

# Über Lie'sche Ringe mit Primzahlcharakteristik.

Von HANS ZASSENHAUS in Hamburg.

## Inhalt.

	Seite
Einleitung .....	1
<b>I. Allgemeine Theorie der Lie'schen Ringe.</b> .....	<b>7</b>
§ 1. Lie'sche Ringe und Unterringe .....	7
(1. Lie'sche Ringe, 2. Komplexrechnung, 3. Homomorphiebegriff, 4. Abelsche und auflösbare Lie'sche Ringe, Radikal, Kern, 5. Nilpotente Lie'sche Ringe, 6. Einfache Lie'sche Ringe, 7. Zerfallbare Lie'sche Ringe, 8. Die Diskriminante eines Lie'schen Ringes.)	
§ 2. Aufspaltung Lie'scher Ringe nach Cartan .....	24
(1. Der Satz von Engel, 2. Produktdarstellungen, 3. Eigenwertverteilungen auf nilpotenten Lie'schen Ringen, 4. Aufspaltung Lie'scher Ringe in Eigenmoduln nilpotenter Teilringe.)	
§ 3. Einfachheitsbeweise .....	34
§ 4. Die Endomorphismen eines Lie'schen Ringes .....	49
<b>II. Darstellungstheorie nilpotenter Lie'scher Ringe</b> .....	<b>61</b>
§ 1. $(L, \sigma)$ -Moduln .....	61
§ 2. Potenzringe von Lie'schen $k$ -Ringern .....	64
§ 3. Konstruktion von $(L, \sigma)$ -Moduln .....	68
§ 4. $\sigma$ -einfache Lie'sche Ringe .....	74
§ 5. Bestimmungen der endlichen irreduziblen $(L, \sigma)$ -Moduln über algebraisch abgeschlossenen Grundkörper .....	81
§ 6. Eine Identität .....	89
§ 7. Eigenfunktionen und irreduzible Darstellungen von nilpotenten Lie'schen Ringen .....	95

Ausgegangen bin ich bei meinen Untersuchungen von den folgenden beiden Wahrnehmungen:

1. Der Satz von ENGEL gilt allgemein<sup>1)</sup>.
2. Bei Charakteristik  $p > 0$  gilt das folgende Analogon der Hausdorffschen Formel:

$$(1) \quad (x + y)^p = x^p + y^p + L(x, y),$$

wobei  $L(x, y)$  ein aus  $x$  und  $y$  durch Anwendung der Kreismultiplikation:  $u \circ v = uv - vu$  und Addition aus  $x$  und  $y$  hervorgegangener homo-

---

<sup>1)</sup> Ein Lie'scher Ring von endlichem Rang über einen Körper ist genau dann nilpotent, wenn schon wiederholtes Klammern mit jedem festen Element stets zu Null führt. — Ein Beweis ist von ZORN veröffentlicht worden, wie ich nachträglich aus dem Zentralblatt ersehen habe.

gener Ausdruck  $p$ -ten Grades ist<sup>1)</sup>. Z. B.  $(x + y)^2 = x^2 + y^2 + x \circ y$  bei char. 2.

Bei dem von mir zum Beweise der Formel eingeschlagenen Wege habe ich mit Hilfe der von MAGNUS stammenden Theorie der Dimensionsgruppen zuerst die *HALLSche Formel*:

$$(2) \quad (xy)^p = x^p y^p C(xy)^p D(x, y)$$

bewiesen, in der  $x$  und  $y$  Erzeugende einer freien Gruppe  $\mathfrak{F}$  sind,  $C(x, y)$  in der Kommutatorgruppe von  $\mathfrak{F}$  liegt und  $D(x, y)$  im  $p$ -ten Glied der absteigenden Zentralreihe enthalten ist. Nimmt man nur die Anfangsglieder in den MAGNUSschen Entwicklungen der Gruppenelemente in Potenzreihen, so stellt sich Formel (1) als Analogon zu Formel (2) heraus, wenn statt Multiplikation in Gruppen Addition im Lie'schen Ring und statt Kommutatorbildung in Gruppen Klammermultiplikation in Lie'schen Ringen gesetzt wird<sup>2)</sup>.

3. Habe ich bemerkt, daß sich jeder endlichen  $p$ -Gruppe  $\mathfrak{G}$  ein nilpotenter Lie'scher Ring  $L_{\mathfrak{G}}$  mit der Charakteristik  $p$  eindeutig zuordnen läßt, so daß sich aus der Struktur von  $L_{\mathfrak{G}}$  die Struktur von  $\mathfrak{G}$  weitgehend bestimmen läßt.

Wie man umgekehrt von einem nilpotenten Lie'schen Ring mit Primzahlcharakteristik  $p$  zu einer  $p$ -Gruppe gelangt, habe ich noch nicht beantworten können.

Ich möchte eine Vorarbeit leisten zur Aufstellung aller einfachen Lie'schen Ringe vom endlichen Range über einem algebraisch abgeschlossenen Körper mit Primzahlcharakteristik.

Die entsprechende Aufgabe im Fall der Charakteristik 0 hat CARTAN gelöst. Nach der Methode von CARTAN sucht man zu gegebenem Lieschen Ring  $L$  mit endlichem Range  $r$  über einem algebraisch abgeschlossenen Grundkörper  $k$  eine Basis  $l_1, l_2, \dots, l_r$ , ordnet jedem Element  $x$  aus  $L$  vermöge der Multiplikationsregel  $x \circ l_i = \sum_{k=1}^r \alpha_{ik}^x l_k$  die Matrix  $x = (\alpha_{ik}^x)$  zu<sup>3)</sup>, sucht sich ein Element  $h$  aus, dessen zugeordnete Matrix  $\bar{h}$  möglichst viele verschiedene Eigenwerte hat und bettet  $h$  in einen möglichst großen nilpotenten Teilring  $H$  von  $L$  ein. Darauf wird  $L$  in

<sup>1)</sup> Die HAUSDORFFSche Formel ist ein Additionstheorem für die  $e$ -Funktion bei nichtkommutativen Variablen. Bei Charakteristik  $p > 0$  ist die  $e$ -Funktion durch  $x^p$  zu ersetzen.

<sup>2)</sup> Die Anregung zu meinen Untersuchungen verdanke ich Bemerkungen von Herrn ARTIN und dem Studium der MAGNUSschen Arbeiten. Einen direkten Beweis der Formel (1) hat mir ARTIN mitgeteilt. — Wie mir E. WITT kürzlich mitteilte, hat er die Feststellungen 1. und 2. schon vor längerer Zeit gemacht.

<sup>3)</sup> Die Abbildung  $x \rightarrow \bar{x}$  ist die reguläre Darstellung von  $L$  in Matrizen.

eine direkte Summe von Eigenmoduln nach  $H$  zerlegt:

$$L = L_0 + L_\alpha + L_\beta + \dots,$$

so daß  $L_0, L_\alpha, L_\beta, \dots$  aus allen Elementen von  $L$  besteht, die zu den (lauter verschiedenen) Eigenwert(verteilung)en  $0, \alpha, \beta, \dots$  gehören. Da  $H$  nilpotent ist, so liegt  $H$  in  $L_0$  und aus dem Satz von ENGEL folgt, daß sogar  $H = L_0$  ist. Setzen wir weiter voraus, daß  $L$  ein einfacher Lie'scher Ring ist, so zeigt CARTAN bei Charakteristik 0, daß  $H$  abelsch ist, d. h. daß  $h \circ h' = 0$  für alle  $h, h'$  aus  $H$  ist, ferner zeigt CARTAN, daß die Eigenmoduln  $L_\alpha$  ( $\alpha \neq 0$ ) alle eingliedrig sind. Auf diesen beiden Tatsachen fußend, führt CARTAN die Bestimmung aller endlichen einfachen Lie'schen Ringe bei Charakteristik 0 aus.

In allen mir bekannten einfachen Lie'schen Ringen mit Primzahlcharakteristik  $p$  ist  $H$  abelsch. Dagegen ist die Dimension der Eigenmoduln  $L_\alpha, L_\beta, \dots$  gleich 2 in den einfachen Lie'schen Ringen, die aus den Matrizenringen<sup>1)</sup> über einem Grundkörper mit Charakteristik 2 durch Ableitung und Bildung des Faktorringes nach dem Zentrum entstehen.

Als Hilfsmittel für den Nachweis, daß  $H$  abelsch ist, benutzt CARTAN die Tatsache, daß die Diskriminante eines einfachen Lie'schen Ringes von endlichem Range über einem Körper der Charakteristik Null von Null verschieden ist. Das ist nicht mehr wahr bei Primzahlcharakteristik. Ein Gegenbeispiel bilden die durch Ableitung und Bildung des Faktorringes nach dem Zentrum aus den Matrizenringen  $p$ l-ten Grades entstehenden einfachen Lie'schen Ringe, ferner eine Reihe von WITT angegebener Typen<sup>2)</sup>.

Bei Primzahlcharakteristik habe ich keinen Beweis dafür gefunden, daß  $H$  abelsch sein muß.

Ich nehme daher vorläufig an, daß es einfache Lie'sche Ringe mit Primzahlcharakteristik gibt, in denen der nach CARTAN konstruierte maximal nilpotente Teilring  $H$  nicht abelsch ist und die Eigenmoduln nicht mehr eingliedrig sind.

Die Eigenmoduln  $L_\alpha, L_\beta, \dots$  vermitteln vermöge der Zuordnung  $h \rightarrow \begin{pmatrix} x_\alpha \\ h \circ x_\alpha \end{pmatrix}$  Darstellungen von  $H$  in linearen Transformationen. Es entsteht die Aufgabe, *alle irreduziblen Darstellungen eines nilpotenten*

<sup>1)</sup> Grad der Matrizenringe  $> 2$ .

<sup>2)</sup>  $M$  sei ein Teilmodul aus endlich vielen Elementen eines Körpers  $k$  mit Primzahlcharakteristik  $p$ . Jedem Element  $\alpha$  aus  $M$  ordnen wir ein Basiselement  $e_\alpha$  eines Lie'schen Ringes  $L$  über  $k$  zu und setzen fest:  $e_\alpha \circ e_\beta = (\alpha - \beta) e_{\alpha + \beta}$ . Man bestätigt leicht die Gültigkeit der Jakobiidentität. Wenn  $p > 2$ , so ist  $L$  einfach. Die Diskriminante von  $L$  ist 0, wie man entweder direkt nachrechnen kann oder aus einem allgemeinen Satz entnimmt.

*r*-gliedrigen Lie'schen Ringes *H* über einem algebraisch abgeschlossenen Körper *k* aufzufinden.

Bei Charakteristik Null gilt der Satz von LIE:

1. Der Grad jeder irreduziblen Darstellung von *H* ist 1.
2. Jede Darstellungsmatrix hat nur einen Eigenwert, so daß dem Element *h* aus *H* eindeutig ein Eigenwert aus *k* zugeordnet ist.
3. Die Eigenwerte bilden eine Linearform. Wenn also die Eigenwerte zu den Elementen einer Basis von *H* über *k* bekannt sind, dann ist damit die ganze Eigenwertverteilung bekannt. Bei Primzahlcharakteristik *p* habe ich erhalten:

1. Der Grad jeder irreduziblen Darstellung ist eine *p*-Potenz (ev.  $p^0$ ).
2. Bei einer irreduziblen Darstellung  $h \rightarrow \bar{h}$  von *H* in Matrizen hat die Matrix  $\bar{h}$  nur einen Eigenwert  $\alpha_h$ .
3. Wird eine geeignete Basis von *H* über *k* gewählt<sup>1)</sup>, dann ist die ganze Eigenwertverteilung schon eindeutig durch die Eigenwerte der *r*-Basiselemente und die Struktur von *H* bestimmt.

Allerdings ist der Eigenwert  $\alpha_h$  von *h* keine Linearform der Eigenwerte der Basiselemente, sondern im allgemeinen wird  $\alpha_h$  eine Linearkombination aus gewissen *p*'-ten Wurzeln von Polynomen *p*'-ten Grades in den Komponenten  $\lambda_1, \lambda_2, \dots, \lambda_r$ . Zum Beweise dieser Tatsache wird die Formel (1) verwendet.

4. Die irreduziblen Darstellungen von *H* lassen sich explizite angeben, vorausgesetzt, daß die irreduziblen Darstellungen für geeignete echte Teilringe von *H* schon bekannt sind<sup>2)</sup>.

Eigenwertverteilung und irreduzible Darstellung bestimmen sich gegenseitig eineindeutig.

Dies ist das Hauptergebnis der bisher von mir geführten Untersuchung.

Hieran möchte ich die Bemerkung anschließen, daß ich die Lie'schen Ringe mit Primzahlcharakteristik nicht nur um ihrer selbst willen untersuche, sondern auch aus dem Grunde, weil die Vermutung besteht, daß zwischen Lie'schen Ringen aus endlich vielen Elementen und den endlichen Gruppen eine sinnvolle Beziehung besteht auf zweierlei Art:

1. Den Aussagen in Gruppen über Kommutatorbildung und Multiplikation entsprechen ähnliche Aussagen über Kreismultiplikation und Addition in Lie'schen Ringen.

<sup>1)</sup> Nämlich eine Basis  $h_1, h_2, \dots, h_r$ , so daß  $h_i \circ h_k$  in  $\{h_{i+1}, h_{i+2}, \dots, h_r\}$  enthalten ist (insbesondere:  $h_r \circ h_k = 0$ ).

<sup>2)</sup> Bei der Aufstellung der irreduziblen Darstellungen überlegt man sich, wie man eine irreduzible Darstellung eines Teilringes vom Range  $r - 1$  einbetten kann in eine irreduzible Darstellung des ganzen Ringes. Indem man gleichzeitig die assoziativen Einbettungsringe betrachtet, kommt man zwangsläufig zu den Ergebnissen.

2. Man kann versuchen, jeder endlichen Gruppe nach Möglichkeit eindeutig einen Lie'schen Ring aus endlich vielen Elementen zuzuordnen, so daß sich Fragen über die endliche Gruppe in Fragen über den zugeordneten Lie'schen Ring verwandeln lassen, ähnlich wie es in der Theorie der kontinuierlichen Gruppen geschieht.

Nach dem ersten Gesichtspunkt habe ich die allgemeine Theorie der Lie'schen Ringe weitgehend der Gruppentheorie angeglichen und dabei auch neue Ergebnisse erhalten. Z. B. gilt die SCHREIERSche Erweiterungstheorie auch für Lie'sche Ringe einschließlich des Satzes von ARTIN über die Konstruktion der Zerfallungsgruppe. Ferner lassen sich die HALLSchen Sätze und Begriffe aus der Theorie der  $p$ -Gruppen auf die Theorie der nilpotenten Lie'schen Ringe übertragen<sup>1)</sup>. — Dem Satz von ENGEL über die Kennzeichnung der nilpotenten Lie'schen Ringe entspricht der folgende Satz der Gruppentheorie: Wenn in einer endlichen Gruppe Kommutatorbildung mit jedem festen Element genügend oft fortgesetzt stets zu 1 führt, so führt überhaupt jede Kommutatorbildung genügend oft wiederholt immer zu 1<sup>2)</sup>. Endliche Gruppen, in denen jede genügend oft wiederholte Kommutatorbildung zu 1 führt, habe ich nilpotent genannt. Sie sind direktes Produkt ihrer Sylowgruppen. Also ist die Theorie endlicher nilpotenter Gruppen gleichwertig mit der Theorie der  $p$ -Gruppen.

Nach dem zweiten von ARTIN herrührenden Gesichtspunkt habe ich z. B. jeder  $p$ -Gruppe einen nilpotenten Lie'schen Ring mit Primzahlcharakteristik zugeordnet. Für beliebige endliche Gruppen ist noch kein Verfahren der Zuordnung gefunden worden. Es ist noch nicht einmal bekannt, welche Charakteristik der Lie'sche Ring haben soll. Jedenfalls muß sie in der Gruppenordnung aufgehen. Es wäre dann zu wünschen, daß sich die Aufstellung der endlichen einfachen Gruppen auf die Aufstellung der einfachen Lie'schen Ringe aus endlich vielen Elementen zurückführen läßt<sup>3)</sup>. Interessanter wäre die Lösung der

<sup>1)</sup> Dort liefern sie allerdings keine tiefsinnigen Aussagen.

<sup>2)</sup> Beweis leicht durch Induktion nach der Gruppenordnung und Anwendung der Sätze über Verlagerung in eine Untergruppe.

<sup>3)</sup> Schwierig ist der Weg von der endlichen einfachen Gruppe zu dem einfachen Lie'schen Ring. Der Weg in umgekehrter Richtung ist leicht, denn schon in der Theorie der kontinuierlichen Gruppen braucht man nicht die HAUSDORFFSche Formel anzuwenden, sondern kann direkt durch *Bildung der Automorphismengruppe und Aufsuchen der nicht auflösbaren Kompositionsfaktoren* vom einfachen Lie'schen Ring zur einfachen kontinuierlichen Gruppe gelangen. Dieses Verfahren läßt sich auf Lie'sche Ringe aus endlich vielen Elementen übertragen. Von Interesse wäre es, die Automorphismengruppen der von WITT gefundenen Typen zu untersuchen, vielleicht ergeben sich neue einfache endliche Gruppen.

Der Weg vom einfachen Lie'schen Ring über algebraisch abgeschlossenen Grundkörper zu Lie'schem Ring über einem Galoisfeld ist leicht.

Aufgabe der Bestimmung aller endlichen einfachen Gruppen nach dem ersten Gesichtspunkt. Es würde sich dabei um ein sinnvolles Äquivalent der CARTANSchen Methode in Gruppen handeln.

Fassen wir z. B. die Ikosaedergruppe auf als Gruppe aller 2-reihigen Kollineationen mit Determinante 1 über dem Körper aus fünf Elementen, so haben wir an die Stelle des maximal nilpotenten Lie'schen Teilringes  $H$  zu setzen:  $\mathfrak{H} = ((2\ 3)(4\ 5))$  und an die Stelle der Eigenmoduln  $L_\alpha, L_\beta$  die beiden Gruppen

$$\mathfrak{L}_\alpha = ((1\ 2\ 4\ 5\ 3)),$$

$$\mathfrak{L}_\beta = ((1\ 2\ 5\ 4\ 3)),$$

die von den beiden Elementen aus  $\mathfrak{H}$  in sich transformiert werden. Wollten wir der Ikosaedergruppe einen einfachen Lie'schen Ring zuordnen, so müßten wir das Analogon zu dem der linearen Gruppe im Kontinuierlichen zugeordneten Lie'schen Ringe suchen. Das wäre die Ableitung des Matrizenringes zweiten Grades über den Körper aus fünf Elementen mit den folgenden drei Basiselementen  $e_{11} - e_{22}, e_{12}, e_{21}$ , wobei die Rechenregeln

$$(e_{11} - e_{22}) \circ (e_{11} - e_{22}) = e_{12} \circ e_{12} = e_{21} \circ e_{21} = 0,$$

$(e_{11} - e_{22}) \circ e_{12} = 2e_{12}, \quad (e_{11} - e_{22}) \circ e_{21} = -2e_{21}, \quad e_{12} \circ e_{21} = e_{11} - e_{22}$  gelten, so daß

$$H = \{e_{11} - e_{22}\}, \quad L_\alpha = \{e_{12}\}, \quad L_\beta = \{e_{21}\}.$$

Entsprechende Überlegungen lassen sich aufstellen, wenn die Ikosaedergruppe als Gruppe der 2-reihigen Matrizen mit Determinante 1 und Koeffizienten aus dem Galoisfeld aus vier Elementen aufgefaßt wird<sup>1)</sup>.

Die Behandlungsweise nach dem ersten Gesichtspunkt ist insofern interessanter, als sie auch eine neue Methode zur Behandlung kontinuierlicher Gruppen liefert. Die Aufgabestellung lautet dann etwa so: Gegeben sei eine endliche einfache kontinuierliche Gruppe, an Stelle Klammersmultiplikation der infinitesimalen Transformationen wende man Kommutatorbildung der endlichen Transformationen an und führe die CARTANSche Theorie direkt in der Gruppe durch, ohne erst zum Ring der infinitesimalen Transformationen überzugehen. Da bekanntlich außer endlich vielen Ausnahmetypen nur geometrische Gruppen erhalten werden, so entsteht die folgende Frage:

<sup>1)</sup> Will man die Überlegung für irgendeine endliche Gruppe machen, so wird man auf folgenden noch unbewiesenen Satz geführt: *Eine endliche einfache Gruppe, in der jede Sylowgruppe ihr eigener Normalisator ist, hat Primzahlpotenzordnung.* Auf diesen Satz bin ich auch bei der Untersuchung der endlichen Fastkörper gestoßen. Der Beweis wäre sehr wichtig.



Setzen wir in Gruppen  $(a, b) = a b a^{-1} b^{-1}$ ,  $(a, b, c) = (a, (b, c))$ ,  $a^x = x a x^{-1} = (x, a) a$ , so entsprechen den Regeln (1)–(3) die Regeln

$$(1'a) \quad (a, bc) = (a, b)(a, c)^b,$$

$$(1'b) \quad (bc, a) = (c, a)^b(b, a),$$

$$(2') \quad (a, a) = e,$$

$$(3') \quad (a, b, c)(b, c, a)(c, a, b) = (b, c)^a(c, b)(c, a)^b(c, b)^a(a, b)(a, c)^b(b, c)(b, a)$$

(Identität von WITT).

Die Addition im Lie'schen Ring ist kommutativ, dagegen die Multiplikation in einer Gruppe im allgemeinen nicht. Daher muß die Übertragung vorsichtig geschehen.

Es sei  $k$  ein kommutativer Ring mit Einheits-Element. Ein Modul  $\mathfrak{M}$  heie  $k$ -Modul, wenn fur jeden Skalar  $\lambda$  aus  $k$  und jedes Element  $u$  aus  $\mathfrak{M}$  eindeutig das Produkt  $\lambda u$  als Element aus  $\mathfrak{M}$  erklart ist. so da

$$(4) \quad \lambda(u + v) = \lambda u + \lambda v, \quad (\lambda + \mu)u = \lambda u + \mu u, \quad (\lambda \mu)u = \lambda(\mu u),$$

$$(5) \quad 1u = u^1).$$

Beispiel: Die  $n$ -dimensionalen  $k$ -Vektormoduln. Als  $n$ -gliedrige  $k$ -Moduln mogen alle  $k$ -Moduln bezeichnet werden, die operatorisomorph zum  $n$ -dimensionalen Vektormodul sind.

Ein Lie'scher Ring heit *Lie'scher  $k$ -Ring*, wenn er ein  $k$ -Modul ist, in dem die Rechenregel  $\lambda(u \circ v) = (\lambda u) \circ v = u \circ (\lambda v)$  gilt. Ein Lie'scher  $k$ -Ring heie  $n$ -gliedrig, wenn er als  $k$ -Modul betrachtet,  $n$ -gliedrig ist.

*Ein distributiver  $k$ -Ring  $L$ , der durch Addition, Subtraktion und Multiplikation mit Elementen aus  $k$  aus der Teilmenge  $K$  erzeugt wird, ist dann und nur dann ein Lie'scher Ring, wenn:*

$$\text{I} \quad x \circ x = 0,$$

$$\text{II} \quad x \circ y + y \circ x = 0,$$

$$\text{III} \quad x \circ (y \circ z) + y \circ (z \circ x) + z \circ (x \circ y) = 0$$

fur alle  $x, y, z$  aus  $K$ .

Der Beweis ist klar.

Auf Grund dieses Satzes konstruieren wir Lie'sche  $k$ -Ringe in folgender Weise. Zunchst ist ein distributiver Ring  $L$  mit der  $k$ -Basis  $B = (\dots u \dots v \dots)$  eindeutig bestimmt durch jedes System von „Zusammensetzungskonstanten“, fur das bei festem  $u, v$  nur endlich viele  $\gamma_{uv}^x$

1) Es werden nur eigentliche  $k$ -Moduln betrachtet.



von Null verschieden sind. Nämlich  $L$  ist gleich der Menge aller formalen Summen  $\sum \lambda_u u$  ( $\lambda_u \in k$ ), in denen nur endlich viele Koeffizienten  $\lambda_u$  von Null verschieden sind, mit den Rechenregeln:

$$\begin{aligned} (\sum \lambda_u u) + (\sum \mu_u u) &= \sum (\lambda_u + \mu_u) u, \\ \lambda \cdot (\sum \lambda_u \cdot u) &= \sum (\lambda \cdot \lambda_u) \cdot u, \\ (\sum \lambda_u u) \circ (\sum \mu_v v) &= \sum_x (\sum_u \sum_v \lambda_u \mu_v \gamma_{uv}^x) \cdot x, \end{aligned}$$

und es folgt nun:

Der eben konstruierte distributive Ring  $L$  mit der Basis  $B = (\dots u \dots \dots v \dots w \dots)$  über  $k$  ist dann und nur dann ein Lie'scher Ring, wenn für die Zusammensetzungsconstanten  $\gamma_{uv}^x$  die Bedingungen:

$$\begin{aligned} \text{I} \quad & \gamma_{uu}^x = 0. \\ \text{II} \quad & \gamma_{uv}^x + \gamma_{vu}^x = 0. \\ \text{III} \quad & \sum_y (\gamma_{uy}^x \gamma_{vw}^y + \gamma_{vy}^x \gamma_{wu}^y + \gamma_{wy}^x \gamma_{uv}^y) = 0. \end{aligned}$$

erfüllt sind.

*Bemerkung:* Die Bedingungen I, II, III sind nicht alle voneinander unabhängig. Wenn II für das Paar  $(u, v)$  gilt, so auch für das Paar  $(v, u)$ . Wenn ferner in einem Tripel  $(u, v, w)$  zwei Komponenten einander gleich sind, so folgt III aus I und II. Wenn schließlich III für ein Tripel  $(u, v, w)$  gilt, so gilt III auf Grund von I und II auch für alle Tripel, die aus dem gegebenen durch Permutation der Komponenten entstehen.

$k$ -Schiefringe sind stets Lie'sche  $k$ -Ringe. Wir verabreden, daß jede Multiplikation der Addition vorangeht, daß die gewöhnliche Multiplikation der Kreismultiplikation vorangeht und daß jedes Funktionszeichen der Multiplikation und der Addition vorangeht, z. B.

$$\begin{aligned} a \circ b + c &= (a \circ b) + c, \\ a \cdot b \circ c &= (a \cdot b) \circ c, \\ \sigma a \circ b &= (\sigma a) \circ b, \\ \sigma a + b &= (\sigma a) + b. \end{aligned}$$

Eine nicht leere Teilmenge  $U$  von  $L$  heißt *Lie'scher  $k$ -Teilring*, wenn mit  $a$  und  $b$  auch  $a + b$ ,  $\lambda a$  und  $a \circ b$  in  $U$  enthalten sind.  $U$  ist mit den in  $L$  erklärten Verknüpfungen ein Lie'scher  $k$ -Ring.

## 2. Komplexrechnung.

Jede Teilmenge von  $L$  heiße *Komplex*. Die Vereinigungsmenge von zwei Komplexen  $U$  und  $V$  werde mit  $U \cup V$  bezeichnet, der Durchschnitt

mit  $U \cap V$ . Als Summe  $U + V$  bzw. Kreisprodukt  $U \circ V$  von  $U$  und  $V$  werde die Menge aller  $u + v$  bzw.  $u \circ v$  mit  $u \in U, v \in V$  bezeichnet. Der von dem Komplex  $U$  erzeugte  $k$ -Modul werde mit  $\{U\}$  bezeichnet. Außer anderen leicht abzuleitenden Rechenregeln gilt

$$(5a) \quad \{U \circ V\} = \{V \circ U\} = \{\{U\} \circ \{V\}\}.$$

Aus der Jakobiidentität folgt für beliebige Komplexe  $U, V, W$

$$(6) \quad U \circ (V \circ W) \subseteq V \circ (W \circ U) + W \circ (U \circ V).$$

$K$  und  $U$  seien zwei Komplexe. Wir setzen

$$\underline{K}^0 U = U, \quad \underline{K} U = K \circ U, \quad \underline{K}^i U = \underline{K}(\underline{K}^{i-1} U) \quad (i = 1, 2, \dots).$$

Es gelten die Regeln

$$(7a) \quad \{\underline{K}^i \{U\}\} = \{\underline{K}^i U\},$$

$$(7b) \quad \underline{K}^i(\underline{K}^k U) \subseteq \{\underline{K}^{i+k} U\}.$$

1. Beweis: (7a) folgt durch mehrfache Anwendung von (5a). Ferner ist (7b) für  $i = 0, 1$  klar, sei  $i > 1$  und schon bewiesen, daß

$$\underline{K}^{i-1}(\underline{K}^k U) \subseteq \{\underline{K}^{i+k-1} U\}.$$

Dann folgt:

$$\begin{aligned} \underline{K}^i(\underline{K}^k U) &= \underline{K}(\underline{K}^{i-1}(\underline{K}^k U)) \subseteq \underline{K}\{\underline{K}^{i+k-1} U\} \subseteq \{\underline{K}\{\underline{K}^{i+k-1} U\}\} \\ &= \{\underline{K}(\underline{K}^{i+k-1} U)\} = \{\underline{K}^{i+k} U\}. \end{aligned}$$

Wir setzen

$$\underline{K}^{i-1} K = K^{[i]} \quad (i = 1, 2, \dots).$$

Dann gilt

$$K^{[i]} \circ K^{[k]} \subseteq \{K^{[i+k]}\},$$

also ist

$$(8) \quad \{\underset{\circ}{K}\} = \{K^{[1]}\} + \{K^{[2]}\} + \{K^{[3]}\} + \dots$$

ein Lie'scher  $k$ -Teilring. Er heißt der von  $K$  erzeugte Teilring. Jeder Lie'sche  $k$ -Teilring, der  $K$  enthält, enthält auch  $\{\underset{\circ}{K}\}$ .

Weitere Verfahren zur Bildung von Lie'schen  $k$ -Teilringen:

1. Ein  $k$ -Teilring eines  $k$ -Teilringes ist ein  $k$ -Teilring.
2. Der Durchschnitt zweier  $k$ -Teilringe ist ein  $k$ -Teilring.
3. Der Normalisator  $N(K)$  des Komplexes  $K$  ist die Menge aller  $x$  aus  $L$ , für die  $x \circ K \subseteq \{K\}$ . Es ist klar, daß  $N(K)$  ein  $k$ -Modul ist. Es gilt für alle  $x$  aus  $N(K)$ :

$$x \circ \{K\} \subseteq \{K\}, \text{ also } NK = N\{K\}.$$

Ferner für alle  $x$  und  $y$  aus  $N(K)$ :

$$\begin{aligned} (x \circ y) \circ \{K\} \\ \subseteq x \circ (y \circ \{K\}) + y \circ (x \circ \{K\}) &\subseteq x \circ \{K\} + y \circ \{K\} \\ \subseteq \{K\} + \{K\} &\subseteq \{K\}. \end{aligned}$$

Also ist  $N(K)$  ein Lie'scher  $k$ -Ring.

4. Der Zentralisator  $Z(K)$  des Komplexes  $K$  ist die Menge aller  $x$  für die  $x \circ K = 0$ .  $Z(K)$  ist ein Lie'scher  $k$ -Teilring.
5. Wenn der  $k$ -Teilring  $V$  im Normalisator des  $k$ -Teilrings  $U$  enthalten ist, dann ist auch  $U + V$  ein  $k$ -Teilring.

### 3. Homomorphiebegriff.

Die eindeutige Abbildung  $a \rightarrow A$  eines Lie'schen  $k$ -Ringes  $L$  auf Elemente  $A$  des Lie'schen  $k$ -Ringes  $\bar{L}$  heißt *Homomorphie* von  $L$  in  $\bar{L}$ , wenn  $a + b \rightarrow A + B$ ,  $\lambda a \rightarrow \lambda A$ ,  $a \circ b \rightarrow A \circ B$ . Alle Bildelemente  $A$  bilden einen Lie'schen  $k$ -Ring  $L^*$ , den Bildring.  $L^*$  ist *homomorph* zu  $L$ . Falls die Abbildung von  $L$  in  $\bar{L}$  umkehrbar eindeutig ist, so heißt sie *Isomorphie*.  $L$  und  $L^*$  sind dann *isomorph* (aufeinander abgebildet).

Eine Homomorphie von  $L$  in einen  $k$ -Schiefring  $\mathfrak{S}$  heißt *Darstellung* von  $L$  in dem  $k$ -Schiefring  $\mathfrak{S}$ . Dabei wird insbesondere gefordert: Wenn  $a \rightarrow A$ ,  $b \rightarrow B$ , so  $a \circ b \rightarrow AB - BA$ . Der Bildring heißt auch *Darstellungsring*.

Die Darstellung heißt *treu*, wenn es sich um eine Isomorphie handelt.

Ein  $k$ -Modul  $\mathfrak{M}$  heißt *Darstellungsmodul* von  $L$ , wenn eine Multiplikation der Elemente  $u$  aus  $\mathfrak{M}$  von links her mit Elementen  $a$  aus  $L$  eindeutig erklärt ist, so daß  $au$  in  $\mathfrak{M}$  liegt, ferner:

$$\begin{aligned} a(u + v) &= au + av, & (a + b)u &= au + bu, \\ (\lambda a)u &= a(\lambda u) = \lambda(au), \\ (a \circ b)u &= a(bu) - b(au). \end{aligned}$$

Jedem Element  $a$  aus  $L$  ist also eine lineare Transformation  $A$  von  $\mathfrak{M}$  eindeutig zugeordnet, wobei  $A$  definiert ist durch:  $Au = au$ . Die Abbildung  $a \rightarrow A$  ist eine Darstellung von  $L$  in linearen Transformationen von  $\mathfrak{M}$ . — Wenn umgekehrt die Abbildung  $a \rightarrow A$  eine Darstellung von  $L$  in linearen Transformationen des  $k$ -Moduls  $\mathfrak{M}$  ist, so wird  $\mathfrak{M}$  durch die Festsetzung  $au = Au$  zu einem Darstellungsmodul.

Ein im Darstellungsmodul  $\mathfrak{M}$  enthaltener  $k$ -Modul  $\mathfrak{m}$  heißt *invarianter Teilmodul*, wenn  $L\mathfrak{m} \subseteq \mathfrak{m}$ , d. h. wenn  $\mathfrak{m}$  ebenfalls Darstellungsmodul ist. Der Faktormodul  $\mathfrak{M}/\mathfrak{m}$  ist ebenfalls ein  $L$ -Modul, wobei definiert

wird  $a(u + m) = au + m$ . Wie üblich werden jetzt die Begriffe *äquivalente, reduzible, irreduzible, halbreduzible, vollreduzible, zerfällbare, unzerfällbare* Darstellungsmodul bzw. Darstellungen erklärt.

Falls  $k$  ein Körper und der Darstellungsmodul  $n$  Basiselemente über  $k$  hat, so sagen wir, daß die zugehörige Darstellung den Grad  $n$  hat. Eine Darstellung  $n$ -ten Grades ist halbreduzibel.

$L$  ist Darstellungsmodul von sich selbst. Dabei wird dem Element  $a$  aus  $L$  die durch

$$au = a \circ u$$

für alle  $u$  aus  $L$  erklärte lineare Transformation  $a$  von  $L$  zugeordnet. Die Abbildung  $a \rightarrow a$  ist eine Darstellung von  $\bar{L}$  in linearen Transformationen von  $L$ , die *reguläre Darstellung*.

Die invarianten Teilmoduln bei der regulären Darstellung heißen *Ideale*. Ein Ideal von  $L$  ist also ein in  $L$  enthaltener  $k$ -Modul, der mit  $u$  auch alle  $a \circ u$  enthält. Ein Ideal ist ein Lie'scher  $k$ -Teilring. Aus der Gültigkeit des Antikommutativgesetzes folgt, daß jedes Ideal zweiseitig ist. Der Restklassenmodul  $L/A$  nach dem Ideal  $A$  wird vermöge der Festsetzung  $(a + A) \circ (b + A) = a \circ b + A$  zu einem Lie'schen  $k$ -Ring, dem *Faktorring von  $L$  nach  $A$* .

**Erster Isomorphiesatz:** Bei einer Homomorphie von  $L$  bilden die auf Null abgebildeten Elemente ein Ideal und der Faktorring nach diesem Ideal ist isomorph zum Bildring.

**Zweiter Isomorphiesatz:** Wenn  $A$  Ideal von  $L$ ,  $U$  Lie'scher  $k$ -Teilring von  $L$ , so sind  $U/U \cap A$  und  $U + A/A$  zueinander isomorphe Lie'sche Ringe.

Ein halbreduzibler  $L$ -Modul  $\mathfrak{M}$  ist definiert als  $L$ -Modul mit einer  *$L$ -Kompositionsreihe*  $\mathfrak{M} = \mathfrak{M}_0 \supset \mathfrak{M}_1 \cdots \supset \mathfrak{M}_r = 0$ , so daß zwischen dem  $L$ -Modul  $\mathfrak{M}_i$  und dem  $L$ -Modul  $\mathfrak{M}_{i+1}$  kein von  $\mathfrak{M}_i$  und  $\mathfrak{M}_{i+1}$  verschiedener  $L$ -Modul enthalten ist. Die Faktormoduln  $\mathfrak{M}_i/\mathfrak{M}_{i+1}$  sind irreduzible  $L$ -Moduln. Sie heißen die zu der  $L$ -Kompositionsreihe gehörigen  *$L$ -Komponenten* von  $\mathfrak{M}$ . Die irreduziblen Komponenten einer halbreduziblen Darstellung sind nach dem Satz von JORDAN-HÖLDER-SCHREIER eindeutig bis auf Äquivalenz und Reihenfolge bestimmt. Ferner sind nach dem Satz von REMAK-SCHMIDT-FITTING die unzerfällbaren Komponenten einer halbreduziblen Darstellung bis auf Äquivalenz eindeutig bestimmt.

Wir wollen kurz die bekannten Verfahren zur Bildung von invarianten Teilmoduln eines Darstellungsmoduls  $\mathfrak{M}$  aufzählen:

1. Sei  $K$  eine nicht leere Teilmenge von  $\mathfrak{M}$ . Durch fortgesetzte Multiplikation der Elemente aus  $K$  mit Elementen aus  $k$  und aus  $L$  und durch Addition entsteht ein  $L$ -Modul  $\{K\}_L$ , der von  $K$  unter  $L$  erzeugte Modul. Jeder  $L$ -Teilmodul, der  $K$  enthält, enthält auch  $K$ .

2. Durchschnitt und Modulsumme zweier  $L$ -Teilmoduln sind wieder  $L$ -Teilmoduln.
3. Wenn der Teilmodul  $m_1$  den  $L$ -Modul  $m$  enthält und  $m_1/m$  ein  $L$ -Teilmodul von  $\mathfrak{M}/m$  ist, dann ist  $m_1$  selbst ein  $L$ -Modul.
4. Wenn  $m_1 \subseteq m_2 \subseteq m_3 \cdots$  eine aufsteigend geordnete Kette von  $L$ -Moduln ist, dann ist die Vereinigungsmenge aller  $\mathfrak{M}$  selbst ein  $\mathfrak{M}$ -Modul.
5. Wenn  $A$  Ideal von  $L$ , so bilden alle Elemente  $u$  aus  $\mathfrak{M}$ , für die  $Au = 0$ , zusammen einen  $L$ -Modul  $\mathfrak{z}(\mathfrak{M}, A)$  von  $\mathfrak{M}$ . Um das einzusehen, muß gezeigt werden, daß  $axu = 0$  für alle  $x$  aus  $L$ ,  $a$  aus  $A$ ,  $u$  aus  $\mathfrak{z}$ . Es ist aber  $axu = (a \circ x)u + x(Au) = 0$ . Nun definieren wir rekursiv die *aufsteigende  $L$ -Zentralreihe von  $\mathfrak{M}$* :

$$0 = \mathfrak{z}_0 \subseteq \mathfrak{z}_1 \subseteq \mathfrak{z}_2 \cdots \subseteq \mathfrak{z}_i \cdots,$$

wobei  $\mathfrak{z}_i/\mathfrak{z}_{i-1}$  das  $L$ -Zentrum von  $\mathfrak{M}/\mathfrak{z}_{i-1}$  ist.

6. Wenn  $A$  ein Ideal von  $L$  ist, so ist der aus  $A\mathfrak{M}$  erzeugte  $k$ -Teilmodul  $\{A\mathfrak{M}\}$  ein  $L$ -Modul. Es muß dazu gezeigt werden, daß  $xau$  in  $\{A\mathfrak{M}\}$  enthalten ist für alle  $x$  aus  $L$ ,  $a$  aus  $A$ ,  $u$  aus  $\mathfrak{M}$ . Nun ist  $xau = (x \circ a)u + a(xu)$ , und da  $x \circ a$  in  $A$ ,  $xu$  in  $\mathfrak{M}$  liegt, so liegt  $xau$  in  $\{A\mathfrak{M}\}$ .
7. *Absteigende  $L$ -Zentralreihe von  $\mathfrak{M}$* :

$$\mathfrak{z}_1 = \mathfrak{M}, \quad \mathfrak{z}_2 = \{L\mathfrak{z}_1\}, \quad \cdots, \quad \mathfrak{z}_i(\mathfrak{M}, L) = \{L\mathfrak{z}_{i-1}\}.$$

Fassen wir  $L$  als Darstellungsmodul von sich selbst auf, so erhalten wir folgende Verfahren zur Bildung von Idealen:

1. Eine beliebige nicht leere Teilmenge  $K$  von  $L$  erzeugt ein Ideal  $\{K\}_L$ .
2. Durchschnitt und Summe zweier Ideale ist wieder ein Ideal.
3. Wenn der Teilmodul  $A_1$  von  $L$  das Ideal  $A$  enthält und  $A_1/A$  Ideal von  $L/A$  ist, dann ist  $A_1$  Ideal von  $L$ .
4. Ist  $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$  eine aufsteigend geordnete Kette von Idealen, so ist die Vereinigungsmenge aller  $A_i$  selbst ein Ideal.
5. Alle Nullmacher  $x$  aus  $L$ , definiert durch  $x \circ L = 0$ , bilden ein Ideal  $\mathfrak{z}(L)$ , das *Zentrum* von  $L$ . Die *aufsteigende Zentralreihe*

$$0 = \mathfrak{z}_0 \subseteq \mathfrak{z}_1 \subseteq \mathfrak{z}_2 \cdots \subseteq \mathfrak{z}_i \subseteq \cdots$$

von  $L$  wird rekursiv definiert:  $\mathfrak{z}_0 = 0$ ,  $\mathfrak{z}_1 = \mathfrak{z}$ ,  $\cdots$ ,  $\mathfrak{z}_i/\mathfrak{z}_{i-1}$  ist das Zentrum von  $L/\mathfrak{z}_{i-1}$ .

6. Mit zwei Idealen  $A$  und  $B$  ist auch der aus  $A \circ B$  erzeugte Teilmodul ein Ideal. Es möge, da kein Mißverständnis möglich ist, ebenfalls mit  $A \circ B$  bezeichnet werden.

## 7. Die absteigende Zentralreihe

$$L = \mathfrak{Z}_1 \supseteq \mathfrak{Z}_2 \cdots$$

wird rekursiv definiert:  $\mathfrak{Z}_1 = L$ ,  $\mathfrak{Z}_2 = L \circ \mathfrak{Z}_1$ ,  $\dots$ ,  $\mathfrak{Z}_i = L \circ \mathfrak{Z}_{i-1}$ .

## 8. Die Reihe der höheren Ableitungen

$$L \supseteq D^0 L \supseteq D^1 L \supseteq D^2 L \supseteq \dots$$

wird rekursiv definiert:  $D^0 L = L$ ,  $D^1 L = L \circ L$ ,  $D^i L = D(D^{i-1} L)$  ( $i = 1, 2, \dots$ ).  $D^i L$  heißt die  $i$ -te Ableitung von  $L$ .

Eine Kette  $L = A_0 \supseteq A_1 \supseteq A_2 \cdots \supseteq A_r = 0$  aus Idealen von  $L$  heißt *Hauptreihe von  $L$  von der Länge  $r$* , wenn zwischen  $A_i$  und  $A_{i+1}$  kein von  $A_i$  und  $A_{i+1}$  verschiedenes Ideal enthalten ist. Die Faktorringe  $A_i/A_{i+1}$  heißen die zu der Hauptreihe gehörigen *Hauptfaktoren* ( $i = 0, 1, 2, \dots, r-1$ ).

Eine Kette  $L = B_0 \supseteq B_1 \supseteq B_2 \cdots \supseteq B_s = 0$  aus  $k$ -Teilringen von  $L$  heißt *Kompositionsreihe von  $L$* , wenn  $B_{i+1}$  Ideal von  $B_i$  ist und wenn zwischen  $B_i$  und  $B_{i+1}$  kein von  $B_i$  und  $B_{i+1}$  verschiedenes Ideal von  $B$  liegt. Die Faktorringe  $B_i/B_{i+1}$  heißen die zu der Kompositionsreihe gehörigen *Kompositionsfaktoren von  $L$* . Nach JORDAN-HÖLDER-SCHREIER sind die Hauptfaktoren bzw. die Kompositionsfaktoren eines Lie'schen Ringes, der eine Hauptreihe bzw. eine Kompositionsreihe besitzt, eindeutig bis auf die Reihenfolge im Sinne der Isomorphie bestimmt.

