## Werk

**Titel:** Journal für die reine und angewandte Mathematik
**Verlag:** de Gruyter
**Jahr:** 1937
**Kollektion:** Mathematica
**Digitalisiert:** Niedersächsische Staats- und Universitätsbibliothek Göttingen
**Werk Id:** PPN243919689_0176
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0176

**LOG Id:** LOG_0022
**LOG Titel:** Die Gruppe der pn-primären Zahlen für einen Primteiler ... von p.
**LOG Typ:** article

## Übergeordnetes Werk

**Werk Id:** PPN243919689
**PURL:** http://resolver.sub.uni-goettingen.de/purl?PPN243919689



## Contact

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

# Die Gruppe der $p^n$-primären Zahlen für einen Primteiler $\mathfrak{p}$ von $p$.

Von *Helmut Hasse* in Göttingen.

In meinem Zahlbericht, Teil II, § 9, mußte ich die Frage nach einer Kongruenzcharakterisierung der $p^n$-primären Zahlen für einen Primteiler $\mathfrak{p}$ von $p$ offen lassen. Ich gebe nachstehend eine solche Charakterisierung. Diese stützt sich einerseits auf die Einführung eines erweiterten Potenzbegriffs, der seine Grundlegung in der Strukturtheorie der diskret bewerteten perfekten Körper findet [1]), andrerseits auf die Theorie der zyklischen Erweiterungen vom Grade $p^n$ bei Charakteristik $p$ [2]). Diesen neueren Untersuchungen entsprechend behandle ich die Frage gleich allgemeiner, als es für die Anwendung auf algebraische Zahlkörper erforderlich ist.

## 1.

Sei $l$ ein diskret bewerteter perfekter Körper der Charakteristik 0 mit vollkommenem Restklassenkörper $\mathfrak{k}$ der Primzahlcharakteristik $p$. Nach der angeführten Strukturtheorie ist $l$ eine voll-verzweigte (Eisensteinsche) Erweiterung endlichen Grades eines eindeutig bestimmten perfekten unverzweigten Teilkörpers $k$ mit demselben Restklassenkörper $\mathfrak{k}$.

Zu jedem gegebenen vollkommenen Restklassenkörper $\mathfrak{k}$ der Charakteristik $p$ existiert genau ein diskret bewerteter perfekter unverzweigter Körper $k$ der Charakteristik 0, bestehend aus allen Reihen

$$\alpha = \sum_{\nu=\nu_0}^{\infty} \alpha_\nu p^\nu$$

mit Koeffizienten $\alpha_\nu$ aus einem $\mathfrak{k}$ multiplikationstreu zugeordneten Repräsentantensystem und mit einer durch $\mathfrak{k}$ eindeutig bestimmten Additionsvorschrift. Jeder Automorphismus $S$ von $\mathfrak{k}$ überträgt sich zunächst auf das multiplikationstreue Repräsentantensystem und dann in der Form

$$\alpha^S = \sum_{\nu=\nu_0}^{\infty} \alpha_\nu^S p^\nu$$

[1]) Siehe H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, Journ. f. Math. **170** (1934), 4—63. Eine neue einfachere Begründung dieser Theorie gab kürzlich O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper, Göttinger Nachrichten (Neue Folge) I 1 (1936), 151—161; eine ausführliche Darstellung des hier in Frage kommenden, auf vollkommene Restklassenkörper bezüglichen Teils dieser Arbeit gibt E. Witt in der in diesem Heft, S. 126—140, erscheinenden Arbeit: Zyklische Körper und Algebren der Charakteristik $p$ vom Grad $p^n$. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik $p$, auf die ich mich hier ohne weitere Einzelverweise beziehen werde.

[2]) Siehe schon A. A. Albert, Cyclic fields of degree $p^n$ over $F$ of characteristic $p$, Bull. Amer. Math. Soc. **40** (1934), 625—631; E. Witt, Konstruktion von galoisschen Körpern der Charakteristik $p$ zu vorgegebener Gruppe der Ordnung $p^l$, Journ. f. Math. **174** (1936), 237—245. Eine neue, für den Zweck dieser Arbeit besonders brauchbare Begründung gibt Witt in der unter [1]) genannten Arbeit.

auf $k$. $k$ enthält insbesondere den dem Primkörper $\mathfrak{k}_0$ der Charakteristik $p$ zugeordneten Teilkörper $k_0$ der Charakteristik 0, den Körper der $p$-adischen Zahlen.

