GALOISSCHE THEORIE DER ALGEBRAISCHEN ZAHLKÖRPER UNENDLICHEN GRADES

Von

Mikao MORIYA

EINLEITUNG.

Die vorliegende Arbeit ist einerseits eine Ergänzung einer in Math. Ann. Bd. 108 erschienenen Arbeit[1] von HERBRAND und anderseits eine Fortsetzung von §7 meiner kürzlich erschienenen Arbeit[2] über die Theorie der algebraischen Zahlkörper unendlichen Grades. In jener Arbeit habe ich endliche normale Erweiterungskörper über einem algebraischen Zahlkörper unendlichen Grades in Betracht gezogen. Dagegen will ich in dieser Arbeit normale Erweiterungskörper unendlichen Grades über einem beliebigen algebraischen Zahlkörper (von endlichem oder unendlichem Grade) behandeln. Selbstverständlich ist dabei die Existenz solcher Erweiterungskörper vorausgesetzt[3].

Im folgenden ersten Paragraphen schicke ich als Vorbereitung einige Sätze über die Werte der Ideale voran, deren manche schon von HERBRAND bewiesen worden sind. Im zweiten Paragraphen behandle ich die algebraische Theorie der Normalkörper unendlichen Grades. Diese Theorie ist schon von Herrn KRULL[4] fast vollständig aufgebaut. Im dritten Paragraphen definiere ich die Zerlegungsgruppe und

(1) HERBRAND, Théorie arithmétique des corps de nombres de degré infini, II, Math. Ann., Bd. 108 (1933). Diese Arbeit zitiere ich mit H. II. Eine andere Arbeit von HERBRAND mit dem gleichen Titel, Math. Ann., Bd. 106 (1932), bezeichne ich mit H. I.

(2) MORIYA, Theorie der algebraischen Zahlkörper unendlichen Grades, Jour. Fac. Science, Hokkaido Imp. Univ., Ser. I, Vol. 3 (1935). Diese Arbeit zitiere ich mit M.

(3) Wenn der Grundkörper algebraisch abgeschlossen ist, so existiert kein algebraischer Erweiterungskörper mehr.

(4) KRULL, Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., Bd. 100 (1928). Ich zitiere diese Arbeit mit K.

Journal of the Faculty of Science, Hokkaido Imp. Univ., Ser. I, Vol. IV, No. 2, 1936.

Trägheitsgruppe eines Primideals wie HERBRAND. Im vierten Paragraphen werde ich die Verzweigungsgruppe, welche nach manchen Autoren auch die erste Verzweigungsgruppe genannt ist, etwas anders definieren als in der Arbeit von HERBRAND[1]. Für die höheren Verzweigungsgruppen ist die systematische Theorie leider bis heute noch nicht aufgebaut, weil man in algebraischen Zahlkörpern unendlichen Grades die Verzweigungsgruppen nicht mehr allgemein durch Kongruenz definieren kann, wie es üblich ist. Trotzdem werde ich doch die (erste) Verzweigungsgruppe vom gruppentheoretischen Standpunkte aus definieren. Diese anscheined etwas künstliche Definition ist dann gerechtfertigt, wenn man zum Verzweigungskörper (der Invariantenkörper der Verzweigungsgruppe) übergeht. Im Schlussparagraphen definiere ich, der Zerlegungs-, Trägheits- und Verzweigungsgruppe entsprechend, den Zerlegungs-, Trägheits- und Verzweigungskörper und untersuche, welche Primidealzerlegung in den drei oben genannten Körpern stattfindet.

§ 1. WERTE DER IDEALE.

In diesem Paragraphen bedeutet k durchweg einen algebraischen Zahlkörper (von endlichem oder unendliehem Grade über dem rationalen Zahlkörper) und K einen algebraischen (nicht notwendig galoisschen) Zahlkörper unendlichen Grades über k. Dann kann man immer eine Reihe der Körper $k = K_0, K_1, \ldots, K_n, \ldots$ von endlichem Grade über k finden, derart dass K_i in K_{i+1} enthalten ($i = 0, 1, \ldots, n, \ldots$) und der Körper K als der Vereinigungskörper dieser Körperreihe definiert wird. Bekanntlich ist für den Körper K die Wahl der Körperreihe nicht eindeutig, aber im folgenden nehmen wir eine beliebige Körperreihe $K_0, K_1, \ldots, K_n, \ldots$ heraus, und halten dann immer diese Körperreihe fest. Wir gebrauchen ferner die Bezeichnung $K = \{K_n\}$.

Nun betrachten wir in K ein Primideal $\mathfrak{P}$. Dann kann man nach § 6 von M. die normierte Bewertung Φ in bezug auf $\mathfrak{P}$ herstellen, weil

(1) H. II.

K ein algebraischer Zahlkörper ist, und infolgedessen als ein Vereinigungskörper von unendlich (abzählbar) vielen algebraischen Zahlkörpern endlichen Grades definiert ist. Wenn $\mathfrak{p}$ das durch $\mathfrak{P}$ teilbare Primideal aus k ist, dann will ich zeigen, dass die normierte Bewertung Φ eine Erweiterung der normierten Bewertung φ bezüglich $\mathfrak{p}$ ist. Denn alle Zahlen aus $\mathfrak{p}$ besitzen positive Bewertungen hinsichtlich Φ, weil $\mathfrak{P}$ ein Teiler von $\mathfrak{p}$ ist. Aber die zu $\mathfrak{p}$ primen ganzen Zahlen aus k gehören nicht zu $\mathfrak{P}$, besitzen also die Bewertungen 0 bezüglich Φ. Also ist Φ eine Bewertung in bezug auf $\mathfrak{p}$[1]. Ist ferner p die durch $\mathfrak{P}$ teilbare Primzahl, so ist $\Phi(p) = 1$, weil Φ die normierte Bewertung von $\mathfrak{P}$ ist. Also induziert Φ in k die normierte Bewertung von $\mathfrak{p}$. Da in k nur eine einzige normierte Bewertung von $\mathfrak{p}$ existiert[2], so ist unsere Behauptung bewiesen.

Bezeichnet man nun mit $\mathfrak{O}$ die Menge aller ganzen algebraischen Zahlen aus K, so ist für ein Ideal $\mathfrak{a}$ aus k $\mathfrak{a}\mathfrak{O}$[3] ein Ideal aus K. Ist φ bzw. Φ die normierte Bewertung des oben erwähnten Primideals $\mathfrak{p}$ bzw. $\mathfrak{P}$, so ist es klar, dass die untere Grenze von Bewertungen aller Zahlen aus $\mathfrak{a}$ in bezug auf Φ (also auch in bezug auf φ) nicht kleiner ist als der Wert[4] von $\mathfrak{a}\mathfrak{O}$ in bezug auf $\mathfrak{P}$. Es ist also

$$w_{\mathfrak{p}}(\mathfrak{a}) \geqq w_{\mathfrak{P}}(\mathfrak{a}\mathfrak{O})^{(5)} .$$

Sind α_i bzw. $\rho_i (i = 1, \ldots, r)$ die Zahlen aus $\mathfrak{a}$ bzw. $\mathfrak{O}$, so ist eine Zahl aus $\mathfrak{a}\mathfrak{O}$ von der Form

$$\alpha_1\rho_1 + \ldots\ldots\ldots + \alpha_r\rho_r .$$

Daher ist

$$\begin{aligned}\Phi(\alpha_1\rho_1 + \ldots\ldots + \alpha_r\rho_r) &\geqq \text{Min}\,(\Phi(\alpha_1\rho_1), \ldots\ldots, \Phi(\alpha_r\rho_r)) \\ &\geqq \text{Min}\,(\Phi(\alpha_1), \ldots\ldots, \Phi(\alpha_r)) \\ &\geqq \text{Min}\,(\varphi(\alpha_1), \ldots\ldots, \varphi(\alpha_r)) .\end{aligned}$$

(1) M. S. 164.
(2) M. S. 167.
(3) Dieses Ideal $\mathfrak{a}\mathfrak{O}$ nenne ich auch kurz „Ideal $\mathfrak{a}$ aus K".
(4) Für die Definition der Werte von Idealen siehe M. S. 167.
(5) $w_{\mathfrak{p}}$, $w_{\mathfrak{P}}$ bezeichnen resp. die Werte in bezug auf $\mathfrak{p}$, $\mathfrak{P}$.

Hieraus folgt sofort

$$w_{\mathfrak{p}}(\mathfrak{a}) \leqq w_{\mathfrak{P}}(\mathfrak{a}\mathfrak{O}) .$$

Also ist

$$w_{\mathfrak{p}}(\mathfrak{a}) = w_{\mathfrak{P}}(\mathfrak{a}\mathfrak{O}) .$$

Aus dem obigen Beweisgang folgt noch: *Wenn* $\mathfrak{a}$ *in bezug auf* $\mathfrak{p}$ *endlich ist, dann ist* $\mathfrak{O}\mathfrak{a}$ *auch endlich in bezug auf* $\mathfrak{P}$, *und umgekehrt*[1].

Im folgenden sprechen wir kurz ohne weitere Erklärung vom *Werte eines Primärideals* $\mathfrak{Q}$ (im Spezialfall kann $\mathfrak{Q}$ ein *Primideal* sein). Dieser bedeutet immer den Wert von $\mathfrak{Q}$ in bezug auf das zu $\mathfrak{Q}$ gehörige Primideal $\mathfrak{P}$. Als Bezeichnung gebrauchen wir oft w statt $w_{\mathfrak{P}}$. Der Ausdruck „*endlich*“ oder „*unendlich*“ über das Primärideal $\mathfrak{Q}$ ist auch auf dieses Primideal $\mathfrak{P}$ bezogen.

Satz 1. *Es sei* $\mathfrak{a}$ *ein ganzes Ideal aus* k *und* $\mathfrak{Q}$ *eine Primärkomponente von* $\mathfrak{a}$ *aus* K, *die zu einem Primideal* $\mathfrak{P}$ *gehört. Dann besitzt* $\mathfrak{Q}$ *den gleichen Wert mit* $\mathfrak{a}$, *und* $\mathfrak{Q}$ *ist endlich oder unendlich, je nachdem ob* $\mathfrak{a}$ *in* k *hinsichtlich des durch* $\mathfrak{P}$ *teilbaren Primideals* $\mathfrak{p}$ *endlich oder unendlich ist.*

Beweis. In K bedeutet das Ideal $\mathfrak{a}$ ein Ideal $\mathfrak{a}\mathfrak{O}$. Nach dem oben Bewiesenen ist $w_{\mathfrak{p}}(\mathfrak{a}) = w_{\mathfrak{P}}(\mathfrak{a}\mathfrak{O})$ und $\mathfrak{a}$, $\mathfrak{a}\mathfrak{O}$ sind beide zugleich endlich oder unendlich resp. in k, K. Da nach Satz 32 von M. $\mathfrak{a}\mathfrak{O}$ und $\mathfrak{Q}$ denselben Wert (in bezug auf $\mathfrak{P}$) besitzen, und zugleich endlich oder unendlich sind, so folgt ohne weiteres die Behauptung des Satzes.

Wir beweisen nun

Satz 2. *Es sei* $\mathfrak{Q}$ *ein ganzes Primärideal (Primideal) aus* K. *Dann ist der Durchschnitt* $\mathfrak{Q}'$ *von* $\mathfrak{Q}$ *mit einem Teilkörper* K' *von* K *über* k *auch ein Primärideal (Primideal) aus* K'.

Beweis. Dass $\mathfrak{Q}'$ ein Ideal aus K' ist, kann man leicht bestätigen. Ist für zwei ganze Zahlen α', β' aus K'

$$\alpha'\beta' \equiv 0 \quad \text{und} \quad \alpha' \not\equiv 0 \mod \mathfrak{Q}' ,$$

(1) Die Definition der endlichen Ideale findet man in S. 170 von M.

so ist selbstverständlich

$$\alpha'\beta' \equiv 0 \quad \text{und} \quad \alpha' \not\equiv 0 \quad \text{mod} \ \mathfrak{Q} .$$

Da aber $\mathfrak{Q}$ ein Primärideal ist, so gibt es eine natürliche Zahl ρ, so dass

$$\beta'^{\rho} \equiv 0 \quad \text{mod} \ \mathfrak{Q}^{(1)}$$

wird. Hieraus folgt $\beta'^{\rho} \equiv 0 \ \text{mod} \ \mathfrak{Q}'$, weil β'^{ρ} eine Zahl aus K' ist, w. z. b. w.

Da K als ein algebraischer Zahlkörper immer ein Vereinigungskörper von unendlich (abzählbar) vielen algebraischen Zahlkörpern von endlichem Grade ist, so kann man nach § 6 von M. schliessen, dass ein Primärideal aus K durch ein einziges Primideal teilbar ist. Diese Tatsache trifft auch für die Primärideale aus jedem Teilkörper von K über k zu.

Wenn insbesondere ein Primideal $\mathfrak{P}$ endlich ist, dann ist jedes zu $\mathfrak{P}$ gehörige ganze Primärideal aus K eine Potenz von $\mathfrak{P}$. Wir können nämlich annehmen, dass K als ein Vereinigungskörper von unendlich (abzählbar) vielen algebraischen Zahlkörpern von endlichem Grade $\mathfrak{R}_1$, $\mathfrak{R}_2$, ..., $\mathfrak{R}_n$, ... definiert ist. Dann ist ein endliches Primideal $\mathfrak{P}$ aus K ein Vereinigungsideal von $\mathfrak{P}_1$, $\mathfrak{P}_2$, ..., $\mathfrak{P}_n$, ..., wo $\mathfrak{P}_i = \mathfrak{P} \frown \mathfrak{R}_i \ (i \geqq 1)$ (das durch $\mathfrak{P}$ teilbare Primideal aus $\mathfrak{R}_i$) ist. Nach Definition der endlichen Primideale ist von einem Index i an

$$w(\mathfrak{P}_i) = w(\mathfrak{P}_{i+1}) = \ldots\ldots = w(\mathfrak{P}) ,$$

und $\mathfrak{P}_j$ ist genau durch $\mathfrak{P}_{j+1}$ teilbar $(j \geqq i)$[2].

Wenn $\mathfrak{Q}$ ein zu $\mathfrak{P}$ gehöriges ganzes Primärideal aus K ist, so ist

$$\mathfrak{Q} \frown \mathfrak{R}_n = \mathfrak{Q}_n = \mathfrak{P}_n^{a_n}{}^{(3)} .$$

---

(1) V. D. WAERDEN, Moderne Algebra, zweiter Teil, S. 31.
Wenn $\mathfrak{Q}$ insbesondere ein Primideal ist, dann ist bekanntlich $\rho = 1$.

(2) M. S. 171.

(3) M. S. 172.

Da $w(\mathfrak{Q}_1) \geqq w(\mathfrak{Q}_2) \geqq \ldots. \geqq w(\mathfrak{Q}_n) \geqq \ldots. \geqq w(\mathfrak{Q})$ ist[1], so ist nach § 6 von M.

$$\frac{a_i}{u_i} \geqq \frac{a_{i+1}}{u_{i+1}} \geqq \ldots. \geqq \frac{a_n}{u_n} \geqq \ldots. \geqq w(\mathfrak{Q}) .$$

Dabei bedeutet u_n den genauen Exponenten von $\mathfrak{P}_n$ in der zu $\mathfrak{P}$ gehörigen Primzahl p, und es ist $\frac{1}{u_n} = w(\mathfrak{P}_n)$. Da nach Voraussetzung

$$w(\mathfrak{P}_i) = w(\mathfrak{P}_{i+1}) = \ldots. = w(\mathfrak{P}) \leqq w(\mathfrak{Q})$$

ist, so ist die abnehmende Folge

$$\frac{a_1}{u_1}, \frac{a_2}{u_2}, \ldots., \frac{a_n}{u_n}, \ldots.$$

nach unten beschränkt, besitzt sie also den Grenzwert. Da aber a_1, a_2, ..., a_n, ... natürliche Zahlen und $u_i = u_{i+1} = \ldots. = u_n = \ldots.$ sind, so kann man leicht bestätigen, dass für hinreichend grosses N immer

$$a_m = a \neq 0$$

ist, falls $m > N$ ist.

Nun wollen wir zeigen, dass $\mathfrak{Q} = \mathfrak{P}^a$ ist. Offenbar enthält $\mathfrak{P}^a$ für $m > N$ $\mathfrak{P}_m^a$. Also ist $\mathfrak{Q}$ durch $\mathfrak{P}^a$ teilbar, weil $\mathfrak{Q}_m = \mathfrak{P}_m^{a_m} < \mathfrak{P}^a$ ist. Umgekehrt ist eine beliebige Zahl α aus $\mathfrak{P}^a$ von der Form $\sum_{i=1}^{r} \alpha_i^{(1)} \ldots \alpha_i^{(a)}$, wo $\alpha_i^{(k)}$ $(k = 1, \ldots., a)$ die Zahlen aus $\mathfrak{P}$ bedeuten. Wenn man für $m > N$ den Index m hinreichend gross wählt, dann gehört jedes $\alpha_i^{(k)}$ zum Primideal $\mathfrak{P}_m$ aus $\mathfrak{R}_m$. Also ist α eine Zahl aus $\mathfrak{P}_m^a$. Dies zeigt aber, dass die Zahl α zu $\mathfrak{Q}$ gehört. Also ist $\mathfrak{P}^a$ durch $\mathfrak{Q}$ teilbar. Daher muss

$$\mathfrak{Q} = \mathfrak{P}^a$$

sein. Also erhält man folgenden Satz:

---

(1) Hierbei bedeutet w den Wert in bezug auf das Primideal $\mathfrak{P}$.

Satz 3. *Wenn ein Primideal* $\mathfrak{P}$ *aus* K *endlich ist, dann ist jedes zu* $\mathfrak{P}$ *gehörige ganze Primärideal eine Potenz von* $\mathfrak{P}$.

Hieraus folgt noch:

Zusatz. Ist $\mathfrak{P}$ ein endliches Primideal aus K, so ist dann und nur dann

$$\mathfrak{P}^a = \mathfrak{P}^b ,$$

wenn $a = b$ ist.

Denn nach dem früher Gezeigten sind von einem geeigneten Index I an

$$\mathfrak{P}^a \cap \mathfrak{R}_j = \mathfrak{P}_j^a \qquad \text{und} \qquad \mathfrak{P}^b \cap \mathfrak{R}_j = \mathfrak{P}_j^b \qquad (j \geqq I) .$$

Wenn aber $\mathfrak{P}^a = \mathfrak{P}^b$ ist, dann muss zugleich $\mathfrak{P}_j^a$ durch $\mathfrak{P}_j^b$, und $\mathfrak{P}_j^b$ durch $\mathfrak{P}_j^a$ teilbar sein, ist also $a = b$. Wenn umgekehrt $a = b$ ist, dann ist offenbar $\mathfrak{P}^a = \mathfrak{P}^b$.

Wir betrachten nun im Körper K ein ganzes Primärideal $\mathfrak{Q}$ und bezeichnen mit $\mathfrak{Q}_n$ den Durchschnitt $\mathfrak{Q} \cap K_n$ von $\mathfrak{Q}$ mit K_n . Dann ist nach Definition des Wertes

$$w(\mathfrak{Q}_0) \geqq w(\mathfrak{Q}_1) \geqq \ldots . \geqq w(\mathfrak{Q}) .$$

Da jede Zahl aus $\mathfrak{Q}$ schon in einem geeigneten $\mathfrak{Q}_n$ enthalten sein muss, so ist $w(\mathfrak{Q})$ offenbar der Grenzwert der Zahlfolge

$$w(\mathfrak{Q}_0) , \ldots . , w(\mathfrak{Q}_n) , \ldots .$$

Wenn insbesondere von einem Index i an immer

$$w(\mathfrak{Q}_j) > w(\mathfrak{Q}_{j+1})$$

$(j \geqq i)$ ist, dann ist $\mathfrak{Q}$ ein unendliches Primärideal. Denn sonst gäbe es in $\mathfrak{Q}$, also schon in einem geeigneten $\mathfrak{Q}_\varkappa (\varkappa \geqq 0)$, eine Zahl α, deren Bewertung gleich $w(\mathfrak{Q})$ wäre. Hieraus folgte

$$w(\mathfrak{Q}_\varkappa) = w(\mathfrak{Q}_{\varkappa+1}) = \ldots . = w(\mathfrak{Q}) ,$$

was Widerspruch wäre.

