Ueber die Zerlegung der Ideale eines Zahlenkörpers in Primideale.

Von

David Hilbert in Königsberg i. Pr.

Die Grundlage für die Theorie der algebraischen Zahlen bildet der Satz, dass jedes Ideal eines Zahlenkörpers auf eine und nur auf eine Weise in Primideale zerlegt werden kann. Dieser Satz ist zuerst von R. Dedekind*) allgemein ausgesprochen und bewiesen worden. Einen zweiten wesentlich hiervon verschiedenen Beweis gab L. Kronecker**). Die vorliegende Abhandlung enthält einen neuen Beweis***) dieses Satzes.

Es sei ein beliebiger Zahlenkörper vom n^{ten} Grade vorgelegt; dann stelle ich folgende Definitionen auf:

Ein unendliches System von ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots$ des Körpers, welches die Eigenschaft besitzt, dass eine jede lineare Combination $\varkappa_1\alpha_1 + \varkappa_2\alpha_2 + \cdots$ derselben wiederum dem Systeme angehört, heisst ein *Ideal* $\mathfrak{j}$ des Körpers; dabei bedeuten $\varkappa_1, \varkappa_2, \ldots$ beliebige ganze algebraische Zahlen des Körpers. Sind $\alpha_1, \ldots, \alpha_m$ solche m Zahlen des Ideals $\mathfrak{j}$, durch deren lineare Combination unter Benutzung ganzer algebraischer Coefficienten alle Zahlen des Ideals erhalten werden können, so setze ich kurz

$$\mathfrak{j} = (\alpha_1, \ldots, \alpha_m).$$

Wie leicht gezeigt werden kann, giebt es im Ideal $\mathfrak{j}$ stets n Zahlen $\alpha_1^0, \ldots, \alpha_n^0$ von der Art, dass eine jede Zahl des Ideals gleich einer linearen Combination derselben von der Gestalt $k_1\alpha_1^0 + \cdots + k_n\alpha_n^0$ ist, wo $k_1, \ldots, k_n$ ganze rationale Zahlen sind. Die Zahlen $\alpha_1^0, \ldots, \alpha_n^0$ heissen eine *Basis* des Ideals $\mathfrak{j}$.

*) Vorlesungen über Zahlentheorie von Dirichlet. Supplement XI.

**) Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Crelle, Bd. 92.

***) Den Gedankengang dieses Beweises habe ich in der Versammlung der deutschen Mathematiker-Vereinigung München 1893 vorgetragen.

Ein Ideal, welches alle und nur die Zahlen von der Gestalt $\varkappa\eta$ enthält, wo $\varkappa$ jede beliebige ganze Zahl des Körpers darstellt, heisst ein *Hauptideal*, und wird mit (η) oder auch kurz mit η bezeichnet.

Eine jede Zahl α des Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ heisst *congruent* 0 nach dem Ideal $\mathfrak{j}$ oder in Zeichen:

$$\alpha \equiv 0 \quad (\mathfrak{j}).$$

Wenn alle Zahlen eines Ideals $\mathfrak{k}$ congruent 0 nach $\mathfrak{j}$ sind, so heisst das Ideal $\mathfrak{k}$ *congruent* 0 nach $\mathfrak{j}$ oder in Zeichen

$$\mathfrak{k} \equiv 0 \quad (\mathfrak{j}).$$

Offenbar ist jedes Ideal $\mathfrak{j}$ congruent 0 nach dem Ideal 1 und nach dem Ideal $\mathfrak{j}$ selbst.

Ein von 1 verschiedenes Ideal $\mathfrak{p}$, welches nach keinem anderen Ideal ausser nach 1 und nach sich selbst $\equiv 0$ ist, heisst ein *Primideal*.