Für Einseinheiten, d. h. Elemente aus $l$ der Form $1-\xi$ mit $\xi \equiv 0 \bmod \mathfrak{p}$, wo $\mathfrak{p}$ das Primideal von $l$ bezeichnet, sind in bekannter Weise die Potenzen $(1-\xi)^a$ mit ganzen Exponenten $a$ aus dem $p$-adischen Zahlkörper $k_0$ erklärt, nämlich als

$$(1-\xi)^a = \sum_{\nu=0}^{\infty} (-1)^\nu \binom{a}{\nu} \xi^\nu,$$

und es gelten dafür die Regeln:

$$(1_0) \qquad (1-\xi)^a \equiv 1 - a\xi \bmod \xi^2,$$

$$(2_0) \qquad (1-\xi)^a (1-\xi)^b = (1-\xi)^{a+b},$$

$$(3_0) \qquad ((1-\xi)^a)^b = (1-\xi)^{ab},$$

$$(4_0) \qquad (1-\xi_1)^a (1-\xi_2)^a = ((1-\xi_1)(1-\xi_2))^a.$$

Ich will diesen Potenzbegriff auf ganze Exponenten $\alpha$ aus dem unverzweigten Teilkörper $k$ von $l$ erweitern.

Dazu gehe ich aus von der für $\eta \equiv 0 \bmod \mathfrak{p}$ aus $l$ konvergenten Logarithmusreihe

$$-\log(1-\eta) = \sum_{n=1}^{\infty} \frac{\eta^n}{n}.$$

Diese spalte ich unter Einführung der ebenfalls für $\eta \equiv 0 \bmod \mathfrak{p}$ konvergenten Reihe

$$L(1-\eta) = \sum_{\varrho=0}^{\infty} \frac{\eta^{p^\varrho}}{p^\varrho}$$

folgendermaßen auf:

$$-\log(1-\eta) = \sum_{(m,p)=1} \frac{1}{m} L(1-\eta^m).$$

Durch Umkehrung mittels der Möbiusschen $\mu$-Funktion ergibt sich daraus

$$\begin{aligned} L(1-\eta) &= -\sum_{(m,p)=1} \frac{\mu(m)}{m} \log(1-\eta^m) \\ &= -\sum_{(m,p)=1} \log(1-\eta^m)^{\frac{\mu(m)}{m}} \\ &= -\log \prod_{(m,p)=1} (1-\eta^m)^{\frac{\mu(m)}{m}} \\ &= -\log P(1-\eta), \end{aligned}$$

wo

$$P(1-\eta) = \prod_{(m,p)=1} (1-\eta^m)^{\frac{\mu(m)}{m}}$$

gesetzt ist; dies Produkt konvergiert ebenfalls für $\eta \equiv 0 \bmod \mathfrak{p}$. Es besitzt eine Potenzreihenentwicklung

$$P(1-\eta) = 1 - \eta - c_2\eta^2 - c_3\eta^3 - \cdots$$

mit ganzen $p$-adischen Koeffizienten $c_2, c_3, \ldots$ Daher läßt sich die Beziehung

$$1-\xi = P(1-\eta)$$

im Bereich der $\xi \equiv 0 \bmod \mathfrak{p}$ aus $l$ eindeutig umkehren, und zwar in der Form

$$1-\eta = Q(1-\xi),$$

wo

$$Q(1-\xi) = 1 - \xi - d_2\xi^2 - d_3\xi^3 - \cdots$$

mit ganzen $p$-adischen Koeffizienten $d_2, d_3, \ldots$ ist. Durch die Relationen

$$1 - \xi = P(1-\eta), \quad 1 - \eta = Q(1-\xi)$$

wird also eine umkehrbar eindeutige Abbildung der Gruppe der Einseinheiten von $l$ auf sich geliefert, bei der überdies

$$1 - \xi \equiv 1 - \eta \bmod. (\xi^2 \sim \eta^2)$$

gilt. Dabei ist nach obigem

$$-\log(1-\xi) = L(1-\eta);$$

die Abbildung bewirkt also, daß die Logarithmusreihe

$$-\log(1-\xi) = \sum_{n=1}^{\infty} \frac{\xi^n}{n}$$

in die einfachere Reihe

$$L(1-\eta) = \sum_{\varrho=0}^{\infty} \frac{\eta^{p^\varrho}}{p^\varrho}$$

übergeführt wird [3]).