## 4. Abelsche und auflösbare Lie'sche Ringe, Radikal, Kern.

Ein Lie'scher  $k$ -Ring  $A$  heißt *abelsch*, wenn  $A \circ A = 0$ . Gleichwertig damit ist jede der beiden Aussagen  $\mathfrak{z}(A) = A$ ,  $D(A) = 0$ . Für einen beliebigen Lie'schen  $k$ -Ring  $L$  ist der Faktorring  $L/DL$  abelsch und jedes Ideal mit abelschem Faktorring enthält  $D L$ . Daher nennen wir den Faktorring  $L/D L$  den *maximal abelschen Faktorring*.

Bei einer homomorphen Abbildung  $x \rightarrow \bar{x}$  von  $L$  auf  $\bar{L}$  wird  $D L$  auf  $D \bar{L}$  abgebildet. Durch vollständige Induktion folgt:  $D^i L = D^i \bar{L}$ . Setzen wir für  $L$  den Faktorring von  $L$  nach dem Ideal  $A$  ein, so folgt:

$$(9) \quad (D^i L + A)/A = D^i(L/A).$$

Ferner folgt für jeden Lie'schen  $k$ -Teilring  $U$  von  $L$  durch vollständige Induktion:

$$(10) \quad D^i U \subseteq D^i L.$$

Der Lie'sche  $k$ -Ring  $L$  heißt *auflösbar*, wenn es einen Index  $i$  gibt, so daß  $D^i L = 0$ . Er heißt  $j$ -stufig *metabelsch*, wenn  $D^j L = 0$ , aber  $D^{j-1} L \neq 0$ . Abelsch ungleich Null ist also gleichbedeutend mit 1-stufig

metabelsch. Der Nullring heie 0-stufig metabelsch. Jeder Faktoring und jeder Teilring eines  $j$ -stufig metabelschen Lie'schen  $k$ -Ringes ist hchstens  $j$ -stufig metabelsch.

Sei  $L$  ein beliebiger Lie'scher  $k$ -Ring.

**Satz 1:** *Wenn das Ideal  $A$  und der Faktoring  $L/A$  auflsbar sind, so ist auch  $L$  auflsbar.*

Beweis: Sei  $D^k L \subseteq A$ ,  $D^r A = 0$ , dann folgt

$$D^{k+r} L = D^r (D^k L) \subseteq D^r A, \quad D^{k+r} L = 0.$$

**Satz 2:** *Wenn das Ideal  $A$  und der Teilring  $U$  auflsbar sind, so ist auch  $A + U$  auflsbar.*

Beweis: Da  $(A + U)/A \cong U/U \cap A$ , so ist  $(A + U)/A$  auflsbar, also ist nach Satz 1 auch  $A + U$  auflsbar.

Definition: Das Ideal  $R$  von  $L$  heit *Radikal* von  $L$ , wenn  $R$  ein auflsbares Ideal ist und wenn jedes Ideal von  $L$ , das  $R$  als echten Unterring enthlt, nicht mehr auflsbar ist.

**Satz 3:** *Falls das Radikal  $R$  eines Lie'schen  $k$ -Ringes  $L$  vorhanden ist, so ist es gleich der Vereinigungsmenge aller auflsbaren Ideale von  $L$ , also ist  $R$  eindeutig bestimmt.*

Beweis:  $R$  ist auflsbares Ideal von  $L$ . Wenn  $A$  beliebiges auflsbares Ideal von  $L$ , so ist  $R + A$  ein Ideal, das nach Satz 2 auflsbar ist. Da  $R$  in  $R + A$  enthalten ist, so folgt  $R = R + A$ ,  $A \subseteq R$ .

Definition: Ein Lie'scher  $k$ -Ring heit *halbeinfach*, wenn sein Radikal vorhanden und gleich Null ist.

Wenn  $A$  ein  $k$ -stufig metabelsches Ideal von  $L$  ist, so ist  $D^{k-1} A$  ein abelsches Ideal  $\neq 0$  von  $L$ , daher folgt:

*Ein Lie'scher  $k$ -Ring ist dann und nur dann halbeinfach, wenn jedes abelsche Ideal verschwindet.*

Falls das Radikal eines Lie'schen  $k$ -Ringes existiert, so ist der Faktoring nach dem Radikal halbeinfach.

Definition: Ein Lie'scher  $k$ -Ring heit *vollkommen*, wenn er mit seiner Ableitung bereinstimmt. Jeder Faktoring eines vollkommenen Ideals ist vollkommen.

**Satz 4:** *Wenn  $A$  ein vollkommenes Ideal von  $L$  und  $U$  ein vollkommener Teilring von  $L$ , so ist auch  $A + U$  ein vollkommener Teilring von  $L$ .*

Beweis: Es ist

$$DA = A, \quad DU = U, \quad A + U \supseteq D(A + U) \supseteq DA + DU = A + U, \quad \text{also}$$

$$D(A + U) = A + U.$$

**Definition:** Das Ideal  $V$  heißt *größtes vollkommenes Ideal* von  $L$ , wenn  $V$  ein vollkommenes Ideal von  $L$  ist und jedes Ideal von  $L$ , das  $V$  als echten Unterring enthält, nicht mehr vollkommen ist.

**Satz 5:** *In jedem Lie'schen  $k$ -Ring  $L$  gibt es ein und nur ein größtes vollkommenes Ideal  $V$ .  $V$  ist die Vereinigungsmenge aller vollkommenen Ideale.*

**Beweis:**  $V$  sei die Vereinigungsmenge aller vollkommenen Ideale. Da das Nullideal vollkommen ist, so ist  $V$  nicht leer. Sind  $A$  und  $B$  zwei vollkommene Ideale, so ist nach Satz 4 auch das Ideal  $A + B$  vollkommen. Demnach ist  $V$  ein  $k$ -Teilring von  $L$ . Da  $L \circ A \subseteq A$  für jedes vollkommene Ideal  $A$ , so ist auch  $L \circ V \subseteq V$ , also ist  $V$  ein Ideal von  $L$ .

Da die Ableitung von  $V$  die Ableitung jedes vollkommenen Ideales von  $L$  enthält, so ist  $DV = V$ . Nun ist klar, daß  $V$  größtes vollkommenes Ideal ist und daß jedes größte vollkommene Ideal von  $L$  mit  $V$  übereinstimmt.

Ein vollkommener  $k$ -Teilring ist in jeder Ableitung des ganzen Lie'schen Ringes enthalten.

Aus  $DA = A$  folgt nämlich  $D^i A = A$  und da  $D^i A \subseteq D^i L$ , so  $A \subseteq D^i L$ .

Wenn in dem Lie'schen  $k$ -Ring  $L$  der Minimalkettensatz für Ideale gilt, so ist jede genügend hohe Ableitung von  $L$  gleich dem größten vollkommenen Ideal. Es gibt nämlich in der Kette

$$L \supseteq DL \supseteq D^2 L \dots \supseteq D^i L \supseteq \dots$$

ein Glied, das gleich dem folgenden Gliede ist, so daß etwa

$$D^i L = D^{i+1} L,$$

also

$$D^i L = D^{i+1} L = D^{i+2} L = \dots$$

Demnach ist  $D^i L$  ein vollkommenes Ideal. Da die  $i$ -te Ableitung von  $L$  jedes vollkommene Ideal enthält, so ist  $D^i L$  größtes vollkommenes Ideal.

**Voraussetzung:** Das größte vollkommene Ideal  $V$  des Lie'schen  $k$ -Ringes  $L$  besitze ein Radikal  $RV$ . Das ist z. B. der Fall, wenn  $k$  ein Körper und  $L$  endlichgliedrig über  $k$ .

**Definition:** Der Restklassenring des größten vollkommenen Ideals nach seinem Radikal heißt der *Kern* des Lie'schen Ringes.

Der Kern ist halbeinfach und vollkommen. Er ist dann und nur dann Null, wenn der volle Lie'sche Ring auflösbar ist.



### 5. Nilpotente Lie'sche Ringe.

Definition: Ein Lie'scher  $k$ -Ring  $L$  heißt *nilpotent mit der Klasse  $c$* , wenn

$$\begin{aligned}\mathfrak{Z}_{c+1}(L) &= 0, \\ \mathfrak{Z}_c(L) &\neq 0.\end{aligned}$$

Wenn  $L = 0$ , so heißt  $L$  nilpotent mit der Klasse 0. Wir übertragen nun gewisse Aussagen von HALL über nilpotente Gruppen<sup>1)</sup>. Ein Lie'scher  $k$ -Ring  $L$  ist dann und nur dann nilpotent, wenn eine *Zentralreihe* existiert, das ist eine Kette von  $k$ -Teilringen:

$$(10a) \quad L = A_1 \supseteq A_2 \supseteq A_3 \cdots \supseteq A_{r+1} = 0,$$

so daß

$$L \circ A_i \subseteq A_{i+1} \quad (i = 1, 2, \dots, r).$$

Nämlich durch Induktion folgt:

$$(10aa) \quad \mathfrak{Z}_i(L) \subseteq A_i, \quad \mathfrak{Z}_{r+1}(L) = 0 \quad \text{und}$$

wenn umgekehrt  $L$  nilpotent mit der Klasse  $c$ , so ist:

$$(10b) \quad L = \mathfrak{Z}_1 \supset \mathfrak{Z}_2 \cdots \supset \mathfrak{Z}_{c+1} = 0$$

eine Zentralreihe mit der Länge  $c$ . Die Länge jeder Zentralreihe ist mindestens  $c$ .

Für die Zentralreihe (10a) folgt durch Induktion:

$$A_{r+1-i} \subseteq \mathfrak{Z}_i(L) \quad (i = 1, 2, \dots, r+1),$$

also

$$\mathfrak{Z}_r(L) = L.$$

Wenden wir diese Überlegung auf die Zentralreihe (10b) an, so folgt

$$\mathfrak{Z}_c(L) = L.$$

Wenn  $\mathfrak{Z}_\varrho(L) = L$ , so ist

$$L = \mathfrak{Z}_\varrho \supseteq \mathfrak{Z}_{\varrho-1} \cdots \supseteq \mathfrak{Z}_0 = 0$$

eine Zentralreihe mit der Länge 0, also ist  $\varrho \geq c$ . Demnach kann die Klasse eines Lie'schen Ringes auch aus der Relation:

$$(10c) \quad 0 = \mathfrak{Z}_0 \subset \mathfrak{Z}_1 \subset \mathfrak{Z}_2 \cdots \subset \mathfrak{Z}_c = L$$

abgelesen werden. Aus (10 a a) folgt:

$$(10d) \quad \mathfrak{Z}_i(L) \subseteq \mathfrak{Z}_{c+1-i}(L) \quad (i = 1, 2, \dots, c+1).$$

<sup>1)</sup> A contribution to the theory of groups of prime power orders. Proc. Lond. M. S. II 36.

Ferner ist:

$$(10e) \quad \mathfrak{Z}_i(L) \subseteq \mathfrak{Z}_{c-i}(L) \quad (i = 1, 2, \dots, c).$$

Denn aus  $\mathfrak{Z}_i \subseteq \mathfrak{Z}_k$  folgt durch Induktion:

$$\mathfrak{Z}_{i+j} \subseteq \mathfrak{Z}_{k-j},$$

also würde aus  $\mathfrak{Z}_i \subseteq \mathfrak{Z}_{c-i}$  der Widerspruch  $\mathfrak{Z}_c = 0$  folgen.

Wenn  $A_1 \supseteq A_2 \cdots$  eine Kette von  $k$  Unterringen des beliebigen Lie'schen  $k$ -Ringes  $L$  ist, so daß:  $L \circ A_i \subseteq A_{i+1}$  ( $i = 1, 2, \dots$ ), so werden wir zeigen, daß

$$(10f) \quad \mathfrak{Z}_i \circ A_k \subseteq A_{i+k}.$$

Das ist richtig nach Annahme über die  $A_k$ , wenn  $i = 1$ .

Es sei schon bewiesen für  $i = 1, 2, \dots, j-1$ , und es sei  $j > 1$ .

Dann ist

$$\begin{aligned} \mathfrak{Z}_j \circ A_k &= (L \circ \mathfrak{Z}_{j-1}) \circ A_k \\ &= A_k \circ (L \circ \mathfrak{Z}_{j-1}) \\ &\subseteq L \circ (\mathfrak{Z}_{j-1} \circ A_k) + \mathfrak{Z}_{j-1} \circ (A_k \circ L) \\ &\subseteq L \circ A_{k+j-1} + \mathfrak{Z}_{j-1} \circ A_{k+1} \\ &\subseteq A_{k+j} + A_{k+j} \\ &\subseteq A_{k+j}. \end{aligned}$$

Setzen wir  $A_k = \mathfrak{Z}_k$ , so folgt:

$$(10g) \quad \mathfrak{Z}_i \circ \mathfrak{Z}_k \subseteq \mathfrak{Z}_{i+k}.$$

Setzen wir

$$A_1 = \mathfrak{Z}_k, A_2 = \mathfrak{Z}_{k-1}, \dots, A_{k+1} = \mathfrak{Z}_0, A_{k+1+j} = \mathfrak{Z}_{-j} = 0,$$

so folgt:

$$(10h) \quad \mathfrak{Z}_i \circ \mathfrak{Z}_k \subseteq \mathfrak{Z}_{k-i}.$$

Mit Hilfe von (10g) wird durch Induktion bewiesen:

$$(10i) \quad D^i L \subseteq \mathfrak{Z}^i(L).$$

Demnach ist ein Lie'scher Ring, der nilpotent mit der Klasse  $c$  ist,  $k$ -stufig metabelsch, wobei  $k$  durch die Ungleichung

$$(10j) \quad 2^{k-1} \leq c$$

beschränkt ist.

Wenn  $L$  beliebig, so bildet eine homomorphe Abbildung  $\sigma$  das Ideal  $\mathfrak{Z}_i$  auf  $\mathfrak{Z}_i(\sigma L)$  ab, wie man durch Induktion beweist. Ist insbesondere  $\sigma$  die Abbildung von  $L$  auf die Restklassen nach einem Ideale  $A$ , so

folgt:

$$\mathfrak{Z}_i(L/A) = (\mathfrak{Z}_i(L) + A) / A.$$

Ferner gilt für jeden  $k$ -Unterring  $U$  von  $L$ :

$$\mathfrak{Z}_i(U) \subseteq \mathfrak{Z}_i(L).$$

*Wenn ein Lie'scher  $k$ -Ring nilpotent mit der Klasse  $c$  ist, so ist jeder Faktorring und jeder Unterring nilpotent mit einer Klasse, die nicht größer als  $c$  ist.*

Die Übertragung eines Satzes von HALL lautet:

**Satz 6:** *Liegt das Ideal  $A$  nicht in  $\mathfrak{Z}_i$ , wohl aber in  $\mathfrak{Z}_{i+1}$ , so besteht die Idealkette ohne Wiederholungen*

$$A \supset A \cap \mathfrak{Z}_i \supset A \cap \mathfrak{Z}_{i-1} \supset \dots \supset 0.$$

Beweis: Es ist

$$L \circ A \subseteq A \cap (L \circ \mathfrak{Z}_{i+1}) \subseteq A \cap \mathfrak{Z}_i.$$

Da  $A$  nicht in  $\mathfrak{Z}_i$  liegt, so liegt  $L \circ A$  nicht in  $\mathfrak{Z}_{i-1}$ , erst recht liegt  $A \cap \mathfrak{Z}_i$  nicht in  $\mathfrak{Z}_{i-1}$ . Denselben Schluß wende man auf  $A \cap \mathfrak{Z}_i$  statt auf  $A$  an usf.

*Folgerung: Jedes von Null verschiedene Ideal eines nilpotenten Lie'schen  $k$ -Ringes enthält einen von Null verschiedenen Nullmacher des ganzen Ringes.*

**Satz 7:** *In einem nilpotenten Lie'schen  $k$ -Ring  $L$  mit der Klasse  $c$  ist es möglich, von jedem  $k$ -Unterring  $U$  aus durch höchstens  $c$ -malige Normalisatorbildung zu  $L$  aufzusteigen.*

Beweis: Setze  $U_0 = U$ ,  $U_1$  sei der Normalisator  $N(U)$  von  $U$ ,  $U_2 = N(U_1)$ ,  $\dots$ ,  $U_i = N(U_{i-1})$ ,  $\dots$ . Es gilt  $\mathfrak{Z}_0 \subseteq U_0$ . Sei schon bewiesen, daß  $\mathfrak{Z}_i \subseteq U_i$ , dann folgt:

$$\mathfrak{Z}_{i+1} \circ U_i \subseteq \mathfrak{Z}_{i+1} \circ L \subseteq \mathfrak{Z}_i \subseteq U_i, \quad \mathfrak{Z}_{i+1} \subseteq U_{i+1},$$

also schließlich:  $\mathfrak{Z}_c \subseteq U_c$ ,  $U_c = L$ .

*Folgerung: Der Normalisator jedes echten  $k$ -Teilringes eines nilpotenten Lie'schen  $k$ -Ringes ist umfassender als der Teilring. Jeder maximale Teilring eines nilpotenten Lie'schen  $k$ -Ringes ist ein Ideal*

Es sei  $L$  ein Lie'scher  $k$ -Ring, und  $A, B$  seien zwei Ideale von  $L$ . Durch Induktion zeigen wir:

$$\mathfrak{Z}_m(A + B) \subseteq \mathfrak{Z}_m(A) + \mathfrak{Z}_m(B) + \sum_{\mu=1}^{m-1} \mathfrak{Z}_\mu(A) \cap \mathfrak{Z}_{m-\mu}(B).$$

Das ist richtig für den Index 1. Es sei schon bewiesen für den Index  $m$  dann folgt:

$$\begin{aligned}
 \mathfrak{Z}_{m+1}(A+B) &= (A+B) \circ \mathfrak{Z}_m(A+B) \\
 &= A \circ \mathfrak{Z}_m(A+B) + B \circ \mathfrak{Z}_m(A+B) \\
 &\subseteq \mathfrak{Z}_{m+1}(A) + A \cap \mathfrak{Z}_m(B) + \sum_{\mu=1}^{m-1} \mathfrak{Z}_{\mu+1}(A) \cap \mathfrak{Z}_{m-\mu}(B) \\
 &+ \dots \\
 &\subseteq \mathfrak{Z}_{m+1}(A) + \mathfrak{Z}_{m+1}(B) + \sum_{\mu=1}^m \mathfrak{Z}_{\mu}(A) \cap \mathfrak{Z}_{m+1-\mu}(B).
 \end{aligned}$$

Dabei ist zu beachten, daß mit  $A$  auch  $\mathfrak{Z}_r(A)$  Ideal von  $L$  ist und daß für zwei Ideale  $C, D$  gilt:  $C \circ D \subseteq C \cap D$ .

Wenn das Ideal  $A$  nilpotent mit der Klasse  $c$ , das Ideal  $B$  nilpotent mit der Klasse  $d$  ist, so ist das Ideal  $A+B$  nilpotent mit einer Klasse nicht größer als  $c+d+1$ .

Wie im Beweis von Satz 5 folgt, daß die Vereinigungsmenge  $N$  aller nilpotenten Ideale von  $L$  selbst ein Ideal ist.

Wenn in  $L$  der Maximalkettensatz für Ideale gilt, so ist  $N$  Summe von endlich vielen nilpotenten Idealen, also selbst nilpotent.

Definition: Falls die Vereinigungsmenge  $N$  aller nilpotenten Ideale von  $L$  ein nilpotentes Ideal ist, so heie  $N$  das *maximalnilpotente Ideal* von  $L$ .  $N$  ist gekennzeichnet durch die beiden Eigenschaften:

1.  $N$  ist nilpotentes Ideal von  $L$ ,
2. Jedes  $N$  als echten Teilring umfassende Ideal von  $L$  ist nicht mehr nilpotent.

Sei  $L$  ein  $r$ -gliedriger nilpotenter Lie'scher Ring über dem Körper  $k$ , dessen Klasse  $c$  ist. Wir setzen:

$$\begin{aligned}
 \mathfrak{z}_1 &= \{h_{r_1}, h_{r_1+1}, \dots, h_r\}, \\
 \mathfrak{z}_2 &= \{h_{r_2}, h_{r_2+1}, \dots, h_{r_1} \dots, h_r\}, \\
 &\dots \\
 \mathfrak{z}_{c-1} &= \{h_{r_{c-1}}, \dots, h_{r_1}, \dots, h_r\}, \\
 L = \mathfrak{z}_c &= \{h_1, h_2, \dots, h_{r_{c-1}}, \dots, h_r\}.
 \end{aligned}$$

Dann sind die  $k$ -Teilmoduln

$$A_i = \{h_i, h_{i+1}, \dots, h_r\} \quad (i = 1, 2, \dots, r)$$

Ideale von  $L$ .

Die Kette

$$L = A_1 \supset A_2 \supset A_3 \dots \supset A_r \supset 0$$

ist eine Hauptreihe von  $L$ . Demnach sind die Hauptfaktoren von  $L$  1-gliedrige Ideale.

Wir beachten, daß:  $L \circ A_i \subseteq A_{i+1}$  ( $i = 1, 2, \dots, r$ ;  $A_{r+1} = 0$ ).

Definition: Eine Basis  $a_1, a_2, \dots, a_r$  eines  $r$ -gliedrigen Lie'schen Ringes  $L$  über dem Körper  $k$  heißt *reguläre Basis*, wenn

$$a_i \circ a_k \subseteq \{a_{i+1}, \dots, a_r\},$$

insbesondere  $a_r \circ a_k = 0$ .

Wenn  $L$  eine reguläre Basis besitzt, so ist  $L$  nilpotent und die Ideale  $A_i = \{a_i, a_{i+1}, \dots, a_r\}$  bilden zusammen mit 0 eine Hauptreihe. Umgekehrt besitzt ein nilpotenter  $r$ -gliedriger Lie'scher Ring über dem Körper  $k$  stets eine reguläre Basis, wie oben gezeigt.

In Satz 7 wird eine kennzeichnende Eigenschaft nilpotenter Lie'scher Ringe ausgedrückt. Es gilt nämlich:

**Satz 8:** Wenn in dem  $r$ -gliedrigen Lie'schen Ring  $L$  über dem Körper  $k$  der Normalisator jedes echten  $k$ -Teilringes stets wirklich umfassender ist und dieselbe Eigenschaft auch für alle  $k$ -Teilringe von  $L$  erfüllt ist, dann ist  $L$  nilpotent.

Beweis: Wir führen den Beweis des Satzes durch vollständige Induktion nach  $r$ . Wenn  $r = 1$ , so ist der Satz klar. Sei  $r > 1$  und der Satz bewiesen für Lie'sche  $k$ -Ringe, deren Rang über  $k$  kleiner als  $r$  ist. Dann ist nach Induktionsvoraussetzung jeder echte  $k$ -Teilring von  $L$  nilpotent.  $L$  enthält sicher einen maximalen  $k$ -Teilring, etwa  $A$ . Da  $A \subset N(A)$ , so  $L = N(A)$ . Daher ist  $A$  ein Ideal von  $L$  und da  $A$  maximaler Teilring, so ist  $A$   $(r-1)$ -gliedrig, also

$$L = \{b, A\}.$$

Wir betten  $b$  ein in einen maximalen  $k$ -Teilring  $B$  von  $L$ . Wie oben folgt, daß  $B$  ein nilpotentes Ideal von  $L$  ist. Da  $L$  die Summe der nilpotenten Ideale  $A$  und  $B$  ist, so ist  $L$  selbst nilpotent, w. z. b. w.

## 6. Einfache Lie'sche Ringe.

Ein Lie'scher  $k$ -Ring  $L$  heißt *einfach*, wenn er von Null verschieden ist und kein von 0 und  $L$  verschiedenes Ideal enthält. Die Kompositionsfaktoren eines Lie'schen Ringes mit Kompositionsreihe sind einfach.

Es sei  $L$  ein einfacher Lie'scher  $k$ -Ring. Alle Elemente  $\lambda$  aus  $k$ , für die  $\lambda L = 0$ , bilden ein Ideal  $k_0$  von  $k$ . Da  $1 \cdot L = L \neq 0$ , so ist  $k_0 \neq k$ . Setzen wir  $\bar{k} = k/k_0$  und  $(\lambda + k_0)x = \lambda x$  für alle  $x$  aus  $L$ , so ist  $L$  ein einfacher Lie'scher  $\bar{k}$ -Ring, und es ist  $(\bar{k})_0 = 0$ . Also ist  $\lambda L \neq 0$  für alle von Null verschiedenen  $\lambda$  aus  $\bar{k}$ . Da  $\lambda L$  ein Ideal von  $L$ , so ist  $\lambda L = L$ , wenn  $\lambda \neq 0$ . Alle Elemente  $x$  aus  $L$ , für die  $\lambda x = 0$ , bilden ein Ideal  $L_\lambda$  von  $L$ . Wenn  $\lambda \neq 0$ , so ist  $L_\lambda \neq L$ , also  $L_\lambda = 0$ . Aus  $\lambda \mu = 0$ ,  $\lambda \neq 0$  folgt:  $\lambda \mu L = 0$ ,  $\lambda L = L$ ,  $\mu L = 0$ ,  $\mu = 0$ . Also

ist der Quotientenring  $\bar{k}$  von  $\bar{k}$  ein Körper. Für jedes  $\lambda \neq 0$  ist  $\lambda L = L$ ,  $L_\lambda = 0$ , also die Gleichung  $\lambda x = a$  für jedes  $a$  aus  $L$  eindeutig lösbar. Die Lösung heiÙe  $\lambda^{-1} a$ . Wir setzen  $(\lambda \mu^{-1}) a = \lambda (\mu^{-1} a)$  und überzeugen uns leicht davon, daß  $L$  ein einfacher Lie'scher  $\bar{k}$ -Ring geworden ist. Als Resultat haben wir:

*Jeder einfache Lie'sche  $k$ -Ring  $L$  kann als einfacher Lie'scher Ring über einem durch  $k$  und  $L$  eindeutig bestimmten Körper  $\bar{k}$  aufgefaÙt werden.*

### 7. Zerfällbare Lie'sche Ringe.

Die Zerfällbarkeit der regulären Darstellung des Lie'schen  $k$ -Ringes  $L$  ist gleichwertig mit der Existenz einer direkten Zerlegung  $L = L_1 + L_2$  von  $L$  in zwei von Null verschiedene Ideale  $L_1, L_2$ , deren Durchschnitt Null ist. Da  $L_1 \circ L_2 \subseteq L_1 \cap L_2$ , so folgt  $L_1 \circ L_2 = 0$ . Die Elemente aus  $L$  lassen sich demnach eindeutig in der Form  $x = H_1 x + H_2 x$  schreiben, wobei  $H_1, H_2$  die Zerlegungsoperatoren zu der vorgelegten direkten Zerlegung von  $L$  sind, so daß  $H_i L = L_i$ . Die Zerlegungsoperatoren  $H_1, H_2$  sind eindeutige Abbildungen von  $L$  in sich, die durch die Eigenschaften:

$$(11) \quad H_i(x + y) = H_i x + H_i y,$$

$$(12) \quad H_i(\lambda x) = \lambda H_i x,$$

$$(13) \quad H_1, H_2 \neq 0,$$

$$(14) \quad H_1 H_2 = H_2 H_1 = \underline{0},$$

$$(15) \quad H_1 + H_2 = \underline{1}$$

gekennzeichnet sind. Wir merken an, daß

$$(16) \quad H_i x \circ y = -y \circ H_i x = H_i x \circ H_i y \quad (i = 1, 2)$$

ist. Wenn umgekehrt zwei Lie'sche  $k$ -Ringe  $L_1, L_2$  gegeben sind, so konstruieren wir die Ringsumme von  $L_1$  und  $L_2$  als den Lie'schen  $k$ -Ring  $L$ , bestehend aus allen geordneten Paaren  $(x_1, x_2)$  ( $x_i \in L_i$ ) mit den Rechenregeln

$$(17) \quad (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(18) \quad \lambda (x_1, x_2) = (\lambda x_1, \lambda x_2),$$

$$(19) \quad (x_1, x_2) \circ (y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2).$$

Durch die Zuordnung  $x_1 \rightarrow (x_1, 0)$  bzw.  $x_2 \rightarrow (0, x_2)$  wird  $L_i$  isomorph auf ein Ideal  $\bar{L}_i$  von  $L$  abgebildet, so daß die direkte Zerlegung  $L = \bar{L}_1 + \bar{L}_2$  besteht. Entsprechendes gilt für die Zerlegung in mehr als zwei Summanden.

Ein Lie'scher  $k$ -Ring heißt *zerlegbar*, wenn er zu der Ringsumme zweier von Null verschiedener Lie'scher  $k$ -Ringe isomorph ist oder wenn er Null ist. Der Satz von REMAK-SCHMIDT-FITTING ergibt, daß bei jeder direkten Zerlegung eines Lie'schen  $k$ -Ringes in unzerlegbare Summanden die Summanden der Zerlegung bis auf die Reihenfolge im Sinne der Isomorphie eindeutig bestimmt sind.

Ableitung, Radikal, Kern, maximalnilpotentes Ideal und das Zentrum einer Ringsumme ist gleich der Ringsumme der Ableitungen, Radikale, Kerne, maximalpotenten Ideale bzw. Zentren der Summanden.

### 8. Die Diskriminante eines Lie'schen Ringes.

Sei  $L$  ein  $n$ -gliedriger Lie'scher Ring über dem Körper  $k$ . CARTAN hat jeder Basis  $x_1, x_2, \dots, x_n$  von  $L$  über  $k$  eine Zahl aus  $k$ , die zugehörige „Diskriminante“ zugeordnet. Die Haupteigenschaften dieses Begriffes mögen kurz referiert werden.

Wir setzen

$$D(x_1, x_2, \dots, x_n) = \text{Det.} (Sp(\underline{x_i} \underline{x_k})),$$

dabei ist  $Sp\ c$  gleich der Spur der linearen Transformation  $c$  und  $\underline{x}$  ist die dem Element  $x$  aus  $L$  bei der regulären Darstellung zugeordnete lineare Transformation. Ist etwa

$$x_i \circ x_k = \sum_{\nu=1}^n \gamma_{ik}^{\nu} x_{\nu},$$

so rechnen wir aus:

$$D(x_1, x_2, \dots, x_n) = \left| \sum_{\nu, \mu}^n \gamma_{i\nu}^{\mu} \gamma_{k\mu}^{\nu} \right|.$$

Bei Wahl einer neuen Basis multipliziert sich die Diskriminante mit dem Quadrat der Substitutionsdeterminante. Das Nichtverschwinden der Diskriminante ist eine invariante Eigenschaft. Sie ist gleichwertig mit jeder der beiden folgenden Aussagen:

1. Aus  $Sp(\underline{x} \underline{y}) = 0$  für alle  $y$  aus  $L$  folgt  $x = 0$ ,
2. für beliebige Zahlen  $\alpha_1, \alpha_2, \dots, \alpha_n$  ist das Gleichungssystem

$$Sp(\underline{x} \underline{x_i}) = \alpha_i \quad (i = 1, 2, \dots, n)$$

stets lösbar.

Wenn die Diskriminante eines Lie'schen  $k$ -Ringes nicht verschwindet, so ist auch die Diskriminante jedes von Null verschiedenen Ideals bzw. Faktoringes von Null verschieden, ferner ist dann der volle Lie'sche Ring halbeinfach und gleich der Ringsumme von endlich vielen nichtabelschen einfachen Lie'schen  $k$ -Ringern mit von Null verschiedener

Diskriminante. Wenn die Charakteristik von  $k$  gleich Null ist, so ist das Nichtverschwinden der Diskriminante die hinreichende und notwendige Bedingung für Halbeinfachheit.

## § 2. Aufspaltung Lie'scher Ringe nach Cartan.

### 1. Der Satz von Engel.

Definition: Die Darstellung des Lie'schen  $k$ -Ringes  $L$  mittels des Darstellungsmoduls  $\mathfrak{M}$  heißt *Nildarstellung*, wenn es für jedes Element  $a$  aus  $L$  und jeden Vektor  $u$  aus  $\mathfrak{M}$  einen Exponenten  $\mu$  gibt, so daß

$$a^\mu u = 0.$$

Beispiel: Wenn  $\mathfrak{M}$  ein beliebiger  $k$ -Modul, so wird durch die Festsetzung  $au = 0$  für alle  $a$  aus  $L$ ,  $u$  aus  $\mathfrak{M}$  eine Darstellung von  $L$ , die *Nulldarstellung*, erklärt. Jede Nulldarstellung ist eine Nildarstellung. Wenn  $\mathfrak{M}$  eine Nildarstellung von  $L$  vermittelt, so vermittelt auch jeder  $L$ -invariante Teilmodul  $\mathfrak{m}$  und jeder Faktormodul  $\mathfrak{M}/\mathfrak{m}$  eine Nildarstellung von  $L$ .

**Hilfssatz 1:** *Bei jeder irreduziblen Nildarstellung des Lie'schen  $k$ -Ringes  $L$  erfährt das Zentrum  $\mathfrak{z}$  von  $L$  eine Nulldarstellung.*

Beweis: Der  $L$ -Modul  $\mathfrak{M}$  vermittelt eine irreduzible Nildarstellung. Für jedes Element  $z$  aus  $\mathfrak{z}$  bilden alle Vektoren  $u$  aus  $\mathfrak{M}$ , für die  $zu = 0$ , einen  $k$ -Modul  $\mathfrak{M}_z$ .  $\mathfrak{M}_z$  ist sogar  $L$ -Modul, denn aus  $zu = 0$ ,  $a \circ z = 0$  folgt

$$\begin{aligned} z(au) &= (za - az)u + azu \\ &= (z \circ a)u + a(zu) \\ &= 0, \\ & \quad au \in \mathfrak{M}_z. \end{aligned}$$

Ferner ist  $\mathfrak{M}_z \neq 0$ . Denn es gibt ein von Null verschiedenes Element  $v$  in  $\mathfrak{M}$  und nach Voraussetzung einen Exponenten  $\mu$ , so daß

$$\begin{aligned} z^\mu v &= 0, \\ z^{\mu-1} v &\neq 0, \end{aligned}$$

wobei  $z^0 v = v$  gesetzt ist.

Setzen wir nun  $u = z^{\mu-1} v$ , so folgt  $u \neq 0$ ,  $zu = 0$ , also  $0 \neq u \in \mathfrak{M}_z$ . Da  $\mathfrak{M}$  ein irreduzibler  $L$ -Modul, so stimmt  $\mathfrak{M}$  mit  $\mathfrak{M}_z$  überein für alle  $z$  aus  $\mathfrak{z}$ , d. h.  $\mathfrak{z}\mathfrak{M} = 0$ , w. z. b. w.

**Hilfssatz 2:** *Jede irreduzible Nildarstellung eines nilpotenten Lie'schen Ringes ist eine Nulldarstellung.*

Beweis:  $L$  sei nilpotent mit der Klasse  $c$  und der  $L$ -Modul  $\mathfrak{M}$  vermittele eine irreduzible Nildarstellung.  $0 = \mathfrak{z}_0 \subset \mathfrak{z}_1 \cdots \subset \mathfrak{z}_c = L$  sei



die aufsteigende Zentralreihe von  $L$ . Es ist  $\mathfrak{z}_0 \mathfrak{M} = 0$ . Sei schon bewiesen, daß  $\mathfrak{z}_i \mathfrak{M} = 0$  ( $i < c$ ). Dann induziert die vorgelegte irreduzible Nildarstellung von  $L$  eine irreduzible Nildarstellung von  $L/\mathfrak{z}_i$ . Bei ihr erfährt nach Hilfssatz 1 das Zentrum von  $L/\mathfrak{z}_i$  eine Nildarstellung, also ist  $\mathfrak{z}_{i+1} \mathfrak{M} = 0$ . Nach  $c$  Schritten folgt  $\mathfrak{z}_c \mathfrak{M} = 0$ ,  $L\mathfrak{M} = 0$ , w. z. b. w.

**Satz 9** (Satz von ENGEL): *Ein  $r$ -gliedriger Lie'scher Ring  $L$  über dem Körper  $k$  ist dann und nur dann nilpotent, wenn seine reguläre Darstellung eine Nildarstellung ist.*

Beweis: 1. Wenn  $L$  nilpotent ist, so gibt es eine natürliche Zahl  $c$ , so daß  $\mathfrak{z}_{c+1}(L) = 0$ , also ist

$$\underbrace{(a)^c u = a \circ (a \circ \dots (a \circ u) \dots)}_{c\text{-mal}} = 0$$

für alle  $a$  und  $u$  aus  $L$ .

2. Es sei die reguläre Darstellung von  $L$  eine Nildarstellung. Zu beweisen ist, daß  $L$  nilpotent ist. Wenn  $r = 1$ , so ist  $L$  sogar abelsch. Es sei  $r > 1$  und der Satz schon bewiesen für höchstens  $(r - 1)$ -gliedrige Lie'sche  $k$ -Ringe. Für jeden echten  $k$ -Teilring  $U$  von  $L$  ist dessen reguläre Darstellung Nildarstellung, also ist nach Induktionsvoraussetzung jeder echte  $k$ -Teilring  $U$  nilpotent.

Die reguläre Darstellung von  $L$  induziert eine Nildarstellung von  $U$  mit  $L$  als dem zugehörigen Darstellungsmodul. Darin ist  $U$  als  $U$ -invarianten Teilmodul enthalten und in dem Faktormodul  $L/U$  wird ebenfalls eine Nildarstellung von  $U$  induziert. Da  $L/U$  ein endlich-gliedriger  $k$ -Modul, so enthält  $L/U$  einen irreduziblen  $U$ -Modul, etwa  $U_1/U$ . Dann ist  $U_1$  ein in  $L$  enthaltener  $k$ -Modul mit der Eigenschaft  $U \circ U_1 \subseteq U_1$ . Da  $U$  nilpotent, so folgt nach Hilfssatz 2, daß

$$U(U_1/U) = 0,$$

d. h.  $U \circ U_1 \subseteq U$ .

Hieraus schließen wir, daß der Normalisator jedes echten  $k$ -Teilringes von  $L$  wirklich umfassender als der Teilring selbst ist. Ferner ist jeder echte Teilring nilpotent. Nach Satz 8 (§ 1) folgt hieraus die Behauptung.

**Kriterium:** *Der Lie'sche Ring  $L$  mit endlicher Basis über dem Körper  $k$  ist dann und nur dann nilpotent, wenn bei der regulären Darstellung jede lineare Transformation des Darstellungsrings genau einen Eigenwert<sup>1)</sup> besitzt.*

Denn wegen  $xx = x \circ x = 0$  für alle Elemente  $x$  des Lie'schen Ringes kommt nur 0 als Eigenwert vor.

<sup>1)</sup> Natürlich in einer gewissen Vielfachheit.

## 2. Produktdarstellungen.

Es sei  $k$  ein Ring mit Einheitsselement.

Definition: Der Produktmodul  $\mathfrak{P}$  der  $k$ -Moduln  $\mathfrak{M}$  und  $\mathfrak{M}'$  ist der Modul mit den Erzeugenden  $uv$  ( $u \in \mathfrak{M}$ ,  $v \in \mathfrak{M}'$ ) und den definierenden Relationen:

$$(20) \quad u_1 v_1 + u_2 v_2 = u_2 v_2 + u_1 v_1,$$

$$(21) \quad u(v_1 + v_2) = uv_1 + uv_2,$$

$$(22) \quad (u_1 + u_2)v = u_1 v + u_2 v,$$

$$(23) \quad u(\lambda v) = (\lambda u)v \quad (\lambda \in k).$$

Die skalare Multiplikation der Elemente von  $\mathfrak{P}$  erklären wir durch die Festsetzung:

$$(24) \quad \lambda \left( \sum_{i=1}^r \pm u_i v_i \right) = \sum_{i=1}^r (\pm \lambda u_i) v_i.$$

Sie ist eindeutig definiert, weil jede definierende Relation von  $\mathfrak{P}$  bei Multiplikation von links her mit  $\lambda$  eine Relation von  $\mathfrak{P}$  ergibt. Es ist klar, daß die üblichen Rechenregeln der skalaren Multiplikation erfüllt sind.  $\mathfrak{P}$  ist ein  $k$ -Modul.

Wenn  $\mathfrak{M}$  und  $\mathfrak{M}'$   $k$ -Vektormoduln mit der Basis  $x_1, x_2, \dots, x_n$  bzw.  $y_1, y_2, \dots, y_m$  sind, so ist der Produktmodul ein  $k$ -Vektormodul mit der Basis  $x_i y_k$  ( $i = 1, 2, \dots, n$ ;  $k = 1, 2, \dots, m$ ).

Wenn  $\sigma$  bzw.  $\tau$  lineare Transformationen von  $\mathfrak{M}$  bzw.  $\mathfrak{M}'$  sind, so wird durch die Festsetzung  $\bar{\sigma}(uv) = (\sigma u)v$  bzw.  $\bar{\tau}(uv) = u(\tau v)$  eindeutig eine lineare Transformation  $\bar{\sigma}$  bzw.  $\bar{\tau}$  von  $\mathfrak{P}$  definiert. (Man hat zu setzen:  $\bar{\sigma} \left( \sum_{i=1}^r \pm u_i v_i \right) = \sum_{i=1}^r \pm (\sigma u_i) v_i$  und nachzuweisen, daß  $\bar{\sigma}$  jede definierende Relation auf eine Relation von  $\mathfrak{P}$  abbildet und daß  $\bar{\sigma}$  den Forderungen an lineare Transformationen genügt; entsprechend für  $\bar{\tau}$ ).

Nun sei  $L$  ein Lie'scher  $k$ -Ring, und es seien  $\mathfrak{M}$  und  $\mathfrak{M}'$   $L$ -Moduln. Dann wird durch die Festsetzung

$$(25) \quad \bar{a}(uv) = (au)v + u(av)$$

jedem Element  $a$  aus  $L$  eindeutig eine lineare Transformation  $a$  des Produktmoduls zugeordnet. Wir dürfen daher setzen:

$$(26) \quad a(uv) = (au)v + u(av)$$

und können dann leicht nachrechnen, daß der Produktmodul zweier  $L$ -Moduln wieder ein  $L$ -Modul ist. Z. B.:

$$\begin{aligned}
 a(b(uv)) - b(a(uv)) &= a(bu \cdot v + u \cdot bv) - b(au \cdot v + u \cdot av) \\
 &= abu \cdot v + bu \cdot av + au \cdot bv + u \cdot abv \\
 &\quad - bau \cdot v - au \cdot bv - bu \cdot av - u \cdot bav \\
 &= (ab - ba)u \cdot v + u \cdot (ab - ba)v \\
 &= (a \circ b)u \cdot v + u \cdot (a \circ b)v \\
 &= (a \circ b)(uv).
 \end{aligned}$$

Wir nennen die zum Produktmodul gehörige Darstellung von  $L$  die *Produktdarstellung* der zu  $\mathfrak{M}$  bzw.  $\mathfrak{M}'$  gehörigen Darstellungen von  $L$ . Es seien  $\sigma'$  bzw.  $\sigma''$  lineare Transformationen von  $\mathfrak{M}$  bzw.  $\mathfrak{M}'$  und  $\sigma$  die lineare Transformation, die durch die Festsetzung

$$(26a) \quad \sigma(uv) = \sigma' u \cdot v + u \cdot \sigma'' v$$

erklärt wird. Durch Induktion nach  $n$  beweisen wir die Formeln

$$(26b) \quad \sigma^n(uv) = \sum_{i=0}^n \binom{n}{i} \sigma'^i u \cdot \sigma''^{n-i} v.$$

Setzen wir hier  $\sigma' u = (a - \alpha)u$ ,  $\sigma'' v = (a - \beta)v$  ( $a \in L$ ), so erhalten wir:

$$(27) \quad (a - (\alpha + \beta))^n(uv) = \sum_{i=0}^n \binom{n}{i} (a - \alpha)^i u \cdot (a - \beta)^{n-i} v.$$

Fassen wir  $L$  als  $L$ -Modul auf, so entsteht die reguläre Darstellung  $a \rightarrow \underline{a} = \begin{pmatrix} x \\ a \circ x \end{pmatrix}$  von  $L$  in linearen Transformationen. Da

$$\underline{a}(x \circ y) = a \circ (x \circ y) = x \circ (a \circ y) + (a \circ x) \circ y = x \circ \underline{a}y + \underline{a}x \circ y,$$

so ist  $L$  operator-homomorphes Bild des Produktmoduls aus  $L$  und  $L$ . Also folgt die Formel:

$$(28) \quad (\underline{a} - (\alpha + \beta)^n(x \circ y)) = \sum_{i=0}^n \binom{n}{i} (\underline{a} - \alpha)^i x \circ (\underline{a} - \beta)^{n-i} y, \quad (a, x, y \in L).$$

Ferner folgt für jeden  $L$ -Modul  $\mathfrak{M}$ , daß

$$a(xu) = (a \circ x)u + xau = (\underline{a}x)u + x(au), \quad (a, x \in L; u \in \mathfrak{M});$$

also ist  $\mathfrak{M}$  operator-homomorphes Bild des Produktmoduls von  $L$  mit  $\mathfrak{M}$ , und es folgt die Formel:

$$(29) \quad (a - (\alpha + \beta))^n xu = \sum_{i=0}^n \binom{n}{i} (\underline{a} - \alpha)^i x \cdot (a - \beta)^{n-i} u.$$

### 3. Eigenwertverteilungen auf nilpotenten Lie'schen Ringen.

Es sei  $k$  ein algebraisch abgeschlossener Körper,  $H$  ein nilpotenter Lie'scher  $k$ -Ring von der Klasse  $c$  und  $\mathfrak{M}$  ein  $H$ -Modul von endlicher Dimension über  $k$ .

