ÜBER ZUSAMMENGESETZTE ALGEBRAISCHE KÖRPER.

VON

ÖYSTEIN ORE

in OSLO.

§ 1. Übersicht.

Wenn eine algebraische Zahl α gegeben ist, so bilden alle rationalen, rationalzahligen Funktionen von α einen Zahlkörper k. Wenn zwei algebraische Zahlen α und α' gegeben sind, kann man zuerst die beiden entsprechenden Körper k und k' bilden, welche aus allen rationalen rationalzahligen Funktionen von α, bzw. α' bestehen. Man kann aber noch den weiteren, *aus k und k' zusammengesetzten Körper* K ableiten, der aus allen rationalen, rationalzahligen Funktionen von α und α' besteht. Der Körper K ist, wie man sieht, der kleinste algebraische Zahlkörper, der sowohl k als k' enthält.

Wenn n, n' und N die Gradzahlen von k, k' und K angeben, so ist

$$N \leqq nn',$$

und weiter muss N sowohl durch n als durch n' teilbar sein. Wenn daher n zu n' relativ prim ist, folgt sofort

$$N = nn'.$$

Haben die beiden Körper k und k' einen gemeinsamen Unterkörper $\varkappa$ vom Grade $\nu > 1$, so folgt einfach, dass

$$N \leqq \frac{nn'}{\nu} < nn'$$

ist. Dagegen kann man aber nicht, wie man an Beispielen erkennt, umgekehrt schliessen, dass $N = nn'$ sein muss, wenn kein solcher gemeinsamer Unterkörper existiert.

Es ist jetzt von Interesse zu untersuchen, wie die arithmetischen Eigenschaften des Körpers K von den Eigenschaften der Komponenten k und k' abhängen, besonders die Frage nach der Zerlegung der Primzahlen in Primideale in K und weiter die Zusammensetzung der Körperdifferente und Körperdiskriminante dieses Körpers. Betreffend die Körperdiskriminante D von K gilt der einfach beweisbare Satz[1]: D enthält alle und nur diejenigen Primzahlen als Faktoren, welche in der Körperdiskriminante d von k oder d' von k' oder in beiden aufgehen.

Ehe ich zu meinen Untersuchungen übergehe, möchte ich zuerst kurz die verschiedenen früheren Arbeiten auf diesem Gebiete erwähnen. Diese Arbeiten behandeln beinahe alle den Fall, dass der Grad des zusammengesetzten Körpers gleich dem Produkte der Gradzahlen der beiden ursprünglichen Körper ist, also $N=n\,n'$. Ich werde mich auch im Folgenden auf diesen Fall beschränken, in einer späteren Arbeit werde ich auch den allgemeinsten Fall behandeln.

Herr Hilbert[2] hat bewiesen: Wenn die Diskriminanten d und d' zu einander relativ prim sind, so ist notwendigerweise $N = n\,n'$ und die Körperdiskriminante von K ist durch

$$D = d^{n'}\, d'^{n}$$

bestimmt.

Von Herrn Hensel[3] wurde der folgende wichtige Satz bewiesen: Wenn die Primzahl p in k und k' die Primidealzerlegungen

$$p = \mathfrak{p}_1^{a_1}\, \mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_r^{a_r},\quad N\mathfrak{p}_i = p^{f_i}$$

$$p = \mathfrak{p}_1'^{a'_1}\, \mathfrak{p}_2'^{a'_2} \cdots \mathfrak{p}_{r'}'^{a'_{r'}},\quad N\mathfrak{p}'_j = p^{f'_j}$$

hat, und wenn weiter vorausgesetzt wird, dass keiner der Exponenten a_i oder a'_j durch p teilbar ist, so wird D durch p in einer Potenz mit dem Exponenten

---

[1] Man sehe P. Bachmann: Allgemeine Arithmetik der Zahlenkörper, Kap. 11. Leipzig 1905.

[2] D. Hilbert: Bericht über die Theorie der algebraischen Zahlkörper. § 52. Jahresbericht d. deutschen Mathematikervereinigung. Bd. IV [1897].

[3] K. Hensel: Über Gattungen, welche durch Komposition aus aus zwei anderen Gattungen entstehen. Journal f. Mathematik 105. S. 329—344. [1889]. Eine ausführliche Darstellung der Untersuchungen von Hensel findet man auch in dem oben zitierten Buche von P. Bachmann. S. 457—470.

$$\sum_{i=1}^{r}\sum_{j=1}^{r'} f_i f_j' (a_i a'_j - \alpha_{ij})$$

genau teilbar, wobei α_{ij} den grössten gemeinsamen Faktor von a_i und a_j bedeutet.

In einer Note zeigt Herr BAUER[1], dass die Hilbertschen Resultate ohne Anwendung der Idealtheorie abgeleitet werden können.

Weiter hat Frl. J. CAMERON[2] für Spezialfälle die Primidealzerlegung in einem zusammengesetzten Körper behandelt; leider scheint aber die Arbeit mit mehreren Fehlern behaftet zu sein.

In mehreren Noten hat Herr BAUER[3] die Zusammensetzung von Galoisschen Körpern behandelt, und weiter hat Herr RELLA[4] eine Arbeit über die Zusammensetzung von einem Kreisteilungskörper mit einem beliebigen algebraischen Körper publiziert.

§ 2. Beweis eines Hilfssatzes.

Für die folgenden Untersuchungen ist ein Hilfssatz über Primfunktionen für einen Primidealmodul notwendig, und ich werde sofort den notwendigen Beweis für ihn bringen. Es sei $\Phi(x)$ ein Polynom mit Koeffizienten, welche ganze Zahlen aus einem algebraischen Körper k sind, und weiter sei $\mathfrak{p}$ ein Primideal in k. Das Polynom $\Phi(x)$ heisst dann *Primfunktion* (mod $\mathfrak{p}$), wenn $\Phi(x)$ ausser sich selbst und Konstanten keine Teiler (mod $\mathfrak{p}$) enthält.

Man beweist für die Primfunktionen für einen Primidealmodul die entsprechenden Sätze wie für die Primfunktionen im rationalen Bereiche in Bezug auf einen Primzahlmodul. Ist z. B. der Grad von $\mathfrak{p}$ gleich f, so ist die Funktion

$$x^{p^{fm}} - x \pmod{\mathfrak{p}}$$

kongruent dem Produkte aller verschiedenen Primfunktionen (mod $\mathfrak{p}$), deren Grade Teiler von m sind.

