

Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1950

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN243919689_0188

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0188

LOG Id: LOG_0004

LOG Titel: Idealdifferentationen und Differenten.

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN243919689

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN243919689>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Idealdifferentiation und Differenten.

Von Emmy Noether $\dagger$ ¹⁾.

Einleitung.

Der Hauptsatz der Verzweigungstheorie des algebraischen Zahlkörpers sagt bekanntlich aus, daß die Differenten (das Verzweigungsideal) mindestens durch die $(\varrho - 1)$ -te Potenz eines Primideals teilbar ist, das zur ϱ -ten Potenz in seiner Primzahl p aufgeht, und zwar genau durch die $(\varrho - 1)$ -te Potenz, wenn ϱ nicht durch p teilbar ist, durch eine höhere, wenn ϱ durch p teilbar ist.

Dieser Satz ist das Analogon dazu, daß der Differentialquotient $f'(x)$ eines Polynoms $f(x)$ mindestens durch die $(\varrho - 1)$ -te Potenz eines Linearfaktors teilbar ist, der in $f(x)$ zur ϱ -ten Potenz aufgeht, und zwar genau durch die $(\varrho - 1)$ -te Potenz, wenn ϱ nicht durch die Charakteristik des Koeffizientenbereichs teilbar ist, durch eine höhere, wenn ϱ durch diese Charakteristik teilbar ist.

Ich zeige im folgenden, daß es sich hier um mehr als eine formale Analogie handelt. Die Differenten läßt sich auffassen als Differentialquotient eines definierenden Ideals des Zahlkörpers K in einem zugeordneten ganzzahligen Polynombereich von $x_1, \dots, x_n$, der Differentialquotient genommen an der Stelle $x = \omega$, also für $x_1 = \omega_1, \dots, x_n = \omega_n$, wo $\omega_1, \dots, \omega_n$ eine Modulbasis des Systems der ganzen Zahlen aus K — der Hauptordnung $\mathfrak{o}$ — bedeutet. Dabei entspricht das definierende Ideal $\mathfrak{M}$ der Gesamtheit der Relationen zwischen den ω , besteht also aus allen ganzzahligen Polynomen $f(x)$, für die $f(\omega)$ verschwindet. Der Differentialquotient $\mathfrak{M}'[x \rightarrow \omega]$ aber ist definiert als Differenzenquotient, genommen an der Stelle $x = \omega$.

Man betrachte nämlich — wegen $f(\omega) = 0$ — das Ideal $\mathfrak{M}$ als aus allen Differenzen $f(x) - f(\omega)$ bestehend, bilde weiter das Differenzenideal $\mathfrak{P} = (x_1 - \omega_1, \dots, x_n - \omega_n)$ und den Differenzenquotient $\mathfrak{A} = \mathfrak{M} : \mathfrak{P}$, wobei die Quotientenbildung den üblichen Idealquotienten bedeutet, genommen im Polynombereich der x mit ganzen Zahlen aus K , also Zahlen aus $\mathfrak{o}$, als Koeffizienten. Dann wird die Differenten $\mathfrak{D}$ definiert durch

$$\mathfrak{D} = \mathfrak{A} [x \rightarrow \omega].$$

Die Erweiterung des Koeffizientenbereichs ist notwendig, damit Differenzenideal und Differenzenquotient überhaupt definiert sind. Es handelt sich also um die direkte Ver-

¹⁾ Die vorliegende von E. Noether nachgelassene, im Winter 1927/28 niedergeschriebene Arbeit wurde dem Herausgeber freundlicherweise von H. Grell zur Verfügung gestellt. Sie gibt eine ausführliche Darstellung des auf der D. M. V.-Tagung in Prag 1929 gehaltenen Vortrags gleichen Titels; siehe Jahresbericht D. M. V. 39 (1930), S. 17 kursiv. Ab § 6, 3 sollte das Manuskript offenbar noch genauer überarbeitet werden. Der Kenner wird jedoch die hier bis auf kleine Abrundungen unverändert gelassene skizzenhafte Darstellung ohne weiteres verstehen.

allgemeinerung des Differentialquotienten eines Polynoms einer Unbestimmten x

$$f'(\xi) = (f(x) - f(\xi)) : (x - \xi),$$

genommen an der Stelle $x = \xi$, wobei auch hier der Polynombereich durch Adjunktion von ξ erweitert werden muß, damit die Differenzen definiert sind. Tatsächlich geht auch der Idealdifferentialquotient in den Polynomdifferentialquotienten über, sobald die Basis der ω aus den Potenzen eines einzigen Elementes besteht.

Die hier gegebene Definition der Differentie schließt somit direkt an Bekanntes an, sie führt aber nichtinvariante Zwischenglieder ein, insofern, als das Ideal $\mathfrak{M}$ von der gewählten Basis abhängt. Eine gleichbedeutende, *vollständig invariante Definition* erhält man, wenn man statt des ganzzahligen Polynombereichs einen zur Hauptordnung $\mathfrak{o}$ isomorphen Ring $\mathfrak{D}$ einführt — der dem Restklassenring nach $\mathfrak{M}$ isomorph wird — und dessen Koeffizientenbereich durch $\mathfrak{o}$ zu $\mathfrak{D}_0$ erweitert²⁾. Das Differenzenideal $\mathfrak{P}$ wird hier aus allen Differenzen $(x - \xi)$ abgeleitet, wo x und ξ sich vermöge des Isomorphismus von $\mathfrak{D}$ zu $\mathfrak{o}$ entsprechen; der Differenzenquotient $\mathfrak{A}$ wird gleich dem Quotienten des Nullideals durch $\mathfrak{P}$; die Differentie entsteht aus $\mathfrak{A}$, indem jeweils x durch das isomorphe ξ ersetzt wird.

Diese invariante Definition wird im folgenden an die Spitze gestellt, und zwar wird so direkt die Differentie eines beliebigen kommutativen Ringes in bezug auf einen Unterring definiert, wobei nur gewisse Voraussetzungen in bezug auf die Möglichkeit der Koeffizientenerweiterung erfüllt sein müssen, was z. B. immer der Fall ist bei Existenz einer Modulbasis, eventuell unter Übergang zu gewissen Quotientenringen. Damit ist dann insbesondere auch die Differentie einer beliebigen *Ordnung* des Zahlkörpers definiert, ebenso die Differentie des Restklassenringes einer Ordnung etwa nach einer Primzahlpotenz; weiter auch die Relativedifferentie und die Differentie im Fall der algebraischen Funktionen von mehreren Unbestimmten. Die Übereinstimmung der Differentialdefinition der Differentie mit der üblichen folgt aus einer genauen, auf der direkten Summenzerlegung beruhenden Strukturuntersuchung des dem Zahlkörper durch direkte Produktbildung zugeordneten galoisschen Erweiterungsringes³⁾ — eine Untersuchung, die im Spezialfall des Restklassenringes nach einem Polynom einer Unbestimmten auf eine Analyse der Lagrangeschen Interpolationsformel hinauskommt. Genauer verstehe ich darunter folgendes:

Es werde ein dem Zahlkörper K isomorpher Ring $\mathfrak{R}$ eingeführt, der $\mathfrak{D}$ umfaßt, und sein Koeffizientenbereich — die rationalen Zahlen — durch den galoisschen Körper Γ von K erweitert. Dieses erweiterte System $\mathfrak{R}_\Gamma$ wird direkte Summe von n einfachen Komponenten, die den n Isomorphismen (Übergang zu den konjugierten Körpern) von K entsprechen und Erweiterungen des Differenzenquotienten $\mathfrak{A}$ und seiner Konjugierten sind; zugleich wird das Nullideal von $\mathfrak{R}_\Gamma$ Durchschnitt der n aus dem Differenzenideal und seinen Konjugierten abgeleiteten Ideale. Die einfachen Komponenten werden von der Form $\Gamma e^{(i)}$, wo $e^{(i)}$ die Komponente der Einheit bedeutet; der Differenzenquotient wird — da $e^{(1)}$ für $x = \xi$ in die Einheit übergeht — gleich $\mathfrak{d}e^{(1)}$, unter $\mathfrak{d}$ die Differentie von $\mathfrak{o}$ verstanden. Die Differentie $\mathfrak{d}$ besteht aus allen Elementen des Körpers, die mit $e^{(1)}$ multipliziert in $\mathfrak{D}_0$ liegen, dem *direkten Produkt der Ordnung mit*

²⁾ Die Erweiterung des Koeffizientenbereichs — direkte Produktbildung — wird in § 1 auch für nicht-kommutative Ringe behandelt, allgemeiner als für die Zwecke dieser Arbeit erforderlich. Dafür genügt § 2 in der Spezialisierung auf kommutative Ringe und endliche Basis.

³⁾ Es handelt sich hier um eine Weiterführung der meiner Diskriminantenarbeit zugrunde liegenden Überlegungen, wobei aber die Kenntnis dieser Arbeit nicht vorausgesetzt wird. Vgl. *E. Noether, Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- und Funktionenkörpers*, *J. Math.* **157** (1927), 82—104.

sich selbst. Entsprechendes gilt für die Konjugierten. Um von da aus die Definition durch den komplementären Modul zu gewinnen, ist zu beachten, daß $e^{(i)}$ eine Linearform in der den ω entsprechenden Basis $x_1, \dots, x_n$ von $\mathfrak{Q}$ bzw. $\mathfrak{R}$ wird; die Koeffizienten der x in den $e^{(i)}$ aber ergeben gerade eine Basis des komplementären Moduls von $\mathfrak{o}$ (und seinen Konjugierten). Aus der Tatsache, daß der Differenzenquotient $\mathfrak{A}$ Koeffizienten aus $\mathfrak{o}$ hat, folgt sofort, daß die Differenten gleich dem Quotienten von $\mathfrak{o}$ durch seinen Komplementärmodul wird, wodurch die Dedekindsche Definition gewonnen ist. Die angegebenen Betrachtungen sind nicht auf die Hauptordnung beschränkt; sie charakterisieren die Differenten jeder Ordnung als Quotient der Ordnung durch ihren Komplementärmodul.

Die Übereinstimmung der Differentialdefinition mit der Definition durch die Fundamentalgleichung — im Fall der Hauptordnung — folgt aus der oben erwähnten Tatsache, daß der Idealdifferentialquotient in den Polynomdifferentialquotienten übergeht, sobald die Basis aus den Potenzen eines Elementes, hier der Fundamentalform, besteht. Damit ist dann auch der begriffliche Zusammenhang dieser letzteren Definition mit der Dedekindschen gegeben.

Unter Zugrundelegung der Fundamentalgleichung — im Fall der Hauptordnung — folgt bekanntlich direkt der am Anfang erwähnte Hauptsatz. Zu einer genauen Exponentenbestimmung führt die Betrachtung der Differenten $\mathfrak{d}[p^t]$ des Restklassenringes der Hauptordnung nach p^t mit genügend hohem t — es genügt $t=n$, was für Körper zweiten Grades auch notwendig ist — wobei es wesentlich ist, daß die Differenten $\mathfrak{d}$, betrachtet mod p^t , genau in $\mathfrak{d}[p^t]$ übergeht. Hier kann man sich wieder — da der direkten Summe des Ringes die direkte Summe der Differenten entspricht — auf den Restklassenring nach p^t beschränken. Dieser letztere aber wird isomorph dem Restklassenring nach einem Polynom in einer Unbestimmten mit Koeffizienten mod p^t ; und die Differentiation dieses Polynoms ergibt — wie Ö. Ore, der auf anderem Wege zu einem solchen Polynom kam, gezeigt hat⁴⁾ — den genauen Überblick über die überhaupt möglichen Exponenten mit Hilfe der Supplementzahlen.

Schließlich ergibt die Strukturuntersuchung noch den bekannten Satz, daß die Differenten eines Oberkörpers von K gleich dem Produkt der Relativedifferenten mit der Differenten von K wird, und zwar als Folge der Tatsache, daß dieselbe Multiplikationseigenschaft für die Einheiten der direkten Summenzerlegung und damit für die Komplementärmoduln erfüllt ist.

Die angegebenen Tatsachen gelten überhaupt alle für Relativedifferenten durch Übergang zu gewissen Quotientenringen genau so, wie ich das in der Diskriminantenarbeit für Relativediskriminanten ausgeführt habe. Es bleibt weiter — durch Übergang zum Funktionalbereich — alles erhalten für algebraische Funktionenkörper mit Koeffizientenkörper der Charakteristik Null, während bei Charakteristik p und bei ganzzahligen algebraischen Funktionen zwar die Struktureigenschaften erhalten bleiben (im wesentlichen sogar ohne Übergang zum Funktionalbereich), die Verzweigungstheorie aber wegen des Auftretens von inseparablen Erweiterungskörpern sich ändert, was hier nicht mehr ausgeführt wird. Als wesentlichstes Ergebnis möchte ich die oben skizzierten vollständig invarianten, auch für algebraische Funktionen mehrerer Unbestimmten gültigen Struktursätze (§ 5 und § 6) bezeichnen; der Übergang zum Komplementärmodul bedeutet schon ein Auflösen in Koeffizientenidentitäten und ist nur durchgeführt, um Bekanntes einzuordnen.

⁴⁾ Anmerkung bei der Herausgabe: Dieses Zitat ist im Manuskript nicht ausgefüllt. Siehe die Hinweise in dem nur skizzierten § 7 der Arbeit.

§ 1. Erweiterung des Koeffizientenbereichs eines Ringes oder direkte Produktbildung. Definierendes Ideal⁵⁾.

In diesem Paragraphen werden allgemeine Ringe zugrunde gelegt, für die das kommutative Gesetz der Multiplikation *nicht* vorausgesetzt wird. Dagegen wird der Einfachheit halber die Existenz des Einheitselementes vorausgesetzt, und zwar, sofern nicht ausdrücklich das Gegenteil vermerkt, in der ganzen Arbeit.

1. Definition des direkten Produktes. Ein Ring $\mathfrak{D} \times \mathfrak{o}$ oder $\mathfrak{D}_0$ heißt *direktes Produkt* der Ringe $\mathfrak{D}$ und $\mathfrak{o}$ in bezug auf $\mathfrak{h}$ — oder auch *aus $\mathfrak{D}$ durch Erweiterung des Koeffizientenbereichs $\mathfrak{h}$ zu $\mathfrak{o}$ entstanden*⁶⁾ —, wenn die folgenden Bedingungen erfüllt sind:

(1) $\mathfrak{D}_0$ enthält $\mathfrak{D}$ und $\mathfrak{o}$ als Unterring und wird gleich dem Produkt dieser Ringe (also gleich dem Durchschnitt aller $\mathfrak{D}$ und $\mathfrak{o}$ umfassenden Ringe in $\mathfrak{D}_0$).

(2) Der Durchschnitt von $\mathfrak{D}$ und $\mathfrak{o}$ ist durch $\mathfrak{h}$ gegeben, wo $\mathfrak{h}$ das Einheitsselement von $\mathfrak{D}_0$ enthält.

