Zeitschrift: Commentarii Mathematici Helvetici

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 7 (1934-1935)

Artikel: Über die Gradteilerzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern.

Autor: Gut, Max

DOI: https://doi.org/10.5169/seals-515588

Über die Gradteilerzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern

Von Max Gut, Zürich

Die vorliegende Arbeit ist die Fortsetzung von zwei in dieser Zeitschrift erschienenen Arbeiten[1]) und bringt die Zerlegung derjenigen Primideale eines die 5. Einheitswurzeln enthaltenden algebraischen Zahlkörpers k in einem relativ-ikosaedrischen Erweiterungskörper K, welche Teiler von 60 sind. Die Untersuchung zeigt aber, daß diese Zerlegung stark vom Grundkörper abhängt, nämlich besonders von der absoluten Ordnung des zu zerlegenden Primideales von k, und ich beschränke mich daher hier auf solche Grundkörper k, deren Relativdifferente in bezug auf den Körper der 5. Einheitswurzeln zu 60 teilerfremd ist.

Als Korollar ergibt sich die notwendige und hinreichende Bedingung dafür, daß in der Relativdiskriminanten von K in bezug auf k kein Primideal $\mathfrak{p}$ von k auftritt, das ein Teiler von 60 ist, und damit in Verbindung mit einem früheren Resultate[2]) die notwendige und hinreichende Bedingung dafür, daß die Relativdiskriminante von K in bezug auf k gleich 1 ist.

Ist $\mathfrak{p}$ ein Teiler von 3, so kann man die Größe $\varkappa - 12^3$ immer auf eine solche Form bringen, daß $\mathfrak{p}$ nicht zugleich im Zähler und Nenner von $\varkappa - 12^3$ aufgeht. Dann teilt $\mathfrak{p}$ dann und nur dann die Relativdiskriminante von K in bezug auf k *nicht*, wenn entweder der Exponent der Potenz, in der $\mathfrak{p}$ im Zähler von $\varkappa - 12^3$ aufgeht, mindestens gleich 6 und gerade ist, oder dieser Exponent gleich Null und gleichzeitig der Exponent der Potenz, in der $\mathfrak{p}$ im Nenner von $\varkappa - 12^3$ aufgeht, durch 5 teilbar ist.

Ist $\mathfrak{p}$ ein Teiler von 2, so kann man die Größe $\varkappa$ immer auf eine solche Form bringen, daß $\mathfrak{p}$ nicht zugleich im Zähler und Nenner von $\varkappa$ aufgeht. Dann teilt $\mathfrak{p}$ dann und nur dann die Relativdiskriminante von K in bezug auf k *nicht*, wenn entweder der Exponent der Potenz, in der $\mathfrak{p}$ im Zähler von $\varkappa$ auftritt, mindestens gleich 12 und durch 3 teilbar ist, oder dieser Exponent gleich Null, und gleichzeitig der Exponent der Potenz, in der $\mathfrak{p}$ im Nenner von $\varkappa$ aufgeht, durch 5 teilbar ist.

---

[1]) vgl. die Note: Über die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern, vol. 4 (1932), pg. 219, zitiert mit N., und: Weitere Untersuchungen über die Primidealzerlegung in gewissen relativ-ikosaedrischen Zahlkörpern, vol. 6 (1933), pg. 47, zitiert mit W.

[2]) W., S. 48.

Ist $\mathfrak{p}$ ein Teiler von 5, so kann man $\varkappa$ immer eine solche Form geben, daß von den 3 Größen: Zähler von $\varkappa$, Zähler von $\varkappa - 12^3$ und Nenner von $\varkappa$ höchstens eine durch $\mathfrak{p}$ teilbar ist, und dann lautet die notwendige und hinreichende Bedingung dafür, daß $\mathfrak{p}$ *nicht* in der Relativdiskriminanten von K in bezug auf k auftritt, so:

1. Ist der Exponent der Potenz, in welcher $\mathfrak{p}$ im Zähler von $\varkappa$ auftritt, positiv, so muß er mindestens gleich 10 und $\equiv 1 \pmod{3}$ sein.

2. Ist der Exponent der Potenz, in welcher $\mathfrak{p}$ im Zähler von $\varkappa - 12^3$ auftritt, positiv, so muß er mindestens gleich 10 und gerade sein.

3. Ist der Exponent der Potenz, in welcher $\mathfrak{p}$ im Nenner von $\varkappa$ auftritt, positiv und gleich v, so muß er durch 5 teilbar und außerdem $\frac{1}{\varkappa}$ fünfter Potenzrest mod. $\mathfrak{p}^{v+5}$ sein.

4. Sind alle die erwähnten drei Exponenten gleich Null, und ist mit ganzem γ von k und für δ in k mit zu $\mathfrak{p}$ teilerfremdem Nenner $\varkappa = \gamma^5 + (1 - \varepsilon)\,\delta$, ferner (für positives s): $\mathfrak{p}^s \mid \varkappa - \gamma^5 - 5\,\gamma^4 - 40\,\gamma^3$, so muß $s \geqq 5$ sein ($\varepsilon = e^{\frac{2\pi i}{5}}$).

Für einige Hauptfälle werden die Untersuchungen nicht weitläufiger, wenn man voraussetzt, daß die absolute Ordnung e eines Primteilers $\mathfrak{p}$ von 2 oder von 3 in k beliebig, und nicht gerade $e = 1$ genommen wird, und wir verzichten daher in diesen Fällen auf die oben erwähnte Beschränkung des Grundkörpers[3]).

§ 1.

Ist k ein beliebiger Grundkörper, der also die 5. Einheitswurzeln nicht zu enthalten braucht, so entscheidet, wie aus der Tabelle W., Seite 52, zu entnehmen ist und dort auch schon auf Seite 51 bemerkt wurde, der Zerlegungstypus in einem Erweiterungskörper $\bar{k}$ vom 12. Relativgrade in bezug auf k (welcher Erweiterungskörper also zu einer zyklischen Gruppe von der Ordnung 5 gehört $\mathfrak{U} = \mathscr{C}_5$) jedenfalls immer über den Zerlegungstypus in K. In der Folge wird es sich aber als vorteilhaft erweisen, auch Resolventen 6. Grades der Ikosaedergleichung herbeizuziehen, und wir geben daher hier zuerst noch die entsprechende Tafel für den Fall, daß die Untergruppe $\mathfrak{U}$ gleich einer Diedergruppe $\mathscr{D}_{10}$ von der Ordnung 10 ist:

[3]) Umgekehrt wäre es sehr zu begrüßen, wenn eine Darstellung der ganzen Theorie bei Beschränkung von k auf den Körper der 5. Einheitswurzeln selbst gegeben würde, da hiebei viele Unterfälle wegfallen und einfache Resultate zu erwarten sind.

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

§ 2.

Während wir den Zerlegungstypus der zu 60 teilerfremden Primideale $\mathfrak{p}$ von k in der vorangehenden Arbeit unter Verwendung zweier einfacher Hilfssätze unmittelbar vermöge der beiden Hauptsätze der Ore'schen Theorie bestimmten, werden wir in dieser Arbeit ausgiebig Gebrauch machen von den Newton'schen Polygonen. Diese Anwendung der Newton'schen Polygone in der Theorie der algebraischen Zahlkörper läßt sich folgendermaßen zusammenfassen[4]:

Es sei $f(x)$ ein normiertes irreduzibles Polynom eines beliebigen algebraischen Zahlkörpers k, und K ein durch *eine* Wurzel von $f(x)$

[4]) *Ö. Ore*, Newton'sche Polygone in der Theorie der algebraischen Körper. Math. Ann., Band 99 (1928), S. 84. Die Theorie ist dort nur durchgeführt für den Fall, daß der Grundkörper der rationale Zahlkörper ist. Wir formulieren sie hier für einen beliebigen Grundkörper k, da sie sich offenbar übertragen läßt, wobei aber eine explizite Darstellung wohl eine ziemliche Arbeit erfordern dürfte.

festgelegter Erweiterungskörper von k, ferner $\mathfrak{p}$ irgend ein Primideal von k, endlich a eine natürliche Zahl, die größer ist als der Exponent der Potenz, in der $\mathfrak{p}$ in der Diskriminante von $f(x)$ aufgeht. Es sei dann

$$f(x) \equiv \varphi_1(x)^{a_1}\, \varphi_2(x)^{a_2} \ldots\ldots \varphi_s(x)^{a_s} \pmod{\mathfrak{p}}$$

die Zerlegung mod. $\mathfrak{p}$ von $f(x)$ in normierte Primpolynome von k; für jedes $t = 1, 2, \ldots s$ sei m_t der Grad von $\varphi_t(x)$, und gemäß dem Schönemann'schen Satze:

$$f(x) \equiv \Phi_1(x)\, \Phi_2(x) \ldots\ldots \Phi_s(x) \pmod{\mathfrak{p}^{\alpha}},$$

wobei für jeden Index t:

$$\Phi_t(x) \equiv \varphi_t(x)^{a_t} \pmod{\mathfrak{p}}.$$

Dann folgt zunächst aus dieser Tatsache, daß das Primideal $\mathfrak{p}$ in K eine Idealzerlegung von der Form hat:

$$\mathfrak{p} = \mathfrak{A}_1\, \mathfrak{A}_2 \ldots\ldots \mathfrak{A}_s,$$

wobei die Ideale $\mathfrak{A}_t$ zueinander teilerfremd sind, und die Relativnorm von $\mathfrak{A}_t$, genommen in K in bezug auf k ist:

$$N_{K/k}(\mathfrak{A}_t) = \mathfrak{p}^{a_t m_t}.$$

Um die weitere Zerlegung eines dieser Ideale $\mathfrak{A}_t$ zu bestimmen, konstruiere man das Polygon $(\pi, \varphi_t(x))$ von $\Phi_t(x)$ oder von $f(x)$, wo π eine Hensel'sche Primzahl in bezug auf $\mathfrak{p}$ ist, d. h. eine ganze Zahl von k, die durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar ist. Hat dann unter Weglassung des Index t die i-te Seite des Newton'schen Polygones von $\Phi(x)$ die Länge l_i und die Höhe h_i, ist ferner

$$\left.\begin{aligned} l_i &= \varepsilon_i \lambda_i \\ h_i &= \varepsilon_i \varkappa_i \end{aligned}\right\} \text{ so daß } (\lambda_i, \varkappa_i) = 1,$$

entspricht dieser Seite das Polynom $F_i(x, y)$ vom Grade ε_i in y, und hat dieses die Primpolynomzerlegung $(\text{modd. } \pi, \varphi(x))$:

$$F_i(x, y) \equiv F_1^{(i)}(x, y)^{a_1^{(i)}} \cdot F_2^{(i)}(x, y)^{a_2^{(i)}} \ldots F_{t_i}^{(i)}(x, y)^{a_{t_i}^{(i)}} \quad (\text{modd.}\, \pi, \varphi(x)),$$

so besteht für $\mathfrak{A}$ die weitere Zerlegung:

$$\mathfrak{A} = \prod_{i=1}^{S} \prod_{j=1}^{t_i} \mathfrak{C}_j^{(i)\lambda_i}, \quad N_{K/k}(\mathfrak{C}_j^{(i)}) = \mathfrak{p}^{m m_j^{(i)} a_j^{(i)}},$$

wobei alle Ideale $\mathfrak{C}_j^{(i)}$ zueinander teilerfremd sind. Hiebei bedeutet S die Anzahl der Seiten des Newton'schen Polygons und $m_j^{(i)}$ ist der Grad von $F_j^{(i)}(x, y)$ als Polynom in y aufgefaßt.

