## Werk

**Titel:** Mathematische Annalen
**Ort:** Berlin
**Jahr:** 1930
**Kollektion:** Mathematica
**Digitalisiert:** Niedersächsische Staats- und Universitätsbibliothek Göttingen
**Werk Id:** PPN235181684_0102
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN235181684_0102

**LOG Id:** LOG_0016
**LOG Titel:** Abriß einer arithmetischen Theorie der Galoisschen Körper. (Zweite Mitteilung)
**LOG Typ:** article

## Übergeordnetes Werk

**Werk Id:** PPN235181684
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN235181684
**OPAC:** http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235181684



## Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

# Abriß einer arithmetischen Theorie der Galoisschen Körper.

(Zweite Mitteilung.)

Von

Öystein Ore in New Haven (Conn., U. S. A.).

---

In der ersten Mitteilung[1]) ist zunächst der einfachste, *reguläre* Fall der Zerlegungsgruppe untersucht worden, wo also höhere Verzweigungsgruppen nicht vorkommen. Weiter wurde in A, Kap. 2 die Grundlage für die Behandlung des *irregulären* Falles gegeben, indem gezeigt wurde, daß bei relativ-zyklischen Körpern vom Primzahlgrade $p$ das volle Restsystem $(\mathrm{mod}\ \mathfrak{P}^{\alpha})$, wo $\mathfrak{P}$ ein Primidealteiler von $p$ ist, immer durch Adjunktion einer Wurzel einer binomischen oder einer trinomischen Normalkongruenz $(\mathrm{mod}\ \mathfrak{P}^{\alpha})$ erhalten werden kann. Die Form der Normalkongruenzen hängt nur von der Relativdifferente des Körpers ab.

In dieser zweiten Mitteilung werden nun diese Resultate für den Aufbau einer Theorie des irregulären Falles angewandt, welche wieder zum Studium der Zerlegungsgruppe dient.

Anstatt der Reihe der Verzweigungsgruppen wird zuerst eine Kompositionsreihe der Zerlegungsgruppe betrachtet; dementsprechend erhält man eine Reihe von relativ-zyklischen Körpern vom Relativgrade $p$, welche ich Irregularkörper genannt habe und welche die Reihe der Verzweigungskörper enthält. Daraus folgt der Hauptsatz, daß man den vollständigen Restbereich $(\mathrm{mod}\ \mathfrak{P}^{\alpha})$ durch sukzessive Adjunktionen der Wurzeln von binomischen und trinomischen Normalkongruenzen von der Form

$$x^p - \frac{1}{r_i}\tau^{b_i}\pi_{i-1}^{c_i+1}x^{r_i} - \beta_{i-1}\pi_{i-1} \equiv 0 \pmod{\mathfrak{P}^{\alpha}}$$

oder

$$x^p - \beta_{i-1}\pi_{i-1} \equiv 0 \pmod{\mathfrak{P}^{\alpha}}$$

---

[1]) Math. Annalen **100** (1928), S. 650—673. Diese Abhandlung wird im folgenden kurz mit A bezeichnet.

aufbauen kann. Weiter werden die Verzweigungen $\mu_i$ [2]) durch die Konstanten der Normalkongruenzen bestimmt, woraus sofort unter Anwendung der Dedekind-Henselschen Ungleichung obere Grenzen für die $\mu_i$ angegeben werden können. Als Schlußstein von Kap. 1 wird bewiesen, daß die Normalkongruenzen für ein gegebenes Primideal entweder alle binomisch oder alle trinomisch sind, und daß im trinomischen Falle der Exponent $r_i = r$ eine von $i$ unabhängige Konstante ist. Als eine Anwendung hiervon folgt für die Verzweigungen

$$\mu_1 \equiv \mu_2 \equiv \ldots \equiv 1 - r \pmod{p},$$

worin der Satz von Speiser [3]) enthalten ist, daß alle Verzweigungen einander $(\mathrm{mod}\ p)$ kongruent sind.

In Kap. 2 wird diese allgemeine Theorie zu einer vollständigen Untersuchung des binomischen Falles angewandt. In diesem Falle ist

$$e_0 \equiv 0 \pmod{p-1}, \qquad \mu_i = \frac{e_0 p^i}{p-1} + 1 \qquad (i = 1, 2, \ldots, s)$$

und die Verzweigungsgruppe ist zyklisch. Die vollständige Struktur der Trägheitsgruppe (Satz 16) und Zerlegungsgruppe (Satz 17) wird bestimmt. Die Form der Zerlegungsgruppe ist verhältnismäßig kompliziert, aber gruppentheoretisch interessant. Im binomischen Falle wird die Trägheitsgruppe nur für $p = 2$ Abelsch.

In einer letzten Mitteilung sollen verschiedene andere Fragen der arithmetischen Theorie der Galoisschen Körper behandelt werden, speziell wird der trinomische Fall eingehender studiert.

## Kapitel 1.
## Normalkongruenzen für die Irregularkörper.

### § 1.
### Einführung der Irregularkörper.

Für den regulären Fall ist in A, Kap. 1 die vollständige Beziehung zwischen Gruppeneigenschaften und Gleichungseigenschaften aufgestellt. Dieselbe Aufgabe soll nun in dem schwierigeren Falle behandelt werden, wo auch höhere Verzweigungsgruppen vorkommen.

Den Galoisschen Körper $K$ erhält man (vgl. A, Kap. 1, § 1) aus dem Regularkörper $K_0$ (= erster Verzweigungskörper) dadurch, daß man durch sukzessive Adjunktionen die Reihe der höheren Verzweigungskörper

$$K_0 = K_{V_1}, K_{V_2}, \ldots, K_{V_{h+1}} = K \tag{1}$$

[2]) Man vgl. A, Kap. 1, § 1.

[3]) A. Speiser, Die Zerlegungsgruppe, Journ. f. Math. **149** (1919), S. 174–188. Diese Arbeit wird im folgenden als Speiser zitiert.

aufbaut. Hier ist allgemein $K_{V_i}$ ein Relativkörper vom Grade $p^{s_{i-1}}$ zu $K_{V_{i-1}}$, wobei also

$$s_1 + s_2 + \ldots + s_k = s, \tag{2}$$

wenn die Ordnung $e$ des betrachteten Primideals $\mathfrak{P}$ die Form $e = e_0 p^s$, $(e_0, p) = 1$ hat. Weiter sei

$$G_0 = G_{V_1}, G_{V_2}, \ldots, G_{V_{k+1}} = 1 \tag{3}$$

die Reihe der entsprechenden Verzweigungsgruppen, wo bekanntlich die Faktorgruppe $G_{V_{i-1}}/G_{V_i}$ Abelsch und vom Typus $\overbrace{p, p, \ldots, p}^{s_{i-1}}$ ist. Wie früher werden die Zerlegungsgruppe und Trägheitsgruppe mit $G_Z$ und $G_T$ bezeichnet.

Im folgenden erweist es sich nun sehr oft als vorteilhaft, nicht mit den Gruppen (1), sondern mit einer Kompositionsreihe der Gruppe $G_0$

$$(G_{V_1} =)\, G_0, G_1, G_2, \ldots, G_s = 1 \tag{4}$$

zu operieren, wobei allgemein die Gruppe $G_i$ die $i$-te *Irregulargruppe* heißen soll. Die Faktorgruppe $G_{i-1}/G_i$ ist zyklisch von der Ordnung $p$ und die Gruppe $G_i$ hat folglich die Ordnung $p^{s-i}$. Entsprechend (4) erhält man eine Reihe von $s$ *Irregularkörpern*

$$(K_{V_1} =)\, K_0, K_1, \ldots, K_s = K, \tag{5}$$

wobei $K_i$ ein zyklischer Relativkörper vom Relativgrade $p$ zu $K_{i-1}$ ist. Der Relativgrad zu $K_T$ von $K_i$ wird $e_0 p^i$, während der Galoissche Körper $K$ ein Relativkörper vom Grade $p^{s-i}$ zu $K_i$ wird.

Die Kompositionsreihe (4) wird in der folgenden Weise definiert: Es sei $S_1$ eine Substitution in $G_{V_1}$, welche nicht zu $G_{V_2}$ gehört. Wenn dann $\pi$ eine Primzahl in bezug auf $\mathfrak{P}$ in $K$ ist, so folgt nach der Definition von $G_{V_1}$

$$S_1 : \pi \equiv \pi + \omega_1 \pi^{\mu_1} \pmod{\mathfrak{P}^{\mu_1+1}}, \tag{6}$$

wo $\mu_1$ die in A, Kap. 1, § 1 definierte Verzweigung von $G_{V_1}$ ist. Durch Wiederholung erhält man aus (6)

$$S_1^r : \pi \equiv \pi + r\omega_1 \pi^{\mu_1} \pmod{\mathfrak{P}^{\mu_1+1}},$$

so daß speziell $S_1^p$ eine Substitution in $G_{V_2}$ ist.