Ist nun aber von einem Index i an immer

$$w(\mathfrak{Q}_j) = w(\mathfrak{Q}_{j+1}) \qquad (j \geqq i),$$

so gibt es einen Index $\nu\,(\nu \geqq i)$ derart, dass $\mathfrak{Q}_\nu, \mathfrak{Q}_{\nu+1}, \ldots$. resp, in $K_\nu, K_{\nu+1}, \ldots$. endliche Ideale sind, falls $\mathfrak{Q}$ in K endlich ist. Denn in diesem Fall existiert in $\mathfrak{Q}$ eine Zahl α, deren Bewertung gleich $w(\mathfrak{Q})$ ist. Da aber α schon einem geeigneten Ideal $\mathfrak{Q}_\nu\,(\nu \geqq i)$ angehört, und $w(\mathfrak{Q}_\nu) = w(\mathfrak{Q}_{\nu+1}) = \ldots. = w(\mathfrak{Q})$ ist, so folgt die Behauptung.

Wenn dagegen $\mathfrak{Q}$ unendlich ist, dann müssen $\mathfrak{Q}_i, \mathfrak{Q}_{i+1}, \ldots.$ ersichtlich unendlich sein, weil $w(\mathfrak{Q}_i) = w(\mathfrak{Q}_{i+1}) = \ldots. = w(\mathfrak{Q})$ und $\mathfrak{Q}_i < \mathfrak{Q}_{i+1} < \ldots. < \mathfrak{Q}$ ist. Damit ist bewiesen:

Satz 4. *Es sei $\mathfrak{Q}$ ein ganzes Primärideal (Primideal) aus K und $\mathfrak{Q}_n = \mathfrak{Q} \frown K_n$. Dann gilt:*

1.) Die Zahlfolge

$$w(\mathfrak{Q}_1), w(\mathfrak{Q}_2), \ldots., w(\mathfrak{Q}_n), \ldots.$$

nicht zunehmend.

2.) $w(\mathfrak{Q})$ ist der Grenzwert der obigen Zahlfolge.

a.) $\mathfrak{Q}$ ist ein unendliches Ideal, falls von einem Index an die obige Zahlfolge wirklich abnehmend ist.

b.) Wenn von einem Index an die Glieder der obigen Zahlfolge sämtlich gleich sind, so sind von einer gewissen Stelle ν an die Primärideale $\mathfrak{Q}_\nu, \mathfrak{Q}_{\nu+1}, \ldots.$ endlich oder unendlich, je nachdem ob $\mathfrak{Q}$ endlich oder unendlich ist[1].

Nun ziehen wir zunächst den Fall in Betracht, dass der Grundkörper k ein endlicher algebraischer Zahlkörper ist. In diesem Fall findet für ein beliebiges Primideal $\mathfrak{p}$ aus k folgende Primidealzerlegung in K_i statt:

$$\mathfrak{p} = \mathfrak{P}_{i1}^{e_{i1}} \ldots. \mathfrak{P}_{ir_i}^{e_{ir_i}},$$

(1) H. II. S. 701.

wobei $\mathfrak{P}_{i1}, \ldots, \mathfrak{P}_{ir_i}$ Primideale aus K_i bedeuten. Aber die obige Primidealzerlegung bleibt auch gültig, wenn k ein unendlicher algebraischer Zahlkörper ist, und zwar ist $\mathfrak{p}$ genau durch $\mathfrak{P}_{i\rho}^{e_{i\rho}}$ teilbar, d.h. $e_{i\rho}$ ist der genaue Exponent von $\mathfrak{P}_{i\rho}$ in $\mathfrak{p}$ $(\rho = 1, \ldots, r_i)$, falls $\mathfrak{p}$ ein endliches Primideal aus k ist, und die obige Zerlegung ist eindeutig[1].

Wenn aber $\mathfrak{p}$ ein unendliches Primideal aus k ist, dann ist diese Zerlegung nicht mehr eindeutig. Aber in diesem Fall kann man auch den Exponenten $e_{i\rho}$ eines Primteilers $\mathfrak{P}_{i\rho}$ von $\mathfrak{p}$ eindeutig definieren, welcher im gewissen Sinne—und sogar wenn k von endlichem Grade ist, völlig—mit dem gewöhnlichen Exponenten eines Primideals aus einem endlichen algebraischen Zahlkörper übereinstimmt[2]. Wenn also $e_{i\rho}$ die Exponenten von $\mathfrak{P}_{i\rho}$ in $\mathfrak{p}$ bedeuten $(\rho = 1, \ldots, r_i)$, dann ist die Primidealzerlegung

$$\mathfrak{p} = \mathfrak{P}_{i1}^{e_{i1}} \ldots \mathfrak{P}_{ir_i}^{e_{ir_i}}$$

jedenfalls eindeutig.

Ferner kann man auf jeden Fall für ein Primideal aus K_i seinen Grad (genauer gesagt „Relativgrad“) nach k definieren.

Wenn man nun mit $e_{i\rho}$ bzw. $f_{i\rho}$ den Exponenten bzw. Grad von $\mathfrak{P}_{i\rho}$ nach k bezeichnet, dann gilt

$$n_i = \sum_{\rho=1}^{r_i} e_{i\rho} f_{i\rho} \quad ,^{(3)}$$

wo n_i der Grad von K_i nach k ist.

Ist p die durch $\mathfrak{p}$ teilbare Primzahl ist, dann heisst der zu p prime, grösste Teiler $e_{i\rho}^{(0)}$ von $e_{i\rho}$ der reduzierte Exponent von $\mathfrak{P}_{i\rho}$ in $\mathfrak{p}$.

Es seien $K_i \subset K_j$ zwei Teilkörper aus der Körperreihe von $K = \{K_n\}$, $\mathfrak{P}_i$, $\mathfrak{P}_j$ resp. Primideale aus K_i, K_j, und $\mathfrak{P}_i$ durch $\mathfrak{P}_j$ teilbar. Dann ist der Grad von $\mathfrak{P}_j$ nach k durch den von $\mathfrak{P}_i$ nach k teilbar. Und dies gilt auch für den reduzierten Exponenten bzw. den Exponenten von $\mathfrak{P}_i$ und $\mathfrak{P}_j$[4].

(1) H. I. S. 481.
(2) H. I. S. 484.
(3) H. I. S. 484.
(4) H. I. S. 485.

Nun wollen wir den *Grad*, den *reduzierten Exponenten* und den *Exponenten* eines Primteilers $\mathfrak{P}$ von $\mathfrak{p}$ aus K definieren. Dafür betrachten wir einen Teilkörper K_i aus der Körperreihe $K_1, K_2, \ldots, K_n, \ldots$ von K. Sind f_i, $e_i^{(0)}$, e_i resp. der Grad, der reduzierte Exponent und der Exponent von $\mathfrak{P}_i = \mathfrak{P} \cap K_i$ nach k, so definiere ich

$$F = \lim_{i=\infty} f_i, \quad E^{(0)} = \lim_{i=\infty} e_i^{(0)}, \quad E = \lim_{i=\infty} e_i$$

resp. als den *Grad*, den *reduzierten Exponenten* und den *Exponenten* von $\mathfrak{P}$ nach k.

Da $f_j \geqq f_i$ $(j > i)$ ist, so existiert jedenfalls

$$\lim_{i=\infty} f_i,$$

wenn man $\lim_{i=\infty} f_i$ das Symbol ∞ zuordnet, falls f_i über alle Grenzen wächst. Dasselbe trifft auch für den reduzierten Exponenten und den Exponenten von $\mathfrak{P}$ zu.

Ferner kann man leicht zeigen, dass der Grad, der reduzierte Exponent und der Exponent von $\mathfrak{P}$ nach k ganz unabhängig von der Wahl der Körperreihe $K_1, \ldots, K_n, \ldots$ von K über k sind[1]. Sie sind also durch ein Primideal $\mathfrak{P}$ eindeutig bestimmt. Wenn eine ganze rationale Zahl a in irgendeinem von $f_1, f_2, \ldots, f_n, \ldots$ (ebenfalls von $e_1^{(0)}, e_2^{(0)}, \ldots, e_n^{(0)}, \ldots$ oder $e_1, e_2, \ldots, e_n, \ldots$) aufgeht, dann heisse „*F durch a teilbar*“ (ebenfalls „*$E^{(0)}$*“ oder „*E durch a teilbar*“). Sonst heisse „*a prim zu F*“ (ebenfalls „*a prim zu $E^{(0)}$*“ oder „*E*“).

Es gilt nun folgender

Satz 5. *Es sei $\mathfrak{p}$ ein Primideal aus k, $\mathfrak{Q}$ eine Primärkomponente von $\mathfrak{p}$ in K, und $\mathfrak{P}$ das zu $\mathfrak{Q}$ gehörige Primideal aus K. Dann gilt:*

1.) $\mathfrak{Q}$ ist unendlich, falls $\mathfrak{p}$ (in k) unendlich ist. Es ist $\mathfrak{P} = \mathfrak{Q}$.

2.) $\mathfrak{P}$ ist endlich, falls $\mathfrak{p}$ (in k) endlich und der Exponent e von $\mathfrak{P}$ in $\mathfrak{p}$ endlich ist. Es ist $\mathfrak{Q} = \mathfrak{P}^e$.

(1) H. II. S. 702. Am Beweis von HERBRAND haften Druckfehler.

3.) $\mathfrak{P}$ *ist unendlich und* $\mathfrak{Q}$ *endlich, wenn* $\mathfrak{p}$ *endlich und der Exponent e von* $\mathfrak{P}$ *in* $\mathfrak{p}$ *unendlich ist*[1].

Beweis. Ist $\mathfrak{p}$ in k unendliches Primideal, so ist $w_{\mathfrak{p}}(\mathfrak{p}) = 0$[2]. Nach Satz 1 ist also $w_{\mathfrak{P}}(\mathfrak{Q}) = w_{\mathfrak{p}}(\mathfrak{p}) = 0$ und $\mathfrak{Q}$ ein unendliches Ideal aus K. Nach unserer Festsetzung kann man einfach $w(\mathfrak{Q}) = 0$ setzen. Da aber $w(\mathfrak{P}) \geqq 0$ ist, und aus $\mathfrak{P} \mid \mathfrak{Q}$ $w(\mathfrak{Q}) \geqq w(\mathfrak{P})$ folgt, so ist

$$w(\mathfrak{P}) = 0 .$$

Da $w(\mathfrak{P}) = w(\mathfrak{Q}) = 0$ und $\mathfrak{P}$, $\mathfrak{Q}$ beide unendliche Ideale sind, so ist nach Satz 31 von M. $\mathfrak{P} = \mathfrak{Q}$.

Wenn allgemein $\mathfrak{p}$ in k endlich ist, dann ist $\mathfrak{P}_n = \mathfrak{P} \frown K_n$ endlich (in K_n) und $w(\mathfrak{p}) = w(\mathfrak{P}_n^{e_n})$. Denn nach H. I. S. 481 ist $\mathfrak{P}_n$ in K_n endlich und $\mathfrak{P}_n^{e_n}$ eine Primärkomponente von $\mathfrak{p}$ in K_n, wo e_n den Exponenten von $\mathfrak{P}_n$ in $\mathfrak{p}$ bedeutet, und hieraus folgt wie für Satz 1

$$w(\mathfrak{p}) = e_n w(\mathfrak{P}_n) .$$

Da $\mathfrak{P} = \{ \mathfrak{P}_n \}$ ist, so ist nach Satz 4 $\lim\limits_{n\to\infty} w(\mathfrak{P}_n) = w(\mathfrak{P})$.

Im Fall 2.) gibt es nach Voraussetzung einen Index i, derart, dass für jede natürliche Zahl $n \geqq i$ $e_n = e$ ist. Also ist $w(\mathfrak{P}_n) = \frac{w(\mathfrak{p})}{e}$ und infolgedessen

$$w(\mathfrak{P}) = \lim_{n\to\infty} w(\mathfrak{P}_n) = \frac{w(\mathfrak{p})}{e} \neq 0 ,$$

weil $\mathfrak{p}$ in k ein endliches Ideal ist. Also muss $\mathfrak{P}$ auch endlich sein, weil sonst $w(\mathfrak{P}) = 0$ sein müsste[3]. Nach Satz 3 folgt weiter

$$\mathfrak{Q} = \mathfrak{P}^e .$$

Denn nach Satz 3 ist die Primärkomponente $\mathfrak{Q}$ eine bestimmte Potenz von $\mathfrak{P}$, weil es ein ganzes Primärideal ist. Es sei also $\mathfrak{Q} = \mathfrak{P}^a$. Dann

(1) H. II. S. 703.
(2) Siehe etwa M. S. 171.
(3) Siehe etwa M. S. 171.

ist nach Satz 1 $w(\mathfrak{p}) = w(\mathfrak{P}^a) = aw(\mathfrak{P})$. Da aber $ew(\mathfrak{P}) = w(\mathfrak{p})$ ist, so ist $a = e$, w. z. b. w.

Im Fall 3.) ist $w(\mathfrak{P}) = 0$, weil $\lim_{n\to\infty} e_n = \infty$ ist, d.h. $\mathfrak{P}$ ist unendliches Ideal. Trotzdem ist nach Satz 1 die Primärkomponente $\mathfrak{Q}$ von $\mathfrak{p}$ endliches Ideal.

§ 2. NORMALKÖRPER UNENDLICHEN GRADES.

In diesem Paragraphen betrachten wir besonders einen Normalkörper N von unendlichem Grade über k. Nach Herrn KRULL[1] kann man dabei eine Körperreihe $N_0 = k \subseteq N_1 \subseteq \ldots \subseteq N_n \subseteq \ldots$ finden, derart dass jeder Körper N_i normal und von endlichem Grade über k ist. Ebenso wie für endliche normale Erweiterungskörper kann man die Automorphismen von N über k definieren. Und zwar ist ein Automorphismus J von N über k durch eine sogenannte reguläre Abbildungsfolge $J_1, J_2, \ldots, J_n, \ldots$ definiert. Dabei bedeutet $J_n (n \geqq 1)$ einen Automorphismus von N_n über k und ausserdem ist J_{n+1} stets eine Erweiterung von J_n, d.h. J_{n+1} induziert in N_n den Automorphismus J_n. Dadurch wirkt J auf die Zahlen aus N_n wie der Automorphismus J_n von N_n über k ein. Offenbar ist diese reguläre Abbildungsfolge durch einen Automorphismus J von N über k eindeutig bestimmt, wenn man die Körperreihe festsetzt. Umgekehrt, wenn eine reguläre Abbildungsfolge vorliegt, dann bestimmt sie auch einen Automorphismus von N über k.

Selbstverständlich kann man für einen bestimmten Normalkörper N über k verschiedene Körperreihen und infolgedessen für einen Automorphismus J auch verschiedene reguläre Abbildungsfolgen bilden. Aber im folgenden legen wir stets eine beliebige Körperreihe $N_1, N_2, N_n, \ldots$ fest, und die reguläre Abbildungsfolge eines Automorphismus J von N über k wird danach durch diese Körperreihe bestimmt. Zur Abkürzung benutzen wir für einen Automorphismus J, welcher durch die reguläre Abbildungsfolge $J_1, J_2, \ldots, J_n, \ldots$ bestimmt ist, folgende Bezeichnung: $J = \{J_n\}$.

(1) Folgende Ausführung von Herrn KRULL findet man im Buch, HAUPT, Einführung in die Algebra, Bd. II.

Es seien nun $J = \{J_n\}$ und $J' = \{J'_n\}$ zwei Automorphismen von N über k. Dann definieren wir die Komposition von J' und J als eine Nacheinanderausführung von J' und J, und bezeichnen sie mit JJ'. JJ' heisst auch das Produkt von J' mit J. Ohne Schwierigkeit kann man dabei bestätigen, dass der Automorphismus JJ' durch die Abbildungsfolge $\{J_nJ'_n\}$ definiert ist. Also bildet die Gesamtheit aller Automorphismen von N über k die sogenannte *galoissche Gruppe* von N nach k in bezug auf die oben definierte Komposition. Wir bezeichnen im folgenden die galoissche Gruppe von N nach k mit $\mathfrak{G}$.

Ist nun J_n ein beliebiger Automorphismus von N_n über k, so gibt es bekanntlich in N_{n+1} einen Automorphismus J_{n+1} über k von der Art, dass J_{n+1} in N_n den Automorphismus J_n induziert. Man kann weiter in N_{n+2} einen Automorphismus J_{n+2}, welcher eine Erweiterung von J_{n+1} ist, finden, u. s. w. Ferner seien $J_1, J_2, \ldots, J_{n-1}$ resp. die durch J_n in $N_1, N_2, \ldots, N_{n-1}$ induzierten Automorphismen. Dann kann man eine Abbildungsfolge

$$J_1, J_2, \ldots, J_{n-1}, J_n, J_{n+1}, \ldots$$

bilden, die in N einen Automorphismus J über k definiert. Offenbar induziert J in N_n den vorher gegebenen Automorphismus J_n. Damit ist gezeigt:

Die galoissche Gruppe $\mathfrak{G}$ von N nach k induziert in einem beliebigen Normalkörper N_n die ganze galoissche Gruppe von N_n nach k.

Es sei $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine Folge der Automorphismen aus $\mathfrak{G}$. Dann heisst diese Folge eine *Fundamentalfolge über k*, wenn es für einen beliebigen endlichen Teilkörper[1] K von N über k einen geeigneten Index ν[2] gibt, derart dass alle $J^{(\nu)}(J^{(\nu+l)})^{-1}$ $(l \geqq 0)$ den Körper K elementweise invariant lassen.

Es sei wieder $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine Folge der Automorphismen aus $\mathfrak{G}$, und J ein Automorphismus aus $\mathfrak{G}$, so dass für einen beliebigen endlichen Teilkörper K von N über k ein geeigneter Index ν existiert, derart dass für alle $\kappa \geqq \nu$ die

(1) Das heisst *K von endlichem Grade über k*.

(2) Der Index ν hängt vom Körper K ab.

$$J(J^{(\varkappa)})^{-1}$$

K elementweise invariant lassen. Dann heisse J der *Grenzautomorphismus* der obigen Folge, und man sagt auch, dass die obige Folge zu J *konvergiert.*

Eine konvergente Folge ist immer eine Fundamentalfolge und sie besitzt nur einen einzigen Grenzautomorphismus. Denn ist $J^{(1)}$, $J^{(2)}$, ..., $J^{(n)}$, ... zu J konvergiert, so gibt es für einen beliebigen endlichen Teilkörper K von N über k einen Index ν, so dass für alle $\kappa \geqq \nu$ die

$$J(J^{(\varkappa)})^{-1}$$

K elementweise invariant lassen. Hieraus folgt, dass für $\kappa \geqq \nu$

$$\left(J(J^{(\nu)})^{-1}\right)^{-1}\left(J(J^{(\varkappa)})^{-1}\right) = J^{(\nu)}(J^{(\varkappa)})^{-1}$$

sicher K elementweise invariant lässt, d. h. die obige konvergente Folge bildet eine Fundamentalfolge. Ist nun J' ein Grenzautomorphismus, so kann man für einen beliebigen endlichen Teilkörper K von N über k einen geeigneten Index ν finden, derart dass für $\kappa \geqq \nu$ $J(J^{(\varkappa)})^{-1}$ und $J'(J^{(\varkappa)})^{-1}$ K elementweise invariant lassen. Also ist K bei Ausübung von

$$J(J^{(\varkappa)-1})\left(J'(J^{(\varkappa)-1})\right)^{-1} = J(J')^{-1}$$

elementweise invariant. Da K ein beliebiger endlicher Teilkörper sein kann, so muss $J = J'$ sein. Denn ist $J \neq J'$, so kann man sicher eine Zahl α aus N finden, derart dass $\alpha^J \neq \alpha^{J'}$ wird. In einem α enthaltenden, endlichen Teilkörper K von N über k lässt $J(J')^{-1}$ nicht mehr α invariant, was aber Widerspruch ist. Also muss $J = J'$ sein.

Um praktisch zu entscheiden, ob eine gegebene Folge fundamental (konvergent) ist, nehmen wir eine beliebige Normalkörperreihe $k = N_0'$, N_1', ..., N_n', ... von N heraus, und wir brauchen nur zu prüfen, ob die gegebene Folge in bezug auf diese Körperreihe fundamental (konvergent) ist. Denn ist die gegebene Folge fundamental (konvergent), so muss sie hinsichtlich dieser Körperreihe fundamental (konvergent)

sein. Ist aber umgekehrt eine Folge fundamental (konvergent) in bezug auf N_0', N_1', ..., N_n', ..., so ist zunächst ein beliebiger endlicher Teilkörper von N über k in einem geeigneten Körper aus der obigen Körperreihe enthalten. Hieraus folgt ohne weiteres, dass die gegebene Folge fundamental (konvergent) ist.

Man soll aber hierbei beachten, dass die Begriffe der Fundamentalfolge und der Konvergenz wesentlich vom Grundkörper k abhängig sind.

Eine Gruppe heisse *abgeschlossen*, wenn die Grenzelemente aller Fundamentalfolgen aus dieser Gruppe auch sich selbst angehören.

