Treue Darstellung Liescher Ringe.

Von *Ernst Witt* in Göttingen.

Ein *Liescher Ring* $\mathfrak{L}$ mit den Elementen $a, b, \ldots$ ist hinsichtlich der distributiven Multiplikation durch die Regeln

$$aa = 0, \qquad (ab)\,c + (bc)\,a + (ca)\,b = 0$$

gekennzeichnet. Es folgt

$$ab + ba = (a+b)\,(a+b) - aa - bb = 0.$$

In einem *assoziativen Ring* $\mathfrak{A}$ mit den Elementen $A, B, \ldots$ werde die Kommutatorbildung $A \circ B = AB - BA$ eingeführt. Mit dem neuen Verknüpfungszeichen $\circ$ bilden die Elemente aus $\mathfrak{A}$ einen Lieschen Ring.

Bei einer *Darstellung* des Lieschen Ringes $\mathfrak{L}$ im assoziativen Ring $\mathfrak{A}$ werden den Elementen a aus $\mathfrak{L}$ gewisse Elemente A aus $\mathfrak{A}$ zugeordnet, derart, daß $a + b$ und ab übergeht in $A + B$ bzw. $AB - BA$. Diese Darstellung heißt *treu*, wenn bei dieser Zuordnung nur die Null in Null übergeht.

Wir werden hier folgende Sätze beweisen:

Satz 1. *Es sei $\mathfrak{L}$ ein Liescher Ring mit dem Körper K als Operatorenbereich. Es gibt genau einen zugehörigen assoziativen Ring $\mathfrak{A}$, der folgende Eigenschaften aufweist:*

Der assoziative Ring $\mathfrak{A}$ enthält eine treue Darstellung (a) des Lieschen Ringes $\mathfrak{L}$ und wird von ihr erzeugt;

wenn irgendein assoziativer Ring $\mathfrak{a}$ eine Darstellung $\bar{a}$ des Lieschen Ringes $\mathfrak{L}$ enthält und von ihr erzeugt wird, so läßt sich der Ring in solcher Weise homomorph auf den Ring $\mathfrak{a}$ abbilden, daß dabei (a) in $\bar{a}$ übergeht.

Angeregt wurde diese Arbeit durch einen Vortrag von Magnus auf der Mathematikertagung in Bad Salzbrunn (September 1936). Magnus vermutete damals den

Satz 2. *Die durch Zuordnung s_i auf S_i entstehende Darstellung des freien Lieschen Ringes $\mathfrak{L}_q$ mit den q Erzeugenden s_i im freien assoziativen Ring $\mathfrak{A}_q$ mit den q Erzeugenden S_i ist treu.*

Satz 3. *Im freien Lieschen Ring bilden die homogenen Ausdrücke vom Grad n in den q Erzeugenden einen Modul Ψ_n vom Rang*

$$\psi_n = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{\frac{n}{d}}.$$

Die homogenen Ausdrücke vom Grad $n_1, \ldots, n_q$ in den Erzeugenden $s_1, \ldots, s_q$ bilden einen Modul $\Psi(n_1, \ldots, n_q)$ vom Rang

$$\psi(n_1, \ldots, n_q) = \frac{1}{n} \sum_{d \mid n_i} \frac{\mu(d)\, \frac{n}{d}\,!}{\frac{n_1}{d}\,! \cdots \frac{n_q}{d}\,!} \qquad (n = n_1 + \cdots + n_q).$$

Es ist merkwürdig, daß die erste Rangformel übereinstimmt mit der bekannten Gaußschen Formel für die Anzahl der Primpolynome $x^n + a_1x^{n-1} + \cdots + a_n$ im Galoisfeld von q Elementen. —

Wir werden zum Schluß noch einige Anwendungen auf die Gruppentheorie bringen. Für eine Gruppe $\mathfrak{G}$ erklären wir rekursiv die Normalteiler $\mathfrak{G}^n$ ($\mathfrak{G}^1 = \mathfrak{G}$): Es sei $\mathfrak{G}^n$ die von allen Kommutatoren $a\,a_{n-1}a^{-1}a_{n-1}^{-1}$ (a aus $\mathfrak{G}$ und a_{n-1} aus $\mathfrak{G}^{n-1}$) erzeugte Untergruppe.

Satz 4. *Für die freie Gruppe $\mathfrak{G}_q$ mit q Erzeugenden ist die Faktorgruppe $\mathfrak{G}_q^n/\mathfrak{G}_q^{n+1}$ isomorph mit der freien abelschen Gruppe von ψ_n Erzeugenden.*

1.

Beweis von Satz 1. Der Körper K sei Operatorenbereich des Lieschen Ringes $\mathfrak{L}$. Die Elemente von K und $\mathfrak{L}$ seien mit $\alpha, \beta, \ldots$ bzw. mit $a, b, \ldots$ bezeichnet. $\mathfrak{L}$ hat als K-Modul eine (wohl-)geordnete Basis $u_1, u_2, \ldots$ derart, daß sich jedes Element a auf genau eine Weise als endliche Summe $a = \Sigma\alpha_i u_i$ darstellen läßt.