Wenn man jede Zahl eines Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ mit jeder Zahl eines zweiten Ideals $\mathfrak{k} = (\beta_1, \ldots, \beta_l)$ multiplicirt und die so erhaltenen Zahlen linear mittelst beliebiger ganzer algebraischer Coefficienten combinirt, so wird das so entstehende neue Ideal das *Product* jener beiden Ideale genannt d. h. in Zeichen

$$\mathfrak{j}\mathfrak{k} = (\alpha_1\beta_1, \ldots, \alpha_m\beta_1, \ldots, \alpha_1\beta_l, \ldots, \alpha_m\beta_l).$$

Ein Ideal $\mathfrak{r}$ heisst durch das Ideal $\mathfrak{j}$ *theilbar*, wenn ein Ideal $\mathfrak{k}$ existirt, derart, dass $\mathfrak{r} = \mathfrak{j}\mathfrak{k}$ ist. Ist $\mathfrak{r}$ durch $\mathfrak{j}$ theilbar, so ist $\mathfrak{r} \equiv 0$ nach dem Ideal $\mathfrak{j}$.

1. Ein Ideal $\mathfrak{j}$ kann nur nach einer endlichen Anzahl von Idealen $\equiv 0$ sein.

Zum Beweise bilde man die Norm a einer beliebigen Zahl α des Ideals $\mathfrak{j}$; ist dann etwa $\mathfrak{k}$ ein Ideal, nach welchem $\mathfrak{j} \equiv 0$ ist, so muss offenbar auch $a \equiv 0$ nach $\mathfrak{k}$ sein. Die n Basiszahlen von $\mathfrak{k}$ seien von der Gestalt

$$\begin{aligned} &k_{11}\,\omega_1 + k_{12}\,\omega_2 + \cdots + k_{1n}\omega_n, \\ &\cdots\cdots\cdots\cdots\cdots \\ &k_{n1}\,\omega_1 + k_{n2}\omega_2 + \cdots + k_{nn}\omega_n, \end{aligned}$$

wo $\omega_1, \ldots, \omega_n$ eine Basis der ganzen Zahlen des Körpers und wo $k_{11}, k_{12}, \ldots, k_{nn}$ ganze rationale Zahlen sind. Bedeuten $k'_{11}, k'_{12}, \ldots, k'_{nn}$ bezüglich die kleinsten positiven Reste der Zahlen, $k_{11}, k_{12}, \ldots, k_{nn}$ nach dem Modul a, so wird

$$\begin{aligned} \mathfrak{k} &= (k_{11}\omega_1 + \cdots + k_{1n}\omega_n, \cdots, k_{n1}\omega_1 + \cdots + k_{nn}\omega_n) \\ &= (k'_{11}\omega_1 + \cdots + k'_{1n}\omega_n, \cdots, k'_{n1}\omega_1 + \cdots + k'_{nn}\omega_n,\ a) \end{aligned}$$

und diese Darstellung des Ideals $\mathfrak{k}$ lässt unmittelbar die Richtigkeit der Behauptung erkennen.

2. Ein jedes von 1 verschiedene Ideal $\mathfrak{j}$ ist $\equiv 0$ nach mindestens einem Primideal $\mathfrak{p}$.

Denn falls $\mathfrak{j}$ nicht schon selbst ein Primideal ist, so giebt es ein von $\mathfrak{j}$ und von 1 verschiedenes Ideal $\mathfrak{j}_1$ nach welchem $\mathfrak{j} \equiv 0$ ist. Es sei ferner $\mathfrak{j}_2$ ein von 1 und von $\mathfrak{j}_1$ verschiedenes Ideal, nach welchem $\mathfrak{j}_1 \equiv 0$ ist; $\mathfrak{j}_3$ ein von $\mathfrak{j}_2$ und 1 verschiedenes Ideal, nach welchem $\mathfrak{j}_2 \equiv 0$ ist u. s. f. In der Reihe $\mathfrak{j}, \mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \ldots$ ist jedes Ideal $\equiv 0$ nach allen folgenden Idealen. Ueberdies sind sämmtliche Ideale dieser Reihe unter einander verschieden. Denn die Annahme $\mathfrak{j}_r = \mathfrak{j}_s$, $r > s$ hätte $\mathfrak{j}_r \equiv 0$ nach $\mathfrak{j}_s$ und mithin auch nach $\mathfrak{j}_{r-1}$ zur Folge; da jedoch auch $\mathfrak{j}_{r-1} \equiv 0$ nach $\mathfrak{j}_r$ ist, so wäre nothwendig $\mathfrak{j}_{r-1} = \mathfrak{j}_r$ und dieser Umstand widerspricht der Voraussetzung. Nach Satz 1 bricht die Reihe dieser Ideale $\mathfrak{j}, \mathfrak{j}_1, \mathfrak{j}_2, \mathfrak{j}_3, \ldots$ ab. Das letzte Ideal ist ein Primideal.