---

[1] M. BAUER: Beweis von einigen bekannten Sätzen über zusammengesetzte Körper ohne Anwendung der Idealtheorie. Jahresbericht d. Deutschen Mathematikervereinigung 30. S. 186—188 [1921].

[2] J. CAMERON: Über die Zerlegung einer Primzahl in einem komponierten Körper. Dissertation, Marburg 1912.

[3] M. BAUER, Mathematische Annalen Bd. 77 und 83, Journal f. Mathematik, Bd. 150.

[4] T. RELLA: Die Zerlegungsgesetze für die Primideale eines beliebigen algebraischen Zahlkörpers im Körper der l-ten Einheitswurzel. Mathematische Zeitschrift S. 11—16. Bd. 5 [1919]. Es wird vorausgesetzt, dass l eine Primzahl ist.

Es soll aber hier untersucht werden, wenn $\varphi(x)$ eine Primfunktion im rationalen Bereiche (mod p) ist, wie dann $\varphi(x)$ (mod $\mathfrak{p}$) zerfällt, wobei $\mathfrak{p}$ ein Teiler von p im Körper k ist.

Es sei jetzt

$$\Phi(x)=\Phi(\omega, x)=x^k+\omega_1 x^{k-1}+\cdots+\omega_k$$

eine Primfunktion (mod $\mathfrak{p}$), welche $\varphi(x)$ teilt, wofür also eine Kongruenz

$$\varphi(x)\equiv\Phi(\omega, x)\,\Psi(\omega, x) \pmod{\mathfrak{p}}$$

besteht. Wenn man diese Kongruenz zur p-ten Potenz erhebt und dann weiter x statt x^p schreibt, erhält man

$$\varphi(x)\equiv\Phi(\omega^p, x)\,\Psi(\omega^p, x) \pmod{\mathfrak{p}}.$$

In dieser Weise zeigt man, dass die Polynome

$$\Phi(\omega, x),\ \Phi(\omega^p, x)\cdots\Phi(\omega^{p^{f-1}}, x) \tag{1}$$

sämtlich Teiler von $\varphi(x)$ sind, und weiter sieht man ein, dass alle diese Polynome Primfunktionen (mod $\mathfrak{p}$) sind. Denn z. B. aus

$$\Phi(\omega^p, x)\equiv\Phi_1(\omega, x)\,\Phi_2(\omega, x) \pmod{\mathfrak{p}}$$

folgt sofort

$$\Phi(\omega, x^{p^{f-1}})\equiv\Phi_1(\omega^{p^{f-1}}, x^{p^{f-1}})\,\Phi(\omega^{p^{f-1}}, x^{p^{f-1}}) \pmod{\mathfrak{p}},$$

und also auch

$$\Phi(\omega, x)\equiv\Phi_1(\omega^{p^{f-1}}, x)\,\Phi_2(\omega^{p^{f-1}}, x) \pmod{\mathfrak{p}},$$

was nicht möglich ist, da $\Phi(\omega, x)$ (mod $\mathfrak{p}$) eine Primfunktion ist.

Multipliziert man die Primfunktionen (1) mit einander, so wird das Produkt kongruent einem rationalen Polynome, und folglich gleich einer Potenz von $\varphi(x)$. $\varphi(x)$ kann also (mod $\mathfrak{p}$) nicht andere Primfunktionen als (1) enthalten.

Die Primfunktionen (1) sind im Allgemeinen nicht alle von einander verschieden. Nun kann aber $\varphi(x)$, wie man leicht sieht, nicht mehrfache Faktoren (mod $\mathfrak{p}$) enthalten; wenn daher

$$\Phi_1(x),\ \Phi_2(x), \ldots \Phi_e(x)$$

die verschiedenen unter den Primfunktionen (1) bezeichnen, so ist

$$\varphi(x) \equiv \Phi_1(x)\,\Phi_2(x) \ldots \Phi_e(x) \pmod{\mathfrak{p}}.$$

Hierbei ist die Zahl e ein Teiler von m, wenn m den Grad von $\varphi(x)$ angibt, indem man $m=ek$ hat.

Es soll nun gezeigt werden, dass e gleich dem grössten gemeinsamen Faktor von m und f ist. Bezeichnet man den grössten gemeinsamen Faktor von m und f mit e', so ist also $m=e'm'$, $f=e'f'$, wo m' zu f' relativ prim ist.

Die Primfunktion $\varphi(x)$ ist $(\mathrm{mod}\ p)$ ein Teiler von

$$x^{p^m} - x = x^{p^{e'm'}} - x,$$

und man beweist dann einfach, dass $\varphi(x)$ auch ein Teiler von

$$x^{p^{m'e'f'}} - x = x^{p^{m'f}} - x \pmod{p}$$

ist. Diese Funktion enthält aber, nach einer früheren Bemerkung, nur Primfunktionen $(\mathrm{mod}\ \mathfrak{p})$, deren Grade Teiler von m' sind. Der Grad k einer Primfunktion $\Phi_i(x)$ ist also ein Teiler von m'.

Man beweist aber leicht, dass k kein echter Teiler von m' sein kann. Denn die Primfunktionen $\Phi_i(x)$ müssen sicher die Funktion

$$x^{p^{fk}} - x = x^{p^{e'f'k}} - x \pmod{\mathfrak{p}}$$

teilen, und daraus folgt einfach, dass $\varphi(x)$ $(\mathrm{mod}\ p)$ die Funktion

$$x^{p^{e'f'k}} - x$$

teilen muss. Dies ist aber nicht möglich ausser wenn $m'=k$ ist, indem f' zu m' relativ prim ist.

Man hat daher den folgenden Sats bewiesen:

Satz 1. Eine Primfunktion $\varphi(x)$ (mod p) zerfällt (mod $\mathfrak{p}$) in e vershiedene Primfaktoren gleicher Grade

$$\varphi(x) \equiv \Phi_1(x)\,\Phi_2(x) \cdots \Phi_e(x) \pmod{\mathfrak{p}}.$$

Die Zahl e ist der grösste gemeinsame Faktor vom Grade m der Primfunktion $\varphi(x)$ und vom Grade f des Primideals $\mathfrak{p}$.