(Wer das Auswahlpostulat vermeiden will, möge sich auf Liesche Ringe $\mathfrak{L}$ mit abzählbarer Basis beschränken. Zum Beweis von Satz 2 ist das auch vollständig genügend. Im nicht abzählbaren Fall müssen zur Numerierung der Basiselemente auch transfinite Ordnungszahlen verwendet werden.)

Wir führen den K-Modul $\mathfrak{A}$ ein, dessen Basiselemente die Klammersymbole

$$(u_{i_1}, \ldots, u_{i_r}) \qquad (i_1 \leqq \cdots \leqq i_r)$$

sind.

Hilfssatz. Innerhalb $\mathfrak{A}$ lassen sich allgemeinere Klammersymbole $(a_1, \ldots, a_r)$ erklären mit den Eigenschaften

I. $(\ldots, a, b, \ldots) - (\ldots, b, a, \ldots) = (\ldots, ab, \ldots)$,

II. $(a_1, \ldots, a_r)$ *ist linear in jeder Komponente.*

Für eingliedrige Klammersymbole (a) ist dies selbstverständlich.

Wir nehmen an, für $r < n$ seien schon allgemeine Klammersymbole $(a_1, \ldots, a_r)$ eingeführt. Es ist zu beweisen, daß innerhalb $\mathfrak{A}$ auch die Klammern $(a_1, \ldots, a_n)$ eindeutig so eingeführt werden können, daß I und II erfüllt ist.

Klammern $(a_1, \ldots, a_n)$ mit n Komponenten aus dem Lieschen Ring behandeln wir zunächst als Unbestimmte. Ferner seien $t_1, \ldots, t_{n-1}$ assoziative Unbestimmte. Wir führen Operatoren P_{t_i} und Q_{t_i} ein durch

$$(1) \qquad P_{t_i}(a_1, \ldots, a_i, a_{i+1}, \ldots, a_n) = (a_1, \ldots, a_{i+1}, a_i, \ldots, a_n),$$

$$(2) \qquad Q_{t_i}(a_1, \ldots, a_i, a_{i+1}, \ldots, a_n) = (a_1, \ldots, a_i\, a_{i+1}, \ldots, a_n),$$

und setzen für irgendein Produkt $A = t_\alpha t_\beta \cdots t_\delta$

$$(3a) \qquad P_{t_\alpha t_\beta \cdots t_\delta} = P_{t_\alpha} P_{t_\beta} \cdots P_{t_\delta}$$

und

$$(3b) \qquad Q_{t_\alpha t_\beta t_\gamma \cdots t_\delta} = Q_{t_\alpha} P_{t_\beta t_\gamma \cdots t_\delta} + Q_{t_\beta} P_{t_\gamma \cdots t_\delta} + \cdots + Q_{t_\delta}.$$

Es folgen die Regeln

$$(4) \qquad P_{AB} = P_A P_B \quad \text{und} \quad Q_{AB} = Q_A P_B + Q_B.$$

Es ist klar, daß für die Größen

$$(5) \qquad E = t_i^2, \quad (t_i t_{i-1})^3, \quad (t_i t_{i-\nu})^2 \qquad (\nu \geqq 2)$$

$P_E = 1$ ist. Wir zeigen jetzt, daß $Q_E = 0$ ist, und zwar berechnen wir der einfacheren Schreibweise halber für jeden Typus von E jeweils ein Beispiel.

Für $E = t_1^2$ ist $Q_E(a, b, *) = (ab, *) + (ba, *) = 0$.

Für $E = (t_2 t_1)^3$ ist $Q_E(a, b, c, *)$

$$= \underbrace{(ab, c, *) + (c, ba, *)}_{(ab \cdot c, *)} + \underbrace{(bc, a, *) + (a, cb, *)}_{(bc \cdot a, *)} + \underbrace{(ca, b, *) + (b, ac, *)}_{(ca \cdot b, *)} = 0.$$

Für $E = (t_3 t_1)^2$ ist $Q_E(a, b, c, d, *)$

$$= \underbrace{(ab, c, d, *) + (ba, d, c, *)}_{(ab, cd, *)} + \underbrace{(a, b, dc, *) + (b, a, cd, *)}_{(ab, dc, *)} = 0.$$

Aus $P_E = 1$ und $Q_E = 0$ folgt nach (4)

$$P_{AEB} = P_{AB} \quad \text{und} \quad Q_{AEB} = Q_{AB}, \tag{6}$$

in den Indizes von P und Q dürfen also solche E immer durch 1 ersetzt werden.

Nach E. H. Moore wird die symmetrische Gruppe $\mathfrak{S}_n$ der Ordnung $n!$ abstrakt durch die Relationen

$$(t_i t_k)^{m_{ik}} = 1, \qquad m_{ik} = \begin{cases} 3 & \text{für } i - k = \pm 1 \\ 2 & \text{sonst} \end{cases} \qquad (i, k = 1, \ldots, n-1) \tag{7}$$

geliefert [1]). Wir sind demnach berechtigt, die Indizes von P und Q als Elemente der symmetrischen Gruppe anzusehen. Überdies können wir die Permutationen P_π mit π identifizieren.