Wir werden  $\mathfrak{M}$  aufspalten in eine direkte Summe aus „Eigenmoduln“ von  $H$ .

Wir sagen: Das Element  $u$  aus  $\mathfrak{M}$  gehört zum Eigenwert  $\alpha$  von  $h$ , wenn es einen Exponenten  $\nu$  gibt, so daß

$$(h - \alpha)^\nu u = 0.$$

Für ein festes Element  $h$  bilden alle zum Eigenwert  $\alpha$  von  $h$  gehörigen Elemente aus  $\mathfrak{M}$  einen  $k$ -Teilmodul  $\mathfrak{M}(h, \alpha)$ . Es gilt die direkte Zerlegung:

$$(30) \quad \mathfrak{M} = \sum_{\alpha} \mathfrak{M}(h, \alpha),$$

wobei zu beachten ist, daß nur endlich viele Summanden von Null verschieden sind.

**Hilfssatz 3:** Wenn  $\mathfrak{M}$  und  $\mathfrak{M}'$   $H$ -Moduln sind, dann ist gemäß (26) der Produktmodul  $\mathfrak{P}$  ebenfalls  $H$ -Modul, und es gilt:

$$(31) \quad \sum_{\alpha+\beta=\gamma} \mathfrak{M}(h, \alpha) \cdot \mathfrak{M}'(h, \beta) = \mathfrak{P}(h, \gamma).$$

Beweis: Sei  $(h - \alpha)^\nu u = 0$ ,  $(h - \beta)^\mu v = 0$  ( $u \in \mathfrak{M}$ ,  $v \in \mathfrak{M}'$ ). In Formel (27) setze man  $n = \nu + \mu$  und findet, daß rechts jeder Summand Null ist, denn entweder ist  $i \geq \nu$ ,  $(h - \alpha)^i u = 0$  oder  $n - i \geq \mu$ ,  $(h - \beta)^{n-i} v = 0$ . Also folgt:

$$(32) \quad \mathfrak{M}(h, \alpha) \cdot \mathfrak{M}'(h, \beta) \subseteq \mathfrak{P}(h, \alpha + \beta).$$

Da die beiden direkten Zerlegungen

$$\begin{aligned} \mathfrak{P} &= \sum_{\alpha, \beta} \mathfrak{M}(h, \alpha) \cdot \mathfrak{M}'(h, \beta), \\ \mathfrak{P} &= \sum_{\gamma} \mathfrak{P}(h, \gamma) \end{aligned}$$

bestehen, so folgt (31).

Wenn wir  $H$  als  $H$ -Modul auffassen, so gehört für jedes Element  $h$  ganz  $H$  zum Eigenwert 0, denn  $H$  ist nilpotent. Ferner ist  $\mathfrak{M}$  operatorhomomorph zu dem Produktmodul von  $H$  mit  $\mathfrak{M}$ . Aus Gleichung (32) folgt, daß  $\mathfrak{M}(h, \alpha)$  unter  $H$  invariant ist.

Wir sagen:  $h$  hat in  $\mathfrak{M}$  die Eigenwerte  $\alpha_1, \alpha_2, \dots, \alpha_j$ , wenn  $\mathfrak{M}(h, \alpha_i) \neq 0$  ( $i = 1, 2, \dots, j$ ), aber  $\mathfrak{M}(h, \alpha) = 0$ , falls  $\alpha \neq \alpha_1, \alpha_2, \dots, \alpha_j$ .

Wir sagen: Das  $\gamma$ -tupel  $h_1, h_2, \dots, h_\nu$  hat in den  $H$ -Moduln  $m$  bzw.  $m'$  *getrennte Eigenwerte*, wenn  $m, m' \neq 0$  und aus  $m(h_1, \alpha_1) \cap m(h_2, \alpha_2) \dots \cap m(h_\nu, \alpha_\nu) \neq 0$  folgt  $m'(h_1, \alpha_1) \cap m'(h_2, \alpha_2) \dots \cap m'(h_\nu, \alpha_\nu) = 0$  und aus  $m'(h_1, \alpha_1) \cap m'(h_2, \alpha_2) \dots \cap m'(h_\nu, \alpha_\nu) \neq 0$  folgt  $m(h_1, \alpha_1) \cap m(h_2, \alpha_2) \dots \cap m(h_\nu, \alpha_\nu) = 0$ .

Wir sagen: Die  $H$ -Moduln  $m$  und  $m'$  liegen *getrennt*, wenn es gewisse endlich viele Elemente aus  $H$  gibt, die in  $m$  und  $m'$  getrennte Eigenwerte haben.

Dann ist die direkte Zerlegung (30), in der die Nullsummanden wegzulassen sind, eine Zerlegung des  $H$ -Moduls  $\mathfrak{M}$  in getrennt liegende  $H$ -Moduln. Da  $\mathfrak{M}$  ein endlicher  $k$ -Modul, so gibt es eine direkte Zerlegung:

$$(33) \quad \mathfrak{M} = \mathfrak{M}_1 + \mathfrak{M}_2 \dots + \mathfrak{M}_s$$

in möglichst viele getrennt liegende  $H$ -Moduln. Aus dem vorhin Gezeigten folgt, daß jedes Element aus  $H$  in jedem Teilmodul  $\mathfrak{M}_i$  nur einen Eigenwert  $\alpha_h^{(i)}$  hat. Wir nennen die Funktion  $\alpha_h^{(i)}$  *Eigenwertverteilung auf  $H$* . Nach Konstruktion sind die Eigenwertverteilungen  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(s)}$  alle untereinander verschieden. Wir sagen: ein  $H$ -Modul, in dem jedes Element  $h$  aus  $H$  nur einen Eigenwert  $\alpha_h$  hat, heißt zu  $\alpha$  *gehöriger Eigenmodul*. Eigenmoduln zu verschiedenen Eigenwertverteilungen liegen getrennt.

Aus dem eben Gezeigten folgt:

*Jeder irreduzible  $H$ -Modul ist ein Eigenmodul.*

Da die irreduziblen Komponenten des  $H$ -Moduls  $\mathfrak{M}$  eindeutig bestimmt sind, so sind auch die Eigenwertverteilungen  $\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(s)}$  eindeutig bestimmt.  $\mathfrak{M}_i$  besteht aus allen Elementen  $u$  aus  $\mathfrak{M}$ , für die es zu jedem  $h$  aus  $H$  einen Exponenten  $\nu$  gibt, so daß  $(h - \alpha_h^{(i)})^\nu u = 0$ . Also ist die Zerlegung (33) von  $\mathfrak{M}$  in getrennt liegende Eigenmoduln von  $H$  eindeutig bestimmt.

**Satz 10.** *Wenn die Charakteristik des algebraisch abgeschlossenen Grundkörpers gleich Null ist, so hat jede irreduzible Darstellung des  $r$ -gliedrigen nilpotenten Lie'schen  $k$ -Ringes  $H$  den Grad 1.*

*Die irreduziblen Darstellungen von  $H$  werden jede genau einmal auf folgendem Wege erhalten. Man ergänze eine Basis der Ableitung  $H'$  von  $H$ , etwa  $h_{x+1}, h_{x+2}, \dots, h_r$ , zu einer Basis  $h_1, h_2, \dots, h_r$  von  $H$  über  $k$  und ordne nun dem Element  $h = \xi_1 h_1 + \xi_2 h_2 \dots + \xi_r h_r$  aus  $H$  die lineare Transformation:*

$$(33a) \quad \bar{h} = (\xi_1 \alpha_1 + \xi_2 \alpha_2 \dots + \xi_x \alpha_x) \cdot 1$$

*1. Grades zu, wobei die  $x$  Konstanten  $\alpha_1, \alpha_2, \dots, \alpha_x$  die Darstellung eindeutig bestimmen und beliebig vorgeschrieben werden dürfen.*

Beweis: Es ist klar, daß durch die Vorschrift (33 a) eine irreduzible Darstellung 1. Grades von  $H$  erklärt wird.

Es sei umgekehrt  $h \rightarrow \bar{h}$  eine irreduzible Darstellung von  $H$  in linearen Transformationen eines  $f$ -gliedrigen  $k$ -Moduls  $\mathfrak{M}$ . Dann hat  $h$  nur einen Eigenwert  $\alpha_h$ , also ist die Spur der linearen Transformation gleich  $f \cdot \alpha_h$ . Wir setzen:

$$Sp\ h = Sp\ \bar{h} = f \alpha_h.$$

Dann ist

$$Sp\ (h + h') = Sp\ h + Sp\ h',$$

$$Sp\ (\lambda h) = \lambda Sp\ h;$$

$$\begin{aligned} Sp\ (h \circ h') &= Sp\ (\bar{h} \circ \bar{h}') \\ &= Sp\ (\bar{h} \bar{h}' - \bar{h}' \bar{h}) \\ &= Sp\ (\bar{h} \bar{h}') - Sp\ (\bar{h}' \bar{h}) = 0. \end{aligned}$$

Also bilden alle Elemente aus  $H$ , deren Spur verschwindet, ein Ideal  $H_1$ , und es ist entweder  $H = H_1$  oder  $H/H_1$  1-gliedrig. Da die Charakteristik von  $k$  Null ist, so verschwindet die Eigenwertverteilung  $\alpha$  auf  $H_1$ . Demnach induziert die gegebene Darstellung von  $H$  eine Nil-darstellung von  $H_1$ . Nach Hilfssatz 2 bilden alle Elemente  $u$  aus  $\mathfrak{M}$ , die von  $H_1$  annulliert werden, einen  $k$ -Teilmodul  $\mathfrak{M}_0 \neq 0$  von  $\mathfrak{M}$ .  $\mathfrak{M}_0$  ist unter  $H$  invariant, denn aus  $h \in H$ ,  $h' \in H_1$ ,  $u \in \mathfrak{M}_0$  folgt:

$$h' \circ h \in H_1,$$

$$\begin{aligned} h' (h u) &= (h' h - h h') u - h h' u \\ &= (h' \circ h) u - h (h' u) = 0, \\ h u &\in \mathfrak{M}_0. \end{aligned}$$

Da  $\mathfrak{M}$  ein irreduzibler  $H$ -Modul, so ist  $\mathfrak{M}_0 = \mathfrak{M}$ ,  $H_1 \mathfrak{M} = 0$ . Da  $H/H_1$  abelsch, so liegt  $H$  in  $H_1$ , ferner ist der Darstellungsring  $\bar{H}$  abelsch. Da er irreduzibel ist, so hat er den Grad 1. Demnach ist dem Element  $h$  aus  $H$  die lineare Transformation  $\alpha_h \cdot \mathbf{1}$  1. Grades zugeordnet.

Setzen wir  $\alpha_{h_i} = \alpha_i$ , so folgt wegen  $\bar{H}_1 = 0$ , daß

$$\alpha_{x+1} = \alpha_{x+2} \cdots = \alpha_r = 0,$$

ferner aus den Darstellungsbedingungen:

$$\alpha_{\xi_1 h_1 + \xi_2 h_2 \cdots + \xi_r h_r} = \xi_1 \alpha_1 + \xi_2 \alpha_2 \cdots + \xi_r \alpha_r,$$

womit alles bewiesen ist.

**4. Aufspaltung Lie'scher Ringe in Eigenmoduln nilpotenter Teilringe.**

Sei  $L$  ein Lie'scher Ring mit endlich vielen Basiselementen über dem algebraisch abgeschlossenen Grundkörper  $k$  und  $H$  ein nilpotenter  $k$ -Teilring von  $L$ .

Die reguläre Darstellung von  $L$  induziert eine Darstellung von  $H$  und gemäß Abschnitt 3 existiert eine eindeutig bestimmte direkte Aufspaltung

$$(34) \quad L = L_0 + L_\alpha + L_\beta + \dots$$

von  $L$  in Eigenmoduln von  $H$ . Dabei bezeichnen wir mit  $0$  kurz die Eigenwertverteilung von  $H$ , bei der jedem Element aus  $H$  der Eigenwert  $0$  zugeordnet wird.  $0, \alpha, \beta, \dots$  durchläuft alle Eigenwertverteilungen von  $H$ .

$L_\gamma$  besteht aus allen Elementen  $u$  aus  $L$ , für die es zu jedem Element  $h$  aus  $H$  einen Exponenten  $\nu$  gibt, so daß  $(h - \gamma h)^\nu u = 0$ . Wenn  $\mathfrak{M}$  ein  $L$ -Modul ist, so möge mit  $\mathfrak{M}(H, \gamma)$  der in der Aufspaltung (33) zur Eigenwertverteilung  $\gamma$  von  $H$  gehörige Eigenmodul bezeichnet werden, so daß die direkte Zerlegung

$$(35) \quad \mathfrak{M} = \sum_{\gamma} \mathfrak{M}(H, \gamma)$$

besteht.

Aus (32) folgt nun

$$(36) \quad L_\gamma \mathfrak{M}(H, \delta) \subseteq \mathfrak{M}(H, \gamma + \delta).$$

Setzen wir hier  $\mathfrak{M} = L$ , so folgt:

$$(37) \quad L_\gamma \circ L_\delta \subseteq L_{\gamma+\delta}.$$

Insbesondere

$$(38) \quad L_0 \circ L_0 \subseteq L_0.$$

Also ist  $L_0$  ein Lie'scher  $k$ -Teilring von  $L$ . Da  $H$  nilpotent ist, so folgt  $H \subseteq L_0$ .

Für alle  $\gamma \neq 0$  gilt  $H \circ L_\gamma = L_\gamma$ , denn es gibt dann in  $H$  ein Element  $h$ , so daß  $h$  eine nichtsinguläre lineare Transformation von  $L_\gamma$  induziert. Für die Elemente  $u$  des Normalisators  $N(H)$  von  $H$  in  $L$  gilt  $H \circ u \subseteq H$ , also gehören diese  $u$  zur Eigenwertverteilung  $0$ , d. h.

$$(39) \quad N(H) \subseteq L_0.$$

Wenn  $H$  echter Teilmodul von  $L_0$ , so ist  $H$  auch echter Teilmodul von  $N(H)$ , denn der Darstellungsmodul  $L_0/H$  von  $H$  enthält dann einen irreduziblen  $H$ -Modul  $H_1/H$  und da  $L_0/H$  eine Nildarstellung von  $H$  vermittelt, so folgt nach Hilfssatz 2, daß  $H \circ H_1 \subseteq H$ , also  $H \subset H_1 \subseteq N(H)$ .

CARTAN hat gezeigt, daß  $H$  so gewählt werden kann, daß  $H = L_0$ , anders gesagt, daß der nilpotente  $k$ -Teilring  $H$  mit seinem Normalisator zusammenfällt.

Es sei  $L$  ein  $n$ -gliedriger Lie'scher Ring über dem algebraisch abgeschlossenen Körper  $k$ . Jedem Element aus  $L$  wird bei der regulären Darstellung eine lineare Transformation mit höchstens  $n$  verschiedenen Eigenwerten zugeordnet. Wir suchen ein Element  $h_1$  in  $L$ , dem bei der regulären Darstellung von  $L$  eine lineare Transformation  $h_1$  mit möglichst vielen verschiedenen Eigenwerten zugeordnet wird.

Es sei

$$(1) \quad L = K + L_2 + L_3 \cdots + L_s$$

die Aufspaltung von  $L$  in die Eigenmoduln von  $\{h_1\}$ , wobei  $K$  der zum Eigenwert 0 gehörige Eigenmodul sei.

Mit den üblichen Schlußweisen wird jetzt gezeigt, daß  $K$  nilpotent sein muß. Wir wählen eine Basis  $h_1, h_2, \dots, h_r$  des  $k$ -Moduls  $K$ . Für die Elemente  $x_\alpha$  aus  $L_\alpha$  wird durch die Abbildung  $x_\alpha \rightarrow h_i \circ x_\alpha$  eine gewisse lineare Transformation  $\underline{h}_i^{(\alpha)}$  definiert. Dem allgemeinen Element  $h = \xi_1 h_1 + \xi_2 h_2 \cdots + \xi_r h_r$  ist entsprechend die lineare Transformation  $\underline{h}^{(\alpha)} = \xi_1 \underline{h}_1^{(\alpha)} + \xi_2 \underline{h}_2^{(\alpha)} \cdots + \xi_r \underline{h}_r^{(\alpha)}$  zugeordnet. Ihre charakteristische Gleichung  $f_\alpha(t, x)$  ist gleich der Determinante der Matrix  $tE - h^{(\alpha)}$ , also ein Polynom  $n_\alpha$ -ten Grades mit Koeffizienten aus dem Polynombereich  $k[\xi] = k[\xi_1, \xi_2, \dots, \xi_r]$  und mit 1 als Koeffizient der höchsten  $t$ -Potenz. Bekanntlich gibt es einen bis auf eine Konstante  $\neq 0$  eindeutig bestimmten größten gemeinschaftlichen Teiler  $d_{\alpha, \beta}(t, \xi)$  von  $f_\alpha$  und  $f_\beta$  im Polynombereich  $k[\xi, t]$ . Da der Koeffizient der höchsten  $t$ -Potenz in  $f_\alpha$  gleich 1 ist, so ist der Koeffizient der höchsten  $t$ -Potenz von  $d_{\alpha, \beta}$  eine Konstante  $\neq 0$ , also bleibt der Grad von  $d_{\alpha, \beta}$  in  $t$  erhalten, wenn für  $\xi$  ein  $r$ -tupel von Elementen aus  $k$  eingesetzt wird. Setzen wir für  $\xi$  den Wert  $(1, 0, \dots, 0)$  ein, so geht  $f_\alpha(\xi, t)$  in das charakteristische Polynom von  $\underline{h}_1^{(\alpha)}$  über, also in das Polynom  $(t - \alpha_1)^{n_\alpha}$ . Da nun die  $s$  Eigenwerte von  $h_1$ , die zu den  $s$  Teilmoduln  $L_\gamma$  gehören, untereinander verschieden sind, so sind die durch Einsetzung aus den  $f_\alpha$  entstandenen  $s$  Polynome in  $t$  untereinander teilerfremd. Wenn  $\alpha \neq \beta$ , so geht  $d_{\alpha, \beta}$  in einen gemeinsamen Teiler der Polynome  $(x - \alpha_1)^{n_\alpha}$  und  $(x - \beta_1)^{n_\beta}$  über, also ist der Grad von  $d_{\alpha, \beta}$  in  $t$  Null. Folglich ist  $d_{\alpha, \beta}[\xi, t]$  eine Konstante  $\neq 0$ . Da die Polynome  $f_\alpha(\xi, t)$  als Polynome aus  $k[t, \xi]$  betrachtet, untereinander teilerfremd sind, so sind sie auch als Polynome aus  $k(\xi)[t]$  bekanntlich teilerfremd. Rechnen wir den größten gemeinschaftlichen Teiler von  $f_\alpha$  und  $f_\beta$ , falls  $\alpha \neq \beta$ , in  $k(\xi)[t]$  mit Hilfe des Euklidischen Divisionsalgorithmus aus, so erhalten wir 1, und es treten während der Division nur endlich viele Nennerpolynome aus  $k[\xi]$  auf. Das Produkt



aller dieser Nenner für alle Paare  $\alpha, \beta$  sei das Polynom  $N(\xi)$  aus  $k[\xi]$ . Wenn wir für  $\xi$  Werte einsetzen, für die  $N(\xi)$  nicht verschwindet, so ergibt sich als g. g. T. der durch Einsetzung aus den  $f_\alpha$  entstandenen Polynome aus  $k[t]$  für je zwei verschiedene Eigenwertverteilungen  $\alpha, \beta$  nach dem Euklidischen Divisionsalgorithmus der Wert 1.

Das zu dem Eigenwert 0 gehörige Polynom  $f_0(\xi, t)$  vom Grade  $n_0$  muß noch besonders betrachtet werden. Falls die Charakteristik  $p$  von  $k$  eine natürliche Primzahl ist, so sei  $p^l$  die höchste Potenz von  $p$ , die in den Exponenten aller wirklich in  $f_0$  vorkommenden  $t$ -Potenzen aufgeht.

Setzen wir noch zur Abkürzung  $\eta = \left( \sqrt[p^l]{\xi_1}, \sqrt[p^l]{\xi_2}, \dots, \sqrt[p^l]{\xi_r} \right)$ , falls  $p > 0$  und  $l > 0$  bzw.  $n = \xi$  sonst, so wird  $f_0(\xi, t)$  die  $p^l$ -te Potenz eines Polynomes  $g(\eta, t)$  aus  $k[\eta, t]$  vom Grade  $m = \frac{n}{p^l}$  in  $t$  und mit nicht verschwindender partieller Ableitung nach  $t$ . Der größte gemeinschaftliche Teiler von  $g(\eta, t)$  und  $\frac{\partial}{\partial t} g(\eta, t)$  sei  $d(\eta, t)$ , so daß

$$(2a) \quad g(\eta, t) = g_1(\eta, t) d(\eta, t),$$

$$(2b) \quad \frac{\partial}{\partial t} g(\eta, t) = g_2(\eta, t) d(\eta, t)$$

ist und  $g_1, g_2$  teilerfremde Polynome  $\neq 0$  aus  $k[\eta, t]$  sind. Wie oben schließen wir, daß der Grad von  $d(\eta, t)$  in  $t$  erhalten bleibt, wenn für  $\eta$  ein  $r$ -tupel von Elementen aus  $k$  eingesetzt wird, ferner kann wie oben ein Hilfspolynom  $M(\eta)$  bestimmt werden, so daß für alle Stellen, in denen  $M(\eta)$  nicht verschwindet, die durch Einsetzung aus  $g_1, g_2$  entstandenen Polynome teilerfremd sind.

Da  $k$  als algebraisch abgeschlossener Körper unendlich viele Elemente enthält, so gibt es eine von Null verschiedene Stelle  $\lambda_1, \lambda_2, \dots, \lambda_r$ , in der die Polynome  $N, M$  und  $g_2(\eta, t)$  nicht verschwinden. Für das von Null verschiedene Element  $h' = \lambda_1 h_1 + \lambda_2 h_2 + \dots + \lambda_r h_r$  sind die zugehörigen charakteristischen Polynome teilerfremd, also haben sie auch zu je zweien keine gemeinsame Nullstelle. Demnach hat  $h'$  bei der regulären Darstellung von  $L$  mindestens soviele verschiedene Eigenwerte wie  $h_1$ . Da die Anzahl  $s$  der verschiedenen Eigenwerte von  $h_1$  die Höchstzahl ist, so hat auch  $h'$  genau  $s$  verschiedene Eigenwerte. Folglich ist das charakteristische Polynom von  $h'^{(p)}$  die  $n_\gamma$ -te Potenz eines Linearfaktors. Da  $h' \neq 0$  und  $h' \circ h' = 0$ , so hat  $h'$  in  $K$  sicher den Eigenwert 0. Daher ist das charakteristische Polynom  $f_0(\lambda, t)$  von  $h'$  in  $K$  einfach gleich  $t^{n_0}$ , folglich  $g(\lambda, t) = t^m$ . Aus den Gleichungen (1), (2) folgt durch Einsetzen:

$$t^m = g_1(\lambda, t) d(\lambda, t), \quad m t^{m-1} = g_2(\lambda, t) d(\lambda, t),$$

wobei  $g_2(\lambda, t) \neq 0$  und  $g_1(\lambda, t)$  und  $g_2(\lambda, t)$  teilerfremd sind. Also hat  $d(\lambda, t)$  den Grad  $m-1$ , folglich hat auch  $d(\eta, t)$  den Grad  $m-1$ . Da der g. g. T. von  $g(\eta, t)$  mit der partiellen Ableitung nach  $t$  in  $t$  den Grad  $m-1$  hat, so hat  $g$  die Form  $(t - \psi(\eta))^m$ , und es ist

$$f_0(\xi, t) = (t - \psi(\eta))^{n_0}.$$

Jedes Element aus  $K$  hat also bei der regulären Darstellung von  $K$  nur einen Eigenwert. Nach dem Kriterium im Abschnitt 1 folgt, daß  $K$  ein nilpotenter Lie'scher  $k$ -Ring ist.

Auf dieselbe Weise wie eben schließen wir, daß auch für alle  $\alpha$ :

$$f_\alpha(\xi, t) = (t - \psi_\alpha(\eta_\alpha))^{n_\alpha}$$

ist, wobei  $\eta_\alpha$  durch hinreichend oft wiederholtes Ausziehen der  $p$ -ten Wurzel aus  $\xi$  entsteht. Hieraus ist ersichtlich, daß die Moduln  $L_i$  die verschiedenen zu dem nilpotenten Teilring  $K$  von  $L$  gehörigen Eigenmoduln sind.

Die Zerlegung (1) von  $L$  nach dem nilpotenten Teilring  $K$  heiße *Cartansche Zerlegung* von  $L$ . Wichtig ist die Tatsache, daß der zur Eigenwertverteilung 0 gehörige Eigenmodul von  $K$  grade mit  $K$  übereinstimmt.

Als Nebenresultat erhalten wir:

**Satz 11.:** *Ein Lie'scher  $k$ -Ring  $L$  aus Matrizen  $f$ -ten Grades, in dem jede Matrix  $x$  nur einen Eigenwert  $\alpha_x$  hat, ist nilpotent.*

Beweis: Sei  $\mathfrak{M}$  ein zugehöriger Darstellungsmodul. Dann folgt aus Hilfssatz 3:

$$L_\alpha \mathfrak{M}(H, \beta) \subseteq \mathfrak{M}(H, \alpha + \beta)$$

und nach Voraussetzung  $\mathfrak{M} = \mathfrak{M}(H, \beta)$  mit festem  $\beta$ , also  $L_\alpha \mathfrak{M} = 0$ , wenn  $\alpha \neq 0$ , also  $L_\alpha = 0$ , wenn  $\alpha \neq 0$ ,  $L = L_0 = H$ .

### § 3. Einfachheitsbeweise.

Wir bezeichnen mit  $M_n(k)$  den Schieferring aller  $n$ -reihigen Matrizen mit Koeffizienten aus dem Körper  $k$  mit der Charakteristik  $\chi$ .  $M_n(k)$  besitzt als Basis die  $n$  Matrizeneinheiten  $e_{ik}$  ( $i, k = 1, 2, \dots, n$ ) mit den Rechenregeln

$$(3a) \quad e_{ik} \cdot e_{rs} = \delta_{kr} e_{is}.$$

Der Lie'sche Ring  $M_n$  besitzt die  $n^2$  Basiselemente  $e_{ik}$  ( $i, k = 1, 2, \dots, n$ ) mit den Rechenregeln

$$(3b) \quad e_{ik} \circ e_{rs} = \delta_{rk} e_{is} - \delta_{is} e_{rk}.$$

Alle Matrizen aus  $M_n$ , deren Spur Null ist, bilden ein Ideal  $SM_n$ <sup>1)</sup> mit den Basiselementen

$$d_i = e_{ii} - e_{11} \quad (i = 2, 3, \dots, n), \quad e_{ik} \quad (i \neq k; i, k = 1, 2, \dots, n)$$

und den Rechenregeln

- (4)  $d_1 = 0, \quad d_{ik} = d_i - d_k \quad (i \neq k),$   
 (a)  $d_{ik} \circ d_{rs} = 0 \quad (i \neq k, r \neq s),$   
 (b)  $d_{ik} \circ e_{rs} = (\delta_{ir} - \delta_{is} - \delta_{kr} + \delta_{ks}) e_{rs} \quad (i \neq k, r \neq s),$   
 (c)  $e_{ik} \circ e_{rs} = \delta_{rk} e_{is} - \delta_{is} e_{rk} \quad (i \neq k; r \neq s; (rs) \neq (ki)).$   
 (d)  $e_{ik} \circ e_{ki} = d_{ik} \quad (i \neq k).$

Aus den Formeln (3b) folgt, daß

(e)  $D(M_n) = SM_n.$

Aus (b), (d) folgt, daß

(f)  $D(SM_n) = SM_n,$

ausgenommen im Fall  $\chi = 2, n = 2$ . Im Falle  $\chi = 2, n = 2$  ist

$$D(SM_2) = k \cdot e, \quad \left( e = \sum_1 e_{ii} \right) \quad \text{und} \quad D(ke) = 0,$$

und dann ist also  $M$  dreistufig metabelsch.

Das Zentrum  $M_n$  ist  $k \cdot e$ . Der Faktorring von  $M_n$  nach  $k \cdot e$  werde mit  $PM_n$ <sup>2)</sup> bezeichnet.  $PM_n$  hat als Basiselemente:

$$\bar{e}_{ik} = e_{ik} + \mathfrak{z}(M_n) \quad ((ik) \neq (nn))$$

mit den Rechenregeln:

(g)  $\bar{e}_{nn} = -\sum_1^{n-1} \bar{e}_{ii}, \quad \bar{e}_{ik} \circ \bar{e}_{rs} = \delta_{rk} \bar{e}_{is} - \delta_{is} \bar{e}_{rk}.$

Mit  $PSM_n$  bezeichnen wir den Faktorring von  $SM_n$  nach  $k \cdot e \cap SM_n$ .

Wenn  $n \not\equiv 0 \pmod{\chi}$ , so ist  $PSM_n = SM_n$ ; wenn  $n \equiv 0 \pmod{\chi}$ , so hat  $PSM_n$  als Basis die Elemente  $\bar{d}_2, \bar{d}_3, \dots, \bar{d}_{n-1}, \bar{e}_{ik} \quad (i \neq k)$  mit den Rechenregeln:

(h)  $\bar{d}_n = -\sum_{i=2}^{n-1} \bar{d}_i, \bar{d}_1 = 0, \bar{d}_{ik} = \bar{d}_i - \bar{d}_k \quad (i \neq k),$

ferner (a)–(d) quergestrichen.

**Satz 12:** Die 2.  $(n-1)$  Elemente  $e_{i, i+1} (1 \leq i < n), e_{i, i-1} (1 < i \leq n)$  bilden ein Erzeugendensystem von  $SM_n$ .

Beweis: Von vornherein sei  $n > 1$ .  $L$  sei der aus den obenstehenden 2.  $(n-1)$  Elementen erzeugte Lie'sche  $k$ -Ring.  $L$  ist in  $SM_n$

<sup>1)</sup>  $S =$  speziell.

<sup>2)</sup>  $P =$  projektiv.

enthalten. Wir wissen, daß  $e_{ij}, e_{ji} \in L$ , falls  $1 \leq i < j \leq n$  und  $i - j = 1$ . Es sei schon gezeigt, daß  $e_{ij}, e_{ji} \in L$ , falls  $1 \leq i < j \leq n$  und  $j - i = \nu$ . Nun sei  $1 \leq l < k \leq n$ ,  $k - l = \nu + 1$ . Dann ist

$$e_{lk} = e_{l, l+1} \circ e_{l+1, k}, \quad e_{kl} = e_{k, l+1} \circ e_{l+1, l},$$

also

$$e_{lk}, \quad e_{kl} \in L.$$

Nach  $(n - 1)$ -maliger Anwendung dieses Schlusses folgt, daß alle  $e_{ik} (i \neq k)$  in  $L$  enthalten sind. Dann ist auch  $d_i = d_{i1} = e_{i1} \circ e_{1i}$  in  $L$  enthalten, also auch  $SM_n$ . Folglich ist  $SM_n = L$ , w. z. b. w.

**Satz 13:** Die Lie'sche Algebra  $PSM_n$  ist einfach und nichtabelsch, wenn  $n > 1$ , ausgenommen im Falle  $n = 2$ ,  $\chi = 2$  (dann ist  $PSM_n$  abelsch).

Beweis: Es sei  $A$  ein nicht in  $\mathfrak{z}(M_n)$  enthaltenes Ideal von  $SM_n$ . Wir werden zeigen, daß  $A = SM_n$ . Daraus folgt dann die Behauptung. Es gibt in  $A$  ein Element  $a = \sum \alpha_{ik} e_{ik}$ , das nicht in  $\mathfrak{z}(M_n)$  enthalten ist.

1.  $a$  ist mit allen  $d_{ik} = e_{ii} - e_{kk}$  vertauschbar. Aus  $a \circ d_{ik} = 0$  ( $i \neq k$ ) folgt  $\alpha_{ik} = 0$ , wenn  $\chi \neq 2$ . Wenn  $\chi = 2$ , so ist  $n > 2$ , also gibt es zu jedem Indexpaar  $i \neq k$  noch einen von  $i$  und  $k$  verschiedenen Index  $l$ , und es folgt aus  $d_{il} \circ a = 0$  wiederum, daß  $\alpha_{ik} = 0$ . Demnach ist  $a = \sum_{i=1}^n \alpha_{ii} e_{ii}$ . Da  $a$  nicht in  $\mathfrak{z}(M_n)$  enthalten ist, so gibt es ein Indexpaar  $i \neq k$ , für das  $\alpha_{ii} \neq \alpha_{kk}$ , und es folgt  $a \circ e_{ik} = (\alpha_{ii} - \alpha_{kk}) e_{ik} \in A$ ,  $e_{ik} \in A$ . Da ferner  $a$  in  $SM_n$  enthalten ist, so ist  $\sum_{i=1}^n \alpha_{ii} = 0$ , also  $n > 2$ .

2.  $a$  ist nicht mit allen  $d_{ik}$  vertauschbar. Dann gibt es ein Indexpaar  $i \neq k$ , für das  $\alpha_{ik} \neq 0$ .

2a)  $n = 2$ . Dann ist  $\chi \neq 2$ . Wir bilden  $b = d_{12} \circ a$  und finden

$$A \ni b = \beta_{12} e_{12} + \beta_{21} e_{21} \neq 0.$$

Sei etwa  $\beta_{12} \neq 0$ . Dann ist

$$\begin{aligned} A \ni b \circ e_{21} &= \beta_{12} d_{12}, & d_{12} &\in A, & e_{12} &= \frac{1}{2} \cdot d_{12} \circ e_{12} \in A, \\ e_{21} &= -\frac{1}{2} \cdot d_{21} \circ e_{12} \circ \in A, & A &= SM_2. \end{aligned}$$

2b)  $n > 2$ . Es gibt einen Index  $l \neq i, k$ . Wir bilden  $c = d_{kl} \circ (d_{il} \circ a)$  und finden, daß

$$0 \neq c = \gamma_{ik} e_{ik} + \gamma_{ki} e_{ki} \in A.$$

Sei etwa  $\gamma_{ik} \neq 0$ . Dann ist

$$0 \neq d = c \circ e_{kl} = \gamma_{ik} e_{il} \in A.$$

In jedem Fall liegt ein  $e_{ik} (i \neq k)$  in  $A$  und wir dürfen weiterhin annehmen, daß  $n > 2$ . Es sei  $l$  ein von  $i$  und  $k$  verschiedener Index.

Es folgt:

$$\begin{aligned} e_{il} &= e_{ik} \circ e_{kl} \in A, & e_{lk} &= e_{li} \circ e_{ik} \in A, & e_{kl} &= e_{ki} \circ e_{il} \in A, \\ e_{li} &= e_{lk} \circ e_{ki} \in A, & e_{ki} &= e_{kl} \circ e_{li} \in A. \end{aligned}$$

Wenn ferner der Index  $m$  von  $i, k, l$  verschieden ist, so ist

$$e_{lm} = e_{li} \circ e_{im} \in A.$$

Demnach ist  $e_{\nu\mu}$  in  $A$  enthalten für alle  $\nu \neq \mu$ , schließlich

$$d_{\nu\mu} = e_{\nu\mu} \circ e_{\mu\nu} \in A,$$

also  $A = SM_n$ , w. z. b. w.

Es sei  $k$  ein vollkommener Körper mit der Charakteristik  $\chi$  und  $m$  sei der aus dem Einheitslement von  $k$  durch fortgesetzte Addition und Subtraktion erzeugte Modul.

Wir suchen alle einfachen, nichtabelschen Lie'schen Ringe  $L$  mit einer Basis

$$e_0, e_{\alpha_1}, e_{\alpha_2}, \dots, e_{\alpha_r}$$

über  $k$ , so daß  $\alpha_1 = 0, \alpha_2, \alpha_3, \dots, \alpha_r$   $r$  verschiedene Elemente aus  $m$  sind und

$$(1) \quad e_0 \circ e_{\alpha_i} = \alpha_i e_{\alpha_i} \quad (i = 1, 2, \dots, r).$$

Der von dem Basiselemente  $e_0$  erzeugte  $k$ -Modul  $H$  ist ein nilpotenter Teilring von  $L$ . Bezeichnen wir mit  $(\alpha)$  diejenige Eigenwertverteilung auf  $H$ , bei der dem Element  $e_0$  der Eigenwert  $\alpha$  zugeordnet wird, und mit  $L_\alpha$  den zu  $(\alpha)$  gehörigen Eigenmodul, dann folgt:  $\{e_{\alpha_i}\} \subseteq L_{\alpha_i}$ , ( $i = 1, 2, \dots, r$ ), also

$$(2) \quad L = \sum_1^r L_{\alpha_i}.$$

Da (2) eine direkte Zerlegung, so folgt  $L_{\alpha_i} = \{e_{\alpha_i}\}$

Wir setzen:

$$(3) \quad e_\alpha = 0,$$

wenn  $\alpha \neq \alpha_1, \alpha_2, \dots, \alpha_r$ . Dann gilt allgemein:

$$(4) \quad L_\alpha = \{e_\alpha\}.$$

Da  $L_\alpha \circ L_\beta \subseteq L_{\alpha+\beta}$ , so

$$(5) \quad e_\alpha \circ e_\beta \in \{e_{\alpha+\beta}\}.$$

Da  $L$  einfach und nicht abelsch ist, so ist  $L$  vollkommen, d. h.

$$(6) \quad D(L) = L.$$

Andererseits ist

$$D(L) = \sum_{i,j=1}^r \{e_{\alpha_i} \circ e_{\alpha_j}\} \subseteq \sum_{j=2}^r L_{\alpha_j} + \sum_{i=1}^r \{e_{-\alpha_i} \circ e_{\alpha_i}\}.$$

Da nun  $\{e_{-\alpha_i} \circ e_{\alpha_i}\} \subseteq L_0$ , so folgt aus (2) und (6):

$$(7) \quad \sum_{i=1}^r \{e_{-\alpha_i} \circ e_{\alpha_i}\} = L_0.$$

Demnach gibt es in  $\mathfrak{m}$  ein Element  $\varepsilon$ , so daß

$$(8) \quad e_{-\varepsilon} \circ e_{\varepsilon} \neq 0, \quad \text{etwa } e_{-\varepsilon} \circ e_{\varepsilon} = \mu e_0 \quad \text{und } \mu \neq 0.$$

Da  $e_{\varepsilon} \circ e_{\varepsilon} = 0$ , so ist  $\varepsilon \neq -\varepsilon$ ,

$$(9) \quad 2\varepsilon \neq 0, \quad \text{also } \chi \neq 2 \quad \text{und } \varepsilon \neq 0.$$

Wenn  $L = \{e_0, e_{\varepsilon}, e_{-\varepsilon}\}$ , so setzen wir

$$d_0 = \varepsilon^{-1} e_0, \quad d_1 = e_{\varepsilon}, \quad d^{-1} = 2\mu^{-1}\varepsilon^{-1} e_{-\varepsilon}$$

und erhalten die Basisdarstellung

$$L = \{d_0, d_1, d_{-1}\}$$

mit den Rechenregeln:

$$d_{\alpha} \circ d_{\beta} = (\beta - \alpha) d_{\alpha+\beta} \quad (\alpha, \beta = 0, \pm 1).$$

Setzen wir in  $M_2(k)$ :  $d'_0 = e_{11}$ ,  $d'_1 = e_{12}$ ,  $d'_{-1} = e_{21}$ , so finden wir, daß

$$d'_{\alpha} \circ d'_{\beta} \equiv (\beta - \alpha) d'_{\alpha+\beta} \pmod{z(M)},$$

also ist  $L$  isomorph zu  $PM_{\mathfrak{g}}(k)$  und da  $\chi \neq 2$ , so ist  $L$  einfach, wie schon früher gezeigt.

Die Fälle  $r = 3$  bzw.  $\chi = 2, 3$  sind damit völlig zu Ende untersucht, es sei fortan  $r > 3$  und  $\chi \neq 2, 3$ .

Nun wollen wir einige Formeln ableiten. Es seien  $\alpha, \gamma$  Elemente aus  $\mathfrak{m}$  und es sei  $x_0$  ein Element aus  $L_{\gamma}$ , ferner sei  $\alpha \neq 0$ ,  $e_{-\alpha} \circ e_{\alpha} = \lambda e_0$ . Man setze rekursiv:

$$e_{\alpha} \circ x_0 = x_1, \quad e_{\alpha} \circ x_1 = x_2, \quad \dots, \quad e_{\alpha} \circ x_i = x_{i+1}, \quad \dots$$

Dann folgt:

$$x_0 \in L_{\gamma}, \quad x_1 \in L_{\gamma+\alpha}, \quad \dots, \quad x_i \in L_{\gamma+i\alpha}, \quad \dots,$$

ferner  $e_{\alpha} \circ (e_{-\alpha} \circ x_0) \in L_{\gamma}$  und da entweder  $x_0 = 0$  oder  $\{x_0\} = L_{\gamma}$ , so ist sogar

$$(10) \quad e_{\alpha} \circ (e_{-\alpha} \circ x_0) = \nu_0 x_0.$$

Ähnlich schließen wir, daß der Ansatz:

$$(11a) \quad e_{-\alpha} \circ x_i = \nu_i x_{i-1},$$

also

$$(11) \quad e_{\alpha} \circ (e_{-\alpha} \circ x_i) = \nu_i x_i \quad (i = 1, 2, \dots)$$

erlaubt ist. Jetzt folgt:

$$\begin{aligned} (12) \quad 0 &= x_0 \circ (e_{\alpha} \circ e_{-\alpha}) + e_{\alpha} \circ (e_{-\alpha} \circ x_0) + e_{-\alpha} \circ (x_0 \circ e_{\alpha}), \\ 0 &= x_{i-1} \circ (e_{\alpha} \circ e_{-\alpha}) + e_{\alpha} \circ (e_{-\alpha} \circ x_{i-1}) + e_{-\alpha} \circ (x_{i-1} \circ e_{\alpha}) \\ &= x_{i-1} \circ -\lambda e_0 + \nu_{i-1} x_{i-1} + e_{-\alpha} \circ -x_i \\ &= x_{i-1} (\lambda (\gamma + (i-1)\alpha) + \nu_{i-1} - \nu_i). \end{aligned}$$

Entweder ist  $x_{i-1} = 0$ , oder es ist

$$(13) \quad v_i = v_{i-1} + \lambda(\gamma + (i-1)\alpha).$$

Wenn aber  $x_{i-1} = 0$ , so bleibt der Ansatz (11a) gültig, auch wenn wir  $v_i$  durch  $v_{i-1} + \lambda(\gamma + (i-1)\alpha)$  ersetzen. Nach Ausführung dieser Ersetzung für  $i = 2, 3, \dots$  gilt (13) für  $i = 1, 2, 3, \dots$ . Die Auflösung der Rekursionsformel (13) ergibt

$$(14) \quad v_i = v_0 + \lambda \left( i\gamma + \binom{i}{2} \alpha \right).$$

Nun behaupten wir, daß es eine natürliche Zahl  $l$  gibt, so daß

$$x_{l-1} \neq 0, \quad x_l = x_{l+1} = \dots = 0.$$

(Durch diese Eigenschaften ist  $l$  dann eindeutig bestimmt.) Wäre nämlich im Gegenteil  $x_i \neq 0$  ( $i = 0, 1, 2, \dots$ ), so wäre

$$L_{\gamma+i\alpha} \neq 0 \quad (i = 0, 1, 2, \dots).$$

Da aber  $\alpha \neq 0$  und nur endlich viele  $L_\beta$  von Null verschieden sind, so müßte  $\chi > 0$  sein. Da  $\gamma$  und  $\alpha$  dem in  $k$  enthaltenen Primkörper angehören und  $\alpha \neq 0$  ist, so ist  $\alpha^{-1}(\gamma - \alpha) \bmod \chi$  einem reduzierten Rest  $j$  kongruent ( $0 \leq j < \chi$ ), so daß  $L_{\gamma+j\alpha} = L_\alpha$ , also  $e_\alpha \circ L_{\gamma+j\alpha} = 0$ , und es wäre doch  $e_\alpha \circ x_j = 0$ . Die Zahl  $l$  existiert auf jeden Fall und wenn  $\chi > 0$ , so ist  $l \leq \chi$ .

Die Eigenwertsequenz  $\gamma, \gamma + \alpha, \dots, \gamma + (l-1)\alpha$  heißt die zu  $\alpha, \gamma$  gehörige Serie. Die Zahl  $l$  heißt die Länge der Serie. Die Gestalt der Serie hängt nicht ab von der Auswahl des von Null verschiedenen Elementes  $x_0$  aus  $L_\gamma$ . Die Länge  $l$  ist dadurch gekennzeichnet, daß:

$$L_\alpha \circ L_{\gamma+i\alpha} \neq 0, \text{ wenn } 0 \leq i < l-2, \text{ und } L_\alpha \circ L_{\gamma+(l-1)\alpha} = 0.$$

Da  $x_{l-1} \neq 0, x_l = 0$ , so folgt aus (11a), daß  $v_l = 0$ , also ist:

$$(15) \quad v_0 + \lambda \left( l\gamma + \binom{l}{2} \alpha \right) = 0.$$

Da  $e_\alpha \circ L_\alpha = 0$ , so kann  $\alpha$  nur als Endglied in einer zugehörigen Serie vorkommen. Diese Bemerkung ist für das Folgende zu beachten.