Mit Hilfe dieses Satzes beweist man auch einfach, dass $\varphi(x)$ auch für jede Potenz von $\mathfrak{p}$ reduzibel wird, und dass man eine Zerlegung

$$\varphi(x) \equiv \Phi_1^{(\alpha)}(x)\, \Phi_2^{(\alpha)}(x) \cdots \Phi_e^{(\alpha)}(x) \pmod{\mathfrak{p}^\alpha},$$

hat, wobei allgemein

$$\Phi_i^{(\alpha)}(x) \equiv \Phi_i(x) \pmod{\mathfrak{p}} \qquad (i = 1, 2, \ldots e)$$

ist.

§ 3. Bezeichnungen.

Es seien jetzt zwei algebraische Körper k und k' von den Graden n und n' gegeben. Im Folgenden sollen alle Zahlen, Ideale usw. aus dem Körper k' mit Buchstaben bezeichnet werden, welche mit einem Striche versehen sind.

Es seien ω und ω' zwei erzeugende ganze Zahlen für k bzw. k'; die Zahlen in k und k' haben dann alle die Form

$$\begin{aligned} \alpha &= a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1}, \\ \alpha' &= a'_0 + a'_1\omega' + \cdots + a'_{n'-1}\omega'^{n'-1}. \end{aligned} \tag{2}$$

Aus k und k' bildet man den zusammengesetzten Körper K, der sowohl k als k' als Unterkörper enthält. Wenn der Grad von K gleich N ist, wird aber, wie schon früher bemerkt, $N = nn'$ vorausgesetzt. Alle Grössen aus K sollen im Folgenden mit grossen Buchstaben bezeichnet werden. K wird aus allen Zahlen von der Form

$$\Omega = \sum_{i,j} A_{i,j}\, \omega^i \omega'^j \tag{3}$$

bestehen, wobei die $A_{i,j}$ rational sind, und weiter $i < n$, $j < n'$ vorausgesetzt werden kann.

Weiter seien

$$f(x) = 0, \qquad f_1(x) = 0$$

die beiden im rationalen Gebiete irreduziblen Gleichungen, welchen die Zahlen ω und ω' genügen. Der Grad von $f(x)$ ist dann n, und der Grad von $f_1(x)$ gleich n'. Da aber der Grad von K gleich $N = nn'$ ist, muss auch das Polynom $f(x)$ im Körper k' irreduzibel bleiben, und ebenso $f_1(x)$ in k irreduzibel, indem sonst der Grad von K kleiner als nn' würde. Umgekehrt ist dies natürlich auch hinreichend dafür, dass der Grad des zusammengesetzten Körpers gleich dem Produkte der Grade Teilkörper ist.

Zunächst soll untersucht werden, wie die Primidealzerlegung einer rationalen Primzahl p im zusammengesetzten Körper K mit den Zerlegungen von p in den beiden Körpern k und k' zusammenhängt.

Es wird daher vorausgesetzt, dass

$$p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i = p^{f_i} \tag{4}$$

und

$$p = \mathfrak{p}_1'^{e_1'}\mathfrak{p}_2'^{e_2'}\cdots\mathfrak{p}_{r'}'^{e_{r'}'}, \quad N_1\mathfrak{p}_i' = p^{f_i'} \tag{5}$$

die beiden Zerlegungen von p in k und k' sind. Das Zeichen N_1 soll die in k' genommene Norm einer Grösse bezeichnen.

Bekanntlich steht die Primidealzerlegung (4) von p in engem Zusammenhange mit den Eigenschaften des Polynoms $f(x)$. Es sei nämlich die Diskriminante von $f(x)$ genau durch p^ϱ teilbar. Zerlegt man $f(x)$ (mod p^α) in unzerlegbare Faktoren (mod p^α), wobei $\alpha > 2\varrho + 1$ gewählt wird, so hat man

$$f(x) \equiv f_1(x) f_2(x) \cdots f_r(x) \pmod{p^\alpha} \tag{6}$$

und hier ist, wenn n_i den Grad eines Primfaktors $f_i(x)$ bezeichnet, $n_i = e_i f_i$. Umgekehrt folgt aus dem Bestehen der Zerlegung (6) (mod p^α), dass p eine entsprechende Idealzerlegung (4) besitzt, wobei jedoch die Ordnungen e_i und die Gradzahlen f_i der Primideale nicht vollständig bestimmt sind, indem man nur die Relation $n_i = e_i f_i$ kennt. Weiter besteht zwischen dem Primideale $\mathfrak{p}_i$ und dem entsprechenden irreduziblen Faktor $f_i(x)$ die Beziehung, dass

$$f_i(\omega) \equiv 0 \pmod{\mathfrak{p}_i^\beta}$$

ist, wobei β durch eine hinreichend grosse Wahl von α auch beliebig gross wird.

Entsprechendes gilt natürlich auch betreffend die Zerlegung (5) in k' und $f_1(x)$. Es ist weiter von Wichtigkeit, dass sich diese Betrachtungen sofort auf Relativkörper ausdehnen lassen; wenn daher $\mathfrak{p}$ ein Primideal im Unterkörper ist, so findet man die Primidealzerlegung von $\mathfrak{p}$ im Oberkörper, wenn man die definierende Gleichung des Oberkörpers in unzerlegbaren Funktionen (mod $\mathfrak{p}^\alpha$) zerlegt.

§ 4. Bestimmung der Zerlegung einer Primzahl im zusammengesetzten Körper.

Unter Anwendung der Schlussbemerkungen des § 3 kann man verhältnismässig einfach die Primidealzerlegung einer Primzahl p im Körper K bestim-

men. Man fasst nämlich K als Relativkörper in Bezug auf k' auf und die in k' irreduzible Gleichung $f(x)=0$ definiert dann eine Zahl im Relativkörper.

Soll man daher die Primidealzerlegung in K von einem Primideale $\mathfrak{p}'_j$ in k' bestimmen, so braucht man nur das Polynom $f(x)$ in irreduzible Faktoren (mod $\mathfrak{p}'^{\alpha}_j$) zu zerlegen, wobei der Exponent α hinreichend gross gewählt wird.