Es folgt nun leicht, daß man genau $s_1 \pmod{\mathfrak{P}}$ linear unabhängige Zahlen

$$\omega_1, \omega_2, \ldots, \omega_{s_1} \tag{7}$$

so bestimmen kann, daß, wenn $S$ eine beliebige Substitution in $G_{V_1}$ ist, wird

$$S : \pi \equiv \pi + \alpha \pi^{\mu_1} \pmod{\mathfrak{P}^{\mu_1+1}},$$

wobei $\alpha$ die Form

$$\alpha = r_1 \omega_1 + r_2 \omega_2 + \ldots + r_{s_1} \omega_{s_1}$$

mit ganzen rationalen $r_i$ hat. Wenn daher $S_i$ eine Substitution ist, für die

$$S_i : \pi \equiv \pi + \omega_i \pi^{\mu_1} \pmod{\mathfrak{P}^{\mu_1+1}},$$

so kann man die ganze Verzweigungsgruppe $G_{V_1}$ in der Form

$$G_{V_1} = S_1^{r_1} S_2^{r_2} \ldots S_{s_1}^{r_{s_1}} G_{V_2} \qquad (r_i = 0, 1, \ldots, p-1)$$

darstellen, wobei immer $S_i^p$ eine Substitution in $G_{V_2}$ ist, und weiter

$$S_i S_j = S_j S_i S^{(2)},$$

wo $S^{(2)}$ in $G_{V_2}$ liegt.

Diejenigen Substitutionen in $G_{V_1}$, welche $S_1$ nicht enthalten, bilden eine Gruppe $p^{s-1}$-ter Ordnung, und diese ist die erste Irregulargruppe $G_1$. Die Gruppe $G_1$ ist offenbar ein Normalteiler von $G_0$ und $G_0/G_1$ ist zyklisch von der Ordnung $p$. Ebenso bilden diejenigen Substitutionen, welche weder $S_1$ noch $S_2$ enthalten, die zweite Irregulargruppe $G_2$ von der Ordnung $p^{s-2}$ usw. Durch eine ähnliche Behandlung der nächsten Verzweigungsgruppen erhält man leicht:

Satz 1. *Man kann in der ersten Verzweigungsgruppe $s$ Substitutionen*

$$S_1, S_2, \ldots, S_s \tag{8}$$

*so bestimmen, daß die Gruppe in der Form*

$$G_0 = S_1^{r_1} S_2^{r_2} \ldots S_s^{r_s} \qquad (r_j = 0, 1, \ldots, p-1)$$

*dargestellt werden kann. Die $i$-te Irregulargruppe ist dann durch*

$$G_i = S_{i+1}^{r_i} \ldots S_s^{r_s} \qquad (r_j = 0, 1, \ldots, p-1) \tag{9}$$

*definiert, wobei für alle $i$ immer $S_{i+1}^p$ in einer Gruppe $G_j$ $(j \geqq i+1)$ enthalten ist.*

Es ist einleuchtend, daß in (8) die $s_1$ ersten Substitutionen $S_i$ in $G_{V_1}$, die $s_2$ nächsten in $G_{V_2}$ usw. liegen. Für die Irregularkörper $K_i$, welche den Irregulargruppen (9) entsprechen, werden wir der Bequemlichkeit wegen die kürzere Ausdrucksweise anwenden, daß $K_i$ *zwischen den Verzweigungskörpern $K_{V_r}$ und $K_{V_{r+1}}$ liegt*, wenn $K_i$ ein (echter oder unechter) Unterkörper von $K_{V_{r+1}}$, aber nicht von $K_{V_r}$ ist.

Eine Verzweigungsgruppe ist bekanntlich ein Normalteiler von allen vorangehenden Verzweigungsgruppen, sowie von der Trägheitsgruppe $G_T$ und Zerlegungsgruppe $G_Z$. Eine Irregulargruppe ist, wie man leicht sieht, ein Normalteiler von allen vorangehenden Irregulargruppen, aber allgemein nicht von $G_T$ und $G_Z$. Wenn $S_{i+1}$ eine Substitution ist, für die

$$S_{i+1} : \pi \equiv \pi + \omega \pi^{\mu_r} \pmod{\mathfrak{P}^{\mu_r+1}}$$

ist, so folgt leicht mit den Bezeichnungen in A, Kap. 1, § 5 [4])

$$(10) \qquad T^{-1} S_{i+1} T : \pi \equiv \pi + \omega \tau^{b_0 p^{-s(\mu_r-1)} \pi^{\mu_r}} \pmod{\mathfrak{P}^{\mu_r+1}}$$

$$(11) \qquad Z^{-1} S_{i+1} Z : \pi \equiv \pi + \omega^p \tau^{\lambda_0 p^{-s(\mu_r-1)} \pi^{\mu_r}} \pmod{\mathfrak{P}^{\mu_r+1}},$$

wo

$$\lambda_0 = \frac{a_0(p-1)}{e_0}, \qquad b_0 = \frac{p^f - 1}{e_0}.$$

## § 2.

## Normalkongruenzen für die Irregularkörper.

Im folgenden sollen nun die Eigenschaften der Irregularkörper eingehender studiert werden. Nach einer Bemerkung in A, Kap. 1, § 3 folgt sofort, daß wenn $\mathfrak{P}_0$ das Primideal im Regularkörper bezeichnet, worin $\mathfrak{P}$ aufgeht, so besteht in den Irregularkörpern eine Zerlegung

$$\mathfrak{P}_0 = \mathfrak{P}_1^p = \mathfrak{P}_2^{p^2} = \ldots = \mathfrak{P}_s^{p^s} = \mathfrak{P}^{p^s},$$

wobei jedes Primideal $\mathfrak{P}_i$ den Relativgrad 1 hat. Da nun $K_i$ nach der Definition ein relativ-zyklischer Körper vom Relativgrade $p$ zu $K_{i-1}$ ist, so kann man die Resultate aus A, Kap. 2, § 4 anwenden. Man erhält daraus eine Reihe von Tatsachen, welche in dem folgenden Hauptsatz zusammengefaßt werden können:

Satz 2. *Wenn $\pi_{i-1}$ eine Primzahl in $K_{i-1}$ in bezug auf $\mathfrak{P}_{i-1}$ ist, so kann man immer eine Primzahl $\pi_i$ in $K_i$ in bezug auf $\mathfrak{P}_i$ so bestimmen, daß $\pi_i$ für ein beliebig hohes $\alpha$ entweder einer binomischen Kongruenz*

$$(12) \qquad x^p - \pi_{i-1}\beta_{i-1} \equiv 0 \pmod{\mathfrak{P}^\alpha} \qquad (i = 1, 2, \ldots, s)$$

*oder einer trinomischen Kongruenz*

$$(13) \qquad x^p - \frac{1}{r_i}\tau^{b_i}\pi_{i-1}^{c_i+1} x^{r_i} - \pi_{i-1}\beta_{i-1} \equiv 0 \pmod{\mathfrak{P}^\alpha} \qquad (i = 1, 2, \ldots, s)$$

*genügt. Der binomische oder trinomische Fall tritt ein, je nachdem die relative Supplementzahl $\varrho_i$ von $\mathfrak{P}_i$ in bezug auf $K_{i-1}$ durch*

$$(14) \qquad \varrho_i = e_0 p^i$$

*oder*

$$(15) \qquad \varrho_i = c_i p + r_i < e_0 p^i \qquad (1 \leqq r_i \leqq p-1)$$

*gegeben ist; dabei ist also bekanntlich $\varrho_i$ dadurch definiert, daß die Relativdifferente von $K_i$ in bezug auf $K_{i-1}$ genau durch $\mathfrak{P}_i^{p-1+\varrho_i}$ teilbar sein*

[4]) Entsprechende Formeln kommen bei Speiser vor. Vgl. Speiser, Formel I u. II, § 3.

*soll. In jedem Falle ist*

$$\varrho_i \equiv 0 \pmod{p-1} \tag{16}$$

*und weiter im trinomischen Falle*

$$b_i \equiv 0 \pmod{p-1}. \tag{17}$$

*Die Zahl $\beta_{i-1}$, welche also in $K_{i-1}$ liegt, kann immer in der Form*

$$\beta_{i-1} = 1 + \tau^{a_i} \pi_{i-1} + \ldots + \tau^{a\frac{\varrho_i}{p-1}} \pi_{i-1}^{\frac{\varrho_i}{p-1}} \tag{18}$$

*geschrieben werden.*

## § 3.

## Bestimmung der Verzweigungen.

Die Normalkongruenzen des Satzes 2 sind nun die wichtigsten Hilfsmittel für das Studium der arithmetischen Eigenschaften des Galoisschen Körpers.

Die erste Aufgabe, welche hier behandelt werden soll, ist die Bestimmung des Zusammenhanges zwischen den Supplementzahlen $\varrho_i$ und den in A, Kap. 1, § 1 definierten Verzweigungen $\mu_r$. Die Verzweigung $\mu_r$ einer Verzweigungsgruppe $G_{V_r}$ war dadurch festgelegt, daß wenn $S$ eine Substitution in $G_{V_r}$, $\pi$ eine Primzahl in bezug auf $\mathsf{P}$ bedeutet, so ist

$$S:\pi \equiv \pi + \omega \pi^{\mu_r} (\mathrm{mod}\ \mathsf{P}^{\mu_r+1}),$$

wo $\omega$ nicht durch $\mathsf{P}$ teilbar ist.

