Weitere Untersuchungen über die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern.

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

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **6 (1934)**

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-7579

Weitere Untersuchungen über die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern

Von MAX GUT, New Haven, Conn., U.S.A.

Es sei k ein algebraischer Zahlkörper, welcher den Körper der 5. Einheitswurzeln enthält. Ist K ein algebraischer Erweiterungskörper, dessen Relativgruppe die Ikosaedergruppe ist, so kann man immer — event. muß man noch voraussetzen, daß eine gewisse Quadratwurzel in k liegt — in K eine relativbestimmende Zahl Ξ so finden, daß ihre Relativgleichung in bezug auf k von der Form:

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

ist, wo ζ und ν zwei ganze Zahlen von k sind. In einer im Festband zu Ehren des Internationalen Mathematiker-Kongresses Zürich 1932 erschienenen Note[1]) habe ich eine Methode angegeben zur Bestimmung der Primidealzerlegung der Primideale $\mathfrak{p}$ von k in K[2]). In der vorliegenden Arbeit habe ich nun einen Teil der Untersuchungen durchgeführt. Ist $\mathfrak{p}$ irgend ein zum Relativgrade 60 teilerfremdes Primideal von k, so können wir die Anzahl R der voneinander verschiedenen Primteiler $\mathfrak{P}$ in K von $\mathfrak{p}$, ihren gemeinsamen Relativgrad F und ihre gemeinsame Relativordnung E angeben. Diese Zerfällung hängt nur ab von der in (1) auftretenden Größe

$$\varkappa=2^{6}3^{3}\frac{\zeta}{\nu}$$

des Grundkörpers.

Als Korollar ergibt sich die notwendige und hinreichende Bedingung dafür, daß in der Relativdiskriminanten von K in bezug auf k kein zum

[1]) Commentarii Mathematici Helvetici, Band 4, S. 219, im folgenden zitiert mit *N.*

[2]) Unter der Voraussetzung, daß man schon weiß, daß $\mathfrak{p}$ unverzweigt und zum Relativgrade 60 teilerfremd ist, wurde in *N.* beiläufig auf Grund einer Bemerkung Artin's auch schon der Relativgrad der Primidealteiler von $\mathfrak{p}$ angegeben. Wir werden aber hier viel einfachere Kriterien erhalten, weil, wie wir es in *N.*, S. 228 vermuteten, Primidealteiler von $D[F(R)]$ in vielen Unterfällen nicht unverzweigt sein können.

Relativgrad teilerfremdes Primideal $\mathfrak{p}$ von k auftritt. Man kann nämlich bei der Untersuchung nach einem bestimmten solchen Primideale $\mathfrak{p}$ immer voraussetzen, daß es nicht zugleich im Zähler und Nenner von x auftritt[3]), und wir wollen hier immer annehmen, daß man x auf diese Form gebracht habe. Dann teilt $\mathfrak{p}$ dann und nur dann die Relativdiskriminante *nicht*, wenn folgende drei Bedingungen gleichzeitig erfüllt sind:[4])

1. Der Exponent der Potenz, in der $\mathfrak{p}$ im Zähler von x aufgeht, muß durch 3 teilbar sein.
2. Der Exponent der Potenz, in der $\mathfrak{p}$ im Zähler von $x-2^6\,3^3$ aufgeht, muß durch 2 teilbar sein.
3. Der Exponent der Potenz, in der $\mathfrak{p}$ im Nenner von x aufgeht, muß durch 5 teilbar sein.

Ohne weiter darauf einzugehen, möchte ich hier nur darauf hinweisen, daß dieses Resultat offensichtlich in enger Beziehung steht zu der Formel (63), S. 60 des Klein'schen Ikosaederbuches, wobei zu beachten ist, daß die Nullstellen der dort auftretenden Formen f, H und T die Fixpunkte der Ikosaedersubstitutionen von den Perioden 5, bezw. 3, bezw. 2 sind.

§ 1.

Es sei zunächst in diesem und im nächsten Abschnitt k irgend ein algebraischer Zahlkörper, der also die 5. Einheitswurzeln nicht zu enthalten braucht, und K ein in bezug auf k relativ-ikosaedrischer Zahlkörper. Die Relativgruppe ist also die Ikosaedergruppe $\mathfrak{G}$. Sie hat im ganzen folgende 59 Untergruppen[5]):

Die Ikosaedergruppe $\mathfrak{G}$ von der Ordnung 60 selbst.

5	gleichberechtigte	Tetraedergruppen	$\mathfrak{T}$	von	der	Ordnung	12
6	„	Diedergruppen	$\mathfrak{D}_{10}$	„	„	„	10
10	„	„	$\mathfrak{D}_6$	„	„	„	6
5	„	„	$\mathfrak{D}_4$	„	„	„ (Vierergruppen)	4
6	„	zyklische Gruppen	$\mathfrak{C}_5$	„	„	Ordnung	5
10	„	„ „	$\mathfrak{C}_3$	„	„	„	3
15	„	„ „	$\mathfrak{C}_2$	„	„	„	2

und die Identität 1.

---

[3]) *N.*, S. 228.

[4]) Eine irreduzible Gleichung, welche diese Bedingung erfüllt, ist z. B. in *N.*, S. 229 angegeben.

[5]) Vgl. Ikosaederbuch, § 8, S. 16 ff., oder auch *Speiser*, Die Theorie der Gruppen von endlicher Ordnung, Berlin 1923, S. 10.

Wir bezeichnen mit f den absoluten Grad, mit e die absolute Ordnung eines Primideales $\mathfrak{p}$ des Grundkörpers k, welches die rationale (positive) Primzahl p teilt. Wir bezeichnen ferner mit $\mathfrak{Z}$ die relative Zerlegungsgruppe, mit $\mathfrak{T}$ die relative Trägheitsgruppe und mit $\mathfrak{V}$ die relative Verzweigungsgruppe eines Primteilers $\mathfrak{P}$ in K von $\mathfrak{p}$ in bezug auf k.

Auf Grund der Hilbert'schen Sätze über die Primidealzerlegung in relativ-Galois'schen Zahlkörpern und der Struktur der Ikosaedergruppe ergeben sich dann in bezug auf die Werte R (Anzahl der voneinander verschiedenen Primteiler $\mathfrak{P}$ in K von $\mathfrak{p}$), F (Relativgrad von $\mathfrak{P}$ in bezug auf k) und E (Relativordnung von $\mathfrak{P}$ in bezug auf k)[6]) folgende 15 möglichen Typen:

α) Zunächst kann die Zerlegungsgruppe $\mathfrak{Z}$ nicht die Ikosaedergruppe $\mathfrak{G}$ selbst sein, denn $\mathfrak{G}$ ist nicht auflösbar, während $\mathfrak{Z}$ auflösbar ist. *Kein Primideal bleibt also unzerlegt.*

β) Wir fragen uns, ob $\mathfrak{Z}$ gleich einer Tetraedergruppe $\mathfrak{T}$ sein kann? Dann müßte die Trägheitsgruppe $\mathfrak{T}$ entweder gleich $\mathfrak{T}$ oder einer $\mathfrak{D}_4$ sein, denn das sind die einzigen Normalteiler von $\mathfrak{T}$ mit zyklischer Faktorgruppe. Aus der ersten Annahme $\mathfrak{Z} = \mathfrak{T} = \mathfrak{T}$ folgt, daß $\mathfrak{V}$ aus dem gleichen Grunde entweder gleich $\mathfrak{T}$ oder einer $\mathfrak{D}_4$ ist. Anderseits ist die Ordnung von $\mathfrak{V}$ eine Potenz von p. Also ist nur der Fall möglich:

1. $\mathfrak{Z}=\mathfrak{T}$, $\mathfrak{T}=\mathfrak{T}$, $\mathfrak{V}=\mathfrak{D}_4$; $R=5$, $F=1$, $E=12$, $E_0=3$; $\mathfrak{p}|2$; $2^f \equiv 1 \pmod 3$.

Aus der zweiten Annahme $\mathfrak{Z} = \mathfrak{T}$, $\mathfrak{T} = \mathfrak{D}_4$ folgt, weil $\mathfrak{D}_4$ oder eine $\mathfrak{C}_2$ die einzigen Normalteiler von $\mathfrak{D}_4$ mit zyklischer Faktorgruppe sind, daß die Ordnung von $\mathfrak{V}$ eine durch 2 teilbare Zahl ist. Also muß $\mathfrak{p}$ ein Teiler von 2 sein, und da E_0 dann zu 2 teilerfremd sein muß:

2. $\mathfrak{Z} = \mathfrak{T}$, $\mathfrak{T} = \mathfrak{D}_4$, $\mathfrak{V} = \mathfrak{D}_4$; $R = 5$, $F = 3$, $E = 4$, $E_0 = 1$; $\mathfrak{p} \mid 2$.

γ) Kann die Zerlegungsgruppe gleich einer $\mathfrak{D}_{2n}$ sein, wo $n = 5, 3, 2$ ist? Dann müßte die Trägheitsgruppe entweder gleich $\mathfrak{D}_{2n}$ oder gleich der, bezw. für $n = 2$ einer in ihr enthaltenen $\mathfrak{C}_n$ sein, denn das sind die einzigen Normalteiler von $\mathfrak{D}_{2n}$ mit zyklischer Faktorgruppe. Im ersten Fall $\mathfrak{Z} = \mathfrak{T} = \mathfrak{D}_{2n}$ folgt aus demselben Grunde und weil die Ordnung von $\mathfrak{V}$ eine Primzahlpotenz ist, für $n = 5$ und 3, daß dann $\mathfrak{V} = \mathfrak{C}_n$ sein

[6]) Mit E_0 bezeichnen wir ferner, wie üblich, die Ordnung der Faktorgruppe $\mathfrak{T}/\mathfrak{V}$, wir wollen aber die Unterfälle mit gleichen R, F und E, aber verschiedenem E_0 nicht besonders zählen.

muß, für $n = 2$ wegen $(E_0, 2) = 1$, daß $\mathfrak{V} = \mathfrak{D}_4$ sein muß. Das ist nur für die Primteiler $\mathfrak{p}$ von n möglich. Im zweiten Falle $\mathfrak{Z} = \mathfrak{D}_{2n}$, $\mathfrak{T} = \mathfrak{C}_n$, muß $\mathfrak{V} = \mathfrak{C}_n$ oder $\mathfrak{V} = 1$ sein. Der erste Unterfall $\mathfrak{Z} = \mathfrak{D}_{2n}$, $\mathfrak{T} = \mathfrak{V} = \mathfrak{C}_n$ ist nur für die Primteiler $\mathfrak{p}$ von n möglich, der zweite Unterfall $\mathfrak{Z} = \mathfrak{D}_{2n}$, $\mathfrak{T} = \mathfrak{C}_n$, $\mathfrak{V} = 1$ nur für die zu n teilerfremden Primteiler $\mathfrak{p}$ möglich, für welche $p^{2f} \equiv 1 \pmod{n}$ ist. Für $n = 5, 3, 2$ ergeben sich so folgende Unterfälle:

3. $\mathfrak{Z} = \mathfrak{D}_{10}$, $\mathfrak{T} = \mathfrak{D}_{10}$, $\mathfrak{V} = \mathfrak{C}_5$; $R = 6$, $F = 1$, $E = 10$, $E_0 = 2$; $\mathfrak{p} | 5$.

