TREUE DARSTELLUNGEN BELIEBIGER LIESCHER RINGE

VON ERNST WITT IN HAMBURG

In der vorliegenden Note beweisen wir den Satz, dass jeder Liesche Ring treue Darstellungen in assoziativen Ringen besitzt, unter ausschliesslicher Verwendung finiter Verfahren. Dabei ist folgendes zu bedenken: Ist ein Liescher Ring etwa durch Erzeugende und definierende Relationen gegeben, so existiert im allgemeinen kein finites Verfahren, um festzustellen, ob zwei gegebene Ausdrücke das gleiche Element bezeichnen. Umso weniger wird es möglich sein, sämtliche linearen Beziehungen zwischen vorgelegten Elementen wirklich aufzustellen. Diese Tatsache erschwert natürlich die Beweisführung.

1. Ein *Liescher Ring* ist ein Modul, in dem eine mit der Addition distributive Multiplikation ab erklärt ist, die den Bedingungen

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

genügt.

Ist jedem Element a eines Lieschen Ringes L ein Element d_a eines assoziativen Ringes A zugeordnet derart, dass dabei die Regeln

$$d_{a+b} = d_a + d_b, \quad d_{ab} = d_a d_b - d_b d_a$$

gelten, so heisst die Abbildung $a \rightarrow d_a$ eine *Darstellung* von L im assoziativen Ring A . Der Teilring von A , den die Elemente d_a erzeugen, wird die zugehörige *Darstellungshülle* genannt.

Eine Darstellung $a \rightarrow d_a$ heisst *treu*, wenn $d_c = 0$ nur für $c = 0$ zutrifft, wenn also die Modulisomorphie $a \leftrightarrow d_a$ besteht. In diesem Falle kann man, unter Verwendung der Schreibweise $a \circ b$ für das Liesche Produkt ohne Schaden d_a mit a identifizieren. Hierdurch erscheint der Liesche Ring eingebettet in den assoziativen Ring.

2. Zunächst führen wir nun durch eine naheliegende abstrakte Konstruktion die universelle Darstellungshülle eines Lieschen Ringes ein, deren feineren Eigenschaften dann anschliessend untersucht werden, ähnlich wie man es etwa in der Topologie mit dem auf RIEMANN zurückgehenden Begriff der universellen Überlagerung macht. Solche Universalstrukturen vertiefen und vereinfachen zugleich die mathematische Anschauung.

Zu einem beliebig gegebenen Lieschen Ring L definieren wir einen assoziativen Ring H durch die erzeugenden Elemente z_a , die den a aus L eineindeutig zugeordnet sind, und durch die Relationen

1. Grades $z_a + z_b - z_{a+b} = 0$,
2. Grades $z_a z_b - z_b z_a - z_{ab} = 0$.

Die Abbildung $a \rightarrow z_a$ ist offenbar eine Darstellung von L in H , und H ist die zugehörige Darstellungshülle. H nennen wir die *universelle Darstellungshülle* des Lieschen Ringes L , denn jede andere Darstellungshülle zu einer Darstellung $a \rightarrow d_a$ von L ist homomorphes Bild von H vermöge $z_a \rightarrow d_a$.

Ein wichtiges Beispiel: Ist L der freie Liesche Ring mit den Erzeugenden x_k , so erhält man eine Darstellung von L in dem freien assoziativen Ring A mit entsprechenden Erzeugenden X_k durch die Zuordnung $x_k \rightarrow X_k$. H lässt sich demnach homomorph auf A abbilden durch $z_k \rightarrow X_k$, und mit A ist auch H ein freier Ring. Mit anderen Worten:

Die universelle Darstellungshülle des freien Lieschen Ringes mit den Erzeugenden x_k ist isomorph zu dem freien assoziativen Ring mit entsprechenden Erzeugenden X_k .

3. In der universellen Darstellungshülle H eines beliebig vorgelegten Lieschen Ringes L ist zufolge der ersten definierenden Regel z_a eine lineare Funktion von a . Die zweite Regel kann nun *approximativ* als *Kommutativgesetz* $z_a z_b = z_b z_a$ aufgefasst werden — bis auf einen Fehler ersten Grades z_{ab} . Diese Deutung kommt dann zu ihrem Recht, wenn man, bildlich gesprochen, zeigen kann, dass auch eine Anhäufung solcher Fehler keine nennenswerte Störung verursacht.