Aus A, Kap. 1, § 5 folgt, daß eine beliebige Primzahl $\pi$ in $K$ einer irreduziblen Kongruenz

$$F_0(x) = x^{p^s} + \pi_0 C_1^{(0)} x^{p^s-1} + \ldots + \pi_0 C_{p^s}^{(0)} \equiv 0 \pmod{\mathsf{P}^a} \tag{19}$$

im Regularkörper genügt, und die Zahl $F_0'(\pi)$ wird genau dieselbe Potenz von $\mathsf{P}$ enthalten wie die Relativdifferente von $K$ in bezug auf $K_0$.

Es seien nun

$$\pi = \pi_1, \pi_2, \ldots, \pi_{p^s} \tag{20}$$

die verschiedenen Primzahlen, welche man erhält, wenn man auf $\pi$ die $p^s$ Substitutionen der Regulargruppe $G_0$ anwendet. Diese sind natürlich alle Wurzeln von (19) und man erhält daraus sofort

$$F_0'(\pi) \equiv (\pi - \pi_2)(\pi - \pi_3)\ldots(\pi - \pi_{p^s}) \pmod{\mathsf{P}^a}. \tag{21}$$

In (21) sind aber $p^s - p^{s-s_1}$ Faktoren genau durch $\mathsf{P}^{\mu_1}$, weiter $p^{s-s_1} - p^{s-s_1-s_2}$ genau durch $\mathsf{P}^{\mu_2}$ teilbar usw. und die Relativdifferente wird folglich genau durch $\mathsf{P}^{\Delta_0}$ teilbar, wo

$$\Delta_0 = (p^s - p^{s-s_1})\mu_1 + (p^{s-s_1} - p^{s-s_1-s_2})\mu_2 + \ldots + (p^{s_k} - 1)\mu_k. \tag{22}$$

Da die Differente des Regularkörpers genau durch $\mathfrak{P}^{p^s(e_0-1)}$ teilbar ist, erhält man den bekannten Hilbertschen Satz:

Satz 3. *Die Differente des Galoisschen Körpers $K$ ist genau durch $\mathfrak{P}^{\Delta}$ teilbar, wo*

$$\Delta = e - p^s + (p^s - p^{s-s_1})\mu_1 + \ldots + (p^{s_k} - 1)\mu_k.$$

Unsere Aufgabe war aber speziell die Relativdifferente eines Irregularkörpers $K_i$ in bezug auf $K_{i-1}$ zu berechnen. Betrachtet man zunächst den ersten Irregularkörper $K_1$, so folgt leicht nach der eben angewandten Methode, daß die Relativdifferente von $K$ in bezug auf $K_1$ genau durch $\mathfrak{P}^{\Delta_1}$ teilbar ist, wo

$$\Delta_1 = (p^{s-1} - p^{s-s_1})\mu_1 + \ldots + (p^{s_k} - 1)\mu_k,$$

und allgemein beweist man, daß die Relativdifferente von $K$ in bezug auf $K_i$ genau durch $\mathfrak{P}^{\Delta_i}$ teilbar ist, wo

$$\Delta_i = (p^{s-i} - p^{s-s_1-\ldots-s_v})\mu_v + \ldots + (p^{s_k} - 1)\mu_k,$$

wenn $K_i$ zwischen $K_{V_v}$ und $K_{V_{v+1}}$ liegt.

Daraus folgt aber sofort nach einem bekannten Satz über Differenten, daß die Relativdifferente von $K_i$ in bezug auf $K_{i-1}$ genau durch

$$\mathfrak{P}^{\Delta_{i-1}-\Delta_i} = \mathfrak{P}^{p^{s-i}(p-1)\mu_v}$$

teilbar ist, und man hat den Satz:

Satz 4. *Wenn der Irregularkörper $K_i$ zwischen $K_{V_v}$ und $K_{V_{v+1}}$ liegt, so ist die Relativdifferente von $K_i$ in bezug auf $K_{i-1}$ genau durch $\mathfrak{P}_i^{(p-1)\mu_v}$ teilbar.*

Dieser Satz gibt sofort die Relation zwischen den Verzweigungen $\mu_v$ und den Supplementzahlen $\varrho_i$. Die Relativdifferente von $K_i$ zu $K_{i-1}$ ist nämlich andererseits genau durch $P_i^{p-1+\varrho_i}$ teilbar, also nach Satz 4

$$p - 1 + \varrho_i = (p-1)\mu_v$$

und nach (16)

$$\mu_v = \frac{\varrho_i}{p-1} + 1.$$

Satz 5. *Wenn $K_i$ zwischen $K_{V_v}$ und $K_{V_{v+1}}$ liegt, besteht zwischen der Verzweigung $\mu_v$ und der relativen Supplementzahl $\varrho_i$ die Beziehung*

$$\mu_v = \frac{\varrho_i}{p-1} + 1. \tag{23}$$

*Für alle Körper $K_i$ zwischen $K_{V_v}$ und $K_{V_{v+1}}$ hat daher $\varrho_i$ denselben Wert, und die Reihe der Zahlen*

$$\frac{\varrho_i}{p-1} + 1 \qquad (i = 1, 2, \ldots, s) \tag{24}$$

*stimmt mit der Reihe*

$$\overbrace{\mu_1, \cdots \mu_1}^{s_1}, \quad \overbrace{\mu_2, \cdots \mu_2}^{s_2}, \cdots \overbrace{\mu_k, \cdots \mu_k}^{s_k} \tag{25}$$

*überein.*

Aus Satz 5 fließen schon verschiedene wichtige Eigenschaften des Körpers. Die Gleichung (7) in A, Kap. 1 zeigt sofort, daß

$$\varrho_1 \leqq \varrho_2 \leqq \varrho_3 \leqq \cdots \leqq \varrho_s. \tag{26}$$

Weiter leitet man aber unter Anwendung der Dedekind-Henselschen Ungleichung obere Grenzen für die Verzweigungen ab, welche das Resultat von Speiser[5]) verschärfen.

Aus (14) und (15) folgt nämlich $\varrho_i \leqq e_0 p^i$, und aus der Identität der beiden Reihen (24) und (25) ergibt sich dann

$$\mu_1 \leqq \left[\frac{e_0 p}{p-1}\right] + 1, \qquad \mu_2 \leqq \left[\frac{e_0 p^{s_1+1}}{p-1}\right] + 1, \ldots$$

und es besteht der allgemeine Satz:

Satz 6. *Für die Verzweigungen $\mu_r$ hat man die obere Begrenzung*

$$\mu_r \leqq \left[\frac{e_0 p^{s_1+\ldots+s_{r-1}+1}}{p-1}\right] + 1 \qquad (r = 1, 2, \ldots, k). \tag{27}$$

Speziell ist also für die größte Verzweigung

$$\mu_k \leqq \left[\frac{e_0 p^{s-s_k+1}}{p-1}\right] + 1 = \left[\frac{e}{(p-1)\, p^{s_k-1}}\right] + 1,$$

also sicher

$$\mu_k \leqq \left[\frac{e}{p-1}\right] + 1, \tag{28}$$

wie von Herrn Speiser bewiesen.

## § 4.

## Einteilung der Normalkongruenzen.

Es soll nun gezeigt werden, daß das System der Normalkongruenzen, welche nach Satz 2 das vollständige Restsystem (mod $\mathfrak{P}^\alpha$) in $K$ definieren, eine ganz spezielle und einfache Form haben muß. Dies folgt aus dem folgenden wichtigen Satz, der in diesem Paragraphen bewiesen werden soll:

Satz 7. *In der Reihe der Normalkongruenzen, welche nach Satz 2 die sukzessiven Irregularkörper definieren, sind entweder alle Kongruenzen binomisch*

$$x^p - \pi_{i-1}\beta_{i-1} \equiv 0 \pmod{\mathfrak{P}^\alpha} \qquad (i = 1, 2, \ldots, s) \tag{29}$$

[5]) Speiser, § 3, S. 183.

*oder alle trinomisch*

$$(30) \qquad x^p - \frac{1}{r}\tau^{b_i}\pi_{i-1}^{c_i+1}x^r - \pi_{i-1}\beta_{i-1} \equiv 0 \pmod{\mathfrak{P}^\alpha} \qquad (i = 1, 2, \ldots, s),$$

*wobei der Exponent r von i unabhängig ist.*

Durch diesen Satz kann man also immer die Untersuchungen in zwei Fälle zerlegen, je nachdem das Primideal $\mathfrak{P}$ einer Kette von binomischen oder einer Kette von trinomischen Kongruenzen entspricht.