Die Kongruenz $5^f \equiv 1 \pmod{2}$ bildet keine Forderung und ist daher weggelassen.

4. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{D}_{10}, & \mathfrak{T} = \mathfrak{C}_5, & \mathfrak{V} = \mathfrak{C}_5 \\ \mathfrak{Z} = \mathfrak{D}_{10}, & \mathfrak{T} = \mathfrak{C}_5, & \mathfrak{V} = 1 \end{matrix}\right\} R = 6, F = 2, E = 5 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 5. \\ E_0 = 5 ; p^{2f} \equiv 1 \pmod{5}. \end{matrix}\right.$

5. $\mathfrak{Z} = \mathfrak{D}_6$, $\mathfrak{T} = \mathfrak{D}_6$, $\mathfrak{V} = \mathfrak{C}_3$; $R = 10$, $F = 1$, $E = 6$, $E_0 = 2$; $\mathfrak{p} | 3$.

Die Kongruenz $3^f \equiv 1 \pmod{2}$ bildet keine Forderung und ist daher weggelassen.

6. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{D}_6, & \mathfrak{T} = \mathfrak{C}_3, & \mathfrak{V} = \mathfrak{C}_3 \\ \mathfrak{Z} = \mathfrak{D}_6, & \mathfrak{T} = \mathfrak{C}_3, & \mathfrak{V} = 1 \end{matrix}\right\} R = 10, F = 2, E = 3 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 3 \\ E_0 = 3 ; p \neq 3. \end{matrix}\right.$

7. $\mathfrak{Z} = \mathfrak{D}_4$, $\mathfrak{T} = \mathfrak{D}_4$, $\mathfrak{V} = \mathfrak{D}_4$; $R = 15$, $F = 1$, $E = 4$, $E_0 = 1$; $\mathfrak{p} | 2$.

8. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{D}_4, & \mathfrak{T} = \mathfrak{C}_2, & \mathfrak{V} = \mathfrak{C}_2 \\ \mathfrak{Z} = \mathfrak{D}_4, & \mathfrak{T} = \mathfrak{C}_2, & \mathfrak{V} = 1 \end{matrix}\right\} R = 15, F = 2, E = 2 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 2 \\ E_0 = 2 ; p \neq 2. \end{matrix}\right.$

δ) Ist $\mathfrak{Z} = \mathfrak{C}_n$, so ergeben sich, wie man leicht einsieht, die folgenden möglichen Typen:

9. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{C}_5, & \mathfrak{T} = \mathfrak{C}_5, & \mathfrak{V} = \mathfrak{C}_5 \\ \mathfrak{Z} = \mathfrak{C}_5, & \mathfrak{T} = \mathfrak{C}_5, & \mathfrak{V} = 1 \end{matrix}\right\} R = 12, F = 1, E = 5 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 5 \\ E_0 = 5 ; p^f \equiv 1 \pmod{5}. \end{matrix}\right.$

10. $\mathfrak{Z} = \mathfrak{C}_5, \mathfrak{T} = 1, \mathfrak{V} = 1$; $R = 12, F = 5, E = 1$.

11. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{C}_3, & \mathfrak{T} = \mathfrak{C}_3, & \mathfrak{V} = \mathfrak{C}_3 \\ \mathfrak{Z} = \mathfrak{C}_3, & \mathfrak{T} = \mathfrak{C}_3, & \mathfrak{V} = 1 \end{matrix}\right\} R = 20, F = 1, E = 3 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 3 \\ E_0 = 3 ; p^f \equiv 1 \pmod{3}. \end{matrix}\right.$

12. $\mathfrak{Z} = \mathfrak{C}_3, \mathfrak{T} = 1, \mathfrak{V} = 1$; $R = 20, F = 3, E = 1$.

13. $\left.\begin{matrix} \mathfrak{Z} = \mathfrak{C}_2, & \mathfrak{T} = \mathfrak{C}_2, & \mathfrak{V} = \mathfrak{C}_2 \\ \mathfrak{Z} = \mathfrak{C}_2, & \mathfrak{T} = \mathfrak{C}_2, & \mathfrak{V} = 1 \end{matrix}\right\} R = 30, F = 1, E = 2 \left\{\begin{matrix} E_0 = 1 ; \mathfrak{p} | 2 \\ E_0 = 2 ; p \neq 2. \end{matrix}\right.$

14. $\mathfrak{Z} = \mathfrak{C}_2$, $\mathfrak{T} = 1$, $\mathfrak{V} = 1$; $R = 30$, $F = 2$, $E = 1$.

ε) Ist endlich $\mathfrak{Z} = 1$ so ergibt sich die letzte Möglichkeit:

15. $\mathfrak{Z} = 1$, $\mathfrak{T} = 1$, $\mathfrak{V} = 1$; $R = 60$, $F = 1$, $E = 1$.

Die Fälle 10, 12, 14 und 15 sind die einzigen mit $E = 1$ und wurden schon von Artin[7]) angegeben.

§ 2.

Es sei $\overline{k}$ ein echter Oberkörper von k, aber echter Unterkörper von K. Der Körper $\overline{k}$ möge zur Untergruppe $\mathfrak{U}$ von $\mathfrak{G}$ gehören, d. h. alle Zahlen von $\overline{k}$ sind invariant unter den Substitutionen von $\mathfrak{U}$, und $\mathfrak{U}$ ist die größte Untergruppe von $\mathfrak{G}$ mit dieser Eigenschaft. Auf Grund bekannter Sätze von Dedekind ergibt sich dann aus dem Zerlegungstypus von $\mathfrak{p}$ in K die Primidealzerlegung von $\mathfrak{p}$ in Primideale $\overline{\mathfrak{p}}$ von $\overline{k}$.[8]) Relativgrad und Relativordnung eines Primideales $\overline{\mathfrak{p}}$ von $\overline{k}$ in bezug auf k mögen dann generell mit $\overline{f}$, bezw. $\overline{e}$ bezeichnet werden. Sie sind natürlich im Allgemeinen für die verschiedenen Primteiler eines festen Primideales $\mathfrak{p}$ von k verschieden, da $\overline{k}$ nicht galois'sch in bezug auf k ist.

In der folgenden Tabelle gebe ich die Resultate dieser Untersuchungen für die 15 möglichen Typen an, und zwar links für den Fall, daß $\mathfrak{U}$ eine Tetraedergruppe $\mathfrak{T}$ ist, also $\overline{k}$ den Relativgrad 5 in bezug auf k hat, und rechts für den Fall, daß $\mathfrak{U}$ eine zyklische Gruppe $\mathfrak{C}_5$ ist, also $\overline{k}$ den Relativgrad 12 in bezug auf k hat. Sind die Relativgrade aller voneinander verschiedenen Primideale $\overline{\mathfrak{p}}$, welche ein festes Primideal $\mathfrak{p}$ von k teilen, gleich groß, so geben wir in der Tabelle nur einen Wert an, sind sie verschieden, so gibt die erste Zahl in der Rubrik: „Relativgrad der $\overline{\mathfrak{p}}$“ den Wert $\overline{f}_1$ von $\overline{\mathfrak{p}}_1$, die zweite Zahl den Wert $\overline{f}_2$ von $\overline{\mathfrak{p}}_2$, u. s. w.

Wie man erkennt, entscheidet (ohne weitere Kenntnisse) der Zerlegungstypus links nicht in allen Fällen, welche Werte R, F und E zu gelten haben, während der Zerlegungstypus rechts dies tut. In dieser Arbeit benötigen wir übrigens die rechte Seite der Tabelle ($\mathfrak{U} = \mathfrak{C}_5$) nur für den 4. und 9. Fall.

[7]) *E. Artin,* Ueber die Zetafunktionen gewisser algebraischer Zahlkörper, Math. Ann., Band 89, S. 147-156, vgl. besonders S. 154.

[8]) Vgl. z. B. *H. Weber*, Lehrbuch der Algebra, 2. Band, Braunschweig 1899, S. 657 ff.

Fall	$\mathfrak{U}=\mathfrak{J}$, Relativgrad von $\bar{k}$ in bezug auf k ist 5		$\mathfrak{U}=\mathfrak{C}_5$, Relativgrad von $\bar{k}$ in bezug auf k ist 12		R	F	E
	Zerlegung von $\mathfrak{p}$	Relativgrad der $\bar{\mathfrak{p}}$	Zerlegung von $\mathfrak{p}$	Relativgrad der $\bar{\mathfrak{p}}$			
1	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^4$	1	$\bar{\mathfrak{p}}^{12}$	1	5	1	12
2	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^4$	1	$\bar{\mathfrak{p}}^4$	3	5	3	4
3	$\bar{\mathfrak{p}}^5$	1	$\bar{\mathfrak{p}}_1^2\bar{\mathfrak{p}}_2^{10}$	1	6	1	10
4	$\bar{\mathfrak{p}}^5$	1	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^5$	2	6	2	5
5	$\bar{\mathfrak{p}}_1^2\bar{\mathfrak{p}}_2^3$	1	$\bar{\mathfrak{p}}_1^6\bar{\mathfrak{p}}_2^6$	1	10	1	6
6	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^3$	2, 1	$\bar{\mathfrak{p}}_1^3\bar{\mathfrak{p}}_2^3$	2	10	2	3
7	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^4$	1	$\bar{\mathfrak{p}}_1^4\bar{\mathfrak{p}}_2^4\bar{\mathfrak{p}}_3^4$	1	15	1	4
8	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^2$	1, 2	$\bar{\mathfrak{p}}_1^2\bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_3^2$	2	15	2	2
9	$\bar{\mathfrak{p}}^5$	1	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3^5\bar{\mathfrak{p}}_4^5$	1	12	1	5
10	$\bar{\mathfrak{p}}$	5	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4$	1, 1, 5, 5	12	5	1
11	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3^3$	1	$\bar{\mathfrak{p}}_1^3\bar{\mathfrak{p}}_2^3\bar{\mathfrak{p}}_3^3\bar{\mathfrak{p}}_4^3$	1	20	1	3
12	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3$	1, 1, 3	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4$	3	20	3	1
13	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_3^2$	1	$\bar{\mathfrak{p}}_1^2\bar{\mathfrak{p}}_2^2\bar{\mathfrak{p}}_3^2\bar{\mathfrak{p}}_4^2\bar{\mathfrak{p}}_5^2\bar{\mathfrak{p}}_6^2$	1	30	1	2
14	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3$	1, 2, 2	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4\bar{\mathfrak{p}}_5\bar{\mathfrak{p}}_6$	2	30	2	1
15	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4\bar{\mathfrak{p}}_5$	1	$\bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4\bar{\mathfrak{p}}_5\bar{\mathfrak{p}}_6\bar{\mathfrak{p}}_7\bar{\mathfrak{p}}_8\bar{\mathfrak{p}}_9\bar{\mathfrak{p}}_{10}\bar{\mathfrak{p}}_{11}\bar{\mathfrak{p}}_{12}$	1	60	1	1

Die Fälle 1, 2 und 7 können nur für die Primidealteiler $\mathfrak{p}$ von 2, der Fall 5 nur für die Primidealteiler von 3, und der Fall 3 nur für die Primidealteiler von 5 eintreten.

§ 3.

Um die Betrachtungen im folgenden Abschnitt nicht unterbrechen zu müssen, wollen wir hier den Beweis zweier Hilfssätze, übrigens von ungleicher Natur, einschalten.