(3) $\mathfrak{D}$ und $\mathfrak{o}$ sind elementweise vertauschbar; somit besteht $\mathfrak{D}_0$ aus der Gesamtheit der bilinearen Verbindungen $x_{i_1}y_{i_1} + \dots + x_{i_r}y_{i_r}$, wo die x bzw. y alle Systeme von je endlich vielen Elementen aus $\mathfrak{D}$ bzw. $\mathfrak{o}$ durchlaufen, und $\mathfrak{h}$ ist im Zentrum von $\mathfrak{D}$ und $\mathfrak{o}$ und damit von $\mathfrak{D}_0$ gelegen.

(4) Zwei Elemente aus $\mathfrak{D}_0$ sind nur dann (und natürlich stets dann) gleich, wenn sie auf mindestens eine Art formal gleich werden vermöge der in $\mathfrak{D}$ einerseits und in $\mathfrak{o}$ andererseits bestehenden Relationen. Darunter ist das folgende zu verstehen: Gilt $x_1y_1 + \dots + x_ny_n = 0$ in $\mathfrak{D}_0$, so läßt sich dieser Ausdruck durch Zufügen von Summen formal verschwindender Verbindungen $(\gamma h)\delta - \gamma(h\delta)$, wo h in $\mathfrak{h}$, γ in $\mathfrak{D}$ und δ in $\mathfrak{o}$, umformen in

$$(z_1\alpha_1 + \dots + z_r\alpha_r) + (t_1\beta_1 + \dots + t_s\beta_s)$$

mit $z_1 = 0, \dots, z_r = 0$; $\beta_1 = 0, \dots, \beta_s = 0$, wo α, β in $\mathfrak{o}$ und z, t in $\mathfrak{D}$, so daß also $z = 0$ Relationen zwischen den x, γ, h in $\mathfrak{D}$ und $\beta = 0$ Relationen zwischen den y, δ, h in $\mathfrak{o}$ bedeuten⁷⁾.

Zwei Elemente aus $\mathfrak{D}_0$ sind nur dann gleich, wenn ihre Differenz auf die angegebene Art verschwindet.

Durch die Forderung des direkten Produktes sind also die Gleichheits- und Verknüpfungsbeziehungen (Addition und Multiplikation) eindeutig durch diejenigen der Faktoren festgelegt. Daraus folgt: Sind $\mathfrak{D}$, $\mathfrak{o}$ und ihr Durchschnitt $\mathfrak{h}$ isomorph zu $\mathfrak{D}$, $\mathfrak{o}$ und $\mathfrak{h}$, und existiert das direkte Produkt $\mathfrak{D} \times \mathfrak{o}$, so existiert auch $\mathfrak{D} \times \mathfrak{o}$ und wird zu $\mathfrak{D} \times \mathfrak{o}$ isomorph.

Jeder Ring $\mathfrak{S}$, der gleich dem Produkt von $\mathfrak{D}$ und $\mathfrak{o}$ wird, derart, daß $\mathfrak{D}$ und $\mathfrak{o}$ elementweise vertauschbar sind, wird homomorphes Bild von $\mathfrak{D} \times \mathfrak{o}$, wobei die Abbildung von $\mathfrak{D}$ zu $\mathfrak{D}$ bzw. $\mathfrak{o}$ zu $\mathfrak{o}$ isomorph bleibt. Denn die Gleichheit in $\mathfrak{D} \times \mathfrak{o}$ wird durch diejenige in $\mathfrak{S}$ umfaßt und stimmt für $\mathfrak{D}$ bzw. $\mathfrak{o}$ mit der von $\mathfrak{D}$ bzw. $\mathfrak{o}$ in $\mathfrak{D} \times \mathfrak{o}$ überein⁸⁾.

2. Notwendige und hinreichende Bedingungen für die Existenz des direkten Produkts in bezug auf einen Unterring. Sind $\mathfrak{D}$ und $\mathfrak{o}$ Ringe, deren Durchschnitt durch den im Zentrum beider gelegenen Ring $\mathfrak{h}$ gegeben ist, so braucht das direkte Produkt in bezug auf $\mathfrak{h}$ nicht zu existieren, wie das folgende Beispiel zeigt: Sei $\mathfrak{h}$ der Ring der ganzen rationalen Zahlen, $\mathfrak{D} = \mathfrak{h}[x]$ mit $1 - 2x = 0$, und $\mathfrak{o} = \mathfrak{h}[y]$ mit $1 - 2y = 0$, wo y

⁵⁾ Für kritische Bemerkungen zu diesem Paragraphen bin ich B. L. van der Waerden zu Dank verpflichtet.

⁶⁾ Die zweite im folgenden meist gebrauchte Schreibweise soll an die Erweiterung des Koeffizientenbereichs erinnern; die erste ist die übliche Bezeichnung des direkten Produktes.

⁷⁾ Setzt man die Existenz des Einheitselementes nicht voraus, so treten in (3) und (4) noch lineare Zusatzglieder auf.

⁸⁾ Vergleiche auch § 1, 4.

ein neues Symbol bedeutet. Es werden also $\mathfrak{D}$ und $\mathfrak{o}$ in bezug auf $\mathfrak{h}$ äquivalente Ringe, deren mengentheoretischer Durchschnitt durch $\mathfrak{h}$ gegeben ist, während zwischen den Symbolen x und y keine Verknüpfungen gegeben sind. Es gibt keinen $\mathfrak{D}$ und $\mathfrak{o}$ umfassenden Ring R derart, daß in R — wo also jetzt Verknüpfungen zwischen x und y bestehen — der Durchschnitt durch $\mathfrak{h}$ gegeben ist. Denn in R folgt:

$$0 = (1-2x)y - x(1-2y) = y - x,$$

wobei Vertauschbarkeit von x und y sogar nicht benutzt wird⁹⁾.

Die notwendige und hinreichende Bedingung für die Existenz des direkten Produktes ist die folgende:

Es muß mindestens einen $\mathfrak{D}$ und $\mathfrak{o}$ umfassenden Ring R geben derart, daß der Durchschnitt von $\mathfrak{D}$ und $\mathfrak{o}$ durch $\mathfrak{h}$ gegeben ist und daß $\mathfrak{D}$ und $\mathfrak{o}$ elementweise vertauschbar werden.

Existiert nämlich das direkte Produkt, so ist es selbst ein solcher Ring R . Um umgekehrt das direkte Produkt zu konstruieren, darf vorausgesetzt werden — diese Voraussetzung wird im folgenden stets gemacht —, daß zwischen den nicht zu $\mathfrak{h}$ gehörigen Elementen von $\mathfrak{D}$ und $\mathfrak{o}$ keine Verknüpfungen bestehen, da dies durch Übergang zu äquivalenter Erweiterung von $\mathfrak{h}$ — Einführung anderer Symbole — stets erreichbar ist^{9a)}. Es enthalte weiter $\mathfrak{h}$ das Einheitselement e von $\mathfrak{D}$ und $\mathfrak{o}$ (vgl. dazu aber Anmerkung⁷⁾). Man definiere jetzt $\mathfrak{T}$ als Menge aller bilinearen Verbindungen

$$x_{i_1}y_{i_1} + \cdots + x_{i_r}y_{i_r} = y_{i_1}x_{i_1} + \cdots + y_{i_r}x_{i_r},$$

wo die x und y alle Systeme von je endlich vielen Elementen aus $\mathfrak{D}$ bzw. $\mathfrak{o}$ durchlaufen und die x und y also in $\mathfrak{T}$ vertauschbar werden. Man setze zwei solche Verbindungen dann und nur dann gleich, wenn sie vermöge der Relationen in $\mathfrak{D}$ und $\mathfrak{o}$ formal gleich werden in dem unter 1, (4) präzisierten Sinn. Man definiere weiter Summe und Produkt von $\alpha_{i_1}x_{i_1} + \cdots + \alpha_{i_r}x_{i_r}$ und $\beta_{i_1}x_{i_1} + \cdots + \beta_{i_r}x_{i_r}$, wo unter den α, β auch Nullen auftreten können, durch

$$(\alpha_{i_1} + \beta_{i_1})x_{i_1} + \cdots + (\alpha_{i_r} + \beta_{i_r})x_{i_r} \text{ und } \sum \alpha_{i_\lambda}\beta_{i_\mu}x_{i_\lambda}x_{i_\mu}.$$

Diese Definition ist eindeutig im Sinn der Gleichheit, da jede Nullrelation (im Sinne von 1, (4)) durch Rechts- oder Linksmultiplikation mit einem Element aus $\mathfrak{o}$ oder $\mathfrak{D}$ wieder in eine solche übergeht und dasselbe für Summe und Differenz dieser Nullrelationen gilt. Das System $\mathfrak{T}$ bildet einen $\mathfrak{D}$ und $\mathfrak{o}$ umfassenden Ring, der in bezug auf Gleichheit, Addition und Multiplikation den Bedingungen des direkten Produktes genügt. $\mathfrak{T}$ genügt aber auch der Durchschnittsbedingung als Folge der allgemeinen Einbettungsvoraussetzung. Sei nämlich $\mathfrak{S}$ das Produkt von $\mathfrak{D}$ und $\mathfrak{o}$ in R , dann wird $\mathfrak{S}$ nach 1 homomorphes Bild von $\mathfrak{T}$, isomorph in bezug auf $\mathfrak{D}$ und $\mathfrak{o}$. Eine Relation $x = y$ in $\mathfrak{T}$, wo x in $\mathfrak{D}$ und y in $\mathfrak{o}$, zieht somit dieselbe Relation in $\mathfrak{S}$ nach sich; also liegen in $\mathfrak{S}$ nach Voraussetzung beide Elemente in $\mathfrak{h}$, und wegen des Isomorphismus in bezug auf $\mathfrak{D}$ und $\mathfrak{o}$ einzeln gilt dasselbe für $\mathfrak{T}$. Die Einbettungsvoraussetzung ist also notwendig und hinreichend.

3. Definierendes Ideal eines Ringes in bezug auf einen Unterring. Ein System S von Elementen $\dots, z, \dots$ aus $\mathfrak{D}$ heißt *Erzeugendensystem* von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$, wenn $\mathfrak{D}$ gleich dem durch $\mathfrak{h}$ und S in $\mathfrak{D}$ erzeugten Ring wird — also gleich dem Durchschnitt aller $\mathfrak{h}$ und S umfassenden Ringe aus $\mathfrak{D}$; in Zeichen $\mathfrak{D} = \mathfrak{h}[S]$. Es sei wieder $\mathfrak{h}$ als Unterring des Zentrums von $\mathfrak{D}$ vorausgesetzt; es wird dann $\mathfrak{D}$ homomorphes Bild des nichtkommutativen

⁹⁾ Der in einem festen Ring gelegene Quotientenring eines kommutativen Ringes — hier Adjunktion von $\frac{1}{2}$ — ist eben eindeutig. Es handelt sich um das Analogon dazu, daß zwei äquivalente und verschiedene galoissche Körpererweiterungen sich nicht in einen gemeinsamen Umfassungskörper einbetten lassen. Hier gibt es — durch direkte Produktbildung — allerdings noch Einbettung in einen Ring mit Nullteilern.

^{9a)} Vgl. § 2, 1 und Fußnote ¹¹⁾.

Polynombereichs $\mathfrak{h}[\dots Z \dots]$, wo Z Unbestimmte bedeuten, und das System der Unbestimmten von gleicher Mächtigkeit ist wie S . Unter dem nichtkommutativen Polynombereich wird dabei das System aller endlichen Summen $\sum h_i P_i = \sum P_i h_i$ verstanden, wo die P_i Potenzprodukte einschließlich der dem Exponenten 0 entsprechenden Einheit sind:

$$P_i = Z_{i_1}^{a_1} Z_{i_2}^{a_2} \dots Z_{i_n}^{a_n}$$

(wobei natürlich die gleichen Indizes sich wiederholen können), und wo die Gleichheit als Koeffizientengleichheit in bezug auf die verschiedenen Potenzprodukte definiert ist. Aus dem Homomorphismus folgt, daß $\mathfrak{D}$ isomorph wird dem Restklassenring $\mathfrak{h}[\dots Z \dots]/\mathfrak{M}$, wo das zweiseitige Ideal $\mathfrak{M}$ aus allen Polynomen $F(Z)$ (Elementen aus $\mathfrak{h}[\dots Z \dots]$) besteht derart, daß $F(z)$ in $\mathfrak{D}$ verschwindet — wo Z und z sich vermöge des Homomorphismus entsprechen. Das Ideal $\mathfrak{M}$ heißt ein definierendes Ideal in bezug auf $\mathfrak{h}$, und zwar das dem Erzeugendensystem der z entsprechende Ideal. Die Definition zeigt, daß isomorphe Ringe in bezug auf isomorph entsprechende Unterringe $\mathfrak{h}$, $\bar{\mathfrak{h}}$ und Erzeugendensysteme S und $\bar{S}$ auch isomorphe definierende Ideale besitzen — die insbesondere, wenn $\mathfrak{h}$ mit $\bar{\mathfrak{h}}$ zusammenfällt, auch als identisch angenommen werden dürfen.

Da $\mathfrak{h}$ im Zentrum von $\mathfrak{D}$ angenommen war, wird $\mathfrak{D}$ sicher kommutativ, wenn es ein Erzeugendensystem S besitzt, das aus einem einzigen Element z besteht. Wird $\mathfrak{M}$ noch Hauptideal, so heißt die einem Basispolynom $G(Z)$ von $\mathfrak{M}$ entsprechende Gleichung $G(z) = 0$ eine definierende Gleichung von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$.

4. Das definierende Ideal eines direkten Produktes. Es sei (wie unter 3) $\mathfrak{D}$ isomorph zu $\mathfrak{h}[\dots Z \dots]/\mathfrak{M}$, wo also $\mathfrak{M}$ definierendes Ideal. Neben $\mathfrak{h}[\dots Z \dots]$ werde der Polynombereich $\mathfrak{o}[\dots Z \dots]$ betrachtet, also das System aller endlichen Summen

$$\sum \gamma_i P_i = \sum P_i \gamma_i \quad \text{mit} \quad \gamma_i \text{ aus } \mathfrak{o},$$

die Gleichheit als Koeffizientengleichheit definiert. $\mathfrak{o}[Z]$ umfaßt $\mathfrak{h}[Z]$ und ist direktes Produkt von $\mathfrak{h}[\dots Z \dots]$ und $\mathfrak{o}$ in bezug auf $\mathfrak{h}$, anders ausgedrückt: aus $\mathfrak{h}[\dots Z \dots]$ durch Erweiterung des Koeffizientenbereichs hervorgegangen¹⁰⁾. Es bedeute $\mathfrak{M}_0$ das Erweiterungsideal von $\mathfrak{M}$ in bezug auf $\mathfrak{o}[\dots Z \dots]$ — Durchschnitt aller $\mathfrak{M}$ umfassenden zweiseitigen Ideale aus $\mathfrak{o}[\dots Z \dots]$ —, also das System aller linearen Verbindungen der Elemente aus $\mathfrak{M}$ mit Koeffizienten aus $\mathfrak{o}$, das wegen der Vertauschbarkeit von $\mathfrak{o}$ mit den Z schon ein zweiseitiges Ideal bildet. Falls das direkte Produkt $\mathfrak{D}_0$ in bezug auf $\mathfrak{h}$ existiert, so wird $\mathfrak{D}_0$ isomorph zu $\mathfrak{o}[\dots Z \dots]/\mathfrak{M}_0$. Denn $\mathfrak{D}_0$ wird homomorphes Bild von $\mathfrak{o}[\dots Z \dots]$, also isomorph dem Restklassenring nach dem definierenden Ideal von $\mathfrak{D}_0$ in bezug auf $\mathfrak{o}$, entsprechend dem Erzeugendensystem der z . Nach der Gleichheitsdefinition 1, (4) aber lassen sich die zwischen den z in $\mathfrak{D}_0$ bestehenden Relationen als lineare Kombinationen mit Koeffizienten aus $\mathfrak{o}$ der in $\mathfrak{D}$ bestehenden schreiben; also wird $\mathfrak{M}_0$ definierendes Ideal.

