Ueber die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern.

Autor(en): **Gut, Max**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **4 (1932)**

PDF erstellt am: **28.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-5621

Ueber die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern

von MAX GUT, Zürich.

Es sei k ein algebraischer Zahlkörper, welcher den Körper der 5. Einheitswurzel als Unterkörper enthält, und K ein in bezug auf k relativ-ikosaedrischer Zahlkörper. In K kann man eine relativbestimmende Zahl Ξ so finden, daß ihre Relativgleichung in bezug auf k von der Form

$$(1)\qquad -[-\Xi^{20}-1+228(\Xi^{15}-\Xi^{5})-494\,\Xi^{10}]^{3} + 2^{6}3^{3}\frac{\zeta}{\nu}[\Xi(\Xi^{10}+11\Xi^{5}-1)]^{5}=0$$

ist, wobei ζ und ν ganze Zahlen von k sind, deren Quotient $\frac{\zeta}{\nu}$ durch Ξ eindeutig bestimmt ist.[1] Ist dann $\mathfrak{p}$ ein Primideal von k, so zerfällt $\mathfrak{p}$ in K in Primidealteiler $\mathfrak{P}$ vom Ften Relativgrad, und es wird in dieser Arbeit untersucht, welchen Wert F bei bekanntem ζ und ν hat, wenn $\mathfrak{p}$ zu 2, 3, 5 und zur Relativdiskriminanten von K in bezug auf k teilerfremd ist. Ich betrachte dabei zuerst den Fall, daß ζ und ν zueinander teilerfremd gewählt werden können.[2]

Es sei $\varepsilon = e^{\frac{2\pi i}{5}}$ und für $n = 0, 1, 2, 3, 4$:

$$t_n(x_1, x_2) = \varepsilon^{3n}x_1^6 + 2\varepsilon^{2n}x_1^5x_2 - 5\varepsilon^{n}x_1^4x_2^2 - 5\varepsilon^{4n}x_1^2x_2^4 - 2\varepsilon^{3n}x_1x_2^5 + \varepsilon^{2n}x_2^6$$

und

$$\frac{t_n^2(\Xi, 1)}{\Xi(\Xi^{10}+11\Xi^{5}-1)} = r_n = \frac{R_n}{\nu},$$

so genügen diese 5 Werte R_n der Gleichung 5. Grades

$$(2)\qquad F(R) = (R-3\nu)^3(R^2-11\nu R+64\nu^2)+2^6\,3^3\,\nu^4\zeta = R(R^2-10\nu R+45\nu^2)^2+2^6\,3^3\,\nu^4(\zeta-\nu)=0$$

---

[1]) *A. Speiser*, Die Theorie der Gruppen von endlicher Ordnung, Berlin 1923, S. 189. Die Größe, die Herr Speiser dort mit $\sqrt{d}$ bezeichnet, soll natürlich in k liegen.

[2]) Das kann man immer voraussetzen, wenn k ein einklassiger Körper ist, z. B. der Körper der 5. Einheitswurzel selbst. Die Tatsache, daß die Klassenzahl des Körpers der 5. Einheitswurzel gleich 1 ist, wird z. B. kurz gezeigt in *R. Fueter*, Synthetische Zahlentheorie, Berlin und Leipzig 1917, S. 222.

in bezug auf k.[3]) Umgekehrt ist Ξ eine rationale Funktion der Größen $r_n = \frac{R_n}{v}$, wobei diese rationale Funktion ihre Koeffizienten im Körper der 5. Einheitswurzel hat. Ist daher R ein beliebiger der Werte R_n, etwa gleich R_0 und $\bar{k} = \bar{k}(k, R)$, so ist K der in bezug auf k relativ-Galois'sche Körper kleinsten Relativgrades, der $\bar{k}$ als Unterkörper enthält.

Die Diskriminante von $F(R)$ berechnet sich leicht zu

$$D(F(R)) = 2^{24}\, 3^{12}\, 5^5\, \zeta^2\, v^{16}\, (\zeta - v)^2. \tag{3}$$

Sie ist wegen $\sqrt{5} = -(\varepsilon - \varepsilon^4)(\varepsilon^2 - \varepsilon^3)$ eine Quadratzahl in k.

Es möge jetzt $\mathfrak{p}$ bezw. genau in der $u.$, $v.$, $w.$ten Potenz in ζ, v, $(\zeta - v)$ aufgehen, dann ist also die Diskriminante von $F(R)$ genau durch $\mathfrak{p}^t$ teilbar, wo $t = 2u + 16v + 2w$ ist.