1. Hilfssatz:

Es sei k ein algebraischer Zahlkörper, $\bar{k}$ ein Oberkörper, p eine rationale Primzahl, $\mathfrak{p}$ ein Primideal in k, welches p teilt, und $\bar{\mathfrak{p}}$ ein Primideal in $\bar{k}$, welches $\mathfrak{p}$ teilt und in bezug auf k den Relativgrad $\bar{f}$ hat. Es sei ferner q eine von p verschiedene rationale Primzahl und α eine Zahl von k, die q-ter Potenznichtrest mod $\mathfrak{p}$ ist, sodaß also die Kongruenz

$$x^q \equiv \alpha \pmod{\mathfrak{p}} \tag{2}$$

in k nicht lösbar ist. Es sei dagegen die Kongruenz

$$x^q \equiv \alpha \pmod{\bar{\mathfrak{p}}}$$

in $\bar{k}$ lösbar. Dann ist q ein Teiler von $\bar{f}$.

Beweis: Die Reste mod $\mathfrak{p}$ in k bilden ein Galoisfeld $GF(p^f)$, wo f der absolute Grad von $\mathfrak{p}$ ist. Die Reste mod $\bar{\mathfrak{p}}$ in $\bar{k}$ bilden ein $GF(p^{f\bar{f}})$. Das Polynom

$$x^q - \alpha \tag{3}$$

hat in $GF(p^f)$ nach Voraussetzung keinen Linearfaktor. Dann muß aber q ein Teiler von $p^f - 1$ sein, denn sonst wäre die Kongruenz (2) lösbar im $GF(p^f)$. Es sei λ ein erzeugendes Element der multiplikativen Restklassengruppe des $GF(p^f)$. Ist A eine Wurzel des Polynoms (3), so sind *alle* seine Wurzeln gegeben durch

$$A\lambda^{\frac{p^f-1}{q}i}, \quad i = 0, 1, 2, \ldots, q-1, \tag{4}$$

denn $\left(A\lambda^{\frac{p^f-1}{q}i}\right)^q = A^q \lambda^{(p^f-1)i} \equiv A^q \equiv \alpha \pmod{\bar{\mathfrak{p}}}$.

Die q Wurzeln (4) sind mod $\bar{\mathfrak{p}}$ voneinander verschieden, anderseits folgt aus ihrer Form, daß alle den gleichen Relativgrad in bezug auf $GF(p^f)$ haben, also muß er gleich 1 oder gleich q sein. Die erste Annahme wiederspricht der Voraussetzung. Daher ist $x^q - \alpha$ irreduzibel im $GF(p^f)$. Anderseits zerfällt es in Linearfaktoren im $GF(p^{f\bar{f}})$. Folglich muß der Relativgrad $\bar{f}$ ein Vielfaches von q sein, w. z. b. w.

Definition:

Es sei $\mathfrak{p}$ ein Primideal in einem Körper k, α eine Zahl, bezw. $\mathfrak{a}$ ein

Ideal in k, je mit zu $\mathfrak{p}$ teilerfremdem Nenner und s eine ganze rationale nicht negative Zahl. Dann sagen wir, α, bezw. $\mathfrak{a}$ sei *genau* durch $\mathfrak{p}^s$ teilbar, und schreiben

$$\mathfrak{p}^s \,\|\, \alpha, \text{ bezw. } \mathfrak{p}^s \,\|\, \mathfrak{a},$$

wenn der Zähler von α, bezw. $\mathfrak{a}$ durch $\mathfrak{p}^s$, aber nicht mehr durch $\mathfrak{p}^{s+1}$ teilbar ist.

2. Hilfssatz:

Es sei l eine Primzahl und $\varepsilon \neq 1$ eine l-te Einheitswurzel, $\mathfrak{p}$ ein zu l teilerfremdes Primideal eines algebraischen Zahlkörpers k, π ganz und $\mathfrak{p} \,\|\, \pi$; ferner m' eine positive ganze rationale Zahl und $m = m' l$. Es sei dann ein Polynom l-ten Grades $L(x)$ gegeben, dessen Koeffizienten Zahlen von k sind, deren Nenner zu $\mathfrak{p}$ teilerfremd sind, und der Koeffizient der höchsten Potenz von x sei gleich 1. Es sei ferner $D[L(x)]$ die Diskriminante von $L(x)$ und $\mathfrak{p}^t \,\|\, D[L(x)]$.

Es sei schließlich N eine beliebig große positive ganze rationale Zahl, die jedenfalls größer als t und ein für allemal fixiert sei. Dann kann man die Koeffizienten von $L(x)$ so als Polynome in π^m schreiben, daß die Koeffizienten dieser letzteren Polynome Zahlen in k mit zu $\mathfrak{p}$ teilerfremden Nennern sind, welche Zahlen mod $\mathfrak{p}^N$ eindeutig bestimmt sein mögen, so daß das entstehende Polynom in 2 Variabeln $L^*(x, \pi^m)$ jedenfalls

$$L^*(x, \pi^m) \equiv L(x) \qquad (\mathrm{mod}\ \mathfrak{p}^N).$$

Es möge dann $T \leqq \frac{t}{m}$ irgend eine positive ganze rationale Zahl sein, und wir betrachten das Produkt:

$$\prod_{i=1}^{l} \left(x - \sum_{h=0}^{Tl} \gamma_h \, \varepsilon^{ih} \, \pi^{m'h}\right), \tag{5}$$

wo die Konstanten γ_h Zahlen mit zu $\mathfrak{p}$ teilerfremden Nennern von k sind, die mod $\mathfrak{p}^N$ gewertet sein mögen. Weil das Produkt (5) eine ganze symmetrische Funktion der l Größen $(\varepsilon^i \pi^{m'})$, $i = 1, 2, \ldots, l$, ist, so ist (5) von der Form:

$$x^l + P_1(\pi^m)\, x^{l-1} + P_2(\pi^m)\, x^{l-2} + \ldots + P_l(\pi^m), \tag{6}$$

wo $P_i(y)$, $i = 1, 2, \ldots, l$, Polynome von y mit Koeffizienten in k sind, deren Nenner zu $\mathfrak{p}$ teilerfremd sind. Wir wollen annehmen, es sei uns schon

gelungen, $\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{Tl}$ so zu bestimmen, daß bis und mit der Potenz π^{Tm} dis Koeffizienten von $L^*(x, \pi^m)$ und die des Ausdruckes (6) (mod $\mathfrak{p}^N$) übereinstimmen.

Versucht man dann, Zahlen mit zu $\mathfrak{p}$ teilerfremden Nennern in k: $\xi_1, \xi_2, \ldots, \xi_l$, die ebenfalls mod $\mathfrak{p}^N$ gewertet sein mögen, in

$$\prod_{i=1}^{l}(x - \sum_{h=0}^{Tl} \gamma_h \varepsilon^{ih} \pi^{m'h} - \pi^{Tm} \sum_{s=1}^{l} \xi_s \varepsilon^{is} \pi^{m's})$$

so zu bestimmen, daß bis und mit der Potenz $\pi^{(T+1)m}$ die Koeffizienten der Potenzen von x und π^m dieses Produktes und die von $L^*(x, \pi^m)$ (mod $\mathfrak{p}^N$) übereinstimmen, so ergibt sich durch Koeffizientenvergleichung des Polynoms in x, das mit $\pi^{(T+1)m}$ multipliziert ist, ein System von l *linearen* Kongruenzen (mod $\mathfrak{p}^N$) für die Zahlen $\xi_1, \xi_2, \ldots, \xi_l$. Der Nenner der Determinante dieses Kongruenzensystems ist gewiß zu $\mathfrak{p}$ teilerfremd, gilt dies aber auch vom Zähler[9]), wenn man von $T = 1$ zu $T = 2$ geht, so sind bei allgemeinem T die Koeffizienten $\xi_1, \xi_2, \ldots, \xi_l$, zwar natürlich von T abhängig, aber mod $\mathfrak{p}^N$ eindeutig bestimmbar. M. a. W. das Polynom $L^*(x, \pi^m)$, resp. $L(x)$ ist dann nach einer beliebig hohen Potenz von $\mathfrak{p}$ in Linearfaktoren zerlegbar.

Beweis: Wir wollen das Kongruenzzeichen im folgenden in einem erweiterten Sinne so verwenden, daß die beiden Seiten einer Kongruenz nur für die Koeffizienten von $\pi^0, \pi^m, \pi^{2m}, \ldots$ bis und mit der Potenz $\pi^{(T+1)m}$ nach dem vorgeschriebenen Modul kongruente Werte haben, dann soll sein

$$L^*(x, \pi^m) \equiv \prod_{i=1}^{l} \left\{ \left[x - \sum_{h=0}^{Tl} \gamma_h \varepsilon^{ih} \pi^{m'h} \right] - \pi^{Tm} \sum_{s=1}^{l} \xi_s \varepsilon^{is} \pi^{m's} \right\} \pmod{\mathfrak{p}^N}$$

d. h.

$$L^*(x, \pi^m) \equiv \prod_{i=1}^{l} \left[x - \sum_{h=0}^{Tl} \gamma_h \varepsilon^{ih} \pi^{m'h} \right] - \pi^{Tm} \sum_{i=1}^{l} \left\{ \left[\sum_{s=1}^{l} \xi_s \varepsilon^{is} \pi^{m's} \right] \prod_{\substack{j=1 \\ j \neq i}}^{l} \left[x - \sum_{k=0}^{l-1} \gamma_k \varepsilon^{jk} \pi^{m'k} \right] \right\} \pmod{\mathfrak{p}^N}$$

oder

$$L^*(x, \pi^m) - \prod_{i=1}^{l} \left[x - \sum_{h=0}^{Tl} \gamma_h \varepsilon^{ih} \pi^{m'h} \right] \equiv - \pi^{Tm} \sum_{i=1}^{l} \left\{ \left[\sum_{s=1}^{l} \xi_s \varepsilon^{is} \pi^{m's} \right] \prod_{\substack{j=1 \\ j \neq i}}^{l} \left[x - \sum_{k=0}^{l-1} \gamma_k \varepsilon^{jk} \pi^{m'k} \right] \right\} \pmod{\mathfrak{p}^N}.$$

[9]) Dies wird gewiß nicht der Fall sein, wenn $\mathfrak{p}$ ein Teiler von l ist, denn dann ist diese Determinante ersichtlich durch l teilbar. Deshalb haben wir oben vorausgesetzt, daß $(\mathfrak{p}, l) = 1$ ist.

Läßt man höhere Potenzen als $\pi^{(T+1)m}$ weg, so steht hier, wegen unserer Voraussetzung über (5), und weil beide Seiten ganze symmetrische Funktionen der l Größen $(\varepsilon^i \pi^{m'})$, $i = 1, 2, \ldots, l$, sind, auf beiden Seiten der Kongruenz die Größe $\pi^{(T+1)m}$, multipliziert mit einem Polynom von höchstens $(l-1)$-tem Grade in x. Die Koeffizientenvergleichung mod $\mathfrak{p}^N$ von diesen beiden Polynomen liefert in der Tat, wie man sieht, ein lineares Kongruenzensystem mod $\mathfrak{p}^N$ für $\xi_1, \xi_2, \ldots, \xi_l$, denn die rechte Seite hängt linear von diesen Größen ab. Ferner sieht man, daß die Determinante dieses Kongruenzensystems nicht von T abhängt, sondern nur von $\gamma_0, \gamma_1, \ldots, \gamma_{l-1}$. Daraus folgt aber das Behauptete.