Da aber schon die Zerlegung (6) von $f(x)$ (mod p^{α}) besteht, so hat man auch dieselbe Zerlegung von $f(x)$ (mod $\mathfrak{p}'^{\alpha}_j$), indem $\mathfrak{p}'_j$ ein Teiler von p ist. Natürlich sind dann die Faktoren $f_i(x)$ im Allgemeinen nicht (mod $\mathfrak{p}'^{\alpha}_j$) unzerlegbar, aber jedenfalls folgt daraus, dass das Primideal $\mathfrak{p}'_j$ in K eine Zerlegung

$$\mathfrak{p}'_j = A_{1j} A_{2j} \cdots A_{rj} \tag{7}$$

besitzt, wobei die Ideale A_{ij} zu einander relativ prim sind, aber doch nicht Primideale in K zu sein brauchen.

Mit Hilfe der Zerlegung (5) von p in k' folgt dann aus (7):

Die Primzahl p besitzt in K die Zerlegung

$$p = \prod_{i,j} A_{ij}^{e'_j} \qquad (i=1, 2, \ldots r; \quad j=1, 2, \ldots r'), \tag{8}$$

wobei die Ideale $A_{i,j}$ alle zu einander relativ prim sind.

Es bleibt also nur übrig die Zerlegung der Ideale $A_{i,j}$ genauer zu studieren, und um dies zu erreichen muss man die Zerlegung eines Faktors $f_i(x)$ (mod $\mathfrak{p}^{\alpha}_j$) in Primfaktoren mit Koeffizienten in k' bestimmen. Man kann aber diese Untersuchung dadurch erleichtern, dass man $f_i(x)$ auf eine spezielle Form reduziert. Wählt man nämlich die Zahl ω als Primitivzahl in Bezug auf das Ideal $\mathfrak{p}_i$, so kann man eine Primfunktion $\varphi(x)$ (mod p) vom Grade f_i so bestimmen, dass

$$f(x) \equiv Q(x)\,(\varphi(x)^{e_i} + p\,M(x)) \pmod{p^{\alpha}}$$

ist. Hier kann man weiter voraussetzen, dass $Q(x)$ (mod p) nicht durch $\varphi(x)$ teilbar ist, und weiter auch $M(x)$ nicht durch $\varphi(x)$ (mod p) teilbar.

Man kann also

$$f_i(x) = \varphi(x)^{e_i} + p\,M(x) \tag{9}$$

annehmen, und man soll die Zerlegung von $f_i(x)$ (mod $\mathfrak{p}'^{\alpha}_j$) studieren.

Wenn φ_{ij} der grösste gemeinsame Faktor von f_i und f_j' ist, so zerfällt $\varphi(x)$ (mod $\mathfrak{p}'_j$) nach Satz I in φ_{ij} Primfaktoren

$$\varphi(x) \equiv \Phi_1(x)\,\Phi_2(x)\cdots\Phi_{\varphi_{ij}}(x) \pmod{\mathfrak{p}'_j}, \tag{10}$$

wobei der Grad von $\Phi_k(x)$ gleich $\frac{f_i}{\varphi_{ij}}$ ist. Nach der Schlussbemerkung des § 2 kann man auch voraussetzen, dass die Primfunktionen $\Phi_k(x)$ so gewählt sind dass statt (10) sogar die Kongruenz

$$\varphi(x) \equiv \Phi_1(x)\,\Phi_2(x)\cdots\Phi_{\varphi_{ij}}(x) \pmod{\mathfrak{p}_j'^{\alpha}} \tag{11}$$

besteht, wobei α fest, aber beliebig gross gedacht werden kann.

Es folgt jetzt aus (10) oder (11) nach (9)

$$f_i(x) \equiv \Phi_1(x)^{e_i}\,\Phi_2(x)^{e_i}\cdots\Phi_{\varphi_{ij}}(x)^{e_i} \pmod{\mathfrak{p}'_j},$$

und man beweist dann einfach, dass auch eine Zerlegung

$$f_i(x) \equiv \Psi_1(x)\,\Psi_2(x)\cdots\Psi_{\varphi_{ij}}(x) \pmod{\mathfrak{p}_j'^{\alpha}} \tag{12}$$

besteht, wobei

$$\Psi_k(x) = \Phi_k(x)^{e_i} + M_k(x) \qquad (k = 1, 2, \ldots, \varphi_{ij}) \tag{13}$$

und

$$M_k(x) \equiv 0 \pmod{\mathfrak{p}'_j}$$

ist.

Es soll jetzt untersucht werden, welche Potenz von $\mathfrak{p}'_j$ in den Koeffizienten von $M_k(x)$ aufgeht.

Setzt man

$$\Pi_k(x) = \Phi_1(x)\,\Phi_2(x)\cdots\Phi_{k-1}(x)\,\Phi_{k+1}(x)\cdots\Phi_{\varphi_{ij}}(x),$$

so hat man nach (12) und (13)

$$f_i(x) \equiv \Psi_k(x)\,(\Pi_k(x)^{e_i} + N_k(x)) \pmod{\mathfrak{p}_j'^{\alpha}},$$

wobei auch

$$N_k(x) \equiv 0 \pmod{\mathfrak{p}'_j}$$

ist. Setzt man hier (9) und (13) ein und multipliziert aus, so erhält man nach (12)

$$p\,M(x) \equiv M_k(x)\,\Pi_k(x)^{e_i} + N_k(x)\,\Phi_k(x)^{e_i} + M_k(x)\,N_k(x) \pmod{\mathfrak{p}_j'^{\alpha}}. \tag{14}$$

Nimmt man nun an, dass $\mathfrak{p}_j'^{\beta}$ die höchste Potenz von $\mathfrak{p}'_j$ ist, welche in allen Koeffizienten von $M_k(x)$ aufgeht und entsprechend $\mathfrak{p}_j'^{\gamma}$ für $N_k(x)$, so wird

das Produkt $M_k(x)N_k(x)$ genau durch $\mathfrak{p}'^{\beta+\gamma}_j$ teilbar. Weiter ist p genau durch $\mathfrak{p}'^{e'j}_j$ teilbar, und es folgt leicht, dass man $\beta+\gamma \geqq e'_j$ haben muss. Denn wäre $\beta+\gamma<e'_j$, so würde man nach (14) die Kongruenz

$$M_k(x)\,\Pi_k(x)^{e_i} + N_k(x)\,\Phi_k(x)^{e_i} \equiv 0 \pmod{\mathfrak{p}'^{\beta+\gamma}_j} \tag{15}$$

haben, und da die Resultante von $\Pi_k(x)$ und $\Phi_k(x)$ nicht durch $\mathfrak{p}'_j$ teilbar ist, so kommt aus (15) leicht

$$M_k(x) \equiv 0,\ N_k(x) \equiv 0 \pmod{\mathfrak{p}'^{\beta+\gamma}_j},$$

was aber nach der Definition der Zahlen β und γ nicht möglich ist.