Bemerkung. Dieselbe Überlegung ergibt noch eine symmetrische, aber umständlichere Darstellung des direkten Produktes und des zugehörigen definierenden Ideals. Es sei $\mathfrak{o}$ isomorph $\mathfrak{h}[\dots Y \dots]/\mathfrak{N}$, wo Y von den Z verschiedene Symbole bedeuten, so daß der Polynombereich $\mathfrak{h}[\dots Y \dots Z \dots]$ definiert ist. Dann wird $\mathfrak{D}_0$ isomorph

$$\mathfrak{h}[\dots Y \dots Z \dots]/(\mathfrak{M}, \mathfrak{N}, \dots YZ - ZY \dots),$$

wo das rechtsstehende definierende Ideal durch $\mathfrak{M}$, $\mathfrak{N}$ und alle Kombinationen $YZ - ZY$ erzeugt ist. (Letztere drücken die Vertauschbarkeit der Elemente von $\mathfrak{o}$ und $\mathfrak{D}$ aus, erstere die Tatsache, daß die Relationen in $\mathfrak{D}_0$ Folgen der in $\mathfrak{D}$ und $\mathfrak{o}$ einzeln sind.)

¹⁰⁾ Denn Gleichheits- und Verknüpfungsbedingungen sind erfüllt, und aus $\gamma = h + h_1 P_1 + \dots + h_r P_r$ folgt nach der Gleichheit in $\mathfrak{o}[\dots Z \dots]$, daß $\gamma = h$. Vgl. dazu § 2, 2. Die Tatsache, daß $\mathfrak{o}[\dots Z \dots]$ direktes Produkt ist, wird in dieser Nummer nicht benutzt.

§ 2. Ringe mit unabhängiger Modulbasis. Konstruktion des direkten Produktes.

1. Konstruktion des direkten Produktes. Ein System T von Elementen $\dots$ aus $\mathfrak{D}$ heißt eine $\mathfrak{h}$ -Modulbasis von $\mathfrak{D}$, wenn $\mathfrak{D}$ gleich dem aus T in $\mathfrak{D}$ abgeleiteten $\mathfrak{h}$ -Modul wird. Es besteht dann $\mathfrak{D}$ wegen der Existenz der Einheit in $\mathfrak{h}$ aus allen linearen Verbindungen $h_{i_1}t_{i_1} + \dots + h_{i_r}t_{i_r}$. Die Modulbasis heißt unabhängig, wenn aus

$$h_{i_1}t_{i_1} + \dots + h_{i_r}t_{i_r} = 0 \quad \text{stets} \quad h_{i_1} = 0, \dots, h_{i_r} = 0$$

folgt. Besitzt $\mathfrak{D}$ eine unabhängige, das Einheitselement enthaltende Modulbasis, so existiert das direkte Produkt $\mathfrak{D}_0$ bei beliebigem Erweiterungsring $\mathfrak{o}$ von $\mathfrak{h}$, für den nur $\mathfrak{h}$ Unterring des Zentrums und dessen mengentheoretischer Durchschnitt $[\mathfrak{D}, \mathfrak{o}]$ durch $\mathfrak{h}$ gegeben ist¹¹⁾. Es genügt nach § 1, 2, einen entsprechenden Einbettungsring $\mathfrak{R}$ zu konstruieren, der sich dann hier schon als das direkte Produkt erweisen wird. Es sei $\mathfrak{R}$ definiert als Gesamtheit aller linearen Verbindungen

$$\gamma_{i_1}t_{i_1} + \dots + \gamma_{i_r}t_{i_r} = t_{i_1}\gamma_{i_1} + \dots + t_{i_r}\gamma_{i_r},$$

wobei die t_{i_r} alle Systeme je endlich vieler Elemente der unabhängigen Basis T durchlaufen, die γ entsprechend aus $\mathfrak{o}$. Die Gleichheit sei als Koeffizientengleichheit in den t_{i_r} definiert, Summe und Produkt nach den üblichen Rechenregeln, wie unter § 1, 2. Wegen der Basiseigenschaft ist das Produkt irgend zweier t_{i_r} eine lineare Verbindung endlich vieler mit Koeffizienten aus $\mathfrak{h}$, es wird also $\mathfrak{R}$ ein Ring. $\mathfrak{R}$ umfaßt $\mathfrak{D}$, da $\mathfrak{h}$ Unterring von $\mathfrak{o}$ ist; und es umfaßt $\mathfrak{o}$, da T das Einheitselement enthält. Da weiter die γ_{i_r} sowohl mit den h_{i_r} wie mit den t_{i_r} elementweise vertauschbar sind, wird $\mathfrak{o}$ in $\mathfrak{R}$ mit $\mathfrak{D}$ elementweise vertauschbar. Schließlich ist in $\mathfrak{R}$ der Durchschnitt von $\mathfrak{D}$ und $\mathfrak{o}$ durch $\mathfrak{h}$ gegeben, denn eine Relation

$$\gamma = \gamma e = h_1t_1 + \dots + h_rt_r$$

ergibt nach der Gleichheitsdefinition — da e nach Voraussetzung Element der Basis ist —, daß ein t gleich e ist, die übrigen verschwinden, und somit $\gamma = h$. Somit existiert das direkte Produkt; es wird gleich $\mathfrak{R}$, das gleich dem Produkt von $\mathfrak{D}$ und $\mathfrak{o}$ ist und der Vertauschbarkeits- und Gleichheitsbedingung genügt (da die Elemente der Basis unabhängig sind, geht diese Bedingung in Koeffizientengleichheit über). Diese Basis T von $\mathfrak{D}$ wird zugleich $\mathfrak{o}$ -Basis von $\mathfrak{D}_0$.

2. Erweiterungs- und Verengungsmoduln. Ist $\mathfrak{B}$ ein $\mathfrak{h}$ -Modul aus $\mathfrak{D}$, so wird unter seiner Erweiterung $\mathfrak{B}_0$ der $\mathfrak{o}$ -Modul aus $\mathfrak{D}_0$ verstanden, der Durchschnitt aller $\mathfrak{B}$ umfassenden $\mathfrak{o}$ -Moduln aus $\mathfrak{D}_0$ ist. Ist $\mathfrak{C}$ ein $\mathfrak{o}$ -Modul aus $\mathfrak{D}_0$, so ist sein Verengungsmodul $\mathfrak{C}_{\mathfrak{h}}$ in $\mathfrak{D}$ als Durchschnitt $[\mathfrak{C}, \mathfrak{D}]$ definiert. Ist $\mathfrak{B}$ zugleich Ideal in $\mathfrak{D}$, so wird $\mathfrak{B}_0$ Ideal in $\mathfrak{D}_0$; ist $\mathfrak{C}$ Ideal in $\mathfrak{D}_0$, so wird $[\mathfrak{C}, \mathfrak{D}]$ Ideal in $\mathfrak{D}$.

Satz. Besitzt ein Modul $\mathfrak{B}$ aus $\mathfrak{D}$ eine unabhängige $\mathfrak{h}$ -Modulbasis, die sich zu einer unabhängigen $\mathfrak{h}$ -Modulbasis von $\mathfrak{D}$ ergänzen läßt, so ist $\mathfrak{B}$ Verengung seines Erweiterungsmoduls $\mathfrak{B}_0$ in $\mathfrak{D}_0$.

Beweis. Es bedeute T eine unabhängige $\mathfrak{h}$ -Modulbasis von $\mathfrak{B}$, die sich nach Voraussetzung durch ein System $\bar{T}$ von Elementen $\bar{t}$ aus $\mathfrak{D}$ zu einer unabhängigen $\mathfrak{h}$ -Modulbasis von $\mathfrak{D}$ ergänzen läßt. Es wird T dann zugleich unabhängige $\mathfrak{o}$ -Basis von $\mathfrak{B}_0$, und T und $\bar{T}$ zusammen eine solche von $\mathfrak{D}_0$.

¹¹⁾ Natürlich könnte symmetrisch dazu auch die Basisvoraussetzung für $\mathfrak{o}$ gemacht werden. Nach § 2, 2 wird — ohne Beschränkung der Allgemeinheit; vgl. E. Noether, Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- oder Funktionenkörpers, dies. Journ. 157 (1927), 82—104, §§ 1, 2 — vorausgesetzt, daß zwischen den nicht zu $\mathfrak{h}$ gehörigen Elementen aus $\mathfrak{D}$ und $\mathfrak{o}$ keine Verknüpfungen bestehen.

Es ist $\mathfrak{B}$ enthalten im Durchschnitt $[\mathfrak{B}_0, \mathfrak{D}]$. Sei umgekehrt c ein Element dieses Verengungsmoduls. Als Element von $\mathfrak{B}_0$ läßt c eine Darstellung durch Elemente von T zu, die zugleich eine Darstellung durch die $\mathfrak{o}$ -Basis $T, \bar{T}$ von $\mathfrak{D}_0$ bedeutet:

$$c = \gamma_1 t_1 + \cdots + \gamma_r t_r \quad \text{mit } \gamma \text{ aus } \mathfrak{o}.$$

Als Element von $\mathfrak{D}$ besitzt c eine Darstellung durch die $\mathfrak{h}$ -Basis von $T, \bar{T}$ von $\mathfrak{D}$, also:

$$c = h_{i_1} t_{i_1} + \cdots + h_{i_r} t_{i_r} + h_{j_1} \bar{t}_{j_1} + \cdots + h_{j_s} \bar{t}_{j_s},$$

die ebenfalls zugleich, da $\mathfrak{D}$ Unterring von $\mathfrak{D}_0$ und $\mathfrak{h}$ Unterring von $\mathfrak{o}$, eine Darstellung durch die $\mathfrak{o}$ -Basis $T, \bar{T}$ von $\mathfrak{D}_0$ bedeutet. Also müssen beide Darstellungen koeffizienten- gleich sein; die Koeffizienten der $\bar{t}$ verschwinden und

$$c = h_{i_1} t_{i_1} + \cdots + h_{i_r} t_{i_r}$$

zeigt, daß c Element aus $\mathfrak{B}$ ist. Damit ist $\mathfrak{B}$ als *Verengungsmodul* erkannt.

Zusatzbemerkung. Der Beweis benutzt nur etwas geringere Voraussetzungen als die im Satz formulierten und beweist die übrigen; es gilt die *verschärfte Fassung*:

Es wird $\mathfrak{B}$ Verengungsmodul seiner Erweiterung $\mathfrak{B}_0$, wenn es in $\mathfrak{D}$ eine unabhängige $\mathfrak{h}$ -Modulbasis $T, \bar{T}$ gibt, wo T in $\mathfrak{B}$, derart, daß T zugleich (unabhängige) $\mathfrak{o}$ -Modulbasis von $\mathfrak{B}_0$ ist. Es erweist sich dann T auch als unabhängige $\mathfrak{h}$ -Modulbasis von $\mathfrak{B}$.

3. Hinreichendes Kriterium für Existenz des direkten Produktes. Es kann vorkommen (z. B. bei der Relativedifferenten), daß erst bei Erweiterung des Koeffizientenbereichs $\mathfrak{h}$ eine unabhängige Modulbasis existiert. Die Existenz des direkten Produktes kann sich dann entnehmen lassen aus dem *hinreichenden Kriterium*:

Gibt es einen Erweiterungsring $\mathfrak{k}$ von $\mathfrak{h}$ derart, daß die direkten Produkte $\mathfrak{D}_{\mathfrak{k}}$ und $\mathfrak{o}_{\mathfrak{k}}$ in bezug auf $\mathfrak{h}$ und weiter $\mathfrak{D}_{\mathfrak{k}} \times \mathfrak{o}_{\mathfrak{k}}$ in bezug auf $\mathfrak{k}$ existieren, so existiert $\mathfrak{D} \times \mathfrak{o}$ in bezug auf $\mathfrak{h}$.

Es ist zu zeigen, daß $\mathfrak{K} = \mathfrak{D}_{\mathfrak{k}} \times \mathfrak{o}_{\mathfrak{k}}$ ein Einbettungsring im Sinn von 2 wird. In der Tat werden $\mathfrak{D}$ und $\mathfrak{o}$ als Unterringe von $\mathfrak{D}_{\mathfrak{k}}$ und $\mathfrak{o}_{\mathfrak{k}}$ elementweise vertauschbar; weiter gilt

$$[\mathfrak{D}, \mathfrak{o}] \subseteq [\mathfrak{D}_{\mathfrak{k}}, \mathfrak{o}_{\mathfrak{k}}] = \mathfrak{k};$$

ebenso $[\mathfrak{D}, \mathfrak{o}] \subseteq \mathfrak{D}$; also $[\mathfrak{D}, \mathfrak{o}] \subseteq [\mathfrak{D}, \mathfrak{k}] = \mathfrak{h}$, und somit $[\mathfrak{D}, \mathfrak{o}] = \mathfrak{h}$, womit $\mathfrak{K}$ als Einbettungsring nachgewiesen ist.

Bemerkung. Der Beweis benutzt die Durchschnittsvoraussetzung nur bei $\mathfrak{D}_{\mathfrak{k}}$, nicht bei $\mathfrak{o}_{\mathfrak{k}}$, welch letzterer Ring also auch einfach das Produkt von $\mathfrak{o}$ und $\mathfrak{k}$ sein kann.

§ 3. Differenten eines Ringes nach einem Unterring. Differentialquotient eines definierenden Ideals.

Von jetzt an seien alle auftretenden Ringe als *kommutativ* angenommen¹²⁾. Weiter sei stets vorausgesetzt, daß die Ringe $\mathfrak{D}$ und $\mathfrak{o}$ *isomorphe*, und zwar *äquivalente Erweiterungen des Unterringes $\mathfrak{h}$* seien (daß also die Abbildung von $\mathfrak{D}$ auf $\mathfrak{o}$ Fortsetzung der identischen von $\mathfrak{h}$ sei) und daß das direkte Produkt $\mathfrak{D}_0$ in bezug auf $\mathfrak{h}$ existiert.