Wir gehen nun aus von einem Basiselement des Moduls $\mathfrak{A}$

$$U = (u_{i_1}, \ldots, u_{i_n}) \qquad (i_1 \leqq \cdots \leqq i_n). \tag{8}$$

Wenn $\pi \varepsilon U = \pi U$ ist ($\varepsilon \neq 1$), so ist $\varepsilon U = U$, d. h. einige i_ν sind einander gleich. Eine Permutation ε, welche die Klammer U nicht ändert, kann als Produkt von solchen Transpositionen t_i mit $t_i U = U$ dargestellt werden. Für diese t_i ist $Q_{t_i} U = 0$, daher ist auch $Q_\varepsilon U = 0$. So folgt schließlich $Q_{\pi\varepsilon} U = Q_\pi U$.

Demnach tritt auch im Fall einiger gleicher i_ν keine Mehrdeutigkeit auf, wenn wir das permutierte Symbol πU durch das Element $U - Q_\pi U$ des Moduls $\mathfrak{A}$ erklären:

$$\pi U = U - Q_\pi U. \tag{9}$$

Für diese Elemente πU folgt nach (4) die Regel I:

$$\pi U - t_i \pi U = Q_{t_i} \pi U.$$

Klammern mit allgemeinen Komponenten $a_\nu = \sum_j \alpha_{\nu j} u_j$ erklären wir jetzt innerhalb $\mathfrak{A}$ durch

$$(a_1, \ldots, a_n) = \sum_{j_1, \ldots, j_n} \alpha_{1 j_1} \cdots \alpha_{n j_n} (u_{j_1}, \ldots, u_{j_n}). \tag{10}$$

Da für die in dieser Weise eingeführten Klammern $(a_1, \ldots, a_n)$ die Regeln II und I bestehen, ist der Induktionsbeweis für den Hilfssatz beendet.

2.

Im Modul $\mathfrak{A}$ führen wir nunmehr eine beiderseitig distributive Multiplikation ein, indem wir die Produkte der Basiselemente definieren:

$$(u_{i_1}, \ldots, u_{i_n}) \cdot (u_{k_1}, \ldots, u_{k_m}) = (u_{i_1}, \ldots, u_{i_n}, u_{k_1}, \ldots, u_{k_m}), \quad (i_1 \leqq \cdots \leqq i_n; k_1 \leqq \cdots \leqq k_m).$$

Durch Induktion nach $n + m$ folgt aus I und II, daß auch die Multiplikation beliebiger Klammern nach derselben Vorschrift erfolgt:

$$\text{III.} \qquad (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m).$$

[1]) L. E. Dickson, Linear groups (Lpz. 1901), p. 287.

Aus dieser Regel ist ersichtlich, daß $\mathfrak{A}$ bei dieser Multiplikation ein assoziativer Ring ist. Wegen der aus I und III folgenden Regel

$$(ab) = (a, b) - (b, a) = (a)\,(b) - (b)\,(a)$$

erfährt der Liesche Ring $\mathfrak{L}$ durch die Zuordnung a auf (a) eine treue Darstellung in unserem konstruierten assoziativen Ring $\mathfrak{A}$. —

Es sei $\mathfrak{a}$ irgendein assoziativer Ring, der eine Darstellung $\bar{a}$ des Lieschen Ringes $\mathfrak{L}$ enthält und von ihr erzeugt wird. Durch die Basiszuordnung

$$(u_{i_1}, \ldots, u_{i_n}) \text{ auf } \bar{u}_{i_1}, \ldots, \bar{u}_{i_n} \qquad (i_1 \leqq \cdots \leqq i_n)$$

wird zunächst $\mathfrak{A}$ als Modul homomorph auf einen Teil von $\mathfrak{a}$ abgebildet. Durch Induktion nach n folgt aus I und II, daß dabei auch beliebige Klammern nach derselben Vorschrift abgebildet werden, nämlich

$$(a_1, \ldots, a_n) \text{ auf } \bar{a}_1 \cdots \bar{a}_n\,.$$

Hieraus ist ersichtlich, daß Produkte in Produkte übergehen, daß jedes Element von $\mathfrak{a}$ Bild ist, und daß bei dieser Ringabbildung von $\mathfrak{A}$ auf $\mathfrak{a}$ die Darstellung (a) in die Darstellung $\bar{a}$ des Lieschen Ringes $\mathfrak{L}$ übergeht.

Damit ist gezeigt, daß unser assoziativer Ring $\mathfrak{A}$ alle Eigenschaften aufweist, wie sie in Satz 1 gefordert werden.

Es sei $\mathfrak{B}$ ein assoziativer Ring, der eine treue Darstellung $[a]$ des Lieschen Ringes $\mathfrak{L}$ enthält und von ihr erzeugt wird. Ferner habe $\mathfrak{B}$ die in Satz 1 geforderten Eigenschaften. $\mathfrak{A}$ und $\mathfrak{B}$ lassen sich dann so aufeinander abbilden, daß sich dabei die Darstellungen (a) und $[a]$ entsprechen. Da diese Darstellungen schon die ganzen Ringe erzeugen, ist $\mathfrak{A} \cong \mathfrak{B}$.

Damit ist Satz 1 in allen Teilen bewiesen.

3.