**Hilfssatz 4:** Wenn

$$\text{a) } e_{-\alpha} \circ x_0 = 0, \quad \text{b) } e_{-\alpha} \circ e_\alpha \neq 0, \quad \text{c) } x_0 \circ x_{l-1} = 0,$$

so ist

$$x_i \circ x_j = 0 \quad (0 \leq i \leq j < l).$$

**Beweis:** Sei  $0 \leq i \leq l, n_{ij} = l - (j - i)$ . Wir führen den Beweis durch endliche Induktion nach  $n_{ij}$ . Es ist:  $1 \leq n_{ij} \leq l$ . Wenn  $n_{ij} = 1$ , so ist  $i = 0, j = l - 1$  und nach Vor. c) der Hilfssatz bewiesen. Wenn  $n_{ij} = l$ , so ist  $i = j$  und die Behauptung klar. Nun sei  $1 < n_{ij} < l$  und schon bewiesen, daß  $x_{i'} \circ x_{j'} = 0$ , sobald  $n_{i'j'} < n_{ij}$ . Wir unterscheiden zwei Fälle:

1.  $i > 0$ . Dann ist

$$x_i \circ x_j = (e_\alpha \circ x_{i-1}) \circ x_j = -(x_{i-1} \circ x_j) \circ e_\alpha - (x_j \circ e_\alpha) \circ x_{i-1}$$

und entweder ist

$$j = l - 1, \quad x_j \circ e_\alpha = 0 \quad \text{oder} \quad j < l - 1. \quad x_j \circ e_\alpha = -x_{j+1}$$

und nach Induktionsvoraussetzung

$$x_{j+1} \circ x_{i-1} = -x_{i-1} \circ x_{j+1} = 0.$$

Ebenso ist nach Ind. vor.  $x_{i-1} \circ x_j = 0$ . Also ist  $x_i \circ x_j = 0$ .

2.  $i = 0$ . Dann ist  $j < l - 1$ . Nach Vor. a) ist  $\nu_0 = 0$ , nach Vor. b) ist  $\lambda \neq 0$ , also ist

$$l\gamma + \binom{l}{2} \alpha = 0.$$

Wäre  $l \equiv 0 \pmod{\chi}$ , so würde folgen  $\chi > 0$ , und da dann  $l \leq \chi$ , so wäre  $l = \chi$ . Da  $\alpha$  und  $\gamma$  in  $m$  liegen, so würde die zu  $\alpha, \gamma$  gehörige Serie ganz in  $m$  ausfüllen. Da  $\alpha$  nur als Endglied in der Serie vorkommen darf, so müßte  $\alpha = \gamma + (\chi - 1)\alpha$  sein. Dann würde die Beweismethode unter 1. ergeben:

$$x_i \circ x_{l-1} = 0$$

und da

$$\{x_{l-1}\} = \{e_\alpha\}, \quad \{x_{l-3}\} = \{e_{-\alpha}\},$$

so würde der Widerspruch  $e_{-\alpha} \circ e_\alpha = 0$  folgen. Wir dürfen also annehmen, daß  $l \not\equiv 0 \pmod{\chi}$ . Da das Polynom  $f(\xi) = \left( \xi\gamma + \binom{\xi}{2} \alpha \right)$  nun die beiden verschiedenen Nullstellen 0 und 1 hat und da es quadratisch ist, so ist

$$\begin{aligned} f(j+1) &= (j+1)\gamma + \binom{j+1}{2} \alpha \neq 0, \\ x_0 \circ x_j &= \lambda^{-1} f(j+1)^{-1} x_0 \circ (e_{-\alpha} \circ x_{j+1}), \\ x_0 \circ (e_{-\alpha} \circ x_{j+1}) &= x_{j+1} \circ (e_{-\alpha} \circ x_0) + e_{-\alpha} \circ (x_0 \circ x_{j+1}). \end{aligned}$$

Nach Induktionsvoraussetzung ist  $x_0 \circ x_{j+1} = 0$ . Nach Vor. a) ist  $e_{-\alpha} \circ x_0 = 0$ . Also ist

$$x_0 \circ (e_{-\alpha} \circ x_{j+1}) = 0,$$

mithin  $x_0 \circ x_j = 0$ , w. z. b. w.

Der Fall  $\chi = 0$  werde vorweg behandelt. Für ein festes  $\alpha_q$  setzen wir:

$$y_0 = e_{\alpha_q}, \quad y_{-1} = e_{-\varepsilon} \circ y_0, \dots, y_{-i} = e_{-\varepsilon} \circ y_{-(i-1)} \dots$$

Da  $y_{-i} \in L_{\alpha_q - i\varepsilon}$  und wegen  $\varepsilon \neq 0$  die Zahlen  $\alpha_q, \alpha_q - \varepsilon, \dots, \alpha_q - i\varepsilon$  alle untereinander verschieden sind, so gibt es eine Zahl  $j$ , so daß  $y_{-j} \neq 0, y_{-j-1} = 0$ . Für die zu  $\varepsilon, y_{-j}$  gehörige Serie ist  $\nu_0 = 0, \lambda \neq 0$  zu setzen. Formel (15) ergibt:

$$\alpha_q - j\varepsilon = -(l-1)/2 \cdot \varepsilon.$$

Nennen wir nun eine nichtganze Zahl, deren Doppeltes ganz ist, *halbganze Zahl*, so folgt: Die Quotienten  $\alpha_q \varepsilon^{-1}$  sind entweder ganz oder halbganz.

Unter den Quotienten  $\alpha_q \varepsilon^{-1}$  sei  $\alpha_\nu \varepsilon^{-1}$  die kleinste ganze Zahl. Dann ist  $L_{\alpha_\nu - \varepsilon} = 0, e_{-\varepsilon} \circ e_{\alpha_\nu} = 0$ . Für die zu  $\varepsilon, \alpha_\nu$  gehörige Serie ist in Formel (15)  $\nu_0 = 0, \lambda \neq 0$  zu setzen. Wir finden:

$$\alpha_\nu + (l-1)/2 \cdot \varepsilon = 0.$$



Demnach lautet die zu  $\varepsilon, \alpha_\nu$  gehörige Serie  $\alpha_\nu, \alpha_\nu + \varepsilon, \dots, -\varepsilon, 0, \varepsilon, \dots, -\alpha_\nu - \varepsilon, -\alpha_\nu$ . Da  $\varepsilon$  nur als Endglied in der Serie vorkommen darf, so folgt  $\varepsilon = -\alpha_\nu$ . Also ist  $-1$  die kleinste ganze Zahl unter den Quotienten  $\alpha_\rho \varepsilon^{-1}$ . Ersetzen wir in der Betrachtung  $\varepsilon$  durch  $-\varepsilon$ , so folgt ebenso, daß  $+1$  die größte ganze Zahl unter den Quotienten  $\alpha_\rho \varepsilon^{-1}$  ist. Als ganzzahlige Vielfache von  $\varepsilon$  kommen also nur

$$(16) \quad 0, +\varepsilon, -\varepsilon$$

unter den  $\alpha_\rho$  vor. Da  $r > 3$  sein soll, so müssen auch halbganze Vielfache von  $\varepsilon$  unter den  $\alpha_\rho$  vorkommen. Es sei  $\alpha_x \varepsilon^{-1}$  die kleinste halbganze Zahl unter den Quotienten  $\alpha_\rho \varepsilon^{-1}$ . Wie vorhin lautet die zu  $\varepsilon, \alpha_x$  gehörige Serie

$$(17) \quad \alpha_x, \alpha_x + \varepsilon, \dots, -\varepsilon/2, +\varepsilon/2, \dots, -\alpha_x,$$

und es ist  $e_\varepsilon \circ e_{\alpha_x + i\varepsilon} \neq 0$ , sobald  $\alpha_x + i\varepsilon$  zur Serie gehört und vom Endglied verschieden ist. Wenn wir in der vorstehenden Betrachtung  $\varepsilon$  durch  $-\varepsilon$  ersetzen, so folgt wegen  $e_{-\varepsilon} \circ e_{\alpha_x} = 0, e_\varepsilon \circ e_{-\alpha_x} = 0$ , daß durch (17) schon alle halbganzen Vielfache von  $\varepsilon$  unter den  $\alpha_\rho$  erschöpft sind. Demnach werden in (16) zusammen mit (17) schon alle  $\alpha_\rho$  aufgezählt. Wäre nun  $e_{-\alpha_x} \circ e_{\alpha_x} = 0$ , so würde nach Hilfssatz 4 folgen, daß jedes Kreisprodukt von halbganzen Vielfachen von  $\varepsilon$  verschwindet, dann wäre aber

$$L_1 = \{e_{\alpha_x}, e_{\alpha_x + \varepsilon}, \dots, e_{-\alpha_x}\}$$

ein von Null und  $L$  verschiedenes Ideal von  $L$ , was mit der Einfachheit von  $L$  im Widerspruch steht. Demnach ist

$$e_{\alpha_x} \circ e_{-\alpha_x} \neq 0.$$

Wir dürfen daher in der vorstehenden Betrachtung  $\varepsilon$  durch  $\alpha_x$  ersetzen und finden, daß entweder  $\varepsilon = 0, \pm \alpha_x$  oder daß  $\varepsilon$  halbganzes Vielfaches von  $\alpha_x$  ist. Da aber  $\varepsilon \neq 0$  und  $\alpha_x$  selbst halbganzes Vielfaches von  $\varepsilon$  ist, so führen beide Alternativen auf einen Widerspruch.

Der Fall  $r > 3$  ist bei Charakteristik 0 unmöglich. Es sei daher von nun an  $\chi > 3$ .

Wir ordnen die  $\alpha_\rho$  in folgender Weise an:

$$-\varepsilon, 0, \varepsilon, \alpha_4 = i_4 \varepsilon, \dots, \alpha_r = i_r \varepsilon.$$

wobei

$$1 < i_4 < i_5 < \dots < i_r < \chi - 1.$$

**A)** Wir prüfen zunächst die Annahme, daß die Länge jeder Serie kleiner als  $\chi$  ist. Entweder ist  $i_4 > 2$ , dann ist

$$e_{-\varepsilon} \circ e_{\alpha_4} = 0,$$

oder es ist  $i_4 = 2$ , dann ist

$$e_{-\varepsilon} \circ e_{\alpha_4} \in L_\varepsilon, \quad e_\varepsilon \circ (e_{-\varepsilon} \circ e_{\alpha_4}) = 0.$$

In jedem Fall ist:

$$(18) \quad e_\varepsilon \circ (e_{-\varepsilon} \circ e_{\alpha_4}) = 0.$$

Nun sei

$$(19) \quad e_\varepsilon \circ (e_{-\varepsilon} \circ e_{\alpha_j}) = 0 \quad (4 \leq j \leq r).$$

Die zu  $\varepsilon, \alpha_j$  gehörige Serie sei

$$(20) \quad \alpha_j, \alpha_j + \varepsilon, \dots, \alpha_j + (l' - 1)\varepsilon.$$

Wenn  $\varepsilon$  selbst in der Serie (20) vorkommt, so muß  $\varepsilon$  das Endglied sein, also

$$(19a) \quad \varepsilon = \alpha_j + (l' - 1)\varepsilon.$$

In der Formel (15) darf  $\lambda \neq 0$  und wegen (19)  $\nu_0 = 0$  eingesetzt werden. Es folgt:

$$l' \alpha_j + \binom{l'}{2} \varepsilon = 0;$$

(19a) eingesetzt ergibt:  $2 \cdot l' (3 - l') \equiv 0 \pmod{\chi}$  und da  $\chi > 3$ , so ist  $l' \equiv 0 \pmod{\chi}$ , also  $l' = \chi$ . Da das unserer Annahme A) widerspricht, so kommt  $\varepsilon$  nicht in der Serie (20) vor. Da  $e_{\varepsilon} \circ e_{-\varepsilon} \neq 0$ ,  $e_{\varepsilon} \circ e_0 \neq 0$ , so kommen auch  $-\varepsilon$  und 0 nicht in der Serie vor. Daher ist

$$l' < \chi, \quad \alpha_j + (l' - 1)\varepsilon = \alpha_{j+l'-1}$$

und

$$(21a) \quad i_{j+l'-1} \leq i_r.$$

In Formel (15) darf  $\lambda \neq 0$ ,  $l' \equiv 0 \pmod{\chi}$ , ferner wegen (19)  $\nu_0 = 0$  eingesetzt werden. Es folgt:

$$(21b) \quad \alpha_j + (\alpha_j + (l' - 1)\varepsilon) = 2\alpha_j + (l' - 1)\varepsilon = 0.$$

Demnach ist:

$$(21c) \quad i_j + (i_j + (l' - 1)) = \chi,$$

$$(21d) \quad i_j < \chi/2,$$

$$(21e) \quad i_{j+l'-1} > \chi/2$$

und aus (21c) mod 2:

$$(21f) \quad l' \equiv 0 \pmod{2}.$$

Nun sei

$$(22) \quad \alpha_4, \alpha_4 + \varepsilon, \dots, \alpha_4 + (l - 1)\varepsilon$$

die zu  $\varepsilon, \alpha_4$  gehörige Serie. Das Endglied ist gleich  $\alpha_{l+3}$ , es ist also

$$e_{\varepsilon} \circ e_{\alpha_{l+3}} = 0$$

und nach (21e):

$$(22a) \quad i_{l+3} > \chi/2.$$

Wäre hier  $l + 3 \neq i_r$ , so wäre sicher

$$e_{\varepsilon} \circ (e_{-\varepsilon} \circ e_{\alpha_{l+4}}) = 0.$$

Denn entweder ist

$$i_{l+4} > i_{l+3} + 1, \quad \text{also} \quad e_{-\varepsilon} \circ e_{\alpha_{l+4}} = 0,$$

oder es ist  $i_{l+4} = i_{l+3} + 1$ , dann ist

$$e_{-\varepsilon} \circ e_{\alpha_{l+4}} \in \{e_{\alpha_{l+3}}\}$$

und da  $e_{\varepsilon} \circ \{e_{\alpha_{l+3}}\} = 0$ , so folgt

$$e_{\varepsilon} \circ (e_{-\varepsilon} \circ e_{\alpha_{l+4}}) = 0.$$

Dann würde die zu  $\varepsilon, \alpha_{l+4}$  gehörige Serie der Bedingung (18) genügen, und es wäre gemäß (21d)  $i_{l+4} < \chi/2$ . Da andererseits  $i_{l+4} > i_{l+3}$ , so würde nach (22a) ein Widerspruch folgen. Also ist  $i_r = i_4 + (l - 1)$ , d. h. die  $\alpha_{\rho}$  werden erschöpft durch die Serie (22) und durch die Serie

$$(23) \quad -\varepsilon, 0, +\varepsilon.$$

Also ist  $l = r - 3$  und nach (21b):

$$(24a) \quad \alpha_4 = -(r-4)/2 \cdot \varepsilon, \quad \alpha_r = (r-4)/2 \cdot \varepsilon.$$

Ferner nach (21f)

$$(24b) \quad r \equiv 1 \pmod{2}.$$

Aus  $e_\varepsilon \circ e_\alpha = 0$  folgt also

$$\alpha = \varepsilon \text{ oder } \alpha = (r-4)/2 \cdot \varepsilon.$$

Wir schließen, daß allgemein aus  $e_{-\delta} \circ e_\delta \neq 0$  und  $e_\delta \circ e_\alpha = 0$  folgt:

$$\alpha = \delta \text{ oder } \alpha = (r-4)/2 \cdot \delta.$$

Da  $\varepsilon \neq \alpha_r$ ,  $\varepsilon \circ \alpha_r = 0$ , so würde aus  $e_{-\alpha_r} \circ e_{\alpha_r} \neq 0$  folgen, daß

$$\varepsilon = (r-4)/2 \cdot \alpha_r, \quad 1 \equiv (r-4)^2/4 \pmod{\chi}, \quad r \equiv 2, 6 \pmod{\chi}, \quad r = 2, 6$$

im Widerspruch zu (24b). Also ist  $e_{-\alpha_r} \circ e_{\alpha_r} = 0$ .

1. Es sei

$$(25) \quad e_{-\varepsilon} \circ e_{\alpha_4} = 0.$$

Wird in Hilfssatz 4 statt  $\alpha$  nun  $\varepsilon$  und statt  $\gamma$  nun  $\alpha_4$  eingesetzt, so folgt

$$(25a) \quad e_{\alpha_i} \circ e_{\alpha_j} = 0, \text{ wenn } 3 < i \leq j \leq r.$$

Aus (25) und (25a) folgt, daß die Elemente

$$(26) \quad e_{\alpha_4}, e_{\alpha_5}, \dots, e_{\alpha_r}$$

die  $k$ -Basis eines von 0 und  $L$  verschiedenen Ideals von  $L$  sind, was mit der vorausgesetzten Einfachheit von  $L$  im Widerspruch steht. Wir müssen also annehmen, daß

$$2. e_{-\varepsilon} \circ e_{\alpha_4} \neq 0.$$

Da  $e_{-\varepsilon} \circ e_{\alpha_4} \in L_{\alpha_4 - \varepsilon}$ , so ist  $\alpha_4 = 2\varepsilon$ ,

$$(27) \quad e_{-\varepsilon} \circ e_{2\varepsilon} \neq 0.$$

Weiter folgt aus (24a), daß  $r = \chi$ . Setzen wir nun

$$\begin{aligned} x_0 &= e_{2\varepsilon}, \\ x_1 &= e_\varepsilon \circ x_0, \dots, x_i = e_\varepsilon \circ x_{i-1}, \dots, e_\varepsilon \circ (e_{-\varepsilon} \circ x_0) = \nu_0 x_0, \\ e_{-\varepsilon} \circ x_i &= \nu_i x_{i-1} \quad (0 < i < \chi - 3), \end{aligned}$$

so folgt  $\nu_0 = 0$  und gemäß (14):

$$\nu_i = \mu \left( i \cdot 2\varepsilon + \binom{i}{2} \varepsilon \right), \quad 2\nu_i = \mu \varepsilon i (i+3),$$

und es ist ersichtlich  $\nu_i \neq 0$ , wenn  $0 < i < \chi - 3$ . Jetzt folgt

$$(28) \quad e_{-\varepsilon} \circ e_{i\varepsilon} \neq 0, \text{ wenn } 2 < i < \chi - 1.$$

Aus (27), (28) folgt, daß die zu  $e_{-\varepsilon} \cdot e_{(\chi-2)\varepsilon}$  gehörige Serie lautet:

$$e_{(\chi-2)\varepsilon}, e_{(\chi-3)\varepsilon}, \dots, e_{2\varepsilon}, e_\varepsilon, e_0, e_{-\varepsilon}.$$

**B)** Wir haben also doch nur die Annahme zu prüfen, daß es irgendeine Serie von der Länge  $\chi$  gibt. Sie laute:

$$(29) \quad \alpha, \quad \alpha + \beta, \quad \dots, \quad \alpha + (\chi - 1)\beta.$$

Da diese  $\chi$  Elemente verschieden sein sollen, so muß  $\beta \neq 0$  sein, und es werden in (29) alle Elemente aus  $m$  aufgezählt. Wir setzen:

$$e'_i = -\beta^{-1} e_{-i}\beta \quad (-1 \leq i < \chi - 1)$$

und finden, daß

$$L = \{e'_{-1}, e'_0, \dots, e'_{\chi-1}\}, \quad e'_0 \circ e'_i = i e'_i \quad (i \text{ beliebig})$$

und

$$e'_{-1} \circ e'_i \neq 0, \quad \text{wenn } 0 \leq i < \chi - 1.$$

Wir können und wollen voraussetzen, daß

$$e_{-1} \circ e_i \neq 0, \quad \text{wenn } 0 \leq i < \chi - 1.$$

Wenn  $0 \leq i < \chi - 1$ , so ist der Ansatz  $e_{-1} \circ e_i = (i+1)\lambda_i e_{i-1}$  erlaubt, und es ist  $\lambda_i \neq 0$ , außerdem wissen wir, daß  $\lambda_0 = 1$ . Wir setzen

$$\begin{aligned} e''_{-1} &= e_{-1}, & e''_0 &= e_0, & e''_1 &= \lambda_1^{-1} e_1, \\ e''_2 &= \lambda_1^{-1} \lambda_2^{-1} e_2, & \dots, & & e''_{\chi-2} &= \lambda_1^{-1} \cdot \lambda_2^{-1} \cdot \dots \cdot \lambda_{\chi-2}^{-1} e_{\chi-2}. \end{aligned}$$

Dann ist:

$$L = \{e''_{-1}, e''_0, \dots, e''_{\chi-2}\}, \quad e''_x \circ e''_i = (i-x)e''_{x+i}, \quad \text{wenn } x \equiv 0 \text{ oder } -1 \pmod{\chi}$$

Es sei also von vornherein:

$$(30) \quad e_{-1} \circ e_i = (i+1)e_{i-1}.$$

Falls  $e_1 \circ e_{-2} = 0$ , so setzen wir

$$e'_i = \sum_{\nu=-1}^i \binom{i+1}{\nu+1} \mu^{i-\nu} e_\nu \quad (-1 \leq i < \chi - 1),$$

wobei über die Konstante  $\mu$  noch geeignet verfügt werden soll. Wir erhalten:

$$e'_{-1} \circ e'_i = e_{-1} \circ e'_i = \sum_{\nu=-2}^{i-1} (\nu+2) \binom{i+1}{\nu+2} \mu^{i-1-\nu} e_\nu.$$

Da  $(\nu+2) \binom{i+1}{\nu+2}$  für  $\nu = -2$  oder  $i$  verschwindet und

$$(\nu+2) \binom{i+1}{\nu+2} = (i+1) \binom{i}{\nu+1},$$

so folgt weiter

$$e_{-1} \circ e'_i = i \cdot \sum_{\nu=-1}^i \binom{i}{\nu+1} \mu^{i-1-\nu} e_\nu = (i+1) e'_{i-1}.$$

Ferner ist:

$$e'_0 \circ e'_i = (e_0 + \mu e_{-1}) \circ e_i = \sum_{\nu=-1}^i \nu \binom{i+1}{\nu+1} \mu^{i-\nu} e_\nu + \sum_{\nu=-2}^{i-1} (\nu+2) \binom{i+1}{\nu+2} \mu^{i-\nu} e_\nu.$$

Da  $(\nu + 2) \binom{i+1}{\nu+2}$  verschwindet, wenn  $\nu = -2$  oder  $= i$ , so folgt weiter:

$$e'_0 \circ e'_i = \sum_{\nu=-1}^i \left( \nu \binom{i+1}{\nu+1} + (\nu+2) \binom{i+1}{\nu+2} \right) \mu^{i-\nu} e_\nu.$$

Man bestätigt leicht, daß

$$\nu \binom{i+1}{\nu+1} + (\nu+2) \binom{i+1}{\nu+2} = i \binom{i+1}{\nu+1},$$

also ist

$$e'_0 \circ e'_i = i e'_i.$$

Ferner ist sofort zu sehen, daß  $e_i \neq 0$  ( $i$  bel.), also hat  $e_0$  bei der regulären Darstellung die Eigenwerte  $-1, 0, \dots, \chi - 2$ , und  $e_i$  ist ein zu  $i$  gehöriges Eigenelement. Folglich sind die  $\chi$  Elemente  $e_{-1}, e_0, \dots, e_{\chi-2}$  linear unabhängig, bilden also eine  $k$ -Basis von  $L$ . Wie wir schon wissen, muß  $e'_\alpha \circ e'_\beta \in \{e'_{\alpha+\beta}\}$  sein, insbesondere

$$e'_1 \circ e'_{-2} \in \{e'_{-1}\} = \{e_{-1}\}.$$

Wir stellen  $e_1 \circ e_{-2}$  als Linearkombination der  $e_i$  dar und sammeln die Komponenten von  $e_{-1}$ , dann erhalten wir:

$$\begin{aligned} e'_1 \circ e'_{-2} &= e'_1 \circ e_{\chi-2} = e_1 \circ e_{\chi-2} + 2\mu e_0 \circ \mu^{\chi-1} e_{-1} + \mu^2 e_{-1} \circ (\chi-1) \mu^{\chi-2} e_0 \\ &= -3\mu^{\chi-1} e_{-1} (e_1 \circ e_{\chi-2} = e_1 \circ e_{-2} =: 0!). \end{aligned}$$

Nun verfügen wir über  $\mu$ , indem wir setzen  $\mu = 1$  (oder  $2, \dots, \chi - 1$ ) und erhalten

$$e'_1 \circ e'_{-2} = -3 e'_{-1}.$$

Nachdem wir ev. die Basis  $e_{-1}, e_0, \dots, e_{\chi-2}$  durch die Basis  $e'_{-1}, e'_0, \dots, e'_{\chi-2}$  von  $L$  ersetzt haben, dürfen wir annehmen, daß  $e_1 \circ e_{-2} \neq 0$ . Da  $\chi > 3$ , so ist der Ansatz:  $e_1 \circ e_{-2} = 3\xi e_{-1}$  erlaubt, und es ist  $\xi \neq 0$ . Da  $k$  vollkommen, so ist die Gleichung  $\xi^{-1} = \eta^\chi$  in  $k$  lösbar. Wir führen die Substitution

$$e''_i = \eta^i e_i \quad (-1 \leq i < \chi - 1)$$

aus und erhalten:

$$e''_{-1} \circ e''_i = (i+1) e''_{i-1}, \quad e''_0 \circ e''_i = i e''_i, \quad e''_1 \circ e''_{-2} = -3 e''_{-1}.$$

Mithin dürfen wir über  $L$  voraussetzen, daß

$$(31) \quad e_{-1} \circ e_i = (i+1) e_{i-1} \quad (i \in m),$$

$$(32) \quad e_1 \circ e_{-2} = -3 e_{-1}.$$

**Hilfssatz 5:** Aus den Gleichungen (1), (31), (32) folgt

$$(33) \quad e_i \circ e_j = (j-i) e_{i+j}, \quad \text{wenn } -1 \leq i \leq j < \chi - 1 \text{ und } i+j < \chi - 1,$$

also auch

$$e_j \circ e_i = (i-j) e_{j+i}.$$

Beweis: (33) ist klar, wenn  $i = j$ , sei also weiterhin  $i < j$ . Wir wenden endliche Induktion nach  $n_{ij} = \chi - (j - i)$  an. Es ist  $1 \leq n_{ij} < \chi$ . Wenn  $n_{ij} = 1$ , so ist  $i = -1, j = \chi - 2$  und dann ist (33) gemäß (31) richtig. Sei weiter  $1 < n_{ij} \leq \chi - 1$

und (33) schon gezeigt für alle Paare  $i', j'$ , für die  $n_{i'j'} < n_{ij}$ . Wenn  $i = -1$  bzw. 0 so ist (33) gemäß (31) bzw. (1) richtig. Sei also  $i > 0$ .

1.  $j < \chi - 2$ . Dann ist

$$j + 2 \not\equiv 0 \pmod{\chi},$$

$$e_j = (j + 2)^{-1} e_{-1} \circ e_{j+1} e_i \circ e_j = (j + 2)^{-1} e_i \circ (e_{-1} \circ e_{j+1}),$$

$$e_i \circ (e_{-1} \circ e_{j+1}) = e_{-1} \circ (e_i \circ e_{j+1}) + e_{j+1} \circ (e_{-1} \circ e_i).$$

Nach Ind. vor. ist

$$e_i \circ e_{j+1} = (j + 1 - i) e_{i+j+1}, \quad e_{j+1} \circ e_{i-1} = (i - j - 2) e_{i+j},$$

ferner ist

$$e_{-1} \circ e_i = (i + 1) e_{i-1}.$$

Nach einiger Rechnung folgt:

$$e_i \circ (e_{-1} \circ e_{j+1}) = (j + 2) (j - i) e_{i+j}, \quad e_i \circ e_j = (j - i) e_{i+j}.$$

2.  $j = \chi - 2$ . Dann ist  $i > 2$ ,

$$e_i = (i - 2)^{-1} e_1 \circ e_{i-1}, \quad e_i \circ e_j = (i - 2)^{-1} (e_1 \circ e_{i-1}) \circ e_j,$$

$$(e_1 \circ e_{i-1}) \circ e_j = (e_1 \circ e_j) \circ e_{i-1} - (e_{i-1} \circ e_j) \circ e_1.$$

Nach Ind. vor. ist

$$e_{i-1} \circ e_j = (j - i + 1) e_{i+j-1} = (-1 - i) e_{i-3}.$$

Ferner ist nach (32)

$$e_1 \circ e_j = -3 e_{-1}$$

und nach (31)

$$e_{-1} \circ e_{i-1} = i e_{i-2},$$

also nach einiger Rechnung:

$$(e_1 \circ e_{i-1}) \circ e_j = (i - 2) (-2 - i) e_{i-2}, \quad e_i \circ e_j = (-2 - i) e_{i-2} = (j - i) e_{i+j}.$$

w. z. b. w.

Nun setzen wir:

$$d_i = (-1)^{i+1} e_{-i} \quad (-1 \leq i < \chi - 1)$$

und finden, daß  $d_0 \circ d_i = i d_i$ , ferner auf Grund von Hilfssatz und von (32), daß  $d_{-1} \circ d_i = (i + 1) d_{i-1}$  und gemäß (31), daß  $d_1 \circ d_{-2} = -3 d_{-1}$ . Aus dem eben bewiesenen Hilfssatz, angewendet auf die  $d_i$ , folgt:

$$d_i \circ d_j = (j - i) d_{i+j}, \quad \text{wenn } -1 \leq i \leq j < \chi - 1 \text{ und } i + j < \chi - 1.$$

Auf die  $e_i$  umgerechnet erhalten wir:

$$(34) \quad e_i \circ e_j = (j - i) e_{i+j}, \quad \text{wenn } -1 \leq i \leq j < \chi - 1 \text{ und } i + j > \chi + 1.$$

also auch

$$e_j \circ e_i = (i - j) e_{j+1}.$$

Durch den Ansatz:

$$e_i \circ e_j = (j - i) \xi_{ij} e_{i+j}, \quad \xi_{ii} = 1$$

sind die Zahlen  $\xi_{ij}$  eindeutig definiert. Wir haben die Zahlen  $\xi_{ij}$  noch zu bestimmen, wenn  $2 \leq i \leq \chi - 2$ ,  $2 \leq j \leq \chi - 2$  und  $i + j = \chi - 1$  oder  $\chi$  oder  $\chi + 1$ . — In allen anderen Fällen sind sie gleich 1. — Man setze:

$$i' = (\chi - 1)/2, \quad j' = (\chi + 1)/2,$$

dann folgt zunächst:

$$i' + j' \equiv 0, \quad j' - i' \equiv 1, \quad 2(1 - j) \equiv 1 \pmod{\chi},$$

ferner

$$\begin{aligned} 0 &= e_1 \circ (e_{i'} \circ e_{j'}) + e_{i'} \circ (e_{j'} \circ e_1) + e_{j'} \circ (e_1 \circ e_{i'}) \\ &= e_1 \circ \xi_{i',j'} e_0 + e_{i'} \circ (1 - j') e_{j'+1} + e_{j'} \circ (i' - 1) e_{j'} \\ &= e_1 (-\xi_{i',j'} + 2(1 - j') \xi_{i',j'+1}), \end{aligned}$$

also ist

$$\xi_{i',j'} = \xi_{i',j'+1}.$$

Ähnlich folgt

$$\xi_{i'-1,j'} = \xi_{i',j'} \text{ aus der Relation: } 0 = e_{-1} \circ (e_{i'} \circ e_{j'}) + \dots.$$

Jetzt zeigen wir unter der Voraussetzung:

$$2 < i < j < \chi - 2, \quad i + j = \chi, \quad \xi_{i-1,j} = \xi_{ij} = \xi_{i,j+1} = \xi,$$

daß (a)  $\xi_{i-1,j+1} = \xi$  und falls sogar  $3 < i < j < \chi - 3$ , so (b)  $\xi_{i-2,j+1} = \xi_{i-1,j+2} = \xi$ . Das möge sich der Leser herleiten aus den Jacobiidentitäten:

$$\begin{aligned} 0 &= e_1 \circ (e_{i-1} \circ e_j) + \dots, & 0 &= e_1 \circ (e_{i-1} \circ e_{j-1}) + \dots, \\ 0 &= e_{-1} \circ (e_{i-1} \circ e_{j+1}) + \dots \end{aligned}$$

Durch endliche Induktion schließen wir aus den eben gefundenen Resultaten, daß  $\xi_{ij} = \xi_{i',j'} = \xi$ , wenn  $2 \leq i < j < \chi - 2$ ,  $i + j = \chi - 1$  oder  $\chi$  oder  $\chi + 1$ . Aus der Jacobiidentität  $0 = e_1 \circ (e_2 \circ e_{-2}) + \dots$  folgt nunmehr, daß  $\xi = 1$ . Also gilt allgemein:

$$(35) \quad e_i \circ e_j = (j - i) e_{i+j} \quad (i, j \in m).$$

Nun wollen wir Lie'sche Ringe von dem gesuchten Typus konstruieren. Es sei  $M$  ein in  $k$  enthaltener Modul. Jedem Element  $\alpha$  aus  $M$  ordnen wir ein Symbol  $e_\alpha$  zu. Gemäß § 1 konstruieren wir einen distributiven Ring  $L = L(k, M)$  mit den Elementen  $e_\alpha$  ( $\alpha \in M$ ) als Basis und der Rechenregel:

$$e_\alpha \circ e_\beta = (\beta - \alpha) e_{\alpha+\beta}.$$

Ohne weiteres bestätigen wir, daß die Bedingungen I, II (§ 1; 1) erfüllt sind. Ferner ist:

$$\begin{aligned} e_\alpha \circ (e_\beta \circ e_\gamma) + e_\beta \circ (e_\gamma \circ e_\alpha) + e_\gamma \circ (e_\alpha \circ e_\beta) \\ = e_{\alpha+\beta+\gamma} ((\alpha - \beta - \gamma)(\beta - \gamma) + (\beta - \gamma - \alpha)(\gamma - \alpha) \\ + (\gamma - \alpha - \beta)(\alpha - \beta)) = 0, \end{aligned}$$

wie sofort nachgerechnet wird. Demnach ist auch III erfüllt, also ist  $L(k, M)$  ein Lie'scher  $k$ -Ring.

Wenn das in  $M$  enthaltene Element  $\alpha$  von Null verschieden ist, so ist  $(\alpha^{-1} e_0) \circ e_\alpha = e_\alpha$ , also ist dann  $e_\alpha$  in  $D(L)$  enthalten. Falls  $\chi(k) \neq 2$

und  $M \neq 0$ , so gibt es ein  $\alpha \neq 0$  und für dieses  $\alpha$  ist

$$((2\alpha)^{-1}e_{-\alpha}) \circ e_{\alpha} = e_0,$$

also ist dann  $e_0$  in  $D(L)$  enthalten und  $L = D(L)$ . Falls aber  $\chi(k) = 2$ ,  $M \neq 0$ , so bilden alle  $e_{\alpha}$ , für die  $0 \neq \alpha \in M$ , die Basis eines  $k$ -Moduls, der ersichtlich alle Kreisprodukte von je zwei Basiselementen von  $L$  enthält. Zusammen mit dem oben gezeigten folgt, daß  $D(L)$  die Elemente  $e_{\alpha}$  mit  $0 \neq \alpha \in M$  als Basis über  $k$  besitzt.

Wenn  $M = 0$ , so ist  $L$  eingliedrig, also abelsch.

*Bemerkung:* Wenn  $\chi \neq 0$ , so sind  $L(k, M)$  und  $L(k, \lambda M)$  isomorph.

Sei nämlich

$$L(k, M) = \sum_{\alpha \in M} k e_{\alpha}, \quad e_{\alpha} \cdot e_{\beta} = (\beta - \alpha) e_{\alpha + \beta},$$

$$L(k, \lambda M) = \sum_{\alpha \in M} k d_{\lambda \alpha}, \quad d_{\lambda \alpha} \circ d_{\lambda \beta} = (\beta - \alpha) d_{\lambda(\alpha + \beta)} \quad (\alpha, \beta \in M),$$

dann bilden wir ab:

$$\sum_{\alpha \in M} \lambda_{\alpha} e_{\alpha} \longrightarrow \sum_{\alpha \in M} \lambda \cdot \lambda_{\alpha} d_{\lambda \alpha}.$$

Wenn nun  $\chi > 0$ , so entsteht jeder Modul  $M$ , der aus  $\chi$  Elementen besteht, durch Multiplikation mit einem Körperelement  $\neq 0$  aus dem Modul  $m = (0, 1, \dots, \chi - 1)$  hervor. Also sind die  $\chi$ -gliedrigen Lie'schen Ringe  $L(k, M)$  alle untereinander isomorph. Wir bezeichnen den  $\chi$ -gliedrigen Ring  $L(k, m)$  daher mit  $L(k, \chi)$ .

**Satz 14:** Wenn  $M \neq 0$ , so ist  $D(L)$  ein einfacher Lie'scher  $k$ -Ring.

*Beweis:* Sei  $M \neq 0$ . Dann ist  $D(L) \neq 0$ . Wir haben zu zeigen, daß jedes von Null verschiedene Ideal von  $A$  von  $D(L)$  mit  $D(L)$  übereinstimmt. Es gibt von Null verschiedene Elemente  $a$  in  $A$  und  $a$  hat eindeutig die Form

$$a = \sum_1^r \lambda_i e_{\alpha_i}$$

$$(r > 0; \lambda_i \neq 0, \alpha_i \in M (i = 1, 2, \dots, r); \alpha_i \neq \alpha_k, \text{ wenn } i \neq k).$$

Wir wählen  $a$  so, daß die Anzahl  $r$  der von Null verschiedenen Komponenten von  $a$  möglichst klein wird. Wäre  $r > 1$ , so wäre  $e_{\alpha_1} \in D(L)$ ,  $0 \neq a' = e_{\alpha_1} \circ a \in A$  und  $a'$  hätte nur  $r - 1$  von Null verschiedene Komponenten. Also ist  $r = 1$ ,  $a = \lambda e_{\alpha}$ ,  $\lambda \neq 0$ . Dann liegt auch  $e_{\alpha}$  in  $A$ . Wenn  $\chi \neq 2$ , so liegt  $e_{-\alpha}$  in  $D(L)$ , also ist entweder schon  $\alpha = 0$  oder  $\alpha \neq 0$  und  $e_0 = (2\alpha) e_{-\alpha} \circ e_{\alpha}$  in  $A$  enthalten, mithin auch

$$e_{\beta} = \beta^{-1} e_0 \circ e_{\beta} \in A \text{ für alle } \beta \neq 0$$

und daher  $A = L$ . Wenn  $\chi = 2$ , so folgt  $\alpha \neq 0$ . Wenn  $M \ni \beta \neq 0, \alpha$ , so folgt weiter, daß  $e_{\beta - \alpha}$  in  $D(L)$  liegt, also liegt  $e_{\beta} = \beta^{-1} e_{\alpha} \circ e_{\beta - \alpha}$  in  $A$ , mithin ist  $A = D(L)$ , w. z. b. w.



**Satz 15:** Die einfachen und nicht abelschen Lie'schen Ringe mit einer Basis  $e_0, e_{\alpha_1}, \dots, e_{\alpha_r}$  über dem Körper  $k$  mit der Charakteristik  $\chi$ , so daß  $0 = \alpha_1, \alpha_2, \dots, \alpha_r \pmod{\chi}$  inkongruente ganze Zahlen sind und die Rechenregel  $e_0 \circ e_{\alpha_i} = \alpha_i e_{\alpha_i}$  gilt, haben einen der beiden Typen:

1.  $L \cong SM_2(k)$  ( $\chi \neq 2$ ),
2.  $L \cong L(k, \chi)$  ( $\chi > 3$ ) ( $L(k, 3) \cong SM_2!$ ).

#### § 4. Die Endomorphismen eines Lie'schen Ringes.

Es sei  $k$  ein Ring mit Einheitsselement,  $L$  sei ein Lie'scher  $k$ -Ring und  $A$  ein Ideal von  $L$ . Welche Eigenschaften haben die durch die Festsetzung  $\underline{x}a = x \circ a$  mit festem  $x$  aus  $L$ , beliebigem  $a$  aus  $A$ , erklärten eindeutigen Abbildungen von  $A$  in sich? Offenbar ist

$$\underline{x}(a+b) = \underline{x}a + \underline{x}b, \quad \underline{x}(\lambda a) = \lambda \underline{x}a,$$

schließlich

$$\begin{aligned} \underline{x}(a \circ b) &= x \circ (a \circ b) = -a \circ (b \circ x) - b \circ (x \circ a) \\ &= a \circ \underline{x}b + \underline{x}a \circ b. \end{aligned}$$

Definition: *Endomorphismus* des Lie'schen  $k$ -Ringes  $L$  heißt jede eindeutige Abbildung  $\sigma$  von  $L$  in sich, bei der

- (1)  $\sigma(a+b) = \sigma a + \sigma b,$
- (2)  $\sigma(\lambda a) = \lambda \sigma a \quad (\lambda \in k),$
- (3)  $\sigma(a \circ b) = a \circ (\sigma b) + (\sigma a) \circ b,$

z. B. wird durch die Festsetzung  $\underline{x}a = x \circ a$  ( $a \in L$ ) jedem Element  $x$  aus  $L$  eindeutig ein Endomorphismus  $\underline{x}$  zugeordnet. Die Gleichung (3) ist dabei gleichbedeutend mit der Jacobi-Identität.  $\underline{x}$  heißt der zu  $x$  gehörige *innere Endomorphismus*.

Alle Endomorphismen von  $L$  bilden einen Lie'schen  $k$ -Ring  $E(L)$ , wobei die naheliegenden Rechenregeln

$$\begin{aligned} (\sigma + \tau) a &= \sigma a + \tau a, \\ (\lambda \sigma) a &= \lambda (\sigma a), \\ (\sigma \circ \tau) a &= \sigma(\tau a) - \tau(\sigma a) \end{aligned}$$

verwendet werden. Zu zeigen ist hier nur, daß mit  $\sigma$  zugleich  $\lambda \sigma$  und daß mit  $\sigma$  und  $\tau$  zugleich auch  $\sigma + \tau$  und  $\sigma \circ \tau$  Endomorphismen sind.

Die inneren Endomorphismen bilden ebenfalls einen Lie'schen Ring  $I(L)$ , denn die Abbildung  $x \rightarrow \underline{x}$  ist ja die reguläre Darstellung von  $L$  in linearen Transformationen des  $k$ -Moduls  $L$  und dabei wird  $L$

gerade auf  $I(L)$  abgebildet. Also folgt  $I(L) \cong L/\mathfrak{I}(L)$ .  $I(L)$  ist ein Ideal von  $E(L)$ , denn es ist:

$$\begin{aligned} (\sigma \circ \underline{x}) a &= \underline{\sigma x} a - \underline{x} \sigma a = \sigma(x \circ a) - x \circ \sigma a \\ &= \sigma x \circ a && \text{(nach (3)),} \\ (3a) \quad \sigma \circ \underline{x} &= \underline{\sigma x}. \end{aligned}$$

Der Faktorring  $E(L)/I(L)$  heißt der *äußere Endomorphismenring* von  $L$ .

Nach Formel (26a, b) des § 1, 2 gilt für jeden Endomorphismus  $\sigma$  von  $L$ :

$$(4) \quad \sigma^n(x \circ y) = \sum_{i=0}^n \binom{n}{i} \sigma^i x \circ \sigma^{n-i} y.$$

Wenn die Charakteristik von  $L$  eine Primzahl  $p$  ist, so folgt:

$$(5) \quad \sigma^{p^\nu}(x \circ y) = x \circ \sigma^{p^\nu} y + \sigma^{p^\nu} x \circ y \quad (\nu = 0, 1, 2, \dots).$$

Daraus folgt:

(6) Die  $p^\nu$ -te Potenz jedes Endomorphismus eines Lie'schen  $k$ -Ringes mit der Primzahlcharakteristik  $p$  ist wieder ein Endomorphismus.

Wenn  $K$  ein Lie'scher Teilring,  $N(K)$  der Normalisator von  $K$  ist,  $Z(K)$  der Zentralisator von  $K$  ist, dann wird durch die Abbildung  $x \rightarrow \tilde{x} = \begin{pmatrix} a \\ x \circ a \end{pmatrix}$  ( $a$  bel. aus  $L$ ) jedem  $x$  aus  $N(L)$  eindeutig ein Endomorphismus  $\tilde{x}$  von  $L$  zugeordnet. Die Zuordnung  $x \rightarrow \tilde{x}$  ist eine Darstellung von  $N(L)$  in Endomorphismen von  $K$ , bei der genau  $Z(K)$  auf Null abgebildet wird, so daß der Faktorring  $N(L)/Z(L)$  isomorph ist zu einem Lie'schen  $k$ -Ring aus Endomorphismen von  $L$ . Der Faktorring  $L + Z(L)/Z(L)$  ist isomorph zu  $I(L)$ . Der Faktorring  $\Lambda(L)/L + Z(L)$  ist isomorph zu einem gewissen  $k$ -Teilring des äußeren Endomorphismenringes von  $L$ .

Wenn  $\Sigma$  eine Menge von Endomorphismen von  $L$  ist und  $K$  ein Komplex aus  $L$ , so sagen wir:  $K$  ist *unter  $\Sigma$  invariant*, wenn  $\sigma a \in K$  für alle  $\sigma$  aus  $\Sigma$ ,  $a$  aus  $K$ .