Wenn dann $\mathfrak{P}_j^{(i)}$ ein Primidealteiler von $\mathfrak{C}_j^{(i)}$ in K ist, so ist der Relativgrad von $\mathfrak{P}_j^{(i)}$ durch $m m_j^{(i)}$ teilbar. Ist dann $a_j^{(i)} = 1$, so wird daher $\mathfrak{C}_j^{(i)}$ gleich einem Primideal $\mathfrak{P}_j^{(i)}$ von K vom Relativgrade $m m_j^{(i)}$ und von der Relativordnung λ_i in bezug auf k. Ist bei einer relativ-definierenden Gleichung $f(x) = 0$ jedes $a_j^{(i)} = 1$, so nennt man $f(x)$ *regulär* in bezug auf $\mathfrak{p}$.

Ein einfacher Kunstgriff gestattet im folgenden oft, reguläre Gleichungen mit $\varphi(x) = x$ zu bekommen. Ist nämlich das normierte, irreduzible, relativ-definierende Polynom $f(x)$ zunächst nicht kongruent x^n (mod. $\mathfrak{p}$), wo n der Grad von $f(x)$ ist, so setze man $\tilde{\omega}\, x = X$, wo $\tilde{\omega}$ eine durch $\mathfrak{p}$ teilbare ganze Zahl von k ist, dann ist

$$f^*(X) = \tilde{\omega}^n f\left(\frac{X}{\tilde{\omega}}\right) = 0$$

ein normiertes, irreduzibles, relativ-definierendes Polynom und

$$f^*(X) \equiv X^n \pmod{\mathfrak{p}}.$$

Verwendet man dieses Verfahren, so wird für jedes i die Ordinate des Newton'schen Polygons (π, x) von $f(x)$, die dem Koeffizienten von x^{n-i} entspricht, um Ni erhöht, falls die natürliche Zahl N der Exponent der Potenz ist, in welcher $\mathfrak{p}$ in $\tilde{\omega}$ aufgeht. Wenn dieser Kunstgriff bei einem Polynom $f(x)$ zu verwenden ist, so werden wir daher nur sagen: „Man stelle $f(x)$ auf eine Treppe". Wie man nämlich leicht einsieht, ist die explizite Durchführung der Substitution $\tilde{\omega}\, x = X$ überflüssig, und man hat nur das Newton'sche Polygon von $f(x)$ schon von vorneherein auf einer geraden Strecke („Treppe") aufzuzeichnen, die durch den Koordinatenursprung und einen Gitterpunkt (n, nN) geht, wo n der Grad von $f(x)$ und N eine beliebige natürliche Zahl ist.

Man erkennt ferner unmittelbar, daß es bei der Untersuchung einer relativ-definierenden, normierten Gleichung $f(x) = 0$ nach einem bestimmten Primideal $\mathfrak{p}$ nichts ausmacht, wenn $f(x)$ gebrochene algebraische Zahlkoeffizienten hat, wenn deren Nenner alle zu $\mathfrak{p}$ teilerfremd sind, und wir werden von diesem Umstand beständig Gebrauch machen, um die Darstellung kürzer zu gestalten. Unter der Potenz, in der $\mathfrak{p}$ in der Diskriminanten von $f(x)$ aufgeht, versteht man dann immer die Potenz, in der es im Zähler derselben aufgeht.

Mit einer einzigen Ausnahme ist es mir in allen Fällen gelungen, reguläre Gleichungen zu finden, bezw. den Zerlegungstypus von $\mathfrak{p}$ vermöge einer Kongruenz mod. $\mathfrak{p}$ zu charakterisieren, resp. vermöge einer Kongruenz, die mit einer solchen oder einer Folge von wenigen solchen Kongruenzen äquivalent ist. Dieser Ausnahmefall betrifft einen Unterfall bei der Zerlegung eines Primteilers $\mathfrak{p}$ von 2, vgl. Ende von § 4. Immerhin kann auch in diesem Falle die Entscheidung wenigstens von einer Kongruenz 4. Grades (aber eben nach einer höheren Potenz von $\mathfrak{p}$) abhängig gemacht werden.

Wie man ohne Schwierigkeit erkennt, lassen sich mit Hilfe der hier angewandten Methode, insbesondere des erwähnten Kunstgriffes, auch die in W. in § 4 enthaltenen Untersuchungen ganz bedeutend viel kürzer gestalten[5]). Ich komme hier nicht darauf zurück, da sich ja natürlich nichts an den Resultaten ändert. Daß die dort in den Überschriften der Unterfälle auftretenden binomischen Kongruenzen ihrem Wesen nach auch Kongruenzen mod. $\mathfrak{p}$ sind, ist auch klar, denn sie bringen nur die Freiheit in der Wahl einer Hensel'schen Primzahl zum Ausdruck.

Jede in der Folge verwendete Resolvente entspringt einer der drei folgenden Gleichungen 21, S. 102; 49, S. 111, resp. 63, S. 60 des Ikosaederbuches[6]):

$$\left.\begin{aligned} \varkappa : \varkappa - 12^3 : 1 = {} & [r-3]^3\ [r^2 - 11\,r + 64] \\ & : r\,[r^2 - 10\,r + 45]^2 \\ & : -1 \end{aligned}\right\} \tag{1}$$

$$\left.\begin{aligned} \varkappa : \varkappa - 12^3 : 1 = {} & [\xi^2 - 10\,\xi + 5]^3 \\ & : [\xi^2 - 4\,\xi - 1]^2\ [\xi^2 - 22\,\xi + 125] \\ & : -\xi \end{aligned}\right\} \tag{2}$$

$$\left.\begin{aligned} \varkappa : \varkappa - 12^3 : 1 = {} & [-(\Xi^{20}+1) + 228\,(\Xi^{15} - \Xi^5) - 494\,\Xi^{10}]^3 \\ & : \ -[(\Xi^{30}+1) + 522\,(\Xi^{25} - \Xi^5) - 10005\,(\Xi^{20} + \Xi^{10})]^2 \\ & : \Xi^5\,[(\Xi^{10} - 1) + 11\,\Xi^5]^5. \end{aligned}\right\} \tag{3}$$

---

[5]) Auch § 3 von W. kann dann weggelassen werden.

[6]) *Klein, Felix,* Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade, Leipzig 1884. Vgl. hiezu auch N., S. 219/220 und W., S. 47 und 56.

§ 3.

Es sei in folgendem und bis am Schlusse dieser Arbeit k wieder ein algebraischer Zahlkörper, der die 5. Einheitswurzeln enthält, und (3) die einen relativ-ikosaedrischen Erweiterungskörper K von k definierende Gleichung.

In diesem Abschnitt untersuchen wir die Zerlegung der in 3 aufgehenden Primideale von k, $\mathfrak{p}$ möge also in § 3 immer ein solches bedeuten[7]). Man kann $\varkappa$ auf eine solche Form bringen, daß in

$$\varkappa = \frac{\lambda}{\mu}$$

die beiden ganzen Zahlen λ und μ von k nicht gleichzeitig durch $\mathfrak{p}$ teilbar sind[8]). Ist in diesem Abschnitt immer[9]):

$$\mathfrak{p}^{u} \,\|\, \lambda, \quad \mathfrak{p}^{v} \,\|\, \mu, \quad \mathfrak{p}^{w} \,\|\, \lambda - 12^3\mu, \quad \mathfrak{p}^{e} \,\|\, 3,$$

dann sind also die beiden Exponenten u und w entweder beide gleichzeitig gleich 0, oder beide gleichzeitig positiv. Es ergeben sich daher 3 Hauptfälle, die ich, um die Analogie mit N. und W. zu wahren, folgendermaßen bezeichne:

A.) $u = v = w = 0.$
F.) $v > 0, \; u = w = 0.$
G.) $v = 0, \; u > 0, \; w > 0.$

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

Je nachdem die Zerlegung von

$$(r - 3)^3\,(r^2 - 11\,r + 64) + \varkappa \equiv r^3\,(r - 1)^2 + \varkappa \equiv 0 \;(mod.\ \mathfrak{p}) \qquad (4)$$

in Primpolynome mod. $\mathfrak{p}$ *genau keinen, zwei, einen, bezw. fünf Linearfaktoren hat, gilt der Fall 10, 12, 14, bezw. 15.*

Denn die Diskriminante des ersten Polynomes in (4) [vgl. auch Formel (1)] ist gleich

$$5^5\,\varkappa^2\,(\varkappa - 12^3)^2, \qquad (5)$$

also teilerfremd zu $\mathfrak{p}$, so daß der Satz unmittelbar aus der Tabelle W., S. 52 folgt.

---

7) Weil für die Teiler von 3 die Verhältnisse am einfachsten sind, nehmen wir diese Primteiler zuerst.
8) Vgl. N., S. 228.
9) Vgl. W., S. 53/54.

F.) $v > 0,\ u = w = 0$.

$v \not\equiv 0$ **(mod. 5):** *Fall 9.*

$$v \equiv 0 \text{ (mod. 5)}: \begin{cases} \dfrac{1}{\varkappa} \textit{ fünfter Potenznichtrest mod. } \mathfrak{p}^{v+1}: \textit{Fall 10.} \\ \dfrac{1}{\varkappa} \textit{ fünfter Potenzrest mod. } \mathfrak{p}^{v+1}: \textit{Fall 15.} \end{cases}$$

Setzt man in (1) die Größe $r = 3 + \dfrac{1}{x}$, so erhält man die Resolvente:

$$f(x) = x^5 + 40\,\frac{1}{\varkappa}\,x^2 - 5\,\frac{1}{\varkappa}\,x + \frac{1}{\varkappa} = 0. \tag{6}$$

Falls $v \not\equiv 0$ (mod. 5) ist, hat das zugehörige Newton'sche Polygon nur eine Seite mit $\lambda_1 = 5$, so daß der Fall 4 oder der Fall 9 eintreten muß. Setzt man in (3) die Größe $\Xi^5 = \varkappa x$, so ist für die daraus entstehende normierte Resolvente 12. Grades:

$$g(x) \equiv x^{11}(x+1) \quad (\text{mod. } \mathfrak{p}).$$

Daher hat $\mathfrak{p}$ im zugehörigen Erweiterungskörper $\bar{k}$ vom Relativgrade 12 über k einen Primidealteiler vom Relativgrad und von der Relativordnung 1. Mithin gilt, wie aus der rechten Seite der Tabelle W., S. 52 folgt, der Fall 9 und nicht der Fall 4.

Falls $v \equiv 0$ (mod. 5) ist, hat das Newton'sche Polygon nur eine Seite und das zugeordnete Polynom von (6) ist:

$$F_1(x, y) \equiv y^5 + \left(\frac{1}{\varkappa}\right) \cdot \frac{1}{\pi^v} \quad (\text{mod. } \mathfrak{p}),$$

wo π eine Hensel'sche Primzahl in bezug auf das Primideal $\mathfrak{p}$ bedeutet. Je nachdem, ob $\dfrac{1}{\varkappa}$ fünfter Potenznichtrest (mod. $\mathfrak{p}^{v+1}$) ist oder nicht, ist dieses Polynom irreduzibel (mod. $\mathfrak{p}$) oder zerfällt in 5 voneinander verschiedene Linearfaktoren, da k die fünften Einheitswurzeln enthält.

