ÜBER EINEN SATZ VON HERBRAND

Von

Mikao MORIYA

§ 1.

Es sei k ein algebraischer Zahlkörper von endlichem Grade und K_1, K_2 seien zwei endliche Erweiterungskörper über k. Ferner sei $\mathfrak{P}$ ein Primideal aus K_1K_2 (K_1K_2 ist das Kompositum von K_1 und K_2), und $\mathfrak{P}_1$ bzw. $\mathfrak{P}_2$ das durch $\mathfrak{P}$ teilbare Primideal aus K_1 bzw. K_2. Dann bezeichnen wir mit f_1 bzw. f_2 den Relativgrad von $\mathfrak{P}_1$ bzw. $\mathfrak{P}_2$ nach k, und mit $e_1 = e_1^{(0)}p^{m_1}$ bzw. $e_2 = e_2^{(0)}p^{m_2}$ den Exponenten[1] von $\mathfrak{P}_1$ bzw. $\mathfrak{P}_2$ nach k, wobei p die durch $\mathfrak{P}$ teilbare Primzahl ist und $(e_1^{(0)}, p) = 1$, $(e_2^{(0)}, p) = 1$ sind. Ferner bezeichnen wir mit f, $e = e^{(0)}p^m$ resp. den Relativgrad, den Exponenten von $\mathfrak{P}$ nach K_2, wobei $(e^{(0)}, p)=1$ gesetzt ist.

Es fragt sich nun, wie der Relativgrad f bzw. der Exponent e durch f_1 und f_2 bzw. durch e_1 und e_2 bestimmt wird. Als eine Antwort für diese Frage hat HERBRAND in einer Arbeit[2] folgenden Satz angegeben:

$$(A)\quad \begin{cases} \textit{1.)}\ \ e_1 \ \textit{ist durch}\ e\ \textit{teilbar}. \\ \textit{2.)}\ \ f = \dfrac{f_1}{(f_1, f_2)}. \\ \textit{3.)}\ \ e^{(0)} = \dfrac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})}. \end{cases}$$

Aber leider steckt im Beweis dieses eleganten Satzes ein Fehler. Deshalb führt der obige Satz, wie gleich gezeigt wird, zu Widerspruch.

(1) D.h. $\mathfrak{p}_1$ bzw. $\mathfrak{p}_2$ ist genau durch $\mathfrak{P}_1^{e_1}$ bzw. $\mathfrak{P}_2^{e_2}$ teilbar.

(2) HERBRAND, Théorie arithmétique des corps de nombres de degré infini, Math. Ann., Bd. 106 (1932), S. 489, Lemme 2. Ich bezeichne diese Arbeit mit H.I.

Wir betrachten nämlich über dem rationalen Zahlkörper R zwei kubische Zahlkörper $K_1 = R(\sqrt[3]{2})$ und $K_2 = R(\rho\sqrt[3]{2})$, wobei ρ eine primitive 3. Einheitswurzel bedeutet. Bildet man dann das Kompositum

$$K_1K_2 = R(\rho, \sqrt[3]{2}),$$

so enthält K_1K_2 den Körper $R(\rho)$. Da 2 eine primitive Wurzel modulo 3 ist, so ist das Hauptideal (2) im Körper $R(\rho)$ ein Primideal und (2) besitzt den Grad 2 nach R.[1]

Betrachtet man nun über $R(\rho)$ den Körper $K_1K_2 = R(\rho, \sqrt[3]{2})$ und bezeichnet durch $\mathfrak{P}$ ein in (2) aufgehendes Primideal aus K_1K_2, so ist in K_1K_2

$$(2) = \mathfrak{P}^3. \text{[2]}$$

Also besitzt das Primideal $\mathfrak{P}$ aus K_1K_2 den Grad 2 und den Exponenten 3 nach R, und das Hauptideal (2) besitzt in K_1K_2 nur einen einzigen Primteiler $\mathfrak{P}$. Nun bezeichnen wir mit $\mathfrak{P}_1$ bzw. $\mathfrak{P}_2$ das durch $\mathfrak{P}$ teilbare Primideal aus K_1 bzw. K_2. Dann besitzt in K_1 das Hauptideal (2) einen einzigen Primteiler $\mathfrak{P}_1$. Es gilt also in K_1

