Zahlentheoretische Sätze aus der Gruppentheorie.

Von

A. Speiser in Zürich.

In den folgenden Zeilen wird ein System von Matrizen behandelt, das nach einem, von dem gewöhnlichen verschiedenen Gesetz der Matrizenkomposition eine Gruppe bildet. Satz 1 gibt vollständigen Aufschluß über die Natur derartiger Gruppen. § 2 enthält Anwendungen auf die Frage, welches der einfachste algebraische Körper ist, in dem eine Darstellung einer endlichen Gruppe von Matrizen (im gewöhnlichen Sinne) gegeben werden kann¹⁾. Wir zeigen u. a., daß dies für eine irreduzible Darstellung ungeraden Grades mit reellem Charakterensystem stets der Körper der Charaktere ist.

§ 1.

Gegeben sei ein algebraischer Körper K , der in dem Grundkörper k Galoissch ist und in diesem Bereich die Gruppe $\mathfrak{G}$ mit den Elementen $E, A, B, \dots, S, T, \dots$ besitzt.

Wir definieren nun eine Darstellung der Gruppe $\mathfrak{G}$ durch Matrizen nach einem von dem gewöhnlichen verschiedenen Gesetz der Zusammensetzung.

Definition: Jedem Element $E, A, B, \dots$ von $\mathfrak{G}$ sei eine Matrix

$$M_E, M_A, M_B, \dots$$

von nicht verschwindender Determinante zugeordnet, deren Koeffizienten in K liegen. Die konjugiert algebraischen Matrizen seien:

$$M_E^S, M_A^S, \dots \quad (S = E, A, B, \dots)$$

¹⁾ Über dieses Problem vgl. die grundlegende Abhandlung von Herrn I. Schur: *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen*, Berl. Ber. 1906, S. 164–184.

Diese Matrizen mögen folgendem Gruppengesetz gehorchen:

$$\mathfrak{U}: \quad M_S^T M_T = M_{ST}.$$

Man überzeugt sich leicht, daß das assoziative Gesetz erfüllt ist. Setzt man $S = E$, so ergibt sich:

$$M_E^T M_T = M_{ET} = M_T, \quad \text{also} \quad M_E = E = (e_{ik}), \quad e_{ik} = \begin{cases} 1 & (i = k) \\ 0 & (i \neq k) \end{cases}$$

Zunächst zeigen wir, daß es derartige Darstellungen gibt. Sei nämlich M eine Matrix in K mit von 0 verschiedener Determinante; setzt man

$$M_S = (M^S)^{-1} M, \quad (S = E, A, B, \dots)$$

so genügen diese Matrizen $M_E, M_A, M_B, \dots$ der Definition, denn es wird:

$$M_S^T M_T = ((M^S)^{-1} M)^T (M^T)^{-1} M = (M^{ST})^{-1} M = M_{ST}.$$

Zu jeder Gruppe lassen sich unendlich viele *äquivalente* angeben. Sei N eine beliebige Matrix in K , so bilden die Matrizen

$$M_E, (N^A)^{-1} M_A N, (N^B)^{-1} M_B N, \dots$$

wiederum eine Gruppe nach dem Gesetz $\mathfrak{U}$. Irgendeine Darstellung von $\mathfrak{G}$ im Grundkörper k bildet auch bei dieser Zusammensetzung eine Gruppe, denn der Übergang zu den konjugierten Matrizen bewirkt alsdann gar keine Veränderung. Insbesondere bildet die identische Darstellung, deren Matrizen sämtlich in der Einheitsmatrix bestehen, eine Gruppe nach $\mathfrak{U}$ und wir zeigen nun, daß jede Gruppe mit der identischen Darstellung äquivalent ist, d. h. wir beweisen den

Satz 1: *Bilden die Matrizen $M_E, M_A, \dots$ eine Gruppe nach der obigen Definition, so gibt es in K eine Matrix M dergestalt, daß*

$$M_S = (M^S)^{-1} M$$

ist.