1. Definition der Differenten. Es sei vorausgesetzt, daß das direkte Produkt $\mathfrak{D}_0$ in bezug auf $\mathfrak{h}$ existiert. Es durchlaufe x alle Elemente aus $\mathfrak{D}$, und ξ bedeute jeweils das

¹²⁾ Ohne diese Voraussetzung müßten Rechts- und Linksdifferenten definiert und es müßte untersucht werden, wie weit diese unter sich übereinstimmen und wie weit sie im Fall von Ordnungen halbeinfacher Systeme mit bekannten Bildungen übereinstimmen (als Verallgemeinerung der Untersuchungen von § 4).

vermöge des Isomorphismus in $\mathfrak{o}$ entsprechende; es bezeichne $\mathfrak{P}$ das durch alle Differenzen $x - \xi$ erzeugte zweiseitige *Differenzenideal* von $\mathfrak{D}_0$,

$$\mathfrak{P} = \{..(x - \xi).. \}^{13)}.$$

Der *Differenzenquotient* $\mathfrak{A}$ ist definiert als Idealquotient des Nullideals durch $\mathfrak{P}$, besteht also aus allen Elementen a aus $\mathfrak{D}_0$, für die $a\mathfrak{P}$ verschwindet,

$$\mathfrak{A} = (0) : \mathfrak{P}.$$

Die *Differente* $\mathfrak{d}$ von $\mathfrak{o}$ in bezug auf $\mathfrak{h}$ ist definiert als $\mathfrak{A}[x \rightarrow \xi]$, entsteht also aus $\mathfrak{A}$, indem in jedem $a = \alpha_{i_1} x_{i_1} + \dots + \alpha_{i_r} x_{i_r}$ aus $\mathfrak{A}$ die x durch die isomorph entsprechenden ξ ersetzt werden. Entsprechend ist die *Differente* $\mathfrak{D}$ von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$ als $\mathfrak{A}[\xi \rightarrow x]$ definiert; da $\mathfrak{A}$ symmetrisch in x und ξ definiert, entsprechen sich $\mathfrak{d}$ und $\mathfrak{D}$, als durch Vertauschen von ξ und x hervorgegangen, vermöge des Isomorphismus von $\mathfrak{o}$ zu $\mathfrak{D}$. Da $\mathfrak{A}$ Ideal in $\mathfrak{D}_0$, also insbesondere $\mathfrak{o}$ -Modul und $\mathfrak{D}$ -Modul, werden $\mathfrak{d}$ und $\mathfrak{D}$ Ideale in $\mathfrak{o}$ und $\mathfrak{D}$.

2. Differentialquotient eines definierenden Ideals. Es sei (§ 1, 3) $\mathfrak{M}$ definierendes Ideal von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$, entsprechend dem Erzeugendensystem der z . Es wird also (§ 1, 3) $\mathfrak{M}$ auch definierendes Ideal von $\mathfrak{o}$ in bezug auf $\mathfrak{h}$, entsprechend dem isomorphen Erzeugendensystem der ξ ; und es wird (§ 1, 4) $\mathfrak{D}_0$ isomorph $\mathfrak{o}[..Z..]/\mathfrak{M}_0$. *Differenzenideal* und *Differenzenquotient* sind jetzt im Polynombereich $\mathfrak{o}[..Z..]$ definiert durch

$$\mathfrak{D} = \{..(Z - \xi).. \}$$

und

$$\mathfrak{C} = \mathfrak{M}_0 : \mathfrak{D} = \{..(F(Z) - F(\xi)).. \} : \{..(Z - \xi).. \}.$$

Der *Differentialquotient* $\mathfrak{M}'$ ist definiert als $\mathfrak{C}[\xi \rightarrow Z]$. Dabei ist zu beachten, daß diese Definition eindeutig ist, unabhängig von der *Darstellung* der Elemente aus $\mathfrak{o}$ durch die Erzeugenden ξ . Denn da $\mathfrak{C}$ Idealquotient, umfaßt es $\mathfrak{M}_0$; zwei Darstellungen eines Elementes von $\mathfrak{o}$ unterscheiden sich durch ein Polynom $F(\xi)$, also nach der Einsetzung von Z durch ein in $\mathfrak{M}$ und damit schon in $\mathfrak{C}$ liegendes $F(Z)$. Das Ideal $\mathfrak{M}'$ wird ein $\mathfrak{M}$ umfassendes Ideal in $\mathfrak{h}[..Z..]$. Der *Differentialquotient* $\mathfrak{M}'$ geht für $Z \rightarrow \xi$ in die *Differente* $\mathfrak{d}$ von $\mathfrak{o}$ über. Denn vermöge einer homomorphen Abbildung entsprechen sich neben Idealen auch die Quotienten. Es wird also $\mathfrak{A}$ homomorphes Bild von $\mathfrak{C}$ vermöge des Homomorphismus zwischen $\mathfrak{o}[..Z..]$ und $\mathfrak{D}_0$, also des Entsprechens von Z und z , da das gleiche für $\mathfrak{P}$ und das Nullideal in bezug auf $\mathfrak{D}$ und $\mathfrak{M}_0$ gilt^{13a)}. Daraus folgt, daß der Substitution $\xi \rightarrow Z$ in $\mathfrak{C}$ vermöge des Homomorphismus die Substitution $\xi \rightarrow z$ in $\mathfrak{A}$ entspricht; es wird also die *Differente* $\mathfrak{D}$ von $\mathfrak{D}$ homomorphes Bild von $\mathfrak{M}'$ vermöge des Entsprechens von Z und z . Also

$$\mathfrak{M}'[Z \rightarrow z] = \mathfrak{D} \quad \text{und} \quad \mathfrak{M}'[Z \rightarrow \xi] = \mathfrak{D}[z \rightarrow \xi] = \mathfrak{d}.$$

3. Differente im Fall einer definierenden Gleichung. Es besitze $\mathfrak{D}$ eine definierende Gleichung $G(z) = 0$ (§ 1, 3, Schluß), wobei weiter noch *vorausgesetzt* sei, daß der *Koeffizient des höchsten Gliedes gleich der Einheit* wird, also

$$G(Z) = Z^n + h_1 Z^{n-1} + \dots + h_n$$

mit Koeffizienten h_i aus $\mathfrak{h}$. Dann ist der Zusammenhang mit dem Polynomdifferentialquotienten hergestellt durch:

¹³⁾ Diese Bezeichnung soll immer für aus Gesamtheiten abgeleitete Ideale angewandt werden.

^{13a)} *Anmerkung bei der Herausgabe:* Es ist wichtig, daß $\mathfrak{M}_0$ die Urbildmenge von (0) darstellt, um das Entsprechen des Quotienten schließen zu können.

Satz. Die Differenten von $\mathfrak{o}$ bzw. $\mathfrak{D}$ in bezug auf $\mathfrak{h}$ ist definiert (d. h. das direkte Produkt $\mathfrak{D}_0$ in bezug auf $\mathfrak{h}$ existiert) und wird Hauptideal mit dem Basiselement $G'(\xi)$ bzw. $G'(z)$, wo $G'(Z)$ den Polynomdifferentialquotienten bedeutet. Der Idealdifferentialquotient $\mathfrak{M}'$ wird gleich $(G'(Z), G(Z))$.

Beweis. Aus der Voraussetzung folgt zuerst, daß die Elemente $e, z, \dots, z^{n-1}$ eine unabhängige Modulbasis von $\mathfrak{D}$ bilden. Denn da der höchste Koeffizient in $G(Z)$ die Einheit ist, bilden diese Potenzen tatsächlich eine $\mathfrak{h}$ -Modulbasis; diese ist aber unabhängig, weil $\mathfrak{M}$ kein Polynom von niedrigerem als n -tem Grad enthalten kann. Der Grad eines Polynoms $K(Z)G(Z)$ ist nämlich gleich der Summe der Gradzahlen der Faktoren, wieder wegen der Voraussetzung über den höchsten Koeffizienten. Wegen der Existenz der Modulbasis existiert also das direkte Produkt $\mathfrak{D}_0$ in bezug auf $\mathfrak{h}$, und damit ist die Differenten definiert. Das Weitere folgt aus der Betrachtung des Differenzenquotienten $\mathfrak{C}$ in $\mathfrak{o}[\dots Z \dots]$ (vgl. 2). Dieser Differenzenquotient wird Hauptideal mit einem Basispolynom

$$C(Z, \xi) = (Z^{n-1} + Z^{n-2}\xi + \dots + \xi^{n-1}) + h_1(Z^{n-2} + \dots + \xi^{n-2}) + \dots + h_{n-1}.$$

Denn C entsteht durch formale Division von $G(Z) - G(\xi)$ durch $Z - \xi$ und gehört somit zu $\mathfrak{C}$, da $Z - \xi$ Basis von $\mathfrak{D}$ wird. Ein beliebiges Polynom läßt sich mod C auf ein solches D reduzieren, das in Z den Grad $n-1$ nicht erreicht; also erreicht das Produkt $D(Z - \xi)$ den Grad n nicht und kann daher nur zu $\mathfrak{M}$ gehören, wenn es verschwindet. Aus $D(Z - \xi) = 0$ folgt aber $D = 0$, da der Koeffizient von Z in $Z - \xi$ die Einheit ist. Also wird C die Basis von $\mathfrak{C}$. Nun aber ergibt sich

$$\mathfrak{M}' = (G'(Z), G(Z)),$$

wie die Substitution $\xi \rightarrow Z$ in C und seine Vielfachen (also $G(Z) = C(Z - \xi)$ und dessen Vielfache) zeigt, und damit kommt

$$\mathfrak{d} = (G'(\xi)) \quad \text{und} \quad \mathfrak{D} = (G'(z)).$$

§ 4. Differenten einer direkten Summe.

Über $\mathfrak{D}$ werden die folgenden Voraussetzungen gemacht:

(1) $\mathfrak{D}$ wird direkte Summe von Idealen

$$\mathfrak{D} = \mathfrak{R}_1 + \dots + \mathfrak{R}_r = \mathfrak{R}_i + \mathfrak{S}_i = \mathfrak{D}e_1 + \dots + \mathfrak{D}e_r,$$

wo die e_i die Komponenten der Einheit bedeuten.

(2) Jedes $\mathfrak{R}_i$ besitzt eine unabhängige $\mathfrak{h}_i$ -Modulbasis T_i , wo $\mathfrak{h}_i$ die Komponente von $\mathfrak{h}$ in $\mathfrak{R}_i$, also $\mathfrak{h}_i = \mathfrak{h}e_i$. Diese Basis T_i enthält die Einheit e_i von $\mathfrak{R}_i$ als Element.

(3) Jeder Durchschnitt $[\mathfrak{h}, \mathfrak{S}_i]$ wird gleich dem Nullelement ($\mathfrak{S}_i$ enthält keine Konstanten).

Wegen des Isomorphismus gelten dieselben Voraussetzungen für $\mathfrak{o}$.

Satz. Unter den angegebenen Voraussetzungen wird die Differenten von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$ direkte Summe der Differenten von $\mathfrak{R}_i$ in bezug auf $\mathfrak{h}_i$.

Der Beweis beruht auf dem Nachweis einer Reihe von Einzeltatsachen.

I. Zunächst folgt, daß auch $\mathfrak{D}$ eine unabhängige, e enthaltende $\mathfrak{h}$ -Modulbasis besitzt, daß also die Differenten von $\mathfrak{D}$ bzw. $\mathfrak{o}$ in bezug auf $\mathfrak{h}$ definiert ist, und zwar besteht diese

Basis aus der Vereinigungsmenge T der Basen T_i von $\mathfrak{R}_i$. Denn aus

$$x = xe_1 + \cdots + xe_r$$

und

$$xe_i = (h_1 e_i) t_{1i} e_i + \cdots + (h_\lambda e_i) t_{\lambda i} e_i = h_1 (t_{1i} e_i) + \cdots + h_\lambda (t_{\lambda i} e_i)$$

ergibt sich, daß T tatsächlich eine $\mathfrak{h}$ -Basis von $\mathfrak{D}$ wird. Diese ist aber auch unabhängig; denn aus einer Relation zwischen den Elementen aus T folgen wegen der direkten Summe Relationen zwischen den Elementen jedes T_i , und damit $he_i = 0$ für alle Koeffizienten. Das ergibt aber $h = 0$ nach Voraussetzung (3); denn wegen

$$h = he_i (\mathfrak{S}_i)$$

folgt aus $he_i = 0$, daß h in $[\mathfrak{h}, \mathfrak{S}_i]$ liegt. Da T weiter die Einheiten e_i von $\mathfrak{R}_i$ als Element enthält, deren Summe e wird, so kann in T ein e_i durch e ersetzt werden, wodurch die allen Bedingungen genügende $\mathfrak{h}$ -Basis $\bar{T}$ entsteht. Hieraus ergibt sich die Existenz von $\mathfrak{D}_0$ und der Differenten von $\mathfrak{D}$ in bezug auf $\mathfrak{h}$.

II. Die Durchschnittsbedingung (3) zieht jetzt die schärfere nach sich:

$$[\mathfrak{o}, \mathfrak{S}_{i(\mathfrak{o})}] = 0,$$

wo $\mathfrak{S}_{i(\mathfrak{o})}$ das in $\mathfrak{D}_0$ aus $\mathfrak{S}_i$ abgeleitete Ideal bedeutet. Sei

$$\alpha = \alpha e = \beta_1 t_1 + \cdots + \beta_\lambda t_\lambda,$$

wo $t_1, \dots, t_\lambda$ Elemente der durch Weglassen von T_i aus T entstehenden Basis sind, α und β aus $\mathfrak{o}$. Bildet man $\bar{T}$, indem man e_i durch e ersetzt, so sind also $e, t_1, \dots, t_\lambda$ voneinander verschiedene Elemente der $\mathfrak{h}$ -Basis $\bar{T}$ von $\mathfrak{D}$. Da aber die Gleichheit in $\mathfrak{D}_0$ in Koeffizientengleichheit in jeder solchen Basis übergeht, ergibt die Relation

$$\alpha = \alpha e = \beta_1 t_1 + \cdots + \beta_\lambda t_\lambda,$$

also $\alpha = 0$, womit die *verschärfte Durchschnittseigenschaft* bewiesen ist. Hieraus ergibt sich insbesondere (wie oben): Aus

$$\alpha \text{ Element von } \mathfrak{o} \text{ und } \alpha \neq 0$$

folgt $\alpha e_i \neq 0$.

III. Eine unmittelbare Folge dieser Durchschnittsbedingung ist: Es wird $\mathfrak{o}$ *ringisomorph* zu seinen der Zerlegung von $\mathfrak{D}$ entsprechenden *Komponenten* $\mathfrak{o}e_i$; dieser Isomorphismus umfaßt den Isomorphismus

$$\mathfrak{h} \simeq \mathfrak{h}_i = \mathfrak{h}e_i.$$

Denn wegen $e_i^2 = e_i$ — und der Vertauschbarkeit von e_i mit allen Elementen aus $\mathfrak{o}$ — wird $\mathfrak{o}e_i$ ringisomorphes Bild von $\mathfrak{o}$; die Beziehung ist aber eineindeutig, da aus $\alpha \neq 0$ auch $\alpha e_i \neq 0$ folgt. Dem Unterring $\mathfrak{h}$ ist dabei die Komponente $\mathfrak{h}_i = \mathfrak{h}e_i$ zugeordnet.