G.) $v = 0,\ u > 0,\ w > 0$.

Beschränkt man sich auf den Fall, dass die absolute Ordnung e von $\mathfrak{p}$ gleich 1 ist, so treten je nach dem Wert von w folgende Fälle auf:

$w = 1$ *und* $w = 5$: *Fall 5.*

$w = 2$ *und* $w = 4$: $\begin{cases} \varkappa - 12^3 \text{ quadratischer Nichtrest mod. } \mathfrak{p}^{w+1}\text{: Fall 6.} \\ \varkappa - 12^3 \text{ quadratischer Rest mod. } \mathfrak{p}^{w+1}\text{: Fall 11.} \end{cases}$

$w = 3$:
- $u \not\equiv 0$ (*mod.* 3): *Fall 5.*
- $u = 3\,u' \geqq 3$ *und mit ganzem* γ *von* k *und für* δ *mit zu* $\mathfrak{p}$ *teilerfremdem Nenner* $\varkappa = 2^3 \cdot 5 \cdot 3^{3u'}\,\gamma^3\,(1 - 3\,\delta)$:
  - $u' = 1$ $\begin{cases} \gamma \not\equiv \delta \;(\textit{mod. } \mathfrak{p})\text{: Fall 5.} \\ \gamma \equiv \delta \;(\textit{mod. } \mathfrak{p})\text{: Fall 13.} \end{cases}$
  - $u' > 1$ $\begin{cases} \delta \not\equiv 0 \;(\textit{mod. } \mathfrak{p})\text{: Fall 5.} \\ \delta \equiv 0 \;(\textit{mod. } \mathfrak{p})\text{: Fall 13.} \end{cases}$

$w = 6$: *Je nachdem, ob die Kongruenz* $y^3 - y^2 + \dfrac{\varkappa - 12^3}{3^6} \equiv 0$ (*mod.* $\mathfrak{p}$) *genau keinen, einen, bezw. 3 Linearfaktoren in* k *hat: Fall 12, 14, bezw. 15.*

$w > 6$:
- w **ungerade**: *Fall 13.*
- w **gerade**: $\begin{cases} \varkappa - 12^3 \text{ quadratischer Nichtrest mod. } \mathfrak{p}^{w+1}\text{: Fall 14.} \\ \varkappa - 12^3 \text{ quadratischer Rest mod. } \mathfrak{p}^{w+1}\text{: Fall 15.} \end{cases}$

Zunächst ist bei beliebigem e in diesem Unterfalle

$$(r - 3)^3\,(r^2 - 11\,r + 64) + \varkappa \equiv r^3\,(r - 1)^2 \;(\text{mod. } \mathfrak{p}),$$

und folglich zerfällt $\mathfrak{p}$ in einem Erweiterungskörper $\bar{k}$ vom 5. Grade in bezug auf k[10]) in mindestens 2 voneinander verschiedene Primideale, für welche das Produkt aus Relativordnung und Relativgrad höchstens die Werte 1, 2 oder 3 haben kann. Gemäß der Tabelle W., S. 52 ergeben sich mithin nur folgende sieben möglichen Fälle: 5, 6; 11, 12, 13, 14 und 15, und die Entscheidung, welcher von diesen Fällen eintritt, fällt jedenfalls schon immer in einem Erweiterungskörper $\bar{k}$ vom 5. Grade in bezug auf k.

Setzt man in (1) die Größe $r^2 - 10\,r + 45 = -\,x$, so erhält man die Resolvente:

$$f\,(x) = x^5 + 45\,x^4 + 10\,(\varkappa - 12^3)\,x^2 + (\varkappa - 12^3)^2 = 0. \tag{7}$$

Es sei die absolute Ordnung e von $\mathfrak{p}$ im folgenden gleich 1[11]).

---

[10]) Natürlich ist hier und in allen analogen Fällen vorausgesetzt, daß $\bar{k}$ in K enthalten sei.

[11]) Man sieht leicht, daß für beliebiges e die Gleichung (7) regulär ist für $w \geqq 6e$. Es ist umgekehrt $r = -(\varkappa - 12^3)\,x^{-2}$, so daß $k\,(r) = k\,(x)$ ist.

Ist $w > 6$, so hat das Newton'sche Polygon 3 Seiten mit den Längen $l_1 = 1$, $l_2 = l_3 = 2$. Für ungerades w sieht man sofort, daß der Fall 13 gilt, für gerades w darf man setzen:

$$F_2(x, y) \equiv F_3(x, y) \equiv y^2 - \frac{\varkappa - 12^3}{3^w} \pmod{\mathfrak{p}}, \tag{8}$$

da -1 wegen $-1 \equiv (\sqrt{5})^2 \pmod{\mathfrak{p}}$ quadratischer Rest mod. $\mathfrak{p}$ ist. Je nachdem also $\varkappa - 12^3$ quadratischer Nichtrest oder Rest (mod. $\mathfrak{p}^{w+1}$) ist, gilt daher der Fall 14 oder 15.

Ist $w = 6$, so hat das Newton'sche Polygon 2 Seiten mit den Längen $l_1 = 3$ und $l_2 = 2$, und

$$F_1(x, y) \equiv y^3 - y^2 + \frac{\varkappa - 12^3}{3^6} \pmod{\mathfrak{p}}, \; F_2(x, y) \equiv y^2 + \frac{\varkappa - 12^3}{3^6} \pmod{\mathfrak{p}}.$$

Da $\dfrac{\partial F_1(x, y)}{\partial y} \equiv -2y \pmod{\mathfrak{p}}$ ist, so ist die Diskriminante von $F_1(x, y)$ teilerfremd zu $\mathfrak{p}$, und es sind daher 3 Unterfälle möglich:

Ist die kubische Kongruenz irreduzibel, so muß der Fall 12 eintreten und die quadratische Kongruenz lösbar sein, da dann $\overline{f_1} = 3$ ist.

Hat die kubische Kongruenz genau einen Linearfaktor, so müssen in $\mathfrak{p}$ genau 3 voneinander verschiedene Primidealteiler von $\overline{k}$ aufgehen, da $\mathfrak{p}$ niemals genau 4 voneinander verschiedene solche hat. Folglich ist die quadratische Kongruenz nicht lösbar, und es gilt der Fall 14.

Hat die kubische Kongruenz 3 Linearfaktoren, so muß aus demselben Grunde die quadratische Kongruenz lösbar sein, und es gilt der Fall 15.

Ist $w = 1$ oder $w = 5$, so hat das Newton'sche Polygon von (7) zwei Seiten mit den Längen $l_1 = 3$, $l_2 = 2$ und die zugehörigen λ_i haben dieselben Werte, folglich gilt der Fall 5.

Ist $w = 2$ oder $w = 4$, so hat das Newton'sche Polygon von (7) ebenfalls zwei Seiten mit denselben Längen $l_1 = 3$ und $l_2 = 2$ und $\lambda_1 = 3$, dagegen $\lambda_2 = 1$ mit demselben zugeordneten Polynome $F_2(x, y)$ wie in (8). Daher gilt der Fall 6 oder der Fall 11, je nachdem $\varkappa - 12^3$ quadratischer Nichtrest (mod. $\mathfrak{p}^{w+1}$) oder quadratischer Rest (mod. $\mathfrak{p}^{w+1}$) ist.

Es bleibt der Fall $w = 3$ zu untersuchen übrig. Dann ist, wegen

$$\varkappa = (\varkappa - 12^3) + 2^6 \cdot 3^3$$

der Wert von $u \geqq 3$.

Ist $\varphi(x) = x - 3$ und $\psi(x) = x - \frac{11}{2}$, so hat

$$f(x) = (x - 3)^3 \, (x^2 - 11\, x + 64) + \varkappa$$

mod. $\mathfrak{p}$ die Primpolynomzerlegung:

$$f(x) \equiv \varphi(x)^3 \cdot \psi(x)^2 \quad (\text{mod. } \mathfrak{p}),$$

also zerfällt $f(x)$ nach dem Schönemann'schen Satze nach einer beliebig hohen Potenz von $\mathfrak{p}$ in einen Faktor 3. Grades und einen Faktor 2. Grades, deren Reihenentwicklungen nach Potenzen von $\varkappa$ die folgenden sind:

$$\Phi(x) = g(\varphi(x)) \equiv \varphi(x)^3 + \frac{\varkappa}{2^9 \cdot 5^2}[-3\varphi(x)^2 + 40\varphi(x) + 320](\text{mod. } \mathfrak{p}^{2u}), \quad (9)$$

$$\Psi(x) \equiv \psi(x)^2 + \frac{(\varkappa - 12^3)}{2^{10} \cdot 5^2}[3 \cdot 2\,\psi(x) - 95] + 3^4 \cdot \frac{\psi(x)}{2^3 \cdot 5^2} + \frac{3^7}{2^4 \cdot 5}(\text{mod. } \mathfrak{p}^{2u}). \quad (10)$$

Da $w = 3$ ist, entspricht $\Psi(x)$ gemäß (10) jedenfalls immer ein Primidealteiler von $\mathfrak{p}$ in $\bar{k}$ mit Relativgrad 1 und Relativordnung 2, und es sind also nur die Fälle 5 und 13 noch möglich.

Ist $u \not\equiv 0$ (mod. 3), so zeigt das Newton'sche Polygon für (9) sofort, daß der Fall 5 eintritt.

Ist $u \equiv 0$ (mod. 3) und $u = 3\,u' \geqq 3$, dann hat, weil der Restklassenring von $\mathfrak{p}$ ein Galoisfeld mit der Charakteristik 3 ist, die Kongruenz:

$$z^3 \equiv \frac{\varkappa}{2^3 \cdot 5 \cdot 3^{3u'}} (\text{mod. } \mathfrak{p})$$

immer eine mod. $\mathfrak{p}$ eindeutige Lösung in k, d. h. $\varkappa$ ist von der Form

$$\varkappa = 2^3 \cdot 5 \cdot 3^{3u'} \gamma^3 (1 - 3\,\delta), \quad (11)$$

wo γ eine zu $\mathfrak{p}$ teilerfremde und mod. $\mathfrak{p}$ eindeutig bestimmte ganze Zahl von k, und δ jedenfalls eine Zahl mit zu $\mathfrak{p}$ teilerfremdem Nenner ist.

Setzt man in (9) die Größe $\varphi(x) = X - 3^{u'}\gamma$, so wird nach dem Taylor'schen Lehrsatze:

$$\Phi(x) = g(X - 3^{u'}\gamma) = G(X) = X^3 + \tfrac{1}{2}g''(-3^{u'}\gamma)X^2 + g'(-3^{u'}\gamma)X + g(-3^{u'}\gamma),$$

oder eingesetzt:

$$G(X) \equiv X^3 + [-3^{u'+1}\gamma + \ldots]X^2 + [3^{2u'+1}\gamma^2 + 3^{3u'}\frac{\gamma^3}{2^3} + \ldots]X +$$

$$+ [3^{3u'+1} \cdot \frac{\gamma^3\delta}{2^6 \cdot 5}(-320 + 3^{u'} \cdot 40\gamma + 3^{2u'+1}\gamma^2) + 3^{4u'} \cdot \frac{\gamma^4}{2^6 \cdot 5}(-40 - 3^{u'+1}\gamma)]$$

$$(\text{mod. } \mathfrak{p}^{6u'}) \quad (12)$$

Hiebei enthalten die bei dem Koeffizienten einer festen Potenz von X angedeuteten weggelassenen Summanden das Primideal $\mathfrak{p}$ in einer höheren Potenz als in *jedem* der *angegebenen* Summanden, und dies soll auch im folgenden überall für die analog aufgeschriebenen Resolventen gelten.