Ich definiere nun für beliebige $\xi \equiv 0 \bmod. \mathfrak{p}$ aus $l$ und beliebige ganze

$$\alpha = \sum_{\nu=0}^{\infty} \alpha_\nu p^\nu$$

aus $k$ (in ihrer eindeutigen Entwicklung nach multiplikationstreuen Repräsentanten $\alpha_\nu$ von $\mathfrak{k}$ in $k$) die Potenz $(1-\xi)^\alpha$ durch

$$(1-\xi)^\alpha = \prod_{\nu=0}^{\infty} (P(1-\alpha_\nu\eta))^{p^\nu},$$

wo $\eta$ zu $\xi$ aus

$$P(1-\eta) = 1 - \xi, \quad \text{also} \quad Q(1-\xi) = 1 - \eta$$

bestimmt ist. Ich beweise dann die Gültigkeit der folgenden Regeln:

(1) $$(1-\xi)^\alpha \equiv 1 - \alpha\xi \bmod. \xi^2,$$

(2) $$(1-\xi)^\alpha (1-\xi)^\beta = (1-\xi)^{\alpha+\beta},$$

(3) $$((1-\xi)^\alpha)^a = (1-\xi)^{a\alpha} \quad \text{für ganze } a \text{ aus } k_0,$$

sowie das Übereinstimmen des erweiterten Potenzbegriffs mit dem oben angeführten speziellen für ganze $\alpha = a$ aus $k_0$.

Die Gültigkeit von (1) ergibt sich ohne weiteres aus dem oben über die Funktionen $P, Q$ Gesagten. Danach ist nämlich

$$P(1-\alpha_\nu\eta) \equiv 1 - \alpha_\nu\eta \equiv 1 - \alpha_\nu\xi \bmod. \xi^2,$$

also

$$(P(1-\alpha_\nu\eta))^{p^\nu} \equiv (1-\alpha_\nu\xi)^{p^\nu} \equiv 1 - \alpha_\nu p^\nu \xi \bmod. \xi^2$$

(daß dies $\equiv 1 \bmod. \xi^2$ für $\nu \geqq 1$ ist, brauchen wir nicht), und somit in der Tat

$$(1-\xi)^\alpha \equiv \prod_{\nu=0}^{\infty} (1 - \alpha_\nu p^\nu \xi) \equiv 1 - \sum_{\nu=0}^{\infty} \alpha_\nu p^\nu \cdot \xi = 1 - \alpha\xi \bmod. \xi^2.$$

---

[3]) Dieser Formalismus wurde bereits mit Vorteil angewandt in E. Artin und H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der $l^n$-ten Potenzreste im Körper der $l^n$-ten Einheitswurzeln, Abh. Math. Seminar Hamburg 6 (1928), 151f.

Zum Beweise von (2) und (3) zeige ich zunächst die Gleichheit der Logarithmen beider Seiten. Es ist nach obigem

$$\begin{aligned}
-\log((1-\xi)^{\alpha}) &= -\sum_{\nu=0}^{\infty} p^{\nu} \log P(1-\alpha_{\nu}\eta) \\
&= \sum_{\nu=0}^{\infty} p^{\nu} L(1-\alpha_{\nu}\eta) \\
&= \sum_{\nu=0}^{\infty} p^{\nu} \sum_{\varrho=0}^{\infty} \frac{\alpha_{\nu}^{p^{\varrho}} \eta^{p^{\varrho}}}{p^{\varrho}} \\
&= \sum_{\varrho=0}^{\infty} \left( \sum_{\nu=0}^{\infty} \alpha_{\nu}^{p^{\varrho}} p^{\nu} \right) \frac{\eta^{p^{\varrho}}}{p^{\varrho}} \\
&= \sum_{\varrho=0}^{\infty} \frac{\alpha^{P^{\varrho}} \eta^{p^{\varrho}}}{p^{\varrho}},
\end{aligned}$$

wo die

$$\alpha^{P^{\varrho}} = \sum_{\nu=0}^{\infty} \alpha_{\nu}^{p^{\varrho}} p^{\nu}$$

aus

$$\alpha = \sum_{\nu=0}^{\infty} \alpha_{\nu} p^{\nu}$$

durch die oben besprochene Übertragung der Automorphismen $P^{\varrho} = (\mathfrak{k} \to \mathfrak{k}^{p^{\varrho}})$ des Restklassenkörpers $\mathfrak{k}$ auf den Körper $k$ entstehen. Wegen der Automorphieeigenschaft hat man einerseits

$$\alpha^{P^{\varrho}} + \beta^{P^{\varrho}} = (\alpha + \beta)^{P^{\varrho}}$$

und daraus

$$\log((1-\xi)^{\alpha}(1-\xi)^{\beta}) = \log((1-\xi)^{\alpha}) + \log((1-\xi)^{\beta}) = \log((1-\xi)^{\alpha+\beta}),$$

andrerseits, da $k_0$ wie $\mathfrak{k}_0$ bei den $P^{\varrho}$ elementweise festbleibt,

$$a\alpha^{P^{\varrho}} = (a\alpha)^{P^{\varrho}}$$

und daraus

$$\log(((1-\xi)^{\alpha})^{a}) = a \log((1-\xi)^{\alpha}) = \log((1-\xi)^{a\alpha}).$$