Mit  $K$  ist auch der aus  $K$  erzeugte  $k$ -Modul  $\{K\}$  und der aus  $K$  erzeugte Lie'sche  $k$ -Ring  $\{K\}$  unter  $\Sigma$  invariant, wie leicht zu sehen.

Ferner ist der Zentralisator  $Z(K)$  unter  $\Sigma$  invariant, denn aus  $x \circ a = 0$  für alle  $a$  aus  $K$  folgt  $(\sigma x) \circ a = \sigma(x \circ a) - x \circ \sigma a = 0 - 0 = 0$ . Wenn  $K$  ein unter  $\Sigma$  invarianter  $k$ -Modul ist, dann ist  $K$  auch invariant unter dem aus  $\Sigma$  erzeugten  $k$ -Modul  $\{\Sigma\}$  und unter dem aus  $\Sigma$  erzeugten Lie'schen  $k$ -Ring  $\{\Sigma\}$ . Ferner ist der Normalisator von  $K$  unter  $\Sigma$  invariant, denn aus  $x \circ a \in K$  für alle  $a$  aus  $K$  folgt:

$$(\sigma x) \circ a = \sigma(x \circ a) - x \circ (\sigma a) \in K + K \leq K.$$

Wenn  $K_1$  und  $K_2$  zwei unter  $\Sigma$  invariante  $k$ -Teilmoduln aus  $L$  sind, so sind auch

$$K_1 + K_2, \quad \{K_1 \circ K_2\}, \quad K_1 \cap K_2$$

unter  $\Sigma$  invariant.

Wenn  $A$  ein unter  $\Sigma$  invariantes Ideal von  $L$  ist, so wird durch die Festsetzung  $\bar{\sigma}(a + A) = \sigma a + A$  jedem Endomorphismus  $\sigma$  aus  $\Sigma$  eindeutig ein Endomorphismus  $\bar{\sigma}$  von  $L/A$  zugeordnet. Er heißt der von  $\sigma$  in  $L/A$  induzierte Endomorphismus. Wir sagen: Alle Endomorphismen  $\bar{\sigma}$  bilden die Übertragung  $\bar{\Sigma}$  über  $L/A$  von der Endomorphismenmenge  $\Sigma$  über  $L$ .

Wenn  $K$  unter  $\Sigma$  invariant ist, dann ist  $K + A/A$  unter  $\bar{\Sigma}$  invariant. Wenn umgekehrt  $B/A$  unter  $\bar{\Sigma}$  invariant ist, dann ist  $B$  unter  $\Sigma$  invariant.

Wenn  $\varrho$  eine homomorphe Abbildung von  $L$  auf einen Bildring  $\bar{L}$  ist, so liegt es nahe, die Endomorphismenmenge  $\Sigma$  über  $L$  zu übertragen auf eine Endomorphismenmenge  $\bar{\Sigma}$  über  $\bar{L}$  durch die Festsetzung

$$(7) \quad \bar{\sigma}(\varrho a) = \varrho(\sigma a).$$

Gleichung (7) definiert dann und nur dann einen Endomorphismus von  $L$ , wenn das Ideal  $A$ , bestehend aus allen Elementen von  $L$ , die durch  $\varrho$  auf 0 abgebildet werden, invariant unter  $\Sigma$  ist. Dann bildet die Menge  $\bar{\Sigma}$  aller Endomorphismen  $\bar{\sigma}$  ( $\sigma \in \Sigma$ ) von  $\bar{L}$  die Übertragung von  $\Sigma$  nach  $\bar{L}$ .

Wenn  $K$  ein unter  $\Sigma$  invarianter Lie'scher  $k$ -Ring, so wird durch die Festsetzung  $\bar{\sigma}a = \sigma a$  für alle  $a$  aus  $K$  jedem aus  $\Sigma$  stammenden Endomorphismus von  $L$  ein Endomorphismus von  $K$  eindeutig zugeordnet. Er heißt der von  $\sigma$  in  $K$  induzierte Endomorphismus. Die Ableitung und das Zentrum von  $K$  sind unter  $\Sigma$  invariant, wie leicht zu sehen.

Definition:  $\Sigma$  sei eine Menge von Endomorphismen des Lie'schen  $k$ -Ringes  $L$ .  $L$  heißt  $\Sigma$ -einfach, wenn es kein von 0 und  $L$  verschiedenes und unter  $\Sigma$  invariantes Ideal von  $L$  gibt: —  $L$  ist sicher dann  $\Sigma$ -einfach, wenn  $L$  schlechthin einfach ist. Die unter  $I(L)$  invarianten  $k$ -Teilmoduln von  $L$  sind gerade die Ideale von  $L$ .

Definition: Ein unter allen Endomorphismen von  $L$  invarianter  $k$ -Teilmodul heißt charakteristisches Ideal von  $L$ .

Z. B. sind 0 und  $L$  charakteristische Ideale.  $L$  heißt charakteristisch einfach, wenn 0 und  $L$  die einzigen charakteristischen Ideale von  $L$  sind.

Ableitung und Zentrum eines charakteristischen Ideals sind charakteristische Ideale, also ist jeder charakteristische einfache Lie'sche Ring stets vollkommen oder abelsch.

Für ein beliebiges Ideal  $A$  und beliebigen Endomorphismus gilt:

$$(8) \quad \sigma(D(A)) \subseteq A.$$

Denn es ist

$$\sigma(a \circ b) = (\sigma a) \circ b + a \circ (\sigma b) \in A + A \subseteq A$$

für beliebige Elemente  $a$  und  $b$  aus  $A$ . Also sind vollkommene Ideale stets charakteristische Ideale.

Eine Kette von charakteristischen Idealen:

$$L = A_0 \supseteq A_1 \supseteq A_2 \cdots \supseteq A_r = 0$$

heißt *charakteristische Kette mit der Länge  $r$* . Z. B. sind

$$L \supseteq \mathfrak{z}_i(L) \supseteq \mathfrak{z}_{i-1}(L) \cdots \supseteq \mathfrak{z}_1(L) = \mathfrak{z}(L) \supseteq \mathfrak{z}_0(L) = 0,$$

$$L = \mathfrak{Z}_1(L) \supseteq \mathfrak{Z}_2(L) \cdots \supseteq \mathfrak{Z}_i(L) \supseteq 0,$$

$$L = D^0(L) \supseteq D^1(L) = D(L) \supseteq D_2(L) \cdots \supseteq D^i(L) \supseteq 0$$

charakteristische Ketten. Eine charakteristische Kette heißt charakteristische Reihe, wenn sie keine Wiederholungen hat, also  $A_i \not\supseteq A_{i+1}$  ( $i = 0, 1, 2, \dots, r-1$ ), und wenn sie nicht mehr verfeinert werden kann, d. h. wenn es kein charakteristisches Ideal von  $L$  gibt, das zwischen  $A_i$  und  $A_{i+1}$  liegt, aber von  $A_i$  und  $A_{i+1}$  verschieden ist. Die Faktorringe  $A_i/A_{i+1}$  sind charakteristisch-einfache Lie'sche Ringe. Wenn umgekehrt die Faktorringe  $A_i/A_{i+1}$  einer charakteristischen Kette einfach sind, so ist die Kette eine charakteristische Reihe. Für charakteristische Ketten bzw. Reihen gelten die bekannten Sätze von SCHREIER bzw. JORDAN-HÖLDER.

Definition: Ein Lie'scher  $k$ -Ring heißt *abgeschlossen*, wenn sein Zentrum verschwindet und wenn jeder Endomorphismus ein innerer Endomorphismus ist.

**Satz 15:** *Der Endomorphismenring eines vollkommenen Lie'schen  $k$ -Ringes ohne Zentrum ist abgeschlossen.*

Beweis:  $L$  sei ein vollkommener Lie'scher  $k$ -Ring ohne Zentrum.  $E(L)$  sei der Endomorphismenring von  $L$ . Da  $L$  kein Zentrum hat, so ist  $L$  isomorph zu  $I(L)$ , also ist  $I(L)$  vollkommen. Das vollkommene Ideal  $I(L)$  ist invariant unter jedem Endomorphismus  $\Sigma$  von  $E(L)$ . Also induziert  $\Sigma$  einen Endomorphismus  $\bar{\sigma}$  von  $I(L)$ .  $x \rightarrow x$  sei die reguläre Darstellung von  $L$  durch  $I(L)$ . Sie ist nach Voraussetzung treu, also wird durch  $\underline{\sigma}x = \bar{\sigma}x$  ein Endomorphismus  $\sigma$  von  $L$  definiert.  $\underline{\sigma}$  sei der dem Element  $\bar{\sigma}$  von  $E(L)$  zugeordnete innere Endomorphismus von  $E(L)$ . Es ist

$$\underline{\Sigma}x = \underline{\bar{\sigma}}x = \underline{\sigma}x = \underline{\sigma}x,$$

also  $(\Sigma - \sigma)x = 0$  für alle  $x$  aus  $I(L)$ . Für den Endomorphismus  $\Sigma' = \Sigma - \underline{\sigma}$  von  $E(L)$  gilt für alle  $\tau$  aus  $E(L)$

$$\begin{aligned} 0 &= \Sigma'(\tau x) = \Sigma'(\tau \circ x) = (\Sigma'\tau) \circ x + \tau \circ (\Sigma'x) \\ &= (\Sigma'\tau) \circ x + 0 = (\Sigma'\tau)x. \end{aligned}$$

Da nun die reguläre Darstellung von  $L$  eine treue Darstellung ist, so ist  $\mathcal{S}'\tau = 0$  für alle  $\tau$  aus  $E(L)$ , also  $\mathcal{S}' = 0$ ,  $\mathcal{S} = \underline{\sigma}$ . Demnach ist jeder Endomorphismus von  $E(L)$  ein innerer Endomorphismus. Das Zentrum von  $E(L)$  ist  $0$ , denn für jedes Zentrumselement  $\zeta$  von  $E(L)$  gilt:  $0 = \zeta \circ \underline{x} = \underline{\zeta x}$  ( $x \in L$ ), also  $\zeta x = 0$ , weil die reguläre Darstellung von  $L$  treu ist, also  $\zeta = 0$ , womit alles bewiesen ist.

**Satz 16:** *Jede Lie'sche Algebra mit von Null verschiedener Diskriminante ist abgeschlossen.*

**Beweis:**  $L$  sei eine Lie'sche Algebra über dem Körper  $k$  mit von Null verschiedener Diskriminante. Wie früher gezeigt, ist das Zentrum von  $L$  gleich Null. Jeden Endomorphismus  $\sigma$  von  $L$  fassen wir als lineare Transformation von  $L$  auf. Nach § 1, 8 ist das Gleichungssystem:

$$\text{Sp}(\underline{xy_k}) = \text{Sp}(\underline{\sigma y_k}) \quad (k = 1, 2, \dots, n)$$

in dem  $y_1, y_2, \dots, y_n$  eine Basis von  $L$  über  $k$  ist, eindeutig lösbar durch eine lineare Transformation  $x$  aus  $L$ . Es folgt:  $\text{Sp}(\underline{xy}) = \text{Sp}(\underline{\sigma y})$  für alle  $y$  aus  $L$ . Für ein beliebiges  $z$  aus  $L$  und den Endomorphismus  $\tau = \sigma - \underline{x}$  ist

$$\begin{aligned} \text{Sp}(\underline{\tau z}) &= 0, & \tau \circ \underline{z} &= \underline{\tau z}, \\ \text{Sp}(\underline{\tau z \cdot y}) &= \text{Sp}(\underline{(\tau \circ z) y}) = \text{Sp}(\underline{\tau z y - z \tau y}) \\ &= \text{Sp}(\underline{\tau(z y - y z)}) + \text{Sp}(\underline{(\tau y) z - z(\tau y)}) \\ &= \text{Sp}(\underline{\tau(z \circ y)}) + \text{Sp}(\underline{(\tau y) \circ z}) = 0 + 0. \end{aligned}$$

Nach § 1, 8 folgt  $\tau z = 0$ ,  $\tau = 0$ ,  $\sigma = \underline{x}$ , w. z. b. w.

**Satz 17:** *Ein Endomorphismus eines Lie'schen  $k$ -Ringes  $L$  ist durch seine Wirkung auf die Elemente eines erzeugenden Systems  $K$  von  $L$  eindeutig bestimmt.*

**Beweis:** Wir haben zu zeigen, daß zwei Endomorphismen  $\sigma$  und  $\tau$  von  $L$ , für die  $\sigma x = \tau x$  für alle  $x$  aus  $K$  gilt, einander gleich sind.

Setzen wir  $\varrho = \sigma - \tau$ , so ist  $\varrho K = 0$  und zu zeigen ist, daß  $\varrho = 0$ .  $L$  ist der aus allen Komplexen  $K^{[r]}$  erzeugte  $k$ -Modul. Zu zeigen ist, daß  $\varrho K^{[r]} = 0$  für alle  $r$ . Es ist  $\varrho K = \varrho K^{[1]}$ . Es sei schon bewiesen, daß  $\varrho K^{[r-1]} = 0$ , und es sei  $r > 1$ . Dann folgt

$$\varrho K^{[r]} = \varrho(K \circ K^{[r-1]}) \subseteq K \circ \varrho K^{[r-1]} + \varrho K \circ K^{[r-1]} = 0.$$

**Definition:** Ein Endomorphismus heißt *zentraler Endomorphismus*, wenn er jedes Element auf ein Zentrumselement abbildet.

**Satz 18:** *Alle zentralen Endomorphismen des Lie'schen  $k$ -Ringes  $L$  bilden zusammen den Zentralisator von  $I(L)$  in  $E(L)$ , also ein Ideal von  $E(L)$ .*

Beweis: 1. Wenn  $\sigma$  ein zentraler Endomorphismus von  $L$  ist,  $x$  ein festes Element aus  $L$ ,  $a$  beliebig aus  $L$ , so ergibt die Gleichung

$$(9) \quad \begin{aligned} (\sigma \circ \underline{x}) a &= (\underline{\sigma x}) a = (\sigma x) \circ a \subseteq \mathfrak{z}(L) \circ L = 0. \\ \sigma \circ \underline{x} &= 0, \quad \sigma \in Z(I(L)). \end{aligned}$$

2. Wenn umgekehrt für den Endomorphismus  $\sigma$  gilt:  $\sigma \circ I(L) = 0$ , so ist für jedes  $x$  aus  $L$ :  $\sigma \circ \underline{x} = \underline{\sigma x} = 0$ , d. h.  $\sigma x \in \mathfrak{z}(L)$ , w. z. b. w. Wir bezeichnen den Lie'schen  $k$ -Ring der zentralen Endomorphismen mit  $ZI(L)$ .

**Hilfssatz 6:** *Es sei  $k$  ein Körper,  $L$  sei ein Lie'scher  $k$ -Ring, die Dimension der  $k$ -Moduln  $L/D(L)$  bzw.  $\mathfrak{z}(L)$  sei gleich  $m$  bzw.  $n$ , dann ist die Dimension von  $ZI(L)$  gleich  $m \cdot n$ .*

Wenn nämlich  $\sigma$  ein zentraler Endomorphismus von  $L$  ist, so ist

$$(9a) \quad \sigma(D(L)) = \sigma(L \circ L) \subseteq L \circ \sigma L + \sigma L \circ L = 0,$$

also induziert  $\sigma$  einen Homomorphismus  $\bar{\sigma}$  zwischen  $L/D(L)$  und  $\mathfrak{z}$ ; wenn umgekehrt  $\bar{\sigma}$  ein  $k$ -Homomorphismus zwischen  $L/D(L)$  und  $\mathfrak{z}$ , so setze man  $\sigma a = \bar{\sigma}(a + D(L))$  und erhält einen zentralen Endomorphismus  $\sigma$  von  $L$ , der gerade den Homomorphismus  $\bar{\sigma}$  zwischen  $L/D(L)$  und  $\mathfrak{z}$  induziert. Der  $k$ -Modul  $ZI(L)$  ist isomorph zu dem  $k$ -Modul aller  $k$ -Homomorphismen von  $L/D(L)$  in  $\mathfrak{z}(L)$ , also isomorph zu dem  $k$ -Modul aller rechteckigen Matrizen mit  $n$  Zeilen und  $m$  Spalten, woraus die Behauptung folgt.

Wenn der Lie'sche  $k$ -Ring  $L$  die Ringsumme der Lie'schen  $k$ -Ringe  $L_1, L_2, \dots, L_r$  ist, so besitzt jedes Element  $x$  aus  $L$  die eindeutige Zerlegung

$$(9a) \quad x = H_1 x + H_2 x + \dots + H_r x \quad (H_i x \in L_i).$$

Entsprechend zerlegen wir jeden Endomorphismus  $\sigma$  in

$$(10) \quad \sigma = \sigma_1 + \sigma_2 \dots + \sigma_r,$$

wobei  $\sigma_i x = H_i \sigma x$  gesetzt ist. Es ist klar, daß  $\sigma_i$  eine lineare Transformation des  $k$ -Moduls  $L$  ist.  $\sigma_i$  ist aber sogar ein Endomorphismus von  $L$ . Denn es ist

$$\begin{aligned} \sigma_i(x \circ y) &= H_i \sigma(x \circ y) = H_i(x \circ \sigma y) + H_i(\sigma x \circ y) \\ &= x \circ (H_i \sigma y) + (H_i \sigma x) \circ y = x \circ \sigma_i y + \sigma_i x \circ y. \end{aligned}$$

Die Ringsumme  $L = L_1 + L_2 + \dots + L_r$  heißt *charakteristisch invariante Zerlegung*, wenn jeder Summand charakteristisches Ideal von  $L$  ist.

**Satz 19:** Sei  $k$  ein Körper und  $L$  ein Lie'scher  $k$ -Ring. Die Ringsumme  $L = L_1 + L_2 + \dots + L_r$  ist dann und nur dann charakteristisch invariant, wenn aus  $\mathfrak{z}(L_i) \neq 0$  folgt:  $D(L_k) = L_k$  ( $k \neq i$ ;  $i, k = 1, 2, \dots, r$ ).

Beweis: 1. Es sei  $\mathfrak{z}(L_i) \neq 0$  und  $D(L_k) \neq 0$  und  $i \neq k$ . Da  $k$  ein Körper, so besitzt der (eigentliche)  $k$ -Modul  $L_i / D(L_i)$  eine  $k$ -Basis. Also gibt es ein Ideal  $A$  von  $L_i$  und ein Element  $v$  aus  $L_i$ , das außerhalb von  $A$  liegt, so daß  $L_i$  die direkte Modulsumme von  $A$  und  $k.v.$  Ferner gibt es im Zentrum von  $L$  ein von 0 verschiedenes Element  $v'$ . Jedes Element  $x$  aus  $L$  hat eindeutig die Form (9a) und die Kongruenz  $H_i x \equiv \xi v(A)$  ist eindeutig lösbar. Durch die Festsetzung  $\sigma x = \xi v'$  wird ein Endomorphismus von  $L$  definiert, wie leicht zu sehen; da dieser Endomorphismus  $L_i$  nicht in sich abbildet, so ist die gegebene Zerlegung von  $L$  nicht charakteristisch invariant.

2. Es sei  $\sigma$  ein Endomorphismus von  $L$ , der den Summand  $L_i$  nicht in sich abbildet. Für  $\sigma$  gilt die Zerlegung (10). Da  $\sigma L_i$  nicht in  $L_i$  enthalten ist, so gibt es einen Index  $k$ , für den ebenfalls  $\sigma_k L_i$  nicht in  $L_i$  enthalten ist. Also ist  $k \neq i$ ,  $\sigma_k L_i \neq 0$ . Für alle  $a$  aus  $L_i$ ,  $b$  aus  $L_k$  folgt:

$$\sigma_k(a \circ b) = \sigma_k(0) = 0 = (\sigma_k a) \circ b + a \circ (\sigma_k b) = (\sigma_k a) \circ b + 0,$$

dennach liegt  $\sigma_k L_i$  im Zentrum von  $L_k$ . Da  $\sigma_k L_i \neq 0$ , so ist  $\mathfrak{z}(L_k) \neq 0$ . Nun ist für alle  $a, a'$  aus  $L$ :

$$(11) \quad \sigma_k(a \circ a') = a \circ \sigma_k a' + \sigma_k a \circ a',$$

also  $\sigma_k D(L_i) = 0$ . Da  $\sigma_k(L_i) \neq 0$ , so ist  $D(L_i) \neq L_i$ . Damit ist alles bewiesen.

Die inneren Endomorphismen eines  $k$ -Schiefringes  $\mathfrak{S}$  genügen der Funktionalgleichung:

$$(12) \quad \tau(xy) = x \cdot \tau y + \tau x \cdot y,$$

denn für jedes Element  $t$  aus  $\mathfrak{S}$  ist ja:

$$\begin{aligned} t \circ xy &= txy - xyt = (tx - xt)y + x'(ty - yt) \\ &= (t \circ x) \cdot y + x \cdot (t \circ y). \end{aligned}$$

Alle linearen Transformationen von  $\mathfrak{S}$ , die der Funktionalgleichung (12) genügen, bilden einen in  $E(S)$  enthaltenen Lie'schen  $k$ -Ring  $E_0(S)$ .

Beweis: Aus (12) folgt  $\tau(x \circ y) = x \circ \tau y + \tau x \circ y$ , also liegt  $E_0(S)$  in  $E(S)$ . Wenn ferner  $\tau$  und  $\tau'$  zwei lineare Transformationen aus  $E(S)$  sind, so ist  $\lambda\tau$  und  $\tau + \tau'$  auch in  $E_0(S)$  enthalten. Ferner ist:

$$\begin{aligned}
(\tau \circ \tau') xy &= \tau(\tau'(xy)) - \tau'(\tau(xy)) \\
&= \tau(x \cdot \tau'y + \tau'x \cdot y) - \tau'(x \cdot \tau y + \tau x \cdot y) \\
&= \tau(x \cdot \tau'y) + \tau(\tau'x \cdot y) - \tau'(x \cdot \tau y) - \tau'(\tau x \cdot y) \\
&= x \cdot \tau\tau'y + \tau\tau'x \cdot y - x \cdot \tau'\tau y - \tau'\tau x \cdot y \\
&\quad + \tau x \cdot \tau'y + \tau'x \cdot \tau y - \tau'x \cdot \tau y - \tau x \cdot \tau'y \\
&= x(\tau\tau'y - \tau'\tau y) + (\tau\tau'x - \tau'\tau x)y \\
&= x \cdot (\tau \circ \tau')y + (\tau \circ \tau')x \cdot y,
\end{aligned}$$

also ist auch  $\tau \circ \tau'$  in  $E_0(S)$  enthalten.

Aus Formel (26 a, b) des § 1, 8 folgt für alle  $\sigma$  aus  $E_0(\mathfrak{S})$ :

$$\sigma^n(xy) = \sum_{i=0}^n \binom{n}{i} \sigma^i x \cdot \sigma^{n-i} y, \quad (x, y \in \mathfrak{S}).$$

Falls  $\mathfrak{S}$  Primzahlcharakteristik  $p$  hat, so folgt:

$$\sigma^{p^\nu}(xy) = x \cdot \sigma^{p^\nu} y + \sigma^{p^\nu} x \cdot y \quad (\nu = 0, 1, 2, \dots).$$

(13) Wenn die Charakteristik des  $k$ -Schiefringes  $\mathfrak{S}$  eine Primzahl  $p$  ist, dann führt das Potenzieren mit  $p$  nicht aus  $E_0(\mathfrak{S})$  hinaus.

Insbesondere ist:

$$x^{p^\nu} \circ y = \underbrace{x \circ (x_0 \cdots (x \circ y) \cdots)}_{p^\nu\text{-mal}} \quad (\nu = 0, 1, 2, \dots).$$

Für Darstellungen  $a \rightarrow \bar{a}$  eines Lie'schen  $k$ -Ringes der Charakteristik  $p$  in assoziativen Ringen schließen wir:

$$(14) \quad \bar{a}^{p^\nu} \circ \bar{b} = \underbrace{\bar{a} \circ (\bar{a} \circ \cdots (\bar{a} \circ \bar{b}) \cdots)}_{p^\nu\text{-mal}}.$$

**Hilfssatz 7:** Wenn  $\Sigma$  eine Menge von Endomorphismen aus  $E_0(\mathfrak{S})$  ist und für einen Komplex  $\mathfrak{K}$  aus  $\mathfrak{S}$  gilt:  $\sum \mathfrak{K} \subseteq \{\mathfrak{K}\}$ , dann ist der aus  $\mathfrak{K}$  erzeugte  $k$ -Schiefring  $\{\mathfrak{K}\}$  unter  $\Sigma$  invariant.

Beweis:  $\{\mathfrak{K}\}$  ist der aus allen Komplexen  $\mathfrak{K}^r$  erzeugte  $k$ -Modul. Wir müssen zeigen, daß  $\sum \mathfrak{K}^r \subseteq \{\mathfrak{K}\}$  für beliebige  $r$ . Wir wissen, daß  $\sum \mathfrak{K} \subseteq \{\mathfrak{K}\}$ . Es sei  $r > 1$  und schon bewiesen, daß  $\sum \mathfrak{K}^{r-1} \subseteq \{\mathfrak{K}\}$ . Da  $\Sigma \subseteq E_0(\mathfrak{S})$ , so folgt:

$$\begin{aligned}
\sum \mathfrak{K}^r &= \sum (\mathfrak{K} \cdot \mathfrak{K}^{r-1}) \subseteq \mathfrak{K} \cdot \sum \mathfrak{K}^{r-1} + \sum \mathfrak{K} \cdot \mathfrak{K}^{r-1} \\
&\subseteq \mathfrak{K} \cdot \{\mathfrak{K}\} + \{\mathfrak{K}\} \cdot \mathfrak{K}^{r-1} \subseteq \{\mathfrak{K}\},
\end{aligned}$$

also gilt  $\sum \mathfrak{K}^r \subseteq \{\mathfrak{K}\}$  für beliebige  $r$ , w. z. b. w.



Zur Bestimmung der äußeren Endomorphismen eines endlichen Lie'schen Ringes  $L$  über algebraisch abgeschlossenem Grundkörper wenden wir das folgende Verfahren an.

Es sei  $L = H + L_\alpha + L_\beta + \dots$  die in § 2, 4 definierte Zerlegung in Eigenmoduln des (passend gewählten) nilpotenten Teilringes  $H$ . Wir definieren bei gegebenem Endomorphismus  $\sigma$  eine neue Lie'sche Algebra  $\bar{L} = L + k \cdot s$ , indem wir setzen

$$\begin{aligned}(x + \lambda s) + (x' + \lambda' s) &= (x + x') + (\lambda + \lambda') s, \\ \lambda' (x + \lambda s) &= \lambda x + \lambda' \lambda s, \\ (x + \lambda s) \circ (x' + \lambda' s) &= x \circ x' + \lambda' \sigma x - \lambda \sigma x'.\end{aligned}$$

Wir überzeugen uns leicht davon, daß  $\bar{L}$  eine Lie'sche Algebra ist, die  $L$  als Ideal enthält und in der die Kreismultiplikation von rechts her mit  $s$  gerade den Endomorphismus  $\sigma$  induziert. Nun zerfällt  $\bar{L}$  unter  $H$  in die Eigenmoduln  $\bar{L} = \bar{L}_0 + \bar{L}_\alpha + \bar{L}_\beta + \dots$ , so daß für alle Eigenwertverteilungen  $\gamma \neq 0$ :  $H \circ \bar{L}_\gamma = \bar{L}_\gamma$ . Da  $H$  im Ideal  $L$  enthalten ist, so ist auch  $H \circ \bar{L}_\gamma$  in  $L$  enthalten, also auch  $\bar{L}_\gamma$  in  $L$ . Demnach:  $\bar{L}_\alpha = L_\alpha$ ,  $\bar{L}_\beta = L_\beta$ ,  $\dots$ . Daher muß es in  $\bar{L}_0$  ein nicht in  $L$  enthaltene Element  $s'$  geben. Indem wir  $s'$  noch durch ein geeignetes skalares Vielfaches ersetzen, erreichen wir, daß  $s' \equiv s (L)$ . Da  $\bar{L}_0 \circ L_\varphi \subseteq L_\varphi$ , so finden wir:

*Jeder Endomorphismus einer Lie'schen Algebra kann so um einen inneren Endomorphismus (additiv) abgeändert werden, daß der abgeänderte Endomorphismus jeden Eigenmodul der Zerlegung des § 2, 4 in sich überführt.*

Alle Endomorphismen  $\sigma$  von  $L$  mit der Eigenschaft  $\sigma H \subseteq H$  bilden den Normalisator  $N(\underline{H})$  von  $\underline{H}$  in  $E(L)$ . Es gilt:

$$\sigma L_\varphi \subseteq L_\varphi, \quad N(\underline{H}) \cap I(L) = \underline{H}.$$

Aus dem eben Gezeigten folgt, daß

$$E(L) = N(\underline{H}) \dot{+} I(L),$$

also nach dem Isomorphiesatz:

$$E(L)/I(L) \cong N(\underline{H})/\underline{H}.$$

Die Zerlegung von  $E(L)$  in Eigenmoduln von  $\underline{H}$  lautet:

$$E(L) = N(\underline{H}) + \underline{L}_\alpha + \underline{L}_\beta + \dots$$

**Hilfssatz 8:** *Wenn  $L$  als Ideal enthalten ist in dem Lie'schen  $k$ -Ring  $L_1$ , wenn ferner der Zentralisator von  $L$  in  $L_1$  gleich Null ist und*

wenn der Normalisator  $N(H)$  von  $H$  in  $L_1$  dieselbe Dimension wie  $N(\underline{H})$  hat, dann ist  $L_1$  isomorph zu  $E(L)$ .

Beweis: Durch die Zuordnung  $x \rightarrow \underline{x} = \begin{pmatrix} a \\ x \circ a \end{pmatrix}$  ( $a$  beliebig aus  $L$ ) wird  $L_1$  isomorph auf einen  $k$ -Teilring  $\underline{L}_1$  von  $E(L)$  abgebildet. Dabei wird  $L$  auf  $I(L)$  abgebildet. Der Normalisator  $N(H)$  von  $H$  in  $L$  wird dabei isomorph auf einen  $k$ -Teilring des Normalisators  $N(\underline{H})$  von  $\underline{H}$  in  $E(L)$  abgebildet. Da  $N(H)$  die gleiche Dimension wie  $N(\underline{H})$  hat, so ist  $\underline{N(H)} = N(\underline{H})$ , also

$$E(L) = N(\underline{H}) + I(L) \subseteq \underline{L}_1, \quad \underline{L}_1 = E(L), \quad L_1 \cong E(L),$$

w. z. b. w.

*Bemerkung:* Wenn das Zentrum von  $L$  gleich Null ist und wenn  $h \circ x = \gamma_h x$  für alle  $h$  aus  $H$ ,  $x$  aus  $L_\gamma$  und alle  $\gamma$ , dann ist  $\sigma H = 0$  für alle  $\sigma$  aus  $N(H)$ , denn es ist

$$\begin{aligned} \sigma h \circ x &= \sigma(h \circ x) - h \circ \sigma x = \gamma_h \sigma x - \gamma_h \sigma x = 0, \\ \sigma H &\subseteq \mathfrak{z}(L) = 0. \end{aligned}$$

Wir setzen  $L = PSM_n$ . Wie früher setzen wir

$$\begin{aligned} H &= \{d_2, d_3, \dots, d_n\}, \quad \text{wenn } n \not\equiv 0 \pmod{\chi(k)}, \\ H &= \{d_2, d_3, \dots, d_{n-1}\}, \quad \text{,, } n \equiv 0 \pmod{\chi(k)}. \end{aligned}$$

Ferner sei  $n > 1$  und wenn  $\chi(k) = 2$ , so sei  $n > 2$ . Dann sind alle Voraussetzungen erfüllt. Um die äußeren Endomorphismen von  $PSM_n$  zu erhalten, müssen wir die Endomorphismen  $\sigma$  von  $PSM_n$  betrachten, für die  $\sigma H \subseteq H$ . Aus der letzten Bemerkung folgt  $\sigma H = 0$ .

1.  $\chi(k) \neq 2$ . Dann sind die von  $H$  verschiedenen Eigenmoduln:  $\{e_{ik}\}$ , ( $i \neq k$ ), also ist  $\sigma e_{ik} \in \{e_{ik}\}$ .
2.  $\chi(k) = 2$ . Dann sind die von  $H$  verschiedenen Eigenmoduln  $\{e_{ik}, e_{ki}\}$ , ( $i \neq k$ ), und es ist  $\sigma e_{ik} \in \{e_{ik}, e_{ki}\}$ .

Da wir  $n > 2$  vorausgesetzt haben, so gibt es zu jedem Paare zweier verschiedener Indizes  $i, k$  noch einen dritten von  $i$  und  $k$  verschiedenen Index  $j$ , so daß:

$$\begin{aligned} \sigma e_{ik} &= \sigma(e_{ij} \circ e_{jk}) \\ &= e_{ij} \circ \sigma e_{jk} + \sigma e_{ij} \circ e_{jk} \subseteq e_{ij} \circ \{e_{jk}, e_{kj}\} + \{e_{ij}, e_{ji}\} \circ e_{jk} \subseteq \{e_{ik}\}, \end{aligned}$$

also ist in jedem Falle  $\sigma e_{ik} = \lambda_{ik} e_{ik}$ .

Da  $0 \neq e_{ik} \circ e_{ki} \in H$ , so ist

$$\begin{aligned} 0 &= \sigma(e_{ik} \circ e_{ki}) = e_{ik} \circ \sigma e_{ki} + \sigma e_{ik} \circ e_{ki} = (\lambda_{ik} + \lambda_{ki}) e_{ik} \circ e_{ki}, \\ \lambda_{ik} + \lambda_{ki} &= 0. \end{aligned}$$

Durch die Zuordnung  $\sigma \rightarrow \xi_\sigma = \{\lambda_{12}, \lambda_{23}, \dots, \lambda_{n-1n}\}$  wird der  $k$ -Modul  $N(H)$  homomorph auf einen  $k$ -Modul  $\mathfrak{M}$  abgebildet, dessen Dimension höchstens  $n - 1$  ist. Wenn  $\xi_\sigma = 0$ , so folgt:

$$\sigma e_{i+1} = \sigma e_{i+1} = 0 \quad (i = 1, 2, \dots, n-1)$$

und da nach Satz 12 die Elemente  $e_{i+1}$  und  $e_{i+1}i$  den ganzen Lie'schen  $k$ -Ring  $\mathfrak{M}$  erzeugen, so folgt nach Satz 17, daß  $\sigma = 0$ . Also ist  $N(H)$  zu  $\mathfrak{M}$  isomorph und  $N(\overline{H})$  höchstens  $(n-1)$ -dimensional. Denken wir uns  $PSM_n$  in  $PM_n$  eingebettet, so liegt  $\{e_{11}, e_{22}, \dots, e_{n-1n-1}\}$  im Normalisator von  $H$  in  $PM_n$ . Aus Hilfssatz 8 folgt, daß

$$E(PSM_n) \cong PM_n.$$

Da nach Satz 13  $PSM_n$  einfach und nichtabelsch ist, so ist nach Satz 15  $PM_n$  abgeschlossen.

$SM_n$  enthält  $\mathfrak{z}(SM_n)$  als charakteristisches Ideal, und es ist  $PSM_n \cong SM_n / \mathfrak{z}(SM_n)$ . Nach dem eben gefundenen Ergebnis gibt es zu jedem Endomorphismus  $\sigma$  von  $SM_n$  stets ein Element  $s$  aus  $M_n$ , so daß

$$\sigma a \equiv s \circ a \pmod{\mathfrak{z}(SM_n)} \text{ für alle } a \text{ aus } SM_n.$$

Setzen wir  $\sigma_0 = \sigma - s$ , so folgt:  $\sigma_0 M_n \equiv 0 \pmod{\mathfrak{z}(SM_n)}$ . Aus § 3 (4 e) und § 4 (9a) folgt  $\sigma_0(SM_n) = 0$ , also  $\sigma = \underline{s}$ . Demnach:

$$E(SM_n) \cong PM_n.$$

$SM_n$  ist als Ableitung von  $M_n$  ein charakteristisches Ideal von  $M_n$ . Nach dem eben Gezeigten gibt es zu jedem Endomorphismus  $\tau$  von  $M$  ein Element  $t$  aus  $M$ , so daß  $\tau a = t \circ a$  für alle  $a$  aus  $SM_n$ . Setzen wir  $\tau_0 = \tau - \underline{t}$ , so folgt  $\tau_0 SM_n = 0$ . Für alle  $x$  aus  $M_n$ ,  $a$  aus  $SM_n$  folgt:

$$\begin{aligned} \tau_0(x \circ a) &= 0 \\ &= x \circ \tau_0 a + \tau_0 x \circ a \\ &= 0 + \tau_0 x \circ a, \\ \tau_0 M_n \circ SM_n &= 0, \end{aligned}$$

also

$$(15) \quad \begin{aligned} \tau_0 M_n &\subseteq \mathfrak{z}(M_n), & \tau_0 &\in ZI(M_n), \\ E(M_n) &= I(M_n) + ZI(M_n). \end{aligned}$$

Da das Zentrum von  $I(M_n)$  gleich Null ist, so folgt:  $I(M_n) \cap ZI(M_n) = 0$ . Also ist die Modulsumme (15) direkt. Nach Hilfssatz 6 folgt, daß  $ZI(M_n)$  die Dimension 1 hat.

Wir bestimmen jetzt für beliebige Grade  $n$  und Charakteristiken  $\chi$  den Lie'schen  $k$ -Ring  $E_0(M_n)$ , bestehend aus allen linearen Transformationen  $\tau$  von  $M_n$ , die der Funktionalgleichung  $\tau(xy) = x \cdot \tau y + \tau x \cdot y$  genügen. Jedenfalls ist  $I(M_n)$  in  $E_0(M_n)$  enthalten. Kann  $\tau$  ein zentraler Endomorphismus sein? Wenn  $\tau$  in  $E_0(M_n) \cap ZI(M_n)$  liegt, so ist

$$\begin{aligned} \tau e_{11} = \tau(e_{11}^2) &= e_{11} \cdot \tau e_{11} + \tau e_{11} \cdot e_{11} = 2 e_{11} \tau e_{11}, & e_{11} \tau e_{11} &= 2 e_{11} \tau e_{11}, \\ e_{11} \tau e_{11} &= 0, & \tau e_{11} &= 2 e_{11} \tau e_{11} = 0, \end{aligned}$$

ferner ist  $\tau(DM_n) = 0$ , also

$$\tau M_n = \tau(DM_n + k e_{11}) = 0, \quad \tau = 0.$$

Demnach ist  $E_0(M_n)$  echter Teilmodul von  $E(M_n)$ , der  $I(M_n)$  enthält. Da die Dimension von  $E(M_n)$ , einen Fall ausgenommen, um 1 größer als die von  $I(M_n)$  ist, so folgt  $E_0(M_n) = I(M_n)$ .

Das bleibt richtig, wenn  $\chi = 2$ ,  $n = 2$ . Man setze nämlich  $H = \{e_{11}, e_{22}\}$ ,  $L_{12} = \{e_{12}, e_{21}\}$ . Für jeden Endomorphismus  $\tau$  aus  $E(M)$  gibt es ein Element  $t$  aus  $M_2$ , so daß  $(\tau - t) \circ H \subseteq H$ . Setzen wir  $\tau' = \tau - t$ , so folgt wie eben, daß  $\tau' e_{11} = \tau' e_{22} = 0$ , also  $\tau' H = 0$ . Ferner gilt

$$\begin{aligned} \tau' \{e_{12}, e_{21}\} &\subseteq \{e_{12}, e_{21}\}, & \tau' e_{12} &= \alpha e_{12} + \beta e_{21}, \\ 0 = \tau' e_{12}^2 &= e_{12} \tau' e_{12} + \tau' e_{12} \cdot e_{12} = \beta e_{11} + \beta e_{22}, & \beta &= 0; \\ & & \tau' e_{12} &= \alpha e_{12}, \end{aligned}$$

ebenso  $\tau' e_{21} = \gamma e_{21}$ . Nun ist

$$0 = \tau' e_{11} = \tau' (e_{12} \cdot e_{21}) = e_{12} \cdot \tau' e_{21} + \tau' e_{12} \cdot e_{21} = (\alpha + \gamma) e_{11}, \quad \alpha = \gamma;$$

also

$$\tau' = \alpha e_{11}, \quad \tau = \underline{t} + \alpha e_{11}.$$

Mithin ist  $E_0(M_n) = I(M_n)$  in allen Fällen.

Als Resultat haben wir

**Satz 20:**  $k$  sei ein Körper mit der Charakteristik  $\chi$ .  $M_n$  sei der Matrizenring  $n$ -ten Grades über  $k$ . Wenn  $n > 1$ ,  $\chi \neq 2$  oder  $n > 2$ ,  $\chi \neq 2$ , so ist der Endomorphismenring von  $PSM_n$  bzw.  $SM_n$  isomorph zu  $PM_n$ . Der Lie'sche  $k$ -Ring  $PM_n$  ist abgeschlossen. Der Endomorphismenring von  $M_n$  ist Ringsumme des Ringes der inneren Endomorphismen und des eindimensionalen Ringes der zentralen Endomorphismen. Für beliebige Grade und beliebige Charakteristik ist jede lineare Transformation des  $k$ -Moduls  $M_n$ , die der Funktionalgleichung  $\tau(xy) = x \cdot \tau y + \tau x \cdot y$  genügt, ein innerer Endomorphismus.

## II. Darstellungstheorie nilpotenter Lie'scher Ringe.

### § 1. $(L, \sigma)$ -Moduln.

Es sei  $k$  ein Körper,  $L$  ein Lie'scher  $k$ -Ring und  $\sigma$  ein Endomorphismus von  $L$ . Ein  $L$ -Modul  $\mathfrak{M}$  heie  $(L, \sigma)$ -Modul, wenn es eine lineare Transformation  $s$  von  $\mathfrak{M}$  gibt, so da

$$(\sigma x)u = (xs - sx)u$$

fr alle  $x$  aus  $L$ ,  $u$  aus  $\mathfrak{M}$ . Der  $(L, \sigma)$ -Modul  $\mathfrak{M}$  heie *irreduzibel*, wenn  $\mathfrak{M}$  keinen von 0 und  $\mathfrak{M}$  verschiedenen, unter  $L$  und  $s$  invarianten  $k$ -Modul enthlt.

Gesucht sind alle irreduziblen  $(L, \sigma)$ -Moduln.

1. Zunchst setzen wir nur voraus, da  $\mathfrak{M}$  ein  $(L, \sigma)$ -Modul ist. Wir bentigen im folgenden den

**Hilfssatz 1:** *Wenn  $\mathfrak{M}_1$  ein in  $\mathfrak{M}$  enthaltener  $L$ -Modul ist, dann ist auch  $\mathfrak{M}_1 + s\mathfrak{M}_1$  ein  $L$ -Modul.*

**Beweis:** Fr alle  $x$  aus  $L$ ,  $u$  aus  $\mathfrak{M}_1$  ist

$$xsu = (xs - sx)u + sxu = (\sigma x)u + s(xu),$$

also  $x s \mathfrak{M}_1 \subseteq \mathfrak{M}_1 + s \mathfrak{M}_1$ , ferner nach Annahme  $x \mathfrak{M}_1 \subseteq \mathfrak{M}_1$ , daher

$$x(\mathfrak{M}_1 + s \mathfrak{M}_1) \subseteq \mathfrak{M}_1 + s \mathfrak{M}_1,$$

w. z. b. w.

2. Jetzt setzen wir noch voraus, da  $\mathfrak{M}$  als  $L$ -Modul betrachtet halbreduzibel ist. Dann enthlt  $\mathfrak{M}$  einen irreduziblen  $L$ -Modul  $m$ . Wir setzen

$$m_0 = 0, \quad m_1 = m, \quad m_2 = m + s m, \quad \dots, \quad m_{i+1} = m_i + s m_i, \quad \dots$$

Aus dem eben bewiesenen Hilfssatz folgt durch Induktion nach  $i$ , da jedes  $m_i$  ein  $L$ -Modul ist. Die  $m_i$  bilden eine aufsteigende Kette von in  $\mathfrak{M}$  enthaltenen  $L$ -Moduln. Da  $\mathfrak{M}$  als  $L$ -Modul betrachtet halbreduzibel ist, so gibt es einen eindeutig bestimmten Index  $m$ , so da

$$0 = m_0 \subset m_1 \subset m_2 \cdots \subset m_m = m_{m+1}.$$

$m_m$  ist ein Null verschiedener  $(L, \sigma)$ -Modul.

3. Nun sei  $\mathfrak{M}$  berdies ein irreduzibler  $(L, \sigma)$ -Modul. Dann ist  $m_m = \mathfrak{M}$ . Aus der Definition von  $m_i$  folgt:

$$m_i = m + s m + \dots + s^{i-1} m \quad (i = 1, 2, \dots, m).$$

Durch die Festsetzung

$$\bar{x}u = xu$$

für alle  $u$  aus  $\mathfrak{M}$  wird eine Darstellung  $x \rightarrow \bar{x}$  von  $L$  in linearen Transformationen von  $\mathfrak{M}$  definiert. Der zugehörige Darstellungsrings werde mit  $\bar{L}$  bezeichnet.