IV. *Weitere Isomorphismen* folgen, wenn noch die entsprechende Zerlegung für $\mathfrak{o}$ herangezogen wird:

$$\mathfrak{o} = \mathfrak{r}_1 + \cdots + \mathfrak{r}_r = \mathfrak{r}_i + \mathfrak{s}_i = \mathfrak{o}\varepsilon_1 + \cdots + \mathfrak{o}\varepsilon_r.$$

Es kommt dann:

$$\mathfrak{o} \simeq \mathfrak{o}e_i, \mathfrak{D} \simeq \mathfrak{D}e_i, \mathfrak{r}_\lambda \simeq \mathfrak{r}_\lambda e_i, \mathfrak{R}_\lambda \simeq \mathfrak{R}_\lambda e_i; \mathfrak{h} \simeq \mathfrak{h}e_i \simeq \mathfrak{h}\varepsilon_i \simeq \mathfrak{h}e_i\varepsilon_i.$$

Die Relation $\mathfrak{D} \simeq \mathfrak{D}e_i$ ist die $\mathfrak{o} \simeq \mathfrak{o}e_i$ genau entsprechende, wenn man in der obigen Betrachtung von $\mathfrak{o}$ statt $\mathfrak{D}$ ausgeht. Ebenso entsprechen sich die beiden folgenden Relationen, deren erste daraus folgt, daß bei $\mathfrak{o} \simeq \mathfrak{o}e_i$ dem Unterring $\mathfrak{r}_\lambda$ auch $\mathfrak{r}_\lambda e_i$ zugeordnet ist; ebenso entsteht

$$\mathfrak{h} \simeq \mathfrak{h}e_i \simeq \mathfrak{h}\varepsilon_i.$$

Da aber $\mathfrak{h}_{\varepsilon_i}$ Unterring von $\mathfrak{o}$ (und $\mathfrak{r}_i$), kommt schließlich noch

$$\mathfrak{h}_{\varepsilon_i} \simeq \mathfrak{h}_{\varepsilon_i} e_i.$$

V. Aus der direkten Summendarstellung von $\mathfrak{D}$ folgt: Ist $\mathfrak{C} = (0) : \mathfrak{B}$ der Quotient des Nullideals durch das Ideal $\mathfrak{B}$ in $\mathfrak{D}$, so wird jede Komponente $\mathfrak{C}_i$ gleich dem Quotienten des Nullideals von $\mathfrak{R}_i$ durch die Komponente $\mathfrak{B}_i$. Aus

$$\mathfrak{B}\mathfrak{C} = (\mathfrak{B}e_1)(\mathfrak{C}e_1) + \cdots + (\mathfrak{B}e_r)(\mathfrak{C}e_r) = 0$$

folgt wegen der direkten Summe einzeln

$$(\mathfrak{B}e_i)(\mathfrak{C}e_i) = 0.$$

Genügt umgekehrt ein Element re_i aus $\mathfrak{R}_i$ der Bedingung $(\mathfrak{B}e_i)(re_i) = 0$, so gilt auch $(\mathfrak{B}e_k)(re_i) = 0$ für $i \neq k$.

Also ist re_i Element aus $\mathfrak{C}$ und zugleich aus $\mathfrak{R}_i$, gehört also der Komponente $\mathfrak{C}_i = \mathfrak{C}e_i$ an. Damit ist $\mathfrak{C}_i = \mathfrak{C}e_i$ als Quotient des Nullideals durch $\mathfrak{B}_i$ erkannt; also auch als Quotient des Nullideals von $\mathfrak{R}_i$ durch $\mathfrak{B}_i$, da aus

$$re_i \mathfrak{B}_i = 0 \quad (\mathfrak{C}_i)$$

immer $re_i \mathfrak{B}_i = 0$ folgt¹⁴). Da neben $\mathfrak{D}$ auch

$$\mathfrak{D}_0 = \mathfrak{D}_0 e_1 + \cdots + \mathfrak{D}_0 e_r$$

direkte Summe wird, gilt der Satz also auch für die Ideale aus $\mathfrak{D}_0$.

VI. *Komponentenzerlegung der Differente.* Nach Definition (vgl. §3, 1) war $\mathfrak{D} = \mathfrak{A}[\xi \rightarrow x]$; also kommt

$$\mathfrak{D} = \mathfrak{D}e_1 + \cdots + \mathfrak{D}e_r = \mathfrak{A}[\xi \rightarrow x]e_1 + \cdots + \mathfrak{A}[\xi \rightarrow x]e_r.$$

Da aber e_i in $\mathfrak{D}$ und damit sich selbst entspricht, da weiter ε_i durch den Isomorphismus in e_i übergeht, und da $e_i^n = e_i$ ist, so wird

$$\mathfrak{A}[\xi \rightarrow x]e_i = \mathfrak{A}e_i[\xi \rightarrow x] = \mathfrak{A}e_i \varepsilon_i[\xi \rightarrow x].$$

Nach V. wird aber $\mathfrak{A}e_i \varepsilon_i$ gleich dem Quotienten $(0) : \mathfrak{B}e_i \varepsilon_i$ und ebenso gleich dem Quotienten des Nullideals von $\mathfrak{R}_i \mathfrak{r}_i$ durch $\mathfrak{B}e_i \varepsilon_i$. Denn die direkte Summenzerlegung in $\mathfrak{D}$ und $\mathfrak{o}$ erzeugt durch Multiplikation die Zerlegung

$$\mathfrak{D}_0 = \sum \mathfrak{D}_0 e_i \varepsilon_i = \sum \mathfrak{R}_i \mathfrak{r}_i,$$

die direkt ist, da $\sum e_i \varepsilon_i = e$ wird und die Orthogonalitätsrelationen für die Einheiten erfüllt sind.

VII. *Nachweis, daß $\mathfrak{D}e_i = \mathfrak{A}e_i \varepsilon_i[\xi \rightarrow x] = (0) : \mathfrak{B}e_i \varepsilon_i$ die Differente von $\mathfrak{R}_i$ in bezug auf $\mathfrak{h}_i$ ist.* Dieser Nachweis beruht auf den Tatsachen: Es wird $\mathfrak{R}_i \mathfrak{r}_i$ gleich $\mathfrak{R}_i \varepsilon_i \times \mathfrak{r}_i e_i$ in bezug auf $\mathfrak{h}_i \varepsilon_i$; dessen Differenzenideal ist durch $\mathfrak{B}e_i \varepsilon_i$ gegeben, sein Differenzenquotient durch $\mathfrak{A}e_i \varepsilon_i$, während $\mathfrak{D}e_i \varepsilon_i$ die Differente von $\mathfrak{R}_i \varepsilon_i$ und entsprechend $\mathfrak{D}e_i \varepsilon_i$ die Differente von $\mathfrak{r}_i e_i$ wird. Die Isomorphismen

$$\mathfrak{R}_i \varepsilon_i \simeq \mathfrak{R}_i \quad \text{und} \quad \mathfrak{r}_i \simeq \mathfrak{r}_i e_i$$

ergeben dann $\mathfrak{D}e_i$ bzw. $\mathfrak{D}e_i \varepsilon_i$ als Differenten von $\mathfrak{R}_i$ in bezug auf $\mathfrak{h}_i$ bzw. von $\mathfrak{r}_i$ in bezug auf $\mathfrak{h}_i \varepsilon_i$.

VIII. *Es wird $\mathfrak{R}_i \mathfrak{r}_i$ gleich dem direkten Produkt $\mathfrak{R}_i \varepsilon_i \times \mathfrak{r}_i e_i$ in bezug auf $\mathfrak{h}_i \varepsilon_i$.* Da $\mathfrak{R}_i$ die $\mathfrak{h}_i$ -Modulbasis T_i besitzt, folgt aus dem Isomorphismus (IV) $\mathfrak{R}_i \simeq \mathfrak{R}_i \varepsilon_i$, daß $T_i \varepsilon_i$ eine $\mathfrak{h}_i \varepsilon_i$ -Modulbasis von $\mathfrak{R}_i \varepsilon_i$ wird. Nun ist $\mathfrak{r}_i e_i$ nach IV. zu $\mathfrak{R}_i \varepsilon_i$ isomorph — da $\mathfrak{r}_i \simeq \mathfrak{R}_i$ ver-

¹⁴) Der Satz folgt auch direkt aus dem unter 2 benutzten Satz, daß bei homomorpher Abbildung sich neben Idealen auch die Quotienten entsprechen.

möge $\mathfrak{o} \simeq \mathfrak{D}$ — und Erweiterungsring von $\mathfrak{h}_{e_i \varepsilon_i}$. Das direkte Produkt besteht also aus allen Linearformen der Elemente von $T_i \varepsilon_i$, mit Koeffizienten aus $r_i e_i$, wobei die Gleichheit als Koeffizientengleichheit definiert ist. Das wird aber vermöge $\mathfrak{D} \times \mathfrak{o}$ genau $\mathfrak{R}_i r_i$, da $T_i = T_i e_i$ und $r_i = r_i \varepsilon_i$ ist und T_i zu einer Modulbasis von $\mathfrak{D}$ gehört.

IX. Das Differenzenideal von $\mathfrak{R}_i \varepsilon_i \times r_i e_i$ ist durch $\mathfrak{P}_{e_i \varepsilon_i}$ gegeben, der Differenzenquotient durch $\mathfrak{A}_{e_i \varepsilon_i}$. Um das einzusehen, schreibe man $\mathfrak{P}$ in der Form

$$\mathfrak{P} = \{\dots, x e_1 - \xi \varepsilon_1, \dots, x e_r - \xi \varepsilon_r, \dots\}.$$

Dann wird

$$\mathfrak{P}_{e_i \varepsilon_i} = \{\dots, x e_i \varepsilon_i - \xi \varepsilon_i e_i, \dots\},$$

also tatsächlich gleich dem Differenzenideal von $\mathfrak{R}_i \varepsilon_i \times r_i e_i$. Da aber (nach VI.) $\mathfrak{A}_{e_i \varepsilon_i}$ gleich dem Quotienten des Nullideals dieses Ringes durch $\mathfrak{P}_{e_i \varepsilon_i}$ wird, ist es als Differenzenquotient erkannt.

X. Die Differenten von $\mathfrak{R}_i \varepsilon_i$ ist gleich $\mathfrak{D}_{e_i \varepsilon_i}$. Die Differenten von $\mathfrak{R}_i \varepsilon_i$ entsteht, indem man in $\mathfrak{A}_{e_i \varepsilon_i}$ jedes Element aus $r_i e_i$ durch sein isomorphes ersetzt; also jeweils $(\xi \varepsilon_i) e_i$ durch $(x e_i) \varepsilon_i$, d. h., da auch $\xi \varepsilon_i$ ein ξ aus $\mathfrak{o}$, das in $x e_i$ übergeht: indem man in $\mathfrak{A}_{e_i \varepsilon_i}$ die Substitution $\xi \rightarrow x$ macht — was $(\xi \varepsilon_i) e_i$ in $(x e_i) \varepsilon_i = x e_i$ überführt — und dann mit ε_i multipliziert. Nun war (nach VI.) $\mathfrak{A}_{e_i \varepsilon_i} [\xi \rightarrow x] = \mathfrak{D}_{e_i}$; also wird die Differenten von $\mathfrak{R}_i \varepsilon_i$ in bezug auf $\mathfrak{h}_{e_i \varepsilon_i}$ gleich $\mathfrak{D}_{e_i \varepsilon_i}$, und symmetrisch dazu die Differenten von $r_i e_i$ gleich $\mathfrak{D}_{e_i \varepsilon_i}$.

XI. Die Differenten von $\mathfrak{R}_i$ wird gleich $\mathfrak{D}_{e_i}$. Denn vermöge des Isomorphismus geht die Differenten von $\mathfrak{R}_i$ in diejenige von $\mathfrak{R}_i \varepsilon_i$ durch Multiplikation mit ε_i über; und da letztere gleich $\mathfrak{D}_{e_i \varepsilon_i}$ wird, so ist also erstere gleich $\mathfrak{D}_{e_i}$. Also:

$$\mathfrak{D} = \mathfrak{D}_{e_1} + \dots + \mathfrak{D}_{e_r},$$

und $\mathfrak{D}_{e_i}$ ist Differenten von $\mathfrak{R}_i$; symmetrisch dazu

$$\mathfrak{d} = \mathfrak{d}_{\varepsilon_1} + \dots + \mathfrak{d}_{\varepsilon_r},$$

und $\mathfrak{d}_{\varepsilon_i}$ ist Differenten von r_i , womit der Satz bewiesen ist.

§ 5. Galoisscher Erweiterungsring eines Körpers. Struktursätze.

1. Die zugrunde liegenden Ringe. Es sei K ein Körper n -ten Grades über einem Grundkörper P , und zwar werde K als separable Erweiterung angenommen. Γ sei ein zugehöriger — bis auf Isomorphie eindeutig bestimmter — galoisscher Körper, der also n Konjugierte $K^{(i)}$ umfaßt und deren Produkt ist, wobei $K = K^{(1)}$ gesetzt ist. Es bedeute $\mathfrak{R}$ eine zu K und folglich allen $K^{(i)}$ isomorphe in bezug auf P äquivalente Erweiterung von P derart, daß der Durchschnitt $[\mathfrak{R}, \Gamma]$ durch P gegeben ist (daß es also keinen gemeinsamen Umfassungskörper von Γ und $\mathfrak{R}$ gibt¹⁵). Da $\mathfrak{R}$ eine unabhängige und endliche, das Einheitselement enthaltende P -Modulbasis besitzt, existieren nach § 2, 1 die direkten Produkte $\mathfrak{R}_\Gamma, \mathfrak{R}_K, \mathfrak{R}_{K^{(i)}}$; es wird $\mathfrak{R}_\Gamma$ das Produkt seiner n Unterringe $\mathfrak{R}_{K^{(i)}}$. Es wird $\mathfrak{R}_\Gamma$ als galoisscher Erweiterungsring von $\mathfrak{R}$ bezeichnet. $\mathfrak{R}_\Gamma$ ist zugleich direktes Produkt von $\mathfrak{R}_K$ und Γ in bezug auf K , da jede unabhängige P -Basis von $\mathfrak{R}$ auch unabhängige K -Basis von $\mathfrak{R}_K$ wird, entsprechend für die Konjugierten¹⁶). Für die Beziehungen zwischen den Idealen dieser Ringe gilt:

¹⁵) Dabei wird natürlich vorausgesetzt — was keine Beschränkung der Allgemeinheit —, daß zwischen den nicht zu P gehörigen Elementen von K und $\mathfrak{R}$ keine Verknüpfungen bestehen (vgl. § 1, 2, § 2, 1 und Fußnote ¹¹)).