§ 4.

Es sei jetzt $\mathfrak{p}$ ein zum Relativgrade 60 teilerfremdes Primideal des Grundkörpers k, welcher den Körper der 5ten Einheitswurzeln enthält, dann können wir immer annehmen, daß das Ideal $(\zeta, \nu, \mathfrak{p}) = (\zeta - \nu, \nu, \mathfrak{p}) = (\zeta, \zeta - \nu, \mathfrak{p})$ gleich dem Einheitsideal ist (vgl. Einleitung). Wir übernehmen jetzt die Bezeichnungen und die Einteilung in Unterfälle, wie wir sie in $N.$ verwendet haben:

Die Gleichung

$$F(R) = (R-3\nu)^3 (R^2 - 11\nu R + 64\nu^2) + 2^6 3^3 \nu^4 \zeta = R(R^2 - 10\nu R + 45\nu^2)^2 + 2^6 3^3 \nu^4 (\zeta - \nu) = 0 \tag{7}$$

legt einen Körper $\bar{k}$ vom Relativgrade 5 in bezug auf k fest, dessen Zahlen invariant sind unter einer Tetraedergruppe $\mathfrak{U} = \mathfrak{T}$. Die Diskriminante von $F(R)$ ist ein Quadrat in k:

$$D(F(R)) = 2^{24} 3^{12} 5^5 \zeta^2 \nu^{16} (\zeta - \nu)^2, \tag{8}$$

und falls $\mathfrak{p}^u \mid \zeta$, $\mathfrak{p}^v \mid \nu$, $\mathfrak{p}^w \mid (\zeta - \nu)$, so ist entsprechend einer eben gemachten Bemerkung von den 3 Zahlen u, v, w höchstens eine von Null verschieden. Nach (8) ist, falls $t = 2u + 16v + 2w$ ist, $\mathfrak{p}^t \mid D(F(R))$.

A. Sei $u = v = w = 0$

Dann ist $t = 0$, $\mathfrak{p}$ unverzweigt, und es muß einer der Fälle 10, 12, 14 oder 15 eintreten.

Zerlegt man $F(R)$ in normierte Primpolynome mod $\mathfrak{p}$, so kann — wie man übrigens nach einem allgemeinen Dedekind'schen Satze weiss[10]) —

[10]) Werke, 1. Band, Braunschweig 1930, S. 212.

keines dieser Primpolynome in höherer als 1. Potenz auftreten, denn sonst wäre es mod $\mathfrak{p}$ ein Faktor von

$$F'(R) = 5\,(R-3\nu)^2\,(R^2-10\,\nu R + 45\,\nu^2).$$

Das würde aber gemäß (7) zum Widerspruche führen, daß wenigstens eine der 3 Zahlen u, v, w positiv sein müßte, gegen Annahme.

Daraus folgt die schon in *N.* angegebene Regel. Wir können sie, wenn wir wollen, auch so formulieren: Es tritt bezw. der Fall 10, 12, 14 oder 15 auf, d. h. es ist bezw. $F = 5, 3, 2$ oder 1, je nachdem die Zerfällung in Primpolynome von

$$(r-3)^3\,(r^2-11\,r+64)+\varkappa$$

mod $\mathfrak{p}$ genau bezw. keinen, zwei, einen oder fünf Lineartaktoren hat.

B. Sei $u > 0$ und -3 quadratischer Rest mod $\mathfrak{p}$

Ist π ganz und $\mathfrak{p} \mid \pi$, so kann man, unabhängig davon, ob -3 quadratischer Rest oder quadratischer Nichtrest mod $\mathfrak{p}$ ist, eine ganze, zu $\mathfrak{p}$ teilerfremde Zahl γ von k so bestimmen, daß

$$\zeta \equiv \gamma\,\pi^u \pmod{\mathfrak{p}^{N+u}}, \tag{9}$$

wo N eine beliebig große ganze rationale Zahl ist, die aber jedenfalls größer als t gewählt sein soll. Ferner gibt es immer zwei ganze Zahlen σ und τ in k, so daß

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

und es ist

$$\sigma \not\equiv \tau,\ \sigma \not\equiv 3,\ \tau \not\equiv 3 \pmod{\mathfrak{p}}. \tag{10}$$

Aus

$$F(R) \equiv (R-3\nu)^3\,(R-\sigma\nu)\,(R-\tau\nu) \pmod{\mathfrak{p}^u}$$

folgt dann nach dem Schönemann'schen Satze[11]) wegen (10) und $v=0$ die Existenz einer Kongruenz von der Form:

[11]) Vgl. z. B. *Ö. Ore*, Ueber den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, erste Mitteilung, Math. Ann., Band 96, S. 313-352, bes. S. 321.

$$F(R) \equiv F_1(R)\ F_2(R)\ F_3(R) \qquad (\mathrm{mod}\ \mathfrak{p}^N), \tag{11}$$

wobei

$$\left.\begin{aligned} F_1(R) &\equiv R - \sigma\nu \\ F_2(R) &\equiv R - \tau\nu \\ F_3(R) &\equiv (R-3\nu)^3 \end{aligned}\right\} (\mathrm{mod}\ \mathfrak{p}). \tag{12}$$

Es folgt daher nach den Hauptsätzen der Ore'schen Theorie[12]), daß in $\mathfrak{p}$ mindestens 3 voneinander verschiedene Primideale $\bar{\mathfrak{p}}$ aufgehen, von denen jedenfalls 2 in bezug auf k Relativordnung und Relativgrad 1 haben. Mithin sind nach unserer Tabelle in Abschnitt 2 nur die Fälle 11, 12 und 15 möglich.

Es sei Θ eine Wurzel von (7), dann folgt aus (7):

$$(\Theta-3\nu)^3\,(\Theta-\sigma\nu)\,(\Theta-\tau\nu) \equiv -\,2^6\,3^3\,\nu^4\,\zeta \qquad (\mathrm{mod}\ \mathfrak{p}^N). \tag{13}$$

Die Faktoren auf der linken Seite dieser Kongruenz sind daher teilbar durch gewisse Primidealteiler $\bar{\mathfrak{p}}$ in $\bar{k}$ von $\mathfrak{p}$. Ein solcher Idealteiler $\bar{\mathfrak{p}}$ kann wegen (10) und $v=0$ nur in einem der 3 Faktoren der linken Seite von (13) aufgehen. Weil es anderseits auch zu jedem mod $\mathfrak{p}^N$ irreduzibeln Faktor von $F(R)$ auch ein zugehöriges Primideal $\bar{\mathfrak{p}}$ gibt[13]), und die Kongruenzen (12) gelten, so muß es — unbeschadet, ob $F_3(R)$ in (11) (mod $\mathfrak{p}^{t+1}$), und daher nach einem bekannten Ore'schen Satze auch (mod $\mathfrak{p}^N$) weiter zerfällt oder nicht — wenigstens einen Primteiler $\bar{\mathfrak{p}}$ von $\mathfrak{p}$ so geben, daß mit $s \geqq 1$

$$\bar{\mathfrak{p}}^s \mid \Theta - 3\nu. \tag{14}$$

Es sei dann für diesen Primteiler

$$\bar{\mathfrak{p}}^{\bar{e}} \mid \mathfrak{p},$$

wo auch $\bar{e} \geqq 1$ ist. Aus (13) folgt dann

$$3s = \bar{e}u. \tag{15}$$

---

[12]) *Ö. Ore,* Ueber den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, zweite Mitteilung, Math. Ann., Band 97, S. 569-598, bes. S. 592 und 594.

[13]) *Ö. Ore,* l. c., S. 326 unten.

I. Wenn $u \not\equiv 0 \pmod 3$ *ist, so gilt der Fall* 11.

In der Tat muß man dann in (15) die Größe $\bar{e} \equiv 0 \pmod 3$, also $\bar{e} = 3$ sein.

II. Ist u durch 3 teilbar und $\sqrt{5}\,\varkappa$ *kubischer Nichtrest mod* $\mathfrak{p}^{u+1}$, *dann tritt der Fall* 12 *auf.*

Sei $u = 3u' \geqq 3$. Nach Voraussetzung ist die Kongruenz

$$x^3 \equiv \sqrt{5}\,\varkappa \pmod{\mathfrak{p}^{u+1}}$$

nicht lösbar, oder wegen (9) die Kongruenz

$$x^3 \equiv \frac{\sqrt{5}\cdot 2^6 3^3 \gamma \pi^{3u'}}{\nu} \pmod{\mathfrak{p}^{3u'+1}},$$

oder also $y = \frac{x}{\pi^{u'}}$ gesetzt, die Kongruenz

$$y^3 \equiv \frac{\sqrt{5}\cdot 2^6 3^3 \gamma}{\nu} \pmod{\mathfrak{p}} \tag{16}$$

in k nicht lösbar.

Nun folgt aber aus (15), daß $s = \bar{e}u'$, und aus (14), daß

$$(\theta - 3\nu)^3 (\theta - \sigma\nu)(\theta - \tau\nu) \equiv (\theta - 3\nu)^3 (3 - \sigma)(3 - \tau)\nu^2 \equiv (\theta - 3\nu)^3 \cdot 40\nu^2 \pmod{\bar{\mathfrak{p}}^{4\bar{e}u'}},$$

mithin nach (13) und (9):

$$(\theta - 3\nu)^3 \cdot 40\nu^2 \equiv -2^6 3^3 \nu^4 \gamma \pi^{3u'} \pmod{\bar{\mathfrak{p}}^{4\bar{e}u'}},$$

und daher

$$\left(-\frac{(\theta - 3\nu)\cdot 2\sqrt{5}}{\pi^{u'}\cdot\nu}\right)^3 \equiv \frac{\sqrt{5}\cdot 2^6 3^3 \gamma}{\nu} \pmod{\bar{\mathfrak{p}}^{\bar{e}u'}}. \tag{17}$$

Da $\bar{e} \geqq 1$, $u' \geqq 1$, so gilt die Kongruenz (17) jedenfalls mod $\bar{\mathfrak{p}}$. Anderseits ist die Kongruenz (16) nicht lösbar in k, daher folgt nach dem ersten Hilfssatz, daß der Relativgrad $\bar{f}$ von $\bar{\mathfrak{p}}$ durch 3 teilbar, und folglich $\bar{f} = 3$ sein muß. Mithin tritt der Fall 12 ein.

III. Ist u durch 3 teilbar und $\sqrt{5}\,\varkappa$ kubischer Rest (mod $\mathfrak{p}^{u+1}$), dann tritt der Fall 15 auf.

Nach Voraussetzung ist dann die Kongruenz

$$x^3 \equiv \sqrt{5}\,\varkappa \pmod{\mathfrak{p}^{u+1}}$$

lösbar. Mithin ist wegen der Voraussetzung über $\mathfrak{p}$ auch die Kongruenz

$$y^3 \equiv \frac{1}{5}\cdot\frac{\zeta}{\nu} \pmod{\mathfrak{p}^{N+u}} \tag{18}$$

lösbar. Sei $\varrho \equiv \frac{-1+\sqrt{-3}}{2} \pmod{\mathfrak{p}^N}$, also $\varrho^2 \equiv \frac{-1-\sqrt{-3}}{2} \pmod{\mathfrak{p}^N}$, und η, $\varrho\eta$, $\varrho^2\eta$ die Wurzeln der Kongruenz (18).