Nun lautet nach Herrn KRULL der *Fundamentalsatz der galoisschen Theorie* folgendermassen:

Zu einem Teilkörper K von N über k gehört eine eindeutig bestimmte abgeschlossene Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$, und umgekehrt.

Bildet man nun den Durchschnitt $K_n = K \frown N_n$ von K mit N_n, so ist $K_0 = k$, K_1, ..., K_n, ... eine Körperreihe und $K_1 \subseteq K_2 \subseteq .... \subseteq K_n \subseteq .....$ Ferner ist der Körper K die Vereinigungsmenge von K_1, K_2, ...,K_n, ... Wir bezeichnen mit $\mathfrak{H}$ die K zugeordnete Untergruppe der galoisschen Gruppe $\mathfrak{G}$ von N nach k. Induzieren $\mathfrak{G}$ und $\mathfrak{H}$ in N_n resp. $\mathfrak{G}_n$ und $\mathfrak{H}_n$, so ist offenbar $\mathfrak{G}_n$ die galoissche Gruppe von N_n über k, und K_n ist der Invariantenkörper von $\mathfrak{H}_n$ in N_n. Denn der Körper K_n ist bei Anwendung von $\mathfrak{H}$ elementweise invariant, weil er ein Teilkörper von K ist. Da aber K_n in N_n enthalten ist, so ist K_n bei Ausübung von $\mathfrak{H}_n$ elementweise invariant. Umgekehrt, wenn eine Zahl aus N_n bei Anwendung aller Automorphismen aus $\mathfrak{H}_n$ invariant ist, dann ist sie offenbar invariant bei Anwendung aller Automorphismen aus $\mathfrak{H}$, weil $\mathfrak{H}$ auf die Zahlen aus N_n immer als $\mathfrak{H}_n$ einwirkt. Also gehört diese Zahl zu K, und folglich zu K_n. Also ist $\mathfrak{H}_n$ die K_n zugeordnete Untergruppe von $\mathfrak{G}_n$.

Wenn insbesondere $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ ist, dann sind alle $\mathfrak{H}_n$ Normalteiler von $\mathfrak{G}_n$ $(n = 1, ...)$, und umgekehrt. Sind nun alle $\mathfrak{H}_n$ Normalteiler von $\mathfrak{G}_n$, so sind offenbar alle K_n Normalteilkörper von N_n über k. Umgekehrt, wenn alle K_n Normalteilkörper von N_n sind, dann ist K ein Normalteilkörper von N über k. Denn ist α eine

Zahl aus K, so gehört α schon zu einem geeigneten Teilkörper K_n. Da K_n über k normal ist, so sind alle Konjugierten zu α (in bezug auf k) auch in K_n, umsomehr in K enthalten, w. z. b. w.

Wir betrachten nun den Invariantenkörper K einer abgeschlossenen Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$. Ist $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine Fundamentalfolge aus $\mathfrak{H}$ über k, so ist sie auch fundamental über K. Zum Beweis nehmen wir die Körperreihe $N_1, N_2, \ldots, N_n, \ldots$ heraus und bilden $\bar{N}_1 = KN_1, \ldots, \bar{N}_n = KN_n, \ldots$. Dann ist offenbar N der Vereinigungskörper von $\bar{N}_1, \bar{N}_2, \ldots, \bar{N}_n, \ldots$. Es genügt nun zu zeigen, dass $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine Fundamentalfolge in bezug auf $\bar{N}_1, \bar{N}_2, \ldots, \bar{N}_n, \ldots$ ist.

Da $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine Fundamentalfolge über k ist, so gibt es für einen Körper N_n einen Index ν derart, dass für alle $\kappa \geqq \nu$ die

$$J^{(\nu)}(J^{(\kappa)})^{-1}$$

N_n elementweise invariant lassen. Ferner ist K bei Ausübung von $J^{(\nu)}(J^{(\kappa)})^{-1}$ elementweise invariant. Also ist der Körper $\bar{N}_n = KN_n$ bei Anwendung von $J^{(\nu)}(J^{(\kappa)})^{-1}$ elementweise invariant, weil jede Zahl aus $\bar{N}_n$ eine rationale Funktion der Zahlen aus K und N_n ist. Selbstverständlich können wir $\bar{N}_n$ aus der obigen Körperreihe beliebig wählen, indem wir dementsprechend N_n passend wählt. Also ist $J^{(1)}, \ldots, J^{(n)}, \ldots$ eine Fundamentalfolge in bezug auf $\bar{N}_1, \ldots, \bar{N}_n, \ldots$.

Nun nehmen wir vorläufig an, dass $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ ist. Also sind zwei nacheinanderfolgende Körper K_i, K_{i+1} resp. Normalteilkörper von N_i, N_{i+1} über k. Es sei nun $\bar{J}_i$ ein Automorphismus von K_i über k und $\bar{J}_{i+1}$ eine Erweiterung von $\bar{J}_i$ aus der galoisschen Gruppe von K_{i+1} nach k. Da N_i über K_i und k normal ist, so gibt es sicher einen Automorphismus J_i aus $\mathfrak{G}_i$, welcher eine Erweiterung von $\bar{J}_i$ ist. Ich will nun zeigen, dass es in $\mathfrak{G}_{i+1}$ einen Automorphismus J_{i+1} gibt, welcher in N_i, K_{i+1} resp. J_i, $\bar{J}_{i+1}$ induziert. Wir haben nämlich schon gesehen, dass $\mathfrak{H}$, angewandt auf N_i, N_{i+1}, resp. $\mathfrak{H}_i$, $\mathfrak{H}_{i+1}$ induziert. Da N_i ein Teilkörper von N_{i+1} ist, so induziert $\mathfrak{H}_{i+1}$ offenbar die Gruppe $\mathfrak{H}_i$, wenn $\mathfrak{H}_{i+1}$ auf N_i angewandt wird. Da die galoissche

Gruppe von K_i nach k der Faktorgruppe $\mathfrak{G}_i/\mathfrak{H}_i$ isomorph ist, so erhält man in N_i die sämtlichen Automorphismen, welche in K_i $\bar{J}_i$ induzieren, indem man J_i^* mit allen Automorphismen aus $\mathfrak{H}_i$ multipliziert, wobei J_i^* ein beliebiger Automorphismus aus $\mathfrak{G}_i$ ist, welcher in K_i $\bar{J}_i$ induziert. Um also $J_i^*\mathfrak{H}_i$ zu bestimmen, nehmen wir aus $\mathfrak{G}_{i+1}$ einen Automorphismus J_{i+1}^* heraus, der in K_{i+1} $\bar{J}_{i+1}$ induziert. Dann induziert offenbar J_{i+1}^* in K_i den Automorphismus $\bar{J}_i$. Bezeichnet man also den durch J_{i+1}^* in N_i induzierten Automorphismus mit J_i^*, so induziert $J_{i+1}^*\mathfrak{H}_{i+1}$ in N_i sicher $J_i^*\mathfrak{H}_i$, weil $\mathfrak{H}_{i+1}$ die Gruppe $\mathfrak{H}_i$ induziert. Wir können also in $J_i^*\mathfrak{H}_i$, den früher schon bestimmten Automorphismus J_i aufsuchen. Weil man nach dem oben Bewiesenen in $J_{i+1}^*\mathfrak{H}_{i+1}$ eine Erweiterung von J_i finden kann, so bezeichne man eine solche mit $J_{i+1}^*H_{i+1}$. Dann induziert $J_{i+1}^*H_{i+1}$ in N_i den Automorphismus J_i und in K_{i+1} den Automorphismus $\bar{J}_{i+1}$, weil H_{i+1} als der identische Automorphismus auf K_{i+1} einwirkt. Damit ist die Existenz desjenigen Automorphismus von N_{i+1} über k, der in N_i bzw. K_{i+1} den Automorphismus J_i bzw. $\bar{J}_{i+1}$ induziert, gesichert.

Nun wollen wir beweisen

Satz 6. *Ein Teilkörper K von N ist dann und nur dann normal, wenn die K zugeordnete Untergruppe $\mathfrak{H}$ ein Normalteiler der galoisschen Gruppe $\mathfrak{G}$ von N nach k ist. Wenn K über k normal ist, dann ist die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ isomorph zur galoisschen Gruppe von K nach k.*

Beweis. Wie wir schon in S. 81 gezeigt haben, ist K dann und nur dann normal über k, wenn die früher bestimmten Körper K_1, K_2. ...., K_n, ... alle über k normal sind. Dies geschieht aber dann und nur dann, wenn $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ ist.

Um die letzte Behauptung zu beweisen, ziehen wir die schon oben benutzte Körperreihe K_1, K_2, ..., K_n, ... in Betracht. Es sei $\bar{J}$ ein beliebiger Automorphismus aus K über k. Dann ist $\bar{J}$ durch eine reguläre Abbildungsfolge $\bar{J}_1$, $\bar{J}_2$, ..., $\bar{J}_n$, ... bestimmt, wobei $\bar{J}_n$

eine reguläre Abbildung[1] von K_n über k ist. Entsprechend dieser regulären Abbildungsfolge können wir nach dem oben Gezeigten in $N_1, N_2, \ldots, N_n, \ldots$ resp. folgende reguläre Abbildungen $J_1, J_2, \ldots, J_n, \ldots$ finden, wobei $J_1, J_2, \ldots, J_n, \ldots$ resp. Erweiterungen von $\bar{J}_1, \bar{J}_2, \ldots, \bar{J}_n, \ldots$ sind. Nämlich wir bestimmen in N_1 eine Erweiterung J_1 von $\bar{J}_1$. Dann kann man nach dem in S. 83 Gezeigten allgemein in einem Körper N_{i+1} den Automorphismus J_{i+1} finden, welcher in K_{i+1} bzw. N_i $\bar{J}_{i+1}$ bzw. J_i induziert $(i \geqq 1)$. Bezeichnet man den durch $J_1, J_2, \ldots, J_n, \ldots$ bestimmten Automorphismus mit J, so induziert J offenbar in K den Automorphismus $\bar{J}$. Da die Automorphismen aus $\mathfrak{H}$ und nur diese diejenigen Automorphismen aus $\mathfrak{G}$ sind, die als der identische Automorphismus auf K einwirken, so kann man leicht bestätigen, dass die Nebengruppe $J\mathfrak{H}$ von $\mathfrak{G}/\mathfrak{H}$ aus allen derjenigen Automorphismen besteht, welche, ausgeübt auf K, den Automorphismus $\bar{J}$ induzieren. Umgekehrt kann man auch leicht beweisen, dass alle Automorphismen aus einer beliebigen Nebengruppe von $\mathfrak{G}/\mathfrak{H}$ in K einen und denselben Automorphismus über k induziert, und durch zwei verschiedene Nebengruppen von $\mathfrak{G}/\mathfrak{H}$ auch zwei verschiedene Automorphismen von K über k induziert werden. Damit ist die letzte Behauptung bewiesen.

Es seien nun $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ eine Folge der Nebengruppen von $\mathfrak{G}/\mathfrak{H}$ und $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ eine zu J konvergierende (über k) Folge, deren Elemente resp. aus $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ herausgenommen sind. Ferner sei Σ die J enthaltende Nebengruppe von $\mathfrak{G}/\mathfrak{H}$. Dann sind alle Automorphismen aus Σ als Grenzautomorphismen von konvergenten Folgen, deren Elemente resp. aus $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ herausgegriffen sind, definiert. Denn ein beliebiger Automorphismus aus Σ ist von der Form JH, wobei H ein Automorphismus aus $\mathfrak{H}$ ist. Dann ist offenbar $J^{(1)}H, J^{(2)}H, \ldots, J^{(n)}H, \ldots$ eine zu JH konvergierende Folge und ihre Elemente sind resp. aus $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ herausgenommen.

---

(1) Reguläre Abbildung bedeutet Automorphismus.

Es sei nun $L^{(1)}, L^{(2)}, \ldots, L^{(n)}, \ldots$ eine beliebige konvergente Folge, deren Elemente resp. aus $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ herausgenommen sind. Dann will ich zeigen, dass der Grenzautomorphismus L dieser Folge auch zu Σ gehört. Nämlich wir können allgemein

$$L^{(n)} = J^{(n)} H^{(n)}$$

setzen, weil $L^{(n)}$ zu $\Sigma^{(n)}$ gehört, wo $H^{(n)}$ zu $\mathfrak{H}$ gehört. Für einen beliebigen endlichen Teilkörper P von N über k kann man einen geeigneten Index ν bzw. κ finden, derart dass für alle $i \geqq \nu$ bzw. $k \geqq \kappa$ die $J(J^{(i)})^{-1}$ bzw. $L(L^{(k)})^{-1}$ den Körper P elementweise invariant lassen. Dann lassen für alle $j \geqq \mathrm{Max}(\nu, \kappa)$ die $J(J^{(j)})^{-1}$ und $L(L^{(j)})^{-1}$ den Körper P elementweise invariant. Setzt man hier $L = JL'$, so ist für $j \geqq \mathrm{Max}(\nu, \kappa)$

$$L(L^{(j)})^{-1} = JL'(H^{(j)})^{-1}(J^{(j)})^{-1} = JL'(H^{(j)})^{-1}J^{-1}J(J^{(j)})^{-1},$$

d. h. $JL'(H^{(j)})^{-1}J^{-1} = JL'J^{-1}J(H^{(j)})^{-1}J^{-1}$ lässt P elementweise invariant. Hieraus folgt ohne weiteres, dass die Folge $JH^{(1)}J^{-1}, JH^{(2)}J^{-1}, \ldots,$ $JH^{(n)}J^{-1}, \ldots$ zu $JL'J^{-1}$ konvergiert. Da $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ ist, so ist $J(H^{(1)})J^{-1}, \ldots, J(H^{(n)})J^{-1}, \ldots$ eine Fundamentalfolge aus $\mathfrak{H}$. Ferner muss der Grenzautomorphismus $JL'J^{-1}$ der obigen Folge der Gruppe $\mathfrak{H}$ angehören, weil $\mathfrak{H}$ eine abgeschlossene Untergruppe von $\mathfrak{G}$ ist. Also ist L' ein Automorphismus aus $\mathfrak{H}$, d. h. L gehört zu Σ.

Wie wir schon gesehen haben, induzieren die obigen Nebengruppen $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ die Automorphismen von K über k. Wir wollen der Abkürzung halber mit $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ schlechthin solche induzierten Automorphismen von K über k bezeichnen. Unsere nächste Aufgabe ist zu beweisen, dass $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ zu Σ konvergiert (über k). Dafür nehme ich einen beliebigen endlichen Teilkörper K' von K über k heraus. Dann existiert ein Index ν, derart dass für alle $j \geqq \nu$ die $J(J^{(j)})^{-1}$ den Körper K' elementweise invariant lassen. Der durch $J(J^{(j)})^{-1}$ induzierte Automorphismus $\Sigma(\Sigma^{(j)})^{-1}$ lässt also K' elementweise invariant, d. h. $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ konvergiert zu Σ, weil K' ein endlicher Teilkörper von K über k ist.

Es sei nun $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ eine zu Σ konvergierende Folge (über k). Dann will ich zeigen, dass man eine zu J konvergierende Folge $J^{(1)}, J^{(2)}, \ldots, J^{(n)}, \ldots$ bilden kann. Dabei bedeutet J bzw. $J^{(n)}$ $(n \geqq 1)$ einen Automorphismus von N über k aus Σ bzw. $\Sigma^{(n)}$. Dafür betrachten wir die Körperreihe $N_1, N_2, \ldots, N_n, \ldots$ von N über k, und bilden wieder die Durchschnitte $K_1 = N_1 \cap K$, $K_2 = N_2 \cap K, \ldots, K_n = N_n \cap K, \ldots$. Da $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(n)}, \ldots$ zu Σ konvergiert, so kann man sicher eine Reihe der natürlichen Zahlen $l_1 < l_2 < \ldots < l_n < \ldots$ so bestimmen, dass für einen beliebigen Index n alle Automorphismen $\Sigma(\Sigma^{(l_n)})^{-1}, \Sigma(\Sigma^{(l_n+1)})^{-1}, \ldots, \Sigma(\Sigma^{(l_{n+1}-1)})^{-1}, \Sigma(\Sigma^{(l_{n+1})})^{-1}, \ldots$ den Körper K_n elementweise invariant lassen. Nun greifen wir aus Σ bzw. $\Sigma^{(n)}$ einen beliebigen Automorphismus J bzw. $L^{(n)}$ von N über k heraus. Dann lässt $J(L^{(l_n)})^{-1}$ den Körper K_n elementweise invariant, weil $J(L^{(l_n)})^{-1}$ auf den Körper K_n wie der Automorphismus $\Sigma(\Sigma^{(l_n)})^{-1}$ einwirkt. Also induziert $J(L^{(l_n)})^{-1}$, ausgeübt auf N_n, einen Automorphismus von N_n über K_n. Da $\mathfrak{H}$, angewandt auf N_n, die ganze galoissche Gruppe von N_n über K_n induziert (nach S. 81), so gibt es in $\mathfrak{H}$ einen geeigneten Automorphismus $H^{(l_n)}$, welcher in N_n denselben Automorphismus über K_n wie $J(L^{(l_n)})^{-1}$ induziert. Ebenso kann man in $\mathfrak{H}$ die Automorphismen $H^{(l_n+1)}, \ldots, H^{(l_{n+1}-1)}$ finden, welche in N_n resp. dieselben Automorphismen über K_n wie $J(L^{(l_n+1)})^{-1}, \ldots, J(L^{(l_{n+1}-1)})^{-1}$ induzieren. Wenn man also n alle natürlichen Zahlen 1, 2, ... durchlaufen lässt, so erhält man $J^{(1)} = H^{(1)}L^{(1)}$, $J^{(2)} = H^{(2)}L^{(2)}, \ldots, J^{(l_n)} = H^{(l_n)}L^{(l_n)}, \ldots$. Diese Automorphismen $J^{(1)}, J^{(2)}, \ldots, J^{(l_n)}, \ldots$ gehören resp. zu $\Sigma^{(1)}, \Sigma^{(2)}, \ldots, \Sigma^{(l_n)}, \ldots$, und sie konvergieren offenbar zu J, weil sie in bezug auf die Körperreihe $N_1, N_2, \ldots, N_n, \ldots$ zu J konvergieren.

Nach dem oben Bewiesenen ist es gezeigt, dass die Isomorphie der galoisschen Gruppe von K nach k zu $\mathfrak{G}/\mathfrak{H}$ so beschaffen ist, dass zwischen ihnen eine eindeutige Zuordnung hinsichtlich der Konvergenz existiert.

Nun wollen wir die Ideale aus N betrachten. Zunächst beweisen wir

Satz 7. *Es sei $\mathfrak{Q}$ ein ganzes Primärideal (im Spezialfall ist $\mathfrak{Q}$ ein Primideal) aus N und $\mathfrak{Q}_n = \mathfrak{Q} \cap N_n$. Ferner sei $J = \{J_n\}$ ein*

Automorphismus von N über k. Dann ist $\mathfrak{Q}^J$ auch Primärideal aus N und $\mathfrak{Q}_n^{Jn} = \mathfrak{Q}^J \frown N_n$[1].

Beweis. Dass $\mathfrak{Q}^J$ ein Ideal aus N ist, kann man sofort einsehen. Es seien nun α, β zwei ganze algebraische Zahlen aus N, so dass

$$\alpha\beta \equiv 0, \qquad \text{aber} \quad \alpha \not\equiv 0 \qquad \text{mod} \quad \mathfrak{Q}^J.$$

Dann folgt ohne weiteres

$$\alpha^{J^{-1}}\beta^{J^{-1}}, \qquad \text{aber} \quad \alpha^{J^{-1}} \not\equiv 0 \qquad \text{mod} \quad \mathfrak{Q}.$$

Da aber $\mathfrak{Q}$ ein Primärideal ist, so muss für eine geeignete natürliche Zahl ρ

$$(\beta^{J^{-1}})^\rho \equiv 0 \qquad \text{mod} \quad \mathfrak{Q}$$

sein. Hieraus schliesst man sofort, dass

$$\beta^\rho \equiv 0 \qquad \text{mod} \quad \mathfrak{Q}^{J(2)}$$

ist. Also ist $\mathfrak{Q}^J$ ein Primärideal.