Ist $\mathfrak{p}$ irgend ein Primideal von k, das nicht in der Relativdiskriminanten von K in bezug auf k, folglich auch nicht in der Relativdiskriminanten von $\bar{k}$ in bezug auf k aufgeht, so hat Artin[4]) schon gezeigt, daß nur folgende 4 Möglichkeiten vorliegen:

1. Fall. $\mathfrak{p}$ ist in $\bar{k}$ Produkt von 5 Primidealen $\bar{\mathfrak{p}}$ vom 1. Relativgrade in bezug auf k. Dann ist $\mathfrak{p}$ in K ein Produkt von 60 verschiedenen Primidealen $\mathfrak{P}$ vom 1. Relativgrad in bezug auf k.

2. Fall. $\mathfrak{p}$ ist in $\bar{k}$ Produkt aus einem Primideal $\bar{\mathfrak{p}}$ vom 1. Relativgrade und zwei Primidealen $\bar{\mathfrak{p}}$ vom 2. Relativgrade in bezug auf k. Dann ist $\mathfrak{p}$ in K ein Produkt von 30 verschiedenen Primidealen $\mathfrak{P}$ vom 2. Relativgrade in bezug auf k.

3. Fall. $\mathfrak{p}$ ist in $\bar{k}$ Produkt aus 2 Primidealen $\bar{\mathfrak{p}}$ vom 1. Relativgrade und 1 Primideal $\bar{\mathfrak{p}}$ vom 3. Relativgrade in bezug auf k. Dann ist $\mathfrak{p}$ in K ein Produkt von 20 verschiedenen Primidealen $\mathfrak{P}$ vom 3. Relativgrade in bezug auf k.

4. Fall. $\mathfrak{p}$ ist in $\bar{k}$ Primideal 5. Relativgrades. Dann ist $\mathfrak{p}$ in K ein Produkt von 12 verschiedenen Primidealen $\mathfrak{P}$ vom 5. Relativgrade in bezug auf k.

---

[3]) *F. Klein,* Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom 5. Grade, Leipzig 1884, S. 101—104. Die Tetraedergruppe, unter welcher R_0 invariant ist, ist dort in der Anmerkung zu S. 26 angegeben.

[4]) *E. Artin,* Über die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann., Band 89, S. 147—156, vgl. besonders S. 154.

Liegt ferner allgemein ein algebraischer Zahlkörper k vor, und ist $s > 1$ eine beliebige natürliche Zahl, so weiß man, daß jedes normierte[5]) Primpolynom mod. $\mathfrak{p}^s$ in k mod. $\mathfrak{p}$ kongruent einer Potenz eines *einzigen* bestimmten normierten Primpolynoms mod. $\mathfrak{p}$ ist[6]). Nach der Ore'schen Theorie gelten, wenn $F(x)$ allgemein ein normiertes irreduzibles Polynom in k ist, dessen eine Wurzel einen Oberkörper K in bezug auf k festlegt, folgende beiden Sätze, von denen der erste die Anzahl r der voneinander verschiedenen Primteiler $\mathfrak{P}_i$ in K von $\mathfrak{p}$ in k und zwar noch nicht Relativgrad F_i und Relativordnung E_i von $\mathfrak{P}_i$ selbst, aber doch deren Produkt liefert, während der zweite dann E_i und F_i gibt: [7])

1. *Satz von Ore:* Ist die Diskriminante von $F(x)$ genau durch $\mathfrak{p}^t$ teilbar, ist $s > t$, und besteht in k für $F(x)$ die Zerlegung in normierte mod. $\mathfrak{p}^s$ irreduzible Faktoren

$$F(x) \equiv F_1(x)\, F_2(x) \ldots F_r(x) \qquad (\text{mod. } \mathfrak{p}^s),$$

wobei der Grad von $F_i(x)$ gleich N_i ist, so hat das Primideal $\mathfrak{p}$ in K die Primidealzerlegung

$$\mathfrak{p} = \mathfrak{P}_1^{E_1}\, \mathfrak{P}_2^{E_2} \ldots \mathfrak{P}_r^{E_r},$$

wobei die Relativnorm von $\mathfrak{P}_i^{E_i}$ in bezug auf k gleich $\mathfrak{p}^{N_i}$ ist.