Beweis von Satz 2. Es werde $\mathfrak{L} = \mathfrak{L}_q$ und $\mathfrak{a} = \mathfrak{A}_q$ gesetzt. Nach Satz 1 läßt sich dann der Ring $\mathfrak{A}$ in solcher Weise auf $\mathfrak{A}_q$ abbilden, daß dabei die erzeugenden Elemente (s_i) von $\mathfrak{A}$ in die freien Erzeugenden S_i von $\mathfrak{A}_q$ übergehen. Dies ist aber nur möglich, falls $\mathfrak{A} \cong \mathfrak{A}_q$, und hieraus folgt der Satz 2.

Beweis von Satz 3. Im freien Lieschen Ring $\mathfrak{L}_q$ sei $u_{n1}, \ldots, u_{n\psi_n}$ eine Basis des Moduls Ψ_n aller homogenen Ausdrücke vom Grad n in den q Erzeugenden s_i. Dann ist

$$u_{11}, \ldots, u_{1\psi_1}, \quad u_{21}, \ldots, u_{2\psi_2}, \text{ usw.}$$

eine geordnete Basis für $\mathfrak{L}_q$. Da $\mathfrak{A} \cong \mathfrak{A}_q$ ist, gibt es genau q^n Basisklammern

$$(u_{\alpha *}, \ldots, u_{\beta *}) \qquad \text{(mit geordneten Komponenten)}$$

vom Grade $n = \alpha + \cdots + \beta$ in den Erzeugenden (s_i) des Ringes $\mathfrak{A}$. Diese Tatsache bedeutet das koeffizientenweise Übereinstimmen der formalen Potenzreihen

$$(11) \qquad (1 - qx)^{-1} = \prod_{d=1}^{\infty} (1 - x^d)^{-\psi_d}\,.$$

Der Logarithmus hiervon ergibt

$$(12) \qquad \sum_{n=1}^{\infty} \frac{(qx)^n}{n} = \sum_{d,\nu=1}^{\infty} \psi_d \frac{x^{d\nu}}{\nu}\,.$$

Die Koeffizienten von x^n/n in (12) lauten

$$(13) \qquad q^n = \sum_{d|n} d\psi_d\,.$$

Nach der Möbiusschen Umkehrung folgt somit die erste Formel von Satz 3

(14) $$n\psi_n = \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Für $\psi(n_1, \ldots, n_q)$ gilt entsprechend die Identität

$$(1 - x_1 - \cdots - x_q)^{-1} = \prod_{d_1, \ldots, d_q} (1 - x_1^{d_1} \cdots x_q^{d_q})^{-\psi(d_1, \ldots, d_q)},$$

in den vertauschbaren Unbestimmten $x_1, \ldots, x_q$. Nach Vornahme derselben Umformungen wie oben ergibt sich hieraus die zweite Formel von Satz 3. —

Für einen Lieschen Ring führen wir rekursiv die Ideale $\mathfrak{L}^n = \mathfrak{L}\mathfrak{L}^{n-1}$ $(\mathfrak{L}^1 = \mathfrak{L})$ ein. Aus den allgemeinen Rechenregeln folgt leicht durch Induktion nach k die Tatsache $\mathfrak{L}^i\mathfrak{L}^k \leqq \mathfrak{L}^{i+k}$. Im freien Lieschen Ring $\mathfrak{L}_q$ setzt sich daher $\mathfrak{L}_q^n$ aus allen Ausdrücken vom n-ten und höheren Grad zusammen.

Ferner werde das Zentrum eines Lieschen Ringes $\mathfrak{L}$ eingeführt. Es besteht aus allen Elementen z mit $z\mathfrak{L} = 0$.

Wir behaupten den

Satz 5. *Der freie Liesche Ring $\mathfrak{L}_q$ $(q > 1)$ hat kein Zentrum. Der Faktorring $\mathfrak{L}_q/\mathfrak{L}_q^{n+1}$ hat das Zentrum $\mathfrak{L}_q^n/\mathfrak{L}_q^{n+1}$ vom Rang ψ_n.*

Beweis. Es ist leicht einzusehen, daß im freien assoziativen Ring $\mathfrak{A}_q$ die Elemente αS_1^f die einzigen homogenen Ausdrücke sind, welche mit der Erzeugenden S_1 vertauschbar sind. Wenn alle Erzeugenden S_i einander gleichgesetzt werden, gehen alle Kommutatorbildungen in 0 über. Daher kann S_1^f für $f > 1$ nicht in der Darstellung von $\mathfrak{L}_q$ liegen. Es folgt:

Die Gleichung $xs_1 = 0$ hat in $\mathfrak{L}_q$ nur die Lösung $x = \alpha s_1$.

Daraus ergibt sich, daß $\mathfrak{L}_q$ $(q > 1)$ kein Zentrum hat. Eine leichte Folgerung ist, daß $\mathfrak{L}_q/\mathfrak{L}_q^{n+1}$ das Zentrum $\mathfrak{L}_q^n/\mathfrak{L}_q^{n+1}$ besitzt.

4.

Wir kommen nun zum gruppentheoretischen Teil der Arbeit.