Nach Satz 2 ist der Durchschnitt $\mathfrak{Q}_n$ von $\mathfrak{Q}$ mit N_n auch ein Primärideal aus N_n. Dann kann man genau so wie für $\mathfrak{Q}^J$ beweisen, dass $\mathfrak{Q}_n^{Jn}$ ein Primärideal aus N_n ist. Wir können aber weiter zeigen, dass $\mathfrak{Q}_n^{Jn}$ der Durchschnitt von $\mathfrak{Q}^J$ mit N_n ist. Denn $\mathfrak{Q}^J$ enthält sicher $\mathfrak{Q}_n^{Jn}$. Wäre aber $\mathfrak{Q}^J \frown N_n = \mathfrak{Q}_n'$ umfangreicher als $\mathfrak{Q}_n^{Jn}$, so müsste $(\mathfrak{Q}_n')^{J^{-1}}$ auch umfangreicher als $\mathfrak{Q}_n$ sein, was aber Widerspruch wäre, weil $(\mathfrak{Q}_n')^{J^{-1}}$ in $\mathfrak{Q}$ und N_n enthalten, und infolgedessen $(\mathfrak{Q}_n')^{J^{-1}} \leqq \mathfrak{Q}_n$ wäre. Damit ist der Beweis beendet.

Unter Benutzung derselben Bezeichnungen wie in Satz 7 sei noch $\mathfrak{P}$ das zu $\mathfrak{Q}$ gehörige Primideal. Dann gilt

Zusatz 1. $\mathfrak{P}^J$ ist das zu $\mathfrak{Q}^J$ gehörige Primideal.

---

(1) Bekanntlich bedeutet $\mathfrak{Q}^J$ eine Menge der Zahlen, welche aus $\mathfrak{Q}$ durch Ausübung von J entstehen.

(2) Wenn $\mathfrak{Q}$ ein Primideal ist, dann ist $\rho = 1$.

Beweis. Nach Satz 7 ist $\mathfrak{P}^J$ ein Primideal aus N. Da $\mathfrak{P}$ ein Teiler von $\mathfrak{Q}$ ist, so ist offenbar $\mathfrak{P}^J$ ein Teiler von $\mathfrak{Q}^J$. Da aber ein Primärideal aus N nur durch ein einziges Primideal teilbar ist, so ist offenbar $\mathfrak{P}^J$ das zu $\mathfrak{Q}^J$ gehörige Primideal.

Wenn nun $\mathfrak{P} = \{\mathfrak{P}_i\}$ insbesondere ein endliches Primideal ist, dann findet für das durch $\mathfrak{P}$ teilbare Primideal $\mathfrak{p}$ aus k folgende Primidealzerlegung in jedem Normalkörper N_n statt:

$$\mathfrak{p} = (\mathfrak{P}_{n1} \ldots . \mathfrak{P}_{n r_n})^{e_n}{}^{(1)}.$$

Da aber $\mathfrak{P}$ ein endliches Ideal ist, so muss es nach Satz 5 einen Index i geben, derart dass für alle $n \geqq i$

$$e_i = e_{i+1} = \ldots . = e_n = \ldots . = e$$

ist.

Betrachtet man einen Automorphismus $J = \{J_n\}$ von N über k, so ist nach Satz 7 $\mathfrak{P}^J$ auch ein Primideal und $\mathfrak{P}_n^J = \mathfrak{P}_n^{J_n}$ ein Primideal aus N_n. Aber dieses Primideal $\mathfrak{P}_n^{J_n}$ kommt sicher in $\mathfrak{P}_{n1}, \ldots . , \mathfrak{P}_{n r_n}$ vor. Also ist nach Satz 5 $\mathfrak{P}^J$ ein endliches Primideal. Nach dieser Tatsache beweist man leicht folgenden Zusatz.

Zusatz 2. Wenn $\mathfrak{P}$ ein endliches Primideal aus K und $\mathfrak{Q} = \mathfrak{P}^a$ ist, dann ist für einen Automorphismus J von N über k

$$\mathfrak{Q}^J = (\mathfrak{P}^J)^a .$$

Denn nach Satz 7 ist $\mathfrak{Q}^J$ ein Primärideal. Da aber nach Satz 3 $\mathfrak{Q}^J$ eine bestimmte Potenz des zu $\mathfrak{Q}^J$ gehörigen Primideals $\mathfrak{P}^J$ ist, so ist offenbar $\mathfrak{Q}^J = (\mathfrak{P}^J)^{a'}$. Nun kann man einerseits beweisen, dass $\mathfrak{Q}^J$ durch $(\mathfrak{P}^J)^a$ teilbar ist. Also muss sicher

$$a' \geqq a$$

sein. Anderseits kann man auch schliessen, dass

$$a \geqq a'$$

(1) H. I. S. 481.

ist, weil $\mathfrak{Q} = (\mathfrak{Q}^J)^{J^{-1}}$ durch $\mathfrak{P}^{a'}$ teilbar ist. Also muss $a = a'$ sein.

Satz 8. *Es sei* $\mathfrak{a}$ *ein ganzes Ideal aus* k *und* $\mathfrak{Q}$ *eine nicht triviale Primärkomponente von* $\mathfrak{a}$ *in* N. *Dann ist für einen beliebigen Automorphismus* J *von* N *über* k $\mathfrak{Q}^J$ *auch eine Primärkomponente von* $\mathfrak{a}$ *in* N.

Beweis. Es sei $\mathfrak{P}$ das zu $\mathfrak{Q}$ gehörige Primideal aus N. Dann folgt aus $\mathfrak{Q} \mid \mathfrak{a}$ ohne weiteres

$$\mathfrak{Q}^J \mid \mathfrak{a} ,$$

weil $\mathfrak{Q}^J \mid \mathfrak{a}^J$ und $\mathfrak{a}^J = \mathfrak{a}$ ist. Nach Zusatz 1 von Satz 7 ist $\mathfrak{Q}^J$ ein zu $\mathfrak{P}^J$ gehöriges Primärideal. Bezeichnet man mit $\mathfrak{Q}'$ die Primärkomponente von $\mathfrak{a}$ in bezug auf $\mathfrak{P}^J$, so ist offenbar

$$\mathfrak{Q}^J \mid \mathfrak{Q}' \mid \mathfrak{a} \text{ (1)}.$$

Hieraus folgt ohne weiteres

$$(\mathfrak{Q}^J)^{J^{-1}} \mid (\mathfrak{Q}')^{J^{-1}} \mid \mathfrak{a}^{J^{-1}} ,$$

also $\mathfrak{Q} \mid (\mathfrak{Q}')^{J^{-1}} \mid \mathfrak{a}$. Da aber $(\mathfrak{Q}')^{J^{-1}}$ nach Satz 7 auch ein Primärideal, welches zu $\mathfrak{P}$ gehört, ist, so muss

$$(\mathfrak{Q}')^{J^{-1}} \mid \mathfrak{Q}$$

sein, weil $\mathfrak{Q}$ die Primärkomponente von $\mathfrak{a}$ in bezug auf $\mathfrak{P}$ ist(2).

Daher ist

$$\mathfrak{Q} = (\mathfrak{Q}')^{J^{-1}} ,$$

ist also

$$\mathfrak{Q}^J = \mathfrak{Q}' ,$$

w. z. b. w.

Wir können nachher einen Schritt weiter beweisen, dass jede Primärkomponente, welche kein Einsideal ist, aus einer solchen beliebigen durch Anwendung eines Automorphismus von N über k entsteht.

---

(1), (2) KRULL, Idealtheorie in unendlichen algebraischen Zahlkörpern, Math. Zeitschr., Bd. 29 (1929), S. 46.

Für einen Normalkörper N über k kann man folgenden Satz beweisen, welcher für die endlichen algebraischen Zahlkörper allgemein durch analytisches Hilfsmittel bewiesen wird.

Satz 9. *Wenn es in einem Normalkörper unendlichen Grades N überhaupt ein endliches Primideal gibt, dessen Grad und Exponent nach k resp. f und e sind, dann gibt es in N unendlich viele Primideale vom Grade f und Exponenten e nach k. Dabei bedeuten f, e natürliche Zahlen.*

Beweis. Es sei $\mathfrak{P}$ ein endliches Primideal, welches die in Voraussetzung genannte Eigenschaft besitzt, und $\mathfrak{p}$ das durch $\mathfrak{P}$ teilbare Primideal aus k. Dann existiert nach Satz 5 ein Index i, derart dass für jedes $n \geqq i$ im Körper N_n folgende Primidealzerlegung stattfindet:

$$\mathfrak{p} = (\mathfrak{P}_{n1} \ldots . \mathfrak{P}_{nr_n})^e ,$$

wobei e eine bestimmte natürliche Zahl ist. Bezeichnet man den Grad von $\mathfrak{P}_{n1}$ nach k mit f_n, so ist

$$f_n e\, r_n = g_n ,$$

wo g_n den Grad von N_n nach k bedeutet. Da nach Definition des Grades $f = \lim_{n\to\infty} f_n$ ist, so gibt es einen Index j, so dass für alle $n \geqq j$

$$f_n = f$$

sind. Daraus folgt sofort, dass die Anzahl r_n der verschiedenen Primteiler von $\mathfrak{p}$ in N_n mit n zusammen über alle Grenzen wächst, weil g_n auch so ist. Also besitzt $\mathfrak{p}$ in N unendlich viele Primteiler. Denn sonst gäbe es einen Index l, so dass für alle $n \geqq l$ $\mathfrak{p}$ in N_n nur endlich viele verschiedene Primteiler besitzte und die Anzahl dieser verschiedenen Primteiler eine von n unabhängige Zahl wäre. Dies wäre aber Widerspruch.

Dass jeder Primteiler von $\mathfrak{p}$ vom Grade f und vom Exponenten e nach k ist, kann man leicht aus der Formel

$$fer_n = g_n$$

für $n \geqq \mathrm{Max}\,(i, j)$ einsehen. Damit ist der Beweis erledigt.

§ 3. ZERLEGUNGS- UND TRÄGHEITSGRUPPE.

In diesem Paragraphen bedeutet N wie im vorigen Paragraphen einen Normalkörper über k und $N = \{N_n\}$. Wir definieren zunächst für ein Primideal $\mathfrak{P} = \{\mathfrak{P}_n\}$ aus N seine Zerlegungsgruppe nach k.

Zerlegungsgruppe. Die Gesamtheit derjenigen Automorphismen von N über k, welche ein Primideal $\mathfrak{P}$ aus N invariant lassen, bildet eine Gruppe $\mathfrak{G}_Z$. Diese Gruppe $\mathfrak{G}_Z$ heisse die *Zerlegungsgruppe* von $\mathfrak{P}$ nach k.

Wir bezeichnen im folgenden mit $\mathfrak{G}_Z^{(n)}$ die Zerlegungsgruppe von $\mathfrak{P}_n$ nach k. Wendet man auf $\mathfrak{P}_n$ einen Automorphismus σ aus $\mathfrak{G}_Z$ an, so erhält man

$$\mathfrak{P}_n^{\sigma} = \mathfrak{P}_n^{\sigma_n},$$

wobei σ_n eine reguläre Abbildung von σ in N_n bedeutet. Da aber $\mathfrak{P}_n^{\sigma_n}$ ein Primideal aus N_n und in $\mathfrak{P} = \mathfrak{P}^{\sigma}$ enthalten ist, so ist nach Definition von $\mathfrak{P}_n$

$$\mathfrak{P}_n^{\sigma_n} = \mathfrak{P}_n .$$

Also induziert ein Automorphismus σ aus $\mathfrak{G}_Z$ im Körper N_n einen Automorphismus σ_n aus $\mathfrak{G}_Z^{(n)}$. Daher ist σ durch die Abbildungsfolge $\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$ definiert, deren Abbildungen resp. zu den Zerlegungsgruppen von $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n, \ldots$ nach k gehören.

Wir betrachten nun zwei nacheinanderfolgende Körper N_i, N_{i+1} aus der Körperreihe von N über k, und in N_i bzw. N_{i+1} das Primideal $\mathfrak{P}_i$ bzw. $\mathfrak{P}_{i+1}$. Ferner bezeichnen wir mit $\mathfrak{G}_Z^{(i)}$ bzw. $\mathfrak{G}_Z^{(i+1)}$ die Zerlegungsgruppe von $\mathfrak{P}_i$ bzw. $\mathfrak{P}_{i+1}$ nach k. Dann kann man genau so wie oben zeigen, dass jeder Automorphismus σ_{i+1} aus $\mathfrak{G}_Z^{(i+1)}$ einen Automorphismus σ_i aus $\mathfrak{G}_Z^{(i)}$ induziert.

Es gilt ferner zwischen $\mathfrak{G}_Z^{(i)}$ und $\mathfrak{G}_Z^{(i+1)}$ folgende Relation

$$\mathfrak{G}_Z^{(i)} \cong \mathfrak{G}_Z^{(i+1)}\mathfrak{H}_i/\mathfrak{H}_i^{(1)},$$

wobei $\mathfrak{H}_i$ die N_i zugeordnete Untergruppe aus der galoisschen Gruppe $\mathfrak{G}_{i+1}$ von N_{i+1} nach k bedeutet. Da jeder Automorphismus aus einer Nebengruppe von $\mathfrak{G}_Z^{(i+1)}\mathfrak{H}_i$ nach $\mathfrak{H}_i$, ausgeübt auf die Zahlen aus N_i, einen und denselben Automorphismus von N_i über k induziert, so kann man aus der obigen Isomorphierelation schliessen, dass es für jeden einen Automorphismus aus $\mathfrak{G}_Z^{(i)}$ mindestens eine seiner Erweiterungen in $\mathfrak{G}_Z^{(i+1)}$ gibt.

Aus dieser Tatsache kann man für einen Automorphismus σ_i aus $\mathfrak{G}_Z^{(i)}$ $(i \geqq 1)$ immer eine Automorphismusreihe

$$\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$$

bilden, in der für $j < i$ σ_j den durch σ_i induzierten Automorphismus aus $\mathfrak{G}_Z^{(j)}$ und für $j > i$ σ_j einen erweiterten Automorphismus von σ_i aus $\mathfrak{G}_Z^{(j)}$ bedeutet. Da offenbar die obige Automorphismusreihe eine reguläre Abbildungsfolge ist, so definiert sie einen Automorphismus von N über k. Weil jedes σ_i der Zerlegungsgruppe $\mathfrak{G}_Z^{(i)}$ von $\mathfrak{P}_i$ nach k angehört, so folgt ohne weiteres, dass

$$\mathfrak{P}^{\sigma} = \{\mathfrak{P}_i^{\sigma_i}\} = \{\mathfrak{P}_i\} = \mathfrak{P}$$

ist, d. h. σ ein Automorphismus aus $\mathfrak{G}_Z$ ist.

Unter Benutzung der obigen Bezeichnungen gilt also

Satz 10. *Jeder Automorphismus aus der Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ nach k ist durch eine reguläre Abbildungsfolge*

$$\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$$

definiert. Dabei ist σ_i ein Automorphismus aus der Zerlegungsgruppe $\mathfrak{G}_Z^{(i)}$ von $\mathfrak{P}_i$ nach k. Ferner induziert $\mathfrak{G}_Z$ in jedem normalen Teil-

(1) HERBRAND, Sur la théorie des groupes de décomposition, d'inertie et de ramification, Journal de Liouville, Tome 10 (1931), S. 483. Diese Arbeit zitiere ich mit H. In dieser Arbeit behandelte HERBRAND den Fall, dass der Grundkörper k von endlichem Grade ist. Für den Fall, wo k von unendlichem Grade ist, weise ich auf H. I. S. 486 hin.

körper N_i aus der Körperreihe von N über k die ganze Zerlegungsgrunpe $\mathfrak{G}_Z^{(i)}$ von $\mathfrak{P}_i$ nach k.

Nun wollen wir mit Hilfe der Zerlegungsgruppe folgenden Satz beweisen.

Satz 11. *Es sei $\mathfrak{p}$ ein Primideal aus k, und $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in N. Dann ist ein Primideal $\mathfrak{P}'$ aus N dann und nur dann Primteiler von $\mathfrak{p}$, wenn $\mathfrak{P}'$ von der Form $\mathfrak{P}^J$ ist, wobei J einen Automorphismus von N über k bedeutet.*

Beweis. Dass für einen beliebigen Automorphismus J das Primideal $\mathfrak{P}^J$ ein Primteiler von $\mathfrak{p}$ ist, kann man aus Satz 8 leicht ablesen. Denn das Ideal $\mathfrak{p}$ besitzt in N die zu $\mathfrak{P}^J$ gehörige Primärkomponente, ist also a fortiori durch $\mathfrak{P}^J$ teilbar.

Es sei nun $\mathfrak{P}'\,(\neq\mathfrak{P})$ ein Primteiler von $\mathfrak{p}$. Dann wollen wir zeigen, dass es einen Automorphismus J gibt, derart dass $\mathfrak{P}'=\mathfrak{P}^J$ ist. Wir bezeichnen nun den Durchschnitt $\mathfrak{P}'\frown N_n$ von $\mathfrak{P}'$ mit N_n durch $\mathfrak{P}'_n$. Dann ist in N_n $\mathfrak{p}$ durch $\mathfrak{P}'_n$ teilbar, weil $\mathfrak{P}'$ ein Primteiler von $\mathfrak{p}$ ist. Da N über k normal ist, so existiert in N_n ein Automorphismus J_n über k, derart dass

$$\mathfrak{P}'_n=\mathfrak{P}_n^{J_n}$$

wird[1], wobei $\mathfrak{P}_n=\mathfrak{P}\frown N_n$ ist $(n\geqq 1)$.

Betrachtet man nun zwei nacheinanderfolgende Körper N_i, N_{i+1}, so ist

$$\mathfrak{P}'_i\,|\,\mathfrak{p}\qquad\text{und}\qquad\mathfrak{P}'_{i+1}\,|\,\mathfrak{P}'_i.$$

Da $\mathfrak{P}'_i=\mathfrak{P}_i^{J_i}$ und $\mathfrak{P}'_{i+1}=\mathfrak{P}_{i+1}^{J_{i+1}}$ ist, so ist

$$\mathfrak{P}_{i+1}^{J_{i+1}}\,|\,\mathfrak{P}_i^{J_i}.$$

Wenn man also mit J'_i den durch J_{i+1} induzierten Automorphismus von N_i über k bezeichnet, dann ist ersichtlich

$$\mathfrak{P}_{i+1}^{J_{i+1}}\,|\,\mathfrak{P}_i^{J'_i},$$

(1) H. I. S. 480–481.

muss also $\mathfrak{P}^{J_i'} = \mathfrak{P}^{J_i}$ sein, weil $\mathfrak{P}_i^{J_i}$, $\mathfrak{P}_i^{J_i'}$ beide durch $\mathfrak{P}_{i+1}'$ teilbare Primideale aus N_i sind. Daher existiert in $\mathfrak{G}_Z^{(i)}$ ein Automorphismus σ_i, so dass

$$J_i = J_i'\sigma_i$$

wird, weil $(J_i')^{-1}J_i$ ein Automorphismus aus $\mathfrak{G}_Z^{(i)}$ ist. Da es nach Satz 10 in $\mathfrak{G}_Z^{(i+1)}$ einen Automorphismus σ_{i+1} gibt, der eine Erweiterung von σ_i ist, so induziert $J_{i+1}\sigma_{i+1}$ in N_i den Automorphismus $J_i'\sigma_i = J_i$. Weil aber $\mathfrak{P}_{i+1}^{J_{i+1}\sigma_{i+1}} = \mathfrak{P}_{i+1}^{J_{i+1}}$ ist[1], so kann man folgendes behaupten:

In allen zwei nacheinanderfolgenden Körpern N_i, N_{i+1} kann man immer zwei Automorphismen J_i, J_{i+1} finden, derart dass J_{i+1} eine Erweiterung von J_i ist, und $\mathfrak{P}_{i+1}' = \mathfrak{P}_{i+1}^{J_{i+1}}$, $\mathfrak{P}_i' = \mathfrak{P}_i^{J_i}$ sind.

Also kann man immer eine reguläre Abbildungsfolge

$$J_1, J_2, \ldots, J_n, \ldots$$

bilden, derart dass für $J = \{J_n\}$

$$\mathfrak{P}' = \mathfrak{P}^J$$

wird. Damit ist der Beweis beendet.

Nach Satz 8 und 11 kann man folgenden Satz beweisen.