Um aus der Gleichheit der Logarithmen in (2) und (3) auf das Bestehen von (2) und (3) selbst zurückzuschließen, fasse man $\xi$ als eine Unbestimmte auf, so daß es sich um Potenzreihen $\sum_{\nu} \gamma_{\nu} \xi^{\nu}$ mit Koeffizienten $\gamma_{\nu}$ aus $k$ handelt. Nennt man eine solche Potenzreihe konvergent, wenn sie bei Einsetzung beliebiger über $k$ algebraischer $\xi$ von positiver $p$-adischer Ordnungszahl $r$ $p$-adisch konvergiert (d. h. wenn $\sum_{\nu} \gamma_{\nu} p^{r\nu}$ für jedes positive rationale $r$ $p$-adisch konvergiert), so sind unsere Formeln und Schlüsse wegen der Willkürlichkeit des Körpers $l$ auch richtig im Sinne dieser allgemeineren Konvergenz. Sind dann $1-\xi_1$, $1-\xi_2$ zwei Einheitspotenzreihen dieser Art, so kann natürlich aus $\log(1-\xi_1) = \log(1-\xi_2)$ auf $\xi_1 = \xi_2$ geschlossen werden. Da die linken und rechten Seiten in (2) und (3) Einheitspotenzreihen in $\xi$ sind, ergibt sich also die Richtigkeit von (2) und (3) für unbestimmte $\xi$; diese Identitäten ergeben dann (2) und (3) für alle $\xi$ positiver $p$-adischer Ordnungszahl aus $l$ durch Einsetzung.

Für ganzes $\alpha = a$ aus $k_0$ wird wegen $a^{p^\varrho} = a$

$$-\log((1-\xi)^\alpha) = a\sum_{\varrho=0}^{\infty}\frac{\eta^{p^\varrho}}{p^\varrho} = aL(1-\eta) = -a\log(1-\xi) = -\log((1-\xi)^a),$$

wo die Potenz links im neu definierten Sinne, rechts im bisherigen Sinne verstanden ist. Daraus folgt ganz analog wie vorher das Übereinstimmen der beiden Potenzen selbst.

Es sei noch bemerkt, daß sich die Regeln $(3_0)$ und $(4_0)$ nicht auch zu entsprechenden Regeln für $((1-\xi)^\alpha)^\beta$ und $(1-\xi_1)^\alpha(1-\xi_2)^\alpha$ verallgemeinern lassen; insbesondere ist schon $((1-\xi)^a)^\alpha$ für ganze $a$ aus $k_0$ im allgemeinen nicht gleich $(1-\xi)^{a\alpha}$, wie nachher noch direkt hervortreten wird. Das macht aber für die beabsichtigte Anwendung nichts aus.

## 2.

Nach der Strukturtheorie der diskret bewerteten perfekten Körper entsprechen sich die

$$\left\{\begin{array}{lll} \text{unverzweigten} & \text{Erweiterungskörper } L & \text{von } l \\ \text{,,} & \text{,,} \quad K & \text{,,} \quad k \\ \text{sämtlichen} & \text{,,} \quad \mathfrak{K} & \text{,,} \quad \mathfrak{k} \end{array}\right\}$$

gegenseitig eindeutig derart, daß

$K$ der größte absolut-unverzweigte Teilkörper von $L$, also $L/K$ voll-verzweigt,

$\mathfrak{K}$ der Restklassenkörper von $K$ und $L$

ist, also analog wie eingangs die Grundkörper $l$, $k$, $\mathfrak{k}$ selbst, und es gilt dabei überdies

$$L = Kl, \quad k = K \cap l,$$

sowie im Falle galoisscher Erweiterungskörper

$$\text{Galoisgruppe } L/l \cong \text{Galoisgruppe } K/k \cong \text{Galoisgruppe } \mathfrak{K}/\mathfrak{k},$$

wobei die erstere Isomorphie durch den Verschiebungssatz der Galoisschen Theorie zustande kommt, die letztere durch die eingangs besprochene Übertragung der Automorphismen des Restklassenkörpers auf den zugehörigen absolut-unverzweigten Körper.