Es sei $\mathfrak{G}$ eine beliebige Gruppe mit den Elementen $a, b, \ldots$. Wir setzen

(15) $$a \circ b = aba^{-1}b^{-1} \text{ und } b^a = aba^{-1}.$$

Satz 6. *Folgende Identitäten gelten identisch in a, b, c:*

(16) $$a \circ a = 1, \quad (a \circ b) \cdot (b \circ a) = 1, \quad a \circ 1 = 1;$$

(17) $$a \circ (bc) = (a \circ b) \cdot (a \circ c)^b;$$

(18) $$(a \circ (b \circ c)) \cdot (b \circ (c \circ a)) \cdot (c \circ (a \circ b)) = (b \circ c)^a (c \circ b) (c \circ a)^b (c \circ b)^a (a \circ b) (a \circ c)^b (b \circ c) (b \circ a).$$

Eine Probe kann in wenigen Minuten durch direktes Ausrechnen gemacht werden.

Die folgenden Sätze 7, 8, 9 stammen von P. Hall [2]). Wir werden sie mit Satz 6 beweisen.

Es seien $\mathfrak{U}$ und $\mathfrak{V}$ zwei Untergruppen von $\mathfrak{G}$ mit den Elementen u bzw. v. Die von allen Kommutatoren $u \circ v$ erzeugte Untergruppe von $\mathfrak{G}$ werde mit $\mathfrak{U} \circ \mathfrak{V}$ bezeichnet. Mit $\mathfrak{U}$ und $\mathfrak{V}$ ist auch $\mathfrak{U} \circ \mathfrak{V}$ Normalteiler von $\mathfrak{G}$ und liegt im Durchschnitt $\mathfrak{U} \frown \mathfrak{V}$.

Satz 7. *$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ seien drei Normalteiler der Gruppe $\mathfrak{G}$.*

Aus $\mathfrak{A} \circ (\mathfrak{B} \circ \mathfrak{C}) = \mathfrak{B} \circ (\mathfrak{C} \circ \mathfrak{A}) = 1$ folgt $\mathfrak{C} \circ (\mathfrak{A} \circ \mathfrak{B}) = 1$.

---

[2]) P. Hall, A contribution to the theory of groups of prime-power order, Proc. Lond. Math. Soc. (2) **36** (1934).

Beweis. Es seien a, b, c beliebige Elemente aus $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$. Nach Voraussetzung ist a mit $b \circ c$ und b mit $a \circ c$ vertauschbar, daher dürfen in der rechten Seite von (18) alle Exponenten gestrichen werden. Ferner sind $a \circ b$ und $a \circ c$ als Elemente aus $\mathfrak{A}$ mit $b \circ c$ vertauschbar, und $a \circ b$ ist als Element aus $\mathfrak{B}$ mit $a \circ c$ vertauschbar. Die rechte Seite von (18) wird also gleich 1, weil sich alle vertauschbaren Klammern kürzen lassen. Auf der linken Seite sind die beiden ersten Faktoren gleich 1, daher folgt

$$c \circ (a \circ b) = 1, \qquad c \circ (\mathfrak{A} \circ \mathfrak{B}) = 1, \qquad \mathfrak{C} \circ (\mathfrak{A} \circ \mathfrak{B}) = 1, \qquad \text{w. z. b. w.}$$

Wir führen jetzt rekursiv die charakteristischen Normalteiler $\mathfrak{G}^n$ der Gruppe $\mathfrak{G}$ ein durch $\mathfrak{G}^n = \mathfrak{G} \circ \mathfrak{G}^{n-1}$ $(\mathfrak{G}^1 = \mathfrak{G})$.

Satz 8. *Für die Normalteiler $\mathfrak{G}^n$ der Gruppe $\mathfrak{G}$ gilt die Regel*

$$\mathfrak{G}^i \circ \mathfrak{G}^k \leqq \mathfrak{G}^{i+k}.$$

Beweis. Für $k = 1$ ist $\mathfrak{G}^i \circ \mathfrak{G}^1 = \mathfrak{G}^{i+1}$. Es sei jetzt $k > 1$ und der Satz schon bis $k - 1$ und für beliebiges i bewiesen. Es werde $\mathfrak{G}^{i+k} = 1$ gesetzt. Dann ist

$$\mathfrak{G}^1 \circ (\mathfrak{G}^{k-1} \circ \mathfrak{G}^i) \leqq \mathfrak{G}^1 \circ \mathfrak{G}^{i+k-1} = 1 \quad \text{und} \quad \mathfrak{G}^{k-1} \circ (\mathfrak{G}^i \circ \mathfrak{G}^1) \leqq \mathfrak{G}^{k-1} \circ \mathfrak{G}^{i+1} = 1,$$

also nach Satz 7 auch $\mathfrak{G}^i \circ \mathfrak{G}^k = \mathfrak{G}^i \circ (\mathfrak{G}^1 \circ \mathfrak{G}^{k-1}) = 1$.