Satz 12. *Es sei* $\mathfrak{q}$ *ein ganzes Primärideal aus k und $\mathfrak{Q}$ eine nicht triviale Primärkomponente von* $\mathfrak{q}$ *in N. Dann erhält man die sämtlichen nicht trivialen Primärkomponenten von* $\mathfrak{q}$ *in N, indem man auf $\mathfrak{Q}$ alle Automorphismen von N über k anwendet.*

Beweis. Dass für einen Automorphismus J von N über k $\mathfrak{Q}^J$ auch eine Primärkomponente ist, hat man schon in Satz 8 gezeigt. Es genügt also zu zeigen, dass für eine beliebige, nicht triviale Primärkomponente $\mathfrak{Q}'$ ein Automorphismus J von N über k existiert, derart dass

$$\mathfrak{Q}' = \mathfrak{Q}^J$$

(1) Die Bezeichnung $\mathfrak{P}_{i+1}^{J_{i+1}\sigma_{i+1}}$ soll man so verstehen, dass man zunächst σ_{i+1} und dann J_{i+1} auf die Zahlen aus $\mathfrak{P}_{i+}$ anwendet.

wird. Da $\mathfrak{q}$ ein Primärideal aus k ist, so ist $\mathfrak{q}$ nur durch ein einziges Primideal $\mathfrak{p}$ aus k teilbar. Nun sei $\mathfrak{Q}'$ eine nicht triviale Primärkomponente von $\mathfrak{q}$ in bezug auf ein Primideal $\mathfrak{P}'$ aus N. Dann ist $\mathfrak{P}'$ in N ein Primteiler von $\mathfrak{p}$. Denn $\mathfrak{p}' = \mathfrak{P}' \cap k$ ist offenbar ein Primideal aus k und $\mathfrak{p}'$ teilt sicher $\mathfrak{q}$, weil $\mathfrak{q}$ durch $\mathfrak{P}'$ teilbar ist. Daher ist $\mathfrak{p} = \mathfrak{p}'$. Also ist $\mathfrak{P}'$ ein Primteiler von $\mathfrak{p}$.

Bezeichnet man nun das zu $\mathfrak{Q}$ gehörige Primideal mit $\mathfrak{P}$, so existiert nach Satz 11 ein Automorphismus J von N über k, derart dass $\mathfrak{P}^J = \mathfrak{P}'$ wird, weil ja $\mathfrak{P}$ und $\mathfrak{P}'$ Primteiler von $\mathfrak{p}$ sind. Also ist $\mathfrak{Q}'$ durch $\mathfrak{P}^J$ teilbar. Da aber $\mathfrak{Q}^J$ die Primärkomponente von $\mathfrak{q}$ in bezug auf das Primideal $\mathfrak{P}^J$ ist (nach Zusatz 1 von Satz 7 und Satz 8), so muss offenbar

$$\mathfrak{Q}' = \mathfrak{Q}^J$$

sein, w. z. b. w.

Nun wollen wir speziell den Fall, wo die Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ nach k eine endliche Gruppe von der Ordnung m ist, betrachten. Bezeichnet man mit $\sigma^{(1)} = \{\sigma_n^{(1)}\}$, $\sigma^{(2)} = \{\sigma_n^{(2)}\}$, ..., $\sigma^{(m)} = \{\sigma_n^{(m)}\}$ m verschiedene Automorphismen aus $\mathfrak{G}_Z$, so kann man einen Index i so finden, dass für jeden Index $j \geqq i$ und für zwei beliebige verschiedene Zahlen κ, ρ aus 1, ..., m immer

$$\sigma_j^{(\kappa)} \neq \sigma_j^{(\rho)}$$

ist. Denn sonst wäre die Ordnung von $\mathfrak{G}_Z$ kleiner als m. Wir können aber noch zeigen, dass jeder Automorphismus $\sigma_j^{(\kappa)}$ $(j \geqq i)$ aus $\mathfrak{G}_Z^{(j)}$ nur eine einzige Erweiterung $\sigma_{j+1}^{(\kappa)}$ aus $\mathfrak{G}_Z^{(j+1)}$ besitzt. Denn hätte $\sigma_j^{(\kappa)}$ zwei verschiedene Erweiterungen in $\mathfrak{G}_Z^{(j+1)}$, dann gäbe es in $\mathfrak{G}_Z^{(j+1)}$ mindestens $m+1$ verschiedene Automorphismen, und infolgedessen nach Satz 10 auch mindestens $m+1$ verschiedene Automorphismen in $\mathfrak{G}_Z$, was aber Widerspruch wäre. Also ist für einen beliebigen Index $j \geqq i$ immer

$$m = e_j f_j^{(1)},$$

(1) H. I. S. 483.

wobei f_j den Grad von $\mathfrak{P}_j$ nach k und e_j den Exponenten von $\mathfrak{P}_j$ in $\mathfrak{p}$ bedeutet. Da aber bekanntlich $e_j \mid e_{j+1}$ und $f_j \mid f_{j+1}$ ist, so folgt aus der obigen Formel

$$e_i = e_{i+1} = \ldots = e \quad \text{und} \quad f_i = f_{i+1} = \ldots = f .$$

Also besitzt nach Definition das Primideal $\mathfrak{P}$ aus N den Grad f und den Exponenten e nach k.

Ist J ein beliebiger Automorphismus von N über k, so ist die Zerlegungsgruppe von $\mathfrak{P}^J$ nach k gerade $J\mathfrak{G}_Z J^{-1}$. Diese Gruppe besitzt offenbar auch die Ordnung m. Beachtet man, dass in einem beliebigen normalen Teilkörper N_n von N über k jeder Primteiler von $\mathfrak{p}$ denselben Grad bzw. denselben Exponenten nach k besitzt, so kann man ohne Schwierigkeit beweisen, dass $\mathfrak{P}^J$ auch den Grad f und den Exponenten e besitzt.

Wir setzen noch weiter voraus, dass $\mathfrak{p}$ ein endliches Ideal aus k ist. Dann ist nach Satz 5 $\mathfrak{P}$ auch endlich und die Primärkomponente von $\mathfrak{p}$ in bezug auf $\mathfrak{P}$ ist $\mathfrak{P}^e$. Also gilt nach Satz 12

Satz 13. *Es sei $\mathfrak{p}$ ein Primideal aus k und $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in N. Ferner sei die Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ nach k eine endliche Gruppe. Dann sind alle Primteiler von $\mathfrak{p}$ in N vom gleichen Grade bzw. vom gleichen Exponenten nach k. Wenn insbesondere $\mathfrak{p}$ ein endliches Ideal aus k ist, dann ist jede nicht triviale Primärkomponente von $\mathfrak{p}$ in N von der Form*

$$(\mathfrak{P}^e)^J ,$$

wobei e den Exponenten von $\mathfrak{P}$ nach k bedeutet und J alle verschiedenen Automorphismen von N über k durchlaufen kann.

Wir beweisen nun

Satz 14. *Die Zerlegungsgruppe $\mathfrak{G}_Z$ von $\mathfrak{P}$ nach k ist eine abgeschlossene Untergruppe der ganzen galoisschen Gruppe von N nach k.*

Beweis. Es sei $\sigma^{(1)}, \sigma^{(2)}, \ldots, \sigma^{(n)}, \ldots$ eine Fundamentalfolge aus $\mathfrak{G}_Z$. Dann enthält die galoissche Gruppe von N nach k den Grenzautomorphismus σ dieser Fundamentalfolge, weil sie abgeschlossen

ist. Ist N_n ein beliebiger Körper aus der Körperreihe $N_1, \ldots N_n, \ldots$. von N, so existiert sicher ein Index i, derart dass für alle $j \geqq i$ die $\sigma(\sigma^{(j)})^{-1}$ den Körper N_n elementweise invariant lassen. Also ist $\mathfrak{P}_n = \mathfrak{P} \frown N_n$ auch bei Ausübung von $\sigma(\sigma^{(j)})^{-1}$ invariant. Bildet man nun $\mathfrak{P}^{\tau(\sigma(j))^{-1}}$, so ist offenbar

$$\mathfrak{P}^{\sigma(\sigma(j))^{-1}} = \mathfrak{P}^{\sigma},$$

weil $\sigma^{(j)}$ zu $\mathfrak{G}_Z$ gehört. Der Durchschnitt von $\mathfrak{P}^{\sigma(\sigma(j))^{-1}}$ mit N_n ist sicher ein Primideal aus N_n und enthält $\mathfrak{P}_n^{\sigma(\sigma(j))^{-1}} = \mathfrak{P}_n$. Also ist

$$\mathfrak{P}_n = \mathfrak{P}^{\sigma} \frown N_n .$$

Da diese Relation für einen beliebigen Index n gilt, so ist sicher

$$\mathfrak{P}^{\sigma} = \mathfrak{P},$$

d. h. σ gehört zu $\mathfrak{G}_Z$, w. z. b. w.

Trägheitsgruppe. Die Gesamtheit derjenigen Automorphismen τ von N über k, für welche die Kongruenz

$$\tau A \equiv A \mod \mathfrak{P}$$

für alle für $\mathfrak{P}$ ganzen Zahlen aus N gilt, bildet die sogenannte *Trägheitsgruppe* $\mathfrak{G}_T$ von $\mathfrak{P}$ nach k.

Aus dieser Definition folgt sofort, dass $\mathfrak{G}_T$ ein Normalteiler der Zerlegungsgruppe von $\mathfrak{G}_Z$ von $\mathfrak{P}$ nach k ist. Wenn ein Automorphismus τ aus $\mathfrak{G}_T$ durch die reguläre Abbildungsfolge

$$\tau_1, \tau_2, \ldots, \tau_n, \ldots$$

definiert ist, dann erkennt mann leicht, dass für alle für $\mathfrak{P}_n$ ganzen Zahlen A_n aus N_n $\tau A_n = \tau_n A_n$, und folglich

$$\tau_n A_n = \tau A_n \equiv A_n \mod \mathfrak{P}_n$$

gilt. Also ist τ_n ein Automorphismus aus der Trägheitsgruppe von $\mathfrak{P}_n$ nach k. Wir wollen im folgenden die Trägheitsgruppe von $\mathfrak{P}_n$ nach k durchweg mit $\mathfrak{G}_T^{(n)}$ bezeichnen.

Es seien $\mathfrak{G}_T^{(i)}$, $\mathfrak{G}_T^{(i+1)}$ resp. die Trägheitsgruppen von $\mathfrak{P}_i$, $\mathfrak{P}_{i+1}$ nach k, und $\mathfrak{H}_i$ die N_i zugeordnete Untergruppe aus der ganzen galoisschen Gruppe von N_{i+1} nach k. Dann gilt bekanntlich

$$\mathfrak{G}_T^{(i)} \cong \mathfrak{G}_T^{(i+1)} \mathfrak{H}_i / \mathfrak{H}_i^{(1)} .$$

Berücksichtigt man diese Isomorphie, so kann man ebenso wie für die Zerlegungsgruppe (siehe S. 92) beweisen, dass für einen beliebigen Automorphismus τ_i aus $\mathfrak{G}_T^{(i)}$ mindestens eine Erweiterung τ_{i+1} in $\mathfrak{G}_T^{(i+1)}$ existiert. Es gilt also

Satz 15. *Die Trägheitsgruppe $\mathfrak{G}_T$ ist ein Normalteiler der Zerlegungsgruppe $\mathfrak{G}_Z$. Ein beliebiger Automorphismus τ aus $\mathfrak{G}_T$ ist durch die reguläre Abbildungsfolge $\tau_1, \tau_2, \ldots, \tau_n, \ldots$ definiert, wobei τ_n ein Automorphismus aus $\mathfrak{G}_T^{(n)}$ ist $(n = 1, \ldots)$. Ferner induziert $\mathfrak{G}_T$ in jedem Teilkörper N_n aus der Körperreihe $N_1, N_2, \ldots, N_n, \ldots$ von N die ganze Trägheitsgruppe $\mathfrak{G}_T^{(n)}$.*

Nun betrachten wir einen Teilkörper N_n aus der Körperreihe von N und bezeichnen die Zerlegungs- bzw. Trägheitsgruppe von $\mathfrak{P}_n$ nach k mit $\mathfrak{G}_Z^{(n)}$ bzw. $\mathfrak{G}_T^{(n)}$, wobei $\mathfrak{P}_n$ das durch $\mathfrak{P}$ teilbare Primideal aus N_n bedeutet. Dann ist bekanntlich die Faktorgruppe $\mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}$ zyklisch (der Grundkörper k mag von endlichem oder unendlichem Grade sein). Die Ordnung f_n dieser Faktorgruppe ist gleich dem Grad von $\mathfrak{P}_n$ nach k[2]. Es gibt also einen Automorphismus σ_n aus $\mathfrak{G}_Z^{(n)}$, derart dass $\sigma_n^{f_n}$ erst in $\mathfrak{G}_T^{(n)}$ übergeht. Diesen Automorphismus σ_n will ich ein erzeugendes Element von $\mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}$ nennen.

Wir setzen nun $n = i$, $i+1$ und für i bzw. $i+1$ gebrauchen alle obigen Bezeichnungen. Zunächst will ich zeigen, dass ein erzeugendes Element σ_{i+1} von $\mathfrak{G}_Z^{(i+1)}/\mathfrak{G}_T^{(i+1)}$ ein erzeugendes Element von $\mathfrak{G}_Z^{(i)}/\mathfrak{G}_T^{(i)}$ induziert. Nämlich $\sigma_{i+1}^a \tau_{i+1}$ stellt alle Automorphismen aus $\mathfrak{G}_Z^{(i+1)}$ dar, wenn a alle ganzen Zahlen von 0 bis $f_{i+1}-1$, und τ_{i+1} alle Automorphismen aus $\mathfrak{G}_T^{(i+1)}$ durchläuft, worin f_{i+1} den Index von $\mathfrak{G}_Z^{(i+1)}$ nach

(1) Siehe H. S. 483, wenn k von endlichem Grade ist, und H. I. S. 486, wenn k von unendlichem Grade ist.

(2) Wenn k von endlichem Grade ist, dann ist diese Tatsache wohlbekannt. Für den Fall, wo k von unendlichem Grade ist, verweise ich auf H. I. S. 483.

$\mathfrak{G}_T^{(i+1)}$ bedeutet. Da aber $\mathfrak{G}_Z^{(i+1)}$ in N_i die ganze Gruppe $\mathfrak{G}_Z^{(i)}$ induziert, so muss σ_{i+1} in N_i ein erzeugendes Element von $\mathfrak{G}_Z^{(i)}/\mathfrak{G}_T^{(i)}$ induzieren. Denn sonst würde durch $\mathfrak{G}_Z^{(i+1)}$ nur ein Teil von $\mathfrak{G}_Z^{(i)}$ induziert, weil $\mathfrak{G}_T^{(i+1)}$ nach Satz 15 die Gruppe $\mathfrak{G}_T^{(i)}$ induziert.

Wir bezeichnen den durch σ_{i+1} in N_i induzierten Automorphismus aus $\mathfrak{G}_Z^{(i)}$ mit $\bar{\sigma}_i$. Dann ist nach dem oben Bewiesenen σ_i von der Form

$$\sigma_i^{\nu}\bar{\tau}_i ,$$

wobei $\bar{\tau}_i$ ein Automorphismus aus $\mathfrak{G}_T^{(i)}$ ist. Ferner ist ν eine positive ganze rationale Zahl, welche zu f_i prim ist. Denn wäre dies nicht der Fall, so wäre $\bar{\sigma}_i$ kein erzeugendes Element von $\mathfrak{G}_Z^{(i)}/\mathfrak{G}_T^{(i)}$. Wir können ferner ohne Einschränkung der Allgemeinheit annehmen, dass $\nu < f_i$ ist. Wir können also eine ganze Zahl ρ_0 so bestimmen, dass

$$\nu\rho_0 \equiv 1 \mod f_i$$

ist. Ist ρ_0 zu f_{i+1} prim, so setze man $\rho = \rho_0$. Wenn aber ρ_0 zu f_{i+1} nicht prim ist, dann bilde man eine Zahl $\rho = \rho_0 + f_i d$. Dabei ist d eine ganze Zahl, welche durch alle derjenigen Primteiler von f_{i+1}, die in ρ_0 nicht aufgehen, sonst aber durch keine anderen Primzahlen teilbar ist. Die so bestimmte Zahl ρ ist jedenfalls prim zu f_{i+1}. Ferner ist offenbar

$$\nu\rho \equiv 1 \mod f_i .$$

Dividiert man nun ρ durch f_{i+1} und bezeichnet mit κ den kleinsten positiven Rest von ρ, so ist

$$\nu\kappa \equiv 1 \mod f_i ,$$

weil f_{i+1} durch f_i teilbar ist. Aus $\bar{\sigma}_i = \sigma_i^{\nu}\bar{\tau}_i$ erhält man also

$$\bar{\sigma}_i^{\kappa} = \sigma_i \tau_i^* ,$$

wenn man einen geeigneten Automorphismus τ_i^* aus $\mathfrak{G}_T^{(i)}$ wählt. Nun können wir nach dem in S. 98 Gezeigten in $\mathfrak{G}_T^{(i+1)}$ eine Erweiterung

τ_{i+1}^* von τ_i^* finden. Betrachtet man nun $\sigma_{i+1}^{\varkappa}(\tau_{i+1}^*)^{-1}$, so induziert dieses in N_i den Automorphismus

$$\bar{\sigma}_i^{\varkappa}(\tau_i^*)^{-1} = \sigma_i ,$$

ist also $\sigma_{i+1}^{\varkappa}(\tau_{i+1}^*)^{-1}$ eine Erweiterung von σ_i. Ferner ist $\sigma_{i+1}^{\varkappa}(\tau_{i+1}^*)^{-1}$ ein erzeugendes Element von $\mathfrak{G}_T^{(i+1)}/\mathfrak{G}_T^{(i+1)}$, weil κ zu f_{i+1} prim ist. Damit ist folgendes bewiesen:

Es existiert ein Automorphismus $\sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots\}$ *in* $\mathfrak{G}_Z$, *dessen* σ_n *für jedes* $n \geqq 1$ *ein erzeugendes Element von* $\mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}$ *ist.*

Durch die Existenz dieses Elementes σ kann man folgenden Satz beweisen.

Satz 16. *Es existiert in* $\mathfrak{G}_Z$ *ein Automorphismus* σ *von der Art, dass jeder Automorphismus aus* $\mathfrak{G}_Z$ *als ein Grenzautomorphismus einer konvergenten Folge, welche aus den Automorphismen von der Form* $\sigma^a\tau$ *besteht, definiert ist. Dabei ist* τ *ein Automorphismus aus* $\mathfrak{G}_Z$ *und* a *eine ganze rationale Zahl.*

Beweis. Es sei ρ ein beliebiger Automorphismus aus $\mathfrak{G}_Z$, welcher durch die reguläre Abbildungsfolge $\rho_1, \rho_2, \ldots, \rho_n, \ldots$ definiert ist. Dann kann man eine reguläre Abbildung ρ_n $(n \geqq 1)$ immer in der Form

$$\sigma_n^{a_n}\tau_n$$

darstellen, wo σ_n eine reguläre Abbildung des schon oben bestimmten Automorphismus σ in N_n, τ_n ein Automorphismus aus $\mathfrak{G}_T^{(n)}$, und a_n eine ganze rationale Zahl ist. Nach Satz 15 existiert in $\mathfrak{G}_T$ eine Erweiterung $\tau^{(n)}$ von τ_n. Wir bilden nun eine Automorphismusreihe $\sigma^{a_1}\tau^{(1)}, \sigma^{a_2}\tau^{(2)}, \ldots, \sigma^{a_n}\tau^{(n)}, \ldots$. Dann konvergiert diese Reihe zu ρ. Denn ist nämlich N_ν ein beliebiger Teilkörper aus der Körperreihe $N_1, N_2, \ldots, N_n, \ldots$ von N, so induzieren $\sigma^{a_\nu}\tau^{(\nu)}$, $\sigma^{a_{\nu+1}}\tau^{(\nu+1)}$, $\ldots$ in N_ν alle einen und denselben Automorphismus ρ_ν, weil für $j \geqq \nu$ $\sigma^{a_j}\tau^{(j)}$ den Automorphismus $\rho_j = \sigma_j^{a_j}\tau_j$ in N_j induziert und dieser eine Erweiterung von $\rho_\nu = \sigma_\nu^{a_\nu}\tau_\nu$ ist. Hieraus folgt die obige Behauptung sofort.

Wir betrachten nun in einem Teilkörper N_n von N die Primidealzerlegung von $\mathfrak{p}$. Findet in N_n folgende Primidealzerlegung

$$\mathfrak{p} = (\mathfrak{P}_{n1} \ldots . \mathfrak{P}_{nr_n})^{e_n}$$

statt, dann ist bekanntlich e_n die Ordnung der Trägheitsgruppe eines Primteilers von $\mathfrak{p}$ nach k. Ist besonders $\mathfrak{G}_T$ eine endliche Gruppe von der Ordnung e, so kann man ebenso wie in S. 95 beweisen, dass von einem geeigneten Index i an der Exponent $e_j\,(i \geqq j)$ immer der Zahl e gleich sein muss. Also besitzt jeder Primteiler von $\mathfrak{p}$ in N den Exponenten e. Daraus kann man ebenso wie in Satz 13 folgenden Satz beweisen.

Satz 17. *Wenn die Trägheitsgruppe von $\mathfrak{P}$ nach k eine endliche Gruppe von der Ordnung e ist, dann ist der Exponent jedes Primteilers von $\mathfrak{p}$ in N gleich e. Wenn insbesondere $\mathfrak{p}$ ein endliches Ideals aus k ist, dann ist jeder Primteiler von $\mathfrak{p}$ in N von der Form*

$$(\mathfrak{P}^J)^e\,,$$

wobei $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in N und J ein beliebiger Automorphismus von N über k ist.