Zur Durchführung dieser Überlegungen betrachten wir im Lieschen Ring L einen *Untermodul* U , der eine *angeordnete Basis* u habe. Jedes Element aus U lasse sich also eindeutig als eine endliche Summe

$$\sum \lambda_u u \qquad (u \text{ aus } u)$$

schreiben, noch mit der Einschränkung, dass λ_u nur mod ε_u bestimmt ist ($\varepsilon_u u = 0$). Die Einführung eines mit einer Basis u versehenen Untermoduls U ist deshalb erforderlich, weil uns die Natur des vorgelegten Lieschen Ringes völlig unbekannt ist, insbesondere braucht ja L selbst keine Basis zu haben.

Im freien assoziativen Ring Z der Erzeugenden z_a , in dem wir uns zunächst bewegen, legen wir nun einige Bezeichnungen fest. In ihm sei

Z^n der Modul aller assoziativen Polynome höchstens n^{ten} Grades. Für eine gegebene Teilmenge M des Lieschen Ringes L bedeute

Z_M^n den Bereich derjenigen Polynome von Grade $\leq n$, bei denen der homogene Bestandteil n^{ten} Grades nur Indizes aus M aufweist. Die Indizes der Bestandteile minderen Grades werden hierdurch nicht eingeengt.

R sei im Ringe Z das von allen Ausdrücken

$$z_a + z_b - z_{a+b}, \quad z_a z_b - z_b z_a - z_{ab}$$

erzeugte Ideal der « Relationen ». Es ist also $Z/R = H$.

R^n , R_M^n bedeute das lineare Erzeugnis aller in Z^n bzw. Z_M^n vorhandenen « Grundrelationen »

- $$\left. \begin{array}{l} 1. \text{ Art } P(z_a + z_b - z_{a+b}) Q \\ 2. \text{ Art } P(z_a z_b - z_b z_a - z_{ab}) Q \end{array} \right\} (P, Q \text{ sind Monome } z_a z_b \dots z_c \text{ oder } 1).$$

Die oben ausgesprochenen Gedanken liefern nun *Reduktionsprozesse* mit folgenden Ergebnis:

Hilfssatz 1. Jedes Element aus Z_U^n lässt sich mod R_U^n auf die Gestalt

$$\sum_i \lambda_i z_{u_{i1}} z_{u_{i2}} \dots z_{u_{in}} + y^{n-1}$$

reduzieren mit geordneten Faktoren

$$u_{i1} \leq u_{i2} \leq \dots \leq u_{in}. \quad (\text{in der Anordnung von } u)$$

Dabei ist λ_i mod dem grössten gemeinsamen Teiler $\varepsilon_i = (\varepsilon_{i1}, \varepsilon_{i2}, \dots, \varepsilon_{in})$ und y^{n-1} aus Z^{n-1} mod R^{n-1} eindeutig bestimmt.

BEWEIS. Wir gehen in Z_U^n zu einem Faktormodul über, indem wir darin zunächst alle Grundrelationen 1. Art Null setzen:

$$P z_{a+b} Q = P z_a Q + P z_b Q.$$

Mit dieser Regel kann jedes homogene Polynom n^{ten} Grades aus Z_U^n eindeutig auf die Form gebracht werden

$$\sum \lambda_i z_{u_{i1}} z_{u_{i2}} \dots z_{u_{in}} \quad (\lambda_i \bmod \varepsilon_i).$$

Hiermit ist Z_U^n auf Z_u^n reduziert. Mit derselben Regel können auch die verbleibenden Grundrelationen von Z_U^n , wie sich unmittelbar aus ihrer Gestalt ergibt, linear durch diejenigen von Z_u^n ausgedrückt werden, d. h. es lässt sich R_U^n auf R_u^n reduzieren.

Erneut gehen wir nun zu einem Faktormodul über, indem wir auch noch alle Grundrelationen 2. Art in Z_u^n zu Null machen:

$$P z_b z_a Q = P z_a z_b Q + P z_{ba} Q.$$

Mit dieser Regel (die übrigens mod R^{n-1} in a und b symmetrisch ist und für $a = b$ identisch gilt) können wir dann in einem Monom

$$z_{u_1} z_{u_2} \dots z_{u_n}$$

die Anzahl j der *Inversionen* $u_\nu > u_\mu$ (für $\nu < \mu$) Schritt für Schritt erniedrigen, solange, bis das Monom schliesslich geordnet ist ($u'_1 \leq u'_2 \leq \dots \leq u'_n$), wobei allerdings bei jedem Schritt ein *Korrekturglied* niedrigeren Grades als n anzubringen ist.