Beweis: Wir bilden die Summe aller Matrizen

$$M_E + M_A + \dots = M.$$

Nach dem Gesetz der Zusammensetzung wird

$$M^S M_S = \sum_T M_T^S M_S = \sum_T M_{TS} = M.$$

Ist die Determinante von M von 0 verschieden, so ist unser Satz bereits bewiesen, denn aus der eben hingeschriebenen Formel folgt:

$$M_S = (M^S)^{-1} M.$$

Um den Satz allgemein zu beweisen, zeigen wir seine Richtigkeit für

den Fall, daß die Matrizen aus einer Zeile und Kolonne bestehen, also gewöhnliche Zahlen sind, und wenden dann vollständige Induktion an.

Wir bezeichnen also M_S mit α_S und verstehen unter β eine Zahl aus K , deren Diskriminante relativ zu k von 0 verschieden ist, und bilden nun die Zahlen:

$$\sum_S (\beta^S)^i \alpha_S = \omega^{(i)}. \quad (i = 0, 1, \dots)$$

Mindestens eine unter ihnen ist von 0 verschieden, andernfalls müßten alle $\alpha_S = 0$ sein. Sei $\omega^{(i)} \neq 0$, so wird

$$\alpha_T = (\omega^{(i)^T})^{-1} \omega^{(i)},$$

womit der Satz bewiesen ist.

Ein Spezialfall dieses eben bewiesenen Satzes ist Satz 90 im Zahlenbericht²⁾ von Hilbert: Jede ganze oder gebrochene Zahl A eines relativ zyklischen Körpers, deren Relativnorm in bezug auf den Grundkörper gleich 1 ist, wird die symbolische $(1 - S)$ -te Potenz einer gewissen ganzen Zahl B . In der Tat sei der Relativgrad l , so bilden die Zahlen

$$1, A, A A^S, \dots, A A^S A^{S^2} \dots A^{S^{l-2}}$$

eine Gruppe nach der obigen Definition, und so wird

$$A = (B^S)^{-1} B.$$

Wir nehmen nun den Satz als bewiesen an für Matrizen mit weniger als n Zeilen und Kolonnen und zeigen seine Gültigkeit für die Anzahl n .

Sei wiederum β eine Zahl, deren Relativediskriminante von 0 verschieden ist, so bilden wir die Matrizen: $\sum_S (\beta^S)^i M_S = M^{(i)}$. Mindestens eine dieser Matrizen besitzt einen Koeffizienten links oben (mit dem Index $(1, 1)$), der von Null verschieden ist, denn M_E hat dort die Zahl 1 stehen. Die erste Zeile dieser Matrix bezeichnen wir mit

$$\omega_1, \omega_2, \dots, \omega_n.$$

Die Matrix M , zu der diese Zeile gehört, genügt der Gleichung:

$$(1) \quad M^S M_S = M.$$

Dies läßt sich in folgender Weise interpretieren:

Man bilde die Form:

$$\omega_1 x_1 + \omega_2 x_2 + \dots + \omega_n x_n.$$

²⁾ Jahresbericht der Deutsch. Mathem. Vereinigung, 4 (1897), S. 272.

Geht man zu einer konjugierten Form über:

$$\omega_1^S x_1 + \omega_2^S x_2 \quad \dots \quad \omega_n^S x_n$$

und übt alsdann auf die Variablen $x_1, x_2, \dots, x_n$ die Substitution M_S aus, so gelangt man zur ursprünglichen Form zurück. In der Tat.

$$\omega_1, \omega_2, \dots, \omega_n$$

ist die erste Zeile von M . Eine Substitution auf die Variablen $x_1, \dots, x_n$ ist gleichbedeutend mit der transponierten Substitution auf die Koeffizienten $\omega_1, \dots, \omega_n$. Die Gleichung (1) besagt, daß die erste Zeile von M^S durch die transponierte Substitution zu M_S übergeht in die erste Zeile von M .