Insbesondere entsprechen sich so gegenseitig eindeutig die

$$\left\{\begin{array}{llll} \text{unverzweigten} & \text{zyklischen} & \text{Erweiterungskörper } L & \text{vom Grade } m \text{ über } l \\ \text{,,} & \text{,,} & \text{,,} \quad K & \text{,,} \quad \text{,,} \quad m \quad \text{,,} \quad k \\ \text{sämtlichen} & \text{,,} & \text{,,} \quad \mathfrak{K} & \text{,,} \quad \text{,,} \quad m \quad \text{,,} \quad \mathfrak{k} \end{array}\right\}.$$

Diese Zuordnung wollen wir im folgenden näher betrachten. Wir setzen dabei voraus, daß $l$ die $m$-ten Einheitswurzeln enthält; eine primitive solche sei mit $\zeta$ bezeichnet. Ferner bezeichne $S$ einen erzeugenden Automorphismus von $L/l$, sowie ohne Mißverständnis gleichzeitig die nach dem eben Gesagten zugeordneten erzeugenden Automorphismen von $K/k$ und $\mathfrak{K}/\mathfrak{k}$.

$L/l$ besitzt eine algebraisch ausgezeichnete Erzeugung, nämlich eine Erzeugung als Kummerscher Körper:

$$L = l(\Theta) \quad \text{mit} \quad \Theta^m = \omega, \qquad \omega \text{ in } l.$$

Dabei liegen $\Theta$, $\omega$ bis auf beliebige Substitutionen

$$\Theta \to \Theta^\varkappa \alpha, \qquad \omega \to \omega^\varkappa \alpha^m \left\{\begin{array}{l} \varkappa \text{ ganz rational, mod. } m, \text{ prim zu } m \\ \alpha \neq 0 \text{ in } l \end{array}\right\}$$

fest. Man kann $\varkappa \equiv 1 \bmod. m$ normieren, indem man bei gegebenen $\zeta, S$ das Automorphieverhalten

$$\Theta^S = \Theta \cdot \zeta$$

fordert. Diese letztere Relation allein legt das Element $\Theta$ innerhalb aller Elemente $\neq 0$ aus $L$ bis auf einen willkürlichen Faktor $\alpha \neq 0$ aus $l$ als eine *bezüglich $\zeta$, $S$ normierte Kummersche Erzeugende von $L/l$* fest. Eine solche kann in bekannter Weise aus einer beliebigen Erzeugenden $\mathsf{A}$ von $K/k$ nach der Methode der Lagrangeschen Resolvente konstruiert werden:

$$\Theta = \sum_{\mu \bmod. m} \zeta^{-\mu} \mathsf{A}^{iS^\mu},$$

wo der Exponent $i$ nur so bestimmt ist, daß $\Theta \neq 0$ ausfällt, was stets für einen der Werte $i = 1, \ldots, m-1$ der Fall ist.

Anstatt durch *eine* Erzeugende $\Theta$ kann man $L/l$ auch invariant durch die multiplikative Gruppe *aller* $\Theta \neq 0$ aus $L$ charakterisieren, für die $\Theta^m = \omega$ in $l$ liegt, oder auch durch die Gruppe der zugehörigen $\omega \neq 0$ aus $l$. Diese Gruppen sind zyklisch von der Ordnung $m$ über der Gruppe der $\alpha \neq 0$ aus $l$ bzw. der Gruppe der $\alpha^m$, und die zuerst beschriebene Erzeugung läuft auf die Auswahl eines Basiselements $\Theta$ bzw. $\omega$ für sie hinaus.

Unsere Fragestellung kann dann folgendermaßen ausgesprochen werden: *Wie hängt diese Kummersche Erzeugung von $L/l$ mit einer entsprechenden arithmetisch ausgezeichneten Erzeugung des Restklassenkörpers $\mathfrak{R}/\mathfrak{k}$ zusammen?*

Die Antwort auf diese Frage fällt naturgemäß ganz verschiedenartig aus, je nachdem welcher der beiden wesentlich zu unterscheidenden Fälle $(m, p) = 1$ oder $m = p^n$ für den Grad $m$ von $L/l$ in seinem Verhältnis zur Charakteristik $p$ von $\mathfrak{k}$ vorliegt. Denn im ersteren Falle besitzt auch $\mathfrak{R}/\mathfrak{k}$ als arithmetisch ausgezeichnete Erzeugung eine solche vom Kummerschen Typus, im letzteren Falle dagegen tritt an deren Stelle eine Erzeugung vom Artin-Schreierschen Typus, in der Albert-Wittschen Verallgemeinerung auf den Grad $p^n$ statt $p$.