Der eben bewiesene Satz kann auch, wie folgt ausgesprochen werden.

Wenn ein Ideal nach keinem Primideal $\equiv 0$ ist, so ist es das Ideal 1.

3. Wenn das Product $\mathfrak{j}\mathfrak{k}$ zweier Ideale $\mathfrak{j}$ und $\mathfrak{k} \equiv 0$ ist nach einem Primideal $\mathfrak{p}$, so ist entweder $\mathfrak{j} \equiv 0$ oder $\mathfrak{k} \equiv 0$ nach dem Primideal $\mathfrak{p}$.

Ist etwa $\mathfrak{j}$ nicht $\equiv 0$ nach $\mathfrak{p}$, so bestimme man eine Zahl α des Ideals $\mathfrak{j}$, welche nicht $\equiv 0$ nach $\mathfrak{p}$ ist. Ferner bilde man aus $\mathfrak{p} = (\pi_1, \ldots, \pi_r)$ durch Hinzufügung der Zahl α das Ideal $(\pi_1, \ldots, \pi_r, \alpha)$. Dieses Ideal ist offenbar weder nach $\mathfrak{p}$ noch nach irgend einem anderen Primideal $\equiv 0$ und folglich nach Satz 2 gleich dem Ideal 1, d. h.

$$1 = \varkappa\alpha + \varkappa_1\pi_1 + \cdots + \varkappa_r\pi_r,$$

wo $\varkappa, \varkappa_1, \ldots, \varkappa_r$ geeignet gewählte ganze algebraische Zahlen des Körpers sind. Die erhaltene Gleichung lautet als Congruenz geschrieben: $1 \equiv \varkappa\alpha$ nach dem Primideal $\mathfrak{p}$. Bezeichnet nun β irgend eine Zahl des Ideals $\mathfrak{k}$, so ist nach Voraussetzung $\alpha\beta \equiv 0$ nach $\mathfrak{p}$. Und hieraus folgt nach Multiplication mit $\varkappa$ die Congruenz $\beta \equiv 0$ nach dem Primideal $\mathfrak{p}$.

4. Wenn ein Ideal $\mathfrak{j} \equiv 0$ nach einem Hauptideal (η) ist, so ist $\mathfrak{j}$ durch (η) theilbar. Aus $\eta\mathfrak{j} = \eta\mathfrak{k}$ folgt nothwendig $\mathfrak{j} = \mathfrak{k}$.

In der That, da alle Zahlen des Ideals $\mathfrak{j} = (\alpha_1, \ldots, \alpha_m)$ durch die Zahl η theilbar sind, so kann man $\alpha_1 = \eta\beta_1, \ldots, \alpha_m = \eta\beta_m$ setzen und hat dann $\mathfrak{j} = (\eta)(\beta_1, \ldots, \beta_m)$. Ist ferner $\eta\mathfrak{j} \equiv 0$ nach $\eta\mathfrak{k}$, so folgt nach Division durch die Zahl η, dass $\mathfrak{j} \equiv 0$ nach $\mathfrak{k}$ ist. Da wegen $\eta\mathfrak{k} \equiv 0$ nach $\eta\mathfrak{j}$ in gleicher Weise auch $\mathfrak{k} \equiv 0$ nach $\mathfrak{j}$ ist, so folgt nothwendig $\mathfrak{j} = \mathfrak{k}$.

5. In einem jeden Primideal $\mathfrak{p}$ giebt es stets eine rationale Primzahl p von der Art, dass eine jede andere ganze rationale Zahl des Ideals $\mathfrak{p}$ diese Primzahl p als Factor enthält.