2. *Satz von Ore:* Ist $F_i(x)$ der entsprechende mod. $\mathfrak{p}^s$ irreduzible Faktor eines Primideales $\mathfrak{P}_i$ des 1. Satzes, und teilt $\mathfrak{p}^{t_i}$ genau die Diskriminante von $F_i(x)$, zerlegt man schließlich $F_i(x)$ weiter in mod. $\mathfrak{p}^s$ irreduzible normierte Faktoren

$$F_i(x) \equiv F_i(x, y_1)\, F_i(x, y_2) \ldots F_i(x, y_{Fi}) \; [\text{modd. } \mathfrak{p}^s, \Phi_i(y)], \; s > 2t_i,$$

wobei $\Phi_i(y)$ ein beliebiges Primpolynom (mod. $\mathfrak{p}$) vom $N_i$ten Grade in k ist, so hat $\mathfrak{P}_i$ dann die relative Ordnungszahl E_i und die relative Gradzahl F_i in bezug auf k, wo E_i die gemeinsame Gradzahl in x der F_i Faktoren der rechten Seite der letzten Kongruenz ist.

Ist daher im folgenden $\mathfrak{p}$ ein zu 2, 3, 5 und zur Relativdiskriminanten des relativ-ikosaedrischen Körpers K in bezug auf k teilerfremdes Primideal von k, so gilt wegen der Struktur von $F'(R)$, bezw. $G'(S)$:

---

[5]) „normiert" bedeutet: Mit höchstem Koeffizienten 1. Die Polynome sollen hier natürlich immer ganze Zahlen von k als Koeffizienten haben.

[6]) Vgl. z. B. S. 321—322 von *Ö. Ore*, Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, Math. Ann., Band 96, S. 313—352 und Band 97, S. 569—598.

[7]) l. c., S. 592, bezw. 594.

A. wenn $u = v = w = 0$ ist
die folgende Vorschrift: man lasse R in

$$\overline{F}(R) = (R - 3v)^3 (R^2 - 11vR + 64v^2)$$

ein vollständiges System von $n(\mathfrak{p}) = p^f$ mod. $\mathfrak{p}$ inkongruenten ganzen Zahlen von k durchlaufen. Damit dann $\mathfrak{p}$ in K in Primideale $\mathfrak{P}$ vom Ften Relativgrade zerfällt, ist notwendig und hinreichend, daß, falls bezw. $F = 1, 2, 3, 5$ sein soll, genau bezw. 5, 1, 2 oder keine dieser Zahlen R die Eigenschaft haben, daß

$$\overline{F}(R) \equiv -2^6 3^3 v^4 \zeta \pmod{\mathfrak{p}}.$$

B. Es sei jetzt $u > 0$ und -3 quadratischer Rest mod. $\mathfrak{p}$.
Dann gibt es zwei ganze Zahlen σ und τ in k, sodaß

$$\left.\begin{aligned} \frac{11}{2} + \frac{3\sqrt{5}\sqrt{-3}}{2} &\equiv \sigma \\ \frac{11}{2} - \frac{3\sqrt{5}\sqrt{-3}}{2} &\equiv \tau \end{aligned}\right\} \pmod{\mathfrak{p}^{t+1}}$$

und, wie man sofort sieht, ist $\sigma \not\equiv \tau$, $\sigma \not\equiv 3$, $\tau \not\equiv 3 \pmod{\mathfrak{p}}$, und $F(R) \equiv (R - 3v)^3 (R - \sigma v)(R - \tau v) + 2^6 3^3 v^4 \zeta \pmod{\mathfrak{p}^{t+1}}$.

Soll für $R \equiv 3v \pmod{\mathfrak{p}}$ das Polynom $F(R) \equiv 0 \pmod{\mathfrak{p}^{t+1}}$ sein, so muß diese Kongruenz a fortiori mod. $\mathfrak{p}^u$ gelten, also muß, falls $u = 3(x-1) + y$, $1 \leqq y \leqq 3$, $1 \leqq x$ ist, R von der Form sein:

$$R = 3v + \alpha \pi^x,$$

wo π hier und weiter unten immer eine Hensel'sche Primzahl in bezug auf das Primideal $\mathfrak{p}$ bedeutet, d. h. $\pi \equiv 0 \pmod{\mathfrak{p}}$, $\pi \not\equiv 0 \pmod{\mathfrak{p}^2}$. Dann wird $F(R) \equiv \alpha^3 \pi^{3x} (\alpha^2 \pi^{2x} - 5\alpha v \pi^x + 40 v^2) + 2^6 3^3 v^4 \zeta \pmod{\mathfrak{p}^{t+1}}$. Ist $y \neq 3$, so kann kein R von dieser Form gefunden werden, sodaß