Um den Satz 7 zu beweisen, wird angenommen, daß $\pi_i$ eine Primzahl ist, welche der Kongruenz (12) oder (13) genügt. Nach A, Kap. 2, § 4 haben dann die übrigen Lösungen die Form

$$(31) \qquad \pi_i + \tau^a \pi_i^{\mu_v}, \quad \pi_i + 2\tau^a \pi_i^{\mu_v}, \ldots, \pi_i + (p-1)\tau^a \pi_i^{\mu_v} \pmod{\mathfrak{P}_i^{\mu_v+1}},$$

wo also wie früher vorausgesetzt wird, daß $K_i$ zwischen $K_{V_v}$ und $K_{V_{v+1}}$ liegt. Man erhält die Wurzeln (31) aus $\pi_i$, indem man wiederholt die Substitution $S_i$ in $G_{i-1}$ anwendet.

Aus $\pi_i$ wird nun die Primzahl $\pi_{i+1}$ in $K_{i+1}$ abgeleitet, wo also $\pi_{i+1}$ entweder einer Kongruenz

$$(32) \qquad x^p - \beta_i \pi_i \equiv 0 \pmod{\mathfrak{P}^\alpha}$$

oder einer Kongruenz

$$(33) \qquad x^p - \frac{1}{r_{i+1}}\tau^{b_{i+1}}\pi_i^{c_{i+1}+1}x^{r_{i+1}} - \pi_i\beta_i \equiv 0 \pmod{\mathfrak{P}^\alpha}$$

genügt.

Der Körper $K_{i+1}$ liegt entweder zwischen $K_{V_v}$ und $K_{V_{v+1}}$ so wie $K_i$, oder zwischen $K_{V_{v+1}}$ und $K_{V_{v+2}}$. Im ersten Falle ist aber nach Satz 5 $\varrho_i = \varrho_{i+1}$, so daß die Kongruenzen für $\pi_i$ und $\pi_{i+1}$ gleichzeitig binomisch oder trinomisch sein müssen; im trinomischen Falle ist dann auch offenbar $r_i = r_{i+1}$, wie bewiesen werden sollte.

Um den Satz 7 zu beweisen, ist es daher nur notwendig den Fall zu betrachten, wo $K_{i+1}$ zwischen $K_{V_{v+1}}$ und $K_{V_{v+2}}$ liegt.

Zuerst wird vorausgesetzt, daß $\pi_i$ einer binomischen Kongruenz genügt, und es soll gezeigt werden, daß dann auch $\pi_{i+1}$ einer binomischen Kongruenz genügen muß.

Nimmt man nämlich an, $\pi_{i+1}$ genüge der trinomischen Kongruenz (33), so wendet man auf $\pi_{i+1}$ die Substitution $S_i$ in $G_{i-1}$ an und erhält eine neue Primzahl $\pi'_{i+1} = S_{i-1} : \pi_{i+1}$. Da nun die Gruppe $G_{i+1}$ ein Normalteiler von $G_{i-1}$ ist, gehört auch $\pi'_{i+1}$ zur Gruppe $G_{i+1}$ und ist also eine Zahl in $K_{i+1}$. Die Primzahl $\pi'_{i+1}$ genügt aber offenbar einer Kongruenz

$$(34) \qquad x^p - \frac{1}{r_{i+1}}\tau^{b_{i+1}}\pi_i'^{c_{i+1}+1}x^{r_{i+1}} - \pi_i'\beta_i' \equiv 0 \pmod{\mathfrak{P}^\alpha}$$

in $K_i$, wobei

$$(35) \qquad \pi_i' \equiv \pi_i + \omega\pi_i^{\mu_v} \pmod{\mathfrak{P}_i^{\mu_v+1}}$$

eine der Zahlen in (31) ist, und $\beta_i'$ geht aus $\beta_i$ hervor, wenn man $\pi_i$ durch $\pi_i'$ ersetzt.

Unter Anwendung der Resultate in A, Kap. 2, § 3 kann man aber zeigen, daß die Kongruenz (34) in $K_{i+1}$ nicht lösbar sein kann. Wird zunächst nach (35)

$$\pi_i' = \pi_i \gamma_i = \pi_i (1 + A \pi_i^{\mu_v - 1}), \quad A \not\equiv 0 \pmod{\mathfrak{P}_i}$$

gesetzt, so erhält die Kongruenz (34) die Form

$$x^p - \frac{1}{r_{i+1}} \tau^{b_{i+1}} \gamma_i^{c_{i+1}+1} \pi_i^{c_{i+1}+1} x^{r_{i+1}} - \pi_i \beta_i'' \equiv 0 \pmod{\mathfrak{P}^a}, \tag{36}$$

wo

$$\beta_i'' \equiv \beta_i + A \pi_i^{\mu_v - 1} \pmod{\mathfrak{P}_i^{\mu_v}}. \tag{37}$$

Nun ist es aber immer möglich, eine Zahl $\gamma_i' = 1 + B \pi_i^{\mu_v - 1}$ in $K_i$ so zu bestimmen, daß

$$\gamma_i^{c_{i+1}+1} \cdot \gamma_i'^{p - r_{i+1}} \equiv 1 \pmod{\mathfrak{P}_i^a},$$

und wenn man daher (36) mit $\gamma_i'^p$ multipliziert und $x$ an der Stelle von $\gamma_i' x$ schreibt, so folgt, daß auch die Kongruenz

$$x^p - \frac{1}{r_{i+1}} \tau^{b_{i+1}} \pi_i^{c_{i+1}+1} x^{r_{i+1}} - \pi_i \beta_i''' \equiv 0 \pmod{\mathfrak{P}^a} \tag{38}$$

gleichzeitig mit (34) in $K_{i+1}$ lösbar sein muß. Dabei ist also nach (37)

$$\beta_i''' = \beta_i'' \gamma_i'^p \equiv \beta_i + A \pi_i^{\mu_v - 1} \pmod{\mathfrak{P}_i^{\mu_v}}. \tag{39}$$

Wendet man aber auf (38) den Satz 4 in A, Kap. 2 an, so folgt sofort nach (39), daß, wenn die Kongruenz (38) in $K_{i+1}$ lösbar sein soll, die Bedingung

$$\mu_v - 1 + r_{i+1} \equiv 0 \pmod{p} \tag{40}$$

erfüllt sein muß. Wenn aber $\pi_i$ einer binomischen Kongruenz genügt, so ist $\varrho_i \equiv 0 \pmod{p}$, und folglich nach Satz 5 $\mu_v \equiv 1 \pmod{p}$, so daß nach (40) auch $r_{i+1}$ durch $p$ teilbar wäre, was offenbar nicht möglich ist. Es ist daher bewiesen, daß, wenn $\pi_i$ einer binomischen Kongruenz genügt, die Kongruenz für $\pi_{i+1}$ und daher für alle folgenden Primzahlen binomisch ist.

Es bleibt folglich nur übrig zu zeigen, daß, wenn $\pi_i$ einer trinomischen Kongruenz genügt, dann $\pi_{i+1}$ keiner binomischen Kongruenz genügen kann. Um dies zu leisten, wendet man auf $\pi_{i+1}$ die Substitution $S_i$ an, und wenn $\pi_{i+1}$ einer binomischen Kongruenz (32) genügte, würde $\pi_{i+1}' = S_i : \pi_{i+1}$ der Kongruenz

$$x^p - \pi_i' \beta_i' \equiv 0 \pmod{\mathfrak{P}^a} \tag{41}$$

genügen, wo die Bezeichnung die frühere ist. Die Kongruenz (41) kann dann weiter in der Form

$$x^p - \pi_i \beta_i'' \equiv 0 \pmod{\mathfrak{P}^\alpha} \tag{42}$$

geschrieben werden, wo wie früher

$$\beta_i'' \equiv \beta_i + A \pi_i^{\mu_\nu - 1} \pmod{\mathfrak{P}_i^{\mu_\nu}}. \tag{43}$$

Wenn aber die Kongruenz (42) in $K_{i+1}$ lösbar sein soll, muß nach Satz 2, A, Kap. 2 die Zahl

$$\frac{\beta_i''}{\beta_i} \equiv 1 + A \pi_i^{\mu_\nu - 1} \pmod{\mathfrak{P}_i^{\mu_\nu}}$$

eine $p$-te Potenz $(\mathrm{mod}\, \mathfrak{P}_i^{\alpha})$ sein, und dies ist weiter, wie leicht aus (28) folgt, nur dann möglich, wenn $\mu_\nu - 1$ durch $p$ teilbar ist. Nach Satz 5 folgt aber daraus weiter, daß $\varrho_i$ durch $p$ teilbar ist, was nicht möglich sein kann, wenn $\pi_i$ einer trinomischen Kongruenz genügt.

Die Normalkongruenzen sind also alle entweder binomisch oder trinomisch, und es bleibt nur zu zeigen, daß im trinomischen Falle der Exponent $r_i$ eine von $i$ unabhängige Konstante ist. Es genügt offenbar zu zeigen, daß $r_i \equiv r_{i+1} \pmod{p}$.