Die *Gesamtkorrektur* hängt nun, wenn nur modulo R^{n-1} gerechnet wird, *nicht von der Reihenfolge* der einzelnen Reduktionsschritte ab, wie jetzt durch Induktion nach der Inversionszahl j bewiesen wird.

Es sei $P z_c z_b z_a Q$ ein Monom vom Grade n und der Inversionszahl j . In der Anordnung sei $c > b > a$ gedacht. Bei der Reduktion kann entweder zuerst z_c mit z_b vertauscht werden, oder aber zuerst z_b mit z_a . In jedem Fall entsteht ein Monom der Inversionszahl $j - 1$. Nach Induktionsvoraussetzung ist also der weitere Verlauf der Reduktion jedesmal ohne Einfluss auf die Gesamtkorrektur. Beide Reduktionen können nun in geeigneter Weise bis zu der gemeinsamen Zwischenstation $P z_a z_b z_c Q$ fortgesetzt werden. Diese Reduktionen lauten ausführlich unter Angabe der Korrekturglieder K_1 bzw. K'_1

Im ersten Fall		Im zweiten Fall	
$P z_c z_b z_a Q$	$K_1 = P z_{cb} z_a Q$	$P z_c z_b z_a Q$	$K'_1 = P z_c z_{ba} Q$
$P z_b z_c z_a Q$	$K_2 = P z_b z_{ca} Q$	$P z_c z_a z_b Q$	$K'_2 = P z_{ca} z_b Q$
$P z_b z_a z_c Q$	$K_3 = P z_{ba} z_c Q$	$P z_a z_c z_b Q$	$K'_3 = P z_a z_{cb} Q$
$P z_a z_b z_c Q$		$P z_a z_b z_c Q$	
.....			

Die Differenz (oder die Bilanz) der beiden Gesamtkorrekturen ist

$$(K_1 - K'_1) + (K_2 - K'_2) + (K_3 - K'_3) \\ \equiv P (z_{(cb)a} + z_{b(ca)} + z_{(ba)c}) Q \equiv 0 \bmod R^{n-1},$$

was zu zeigen war. Hier wurden wesentlich die Rechengesetze des Lieschen Ringes benützt.

Analog kann in einem Monom $P z_b z_a Q z_d z_c S$ entweder zuerst z_b mit z_a vertauscht werden, oder aber zuerst z_d mit z_c . In der Anordnung sei $b > a$ und $d > c$ gedacht. Die weitere Rechnung verläuft ähnlich wie eben:

Erster Fall		Zweiter Fall	
$P z_b z_a Q z_d z_c S$	$K_1 = P z_{ba} Q z_d z_c S$	$P z_b z_a Q z_d z_c S$	$K'_1 = P z_b z_a Q z_{dc} S$
$P z_a z_b Q z_d z_c S$	$K_2 = P z_a z_b Q z_{dc} S$	$P z_b z_a Q z_c z_d S$	$K'_2 = P z_{ba} Q z_c z_d S$
$P z_a z_b Q z_c z_d S$		$P z_a z_b Q z_c z_d S$	
.....			

$$(K_1 - K'_1) + (K_2 - K'_2) \equiv P (z_{ba} Q z_{dc} + z_{ab} Q z_{dc}) S \equiv 0 \bmod R^{n-1}.$$

Mit dieser Unabhängigkeit der Reduktionen «vom Wege» ⁽¹⁾ ist zugleich der Hilfssatz bewiesen.

4. Die folgende Tatsache vermittelt uns nun einen Einblick in die Struktur des Ideals R der Relationen:

Hilfssatz 2. *Eine Relation h^{ten} Grades lässt sich linear durch Grundrelationen von Grade $\leq h$ zusammensetzen:*

$$R \cap Z^h = R^h.$$

Eine Relation h^{ten} Grades R sei aus Grundrelationen höchstens n^{ten} Grades linear zusammengesetzt, symbolisch $R = S^n$. Für den Fall $n > h$ werden wir nun eine analoge Zerlegung $R = S^{n-1}$ herleiten. In derselben Weise können wir dann schrittweise bis zu einer Zerlegung $R = S^h$ gelangen, wie behauptet.