Zunächst ist, wenn wir nach Potenzen von ζ entwickeln, und nur die Glieder bis und mit der ersten Potenz von ζ berücksichtigen, bei allgemeinem, also nicht notwendig durch 3 teilbarem, positivem u, und unabhängig vom Restcharakter von $\sqrt{5}\,\varkappa$:

$$\begin{aligned} F(R) = &\left[(R^2 - 11\,\nu\,R + 64\,\nu^2) + \frac{3^3}{2^3\cdot 5^2}\zeta\,(3R - 64\,\nu) \quad + \ldots\right]\times \\ &\left[(R-3\nu)^3 + \frac{3^3}{2^3\cdot 5^2}\zeta(-3R^2 + 58\,\nu R + 173\,\nu^2) + \ldots\right]. \end{aligned} \tag{19}$$

Für später wollen wir uns merken, daß hier für den quadratischen Faktor eine Zerlegung in Linearfaktoren gemäß (11) und (12) nach einer beliebig hohen Potenz von $\mathfrak{p}$ existiert.

Unter den Annahmen III., daß u durch 3 teilbar und $\sqrt{5}\,\varkappa$ kubischer Rest (mod $\mathfrak{p}^{u+1}$) ist, zerfällt jetzt aber der kubische Faktor mod $\mathfrak{p}^N$ in der Tat in 3 Linearfaktoren. Denn zunächst ist, falls wir nur die Glieder bis und mit der ersten Potenz in ζ berücksichtigen:

$$\begin{aligned} &\left[(R-3\nu)^3 + \frac{3^3}{2^3\cdot 5^2}\zeta(-3R^2 + 58\,\nu R + 173\,\nu^2) + \ldots\right] \equiv \\ &\left[(R-3\nu) + 6\nu\eta - \frac{3}{2}\nu\eta^2 - \frac{3^3}{2^3\cdot 5^2}\zeta + \ldots\right]\times \\ &\left[(R-3\nu) + 6\varrho\nu\eta - \frac{3}{2}\varrho^2\nu\eta^2 - \frac{3^3}{2^3\cdot 5^2}\zeta + \ldots\right]\times \\ &\left[(R-3\nu) + 6\varrho^2\nu\eta - \frac{3}{2}\varrho\nu\eta^2 - \frac{3^3}{2^3\cdot 5^2}\zeta + \ldots\right] \pmod{\mathfrak{p}^N}. \end{aligned} \tag{20}$$

Benutzt man nun den zweiten Hilfssatz mit $l = 3$, $m = u$, $m' = u'$, so sieht man leicht, daß die dort erwähnte Determinante zu $\mathfrak{p}$ teilerfremd

ist. Mithin zerfällt $F(R)$ nach einer beliebig hohen Potenz von $\mathfrak{p}$ in Linearfaktoren, und es tritt der Fall 15 ein.

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

Dann ist $R^2 - 11\nu R + 64\nu^2$ Primpolynom mod $\mathfrak{p}$, und aus

$$F(R) \equiv (R - 3\nu)^3 (R^2 - 11\nu R + 64\nu^2) \pmod{\mathfrak{p}^u}$$

folgt dann nach dem Schönemann'schen Satze die Existenz einer Kongruenz von der Form:

$$F(R) \equiv F_1(R)\ F_2(R) \pmod{\mathfrak{p}^N}, \tag{21}$$

wo

$$\left.\begin{aligned} F_1(R) &\equiv (R - 3\nu)^3 \\ F_2(R) &\equiv R^2 - 11\nu R + 64\nu^2 \end{aligned}\right\} \pmod{\mathfrak{p}}. \tag{22}$$

Nach den Hauptsätzen der Ore'schen Theorie ist dann $\mathfrak{p}$ durch mindestens zwei voneinander verschiedene Primideale $\bar{\mathfrak{p}}$ teilbar, und für eines derselben ist das Produkt aus Relativordnung und Relativgrad gleich 2. Da $\mathfrak{p}$ zu 60 teilerfremd ist, kann also nur einer der Fälle: 6, 13 oder 14 eintreten.

Ist wieder Θ eine Wurzel von (7), so folgt aus (7):

$$(\Theta - 3\nu)^3 (\Theta^2 - 11\nu\Theta + 64\nu^2) = -2^6 3^3 \nu^4 \zeta.$$

Analog wie oben unter B. existiert ein Primidealteiler $\bar{\mathfrak{p}}$ von $\mathfrak{p}$, sodaß mit $s \geqq 1$

$$\bar{\mathfrak{p}}^s \mid \Theta - 3\nu, \tag{23}$$

und

$$3s = \bar{e}u. \tag{24}$$

I. Wenn $u \not\equiv 0 \pmod 3$ ist, so tritt der Fall 6 auf.

In der Tat muß dann in (24) die Größe $\bar{e}$ durch 3 teilbar, also $\bar{e} = 3$ sein. Das bedingt aber den Fall 6.

II. Ist u durch 3 teilbar, so tritt der Fall 14 ein.

Sei wieder $u = 3u' \geqq 3$. Die Kongruenz

$$x^3 \equiv \sqrt{5}\, x \pmod{\mathfrak{p}^{u+1}} \tag{25}$$

ist dann lösbar. Denn nehmen wir das Gegenteil an, so schließt man wie unter B. II., daß der Relativgrad $\overline{f}$ von $\overline{\mathfrak{p}}$ durch 3 teilbar, also gleich 3 sein muß. Das führt aber zu einem Widerspruch, denn keiner der Zerlegungstypen 6, 13 oder 14 hat einen Primidealteiler $\overline{\mathfrak{p}}$ mit der Eigenschaft $\overline{f} = 3$.

Die Kongruenz (25) ist mithin lösbar. Dann ist aber auch die Kongruenz (18) lösbar, und wenn η eine ihrer Wurzeln ist, so existiert jedenfalls eine Zerlegung mod $\mathfrak{p}^N$ von der Form

$$F(R) \equiv F_1(R)\, F_2(R)\, F_3(R) \qquad (\mathrm{mod}\ \mathfrak{p}^N), \tag{26}$$

wo $F_1(R)$ gleich dem ersten Faktor der rechten Seite der Formel (20), $F_2(R)$ gleich dem Produkte des zweiten und dritten Faktors der rechten Seite derselben Formel (20) und $F_3(R)$ gleich dem quadratischen Faktor auf der rechten Seite der Formel (19) ist[14]). Folglich muß entweder der Fall 13 oder der Fall 14 eintreten, und die beiden quadratischen Faktoren in (26) sind irreduzibel mod $\mathfrak{p}^N$. Anderseits zerfallen sie, wie wir nach B. III. wissen, nach Adjunktion der Wurzeln des mod $\mathfrak{p}$ irreduzibeln Polynoms

$$x^2 + 3$$

in Linearfaktoren mod $\mathfrak{p}^N$. Folglich tritt auf Grund des zweiten Ore'schen Hauptsatzes der Fall 14 ein.

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

Ist dann $\mathfrak{p} \mid \pi$, so kann man, unabhängig davon, ob -1 quadratischer Rest oder quadratischer Nichtrest mod $\mathfrak{p}$ ist, eine ganze, zu $\mathfrak{p}$ teilerfremde Zahl γ von k so bestimmen, daß

$$\zeta - \nu \equiv \gamma \pi^w \qquad (\mathrm{mod}\ \mathfrak{p}^{N+w}), \tag{27}$$

wo N wie immer eine beliebig große ganze rationale Zahl ist, die aber jedenfalls größer als t gewählt sein soll. Ferner gibt es immer zwei ganze Zahlen σ und τ in k, so daß

$$\left.\begin{aligned} 5 + 2\sqrt{5}\,\sqrt{-1} &\equiv \sigma \\ 5 - 2\sqrt{5}\,\sqrt{-1} &\equiv \tau \end{aligned}\right\} \qquad (\mathrm{mod}\ \mathfrak{p}^N), \tag{28}$$

[14]) Man beachte, daß das so definierte $F_2(R)$, als symmetrisches Polynom in $\rho\eta$ uud $\rho^2\eta$, alles mod. $\mathfrak{p}^N$ betrachtet. nicht von ρ abhängt.

und es ist

$$\sigma \not\equiv \tau, \quad \sigma \not\equiv 0, \quad \tau \not\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}). \qquad (29)$$

Aus

$$F(R) \equiv R\,(R-\sigma\nu)^2\,(R-\tau\nu)^2 \qquad (\mathrm{mod}\ \mathfrak{p}^w)$$

folgt nach dem Schönemann'schen Satze wegen (29) und $v = 0$ die Existenz einer Kongruenz von der Form:

$$F(R) \equiv F_1(R)\,F_2(R)\,F_3(R) \qquad (\mathrm{mod}\ \mathfrak{p}^N), \qquad (30)$$

wobei

$$\left.\begin{aligned} F_1(R) &\equiv R \\ F_2(R) &\equiv (R-\sigma\nu)^2 \\ F_3(R) &\equiv (R-\tau\nu)^2 \end{aligned}\right\} \qquad (\mathrm{mod}\ \mathfrak{p}). \qquad (31)$$

Es folgt daher nach den Hauptsätzen der Ore'schen Theorie, daß in $\mathfrak{p}$ mindestens 3 voneinander verschiedene Primideale $\overline{\mathfrak{p}}$ von $\overline{k}$ aufgehen, von denen jedenfalls eines Relativordnung und Relativgrad 1 hat. Für die andern Primidealteiler $\overline{\mathfrak{p}}$ kann das Produkt aus Relativgrad und Relativordnung höchstens die Werte 1 oder 2 haben. Mithin sind nach unserer Tabelle in Abschnitt 2 nur die Fälle 13, 14 und 15 möglich.

Jetzt können wir wieder analog wie unter B. weiter schließen, ich führe aber die Schlüsse explizite durch, auch weil der Fall E. sich auf den Fall D. stützt.

Es sei θ eine Wurzel von (7), dann folgt aus (7):

$$\theta\,(\theta-\sigma\nu)^2\,(\theta-\tau\nu)^2 \equiv -2^6\,3^3\,\nu^4\,(\zeta-\nu) \qquad (\mathrm{mod}\ \mathfrak{p}^N). \quad (32)$$

Die Faktoren auf der linken Seite dieser Kongruenz sind daher teilbar durch gewisse Primidealteiler $\overline{\mathfrak{p}}$ in $\overline{k}$ von $\mathfrak{p}$. Ein solcher Idealteiler $\overline{\mathfrak{p}}$ kann wegen (29) und $v = 0$ nur in einem der 3 Faktoren der linken Seite von (32) aufgehen. Weil es anderseits auch zu jedem mod $\mathfrak{p}^N$ irreduzibeln Faktor von $F(R)$ auch ein zugehöriges Primideal $\overline{\mathfrak{p}}$ gibt, und die Kongruenzen (31) gelten, so muß es — unbeschadet ob $F_2(R)$ oder $F_3(R)$ oder beide diese Faktoren in (30) (mod $\mathfrak{p}^{t+1}$) und daher nach einem bekannten Ore'schen Satze auch (mod $\mathfrak{p}^N$) weiter zerfallen oder nicht — wenigstens einen Primteiler $\overline{\mathfrak{p}}$ von $\mathfrak{p}$ so geben, daß mit $s \geqq 1$:

$$\overline{\mathfrak{p}}^s \mid \theta - \sigma\nu. \qquad (33)$$

Es sei dann für diesen Primteiler mit $\bar{e} \geqq 1$:

$$\bar{\mathfrak{p}}^{\bar{e}} \mid \mathfrak{p}.$$

Aus (32) folgt dann

$$2s = \bar{e}w. \tag{34}$$

I. Wenn $w \not\equiv 0 \pmod 2$ ist, so gilt der Fall 13.

In der Tat muß dann in (34) die Größe $\bar{e} \equiv 0 \pmod 2$, also $\bar{e} = 2$ sein.