Zum Beweise nehme man die Norm a einer Zahl von $\mathfrak{p}$ und zerlege a in seine rationalen Primfactoren. Fasst man diese als Hauptideale auf, so ist nach Satz 3 einer derselben etwa $p \equiv 0$ nach dem Primideal $\mathfrak{p}$. Gäbe es nun in $\mathfrak{p}$ noch eine ganze rationale Zahl b, welche nicht durch p theilbar wäre, so bestimme man zwei ganze rationale Zahlen r und s derart, dass $1 = rp + sb$ ist; hieraus würde $1 \equiv 0$ nach $\mathfrak{p}$ folgen, was nicht möglich ist.

Nunmehr nehmen wir zunächst an, dass der vorgelegte Zahlenkörper ein Galois'scher*) Körper sei; dann wird aus jedem Ideal des Körpers jedenfalls wieder ein Ideal des nämlichen Körpers entstehen, wenn wir in jenem Ideal statt einer jeden Zahl eine conjugirte Zahl einsetzen. Sind insbesondere alle aus einem vorgelegten Ideal $\mathfrak{a}$ auf diese Weise entstehenden $n-1$ conjugirten Ideale mit dem vorgelegten Ideal $\mathfrak{a}$ identisch, so nenne ich das Ideal $\mathfrak{a}$ ein *ambiges* Ideal. Dieser Begriff des ambigen Ideals ist ein wesentliches Hilfsmittel meines Beweises. Von einem ambigen Ideal gilt der Satz:

I. *Wenn ein ambiges Ideal* $\mathfrak{a} \equiv 0$ *nach einem Primideal* $\mathfrak{p}$ *ist, so sind alle Zahlen von* $\mathfrak{a}$ *durch* $p^{\frac{1}{n}}$ *theilbar, wo* p *die zu* $\mathfrak{p}$ *gehörige Primzahl bedeutet.*

In der That, wenn α eine Zahl des Ideals $\mathfrak{a}$ ist, so gehören auch die zu α conjugirten Zahlen dem Ideal $\mathfrak{a}$ an; dieselben sind folglich sämmtlich $\equiv 0$ nach dem Primideal $\mathfrak{p}$. Nun sei

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0$$

die Gleichung n^{ten} Grades mit ganzen rationalen Coefficienten $a_1, a_2, \ldots, a_n$ welcher die Zahl α genügt. Diese Coefficienten sind als homogene Functionen der Wurzeln der Gleichung ebenfalls $\equiv 0$ nach dem Primideal $\mathfrak{p}$ und mithin nach Satz 5 durch p theilbar. Die Zahl $\beta = \frac{\alpha}{p^{\frac{1}{n}}}$ genügt der Gleichung

$$\beta^n + \frac{a_1}{p}p^{\frac{n-1}{n}}\beta^{n-1} + \frac{a_2}{p}p^{\frac{n-2}{n}}\beta^{n-2} + \cdots + \frac{a_n}{p} = 0$$

und da die Coefficienten dieser Gleichung sämmtlich ganze algebraische Zahlen sind, so ist auch β eine ganze algebraische Zahl.

---

*) Auch Kronecker beweist den Satz von der Zerlegung in Primideale zuerst für einen Galois'schen Körper; doch ist es bemerkenswerth, dass für die Kronecker'sche Schlussweise dieser Gedanke keineswegs wesentlich ist. Vielmehr lässt sich das Kronecker'sche Beweisverfahren durch eine geringfügige Abänderung in der Reihenfolge der Schlüsse unmittelbar auf beliebige Körper anwenden. Der so abgeänderte Kronecker'sche Beweis kommt somit lediglich mit dem Hilfsmittel der unbestimmten Coefficienten aus.

Ferner lässt sich für ein ambiges Ideal leicht die Richtigkeit des folgenden Satzes erkennen:

II. *Wenn ein ambiges Ideal* $\mathfrak{a} \equiv 0$ *nach einem Primideal* $\mathfrak{p}$ *ist, so giebt es immer eine rationale Zahl* r *von der Art, dass die Zahlen des Ideals* $\mathfrak{a}$ *durch* p^r, *aber nicht sämmtlich durch eine höhere ganze oder gebrochene Potenz von* p *theilbar sind.*

Zum Beweise wähle man eine beliebige Zahl α des Ideals $\mathfrak{a}$; dieselbe genüge der Gleichung n^{ten} Grades