Ist zunächst $u' > 1$, so ist in jeder eckigen Klammer bei X^2 und X der erste Term der für das Newton'sche Polygon in Betracht kommende, und daraus ergibt sich sofort, daß wenn $\delta \not\equiv 0 \pmod{\mathfrak{p}}$ ist, dasselbe aus einer einzigen Seite mit $l_1 = \lambda_1 = 3$ besteht, und es gilt mithin der Fall 5. Ist $\delta \equiv 0 \pmod{\mathfrak{p}}$, so besteht das Newton'sche Polygon aus 2 Seiten mit $l_1 = \lambda_1 = 2$ und $l_2 = \lambda_2 = 1$, und es gilt der Fall 13.

Ist $u' = 1$, so ist nach (11):

$$\begin{aligned} \varkappa - 12^3 &= 2^3 \cdot 5 \cdot 3^3 \gamma^3 (1 - 3\,\delta) - 2^6 \cdot 3^3 \\ &= 2^3 \cdot 3^3 (5\,\gamma^3 - 8) - 2^3 \cdot 5 \cdot 3^4 \gamma^3 \delta \\ &= 2^3 \cdot 3^3 \left[\, 6\,\gamma^3 - 9 - (\gamma^3 - 1)\,\right] - 2^3 \cdot 5 \cdot 3^4 \gamma^3 \delta, \end{aligned}$$

und da $w = 3$ ist, so ist $\gamma \not\equiv 1 \pmod{\mathfrak{p}}$, und folglich auch $1 + \frac{\gamma}{2^3} \not\equiv 0 \pmod{\mathfrak{p}}$. Nach (12) wird:

$$\begin{aligned} G(X) \equiv X^3 &+ \left[-3^2 \gamma + \ldots\right] X^2 + \left[3^3 \gamma^2 \left(1 + \frac{\gamma}{2^3}\right) + \ldots\right] X + \\ &+ \left[-3^4 \gamma^3 \left(\frac{\gamma}{2^3} + \delta\right) + 3^5 \frac{\gamma^4 \delta}{2^3}\right] \quad (\mathrm{mod.}\ \mathfrak{p}^6). \end{aligned}$$

Ist $\gamma \not\equiv \delta \pmod{\mathfrak{p}}$, so hat das Newton'sche Polygon eine Seite mit $l_1 = \lambda_1 = 3$, es gilt also Fall 5. Ist $\gamma \equiv \delta \pmod{\mathfrak{p}}$, so hat das Newton'sche Polygon 2 Seiten mit $l_1 = \lambda_1 = 2$, bezw. $l_2 = \lambda_2 = 1$, und folglich gilt der Fall 13.

§ 4.

In diesem Abschnitt untersuchen wir die Zerlegung der in 2 aufgehenden Primideale von k, und $\mathfrak{p}$ möge also in § 4 immer ein solches bedeuten. Dann folgt, wie in § 3, daß man $\varkappa$ auf eine solche Form bringen kann, daß in $\varkappa = \frac{\lambda}{\mu}$ die beiden ganzen Zahlen λ und μ von k nicht gleichzeitig durch $\mathfrak{p}$ teilbar sind, und falls in diesem Abschnitt immer:

$$\mathfrak{p}^u \parallel \lambda, \quad \mathfrak{p}^v \parallel \mu, \quad \mathfrak{p}^w \parallel \lambda - 12^3 \mu, \quad \mathfrak{p}^e \parallel 2,$$

so ergeben sich dieselben 3 Hauptfälle wie in § 3, und die beiden ersten werden auch bewiesen wie in § 3, weshalb ich für diese nur die Resultate angebe.

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

Je nachdem die Zerlegung von

$$(r - 3)^3 (r^2 - 11r + 64) + \varkappa \equiv r(r+1)^4 + \varkappa \equiv 0 \ (mod.\ \mathfrak{p})$$

in Primpolynome (mod. $\mathfrak{p}$) genau keinen, zwei, einen, bezw. fünf Linearfaktoren hat, gilt der Fall 10, 12, 14, bezw. 15.

F.) $v > 0,\ u = w = 0.$

$v \not\equiv 0$ **(mod. 5):** *Fall 9.*

$$v \equiv 0 \ (\text{mod. } 5)\colon \begin{cases} \dfrac{1}{\varkappa} \text{ fünfter Potenznichtrest mod. } \mathfrak{p}^{v+1}\colon \text{ Fall 10.} \\ \dfrac{1}{\varkappa} \text{ fünfter Potenzrest mod. } \mathfrak{p}^{v+1}\colon \text{ Fall 15.} \end{cases}$$

G.) $v = 0,\ u > 0,\ w > 0.$

Beschränkt man sich auf den Fall, dass die absolute Ordnung e von $\mathfrak{p}$ gleich 1 ist, so treten je nach dem Werte von u folgende Fälle auf:

$u = 1, 2, 5, 7, 10, 11$: *Fall 1.*

$$u = 3, 9\colon \begin{cases} \varkappa \text{ kubischer Nichtrest mod. } \mathfrak{p}^{u+1}\colon \text{ Fall 2.} \\ \varkappa \text{ kubischer Rest mod. } \mathfrak{p}^{u+1}\colon \text{ Fall 7.} \end{cases}$$

$u = 4, 8$ *und mit ganzem γ von k und für δ mit zu $\mathfrak{p}$ teilerfremdem Nenner* $\varkappa = 2^u \gamma^4 (1 - 2\delta)$:

$u = 4$ und $\gamma \not\equiv \delta$ (mod. $\mathfrak{p}$), bezw. $u = 8$ und $\gamma\delta \not\equiv 1$ (mod. $\mathfrak{p}$): Fall 1.
$u = 4$ und $\gamma \equiv \delta$ (mod. $\mathfrak{p}$), bezw. $u = 8$ und $\gamma\delta \equiv 1$ (mod. $\mathfrak{p}$): Fall 11.

$u = 6$: $\begin{cases} \varkappa \text{ kubischer Nichtrest mod. } \mathfrak{p}^{u+1}\colon \text{ Fall 2.} \\ \varkappa \text{ kubischer Rest mod. } \mathfrak{p}^{u+1}\colon \text{ Je nachdem ein gewisses Polynom} \end{cases}$
4. Grades mod. $\mathfrak{p}^{2w+13}$ in 2 quadratische Faktoren zerfällt, bezw. nicht zerfällt, aber nach Adjunktion der Nullstelle eines beliebigen Primpolynoms (mod. $\mathfrak{p}$) vom 2. Grade mod. $\mathfrak{p}^{4w+25}$ in 2 quadratische Faktoren zerfällt, bezw. auch nach einer solchen Adjunktion mod. $\mathfrak{p}^{4w+25}$ nicht zerfällt: Fall 13, bezw. Fall 8, bezw. Fall 7.

$u = 12$: *Je nachdem, ob die Kongruenz* $y^4 + y^3 + \frac{\varkappa}{2^{12}} \equiv 0$ (*mod.* $\mathfrak{p}$) *genau einen, keinen, bezw. vier Linearfaktoren hat*: *Fall 12, 14, bezw. 15.*

$$u > 12: \begin{cases} u \not\equiv 0 \ (\text{mod. } 3): \ \textit{Fall 11.} \\ u \equiv 0 \ (\text{mod. } 3): \begin{cases} \varkappa \ \textit{kubischer Nichtrest mod. } \mathfrak{p}^{u+1}: \ \textit{Fall 12.} \\ \varkappa \ \textit{kubischer Rest mod. } \mathfrak{p}^{u+1}: \ \textit{Fall 15.} \end{cases} \end{cases}$$

Setzt man in (1) die Größe $r = 3 + x$, so ergibt sich die Resolvente:

$$f(x) = x^5 - 5x^4 + 40x^3 + \varkappa = 0. \tag{13}$$

Stellt man $f(x)$ auf eine Treppe, so ergibt sich folgendes[12]:

$u > 12$. Dann besteht das Newton'sche Polygon aus 3 Seiten von den Längen $l_1 = l_2 = 1$, $l_3 = 3$. Ist $u \not\equiv 0$ (mod. 3), so ist $\lambda_3 = 3$, und es gilt daher der Fall 11. Ist $u \equiv 0$ (mod. 3), so ist $\lambda_3 = 1$ und

$$F_3(x, y) \equiv y^3 - \frac{\varkappa}{2^u} \ (\text{mod. } \mathfrak{p}). \tag{14}$$

Die Diskriminante von $F_3(x, y)$ ist $\not\equiv 0$ (mod. $\mathfrak{p}$). Das Polynom (14) ist entweder irreduzibel in k, oder dann zerfällt es in 3 Linearfaktoren. Denn ist a eine seiner Wurzeln in k, so ist

$$F_3(x, y) \equiv (y - a)\,(y - (\varepsilon + \varepsilon^4)\,a)\,(y - (\varepsilon^2 + \varepsilon^3)\,a) \ (\text{mod. } \mathfrak{p}),$$

wo $\varepsilon = e^{\frac{2\pi i}{5}}$. Ist die Kongruenz (14) irreduzibel in k, so gilt der Fall 12, ist sie reduzibel in k, so gilt der Fall 15.

$u = 12$. Dann besteht das Newton'sche Polygon aus 2 Seiten mit $l_1 = 1$, $l_2 = 4$, und

$$F_2(x, y) \equiv y^4 + y^3 + \frac{\varkappa}{2^{12}} \ (\text{mod. } \mathfrak{p}).$$

Da $\frac{\partial F_2(x,y)}{\partial y} \equiv y^2$ (mod. $\mathfrak{p}$), ist die Diskriminante von $F_2(x, y)$ nicht kongruent Null mod. $\mathfrak{p}$. Folglich ist $\mathfrak{p}$ jedenfalls unverzweigt in $\bar{k}$, und es gilt der Fall 12, 14, bezw. 15, je nachdem $F_2(x, y)$ genau einen, keinen, bezw. vier Linearfaktoren mod. $\mathfrak{p}$ in k hat.

Es sei von nun an $1 \leqq u \leqq 11$. Dann besteht das Newton'sche Polygon zu der auf eine Treppe gestellten Resolventen (13) aus 2 Seiten

[12]) Man sieht leicht, daß im allgemeinen Falle das auf die Treppe gestellte Polynom $f(x)$ regulär ist für $u \geqq 12\,e$.

von den Längen $l_1 = 1$ und $l_2 = 4$, und es ergeben sich gemäß der Tabelle W., S. 52 folgende Möglichkeiten:

$u \equiv \pm 1 \pmod{4}$: 1, 2, 7.

$u \equiv 2 \pmod{4}$: 1, 2, 7, 8, 13.

$u \equiv 0 \pmod{4}$: 1, 2, 7, 8, 11, 12, 13, 14, 15.

Wie aus der Tabelle in § 1 hervorgeht, fällt die Entscheidung, welcher Fall eintritt, schon immer in einem Körper $\overline{k}$ vom Relativgrade 6 in bezug auf k, dessen Zahlen also invariant sind unter einer Diedergruppe von der Ordnung 10. Setzt man in (2) die Größe $\xi = x + 5 + 2\sqrt{5}$, so ergibt sich die Resolvente 6. Grades:

$$f(x) = x^6 + 12\sqrt{5}\,x^5 + 240\,x^4 + 320\sqrt{5}\,x^3 + \varkappa x + \varkappa(5 + 2\sqrt{5}),$$

deren Newton'sches Polygon aus einer einzigen Seite (von der Länge 6) besteht.