Ich behandle zunächst kurz den trivialen Fall $(m, p) = 1$. Hier gehört $\zeta$ als über $k$ unverzweigtes Element aus $l$ bereits zu $k$, und seine Restklasse $z$ ist eine primitive $m$-te Einheitswurzel in $\mathfrak{k}$; umgekehrt folgt übrigens aus dem Vorhandensein einer primitiven $m$-ten Einheitswurzel $z$ in $\mathfrak{k}$ auch, daß der multiplikationstreue Repräsentant $\zeta$ von $z$ in $k$ eine primitive $m$-te Einheitswurzel ist. Ist nun dementsprechend

$$\mathfrak{R} = \mathfrak{k}(t) \quad \text{mit} \quad t^m = w, \quad w \text{ in } \mathfrak{k},$$
$$t^S = t \cdot z$$

eine bezüglich $z$, $S$ normierte Kummersche Erzeugung von $\mathfrak{R}/\mathfrak{k}$, so liefert der Übergang zu den multiplikationstreuen Repräsentanten $\Theta$, $\omega$, $\zeta$ von $t$, $w$, $z$ in $K$, $k$, $k$ ersichtlich eine bezüglich $\zeta$, $S$ normierte Kummersche Erzeugung von $K/k$ und damit auch von $L/l$. Allgemeiner entsteht die $L$ in $l$ zugeordnete Gruppe $\omega$ aus der $\mathfrak{R}$ in $\mathfrak{k}$ zugeordneten Gruppe $w$ einfach, indem man zu den multiplikationstreuen Repräsentanten $\omega$ der $w$ übergeht und noch mit beliebigen $m$-ten Potenzen $\alpha^m$ aus $l$ multipliziert.

Ich komme nunmehr zum eigentlichen Ziel dieser Arbeit, der Behandlung des nicht-trivialen Falles $m = p^n$. Hier besitzt $\mathfrak{R}/\mathfrak{k}$ nach Witt eine arithmetisch ausgezeichnete Erzeugung von folgender Art:

$$\mathfrak{R} = \mathfrak{k}(x_n) \quad \text{mit} \quad x_n^p = x_n + c_n.$$

Dabei sind

$$\mathfrak{c}_n = (c_0, \ldots, c_{n-1}), \qquad \mathfrak{x}_n = (x_0, \ldots, x_{n-1})$$

$n$-gliedrige Vektoren aus $\mathfrak{k}$, $\mathfrak{R}$. Die Addition solcher Vektoren ist nicht etwa komponentenweise erklärt, sondern nach dem von Witt entwickelten besonderen Schema, die Potenzierung mit $p$ dagegen komponentenweise. Die Vektoren $\mathfrak{x}_n$, $\mathfrak{c}_n$ liegen bis auf beliebige Substitutionen

$$\mathfrak{x}_n \to \varkappa \mathfrak{x}_n + \mathfrak{a}_n, \qquad \mathfrak{c}_n \to \varkappa \mathfrak{c}_n + (\mathfrak{a}_n^p - \mathfrak{a}_n) \left\{ \begin{array}{c} \varkappa \text{ ganz rational, mod. } p^n, \text{ prim zu } p \\ \mathfrak{a}_n \text{ } n\text{-gliedriger Vektor in } \mathfrak{k} \end{array} \right\}$$

fest. Man kann $\varkappa \equiv 1$ mod. $p^n$ normieren, indem man bei gegebenem $S$ das Automorphieverhalten

$$\mathfrak{x}_n^S = \mathfrak{x}_n + \mathfrak{e}_n$$

fordert, wo

$$\mathfrak{e}_n = (e, 0, \ldots, 0)$$

mit dem Einselement $e$ von $\mathfrak{k}$ gebildet ist. Diese letztere Relation allein legt den Vektor $\mathfrak{x}_n$ innerhalb aller $n$-gliedrigen Vektoren aus $\mathfrak{R}$ bis auf einen willkürlichen Summanden $\mathfrak{a}_n$ aus $\mathfrak{k}$ als eine *bezüglich $S$ normierte Wittsche Erzeugende von* $\mathfrak{R}/\mathfrak{k}$ fest.

Anstatt durch *einen* erzeugenden Vektor $\mathfrak{x}_n$ kann man $\mathfrak{R}/\mathfrak{k}$ auch invariant durch die additive Gruppe *aller* $n$-gliedrigen Vektoren $\mathfrak{x}_n$ aus $\mathfrak{R}$ charakterisieren, für die $\mathfrak{x}_n^p - \mathfrak{x}_n = \mathfrak{c}_n$ in $\mathfrak{k}$ liegt, oder auch durch die Gruppe der zugehörigen Vektoren $\mathfrak{c}_n$ aus $\mathfrak{k}$. Diese Gruppen sind zyklisch von der Ordnung $p^n$ über der Gruppe der $\mathfrak{a}_n$ aus $\mathfrak{k}$ bzw. der Gruppe der $\mathfrak{a}_n^p - \mathfrak{a}_n$, und die zuerst beschriebene Erzeugung läuft auf die Auswahl eines Basiselements $\mathfrak{x}_n$ bzw. $\mathfrak{c}_n$ für sie hinaus.