$$(2) = \mathfrak{P}_1^x.$$

Durch Normbildung erhält man

$$(2)^3 = (2)^{xf_1},$$

wobei f_1 den Grad von $\mathfrak{P}_1$ nach R bedeutet. Hieraus folgt ohne weiteres entweder $x = 3$ oder $f_1 = 3$. Da aber f_1 ein Teiler von 2 sein muss, so müssen unbedingt $x = 3$ und $f_1 = 1$ sein. Es gilt also in K_1

$$(2) = \mathfrak{P}_1^3.$$

Ebenso gilt in K_2

$$(2) = \mathfrak{P}_2^3.$$

(1) Siehe etwa HECKE, Theorie der algebraischen Zahlen (1923), S. 112, Satz 92.
(2) HECKE, loc. cit. S. 150, Satz 118.

Daher ist der Grad von $\mathfrak{P}_1$ bzw. $\mathfrak{P}_2$ nach R gleich 1, und der Grad von $\mathfrak{P}$ nach K_2 ist offenbar 2. Dagegen behauptet der Satz von HERBRAND, dass der Grad von $\mathfrak{P}$ nach K_2

$$\frac{1}{(1,1)}=1$$

sein soll, was aber unmöglich ist.

§ 2.

In diesem Paragraphen will ich zwecks der weiteren Untersuchung den Beweis von HERBRAND für (A) skizzieren. Wir betrachten zunächst über k den kleinsten K_1K_2 enthaltenden, galoisschen Körper N und bezeichnen mit $\mathfrak{G}$ die galoissche Gruppe von N nach k. Ferner bezeichnen wir mit $\mathfrak{P}^*$ einen Primteiler von $\mathfrak{P}$ aus N, und durch $\mathfrak{G}_Z$, $\mathfrak{G}_T$, $\mathfrak{G}_V$ resp. die Zerlegungs-, Trägheits- und Verzweigungsgruppe von $\mathfrak{P}^*$ nach k. Ist nun $\mathfrak{G}_1$ bzw. $\mathfrak{G}_2$ die K_1 bzw. K_2 zugeordnete Untergruppe von $\mathfrak{G}$, so ist $\mathfrak{G}_1 \frown \mathfrak{G}_2$[1] die K_1K_2 zugeordnete Untergruppe von $\mathfrak{G}$. Es sei

$$\mathfrak{G}_V=(\mathfrak{G}_V \frown \mathfrak{G}_1)(\mathfrak{G}_V \frown \mathfrak{G}_2)+\ldots .$$

die Zerlegung von $\mathfrak{G}_V$ nach dem Doppelmodul $(\mathfrak{G}_V \frown \mathfrak{G}_1,\ \mathfrak{G}_V \frown \mathfrak{G}_2)$. Dann ist $[\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1]$[2] nicht kleiner als die Anzahl der in $(\mathfrak{G}_V \frown \mathfrak{G}_1)\cdot(\mathfrak{G}_V \frown \mathfrak{G}_2)$ enthaltenen, voneinander verschiedenen Nebengruppen von $\mathfrak{G}_V \frown \mathfrak{G}_1$. Hieraus folgt ohne weiteres

$$[\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1] \geqq [\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2]\,.$$ [3]

Bekanntlich sind

$$[\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1]=p^{m_1} \quad \text{und} \quad [\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2]=p^{m}\,.$$

(1) $\mathfrak{G}_1 \frown \mathfrak{G}_2$ bezeichnet den Durchschnitt von $\mathfrak{G}_1$ mit $\mathfrak{G}_2$.
(2) Die eckige Klammer bezeichnet den Index der Gruppen.
(3) Siehe etwa SPEISER, Theorie der Gruppen von endlicher Ordnung (1927), S. 63, Satz 64.