Man hat also $\beta+\gamma \geqq e'_j$ und daher besteht nach (14) die Kongruenz

$$M_k(x)\,\Pi_k(x)^{e_i} + N_k(x)\,\Phi_k(x)^{e_i} \equiv 0 \pmod{\mathfrak{p}'^{e_j}_j},$$

woraus wie früher

$$M_k(x) \equiv 0,\ N_k(x) \equiv 0 \pmod{\mathfrak{p}'^{e'j}_j}$$

folgt. Man hat also $\beta \geqq e'_j$, und man muss sogar $\beta = e'_j$ haben. Denn wäre $\beta > e'_j$, so bestünde die Kongruenz

$$p\,M(x) \equiv N_k(x)\,\Pi_k(x)^{e_i} \pmod{\mathfrak{p}'^{e'j+1}_j},$$

woraus man einfach ableitet, dass $M(x) \pmod{\mathfrak{p}'_j}$ durch $\varphi(x)$ teilbar wäre, was aber nicht der Fall ist.

Ist daher π'_j eine Zahl in k', welche genau durch die erste Potenz von $\mathfrak{p}'_j$ teilbar ist, so kann man ein Polynom $P_k(x)$ so bestimmen, dass

$$M_k(x) \equiv \pi'^{e_j}_j P_k(x) \pmod{\mathfrak{p}'^{\alpha}_j} \tag{16}$$

ist, wobei in $P_k(x)$ die Koeffizienten nicht alle durch $\mathfrak{p}'_j$ teilbar sind. Setzt man weiter (16) in (14) ein, so beweist man ohne Schwierigkeit, dass $P_k(x) \pmod{\mathfrak{p}'_j}$ nicht durch $\Phi_k(x)$ teilbar ist.

Man kann die letzten Untersuchungen folgendermassen zusammenfassen:

Der Faktor $f_i(x)$ (9) zerfällt (mod $\mathfrak{p}'^{\alpha}_j$) in φ_{ij} Faktoren wie in (12) angegeben. Hier hat ein Faktor $\Psi_k(x)$ allgemein die Form

$$\Psi_k(x) \equiv \Phi_k(x)^{e_i} + \pi'^{e_j}_j P_k(x), \tag{17}$$

wobei $\Phi_k(x)$ (mod $\mathfrak{p}'_j$) eine Primfunktion ist, die Zahl π'_j genau die erste Potenz von $\mathfrak{p}'_j$ enthält, und das Polynom $P_k(x)$ (mod $\mathfrak{p}'_j$) nicht durch $\Phi_k(x)$ teilbar ist.

Aus der Zerlegung (12) von $f_i(x)$ folgt nun sofort eine weitere Zerlegung des entsprechenden Ideals A_{ij} in (8) indem man

$$A_{ij} = B_1^{(ij)} B_2^{(ij)} \cdots B_{\varphi_{ij}}^{(ij)} \tag{18}$$

erhält, wobei die Ideale $B_k^{(ij)}$ alle zu einander relativ prim sind.

Es werden die Relativnormen im Körper K in Bezug auf k und k' mit den Zeichen ν und ν_1 bezeichnet, und weiter soll N die Absolutnormen angeben. Da der Grad eines Faktors $\Psi_k(x)$ in (12) nach (17) gleich $\frac{f_i e_i}{\varphi_{ij}}$ ist, wird

$$\nu_1(B_k^{(ij)}) = \mathfrak{p}_j'^{\frac{f_i}{\varphi_{ij}}}$$

und daher

$$N(B_k^{(ij)}) = p^{\frac{f_i f_j'}{\varphi_{ij}} \cdot e_i} = p^{F_{ij} e_i}, \tag{19}$$

wobei F_{ij} das kleinste gemeinsame Multiplum von f_i und f_j' bezeichnet.

Das Ideal $B_k^{(ij)}$ ist aber sofort weiter zerlegbar. Aus § 3 folgt nämlich, dass die Zahl $\Psi_k(\omega)$ durch eine beliebig hohe Potenz von jedem Primideale P teilbar wird, das in $B_k^{(ij)}$ aufgeht, wenn man nur die Zahl α hinreichend gross wählt. Aus (17) folgt dann

$$\Phi_k(\omega)^{e_i} + \pi_j'^{e'_j} N_k(\omega) \equiv 0 \pmod{P^\beta}. \tag{20}$$

Wenn nun $B_k^{(ij)}$ genau durch P^L teilbar ist, so wird also auch $\mathfrak{p}'_j$ und π'_j genau durch P^L teilbar, und weiter die Zahl $\pi_j'^{e'_j} N_k(\omega)$ genau durch $P^{Le'_j}$ teilbar. Nimmt man weiter an, dass $\Phi_k(\omega)$ genau durch P^M teilbar ist, so folgt einfach aus (20)

$$L e'_j = M e_i,$$

und wenn daher ε_{ij} der grösste gemeinsame Faktor von e_i und e'_j bezeichnet, so wird immer L durch $\frac{e_i}{\varepsilon_{ij}}$ teilbar.