Dies folgt aber sehr einfach nach der eben angewandten Methode. Man wendet im trinomischen Falle auf $\pi_{i+1}$ die Substitution $S_i$ an, und die so erhaltene Primzahl $\pi_{i+1}'$ wird einer Kongruenz (34) genügen. Wird weiter die Bedingung für die Lösbarkeit dieser Kongruenz in $K_{i+1}$ gesucht, erhält man die Relation (40). Nach Satz 5 ist aber $\mu_\nu - 1 \equiv -r_i \pmod{p}$, und daraus folgt in der Tat $r_i \equiv r_{i+1} \pmod{p}$, wie bewiesen werden sollte.

Wenn man Satz 7 mit den Sätzen 5 und 2 kombiniert, erhält man sofort den weiteren interessanten Satz über die Verzweigungen:

Satz 8. *Im binomischen Falle ist*

$$\mu_1 \equiv \mu_2 \equiv \ldots \equiv \mu_k \equiv 1 \pmod{p}, \tag{44}$$

*während im trinomischen Falle*

$$\mu_1 \equiv \mu_2 \equiv \ldots \equiv \mu_k \equiv 1 - r \pmod{p}. \tag{45}$$

Dieser Satz enthält speziell das Resultat von Speiser[6]), daß alle Verzweigungen einander $(\mathrm{mod}\, p)$ kongruent sein müssen.

Zuletzt sei auch noch erwähnt, daß man aus (15) und (16) noch die weitere Relation

$$c_1 \equiv c_2 \equiv \ldots \equiv c_s \equiv -r \pmod{p-1} \tag{46}$$

erhält.

---

[6]) Speiser, Satz 4, S. 183.

## Kapitel 2.
## Der binomische Fall.

### § 1.
### Bestimmung der Verzweigungen.

Der binomische Fall soll nun eingehend studiert werden, und wie man sehen wird, sind hier die Verhältnisse besonders einfach und übersichtlich.

Aus A, Kap. 2, Satz 5 folgt schon, daß, wenn der binomische Fall eintreten soll, der Regularkörper $K_0$ die $p$-te Einheitswurzel $(\mathrm{mod}\ \mathfrak{P}^\alpha)$ enthalten muß. Wenn aber die Primzahl $\pi_0$ in $K_0$ durch die binomische Normalkongruenz (vgl. A, Kap. 1, Satz 6)

$$x^{e_0} + \tau^{a_0} p \equiv 0 \ (\mathrm{mod}\ \mathfrak{P}^\alpha) \tag{1}$$

definiert ist, so muß, als notwendige und hinreichende Bedingung, daß $K_0$ eine $p$-te Einheitswurzel $(\mathrm{mod}\ \mathfrak{P}^\alpha)$ enthält,

$$e_0 \equiv a_0 \equiv 0 \ (\mathrm{mod}\ p-1)$$

sein.

Weiter folgt aus Satz 2, daß für den $i$-ten Irregularkörper

$$\varrho_i = e_0 p^i \qquad (i = 1, 2, \ldots, s) \tag{2}$$

ist, und da diese alle verschieden sind, folgt nach Satz 5, daß die Reihe der Verzweigungskörper mit der Reihe der Irregularkörper zusammenfällt, indem allgemein

$$K_i = K_{V_{i+1}} \qquad (i = 1, 2, \ldots, s).$$

Nach Satz 5 folgt weiter aus (2), daß die Verzweigung $\mu_i$ durch

$$\mu_i = \frac{e_0 p^i}{p-1} + 1 \qquad (i = 1, 2, \ldots, s)$$

bestimmt ist.

Satz 9. *Im binomischen Falle erhält man den Galoisschen Körper $K$ aus dem Regularkörper $K_0$ durch eine Reihe von $s$ Verzweigungskörpern von den sukzessiven Relativgraden $p$. Die Verzweigung $\mu_i$ hat allgemein den Wert*

$$\mu_i = \frac{e_0 p^i}{p-1} + 1 \qquad (i = 1, 2, \ldots, s), \tag{3}$$

*und die Konstanten des Regularkörpers müssen der Bedingung*

$$e_0 \equiv a_0 \equiv 0 \ (\mathrm{mod}\ p-1) \tag{4}$$

*genügen.*

Zuletzt sei bemerkt, daß in diesem Falle natürlich alle Zahlen $s_i$ in (2), Kap. 1 den gemeinsamen Wert 1 haben, und dann zeigt der Satz 3, Kap. 1, daß die Differente des Galoisschen Körpers durch $\mathfrak{P}^\Delta$ teilbar ist, wo

$$\Delta = (s+1)e - 1.$$

## § 2.

## Sätze über die Verzweigungsgruppen.

Zuerst soll nun bewiesen werden:

Satz 10. *Im binomischen Falle ist die Verzweigungsgruppe zyklisch.*

Dieser Satz wird unter Anwendung einer Methode von Herrn Fueter[7]) einfach in der folgenden Weise bewiesen:

Im allgemeinen Falle, wo also das System der Normalkongruenzen beliebig binomisch oder trinomisch sein darf, sei $V_i$ eine Substitution der $i$-ten Verzweigungsgruppe, folglich

$$V_i : \pi = \pi + \pi^{\mu_i} A_1(\pi), \qquad A_1(\pi) = a_0 + a_1 \pi + \dots .$$

Durch Wiederholung folgt sofort

$$V_i^2 : \pi = \pi + 2\pi^{\mu_i} A_1(\pi) + \pi^{2\mu_i - 1} A_2(\pi), \qquad A_2(\pi) = \mu_i a_0^2 + \dots,$$
$$V_i^3 : \pi = \pi + 3\pi^{\mu_i} A_1(\pi) + 3\pi^{2\mu_i - 1} A_2(\pi) + \pi^{3\mu_i - 2} A_3(\pi),$$
$$A_3(\pi) = \mu_i (2\mu_i - 1)\, a_0^3 + \dots,$$

und daher im allgemeinen

$$(5) \qquad V_i^p : \pi = \pi + \binom{p}{1} \pi^{\mu_i} A_1(\pi) + \binom{p}{2} \pi^{2\mu_i - 1} A_2(\pi) + \dots + \pi^{p\mu_i - p + 1} A_p(\pi),$$

wo

$$(6) \qquad A_p(\pi) = a_0^p \mu_i (2\mu_i - 1) \dots ((p-1)\mu_i - p + 2) + \dots .$$

Nach der Ungleichung (28), Kap. 1 wird nun das letzte Glied in (5) für die Verzweigungsgruppe bestimmend, in der $V_i^p$ liegt.

Nimmt man nun zuerst den binomischen Fall an, so genügt $\mu_i$ nach (3) der Bedingung

$$(7) \qquad p\mu_i - p + 1 = \mu_{i+1},$$

und da in diesem Falle $\mu_i \equiv 1 \pmod p$, wird $A_p(\pi)$ nicht durch $\mathfrak{P}$ teilbar, so daß $V_i^p = V_{i+1}$ eine Substitution der $(i+1)$-ten, aber keiner höheren Verzweigungsgruppe wird; der Satz 10 ist dadurch bewiesen.

Im trinomischen Falle ist $\mu_i \not\equiv 1 \pmod p$ und $A_p(\pi)$ ist folglich durch $\mathfrak{P}$ teilbar; $V_i^p$ gehört daher zu einer Verzweigungsgruppe $G_{V_j}$, $j > i$, wofür

$$\mu_j > p(\mu_i - 1) + 1.$$

Da aber nach Satz 8 $\mu_j \equiv -r + 1 \pmod p$ sein muß, erhält man den folgenden Satz, der zuerst von Speiser[8]) in einer etwas anderen Form abgeleitet worden ist:

---

[7]) R. Fueter, Ein Satz über Iteration von Potenzreihen und seine zahlentheoretische Anwendung, Vierteljahrsschrift d. Naturforschenden Ges. Zürich 1917, S. 67–72.

[8]) Speiser, Satz 5′, S. 184.

Satz 11. *Eine Substitution $V_i^p$ gehört im trinomischen Falle zu einer Verzweigungsgruppe $G_{V_j}$, für die*

$$\mu_j \geqq p\mu_i - r + 1. \tag{8}$$

## § 3.
## Eindeutigkeit der Normalkongruenzen.

Ehe wir zu einer weiteren Untersuchung der Gruppen im binomischen Falle übergehen, sollen ein paar wichtige Hilfssätze über die binomischen Normalkongruenzen bewiesen werden.

Es sei

$$x^p - \pi_i \beta_i \equiv 0 \pmod{\mathfrak{P}^a} \tag{9}$$

die definierende Kongruenz für den $(i+1)$-ten Irregularkörper $K_{i+1}$. Die Zahl $\beta_i$ hat nach Satz 2 die Form

$$\beta_i = 1 + \tau^{a_1}\pi_i + \ldots + \tau^{a_\nu}\pi_i^\nu, \tag{10}$$

wo $\nu = \frac{e_0 p^{i+1}}{p-1}$ ist. Es kann nun gezeigt werden, daß die Primzahl $\pi_{i+1}$ in $K_{i+1}$ sogar so gewählt werden kann, daß in (10) keine Glieder $\tau^{a_j}\pi_i^j$ vorkommen, wo der Exponent $j$ durch $p$ teilbar ist.