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_n = 0,$$

wo allgemein a_i eine ganze rationale Zahl bedeutet, welche durch die ganze Potenz p^{g_i}, aber durch keine höhere Potenz von p theilbar ist. Die kleinste der Zahlen $\frac{g_1}{1}, \frac{g_2}{2}, \cdots, \frac{g_n}{n}$ werde r_α genannt. In allen anderen Zahlen $\alpha', \alpha'', \ldots$, des Ideals $\mathfrak{a}$ denke man sich in gleicher Weise die zugehörigen rationalen Zahlen $r_{\alpha'}, r_{\alpha''}, \ldots$ bestimmt. Da die Nenner dieser rationalen Zahlen die Zahl n nicht übersteigen, so giebt es unter ihnen nothwendig eine kleinste Zahl; ist etwa r_α diese kleinste Zahl, dann erfüllt die Zahl $r = r_\alpha$ die Bedingungen des Satzes. Denn erstens sind offenbar sämmtliche Zahlen des Ideals $\mathfrak{a}$ durch p^{r_α} theilbar. Zweitens nehmen wir an, es wären sämmtliche Zahlen des Ideals $\mathfrak{a}$ durch p^R theilbar, wo R eine rationale Zahl bedeutet; es müssten dann auch die Zahl α und die zu α conjugirten Zahlen durch p^R theilbar sein, und dann wären die Coefficienten $a_1, a_2, \ldots, a_n$ der obigen Gleichung bezüglich durch $p^R, p^{2R}, \ldots, p^{nR}$ theilbar. Hieraus folgt allgemein $iR \leqq g_i$ oder $R \leqq \frac{g_i}{i}$, und da r_α selbst eine der Zahlen $\frac{g_i}{i}$ ist, so ergiebt sich $R \leqq r_\alpha$; d. h. die Zahlen des Ideals $\mathfrak{a}$ sind nicht sämmtlich durch eine höhere als die r_α^{te} Potenz von p theilbar.

Wir beweisen nun für den Galois'schen Körper der Reihe nach die folgenden Sätze:

III. *Zu jedem vorgelegten Primideal* $\mathfrak{p}$ *lässt sich stets ein Ideal* $\mathfrak{k}$ *so bestimmen, dass das Product* $\mathfrak{p}\mathfrak{k}$ *ein Hauptideal ist.*

Zum Beweise bilde man die $n-1$ zu $\mathfrak{p}$ conjugirten Ideale $\mathfrak{p}', \ldots, \mathfrak{p}^{(n-1)}$. Wie man durch Uebergang zu den conjugirten Körpern leicht einsieht, sind diese Ideale sämmtlich ebenfalls Primideale und allen gehört die nämliche Primzahl p zu. Das Product $\mathfrak{a} = \mathfrak{p}\mathfrak{p}' \ldots \mathfrak{p}^{(n-1)}$ ist offenbar ein ambiges Ideal*). Nach Satz II giebt es eine rationale

*) Bezeichnet man mit $\mathfrak{p}, \mathfrak{p}', \ldots, \mathfrak{p}^{(\nu-1)}$ die ν von einander verschiedenen unter den n conjugirten Idealen, so ist auch bereits das Product dieser ν Ideale ein ambiges Ideal und daher gemäss der nachfolgenden Beweisführung gleich einer gebrochenen Potenz von p.