Es ist also

$$m_1 \geqq m .$$

Nun betrachten wir die Faktorgruppe $\mathfrak{G}_Z/\mathfrak{G}_T$. Dann ist diese Faktorgruppe eine zyklische Gruppe. Wir bezeichnen also mit σ ein erzeugendes Element von $\mathfrak{G}_Z/\mathfrak{G}_T$, d.h. es ist

$$\mathfrak{G}_Z = \mathfrak{G}_T + \sigma\mathfrak{G}_T + \cdots\cdots + \sigma^{F-1}\mathfrak{G}_T ,$$

wobei F den Index von $\mathfrak{G}_Z$ nach $\mathfrak{G}_T$ bedeutet. Dann ist

$$\mathfrak{G}_Z/\mathfrak{G}_T = \{\sigma\}\,\mathfrak{G}_T/\mathfrak{G}_T \cong \{\sigma\} / \mathfrak{G}_T \frown \{\sigma\} \cong \{\sigma\} / \{\sigma^F\} .$$

Dabei bedeutet $\{\sigma\}$ die durch σ erzeugte Gruppe, ist also $\{\sigma\}$ eine zyklische Gruppe. Betrachtet man nun die Faktorgruppe

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\,\mathfrak{G}_T/\mathfrak{G}_T ,$$

so folgt aus der obigen Isomorphierelation $\mathfrak{G}_Z/\mathfrak{G}_T \cong \{\sigma\}/\{\sigma^F\}$

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\,\mathfrak{G}_T/\mathfrak{G}_T \cong \{\sigma^x\} / \{\sigma^F\} ,$$

wobei x ein geeigneter Teiler von F ist. Ebenso gilt für einen geeigneten Teiler y von F folgende Isomorphierelation:

$$(\mathfrak{G}_Z \frown \mathfrak{G}_2)\,\mathfrak{G}_T/\mathfrak{G}_T \cong \{\sigma^y\} / \{\sigma^F\} .$$

Also gilt noch folgende Isomorphierelation:

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\mathfrak{G}_T/\mathfrak{G}_T \frown (\mathfrak{G}_Z \frown \mathfrak{G}_2)\mathfrak{G}_T/\mathfrak{G}_T \cong \{\sigma^x\} / \{\sigma^F\} \frown \{\sigma^y\} / \{\sigma^F\}$$
$$\cong \left\{\sigma^{\frac{xy}{(x,y)}}\right\} / \{\sigma^F\} .$$

Da aber

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\mathfrak{G}_T/\mathfrak{G}_T \frown (\mathfrak{G}_Z \frown \mathfrak{G}_2)\mathfrak{G}_T/\mathfrak{G}_T \geqq (\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_T/\mathfrak{G}_T{}^{(1)}$$

---

(1) HERBRAND hat hier

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\,\mathfrak{G}_T/\mathfrak{G}_T \frown (\mathfrak{G}_Z \frown \mathfrak{G}_2)\,\mathfrak{G}_T/\mathfrak{G}_T = (\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\,\mathfrak{G}_T/\mathfrak{G}_T$$

gesetzt, was aber allgemein nicht der Fall ist.

ist, so ist

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_T/\mathfrak{G}_T \cong \left\{\sigma^{a\frac{xy}{(x,\,y)}}\right\} / \{\sigma^F\} ,$$

wo a einen passenden Teiler von F bedeutet.

Aus $(\mathfrak{G}_Z \frown \mathfrak{G}_1)\, \mathfrak{G}_T/\mathfrak{G}_T$ folgt nach dem Isomorphiesatz

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\mathfrak{G}_T/\mathfrak{G}_T \cong \mathfrak{G}_Z \frown \mathfrak{G}_1/\mathfrak{G}_Z \frown \mathfrak{G}_T \frown \mathfrak{G}_1 = \mathfrak{G}_Z \frown \mathfrak{G}_1/\mathfrak{G}_T \frown \mathfrak{G}_1$$
$$\cong \{\sigma^x\} / \{\sigma^F\} .$$

Weil aber $[\mathfrak{G}_Z \frown \mathfrak{G}_1 : \mathfrak{G}_T \frown \mathfrak{G}_1]$ der Relativgrad von $\mathfrak{P}^*$ nach K_1 ist, so folgt aus $\frac{F}{x} = [\mathfrak{G}_Z \frown \mathfrak{G}_1 : \mathfrak{G}_T \frown \mathfrak{G}_1]$, dass x der Relativgrad von $\mathfrak{P}_1$ nach k ist, d.h. $x = f_1$.