Wenn nämlich

$$\tau^{a_{tp}}\pi_i^{tp}, \qquad tp < \nu = \frac{e_0 p^{i+1}}{p-1} \tag{11}$$

das erste Glied dieser Art in (10) ist, kann man

$$\pi'_{i+1} = \pi_{i+1}\,(1 + \omega\pi_i^t)$$

setzen, und erhält für $\pi'_{i+1}$ die Kongruenz

$$x^p - \pi_i \beta'_i \equiv 0 \pmod{\mathfrak{P}^a},$$

wo $\beta'_i$ den Wert

$$\beta'_i = \beta_i(1+\omega\pi_i^t)^p = \beta_i + \beta_i\omega^p\pi_i^{tp} + \ldots + p\beta_i\omega\pi_i^\iota + \ldots \tag{12}$$

hat. Nach der Ungleichung (11) sind aber in (12) alle durch $p$ teilbaren Glieder durch höhere Potenzen von $\mathfrak{P}$ als die Zahl $\pi_i^{tp}$ teilbar, so daß man für $\beta'_i$ die Kongruenz

$$\beta'_i \equiv \beta_i + \omega^p\pi_i^{tp} \pmod{\mathfrak{P}_i^{tp+1}}$$

erhält. Man braucht daher nur $\omega$ so zu bestimmen, daß

$$\omega^p + \tau^{a_{tp}} \equiv 0 \pmod{\mathfrak{P}_i}$$

ist, was offenbar immer möglich ist. In dieser Weise kann man nach und nach alle Glieder (11) in (10) wegschaffen, indem diejenigen Glieder in $\beta'_i$, welche höhere Potenzen als $\pi_i^\nu$ enthalten, nach A, Kap. 2, § 2 für die Lösbarkeit der Kongruenz keine Rolle spielen. Das letzte Glied in (10) ge-

hört auch zu den Ausnahmegliedern (11), aber es ist im allgemeinen nicht möglich dieses Glied wegzubringen.

Wenn $\beta_i$ die Form hat, wo alle Glieder (11) fehlen, soll dies eine *reduzierte Darstellung* für $\beta_i$ heißen. Die Bedeutung der reduzierten Darstellung geht aus dem folgenden Satze hervor:

Satz 12. *Es seien*

$$x^p - \pi_i \beta_i \equiv 0, \qquad x^p - \pi_i \beta_i' \equiv 0 \pmod{\mathfrak{P}^\alpha} \tag{13}$$

*zwei Normalkongruenzen, welche beide $K_{i+1}$ definieren, und worin sowohl $\beta_i$ als $\beta_i'$ reduziert sind. Dann ist*

$$\beta_i' \equiv \beta_i \pmod{\mathfrak{P}_i^\nu} \tag{14}$$

*und weiter muß es eine Zahl $\omega$ geben, so daß*

$$\tau^{a_\nu'} \equiv \tau^{a_\nu} + \omega^p - \omega \tau^{-a_0} \pmod{\mathfrak{P}_i}. \tag{15}$$

Der Satz sagt kurz, daß die reduzierte Darstellung von $\beta_i$, abgesehen vom letzten Gliede, eine eindeutige ist.

Der Beweis ist einfach. Wenn die Kongruenzen (13) gleichzeitig in $K_{i-1}$ lösbar sind, gibt es nach A, Kap. 2, Satz 2 eine solche Zahl $\gamma_i$ in $K_i$, daß

$$\beta_i' \equiv \gamma_i^p \beta_i \pmod{\mathfrak{P}^\alpha}, \tag{16}$$

wo man natürlich $\gamma_i$ in der Form

$$\gamma_i = 1 + A\pi_i^\sigma, \qquad A \not\equiv 0 \pmod{\mathfrak{P}_i} \tag{17}$$

schreiben kann. Für den Beweis des Satzes 12 ist offenbar nur der Fall von Interesse, daß $\sigma \leqq \frac{e_0 p^i}{p-1}$ ist. Wenn $\sigma < \frac{e_0 p^i}{p-1}$ ist, erhält man aus (16)

$$\beta_i' \equiv \beta_i + \beta_i A^p \pi_i^{\sigma p} + \ldots + \beta_i p A \pi_i^\sigma + \ldots \pmod{\mathfrak{P}_i^\alpha}. \tag{18}$$

Hier sind die durch $p$ teilbaren Glieder durch höhere Potenzen von $\mathfrak{P}_i$ als $\pi_i^{\sigma p}$ teilbar und folglich kann $\beta_i'$ in diesem Falle nicht reduziert sein.

Man hat daher in (17) $\sigma = \frac{e_0 p^i}{p-1}$, und in diesem Falle ist nach (18) die Bedingung (14) erfüllt. Aus (18) erhält man dann aber weiter

$$\pi_i^\nu \tau^{a_\nu'} \equiv \pi_i^\nu \tau^{a_\nu} + A^p \pi_i^\nu + pA\pi^{\frac{e_0 p^i}{p-1}} \pmod{\mathfrak{P}_i^{\nu+1}},$$

und wenn man hier den Wert von $p$ aus (1) einsetzt, schließt man weiter

$$\tau^{a_\nu'} \equiv \tau^{a_\nu} + A^p - A\tau^{-a_0} \pmod{\mathfrak{P}_i},$$

wie bewiesen werden sollte.

Man beweist auch leicht die Umkehrung des Satzes 12, daß, wenn (14) und (15) erfüllt sind, die Kongruenzen (13) gleichzeitig in $K_{i+1}$ lösbar sein müssen.

Man kann in (15) voraussetzen, daß $\omega = \omega(\tau)$ eine Zahl im Trägheitskörper ist. Alle Zahlen

$$\omega^p - \omega\tau^{-a_0} \pmod{p}$$

in $K_T$ bilden einen Modul

$$\mathsf{M} = (p, \omega^p - \omega\tau^{-a_0})$$

und man hat daher nach (15)

$$\tau^{a_\nu'} \equiv \tau^{a_\nu} \pmod{\mathsf{M}}.$$

Es folgt leicht, daß alle Zahlen im Trägheitskörper (mod M) in $p$ Klassen von $p^{f-1}$ Zahlen zerfallen. Denn eine Kongruenz

$$\omega_1^p - \omega\tau^{-a_0} \equiv \omega^p - \omega\tau^{-a_0} \pmod{p}$$

kann nur dann bestehen, wenn

$$(\omega_1 - \omega)^p \equiv (\omega_1 - \omega)\tau^{-a_0} \pmod{p},$$

woraus man sofort

$$\omega_1 \equiv \omega + k\tau^{\frac{a_0}{p-1}} \pmod{p} \quad (k = 0, 1, 2, \ldots, p-1)$$

erhält.

## § 4.

## Reduktion der Normalkongruenzen.

Zuletzt soll noch gezeigt werden, wie man durch den Satz 12 eine noch weitere Reduktion der Normalkongruenzen erreichen kann.

Als Beispiel soll zuerst die erste Normalkongruenz

$$x^p - \beta_0\pi_0 \equiv 0 \pmod{\mathsf{P}^\alpha}, \tag{19}$$

welche den ersten Irregularkörper definiert, studiert werden. Wie früher kann man annehmen, daß $\beta_0$ in reduzierter Darstellung gegeben ist:

$$\beta_0 = 1 + \tau^{a_1}\pi_0 + \ldots + \tau^{a\frac{e_0 p}{p-1}}\pi_0^{\frac{e_0 p}{p-1}}, \tag{20}$$

worin, vom letzten Gliede abgesehen, keine Exponenten von $\pi_0$ durch $p$ teilbar sind.