Das Ideal $B_k^{(ij)}$ wird also immer eine $\frac{e_i}{\varepsilon_{ij}}$-te Potenz, und man kann folglich

$$B_k^{(ij)} = (C_k^{(ij)})^{\frac{e_i}{\varepsilon_{ij}}} \tag{21}$$

setzen, und es gilt nach (19)

$$N(C_k^{(ij)}) = p^{\varepsilon_{ij} F_{ij}}.$$

Aus (18) schliesst man nach (21), dass man auch

$$A_{ij} = \overline{D_{ij}^{\frac{e_i}{\varepsilon_{ij}}}} \tag{22}$$

setzen kann, wo

$$D_{ij} = C_1^{(ij)} C_2^{(ij)} \dots C_{\varphi_{ij}}^{(ij)} \tag{23}$$

ist. Wird dann (22) in (8) eingesetzt, so erhält man die folgende Idealzerlegung von p in K

$$p = \prod_{i=1}^{r} \prod_{j=1}^{r'} \overline{D_{ij}^{\frac{e_i e'_j}{\varepsilon_{ij}}}} = \prod_{i=1}^{r} \prod_{j=1}^{r'} D_{ij}^{E_{ij}},$$

wobei E_{ij} das kleinste gemeinsame Multiplum von e_i und e'_j bedeutet.

Satz 2. Hat in den Körpern k und k' die Primzahl p die Primidealzerlegungen

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}, \qquad N\mathfrak{p}_i = p^{f_i},$$
$$p = \mathfrak{p}'_1{}^{e'_1} \mathfrak{p}'_2{}^{e'_2} \cdots \mathfrak{p}'_{r'}{}^{e'_{r'}}, \quad N_1\mathfrak{p}'_i = p^{f'_i},$$

so besitzt p im zusammengesetzten Körper K eine Idealzerlegung

$$p = \prod_{i=1}^{r} \prod_{j=1}^{r'} D_{ij}^{E_{ij}},$$

wobei ein Ideal D_{ij} die weitere Zerlegung

$$D_{ij} = C_1^{(ij)} C_2^{(ij)} \dots C_{\varphi_{ij}}^{(ij)}, \quad N(C_k^{(ij)}) = p^{\varepsilon_{ij} F_{ij}}$$

besitzt. Hierbei ist E_{ij}, bzw. F_{ij} das kleinste gemeinsame Multiplum von e_i und e'_j, bzw. von f_i und f'_j, und weiter ist ε_{ij} bzw. φ_{ij} der grösste gemeinsame Faktor von e_i und e'_j, bzw. von f_i und f'_j. Die Ideale $C_k^{(ij)}$ sind alle zu einander relativ prim.

§ 5. Bestimmung der Primidealzerlegung im allgemeinen Falle.

Nach Satz 2 folgt, dass die Primidealzerlegung von p in K vollständig bestimmt ist, wenn man die Zerlegung der Ideale $C_k^{(ij)}$ in (23) kennt. Um aber die Zerlegung von $C_k^{(ij)}$ zu bestimmen, muss man die Zerlegung des Polynoms (17)

$$\Psi_k(x) = \Phi_k(x)^{e_i} + \pi_j'^{e'_j} P_k(x) \tag{24}$$

in irreduziblen Faktoren (mod $\mathfrak{p}_j'^{\alpha}$) untersuchen.

A. a. O.[1] habe ich eine Methode angegeben, mit der man die Reduzibilität von Polynomen mit rationalen Koeffizienten (mod p^{α}) untersuchen kann; man bildet dazu eine Entwicklung $(p, \varphi(x))$ des Polynoms, wobei $\varphi(x)$ (mod p) eine Primfunktion ist, und konstruiert das zugehörige Polygon. Diese Methode lässt sich aber, wie man leicht sieht, für beliebige algebraische Körper verallgemeinern, indem man dann Entwicklungen $(\mathfrak{p}, \Phi(x))$ bildet, wobei $\Phi(x)$ (mod $\mathfrak{p}$) eine Primfunktion bezeichnet.

Im obigen Falle (24) ist, wie man leicht sieht, das Polygon $(\mathfrak{p}'_j, \Phi_k(x))$ oder, was dasselbe ist, das Polygon $(\pi'_j, \Phi_k(x))$ eine Gerade, welche die Projektionen e_i bzw. e'_j auf die X-achse bzw. Y-achse hat. Es wird der Kürze wegen

$$e_i = \varepsilon_{ij} \lambda_i$$

$$e'_i = \varepsilon_{ij} \varkappa_i$$

gesetzt, wobei also λ_i zu $\varkappa_i$ relativ prim ist.

Die Untersuchung der Reduzibilität von $\Psi_k(x)$ (mod $\mathfrak{p}_j'^{\alpha}$) hängt nun mit der Zerlegbarkeit der Funktion

$$F_k(x, y) = y^{\varepsilon_{ij}} + P_k(x) \ (\text{modd } \mathfrak{p}'_j, \Phi_k(x)) \tag{25}$$

aufs Engste zusammen.

Es habe nämlich $F_k(x, y)$ die Zerlegung in Primfaktoren

$$F_k(x, y) \equiv F_k^{(1)}(x, y)^{s_1} \cdots F_k^{(q)}(x, y)^{s_q} \,(\text{modd } \mathfrak{p}'_j, \Phi_k(x)), \tag{26}$$

wobei der Grad eines Faktors $F_k^{(t)}(x, y)$ in y gleich μ_t ist, wo also nach (25)

$$\mu_1 s_1 + \cdots + \mu_q s_q = \varepsilon_{ij}$$

ist. Dann zerfällt entsprechend $\Psi_k(x)$

$$\Psi_k(x) \equiv \Psi_k^{(1)}(x) \ldots \Psi_k^{(q)}(x) \ (\text{mod } \mathfrak{p}_j'^{\alpha}), \tag{27}$$

wobei der Grad von $\Psi_k^{(t)}(x)$ gleich $\mu_t s_t \lambda_i \dfrac{f_i}{\varphi_{ij}}$ ist.

---

[1] Man sehe z. B. Ö. ORE: Zur Theore der algebraischen Körper, Acta Mathematica, Bd. 44 [1922]. Aus dieser Arbeit leitet man einfach die hier folgenden Ergebnisse ab.

Die Faktoren $\Psi_k^{(t)}(x)$ brauchen jedoch in diesem allgemeinen Falle nicht (mod $\mathfrak{p}_j'^{\alpha}$) irreduzibel zu sein. Wenn aber für einen Faktor $F_k^{(t)}(x, y)$ in (26) der Exponent $s_t = 1$ ist, wird auch der entsprechende Faktor $\Psi_k^{(t)}(x)$ in (27) (mod $\mathfrak{p}_j'^{\alpha}$) irreduzibel. In dem Falle also, wo die Exponenten in (26) alle gleich 1 sind, werden alle Faktoren in (27) (mod $\mathfrak{p}_j'^{\alpha}$) irreduzibel und man zeigt dann leicht, dass das Ideal $C_k^{(ij)}$ in q entsprechende, verschiedene Primideale zerfällt, wobei der Grad eines solchen Primideals gleich $\mu_t f_{ij}$ wird, wo also jetzt

$$\mu_1 + \cdots + \mu_q = \varepsilon_{ij} \tag{28}$$

gilt.