II. Ist w durch 2 teilbar und $\sqrt{5}(\varkappa - 12^3)$ quadratischer Nichtrest mod $\mathfrak{p}^{w+1}$, dann tritt der Fall 14 auf.

Sei $w = 2w' \geqq 2$. Nach Voraussetzung ist die Kongruenz

$$x^2 \equiv \sqrt{5}\,(\varkappa - 12^3) \pmod{\mathfrak{p}^{w+1}}$$

in k nicht lösbar, oder wegen (27) die Kongruenz

$$x^2 \equiv \frac{\sqrt{5} \cdot 2^6 3^3 \gamma \pi^{2w'}}{\nu} \pmod{\mathfrak{p}^{2w'+1}},$$

oder also $y = \frac{x}{\pi^{w'}}$ gesetzt, die Kongruenz

$$y^2 \equiv \frac{\sqrt{5} \cdot 2^6 3^3 \gamma}{\nu} \pmod{\mathfrak{p}} \tag{35}$$

n k nicht lösbar.

Nun folgt aber aus (34), daß $s = \bar{e}w'$, und aus (33) daß

$$\Theta\,(\Theta - \sigma\nu)^2\,(\Theta - \tau\nu)^2 \equiv (\Theta - \sigma\nu)^2 \cdot \sigma\nu \cdot (\sigma - \tau)^2 \nu^2 \equiv (\Theta - \sigma\nu)^2 \cdot (-80\sigma)\nu^3 \pmod{\bar{\mathfrak{p}}^{3\bar{e}w'}},$$

also nach (32) und (27):

$$(\Theta - \sigma\nu)^2 \cdot (-80\sigma)\nu^3 \equiv -2^6 3^3 \nu^4 \gamma \pi^{2w'} \pmod{\bar{\mathfrak{p}}^{3\bar{e}w'}},$$

oder, falls man beide Seiten dieser Kongruenz mit $-\sqrt{5}$ multipliziert:

$$(\Theta - \sigma\nu)^2 (5 - \sqrt{5})^2 (\sigma + 3\sqrt{5})^2 \cdot \nu^3 \equiv \sqrt{5} \cdot 2^6 3^3 \nu^4 \gamma \pi^{2w'} \pmod{\bar{\mathfrak{p}}^{3\bar{e}w'}},$$

und daher

$$\left(\frac{(\theta-\sigma\nu)(5-\sqrt{5})(\sigma+3\sqrt{5})}{\pi^{w'}\cdot\nu}\right)^2\equiv\frac{\sqrt{5}\cdot 2^6 3^3\gamma}{\nu}\pmod{\bar{\mathfrak{p}}^{\bar{e}\bar{w}'}}.\quad(36)$$

Da $\bar{e}\geqq 1$, $w'\geqq 1$, so gilt die Kongruenz (36) jedenfalls (mod $\bar{\mathfrak{p}}$). Anderseits ist die Kongruenz (35) nicht lösbar in k, daher folgt nach dem ersten Hilfssatz, daß der Relativgrad $\bar{f}$ von $\bar{\mathfrak{p}}$ durch 2 teilbar, und folglich gleich 2 sein muß. Mithin tritt der Fall 14 ein.

III. Ist w durch 2 teilbar, und $\sqrt{5}\,(\varkappa-12^3)$ quadratischer Rest mod $\mathfrak{p}^{w+1}$, dann tritt der Fall 15 auf.

Nach Voraussetzung ist dann die Kongruenz

$$x^2\equiv\sqrt{5}\,(\varkappa-12^3)\qquad\pmod{\mathfrak{p}^{w+1}}$$

lösbar. Mithin ist, wie man leicht einsieht, auch die Kongruenz

$$z^2\equiv\frac{1}{15\sqrt{5}}\cdot\frac{\zeta-\nu}{\nu}\qquad\pmod{\mathfrak{p}^{N+w}}\quad(37)$$

lösbar. Es möge dann ω eine Wurzel der Kongruenz (37) sein, dann sei zur Abkürzung:

$$\left.\begin{aligned}\eta&\equiv\frac{1-\sqrt{5}}{4\sqrt{5}}(\sigma-10-3\sqrt{5})\,\omega\equiv\frac{\sqrt{5}-1}{4\sqrt{5}}(\tau+3\sqrt{5})\,\omega\equiv\left(\frac{1+\sqrt{5}}{2}+\frac{1-\sqrt{5}}{2}\sqrt{-1}\right)\omega\\ \xi&\equiv\frac{1-\sqrt{5}}{4\sqrt{5}}(\tau-10-3\sqrt{5})\,\omega\equiv\frac{\sqrt{5}-1}{4\sqrt{5}}(\sigma+3\sqrt{5})\,\omega\equiv\left(\frac{1+\sqrt{5}}{2}-\frac{1-\sqrt{5}}{2}\sqrt{-1}\right)\omega\end{aligned}\right\}\pmod{\mathfrak{p}^{N+w'}}\quad(38)$$

gesetzt. Es ist dann

$$\left.\begin{aligned}\eta^2&\equiv\frac{3}{5\sigma}\cdot\frac{\zeta-\nu}{\nu}\\ \xi^2&\equiv\frac{3}{5\tau}\cdot\frac{\zeta-\nu}{\nu}\end{aligned}\right\}\qquad\pmod{\mathfrak{p}^{N+w}}\quad(39)$$

und

$$\eta\xi\equiv\frac{1}{5\sqrt{5}}\cdot\frac{\zeta-\nu}{\nu}\qquad\pmod{\mathfrak{p}^{N+w}}.\quad(40)$$

Wegen späterer Schlüsse unter E. will ich hier etwas weiter ausholen [15]). Zunächst existiert bei beliebigem, also nicht notwendig geradem, aber positivem w und unabhängig vom Restcharakter von $\sqrt{5}$ $(\varkappa - 12^3)$, ferner unabhängig davon, ob -1 quadratischer Rest oder Nichtrest ist, nach dem Schönemann'schen Satze eine Zerlegung von der Form

$$F(R) \equiv F_1(R)\, F_2(R) \pmod{\mathfrak{p}^N},$$

wo

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

ist. Wenn wir nach Potenzen von $(\zeta - \nu)$ entwickeln, und nur die Glieder bis und mit der ersten Potenz in $(\zeta - \nu)$ berücksichtigen, ist

$$\begin{aligned} F(R) = &\left[R + \frac{2^6}{3\cdot 5^2}(\zeta - \nu) + \ldots\right] \times \\ &\left[(R^2 - 10\nu R + 45\nu^2)^2 + \frac{2^6}{3\cdot 5^2}(\zeta - \nu)(-R^3 + 20\nu R^2 - 190\nu^2 R + 900\nu^3) + \ldots\right] \end{aligned} \tag{41}$$

und es ist wegen der Form von $F(R)$ klar, daß die Koeffizienten der höheren Potenzen von $(\zeta - \nu)$ Polynome im Körper der Zahl ν von höchstens drittem Grade in R sind.

Bei beliebigem, also nicht notwendigerweise geradem, aber positivem w, und unabhängig vom Restcharakter von $\sqrt{5}$ $(\varkappa - 12^3)$ zerlegt sich dann, wenn wir annehmen, daß -1 quadratischer Rest mod $\mathfrak{p}$ ist, nach (30) und (31) der biquadratische Faktor nach einer beliebig hohen Potenz von $\mathfrak{p}$ in zwei quadratische Faktoren. Entwickeln wir nach Potenzen von $(\zeta - \nu)$, wobei wir nur die Glieder bis und mit der ersten Potenz in $(\zeta - \nu)$ berücksichtigen, so ist:

$$\begin{aligned} &\left[(R^2 - 10\nu R + 45\nu^2)^2 + \frac{2^6}{3\cdot 5^2}(\zeta - \nu)(-R^3 + 20\nu R^2 - 190\nu^2 R + 900\nu^3) + \ldots\right] \\ &\equiv \left[(R - \sigma\nu)^2 + \frac{(\zeta - \nu)}{3\cdot 5^2}\Big((53 - 17\sigma)R + (153\sigma - 1125)\nu\Big) + \ldots\right] \times \\ &\quad \left[(R - \tau\nu)^2 + \frac{(\zeta - \nu)}{3\cdot 5^2}\Big((53 - 17\tau)R + (153\tau - 1125)\nu\Big) + \ldots\right] \pmod{\mathfrak{p}^N}. \end{aligned} \tag{42}$$

[15]) Man kann die folgenden Schlüsse sehr vereinfachen, wenn man überall bis und mit dem Gliede $(\zeta - \nu)^2$ explizite entwickelt, denn dann hat man eine Zerlegung mod. $\mathfrak{p}^{t+1}$, was für die Ore'schen Sätze genügt. Die Durchführung der Rechnung zeigt aber, daß man dann große Zahlkoeffizienten in Kauf zu nehmen hat.

Wir können hier annehmen, daß der erste Faktor auf der rechten Seite von (42) eine lineare Funktion von σ ist, und τ nicht enthält, und der zweite Faktor auf der rechten Seite von (42) eine lineare Funktion von τ ist, und σ nicht enthält, denn die beiden Größen genügen gemäß (28) der Kongruenz

$$x^2 - 10x + 45 \equiv 0 \pmod{\mathfrak{p}^N}.$$

Macht man in diesem Sinne in (42) zur Bestimmung der Koeffizienten der nächst höheren Potenzen von $(\zeta - \nu)$ einen Ansatz mit unbestimmten Koeffizienten, so sieht man, mit Rücksicht auf die Form des biquadratischen Faktors in (41) wie beim Beweise des zweiten Hilfssatzes ein, daß der zweite Faktor auf der rechten Seite von (42) aus dem ersten hervorgeht, indem man σ in τ verwandelt.