Ebenso erhält man

$$y = f_2 .$$

Ferner schliesst man aus der Relation

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_T/\mathfrak{G}_T \cong \left\{\sigma^{a\frac{xy}{(x,\,y)}}\right\} / \{\sigma^F$$

genau so wie oben, dass

$$ff_2 = a\frac{xy}{(x,\, y)}$$

ist. Hieraus folgt sofort

$$f = a\frac{f_1}{(f_1,\, f_2)} .$$

Wir wissen noch, dass $\mathfrak{G}_T/\mathfrak{G}_V$ eine zyklische Gruppe ist. Aus dieser Tatsache beweist man ebenso wie oben

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V \geqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V .$$

Hieraus folgt ohne weiteres, dass für eine passende natürliche Zahl b

$$e^{(0)} = b\frac{e_1^{(0)}}{(e_1^{(0)},\, e_2^{(0)})}$$

ist.

Aus der bisherigen Ausführung kann man leicht einsehen, dass *dann und nur dann*

$$f = \frac{f_1}{(f_1, f_2)} \qquad bzw. \quad e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})}$$

ist, wenn

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\mathfrak{G}_T \frown (\mathfrak{G}_Z \frown \mathfrak{G}_2)\mathfrak{G}_T = (\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_T$$

bzw.

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V = (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V$$

ist.

§ 3.

Es liegt nun die Frage vor, wann der Satz von HERBRAND gilt. Wir wollen also in diesem Paragraphen einige Fälle untersuchen, wo der genannte Satz von HERBRAND gilt.

Wie schon im vorigen Paragraphen gezeigt, wird das Problem auf eine rein gruppentheoretische Frage reduziert. Zuerst beweise ich unter Benutzung aller bisherigen Bezeichnungen folgenden Satz.

Satz 1. *Wenn* $p^m = p^{m_1}$ *ist, dann gilt*

1.) e_1 *ist durch* e *teilbar.*

2.) $e^{(0)} = \dfrac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})}$.

Beweis. Wir betrachten nun den Elementenkomplex

$$(\mathfrak{G}_V \frown \mathfrak{G}_1)(\mathfrak{G}_V \frown \mathfrak{G}_2)\,.\text{[1]}$$

Dann enthält dieser Elementenkomplex im ganzen

$$[\mathfrak{G}_V \frown \mathfrak{G}_1 : E][\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2]^{(2)} = p^{m_1}[\mathfrak{G}_V \frown \mathfrak{G}_1 : E]$$

---

(1) $(\mathfrak{G}_V \frown \mathfrak{G}_1)(\mathfrak{G}_V \frown \mathfrak{G}_2)$ ist ein Komplex aller verschiedenen Elemente, welche von der Form $G_V^{(1)} G_V^{(2)}$ sind, wobei $G_V^{(1)}$, $G_V^{(2)}$ resp. beliebige Elemente aus $\mathfrak{G}_V \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_2$ sind.

(2) SPEISER, loc. cit. S. 63. E bedeutet das Einselement.

verschiedene Elemente, weil $[\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2] = p^m = p^{m_1}$ ist.

Offenbar ist

$$[\mathfrak{G}_V : E] = [\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1][\mathfrak{G}_V \frown \mathfrak{G}_1 : E] = p^{m_1}[\mathfrak{G}_V \frown \mathfrak{G}_1 : E] .$$

Da aber $(\mathfrak{G}_V \frown \mathfrak{G}_1)(\mathfrak{G}_V \frown \mathfrak{G}_2)$ in $\mathfrak{G}_V$ enthalten ist, so muss nach der obigen Relation

$$\mathfrak{G}_V = (\mathfrak{G}_V \frown \mathfrak{G}_1)(\mathfrak{G}_V \frown \mathfrak{G}_2)$$

sein, d.h. jedes Element aus $\mathfrak{G}_V$ ist von der Form $H_1 H_2$, wobei H_1, H_2 resp. Elemente aus $\mathfrak{G}_V \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_2$ sind.