$$F(R) \equiv 0 \pmod{\mathfrak{p}^{t+1}}.$$

Daher ist die Zerlegung in normierte mod. $\mathfrak{p}^{t+1}$ irreduzible Faktoren im Sinne des 1. Satzes der Ore'schen Theorie von der Form:

$$F(R) \equiv F_1(R) F_2(R) F_3(R) \pmod{\mathfrak{p}^{t+1}},$$

wobei

$$\left.\begin{aligned} F_1(R) &\equiv R - \sigma\nu \\ F_2(R) &\equiv R - \tau\nu \\ F_3(R) &\equiv (R - 3\nu)^3 \end{aligned}\right\} \text{(mod. } \mathfrak{p}\text{)}.$$

Da die Relativordnung jedes Primteilers $\bar{\mathfrak{p}}$ in $\bar{k}$ von $\mathfrak{p}$ gleich 1 sein muß, ist

$$\mathfrak{p} = \bar{\mathfrak{p}}_1\,\bar{\mathfrak{p}}_2\,\bar{\mathfrak{p}}_3,\quad n(\bar{\mathfrak{p}}_1) = n(\bar{\mathfrak{p}}_2) = \mathfrak{p},\quad n(\bar{\mathfrak{p}}_3) = \mathfrak{p}^3,$$

wo n die Relativnorm von $\bar{k}$ in bezug auf k bedeutet, und mithin:

$$F = 3 \quad (u \text{ nicht durch } 3 \text{ teilbar}).$$

Ist $y = 3$, so muß offenbar $(\alpha, \mathfrak{p}) = 1$ sein. Dann kann man in k ein ganzes, zu $\mathfrak{p}$ teilerfremdes γ so bestimmen, daß

$$\zeta \equiv \gamma\,\pi^{3x} \text{ (mod. } \mathfrak{p}^{6x+1}\text{)},$$

und es wird

$$F(R) \equiv \pi^{3x}\,[\alpha^3\,(\alpha^2\,\pi^{2x} - 5\nu\,\alpha\,\pi^x + 40\nu^2) + 2^6\,3^3\,\nu^4\,\gamma] \text{ (mod. } \mathfrak{p}^{6x+1}\text{)}.$$

Dann ergibt sich leicht folgende Vorschrift:

Man lasse in

$$\overline{\overline{F}}(T) = \pi^{2x}\,T^5 - 5\nu\,\pi^x\,T^4 + 40\nu^2\,T^3$$

T ein vollständiges System von $\varphi(\mathfrak{p}^{3x+1})$ (mod. $\mathfrak{p}^{3x+1}$) inkongruenten und zu $\mathfrak{p}$ teilerfremden ganzen Zahlen von k durchlaufen. Dann zerfällt $\mathfrak{p}$ in K in Primideale vom Ften Relativgrad, wo $F = 1$ oder $F = 3$ ist, je nachdem genau 3 oder keine dieser Zahlen T die Eigenschaft haben, daß

(4) $$\overline{\overline{F}}(T) \equiv -2^6\,3^3\,\nu^4\,\gamma \text{ (mod. } \mathfrak{p}^{3x+1}\text{)}.$$

C. Es sei jetzt $u > 0$ und -3 quadratischer Nichtrest mod. $\mathfrak{p}$.

Dann ist

$$R^2 - 11\nu\,R + 64\nu^2$$

ein Primpolynom mod. $\mathfrak{p}$ und daher a fortiori mod. $\mathfrak{p}^{t+1}$. Da die Rela-

tivordnung jedes Primideals in bezug auf k gleich 1 sein muß, so hat $\mathfrak{p}$ in $\bar{k}$ einen Primteiler $\bar{\mathfrak{p}}$ vom Relativgrade 2: $n(\bar{\mathfrak{p}}) = \mathfrak{p}^2$, mithin muß nach den Sätzen von Ore und Artin $F = 2$ sein.

Dieser Fall ist übrigens nur möglich, wenn u durch 3 teilbar ist, und die Kongruenz (4) hat dann genau *eine* Lösung.