Ist $u \equiv \pm 1 \pmod{6}$, so ist $\lambda_1 = 6$, und es tritt der Fall 1 ein.

Ist $u \equiv \pm 2 \pmod{6}$, so ist $\lambda_1 = 3$, und es tritt Fall 1 oder 11 ein.

Ist $u \equiv 3 \pmod{6}$, so ist $\lambda_1 = 2$ und $F_1(x, y) \equiv y^3 - \frac{\varkappa}{2^u} \pmod{\mathfrak{p}}$.

Diese Kongruenz ist die gleiche wie (14), und folglich ergeben sich nur 2 Möglichkeiten:

Ist $\varkappa$ kubischer Nichtrest (mod. $\mathfrak{p}^{u+1}$), so gilt der Fall 2.

Ist $\varkappa$ kubischer Rest (mod. $\mathfrak{p}^{u+1}$), so gilt der Fall 7.

Ist $u \equiv 0 \pmod{6}$, so ist $\lambda_1 = 1$, und $F_1(x, y) \equiv y^6 - \frac{\varkappa}{2^u} \equiv$

$\equiv \left(y^3 - \sqrt{\frac{\varkappa}{2^u}}\right)^2 \pmod{\mathfrak{p}}$, wobei $\sqrt{\frac{\varkappa}{2^u}}$, wie aus der Theorie der Galoisfelder unmittelbar folgt, mod. $\mathfrak{p}$ kongruent einer mod. $\mathfrak{p}$ eindeutig bestimmten Zahl des Grundkörpers k ist. Da $\sqrt{\frac{\varkappa}{2^u}}$ und $\frac{\varkappa}{2^u}$ gleichzeitig kubische Nichtreste oder kubische Reste mod. $\mathfrak{p}$ sind, so folgt:

Ist $\varkappa$ kubischer Nichtrest (mod. $\mathfrak{p}^{u+1}$), so tritt der Fall 2 oder 12 auf.

Ist $\varkappa$ kubischer Rest (mod. $\mathfrak{p}^{u+1}$), so tritt einer der Fälle 7, 8, 13, 14 oder 15 auf.

Vergleicht man beide Resultate miteinander, so liefern sie die in der Aufstellung erwähnten Fälle mit Ausnahme der Werte $u = 4$ und 8, wo noch die beiden Fälle 1 und 11 möglich sind, und des Wertes $u = 6$, wo, falls $\varkappa$ kubischer Nichtrest mod. $\mathfrak{p}^{u+1}$ ist[13]), der Fall 2 eintreten muß,

[13]) Dies ist offenbar nur dann möglich, wenn $w = 6$ ist, da $\varkappa = (\varkappa - 12^3) + 2^6 . 3^3$.

und falls $\varkappa$ kubischer Rest mod. $\mathfrak{p}^{u+1}$ ist, einer der Fälle 7, 8 oder 13 möglich ist. In jedem Falle kann die Entscheidung, welcher Fall eintritt, in einem Körper $\bar{k}$ vom Relativgrade 5 in bezug auf k getroffen werden.

Weil der Restklassenring von $\mathfrak{p}$ ein Galoisfeld von der Charakteristik 2 ist, hat die Kongruenz

$$z^4 \equiv \frac{\varkappa}{2^u} \pmod{\mathfrak{p}}$$

immer eine mod. $\mathfrak{p}$ eindeutige Lösung in k, d. h. $\varkappa$ ist von der Form

$$\varkappa = 2^u \gamma^4 (1 - 2\delta), \tag{15}$$

wo γ eine zu $\mathfrak{p}$ teilerfremde und mod. $\mathfrak{p}$ eindeutig bestimmte ganze Zahl von k, und δ jedenfalls eine Zahl mit zu $\mathfrak{p}$ teilerfremdem Nenner ist.

Setzt man in (13) die Größe $x = X + 2^{u'}\gamma$, so erhält man die Resolvente

$$f(X + 2^{u'}\gamma) = X^5 + \frac{f''''(2^{u'}\gamma)}{4!}X^4 + \frac{f'''(2^{u'}\gamma)}{3!}X^3 + \frac{f''(2^{u'}\gamma)}{2!}X^2 + \\ + \frac{f'(2^{u'}\gamma)}{1!}X + f(2^{u'}\gamma) = 0. \tag{16}$$

Sei $u = 4u'$, dann wird (16) unter Berücksichtigung von (15) für $u = 4$, d. h. $u' = 1$:

$$X^5 + 5[-1 + 2\gamma]X^4 + 2^3\cdot 5[1 - \gamma + \gamma^2]X^3 + \\ + 2^3\cdot 5\gamma[-3\gamma + 2(\gamma^2 + 3)]X^2 + 2^4\cdot 5\gamma^2[\gamma^2 - 2(\gamma - 3)]X + \\ + 2^5\gamma^3[\gamma(\gamma - \delta) - 2(\gamma - 5)] = 0,$$

bezw. für $u = 8$, d. h. $u' = 2$:

$$X^5 + 5[-1 + 2^2\gamma]X^4 + 2^3\cdot 5[1 - 2\gamma + 2^2\gamma^2]X^3 + \\ + 2^5\cdot 5\gamma[3(1 - \gamma) + 2^2\gamma^2]X^2 + 2^7\cdot 5\gamma^2[3 - 2\gamma(1 - \gamma)]X + \\ + 2^9\gamma^3[(1 - \gamma\delta) + 2(\gamma^2 - \gamma + 2)] = 0.$$

Stellt man diese Polynome auf eine Treppe, so ergibt sich, daß für $u = 4$, wenn $\gamma \not\equiv \delta \pmod{\mathfrak{p}}$, bezw. für $u = 8$, wenn $\gamma\delta \not\equiv 1 \pmod{\mathfrak{p}}$ ist, das Newton'sche Polygon aus 2 Seiten mit den Längen $l_1 = 1$, $l_2 = 4$ besteht, wobei $\lambda_2 = 4$ ist. Es gilt daher der Fall 1 und nicht der Fall 11. Ist für $u = 4$ die Größe $\gamma \equiv \delta \pmod{\mathfrak{p}}$, bezw. für $u = 8$ die Größe $\gamma\delta \equiv 1 \pmod{\mathfrak{p}}$, so besteht das Newton'sche Polygon aus 3 Seiten mit den

Längen $l_1 = 1$, $l_2 = 3$ und $l_3 = 1$, ferner ist $\lambda_2 = 3$. Es gilt daher der Fall 11 und nicht der Fall 1.

Damit bleibt nur noch der Fall zu untersuchen, wo $u = 6$ *und* $\varkappa$ *kubischer Rest mod.* $\mathfrak{p}^{u+1}$ ist. In diesem Falle ist $w \geqq 6$, und das Polynom [vgl. Formel (1)]:

$$f(x) = x(x^2 - 10x + 45)^2 + (\varkappa - 12^3), \tag{17}$$

dessen Diskriminante gemäß Formel (5) das Primideal $\mathfrak{p}$ genau in der $(2w + 12)$ten Potenz enthält, hat die Primpolynomzerlegung:

$$f(x) \equiv x(x+1)^4 \pmod{\mathfrak{p}}.$$

Nach dem Schönemann'schen Satze folgt daraus für eine beliebig große natürliche Zahl N eine Zerlegung von der Form:

$$f(x) \equiv \Psi(x) \cdot \Phi(x) \pmod{\mathfrak{p}^N},$$

wo

$$\left.\begin{aligned} \Psi(x) &\equiv x \\ \Phi(x) &\equiv (x+1)^4 \end{aligned}\right\} \pmod{\mathfrak{p}}.$$

Falls N genügend groß ist, also jedenfalls für $N \geqq 2w + 13$, enthält die Diskriminante von $\Phi(x)$ nach der bekannten Formel, wie sich die Diskriminante eines Produktes von Polynomen aus den Diskriminanten und Resultanten der Faktoren aufbaut[14]), das Primideal $\mathfrak{p}$ in der gleichen Potenz wie die Diskriminante von (17).

Bis auf Glieder in zweiter oder höherer Potenz von $(\varkappa - 12^3)$ ist übrigens[15]):

$$\Phi(x) \equiv (x^2 - 10x + 45)^2 + \frac{\varkappa - 12^3}{3^4 \cdot 5^2}(-x^3 + 20x^2 - 190x + 900) \pmod{\mathfrak{p}^{2w}}.$$

Auf Grund der beiden Hauptsätze der Ore'schen Theorie, eines weiteren Satzes von Ore[16]) und der Tabelle W., S. 52 folgt mithin, daß der Fall 13, bezw. 8, bezw. 7 gilt, je nachdem $\Phi(x)$ mod. $\mathfrak{p}^{2w+13}$ in zwei quadratische Faktoren zerfällt, bezw. nicht zerfällt, aber nach Adjunktion der Nullstelle eines beliebigen Primpolynoms mod. $\mathfrak{p}$ vom 2. Grade von k mod. $\mathfrak{p}^{4w+25}$ in zwei quadratische Faktoren zerfällt, bezw. auch nach einer solchen Adjunktion mod. $\mathfrak{p}^{4w+25}$ nicht zerfällt. Leider habe ich auch unter Her-

---

[14]) Vgl. z. B. *Hensel, K.*, Theorie der algebraischen Zahlen, Erster Band, Leipzig und Berlin 1908, S. 60, Formel (7).

[15]) Vgl. auch W., S. 66, Formel (41).

[16]) Satz 8, S. 584 von: *Ö. Ore*, Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern, zweite Mitteilung. Math. Ann., Band. 97 (1927), S. 569.

beiziehung gewisser Resolventen 6. Grades, die sich hier eventuell gut eignen, keine einfache und vollständige Regel dafür finden können, welcher der 3 Fälle eintritt, weshalb ich es bei dem angegebenen Kriterium bewenden lasse.

§ 5.

In diesem Abschnitt untersuchen wir die Zerlegung der in 5 aufgehenden Primideale $\mathfrak{p}$ von k. Man kann $\varkappa$ auf eine solche Form bringen, daß in $\varkappa = \frac{\lambda}{\mu}$ die beiden ganzen Zahlen λ und μ von k nicht gleichzeitig durch $\mathfrak{p}$ teilbar sind, so daß, falls in diesem Abschnitt immer:

$$\mathfrak{p}^u \mid \lambda\,, \quad \mathfrak{p}^v \mid \mu\,, \quad \mathfrak{p}^w \mid \lambda - 12^3\mu\,, \quad \mathfrak{p}^{4e} \mid 5\,,$$

von den 3 Zahlen u, v, w immer höchstens eine positiv ist. Es ergeben sich daher 4 Hauptfälle, die ich, um die Analogie mit N. und W. zu wahren, folgendermaßen bezeichne:

A.) $u = v = w = 0.$
BC.) $u > 0,\ v = w = 0.$
DE.) $w > 0,\ u = v = 0.$
F.) $v > 0,\ u = w = 0.$

Wir beschränken uns in diesem Abschnitt überall auf den Fall, daß $4e = 4$ ist; wo für gewisse Überlegungen $4e$ beliebig sein darf, wird dies immer ausdrücklich hervorgehoben werden.