Nach § 2, 2, (29)<sup>1)</sup> ist:

$$(1) \quad \bar{a} s^i = \sum_{\nu=0}^i \binom{i}{\nu} s^\nu \overline{\sigma^{i-\nu} a},$$

insbesondere

$$a s^i v \equiv s^i a v (m_i)$$

für alle  $v$  aus  $\mathfrak{m}$ ,  $a$  aus  $L$  ( $i = 0, 1, 2, \dots, m-1$ ).

Demnach vermittelt die Zuordnung

$$(2) \quad v \rightarrow s^i v + m_i$$

einen  $L$ -Homomorphismus von  $\mathfrak{m}$  auf  $m_{i+1}/m_i$ . Wenn nun  $i < m$ , so ist  $m_{i+1}/m_i \neq 0$ , und da  $\mathfrak{m}$  ein irreduzibler  $L$ -Modul ist, so ist die Zuordnung (2) ein  $L$ -Isomorphismus. Wenn die Gleichung

$$v_0 + s v_1 + s^2 v_2 + \dots + s^{m-1} v_{m-1} = 0 \quad (v_i \in \mathfrak{m})$$

besteht, so folgt sukzessiv:

$$v_{m-1} = 0, v_{m-2} = 0, \dots, v_0 = 0.$$

Als Ergebnis haben wir

**Satz 1:** *Der  $L$ -Modul  $\mathfrak{M}$  besitzt  $m$  Kompositionsfaktoren. Sie sind zu  $\mathfrak{m}$   $L$ -isomorph. Jedes Element aus  $\mathfrak{M}$  läßt sich eindeutig in der Form*

$$(3) \quad u = v_0 + s v_1 + \dots + s^{m-1} v_{m-1} \quad (v_i \in \mathfrak{m})$$

*darstellen.*

4. Unter  $u, u', \dots$  mögen Elemente aus  $\mathfrak{M}$ , unter  $v, v_1, v_2, \dots$  mögen Elemente aus  $\mathfrak{m}$  verstanden werden. Nach (1) ist

$$(4) \quad a s^i v = \sum_{\nu=0}^i \binom{i}{\nu} s^\nu (\sigma^{i-\nu} a) v \quad (i = 0, 1, 2, \dots, m-1).$$

Ferner gilt:

$$(5) \quad \begin{aligned} s(s^i v) &= s^{i+1} v \quad (i = 0, 1, 2, \dots, m-2) \\ s(s^{m-1} v) &= s^m v = \sum_0^{m-1} s^i s_i v, \end{aligned}$$

<sup>1)</sup> Man setze  $\alpha = \beta = 0$  und vertausche in jedem Produkt aus zwei Faktoren die Reihenfolge der Faktoren.

wobei die  $s_i$  gewisse lineare Transformationen des  $k$ -Moduls  $m$  sein müssen. Sie genügen Gleichungen, die sich aus den Darstellungsbedingungen (5a)  $(\sigma a) s^{m-1} v = (a s - s a) s^{m-1} v$  ergeben. Wir erhalten:

$$\begin{aligned}
 (\sigma a) s^{m-1} v &= \sum_0^{m-1} \binom{m-1}{\nu} s^\nu (\sigma^{m-\nu} a) v, \\
 a s^m v - s a s^{m-1} v &= \sum_{i=0}^{m-1} \sum_{\nu=0}^i \binom{i}{\nu} s^\nu (\sigma^{i-\nu} a) s_i v \\
 &\quad - \sum_{\nu=0}^{m-1} \binom{m-1}{\nu} s^{\nu+1} (\sigma^{m-1-\nu} a) v.
 \end{aligned}$$

Aus der Eindeutigkeit der Darstellung (3) folgt:

$$\begin{aligned}
 (6) \quad \binom{m}{\nu} (\sigma^{m-\nu} a) v &= (a s_\nu - s_\nu a) v + \sum_{i=\nu+1}^{m-1} \binom{i}{\nu} (\sigma^{i-\nu} a) s_i v \\
 &\quad (\nu = 0, 1, 2, \dots, m-1; a \in L).
 \end{aligned}$$

Umgekehrt folgen aus den Gleichungen (6) die Gleichungen (5a). Durch die Festsetzung

$$x^* v = x v$$

für alle  $v$  aus  $m$  wird eine Darstellung  $x \rightarrow x^*$  von  $L$  in linearen Transformationen von  $m$  definiert. Der zugehörige Darstellungsrings werde mit  $L^*$  bezeichnet.

Aus (4) folgt, daß die lineare Transformation  $\bar{a}$  von  $\mathfrak{M}$  eindeutig durch die linearen Transformationen  $a^*, (\sigma a)^*, \dots, (\sigma^{m-1} a)^*$  von  $m$  und durch die Struktur von  $\mathfrak{M}$  bestimmt ist. Wir schreiben daher symbolisch:

$$(7) \quad \bar{a} = (a^*, (\sigma a)^*, \dots, (\sigma^{m-1} a)^*)$$

und nennen  $(\sigma^i a)^*$  die  $i$ -te Komponente von  $\bar{a}$ . In welcher Beziehung stehen nun die Komponenten dreier Elemente  $\bar{a}, \bar{b}, \bar{c}$  aus  $L$ , wenn  $a \circ b = c$ ? Nach § 4, (4) ist.

$$\sigma^i (a \circ b) = \sum_0^i \binom{i}{\nu} \sigma^\nu a \circ \sigma^{i-\nu} b.$$

Setzen wir jetzt

$$a_i = (\sigma^i a)^*, \quad b_i = (\sigma^i b)^*, \quad c_i = (\sigma^i c)^*,$$

so folgt:

$$\begin{aligned}
 (8) \quad \bar{a} \circ \bar{b} &= (a_0, a_1, \dots, a_{m-1}) \circ (b_0, b_1, \dots, b_{m-1}) = \bar{c} = (c_0, c_1, \dots, c_{m-1}), \\
 c_i &= \sum_{\nu=0}^i \binom{i}{\nu} a_\nu \circ b_{i-\nu}.
 \end{aligned}$$

Die Gleichungen (6) lauten umgerechnet auf Komponentendarstellung von  $\bar{a}$ :

$$(9) \quad \binom{m}{\nu} a_{m-\nu} = a_0 \circ s_\nu + \sum_{i=\nu+1}^{m-1} \binom{i}{\nu} a_{i-\nu} s_i$$

$$(\nu = 0, 1, \dots, m-1; a \in L).$$

## § 2. Potenzringe von Lie'schen $k$ -Ringen.

Wir wollen zu jedem  $k$ -Schiefring  $\mathfrak{S}$  und für jede natürliche Zahl  $m$  den Potenzring  $\mathfrak{S}^{(m)}$  konstruieren nach der Vorschrift:  $\mathfrak{S}^{(m)}$  ist die Menge aller geordneten  $m$ -tupel von Elementen aus  $\mathfrak{S}$  mit den Rechenregeln:

$$(10) \quad (a_0, a_1, \dots, a_{m-1}) + (b_0, b_1, \dots, b_{m-1})$$

$$= (a_0 + b_0, a_1 + b_1, \dots, a_{m-1} + b_{m-1}),$$

$$(11) \quad \lambda (a_0, a_1, \dots, a_{m-1}) = (\lambda a_0, \lambda a_1, \dots, \lambda a_{m-1}),$$

$$(12) \quad (a_0, a_1, \dots, a_{m-1}) \cdot (b_0, b_1, \dots, b_{m-1}) = (c_0, c_1, \dots, c_{m-1}),$$

wobei

$$c_i = \sum_{\nu=0}^i \binom{i}{\nu} a_\nu \cdot b_{i-\nu} \quad (i = 0, 1, 2, \dots, m-1).$$

Es ist klar, daß  $\mathfrak{S}^{(m)}$  ein distributiver  $k$ -Ring ist. Jetzt wollen wir noch zeigen, daß die unter (12) erklärte Multiplikation assoziativ ist. Wir haben zu zeigen, daß  $(AB)C = A(BC)$  für alle Elemente  $A, B, C$  aus  $\mathfrak{S}^{(m)}$ . Da die Distributivgesetze gelten, so genügt es, den Nachweis in den Fällen, wo

$$A = (0 \dots 0, \overset{i}{a}, 0, \dots 0),$$

$$B = (0 \dots 0, \overset{k}{b}, 0, \dots 0),$$

$$C = (0 \dots 0, \overset{l}{c}, 0, \dots 0)$$

ist, zu führen, wenn also in  $A$  alle Komponenten außer der  $i$ -ten gleich Null sind, entsprechend für  $B$  und  $C$ .

Wenn  $i+k+l \geq m$ , so folgt

$$(AB)C = A(BC) = 0.$$

Wenn  $i+k+l = j < m$ , so folgt:

$$(AB)C = \left(0 \dots 0, \binom{i+k}{i} \binom{j}{i+k} (ab)c, 0 \dots 0\right),$$

$$A(BC) = \left(0 \dots 0, \binom{j}{k+l} \binom{k+l}{k} a(bc), 0 \dots 0\right).$$



Nun ist

$$\binom{i+k}{i} \binom{i+k+l}{i+k} = \frac{(i+k+l)!}{i! k! l!} = \binom{i+k+l}{k+l} \binom{k+l}{k},$$

$$(ab)c = a(bc), \quad \text{folglich}$$

$$(AB)C = A(BC).$$

Demnach ist der  $n$ -te Potenzring eines  $k$ -Schiefringes selbst ein  $k$ -Schiefring.  $\mathfrak{S}^{(1)}$  ist isomorph zu  $\mathfrak{S}$ .

Alle Elemente aus  $\mathfrak{S}^{(m)}$  von der Form:  $(0 \cdots 0, a, \dots)$  bilden einen  $k$ -Modul  $\theta_i \mathfrak{S}^{(m)}$ . Es ist

$$(13) \quad \theta_0 \mathfrak{S}^{(m)} = \mathfrak{S}^{(m)}.$$

Aus (12) folgt sofort:

$$(14) \quad \theta_i \mathfrak{S}^{(m)} \cdot \theta_k \mathfrak{S}^{(m)} \subseteq \theta_{i+k} \mathfrak{S}^{(m)},$$

wobei  $\theta_j \mathfrak{S}^{(m)} = 0$  gesetzt ist für alle  $j \geq m$ . Also ist  $\theta_i \mathfrak{S}^{(m)}$  ein zweiseitiges Ideal von  $\mathfrak{S}^{(m)}$

Der Restklassenring  $\mathfrak{S}^{(m)} / \theta_1 \mathfrak{S}^{(m)}$  ist isomorph zu  $\mathfrak{S}$ ,  $\theta_1 \mathfrak{S}^{(m)}$  ist ein nilpotentes zweiseitiges Ideal von  $\mathfrak{S}^{(m)}$ . Wenn  $\mathfrak{A}$  ein in  $\mathfrak{S}^{(m)}$  enthaltener  $k$ -Modul ist, so ist

$$\theta_i \mathfrak{A} = \mathfrak{A} \cap \theta_i \mathfrak{S}^{(m)}$$

ebenfalls ein  $k$ -Modul. Es gilt  $\theta_0 \mathfrak{A} = \mathfrak{A}$ . Wenn  $0 \leq i < m$ , so wird  $\theta_i \mathfrak{A}$  gebildet aus allen Elementen von  $\mathfrak{A}$ , welche die Form  $(0 \cdots 0, a, \dots)$  haben. Alle hier vorkommenden  $i$ -ten Komponenten  $a$  bilden zusammen einen in  $\mathfrak{S}$  enthaltenen  $k$ -Modul  $\mathfrak{A}_i$ . Wir setzen  $\mathfrak{A}_j = 0$ , wenn  $j \geq m$ .

Sind nun  $\mathfrak{A}$  und  $\mathfrak{B}$  zwei  $k$ -Moduln aus  $\mathfrak{S}^{(m)}$ , so gilt:

$$(15) \quad \theta_i \mathfrak{A} \cdot \theta_k \mathfrak{B} \subseteq \theta_{i+k} (\mathfrak{A} \mathfrak{B}),$$

$$(16) \quad \binom{i+k}{i} \mathfrak{A}_i \cdot \mathfrak{B}_k \subseteq \mathfrak{A}_{i+k} (\mathfrak{A} \mathfrak{B}).$$

Wenn  $\mathfrak{A}$  ein  $k$ -Schiefring aus  $\mathfrak{S}^{(m)}$ , so folgt:

$$(17a) \quad \theta_i \mathfrak{A} \cdot \theta_k \mathfrak{A} \subseteq \theta_{i+k} \mathfrak{A},$$

$$(17b) \quad \binom{i+k}{i} \mathfrak{A}_i \cdot \mathfrak{A}_k \subseteq \mathfrak{A}_{i+k},$$

also ist  $\theta_i \mathfrak{A}$  ein zweiseitiges Ideal von  $\mathfrak{A}$ .

Zu jedem  $\mathfrak{S}$ -Modul  $\mathfrak{M}$  konstruieren wir einen  $\mathfrak{S}^{(m)}$ -Modul  $\mathfrak{M} = \mathfrak{M}^{(m)}$  nach folgender Vorschrift:  $s$  sei ein Symbol,  $\mathfrak{M}$  sei die Menge aller

formalen Summen  $v_0 + s v_1 + \dots + s^{m-1} v_{m-1}$  ( $v_i \in \mathfrak{m}$ ) mit den Rechenregeln:

$$(18a) \quad (v_0 + s v_1 \dots + s^{m-1} v_{m-1}) + (v'_0 + \dots + s^{m-1} v'_{m-1}) \\ = ((v_0 + v'_0) + s(v_1 + v'_1) \dots + s^{m-1}(v_{m-1} + v'_{m-1})),$$

$$(18b) \quad \lambda(v_0 + s v_1 \dots + s^{m-1} v_{m-1}) = \lambda v_0 + s \lambda v_1 + \dots + s^{m-1} (\lambda v_{m-1}),$$

$$(19) \quad A(v_0 + s v_1 + \dots + s^{m-1} v_{m-1}) = (v'_0 + s v'_1 + \dots + s^{m-1} v'_{m-1}),$$

wobei  $A = (a_0, a_1, \dots, a_{m-1})$  aus  $\mathfrak{S}^{(m)}$  stammt und

$$v'_i = \sum_{\nu=i}^{m-1} \binom{\nu}{i} a_{\nu-i} v_\nu$$

gesetzt ist.

Es ist klar, daß  $\mathfrak{M}$  ein  $k$ -Modul ist und daß die unter (19) erklärte Multiplikation beiderseits distributiv ist. Ferner gilt die Rechenregel  $(\lambda A)u = \lambda(Au)$  für alle  $\lambda$  aus  $k$ ,  $A$  aus  $\mathfrak{S}$ ,  $u$  aus  $\mathfrak{M}$ . Nun wollen wir noch die Gültigkeit des Assoziativgesetzes  $(AB)u = A(Bu)$  für alle  $A, B$  aus  $\mathfrak{S}$ ,  $u$  aus  $\mathfrak{M}$  nachweisen. Wegen der Gültigkeit der Distributivgesetze dürfen wir uns auf die Fälle, bei denen

$$A = (0 \dots 0, \overset{i}{a}, 0 \dots 0),$$

$$B = (0 \dots 0, \overset{k}{b}, 0 \dots 0),$$

$$u = s^j v \quad (v \in \mathfrak{m}; 0 \leq j < m)$$

ist, beschränken. Wenn  $j < i + k$ , so ist  $(AB)u = A(Bu) = 0$ . Wenn aber  $j - i - k = l \geq 0$ , so ist

$$(AB)u = s^l \binom{i+k}{i} \binom{j}{l} (ab)u,$$

$$A(Bu) = s^l \binom{j}{k} \binom{i+l}{i} a(bu),$$

und da

$$\binom{i+k}{i} \binom{i+k+l}{l} = \binom{i+k+l}{k} \binom{i+l}{i},$$

so folgt:  $(AB)u = A(Bu)$ . Demnach ist  $\mathfrak{M}$  ein  $\mathfrak{S}^{(m)}$ -Modul. Wir bemerken noch, daß in  $\mathfrak{S}^{(m)}$  das Kreisprodukt von  $A$  mit  $B$  nach der Vorschrift

$$A \circ B = AB - BA = (d_0, d_1, \dots, d_{m-1}),$$

$$(20) \quad d_i = \sum_{\nu=0}^i \binom{i}{\nu} (a_\nu \circ b_{i-\nu}) \quad (i = 0, 1, 2, \dots, m-1)$$

gebildet wird.

Jetzt führen wir dieselben Konstruktionen für Lie'sche  $k$ -Ringe  $\mathcal{A}$  aus. Den Potenzring  $\mathcal{A}^{(m)}$  definieren wir als Menge aller geordneten  $m$ -tupel von Elementen aus  $\mathcal{A}$  mit den Rechenregeln (10), (11) und der Regel

$$(21) \quad A \circ B = (a_1, a_2, \dots, a_{m-1}) \circ (b_0, b_1, \dots, b_{m-1}) = (d_0, d_1, \dots, d_{m-1}),$$

wobei

$$(21a) \quad d_i = \sum_0^i \binom{i}{\nu} a_\nu \circ b_{i-\nu} \quad (i = 0, 1, 2, \dots, m-1)$$

gesetzt ist. Ähnlich wie vorhin folgt, daß  $\mathcal{A}^{(m)}$  ein Lie'scher  $k$ -Ring ist.  $\mathcal{A}^{(1)}$  ist isomorph zu  $\mathcal{A}$ . Alle Elemente aus  $\mathcal{A}^{(m)}$  von der Form  $(0 \dots 0, a, 0 \dots 0)$  bilden einen  $k$ -Modul  $\theta_i \mathcal{A}^{(m)}$ . Wir setzen  $\theta_j \mathcal{A}^{(m)} = 0$  für alle  $j \geq m$ . Es gilt

$$(22) \quad \theta_0 \mathcal{A}^{(m)} = \mathcal{A}^{(m)}, \quad \theta_i \mathcal{A}^{(m)} \circ \theta_k \mathcal{A}^{(m)} \subseteq \theta_{i+k} \mathcal{A}^{(m)}.$$

Also ist  $\theta_i \mathcal{A}^{(m)}$  ein Ideal von  $\mathcal{A}^{(m)}$ . Der Restklassenring  $\mathcal{A}^{(m)} / \theta_1 \mathcal{A}^{(m)}$  ist isomorph zu  $\mathcal{A}$ ;  $\theta_1 \mathcal{A}^{(m)}$  ist ein nilpotentes Ideal von  $\mathcal{A}^{(m)}$ . Das Radikal von  $\mathcal{A}^{(m)}$  besteht aus allen  $m$ -tupeln, deren 0-te Komponente im Radikal von  $\mathcal{A}$  liegt. Wenn das Radikal von  $\mathcal{A}$  gleich Null ist, dann stimmt das Radikal von  $\mathcal{A}^{(m)}$  mit  $\theta_1 \mathcal{A}^{(m)}$  überein. — Wenn  $A$  ein in  $\mathcal{A}^{(m)}$  enthaltener  $k$ -Modul ist, dann ist  $\theta_i A = A \cap \theta_i \mathcal{A}^{(m)}$  ebenfalls ein  $k$ -Modul. Es gilt  $\theta_0 A = A$ . Wenn  $0 \leq i < m$ , so wird  $\theta_i A$  gebildet aus allen Elementen von  $A$ , welche die Form  $(0 \dots 0, a, \dots)$  haben. Alle hier vorkommenden  $i$ -ten Komponenten  $a$  bilden zusammen einen in  $\mathcal{A}$  enthaltenen  $k$ -Modul  $\mathcal{I}_i A$ . Wir setzen  $\mathcal{I}_j A = 0$ , wenn  $j \geq m$ . Sind nun  $A$  und  $B$  zwei  $k$ -Moduln aus  $\mathcal{A}^{(m)}$ , so folgt:

$$(23) \quad \theta_i A \circ \theta_k B \subseteq \theta_{i+k} (AB),$$

$$(24) \quad \binom{i+k}{i} \mathcal{I}_i A \circ \mathcal{I}_k B \subseteq \mathcal{I}_{i+k} (AB).$$

Falls  $A$  ein Lie'scher  $k$ -Ring aus  $\mathcal{A}^{(m)}$ , so folgt

$$\theta_i A \circ \theta_k A \subseteq \theta_{i+k} A,$$

$$\binom{i+k}{i} \mathcal{I}_i A \circ \mathcal{I}_k A \subseteq \mathcal{I}_{i+k} A.$$

Also ist  $\theta_i A$  ein Ideal von  $A$ .

Später ist der folgende Hilfssatz wichtig.

**Hilfssatz 2:** Für die  $k$ -Moduln  $A, B$  gelte:  $B \subseteq A \subseteq \mathcal{A}^{(m)}$ . Dann und nur dann ist  $B = A$ , wenn  $\mathcal{I}_i B = \mathcal{I}_i A$  ( $i = 0, 1, \dots, m-1$ ).

Beweis: 1. Wenn  $B = A$ , dann ist  $\mathcal{I}_i B = \mathcal{I}_i A$  für alle  $i$ .

2. Sei  $\mathfrak{A}_i B = \mathfrak{A}_i A$  ( $i = 0, 1, \dots, m-1$ ). Dann ist ersichtlich  $\theta_{m-1} B = \theta_{m-1} A$ . Es sei schon für den Index  $i$  bewiesen, daß  $\theta_{i+1} B = \theta_{i+1} A$ , wobei  $0 \leq i < m-1$ . Jedes Element aus  $\theta_i A$  hat die Form  $X = (0 \dots 0, a, \dots)$  mit  $a$  aus  $\mathfrak{A}_i A$ . Da  $\mathfrak{A}_i B = \mathfrak{A}_i A$ , so gibt es in  $B$  ein Element  $Y$  von der Form  $Y = (0 \dots 0, a, \dots)$ . Da  $B$  in  $A$  enthalten ist, so folgt  $X - Y \in A$ , sogar  $X - Y \subseteq \theta_{i+1} A$ . Da  $\theta_{i+1} A = \theta_{i+1} B$ , so folgt  $X - Y \in B$ ,  $X \in B$ ,  $X \in \theta_i B$ , also  $\theta_i A \subseteq \theta_i B$ . Da  $B \subseteq A$ , so gilt  $\theta_i B \subseteq \theta_i A$ , also ist  $\theta_i B = \theta_i A$ . Nach  $m-1$  Schritten gelangen wir zu der Gleichung  $A = \theta_0 A = \theta_0 B = B$ , w. z. b. w.

Folgerung: Ein in  $\mathcal{A}^{(m)}$  enthaltener  $k$ -Modul  $A$  stimmt dann und nur dann mit  $\mathcal{A}^{(m)}$  überein, wenn  $\mathfrak{A}_i A = \mathcal{A}$  ( $i = 0, 1, \dots, m-1$ ).

Zu jedem  $\mathcal{A}$ -Modul  $m$  konstruieren wir uns einen Modul  $\mathfrak{M} = \mathfrak{m}^{(m)}$  nach der gleichen Vorschrift und mit den gleichen Rechenregeln wie vorhin. Der Nachweis der Gültigkeit der Darstellungsbedingungen wird ähnlich wie vorhin erbracht.

### § 3. Konstruktion von $(L, \sigma)$ -Moduln.

Wir kehren zurück zu den Untersuchungen von § 1. Der Darstellungsring  $\bar{L}$  ist dann nach (7) enthalten in  $L^{*(m)}$ .

1. Wir fragen uns, wie wir die Komponentendarstellung von  $\bar{\sigma}a$  ableiten können aus der Darstellung

$$\bar{a} = (a_0, a_1, \dots, a_{m-1})$$

mit

$$a_i = (\sigma^i a)^* \quad (i = 0, 1, \dots, m-1).$$

Es ist:

$$(\sigma a) s^i v = \sum_{\nu=0}^i \binom{i}{\nu} s^\nu (\sigma^{i-\nu} a) v,$$

also

$$\sigma a = (a_1, a_2, \dots, a_{m-1}, a_m),$$

wobei gesetzt ist  $a_m = (\sigma^m a)^*$ .

Nach (9) ist:

$$(23) \quad (\sigma^m a)^* = a^* \circ s_0 + \sum_{i=1}^{m-1} (\sigma^{i-\nu} a)^* s_i.$$

$$(24) \quad a_m = a_0 \circ s_0 + \sum_{i=1}^{m-1} a_{i-\nu} s_i.$$

Setzen wir allgemein:

$$(25) \quad a_j = (\sigma^j a)^* \quad (j = 0, 1, 2, \dots).$$

so folgt:

$$(26) \quad \overline{\sigma^i a} = (a_i, a_{i+1}, \dots, a_{i+m-1}).$$

Aus (26) leiten wir ab, daß

$$(27) \quad \mathfrak{J}_0 \bar{L} \supseteq \mathfrak{J}_1 \bar{L} \dots \supseteq \mathfrak{J}_{m-1} \bar{L}.$$

Ferner ist ersichtlich

$$(28) \quad \mathfrak{J}_0 \bar{L} = L^*.$$

2. Es sei umgekehrt gegeben ein Lie'scher  $k$ -Ring  $L$ , ein Endomorphismus  $\sigma$  von  $L$ , ein  $L$ -Modul  $\mathfrak{m}$  und eine natürliche Zahl  $m$ . Dann konstruieren wir den  $L$ -Modul  $\mathfrak{M} = \mathfrak{m}^{(m, \sigma)}$  durch die Vorschrift:  $s$  ist ein Symbol,  $\mathfrak{M}$  ist die Menge aller formalen Summen  $v_0 + s v_1 + \dots + s^{m-1} v_{m-1}$  ( $v_i \in \mathfrak{m}$ ) mit den Rechenregeln (18a), (18b), ferner:

$$(29) \quad a(v_0 + s v_1 + \dots + s^{m-1} v_{m-1}) = v'_0 + s v'_1 + \dots + s^{m-1} v'_{m-1},$$

wobei

$$v'_i = \sum_{\nu=i}^{m-1} \binom{\nu}{i} (\sigma^{\nu-1} a) v_\nu \quad (i = 0, 1, 2, \dots, m-1).$$

Wir rechnen leicht nach, daß  $\mathfrak{M}$  wirklich ein  $L$ -Modul ist. Es ist klar, daß wir den zu  $\mathfrak{M}$  gehörigen Darstellungsring  $\bar{L}$  von  $L$  als Unterring von  $L^{*(m)}$  betrachten dürfen, wobei  $L^*$  der zu  $\mathfrak{m}$  gehörige Darstellungsring ist und gleichzeitig  $\mathfrak{M}$  als Modul  $\mathfrak{m}^{(m)}$  gemäß der in § 2 ausgeführten Konstruktion betrachtet wird.

3. Wir kehren zurück zu der im Anfang des Paragraphen fortgeführten Untersuchung. Vorweg möge der Fall behandelt werden, daß  $L^* = 0$ . Da  $\mathfrak{m}$  ein irreduzibler  $L$ -Modul ist, so muß  $\mathfrak{m}$  eindimensional sein. Dann ist  $\mathfrak{m} = k v_0$ ,  $s_i = \lambda_i \cdot \underline{1}$  ( $\lambda_i \in k$ ), wobei  $\underline{1}$  die identische Transformation von  $\mathfrak{m}$  ist. Das zu  $s$  gehörige charakteristische Polynom wird:

$$(30) \quad \chi(\xi) = \xi^m - \sum_0^{m-1} \lambda_i \xi^i.$$

Da  $L^* = 0$ , so ist nach (7)  $\bar{L} = 0$ . Jeder unter  $s$  invariante, in  $\mathfrak{M}$  enthaltene  $k$ -Modul ist daher  $(L, \sigma)$ -Modul. Da  $\mathfrak{M}$  ein irreduzibler  $(L, \sigma)$ -Modul ist, so gibt es keinen von 0 und  $\mathfrak{M}$  verschiedenen, in  $\mathfrak{M}$  enthaltenen, unter  $s$  invarianten  $k$ -Modul. Also ist  $\chi(\xi)$  irreduzibel.

Wenn umgekehrt  $\chi(\xi)$  ein irreduzibles Polynom ist, das in der Gestalt (30) geschrieben worden ist, dann konstruieren wir einen  $(L, \sigma)$ -Modul, indem wir ausgehen von einem  $L$ -Modul  $\mathfrak{m} = k v_0$  mit der Rechenregel:  $av = 0$  ( $a \in L$ ;  $\nu \in \mathfrak{m}$ ), dann nach der Vorschrift unter 2. den zugehörigen Modul  $\mathfrak{M} = \mathfrak{m}^{(m, \sigma)}$  konstruieren und die lineare Trans-

formation  $s$  durch die Rechenregeln:

$$s(s^i v_0) = s^{i+1} v_0 \quad (i = 0, 1, 2, \dots, m-1),$$

$$s(s^{m-1} v_0) = \sum_0^{m-1} \lambda_i s^i v_0$$

definieren. Mithin ist der Fall  $L^* = 0$  vollkommen übersehbar. Wenn der Körper  $k$  algebraisch abgeschlossen ist, so hat  $\chi(\mathfrak{E})$  den Grad 1 und  $\mathfrak{M}$  hat die Dimension 1.

Jetzt möge der Fall  $L^* \neq 0$ ,  $m > 1$ ,  $\mathfrak{J}_{m-1} \bar{L} = L^*$  behandelt werden. Nach (27), (28) ist dann

$$L^* = \mathfrak{J}_0 \bar{L} = \mathfrak{J}_1 \bar{L} \dots = \mathfrak{J}_{m-1} \bar{L}$$

und nach Hilfssatz 2 ist  $\bar{L} = L^{*(m)}$ . Es gibt also in  $L$  Elemente von der Form  $(0 \dots 0, a, 0 \dots 0)$ , wobei  $a$  beliebig aus  $L^*$ . Setzen wir die Komponenten dieser Elemente in die Gleichungen (9) ein, so folgt

$$(31) \quad \binom{m}{\nu} L^* = 0 \quad (\nu = 1, 2, \dots, m-1),$$

$$(32) \quad s_\nu \circ L^* = 0 \quad (\nu = 1, 2, \dots, m-1),$$

$$(33) \quad \binom{i}{\nu} L^* s_i = 0 \quad (1 \leq \nu < i \leq m-1),$$

$$(34) \quad L^* \circ s_0 \subseteq L^*,$$

$$(35) \quad L^* s_\nu \subseteq L^* \quad (\nu = 1, 2, \dots, m-1).$$

Aus (31) folgt, daß alle die Binomialkoeffizienten  $\binom{m}{1}, \binom{m}{2}, \dots, \binom{m}{m-1}$  durch die Charakteristik von  $L^*$  teilbar sind.

**Hilfssatz 3:**  $l-1$  sei eine natürliche Zahl. Der größte gemeinsame Teiler aller Binomialkoeffizienten  $\binom{l}{1}, \binom{l}{2}, \dots, \binom{l}{l-1}$  ist eine Primzahl  $q$  oder 1, je nachdem  $l$  Primzahlpotenz ist oder nicht.

Beweis: 1. Die Primzahl  $q$  gehe in allen Binomialkoeffizienten  $\binom{l}{1}, \binom{l}{2}, \dots, \binom{l}{l-1}$  auf. Da  $q$  Teiler von  $l = \binom{l}{1}$ , so ist  $l = q^\lambda \cdot l_0$  mit  $\lambda > 0$ ,  $(q, l_0) = 1$ . Da  $l-x$  und  $q^\lambda - x$  durch gleich hohe Potenzen von  $q$  teilbar sind, wenn  $x = 0, 1, 2, \dots, q^\lambda - l$ , so ist

$$\binom{l}{q^\lambda} = \frac{(l-0)(l-1) \dots (l-(q^\lambda-1))}{q^\lambda (q^\lambda-1) \dots 2 \cdot 1}$$

nicht durch  $q$  teilbar, also ist  $l = q^\lambda$ .

2. Wenn  $l = q^{\lambda}$ ,  $0 < i < l$ , so ist  $\binom{l}{i} = \frac{q^{\lambda}}{i} \cdot \frac{q^{\lambda}-1}{1} \dots \frac{q^{\lambda}-(i-1)}{i-1}$

durch  $q$  teilbar, w. z. b. w.

Aus Hilfssatz 3 folgt, daß die Charakteristik von  $L^*$  eine Primzahl  $p$  und daß  $m = p^{\mu}$  ( $\mu > 0$ ) ist.

**Hilfssatz 4:** I sei eine Menge von linearen Transformationen des  $k$ -Moduls  $m$ , so daß

1. von 0 verschiedene Transformationen in I vorkommen,
2. kein von 0 und  $m$  verschiedener unter I invarianter  $k$ -Modul in  $m$  enthalten ist. Es soll bewiesen werden, daß aus  $Iv = 0$  ( $v \in I$ ) folgt  $v = 0$ , ferner: Wenn für eine lineare Transformation  $x$  aus I eine der beiden Gleichungen  $xI = 0$  oder  $Ix = 0$  besteht, so ist  $x = 0$ . Alle mit I elementweise vertauschbaren linearen Transformationen bilden einen  $k$ -Schiefkörper  $Z(I)$  mit 1 als Einheitselement.

Beweis: Alle  $v$  aus  $m$ , für die  $Iv = 0$ , bilden einen unter I invarianten  $k$ -Modul  $m'$ . Da nach Voraussetzung  $I m \neq 0$ , so ist  $m' \neq m$ , also folgt nach Voraussetzung, daß  $m' = 0$ .

Wenn  $Ix = 0$ , so ist  $I(xv) = 0$  für alle  $v$  aus  $m$ , also nach dem eben Bewiesenen  $xv = 0$ ,  $x = 0$ . Der aus I durch Multiplikation, Addition und skalare Multiplikation erzeugte  $k$ -Schiefring  $f$  genügt denselben Voraussetzungen wie I. Es sei  $v$  ein Element  $\neq 0$  aus  $m$ . Dann folgt aus dem zuerst Bewiesenen, daß  $f v \neq 0$ , ferner ist  $f(fv) = f^2 v \subseteq f v$ , daher ist  $f v$  ein unter  $f$  invarianter  $k$ -Modul  $\neq 0$ , mithin  $f v = m$ . Wenn nun  $xI = 0$ , so folgt  $x f = 0$ ,  $x m = x(fv) = (x f)v = 0$ ,  $x = 0$ .

Es ist klar, daß  $Z(I) = Z(f)$ , ferner ist leicht zu sehen, daß  $Z(I)$  ein  $k$ -Schiefring ist. Für Elemente  $x$  aus  $Z(f)$  und von Null verschiedene Elemente  $v$  aus  $m$  folgt aus  $xv = 0$ , daß

$$x m = x(fv) = (x f)v = (f x)v = f(xv) = 0, \quad x = 0.$$

Wenn ferner  $x$  ein von Null verschiedenes Element aus  $Z(f)$  ist, so folgt  $x m \neq 0$ ,  $f(xm) = x(fm) \subseteq x m$ , also ist  $x m$  ein unter  $f$  invarianter  $k$ -Modul  $\neq 0$ , daher  $x m = m$ . Aus den beiden letzten Feststellungen folgt, daß es zu jedem von Null verschiedenen Element  $x$  aus  $Z(f)$  eine inverse lineare Transformation  $y$  von  $m$  gibt, so daß  $xy = yx = \underline{1}$ , also für alle  $s$  aus  $f$ :

$$y s = y s(x y) = y(s x) y = y(x s) y = (y x) s y = s y, \quad y \in Z(f).$$

Daher ist  $Z(I)$  ein Schiefkörper.

Korollar. Wenn  $k$  algebraisch abgeschlossen und I eine irreduzible Menge linearer Transformationen des endlichen  $k$ -Moduls  $m$  ist, dann bestehen die mit I elementweise vertauschbaren linearen Transformationen

von  $m$  genau aus den skalaren Vielfachen der identischen Transformation von  $m$ .

Beweis: Wenn  $I = 0$ , dann muß  $m$  1-gliedrig sein und dann ist jede lineare Transformation mit  $I$  elementweise vertauschbar und skalares Vielfaches der identischen Transformation. Wenn  $I \neq 0$ , so bilden die mit  $I$  elementweise vertauschbaren linearen Transformationen, wie oben gezeigt, einen  $k$ -Schiefkörper  $Z(I)$ , der ein hyperkomplexes System über  $k$  ist, weil  $m$  ein endlicher  $k$ -Modul. Da  $k$  algebraisch abgeschlossen, so ist  $Z$  zu  $k$  isomorph, also besteht  $Z$  aus dem skalaren Vielfachen der identischen Transformation.

Aus diesem Hilfssatze folgt, daß alle mit  $L^*$  elementweise vertauschbaren linearen Transformationen von  $m$  einen  $k$ -Schiefkörper  $Z(L^*)$  bilden. Alle Elemente  $x$  aus  $Z(L^*)$ , für die  $L^* x \subseteq L^*$ , bilden einen  $k$ -Schiefring  $Z_0(L^*)$ . Die Gleichungen (32) und (35) besagen, daß  $s_1, s_2, \dots, s_{m-1}$  in  $Z(L^*)$  enthalten sind.

Alle linearen Transformationen  $x$ , für die  $L^* \circ x \subseteq L^*$ , bilden einen Lie'schen  $k$ -Ring  $NL^*$ . Gleichung (34) besagt, daß  $s_0$  in  $NL^*$  enthalten ist.

Aus Hilfssatz 3 in Verbindung mit (33) folgt, daß  $L^* s_i = \underline{0}$ , wenn  $i \neq 0, 1, p, \dots, p^{\mu-1}$ . Aus Hilfssatz 4 folgt:  $s_i \neq \underline{0}$ , wenn  $i \neq 0, 1, p, \dots, p^{\mu-1}$ .

Die gefundenen Formeln werden zur Konstruktion von  $(L, \sigma)$ -Moduln benutzt. Sei also  $k$  ein Körper mit Primzahlcharakteristik  $p$ ,  $L$  ein Lie'scher  $k$ -Ring,  $\sigma$  ein Endomorphismus von  $L$ . Es sei  $m$  ein irreduzibler  $L$ -Modul, so daß durch die Festsetzung  $x^* v = x v$  eine homomorphe Abbildung  $x \rightarrow x^*$  von  $L$  auf den von Null verschiedenen und irreduziblen Lie'schen  $k$ -Ring  $L^*$  erklärt wird. Ferner werde die Gültigkeit einer Relation

$$(36) \quad (\sigma^{p^\mu} a)^* = a^* \circ s_0 + \sum_{i=1}^{\mu-1} (\sigma^{p^i} a)^* s_{p^i}$$

für alle  $a$  aus  $L$  vorausgesetzt, wobei

$$s_0 \in NL^*, \quad s_{p^i} \in Z_0 L^* \quad (i = 1, 2, \dots, \mu - 1).$$

Wir setzen noch  $m = p^\mu$ . Als  $(L, \sigma)$ -Modul verwenden wir den in Abschnitt 2 dieses Paragraphen konstruierten  $L$ -Modul  $\mathfrak{M} = m^{(m, \sigma)}$ , indem wir definieren

$$\begin{aligned} s(s^i v) &= s^{i+1} v & (i = 0, 1, \dots, m-2), \\ s(s^{m-1} v) &= s_0 v + \sum_{i=1}^{\mu-1} s^{p^i} s_{p^i} v. \end{aligned}$$

Wir wollen zeigen, daß hiermit ein  $(L, \sigma)$ -Modul konstruiert worden ist, d. h. wir müssen zeigen, daß  $(as - sa)u = (\sigma a)u$  für alle  $a$  aus  $L$ ,  $u$  aus  $\mathfrak{M}$  gilt.



Im Falle  $0 \leq i < m - 1$  ist

$$\begin{aligned} (as - sa) s^i v &= a s^{i+1} v - s(a s^i v) \\ &= \sum_{\nu=0}^{i+1} \binom{i+1}{\nu} s^\nu (\sigma^{i+1-\nu} a) v - \sum_{\nu=0}^{i+1} \binom{i}{\nu} s^{\nu+1} (\sigma^{i-\nu} a) v \\ &= \sum_{\nu=0}^i \binom{i}{\nu} s^\nu (\sigma^{i+1-\nu} a) v = (\sigma a) s^i v. \end{aligned}$$

Ferner ist

$$\begin{aligned} (as - sa) s^{m-1} v &= a s_0 v + \sum_{i=1}^{u-1} a s^{p^i} s_{p^i} v - \sum_{i=0}^{m-1} \binom{m-1}{i} s^i (\sigma^{m-1-i} a) v. \end{aligned}$$

Da  $\binom{p^i}{j} v = 0$ , wenn  $i \geq 1$ , und  $1 \leq j \leq p^i - 1$ , so folgt:

$$a s^{p^i} s_{p^i} v = (\sigma^{p^i} a) s_{p^i} v + s^{p^i} a s_{p^i} v,$$

also

$$\begin{aligned} (as - sa) s^{m-1} v &= \left( a \circ s_0 + \sum_{i=1}^{\mu-1} (\sigma^{p^i} a) s_{p^i} \right) v \\ &\quad + s_0 a v + \sum_{i=1}^{\mu-1} s^{p^i} a s_{p^i} v \\ &\quad - \sum_{i=1}^{m-1} \binom{m-1}{i-1} s^i (\sigma^{m-i} a) v \\ &\quad - s_0 a v - \sum_{i=1}^{\mu-1} s^{p^i} s_{p^i} a v. \end{aligned}$$

Da nun

$$\binom{p^\mu - 1}{i-1} + \binom{p^\mu - 1}{i} = \binom{p^\mu}{i} \equiv 0 (p),$$

wenn  $0 < i < p^\mu$ , so folgt zusammen mit (36), daß

$$\begin{aligned} (as - sa) s^{m-1} v &= (\sigma^m a) v + \sum_{i=1}^{m-1} \binom{m-1}{i} s^i (\sigma^{m-i} a) v \\ &\quad + \sum_{i=1}^{\mu-1} s^{p^i} (a s_{p^i} - s_{p^i} a) v. \end{aligned}$$

Da wir ferner vorausgesetzt hatten, daß  $s_{p^i}$  in  $Z_0(L^*)$  enthalten ist, also  $(a s_{p^i} - s_{p^i} a) v = 0$ , so folgt

$$\begin{aligned} (as - sa) s^{m-1} v &= \sum_{i=0}^{m-1} \binom{m-1}{i} s^i (\sigma^{m-i} a) v \\ &= (\sigma a) s^{m-1} v, \quad \text{w. z. b. w.} \end{aligned}$$

Der so gefundene  $(L, \sigma)$ -Modul ist nicht notwendig irreduzibel, aber jedenfalls enthält er einen irreduziblen  $(L, \sigma)$ -Modul, dessen  $L$ -Kompositionsfaktoren  $L$ -isomorph zu  $m$  sind.

Eine Relation von der Form (36) besteht sicher dann, wenn  $L$  ein endlicher  $k$ -Modul ist. Ist etwa  $r$  der Rang von  $L$  über  $k$ , so sind die  $r + 1$  untereinander vertauschbaren linearen Transformationen  $\sigma, \sigma^p, \sigma^{p^2}, \dots, \sigma^{p^r}$  linear abhängig. Es besteht daher eine Relation von der Form:

$$\sigma^{p^\lambda} = \sum_0^{\lambda-1} \lambda_i \sigma^{p^i} \quad (\lambda_i \in k), \quad \text{wobei} \quad 0 \leq \lambda \leq r.$$

Mithin ist

$$(\sigma^{p^\lambda} a)^* = \sum_0^{\lambda-1} \lambda_i (\sigma^{p^i} a)^* \quad (a \text{ bel. aus } L).$$

Als Ergebnis erhalten wir den

**Satz 2:** *Wenn  $L$  ein endlicher Lie'scher  $k$ -Ring mit Primzahlcharakteristik ist, so existiert für jeden Endomorphismus  $\sigma$  von  $L$  ein irreduzibler  $(L, \sigma)$ -Modul, der als  $L$ -Modul betrachtet, einen vorgegebenen irreduziblen  $L$ -Modul enthält.*

#### § 4. $\sigma$ -einfache Lie'sche Ringe.

Wir wenden die Untersuchungen des vorigen Paragraphen auf die reguläre Darstellung eines Lie'schen Ringes über dem Grundkörper  $k$  an.

**Satz 3:** *Die abelschen  $\sigma$ -einfachen endlichen Lie'schen  $k$ -Ringe  $L$  werden durch die folgende Konstruktion erhalten: Man suche ein irreduzibles Polynom von der Form*

$$\chi(\xi) = \xi^m - \sum_0^{m-1} \lambda_i \xi^i,$$

definiere in dem  $m$ -gliedrigen  $k$ -Modul  $L = \{u_0, u_1, \dots, u_{m-1}\}$  die Kreismultiplikation durch die Festsetzung  $u_i \circ u_k = 0$  und definiere den Endomorphismus  $\sigma$  durch die Regel:

$$\sigma u_i = u_{i+1} \quad (i = 0, 1, 2, \dots, m-2), \quad \sigma u_{m-1} = \sum_0^{m-1} \lambda_i u_i.$$

**Satz 4:** *Wenn ein  $\sigma$ -einfacher, nichtabelscher Lie'scher  $k$ -Ring mit der Charakteristik 0 eine Hauptreihe besitzt, so ist er schlechthin einfach.*

**Satz 5:** *Wenn die Charakteristik von  $k$  eine Primzahl  $p$  ist, so werden alle  $\sigma$ -einfachen, nichtabelschen Lie'schen  $k$ -Ringe  $L$  durch folgende Konstruktion erhalten:  $\mathcal{A}$  sei ein einfacher, nichtabelscher Lie'scher  $k$ -Ring,  $\sigma_0$  seien ein Endomorphismus von  $\mathcal{A}$ ,  $\sigma_{p^i}$  ( $i = 1, 2, \dots, \mu - 1$ ) seien lineare Transformationen des  $k$ -Moduls  $\mathcal{A}$ , die der Funktionalgleichung*

$$\sigma_{p^i}(a \circ b) = a \circ (\sigma_{p^i} b) \quad (a, b \in \mathcal{A})$$

genügen, dann setzen wir  $L = \mathcal{A}^{(p^\mu)}$  und definieren den Endomorphismus  $\sigma$  von  $L$  durch die Festsetzung

$$\sigma(a_0, a_1, \dots, a_{m-1}) = (a_1, a_2, \dots, a_m),$$

wobei

$$m = p^\mu, \quad a_m = \sigma_0 a_0 + \sum_{i=1}^{\mu-1} \sigma_{p^i} a_{p^i}.$$

Der Beweis von Satz 3 folgt aus Abschnitt 3 des vorigen Paragraphen.