Aus einem Grunde, der mit der am Schluß von 1 gemachten Bemerkung zusammenhängt — ich komme darauf unten in Fußnoten 4, 5 zurück —, ist es für unseren Zweck notwendig, diese Wittsche Erzeugung von $\mathfrak{R}/\mathfrak{k}$ noch dadurch zu überbauen, daß man den obigen $n$-gliedrigen Vektor $\mathfrak{c}_n$ aus $\mathfrak{k}$ beliebig zu einem abzählbar unendlichen Vektor

$$\mathfrak{c} = (c_0, \ldots, c_{n-1}, c_n, \ldots)$$

aus $\mathfrak{k}$ auffüllt, sodaß also $\mathfrak{c}_n$ als der $n$-te Abschnitt von $\mathfrak{c}$ erscheint. Durch

$$\overline{\mathfrak{R}} = \mathfrak{k}(\mathfrak{x}) \quad \text{mit} \quad \mathfrak{x}^p = \mathfrak{x} + \mathfrak{c}$$

wird dann ein Turm (d. h. eine Körperfolge, in der jeder Körper die vorhergehenden enthält) über $\mathfrak{k}$ zyklischer Körper der Grade $p, p^2, \ldots$ definiert. Der abzählbar unendliche Vektor

$$\mathfrak{x} = (x_0, \ldots, x_{n-1}, x_n, \ldots)$$

kann dabei zunächst so gewählt werden, daß sein $n$-ter Abschnitt der obige $n$-gliedrige Vektor $\mathfrak{x}_n$ ist; daher ist der $n$-te Abschnitt des Turmes $\overline{\mathfrak{R}}$ der obige Körper $\mathfrak{R}$. Bezeichnet ferner $S$ eine Fortsetzung des obigen Automorphismus $S$ von $\mathfrak{R}/\mathfrak{k}$ auf $\overline{\mathfrak{R}}/\mathfrak{k}$, so können die weiteren Komponenten von $\mathfrak{x}$ noch so normiert werden, daß

$$\mathfrak{x}^S = \mathfrak{x} + \mathfrak{e}$$

gilt, wo

$$\mathfrak{e} = (e, 0, \ldots)$$

ist, daß also $\mathfrak{x}$ eine bezüglich $S$ normierte Wittsche Erzeugende von $\overline{\mathfrak{R}}/\mathfrak{k}$ ist.

Invariant ist $\overline{\mathfrak{R}}/\mathfrak{k}$ charakterisiert durch die Gruppe aller abzählbar unendlichen Vektoren $\mathfrak{x}$ aus $\overline{\mathfrak{R}}$, für die $\mathfrak{x}^p - \mathfrak{x} = \mathfrak{c}$ in $\mathfrak{k}$ liegt, oder auch durch die Gruppe der zuge-

hörigen Vektoren $\boldsymbol{c}$ aus $\mathfrak{k}$. Durch Bildung der $n$-ten Abschnitte entstehen aus diesen Gruppen $\boldsymbol{x}, \boldsymbol{c}$ die obigen $\mathfrak{R}/\mathfrak{k}$ invariant charakterisierenden Gruppen $\boldsymbol{x}_n, \boldsymbol{c}_n$[4]).

Dem Turm $\overline{\mathfrak{R}}/\mathfrak{k}$ mit $n$-tem Abschnitt $\mathfrak{R}$ entsprechen nach der Strukturtheorie umkehrbar eindeutig Türme $\overline{K}/k$ und $\overline{L}/l$ von gleicher Struktur, deren $n$-te Abschnitte die obigen Körper $K$ und $L$ sind. Den Vektoren

$$\boldsymbol{x} = (x_\nu) \quad \text{aus} \quad \overline{\mathfrak{R}},$$
$$\boldsymbol{c} = (c_\nu) \quad \text{aus} \quad \mathfrak{k}$$

entsprechen ferner umkehrbar eindeutig die Elemente

$$\xi = \sum_{\nu=0}^{\infty} \xi_\nu\, p^\nu \quad \text{aus} \quad \overline{K},$$
$$\gamma = \sum_{\nu=0}^{\infty} \gamma_\nu\, p^\nu \quad \text{aus} \quad k$$

nach dem Teichmüller-Wittschen Schema:

$$\xi_\nu = \text{multiplikationstreuer Repräsentant von } x_\nu^{p^{-\nu}} \text{ in } \overline{K}$$
$$\gamma_\nu = \quad \text{,,} \quad \text{,,} \quad \text{,,} \quad c_\nu^{p^{-\nu}} \text{ in } k,$$

und ebenso dem Vektor $\boldsymbol{e} = (e, 0, \ldots)$ aus $\mathfrak{k}$ das Einselement 1 aus $k$. Den Relationen

