sum \psi(\delta)\varphi(\delta) = 1 + \sum' \psi(\delta')\varphi(\delta') = 1 + p^\omega \times x,$$

was unmöglich ist.

Also ist der Satz bewiesen.

Sätze über Gruppen M, deren Grade m Potenzen p^ω einer Primzahl p sind.

Bezeichnet $\psi(p^\alpha) = \psi_\alpha$ die Anzahl der regulären Gruppen vom Grade p^α, welche Divisoren von M sind, so ist

$$\psi_0 . \varphi(1) + \psi_1 \varphi(p) + \cdots + \psi_\alpha \varphi(p^\alpha) + \cdots + \psi_\omega \varphi(p^\omega) = p^\omega$$

oder, da $\psi_0 = 1$ und $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ ist,

$$\psi_1 + p\psi_2 + \cdots + p^{\alpha-1}\psi_\alpha + \cdots + p^{\omega-1}\psi_\omega = \frac{p^\omega - 1}{p-1}$$
$$= 1 + p + \cdots + p^{\omega-1}.$$

Ist ferner $\psi_\alpha = 0$, so ist auch $\psi_{\alpha+1} = \psi_{\alpha+2} = \text{etc.} = 0$; offenbar kann ψ_1 nie $= 0$ sein, weil $\psi_1 \equiv 1 \pmod p$; ist ferner ψ_ω von Null verschieden, so ist $\psi_1 = \psi_2 = \cdots = \psi_\omega = 1$, also die Gruppe regulär, und umgekehrt.

Gesetzt nun $\overset{\alpha}{P}$ ist ein regulärer Divisor von dem Grade p^α, und $\overset{\alpha}{\mathfrak{P}}$ der Komplex aller in M enthaltenen Objekte φ, für welche $\varphi^{-1}\overset{\alpha}{P}\varphi$

$= \overset{\alpha}{P}$ ist, so ist $\overset{\alpha}{\mathfrak{P}}$ eine Gruppe, ein Divisor von M, und ein Multiplum von $\overset{\alpha}{P}$; der Grad von $\overset{\alpha}{\mathfrak{P}}$ ist daher $= p^{\alpha+\varepsilon}$, worin ε die Werte 0, 1, 2, .. $(\omega - \alpha)$ haben kann; dann ist die Anzahl der voneinander verschiedenen mit $\overset{\alpha}{P}$ konjugierten Gruppen $= p^{\omega-\alpha-\varepsilon}$. Man kann daher setzen

$$\psi_\alpha = (\alpha, 0) + p(\alpha, 1) + \cdots + p^{\omega-\alpha-\varepsilon}(\alpha, \omega-\alpha-\varepsilon) + \cdots + p^{\omega-\alpha}(\alpha, \omega-\alpha),$$

und hierin bedeutet (α, λ) die Anzahl der Systeme von konjugierten regulären Gruppen vom Grade p^α, deren jedes aus p^λ konjugierten Gruppen besteht. Man kann daher

$$(1,0) + p\{(1,1) + (2,0)\} + p^2\{(1,2) + (2,1) + (3,0)\} + \text{etc.} = \frac{p^\omega - 1}{p - 1}$$

setzen. Da also $(1,0) \equiv 1 \pmod{p}$ ist, so kann (1,0) nicht Null sein. Mithin existiert stets mindestens eine (reguläre) Gruppe p^{ten} Grades

$$P = 1 + \theta + \theta^2 + \cdots + \theta^{p-1},$$

welche eigentlicher Divisor von M ist, so daß $\varphi^{-1} P \varphi = P$, wenn φ in M enthalten ist; man kann daher für jedes solche φ setzen

$$\varphi^{-1}\theta\varphi = \theta^n, \quad \varphi^{-2}\theta\varphi^2 = \varphi^{-1}\theta^n\varphi = (\varphi^{-1}\theta\varphi)^n = (\theta^n)^n = \theta^{n^2},$$

$$\text{allgemein} \quad \varphi^{-k}\theta\varphi^k = \theta^{n^k};$$

da nun $\varphi^{p^\omega} = 1$ ist, so folgt für $k = p^\omega$, daß $\theta = \theta^{n^{p^\omega}}$, also $n^{p^\omega} \equiv 1 \pmod{p}$, also auch $n \equiv 1 \pmod{p}$, also $\varphi^{-1}\theta\varphi = \theta$; also ist θ permutabel mit jedem in M enthaltenen Objekt φ.

Reziprozität.