Mit Satz 8 folgt leicht aus (17) und (16)

Satz 9. *Mit einem Element a aus $\mathfrak{G}^\alpha$ und mit Elementen b, b' aus $\mathfrak{G}^\beta$ gelten die Regeln*

$$a \circ (b \cdot b') \equiv (a \circ b) \cdot (a \circ b') \quad \text{und} \quad (b \cdot b') \circ a \equiv (b \circ a) \cdot (b' \circ a) \mod \mathfrak{G}^{\alpha+\beta+1}.$$

Satz 10. *Mit Elementen a, b, c aus $\mathfrak{G}^\alpha, \mathfrak{G}^\beta, \mathfrak{G}^\gamma$ gilt die Regel*

$$(a \circ (b \circ c)) \cdot (b \circ (c \circ a)) \cdot (c \circ (a \circ b)) \equiv 1 \mod \mathfrak{G}^{\alpha+\beta+\gamma+1}.$$

Beweis. Es werde $\mathfrak{G}^{\alpha+\beta+\gamma+1} = 1$ gesetzt. Auf der rechten Seite von (18) kann $(a \circ b)$ gegen $(b \circ a)$, und $(a \circ c)^b$ gegen $(c \circ a)^b$ gekürzt werden. Übrig bleibt

$$(b \circ c)^a\,(c \circ b) \cdot (c \circ b)^a\,(b \circ c) = (a \circ (b \circ c)) \cdot (a \circ (c \circ b)),$$

und nach Satz 9 ist dies gleich 1.

Hilfssatz. *Die Gruppe $\mathfrak{G}$ werde von den Elementen σ_i erzeugt. Die Faktorgruppe $\mathfrak{G}^n/\mathfrak{G}^{n+1}$ wird dann erzeugt von allen Ausdrücken*

$$\sigma_{i_1 \ldots i_n} = \sigma_{i_1} \circ (\sigma_{i_2} \circ (\cdots \circ \sigma_{i_n}) \cdots).$$

Beweis. Es sei $n > 1$ und der Hilfssatz bis $n - 1$ bewiesen. $\mathfrak{G}^{n-1}/\mathfrak{G}^n$ wird erzeugt von allen Ausdrücken $\sigma_{i_2 \ldots i_n}$, daher wird $\mathfrak{G}^n = \mathfrak{G} \circ \mathfrak{G}^{n-1}$ von Elementen der Gestalt

$$x_n = \Big(\prod_{i_1} \sigma_{i_1}^{\pm 1}\Big) \circ \Big(a_n \cdot \prod_{i_2, \ldots, i_n} \sigma_{i_2 \ldots i_n}^{\pm 1}\Big)$$

mit a_n aus $\mathfrak{G}^n$ erzeugt. Nach Satz 9 folgt

$$x_n \equiv \prod_{i_1} (\sigma_{i_1}^{\pm 1} \circ a_n) \cdot \prod_{i_1, \ldots, i_n} (\sigma_{i_1} \circ \sigma_{i_2 \ldots i_n})^{\pm 1} \equiv \prod_{i_1, \ldots, i_n} \sigma_{i_1 \ldots i_n}^{\pm 1} \mod \mathfrak{G}^{n+1}.$$

5.

Wir führen von nun an folgende Bezeichnungen ein:

$\mathfrak{L}_q$ sei der ganzzahlige freie Liesche Ring mit q Erzeugenden s_i,

$\mathfrak{A}_q$ der ganzzahlige freie assoziative Ring mit q Erzeugenden S_i;

auch für diese Ringe gelten die Sätze 2 und 3.

$\mathfrak{G}_q$ sei die freie Gruppe mit q Erzeugenden σ_i.

$\mathfrak{D}_q$ sei der ganzzahlige freie distributive Ring mit q Erzeugenden s_i, d. h. in $\mathfrak{D}_q$ bestehen für die Multiplikation nur die beiden Distributivgesetze.

Λ sei die homomorphe Abbildung von $\mathfrak{D}_q$ auf $\mathfrak{L}_q$, das dabei entstehende

Ideal $\mathfrak{J}$ wird erzeugt von den Größen xx, $x(yz) + y(zx) + z(xy)$ in $\mathfrak{D}_q$.

Δ sei die Abbildung von $\mathfrak{L}_q$ in $\mathfrak{A}_q$ gemäß Satz 2.

Γ bilde die Monome u aus $\mathfrak{D}_q$ auf die entsprechenden Kommutatoren Γu von $\mathfrak{G}_q$ ab, z. B. gehe dabei $u = (s_1(s_2 s_3))\,(s_4 s_4)$ über in $\Gamma u = (\sigma_1 \circ (\sigma_2 \circ \sigma_3)) \circ (\sigma_4 \circ \sigma_4)$.

$\mathfrak{U}$ sei die in $\mathfrak{D}_q$ folgendermaßen erklärte Menge von Elementen U:

(a) $\mathfrak{U}$ enthält alle Ausdrücke uu, $uv + vu$, $u(vw) + v(wu) + w(uv)$ mit Monomen u, v, w;
(b) mit Σu_ν enthält $\mathfrak{U}$ auch noch Σvu_ν und $\Sigma u_\nu v$.

Die Elemente U der Menge $\mathfrak{U}$ sind durchweg Summen von höchstens drei Monomen gleichen Grades in den Erzeugenden. Wir erklären jetzt die Abbildung Γ auch für diese Elemente $U = \Sigma u_\nu$ durch $\Gamma U = \Pi(\Gamma u_\nu)$, wobei die Reihenfolge der Faktoren willkürlich festgesetzt werde.