Wendet man nun auf die Wurzel $\pi_1$ der Kongruenz (19) eine Substitution $T$ der Trägheitsgruppe an, so geht $\pi_1$ in eine Wurzel $\pi_1'$ der Kongruenz

$$x^p - \beta_0'\pi_0\tau^{b_0} \equiv 0 \pmod{\mathsf{P}^\alpha}, \quad b_0 = \frac{p^f - 1}{e_0} \tag{21}$$

über, wo also nach (20)

$$\beta_0' = 1 + \tau^{a_1+b_0}\pi_0 + \tau^{a_2+2b_0}\pi_0^2 + \ldots . \tag{22}$$

Die Zahl $\pi_1' \cdot \tau^{\frac{b_0}{p}}$ genügt aber nach (21) der Kongruenz

$$x^p - \beta_0' \pi_0 \equiv 0 \pmod{\mathfrak{P}^a}, \tag{23}$$

und diese Kongruenz muß gleichzeitig mit (19) in $K_1$ lösbar sein. Da aber nach (22) auch $\beta_0'$ in reduzierter Form ist, so muß $\beta_0'$, abgesehen vom letzten Gliede, mit $\beta_0$ identisch sein, und man hat daher für alle $i$

$$a_i \equiv a_i + i\, b_0 \pmod{p^f - 1},$$

d. h. $i$ ist durch $e_0$ teilbar, und $\beta_0$ hat die einfache Form

$$\beta_0 = 1 + \tau^{a_1} \pi_0^{e_0} + \tau^{a_2} \pi_0^{\frac{e_0 p}{p-1}}. \tag{24}$$

Übt man weiter auf $\pi_1$ die Substitution $Z$ aus der Zerlegungsgruppe aus, so geht $\pi_0$ in $\pi_0 \tau^{\lambda_0}$ über, und man erhält daraus sofort

$$a_1 \equiv p\, a_1 + e_0 \lambda_0 \pmod{p^f - 1},$$

und wenn man hier den Wert $\lambda_0 = \frac{a_0 (p-1)}{e_0}$ einsetzt, kommt ohne Schwierigkeit

$$\tau^{a_1} \equiv k_0 \tau^{-a_0} \pmod{p},$$

wo $k_0$ eine rationale, nicht durch $p$ teilbare Zahl ist. Nach (24) und (1) erhält daher $\beta_0$ die noch einfachere Form

$$\beta_0 = 1 + k_0 p + \tau^{a_2} \pi_0^{\frac{e_0 p}{p-1}}. \tag{25}$$

Im allgemeinen wird aber auch wegen der Bedingung (15) das letzte Glied in (25) verschwinden. Durch die Substitution $T^i$ geht nämlich dieses Glied in

$$\tau^{a_2 + i b_0 \frac{e_0 p}{p-1}} \pi_0^{\frac{e_0 p}{p-1}}$$

über, und hier ist

$$\tau^{a_2 + i b_0 \frac{e_0 p}{p-1}} = \tau^{a_2 + i p \frac{p^f - 1}{p-1}} \equiv k_i \tau^{a_2} \pmod{p},$$

wo die rationale Zahl $k_i$ alle Werte $1, 2, \ldots, p-1$ annehmen kann. Da nun nach Satz 12 immer eine Kongruenz

$$k_i \tau^{a_2} \equiv \tau^{a_2} + \omega^p - \tau^{-a_0} \omega \pmod{p}$$

bestehen muß, so folgt, wenn man $p > 2$ voraussetzt und daher $k_i = 2$ wählen kann,

$$\tau^{a_2} \equiv \omega^p - \tau^{-a_0} \omega \pmod{p},$$

d. h. $\tau^{a_2}$ gehört $(\mathrm{mod}\, p, \omega^p - \tau^{-a_0} \omega)$ zur selben Klasse wie die Zahl 0, und nach § 3 kann man dann die Zahl $\pi_1$ so wählen, daß das letzte

Glied in $\beta_0$ (25) nicht vorkommt. Im Falle $p=2$ kann man nach (25) $\beta_0 = 1 + 2k_0 + 4\omega_1$ schreiben, und wie früher zeigt man, daß die $p^f$ möglichen $\omega_1$ in zwei Klassen (mod 2, $\omega^2 - \omega$) zerfallen. Wenn $f$ nicht durch 2 teilbar ist, gehören die Zahlen 0 und 1 zu verschiedenen Klassen, indem eine Kongruenz

$$\omega^2 - \omega \equiv 1 \pmod{p}$$

nicht lösbar sein kann. Man kann daher in diesem Falle $\omega_1 = 0$ oder $\omega_1 = 1$ annehmen. Wenn $f$ gerade ist, wird man aber nicht immer das letzte Glied als rational annehmen können.

Satz 13. *Im binomischen Falle kann man die Primzahl $\pi_1$ des ersten Irregularkörpers so wählen, daß die Konstante $\beta_0$ durch*

$$\beta_0 = 1 + k_0 p \tag{26}$$

*gegeben ist. Eine Ausnahme bildet nur der Fall, wo $p=2$ und $f$ gerade ist; in diesem Falle hat man auch die Möglichkeit*

$$\beta_0 = 1 + 2k_0 + 4\tau^{h_0}. \tag{27}$$

Im Falle $p > 2$ (und wir beschränken uns vorläufig nur auf diesen Fall) wird $\beta_0$ durch die Substitutionen $T$ und $Z$ nicht geändert, und man kann daher diese Substitutionen so wählen, daß

$$T: \pi_1 \equiv \tau^{\frac{b_0}{p}} \pi_1, \qquad Z: \pi_1 \equiv \tau^{\frac{\lambda_0}{p}} \pi_1 \pmod{\mathfrak{P}^\alpha}.$$

Man kann nun durch Induktion für eine beliebige Normalkongruenz den folgenden Satz beweisen:

Satz 14. *Die Konstante $\beta_i$ der $(i+1)$-ten Normalkongruenz hat für $p > 2$ die Form*

$$\begin{aligned} \beta_i &= 1 + k_1 A_i + k_2 A_i^2 + \ldots, \\ A_i &= \tau^{-\frac{a_0}{p^i}} \pi_i^{e_0}, \end{aligned} \tag{28}$$

*wo alle Koeffizienten $k$ rational sind; speziell fehlt das letzte Glied, welches die Potenz $\pi_i^{\frac{e_0 p^{i+1}}{p-1}}$ enthalten sollte. Weiter ist*

$$T: \pi_{i+1} \equiv \tau^{\frac{b_0}{p^{i+1}}} \pi_{i+1}, \qquad Z: \pi_{i+1} \equiv \tau^{\frac{\lambda_0}{p^{i+1}}} \pi_{i+1} \pmod{\mathfrak{P}^\alpha}. \tag{29}$$

Zunächst sei

$$\beta_i = 1 + \sum \tau^{a_r} \pi_i^r \tag{30}$$

die reduzierte Darstellung der Konstanten der $(i+1)$-ten Normalkongruenz

$$x^p - \beta_i \pi_i \equiv 0 \pmod{\mathfrak{P}^\alpha}. \tag{31}$$

Nimmt man nun den Satz 14 für alle vorangehenden Normalkongruenzen als bewiesen an, so folgt wie im Beweise des Satzes 13, wenn man auf (31) die Substitutionen $T$ und $Z$ anwendet, daß $\beta_i$ in (30) die Form (28) haben muß, wenn man vom letzten Gliede absieht. Durch denselben Kunstgriff, wodurch das letzte Glied in $\beta_0$ weggebracht wurde, zeigt man aber, daß auch in $\beta_i$ dieses Glied bei einer passenden Wahl von $\pi_{i+1}$ zum Fehlen gebracht werden kann. Dann bleibt aber $\beta_i$ durch $Z$ und $T$ ungeändert, und es folgt sofort, daß diese Substitutionen so bestimmt werden können, daß die Kongruenzen (29) bestehen. Der Satz 14 ist dadurch vollständig bewiesen.

Zuletzt sei noch erwähnt, daß man eine noch größere Reduktion der Koeffizienten $\beta_i$ der Normalkongruenzen (31) erhält, wenn man noch die Bedingung ausnützt, daß diese Kongruenzen auch dann lösbar sein müssen, wenn man auf $\pi_i \beta_i$ eine Substitution $V_j$, $j < i$, einer der vorausgehenden Verzweigungsgruppen ausübt.

Aus diesen Betrachtungen erhält man den folgenden Satz, den ich ohne Beweis mitteile:

Satz 15. *Man kann immer die Konstante $\beta_i$ der $(i+1)$-ten Normalkongruenz für $p > 2$ auf die Form*

$$\beta_i = 1 - \frac{1}{e_0 (p^i - 1)} A_i^{p^{i-1}} + p (l_1 A_i + l_2 A_i^2 + \ldots), \tag{32}$$

$$A_i = \tau^{-\frac{a_0}{p^i}} \pi_i^{e_0}$$

*reduzieren, wo alle Koeffizienten $l$ rational sind.*

Aus (32) erhält man z. B. speziell für die Konstante der zweiten Normalkongruenz

$$\beta_1 = 1 - \frac{1}{e_0 (p-1)} \tau^{-\frac{a_0}{p}(p-1)} \pi_1^{e_0 (p-1)} + k p \tau^{-\frac{a_0}{p}} \pi_1^{e_0},$$

wo $k$ eine beliebige rationale Zahl ist.

Wie man sieht, gibt der Satz (32) eine erhebliche Reduktion der Konstanten $\beta_i$. Die Form (32) repräsentiert aber im allgemeinen nicht die möglichst große Vereinfachung, und es ist wirklich möglich, eine absolut einfachste Normalform anzugeben. Es wird aber hier zu weit führen, diese Resultate abzuleiten. Sie sind aber, wie ich später erwähne, für die Bestimmung der Trägheitsgruppe in speziellen Fällen von Wichtigkeit.

## § 5.

## Bestimmung der Trägheits- und Zerlegungsgruppe.

Nach diesen Vorbereitungen ist es im binomischen Falle möglich die vollständige Struktur der Zerlegungs- und Trägheitsgruppe anzugeben.