Zahl $r = \frac{t}{u}$, wo t und u ganze Zahlen sind, von der Beschaffenheit, dass die Zahlen von $\mathfrak{a}$ durch p^r, aber durch keine höhere Potenz von p theilbar sind. Das Ideal $\mathfrak{a}^u$ wird folglich durch p^t theilbar und der Quotient $\mathfrak{b} = \frac{\mathfrak{a}^u}{p^t}$ ist offenbar wieder ein ambiges Ideal. Wir nehmen nun an, es sei $\mathfrak{q}$ ein Primideal, nach welchem $\mathfrak{b} \equiv 0$ ist. Da dann auch $\mathfrak{a}^u \equiv 0$ nach $\mathfrak{q}$ ist, so müsste nach Satz 3 entweder $\mathfrak{p} \equiv 0$ oder $\mathfrak{p}' \equiv 0, \ldots,$ oder $\mathfrak{p}^{(n-1)} \equiv 0$ nach $\mathfrak{q}$ sein. Es sei etwa $\mathfrak{p}^{(m)} \equiv 0$ nach $\mathfrak{q}$, so würde da $\mathfrak{p}^{(m)}$ ein Primideal ist, $\mathfrak{q} = \mathfrak{p}^{(m)}$ folgen, d. h. $\mathfrak{b} \equiv 0$ nach dem Primideal $\mathfrak{p}^{(m)}$ und folglich müsste nach Satz I das Ideal $\mathfrak{b}$ durch $p^{\frac{1}{n}}$ theilbar sein, d. h. $\mathfrak{a}^u$ wäre durch $p^{t+\frac{1}{n}}$ und folglich wären die Zahlen von $\mathfrak{a}$ sämmtlich durch eine höhere als die r^{te} Potenz von p theilbar; dies widerspricht der Wahl des Exponenten r. Aus Satz 2 folgt somit $\mathfrak{b} = 1$, d. h. $\mathfrak{a}^u = p^t$. Setzen wir $\mathfrak{k} = \mathfrak{p}' \ldots \mathfrak{p}^{(n-1)} \mathfrak{a}^{u-1}$, so folgt $\mathfrak{p}\mathfrak{k} = p^t$.

IV. *Ein Ideal* $\mathfrak{j}$ *kann nur auf eine einzige Weise als Product von Primidealen dargestellt werden.*

Zum Beweise nehmen wir an, es gebe zwei Zerlegungen des Ideals $\mathfrak{j}$ etwa:

$$\mathfrak{j} = \mathfrak{p}\,\mathfrak{q}\,\mathfrak{r} \ldots \mathfrak{l},$$
$$\mathfrak{j} = \mathfrak{p}'\mathfrak{q}'\mathfrak{r}' \ldots \mathfrak{l}',$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{l}$ und $\mathfrak{p}', \mathfrak{q}', \mathfrak{r}', \ldots, \mathfrak{l}'$ Primideale sind. Da wegen der ersten Zerlegung das Ideal $\mathfrak{j} \equiv 0$ nach $\mathfrak{p}$ ist, so folgt aus der zweiten Zerlegung nach Satz 3, dass eines der Primideale $\mathfrak{p}', \mathfrak{q}', \mathfrak{r}', \ldots, \mathfrak{l}' \equiv 0$ nach $\mathfrak{p}$ ist. Es sei etwa $\mathfrak{p}' \equiv 0$ nach $\mathfrak{p}$; dann wird, weil $\mathfrak{p}'$ ein Primideal ist, nothwendig $\mathfrak{p}' = \mathfrak{p}$. Nun construire man nach Satz III ein Ideal $\mathfrak{k}$ von der Art, dass $\mathfrak{p}\mathfrak{k}$ gleich einem Hauptideal η wird und multiplicire die beiden obigen Darstellungen von $\mathfrak{j}$ mit $\mathfrak{k}$. Wegen $\mathfrak{p} = \mathfrak{p}'$ folgt dann

$$\eta\,\mathfrak{q}\,\mathfrak{r} \cdots \mathfrak{l} = \eta\,\mathfrak{q}'\mathfrak{r}' \cdots \mathfrak{l}'$$

und hieraus nach Satz 4:

$$\mathfrak{j}' = \mathfrak{q}\,\mathfrak{r} \cdots \mathfrak{l} = \mathfrak{q}'\mathfrak{r}' \cdots \mathfrak{l}'.$$

Auf diese doppelte Zerlegung des Ideals $\mathfrak{j}'$ wende man das eben eingeschlagene Verfahren von neuem an: man erkennt so schliesslich die Identität der beiden vorgelegten Darstellungen des Ideals $\mathfrak{j}$.