¹⁶) Die für alle Konjugierten gleichmäßig geltenden Sätze werden meist nur für $\mathfrak{R}_K$ ausgesprochen, also unter Weglassung der Indizes.

Satz. Jedes Ideal aus $\mathfrak{R}$ ist Verengungsideal seiner Erweiterung in $\mathfrak{R}_K$ oder $\mathfrak{R}_\Gamma$; jedes Ideal aus $\mathfrak{R}_K$ ist Verengungsideal seiner Erweiterung in $\mathfrak{R}_\Gamma$.

Beweis. Da P und K Körper sind, besitzt jeder P -Modul aus $\mathfrak{R}$ bzw. K -Modul aus $\mathfrak{R}_K$ eine unabhängige und endliche P - bzw. K -Modulbasis, die sich zu einer solchen von $\mathfrak{R}$ bzw. $\mathfrak{R}_K$ ergänzen läßt. Der Satz folgt jetzt aus dem Satz in § 2, 2.

Mit $\mathfrak{P}_{K(i)}^{(i)}$ sei das Differenzenideal von $\mathfrak{R}_{K(i)}$ bezeichnet, also

$$\mathfrak{P}_{K(i)}^{(i)} = \{\dots, x - \xi^{(i)}, \dots\},$$

speziell also:

$$\mathfrak{P}_K = \{\dots, x - \xi, \dots\}.$$

Da ξ bzw. $\xi^{(i)}$ das x vermöge des Isomorphismus entsprechende Element aus K bzw. $K^{(i)}$ ist, so sind also die n Differenzenideale untereinander konjugiert.

$\mathfrak{U}_K$ bzw. $\mathfrak{U}_{K(i)}$ bezeichne die Differenzenquotienten $(0) : \mathfrak{P}_K$ in $\mathfrak{R}_K$ und seine Konjugierten. Die Erweiterungs Ideale in $\mathfrak{R}_\Gamma$ seien durch $\mathfrak{P}_\Gamma$ und $\mathfrak{U}_\Gamma$ gegeben. Aus dem Satz dieser Nummer über Erweiterungs- und Verengungs Ideale folgt also insbesondere:

Differenzenideal $\mathfrak{P}_K$ und Differenzenquotient $\mathfrak{U}_K$ sind Verengungs Ideale ihrer Erweiterungen $\mathfrak{P}_\Gamma$ und $\mathfrak{U}_\Gamma$.

2. Direkte Summenzerlegung des galoisschen Erweiterungsringes. Den Zusammenhang von Differenzenideal und Differenzenquotient mit der Struktur des galoisschen Erweiterungsringes gibt der

Struktursatz. Das Nullideal des galoisschen Erweiterungsringes $\mathfrak{R}_\Gamma$ wird der Durchschnitt der Erweiterungen der n konjugierten Differenzenideale; $\mathfrak{R}_\Gamma$ selbst wird direkte Summe der Erweiterungen der n konjugierten Differenzenquotienten. $\mathfrak{R}_{K(i)}$ wird direkte Summe, sein Nullideal Durchschnitt des zugehörigen Differenzenideals und Differenzenquotienten.

Beweis. Der Restklassenring nach jedem $\mathfrak{P}_\Gamma^{(i)}$ ist vom Range eins in bezug auf Γ , da jedes Element mod $\mathfrak{P}_\Gamma^{(i)}$ einem Element aus Γ kongruent ist, aber $\mathfrak{P}_\Gamma^{(i)}$ kein Element $\neq 0$ aus Γ enthalten kann (denn $\mathfrak{P}_\Gamma^{(i)}$ verschwindet für $x \rightarrow \xi^{(i)}$). Da wegen der Separabilität die $\mathfrak{P}_\Gamma^{(i)}$ alle verschieden sind, werden sie also paarweise teilerfremd (Summe von je zweien gleich $\mathfrak{R}_\Gamma$). Somit nimmt der Rang der Ideale

$$\mathfrak{P}_\Gamma^{(1)}, [\mathfrak{P}_\Gamma^{(1)}, \mathfrak{P}_\Gamma^{(2)}], \dots, [\mathfrak{P}_\Gamma^{(1)}, \dots, \mathfrak{P}_\Gamma^{(n)}]$$

um mindestens je eine Einheit ab; der Durchschnitt aller wird das Nullideal, während — wegen der paarweisen Teilerfremdheit — der Durchschnitt von weniger als allen Konjugierten vom Nullideal verschieden sein muß (der Rang hat also bei jedem Schritt um genau eine Einheit abgenommen). Daraus folgt aber nach bekannten Sätzen die folgende eindeutig bestimmte, direkte Summendarstellung von $\mathfrak{R}_\Gamma^{(17)}$:

$$(1) \quad \mathfrak{R}_\Gamma = \mathfrak{C}_\Gamma^{(1)} + \dots + \mathfrak{C}_\Gamma^{(n)} = \Gamma e^{(1)} + \dots + \Gamma e^{(n)} = \mathfrak{C}_\Gamma^{(i)} + \mathfrak{P}_\Gamma^{(i)}; \\ e = e^{(1)} + \dots + e^{(n)}; \mathfrak{C}_\Gamma^{(i)} = [\mathfrak{P}_\Gamma^{(1)}, \dots, \mathfrak{P}_\Gamma^{(i-1)}, \mathfrak{P}_\Gamma^{(i+1)}, \dots].$$

Es ist zu zeigen, daß $\mathfrak{C}_\Gamma$ gleich $\mathfrak{U}_\Gamma$ wird. Das wird daraus folgen, daß die entsprechende Übereinstimmung in $\mathfrak{R}_K$ nachgewiesen wird. Hier gilt die Zerlegung:

$$(2) \quad \mathfrak{R}_K = \mathfrak{C}_K + \mathfrak{P}_K = \mathfrak{R}_K e^{(1)} + \mathfrak{R}_K (e - e^{(1)}).$$

Es liegt nämlich $e^{(1)}$ in $\mathfrak{R}_K$; denn $\mathfrak{C}_\Gamma^{(1)}$ gestattet alle Vertauschungen von $\mathfrak{P}_\Gamma^{(2)}, \dots, \mathfrak{P}_\Gamma^{(n)}$, somit gilt das gleiche für $e^{(1)}$ als Komponente der Einheit in $\mathfrak{C}_\Gamma^{(1)}$. Drückt man daher

¹⁷⁾ Vgl. etwa E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann. 96 (1927), 26—61, § 4, 5.

$e^{(1)}$ durch eine unabhängige K -Basis von $\mathfrak{R}_K$ aus — was möglich ist, da diese zugleich unabhängige Γ -Basis von $\mathfrak{R}_\Gamma$ ist —, so gestatten die Koeffizienten einzeln alle Vertauschungen von $K^{(2)}, \dots, K^{(n)}$, liegen also in K . Wegen $(e^{(1)})^2 = e^{(1)}$ wird die Summendarstellung

$$\mathfrak{R}_K = \mathfrak{R}_K e^{(1)} + \mathfrak{R}_K (e - e^{(1)})$$

direkt; ihre Erweiterung in $\mathfrak{R}_\Gamma$ wird wieder direkt, führt also nach (1) auf $\mathfrak{R}_\Gamma = \mathfrak{C}_\Gamma^{(1)} + \mathfrak{P}_\Gamma^{(1)}$. Somit gilt nach § 2, 2, Schluß:

$$\mathfrak{R}_K e^{(1)} = [\mathfrak{C}_\Gamma, \mathfrak{R}_K] = [\Gamma e^{(1)}, \mathfrak{R}_K] = K e^{(1)} = \mathfrak{C}_K;$$

$$\mathfrak{R}_K (e - e^{(1)}) = [\mathfrak{P}_\Gamma, \mathfrak{R}_K] = \mathfrak{P}_K,$$

womit (2) bewiesen ist.

Aus (2) folgt aber $\mathfrak{C}_K = \mathfrak{A}_K$ und damit $\mathfrak{C}_\Gamma = \mathfrak{A}_\Gamma$. Denn wegen $e^{(1)}(e - e^{(1)}) = 0$ folgt $\mathfrak{C}_K \mathfrak{P}_K = 0$; umgekehrt ergibt $b \mathfrak{P}_K = 0$ auch $b(e - e^{(1)}) = 0$, also wird $b = b e = b e^{(1)}$, und somit wird

$$\mathfrak{C}_K = (0) : \mathfrak{P}_K = \mathfrak{A}_K$$

und durch Erweiterung $\mathfrak{C}_\Gamma = \mathfrak{A}_\Gamma$. Damit gilt aber:

$$(3) \quad \begin{aligned} \mathfrak{R}_\Gamma &= \mathfrak{A}_\Gamma^{(1)} + \dots + \mathfrak{A}_\Gamma^{(n)} = \Gamma e^{(1)} + \dots + \Gamma e^{(n)}; \quad 0 = [\mathfrak{P}_\Gamma^{(1)}, \dots, \mathfrak{P}_\Gamma^{(n)}]; \\ \mathfrak{R}_{K(i)} &= \mathfrak{A}_{K(i)} + \mathfrak{P}_{K(i)}^{(i)} = K^{(i)} e^{(i)} + \mathfrak{P}_{K(i)}^{(i)}; \quad 0 = [\mathfrak{A}_{K(i)}, \mathfrak{P}_{K(i)}^{(i)}], \end{aligned}$$

womit der Satz in allen Teilen bewiesen ist. Es sei noch darauf hingewiesen, daß es sich um einen *völlig invarianten Struktursatz* handelt, da alle auftretenden Bildungen ($\mathfrak{R}_K, \mathfrak{R}_\Gamma, \mathfrak{P}_K, \mathfrak{A}_K$) basisfrei definiert sind¹⁸⁾.

3. Komponentendarstellung von $\mathfrak{R}$ durch konjugierte Elemente. Den konjugierten Differenzenidealen und Differenzenquotienten entspricht eine Darstellung der Elemente von $\mathfrak{R}$ durch konjugierte Komponenten:

Satz. Ist $x = \xi^{(1)} e^{(1)} + \dots + \xi^{(n)} e^{(n)}$ die Komponentendarstellung eines Elementes x aus $\mathfrak{R}$, so sind die n Komponenten untereinander konjugiert. Insbesondere sind $\xi^{(1)}, \dots, \xi^{(n)}$ die n konjugierten Werte, die x vermöge der Isomorphismen von $\mathfrak{R}$ zu $K^{(1)}, \dots, K^{(n)}$ entsprechen.

Daß $e^{(1)}, \dots, e^{(n)}$ untereinander konjugiert sind, zeigen die Relationen (3) in 2, wonach die Automorphismen von Γ , die $\mathfrak{P}_K$ in $\mathfrak{P}_{K(i)}^{(i)}$ überführen, zugleich $e^{(1)}$ in $e^{(i)}$ überführen, welches letzteres ja Element aus $\mathfrak{R}_{K(i)}$ ist. Dieselben Relationen ergeben $x e^{(i)} = \xi^{(i)} e^{(i)}$, wegen $\mathfrak{P}_{K(i)}^{(i)} e^{(i)} = 0$ und damit

$$(x - \xi^{(i)}) e^{(i)} = 0$$

(oder aus der Tatsache, daß $\mathfrak{R}$ als Körper zu seiner Komponente isomorph, diese also durch $K^{(i)} e^{(i)}$ mit isomorpher Zuordnung von x und $\xi^{(i)} e^{(i)}$ gegeben ist).

Aus dem Satz ergibt sich:

Folgerung. Ist $\mathfrak{B}$ ein absoluter Modul in $\mathfrak{R}$ (d. h. enthält $\mathfrak{B}$ neben irgend zwei Elementen noch die Differenz), und sind $\mathfrak{B}^{(1)}, \dots, \mathfrak{B}^{(n)}$ seine Komponenten in $\mathfrak{R}_\Gamma$, so wird $\mathfrak{B}$ gleich dem Durchschnitt $[\mathfrak{R}, \mathfrak{B}^{(1)} + \dots + \mathfrak{B}^{(n)}]$.

Denn $\mathfrak{B}$ ist in diesem Durchschnitt enthalten; soll umgekehrt ein Element aus $\mathfrak{B}^{(1)} + \dots + \mathfrak{B}^{(n)}$ zu $\mathfrak{R}$ gehören, so muß es nach dem Satz eine Summe Konjugierter sein und wird damit ein Element aus $\mathfrak{B}$.

¹⁸⁾ Nicht invariant wäre die hier mögliche Formulierung vermöge einer definierenden Gleichung und der Zerlegung des entsprechenden Polynoms in Linearfaktoren.

4. Komplementäre Basen von $\mathfrak{R}$ und ihr Zusammenhang mit den Komponenten der Einheit. Geht man von der invarianten Struktur zu einer Basisdarstellung über, so vermittelt diese Struktur eine Zusammenfassung der Basen in Paare komplementärer:

Satz. Jeder P -Basis $t_1, \dots, t_n$ von $\mathfrak{R}$ ist eine komplementäre $T_1, \dots, T_n$ in $\mathfrak{R}$ zugeordnet, deren komplementäre wieder die ursprüngliche der t wird. Die zu der komplementären Basis $T_1, \dots, T_n$ isomorphen Basen $A_1^{(i)}, \dots, A_n^{(i)}$ von $K^{(i)}$ sind definiert als die Koeffizienten der Einheitskomponenten $e^{(i)}$ in der durch die t vermittelten Basisdarstellung

$$e^{(i)} = A_1^{(i)} t_1 + \dots + A_n^{(i)} t_n.$$

Sind $\alpha_1^{(i)}, \dots, \alpha_n^{(i)}$ die den t_i entsprechenden Basen, so werden die Matrizen der α und A reziprok. Hängen zwei Basen (s) und (t) von $\mathfrak{R}$ durch eine Transformation

$$(s) = (t) P$$

zusammen, so besteht zwischen den komplementären die kontragrediente Beziehung

$$(S) = P^{-1}(T).$$

Beweis. Seien $e^{(i)} = A_1^{(i)} t_1 + \dots + A_n^{(i)} t_n$ die Basisdarstellungen der n Komponenten $e^{(i)}$ der Einheit, bei Zugrundelegung einer P -Basis $t_1, \dots, t_n$ von $\mathfrak{R}$, die also Γ -Basis von $\mathfrak{R}_\Gamma$ wird. Nach 2 und 3 liegen die $A_1^{(i)}, \dots, A_n^{(i)}$ in $K^{(i)}$, und den verschiedenen $e^{(i)}$ entsprechen konjugierte Koeffizientensysteme A . Bedeutet $\alpha_1^{(i)}, \dots, \alpha_n^{(i)}$ die den $t_1, \dots, t_n$ in $K^{(i)}$ isomorph zugeordnete Basis, so gelten die weiteren Relationen:

$$(1) \quad e^{(i)} [t \rightarrow \alpha^{(i)}] = e; \quad e^{(i)} [t \rightarrow \alpha^{(j)}] = 0 \quad \text{für } i \neq j.$$