Es seien $A = \sum^a \alpha$ und $B = \sum^b \beta$ Divisoren von $S = \sum^s \sigma$

$$s = am, \quad s = bn; \quad am = bn = s$$

und es sei

$C = \sum^c \gamma$ der größte gem. Div. von A und B

$$a = c\nu, \quad b = c\mu; \quad t = m\nu = n\mu; \quad \frac{\mu}{m} = \frac{\nu}{n}.$$

Sind φ, ψ irgend zwei in S enthaltene Objekte, so haben die Komplexe $A\varphi$, $B\psi$ entweder gar keine gemeinschaftlichen Objekte, oder sie haben solche $\alpha\varphi = \beta\psi = \theta$; dann ist auch

$$\gamma\alpha\varphi = \gamma\beta\psi = \gamma\theta$$

sowohl in $A\varphi$ als auch in $B\psi$ enthalten, und umgekehrt: ist $\sigma\theta$ in $A\varphi$ und in $B\psi$ enthalten, so ist $\sigma\alpha$ in A, $\sigma\beta$ in B, folglich σ in A und B enthalten, also $\sigma = \gamma$.

Also $A\varphi$ und $B\psi$ haben entweder gar kein gemeinschaftliches Objekt, oder sie haben c gemeinschaftliche Objekte $C\theta$.

Es sei

$$A = C + C\alpha_1 + \cdots + C\alpha_{\nu-1}; \quad B = C + C\beta_1 + \cdots + C\beta_{\mu-1},$$

so ist

$C\alpha_{\nu'}$ der gleichzeitig in A und $B\alpha_{\nu'}$ enthaltene Komplex,

$C\beta_{\mu'}$ „ „ „ $A\beta_{\mu'}$ und B enthaltene Komplex,

mithin sind

$$A,\ A\beta_1,\ \ldots,\ A\beta_{\mu-1} \qquad \mu \leqq m$$

voneinander verschiedene Komplexe, und ebenso

$$B,\ B\alpha_1,\ \ldots,\ B\alpha_{\nu-1} \qquad \nu \leqq n$$

voneinander verschiedene Komplexe.

$$\begin{array}{l|l}
A = C + C\alpha_1 + \cdots + C\alpha_{\nu-1} & B = C + C\beta_1 + \cdots + C\beta_{\mu-1} \\
A\beta_1 = C\beta_1 + C\alpha_1\beta_1 + \cdots + C\alpha_{\nu-1}\beta_1 & B\alpha_1 = C\alpha_1 + C\beta_1\alpha_1 + \cdots + C\beta_{\mu-1}\alpha_1 \\
\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\
A\beta_{\mu-1} = C\beta_{\mu-1} + C\alpha_1\beta_{\mu-1} + \cdots + C\alpha_{\nu-1}\beta_{\mu-1} & B\alpha_{\nu-1} = C\alpha_{\nu-1} + C\beta_1\alpha_{\nu-1} + \cdots + C\beta_{\mu-1}\alpha_{\nu-1}.
\end{array}$$

Es gehöre x zu der Gruppe A, y zu der Gruppe B, z zur Gruppe C. Den Komplexen A, $A\beta_1$, …, $A\beta_{\mu-1}$ korrespondieren die Wurzeln x, x_1, …, $x_{\mu-1}$ einer in bezug auf y rationalen und irreduktibeln Gleichung.

Es sei $A\beta'$ ein von den vorigen verschiedener Komplex, welchem die Wurzel x' korrespondiert; es sei C' der größte gem. Div. von $\beta'^{-1}A\beta'$ und B

$$B = C' + C'\beta_1' + \cdots + C'\beta_{\mu'-1}'.$$

Erläuterungen zur vorstehenden Abhandlung.

Dedekind erwähnt diese Gruppenstudien in einem Brief an Frobenius 1895 (Bd. 2, S. 419). Die hier des historischen Interesses halber wiedergegebenen Stücke zeigen, wie vollständig Dedekind schon in dieser frühen Zeit im Besitz von Begriffen und Methoden der abstrakten Gruppentheorie war.

Mit der im ersten Stück angegebenen Methode sind alle Gruppen bis zur zehnten Ordnung einschließlich aufgestellt; wie das angegebene Beispiel zeigt, war Dedekind so schon damals zur Quaternionengruppe gelangt. Das scheint er später vergessen zu haben, wie eine Äußerung in einem Brief an Frobenius (Bd. 2, S. 440) zeigt.

Die „Äquivalenz von Gruppen“ gibt eine so scharfe Herausarbeitung des „Homomorphiesatzes“, wie sie erst in neuester Zeit wieder üblich geworden ist.

Das nächste Stück enthält den im Brief von 1895 an Frobenius erwähnten Satz, arbeitet wesentlich mit dem Begriffe des Normalisators.

Auf ähnlichen Überlegungen beruht auch der folgende Beweis, daß eine Gruppe von Primzahlpotenzgrad auflösbar ist.

An die im letzten Stück — Reziprozität — gegebene gegenseitige Reduktion von Körpern (oder Polynomen) schließt ausführlicher die Zerlegung einer Gruppe nach zwei Untergruppen an, die Dedekind später der Idealtheorie in Unterkörpern zugrunde gelegt hat (XXIV); dort erwähnt er auch den Zusammenhang mit der gegenseitigen Reduktion.

Noether.