Die Menge $\mathfrak{U}$ hat zwei wichtige Eigenschaften:

(19) Jedes Element des Ideals $\mathfrak{J}$ ist nach dem Distributivgesetz als $\Sigma \pm U_\mu$ darstellbar.

Auf Grund der Entstehungsweise der Menge $\mathfrak{U}$ folgt nach (16) und nach den Sätzen 8, 9, 10:

(20) $$\Gamma U \equiv 1 \mod \mathfrak{G}^{n+1} \qquad (U \text{ vom Grade } n).$$

Nunmehr schreiten wir zum

Beweis von Satz 4. Die unendlichen Reihen

$$X = 1 + A_1 + A_2 + \cdots \qquad (A_n \text{ homogen vom Grad } n \text{ aus } \mathfrak{A}_q)$$

bilden bei formaler Multiplikation eine Gruppe $\mathfrak{X}$. Diese Gruppe wurde von Magnus eingeführt. Für die Reihen

$$X = 1 + A_i + \cdots, \qquad X' = 1 + A_i' + \cdots, \qquad Y = 1 + B_k + \cdots$$

ergibt sich

(21) $$X \cdot X' = 1 + (A_i + A_i') + \cdots \quad \text{und} \quad XYX^{-1}Y^{-1} = 1 + (A_iB_k - B_kA_i) + \cdots,$$

wobei jeweils Glieder höheren Grades fortgelassen sind.

Durch $\Phi(\sigma_i) = 1 + S_i$ entsteht eine homomorphe Abbildung Φ der freien Gruppe $\mathfrak{G}_q$ auf einen Teil der Gruppe $\mathfrak{X}$. Für ein Element g aus $\mathfrak{G}_q$ sei dabei in der Reihenentwicklung

$$\Phi(g) = 1 + \varphi_1(g) + \varphi_2(g) + \cdots$$

$\varphi_n(g)$ das homogene Glied vom Grad n aus $\mathfrak{A}_q$. Für ein Element g_n aus $\mathfrak{G}_q^n$ beginnt nach der rekursiven Definition $\mathfrak{G}_q^n = \mathfrak{G}_q \circ \mathfrak{G}_q^{n-1}$ und nach (21) die Reihenentwicklung frühestens mit dem Glied $\varphi_n(g_n)$, während alle vorangehenden Glieder verschwinden:

$$\Phi(g_n) = 1 + \varphi_n(g_n) + \varphi_{n+1}(g_n) + \cdots.$$

Da ebenso $\varphi_n(g_{n+1}) = 0$ ist, wird durch φ_n eine homomorphe Abbildung der abelschen Faktorgruppe $\mathfrak{G}_q^n/\mathfrak{G}_q^{n+1}$ auf gewisse Ausdrücke n-ten Grades von $\mathfrak{A}_q$ geliefert, wobei Produkte in Summen übergehen. Diese Abbildung φ_n wollen wir näher untersuchen.

Nach dem Hilfssatz des vorigen Abschnitts dürfen wir

$$(22)\qquad g_n \equiv \prod_\nu (\Gamma u_\nu)^{\pm 1} \mod G_q^{n+1} \qquad (\text{in } \mathfrak{G}_q)$$

mit Monomen u_ν aus $\mathfrak{D}_q$ vom Grad n ansetzen. Aus der Rechenregel (21) folgt

$$\varphi_n(g_n) = \Delta \Lambda \sum_\nu \pm u_\nu \qquad (\text{in } \mathfrak{A}_q).$$

$\varphi_n(g_n)$ liegt also in der Darstellung des Lieschen Ringes $\mathfrak{L}_q$ in $\mathfrak{A}_q$. Da diese Darstellung treu ist, folgt

$$(23)\qquad \Delta^{-1}\varphi_n(g_n) = \Lambda \sum_\nu \pm u_\nu \qquad (\text{in } \mathfrak{L}_q).$$

Hieraus folgt, daß $\mathfrak{G}_q^n/\mathfrak{G}_q^{n+1}$ durch die Abbildung $\Delta^{-1}\varphi_n$ auf den ganzen Modul Ψ_n aller homogenen Elemente n-ten Grades des Lieschen Ringes $\mathfrak{L}_q$ abgebildet wird. Da Ψ_n nach Satz 3 den Rang ψ_n hat, brauchen wir zum Beweis von Satz 4 nur noch zu zeigen, daß $\Delta^{-1}\varphi_n$ eine Isomorphie

$$(24)\qquad \mathfrak{G}_q^n/\mathfrak{G}_q^{n+1} \cong \Psi_n$$

vermittelt.