¹⁾ Der hier gegebene Nachweis für die Unabhängigkeit vom Wegestamm von G. BIRKHOFF. In meiner früheren Arbeit hatte ich statt dessen gezeigt, dass die Gesamtkorrektur «für geschlossene Wege» verschwindet, was im Prinzip auf dasselbe hinausläuft. Dabei stützte ich mich auf eine von E. H. MOORE stammende Darstellung der symmetrischen Gruppe durch Transpositionen mit definierenden Relationen.

In der Zerlegung $R = S^n$ kommen als Indizes nur endlich viele Elemente c_j des Lieschen Ringes L vor. Wenn man nun den Ausdruck S^n distributiv ausklammert und nach Monomen ordnet, so heben sich alle Monome n^{ten} Grades weg, weil ja der Grad von R kleiner als n vorausgesetzt war. Dies Wegheben kann nur dadurch zustande kommen, dass einige der Indizes c_j im Lieschen Ring entweder zusammenfallen oder als Summe von zwei anderen Indizes darstellbar sind, wie man sofort aus der Gestalt der Grundrelationen ersieht. Das sind endlich viele lineare Beziehungen $\sum \alpha_{ij} c_j = 0$.

Nun sei U der Faktormodul der ganzzahligen Linearformen $\sum \xi_j c_j$ mod $\sum \alpha_{ij} c_j$. Nach der sogenannten Elementarteilertheorie lässt sich die Matrix α_{ij} durch endlich viele Elementartransformationen auf Diagonalgestalt bringen, d. h. U lässt sich durch eine endliche Basis u (die wir uns irgendwie geordnet denken) mit definierenden Gleichungen $\varepsilon_i u_i = 0$ beschreiben. Wir nennen diesen Modul U den durch die Elemente c_j und die Relationen $\sum \alpha_{ij} c_j = 0$ bestimmten *idealen* Modul. Als Elemente von L können die c_j natürlich noch weitere Relationen erfüllen, auf die es hier aber nicht ankommt. Wichtig ist nun, dass für $R = S^n$ Hilfssatz 1 mit gleichem Beweis auch bezüglich des idealen Moduls U richtig ist.

[Unter Verzicht auf finite Beweisführung hätte man kürzer wie folgt schliessen können: Die endlich vielen in der Zerlegung $R = S^n$ vorkommenden Indizes c_j aus L erzeugen linear einen Modul in L . Dieser hat nach dem Hauptsatz für abelsche Gruppen eine endliche Basis usw.]

Wendet man nun die Reduktionen des Hilfssatzes 1 an auf R bzw. S^n , so erhält man als Korrekturglieder aus $y^{n-1} R$ bzw. 0 . Wegen $R = S^n$ ergibt dann Hilfssatz 1 $R \equiv 0 \pmod{R^{n-1}}$. Der finite Beweis des hier verwendeten Hilfssatzes 1 bietet zugleich eine Handhabe, eine Zerlegung $R = S^{n-1}$ wirklich in endlich vielen Schritten aufzustellen. Damit ist der Beweis von Hilfssatz 2 beendet.

5. Für $h = 1$ erhalten wir jetzt folgenden grundlegenden Satz:
Satz. *Die universelle Darstellung ist treu.*

Beweis. Aus $z_c \equiv z_d \pmod{R}$ kann nämlich nach Hilfssatz 2 eine Identität:

$$z_c - z_d = \sum \pm (z_a + z_b - z_{a+b})$$

hergeleitet werden. Wird hier überall $z_c = c$, $z_d = d$, usw. eingesetzt, so werden rechts alle Klammern Null. Es folgt $c = d$ und damit die nachzuweisende Eineindeutigkeit bei der universellen Darstellung $c \rightarrow z_c \pmod{R}$.

Indem wir jetzt die Schreibweise $a \circ b$ für das Liesche Produkt verwenden, dürfen wir diesem Satz zufolge in der universellen Darstellungshülle H ohne Schaden z_a mit a identifizieren. Hierdurch erscheint der Liesche Ring L in der universellen Hülle H eingebettet. Die H definierenden Regeln

$$z_a + z_b = z_{a+b}, \quad z_a z_b - z_b z_a = z_{a \circ b}$$

schrumpfen bei der Identifizierung zusammen auf $ab - ba = a \circ b$. H erscheint dann als der Ring aller formalen assoziativen Polynome $\Sigma \lambda a b \dots c$ in den Elementen $a, b, \dots, c$ des Lieschen Ringes. Das hier Bewiesene lässt sich nun auch wie folgt ausdrücken:

Gesetzt, man habe $c = d$ als Ergebnis einer in H verlaufenden assoziativen Rechnung festgestellt. Diese Berechnung kann man dann, nach einem finitem Verfahren so abändern, dass sie schliesslich völlig im Lieschen Ring L verläuft. c und d sind also bereits im Lieschen Ring L gleiche Elemente.