Denn $\mathfrak{P}_{K^{(i)}}^{(i)}$ enthält die Elemente $t_1 - \alpha_1^{(i)}, \dots, t_n - \alpha_n^{(i)}$ — die eine abhängige P -Modulbasis von $\mathfrak{P}_{K^{(i)}}^{(i)}$ bilden —, verschwindet also bei der Substitution $t = \alpha^{(i)}$. Somit folgt aus

$$e \equiv e^{(i)} (\mathfrak{P}_{K^{(i)}}^{(i)})$$

die erste Relation (1), während die zweite daraus folgt, daß $e^{(i)}$ Element aller $\mathfrak{P}_{K^{(j)}}^{(j)}$ ist für $i \neq j$. Nach Koeffizienten aufgelöst lassen sich die Relationen (1) in Matrizenform schreiben:

$$(2) \quad \begin{pmatrix} \alpha_1^{(1)} & \dots & \alpha_n^{(1)} \\ \dots & \dots & \dots \\ \alpha_1^{(n)} & \dots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} A_1^{(1)} & \dots & A_n^{(1)} \\ \dots & \dots & \dots \\ A_1^{(n)} & \dots & A_n^{(n)} \end{pmatrix} = E_n,$$

wo E_n die Einheitsmatrix bedeutet; dadurch sind die A durch die α schon eindeutig bestimmt. Diese Relation (2) zeigt, daß die Determinante der beiden Matrizen nicht verschwindet. Sie zeigt weiter, daß $A_1^{(i)}, \dots, A_n^{(i)}$ linear unabhängig in Bezug auf P wird; denn eine lineare Abhängigkeit wäre auch für die konjugierten Systeme erfüllt, würde also den Rang der A -Matrix verringern, im Widerspruch dazu, daß der Rang von E_n gleich n ist. Es bildet also jeweils $A_1^{(i)}, \dots, A_n^{(i)}$ eine Basis von $K^{(i)}$; da diese Basen konjugiert sind, sind sie alle derselben Basis $T_1, \dots, T_n$ aus $\mathfrak{R}$ isomorph, wobei T_λ nach 3 durch

$$T_\lambda = A_\lambda^{(1)} e^{(1)} + \dots + A_\lambda^{(n)} e^{(n)}$$

bestimmt ist. Die Basis $T_1, \dots, T_n$ wird als die zu $t_1, \dots, t_n$ komplementäre bezeichnet, entsprechend $A_1^{(i)}, \dots, A_n^{(i)}$ als zu $\alpha_1^{(i)}, \dots, \alpha_n^{(i)}$ komplementär. Da die A vermöge (2) schon eindeutig bestimmt sind und diese Relation — durch Übergang zur transponierten Matrix — aus der Basis der T , also der A , die α bestimmt, wird die ursprüngliche Basis der t die komplementäre der T . Vermöge der durch die Komponenten der Einheit

bewirkten Zuordnung zerfallen also alle Basen in Paare komplementärer. Ist s, S ein weiteres Paar komplementärer Basen mit

$$e^{(i)} = B_1^{(i)} s_1 + \cdots + B_n^{(i)} s_n \quad \text{und} \quad (s) = (t) P,$$

so folgt aus

$$A_1 t_1 + \cdots + A_n t_n = B_1 s_1 + \cdots + B_n s_n$$

— identisch in t nach der Substitution $(s) = (t) P$ —, daß B, A sich kontragredient zu den s, t transformieren. Also gilt wegen des Isomorphismus das gleiche für S und T . Damit ist der Satz in allen Teilen bewiesen.

Bemerkung. Ist $c = C_1 t_1 + \cdots + C_n t_n$ die Darstellung eines Elementes aus $\mathfrak{R}$ vermöge einer P -Basis und $c = c_1 T_1 + \cdots + c_n T_n$ die Darstellung desselben Elementes vermöge der komplementären Basis, wo wird

$$C_\lambda = \text{Sp}(c T_\lambda), \quad c_\lambda = \text{Sp}(c t_\lambda),$$

unter $\text{Sp}(x)$ wie üblich die Summe der Konjugierten verstanden:

$$\text{Sp}(x) = \xi^{(1)} + \xi^{(2)} + \cdots + \xi^{(n)}$$

für beliebiges x aus $\mathfrak{R}$. Denn es wird

$$c = \gamma^{(1)} e^{(1)} + \cdots + \gamma^{(n)} e^{(n)} = \sum_{\lambda} \gamma^{(1)} A_\lambda^{(1)} t_\lambda + \cdots + \sum_{\lambda} \gamma^{(n)} A_\lambda^{(n)} t_\lambda,$$

wonach durch Koeffizientenvergleich sich $C_\lambda = \text{Sp}(c T_\lambda)$ ergibt. Die zweite Relation folgt entsprechend durch Vertauschen von t und $T^{19)}$.

§ 5. Zugrundelegung einer definierenden Gleichung. Lagrangesche Interpolationsformel. [Anm. bei der Herausgabe: Diese Nummer ist im Manuskript unausgefüllt geblieben.]

§ 6. Die Differente einer Ordnung.

Die nur auf Körper und ihre galoisschen Erweiterungsringe bezüglichen Struktursätze sollen jetzt im Sinn der *Ganzheit* verschärft werden durch Auszeichnung gewisser Unterringe von P und der in bezug auf sie ganzen Elemente in $\mathfrak{R}$ und K , der Ordnungen. Alle Bezeichnungen von § 5 werden beibehalten²⁰⁾.

1. Die zugrunde liegenden Ringe. Sei $\mathfrak{h}$ ein Unterring von P derart, daß P Quotientenkörper von $\mathfrak{h}$ wird; ferner sei $\mathfrak{h}$ *ganz-abgeschlossen* in P (jedes Element aus P , das ganz in bezug auf $\mathfrak{h}$ ist, gehört zu $\mathfrak{h}$). Es bedeute weiter $\mathfrak{D}$ eine $\mathfrak{h}$ -Ordnung aus $\mathfrak{R}$, d. h. einen $\mathfrak{h}$ umfassenden Unterring von $\mathfrak{R}$, dessen Quotientenkörper durch $\mathfrak{R}$ gegeben ist, und der eine endliche, nicht notwendig unabhängige $\mathfrak{h}$ -Modulbasis besitzt. Alle Elemente von $\mathfrak{D}$ werden dann ganz (in bezug auf $\mathfrak{h}$); die $\mathfrak{h}$ -Modulbasis wird zugleich — im allgemeinen abhängige — P -Modulbasis von $\mathfrak{R}$. Es bezeichne $\mathfrak{o}$ die zu $\mathfrak{D}$ isomorphe Ordnung in K , und $\mathfrak{o}^{(i)}$ die konjugierten in $K^{(i)}$. Der in Γ durch die n konjugierten Ordnungen erzeugte Ring sei $\mathfrak{g}$; dann wird auch $\mathfrak{g}$ Ordnung. Denn $\mathfrak{g}$ umfaßt $\mathfrak{h}$. Die Produkte

¹⁹⁾ Die Betrachtungen dieser Nummer zeigen, daß die invarianten Struktursätze wesentlich einfacher sind als die nichtinvarianten Basissätze. Letztere wurden nur gebraucht, um den Zusammenhang mit Bekanntem zu vermitteln. In der Tat leistet die Zerlegung des galoisschen Erweiterungsringes und die Heranziehung des Komponenten der Einheit alles, was die komplementären Basen (der komplementäre Modul im nächsten Paragraphen) leistet. Auch dort wird der Zusammenhang zwischen Differente und Komplementärmodul nur der Einordnung halber gegeben. Dasselbe gilt für die Betrachtung der Lagrangeschen Interpolationsformel unter 5.

²⁰⁾ Für die Begriffe ganz in bezug auf einen Ring und ganz abgeschlossen vgl. § 1 der in Fußnote ¹⁷⁾ zitierten Arbeit.

aller Elemente der $\mathfrak{h}$ -Basen der $\mathfrak{o}^{(i)}$ bilden eine $\mathfrak{h}$ -Basis von $\mathfrak{g}$ und zugleich eine $\mathbf{P}$ -Basis von Γ .

Es existieren die direkten Produkte $\mathfrak{D}_\mathfrak{o}$ und $\mathfrak{D}_\mathfrak{g}$, wie das hinreichende Kriterium § 2, 3 zeigt (der dortige Ring $\mathfrak{k}$ ist durch $\mathbf{P}$ zu ersetzen). In $\mathfrak{R}_\Gamma$ existiert vorerst das direkte Produkt $\mathfrak{D}_\mathbf{P} = \mathfrak{R}$ in bezug auf $\mathfrak{h}$. Denn $\mathfrak{h}$ liegt im Durchschnitt $[\mathfrak{D}, \mathbf{P}]$; umgekehrt ist jedes Durchschnittselement ganz als Element von $\mathfrak{D}$, also als Element von $\mathbf{P}$ wegen der ganzen Abgeschlossenheit in $\mathfrak{h}$ enthalten. Die linearen Verbindungen mit Koeffizienten aus $\mathbf{P}$ von irgend n linear unabhängigen Elementen aus $\mathfrak{D}$ ergeben jetzt $\mathfrak{R}$ als direktes Produkt. Ebenso wird

$$\mathfrak{o}_\mathbf{P} = \mathbf{K} \quad \text{und} \quad \mathfrak{g}_\mathbf{P} = \Gamma;$$

aus dem direkten Produkt $\mathfrak{R}_\mathbf{K} = \mathfrak{D}_\mathbf{P} \times \mathfrak{o}_\mathbf{P}$ in bezug auf $\mathfrak{h}$ folgt nach dem Kriterium § 2, 3 die Existenz von $\mathfrak{D}_\mathfrak{o}$ in bezug auf $\mathfrak{h}$; ebenso ergibt $\mathfrak{R}_\Gamma = \mathfrak{D}_\mathbf{P} \times \mathfrak{g}_\mathbf{P}$ die Existenz von $\mathfrak{D}_\mathfrak{g}$. Mit $\mathfrak{D}_\mathfrak{o}$ existieren auch die konjugierten Ringe $\mathfrak{D}_{\mathfrak{o}^{(i)}}$. Es wird $\mathfrak{D}_\mathfrak{g}$ als *galoisscher Erweiterungsring der Ordnung $\mathfrak{D}$* bezeichnet.

Die Differenten von $\mathfrak{D}$ bzw. $\mathfrak{o}$ in bezug auf $\mathfrak{h}$ ist also definiert; ebenso die konjugierten Differenten. Es bezeichne

$$\mathfrak{P} = \{\dots, y - \eta, \dots\}$$

das *Differenzenideal* von $\mathfrak{D}_\mathfrak{o}$, und

$$\mathfrak{P}^{(i)} = \{\dots, y - \eta^{(i)}, \dots\}$$

die konjugierten von $\mathfrak{D}_{\mathfrak{o}^{(i)}}$, ebenso

$$\mathfrak{A}^{(i)} = (0) : \mathfrak{P}^{(i)} \quad \text{— der Quotient genommen in } \mathfrak{D}_{\mathfrak{o}^{(i)}} \text{ —}$$

die konjugierten *Differenzenquotienten*, insbesondere

$$\mathfrak{A} = (0) : \mathfrak{P} \quad \text{in } \mathfrak{D}_\mathfrak{o}.$$

Weiter bezeichne

$$\mathfrak{D} = \mathfrak{A}[\eta \rightarrow y]$$

die Differenten von $\mathfrak{D}$, und

$$\mathfrak{d}^{(i)} = \mathfrak{A}[y \rightarrow \eta^{(i)}]$$

die *Differenten* der n konjugierten Ordnungen $\mathfrak{o}^{(i)}$, insbesondere

$$\mathfrak{d} = \mathfrak{A}[y \rightarrow \eta]$$

die Differenten von $\mathfrak{o}^{21)}$.

2. Struktursätze. Dem Struktursatz für galoissche Erweiterungsringe von Körpern (§ 5, 2) steht gegenüber:

Struktursatz für den galoisschen Erweiterungsring von Ordnungen. *Differenzenideal und Differenzenquotient in bezug auf Ordnung und Körper stehen in folgender Beziehung zueinander: Es wird $\mathfrak{P}_\mathbf{K}$ Erweiterung des Differenzenideals $\mathfrak{P}$ von $\mathfrak{D}_\mathfrak{o}$ und ebenso $\mathfrak{A}_\mathbf{K}$ Erweiterung des Differenzenquotienten $\mathfrak{A}$ von $\mathfrak{D}_\mathfrak{o}$, dieser Verengung von $\mathfrak{A}_\mathbf{K}$. Zwischen Differenzenquotient und Differenten und Komponente der Einheit bestehen die Beziehungen*

$$\mathfrak{A} = \mathfrak{d}e^{(1)}, \quad \mathfrak{A}^{(i)} = \mathfrak{d}^{(i)}e^{(i)},$$

also

$$\mathfrak{d} = [\mathfrak{o}, \mathfrak{A}^{(1)} + \dots + \mathfrak{A}^{(n)}].$$

²¹⁾ Die Voraussetzung des in $\mathbf{P}$ ganz abgeschlossenen $\mathfrak{h}$ ist z. B. erfüllt, wenn $\mathfrak{h}$ die Hauptordnung eines Zahlkörpers, insbesondere $\mathfrak{h}$ das System der ganzen rationalen Zahlen ist; es sind also Differenten und Relativedifferenten beliebiger Ordnungen, auch in Relativkörpern, definiert. Weiter kann $\mathfrak{h}$ der Polynombereich von n Unbestimmten sein, was die Differenten in algebraischen Funktionenkörpern von n Unbestimmten ergibt.

Die Differentiale $\mathfrak{d}$ von $\mathfrak{o}$ besteht also aus allen Elementen κ von K derart, daß $\kappa e^{(1)}$ in $\mathfrak{D}_0$ liegt; sie ist vom Nullideal verschieden.