Man kann aber im vorliegenden Falle einfach entscheiden, wann $F_k(x, y)$ (modd $\mathfrak{p}'_j$, $\Phi_k(x)$) nur verschiedene Primfaktoren besitzt. Wenn nämlich $F_k(x, y)$ (modd $\mathfrak{p}'_j$, $\Phi_k(x)$) einen mehrfachen Faktor hat, so muss $F_k(x, y)$ (modd. $\mathfrak{p}'_j$, $\Phi_k(x)$) mit $F'_k(x, y)$ einen Faktor gemeinsam haben (Die Differentiation von $F_k(x, y)$ soll partiell in Bezug auf y ausgeführt werden.) Nun ist aber nach (25)

$$F'_k(x, y) = \varepsilon_{ij} y^{\varepsilon_{ij}-1},$$

so dass $F_k(x, y)$ nur dann mit $F_k'(x, y)$ einen Faktor gemeinsam haben kann, wenn ε_{ij} durch p teilbar ist, und dies erfordert weiter, nach der Bedeutung von ε_{ij}, dass sowohl e_i als e'_j durch p teilbar sein sollen.

Es ist daher bewiesen:

Satz 3. Wenn nicht gleichzeitig e_i und e'_j durch p teilbar ist, zerfällt ein Ideal $C_k^{(ij)}$ in der Zerlegung von p des Satzes 2 in lauter verschiedene Primideale

$$C_k^{(ij)} = P_1 P_2 \cdots P_q, \quad N P_t = p^{\mu_t f_{ij}},$$

wobei die ganzen Zahlen μ der Bedingung

$$\mu_1 + \cdots + \mu_q = \varepsilon_{ij}$$

genügen.

Wenn $\varepsilon_{ij} = 1$ ist, wird also $C_k^{(ij)}$ selbst ein Primideal für alle k.

Aus Satz 2 und Satz 3 leitet man sofort den weiteren, wichtigen Satz ab:

Satz 4. Wenn entweder keiner der Exponenten e_i oder keiner der Exponenten e'_j durch p teilbar ist, so wird die Zerlegung von p im zusammengesetzten Körper K folgendermassen bestimmt:

Es ist

$$p = \prod_{i=1}^{r} \prod_{j=1}^{r'} D_{ij}^{E_{ij}},$$

wobei

$$D_{ij} = C_1^{(ij)} C_2^{(ij)} \cdots C_{\varphi_{ij}}^{(ij)}, \quad \mathfrak{N}(C_k^{(ij)}) = p^{\varepsilon_{ij} F_{ij}}$$

ist und alle Ideale $C_k^{(ij)}$ zu einander relativ prim sind. Ein Ideal $C_k^{(ij)}$ zerfällt in lauter verschiedene Primfaktoren

$$C_k^{(ij)} = P_1 P_2 \cdots P_q, \quad \mathfrak{N} P_t = p^{\mu_t F_{ij}}$$

Hierbei haben die Zahlen $E_{ij}, F_{ij}, \varepsilon_{ij}, \varphi_{ij}$, dieselbe Bedeutung wie in Satz 2 und für die ganzen Zahlen μ_t gilt die Beziehung

$$\mu_1 + \cdots + \mu_q = \varepsilon_{ij}.$$

Im Falle, wo ε_{ij} durch p teilbar ist, werden die Verhältnisse nicht so einfach. Wenn ε_{ij} genau durch p^s teilbar ist, wird $F_k(x, y)$ eine p^s-te Potenz (modd $\mathfrak{p}'_j$, $\Phi_k(x)$), und es kann in diesem Falle $C_k^{(ij)}$ auch mehrfache Primidealfaktoren enthalten. Man zeigt aber leicht, dass die vorkommenden Exponenten $\leqq p^s$ sind. Es ist zu vermuten, dass die Exponenten sonst willkürlich variieren können, so dass man in diesem Falle keinen allgemeinen Satz erhalten kann.

§ 6. Bestimmung der Diskriminante des zusammengesetzten Körpers.

Unter Anwendung der vorhergehenden Untersuchungen lässt sich auch die Diskriminante des zusammengesetzten Körpers einfach bestimmen. Es seien δ, δ_1 und Δ die Körperdifferenten von k, k' und K, und weiter seien d, d_1 und D die Körperdiskriminanten derselben Körper, wobei man bekanntlich

$$N(\delta) = |d|, \quad N_1(\delta_1) = |d_1|, \quad \mathfrak{N}(\Delta) = |D| \tag{29}$$

hat. Weiter weiss man, dass wenn die Primzahl p in k die Primidealzerlegung (4) besitzt, die Körperdifferente δ genau durch $\mathfrak{p}_i^{e_i - 1 + \varrho_i}$ teilbar ist, wobei $\varrho_i = 0$ ist, wenn e_i nicht durch p teilbar ist, dagegen $\varrho_i \geqq 1$, wenn e_i durch p teilbar ist. Die Zahl ϱ_i soll die *Supplementzahl* des Primideals $\mathfrak{p}_i$ heissen. Entsprechend wird in k' die Supplementzahl eines Primideals $\mathfrak{p}'_j$ mit ϱ'_j bezeichnet. Aus (29) folgt dann, dass die Diskriminanten d und d_1 genau durch die Potenzen von p mit den Exponenten

$$\sum_{i=1}^{r} f_i (e_i - 1 + \varrho_i) \quad \text{bzw.} \quad \sum_{j=1}^{r'} f'_j (e'_j - 1 + \varrho'_j)$$

teilbar sind. Wie man sieht, ist die Diskriminante eines Körpers vollständig bestimmt, wenn man den Grad f_i, die Ordnung e_i und die Supplementzahl ϱ_i aller Primideale kennt.