Wir betrachten nun den Fall, dass die Faktorgruppe $\mathfrak{G}_Z/\mathfrak{G}_T$ eine endliche Gruppe von der Ordnung f ist. Dann ist

$$\mathfrak{G}_Z = \mathfrak{G}_T + \sigma^{(1)}\mathfrak{G}_T + \ldots . + \sigma^{(f-1)}\mathfrak{G}_T\,,$$

wobei $\sigma^{(1)}, \sigma^{(2)}, \ldots . , \sigma^{(f-1)}$ geeignete Automorphismen aus $\mathfrak{G}_T$ bedeuten. Da in einem beliebigen Teilkörper N_n aus der Körperreihe von N $\mathfrak{G}_T$ bzw. $\mathfrak{G}_Z$ die Trägheitsgruppe $\mathfrak{G}_T^{(n)}$ bzw. die Zerlegungsgruppe $\mathfrak{G}_Z^{(n)}$ von $\mathfrak{P}_n$ nach k induziert (nach Satz 10 und 15), so ist die Ordnung von $\mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}$ nicht grösser als f. Es gibt also einen Index ν, derart dass für alle $j \geqq \nu$ die Ordnungen von $\mathfrak{G}_Z^{(j)}/\mathfrak{G}_T^{(j)}$ einer bestimmten natürlichen Zahl $\bar{f}$ gleich sind. Dann ist offenbar $\bar{f} \leqq f$.

Nun will ich zeigen, dass $\bar{f} = f$ ist. Es sei $\bar{\sigma}$ ein Automorphismus aus $\mathfrak{G}_Z$. Dann ist $\bar{\sigma}$ durch folgende reguläre Abbildungsfolge

$$\sigma_1^{a_1}\tau_1\,,\ \sigma_2^{a_2}\tau_2\,,\ \ldots .\,,\ \sigma_n^{a_n}\tau_n\,,\ \ldots .$$

definiert, wobei $\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$ die reguläre Abbildungsfolge ist, welche den in S. 100 bestimmten Automorphismus σ definiert, und τ_i Automorphismen aus $\mathfrak{G}_T^{(i)}$ sind $(i = 1, 2, \ldots, n, \ldots)$. Dabei kann man ohne Einschränkung der Allgemeinheit annehmen, dass die Exponenten $a_1, a_2, \ldots, a_n, \ldots$ nicht negativ und resp. kleiner sind als die Ordnungen von $\mathfrak{G}_Z^{(1)}/\mathfrak{G}_T^{(1)}, \mathfrak{G}_Z^{(2)}/\mathfrak{G}_T^{(2)}, \ldots, \mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}, \ldots$. Dann ist für jeden Index $n \geqq \nu$ der Exponent a_n gleich einer bestimmten, nicht negativen ganzen Zahl. Denn für $m > n \geqq \nu$ induziert $\sigma_m^{a_m}\tau_m$ den Automorphismus $\sigma_n^{a_n}\tau_n$ in N_n. Da aber σ_m den Automorphismus σ_n induziert, so induziert $\sigma_m^{a_m}\tau_m$ einen Automorphismus $\sigma_n^{a_m}\bar{\tau}_n$, wobei $\bar{\tau}_n$ der durch τ_m induzierte Automorphismus aus $\mathfrak{G}_T^{(n)}$ ist. Also ist

$$\sigma_n^{a_m}\bar{\tau}_n = \sigma_n^{a_n}\tau_n ,$$

ist also

$$\sigma_n^{a_m - a_n} = \tau_n(\bar{\tau}_n)^{-1} .$$

Da $\tau_n(\bar{\tau}_n)^{-1}$ zu $\mathfrak{G}_T^{(n)}$ gehört, so muss $\sigma_n^{a_m - a_n}$ auch in $\mathfrak{G}_T^{(n)}$ enthalten sein, d. h. $a_m - a_n$ ist durch $\bar{f}$ teilbar, weil σ_n ein erzeugendes Element von $\mathfrak{G}_Z^{(n)}/\mathfrak{G}_T^{(n)}$ ist. Da aber $a_m - a_n$ dem Betrag nach kleiner ist als $\bar{f}$, so muss $a_m = a_n$ sein. Dies gilt für beliebige m und n, welche nicht kleiner sind als ν. Es ist also $a_\nu = a_{\nu+1} = \ldots = a$. Ferner folgt noch, dass

$$\tau_n = \bar{\tau}_n$$

ist, d.h. τ_m ist eine Erweiterung von τ_n. Induziert τ_ν in $N_1, N_2, \ldots, N_{\nu-1}$ resp. die Automorphismen $\bar{\tau}_1, \bar{\tau}_2, \ldots, \bar{\tau}_{\nu-1}$, so definiert

$$\bar{\tau}_1, \bar{\tau}_2, \ldots, \bar{\tau}_{\nu-1}, \tau_\nu, \tau_{\nu+1}, \ldots$$

einen Automorphismus τ aus $\mathfrak{G}_T$. Da $\sigma^a\tau$ durch die reguläre Abbildungsfolge $\sigma_1^a\bar{\tau}_1, \ldots, \sigma_{\nu-1}^a\bar{\tau}_{\nu-1}, a_\nu^a\tau_\nu, \ldots$ definiert ist, so ist sicher

$$\sigma^a\tau = \bar{\sigma}$$

mit $0 \leqq a < \bar{f}$. Es gibt also höchstens $\bar{f}$ verschiedene Nebengruppen von $\mathfrak{G}_Z$ nach $\mathfrak{G}_T$. Nach dem früher Gezeigten ist also

$$f = \bar{f}.$$

Da $\sigma^f = \{\sigma_1^f, \ldots, \sigma_\nu^f, \ldots\}$ ist, so ist σ^f ein Automorphismus aus $\mathfrak{G}_T$. Da aber für eine natürliche Zahl $f' < f$ $\sigma_\nu^{f'}$ zu $\mathfrak{G}_T^{(\nu)}$ nicht gehört, so ist

$$\sigma^{f'}$$

auch kein Automorphismus aus $\mathfrak{G}_T$. Also sind die f Nebengruppen

$$\mathfrak{G}_T, \ \sigma\mathfrak{G}_T, \ \ldots, \ \sigma^{f-1}\mathfrak{G}_T$$

alle voneinander verschieden. Damit ist es gezeigt, dass

$$\mathfrak{G}_Z/\mathfrak{G}_T$$

zyklisch ist, falls $\mathfrak{G}_Z/\mathfrak{G}_T$ endliche Gruppe ist. Ferner ist die Ordnung f von $\mathfrak{G}_Z/\mathfrak{G}_T$ der Grad von $\mathfrak{P}$ nach k, weil für $n \geqq \nu$ $\mathfrak{P}_n$ den Grad f nach k besitzt. Es gilt also

Satz 18. *Wenn die Faktorgruppe $\mathfrak{G}_Z/\mathfrak{G}_T$ eine endliche Gruppe von der Ordnung f ist, so ist $\mathfrak{G}_Z/\mathfrak{G}_T$ zyklisch und f der Grad von $\mathfrak{P}$ nach k.*

Aus Satz 17, 18 und dem in S. 95 Bewiesenen folgt noch

Zusatz. Wenn die Ordnung von $\mathfrak{G}_T$ bzw. $\mathfrak{G}_Z$ e bzw. ef ist, so besitzt jeder Primteiler von $\mathfrak{p}$ den Grad f und den Exponenten e nach k.

Zum Schluss dieses Paragraphen beweisen wir

Satz 19. *Die Trägheitsgruppe von $\mathfrak{P}$ nach k ist abgeschlossen.*

Beweis. Wenn eine Fundamentalfolge

$$\tau^{(1)}, \ \tau^{(2)}, \ \ldots, \ \tau^{(n)}, \ \ldots$$

aus $\mathfrak{G}_T$ vorliegt, dann kann man ebenso wie in Satz 14 beweisen, dass der Grenzautomorphismus τ dieser Folge der galoisschen Gruppe von N nach k angehört. Ist $\tau_1, \tau_2, \ldots, \tau_n, \ldots$ die reguläre Abbildungs-

folge von τ, so ist für eine beliebige für $\mathfrak{P}$ ganze Zahl A_n aus einem beliebigen Teilkörper N_n aus der Körperreihe von N

$$\tau A_n = \tau_n A_n = \tau^{(j_n)} A_n \equiv A_n , \qquad \mod \mathfrak{P}_n ,$$

falls j_n grösser ist als eine geeignete Zahl. Hieraus folgt sofort, dass für alle für $\mathfrak{P}$ ganzen Zahlen A aus N die Kongruenz

$$\tau A \equiv A \qquad \mod \mathfrak{P}$$

gilt. Also gehört τ zu $\mathfrak{G}_T$, w. z. b. w.

§ 4. VERZWEIGUNGSGRUPPE.

In § 7 von M. habe ich die Verzweigungsgruppe in einem Normalkörper von endlichem Grade anders definiert als üblich, wenn der Grundkörper ein unendlicher algebraischer Zahlkörper ist. Die dort angegebene Definition stimmt aber im wesentlichen mit der gewöhnlichen überein, wenn der Grundkörper ein algebraischer Zahlkörper von endlichem Grade ist. Wir wollen also in diesem Paragraphen für die Verzweigungsgruppe auch eine neue Definition geben.

Wir legen wieder eine Normalkörperreihe $N_0 = k$, N_1, ..., N_n, ... eines Normalkörpers N und ihr entsprechend eine Primidealfolge $\mathfrak{P}_0 = \mathfrak{p}$, $\mathfrak{P}_1$, ..., $\mathfrak{P}_n$, ... eines Primideals $\mathfrak{P}$ aus N fest.

Es sei nun v ein Automorphismus aus der Trägheitsgruppe $\mathfrak{G}_T$ von $\mathfrak{P}$ nach k, dessen reguläre Abbildungsfolge $v_1, v_2, \ldots, v_n, \ldots$ sämtlich aus denjenigen regulären Abbildungen besteht, deren Ordnungen Potenzen einer und derselben Primzahl p sind. Dabei ist die Primzahl p durch das Primideal $\mathfrak{P}$ teilbar. Dann ist v_n, wie in Satz 15 bewiesen ist, ein Automorphismus aus der Trägheitsgruppe $\mathfrak{G}_T^{(n)}$ von $\mathfrak{P}_n$ nach k, dessen Ordnung eine bestimmte Potenz von p ist. Also gehört v_n der Verzweigungsgruppe $\mathfrak{G}_V^{(n)}$ von $\mathfrak{P}_n$ nach k an[1]. Also induziert v in jedem Teilkörper N_n einen Automorphismus aus $\mathfrak{G}_V^{(n)}$.

(1) M. S. 182–183.

Wir zeigen ferner, dass alle Automorphismen v aus $\mathfrak{G}_T$ mit der oben genannten Eigenschaft einen Normalteiler von $\mathfrak{G}_Z^{(1)}$ bilden. Nämlich wir bezeichnen die Menge aller solchen Automorphismen v mit $\mathfrak{G}_V$. Sind $v^{(1)}$, $v^{(2)}$ zwei beliebige Automorphismen aus $\mathfrak{G}_V$, welche durch die reguläre Abbildungsfolge

$$v_1^{(1)}, v_2^{(1)}, \ldots, v_n^{(1)}, \ldots$$

bzw.

$$v_1^{(2)}, v_2^{(2)}, \ldots, v_n^{(2)}, \ldots$$

definiert sind, so besteht die reguläre Abbildungsfolge

$$v_1^{(1)}v_1^{(2)}, v_2^{(1)}v_2^{(2)}, \ldots, v_n^{(1)}v_n^{(2)}, \ldots$$

von $v^{(1)}v^{(2)}$ offenbar aus denjenigen regulären Abbildungen, die als ihre Ordnungen Potenzen von p besitzen, weil ja $v_n^{(1)}v_n^{(2)}$ $(n \geqq 1)$ ein Automorphismus aus $\mathfrak{G}_V^{(n)}$ ist.

Ersichtlich gehört der identische Automorphismus zu $\mathfrak{G}_V$ und der inverse Automorphismus v^{-1} von v auch zu $\mathfrak{G}_V$, weil v^{-1} durch $v_1^{-1}, v_2^{-1}, \ldots, v_n^{-1}, \ldots$ definiert ist, und v_n^{-1} $(n \geqq 1)$ eine bestimmte Potenz von p als seine Ordnung besitzt.

Also ist $\mathfrak{G}_V$ eine Untergruppe von $\mathfrak{G}_T$.

Ferner sei σ ein beliebiger Automorphismus aus $\mathfrak{G}_Z$, welcher durch die reguläre Abbildungsfolge $\sigma_1, \sigma_2, \ldots, \sigma_n, \ldots$ definiert ist. Dann ist $\sigma^{-1}v\sigma$ aus $\mathfrak{G}_T$ durch die reguläre Abbildungsfolge

$$\sigma_1^{-1}v_1\sigma_1, \sigma_2^{-1}v_2\sigma_2, \ldots, \sigma_n^{-1}v_n\sigma_n, \ldots$$

definiert. Da aber $\mathfrak{G}_V^{(n)}$ ein Normalteiler von $\mathfrak{G}_Z^{(n)}$ ist[2], so gehört $\sigma_n^{-1}v_n\sigma_n$ offenbar zu $\mathfrak{G}_V^{(n)}$, d.h. die Ordnung von $\sigma_n^{-1}v_n\sigma_n$ ist eine bestimmte Potenz von p. Also gehört $\sigma^{-1}v\sigma$ zu $\mathfrak{G}_V$.

Hierbei will ich darauf aufmerksam machen, dass die obige Definition und die Eigenschaft von $\mathfrak{G}_V$ ganz unabhängig sind von der

(1) $\mathfrak{G}_Z$ bedeutet die Zerlegungsgruppe von $\mathfrak{P}$ nach k.
(2) M. S. 183.

Wahl der Körperreihe von N. Denn ist $N_0' = k, N_1', \ldots, N_n', \ldots$ eine andere Körperreihe von N und $v_1', v_2', \ldots, v_n', \ldots$ die auf diese neue Körperreihe bezogene reguläre Abbildungsfolge von v, so kann man immer einen Körper N_ν aus der früheren Körprreihe finden, derart dass N_ν den Körper N_n' enthält. Also induziert v_ν den Automorphismus v_n' in N_n'. Da für eine geeignete ganze Zahl a $v_\nu^{p^a}$ der identische Automorphismus von N_ν über k ist, so ist der durch $v_\nu^{p^a}$ induzierte Automorphismus $(v_n')^{p^a}$ auch der identische Automorphismus von N_n' über k, d.h. die Ordnung von v_n' ist eine Potenz von p. Umgekehrt kann man beweisen, dass die regulären Abbildungen $v_1, v_2, \ldots, v_n, \ldots$ alle Potenzen von p als ihre Ordnungen besitzen, wenn $v_1', v_2', \ldots, v_n', \ldots$ so sind. Hieraus kann man auch leicht zeigen, dass die oben erwähnte Eigenshaft von $\mathfrak{G}_V$ ganz unanhängig ist von der Wahl der Körperreihe von N. Diese Gruppe $\mathfrak{G}_V$ definiere ich als die *Verzweigungsgruppe* von $\mathfrak{P}$ nach k.

Wir betrachten nun in zwei nacheinanderfolgenden Normalkörpern N_i, N_{i+1} resp. die Verzweigungsgruppen $\mathfrak{G}_V^{(i)}$, $\mathfrak{G}_V^{(i+1)}$ von $\mathfrak{P}_i$, $\mathfrak{P}_{i+1}$. Dann ist nach Satz 43 von M.

$$\mathfrak{G}_V^{(i)} \cong \mathfrak{G}_V^{(i+1)} \mathfrak{H}_i / \mathfrak{H}_i^{(1)},$$

wobei $\mathfrak{H}_i$ die N_i zugeordnete Untergruppe der galoisschen Gruppe von N_{i+1} nach k. Dies zeigt aber, dass man für einen beliebigen Automorphismus aus $\mathfrak{G}_V^{(i)}$ mindestens eine seiner Erweiterungen in $\mathfrak{G}_V^{(i+1)}$ finden kann. Wenn also v_n ein beliebiger Automorphismus aus $\mathfrak{G}_V^{(n)}$ ist, dann existiert in $\mathfrak{G}_V$ mindestens ein Automorphismus v, welcher in N_n den Automorphismus v_n induziert.

Es gilt also

Satz 20. *Die Verzweigungsgruppe $\mathfrak{G}_V$ von $\mathfrak{P}$ nach k ist ein Normalteiler von $\mathfrak{G}_Z$ und $\mathfrak{G}_T$. Ein Automorphismus aus $\mathfrak{G}_V$ induziert in einem jeden Normalteilkörper N_n einen Automorphismus aus der Verzweigungsgruppe $\mathfrak{G}_V^{(n)}$ von $\mathfrak{P}_n$ nach k. Ferner induziert $\mathfrak{G}_V$ in N_n die ganze Verzweigungsgruppe $\mathfrak{G}_V^{(n)}$.*

(1) Siehe H. S. 483, wenn der Grundkörper k von endlichem Grade ist.

Nach Satz 39 von M. ist in N_n

$$\mathfrak{G}_T^{(n)}/\mathfrak{G}_V^{(n)}$$

zyklisch. Also kann man mit derselben Überlegung wie in S. 100 folgenden Satz beweisen.

Satz 21. *Es existiert in $\mathfrak{G}_T$ ein Automorphismus τ, der in jedem Normalteilkörper N_n aus der Körperreihe von N ein erzeugendes Element von $\mathfrak{G}_T^{(n)}/\mathfrak{G}_V^{(n)}$ induziert. Jeder Automorphismus aus $\mathfrak{G}_T$ ist durch eine konvergente Folge definiert, die aus den Automorphismen von der Form $\tau^a v$ besteht, wobei a eine ganze rationale Zahl und v ein Automorphismus aus $\mathfrak{G}_V$ ist.*

Aus Satz 21 folgt ebenso wie für $\mathfrak{G}_Z/\mathfrak{G}_T$ in S. 103 folgender Satz.

Satz 22. *Wenn $\mathfrak{G}_T/\mathfrak{G}_V$ eine endliche Gruppe ist, so ist $\mathfrak{G}_T/\mathfrak{G}_V$ zyklisch und ihre Ordnung gleich dem reduzierten Exponenten von $\mathfrak{P}$ nach k.*

Nun wollen wir den Spezialfall, dass die Ordnung von $\mathfrak{G}_V$ endlich ist, in Betracht ziehen. Wie wir schon für die Zerlegungs- und Trägheitsgruppe gezeigt haben, können wir auch beweisen, dass es einen Index i gibt, derart dass von i an alle Verzweigungsgruppen $\mathfrak{G}_V^{(i)}, \mathfrak{G}_V^{(i+1)}, \ldots, \mathfrak{G}_V^{(n)}, \ldots$ von derselben Ordnung wie der von $\mathfrak{G}_V$ sind. Da diese Ordnung eine bestimmte Potenz von p ist, so ist die Ordnung von $\mathfrak{G}_V$ auch eine Potenz von p.

Wenn insbesondere $\mathfrak{P}$ ein endliches Ideal ist (also ist nach Satz 5 $\mathfrak{p}$ auch endlich), dann ist nach Satz 17 $\mathfrak{G}_T$ und infolgedessen $\mathfrak{G}_V$ auch endlich. Ferner ist nach Zusatz von Satz 3 $\mathfrak{P}^2 \neq \mathfrak{P}$. Es existiert also ein Index ν, derart dass für jedes $j \geqq \nu$

$$N_j \frown \mathfrak{P}^2 = \mathfrak{P}_j^2 \neq \mathfrak{P}_j$$

ist (nach Satz 4). Dann erkennt man nach Anmerkung von S. 183 von M., dass die Verzweigungsgruppe $\mathfrak{G}_V^{(j)}$ von $\mathfrak{P}_j$ nach k aus der Gesamtheit derjenigen Automorphismen v_j besteht, für die die Kongruenz

$$v_j \Gamma_j \equiv \Gamma_j \mod \mathfrak{P}_j^2$$

für alle für $\mathfrak{P}_j$ ganzen Zahlen Γ_j aus N_j gilt. Wäre nun für einen Automorphismus v aus $\mathfrak{G}_V$ und für eine für $\mathfrak{P}$ ganze Zahl Γ aus N

$$v\Gamma \not\equiv \Gamma \mod \mathfrak{P}^2,$$

so gäbe es für einen passenden Index $n \geqq \nu$ einen Körper N_n, zu dem Γ gehörte, und in dem

$$v_n\Gamma \not\equiv \Gamma \mod \mathfrak{P}_n^2$$

wäre, wobei v_n der durch v induzierte Automorphismus aus $\mathfrak{G}_V^{(n)}$ wäre. Dies wäre aber Widerspruch.