Daß $\mathfrak{P}_K$ Erweiterung von $\mathfrak{P}$, folgt daraus, daß $\mathfrak{R}$ gleich $\mathfrak{D}_P$ wird, ebenso K gleich $\mathfrak{o}_P$, so daß also jedes $x - \xi$ aus $\mathfrak{P}_K$ sich linear mit Koeffizienten aus K durch die $y - \eta$ aus $\mathfrak{P}$ ausdrücken läßt. Daraus folgt weiter, daß $\mathfrak{A}_K = (0) : \mathfrak{P}_K$ auch definiert ist als Quotient $(0) : \mathfrak{P}$ in $\mathfrak{R}_K$. Somit besteht $\mathfrak{A} = (0) : \mathfrak{P}$ in $\mathfrak{D}_0$ aus allen Elementen aus $\mathfrak{D}_0$, die zu $\mathfrak{A}_K$ gehören, $\mathfrak{A} = [\mathfrak{D}_0, \mathfrak{A}_K]$, also Verengung von $\mathfrak{A}_K$. Wegen $\mathfrak{A}_K = K e^{(1)}$ wird somit $\mathfrak{A} = \mathfrak{z} e^{(1)}$, wo $\mathfrak{z}$ ein $\mathfrak{o}$ -Modul in K , da $\mathfrak{A}$ ebenfalls $\mathfrak{o}$ -Modul. Nach Definition der Differentiale aber kommt:

$$\mathfrak{d} = \mathfrak{A} [x \rightarrow \xi] = (\mathfrak{z} e^{(1)}) [x \rightarrow \xi] = \mathfrak{z} (e^{(1)} [x \rightarrow \xi]) = \mathfrak{z} e = \mathfrak{z}$$

(vgl. § 5, 4, (1)). Also wird $\mathfrak{z} = \mathfrak{d}$; der Differenzenquotient $\mathfrak{A}$ wird Komponente in K der Differentiale $\mathfrak{d}$ von $\mathfrak{o}$, und entsprechend für die Konjugierten. Das zieht aber nach der Folgerung in § 5, 3 die obige Relation für $\mathfrak{d}$ nach sich. Und

$$\mathfrak{A} = \mathfrak{d} e^{(1)} = [K e^{(1)}, \mathfrak{D}_0]$$

zeigt, daß $\mathfrak{d}$ aus allen Elementen κ aus K besteht, für die $\kappa e^{(1)}$ in $\mathfrak{D}_0$. Damit wird aber $\mathfrak{d}$ vom Nullideal verschieden; denn $e^{(1)}$ ist als Element von $\mathfrak{R}_K = \mathfrak{D}_K$ eine lineare Verbindung endlich vieler Elemente aus $\mathfrak{D}$ mit Koeffizienten aus K , also Quotient eines Elementes aus $\mathfrak{D}_0$ durch ein solches aus $\mathfrak{o}$ (sogar aus $\mathfrak{h}$); dieser Nenner ergibt ein von Null verschiedenes Element von $\mathfrak{d}$. Damit wird aber $\mathfrak{d}$ vom Rang n in bezug auf P oder $\mathfrak{d}_P = K$, so daß $\mathfrak{A}_K$ Erweiterung von $\mathfrak{A}$ wird.

Von hier ab Skizze.

3. Zusammenhang mit Komplementärmodul bei unabhängiger Basis. Ist $t_1, \dots, t_n$ eine unabhängige $\mathfrak{h}$ -Basis von $\mathfrak{D}$, so auch jede Basis $(s) = (t)P$ von $\mathfrak{R}$, sobald P in $\mathfrak{h}$ und unimodular. Dann zeigt aber $(S) = P^{-1}(T)$, daß neben T auch S Basis ein und desselben $\mathfrak{h}$ -Moduls wird, der als Komplementärmodul von $\mathfrak{D}$ bezeichnet wird.

Der letzte Teil des Struktursatzes unter 2 sagt jetzt aus, daß $\mathfrak{d}$ gleich dem Quotienten $\mathfrak{o} : e$ in K wird, unter e den Komplementärmodul verstanden. Denn sei

$$e^{(1)} = A_1 t_1 + \dots + A_n t_n,$$

wo A_λ eine Basis von e ; dann besteht $\mathfrak{d}$ aus allen Elementen δ , für die $\delta e^{(1)}$ in $\mathfrak{D}_0$, d. h. δA_λ in $\mathfrak{o}$ oder $\mathfrak{d} = \mathfrak{o} : e$.

Spezialfall. Reguläre Ordnung mit $e, z, \dots, z^{n-1}$ als Modulbasis:

$$\mathfrak{d} = \{f'(z)\}.$$

Bemerkung. Aus der Bemerkung zu § 5, 4 folgt die weitere bekannte Definition des Komplementärmoduls $\mathfrak{G}$ von $\mathfrak{D}$. Es besteht $\mathfrak{G}$ aus allen Elementen c von $\mathfrak{R}$, für die die Spuren $\text{Sp}(ct)$, d. h. die Spuren $\text{Sp}(co)$ mit beliebigem o aus $\mathfrak{D}$, ganz, d. h. in $\mathfrak{h}$; entsprechend für e in bezug auf $\mathfrak{o}$ und K .

Denn sei $c = c_1 T_1 + \dots + c_n T_n$ mit c_i in $\mathfrak{h}$ eine Darstellung eines Elementes c aus $\mathfrak{G}$ durch die zu t komplementäre Basis von $\mathfrak{R}$. Dann wird $c_\lambda = \text{Sp}(ct_\lambda)$, also in $\mathfrak{h}$; und umgekehrt folgt aus $\text{Sp}(ct_\lambda)$ in $\mathfrak{h}$, daß c_λ in $\mathfrak{h}$, also c in $\mathfrak{G}$.

Zusatz. Wenn eine unabhängige $\mathfrak{h}$ -Modulbasis in der Ordnung existiert, so wird der Differenzenquotient $\mathfrak{A}^{(i)}$ Durchschnitt aller von $\mathfrak{P}^{(i)}$ verschiedenen Differenzenideale, genauer

$$\mathfrak{A}^{(i)} = [\mathfrak{D}_{\mathfrak{o}(t)}, \mathfrak{P}_\mathfrak{g}^{(1)}, \dots, \mathfrak{P}_\mathfrak{g}^{(i-1)}, \mathfrak{P}_\mathfrak{g}^{(i+1)}, \dots, \mathfrak{P}_\mathfrak{g}^{(n)}].$$

Denn nach der verschärften Fassung in § 2, 2 wird dann auch $\mathfrak{P}$ Verengungsideal von $\mathfrak{P}_K$; sei nämlich $e, t_2, \dots, t_n$ eine Modulbasis von $\mathfrak{D}$, also von $\mathfrak{D}_0$, dann auch

$$e, t_2 - \alpha_2, \dots, t_n - \alpha_n;$$

aber $t_2 - \alpha_2, \dots, t_n - \alpha_n$ ist zugleich K -Modulbasis von $\mathfrak{P}_K$. Also sind die Voraussetzungen § 2, 2 (Zusatz) erfüllt. Nun war aber

$$\mathfrak{A}_r = [\mathfrak{P}_r^{(2)}, \dots, \mathfrak{P}_r^{(n)}]; \mathfrak{A}_g = [\mathfrak{A}_r, \mathfrak{D}_g] = [\dots, [\mathfrak{P}_r^{(i)}, \mathfrak{D}_g], \dots] = [\mathfrak{P}_g^{(2)}, \dots, \mathfrak{P}_g^{(n)}].$$

Aber $\mathfrak{A} = [\mathfrak{A}_0, \mathfrak{D}_0]$; somit

$$\mathfrak{A} = [\mathfrak{D}_0, \mathfrak{P}_g^{(2)}, \dots, \mathfrak{P}_g^{(n)}].$$

4. Zusammenhang mit dem Differentialquotient einer Fundamentalgleichung, falls eine solche existiert. Erweitert man die Ordnung $\mathfrak{D}$ durch n Unbestimmte $u_1, \dots, u_n$, bildet also das direkte Produkt $\mathfrak{D}_u$, wo u den Polynombereich $\mathfrak{h}[u_1, \dots, u_n]$ bedeutet, also $\mathfrak{D}_u = \mathfrak{D}[u_1, \dots, u_n]$, so besteht die Erweiterung $\mathfrak{C}_u$ jedes Ideals aus $\mathfrak{D}$ aus allen Polynomen in u mit Koeffizienten aus $\mathfrak{C}$; und umgekehrt ist $\mathfrak{C}$ als das System aller Koeffizienten von $\mathfrak{C}_u$ charakterisiert.

Es bestehe nun eine Fundamentalgleichung; d. h. $e, U, \dots, U^{n-1}$ sollen eine $\mathfrak{h}$ -Modulbasis bilden bei Übergang zum Quotientenring durch ein oder mehrere primitive Polynome $H(u)$ in $\mathfrak{h}[u]$. Dann gehen die Ideale $\mathfrak{C}_u$ über in Systeme, die aus $\mathfrak{C}_u$ durch Multiplikation mit Einheiten ($H(u)$ und seinen negativen und positiven Potenzen) entstehen. Man kann also zur Zurückgewinnung von $\mathfrak{C}$ erst durch Multiplikation mit diesen Einheiten auf $\mathfrak{C}_u$ gelangen (in u ganz) und daraus zu $\mathfrak{C}$. Insbesondere gehe die Differenten $\mathfrak{D}$ von $\mathfrak{D}$ in $\mathfrak{D}_u$ über; wo also $\mathfrak{D}_u$ die Differenten von $\mathfrak{D}_u$. Aber in $\mathfrak{D}_u$ — durch Quotientenbildung mit primitiven $H(u)$ — existiert eine definierende Gleichung $G(U) = 0$. Also wird $G'(U)$ Basispolynom der Differenten, d. h. diese ist abgeleitet aus den Koeffizienten von $G'(U)$. (Es muß noch genauer gezeigt werden, daß $(G'(U))$ wirklich nur $\mathfrak{D}_u$ und nicht noch weiteres enthält; vielleicht nur bei ganzer Abgeschlossenheit von $\mathfrak{o}$ in K gültig. Es könnten ja durch Multiplikation mit Teilern von $H(u)$ noch weitere in $\mathfrak{D}_u$ gelegene Elemente als $\mathfrak{D}_u$ entstehen. Bei ganzer Abgeschlossenheit (5 Axiome) folgt es aus dem Satz, daß die Koeffizientenideale (Inhalte) sich multiplizieren. Damit wird eine Verzweigungstheorie durch Betrachtung der Fundamentalgleichung mod p möglich.)

§ 7. Verzweigungstheorie der Hauptordnung mod p^t .

Sei ein Zahlkörper zugrunde gelegt, $\mathfrak{h}$ seine ganze Zahlen; oder auch ein Relativkörper in bezug auf den Quotientenring der Hauptordnung nach einem Primideal, wo dann p das Basiselement des Primideals dieses Quotientenringes bedeutet. Die Adjunktion der Unbestimmten $u_1, \dots, u_n$ sei vorgenommen; dann besitzt sowohl die Hauptordnung wie der Restklassenring nach p^t die $\mathfrak{h}$ -Modulbasis $e, U, \dots, U^{n-1}$; also wird durch $G'(u)$ in beiden Fällen die Differenten gegeben. *Die Differenten der Hauptordnung geht mod p^t in diejenige des Restklassenringes nach p^t über* (gilt das für beliebige Ordnungen oder nicht?). Wenn aber $p = p_1^{e_1} \dots p_r^{e_r}$, so ist der Restklassenring $\mathfrak{R}$ nach p^t direkte Summe, wo die Komponenten isomorph den Restklassenringen nach $p_i^{t e_i}$, also

$$\mathfrak{R} = \mathfrak{R} e_1 + \dots + \mathfrak{R} e_r;$$

dabei wird e_k für $i \neq k$ durch $p_i^{t e_i}$ teilbar; wenn also

$$\mathfrak{d}[p^t] = \mathfrak{d}[p^t] e_1 + \dots + \mathfrak{d}[p^t] e_r = \mathfrak{d}_1 + \dots + \mathfrak{d}_r$$

und t genügend hoch, so geht p_i in δ_i zur selben Potenz auf wie in $\delta[p^t]$, also wie in δ . Nach § 4 aber wird δ_i die Differente von $\mathfrak{R}_i$; es genügt also, die Differente des Restklassenringes nach p^{et} zu betrachten. Sei ξ so gewählt (Zahlbericht, Satz 29 und 30), daß ξ ganze Zahl,

$$\varphi(\xi) \equiv 0(p), \not\equiv 0(p^2),$$

wo $\varphi(x)$ Primfunktion mod p vom Grade f . Ersetzt man (für $t \geq 2$) dies ξ durch $\xi^* = \xi e_1$, wo e_1 das erste in der Zerlegung des Restklassenringes $\mathfrak{R}$ mod p^t auftretende Idempotent ist, so wird neben $\varphi(\xi^*) \equiv 0(p), \not\equiv 0(p^2)$ sogar $p_1 \equiv (p, \varphi(\xi^*))$. Dann besteht eine Basis bezüglich der ganzen Zahlen mod p^t aus $\xi^\mu \varphi(\xi)^\nu$ mit $\mu = 0, 1, \dots, f-1$; $\nu = 0, 1, \dots, t-1$. Eine unabhängige $\mathfrak{h}$ -Basis (Restklassen nach p^t) ist gegeben durch

$$(1) \quad \xi^{\mu_0} \varphi(\xi)^{\nu_0} \text{ mit } \mu_0 = 0, 1, \dots, f-1; \nu_0 = 0, 1, \dots, t-1.$$

Denn $(\varphi(\xi), p^{et}) = p$; also wegen $(p) = p^e$ im Restklassenring kommt, wenn man von Hauptidealen zu Elementen übergeht: $\varphi(\xi) = pM(\xi)$, wo $M(\xi)$ Einheit im Restklassenring, d. h. $M(\xi) \not\equiv 0(p)$. Man kann also (wegen $p^t = 0$) sukzessive ξ^{et} durch niedrigere Potenzen ausdrücken, zuerst in $M(\xi)$ und dann im Restklassenring; also ist (1) tatsächlich Basis. Die definierende Gleichung in bezug auf diese Basis wird

$$F(x) = \varphi(x)^e + pM(x),$$

wo $M(x)$ mod p nicht durch $\varphi(x)$ teilbar (Ö. Ore, Math. Ann. 96, S. 348), also

$$M(\xi) \not\equiv 0(p).$$

Die Basis ist aber auch unabhängig; denn aus

$$a_0(\xi) + a_1(\xi) \varphi(\xi) + \dots + a_{e-1}(\xi) \varphi(\xi)^{e-1} \equiv 0(p^{te})$$

folgt $\equiv 0(p)$; damit $a_0(\xi) \equiv 0(p)$, also

$$a_0(x) \equiv 0(p);$$

durch Wegdivision von p folgt sukzessive

$$a_0(x) \equiv 0(p), \dots, a_{e-1}(x) \equiv 0(p)$$

und durch Wegdividieren von p dann

$$a_0(x) \equiv 0(p^2), \dots, a_{e-1}(x) \equiv 0(p^2)$$

usw. bis

$$a_0(x) \equiv 0(p^t), \dots, a_{e-1}(x) \equiv 0(p^t).$$

Damit aber wird die Differente des Restklassenringes gegeben durch den Polynomdifferentialquotienten $F'(\xi)$ — es ist alles auf Ore, S. 345, § 3 zurückgeführt. Aus: Ore, Satz 10 (vgl. Dedekind-Hensel) folgt, daß $p^t = p^n$ für jedes p genügt; weiter ergeben sich nach Ore die Supplementzahlen.

Es gilt zugleich alles — durch Übergang zum Quotientenring — für Relativedifferenten, womit Ore, Math. Ann. 97, S. 594, § 4 sich aus Ore, Math. Ann. 96 unmittelbar ergibt. Es kommen nur die Zusätze über die Ausdrückbarkeit der Differente des Oberkörpers als Produkt von Differente des Unterkörpers und Relativedifferenten hinzu (vgl. Einleitung dieser Arbeit).