D. Es sei jetzt $w > 0$ und -1 quadratischer Rest mod. $\mathfrak{p}$.

Dann gibt es zwei ganze Zahlen σ und τ in k, sodaß

$$\left.\begin{aligned} 5 + 2\sqrt{5}\sqrt{-1} &\equiv \sigma \\ 5 - 2\sqrt{5}\sqrt{-1} &\equiv \tau \end{aligned}\right\} \pmod{\mathfrak{p}^{t+1}},$$

und es ist, wie man sofort sieht, $\sigma \not\equiv \tau$, $\sigma \not\equiv 0$, $\tau \not\equiv 0 \pmod{\mathfrak{p}}$, und

$$F(R) \equiv R(R - \sigma\nu)^2 (R - \tau\nu)^2 + 2^6 3^3 \nu^4 (\zeta - \nu) \pmod{\mathfrak{p}^{t+1}}.$$

Soll für $R \equiv \sigma\nu \pmod{\mathfrak{p}}$ das Polynom $F(R) \equiv 0 \pmod{\mathfrak{p}^{t+1}}$ sein, so muß diese Kongruenz a fortiori mod. $\mathfrak{p}^w$ gelten, mithin muß, falls $w = 2(x-1) + y$, $1 \leqq y \leqq 2$, $1 \leqq x$ ist, R von der Form sein

$$R = \sigma\nu + \alpha\pi^x.$$

Dann wird

$$F(R) \equiv \alpha^2 \pi^{2x} (\sigma\nu + \alpha\pi^x)\left((\sigma-\tau)\nu + \alpha\pi^x\right)^2 + 2^6 3^3 \nu^4 (\zeta - \nu) \pmod{\mathfrak{p}^{t+1}}.$$

Ist $y \neq 2$, so kann kein R von dieser Form gefunden werden, daß

$$F(R) \equiv 0 \pmod{\mathfrak{p}^{t+1}}.$$

Daher ist in diesem Falle die Zerlegung in normierte, mod. $\mathfrak{p}^{t+1}$ irreduzible Faktoren im Sinne des 1. Satzes des Ore'schen Theorie von der Form:

$$F(R) \equiv F_1(R)\, F_2(R)\, F_3(R) \pmod{\mathfrak{p}^{t+1}},$$

wobei

$$\left.\begin{aligned} F_1(R) &\equiv R \\ F_2(R) &\equiv (R - \sigma\nu)^2 \\ F_3(R) &\equiv (R - \tau\nu)^2 \end{aligned}\right\} \pmod{\mathfrak{p}}$$

und folglich muß $\mathfrak{p} = \bar{\mathfrak{p}}_1\, \bar{\mathfrak{p}}_2\, \bar{\mathfrak{p}}_3$, $n(\bar{\mathfrak{p}}_1) = \mathfrak{p}$; $n(\bar{\mathfrak{p}}_2) = n(\bar{\mathfrak{p}}_3) = \mathfrak{p}^2$, also

$$F = 2 \quad (w \text{ nicht durch } 2 \text{ teilbar})$$

sein.

Ist $y = 2$, so muß offenbar $(\alpha, \mathfrak{p}) = 1$ sein. Dann kann man in k ein ganzes, zu $\mathfrak{p}$ teilerfremdes γ so bestimmen, daß

$$\zeta - \nu \equiv \gamma \pi^{2x} \pmod{\mathfrak{p}^{4x+1}},$$

und es wird

$$F(R) \equiv \pi^{2x} [\alpha^2 (\alpha^3 \pi^{3x} + (5\sigma - 20)\nu \alpha^2 \pi^{2x} + (20\sigma - 260)\nu^2 \alpha \pi^x - 80\sigma\nu^3) + 2^6 3^3 \nu^4 \gamma] \pmod{\mathfrak{p}^{4x+1}}.$$

Dann ergibt sich leicht folgende Vorschrift:
Man lasse in

$$\overline{\overline{\overline{F}}}(T) = (5\sigma - 20)\nu \pi^{2x} T^4 + (20\sigma - 260)\nu^2 \pi^x T^3 - 80\sigma \nu^3 T^2$$