V. *Ein jedes Ideal* $\mathfrak{j}$ *lässt sich stets als Product von Primidealen darstellen.*

Ist $\mathfrak{p}$ ein Primideal, nach welchem $\mathfrak{j} \equiv 0$ wird, so bestimme man nach Satz III ein Ideal $\mathfrak{k}$ derart, dass $\mathfrak{p}\mathfrak{k}$ gleich einem Hauptideal η wird. Durch Multiplication jener Congruenz mit $\mathfrak{k}$ folgt dann $\mathfrak{k}\mathfrak{j} \equiv 0$

nach dem Ideal $\mathfrak{p}\mathfrak{k}$ und gemäss Satz 4 ist daher $\mathfrak{k}\mathfrak{j} = \eta\mathfrak{j}'$. Nach Multiplication dieser Gleichung mit $\mathfrak{p}$ und Division durch η ergiebt sich $\mathfrak{j} = \mathfrak{p}\mathfrak{j}'$. Wenden wir auf das Ideal $\mathfrak{j}'$ das nämliche Verfahren an, wie soeben auf $\mathfrak{j}$, so ergiebt sich $\mathfrak{j}' = \mathfrak{q}\mathfrak{j}''$, wo $\mathfrak{q}$ ein Primideal bedeutet, nach welchem $\mathfrak{j}' \equiv 0$ ist. In gleicher Weise erhalten wir $\mathfrak{j}'' = \mathfrak{r}\mathfrak{j}'''$; wo $\mathfrak{r}$ ein Primideal bedeutet, nach welchem $\mathfrak{j}'' \equiv 0$ ist u. s. f. Die Einsetzung dieser Werthe von $\mathfrak{j}', \mathfrak{j}'', \ldots$ liefert für das Ideal $\mathfrak{j}$ der Reihe nach die Darstellungen $\mathfrak{j} = \mathfrak{p}\mathfrak{q}\mathfrak{j}''$, $\mathfrak{j} = \mathfrak{p}\mathfrak{q}\mathfrak{r}\mathfrak{j}'''$, ... Nun giebt es nach Satz 1 nur eine endliche Anzahl von Idealen, nach denen $\mathfrak{j} \equiv 0$ ist. Ist m diese Anzahl, so wird jedenfalls das eingeschlagene Verfahren nach m-maliger Anwendung abbrechen. Denn es ist $\mathfrak{j} \equiv 0$ nach den Idealen $\mathfrak{p}$, $\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}\mathfrak{q}\mathfrak{r}$, ... und diese Ideale sind nach IV sämmtlich von einander verschieden. Nach Beendigung des Verfahrens erhalten wir für das Ideal $\mathfrak{j}$ die verlangte Zerlegung:

$$\mathfrak{j} = \mathfrak{p}\mathfrak{q}\mathfrak{r}\cdots\mathfrak{l}$$

wo $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots, \mathfrak{l}$ Primideale sind.

Damit ist der Beweis des Satzes von der Zerlegung in Primideale für einen Galois'schen Körper vollständig geführt.

Wir betrachten nun einen beliebigen Körper niederen als n^{ten} Grades, dessen Zahlen sämmtlich auch Zahlen des eben behandelten Galois'schen Körpers sind und bezeichnen zur Unterscheidung die Zahlen und Ideale dieses niederen Körpers mit grossen Buchstaben. Wir denken uns die Zahlen des Galois'schen Körpers als rationale Functionen der Wurzel ϑ einer irreduciblen Gleichung n^{ten} Grades dargestellt und bezeichnen dann die übrigen $n-1$ Wurzeln dieser Gleichung mit $\vartheta', \vartheta'', \ldots, \vartheta^{(n-1)}$. Diese Wurzeln sind dann rationale Functionen von ϑ und die Einsetzung derselben an Stelle von ϑ bewirkt den Uebergang zu den conjugirten Körpern. Es giebt, wie die Galois'sche Theorie lehrt, eine gewisse Gruppe G von ν Substitutionen: $\vartheta = \vartheta, \vartheta = \vartheta', \ldots, \vartheta = \vartheta^{(\nu-1)}$ von der Eigenschaft, dass jede Zahl des niederen Körpers bei einer Substitution dieser Gruppe ungeändert bleibt und dass auch umgekehrt jede bei diesen Substitutionen ungeändert bleibende Zahl des Galois'schen Körpers dem niederen Körper angehört. Nun zerlege man ein Ideal $\mathfrak{J} = (\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_l)$ des niederen Körpers im Galois'schen Körper in Primideale etwa $\mathfrak{J} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$ und bestimme dann die Ideale $\mathfrak{k}_1, \ldots, \mathfrak{k}_m$ derart, dass die Producte $\mathfrak{p}_1\mathfrak{k}_1, \ldots, \mathfrak{p}_m\mathfrak{k}_m$ Hauptideale werden. Setzen wir $\mathfrak{k} = \mathfrak{k}_1 \ldots \mathfrak{k}_m$, so wird auch $\mathfrak{J}\mathfrak{k}$ gleich einem Hauptideal η und es gilt daher eine Gleichung von der Gestalt