Wir beweisen nun

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V = (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V .$$

Nämlich ein beliebiges Element aus $(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V$ ist einerseits als ein Element aus $(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V$ von der Form

$$G_T^{(1)} H_1 H_2 ,$$

wobei $G_T^{(1)}$, H_1, H_2 resp. Elemente aus $\mathfrak{G}_T \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_2$ sind, und anderseits als ein Element aus $(\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V$ von der Form

$$G_T^{(2)} H_1' H_2' ,$$

wobei $G_T^{(2)}$, H_1', H_2' resp. Elemente aus $\mathfrak{G}_T \frown \mathfrak{G}_2$, $\mathfrak{G}_V \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_2$ sind. Also ist

$$G_T^{(1)} H_1 H_2 = G_T^{(2)} H_1' H_2' .$$

Betrachtet man hier ein Element $G_T^{(2)} H_1' (G_T^{(2)})^{-1}$, so existiert in $\mathfrak{G}_V$ ein Element $H_1'' H_2''$, so dass

$$G_T^{(2)} H_1' (G_T^{(2)})^{-1} = H_1'' H_2'' \qquad \text{d.h.} \quad G_T^{(2)} H_1' = H_1'' H_2'' G_T^{(2)}$$

wird, weil H_1' ein Element aus $\mathfrak{G}_V$ und $\mathfrak{G}_V$ ein Normalteiler von $\mathfrak{G}_T$ ist. Dabei bedeuten H_1'', H_2'' resp. Elemente aus $\mathfrak{G}_V \frown \mathfrak{G}_1$, $\mathfrak{G}_V \frown \mathfrak{G}_2$. Aus $G_T^{(1)} H_1 H_2 = G_T^{(2)} H_1' H_2' = H_1'' H_2'' G_T^{(2)} H_2'$ folgt also

$$(H_1'')^{-1} G_T^{(1)} H_1 = H_2'' G_T^{(2)} H_2' H_2^{-1} \lessdot \mathfrak{G}_2 \,.$$

Da aber H_1, H_1'' Elemente aus $\mathfrak{G}_V \frown \mathfrak{G}_1$, um so mehr Elemente aus $\mathfrak{G}_T \frown \mathfrak{G}_1$ sind, so ist $(H_1'')^{-1} G_T^{(1)} H_1$ einerseits ein Element aus $\mathfrak{G}_T \frown \mathfrak{G}_1$, und anderseits ein Element aus $\mathfrak{G}_2$. Also gehört $(H_1'')^{-1} G_T^{(1)} H_1$ zu $\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2$, d.h. $G_T^{(1)}$ ist ein Element aus $H_1''(\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2) H_1^{-1}$. Da aber H_1'', H_1^{-1} Elemente aus $\mathfrak{G}_V$ sind und $\mathfrak{G}_V$ ein Normalteiler von $\mathfrak{G}_T$ ist, so ist

$$H_1''(\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2) H_1^{-1} \leqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V \,.$$

Also ist

$$G_T^{(1)} \leqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V \,.$$

Hieraus folgt ohne weiteres

$$\mathfrak{G}_T^{(1)} H_1 H_2 \leqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V \,.$$

Damit ist gezeigt, dass

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V \leqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V$$

ist. Da aber anderseits

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_2)\mathfrak{G}_V \geqq (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V$$

ist, so ist offenbar

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)\mathfrak{G}_V \frown (\mathfrak{G}_T \frown \mathfrak{G}_V)\mathfrak{G}_V = (\mathfrak{G}_T \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_V \,.$$

Daher folgt aus § 2

$$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})} \,.$$

$e^{(0)}$ ist also ein Teiler von $e_1^{(0)}$. Weil aber $e = e^{(0)} p^m = e^{(0)} p^{m_1}$ ist, so ist $e_1 = e_1^{(0)} p^{m_1}$ durch e teilbar. Damit ist der Beweis beendet.

Zusatz. Ist mindestens eines von p^{m_1} und p^{m_2} gleich 1, so gilt die Behauptung von Satz 1.