Wir bilden nun die n Linearformen:

$$\begin{aligned} \omega_1 x_1 + \dots + \omega_n x_n &= y_1, \\ x_2 &= y_2, \\ \Omega: \quad &\dots\dots\dots \\ x_n &= y_n. \end{aligned}$$

Übt man auf die Variablen x die Substitution M_S aus, nachdem man die Formen ersetzt hat durch

$$\omega_1^S x_1 \quad \dots + \omega_n^S x_n, \quad x_2, \dots, x_n,$$

so bleibt y_1 ungeändert, während die anderen eine lineare Substitution erfahren.

Transformiert man also die Gruppe $M_E, M_A, \dots$ durch Ω , so werden die Matrizen $(\Omega^S)^{-1} M_S \Omega = M'_S (S \quad E, A, B, \dots)$ wiederum eine Gruppe von der verlangten Art bilden, aber in der reduzierten Form erscheinen:

$$M'_S = \begin{pmatrix} 1 & 0 \\ P_S & N_S \end{pmatrix},$$

wobei P_S eine Spalte von $n - 1$ Koeffizienten und N_S eine Matrix von $n - 1$ Zeilen und Kolonnen bedeuten. Nun bilden offenbar die Matrizen $N_S (S = E, A, B, \dots)$ für sich eine Gruppe und nach Voraussetzung ist sie mit der identischen äquivalent:

$$N_S = (N^S)^{-1} N.$$

Transformiert man die Gruppe mit der Matrix $\begin{pmatrix} 1 & 0 \\ 0 & N^{-1} \end{pmatrix}$, so erhält man wiederum eine äquivalente Gruppe:

$$M''_S = \begin{pmatrix} 1 & 0 \\ 0 & N^S \end{pmatrix} M'_S \begin{pmatrix} 1 & 0 \\ 0 & N^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \dots 0 \\ \alpha_2 & 1 & 0 \dots 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_n & 0 & 0 & \dots 1 \end{pmatrix}$$

und diese Gruppe läßt sich nach der am Anfang des Beweises gegebenen Methode behandeln, die Summe aller Matrizen M_S'' besitzt eine von 0 verschiedene Determinante. Daher ist M_S'' und also auch M_S selbst mit der identischen Darstellung äquivalent, q. e. d.

§ 2.

Wir zeigen nun die Anwendungen, die sich von diesem Satz machen lassen auf das Problem des kleinsten, für eine Substitutionsgruppe notwendigen Zahlkörpers.

Sei Γ eine irreduzible Substitutionsgruppe, deren Koeffizienten dem Galoisschen Zahlkörper K angehören. Der Charakter von Γ möge den Galoisschen Körper k bestimmen. Die Gruppe von K in k sei $\mathfrak{G}$ mit den Elementen $E, A, B, \dots$. Dann sind die sämtlichen relativ konjugierten Darstellungen $\Gamma' = \Gamma^E, \Gamma^A, \Gamma^B, \dots$ äquivalent. Wir bezeichnen mit M_S diejenige Substitution, welche Γ^S in Γ transformiert:

$$M_S^{-1} \Gamma^S M_S = \Gamma.$$

M_S ist alsdann bestimmt bis auf einen Faktor, d. h. bis auf eine multiplikative Matrix aE und das System der M_S ($S = E, A, B, \dots$), bildet bis auf derartige Faktoren eine Gruppe von der in der Definition beschriebener Art. Angenommen, man kann die Matrizen so normieren, daß sie der Definition vollständig genügen, so wird nach Satz 1 $M_S = (M^S)^{-1} M$. Nun bilde man die Darstellung $M \Gamma' M^{-1}$, die mit Γ' äquivalent ist. Die konjugierten Darstellungen werden jetzt:

$$M^S \Gamma^S (M^S)^{-1}, \quad (S = E, A, B, \dots)$$

Nun ist aber

$$\Gamma' = M_S^{-1} \Gamma^S M_S = ((M^S)^{-1} M)^{-1} \Gamma^S (M^S)^{-1} M.$$

Daher wird

$$M \Gamma' M^{-1} = M^S \Gamma^S (M^S)^{-1}.$$

Die Darstellung $M \Gamma' M^{-1}$ ändert sich nicht beim Übergang zu den konjugierten, d. h. sie liegt im Grundkörper k . Unsere Methode gibt uns sogar die Substitution, welche Γ' in die Darstellung im Grundkörper überführt. Auf diesem Weg beweisen wir nun den