Es soll nun die Differente $\mathfrak{A}$ von K untersucht werden. Wenn $\mathfrak{A}_{k'}$ die Relativdifferente des Körpers K in Bezug auf k' ist, besteht bekanntlich die Relation

$$\mathfrak{A} = \delta_1 \mathfrak{A}_{k'}, \tag{30}$$

und da man in diesem Falle δ_1 als bekannt voraussetzen darf, braucht man nur die Relativdifferente $\mathfrak{A}_{k'}$ zu untersuchen.

Es wird jetzt wie in Satz 4 vorausgesetzt, dass entweder keine der Zahlen e_i oder keine der Zahlen e'_j durch p teilbar ist; es werden in diesem Falle die Bezeichnungen so gewählt, dass keine der Zahlen e_i durch p teilbar ist, und man hat daher für alle i einfach $\varrho_i = 0$.

Es sei mit den Bezeichnungen des Satzes 4 P_t ein Primidealteiler des Ideals $C_k^{(ij)}$. Nach den Gleichungen (7), (18) und (21) geht P_t in $\mathfrak{p}'_j$ genau in der Potenz $P_t^{\varepsilon_{ij}}$ auf, und da die Zahl $\frac{e_i}{\varepsilon_{ij}}$ nach der Voraussetzung nicht durch p teilbar sein kann, wird die Relativdifferente $\mathfrak{A}_{k'}$ genau durch

$$P^{\frac{e_i}{\varepsilon_{ij}}-1}$$

teilbar. Da weiter die Differente δ_1 von k_1 genau durch $\mathfrak{p}_j'^{e'_j-1+\varrho'_j}$ teilbar ist, wird also δ_1 genau durch

$$P_t^{\frac{e_i}{\varepsilon_{ij}}(e'_j-1+\varrho'_j)}$$

teilbar und daher nach (30) die Körperdifferente $\mathfrak{A}$ von K genau durch

$$P_t^{E_{ij}-\frac{e_i}{\varepsilon_{ij}}+\varrho'\frac{e_i}{\varepsilon_{ij}}+\frac{e_i}{\varepsilon_{ij}}-1} = P_t^{E_{ij}-1+\varrho'_j\frac{ei}{\varepsilon_{ij}}}$$

teilbar. Da die Primzahl p nach Satz 4 genau durch $P_t^{E_{ij}}$ teilbar ist, kann man diese Resultate kurz so ausdrücken:

Die Supplementzahl des Primideals P_t ist gleich $\varrho'_j \frac{e_i}{\varepsilon_{ij}}$.

Nach (29) leitet man jetzt einfach die genaue Potenz ab, in der p in der Körperdiskriminante von K vorkommt. Es ist nämlich nach Satz 4

$$N\left(P_t^{\left(E_{ij}-1+\varrho'_j\frac{e_i}{\varepsilon_{ij}}\right)}\right)=p^{\mu_t F_{ij}\left(E_{ij}-1+\varrho'_j\frac{e_j}{\varepsilon_{ij}}\right)}$$

und man braucht also um den Exponent zu finden nur den Ausdruck

$$\mu_t F_{ij}\left(E_{ij}-1+\varrho'_j\frac{e_i}{\varepsilon_{ij}}\right)$$

über alle verschiedene Primidealteiler P_t von p in K zu summieren. Lässt man zuerst P_t alle Teiler des Ideals $C_k^{(ij)}$ durchlaufen, so erhält man nach Satz 4, indem man (28) beachtet,

$$\varepsilon_{ij} F_{ij}\left(E_{ij}-1+\varrho'_j\frac{e_i}{\varepsilon_{ij}}\right)=F_{ij}(e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i),$$

und, wenn man weiter diesen Ausdruck für $k=1, 2, \ldots, \varphi_{ij}$ summiert, kommt

$$\varphi_{ij} F_{ij}(e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i)=f_i f'_j(e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i),$$

und, wenn man zuletzt über i und j summiert, erhält man folglich die Summe

$$\sum_{i=1}^{r}\sum_{j=1}^{r'} f_i f'_j(e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i),$$

die also den gewünschten Exponenten darstellt.

Satz 5. Es wird vorausgesetzt, dass keiner der Exponenten e_i durch p teilbar ist, die Exponenten e'_j dürfen dagegen durch p teilbar sein. Dann ist die Diskriminante des zusammengesetzten Körpers genau durch

$$p^{\sum_{i=1}^{r}\sum_{j=1}^{r'} f_i f'_j (e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i)}$$

teilbar, wobei ϱ'_j die Supplementzahlen der Primidealteiler von p in k' bezeichnen.

Wie man sieht, hat man auch

$$\sum_{i=1}^{r}\sum_{j=1}^{r'} f_i f'_j(e_i e'_j-\varepsilon_{ij}+\varrho'_j e_i)=n n'+\sum_{i=1}^{r}\sum_{j=1}^{r'}(\varrho'_j e_i-\varepsilon_{ij}) f_i f'_j.$$

Aus Satz 5 folgt für den Spezialfall, dass keine unter den Zahlen e_i und e'_j durch p teilbar ist, wo also für alle j $\varrho'_j=0$ ist, der früher erwähnte Henselsche Satz.

Nimmt man an, dass die Primzahl p nicht in der Diskriminante d von k aufgeht, so ist für alle i $e_i=1$, und es folgt, dass D genau durch

$$p^{\sum_{i=1}^{r}\sum_{j=1}^{r'} f_i f'_j (e'_j-1+\varrho'_j)} = p^{n\sum_{j=1}^{r'}(e'_j-1+\varrho'_j)f'_j}$$

teilbar wird. Man kann daher sagen:

Wenn die Primzahl p nicht in der Diskriminante d von k aufgeht, und d' genau durch $p^{\sigma'}$ teilbar ist, so geht p in D genau in der Potenz $p^{n\sigma'}$ auf.

Aus dieser Bemerkung folgt sofort, dass wenn die Diskriminanten der Körper k und k' zu einander relativ prim sind,

$$D=d^{n'}\,d'^{\,n}$$

ist, wie schon von HILBERT angegeben.

Durch Anwendung der vorstehenden Resultate kann man eine Reihe von Ergebnissen über die Zusammensetzung von spezielleren Körpern finden, worauf ich jedoch nicht eingehen werde.