Es sei dazu g_n ein Element aus $\mathfrak{G}_q^n$ mit $\Delta^{-1}\varphi_n(g_n) = 0$. Wegen (23) liegt dann $\sum_\nu \pm u_\nu$ im Ideal $\mathfrak{J}$ von $\mathfrak{D}_q$, und nach (19) gilt

$$\sum_\nu \pm u_\nu = \sum_\mu \pm U_\mu \qquad (U_\mu \text{ aus } \mathfrak{U} \text{ vom Grad } n).$$

Diese Gleichung ist eine rein additive Umformung. Da $\mathfrak{G}_q^n/\mathfrak{G}_q^{n+1}$ abelsch ist und wegen (20) folgt jetzt

$$\prod_\nu (Lu_\nu)^{\pm 1} \equiv \prod_\mu (LU_\mu)^{\pm 1} \equiv 1 \mod \mathfrak{G}_q^{n+1},$$

und wegen (22) ist bewiesen, daß g_n sogar in $\mathfrak{G}_q^{n+1}$ liegt. Damit ist die Isomorphie (24) und der Satz 4 bewiesen.

6.

In Bad Salzbrunn vermutete Magnus den folgenden Satz, den wir eben zugleich mitbewiesen haben:

Satz 11. *Es sei g ein Element aus $\mathfrak{G}_q^n$, das nicht in $\mathfrak{G}_q^{n+1}$ liegt. In der oben erklärten Reihenentwicklung*

$$\Phi(g) = 1 + \varphi_1(g) + \varphi_2(g) + \cdots$$

ist dann $\varphi_n(g) \neq 0$, während alle vorangehenden Glieder verschwinden. Dies Anfangsglied $\varphi_n(g)$ liegt in der Darstellung des Lieschen Ringes $\mathfrak{L}_q$ in den assoziativen Ring $\mathfrak{A}_q$.

Es sei dazu folgende Ergänzung erwähnt:

Satz 12. *Durch die oben erklärte Reihenentwicklung*

$$\Phi(g) = 1 + \varphi_1(g) + \varphi_2(g) + \cdots$$

entsteht eine isomorphe Abbildung Φ der freien Gruppe $\mathfrak{G}_q$ auf einen Teil der Gruppe $\mathfrak{X}$ aller Reihen

$$X = 1 + A_1 + A_2 + \cdots \qquad (A_i \text{ aus } \mathfrak{A}_q).$$

(Die Isomorphie bleibt bestehen, wenn die Reihen nur mod p betrachtet werden.)

Die unendliche Kette $\mathfrak{G}_q^1, \mathfrak{G}_q^2, \mathfrak{G}_q^3, \ldots$ hat den Durchschnitt 1.

Beweis. Für

$$g = \sigma_{i_1}^{\alpha_1}\sigma_{i_2}^{\alpha_2}\cdots\sigma_{i_l}^{\alpha_l} \neq 1 \qquad (\sigma_{i_1} \neq \sigma_{i_2} \neq \cdots \neq \sigma_{i_l};\ \alpha_i \neq 0)$$

treten in der Reihe

$$\Phi(g) = \sum_{\nu_1, \ldots, \nu_l} \binom{\alpha_1}{\nu_1} \cdots \binom{\alpha_l}{\nu_l} S_{i_1} \cdots S_{i_l}$$

sicher Glieder mit lauter positiven Exponenten ν_i wirklich auf (sogar mod p), und zwar sind diese Glieder wegen $S_{i_1} \neq S_{i_2} \neq \cdots \neq S_{i_l}$ alle untereinander verschieden. Also folgt $\Phi(g) \neq 1$.

Speziell kommt $\alpha_1 \cdots \alpha_l S_{i_1} \cdots S_{i_l} \neq 0$ vor, daher liegt nach dem vorigen Satz das Element g nicht in $\mathfrak{G}_q^{l+1}$. —

Zum Schluß teilen wir noch folgendes Gegenstück zu Satz 5 mit:

Satz 13. *Die freie Gruppe* $\mathfrak{G}_q$ $(q > 1)$ *hat kein Zentrum.* $\mathfrak{G}_q/\mathfrak{G}_q^{n+1}$ *hat das Zentrum* $\mathfrak{G}_q^n/\mathfrak{G}_q^{n+1}$.

Beweis. Die erste Behauptung folgt z. B. aus der elementaren Tatsache, daß eine Erzeugende nur mit ihren Potenzen vertauschbar ist. Die zweite Behauptung ergibt sich folgendermaßen: Es sei z ein Zentrumselement von $\mathfrak{G}_q/\mathfrak{G}_q^{n+1}$. Die Reihenentwicklung $\Phi(z)$ beginne mit dem ν-ten Glied, z liege also in $\mathfrak{G}_q^\nu$. Es sei etwa $\varphi_\nu(z) \neq \alpha S_1$. Da nach Satz 11 $\varphi_\nu(z)$ in der Darstellung von $\mathfrak{L}_q$ in $\mathfrak{A}_q$ liegt, ist, wie schon früher bemerkt, $\varphi_{\nu+1}(z \circ \sigma_1) = \varphi_\nu(z) \cdot S_1 - S_1 \cdot \varphi_\nu(z) \neq 0$. Weil $z \circ \sigma_1$ in $\mathfrak{G}_q^{n+1}$ liegt, folgt $\nu \geqq n$, und z liegt in $\mathfrak{G}_q^n$. Umgekehrt liegen alle Elemente von $\mathfrak{G}_q^n$ im Zentrum von $\mathfrak{G}_q/\mathfrak{G}_q^{n+1}$, w. z. b. w.

Müllheim (Baden), 10. Oktober 1936.

Eingegangen 13. Oktober 1936.