Satz 2: Wenn eine (irreduzible) Gruppe von ungeradem Grade reelle Charaktere besitzt, so läßt sie sich so transformieren, daß ihre Koeffizienten in dem durch den Charakter bestimmten Körper liegen.

Beweis: Weil das Charakterensystem reell und der Grad ungerade ist, so besitzt Γ bekanntlich eine quadratische Form, die invariant ist.

Diese kann man auf die Gestalt $x_1^2 + \dots + x_n^2$ transformieren durch Einführung gewisser weiterer algebraischer Irrationalitäten. Wir können

also von vornherein annehmen, daß I' orthogonal ist. Dasselbe gilt dann von den konjugierten Darstellungen I'^S . Aus $I' = M_S^{-1} I'^S M_S$ folgt, daß auch diejenige Form die aus $x_1^2 + \dots + x_n^2$ durch die Substitution M_S entsteht, invariant ist unter I' . Nun sind aber $c(x_1^2 + \dots + x_n^2)$ die einzigen invarianten quadratischen Formen, daher muß die neue Form in dieser Gestalt enthalten sein. Aus dem bekannten Satz über die Determinanten quadratischer Formen folgt:

$$c^n = d^2,$$

wobei wir zur Abkürzung d gleich der Determinante von M_S setzen. Nun ist n ungerade, daher $\frac{n-1}{2}$ eine ganze Zahl und $d \cdot c^{-\frac{n-1}{2}} = e$ eine Zahl in K , die der Gleichung $e^n = d$ genügt.

Indem man M_S mit $\frac{1}{e}$ multipliziert, erhält man eine orthogonale Matrix, deren Determinante 1 ist.

Dadurch ist aber der multiplikative Faktor festgelegt, denn $x_1^2 + \dots + x_n^2$ bleibt nur bei den beiden Multiplikationen $x'_i = x_i$ und $x'_i = -x_i$ unverändert, die letztere hat die Determinante -1 , weil n ungerade ist. Wir denken uns nun alle Matrizen M_S in dieser Weise normiert, dann bilden sie, wie leicht ersichtlich, nach der Definition $\mathfrak{U}$ eine Gruppe.

Satz 3: *Wenn eine irreduzible Substitutionsgruppe von geradem Grade mit reellem Charakterensystem eine Substitution enthält, welche die charakteristische Wurzel $+1$ oder -1 in ungerader Vielfachheit besitzt, so läßt sie sich so transformieren, daß ihre Koeffizienten im Körper der Charaktere liegen.*

Beweis: Sei S diese Substitution und sei etwa $+1$ die Wurzel, die m -mal vorkommt (m ungerade). Dann läßt sich S so im Körper K transformieren, daß sie die Gestalt hat: $m \cdot 1 + S'$, d. h. daß in der Hauptdiagonalen erst m -mal die Zahl 1 steht, alsdann die Matrix S' mit $n - m$ Zeilen und Kolonnen folgt und der Rest aus 0 besteht. S' kann als orthogonale Matrix angenommen werden.

Nunmehr ist jede Matrix, welche $m \cdot 1 + S'$ in eine konjugierte $m \cdot 1 + \tilde{S}$ transformiert, *reduziert* und besteht aus zwei Bestandteilen, einem vom Grade m und einem vom Grade $n - m$. Denn zunächst gibt es gewiß eine solche und ferner ist jede mit ihr vertauschbare Matrix ebenfalls von dieser Beschaffenheit. Die Matrizen M_S zerfallen also in zwei Bestandteile von ungeradem Grade, die beide für sich eine Gruppe bilden. Daher läßt sich der Satz 2 anwenden.