Beweis von Satz 4 und Satz 5:  $L$  sei ein nichtabelscher Lie'scher  $k$ -Ring mit Hauptreihe,  $\sigma$  sei ein Endomorphismus von  $L$ . Wir haben den Fall zu untersuchen, daß  $L$   $\sigma$ -einfach, aber nicht schlechthin einfach ist. Da  $L$  eine Hauptreihe besitzt, so enthält  $L$  ein kleinstes Ideal  $A$ . Vermöge der Zuordnungen:

$$x^* v = x \circ v \quad (v \in A),$$

$$\underline{x} u = x \circ u \quad (u \in L)$$

werden zwei Darstellungen  $x \rightarrow x^*$  bzw.  $x \rightarrow \underline{x}$  von  $L$  in linearen Transformationen des  $k$ -Moduls  $L = \mathfrak{M}$  bzw.  $A = \mathfrak{m}$  erklärt.  $\mathfrak{M}$  ist ein irreduzibler  $(L, \sigma)$ -Modul,  $\mathfrak{m}$  ist ein irreduzibler  $L$ -Modul. Nach § 1 sind

$$A_0 = 0, \quad A_i = A + \sigma A + \dots + \sigma^{i-1} A \quad (i = 1, 2, \dots)$$

Ideale von  $L$ . Da  $L$   $\sigma$ -einfach ist und eine Hauptreihe besitzt, so gibt es einen Index  $m > 0$ , so daß  $0 = A_0 \subset A_1 \subset A_2 \dots \subset A_m = L$ . Da  $L$  nicht schlechthin einfach, so ist  $m > 1$ . Wenn  $0 < i < m - 1$ , so ist

$$A_i \circ L \subseteq A_i \subseteq A_{m-1}, \quad \text{also} \quad A_i \mathfrak{M} \subseteq \mathfrak{m}_{m-1}.$$

Nach Gleichung (4) folgt:  $(A_i)^* = 0$ ,

$$(37) \quad \mathfrak{J}_0 \underline{A}_i = 0 \quad (i = 0, 1, 2, \dots, m-1),$$

$$\underline{A} \subseteq \theta_1 \underline{L}.$$

Es sei schon bewiesen, daß  $\underline{A} \subseteq \theta_j \underline{L}$ , wobei  $1 \leq j < m - 1$ . Dann folgt nach (26), daß

$$\mathfrak{J}_j \underline{A} = \mathfrak{J}_0 \sigma^j \underline{A} = 0, \quad \underline{A} \subseteq \theta_{j+1} \underline{L}.$$

Nach  $(m-2)$ -maliger Anwendung dieses Schlusses folgt

$$\underline{A} \subseteq \theta_{m-1} \underline{L}.$$

Aus der Zerlegung  $L = A_{m-1} + \sigma^{m-1} A$  folgt

$$\mathfrak{J}_0 L = \mathfrak{J}_0 \underline{A}_{m-1} + \mathfrak{J}_0 \sigma^{m-1} \underline{A}.$$

Nach (37) ist

$$L^* = \mathfrak{G}_0 \underline{L} = \mathfrak{G}_0 \underline{\sigma^{m-1} A} = \mathfrak{G}_{m-1} \underline{A}.$$

Aus  $L^* = \mathfrak{G}_{m-1} \underline{A} \subseteq \mathfrak{G}_{m-1} \underline{L} \subseteq L^*$  schließen wir  $\mathfrak{G}_{m-1} \underline{L} = L^*$ .

Aus dem Abschnitt 4 des vorigen Paragraphen schließen wir, daß die Charakteristik von  $k$  eine Primzahl von  $p$  ist und daß  $m = p^\mu$ ,  $\underline{L} = L^{*(m)}$ . Da  $L$  nichtabelsch ist, so ist  $\underline{L} = 0$ , also  $L^* \neq 0$ . Wir wissen, daß der  $L$ -Modul  $\mathfrak{M}/\mathfrak{m}_{m-1}$  irreduzibel ist, d. h. daß der Restklassenring  $\mathcal{A} = L/A_{m-1}$  einfach ist. Da nach (37)  $\mathfrak{G}_0(A_{m-1}) = 0$ , d. h.  $A_{m-1}^* = 0$ , so wird durch die Zuordnung

$$(38) \quad R_a = a + A_{m-1} \rightarrow a^* = R_a^*$$

eine homomorphe Abbildung von  $\mathcal{A}$  auf den Ring  $L^*$  definiert. Da  $m$   $L$ -isomorph zu  $\mathfrak{M}/\mathfrak{m}_{m-1}$ , so ist die eben definierte Darstellung von  $\mathcal{A}$  gerade die reguläre Darstellung. Da  $\mathcal{A}$  einfach und der Darstellungsring bei der regulären Darstellung von Null verschieden ist, so ist  $\mathcal{A}$  nichtabelsch. Da  $\mathcal{A}$  einfach und nichtabelsch, so ist die Darstellung (38) treu. Da das Zentrum von  $L$  ein charakteristisches abelsches Ideal ist,  $L$  aber nichtabelsch ist, so folgt aus der  $\sigma$ -Einfachheit von  $L$ , daß das Zentrum von  $L$  gleich Null ist. Die reguläre Darstellung von  $L$  ist treu,  $L$  und  $\underline{L}$  sind isomorph.

Damit haben wir erhalten, daß  $L$  isomorph zu  $\mathcal{A}^{(m)}$  ist, wobei  $m = p^\mu$ ,  $\mathcal{A}$  einfach und nichtabelsch ist.

Im vierten Abschnitt des vorigen Paragraphen wurde gezeigt, daß

$$(\sigma^m a)^* v = (a \circ s_0)^* v + \sum_{i=1}^{\mu-1} (\sigma^{p^i} a)^* s_{p^i} v,$$

wobei

$$s_0 \in NL^*, \quad s_{p^i} \in Z_0 L^* \quad (i = 0, 1, \dots, \mu - 1).$$

Durch die Festsetzung  $\sigma_0 a^* = a^* \circ s_0$  wird ein Endomorphismus  $\sigma_0$  von  $L^*$  definiert, ferner wird durch die Festsetzung  $\sigma_{p^i} a^* = a^* s_{p^i}$  eine lineare Transformation  $\sigma_{p^i}$  des  $k$ -Moduls  $L$  definiert, so daß

$$\sigma_{p^i}(a^* \circ b^*) = a^* \circ \sigma_{p^i} b^* \quad (i = 0, 1, 2, \dots, \mu - 1).$$

Für das Element  $\underline{a} = (a_0, a_1, \dots, a_{m-1})$  aus  $L$  gilt:

$$\underline{\sigma a} = (a_1, a_2, \dots, a_m)$$

mit

$$a_m = \sigma_0 a_0 + \sum_{i=1}^{\mu-1} \sigma_{p^i} a_{p^i}.$$

Zur Konstruktion  $\sigma$ -einfacher Lie'scher Ringe brauchen wir den folgenden Hilfssatz 5:  $\mathcal{A}$  sei ein Lie'scher  $k$ -Ring. Wenn  $m$  ein irreduzibler  $\mathcal{A}$ -Modul ist und wenn  $\mathcal{A}m \neq 0$ , dann ist  $m$  der einzige in  $m^{(m)}$  enthaltene irreduzible  $\mathcal{A}^{(m)}$ -Modul.

Beweis: Die Zuordnung  $a \rightarrow a' = (a, 0 \dots 0)$  bildet  $\mathcal{A}$  isomorph auf einen in  $\mathcal{A}^{(m)}$  enthaltenen Lie'schen  $k$ -Teilring  $\mathcal{A}'$  ab. Da  $av = a'v$  ( $a \in \mathcal{A}; v \in m$ ), so ist  $m$  ein irreduzibler  $\mathcal{A}'$ -Modul, erst recht ein irreduzibler  $\mathcal{A}^{(m)}$ -Modul. Nun sei  $m'$  ein in  $m^{(m)}$  enthaltener irreduzibler  $\mathcal{A}^{(m)}$ -Modul. Dann gibt es ein Element  $u = s^i v_i + s^{i-1} v_{i-1} + \dots + v_0$  in  $m^{(m)}$  mit  $v_i \neq 0$ . Da  $\mathcal{A}m \neq 0$ , so gibt es nach Hilfssatz 4 ein Element  $a$  aus  $\mathcal{A}$ , das  $v_i$  nicht annulliert. Für das in  $\mathcal{A}^{(m)}$  enthaltene Element  $A = (0 \dots 0, a, 0 \dots 0)$  gilt  $Au = av_i \neq 0$ ,  $Au \in m' \cap m$ . Also ist  $m' \cap m$  von Null verschiedener  $\mathcal{A}^{(m)}$ -Modul, und da  $m$  ein irreduzibler  $\mathcal{A}^{(m)}$ -Modul, so ist  $m' \cap m = m$ ,  $m = m'$ , w. z. b. w.

Nun sei  $k$  ein Körper mit Primzahlcharakteristik  $p$ ,  $\mathcal{A}$  ein einfacher nichtabelscher Lie'scher  $k$ -Ring,  $\sigma_0$  ein Endomorphismus von  $\mathcal{A}$ ,  $\mu$  eine natürliche Zahl; ferner seien lineare Transformationen  $\sigma_{p^i}$  des  $k$ -Moduls  $\mathcal{A}$  gegeben, die der Funktionalgleichung  $\sigma_{p^i}(a \circ b) = a \circ \sigma_{p^i} b$  für alle  $a, b$  aus  $\mathcal{A}$  genügen ( $i = 1, 2, \dots, \mu - 1$ ). Wir setzen  $L = \mathcal{A}^{(p^\mu)}$  und definieren

$$\sigma(a_0, a_1, \dots, a_{m-1}) = (a_1, a_2, \dots, a_m)$$

mit

$$m = p^\mu, \quad a_m = \sigma_0 a_0 + \sum_{i=1}^{\mu-1} \sigma_{p^i} a_{p^i}.$$

$\sigma$  ist eine lineare Transformation des  $k$ -Moduls  $L$ . Um zu zeigen, daß  $\sigma$  ein Endomorphismus von  $L$  ist, genügt es, die Gleichung

$$(39) \quad \sigma(A \circ B) = A \circ \sigma B + \sigma A \circ B$$

für Elemente

$$A = (0 \dots 0, \overset{i}{a}, 0 \dots 0),$$

$$B = (0 \dots 0, \overset{k}{b}, 0 \dots 0)$$

aus  $L$  zu beweisen. Wir setzen  $\sigma_i a = 0$  ( $i \neq 0, 1, p, p^2, \dots, p^{\mu-1}$ ;  $a \in \mathcal{A}$ ) und haben die Formeln

$$(39a) \quad \sigma_j(a \circ b) = a \circ \sigma_j b \quad (0 \leq j < m).$$

Wenn  $i + k > m$ , so ist

$$\sigma(A \circ B) = A \circ \sigma B = \sigma A \circ B = 0,$$

woraus (39) folgt. Wenn  $i+k = m$ , so ist

$$\begin{aligned} 0 < i, k < m, \quad \sigma(A \circ B) &= 0, \\ A \circ \sigma B &= \left( 0 \dots 0, \binom{m-1}{i} a \circ b \right), \\ \sigma A \circ B &= \left( 0 \dots 0, \binom{m-1}{k} a \circ b \right), \end{aligned}$$

und da

$$\begin{aligned} \binom{m-1}{k} &= \binom{m-1}{m-1-k} = \binom{m-1}{i-1}, \\ \binom{m-1}{i-1} + \binom{m-1}{i} &= \binom{m}{i} = (p^\mu) \equiv 0 \pmod{p}, \end{aligned}$$

so folgt wiederum (39).

Wenn  $i = 0$ ,  $0 < k < m$ , so ist

$$\begin{aligned} \sigma(A \circ B) &= (0 \dots 0, a \circ b, 0 \dots 0, \sigma_k(a \circ b)), \\ A \circ \sigma B &= (0 \dots 0, a \circ b, 0 \dots 0, a \circ \sigma_k b), \\ \sigma A \circ B &= 0, \end{aligned}$$

woraus (39) wegen (40a) folgt; entsprechend im Falle  $i > 0$ ,  $k = 0$ .

Wenn  $i = k = 0$ , so ist:

$$\begin{aligned} \sigma(A \circ B) &= (0 \dots 0, \sigma_0(a \circ b)), \\ A \circ \sigma B &= (0 \dots 0, a \circ \sigma_0 b), \\ \sigma A \circ B &= (0 \dots 0, \sigma_0 a \circ b). \end{aligned}$$

Da  $\sigma_0$  ein Endomorphismus von  $\mathcal{A}$ , so folgt wiederum (39). Wenn  $0 < k < i+k < m$ , so ist

$$\begin{aligned} \sigma(A \circ B) &= \left( 0 \dots 0, \binom{i+k-1}{i} a \circ b, 0 \dots 0, \binom{i+k}{i} \sigma_{i+k}(a \circ b) \right), \\ A \circ \sigma B &= \left( 0 \dots 0, \binom{i+k-1}{i} a \circ b, 0 \dots 0 \quad 0 \right), \\ \sigma A \circ B &= \left( 0 \dots 0, \binom{i+k-1}{k} a \circ b, 0 \dots 0 \right). \end{aligned}$$

Es ist  $1 < i+k < p^\mu$ . Entweder ist  $i+k$  eine  $p$ -Potenz, dann ist  $\binom{i+k}{i} \equiv 0 \pmod{p}$ , oder es ist  $\sigma_{i+k} = 0$ . Auf jeden Fall ist

$$\binom{i+k}{i} \sigma_{i+k}(a \circ b) = 0.$$

Da nun

$$\binom{i+k-1}{i} + \binom{i+k-1}{k} = \binom{i+k-1}{i} + \binom{i+k-1}{i-1} = \binom{i+k}{i},$$

so folgt wiederum (39).

Es ist noch zu zeigen, daß  $L$   $\sigma$ -einfach ist. Zur regulären Darstellung von  $L$  gehört der Darstellungsmodul  $\mathfrak{M} = L$ .  $\mathfrak{M}$  enthält den  $L$ -Modul  $\mathfrak{m} = \theta_{m-1} L \neq 0$ . Die Zuordnung  $a \rightarrow a' = (a, 0 \dots 0)$  bildet  $\mathcal{A}$  isomorph auf einen Lie'schen  $k$ -Teilring  $\mathcal{A}$  von  $L$  ab. Setzen wir  $av = a' \circ v$  für alle  $v$  aus  $\mathfrak{m}$ , so wird  $\mathcal{A}$  durch  $\mathfrak{m}$  regulär dargestellt, wie sofort zu sehen. Da  $\mathcal{A}$  einfach und nichtabelsch, so ist  $\mathfrak{m}$  ein irreduzibler  $\mathcal{A}$ -Modul, und es ist  $\mathcal{A}\mathfrak{m} \neq 0$ . Ferner ist  $\mathfrak{M} = \mathfrak{m}^{(m)}$ , wie leicht ersichtlich. Nach Hilfssatz 5 folgt, daß  $\mathfrak{m}$  der einzige in  $\mathfrak{M}$  enthaltene irreduzible  $L$ -Modul ist. Jeder in  $\mathfrak{M}$  enthaltene  $(L, \sigma)$ -Modul  $\mathfrak{M}' \neq 0$  muß  $\mathfrak{m}$  enthalten. Da ferner  $\mathfrak{M} = \mathfrak{m} + \sigma\mathfrak{m} + \dots + \sigma^{m-1}\mathfrak{m}$ , so muß  $\mathfrak{M}' = \mathfrak{M}$  sein, also ist  $\mathfrak{M}$  unter  $(L, \sigma)$  irreduzibel, d. h.  $L$  ist  $\sigma$ -einfach, w. z. b. w.

**Satz 6:** *Es sei  $k$  ein Körper mit der Charakteristik 0. In einem endlichen Lie'schen  $k$ -Ring mit Hauptreihe ist das Radikal ein charakteristisches Ideal.*

Beweis:  $L$  sei ein  $n$ -gliedriger Lie'scher  $k$ -Ring,  $R$  sei das Radikal von  $L$ ,  $\sigma$  sei ein Endomorphismus von  $L$ . Zu zeigen ist, daß  $\sigma R \subseteq R$ . Das ist klar, falls  $R = 0$  oder  $R = L$ , also z. B. im Falle  $n = 1$ . Nun sei  $n > 1$  und der Satz bewiesen für Lie'sche  $k$ -Ringe, deren Rang über  $k$  kleiner als  $n$  ist.  $L$  enthält dann ein unter  $\sigma$  invariantes Ideal  $A \neq 0$  mit möglichst kleinem Range über  $k$ .

1. Wenn  $A = L$ , so ist  $L$   $\sigma$ -einfach, also ist nach Satz 4  $L$  abelsch oder schlechthin einfach und nichtabelsch. Daher ist entweder  $R = L$  oder  $R = 0$ , und dann ist der Satz klar.

2. Wenn  $A$  auflösbar, so ist das Radikal von  $L/A$  gleich  $R/A$  und dann bildet der von  $\sigma$  induzierte Endomorphismus von  $L/A$  nach Induktionsvoraussetzung das Radikal  $R/A$  in sich ab, also folgt  $\sigma R \subseteq R$ .

3. Wenn  $A$  nicht auflösbar und von  $L$  verschieden, so ist nach Induktionsvoraussetzung das Radikal von  $A$  ein unter  $\sigma$  invariantes Ideal von  $L$ . Nach Konstruktion von  $A$  folgt, daß das Radikal von  $A$  gleich Null ist. Daher ist  $A \cap R = 0$ ,  $R \circ A = 0$ ,  $R \subseteq Z(A)$ . Da  $A$  ein unter  $\sigma$  invariantes Ideal von  $L$  ist, so ist auch der Zentralisator  $Z(A)$  von  $A$  ein unter  $\sigma$  invariantes Ideal von  $L$ . Da  $A$  nicht auflösbar, so liegt  $A$  nicht im Zentrum von  $L$ , also ist  $Z(A)$  kleiner als  $L$  und nach Induktionsvoraussetzung ist das Radikal  $\bar{R}$  von  $Z(A)$  ein unter  $\sigma$  invariantes Ideal von  $L$ . Da  $\bar{R}$  ein auflösbares Ideal von  $L$ , so folgt  $\bar{R} \subseteq R$ . Anderer

seits ist  $R$  ein auflösbares Ideal von  $Z(A)$ , also liegt  $R$  in  $\bar{R}$ , mithin ist  $R = \bar{R}$  und  $R$  ist unter  $\sigma$  invariant, w. z. b. w.

**Satz 7:** *Über Grundkörpern von der Charakteristik 0 ist jeder endliche charakteristisch einfache Lie'sche Ring entweder abelsch oder schlechthin einfach und nichtabelsch.*

Beweis:  $L$  sei ein endlicher, nichtabelscher, charakteristisch einfacher Lie'scher Ring über dem Körper  $k$  mit der Charakteristik 0. Nach I, § 4 ist  $L$  vollkommen. Nach Satz 6 ist das Radikal von  $L$  gleich Null. Also enthält jedes von Null verschiedene Ideal von  $L$  ein vollkommenes Ideal  $\neq 0$  und da dieses charakteristisch ist, so stimmt es mit  $L$  überein, d. h.  $L$  ist einfach schlechthin.

Ich möchte hier drei Vermutungen aufführen, die ich weder beweisen noch widerlegen kann:

1. Der äußere Endomorphismenring einer einfachen nichtabelschen, Lie'schen Algebra mit Primzahlcharakteristik ist auflösbar.

Das ist eine Analogie zu der Vermutung von O. SCHREIER, daß die äußere Automorphismengruppe einer endlichen Gruppe auflösbar ist.

Nach I, Satz 16 und dem Ergebnis von CARTAN sind einfache Lie'sche Algebren mit Charakteristik 0 abgeschlossen.

2. Jede nichtabelsche charakteristisch einfache Lie'sche Algebra mit Primzahlcharakteristik  $p$  ist  $p$ -Potenzring einer einfachen Lie'schen Algebra.

Bei Charakteristik 0 gibt es nach Satz 7 nur die schlechthin einfachen Lie'schen Ringe.

3. Wenn die Vermutung 1 richtig ist, so läßt sich leicht beweisen, daß der äußere Endomorphismenring jedes  $p$ -Potenzringes einer normal einfachen Lie'schen Algebra mit Primzahlcharakteristik  $p$  auflösbar ist. Aus Vermutung 2 würde dann folgen, daß der Endomorphismenring jeder charakteristisch einfachen nichtabelschen Lie'schen Algebra auflösbar ist. Aus 2 und 3 würde folgen:

**Satz 8:** *Der Kern einer nichtauflösbaren Lie'schen Algebra ist die Ringsumme von einfachen nichtabelschen Algebren.*

Beweis: Von Null verschiedene Kerne sind gekennzeichnet als vollkommene halbeinfache Lie'sche Algebren. Es sei  $L$  ein von Null verschiedener Kern.  $L$  enthält ein charakteristisch einfaches Ideal  $A \neq 0$ . Nach Vermutung 2 und 3 ist der Faktorring  $L/(A + Z(A))$  auflösbar. Also ist  $L = A + Z(A)$ . Jedes auflösbare Ideal von  $A$  ist also auflösbares Ideal von  $L$ . Da  $L$  halbeinfach, so ist das Radikal von  $A$  gleich Null. Gemäß Vermutung 2 ist  $A$  schlechthin einfach und nichtabelsch. Dann ist der Durchschnitt von  $A$  mit  $Z(A)$  gleich Null, also  $L$  die Ringsumme von  $A$  und  $Z(A)$ . Mit  $L$  ist auch  $Z(A)$  vollkommen und halbeinfach. Nun ergibt ein Induktionsschluß die Behauptung.



## § 5. Bestimmungen der endlichen irreduziblen $(L, \sigma)$ -Moduln über algebraisch abgeschlossenen Grundkörper.

Jetzt möge die in § 1 begonnene Untersuchung der irreduziblen  $(L, \sigma)$ -Moduln fortgeführt werden.

1. Die linearen Transformationen aus  $\bar{L}$  erzeugen einen  $k$ -Schiefring  $\mathfrak{S}$  bei fortgesetzter Multiplikation und Addition. Da  $\mathfrak{m}$  ein  $L$ -invarianter Teilmodul von  $\mathfrak{M}$  ist, so ist  $\mathfrak{m}$  auch  $\mathfrak{S}$ -invariant. Durch die Festsetzung  $X^*v = Xv$  für alle  $X$  aus  $\mathfrak{S}$  und  $v$  aus  $\mathfrak{m}$  wird eine Darstellung  $X \rightarrow X^*$  von  $\mathfrak{S}$  in linearen Transformationen von  $\mathfrak{m}$  erklärt. Der zugehörige Darstellungsring werde mit  $\mathfrak{S}^*$  bezeichnet. Da  $\bar{a}^* = a^*$  für alle  $a$  aus  $L$ , so ist  $L^*$  in  $\mathfrak{S}^*$  enthalten. Daher ist  $\mathfrak{S}^*$  ein irreduzibler  $k$ -Ring linearer Transformationen von  $\mathfrak{m}$ . Da der  $k$ -Schiefring  $\mathfrak{S}$  von  $\bar{L}$  erzeugt wird und da  $I \circ s \subseteq \bar{L} \subseteq \mathfrak{S}$ , so folgt nach I, § 4, Hilfssatz 8, daß  $\mathfrak{S} \circ s \subseteq \mathfrak{S}$ . Also wird durch die Festsetzung

$$(40) \quad \bar{\sigma} X = X \circ s$$

für alle  $X$  aus  $\mathfrak{S}$  ein Endomorphismus  $\bar{\sigma}$  von  $\mathfrak{S}$  erklärt. Da  $L$  in  $\mathfrak{S}$  enthalten ist und da  $\mathfrak{M}$  ein irreduzibler  $(L, \sigma)$ -Modul ist, so ist  $\mathfrak{M}$  auch ein irreduzibler  $(\mathfrak{S}, \sigma)$ -Modul. Ersetzen wir in den Überlegungen von § 1  $L$  durch  $\mathfrak{S}$ , so folgt:

$$\mathfrak{S} \subseteq \mathfrak{S}^{*(m)}.$$

Die Gleichungen (6) schreiben sich nun

$$(41) \quad \binom{m}{\nu} (\sigma^{m-\nu} A)^* = A^* \circ s_0 + \sum_{i=\nu+1}^{m-1} (\sigma^{i-\nu} A)^* s_i \quad (A \in \mathfrak{S})$$

$$(\nu = 0, 1, 2, \dots, m-1).$$

2. Jetzt setzen wir zusätzlich voraus, daß der  $k$ -Schiefring  $\mathfrak{S}$  von Null verschieden ist. Dann ist also  $\mathfrak{S}^* \mathfrak{m} \neq 0$ . Nach dem Hilfssatz 4 folgt, daß

$$(42) \quad \mathfrak{S}^* v = \mathfrak{m} \quad \text{für alle } v \neq 0.$$

3. Nun sei überdies  $\mathfrak{S}^*$  ein hyperkomplexes System über  $k$ . Das ist z. B. stets der Fall, wenn  $\mathfrak{m}$  ein endlicher  $k$ -Modul ist. Aus (42) folgt umgekehrt, daß bei unserer Zusatzvoraussetzung  $\mathfrak{m}$  ein endlicher  $k$ -Modul ist.

Da  $\mathfrak{S}^*$  eine treue irreduzible Darstellung besitzt, so ist  $\mathfrak{S}^*$  ein einfaches hyperkomplexes System über  $k$ . Insbesondere ist  $\mathfrak{S}^* \mathfrak{S}^* = \mathfrak{S}^*$ . Nach (27), (28) folgt:

$$\mathfrak{S}^* = \mathfrak{J}_0 \mathfrak{S} \supseteq \mathfrak{J}_1 \mathfrak{S} \dots \supseteq \mathfrak{J}_{m-1} \mathfrak{S}.$$

Ferner ist nach (17 b) jedes  $\mathfrak{J}_i \mathfrak{S}$  zweiseitiges Ideal von  $\mathfrak{S}^*$ . Da  $\mathfrak{S}^*$  einfach, so gibt es eine eindeutig bestimmte natürliche Zahl  $\varkappa$ , so daß

$$(43) \quad \mathfrak{S}^* = \mathfrak{J}_0 \mathfrak{S} = \dots = \mathfrak{J}_{\varkappa-1} \mathfrak{S}, \quad \mathfrak{J}_\varkappa \mathfrak{S} = \mathfrak{J}_{\varkappa+1} \mathfrak{S} = \dots = 0.$$

4. Wir untersuchen näher den Fall  $\varkappa > 1$ . Wenn  $0 < i < \varkappa$ , so ist nach (17 b) und dem eben Gezeigten:

$$0 = \mathfrak{J}_\varkappa \mathfrak{S} = \binom{\varkappa}{i} \mathfrak{J}_i \mathfrak{S}, \quad \mathfrak{J}_{\varkappa-i} \mathfrak{S} = \binom{\varkappa}{i} \mathfrak{S}^* \mathfrak{S}^* = \binom{\varkappa}{i} \mathfrak{S}^*.$$

Also sind die Binomialkoeffizienten  $\binom{\varkappa}{1}, \binom{\varkappa}{2}, \dots, \binom{\varkappa}{\varkappa-1}$  teilbar durch die Charakteristik von  $\mathfrak{S}^*$ . Aus Hilfssatz 3 folgt, daß die Charakteristik von  $\mathfrak{S}^*$  eine Primzahl  $p$  und daß  $\varkappa = p^\mu$  ist ( $\mu \geq 1$ ).

Die Gleichungen (43) fassen wir kurz in folgender Weise zusammen:

(43 a) Zu jedem  $\varkappa$ -tupel von Elementen  $a_0, a_1, \dots, a_{\varkappa-1}$  aus  $\mathfrak{S}^*$  gibt es genau ein Element von der Form  $(a_0, a_1, \dots, a_{\varkappa-1}, \dots)$  in  $\mathfrak{S}$ . Das wird auf dieselbe Weise wie Hilfssatz 2 bewiesen. Wenn also  $0 < j < \varkappa$  und  $a$  ein beliebiges Element aus  $\mathfrak{S}^*$ , so gibt es genau

ein Element von der Form  $(0 \dots 0, a, 0 \dots 0, \dots)$  in  $\mathfrak{S}$ . Setzen wir seine Komponenten in die Gleichung (41) mit  $\nu = m - j$  ein, so folgt

$$\binom{m}{j} \mathfrak{S}^* = 0 \quad (j = 1, 2, \dots, \varkappa - 1)$$

$$p \Big/ \binom{m}{j}.$$

Sei  $p^{\mu'}$  die höchste in  $m$  aufgehörende  $p$ -Potenz. Im Beweis des Hilfssatzes 3 ist gezeigt worden, daß  $\binom{m}{p^{\mu'}}$  nicht durch  $p$  teilbar ist.

Also ist  $\mu' \geq \mu$ .  $\varkappa$  ist Teiler von  $m$ , etwa  $m = \varkappa m_0$ .

5. Wenn  $m_0 = 1$ , so ist nach Hilfssatz 2  $\mathfrak{S} = \mathfrak{S}^{*(m)}$ .

6. Sei weiterhin  $m_0 > 1$ . Für jedes Element  $a$  aus  $\mathfrak{S}^*$  gibt es genau ein Element aus  $\mathfrak{S}$  von der Form

$$A = (0 \dots 0, a, \tau_1 a, \tau_2 a, \dots, \tau_{\varkappa-1} a, \dots).$$

Jetzt wird gezeigt, daß  $\tau_i a = 0$  ( $i = 1, 2, \dots, \varkappa - 1$ ). Es ist nämlich  $i = i' p^{\mu'}$ , wobei  $p$  nicht mehr in  $i'$  aufgeht und  $0 \leq \mu' < \mu$ . In  $\mathfrak{S}$  liegt zu jedem Element  $b$  aus  $\mathfrak{S}^*$  ein Element

$$B = (0 \dots 0, b, 0 \dots 0, \dots).$$

Es ist

$$AB = \left( 0 \cdots 0, \dots \binom{x+i-1+p^\mu}{p^{\mu'}} (x_i a) \cdot b, \dots \right).$$

Da  $AB$  in  $\mathfrak{S}$  enthalten ist und  $\theta_k \mathfrak{S} = 0$ , so ist

$$\binom{x+i+p^{\mu'}-1}{p^{\mu'}} (x_i a) \mathfrak{S}^* = 0.$$

Es ist aber

$$\binom{x+i+p^{\mu'}-1}{p^{\mu'}} \equiv \binom{i+p^{\mu'}-1}{p^{\mu'}} = i' \binom{i' p^{\mu'} + p^{\mu'} - 1}{p^{\mu'} - 1} \not\equiv 0(p),$$

also folgt:  $(x_i a) \mathfrak{S}^*$  und nach Hilfssatz 4 folgt  $\tau_i a = 0$ . Demnach hat  $A$  die Form

$$A = (0 \cdots 0, a, 0 \cdots 0, \tau a, \dots).$$

Dabei ist  $\tau$  eine eindeutige Abbildung von  $\mathfrak{S}^*$  in sich. Ferner ist nach (26) zu jedem  $a$  aus  $\mathfrak{S}^*$  ein Element von der Form

$$A = (0 \cdots 0, a, 0 \cdots 0, \tau a, \dots)$$

in  $\mathfrak{S}$  enthalten. Sei nun  $(a_0, a_1, \dots, a_{x-1}, \dots)$  ein beliebiges Element aus  $\mathfrak{S}$ , dann gibt es Elemente  $A_i$  von der Form

$$A_i = (0 \cdots 0, a_i, 0 \cdots 0, \tau a_i, \dots) \quad (i = 0, 1, 2, \dots, x-1)$$

in  $\mathfrak{S}$ . Da die ersten  $x$ -Komponenten des Elementes  $A = (A_0 + A_1 \cdots + A_{x-1})$  aus  $\mathfrak{S}$  verschwinden, so ist es Null, also  $A = A_0 + A_1 \cdots + A_{x-1}$ . Demnach hat  $A$  die Form

$$A = (a_0, a_1, \dots, a_{x-1}, \tau a_0, \dots).$$

Nach (26) ist

$$(44) \quad \bar{\sigma}^i A = (a_i, a_{i+1}, \dots, a_{m+i-1})$$

und nach dem eben Gezeigten folgt

$$(45) \quad a_{i+x} = \tau a_i.$$

Wenn wir nur voraussetzen, daß  $1 \leq x < m$ , so gibt es zu jedem  $a$  aus  $\mathfrak{S}^*$  genau ein Element von der Form  $A = (a, 0 \cdots 0, \tau a, \dots)$ . Also wird durch  $\tau$  eine eindeutige Abbildung von  $\mathfrak{S}^*$  in sich definiert, die ersichtlich den Regeln

$$(46) \quad \tau(a+b) = \tau a + \tau b,$$

$$(47) \quad \tau(\lambda a) = \lambda \tau a$$

genügt. Ist  $b$  ein zweites Element aus  $\mathfrak{S}^*$ , so gibt es ein Element  $B$  von der Form  $(b, 0 \dots 0, \overset{x}{\tau} b, \dots)$  in  $\mathfrak{S}$ . Dann ist:

$$AB = (ab, 0 \dots 0, a \cdot \overset{x}{\tau} b + \tau a \cdot b, \dots) \in \mathfrak{S},$$

also

$$a \cdot \overset{x}{\tau} b + \tau a \cdot b = \tau(a b).$$

Wenn  $x = 1$ , so lehrt die Formel (45), daß  $\mathfrak{S}$  aus dem  $m$ -tupeln  $(a, \tau a, \dots, \tau^{m-1} a)$  mit  $a \in \mathfrak{S}^*$  besteht.

Als Ergebnis haben wir erhalten:

**Satz 8:** Der  $k$ -Schiefring  $\mathfrak{S}$  hat einen der drei folgenden Typen:

- I.  $\mathfrak{S}$  besteht aus allen  $m$ -tupeln  $(a, \tau a, \tau^2 a, \dots, \tau^{m-1} a)$  mit  $a$  aus  $\mathfrak{S}^*$ , wobei  $m > 1$ .
- II. Die Charakteristik von  $k$  ist eine Primzahl  $p$ .  $\mathfrak{S}$  besteht aus allen  $m$ -tupeln

$$(a_0, a_1, \dots, a_{x-1}, \tau a_0, \tau a_1, \dots, \tau a_{x-1}, \dots, \tau^{m_0-1} a_0, \dots, \tau^{m_0-1} a_{x-1})$$

mit Komponenten  $a_0, a_1, \dots, a_{x-1}$  aus  $\mathfrak{S}^*$ , wobei

$$x = p^\mu (\mu > 0), \quad m = m_0 x (m_0 > 1).$$

- III.  $\mathfrak{S} = \mathfrak{S}^{*(m)}$ , wobei entweder  $m = 1$  oder die Charakteristik von  $k$  ist eine Primzahl  $p$ , und es ist  $m = p^\mu (\mu > 0)$ .

Dabei ist  $\tau$  eine lineare Transformation des  $k$ -Moduls  $\mathfrak{S}^*$ , die der Funktionalgleichung  $\tau(ab) = a \cdot \tau b + \tau a \cdot b$  genügt.

7. Jetzt wollen wir zusätzlich voraussetzen, daß der Grundkörper  $k$  algebraisch abgeschlossen ist.  $\mathfrak{S}^*$  ist ein einfaches hyperkomplexes System über  $k$ , also ein Matrizenring, und da  $m$  eine treue irreduzible Darstellung von  $\mathfrak{S}^*$  vermittelt, so besteht  $\mathfrak{S}^*$  aus allen linearen Transformationen von  $m$ .

Jetzt prüfen wir, ob unter den getroffenen Voraussetzungen die Typen I und II des Satzes 8 überhaupt vorkommen können. Nach I, Satz 20 ist

$$\tau a = a \cdot t$$

mit festem  $t$  aus  $\mathfrak{S}^*$ . Da  $\tau_i t = 0$  ( $i = 1, 2, \dots, m-1$ ), so ist  $T = (t, 0 \dots 0)$  in  $\mathfrak{S}$  enthalten. Jedes Element aus  $\mathfrak{S}$  hat eindeutig die Form

$$A = (a_0, a_1, \dots, a_{x-1}, \tau a_0, \tau a_1, \dots, \tau a_{x-1}, \dots),$$

wobei im Falle I  $x = 1$  gesetzt ist. Da nun

$$A \circ T = (a_0 \circ t, a_1 \circ t, \dots, a_{x-1} \circ t, \dots)$$

und nach (26):

$$\bar{\sigma}^x A = (\tau a_0, \tau a_1, \dots, \tau a_{x-1}, \dots),$$

so folgt:  $A \circ T = \bar{\sigma}^x A$ . Im Falle II folgt nach I, § 4, (13) aus  $\bar{\sigma} A = A \circ s$  und aus  $x = p^\mu$ , daß  $\bar{\sigma}^x A = A \circ s^x$ . Im Falle I ist ebenfalls  $\bar{\sigma}^x A = \bar{\sigma} A = A \circ s = A \circ s^x$ . Demnach ist in beiden Fällen

$$A \circ (s^x - T) = 0$$

für alle  $A$  aus  $\mathfrak{S}$ .

Da  $k$  algebraisch abgeschlossen, so gibt es ein von Null verschiedenes Element  $u$  aus  $\mathfrak{M}$ , so daß  $s'u = \lambda u$ , wobei  $s' = s^x - T$  gesetzt ist.  $\mathfrak{M}_1$  sei der  $k$ -Modul, bestehend aus allen Vektoren  $u$ , für die  $s'u = \lambda u$ . Da  $s'$  mit  $\mathfrak{S}$  elementweise vertauschbar ist, so ist  $\mathfrak{M}_1$  unter  $\mathfrak{S}$  invariant. Da  $\mathfrak{M}_1 \neq 0$ , so enthält  $\mathfrak{M}_1$  einen irreduziblen  $\mathfrak{S}$ -Modul  $m'$ . Für alle  $v'$  aus  $m'$  ist:

$$s^x v' = s' v' + T v' = \lambda v' + T v' \in m'.$$

Also ist  $\mathfrak{M}' = m' + s m' \dots s^{x-1} m'$  unter  $s$  invariant. Wie früher folgt nach Hilfssatz 1, daß  $\mathfrak{M}'$  unter  $\mathfrak{S}$  invariant ist. Da nun  $\mathfrak{M}$  ein irreduzibler  $(\mathfrak{S}, \sigma)$ -Modul, so ist  $\mathfrak{M}' = \mathfrak{M}$ . Wie im § 1 folgt hieraus, daß der  $\mathfrak{S}$ -Modul  $\mathfrak{M}$  höchstens  $x$  Kompositionsfaktoren besitzt, während doch nach Satz 1 die Anzahl in Wirklichkeit  $m$ , also größer als  $x$  ist.

Demnach ist in Satz 8 bei algebraisch abgeschlossenem Grundkörper nur der Typus III möglich.

Dieser Typus wird unter der Annahme  $m > 1$  weiter untersucht. Jetzt wenden wir auf  $\mathfrak{S}$  die Überlegungen des § 3 an. Wir stellen fest, daß  $N\mathfrak{S}^* = \mathfrak{S}^*$ . Da  $k$  algebraisch abgeschlossen, so ist  $Z(S^*) = Z_0(S^*) = k \cdot 1$ . Also ist  $s_j = \underline{0}$ , wenn  $j \neq 0, 1, p, \dots, p^{\mu-1}$

$$s_{p^i} = \mu_i \cdot \underline{1} \quad (i = 1, 2, \dots, \mu - 1).$$

Setzen wir nun

$$(48) \quad f(\xi) = x^{p^\mu} - \sum_{i=0}^{x-1} \mu_i x^{p^i},$$

so folgt

$$(49) \quad (f(\sigma) a)^* = a^* \circ s_0.$$

**Satz 9:** *Das in (48) definierte Polynom  $f(\xi)$  ist unter allen Polynomen*

$$(49) \quad g(\xi) = \xi^{p^\lambda} - \sum_{i=0}^{\lambda-1} \lambda_i \xi^{p^i} \quad (\lambda \geq 0; \text{ wenn } \lambda = 0, \text{ so } \lambda_0 = 0)$$

für die es eine lineare Transformation  $x$  von  $m$  gibt, so daß

$$(50) \quad (g(\sigma) a)^* = a^* \circ x$$

für alle  $a$  aus  $L$ , eindeutig bestimmt als das Polynom niedrigsten Grades, dessen höchster Koeffizient 1 ist.

Beweis: Man setze  $\bar{\sigma}A = A \circ s$  für alle  $A$  aus  $\mathfrak{S}$ . Nach I, § 4, (13) ist  $\sigma^p A = A \circ s^p$ , also  $g(\bar{\sigma})A = A \circ g(s)$ . Nun setzen wir:

$$\varrho A = (A \circ g(s))^* - A^* \circ x.$$

Nach (50) folgt nun:  $\varrho \bar{a} = 0$  für alle  $a$  aus  $L$ . Ferner ist ersichtlich:

$$\varrho(A+B) = \varrho A + \varrho B, \quad \varrho(\lambda A) = \lambda \varrho A, \quad \varrho(AB) = A \cdot \varrho B + \varrho A \cdot B.$$

Da nun  $\mathfrak{S}$  aus  $\bar{L}$  erzeugt wird, so folgt  $\varrho A = 0$  für alle  $A$  aus  $\mathfrak{S}$ , d. h.:

$$(50a) \quad (g(\bar{\sigma})A)^* = A^* \circ x.$$

Sei  $A = (a_0, a_1, \dots, a_{m-1})$  ein Element aus  $\mathfrak{S}$ , dann lautet (50a) auf Komponenten umgerechnet:

$$(51) \quad a_{p\lambda} = a_0 \circ x + \sum_{i=0}^{\lambda-1} \lambda_i a_{p^i}.$$

Wenn hier  $\lambda < \mu$ , so liegt für beliebiges  $a$  aus  $\mathfrak{S}^*$  das Element  $(0 \dots 0, \overset{p^\lambda}{a}, 0 \dots 0)$  in  $\mathfrak{S}$ . Setzen wir seine Komponenten ein in (51), so folgt  $a = 0$ , was der Voraussetzung  $\mathfrak{S}^* \neq 0$  widerspricht.

Wenn aber  $\lambda = \mu$ , so folgt aus (49), daß

$$a_{p\mu} = a_0 \circ s_0 + \sum_{i=0}^{\mu-1} \mu_i a_{p^i},$$

also

$$0 = a_0 \circ (s_0 - x) + \sum_{i=0}^{\mu-1} (\mu_i - \lambda_i) a_{p^i}.$$

Da für  $a_0, a_1, a_p, \dots, a_{p^{\mu-1}}$  ganz beliebige Kombinationen von  $\mu$  Elementen aus  $\mathfrak{S}^*$  eingesetzt werden durften, so folgt  $(\mu_i - \lambda_i) \mathfrak{S}^* = 0$  und da  $\mathfrak{S}^* \neq 0$ , so ist

$$\mu_i = \lambda_i \quad (0 \leq i < \mu),$$

w. z. b. w.

Im Anschluß an den Satz 9 wollen wir noch beweisen, daß  $f(\xi)$  Teiler von jedem der Polynome  $g(\xi)$  ist. Es sei  $\mathfrak{H}$  die Menge aller Polynome

$$h(\xi) = \sum_{i=0}^n \alpha_i \xi^{p^i} \quad (\alpha_i \in k),$$

zu denen es eine lineare Transformation  $x$  gibt, so daß

$$(h(\sigma)a)^* = a^* \circ x$$

für alle  $a$  aus  $L$ . Es ist klar, daß  $\mathfrak{H}$  ein  $k$ -Modul ist. Wir zeigen, daß das Potenzieren mit  $p$  nicht aus  $\mathfrak{H}$  hinausführt.

Man setze  $\tau y = yx - xy = y \circ x$  für alle linearen Transformationen  $y$  von  $\mathfrak{M}$ . Es ist  $(h(\sigma)a)^* = \tau a^*$ . Sei schon bewiesen, daß  $(h(\sigma)^i a)^* = \tau^i a^*$ . Dann folgt

$$(h(\sigma)^{i+1} a)^* = (h(\sigma)(h(\sigma)^i a))^* = \tau(h(\sigma)^i a)^* = \tau(\tau^i a^*) = \tau^{i+1} a^*.$$

Nach  $p$  Schritten folgt:

$$(h(\sigma)^p a)^* = \tau^p a^*.$$

Da  $\tau^p a^* = a^* \circ x^p$ , so führt das Potenzieren mit  $p$  nicht aus  $\mathfrak{S}$  hinaus.