Es gelte nun für einen Automorphismus $v' = \{v_i'\}$ aus $\mathfrak{G}$ und für eine beliebige für $\mathfrak{P}$ ganze Zahl Γ aus N die Kongruenz

$$v'\Gamma \equiv \Gamma \mod \mathfrak{P}^2.$$

Dann ist für jeden Index $n \geqq \nu$ $\mathfrak{P}^2 \cap N_n = \mathfrak{P}_n^2 \neq \mathfrak{P}_n$. Also ist für alle für $\mathfrak{P}$ ganzen Zahlen Γ_n aus N_n

$$v_n'\Gamma_n \equiv \Gamma_n \mod \mathfrak{P}_n^2.$$

Dabei bedeutet v_n' die reguläre Abbildung von v' in N_n. Daher gehört v_n' zur Verzweigungsgruppe $\mathfrak{G}_V^{(n)}$ von $\mathfrak{P}_n$ nach k. Nach Satz 24 von M. sind also $v_1', v_2', \ldots, v_{n-1}'$ resp. die Automorphismen aus $\mathfrak{G}_V^{(1)}, \mathfrak{G}_V^{(2)}, \ldots, \mathfrak{G}_V^{(n-1)}$, d. h. die Ordnungen von $v_1', v_2', \ldots, v_{n-1}'$ sind Potenzen von p. Nach dem eben Gezeigten folgt ohne weiteres, dass die regulären Abbildungen $v_1', v_2', \ldots, v_n', \ldots$ resp. zu den Verzweigungsgruppen $\mathfrak{G}_V^{(1)}, \mathfrak{G}_V^{(2)}, \ldots, \mathfrak{G}_V^{(n)}, \ldots$ gehören, d. h. v' zu $\mathfrak{G}_V$ gehört, weil nach Voraussetzung v' zur Trägheitsgruppe $\mathfrak{G}_T$ gehört und die Ordnungen von $v_1', v_2', \ldots, v_n', \ldots$ Potenzen von p sind.

Wir können weiter leicht beweisen, dass es einen Index κ gibt, derart dass für $j \geqq \kappa$ immer $\mathfrak{G}_T^{(j)}$ bzw. $\mathfrak{G}_V^{(j)}$ mit $\mathfrak{G}_T$ bzw. $\mathfrak{G}_V$ dieselbe Ordnung besitzt. Da $\mathfrak{G}_T$ bzw. $\mathfrak{G}_V$ die ganze Gruppe $\mathfrak{G}_V^{(j)}$ induziert, so kann man ebenso wie in S. 101 leicht schliessen, dass für $j \geqq \kappa$

$$\mathfrak{G}_T/\mathfrak{G}_V \cong \mathfrak{G}_T^{(j)}/\mathfrak{G}_V^{(j)}$$

ist. Da nach Definition von $\mathfrak{G}_V^{(j)}$ die Ordnung von $\mathfrak{G}_T^{(j)}/\mathfrak{G}_V^{(j)}$ zu p prim ist, so ist es auch die von $\mathfrak{G}_T/\mathfrak{G}_V$. Also gilt

Satz 23. *Wenn die Ordnung der Verzweigungsgruppe $\mathfrak{G}_V$ von $\mathfrak{P}$ nach k endlich ist, dann ist die Ordnung von $\mathfrak{G}_V$ eine Potenz von p, wobei p die durch $\mathfrak{P}$ teilbare Primzahl ist. Insbesondere, wenn $\mathfrak{P}$ endliches Ideal ist, dann besteht $\mathfrak{G}_V$ aus allen derjenigen Automorphismen v von N über k, für welche die Kongruenz*

$$v\Gamma \equiv \Gamma \mod \mathfrak{P}^2$$

für alle für $\mathfrak{P}$ ganzen Zahlen aus N besteht. Ferner ist die Faktorgruppe $\mathfrak{G}_T/\mathfrak{G}_V$ zyklisch und ihre Ordnung ist prim zu p.

Wir beweisen nun

Satz 24. *Die Verzweigungsgruppe $\mathfrak{G}_V$ ist abgeschlossen.*

Beweis. Es sei $v^{(1)}, v^{(2)}, \ldots, v^{(n)}, \ldots$ eine konvergente Folge aus $\mathfrak{G}_V$. Dann kann man wie in Satz 19 beweisen, dass es in der Trägheitsgruppe von $\mathfrak{P}$ nach k einen Automorphismus v gibt, welcher gerade der Grenzautomorphismus der obigen konvergenten Folge ist, weil $\mathfrak{G}_V$ eine Untergruppe der abgeschlossenen Gruppe $\mathfrak{G}_T$ ist. Es sei $v_1, v_2, \ldots, v_n, \ldots$ die reguläre Abbildungsfolge von v. Dann ist in einem beliebigen normalen Teilkörper N_n aus der Körperreihe von N über k

$$v_n(v_n^{(j)})^{-1}$$

der identische Automorphismus von N_n über k, falls j grösser ist als eine geeignete natürliche Zahl, wobei $v_n^{(j)}$ den durch $v^{(j)}$ in N_n induzierten Automorphismus bedeutet. Hieraus folgt ohne Schwierigkeit, dass v_n gehört zu $\mathfrak{G}_V^{(n)}$, d. h. die Ordnung von v_n eine Potenz von p ist, w. z. b. w.

Für die höheren Verzweigungsgruppen findet man heute noch keine systematische Theorie wie für die höheren Verzweigungsgruppen in endlichen algebraischen Zahlkörpern. Für die noch etwas tiefer eingehende Untersuchung verweise ich auf die Arbeit von HERBRAND[1].

(1) H. II. S. 711–717.

Zum Schluss dieses Paragraphen beweise ich folgenden Satz.

Satz 25. *Es sei K ein Teilkörper von N über k und $\mathfrak{H}$ die K zugeordnete Untergruppe der galoisschen Gruppe von N nach k. Ferner bezeichnen wir mit $\mathfrak{G}_Z$, $\mathfrak{G}_T$, $\mathfrak{G}_V$ resp. die Zerlegungs-, Trägheits-, Verzweigungsgruppe eines Primideals $\mathfrak{P}$ nach k. Dann gilt:*

1.) *Die Zerlegungsgruppe von $\mathfrak{P}$ nach k ist $\mathfrak{G}_Z \frown \mathfrak{H}$.*

2.) *Die Trägheitsgruppe von $\mathfrak{P}$ nach k ist $\mathfrak{G}_T \frown \mathfrak{H}$.*

3.) *Die Verzweigungsgruppe von $\mathfrak{P}$ nach k ist $\mathfrak{G}_V \frown \mathfrak{H}$.*

Beweis. Die Behauptung 1.) und 2.) folgen leicht aus Definition der beiden Gruppen. Um die Behauptung 3.) zu beweisen, bilden wir eine besondere Körperreihe von N über k. Und zwar bilden wir die Komposita

$$Kk = K = \overline{N}_0, \; KN_1 = \overline{N}_1, \; \ldots\ldots, \; KN_n = \overline{N}_n, \; \ldots\ldots .$$

Dann ist bekanntlich

$$K = \overline{N}_0 \subseteqq \overline{N}_1 \subseteqq \overline{N}_2 \subseteqq \ldots\ldots \subseteqq \overline{N}_n \subseteqq \ldots\ldots ,$$

und die Vereinigungsmenge von $\overline{N}_1, \overline{N}_2, \ldots\ldots, \overline{N}_n, \ldots\ldots$ ist der Körper N[1].

Es sei α_i eine primitive Zahl von N_i über k. Dann ist offenbar α_i auch eine primitive Zahl von $\overline{N}_i$ über K. Ist ρ ein Automorphismus aus $\mathfrak{H}$, so ist bekanntlich der durch ρ induzierte Automorphismus ρ_i in N_i dadurch bestimmt, in welche konjugierte Wurzel die Zahl α_i bei Ausübung von ρ übergeführt wird. Wir nehmen also an, dass α_i bei Ausübung von ρ in α_i' übergeführt wird: in Bezeichnung

$$\rho\alpha_i = \alpha_i' .$$

---

(1) Wenn N über K von endlichem Grade ist, dann gibt es unter $\overline{N}_1, \overline{N}_2, \ldots, \overline{N}_n, \ldots$ endlich viele verschiedene Körper. Wenn aber N über K von unendlichem Grade ist, so gibt es darunter unendlich viele verschiedene Körper.

Ist $f_i(x) = 0$ eine irreduzible Gleichung in K, welcher a_i genügt, so ist

$$0 = \rho(f_i(a_i)) = f_i(\rho a_i) = f_i(a_i') ,$$

weil K bei Anwendung von ρ elementweise invariant ist. a_i' ist daher eine Wurzel von $f_i(x) = 0$. Also bewirkt der durch ρ induzierte Automorphismus $\bar{\rho}_i$ von $\overline{N}_i$ über K den Körper $\overline{N}_i$, ebenso wie der Automorphismus ρ_i. Also ist die Ordnung von ρ_i gleich der von $\bar{\rho}_i$.

Da ein Automorphismus aus der Verzweigungsgruppe $\overline{\mathfrak{G}}_V$ von $\mathfrak{P}$ nach K nach Definition zur Trägheitsgruppe $\mathfrak{G}_T \frown \mathfrak{H}$ von $\mathfrak{P}$ nach K und folglich zu $\mathfrak{H}$ gehört, so besitzt ein solcher Automorphismus die oben erwähnte Eigenschaft wie ρ. Es sei also v ein Automorphismus aus der Verzweigungsgruppe von $\mathfrak{P}$ nach K. Dann besitzt der durch v induzierte Automorphismus $\bar{v}_i$ in $\overline{N}_i$ nach Definition eine Potenz von p als seine Ordnung, ist also die Ordnung von $v_i - v_i$ ist der durch v in N_i induzierte Automorphismus — auch eine Potenz von p. v gehört also nach Definition zu $\mathfrak{G}_V$. Daher ist

$$\overline{\mathfrak{G}}_V \leqq \mathfrak{G}_V \frown \mathfrak{H} .$$

Umgekehrt, wenn $v = \{v_i\}$ ein Automorphismus aus $\mathfrak{G}_V \frown \mathfrak{H}$ ist, dann kann man unter Benutzung der obigen Bezeichnungen beweisen, dass nach Definition von $\mathfrak{G}_V$ die Ordnung von v_i eine Potenz von p ist. Also ist die Ordnung von $\bar{v}_i$ auch eine Potenz von p, wobei i alle natürlichen Zahlen durchlaufen kann. Da v zu $\mathfrak{G}_T \frown \mathfrak{H}$ gehört, so ist nach Definition v ein Automorphismus aus $\overline{\mathfrak{G}}_V$. Also ist $\mathfrak{G}_V \frown \mathfrak{H} \leqq \overline{\mathfrak{G}}_V$. Damit ist es bewiesen, dass

$$\overline{\mathfrak{G}}_V = \mathfrak{G}_V \frown \mathfrak{H}$$

ist.

§ 5. ZERLEGUNGS-, TRÄGHEITS-, UND VERZWEIGUNGSKÖRPER.

In diesem Paragraphen bedeutet N wieder einen Normalkörper unendlichen Grades über k und es ist $N=\{N_n\}$. Im § 3 und § 4 haben wir bewiesen, dass die Zerlegungs-, Trägheits-, und Verzweigungsgruppe abgeschlossene Untergruppen der ganzen galoisschen Gruppe von N nach k sind. Entsprechend diesen Gruppen können wir jetzt den Zerlegungs-, Trägheits-, und Verzweigungskörper definieren.

Zerlegungskörper. Derjenige Körper, welcher der Invariantenkörper der Zerlegungsgruppe $\mathfrak{G}_Z$ eines Primideals $\mathfrak{P}$ aus N nach k ist, heisse der *Zerlegungskörper* von $\mathfrak{P}$, und wir bezeichnen ihn mit K_Z.

Wir bilden nun den Durchschnitt $K_Z^{(i)}=K_Z\frown N_i$ von K_Z mit N_i. Dann ist K_Z nach dem in S. 81 Erwähnten der Vereinigungskörper von $K_Z^{(1)}, K_Z^{(2)}, \ldots, K_Z^{(n)}, \ldots$, wobei die Körper $K_Z^{(1)}, K_Z^{(2)}, \ldots, K_Z^{(n)}, \ldots$ resp. der Invariantenkörper von $\mathfrak{G}_Z^{(1)}, \mathfrak{G}_Z^{(2)}, \ldots, \mathfrak{G}_Z^{(n)}, \ldots$ sind. Dabei ist $\mathfrak{G}_Z^{(i)}$ die durch $\mathfrak{G}_Z$ in N_i induzierte Gruppe und diese ist nach Satz 10 die Zerlegungsgruppe von $\mathfrak{P}_i$ nach k, wo wieder $\mathfrak{P}_i=\mathfrak{P}\frown N_i$ ist. Also ist $K_Z^{(i)}$ der Zerlegungskörper von $\mathfrak{P}_i$.

Es sei $\mathfrak{P}_Z$ das durch $\mathfrak{P}$ teilbare Primideal aus $K_Z^{(i)}$ und $\mathfrak{P}_Z^{(i)}$ das durch $\mathfrak{P}_Z$ teilbare Primideal aus $K_Z^{(i)}$. Dann besitzt $\mathfrak{P}_Z^{(i)}$ nach Satz 34 von M. den Grad 1 und den Exponenten 1 nach k. Nach Definition des Grades und Exponenten besitzt $\mathfrak{P}_Z$ aus K_Z den Grad 1 und den Exponenten 1 nach k. Damit ist bewiesen:

Satz 26. *Der Zerlegungskörper K_Z von $\mathfrak{P}$ ist der Vereinigungskörper von $K_Z^{(1)}, K_Z^{(2)}, \ldots, K_Z^{(n)}, \ldots$, wobei $K_Z^{(i)}$ der Zerlegungskörper von $\mathfrak{P}_i$ über k ist $(i\geqq 1)$. Das durch $\mathfrak{P}$ teilbare Primideal $\mathfrak{P}_Z$ aus K_Z besitzt den Grad 1 und den Exponenten 1 nach k.*

Ferner können wir folgenden Satz beweisen.

Satz 27. Maximaleigenschaft des Zerlegungskörpers.

Der Zerlegungskörper K_Z von $\mathfrak{P}$ ist der maximale Teilkörper von N über k von der Art, dass jeder Teilkörper K von N über k, in

dem das durch $\mathfrak{P}$ teilbare Primideal den Grad 1 und den Exponenten 1 nach k besitzt, in K enthalten ist.

Beweis. Wir bilden nun den Körper $K_i = K \cap N_i$ $(i \geqq 1)$, und bezeichnen das durch $\mathfrak{P}$ teilbare Primideal aus K mit $\mathfrak{P}'$. Da K der Vereinigungskörper von $K_1, K_2, \ldots, K_n, \ldots$ ist, so besitzt $\mathfrak{P}'$ dann und nur dann den Grad 1 und den Exponenten 1 nach k, wenn das durch $\mathfrak{P}'$ (also durch $\mathfrak{P}$) teilbare Primideal $\mathfrak{P}_i'$ aus jedem Körper K_i den Grad 1 und den Exponenten 1 nach k besitzt. Nach Satz 35 von M. (nach der Maximaleigenschaft von $K_Z^{(i)}$) muss dann jeder Körper K_i in $K_Z^{(i)}$ enthalten sein. Also ist K offenbar ein Teilkörper von K_Z.

Trägheitskörper. Wir nennen denjenigen Körper, der der Invariantenkörper der Trägheitsgruppe $\mathfrak{G}_T$ von $\mathfrak{P}$ nach k ist, den *Trägheitskörper* von $\mathfrak{P}$ und bezeichnen ihn mit K_T.

Ebenso wie für den Zerlegungskörper K_Z kann man beweisen

Satz 28. *Der Trägheitskörper K_T von $\mathfrak{P}$ ist der Vereinigungskörper von $K_T^{(1)}, K_T^{(2)}, \ldots, K_T^{(n)}, \ldots$. Dabei bedeutet $K_T^{(i)}$ den Trägheitskörper des durch $\mathfrak{P}$ teilbaren Primideals $\mathfrak{P}_i$ aus N_i. Das durch $\mathfrak{P}$ teilbare Primideal $\mathfrak{P}_T$ aus K_T besitzt den Exponenten 1 nach k und denselben Grad nach k wie den von $\mathfrak{P}$ nach k.*

Beweis. Die erste Hälfte dieses Satzes kann man genau so wie für den Zerlegungskörper beweisen (siehe S. 112). Ist nun $\mathfrak{P}_T^{(n)}$ das durch $\mathfrak{P}$ teilbare Primideal aus $K_T^{(n)}$, so besitzt nach Satz 37 von M. $\mathfrak{P}_T^{(n)}$ den Exponenten 1 und denselben Grad f_n nach k wie den von $\mathfrak{P}_n$. Aus Definition folgt also, dass der Exponent von $\mathfrak{P}$ nach k gleich 1 ist, und der Grad von $\mathfrak{P}_T$ nach k $\lim\limits_{n\to\infty} f_n$ — der Grad von $\mathfrak{P}$ nach k — ist.

Satz 29. Maximaleigenschaft des Trägheitskörpers.

Der Trägheitskörper K_T ist der maximale Teilkörper von N über k, derart dass jeder Teilkörper von N über k, in dem das durch $\mathfrak{P}$ teilbare Primideal den Exponenten 1 nach k besitzt, in K_T enthalten ist.

Beweis. Diesen Satz kann man mit Hilfe von Satz 38 von M. und von Satz 28 ebenso wie Satz 27 beweisen.

Nun ist $\mathfrak{G}_T$ ein Normalteiler von $\mathfrak{G}_Z$, ist also nach Satz 6 der Invariantenkörper K_T von $\mathfrak{G}_T$ ein Normalkörper über K_Z, und die galoissche Gruppe von K_T nach K_Z isomorph zur Faktorgruppe $\mathfrak{G}_Z/\mathfrak{G}_T$. Zieht man das in Satz 16 erhaltene Resultat in Betracht, so ist jeder Automorphismus aus $\mathfrak{G}_Z$ durch eine konvergente (über k) Folge $\sigma^{a_1}\tau^{(1)}, \ldots., \sigma^{a_n}\tau^{(n)}, \ldots.$ definiert, wobei $\tau^{(1)}, \tau^{(2)}, \ldots., \tau^{(n)}, \ldots.$ resp. Automorphismen aus $\mathfrak{G}_T$, und σ ein bestimmter Automorphismus aus $\mathfrak{G}_Z$ sind. Aber nach dem in S. 82 Bewiesenen ist diese Folge auch konvergent über K_Z. Bezeichnet man nun mit Σ den durch σ induzierten Automorphismus von K_T über K_Z, so ist nach dem in S. 85 Bewiesenen die Folge

$$\Sigma^{a_1}, \Sigma^{a_2}, \ldots., \Sigma^{a_n}, \ldots. .$$

über K_Z konvergent. Offenbar ist jedes Glied dieser Folge durch einen Automorphismus Σ erzeugt. Also ist jeder Automorphismus von K_T über K_Z entweder eine Potenz von Σ oder durch eine konvergente Folge von der Form $\Sigma^{a_1}, \Sigma^{a_2}, \ldots., \Sigma^{a_n}, \ldots.$ definiert. Daher ist die galoissche Gruppe von K_T nach K_Z im gewissen Sinne durch einen Automorphismus Σ erzeugt. Diese galoissche Gruppe von K_T nach K_Z ist also nach Herrn KRULL *idealzyklisch*[1].

Damit ist bewiesen:

Satz 30. *Der Trägheitskörper K_T von $\mathfrak{P}$ ist ein Normalkörper über dem Zerlegungskörper K_Z von $\mathfrak{P}$. Die galoissche Gruppe von K_T nach K_Z ist isomorph zu $\mathfrak{G}_Z/\mathfrak{G}_T$, und folglich idealzyklisch.*

Aus Satz 30 folgt noch:

Zusatz. Wenn $\mathfrak{G}_Z/\mathfrak{G}_T$ eine endliche Gruppe von der Ordnung f ist, dann ist $\mathfrak{G}_Z/\mathfrak{G}_T$ zyklisch, und der Exponent bzw. der Grad von $\mathfrak{P}_T$ nach k ist gleich 1 bzw. f.

Diesen Zusatz kann man mit Hilfe von Satz 18 und 28 beweisen.

(1) K. S. 695. Man kann noch einfacher diese Tatsache beweisen, wenn man folgende Tatsache beachtet, dass jeder endliche Teilkörper von K_T über K_Z zyklisch ist. Siehe K. S. 696.