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

Ist mit ganzem zu $\mathfrak{p}$ teilerfremdem γ von k und für δ mit zu $\mathfrak{p}$ teilerfremdem Nenner:

$$\varkappa = \gamma^5 + (1 - \varepsilon)\,\delta, \quad \varepsilon = e^{\frac{2\pi i}{5}}, \tag{18}$$

ferner für positives s:

$$\mathfrak{p}^s \mid \varkappa - \gamma^5 - 5\gamma^4 - 40\gamma^3, \tag{19}$$

so treten je nach dem Wert von s folgende Fälle auf:

$1 \leqq s \leqq 4$: $\begin{cases} \varkappa(\varkappa - 12^3) \text{ quadratischer Nichtrest mod. } \mathfrak{p}\text{: Fall 4.} \\ \varkappa(\varkappa - 12^3) \text{ quadratischer Rest mod. } \mathfrak{p}\text{: Fall 9.} \end{cases}$

$s = 5$: $\begin{cases} \varkappa(\varkappa - 12^3) \text{ quadratischer Nichtrest mod. } \mathfrak{p}\text{: Fall 14.} \\ \varkappa(\varkappa - 12^3) \text{ quadratischer Rest mod. } \mathfrak{p}\text{: Je nachdem die Kongruenz} \end{cases}$

$$y^5 - \gamma^2 (\gamma + 2)^2 y + \frac{\varkappa - \gamma^5 - 5\gamma^4 - 40\gamma^3}{(1-\varepsilon)^5} \equiv 0 \ (mod.\ \mathfrak{p})$$

irreduzibel, bezw. reduzibel ist: Fall 10, bezw. Fall 15.

$s > 5.$ $\begin{cases} \varkappa(\varkappa - 12^3) \text{ quadratischer Nichtrest mod. } \mathfrak{p}: \text{ Fall 14.} \\ \varkappa(\varkappa - 12^3) \text{ quadratischer Rest mod. } \mathfrak{p}: \text{ Fall 15.} \end{cases}$

Zum Beweise machen wir zunächst folgende Vorbemerkung, die übrigens für eine beliebige Ordnung $4e$ von $\mathfrak{p}$ gilt. Setzt man in (3) die Größe $\Xi^5 = x$, so ergibt sich die Resolvente:

$$f(x) = -[-x^4 + 228x^3 - 494x^2 - 228x - 1]^3 + \\ + \varkappa x [x^2 + 11x - 1]^5 = 0. \tag{20}$$

Unter der Annahme $u = v = w = 0$ folgt:

$$f(x) \equiv (x-2)^{12} + \varkappa x (x-2)^{10} \ (\text{mod. } \mathfrak{p}),$$

oder

$$f(x) \equiv [x-2]^{10} \left[(x-2) - 2\varkappa - \sqrt{\varkappa(12^3-\varkappa)}\right] \cdot \\ \cdot \left[(x-2) - 2\varkappa + \sqrt{\varkappa(12^3-\varkappa)}\right] \quad (\text{mod. } \mathfrak{p}).$$

Hier ist

$$-2\varkappa \mp \sqrt{\varkappa(12^3-\varkappa)} \not\equiv 0 \ (\text{mod. } \mathfrak{p}),$$

denn aus der Annahme des Gegenteils folgt

$$-2\varkappa \equiv \pm \sqrt{\varkappa(12^3-\varkappa)} \ (\text{mod. } \mathfrak{p}),$$

und durch Erheben beider Seiten ins Quadrat

$$-\varkappa^2 \equiv 12^3\varkappa - \varkappa^2 \ (\text{mod. } \mathfrak{p}),$$

also $\varkappa \equiv 0$ (mod. $\mathfrak{p}$) gegen Voraussetzung.

Ferner ist

$$-2\varkappa - \sqrt{\varkappa(12^3-\varkappa)} \not\equiv -2\varkappa + \sqrt{\varkappa(12^3-\varkappa)} \ (\text{mod. } \mathfrak{p}),$$

denn aus der Annahme des Gegenteils würde folgen, daß $\varkappa(\varkappa - 12^3) \equiv 0$ (mod. $\mathfrak{p}$) gegen Voraussetzung.

Aus dem Schönemann'schen Satze, den beiden Hauptsätzen der Ore'schen Theorie und weil

$$-1 \equiv 2^2 \ (\text{mod. } \mathfrak{p})$$

folgt daher auf Grund der rechten Seite der Tabelle W., S. 52:

Falls $\varkappa(\varkappa - 12^3)$ quadratischer Nichtrest mod. $\mathfrak{p}$ ist, sind nur die Fälle 4 und 14 möglich, falls $\varkappa(\varkappa - 12^3)$ quadratischer Rest mod. $\mathfrak{p}$ ist, sind nur die Fälle 9, 10 und 15 möglich. Es ist mithin nur noch zu untersuchen, welcher von diesen 5 möglichen Fällen eintritt.

Wir lassen jetzt wieder die Beschränkung auf den Fall, daß $4\,e = 4$ ist, eintreten, dann ist $(1 - \varepsilon)$ eine Hensel'sche Primzahl in bezug auf das Primideal $\mathfrak{p}$ von k. Da der Restklassenring von $\mathfrak{p}$ ein Galoisfeld mit der Charakteristik 5 ist, so ist die Kongruenz

$$\varkappa \equiv \gamma^5 \pmod{\mathfrak{p}}$$

für ein mod. $\mathfrak{p}$ eindeutig bestimmtes zu $\mathfrak{p}$ teilerfremdes ganzes γ von k lösbar, und es gibt folglich ein δ mit zu $\mathfrak{p}$ teilerfremdem Nenner, so daß (18) gilt, und in (19) ist daher s wesentlich positiv.

Setzt man in der Resolvente (13) die Größe $x = X - \gamma$, so erhält man die Resolvente:

$$G(X) = f(X - \gamma) = X^5 + \frac{f''''(-\gamma)}{4!}X^4 + \frac{f'''(-\gamma)}{3!}X^3 + \frac{f''(-\gamma)}{2!}X^2 + \\ + \frac{f'(-\gamma)}{1!}X + f(-\gamma),$$

oder ausgerechnet:

$$G(X) = X^5 - 5[\gamma + 1]X^4 + 5\cdot 2[\gamma^2 + 2\gamma + 4]X^3 - 5\cdot 2\gamma[\gamma^2 + 3\gamma + 12]X^2 + \\ + 5\gamma^2[\gamma^2 + 4\gamma + 24]X + [\varkappa - \gamma^5 - 5\gamma^4 - 40\gamma^3] = 0. \qquad (21)$$

Hier ist die eckige Klammer, die als Faktor bei X auftritt, zu $\mathfrak{p}$ teilerfremd. Denn aus der Annahme des Gegenteils folgt:

$$(\gamma + 2)^2 \equiv 0 \pmod{\mathfrak{p}},$$

und da $\mathfrak{p}$ ein Primideal ist

$$\gamma \equiv -2 \pmod{\mathfrak{p}},$$

also durch Erheben beider Seiten in die 5. Potenz

$$\gamma^5 \equiv -32 + 1760 \equiv 12^3 \pmod{\mathfrak{p}},$$

und mithin wegen (18):

$$\varkappa - 12^3 \equiv 0 \pmod{\mathfrak{p}}$$

gegen Voraussetzung.

Ist in (19) die positive Größe s kleiner als 5, so besteht das Newton'sche Polygon von (21) aus einer einzigen Seite mit $l_1 = 5$, $h_1 = s$; es ist daher $\bar{e} = 5$ und es tritt entsprechend der Vorbemerkung der Fall 4 oder 9 auf.

Ist in (19) die Größe s genau gleich 5, so besteht das Newton'sche Polygon von (21) ebenfalls aus einer einzigen Seite mit $l_1 = h_1 = 5$, $\lambda_1 = 1$, und das zugeordnete Polynom von (21) ist, da

$$\sqrt{5} = (1-\varepsilon)^2 \cdot (\varepsilon^2 + \varepsilon^3) \cdot \varepsilon^4, \tag{22}$$

also

$$\frac{\sqrt{5}}{(1-\varepsilon)^2} \equiv 2 \pmod{\mathfrak{p}}: \tag{23}$$

$$F_1(x, y) \equiv y^5 - \gamma^2 (\gamma + 2)^2 y + \frac{\varkappa - \gamma^5 - 5\gamma^4 - 40\gamma^3}{(1-\varepsilon)^5} \pmod{\mathfrak{p}}.$$

Da $\dfrac{\partial F_1(x,y)}{\partial y} \equiv -\gamma^2 (\gamma + 2)^2 \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so ist die Diskriminante von $F_1(x, y)$ teilerfremd zu $\mathfrak{p}$, und es tritt entsprechend der Vorbemerkung einer der Fälle 10, 14 oder 15 auf.

Ist in (19) die Größe s größer als 5, so besteht das Newton'sche Polygon von (21) aus 2 Seiten mit den Längen $l_1 = 4$ und $l_2 = 1$, und entsprechend der Vorbemerkung und der Tabelle in W., S. 52 kann daher nur der Fall 14 oder 15 auftreten.

Man wird sofort die Frage aufwerfen, ob im Falle A.) $u = v = w = 0$, die beiden Möglichkeiten, *Verzweigung* oder *Nicht-Verzweigung* auch *wirklich* auftreten können. Daß diese Frage zu bejahen ist, zeigen für den Fall, daß der Grundkörper k der Körper der 5. Einheitswurzeln selbst ist, die beiden Beispiele[17]:

$$\varkappa = 2^6 \cdot 3^3 (1 + \varepsilon), \qquad \varkappa - 12^3 = 2^6 \cdot 3^3 \varepsilon;$$

bezw. $$\varkappa = 2^6 \cdot 3^3 (244 + 5^6), \qquad \varkappa - 12^3 = 2^6 \cdot 3^3 (243 + 5^6).$$

Man sieht ohne große Mühe[18]), daß für diese Werte von $\varkappa$ die Galois'sche Gruppe der Gleichung (1) in bezug auf den Körper der 5. Einheitswurzeln die Ikosaedergruppe ist, und in K für $\mathfrak{p} = (1-\varepsilon)$ für den ersten Wert von $\varkappa$ Verzweigung:

$$\text{Fall 4:}\quad (1-\varepsilon) = \left\{ \prod_{i=1}^{6} \mathfrak{P}_i \right\}^5, \quad N_{K/k}(\mathfrak{P}_i) = (1-\varepsilon)^2;$$

für den zweiten Wert von $\varkappa$ keine Verzweigung:

$$\text{Fall 14:}\quad (1-\varepsilon) = \prod_{i=1}^{30} \mathfrak{P}_i, \qquad N_{K/k}(\mathfrak{P}_i) = (1-\varepsilon)^2;$$

eintritt.

---

[17]) Die Größe $(1 + \varepsilon)$ ist eine Einheit von k, denn $(1 + \varepsilon) \cdot (\varepsilon + \varepsilon^3) = -1$.

[18]) Vgl. N., S. 228/229.

BC.) $u > 0,\ v = w = 0.$

Je nach dem Werte von u treten folgende Fälle auf:

$u = 1, 3, 7, 9$: *Fall 3.*

$u = 2, 4, 6, 8$: $\begin{cases} \varkappa(\varkappa - 12^3) \text{ quadratischer Nichtrest mod. } \mathfrak{p}^{u+1}\text{: Fall 4.} \\ \varkappa(\varkappa - 12^3) \text{ quadratischer Rest mod. } \mathfrak{p}^{u+1}\text{: Fall 9.} \end{cases}$

$u = 5$ *und mit ganzem, zu* $\mathfrak{p}$ *teilerfremdem* γ *von* k *und für* δ *mit zu* $\mathfrak{p}$ *teilerfremdem Nenner:*

$$\varkappa = (1 - \varepsilon)^5 \gamma^5 + (1 - \varepsilon)^6 \delta. \tag{24}$$

Ist $\mathfrak{p} \mid \delta$ *und gleichzeitig* $\gamma^3 + \dfrac{2\delta}{(1-\varepsilon)} \equiv 0$ *(mod.* $\mathfrak{p}$*): Fall 13.*

Gilt diese Bedingung nicht: Fall 3.