Unsere Behauptung folgt nun aus dem

**Hilfssatz 6:** *k sei ein Körper mit Primzahlcharakteristik  $p$ ,  $\mathfrak{S}$  sei ein nicht leerer  $k$ -Modul von Polynomen der Gestalt*

$$(52) \quad \sum_{i=0}^x x^i \xi^{p^i} \quad (x_i \in k),$$

in dem mit  $h$  auch  $h^p$  enthalten ist. Dann besteht  $\mathfrak{S}$  aus allen Polynomen

$$(53) \quad h(\xi) = P(f(\xi)),$$

wobei  $f(\xi)$  ein festes Polynom von der Gestalt (52) ist und  $P$  alle Polynome von der Gestalt (52) durchläuft.

Beweis: Wenn  $\mathfrak{S} = 0$ , so setze man  $f(\xi) = 0$ , dann ist der Satz bewiesen. Wenn  $\mathfrak{S}$  von Null verschiedene Polynome enthält, so gibt es in  $\mathfrak{S}$  ein Polynom  $f(\xi)$  niedrigsten Grades, etwa vom Grade  $p^\mu$ . Wir normieren  $f(\xi)$  noch so, daß der höchste Koeffizient 1 wird. Für ein Polynom  $g(\xi)$  vom Grade  $p^\mu$  mit höchstem Koeffizienten  $\alpha$  folgt nach Konstruktion von  $f(\xi)$ , daß  $g(\xi) - \alpha f(\xi) = 0$ , also  $g(\xi) = Q(f(\xi))$  mit  $Q(\xi) = \alpha \xi$ . Ferner ist  $0 = P(f(\xi))$  mit  $P(\xi) = 0$ . Es sei schon bewiesen, daß sich alle Polynome aus  $\mathfrak{S}$ , deren Grad höchstens  $p^{x-1}$  ist, in der Gestalt (53) ausdrücken lassen.  $h(\xi)$  sei ein Polynom aus  $H$  vom Grade  $p^x$  und mit dem höchsten Koeffizienten  $\beta$ . Dann hat  $\beta \cdot f(\xi)^{p^{x-\mu}}$  ebenfalls den Grad  $p^x$  und den höchsten Koeffizienten  $\beta$  und ist in  $\mathfrak{S}$  enthalten. Die Differenz  $h(\xi) - \beta f(\xi)^{p^{x-\mu}}$  ist in  $\mathfrak{S}$  enthalten und hat höchstens den Grad  $p^{x-1}$ , also ist nach Induktionsvoraussetzung

$$h(\xi) - \beta f(\xi)^{p^{x-\mu}} = P_0(f(\xi)),$$

wobei  $P_0(\xi)$  die Form (52) hat. Dann hat  $P(\xi) = P_0(\xi) + \beta \xi^{p^{x-\mu}}$  ebenfalls die Form (52), und es ist  $h(\xi) = P(f(\xi))$ . Demnach lassen sich alle Polynome aus  $\mathfrak{S}$  in der Gestalt (53) ausdrücken.

Die Umkehrung des Satzes ist klar.

Wir bemerken noch, daß bei gegebenem Polynom  $f(\xi)$  die lineare Transformation  $s_0$  bis auf ein skalares Vielfaches der identischen

Transformation als additives Zusatzglied eindeutig bestimmt ist, weil  $Z(L^*) = k \cdot 1$ . Ferner haben wir früher bewiesen, daß es bei Primzahlcharakteristik von  $k$  stets irreduzible  $(L, \sigma)$ -Moduln gibt, die einen vorgegebenen endlichen irreduziblen  $L$ -Modul enthalten. So haben wir als Ergebnis erhalten:

**Satz 10:** Gegeben sei ein  $r$ -gliedriger Lie'scher Ring  $L$  über algebraisch abgeschlossenem Koeffizientenkörper  $k$ , ferner ein Endomorphismus  $\sigma$  von  $L$  und ein endlicher, irreduzibler  $L$ -Modul  $\mathfrak{m}$ . Gesucht sind die endlichen irreduziblen  $(L, \sigma)$ -Moduln  $\mathfrak{M}$ , die als  $L$ -Modul betrachtet, den  $L$ -Modul  $\mathfrak{m}$  enthalten.

Wenn die Charakteristik von  $k$  Null ist, so müssen  $\mathfrak{M}$  und  $\mathfrak{m}$  übereinstimmen, und die Aufgabe ist dann und nur dann lösbar, wenn es eine lineare Transformation  $s$  von  $\mathfrak{m}$  gibt, so daß durchweg gilt:

$$(\sigma a)v = (as - sa)v \quad (a \in L; v \in \mathfrak{m}).$$

Wenn die Charakteristik von  $k$  eine Primzahl  $p$  ist, so ist die Aufgabe stets lösbar. Alle Moduln  $\mathfrak{M}$  werden durch die folgende Konstruktion erhalten: Zwischen den  $r + 1$  linearen Transformationen  $\sigma, \sigma^p, \dots, \sigma^{p^r}$  des  $r$ -gliedrigen  $k$ -Moduls  $L$  besteht eine nichttriviale lineare Relation, die sich auf die Form  $\sigma^{p^r} = \sum_0^x \alpha_i \sigma^{p^i}$  bringen läßt. Unter den endlich vielen Teilern des Polynomes  $g(\xi) = \xi^{p^r} - \sum_{i=0}^{x-1} \alpha_i \xi^{p^i}$  von der Gestalt  $h(\xi) = \xi^{p^\lambda} - \sum_{i=0}^{\lambda-1} \lambda_i \xi^{p^i}$ , für die  $(h(\sigma)a)^* = a^* \circ x$  durch eine lineare Transformation  $x$  von  $\mathfrak{m}$  lösbar ist, sei  $f(\xi) = \xi^{p^\mu} - \sum_{i=0}^{\mu-1} \mu_i \xi^{p^i}$  dasjenige von kleinstem Grade. Es sei etwa  $(f(\sigma)a)^* = a^* \circ s_0$ . In dem gemäß der Vorschrift des § 3 konstruierten  $L$ -Modul  $\mathfrak{M} = \mathfrak{m}^{(m, \sigma)}$  werde die lineare Transformation  $s$  definiert durch die Regeln:

$$(54) \quad \begin{aligned} s(s^i v) &= s^{i+1} v \quad (i = 0, 1, 2, \dots, m-2), \\ s(s^{m-1} v) &= s_0 v + \sum_{i=0}^{x-1} \mu_i s^{p^i} v. \end{aligned}$$

Dann ist  $\mathfrak{M}$  ein irreduzibler  $(L, \sigma)$ -Modul, der als  $L$ -Modul betrachtet den  $L$ -Modul  $\mathfrak{m}$  enthält. Die einzige Willkür in der Konstruktion von  $\mathfrak{M}$  besteht in der Ersetzung von  $s_0$  durch  $s_0 + \lambda \cdot 1$  mit beliebigen  $\lambda$  aus  $k$ .

**Satz 11:** Wenn der Endomorphismus  $\sigma$  des vorigen Satzes nilpotent ist, dann sind alle Eigenwerte der linearen Transformation  $s$  einander gleich. Zu jedem vorgeschriebenen Eigenwert von  $s$  gibt es genau einen irreduziblen  $(L, \sigma)$ -Modul, der als  $L$ -Modul betrachtet den vorgegebenen irreduziblen  $L$ -Modul  $\mathfrak{m}$  enthält.



Beweis: Jedenfalls gilt  $\sigma^r = 0$ . Es sei  $p^q$  die erste Potenz von  $p$ , die nicht kleiner als  $r$  ist, dann ist  $\sigma^{p^q} = 0$ . Das Polynom  $f(\xi)$ , das bei der Konstruktion der irreduziblen  $(L, \sigma)$ -Moduln auftritt, hat  $p$ -Potenzgrad und ist Teiler von  $\xi^{p^q}$ . Also ist  $f(\xi) = \xi^{p^\mu}$  ( $0 \leq \mu \leq q$ ). Daher haben wir die Gleichung  $(\sigma^{p^\mu} a)^* = a^* \circ s_0$  ( $a \in L$ ). Wie früher folgt hieraus  $0 = (\sigma^{p^q} a)^* = a^* \circ s_0^{p^{q-\mu}}$ . Die lineare Transformation  $s_0^{p^{q-\mu}}$  liegt in  $Z(L^*)$  und da  $k$  algebraisch abgeschlossen, so ist  $s_0^{p^{q-\mu}} = \gamma \cdot 1$ . Wir setzen  $\beta = \gamma^{p^{\mu-q}}$  und erhalten

$$(s_0 - \beta \cdot \underline{1})^{p^{q-\mu}} = s_0^{p^{q-\mu}} - \gamma \cdot \underline{1} = \underline{0}.$$

Demnach besitzt die lineare Transformation  $s_0$  nur den einen Eigenwert  $\beta$ . Nun ist nach (54)  $s^{p^\mu} v = \varrho_0 v$  für alle  $v$  aus  $m$ . Also

$$s^{p^q} v = s_0^{p^{q-\mu}} v = \gamma v, \quad s^{p^q} \cdot s_i v = \gamma s_i v \quad (i = 0, 1, 2, \dots, p^{-1}),$$

also

$$s^{p^q} = \gamma \cdot \underline{1}.$$

Setzen wir nun  $\alpha = \gamma^{p^{-q}}$ , so folgt

$$(s - \alpha \cdot \underline{1})^{p^q} = s^{p^q} - \gamma \cdot \underline{1} = \underline{0}.$$

Die lineare Transformation  $s$  von  $\mathfrak{M}$  besitzt nur den einen Eigenwert  $\alpha$ . Fordern wir jetzt, daß umgekehrt  $s$  den Eigenwert  $\alpha$  haben soll, dann muß  $s_0$  den Eigenwert  $\beta = \alpha^{p^\mu}$  haben und durch diese Forderung ist  $s_0$  eindeutig bestimmt. Nämlich nach Satz 10 sind nur die Abänderungen  $s_0 \rightarrow s_0 + \delta \cdot \underline{1}$  erlaubt, dabei geht aber der Eigenwert  $\beta$  von  $s_0$  über in  $\beta + \delta$ . Also ist keine Abänderung mehr zulässig. Damit ist der Satz vollständig bewiesen.

### § 6. Eine Identität.

Wir wollen zeigen, daß in jedem Schieferring, dessen Charakteristik eine Primzahl  $p$  ist, die Identität

$$(55) \quad (x + y)^p = x^p + y^p + \mathcal{A}_p(x, y)$$

gilt, in der  $\mathcal{A}_p(x, y)$  eine gewisse Summe aus Kreisprodukten mit je  $p$  Faktoren, die entweder  $x$  oder  $y$  sind, ist.

Es sei  $\mathfrak{F}$  der Potenzreihenring in zwei nichtkommutativen Variablen  $x, y$  über dem Koeffizientenbereich  $\mathfrak{o}$  der ganzen rationalen Zahlen.  $\mathfrak{F}_n$  sei das  $n$ -te MAGNUSsche Dimensionsideal, bestehend aus allen Potenzreihen, in denen nur Potenzprodukte aus mindestens  $n$  Faktoren  $x$  oder  $y$

vorkommen.  $\mathcal{W}_1$  sei der von  $x$  und  $y$  erzeugte  $\mathfrak{o}$ -Modul.  $\mathcal{W}_2$  sei der von  $x \circ y = xy - yx$  erzeugte  $\mathfrak{o}$ -Modul, allgemein sei  $\mathcal{W}_n$  der von allen Kreisprodukten mit  $n$  Faktoren, die gleich  $x$  oder  $y$  sind, erzeugte  $\mathfrak{o}$ -Modul.

$\mathfrak{F}$  sei die von den Potenzreihen

$$\begin{aligned} s_1 &= 1 + x, & s_1^{-1} &= 1 - x + x^2 - x^3 \dots, \\ s_2 &= 1 + y, & s_2^{-1} &= 1 - y + y^2 - y^3 \dots \end{aligned}$$

erzeugte multiplikative Gruppe.  $\mathfrak{F}_n$  sei die  $n$ -te MAGNUSsche Dimensionsgruppe, bestehend aus allen Potenzreihen aus  $\mathfrak{F}$ , die mod  $\mathfrak{P}_n$  der 1 kongruent sind (deren „Anfangsglied“ mindestens die Dimension  $n$  hat).

MAGNUS hat bewiesen<sup>1)</sup>, daß

1.  $\mathfrak{F}$  die freie Gruppe aus den zwei Erzeugenden  $s_1, s_2$  ist,
2. als Glieder  $n$ -ter Dimensionen der Potenzreihen aus  $\mathfrak{F}_n$  genau die Elemente aus  $\mathcal{W}_n$  auftreten,
3.  $\mathfrak{F}_n$  gleich dem  $n$ -ten Gliede der absteigenden Zentralreihe von  $\mathfrak{F}$  ist,
4. hat MAGNUS einen neuen Beweis der HALLSchen Identität

$$(56) \quad (s_1 s_2)^p = s_1^p s_2^p Z_2^p Z_3^p \dots Z_{p-1}^p Z_p$$

gegeben, in der  $p$  eine Primzahl und  $Z_i$  in  $\mathfrak{F}_i$  enthalten ist.

Das Multiplizieren der Elemente aus  $\mathfrak{P}$  mit  $p$  ist ein Operator  $\underline{p}$ , der  $\mathfrak{P}$  auf ein Ideal  $\underline{p}\mathfrak{P}$  abbildet. Da die Binomialkoeffizienten  $\binom{p}{1}$ ,  $\binom{p}{2}, \dots, \binom{p}{p-1}$  alle durch  $p$  teilbar sind, so gelten die Kongruenzen:

$$\begin{aligned} s_1^p &= (1+x)^p \equiv 1 + x^p (\underline{p}\mathfrak{P} + \mathfrak{P}_{p+1}), \\ s_2^p &\equiv 1 + y^p (\underline{p}\mathfrak{P} + \mathfrak{P}_{p+1}), \\ (s_1 s_2)^p &= (1+(x+y)+xy)^p \equiv 1 + (x+y)^p (\underline{p}\mathfrak{P} + \mathfrak{P}_{p+1}), \end{aligned}$$

da

$$Z_i \equiv 1 (\mathfrak{P}_i) \quad (i = 2, 3, \dots, p-1),$$

so folgt

$$Z_p^p \equiv 1 (\underline{p}\mathfrak{P} + \mathfrak{P}_{p+1}).$$

Schließlich folgt nach dem zweiten Resultat von MAGNUS, daß

$$Z_p \equiv 1 + \mathcal{A}_p(x, y) (\mathfrak{P}_{p+1}),$$

wobei  $\mathcal{A}_p(x, y)$  in  $\mathcal{W}_p$  liegt.

<sup>1)</sup> W. MAGNUS, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. Math. Ann., Bd. 111, 2, S. 259—280. Ferner: Über Beziehungen zwischen höheren Kommutatoren. Crelle, Bd. 177, 2, S. 105—115.

Jetzt folgt aus der HALLSchen Identität die Kongruenz:

$$(x + y)^p \equiv x^p + y^p + \mathcal{A}_p(x, y) (\underline{p}\mathfrak{B} + \mathfrak{B}_{p+1})$$

und da auf beiden Seiten der Kongruenz nur homogene Polynome  $p$ -ten Grades stehen, so folgt eine Identität der Gestalt:

$$(57) \quad (x + y)^p = x^p + y^p + \mathcal{A}_p(x, y) + p P(x, y),$$

in der  $P(x, y)$  ein homogenes Polynom  $p$ -ten Grades in  $x$  und  $y$  mit ganzzahligen Koeffizienten ist.

Daher gilt in jedem Schieferring mit der Charakteristik  $p$  die Identität (55).

E. ARTIN hat mir den folgenden direkten Beweis der Identität (55) mitgeteilt, den ich mit seiner freundlichen Erlaubnis hier veröffentliche.

$\mathfrak{Q}$  sei der Polynombereich zweier nichtkommutativer Variablen  $x$  und  $y$  über dem Körper  $k$  aus  $p$  Elementen. In dem Polynombereich  $\mathfrak{Q}[t]$  einer Variablen  $t$  über  $\mathfrak{Q}$  wird das Differenzieren durch die Festsetzung

$$\frac{d}{dt} \left( \sum_{i=0}^m P_i(x, y) t^i \right) = \sum_{i=0}^m i P_i(x, y) t^{i-1}$$

erklärt. Dann gelten die Rechenregeln:

$$\begin{aligned} \frac{d}{dt} (P(x, y)) &= 0, & \frac{dt}{dt} &= 1, \\ \frac{d}{dt} (f(t) + g(t)) &= \frac{d}{dt} (f(t)) + \frac{d}{dt} g(t), \\ \frac{d}{dt} (f(t) \cdot g(t)) &= f(t) \cdot \frac{dg(t)}{dt} + \frac{df(t)}{dt} \cdot g(t). \end{aligned}$$

Man berechne die Ableitung von  $(xt + y)^p$  auf zwei Weisen und setze in der entstehenden Identität für  $t$  den Wert 1 ein!

Das Differenzieren der Potenzen von  $z = xt + y$  geschieht nach der Regel:

$$(58) \quad \frac{d}{dt} (z^m) = \sum_{i=1}^m \binom{m}{i} (\zeta^{i-1} x) z^{m-i},$$

wobei

$$\zeta u = z \circ u, \quad \zeta^0 u = u, \quad \zeta^{i+1} u = \zeta (\zeta^i u)$$

gesetzt ist. Der Beweis wird durch vollständige Induktion erbracht.

Es ist  $\frac{d}{dt} (z) = x$ , also die Formel (58), für  $m = 1$  richtig. Ist sie

schon für den Exponenten  $n$  bewiesen, so folgt:

$$\begin{aligned} \frac{d}{dt}(z^{n+1}) &= \frac{d}{dt}(z \cdot z^n) = xz^n + z \cdot \frac{d}{dt}(z^n) \\ &= xz^n + \sum_1^n \binom{n}{i} z(\zeta^{i-1}x) z^{n-i}. \end{aligned}$$

Da nun

$$z(\zeta^{i-1}x) = \zeta(\zeta^{i-1}x) + (\zeta^{i-1}x)z,$$

so folgt:

$$\begin{aligned} \frac{d}{dt}(z^{n+1}) &= \sum_{i=0}^n \binom{n}{i} (\zeta^i x) z^{n-i} + \sum_{i=1}^n \binom{n}{i} (\zeta^{i-1} x) z^{n+1-i} \\ &= \zeta^n x + \sum_{i=1}^n \binom{n}{i-1} (\zeta^{i-1} x) z^{n+1-i} \\ &\quad + \sum_{i=1}^n \binom{n}{i} (\zeta^{i-1} x) z^{n+1-i} \\ &= \sum_{i=1}^{n+1} \binom{n+1}{i} (\zeta^{i-1} x) z^{n+1-i} \end{aligned}$$

Also gilt die Formel allgemein.

Für  $\zeta^m x$  wird durch vollständige Induktion die Formel:

$$(59) \quad \zeta^m x = \sum_{i=1}^{m-1} A_{m,i}(x, y) t^{i-1} \quad (m > 1)$$

bewiesen, worin  $A_{m,i}(x, y)$  die Summe über alle Kreisprodukte von der Form  $x_i \circ (x_2 \circ (x_3 \circ \dots (x_{m-1} \circ x_m) \dots))$  mit  $i$  Faktoren  $x$ ,  $m-i$  Faktoren  $y$  und der Bedingung  $x_m = x$ . Da die Binomialkoeffizienten  $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$  durch  $p$  teilbar sind, so folgt:

$$(60) \quad \frac{d}{dt}(z^p) = \zeta^{p-1} x = \sum_{i=1}^{p-1} A_{p,i}(x, y) t^{i-1}.$$

Andererseits ist

$$z^p = (xt + y)^p = x^p t^p + y^p + \sum_{i=1}^{p-1} P_i(x, y) t^i,$$

$$(61) \quad \frac{d}{dt}(z^p) = \sum_{i=1}^{p-1} i P_i(x, y) t^{i-1}.$$

Vergleich von (60) und (61) ergibt:

$$P_i(x, y) = \frac{1}{i} A_{p,i}(x, y) \quad (i = 1, 2, \dots, p-1).$$

$$(xt + y)^p = x^p t^p + y^p + \sum_{i=1}^{p-1} \frac{1}{i} A_{p,i}(x, y) t^i.$$

Wird in dieser Polynomidentität für  $t$  der Wert 1 eingesetzt, so folgt:

$$(x + y)^p = x^p + y^p + A_p(x, y),$$

wobei

$$A_p(x, y) = \sum_{i=1}^{p-1} A_{p,i}(x, y)$$

gesetzt ist.

In einem beliebigen Ring  $P$  mit Charakteristik  $p$  folgt

$$(62) \quad (\xi x + \eta y)^p = \xi^p x^p + \eta^p y^p + \sum_{i=1}^{p-1} \frac{1}{i} \xi^i \eta^{p-i} A_{p,i}(x, y),$$

wobei  $\xi, \eta$  aus  $P$  stammen.

Nun sei  $\Omega$  der Polynombereich der nichtkommutativen Variablen  $x_1, x_2, x_3, \dots, x_n$  über  $\mathfrak{o}$ .  $\Psi_m$  sei der aus allen Kreisprodukten mit  $m$  Faktoren, die jeweils gleich einer der Variablen  $x_i$  sind, durch Addition erzeugte Modul. Als Verallgemeinerung der Identität (62) soll jetzt bewiesen werden, daß Identitäten von der Form

$$(63) \quad \left( \sum_{i=1}^n \xi_i x_i \right)^{p^\nu} = \sum_{i=0}^{\nu} \sum_{(p^i; \mu)} (\xi^{(p^i; \mu)})^{p^{\nu-i}} A_{(p^i; \mu)}^{p^{\nu-i}}(x) \quad (\nu = 0, 1, 2, \dots)$$

bestehen. Dabei wird mit  $(m; \mu)$  irgendeine Partition  $m = \mu_1 + \mu_2 + \dots + \mu_n$  der Zahl  $m$  in  $n$  nicht negative ganze Zahlen  $\mu_1, \mu_2, \dots, \mu_n$  bezeichnet.

$\sum_{(m; \mu)}$  sei das Zeichen für „Summation über alle Partitionen von  $m$ “,  $\xi^{(m; \mu)}$  sei die Abkürzung für  $\xi_1^{\mu_1} \xi_2^{\mu_2} \dots \xi_n^{\mu_n}$  ( $\xi_i \in P$ ),  $P(x)$  sei die Abkürzung für  $P(x_1, x_2, \dots, x_n)$ ,  $\Psi_{(m; \mu)}(x)$  sei der aus allen Kreisprodukten mit  $m$  Faktoren, von denen  $\mu_i$  Faktoren gleich  $x_i$  sind, erzeugte Modul.

$A_{(p^i; \mu)}(x)$  bedeutet ein eindeutig bestimmtes Element aus  $\Psi_{(p^i; \mu)}(x)$ . Vorweg werde bemerkt, daß für alle  $A_{(m; \mu)}(x)$  aus  $\Psi_{m; \mu}$ :

$$(64) \quad A_{(m; \mu)}(\xi_1 x_1, \xi_2 x_2, \dots, \xi_n x_n) = \xi^{(m; \mu)} A_{(m; \mu)}(x).$$

Die eindeutige Bestimmtheit der  $A_{(p^i; \mu)}(x)$  wird durch Induktion nach  $i$  gezeigt, dabei wird in den Identitäten jeweils  $\xi_1 = \xi_2 = \dots = \xi_n = 1$  eingesetzt und die Tatsache benutzt, daß zwei  $A_{(p^i; \mu)}(x)$  mit verschiedener Partition als Polynom in  $x_1, x_2, \dots, x_n$  betrachtet kein Monom gemeinsam haben.

Wenn  $n = 1$ , so ist die Formel (63) klar. Man setze nämlich:

$$A_{(1; \mu)} = x_1, \quad A_{(p^i; \mu)} = 0 \quad (i > 0),$$

wobei  $\mu$  jeweils die einzige Partition  $p^j = p^j$  von  $p^j$  ist. Ferner setze man bei beliebigem  $n$ :  $A_{(1; \mu_i)} = x_i$ , wobei  $\mu_i$  die Partition

$$1 = 0 + 0 + \dots + 0 + 1 + 0 + \dots + 0.$$

Dann gilt die Formel (63) für  $\nu = 0$  und alle  $n$ . Endlich sei  $L(x)$  der aus  $x_1, x_2, \dots, x_n$  erzeugte Lie'sche Ring. Es gilt die direkte Zerlegung:

$$L(x) = \sum_{m=1}^{\infty} \Psi_m(x).$$

Wenn also ein homogenes Polynom  $m$ -ten Grades in  $L(x)$  enthalten ist, so liegt es in  $\Psi_m(x)$ . Hieraus ergibt sich folgende

**Substitutionsregel:** Wenn  $Q(X_1, X_2, \dots, X)$  in  $\Psi_{(r; \mu)}(X_1, X_2, \dots, X_s)$  enthalten ist und  $r$  größer als 1 ist, wenn ferner  $f_i(x)$  in  $\Psi_{x_i}(x)$  ( $i = 1, 2, \dots, s$ ) enthalten ist, so liegt

$$\bar{Q} = Q((f_1(x))^{p^{r_1}}, (f_2(x))^{p^{r_2}}, \dots, (f_s(x))^{p^{r_s}})$$

in  $\Psi_q(x)$  mit

$$q = \sum_{j=1}^s x_j p_j^{\nu_j} \mu_j.$$

Denn  $\bar{Q}$  ist ein homogenes Polynom vom Grade  $q$  und da  $r > 1$ , so folgt nach I, § 4 durch vollständige Induktion nach  $r$  und  $s$ , daß  $\bar{Q}$  in  $L(x)$  enthalten ist.

Nach (55) ist

$$(x_1 + x_2)^p \equiv x_1^p + x_2^p \pmod{\Psi_p(x)}.$$

Sei schon bewiesen, daß

$$\left( \sum_1^i x_j \right)^p \equiv \sum_1^i x_j^p \pmod{\Psi_p(x)},$$

dann folgt

$$\begin{aligned} \left( \sum_{j=1}^{i+1} x_j \right)^p &= \left( \left( \sum_{j=1}^i x_j \right) + x_{i+1} \right)^p \\ &\equiv \left( \sum_{j=1}^i x_j \right)^p + x_{i+1}^p + \mathcal{A}_p \left( \sum_{j=1}^i x_j, x_{i+1} \right) \\ &\equiv \sum_1^i x_j^p + 0 + x_{i+1}^p + 0 \\ &\equiv \sum_{j=1}^{i+1} x_j^p \pmod{\Psi_p}. \end{aligned}$$

Nach  $n - 1$  Schritten folgt:

$$\begin{aligned} \left( \sum_{j=1}^n x_j \right)^p &\equiv \sum_{j=1}^n x_j^p \pmod{\Psi_p(x)}, \\ \left( \sum_{j=1}^n x_j \right)^p &= \sum_{j=1}^n x_j^p + \sum_{(p; \mu)} \mathcal{A}_{(p; \mu)}(x), \end{aligned}$$

wobei  $A_{(p;\mu)}(x)$  aus  $\mathcal{U}_{(p;\mu)}(x)$  stammt. Hieraus folgt nach (64), daß

$$(65) \quad \left( \sum_{j=1}^n \xi_j x_j \right)^p = \sum_{j=1}^n \xi_j^p x_j^p + \sum_{(p;\mu)} \xi^{(p;\mu)} A_{(p;\mu)}(x),$$

mithin gilt die Formel (63) für  $\nu = 0, 1$  und beliebiges  $n$ . Nun sei die Formel (63) schon bewiesen für  $\nu = 0, 1, 2, \dots, \kappa$  ( $\kappa > 1$ ) und beliebiges  $n$ . Insbesondere gilt

$$\left( \sum_{j=1}^n x_j \right)^{p^\kappa} = \sum_{i=0}^{\kappa} \sum_{(p^i;\mu)} A_{(p^i;\mu)}^{p^{\kappa-i}}(x).$$

Aus der Substitutionsregel und nach der bei beliebiger Variabelzahl gültigen Regel (65) folgt:

$$\begin{aligned} \left( \sum_{j=1}^n x_j \right)^{p^{\kappa+1}} &\equiv \sum_{i=0}^{\kappa} \sum_{(p^i;\mu)} A_{(p^i;\mu)}^{p^{\kappa+1-i}}(x) \pmod{\mathcal{U}_{p^{\kappa+1}}(x)}, \\ \left( \sum_{j=1}^n x_j \right)^{p^{\kappa+1}} &= \sum_{i=0}^{\kappa+1} \sum_{(p^i;\mu)} A_{(p^i;\mu)}^{p^{\kappa+1-i}}(x), \end{aligned}$$

wobei  $A_{(p^{\kappa+1};\mu)}(x)$  aus  $\mathcal{U}_{(p^{\kappa+1};\mu)}(x)$  stammt. Ersetzen wir  $x_i$  durch  $\xi_{ix}$ , so folgt nach (64) die Formel (63) für  $\nu = \kappa + 1$ .

Die zu beweisende Formel gilt für  $\nu = \kappa + 1$ , wenn sie für  $\nu = \kappa$  gilt und da sie auch für  $\nu = 0, 1$  richtig ist, so gilt sie allgemein.

### § 7. Eigenfunktionen und irreduzible Darstellungen von nilpotenten Lie'schen Ringen.

$H$  sei ein nilpotenter Lie'scher Ring mit der Klasse  $c$  über algebraisch abgeschlossenem Grundkörper  $k$  mit Charakteristik  $p > 0$ .  $h \rightarrow \bar{h}$  sei eine irreduzible Darstellung von  $H$  in linearen Transformationen eines endlichen  $k$ -Moduls  $\mathfrak{M}$ .  $\bar{H}$  sei der zugehörige Darstellungsring. Nach I, § 2 sind die Eigenwerte jeder linearen Transformation  $h$  alle untereinander gleich, etwa gleich  $\alpha_h$ . Ferner ist

$$\mathfrak{Z}_{c+1}(H) = \mathfrak{Z}_{c+2}(\bar{H}) = \dots = 0.$$

Es sei  $p^\kappa$  die kleinste  $p$ -Potenz größer als  $c - 1$ . Für ein beliebiges Paar von Elementen  $a_1, a_2$  aus  $H$  folgt nach (63):

$$(66) \quad (\bar{a}_1 + \bar{a}_2)^{p^\kappa} = \sum_{i=0}^{p^\kappa} \sum_{(p^i;\mu)} A_{(p^i;\mu)}^{p^{\kappa-i}}(\bar{a}_1, \bar{a}_2).$$

Nach der Substitutionsregel folgt

$$A_{(p^i;\mu)}^{p^{\kappa-i}}(\bar{a}_1, \bar{a}_2) \circ \bar{b} \in \mathcal{U}_{p^{\kappa+1}}(a_1, \bar{a}_2, \bar{b}) \subseteq \mathfrak{Z}_{p^{\kappa+1}}(\bar{H}) = 0$$

für alle  $b$  aus  $H$ . Nach Korollar zu Hilfssatz 4 ist  $\mathcal{A}_{(p^i; \mu)}^{p^{x-i}}(\bar{a}_1, \bar{a}_2)$  Vielfaches der identischen Transformation. Wir definieren:  $\alpha_{(p^i; \mu)}(a_1, a_2)$  ist der Eigenwert, der dem Element  $\mathcal{A}_{(p^i; \mu)}(a_1, a_2)$  durch die Darstellung  $h \rightarrow \bar{h}$  zugeordnet ist, d. h.  $\alpha_{(p^i; \mu)}(a_1, a_2)$  ist der einzige Eigenwert der linearen Transformation  $\mathcal{A}_{(p^i; \mu)}(\bar{a}_1, \bar{a}_2)$ . Aus der Formel (66) folgt:

$$(67) \quad \alpha_{a_1 + a_2} = \sum_{i=0}^{p^x} \sum_{(p^i; \mu)} \alpha_{(p^i; \mu)}^{p^{-i}}(a_1, a_2).$$

Ferner folgt aus  $\bar{\lambda h} = \lambda \cdot \bar{h}$ , daß

$$(68) \quad \alpha_{\lambda h} = \lambda \alpha_h.$$

**Definition:** Eine eindeutige Abbildung  $h \rightarrow \alpha_h$  von  $H$  auf Elemente aus  $k$  heißt *Eigenfunktion* auf  $H$ , wenn die beiden Regeln (67) und (68) erfüllt sind. Mit denselben Schlüssen, vermöge deren die allgemeine Formel (65) aus der besonderen Formel (55) und der Regel (64) abgeleitet wurde, folgt nun aus (67) und (68) die allgemeine Regel

$$(69) \quad \alpha_{\sum_{j=1}^n \xi_j a_j} = \sum_{i=0}^{p^0} \sum_{(p^i; \mu)} (\xi^{(p^i; \mu)} \alpha_{(p^i; \mu)}(a))^{p^{-i}},$$

wobei  $\alpha_{(p^i; \mu)}(a)$  der Wert der Eigenfunktion  $\alpha$  in  $\mathcal{A}_{(p^i; \mu)}(a_1, a_2, \dots, a_n)$  ist.

Da  $(\alpha + \beta)^{p^i} = \alpha^{p^i} + \beta^{p^i}$ , so ist die Summe zweier Eigenfunktionen wieder eine Eigenfunktion. Ferner folgt aus der Definition der Eigenfunktionen, daß jedes skalare Vielfache einer Eigenfunktion wieder Eigenfunktion ist. Alle Eigenfunktionen auf  $H$  bilden also einen  $k$ -Modul  $F(H)$ .

**Hilfssatz 7:** Wenn eine Eigenfunktion verschwindet für alle Elemente einer regulären Basis, so verschwindet sie identisch.

**Beweis:** Der Satz ist klar, wenn  $r = 1$ . Es sei  $r > 1$ , und der Satz sei bewiesen für nilpotente Lie'sche  $k$ -Ringe, deren Rang kleiner als  $r$  ist, ferner sei  $\alpha$  eine Eigenfunktion aus  $H$ , die in  $h_1, h_2, \dots, h_r$  verschwindet, wobei die  $h_i$  die Elemente einer regulären Basis von  $H$  seien. Auf dem  $(r-1)$ -gliedrigen Ideal  $H_1 = \{h_2, h_3, \dots, h_r\}$  wird durch die Festsetzung  $\beta_h = \alpha_h$  für alle  $h$  aus  $H_1$  eine Eigenfunktion  $\beta$  definiert, die in den  $r-1$  Elementen  $h_2, h_3, \dots, h_r$  verschwindet. Da diese Elemente eine reguläre Basis von  $H_1$  bilden, so folgt nach Induktionsvoraussetzung, daß  $\beta_h = 0$  für alle  $h$  aus  $H_1$ . Jedes Element  $h$  aus  $H$  läßt sich eindeutig in der Form  $h = \lambda h_1 + h'$  mit  $h'$  aus  $H_1$  darstellen. Setzen wir in Formel (69)  $a_1 = h_1, a_2 = h'; \xi_1 = \lambda, \xi_2 = 1$  ein, so folgt  $\alpha_h = 0$ , denn es ist  $\alpha_{h_1} = 0$  und alle  $\mathcal{A}_{(p^i; \mu)}$  liegen in  $H_1$ , sobald  $i > 0$ .



Aus diesem Hilfssatz schließen wir, daß durch die Zuordnung

$$(70) \quad \alpha \rightarrow \alpha_{h_1} h_1 + \alpha_{h_2} h_2 \cdots + \alpha_{h_r} h_r$$

eine isomorphe Abbildung des  $k$ -Moduls  $F(H)$  aller Eigenfunktionen auf einen Teilmodul von  $H$  definiert wird. Daher ist die Dimension von  $F(H)$  über  $k$  höchstens gleich  $r$ .

**Satz 12:** Die irreduziblen Darstellungen eines  $r$ -gliedrigen nilpotenten Lie'schen Ringes  $H$  über algebraisch abgeschlossenem Grundkörper  $k$  mit Primzahlcharakteristik  $p$  haben  $p$ -Potenzgrad. Ordnen wir dem Basiselement  $h_i$  einer regulären Basis  $h_1, h_2, \dots, h_r$  den Wert  $\alpha_i$  aus  $k$  zu, so gibt es genau eine irreduzible Darstellung von  $H$ , bei der dem Element  $h_i$  der Eigenwert  $\alpha_i$  zugeordnet ist.

Beweis: Wenn  $r = 1$ , so folgt der Satz nach I, § 2. Es sei die Behauptung bewiesen, falls der Rang von  $H$  kleiner als  $r$  ist, und es sei der Rang  $r$  von  $H$  jetzt größer als 1. Dann ist  $L = \{h_2, h_3, \dots, h_r\}$  ein Ideal von  $H$ , dessen Rang über  $k$  gleich  $r - 1$  ist, so daß  $H = L + kh_1$ . Durch die Festsetzung  $\sigma h = h \circ h_1$  für alle  $h$  aus  $L$  wird ein Endomorphismus  $\sigma$  von  $L$  definiert. Nun sei  $\mathfrak{M}$  ein irreduzibler  $H$ -Modul von endlichem Rang über  $k$ . Dann ist  $\mathfrak{M}$  ein irreduzibler  $(L, \sigma)$ -Modul, wobei dem Endomorphismus  $\sigma$  dieselbe lineare Transformation wie dem Element  $h_1$  aus  $H$  zugeordnet wird. Da mit  $H$  auch  $L$  nilpotent ist, so hat nach Induktionsvoraussetzung jeder in  $\mathfrak{M}$  enthaltene irreduzible  $L$ -Modul  $m$   $p$ -Potenzrang über  $k$ . Nach Satz 10 hat auch  $\mathfrak{M}$   $p$ -Potenzrang. Nun sei jedem Basiselement  $h_i$  ein Element  $\alpha_i$  aus  $k$  zugeordnet. Nach Induktionsvoraussetzung gibt es genau eine irreduzible Darstellung von  $L$ , bei der dem Element  $h_i$  der Eigenwert  $\alpha_i$  zugeordnet wird. Sie werde durch den  $L$ -Modul  $\mathfrak{M}$  vermittelt. Gemäß Satz 11 gibt es genau einen irreduziblen  $(L, \sigma)$ -Modul  $\mathfrak{M}$ , der als  $L$ -Modul betrachtet den  $L$ -Modul  $m$  enthält mit der Eigenschaft, daß dem Element  $h_1$  eine lineare Transformation mit dem Eigenwert  $\alpha_1$  zugeordnet wird. Damit ist alles bewiesen.

Aus diesem Satz und der Bemerkung unter Hilfssatz 8 folgt, daß die Dimension des  $k$ -Moduls aller Eigenfunktionen auf  $H$  genau gleich  $r$  ist und daß jede Eigenfunktion auf  $H$  auch wirklich als Eigenwertverteilung einer eindeutig bestimmten irreduziblen Darstellung von  $H$  vorkommt.

**Satz 13:** Nach Wahl einer geeigneten regulären Basis  $h_1, h_2, \dots, h_r$  des nilpotenten Lie'schen  $k$ -Ringes  $H$  mit der Klasse  $c$  läßt sich bei beliebiger Eigenwertverteilung  $\alpha$  der Eigenwert  $\alpha_{h_i}$  des Elementes

$$h = \xi_1 h_1 + \xi_2 h_2 + \xi_3 h_3 + \cdots + \xi_r h_r$$



Es sei schon bewiesen, daß es Konstanten  $\lambda_{(p^j; \mu)}^{(i)}$  gibt ( $j = 0, 1, 2, \dots, \nu$ ;  $i = \lambda_{p^j}, \dots, r$ ), so daß

$$(72) \quad \left( \sum_{i=1}^r \xi_i \bar{h}_i \right)^{p^\nu} = \sum_{j=0}^{\nu} \sum_{(p^j; \mu)} \sum_{i=\lambda_{p^j}}^r (\xi_{(p^j; \mu)} \lambda_{(p^j; \mu)}^{(i)} \bar{h}_i)^{p^{\nu-j}}.$$

Dann folgt nach der Regel (65) und der Substitutionsregel, daß

$$\begin{aligned} \left( \sum_{i=1}^r \xi_i \bar{h}_i \right)^{p^{\nu+1}} &= \left( \left( \sum_{i=1}^r \xi_i \bar{h}_i \right)^{p^\nu} \right)^p \\ &= \sum_{j=0}^{\nu} \sum_{(p^j; \mu)} \sum_{i=\lambda_{p^j}}^r (\xi_{(p^j; \mu)} \lambda_{(p^j; \mu)}^{(i)} \bar{h}_i)^{p^{\nu+1-j}} \\ &\quad + \sum_{(p^{\nu+1}; \mu)} (\xi_{(p^{\nu+1}; \mu)} \bar{\Gamma}_{(p^{\nu+1}; \mu)}), \end{aligned}$$

wobei  $\bar{\Gamma}_{(p^{\nu+1}; \mu)}$  ein von der Darstellung  $h \rightarrow \bar{h}$  unabhängiges Element aus  $\mathfrak{Z}_{p^{\nu+1}}(H)$  ist, also

$$\bar{\Gamma}_{(p^{\nu+1}; \mu)} = \sum_{i=\lambda_{p^{\nu+1}}}^r \lambda_{(p^{\nu+1}; \mu)}^{(i)} h_i \text{ mit Konstanten } \lambda_{(p^{\nu+1}; \mu)}^{(i)} \text{ aus } k.$$

Hieraus folgt Formel (72) auch für  $\nu+1$  statt  $\nu$ . Nach  $q$  Schritten folgt die Formel:

$$(73) \quad \left( \sum_{i=1}^r \xi_i \bar{h}_i \right)^{p^q} = \sum_{j=0}^q \sum_{(p^j; \mu)} \sum_{i=\lambda_{p^j}}^r (\xi_{(p^j; \mu)} \lambda_{(p^j; \mu)}^{(i)} \bar{h}_i)^{p^{q-j}}.$$

Hierbei sind sinnlose Summen durch 0 zu ersetzen, z. B.  $\sum_{i=\lambda_{c+1}}^r \dots = 0$ .

Für  $i \geq \lambda_{p^j}$  ist  $\bar{h}_i \subseteq \mathfrak{Z}_{p^j}(\bar{H})$  und nach I

$$\bar{h}_i^{p^{q-j}} \circ \bar{h}_k \subseteq Z_{p^q}(\bar{H}) \circ Z_1(\bar{H}) \subseteq Z_{p^q} + 1(\bar{H}) = 0,$$

also sind in (73) alle Summanden rechts mit  $\bar{H}$  elementweise vertauschbar, also nach dem Korollar zu Hilfssatz 4 skalare Vielfache der identischen Transformation. Hieraus folgt wie früher die Formel (71) durch Einsetzen der Eigenwerte und Ausziehen der  $p^q$ -ten Wurzel, w. z. b. w.

Als Nebenresultat erhalten wir:

**Satz 14:** *Ein  $r$ -gliedriger nilpotenter Lie'scher Ring  $H$  über dem algebraisch abgeschlossenen Körper  $k$  mit Charakteristik  $p > 0$  besitzt stets eine treue und vollreduzible Darstellung  $\mathcal{A}$  in Matrizen:  $\mathcal{A}$  kann genau dann irreduzibel gewählt werden, wenn das Zentrum von  $H$  1-gliedrig ist.*

Beweis: Wir ergänzen eine Basis  $h_{x+1}, h_{x+2}, \dots, h_r$  von  $\mathfrak{z}(H)$  zu einer regulären Basis  $h_1, h_2, \dots, h_r$  von  $H$ . Es gibt eine irreduzibel

Darstellung  $\mathcal{A}_i$  von  $H$  mit der Eigenwertverteilung  $\alpha^{(i)}$ , so daß  $\alpha_{h_{x+i}}^{(i)} = 1$ ;  $\alpha_{h_j}^{(i)} = 0$ , wenn  $j \neq x+i$  ( $i = 1, 2, \dots, r-x$ ). Nun sei  $\mathcal{A}$  die Darstellung

$$\begin{pmatrix} \mathcal{A}_1 & & & & 0 \\ & \mathcal{A}_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & \mathcal{A}_{r-x} \end{pmatrix}$$

Alle bei  $\mathcal{A}$  auf Null abgebildeten Elemente aus  $H$  bilden ein Ideal  $H_0$  von  $H$ .

$$z = \sum_{i=1}^{r-x} \xi_i h_{x+i}$$

sei ein in  $H_0$  gelegenes Zentrumselement. Da  $\mathcal{A}(z) = 0$ , so folgt:

$$\begin{aligned} \mathcal{A}_i(z) &= 0, \\ \alpha^{(i)}(z) &= 0 \\ &= \sum_{j=1}^{r-x} \xi_j \alpha_{h_{x+j}}^{(i)} \\ &= \xi_i \quad (i = 1, 2, \dots, r-x). \end{aligned}$$

Also folgt  $z = 0$ ,  $H_0 \cap \mathfrak{z} = 0$  und nach I, Satz 6 folgt  $H_0 = 0$ . Mithin ist  $\mathcal{A}$  eine treue Darstellung. Wenn  $\mathfrak{z}$  1-gliedrig, so ist  $\mathcal{A}$  irreduzibel. Wenn umgekehrt  $\Gamma$  eine treue und irreduzible Darstellung von  $L$  in Matrizen  $f$ -ten Grades ist, dann besteht das Zentrum des Darstellungsringes nur aus Skalarmatrizen, als ist  $\mathfrak{z}$  1-gliedrig, w. z. b. w.