Unter den Annahmen III., daß w gerade und $\sqrt{5}\,(\varkappa - 12^3)$ quadratischer Rest (mod $\mathfrak{p}^{w+1}$) ist, zerfällt jetzt aber jeder der beiden Faktoren auf der rechten Seite von (42) (mod $\mathfrak{p}^N$) in Linearfaktoren. Denn zunächst ist, wenn wir nur die Glieder bis und mit der ersten Potenz in $(\zeta - \nu)$ berücksichtigen:

$$\begin{aligned}
&\left[(R-\sigma\nu)^2 + \frac{(\zeta-\nu)}{3\cdot 5^2}\left((53-17\sigma)R + (153\sigma - 1125)\nu\right) + \ldots\right] \\
&\equiv \left[(R-\sigma\nu) + 6\eta\nu + \frac{(\zeta-\nu)}{2\cdot 3\cdot 5^2}(53-17\sigma) + \ldots\right] \times \qquad (43) \\
&\quad \left[(R-\sigma\nu) - 6\eta\nu + \frac{(\zeta-\nu)}{2\cdot 3\cdot 5^2}(53-17\sigma) - \ldots\right] \qquad \pmod{\mathfrak{p}^N},
\end{aligned}$$

bezw.

$$\begin{aligned}
&\left[(R-\tau\nu)^2 + \frac{(\zeta-\nu)}{3\cdot 5^2}\left((53-17\tau)R + (153\tau - 1125)\nu\right) + \ldots\right] \\
&\equiv \left[(R-\tau\nu) + 6\xi\nu + \frac{(\zeta-\nu)}{2\cdot 3\cdot 5^2}(53-17\tau) + \ldots\right] \times \qquad (44) \\
&\quad \left[(R-\tau\nu) - 6\xi\nu + \frac{(\zeta-\nu)}{2\cdot 3\cdot 5^2}(53-17\tau) - \ldots\right] \qquad \pmod{\mathfrak{p}^N}.
\end{aligned}$$

Benutzt man nun den 2. Hilfssatz mit $l = 2$, $m = w$, $m' = w'$, so sieht man leicht, daß die dort erwähnte Determinante zu $\mathfrak{p}$ teilerfremd ist, m. a. W. die beiden Faktoren der rechten Seite von (42) zerfallen nach einer beliebig hohen Potenz von $\mathfrak{p}$ in Linearfaktoren. Folglich tritt der

Fall 15 ein. Wir wollen uns für später merken, daß die Entwickelungen der Linearfaktoren auf der rechten Seite von (43) nach Potenzen von η fortschreiten, wobei man die geraden Potenzen gemäß (39) ersetzen kann, so daß diese Linearfaktoren lineare Funktionen in η sind. Ferner können wir auch annehmen, daß sie lineare Funktionen von σ sind. Der zweite Linearfaktor auf der rechten Seite von (43) geht dann aus dem ersten hervor, indem man η in $-\eta$ verwandelt. Ferner geht gemäß unserer Bemerkung zur Formel (42), und mit Rücksicht auf die Formeln (38) und (39) der erste Linearfaktor der rechten Seite von (44) aus dem ersten Linearfaktor der rechten Seite von (43) dadurch hervor, daß man gleichzeitig σ in τ und η in ξ verwandelt. Der zweite Linearfaktor auf der rechten Seite von (44) geht aus dem ersten dadurch hervor, daß man ξ in $-\xi$ verwandelt.

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

Dann ist $R^2 - 10\nu R + 45\nu^2$ Primpolynom mod $\mathfrak{p}$, und aus

$$F(R) \equiv R(R^2 - 10\nu R + 45\nu^2)^2 \pmod{\mathfrak{p}^w}$$

folgt dann nach dem Schönemann'schen Satze die Existenz einer Kongruenz von der Form:

$$F(R) \equiv F_1(R)\, F_2(R) \pmod{\mathfrak{p}^N}, \qquad (45)$$

wo

$$\left.\begin{aligned} F_1(R) &\equiv R \\ F_2(R) &\equiv (R^2 - 10\nu R + 45\nu^2)^2 \end{aligned}\right\} \pmod{\mathfrak{p}}. \qquad (46)$$

Folglich gibt es einen Primteiler $\bar{\mathfrak{p}}$ von $\mathfrak{p}$ mit Relativgrad und Relativordnung 1. Ferner ist $F_2(R)$ nach unserer Annahme entweder unzerlegbar (mod $\mathfrak{p}^{t+1}$), und daher (mod $\mathfrak{p}^N$) in k, und dann haben wir in $\bar{k}$ einen einzigen weitern, von $\bar{\mathfrak{p}}$ verschiedenen Primteiler von $\mathfrak{p}$, für welchen Produkt aus Relativordnung und Relativgrad gleich 4 ist, oder $F_2(R)$ ist in k (mod $\mathfrak{p}^{t+1}$), und daher auch (mod $\mathfrak{p}^N$) in 2 quadratische Faktoren zerlegbar und wir haben in $\bar{k}$ genau zwei weitere, von $\bar{\mathfrak{p}}$ und untereinander verschiedene Primteiler von $\mathfrak{p}$, für welche das Produkt aus Relativordnung und Relativgrad gleich 2 ist. Mithin sind, da $\mathfrak{p}$ immer zu 60 teilerfremd ist, gemäß unserer Tabelle in Abschnitt 2 nur die Fälle 8, 13 und 14 möglich.

Ist wieder Θ eine Wurzel von (7), so folgt aus (7):

$$\Theta\,(\Theta^2 - 10\,\nu\,\Theta + 45\,\nu^2)^2 = -2^6\,3^3\,\nu^4\,(\zeta - \nu). \tag{47}$$

Die beiden Faktoren auf der linken Seite dieser Gleichung sind daher wieder durch gewisse Primideale $\bar{\mathfrak{p}}$ in $\bar{k}$ von $\mathfrak{p}$ teilbar. Ein solches Primideal kann nur in einem der beiden Faktoren der linken Seite von (47) aufgehen, da sonst die unmögliche Kongruenz $45\,\nu^2 \equiv 0 \pmod{\mathfrak{p}}$ folgen würde. Wie oben unter D. existiert ein Primteiler $\bar{\mathfrak{p}}$ von $\mathfrak{p}$, so daß mit $s \geqq 1$

$$\bar{\mathfrak{p}}^s \mid \Theta^2 - 10\,\nu\,\Theta + 45\,\nu^2. \tag{48}$$

Ist für diesen Primteiler mit $\bar{e} \geqq 1$:

$$\bar{\mathfrak{p}}^{\bar{e}} \mid \mathfrak{p}$$

so folgt aus (48) und (47):

$$2\,s = \bar{e}\,w. \tag{49}$$

I. Wenn $w \not\equiv 0 \pmod 2$ ist, so gilt der Fall 8.

In der Tat muß dann in (49) die Größe $\bar{e} \equiv 0 \pmod 2$, also $\bar{e} = 2$ sein, und der Fall 8 oder 13 eintreten. Aber der letztere Fall ist auszuschließen. Denn dann gäbe es nach den Ore'schen Sätzen eine Zerlegung von $F(R)$ in irreduzible Faktoren $(\mathrm{mod}\ \mathfrak{p}^N)$, so daß

$$F(R) \equiv F_1(R)\,F_2(R)\,F_3(R) \qquad (\mathrm{mod}\ \mathfrak{p}^N), \tag{50}$$

wobei

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

Adjungiert man aber in (50) die Wurzeln des mod $\mathfrak{p}$ irreduzibeln Polynoms

$$x^2 - 10\,x + 45,$$

so zerfällt jeder der beiden Faktoren $F_2(R)$ und $F_3(R)$ nach dem Schönemannschen Satze $(\mathrm{mod}\ \mathfrak{p}^N)$ in Linearfaktoren. Denn es ist dann

$$F_2(R) \equiv F_3(R) \equiv (R - \sigma\,\nu)\,(R - \tau\,\nu) \qquad (\mathrm{mod}\ \mathfrak{p}),$$

wo $\sigma\nu \not\equiv \tau\nu \pmod{\mathfrak{p}}$. Daher müßte nach dem zweiten Ore'schen Satze $\bar{e} = 1$ sein gegen Annahme. Folglich tritt der Fall 8 ein.

II. Wenn $w \equiv 0 \pmod 2$ ist, so tritt der Fall 14 ein.
Ich unterscheide 2 Unterfälle, je nachdem die Kongruenz

$$x^2 \equiv \sqrt{5}\,(x - 12^3) \qquad \pmod{\mathfrak{p}^{w+1}}$$

und daher auch die Kongruenz (37) lösbar ist oder nicht.

Ist die Kongruenz (37) lösbar, dann zerfällt der biquadratische Faktor in (45) und (46) in zwei irreduzible quadratische Faktoren mod $\mathfrak{p}^N$. Den einen dieser Faktoren erhalten wir, wenn wir den ersten Linearfaktor auf der rechten Seite von (43) mit dem ersten Linearfaktor auf der rechten Seite von (44) miteinander multiplizieren. Denn gemäß (28) und (38) fällt dann die Größe $\sqrt{-1} \pmod{\mathfrak{p}^N}$ heraus und wir erhalten $(\mathrm{mod}\ \mathfrak{p}^N)$ eine Entwicklung nach Potenzen von ω, deren Koeffizienten in k sind. Wenn wir nur die Glieder bis und mit der ersten Potenz in $(\zeta - \nu)$ berücksichtigen, so ist

$$\begin{aligned}
&\left[(R - \sigma\nu) + 6\eta\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\sigma) + \ldots\right] \times \\
&\left[(R - \tau\nu) + 6\xi\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\tau) + \ldots\right] \equiv \\
&\left[(R^2 - 10\nu R + 45\nu^2) + 6\omega\nu\left((1+\sqrt{5})R + (5-7\sqrt{5})\nu\right)\right. \\
&\qquad \left. + \frac{2^2}{3.5^2}(\zeta-\nu)\left(-8R + (125+27\sqrt{5})\nu\right) + \ldots\right] \pmod{\mathfrak{p}^N}.
\end{aligned} \tag{51}$$

Den zweiten Faktor gewinnt man analog, wenn man den zweiten Linearfaktor auf der rechten Seite von (43) mit dem zweiten Linearfaktor auf der rechten Seite von (44) miteinander multipliziert. Mit Rücksicht auf (38) ist:

$$\begin{aligned}
&\left[(R - \sigma\nu) - 6\eta\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\sigma) - \ldots\right] \times \\
&\left[(R - \tau\nu) - 6\xi\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\tau) - \ldots\right] \equiv \\
&\left[(R^2 - 10\nu R + 45\nu^2) - 6\omega\nu\left((1+\sqrt{5})R + (5-7\sqrt{5})\nu\right)\right. \\
&\qquad \left. + \frac{2^2}{3.5^2}(\zeta-\nu)\left(-8R + (125+27\sqrt{5})\nu\right) - \ldots\right] \pmod{\mathfrak{p}^N}.
\end{aligned} \tag{52}$$

Das Produkt der rechten Seiten von (51) und (52) ist dann gemäß (42), (43) und (44) gleich dem biquadratischen Faktor in (45) und (46). Mithin ist der Fall 8 auszuschließen und es gilt der Fall 13 oder der Fall 14. Aber auf Grund des zweiten Ore'schen Satzes gilt der Fall 14. Denn adjungiert man die Wurzeln des mod $\mathfrak{p}$ irreduzibeln Polynoms

$$x^2 + 1,$$

so sieht man mit Rücksicht auf (28) und (38) leicht ein, daß jeder der beiden quadratischen Faktoren mod $\mathfrak{p}^N$ in Linearfaktoren zerfällt.