Beweis. Es ist

$$[\mathfrak{G}_V : E] = [\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1][\mathfrak{G}_V \frown \mathfrak{G}_1 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2][\mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2 : E]$$
$$= [\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_2][\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2][\mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2 : E] .$$

Ist $p^{m_1} = 1$, so muss nach $m_1 \geqq m \geqq 0$ $p^m = 1$ sein, d.h. $p^m = p^{m_1}$. Wenn aber $p^{m_2} = 1$ ist, dann folgt aus $[\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_2] = p^{m_2} = 1$ und

$$[\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2] = p^m \leqq p^{m_1} ,$$

$$p^m = p^{m_1} ,$$

weil hierbei $[\mathfrak{G}_V \frown \mathfrak{G}_2 : \mathfrak{G}_V \frown \mathfrak{G}_1 \frown \mathfrak{G}_2]$ durch $[\mathfrak{G}_V : \mathfrak{G}_V \frown \mathfrak{G}_1] = p^{m_1}$ teilbar sein muss. Also ist jedenfalls

$$p^m = p^{m_1} .$$

Hieraus folgt die Behauptung sofort aus Satz 1.

Wir beweisen nun

Satz 2. *Ist* $e = e_1$, *so ist*

1.) $$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})} .$$

2.) $$f = \frac{f_1}{(f_1, f_2)} .$$

Beweis. Da $e = e^{(0)} p^m$ und $e_1 = e_1^{(0)} p^{m_1}$ sind, so muss nach Voraussetzung

$$p^m = p^{m_1}$$

sein, weil $e^{(0)}$, $e_1^{(0)}$ beide zu p prim sind. Somit folgt *1.)* aus Satz 1.

Um *2.)* zu beweisen, betrachten wir den Elementenkomplex

$$(\mathfrak{G}_T \frown \mathfrak{G}_1)(\mathfrak{G}_T \frown \mathfrak{G}_2) .$$

Mit derselben Überlegung wie im Beweis von Satz 1 kann man auch beweisen, dass $(\mathfrak{G}_T \frown \mathfrak{G}_1)(\mathfrak{G}_T \frown \mathfrak{G}_2) = \mathfrak{G}_T$ ist.(1) Ferner kann man auch wie im Beweis für Satz 1 schliessen, dass

$$(\mathfrak{G}_Z \frown \mathfrak{G}_1)\mathfrak{G}_T \frown (\mathfrak{G}_Z \frown \mathfrak{G}_2)\mathfrak{G}_T = (\mathfrak{G}_Z \frown \mathfrak{G}_1 \frown \mathfrak{G}_2)\mathfrak{G}_T$$

ist. Hieraus folgt nach § 2 sofort, dass

$$f = \frac{f_1}{(f_1, f_2)}$$

ist, w.z.b.w.

Aus Satz 2 folgt nun

$$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})},$$

falls $e = e_1$ ist. Dies bedeutet aber, dass

$$(e_1^{(0)}, e_2^{(0)}) = 1$$

ist. Denn sonst würde $e^{(0)}$ kleiner als $e_1^{(0)}$, was aber unmöglich wäre, weil $e = p^m e^{(0)} = p^{m_1} e^{(0)} = p^{m_1} e_1^{(0)} = e_1$ sein müsste.

Sind umgekehrt $(e_1^{(0)}, e_2^{(0)}) = 1$ und $p^m = p^{m_1}$, so ist

$$e_1 = e .$$

Nämlich nach Satz 1 ist hierbei

$$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})} .$$

Weil aber $(e_1^{(0)}, e_2^{(0)}) = 1$ ist, so ist $e^{(0)} = e_1^{(0)}$. Hieraus folgt ohne weiteres

$$e = p^m e^{(0)} = p^{m_1} e_1^{(0)} = e_1 .$$

(1) Man soll bloss im Beweis von Satz 1 $\mathfrak{G}_V$ durch $\mathfrak{G}_T$ und p^m, p^{m_1} resp. durch e, e_1 ersetzen.

Es gilt also folgender

Satz 3. *Sind* $p^m = p^{m_1}$ *und* $(e_1^{(0)}, e_2^{(0)}) = 1$, *so gilt:*

1.) $$e = e_1 .$$

2.) $$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})} = e_1^{(0)} .$$

3.) $$f = \frac{f_1}{(f_1, f_2)} .$$

Beweis. Nach dem oben Gesagten folgt aus Voraussetzung

$$e = e_1 .$$

Aus $e = e_1$ und Satz 2 folgen die zwei letzten Behauptungen sofort.

Zusatz. Ist $(e_1, e_2) = 1$, so gilt die Behauptung von Satz 3.