T ein vollständiges System von $\varphi(\mathfrak{p}^{2x+1})$ mod. $\mathfrak{p}^{2x+1}$ inkongruenter und zu $\mathfrak{p}$ teilerfremder ganzer Zahlen durchlaufen. Dann zerfällt $\mathfrak{p}$ in K in Primideale vom Ften Relativgrad in bezug auf k, wo $F = 1$ oder $F = 2$ ist, je nachdem genau 2 oder keine dieser Zahlen T die Eigenschaft haben, daß

$$\overline{\overline{\overline{F}}}(T) \equiv -2^6 3^3 \nu^4 \gamma \pmod{\mathfrak{p}^{2x+1}}.$$

E. Es sei jetzt $w > 0$ und -1 quadratischer Nichtrest mod. $\mathfrak{p}$.

Dann ist

$$R^2 - 10\nu R + 45\nu^2$$

ein Primpolynom mod. $\mathfrak{p}$, und mithin a fortiori mod. $\mathfrak{p}^{t+1}$. Da die Relativordnung jedes Primideales gleich 1 sein muß, und es keine Primideale $\bar{\mathfrak{p}}$ in $\bar{k}$ geben kann, deren Relativgrad $\bar{f} = 4$ ist, so ist die Zerlegung in normierte, mod. $\mathfrak{p}^{t+1}$ irreduzible Faktoren im Sinne des 1. Satzes der Ore'schen Theorie von der Form:

$$F(R) \equiv F_1(R)\, F_2(R)\, F_3(R) \pmod{\mathfrak{p}^{t+1}},$$

wobei

$$\left.\begin{aligned} F_1(R) &\equiv R \\ F_2(R) \equiv F_3(R) &\equiv R^2 - 10\nu R + 45\nu^2 \end{aligned}\right\} (\text{mod. } \mathfrak{p}),$$

und daher $\mathfrak{p} = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \bar{\mathfrak{p}}_3$, $n(\bar{\mathfrak{p}}_1) = \mathfrak{p}$; $n(\bar{\mathfrak{p}}_2) = n(\bar{\mathfrak{p}}_3) = \mathfrak{p}^2$, also muß $F = 2$ sein.

F. Es sei endlich $v > 0$.

Setzt man jetzt

$$R = 3\nu + \frac{12\nu\zeta}{S},$$

so erhält man die Resolvente

$$G(S) = S^5 + 4\nu\zeta^2(10S^2 - 15\zeta S + 36\zeta^2) = 0,$$

deren Diskriminante gleich

$$D[G(S)] = 2^{16}\, 3^8\, 5^5\, \zeta^{14}\nu^4(\zeta - \nu)^2$$

ist. Für diese Resolvente ist also $t = 14u + 4v + 2w$.

Wir fragen: Kann $G(S) \equiv 0 \pmod{\mathfrak{p}^{t+1}}$ sein, also die Zerlegung in normierte mod. $\mathfrak{p}^{t+1}$ irreduzible Faktoren einen Linearfaktor haben? Es muß für ein solches S a fortiori die Kongruenz gelten:

$$G(S) \equiv S^5 \equiv 0 \pmod{\mathfrak{p}^v}.$$

Wir bringen v in die Form $v = 5(x-1) + y$, wo $1 \leqq y \leqq 5$ ist und $1 \leqq x$. Es muß dann also notwendigerweise

$$S \equiv 0 \pmod{\mathfrak{p}^x}$$

sein. Mithin ist S von der Form $S = \alpha\pi^x + \beta\pi^{x+1}$, wobei α und β zwei ganze Zahlen aus k sind. Dann wird:

$$\begin{aligned} &G(\alpha\pi^x + \beta\pi^{x+1}) = \\ &= [\alpha^5\pi^{5x} + 5\alpha^4\beta\pi^{5x+1} + 10\alpha^3\beta^2\pi^{5x+2} + 10\alpha^2\beta^3\pi^{5x+3} + 5\alpha\beta^4\pi^{5x+4} + \beta^5\pi^{5x+5}] + \\ &+ 4\nu\zeta^2[10\alpha^2\pi^{2x} + 20\alpha\beta\pi^{2x+1} + 10\beta^2\pi^{2x+2} - 15\zeta\alpha\pi^x - 15\zeta\beta\pi^{x+1} \\ &\qquad + 36\zeta^2] \end{aligned}$$