$u = 10$: *Je nachdem die Zerlegung von*

$$y^5 + 2y^3 + \frac{\varkappa}{(1-\varepsilon)^{10}}$$

in Primpolynome mod. $\mathfrak{p}$ *genau keinen, zwei, einen, bezw. fünf Linearfaktoren hat: Fall 10, 12, 14, bezw. 15.*

$u > 10$:

- $u \not\equiv 1 \pmod{3}$: $\begin{cases} 2 \text{ quadratischer Nichtrest mod. } \mathfrak{p}\text{: Fall 6.} \\ 2 \text{ quadratischer Rest mod. } \mathfrak{p}\text{: Fall 11.} \end{cases}$
- $u \equiv 1 \pmod{3}$: *Je nachdem die Kongruenz*

$$y^3 \equiv \frac{\varkappa(\varkappa - 12^3)}{(1-\varepsilon)^u} \quad (\mathit{mod.}\ \mathfrak{p})$$

genau keinen, einen, bezw. drei Linearfaktoren hat: Fall 12, 14, bezw. 15.

Ist $u > 10$, so besteht das Newton'sche Polygon von (13):

$$f(x) = x^5 - 5x^4 + 40x^3 + \varkappa = 0$$

aus 2 Seiten mit den Längen $l_1 = 2$ und $l_2 = 3$ [19]). Ist hiebei $u \not\equiv 1$ (mod. 3), so ist $\lambda_2 = 3$, ferner ist

$$F_1(x, y) \equiv y^2 + 2 \quad (\text{mod. } \mathfrak{p}).$$

Je nachdem, ob -2 oder was wegen $-1 \equiv 2^2$ (mod. $\mathfrak{p}$) auf dasselbe herauskommt, 2 quadratischer Nichtrest oder quadratischer Rest mod. $\mathfrak{p}$

[19]) Wie man leicht erkennt, ist im allgemeinen Falle dieses Polynom für $u \geqq 10$ e regulär in bezug auf $\mathfrak{p}$.

ist, gilt folglich der Fall 6 oder der Fall 11 [20]). Ist dagegen $u \equiv 1 \pmod{3}$, so ist $\lambda_2 = 1$ und

$$F_2(x, y) \equiv y^3 - \frac{2\varkappa}{(1-\varepsilon)^u} \equiv y^3 - \frac{\varkappa(\varkappa - 12^3)}{(1-\varepsilon)^u} \pmod{\mathfrak{p}},$$

woraus die angegebene Regel folgt.

Ist $u = 10$, so besteht das Newton'sche Polygon aus einer einzigen Seite von der Länge $l_1 = 5$ und

$$F_1(x, y) \equiv y^5 + 2y^3 + \frac{\varkappa}{(1-\varepsilon)^{10}} \pmod{\mathfrak{p}}.$$

Da $\dfrac{\partial F_1(x, y)}{\partial y} \equiv y^2 \pmod{\mathfrak{p}}$, so ist die Diskriminante von $F_1(x, y)$ zu $\mathfrak{p}$ teilerfremd, und hieraus ergibt sich die oben angegebene Regel.

Es sei von jetzt an $u < 10$. Ist $u \neq 5$, so besteht das Newton'sche Polygon ebenfalls aus einer einzigen Seite mit $\lambda_1 = 5$. Mithin tritt dann gemäß der Tabelle W., S. 52 einer der Fälle 3, 4 oder 9 ein.

Ist $u = 5$, so ist die Kongruenz

$$\frac{\varkappa}{(1-\varepsilon)^5} \equiv \gamma^5 \pmod{\mathfrak{p}}$$

für ein mod. $\mathfrak{p}$ eindeutig bestimmtes zu $\mathfrak{p}$ teilerfremdes ganzes γ von k lösbar, und es gibt daher ein δ mit zu $\mathfrak{p}$ teilerfremdem Nenner, so daß (24) gilt. Setzt man in (13) die Größe $x = (1-\varepsilon)\, t$, so ergibt sich unter Berücksichtigung von (24) die Resolvente:

$$g(t) = t^5 - \frac{5}{(1-\varepsilon)}\, t^4 + \frac{5}{(1-\varepsilon)^2}\, 8t^3 + \gamma^5 + (1-\varepsilon)\,\delta = 0,$$

und setzt man hier $t = X - \gamma$, so erhält man die Resolvente:

$$G(X) = g(X - \gamma) = X^5 + \frac{g''''(-\gamma)}{4\,!} X^4 + \frac{g'''(-\gamma)}{3\,!} X^3 +$$

$$+ \frac{g''(-\gamma)}{2\,!} X^2 + \frac{g'(-\gamma)}{1\,!} X + g(-\gamma) = 0,$$

oder ausgerechnet:

[20]) Ist der Grundkörper k der Körper der 5. Einheitswurzeln selbst, so tritt der Fall 11 nie auf, was sich auch sofort aus W., S. 50, Fall 11 ergibt, da für $p = 5$ und $f = 1$ die Kongruenz $p^f \equiv 1 \pmod{3}$ nicht erfüllt ist. Für $u \equiv 1 \pmod{3}$ fallen dann die Fälle 12 und 15 außer Betracht.

$$G(X) = X^5 + \left[-\frac{5}{(1-\varepsilon)} + \ldots\right] X^4 + \left[\frac{5}{(1-\varepsilon)^2} \cdot 8 + \ldots\right] X^3 +$$
$$+ \left[-\frac{5}{(1-\varepsilon)^2} \cdot 24\gamma + \ldots\right] X^2 + \left[\frac{5}{(1-\varepsilon)^2} \cdot 24\gamma^2 + \ldots\right] X +$$
$$-(1-\varepsilon)\left[\frac{5}{(1-\varepsilon)^2} \cdot \gamma^4 + \frac{5}{(1-\varepsilon)^3} \cdot 8\gamma^3 - \delta\right] = 0.$$

Ist hier $\mathfrak{p} \nmid \delta$ und gleichzeitig $\gamma^3 + \frac{2\delta}{(1-\varepsilon)} \equiv 0 \pmod{\mathfrak{p}}$, so besteht das Newton'sche Polygon aus 2 Seiten mit $l_1 = 4$, $h_1 = 2$, $\lambda_1 = 2$ und $l_2 = 1$, wobei wegen (23):

$$F_1(x, y) \equiv y^2 - (2\gamma)^2 \equiv (y + 2\gamma)(y - 2\gamma) \pmod{\mathfrak{p}}$$

ist, und es tritt daher, da $\mathfrak{p}$ ein Teiler von 5 ist, gemäß der Tabelle in W., S. 52, der Fall 13 ein. In jedem andern Falle besteht das Newton'sche Polygon aus einer einzigen Seite mit $l_1 = \lambda_1 = 5$, und es tritt daher einer der Fälle 3, 4 oder 9 ein.

Es ist noch zu entscheiden, welcher der drei Fälle: 3, 4 oder 9 bei $u < 10$ eintritt, und es ergibt sich aus der Tabelle W., S. 52 und der Tabelle in § 1 dieser Arbeit, daß diese Entscheidung weder vermöge einer Resolventen fünften, noch einer sechsten, dagegen vermöge einer Resolventen zwölften Grades getroffen werden kann. Setzt man in (20) die Größe $x = Z + 7$, so ergibt sich die Resolvente

$$G(Z) = [Z^4 - 2^3 \cdot 5^2 Z^3 - 2^5 \cdot 5^3 Z^2 - 2^3 \cdot 5^5 Z - 2^4 \cdot 5^5]^3 +$$
$$+ \varkappa [Z + 7] \cdot [Z^2 + 5^2 Z + 5^3]^5 = 0, \qquad (25)$$

und im Falle $u < 10$ liefert das zugehörige Newton'sche Polygon immer die Entscheidung, welcher der 3 Fälle eintritt. Hiebei ist noch zu beachten, daß

$$-2\varkappa \equiv 2^2 \cdot (\varkappa - 12^3)\varkappa \pmod{\mathfrak{p}^{u+1}}.$$

DE.) $w > 0$, $u = v = 0$.

In bemerkenswerter Analogie zum Hauptfalle BC.) treten je nach dem Werte von w folgende Fälle auf:

$w = 1, 3, 7, 9$: *Fall 3.*

$w = 2, 4, 6, 8$: $\begin{cases} \varkappa(\varkappa - 12^3) \text{ quadratischer Nichtrest mod. } \mathfrak{p}^{w+1}\text{: Fall 4.} \\ \varkappa(\varkappa - 12^3) \text{ quadratischer Rest mod. } \mathfrak{p}^{w+1}\text{: Fall 9.} \end{cases}$

$w = 5$ *und mit ganzem, zu $\mathfrak{p}$ teilerfremdem γ von k und für δ mit zu $\mathfrak{p}$ teilerfremdem Nenner:*

$$\varkappa - 12^3 = (1-\varepsilon)^5 \gamma^5 + (1-\varepsilon)^6 \delta. \qquad (26)$$

Ist $\mathfrak{p} \mid \delta$ *und ausserdem* $\gamma^3 + \frac{2\delta}{(1-\varepsilon)} \equiv 0$ (*mod.* $\mathfrak{p}$): *Fall 13.*

Gilt diese Bedingung nicht: Fall 3.

$w = 10$: *Je nachdem die Zerlegung von* $y^5 + y^4 - \frac{(\varkappa - 12^3)^2}{5^5}$ *in Primpolynome mod.* $\mathfrak{p}$ *genau keinen, einen, bezw. fünf Linearfaktoren hat: Fall 10, 14, bezw. 15.*

$w > 10$: $\begin{cases} w \equiv 1 \pmod{2}: & \textit{Fall 13.} \\ w \equiv 0 \pmod{2}: & \begin{cases} \varkappa(\varkappa - 12^3) \textit{ quadratischer Nichtrest mod. } \mathfrak{p}^{w+1}: \textit{Fall 14.} \\ \varkappa(\varkappa - 12^3) \textit{ quadratischer Rest mod. } \mathfrak{p}^{w+1}: \textit{Fall 15.} \end{cases} \end{cases}$

Wir machen zunächst eine Vorbemerkung, die für beliebiges e gilt. Setzt man in (25) die Größe $\varkappa = (\varkappa - 12^3) + 12^3$, so wird, falls nur der Nenner von $\varkappa$ zu $\mathfrak{p}$ teilerfremd ist:

$$G(Z) \equiv Z^{10}\,[Z^2 + 3Z - 29 + (\varkappa - 12^3)(Z + 7)] \pmod{\mathfrak{p}^{12e}}, \quad (27)$$

und für $w > 0$:

$$G(Z) \equiv Z^{10}(Z-1)^2 \pmod{\mathfrak{p}}.$$

Es folgt vermöge des Satzes von Schönemann und der beiden Hauptsätze von Ore, daß es im Körper $\bar{k}$ vom Relativgrade 12 über k bei der Primidealpotenzdarstellung von $\mathfrak{p}$ jedenfalls ein Ideal $\bar{\mathfrak{l}}$ mit $N_{\bar{k}/k}(\bar{\mathfrak{l}}) = \mathfrak{p}^2$ gibt, das teilerfremd ist zu allen andern Primidealteilern von $\mathfrak{p}$ in $\bar{k}$. Für beliebiges $4e$ sind daher im Hauptfalle DE.) nur die Fälle 3, 4, 9, 10, 13, 14, 15 möglich.