Beweis. In diesem Fall ist eines von p^{m_1} und p^{m_2} gleich 1. Ist zunächst $p^{m_1} = 1$, so muss nach $0 \leqq m \leqq m_1$ auch $p^m = 1 = p^{m_1}$ sein. Wenn aber $p^{m_2} = 1$ ist, dann muss $p^{m_2+m} = p^m$ durch p^{m_1} teilbar sein. Hieraus folgt ohne weiteres $p^{m_1} = p^m$, weil $m \leqq m_1$ ist. Auf jeden Fall ist also $p^m = p^{m_1}$.

Da aber $(e_1, e_2) = 1$ ist, so muss natürlich

$$(e_1^{(0)}, e_2^{(0)}) = 1$$

sein. Aus Satz 3 folgt daher die Behauptung des Satzes.

Bemerkung. Im Zusatz von Satz 3 sind $(e_1, e_2) = 1 = (e_1^{(0)}, e_2^{(0)})$ und $p^m = p^{m_1}$. Also folgt aus

$$e^{(0)} = \frac{e_1^{(0)}}{(e_1^{(0)}, e_2^{(0)})}$$

$$e = p^m e^{(0)} = \frac{p^{m_1} e_1^{(0)}}{(e_1, e_2)} = \frac{e_1}{(e_1, e_2)} .$$

Als Anwendung von Satz 3 kann man einige bekannte Sätze herleiten.

1.) $e_1 = 1$ *oder* $e_2 = 1$.

In diesem Fall ist natürlich

$$(e_1, e_2) = 1 .$$

Hieraus folgt nach Zusatz von Satz 3 die Relation (A).[1]

2.) K_1, K_2 *sind beide galoissch über* k, *und* $([K_1 : K_1 \frown K_2], [K_2 : K_1 \frown K_2]) = 1$.[2]

Bezeichnet man nun durch $\bar{f}$, $\bar{e}$ resp. den Relativgrad, den Exponenten des durch $\mathfrak{P}^*$ teilbaren Primideals aus $K_1 \frown K_2$, so sind $\frac{f_1}{\bar{f}}$, $\frac{e_1}{\bar{e}_1}$ resp. der Relativgrad, der Exponent von $\mathfrak{P}_1$ nach $K_1 \frown K_2$ und $\frac{f_2}{\bar{f}}$, $\frac{e_2}{\bar{e}}$ resp. der Relativgrad, der Exponent von $\mathfrak{P}_2$ nach $K_1 \frown K_2$. Dann ist bekanntlich $\frac{e_1}{\bar{e}}$ bzw. $\frac{e_2}{\bar{e}}$ ein Teiler von $[K_1 : K_1 \frown K_2]$ bzw. $[K_2 : K_1 \frown K_2]$, d.h. $\frac{e_1}{\bar{e}}$, $\frac{e_2}{\bar{e}}$ sind zueinander prim.

Nach Zusatz von Satz 3 ist

$$f = \frac{\frac{f_1}{\bar{f}}}{\left(\frac{f_1}{\bar{f}}, \frac{f_2}{\bar{f}}\right)} = \frac{f_1}{(f_1, f_2)} .$$

Ebenso folgt aus Bemerkung zu Zusatz von Satz 3

$$e = \frac{e_1}{(e_1, e_2)} .$$

Bemerkung. Wir bemerken hier, dass Satz 1, 2, 3, und ihre Zusätze alle auf den Fall übertragen werden können, wo k ein unend-

(1) Im Fall, wo eines von K_1, K_2 über k galoissch ist, ist dieser Satz von HERBRAND bewiesen. Siehe HERBRAND, Sur la théorie des groupes de décomposition, d'inertie et de ramification, Journ. d. Liouville, XI. Série, Tome 10, Théorème 5. Im Fall, wo K_1, K_2 beide über k galoissch und $e_1 = 1 = e_2$ sind, ist ein Teil dieses Satzes von BAUER bewiesen. Siehe BAUER, Über relativ galoissche Zahlkörper, Math. Ann., Bd. 83 (1921).

(2) BAUER. loc. cit.

licher algebraischer Zahlkörper und K_1, K_2 endliche Erweiterungen von k sind.

§ 4.