Soll $G(\alpha\,\pi^x + \beta\,\pi^{x+1}) \equiv 0 \pmod{\mathfrak{p}^{v+1}}$ gelten, so muß

$$G(\alpha\,\pi^x + \beta\,\pi^{x+1}) \equiv \alpha^5\,\pi^{5x} + 144\,\nu\,\zeta^4 \equiv 0 \pmod{\mathfrak{p}^{5(x-1)+y+1}}$$

sein. Diese Kongruenz ist aber nicht erfüllbar für $y \neq 5$. Ist mithin v nicht durch 5 teilbar, so kann die Zerlegung in normierte mod. $\mathfrak{p}^{4v+1}$ irreduzible Faktoren nur von einer der beiden Formen sein:

$$\left.\begin{array}{l} G(S) \equiv G_1(S) \\ \text{oder} \qquad G(S) \equiv G_2(S)\,G_3(S) \end{array}\right\} \pmod{\mathfrak{p}^{4v+1}},$$

wo $G_1(S)$ in S vom Grade 5, $G_2(S)$ vom Grade 2 und $G_3(S)$ vom Grade 3 ist. Der letzte Fall ist auszuschließen, weil F durch 6 teilbar sein müßte, mithin bleibt nur der erste, und da die Relativordnung immer gleich 1 sein soll, muß

$$F = 5 \quad (v \text{ nicht durch } 5 \text{ teilbar})$$

sein.

Es bleibt der Fall, wo $v = 5x \geqq 5$ ist. Dann kann man in k ein ganzes zu $\mathfrak{p}$ teilerfremdes γ so bestimmen, daß

$$\nu \equiv \gamma\,\pi^{5x} \pmod{\mathfrak{p}^{20x+1}}$$

ist. Soll $G(\alpha\,\pi^x + \beta\,\pi^{x+1}) \equiv 0 \pmod{\mathfrak{p}^{20x+1}}$ sein, so sieht man, daß $(\alpha, \mathfrak{p}) = 1$ sein muß, d. h. soll also für ein S aus k die Kongruenz $G(S) \equiv 0 \pmod{\mathfrak{p}^{20x+1}}$ gelten, so muß S die Form haben: $S = \alpha\,\pi^x$, wo α zu $\mathfrak{p}$ teilerfremd ist. Dann ergibt sich leicht folgende Vorschrift:

Man lasse T in

$$\overline{G}(T) = T^5 + 40\,\gamma\,\zeta^2\,\pi^{2x}T^2 - 60\,\gamma\,\zeta^3\,\pi^x\,T$$

ein vollständiges System von $\varphi(\mathfrak{p}^{15x+1})$ mod. $\mathfrak{p}^{15x+1}$ inkongruenter und zu $\mathfrak{p}$ teilerfremder ganzer Zahlen von k durchlaufen. Damit $\mathfrak{p}$ in K in Primideale vom Ften Relativgrad zerfällt, ist notwendig und hinreichend, falls bezw. $F = 1, 2, 3, 5$ sein soll, genau 5, 1, 2 oder keine dieser Zahlen T die Eigenschaft haben, daß

$$\overline{G}(T) \equiv -144\,\gamma\,\zeta^4 \pmod{\mathfrak{p}^{15x+1}}.$$

Es ist übrigens

$$\overline{G}'(T) = 5T^4 + 80\gamma\,\zeta^2\,\pi^{2x}\,T - 60\gamma\,\zeta^3\,\pi^x,$$

und mithin kann für kein zu $\mathfrak{p}$ teilerfremdes T

$$\overline{G}'(T) \equiv 0 \pmod{\mathfrak{p}}$$

sein.

Nach der gleichen Methode lassen sich offenbar auch die Fälle erledigen, wo ζ und ν gemeinschaftliche Idealteiler $\mathfrak{p}$ haben. Denn ist $\mathfrak{p}^s$ die höchste Potenz von $\mathfrak{p}$, die sowohl in ζ wie in ν aufgeht, so kürze man $\frac{\zeta}{\nu}$ mit $\mathfrak{p}^s$, erweitere den entstehenden Bruch mit einem zu $\mathfrak{p}$ teilerfremden Ideale, das in der gleichen Nebenidealklasse wie $\mathfrak{p}^s$ liegt, und führe dann die Betrachtung mod. $\mathfrak{p}$ durch. Offenbar ist jetzt noch die Existenz solcher Primideale, die zwar $D[F(R)]$, aber nicht die Relativdiskriminante von K in bezug auf k teilen, ferner die Primidealzerlegung der Ideale, die die letztere oder 2, 3 oder 5 teilen, zu untersuchen. Ich hoffe dies in einer ausführlichen Arbeit zu tun, prinzipiell reichen hiebei ja die beiden Ore'schen Sätze in Verbindung mit den Hilbert'schen Sätzen über die Primidealzerlegung in den Galois'schen Körpern und die Dedekind'schen Sätze über die Primidealzerlegung in deren Unterkörpern aus. Immerhin wirft schon der Fall A, weil er doch immer für alle außer den endlich vielen Primidealen, welche $D[F(R)]$ teilen und für alle hier betrachteten Grundkörper k gilt, viel Licht auf das Problem, durch reine Kongruenzen die Zerfällung der Primideale in einem relativ-ikosaedrischen Körper zu charakterisieren.