Da nach Satz 10 die Verzweigungsgruppe im binomischen Falle zyklisch ist, kann man eine solche Substitution $V$ bestimmen, daß

$$G_V = V^k \qquad (k = 0, 1, \ldots, p^s - 1).$$

Weiter ist aber nach (29) für $i = s - 1$

$$T : \pi \equiv \tau^{\frac{b_0}{p^s}} \pi, \qquad Z : \pi \equiv \tau^{\frac{l_0}{p^s}} \pi \pmod{\mathfrak{P}^a} \tag{33}$$

und daraus folgt ohne Schwierigkeiten

$$T^{e_0} = 1, \qquad Z^f = T^{a_0}, \qquad Z^{-1} T Z = T^p.$$

Da $G_V$ ein Normalteiler von $G_Z$ und $G_T$ ist, so wird

$$Z^{-1} V Z = V^{z_0}, \qquad T^{-1} V T = V^{t_0} \tag{34}$$

und unsere Aufgabe ist vollständig gelöst, wenn die Konstanten $t_0$ und $z_0 \pmod{p^s}$ bestimmt sind.

Man kann zunächst die Eigenschaften von $z_0$ und $t_0 \pmod p$ ableiten. Wenn nämlich

$$V : \pi_1 = \pi_1 + \tau^{-\frac{a_0}{p-1}} \pi_1^{\frac{e_0 p}{p-1}+1} + \ldots,$$

erhält man wie in (10), Kap. 1

$$T^{-1} V T : \pi_1 = \pi_1 + \tau^{-\frac{a_0}{p-1} + \frac{p'-1}{p-1}} \pi_1^{\frac{e_0 p}{p-1}+1} + \ldots.$$

Hier ist aber

$$d_0 \equiv \tau^{\frac{p'-1}{p-1}} \pmod p$$

eine rationale Zahl, und da $\tau$ eine primitive Wurzel der Kongruenz

$$x^{p^f - 1} - 1 \equiv 0 \pmod{p^a}$$

ist, so folgt, daß $t_0 \equiv d_0 \pmod p$ eine primitive Wurzel der Kongruenz $x^{p-1} \equiv 1 \pmod p$ ist, d. h. $t_0$ gehört zum Exponenten $p - 1 \pmod p$. Man sieht auch leicht, daß durch eine passende Wahl von $T$ die Zahl $t_0$ eine beliebige der $\varphi(p-1)$ zu $p - 1 \pmod p$ gehörenden Zahlen sein kann.

Aus (11), Kap. 1 erhält man in derselben Weise $z_0 \equiv 1 \pmod p$.

Um aber die Konstante $t_0$ vollständig zu bestimmen, bemerkt man, daß nach (34)

$$T^{-(p-1)} V T^{p-1} = V^{t_0^{p-1}}. \tag{35}$$

Wenn nun

$$\pi' = V : \pi = \pi + \sum_i \tau^{a_i} \pi^{r_i} \tag{36}$$

gesetzt wird, erhält man einfach nach (33)

$$\pi'' = T^{-(p-1)} V T^{p-1} : \pi = \pi + \sum_i \tau^{a_i + (r_i - 1)(p-1)\frac{b_0}{p^s}},$$

und folglich ist

$$\pi' - \pi'' = \sum_i \tau^{a_i} \pi^{r_i} \left(1 - \tau^{(r_i-1)(p-1)\frac{b_0}{p^s}}\right). \tag{37}$$

Diese Differenz muß aber natürlich genau durch $\mathfrak{P}^{\frac{e_0 p^j}{p-1}+1}$ teilbar sein, wo $j$ eine der Zahlen $1, 2, \ldots, s$ bezeichnet. Wird aber in (37) $r_i = \frac{e_0 p^j}{p-1}+1$ gesetzt, so verschwindet der entsprechende Koeffizient in dieser Summe, und man hat folglich $\pi' = \pi''$. Nach (35) ist daher

$$T^{-(p-1)} V T^{p-1} = V,$$

und $t_0$ muß eine primitive Wurzel der Kongruenz

$$t_0^{p-1} \equiv 1 \pmod{p^s}$$

sein. Die Trägheitsgruppe ist dadurch vollständig bestimmt.

Satz 16. *Im binomischen Falle hat die Trägheitsgruppe die Form*

$$G_T = T^i V^j \quad (i = 0, 1, \ldots, e_0 - 1;\ j = 0, 1, \ldots, p^s),$$

*wo*

$$T^{e_0} = V^{p^s} = 1, \qquad T^{-1} V T = V^{t_0},$$

*und $t_0$ ist eine primitive Wurzel der Kongruenz*

$$t_0^{p-1} - 1 \equiv 0 \pmod{p^s}.$$

Dieser Satz ist nur für $p > 2$ bewiesen; durch einige einfache Übertragungen auf den Fall $p = 2$ zeigt man aber, daß der Satz auch für diese Primzahl richtig bleibt.

Aus Satz 13 folgt nämlich, daß $\beta_0$ durch die Substitution $T$ nicht geändert wird, während $\pi_0$ in $\pi_0 \tau^{b_0}$ übergeht. Man kann daher $T$ so wählen, daß $T: \pi_1 = \tau^{\frac{b_0}{2}} \pi_1$, und durch Induktion beweist man wie in (28), daß

$$\beta_i = 1 + \tau^{a_1} \pi_i^{e_0} + \tau^{a_3} \pi_i^{3 e_0} + \ldots + \tau^{a_{2i+1}} \pi_i^{2^{i+1} e_0},$$

wo, abgesehen vom letzten Gliede, nur ungerade Exponenten vorkommen. $\beta_i$ wird also auch durch $T$ nicht geändert, und man erhält in dieser Weise bei einer passenden Wahl von $T$

$$T: \pi \equiv \tau^{\frac{b_0}{2^s}} \pi \pmod{\mathfrak{P}^a},$$

woraus wie früher die Richtigkeit des Satzes 16 für $p = 2$ folgt. Es sei nebenbei bemerkt, daß die Trägheitsgruppe im Falle $p = 2$ Abelsch wird, und zwar zyklisch, indem die Exponenten $e_0$ und $p^s$ relativ prim sind. Dies ist der einzige Fall, wo die Trägheitsgruppe bei binomischen Kongruenzen Abelsch werden kann.

Zuletzt soll noch die vollständige Zerlegungsgruppe bestimmt werden, und man braucht dafür nur die Konstante $z_0$ in (34) abzuleiten. Nach (34) folgt aber

$$Z^{-f} V Z^f = V^{z_0^f}$$

oder da $Z^f = T^{a_0}$, folgt aus Satz 16

$$T^{-a_0} V T^{a_0} = V^{t_0^{a_0}} = V,$$

indem $a_0$ nach Satz 9 durch $p-1$ teilbar ist. Man hat also

$$z_0^f \equiv 1 \pmod{p^s}.$$

Da aber $z_0 \equiv 1 \pmod{p}$, zeigt man leicht, wenn $f$ nicht durch $p$ teilbar ist, daß $z_0 \equiv 1 \pmod{p^s}$ sein muß. Wenn aber $f$ genau durch $p^{\varphi_0}$ teilbar ist, kann man nur $z_0 \equiv 1 \pmod{p^{s-\varphi_0}}$ schließen.

Satz 17. *Im binomischen Falle $p > 2$ hat die volle Zerlegungsgruppe die Form*

$$G_Z = Z^h T^i V^j \qquad \begin{matrix} (h = 0, 1, \ldots, f-1;\ i = 0, 1, \ldots, e_0 - 1) \\ (j = 0, 1, \ldots, p^s - 1), \end{matrix}$$

*wo*

$$Z^f = T^{a_0}, \quad T^{e_0} = V^{p^s} = 1, \quad Z^{-1} T Z = T^p$$

*und*

$$Z^{-1} V Z = V^{z_0}, \qquad T^{-1} V T = V^{t_0}, \tag{38}$$

*wo $t_0$ eine beliebige primitive Wurzel der Kongruenz $t_0^{p-1} - 1 \equiv 0 \pmod{p^s}$ bezeichnet, und $z_0 \equiv 1 \pmod{p^{s-\varphi_0}}$, wenn $f$ genau durch $p^{\varphi_0}$ teilbar ist. Wenn $f$ nicht durch $p$ teilbar ist, kann man in (38) einfach $z_0 = 1$ setzen.*

Es sei auch erwähnt, daß man wirklich Beispiele angeben kann, wo $z_0$ in (38) nicht gleich 1 ist. Die vollständige Bestimmung von $z_0$ hängt mit der am Ende des § 4 erwähnten größtmöglichen Reduktion der Konstanten $\beta_i$ zusammen, und ich werde bei einer späteren Gelegenheit auf die Lösung dieses Problems zurückkommen.

Ebenso wird es hier zu weit führen, noch den Ergänzungssatz zu Satz 17 für $p = 2$ ausführlich zu beweisen. Es soll nur angegeben werden, daß, wenn in diesem Falle $f$ ungerade ist, die Zerlegungsgruppe genau die Form des Satzes 17 hat, wobei in (38) $z_0 = t_0 = 1$ ist.

(Eingegangen am 21. 12. 1928.)