$$\eta = \mathsf{A}_1\varkappa_1 + \mathsf{A}_2\varkappa_2 + \cdots + \mathsf{A}_l\varkappa_l,$$

wo $\varkappa_1, \varkappa_2, \ldots, \varkappa_l$ Zahlen des Ideals $\mathfrak{k}$ sind. Auf diese Gleichung wende man die Substitutionen $\vartheta = \vartheta', \ldots, \vartheta = \vartheta^{(\nu-1)}$ an; es ergeben sich dann der Reihe nach $\nu - 1$ Gleichungen von der Gestalt

$$\eta' = A_1 x_1' + A_2 x_2' + \cdots + A_l x_l',$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\eta^{(\nu-1)} = A_1 x_1^{(\nu-1)} + A_2 x_2^{(\nu-1)} + \cdots + A_l x_l^{(\nu-1)}.$$

Die Multiplication aller ν Gleichungen liefert

$$H = A_2^{\nu} K_1 + A_1^{\nu-1} A_2 K_2 + A_1^{\nu-2} A_2^2 K_3 + \cdots + A_l^{\nu} K_M,$$

wo sowohl $H = \eta\eta' \ldots \eta^{(\nu-1)}$ als auch die Coefficienten $K_1, \ldots, K_M$ bei Anwendung der Substitutionen der Gruppe G ungeändert bleiben und daher Zahlen des niederen Körpers sind. Bezeichnen wir das Ideal $(K_1, \ldots, K_M)$ des niederen Körpers mit $\mathfrak{K}$, so gilt im niederen Körper die Gleichung $H = \mathfrak{J}^{\nu}\mathfrak{K}$. In der That ist H in Folge der vorigen Gleichung eine Zahl des Ideals $\mathfrak{J}^{\nu}\mathfrak{K}$ und es bedarf daher nur des Nachweises, dass jede Zahl des Ideals $\mathfrak{J}^{\nu}\mathfrak{K}$ durch H theilbar ist. Nun ergiebt wegen $\eta = \mathfrak{J}\mathfrak{k}$ jede der Zahlen $A_1, \ldots, A_l$ mit jeder der Zahlen $x_1, \ldots, x_l$ multiplicirt ein durch η theilbares Product, ebenso ergiebt jede der Zahlen $A_1, \ldots, A_l$ mit jeder der Zahlen $x_1', \ldots, x_l'$ multiplicirt ein durch η' theilbares Product u. s. f. und hieraus folgt, dass das Product von irgend ν Zahlen $A_1, \ldots, A_l$, multiplicirt mit einer der Zahlen $K_1, \ldots, K_M$ durch $\eta\eta' \ldots \eta^{(\nu-1)} = H$ theilbar ist. Setzen wir $\mathfrak{J}^{\nu-1}\mathfrak{K} = \mathfrak{L}$, so wird $\mathfrak{J}\mathfrak{L} = H$ und diese Gleichung zeigt, dass zu jedem vorgelegten Ideal des niederen Körpers stets ein Ideal $\mathfrak{L}$ des niederen Körpers derart bestimmt werden kann, dass das Product $\mathfrak{J}\mathfrak{L}$ ein Hauptideal H des niederen Körpers wird. Aus diesem Satze kann der Satz von der eindeutigen Zerlegung eines Ideals in Primideale für den niederen Körper genau so geschlossen werden, wie oben aus Satz III die Sätze IV und V abgeleitet worden sind. Da ferner ein jeder beliebige Körper als ein Körper aufgefasst werden kann, welcher in einem Galois'schen Körper als niederer Körper enthalten ist, so haben wir hiermit den Satz von der eindeutigen Zerlegung eines Ideals allgemein als gültig erkannt.

Ostseebad Cranz, den 26. September 1893.