Obige Beweise liefern auch noch folgenden allgemeineren Satz:

SATZ. *Ein Liescher Ring L mit einem kommutativen Operatorenring Ω hat eine treue assoziative Darstellung, falls sich zu jedem idealen Modul von L mit endlich vielen Erzeugenden und endlich vielen Relationen ein kanonischer Homomorphismus in eine direkte Summe idealer eingliedriger Moduln konstruieren lässt.*

Dabei heisse ein Homomorphismus zwischen idealen Moduln kanonisch, wenn er in L betrachtet, die identische Abbildung induziert.

Man braucht nämlich nur als Z den freien assoziativen Ring mit Ω als Operatorenbereich und den Elementen z_a als Erzeugenden zu nehmen und die Ausdrücke $z_a + z_b - z_{a+b}$ durch $\lambda z_a - \mu z_b - z_{\lambda a + \mu b}$, λ und μ aus Ω , zu ersetzen. Alle oben durchgeführten Schlüsse lassen sich dann in derselben Weise ziehen wie bisher. Dabei sind die oben vorkommenden ε_i Ideale aus Ω . Operatorenringe Ω , die den in diesem Satze genannten Bedingungen genügen, sind z. B. die Ringe, in denen jedes Ideal mit zwei Erzeugenden Hauptideal ist, speziell Ringe mit Euklidischem Algorithmus.

6. Abschliessend geben wir einige Tatsachen an, die fast unmittelbare Folgen der bisherigen Ergebnisse sind.

Es sei a ein Ideal im Lieschen Ring L . In der universellen Hülle H von L sei $A = HaH$ das von a assoziativ erzeugte Ideal. Die universelle Hülle von L/a ist dann isomorph H/A . Es gilt $L \cap A = a$.

Es sei L_1 ein *Unterring* des Lieschen Ringes L . In der universellen Hülle H von L sei H_1 der von L_1 assoziativ erzeugte Unterring. Man wird nun erwarten, dass die universelle Hülle von L_1 isomorph mit H_1 ist. In vielen Fällen stimmt das tatsächlich, z. B. dann, wenn L_1 eine Basis hat, die sich zu einer Basis von L ergänzen lässt - aber im Allgemeinen ist die Erwartung leider falsch: Es gibt für L bereits ein *Gegenbeispiel* von 4 Elementen (aus $2y = 0$ kann nicht $yy = 0$ geschlossen werden, aber aus $y = 2x$, $4x = 0$ folgt $yy = 4x \cdot x = 0$).

Anknüpfend an 2. heben wir schliesslich noch folgende Formulierung hervor:

Die Erzeugenden eines freien assoziativen Ringes erzeugen hinsichtlich der Kommutatorbildung $A \circ B = AB - BA$ einen freien Lieschen Ring.

Zusatz bei der Korrektur: Wie mir freundlicherweise Herr Lazard mitteilt, hat inzwischen A. I. Schirschov (Usp. Mat. N. VII, 5 (57), S. 173-176) einen Lieschen Ring mit passendem Operatorenbereich Ω angegeben, der keine treuen assoziativen Darstellungen besitzt.

L I T E R A T U R

- BIRKHOFF, G., Representability of Lie algebras and Lie groups by matrices. Ann. Math. II, s. 38, 526 - 532 (1937).
- KOUROCHKINE, V. M., Die Darstellung Liescher Ringe in assoziativen Ringen. Mat. Sbornik, 28 (70), 2, 467 - 472 (1951).
- LAZARD, M., Sur les algèbres enveloppantes universelles de certaines algèbres de Lie. C. r. Acad. Sci., Paris 234, 788 - 791 (1952).
- MAGNUS, W., Über Beziehungen zwischen höheren Kommutatoren, Crelles J. 177, 105 - 115 (1937).
- WITT, E., Treue Darstellung Liescher Ringe, Crelles J. 177, 152 - 160 (1937).