Verzweigungskörper. Der Invariantenkörper der Verzweigungsgruppe $\mathfrak{G}_V$ eines Primideals $\mathfrak{P}$ aus N heisse der *Verzweigungskörper* und wir bezeichnen ihn mit K_V.

Wir beweisen nun folgenden Satz.

Satz 31. *Der Verzweigungskörper K_V von $\mathfrak{P}$ ist der Vereinigungskörper von $K_V^{(1)}$, $K_V^{(2)}$, ..., $K_V^{(n)}$, ... Dabei bedeutet $K_V^{(n)}$ den Verzweigungskörper von $\mathfrak{P}_n$ über k. Ferner besitzt das durch $\mathfrak{P}$ teilbare Primideal $\mathfrak{P}_V$ aus K_V den Exponenten $E^{(0)}$ und den Grad F nach k, wobei $E^{(0)}$ und F resp. der reduzierte Exponent und der Grad von $\mathfrak{P}$ nach k sind.*

Beweis. Die erste Hälfte dieses Satzes kann man ebenso leicht wie für den Zerlegungskörper beweisen (siehe S. 112).

Bezeichnet man nun mit $\mathfrak{P}_V^{(n)}$ das durch $\mathfrak{P}$ teilbare Primideal aus $K_V^{(n)}$, so sind nach Satz 40 von M. der Exponent und der Grad von $\mathfrak{P}_V^{(n)}$ nach k resp. $e_n^{(0)}$ und f_n, wo $e_n^{(0)}$ und f_n resp. der reduzierte Exponent und der Grad von $\mathfrak{P}_n$ nach k sind. Da nach Definition $E^{(0)} = \lim_{n\to\infty} e_n^{(0)}$ und $F = \lim_{n\to\infty} f_n$ resp. der Exponent und der Grad von $\mathfrak{P}_V$ nach k ist, so folgt die letzte Behauptung.

Im obigen Beweis ist $E^{(0)}$ zu p prim, wo p die durch $\mathfrak{P}$ teilbare Primzahl bedeutet. Denn $e_n^{(0)}$ ist der reduzierte Exponent von $\mathfrak{P}_n$ nach k, ist also zu p prim.

Nun beweisen wir

Satz 32. Maximaleigenschaft des Verzweigungskörpers.

Der Verzweigungskörper K_V ist der maximale Teilkörper von N, derart dass jeder Teilkörper K von N über k, in dem das durch $\mathfrak{P}$ teilbare Primideal den zu p primen Exponenten besitzt, in K_V enthalten ist. Dabei ist p die durch $\mathfrak{P}$ teilbare Primzahl.

Beweis. Wir können diesen Beweis genau so ausführen wie für Satz 26, indem man Satz 41 von M. benutzt.

Nach Satz 21 kann man folgenden Satz genau so wie Satz 30 beweisen.

Satz 33. *Der Körper K_V ist ein Normalkörper über K_T und seine galoissche Gruppe nach K_T ist isomorph zu $\mathfrak{G}_T/\mathfrak{G}_V$, also idealzyklisch.*

Aus Satz 33 folgt noch:

Zusatz. Wenn $\mathfrak{G}_T/\mathfrak{G}_V$ eine endliche Gruppe ist, dann ist der Grad von K_V nach K_T gleich dem Exponenten von $\mathfrak{P}_V$ nach k, wobei $\mathfrak{P}_V$ das durch $\mathfrak{P}$ teilbare Primideal aus K_V bedeutet.

Beweis. Nach Voraussetzung folgt aus Satz 22, dass der Grad von K_V nach K_T dem reduzierten Exponenten von $\mathfrak{P}$ nach k gleich ist. Daher ergibt sich die Behauptung aus Satz 31.

Wir beweisen nun folgenden Satz.

Satz 34. *Es seien* $\mathfrak{A}$, $\mathfrak{B}$ *zwei abgeschlossene Untergruppen der ganzen galoisschen Gruppe* $\mathfrak{G}$ *von* N *nach* k, *und ferner* $\mathfrak{B}$ *ein Normalteiler von* $\mathfrak{G}$. *Dann ist* $\mathfrak{AB}$ *eine abgeschlossene Untergruppe.*

Beweis. Dass $\mathfrak{AB}$ eine Untergruppe von $\mathfrak{G}$ bildet, kann man leicht bestätigen.

Da $\mathfrak{B}$ ein Normalteiler von $\mathfrak{G}$ ist, so ist jedes Element aus $\mathfrak{AB}$ von der Form $\alpha\beta$, wobei α bzw. β ein Automorphismus aus $\mathfrak{A}$ bzw. $\mathfrak{B}$ ist.

Nun sei $\alpha^{(1)}\beta^{(1)}, \ldots, \alpha^{(n)}\beta^{(n)}, \ldots$ eine Fundamentalfolge aus $\mathfrak{AB}$. Dann besitzt diese Folge ihren Grenzautomorphismus γ in $\mathfrak{G}$. Ist $\gamma_1, \gamma_2, \ldots, \gamma_n, \ldots$ die reguläre Abbildungsfolge von γ, so existiert ein Index κ, derart dass in N_n $\alpha^{(\kappa)}\beta^{(\kappa)}, \alpha^{(\kappa+1)}\beta^{(\kappa+1)}, \ldots$ den Automorphismus γ_n induzieren.

Es seien $\alpha_n^{(1)}, \alpha_n^{(2)}, \ldots, \alpha_n^{(i_n)}$ bzw. $\beta_n^{(1)}, \beta_n^{(2)}, \ldots, \beta_n^{(j_n)}$ die sämtlichen verschiedenen Automorphismen[1], welche $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}, \ldots$ bzw. $\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)}, \ldots$ in N_n induzieren. Dann können wir daraus alle möglichen zu γ_n gleichen Produkte, etwa

$$\alpha_n^{(1)}\beta_n^{(1)}, \ldots, \alpha_n^{(k_n)}\beta_n^{(k_n)},$$

bilden. Für $n = 1, 2, \ldots$ bilden wir alle solchen Produkte:

$$\left.\begin{array}{llll} \gamma_1 = \alpha_1^{(1)}\beta_1^{(1)}, & \gamma_1 = \alpha_1^{(2)}\beta_1^{(2)}, & \ldots, & \gamma_1 = \alpha_1^{(k_1)}\beta_1^{(k_1)}, \\ \gamma_2 = \alpha_2^{(1)}\beta_2^{(1)}, & \gamma_2 = \alpha_2^{(2)}\beta_2^{(2)}, & \ldots, & \gamma_2 = \alpha_2^{(k_2)}\beta_2^{(k_2)}, \\ \vdots & & & \\ \gamma_\nu = \alpha_\nu^{(1)}\beta_\nu^{(1)}, & \gamma_\nu = \alpha_\nu^{(2)}\beta_\nu^{(2)}, & \ldots, & \gamma_\nu = \alpha_\nu^{(k_\nu)}\beta_\nu^{(k_\nu)}, \\ \vdots & & & \end{array}\right\} \quad (\mathrm{I}).$$

(1) Die Anzahl von solchen induzierten Automorphismen ist endlich, weil die Anzahl der Automorphismen von N_n über k endlich ist.

Es sei $\gamma_\nu = \alpha_\nu\beta_\nu$ ein Beliebiges aus $\alpha_\nu^{(1)}\beta_\nu^{(1)}, \ldots, \alpha_\nu^{(k_\nu)}\beta_\nu^{(k_\nu)}$. Dann kann man für $1 \leqq \rho < \nu$ in $\alpha_\rho^{(1)}\beta_\rho^{(1)}, \ldots, \alpha_\rho^{(k_\rho)}\beta_\rho^{(k_\rho)}$ mindestens ein $\alpha_\rho\beta_\rho$ finden, dessen Faktor α_ρ bzw. β_ρ in N_ν α_ν bzw. β_ν als seine Erweiterung besitzt. Denn induziert α_ν bzw. β_ν in N_ρ $\bar{\alpha}_\rho$ bzw. $\bar{\beta}_\tau$, so kann man etwa

$$\bar{\alpha}_\rho = \alpha_\rho \qquad \text{und} \qquad \bar{\beta}_\rho = \beta_\rho$$

setzen.

Es sei für $l \geqq 1$

$$\gamma_l = \alpha_l\beta_l, \ \gamma_{l+1} = \alpha_{l+1}\beta_{l+1}, \ \ldots, \ \gamma_\nu = \alpha_\nu\beta_\nu, \ \ldots$$

eine reguläre Abbildungsfolge von γ, wobei $\alpha_l, \ldots, \alpha_\nu, \ldots$ bzw. $\beta_l, \ldots, \beta_\nu, \ldots$ in Produkten von (I) als Faktoren auftreten. Wenn in zwei beliebigen nacheinanderfolgenden Automorphismen aus α_l, $\alpha_{l+1}, \ldots, \alpha_\nu$ bzw. $\beta_l, \beta_{l+1}, \ldots, \beta_\nu$ jeder nachfolgende seinen vorstehenden induziert, aber $\alpha_{\nu+1}$ oder $\beta_{\nu+1}$ resp. keine Erweiterung von α_ν oder β_ν ist, dann heisse

$$\gamma_l = \alpha_l\beta_l, \ \ldots, \ \gamma_\nu = \alpha_\nu\beta_\nu$$

eine *fortsetzbare Folge* von $\alpha_l\beta_l$. Für ein bestimmtes $\alpha_l\beta_l$ bilde man alle möglichen fortsetzbaren Folgen. Dann nennt man die Maximalanzahl der Glieder von allen möglichen fortsetzbaren Folgen von $\alpha_l\beta_l$ den *Index* von $\alpha_l\beta_l$. Wenn es keine Maximalanzahl gibt, dann sagt man, dass der Index von $\alpha_l\beta_l$ unendlich wird[1].

Nun betrachten wir die Indizes aller $\alpha_1^{(1)}\beta_1^{(1)}, \ldots, \alpha_1^{(k_1)}\beta_1^{(k_1)}$. Dann gibt es darunter mindestens einen Index, welcher unendlich wird. Denn wäre dies nicht der Fall, so gäbe es eine Zahl m, derart dass die Indizes von $\alpha_1^{(1)}\beta_1^{(1)}, \ldots, \alpha_1^{(k_1)}\beta_1^{(k_1)}$ kleiner wären als m. Anderseits gibt es aber nach dem oben Gezeigten für eine natürlcihe Zahl $\nu > m$ $\gamma_\nu = \alpha_\nu\beta_\nu$, das in N_1 eines von $\alpha_1^{(1)}\beta_1^{(1)}, \ldots, \alpha_1^{(k_1)}\beta_1^{(k_1)}$ induziert, d. h. eines von $\alpha_1^{(1)}\beta_1^{(1)}, \ldots, \alpha_1^{(k_1)}\beta_1^{(k_1)}$ besitzt mindestens den Index m. Dies steht in Widerspruch gegen die obige Annahme. Es gibt also einen Automorphismus, etwa $\alpha_1^{(1)}\beta_1^{(1)}$, dessen Index unendlich wird.

(1) Diesen Gedanken verdanke ich Herrn KUNUGI.

Nun betrachten wir die zweiten Glieder von allen möglichen fortsetzbaren Folgen von $\alpha_1^{(1)}\beta_1^{(1)}$. Es seien etwa

$$\alpha_2^{(1)}\beta_2^{(1)}, \ldots\ldots, \alpha_2^{(l_2)}\beta_2^{(l_2)}$$

alle solchen Glieder. Von $\alpha_2^{(1)}\beta_2^{(1)}, \ldots\ldots, \alpha_2^{(l_2)}\beta_2^{(l_2)}$ ausgehend, bilden wir dann alle möglichen fortsetzbaren Folgen wie oben und betrachten die Indizes von $\alpha_2^{(1)}\beta_2^{(1)}, \ldots\ldots, \alpha_2^{(l_2)}\beta_2^{(l_2)}$. Da die Gesamtheit aller möglichen fortsetzbaren Folgen von $\alpha_2^{(1)}\beta_2^{(1)}, \ldots\ldots, \alpha_2^{(l_2)}\beta_2^{(l_2)}$ mit der von allen möglichen fortsetzbaren von $\alpha_1^{(1)}\beta_1^{(1)}$ übereinstimmt, so muss mindestens eines von $\alpha_2^{(1)}\beta_2^{(1)}, \ldots\ldots, \alpha_2^{(l_2)}\beta_2^{(l_2)}$, also etwa $\alpha_2^{(1)}\beta_2^{(1)}$, denjenigen Index besitzen, welcher unendlich wird. So bestimmen wir etwa $\alpha_1^{(1)}\beta_1^{(1)}, \ldots\ldots, \alpha_{\nu-1}^{(1)}\beta_{\nu-1}^{(1)}$, deren Indizes unendlich werden.

Es seien etwa $\alpha_\nu^{(1)}\beta_\nu^{(1)}, \ldots\ldots, \alpha_\nu^{(l_\nu)}\beta_\nu^{(l_\nu)}$ die zweiten Glieder von allen möglichen fortsetzbaren Folgen von $\alpha_{\nu-1}^{(1)}\beta_{\nu-1}^{(1)}$ (also die ν-ten Glieder der gewissen forsetzbaren Folgen von $\alpha_1^{(1)}\beta_1^{(1)}$). Wir können wieder leicht zeigen, dass mindestens eines von $\alpha_\nu^{(1)}\beta_\nu^{(1)}, \ldots\ldots, \alpha_\nu^{(l_\nu)}\beta_\nu^{(l_\nu)}$ denjenigen Index, welcher unendlich wird, besitzt, weil der Index von $\alpha_{\nu-1}^{(1)}\beta_{\nu-1}^{(1)}$ unendlich wird. Es sei etwa $\alpha_\nu^{(1)}\beta_\nu^{(1)}$ ein solches. So können wir auch $\alpha_{\nu+1}^{(1)}\beta_{\nu+1}^{(1)}, \ldots\ldots$ bilden, deren Indizes unendlich werden.

Betrachtet man nun

$$\gamma_1 = \alpha_1^{(1)}\beta_1^{(1)}, \ \gamma_2 = \alpha_2^{(1)}\beta_2^{(1)}, \ \ldots\ldots, \ \gamma_\nu = \alpha_\nu^{(1)}\beta_\nu^{(1)}, \ \ldots\ldots,$$

so ist dies sicher eine reguläre Abbildungsfolge von γ, welche folgende Eigenschaft besitzt:

$$\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots\ldots, \alpha_\nu^{(1)}, \ldots\ldots \text{ bzw. } \beta_1^{(1)}, \beta_2^{(1)}, \ldots\ldots, \beta_\nu^{(1)}, \ldots\ldots$$

bilden eine reguläre Abbildungsfolge.

Nach der Wahl von $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots\ldots, \alpha_\nu^{(1)}, \ldots\ldots$ kann man aus den Faktoren von $\alpha^{(1)}\beta^{(1)}, \ldots\ldots, \alpha^{(n)}\beta^{(n)}, \ldots\ldots$ folgende Automorphismen $\alpha^{(r_1)}, \alpha^{(r_2)}, \ldots\ldots, \alpha^{(r_\nu)}, \ldots\ldots$ herausgreifen[1], welche resp. $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots\ldots, \alpha_\nu^{(1)}, \ldots\ldots$ induzieren.

(1) $r_1, r_2, \ldots\ldots, r_\nu, \ldots\ldots$ brauchen nicht notwendig voneinander verschieden zu sein, aber es ist $r_1 \leqq r_2 \leqq \ldots\ldots \leqq r_\nu \leqq \ldots\ldots$.

Wir zeigen nun, dass $\alpha^{(r_1)}, \alpha^{(r_2)}, \ldots, \alpha^{(r_\nu)}, \ldots$ eine Fundamentalfolge ist. Denn ist $\rho \geqq \nu$, so induziert jedes

$$\alpha^{(r_\nu)}(\alpha^{(r_\rho)})^{-1}$$

in N_ν den identischen Automorphismus, weil in N_ν, N_ρ α^{r_ν}, α^{r_ρ} resp. $\alpha_\nu^{(1)}$, $\alpha_\rho^{(1)}$ induzieren, und $\alpha_\rho^{(1)}$ in N_ν $\alpha_\nu^{(1)}$ induziert. Da $\mathfrak{A}$ eine abgeschlossene Untergruppe ist, so besitzt $\alpha^{(r_1)}, \alpha^{(r_2)}, \ldots, \alpha^{(r_\nu)}, \ldots$ in $\mathfrak{A}$ den Grenzautomorphismus α, und α ist offenbar durch die reguläre Abbildungsfolge $\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_\nu^{(1)}, \ldots$ definiert. Ebenso existiert in $\mathfrak{B}$ ein Automorphismus β, welcher durch $\beta_1^{(1)}, \beta_2^{(1)}, \ldots, \beta_\nu^{(1)}, \ldots$ definiert ist.

Das Produkt $\alpha\beta$ von α mit β ist offenbar durch die reguläre Abbildungsfolge.

$$\gamma_1 = \alpha_1^{(1)}\beta_1^{(1)}, \ldots, \gamma_\nu = \alpha_\nu^{(1)}\beta_\nu^{(1)}, \ldots$$

definiert. Also ist $\alpha\beta = \gamma$. Damit ist es bewiesen, dass $\mathfrak{AB}$ eine abgeschlossene Untergruppe ist.

Wir beweisen zum Schluss folgenden Satz.

Satz 35. *Es sei $\overline{K}$ ein beliebiger Normalkörper zwischen N und k, und $\mathfrak{H}$ die $\overline{K}$ zugeordnete Untergruppe der galoisschen Gruppe von N nach k. Ferner seien $\mathfrak{G}_Z$, $\mathfrak{G}_T$, $\mathfrak{G}_V$ resp. die Zerlegungs-, Trägheits-, Verzweigungsgruppe eines Primideals $\mathfrak{P}$ aus N nach k und $\overline{\mathfrak{P}}$ das durch $\mathfrak{P}$ teilbare Primideal aus $\overline{K}$. Dann gilt:*

1.) *Die Zerlegungsgruppe von $\overline{\mathfrak{P}}$ nach k ist isomorph zu $\mathfrak{G}_Z\mathfrak{H}/\mathfrak{H}$.*

2.) *Die Trägheitsgruppe von $\overline{\mathfrak{P}}$ nach k ist isomorph zu $\mathfrak{G}_T\mathfrak{H}/\mathfrak{H}$.*

3.) *Die Verzweigungsgruppe von $\overline{\mathfrak{P}}$ nach k ist isomorph zu $\mathfrak{G}_V\mathfrak{H}/\mathfrak{H}$.*

Beweis. Wir betrachten zunächst den Zerlegungskörper $\overline{K}_Z$ von $\overline{\mathfrak{P}}$ über k. In $\overline{K}_Z$ besitzt das durch $\overline{\mathfrak{P}}$ teilbare Primideal den Grad 1 und den Exponenten 1 nach k. Nach Satz 27 ist $\overline{K}_Z$ im Zerlegungskörper K_Z von $\mathfrak{P}$ über k enthalten. Da aber $\overline{K}_Z$ in $\overline{K}$ enthalten ist,

so ist es im Durchschnitt von K_Z mit $\overline{K}$ enthalten. Also ist $\overline{K}_Z$ bei Ausübung aller Automorphismen aus $\mathfrak{G}_Z$ und $\mathfrak{H}$ elementweise invariant. Also ist $\mathfrak{G}_Z\mathfrak{H}$ eine Untergruppe der $\overline{K}_Z$ zugeordneten Untergruppe.

Da $\mathfrak{G}_Z$, $\mathfrak{H}$ abgeschlossene Gruppen und $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$ sind, so ist nach Satz 34 $\mathfrak{G}_Z\mathfrak{H}$ eine abgeschlossene Untergruppe. Also existiert der Invariantenkörper K' von $\mathfrak{G}_Z\mathfrak{H}$. Dann ist nach dem oben Bewiesenen $\overline{K}_Z \subseteqq K'$. K' ist offenbar ein Teilkörper von K_Z und $\overline{K}$. In K' besitzt das durch $\mathfrak{P}$ teilbare Primideal den Grad 1 und den Exponenten 1 nach k, weil sonst $\mathfrak{P}_Z^{(1)}$ nicht mehr den Grad 1 und den Exponenten 1 nach k besitzen könnte. Also ist nach Satz 27 K' in $\overline{K}_Z$ enthalten. Daher ist

$$K' = \overline{K}_Z .$$

Die K_Z zugeordnete Untergruppe ist also $\mathfrak{G}_Z\mathfrak{H}$. Hieraus folgt nach Satz 6 die Behauptung 1.).

Die Behauptung 2.) und 3.) kann man ebenso wie die Behauptung 1.) beweisen, indem man an der Stelle von Satz 27 resp. Satz 29 und 32 benutzt.

---

(1) $\mathfrak{P}_Z$ ist das durch $\mathfrak{P}$ teilbare Primideal aus K_Z.