Wir beschränken uns wieder auf den Fall, dass $4e = 4$ ist, und nehmen die Resolvente (7):

$$f(x) = x^5 + 45x^4 + 10(\varkappa - 12^3)x^2 + (\varkappa - 12^3)^2 = 0$$

zu Hilfe[21]).

Sei $w > 10$. Dann besteht das Newton'sche Polygon aus 2 Seiten von den Längen $l_1 = 1$ und $l_2 = 4$. Ist $w \equiv 1 \pmod{2}$, so ist $\lambda_2 = 2$, und es ist nur der Fall 13 möglich. Ist $w \equiv 0 \pmod{2}$, so ist

[21]) Wie man leicht erkennt, ist im allgemeinen Falle für $w \geqq 10e$ diese Resolvente regulär in bezug auf $\mathfrak{p}$.

$$F_2(x,y) \equiv y^4 - \left(\frac{\varkappa - 12^3}{\sqrt{5}\,(1-\varepsilon)^{w-2}}\right)^2 \equiv$$

$$\equiv \left(y^2 - \frac{\varkappa - 12^3}{\sqrt{5}\,(1-\varepsilon)^{w-2}}\right)\left(y^2 + \frac{\varkappa - 12^3}{\sqrt{5}\,(1-\varepsilon)^{w-2}}\right) \pmod{\mathfrak{p}},$$

woraus sich wegen (23) und den beiden Kongruenzen: $-2 \equiv \varkappa \pmod{\mathfrak{p}}$ und $-1 \equiv 2^2 \pmod{\mathfrak{p}}$ die angegebene Regel ergibt.

Ist $w = 10$, so besteht das Newton'sche Polygon aus einer einzigen Seite, und wegen (23) ist

$$F_1(x,y) \equiv y^5 + y^4 + \frac{(\varkappa - 12^3)^2}{(1-\varepsilon)^{20}} \pmod{\mathfrak{p}},$$

und da $\dfrac{\partial F_1(x,y)}{\partial y} \equiv -y^3 \pmod{\mathfrak{p}}$, so folgt unter Beachtung der Vorbemerkung die angegebene Regel.

Es sei von jetzt an $w < 10$. Ist $w \neq 5$, so besteht das Newton'sche Polygon aus einer einzigen Seite mit $\lambda_1 = 5$, und es tritt folglich einer der Fälle 3, 4 oder 9 ein. Für $w = 5$ kann man analog wie in BC.) für $u = 5$ schließen, indem man zunächst in (1):

$$r\,(r^2 - 10\,r + 45)^2 + (\varkappa - 12^3) = 0$$

die Größe $r = (1-\varepsilon)\,t$ setzt und (26) beachtet. In der entstehenden normierten Resolventen setze man dann $t = X - \gamma$, dann liefert die Resolvente 5. Grades in X das Resultat, daß falls $\mathfrak{p} \mid \delta$ und gleichzeitig $\gamma^3 + \dfrac{2\,\delta}{(1-\varepsilon)} \equiv 0 \pmod{\mathfrak{p}}$ ist, der Fall 13 eintritt, falls aber diese Bedingung nicht erfüllt ist, einer der Fälle 3, 4 oder 9 eintritt.

Es ist jetzt wie unter BC.) noch zu entscheiden, welcher der 3 Fälle 3, 4 oder 9 bei $w < 10$ eintritt. Unter Berücksichtigung des Schönemann'schen Satzes, insbesondere der Tatsache, daß in einer Schönemann'schen Zerlegung mod. $\mathfrak{p}^\alpha$ in normierte Faktoren für die mod. $\mathfrak{p}$ zueinander relativ primen Polynome die einzelnen Faktoren für eine *beliebige* natürliche Zahl a bekanntlich mod. $\mathfrak{p}^\alpha$ eindeutig bestimmt sind, und auf Grund der beiden Hauptsätze von Ore erhält man sofort die oben angegebene Regel, wenn man (27) unter folgender Form schreibt:

$$G(Z) \equiv Z^{10}\left[\left(Z + \frac{3 + (\varkappa - 12^3)}{2}\right)^2 - \frac{\varkappa\,(\varkappa - 12^3)}{4}\right] \pmod{\mathfrak{p}^{12}},$$

und die Theorie der Newton'schen Polygone auf den zweiten Faktor anwendet.

F.) $v > 0$, $u = w = 0$.

Je nach dem Werte von v treten folgende Fälle auf:

$v \not\equiv 0 \pmod{5}$: *Fall 9.*

$v \equiv 0 \pmod{5}$: $\begin{cases} \frac{1}{\varkappa} \text{ fünfter Potenznichtrest mod. } \mathfrak{p}^{v+5}\text{: Fall 9.} \\ \frac{1}{\varkappa} \text{ fünfter Potenzrest mod. } \mathfrak{p}^{v+5}\text{, und mit zu } \mathfrak{p} \text{ teilerfremdem} \end{cases}$

ganzem γ von k und für δ mit zu $\mathfrak{p}$ teilerfremdem Nenner

$$\frac{1}{\varkappa} = (1 - \varepsilon)^v \gamma^5 [1 + (1 - \varepsilon)^5 \delta]. \tag{28}$$

Je nachdem, ob die Kongruenz

$$y^5 - y + \left(\delta - (1 - \varepsilon)^{\frac{v}{5} - 1} \gamma\right) \equiv 0 \ (mod.\ \mathfrak{p}) \tag{29}$$

irreduzibel, bezw. reduzibel ist mod. $\mathfrak{p}$: Fall 10, bezw. Fall 15.

Zum Beweise machen wir zunächst folgende Vorbemerkung, die übrigens für eine beliebige Ordnung $4e$ von $\mathfrak{p}$ gilt. Setzt man in (25) die Größe $Z = \varkappa z$, so erhält man eine normierte Resolvente $g(z) = 0$, für welche

$$g(z) \equiv z^{11} (z + 1) \ (\text{mod. } \mathfrak{p}). \tag{30}$$

Nach bekannten Sätzen folgt aus (30), daß $\mathfrak{p}$ im zugehörigen Erweiterungskörper $\bar{k}$ vom Relativgrade 12 in bezug auf k jedenfalls einen Primidealteiler $\bar{\mathfrak{p}}$ vom Relativgrad und von der Relativordnung 1 besitzt, der zu allen andern Primidealteilern von $\mathfrak{p}$ in $\bar{k}$ teilerfremd ist. Es kann mithin nur einer der Fälle 9, 10 oder 15 eintreten.

Wir verwenden jetzt die Resolvente (6):

$$f(x) = x^5 + 40 \frac{1}{\varkappa} x^2 - 5 \frac{1}{\varkappa} x + \frac{1}{\varkappa} = 0,$$

und nehmen für das folgende wieder an, daß $4e = 4$ ist.

Ist $v \not\equiv 0$ **(mod. 5)**, so zeigt das dieser Resolventen zugeordnete Newton'sche Polygon, daß der Fall 9 eintritt.

Es sei also im folgenden: $v = 5v'$, *wo* $v' \geqq 1$ ist, und zunächst mit ganzem γ von k und für ϑ mit zu $\mathfrak{p}$ teilerfremdem Nenner:

$$\frac{1}{\varkappa} = (1 - \varepsilon)^{5v'} \gamma^5 [\, 1 + (1 - \varepsilon)\, \vartheta\,]. \tag{31}$$

Setzt man in der Resolventen (6) die Größe $x = (1 - \varepsilon)^{v'} t$, so erhält man die folgende:

$$g(t) = t^5 + \frac{5}{\varkappa(1-\varepsilon)^{3v'}} \cdot 8t^2 - \frac{5}{\varkappa(1-\varepsilon)^{4v'}}\, t + \frac{1}{\varkappa(1-\varepsilon)^{5v'}} = 0.$$

Setzt man hier $t = X - \gamma$, so ergibt sich endlich folgende Resolvente:

$$G(X) = g(X-\gamma) = X^5 + \frac{g''''(-\gamma)}{4!} X^4 + \frac{g'''(-\gamma)}{3!} X^3 +$$

$$+ \frac{g''(-\gamma)}{2!} X^2 + \frac{g'(-\gamma)}{1!} X + g(-\gamma) = 0,$$

oder ausgerechnet:

$$X^5 - 5\gamma X^4 + 10\gamma^2 X^3 + [-5\cdot 2\gamma^3 + \ldots] X^2 + [5\gamma^4 + \ldots] X +$$

$$+ \left[\frac{5}{\varkappa(1-\varepsilon)^{3v'}}\, 8\gamma^2 + \frac{5}{\varkappa(1-\varepsilon)^{4v'}}\, \gamma + \gamma^5 (1-\varepsilon)\, \vartheta\right] = 0. \quad (32)$$

Ist hier $\vartheta \not\equiv 0 \pmod{\mathfrak{p}^4}$, so besteht das zugehörige Newton'sche Polygon aus einer einzigen Seite mit $\lambda_1 = 5$, und es gilt daher der Fall 9 wie eben.

Ist $\vartheta \equiv 0 \pmod{\mathfrak{p}^4}$, so sei $\vartheta = (1-\varepsilon)^4\, \delta$. Setzt man diesen Wert von ϑ in (31) ein, so geht (31) in die Gleichung (28) über. Trägt man endlich den Wert von $\frac{1}{\varkappa}$ gemäß (28) in (32) ein, und setzt noch $X = \gamma x$, so ergibt sich die normierte Resolvente:

$$x^5 - 5x^4 + 5\cdot 2x^3 + [-5\cdot 2 + \ldots] x^2 + [5 + \ldots] x +$$

$$+ (1-\varepsilon)^5 \left[\delta + (1-\varepsilon)^{v'-1}\cdot\gamma\cdot \frac{5}{(1-\varepsilon)^4}\left(1 + (1-\varepsilon)^{v'}\cdot 8\gamma\right)\left(1 + (1-\varepsilon)^5\delta\right)\right] = 0. \quad (33)$$

Ist hier $\delta - (1-\varepsilon)^{v'-1}\gamma \equiv 0 \pmod{\mathfrak{p}}$, so besteht das Newton'sche Polygon von (33) aus 2 Seiten von den Längen $l_1 = 4$ und $l_2 = 1$, und es tritt der Fall 15 ein. In diesem Falle ist die Kongruenz (29) reduzibel, da sie dann den Linearfaktor y hat. Ist $\delta - (1-\varepsilon)^{v'-1}\gamma \not\equiv 0 \pmod{\mathfrak{p}}$, so besteht das Newton'sche Polygon von (33) aus einer einzigen Seite mit $\lambda_1 = 1$ und $F_1(x, y)$ ist mod. $\mathfrak{p}$ kongruent dem Ausdrucke (29). Da $\frac{\partial F_1(x, y)}{\partial y} \equiv -1 \pmod{\mathfrak{p}}$, ist dann die Diskriminante von $F_1(x, y)$ mod. $\mathfrak{p}$ nicht kongruent Null, und damit ist alles bewiesen.

(Eingegangen den 19. August 1934.)