Ich gehe zum zweiten Unterfall über. Ist die Kongruenz (37) nicht lösbar, so ist, weil -1 quadratischer Nichtrest mod $\mathfrak{p}$ ist, wie man leicht einsieht, die Kongruenz

$$z^2 \equiv -\frac{1}{15\sqrt{5}} \cdot \frac{\zeta - \nu}{\nu} \pmod{\mathfrak{p}^{N+w}} \qquad (53)$$

lösbar. Jetzt zerfällt aber der biquadratische Faktor in (45) und (46) ebenfalls in 2 irreduzible quadratische Faktoren (mod $\mathfrak{p}^N$). Den einen dieser quadratischen Faktoren gewinnen wir, wenn wir den ersten Linearfaktor auf der rechten Seite von (43) mit dem zweiten Linearfaktor auf der rechten Seite von (44) miteinander multiplizieren. Denn ist (vgl. Formeln (38), bezw. (37) und (53)):

$$\bar{\omega} \equiv +\sqrt{-1}\,.\,\omega \pmod{\mathfrak{p}^{N+w'}}$$

eine Wurzel von (53), so ist:

$$\left.\begin{aligned} \eta - \xi &\equiv (1 - \sqrt{5})\,\bar{\omega} \\ \eta\tau - \xi\sigma &\equiv (-5 - 7\sqrt{5})\,\bar{\omega} \end{aligned}\right\} \pmod{\mathfrak{p}^{N+w'}}. \qquad (54)$$

Ferner gilt immer die Formel (40). Es ergibt sich daher eine Entwicklung von der Form:

$$\begin{aligned} &\left[(R - \sigma\nu) + 6\eta\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\sigma) + \ldots\right] \times \\ &\left[(R - \tau\nu) - 6\xi\nu + \frac{(\zeta-\nu)}{2.3.5^2}(53 - 17\tau) - \ldots\right] \equiv \\ &\left[(R^2 - 10\nu R + 45\nu^2) + 6\bar{\omega}\nu\left((1-\sqrt{5})R + (5+7\sqrt{5})\nu\right)\right. \\ &\quad \left. + \frac{2^2}{3\cdot 5^2}(\zeta-\nu)\left(-8R + (125 - 27\sqrt{5})\nu\right) + \ldots\right] \pmod{\mathfrak{p}^N}, \end{aligned} \qquad (55)$$

wo wir die Entwicklung nach Potenzen von $\bar{\omega}$ nur bis und mit der 2. Potenz angeben. Entsprechend liefert das Produkt des zweiten Linearfaktors auf der rechten Seite von (43) mit dem ersten Linearfaktor auf der rechten Seite von (44) den andern mod $\mathfrak{p}^N$ irreduzibeln quadratischen Faktor des biquadratischen Faktors in (45) und (46). Er geht gemäß (54) aus (55) hervor, indem man $\bar{\omega}$ in $-\bar{\omega}$ verwandelt. Der weitere Schluß ist derselbe wie im ersten Unterfall.

F. Sei $v > 0$.

Dann setzen wir[16])

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

und nehmen bequem die Resolvente

$$G(S) = S^5 + 4\nu\zeta^2(10S^2 - 15\zeta S + 36\zeta^2) = 0 \qquad (56)$$

zu Hilfe, deren Diskriminante übrigens gleich

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

ist[17]). Ist, wie immer, $\mathfrak{p}^t \mid D[G(S)]$, so ist also $t = 14u + 4v + 2w$.

Ist $\mathfrak{p} \mid \pi$ und N wie oben eine beliebig große ganze rationale Zahl, die größer als t ist, so gibt es eine ganze, zu $\mathfrak{p}$ teilerfremde Zahl γ in k, so daß

$$\nu \equiv \gamma\pi^v \pmod{\mathfrak{p}^{N+v}}. \qquad (57)$$

Ist Θ eine Wurzel von (56), so folgt aus (56):

$$\Theta^5 = -4\nu\zeta^2(10\Theta^2 - 15\zeta\Theta + 36\zeta^2). \qquad (58)$$

Es folgt aus (58), daß Θ nicht teilerfremd ist zu $\mathfrak{p}$, und es existiert daher wenigstens ein Primidealteiler $\bar{\mathfrak{p}}$ in $\bar{k}$ von $\mathfrak{p}$, so daß mit $s \geqq 1$:

$$\bar{\mathfrak{p}}^s \mid \Theta. \qquad (59)$$

Ist mit $\bar{e} \geqq 1$:

$$\bar{\mathfrak{p}}^{\bar{e}} \mid \mathfrak{p},$$

---

16) Vgl. *N.*, S. 226.

17) Dieser Wert ergiebt sich leicht aus den Formeln (1), (2) und (3) der Seite 182 des Ikosaederbuches von F. Klein. Wir notieren ihn der Vollständigkeit halber, obwohl wir ihn hier für die weiteren Entwicklungen nicht zu kennen brauchen.

so folgt aus (59) und (58), da $u = 0$ und $\mathfrak{p}$ immer zu 60 teilerfremd ist:

$$5s = \bar{e}v. \tag{60}$$

I. Ist $v \not\equiv 0 \pmod 5$, so tritt der Fall 9 ein.

In der Tat muß dann in (60) die Größe $\bar{e} \equiv 0 \pmod 5$, also $\bar{e} = 5$ sein. Mithin kommen nach unserer Tabelle wegen der Voraussetzung über $\mathfrak{p}$ nur die Fälle 4 und 9 in Betracht. Die Entscheidung, welcher Fall eintritt, fällt bequem im Unterkörper $\bar{\bar{k}}$ vom 12. Relativgrade in bezug auf k, dessen Zahlen invariant sind unter einer Untergruppe $\mathfrak{U} = \mathfrak{C}_5$. Setzt man in der Ikosaedergleichung (1) $E^5 = \frac{T}{\nu}$, so erhält man die Resolvente 12. Grades:

$$K(T) = -\left[-T^4 + 228\nu T^3 - 494\nu^2 T^2 - 228\nu^3 T - \nu^4\right]^3 + 2^6 3^3 \zeta T \left[T^2 + 11\nu T - \nu^2\right]^5 = 0,$$

deren Wurzeln $\bar{\bar{k}}$ in bezug auf k festlegen. Es ist

$$K(T) \equiv (T + 2^6 3^3 \zeta) \cdot T^{11} \pmod{\mathfrak{p}},$$

und da $2^6 3^3 \zeta \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so existiert nach dem Schönemann'schen Satze für ein beliebig großes N eine Zerlegung:

$$K(T) \equiv K_1(T)\, K_2(T) \pmod{\mathfrak{p}^N},$$

wo

$$\left.\begin{aligned} K_1(T) &\equiv T + 2^6 3^3 \zeta \\ K_2(T) &\equiv T^{11} \end{aligned}\right\} \pmod{\mathfrak{p}}.$$

Folglich existiert nach dem ersten Ore'schen Satz wenigstens ein Primidealteiler $\bar{\bar{\mathfrak{p}}}$ in $\bar{\bar{k}}$ von $\mathfrak{p}$, dessen Relativordnung und Relativgrad beide gleich 1 sind. Mithin kann nach unserer Tabelle in Abschnitt 2 der Fall 4 nicht eintreten, und es gilt daher der Fall 9.

II. Wenn v durch 5 teilbar und $\frac{I}{\varkappa}$ fünfter Potenznichtrest (mod $\mathfrak{p}^{v+1}$) ist, so tritt der Fall 10 ein.

Sei $v = 5v' \geqq 5$. Nach Voraussetzung ist die Kongruenz

$$x^5 \equiv \frac{\mathrm{I}}{\varkappa} \pmod{\mathfrak{p}^{v+1}}$$

in k nicht lösbar. Wegen (57) ist daher auch die Kongruenz

$$x^5 \equiv \frac{\gamma \pi^{5v'}}{2^6 3^3 \zeta} \pmod{\mathfrak{p}^{5v'+1}},$$

oder also, $y = \frac{x}{\pi^{v'}}$ gesetzt, die Kongruenz

$$y^5 \equiv \frac{\gamma}{2^6 3^3 \zeta} \pmod{\mathfrak{p}} \qquad (61)$$

in k nicht lösbar.

Aus (60) folgt, daß $s = \bar{e}v'$ ist, und aus (59), (58) und (57), daß

$$\Theta^5 \equiv -144 \zeta^4 \gamma \pi^{5v'} \pmod{\bar{\mathfrak{p}}^{6\bar{e}v'}}.$$

Dividiert man hier beide Seiten durch die zu $\mathfrak{p}$ teilerfremde Zahl $-2^{10} 3^5 \zeta^5$, so wird:

$$\left(-\frac{\Theta}{2^2 3 \zeta}\right)^5 \equiv \frac{\gamma \pi^{5v'}}{2^6 3^3 \zeta} \pmod{\bar{\mathfrak{p}}^{6\bar{e}v'}},$$

und daher ist

$$\left(-\frac{\Theta}{2^2 3 . \zeta \pi^{v'}}\right)^5 \equiv \frac{\gamma}{2^6 3^3 \zeta} \pmod{\bar{\mathfrak{p}}^{\bar{e}v'}}. \qquad (62)$$

Da $\bar{e} \geqq 1$, $v' \geqq 1$, so gilt die Kongruenz (62) jedenfalls mod $\bar{\mathfrak{p}}$. Anderseits ist die Kongruenz (61) nicht lösbar in k. Daher folgt nach dem ersten Hilfssatze, daß der Relativgrad $\bar{f}$ von $\bar{\mathfrak{p}}$ durch 5 teilbar, und folglich $\bar{f} = 5$ sein muß. Das bedingt aber nach unserer Tabelle in Abschnitt 2 den Fall 10.

III. Wenn v durch 5 teilbar und $\frac{I}{\varkappa}$ fünfter Potenzrest (mod $\mathfrak{p}^{v+1}$) ist, dann tritt der Fall 15 ein.

Nach Voraussetzung ist also jetzt die Kongruenz

$$x^5 \equiv \frac{1}{\varkappa} \pmod{\mathfrak{p}^{\nu+1}}$$

in k lösbar, und daher, wie man leicht einsieht, auch die Kongruenz

$$y^5 \equiv \frac{\nu}{2^6\, 3^3\, \zeta} \pmod{\mathfrak{p}^{N+\nu}} \qquad (63)$$

in k lösbar. Ist η irgend eine Wurzel der Kongruenz (63), so ist, wenn wir nach Potenzen von ν entwickeln, und nur die Glieder bis und mit der ersten Potenz in ν berücksichtigen, falls $\varepsilon \neq 1$ eine 5^{te} Einheitswurzel ist:

$$G(S) \equiv \prod_{i=1}^{5} \left[S + \varepsilon^i \cdot 12\,\zeta\eta + \varepsilon^{2i} \cdot 12\,\zeta\eta^2 + \varepsilon^{3i} \cdot 84\,\zeta\eta^3 - \varepsilon^{4i} \cdot 84\,\zeta\eta^4 + 0.\nu + \ldots \right] \pmod{\mathfrak{p}^N}.$$

Wendet man hier den zweiten Hilfssatz mit $l = 5$, $m = v$, $m' = v'$ an, so sieht man, daß die dort erwähnte Determinante zu $\mathfrak{p}$ teilerfremd ist, und folglich $G(S)$ nach einer beliebig hohen Potenz von $\mathfrak{p}$ in Linearfaktoren zerlegbar ist. Folglich tritt nach dem ersten Ore'schen Satze, da ε nach Voraussetzung in k liegt, der Fall 15 ein.

Man sieht, daß sich unsere Ausführungen und Resultate sehr vereinfachen, wenn man annimmt, daß der Grundkörper die 60. Einheitswurzeln enthält.

(Eingegangen den 18. Februar 1933)