Man kann leicht auf Grund unserer Resultate und einer Überlegung, wie sie Herr Speiser in einer seiner Arbeiten gemacht hat[8]), Gleichungen 5. Grades von der Form (2) oder Gleichungen 60. Grades von der Form (1) hinschreiben, deren Gruppe die Ikosaedergruppe, und nicht etwa eine eigentliche Untergruppe derselben ist. Wir zeigen das Verfahren kurz an einem Beispiel. Wenn etwa k gleich dem Körper der 5. Einheitswurzel selbst ist, und man z. B. einen relativ-ikosaedrischen Körper haben will, für welchen $\nu = 1$ ist, so sieht man rasch, daß wenn man etwa $\zeta \equiv -4 \pmod{11}$ wählt und $\mathfrak{p}$ ein Primteiler von 11 in k ist[9]), daß die Kongruenz:

[8]) *A. Speiser*, Die Zerlegung von Primzahlen in algebraischen Zahlkörpern. Transactions of the American Mathematical Society vol. 23, No. 2, 1922, S. 177 unten.

[9]) Man beachte, daß alle Primideale $\mathfrak{p}$ des Körpers der 5. Einheitswurzel, die eine Primzahl von der Form $p = 10n + 1$ teilen, in diesem Grundkörper den absoluten Grad $f = 1$ haben, also 0, 1, 2 ... $10n$ ein vollständiges Restsystem mod. $\mathfrak{p}$ inkongruenter Zahlen bilden.

$$F(R) \equiv 0 \pmod{\mathfrak{p}}$$

keine Lösung R in k hat. Ebenso sieht man leicht ein, daß $F(R)$ mod $\mathfrak{p}$ nicht in einen Faktor 2. Grades und einen Faktor 3. Grades in k zerfallen kann. Mithin wird $\mathfrak{p}$ in k nach dem 1. Ore'schen Satze und weil es nicht in $D[F(R)]$ aufgehen kann, ein Primideal $\bar{\mathfrak{p}}$ vom 5. Relativgrad in bezug auf k. Setzt man jetzt etwa $\zeta \equiv -4 \pmod{31}$, so sieht man sofort, daß wenn $\mathfrak{p}$ ein Primteiler von 31 in k ist, die Kongruenz:

$$F(R) \equiv 0 \pmod{\mathfrak{p}}$$

n k genau nur die Lösungen $R \equiv -7$ und $R \equiv -9 \pmod{\mathfrak{p}}$ hat, und daher in $\bar{k}$ nach dem 1. Ore'schen Satze so zerfällt: $\mathfrak{p} = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \bar{\mathfrak{p}}_3$, wobei $\bar{\mathfrak{p}}_1$ und $\bar{\mathfrak{p}}_2$ vom 1., dagegen $\bar{\mathfrak{p}}_3$ vom 3. Relativgrade in bezug auf k sind. Da die Diskriminante $D[F(R)]$ ein vollständiges Quadrat in k ist und anderseits die Ikosaedergruppe keine Untergruppen von der Ordnung 15 oder 30 hat, muß die Gruppe der Gleichung die Ikosaedergruppe sein. Also definiert z. B.

$$-4 = \frac{[-\Xi^{20} - 1 + 228(\Xi^{15} - \Xi^{5}) - 494\,\Xi^{10}]^3}{2^6\,3^3\,[\Xi(\Xi^{10} + 11\,\Xi^{5} - 1)]^5}$$

einen zum Körper der 5. Einheitswurzel relativ-ikosaedrischen Zahlkörper. Von ihm können wir leicht die Zerlegung aller zu 2, 3 und 5 teilerfremden Primideale nach Vorschrift A angeben, weil dann nach (3 immer $u = v = w = 0$ ist.

(Eingegangen den 17. Februar 1932)