Im vorigen Paragraphen haben wir gezeigt, dass der Satz von HERBRAND unter gewissen Beschränkungen beweisbar ist. Deshalb wollen wir in diesem Paragraphen die Sätze, welche HERBRAND unter keinen Einschränkungen mit Hilfe seines Lemmas 2 bewiesen hat, auf andere Weise beweisen.

Wir betrachten einen algebraischen Zahlkörper unendlichen Grades k, welcher als der Vereinigungskörper von algebraischen Zahlkörpern endlichen Grades $k_1 < k_2 < \cdots < k_j < \cdots$ definiert ist, und einen algebraischen Zahlkörper K von endlichem Grade über k. Dann können wir offenbar eine algebraische Zahl ϑ aus K und einen passenden Index I finden, derart dass für jeden Index $j \geqq I$

$$[K_j = k_j(\theta) : k_j] = [K : k]$$

ist. Wir greifen nun aus K ein Primideal $\mathfrak{P}$ und aus k das durch $\mathfrak{P}$ teilbare Primideal $\mathfrak{p}$ heraus. Sind $\mathfrak{P}_j$, $\mathfrak{p}_j$ resp. die durch $\mathfrak{P}$ teilbaren Primideale aus K_j, k_j $(j \geqq I)$, so kann man wie HERBRAND annehmen, dass der Relativgrad(1) f, der Exponent(2) e, der reduzierte Exponent(3) $e^{(0)}$ von $\mathfrak{P}$ nach k resp. dem Relativgrad f_j, dem Exponenten e_j, dem reduzierten Exponenten(4) $e_j^{(0)}$ von $\mathfrak{P}_j$ nach k_j gleich sind.

Als théorème 18(5) hat HERBRAND mit Hilfe seines Lemmas 2 folgenden Satz bewiesen:

Der unendliche Teil(6) des absoluten Grades(7) von $\mathfrak{p}$ ist prim zu f.

Beweis. Nach der Wahl des Index I sind der Relativgrad f_j, der Exponent e_j von $\mathfrak{P}_j$ aus K_j nach k_j resp. f, e, falls $j \geqq I$ ist. Es sind also für $\mathfrak{P}_j$, $\mathfrak{P}_{j+1}$

$$f_j = f = f_{j+1} \qquad \text{und} \qquad e_j = e = e_{j+1}\,.$$

(1), (2) H. I. S. 484.
(3), (5) H. I. S. 492.
(4), (7) H. I. S. 478.
(6) H. I. S. 477. Der unendliche Teil bedeutet "partie infinie".

Also folgt aus Satz 2

$$f = f_{j+1} = \frac{f_j}{(f_j, \varphi_j)} = \frac{f}{(f, \varphi_j)},$$

wobei φ_j den Relativgrad von $\mathfrak{p}_{j+1}$ aus k_{j+1} nach k_j bedeutet. Aus der obigen Formel folgt sofort, dass

$$(\varphi_j, f) = 1$$

ist. Dies gilt aber für alle f_j, falls $j \geqq I$ ist. Damit ist es bewiesen, dass f zum unendlichen Teil des absoluten Grades von $\mathfrak{p}$ prim ist. Also ist der Beweis fertig.

Im obigen Beweis haben wir die Tatsache, dass für $j \geqq I$

$$e_j = e = e_{j+1}$$

ist, benutzt. Nach Satz 2 folgt aus $e_j = e_{j+1}$

$$e_{j+1}^{(0)} = \frac{e_j^{(0)}}{(e_j^{(0)}, \varepsilon_j^{(0)})},$$

wobei $\varepsilon_j^{(0)}$ den reduzierten Exponenten von $\mathfrak{p}_{j+1}$ nach k_j bedeutet. Da aber nach der Wahl des Index I

$$e_j^{(0)} = e^{(0)} = e_{j+1}^{(0)}$$

ist, so muss offenbar

$$(e_j^{(0)}, \varepsilon_j^{(0)}) = 1$$

sein, falls $j \geqq I$ ist. Damit ist folgender Satz, welcher HERBRAND als théorème 20 angegeben hat, bewiesen:

Der unendliche Teil des absoluten reduzierten Exponenten[1] *von* $\mathfrak{p}$ *ist prim zu* $e^{(0)}$.

---

(1) H. I. S. 493.