$$\boldsymbol{x}^p = \boldsymbol{x} + \boldsymbol{c}, \quad \boldsymbol{x}^S = \boldsymbol{x} + \boldsymbol{e}$$

in $\overline{\mathfrak{R}}$ entsprechen die Relationen

$$\xi^P = \xi + \gamma, \quad \xi^S = \xi + 1$$

in $\overline{K}$. Dabei ist $P$ der (schon in **1** eingeführte) Automorphismus von $\overline{K}/k_0$ mit der Wirkung

$$\xi^P = \sum_{\nu=0}^{\infty} \xi_\nu^p\, p^\nu,$$

entstehend durch Übertragung des Automorphismus $\overline{\mathfrak{R}} \to \overline{\mathfrak{R}}^p$ von $\overline{\mathfrak{R}}/\mathfrak{k}_0$ auf $\overline{K}/k_0$ nach dem eingangs besprochenen Schema; $S$ entsteht nach dem gleichen Schema durch Übertragung des Automorphismus $S$ von $\overline{\mathfrak{R}}/\mathfrak{k}$ auf $\overline{K}/k$ und ist eine Fortsetzung des Automorphismus $S$ von $K/k$.

Nun ist $\zeta$ eine Einseinheit aus $l$ und $\xi$ ein ganzes Element aus $\overline{K}$. Daher können wir im Sinne des in **1** eingeführten erweiterten Potenzbegriffs die Potenzen

$$\Theta = \zeta^\xi, \qquad \omega = \zeta^{p^n \xi}$$

bilden; an Stelle der Körper $\mathfrak{k}, k, l$ in **1** sind hier die Körper $\overline{\mathfrak{R}}, \overline{K}, \overline{L}$ zugrunde zu legen, so daß also die Elemente $\Theta, \omega$ jedenfalls in $\overline{L}$ liegen. Nach den Potenzregeln (2), (3) hat man

$$\Theta^S = \zeta^{\xi S} = \zeta^{\xi+1} = \zeta^\xi \cdot \zeta = \Theta \cdot \zeta \text{ [5])},$$
$$\Theta^{p^n} = (\zeta^\xi)^{p^n} = \zeta^{p^n \xi} = \omega.$$

---

[4]) Es sei ausdrücklich bemerkt, daß der speziellen Auffüllung von $\boldsymbol{c}_n$ zu $\boldsymbol{c}$ durch lauter Nullen keineswegs die entsprechende spezielle Auffüllung von $\boldsymbol{x}_n$ zu $\boldsymbol{x}$ entspricht.

[5]) Würde man nur mit den $n$-gliedrigen Vektoren $\boldsymbol{x}_n$, $\boldsymbol{c}_n$, $\boldsymbol{e}_n$ arbeiten, so hätte man nur

$$\xi^P \equiv \xi + 1 \bmod p^n.$$

und daraus kann nicht auf

$$\zeta^{\xi^P} = \zeta^{\xi+1}$$

geschlossen werden, ebenso wie $\zeta^{p^n \xi}$ nach dem Ergebnis des Textes sicher nicht gleich 1 ist, obwohl $\zeta^{p^n} = 1$ ist. Die Potenzregel (3) bleibt eben bei Vertauschung der Rollen von $a$ und $\alpha$ nicht allgemein gültig.

Hiernach liegt $\omega$ in $l$, also $\Theta$ in $L$, und es ist

$$L = l(\Theta),$$

d. h. $\Theta$ ist eine bezüglich $\zeta$, $S$ normierte Kummersche Erzeugung von $L/l$ [6]).

Allgemeiner entnimmt man aus den vorstehenden Ausführungen ohne weiteres: *Die $L$ invariant zugeordneten Gruppen $\Theta$ in $L$ und $\omega$ in $l$ entstehen in der Form*

$$\Theta = \zeta^{\xi}\alpha, \quad \omega = \zeta^{p^n\xi}\alpha^{p^n} \qquad (\alpha \neq 0 \text{ in } l),$$

*wo $\xi$ die additive Gruppe aller ganzen Elemente aus $\overline{K}$ durchläuft, für die*

$$\xi^P = \xi + \gamma$$

*mit ganzem $\gamma$ aus $k$ ist.*

Damit ist der Mechanismus aufgedeckt, nach dem die Kummersche Erzeugung von $L/l$ mit der Wittschen Erzeugung von $\mathfrak{R}/\mathfrak{k}$ zusammenhängt.

## 3.

Ich gehe noch kurz auf den für die Anwendung auf algebraische Zahlkörper in Frage kommenden Spezialfall ein, daß $k$ ein endlicher Körper von $q = p^f$ Elementen ist. Dann gibt es nur einen einzigen Turm $\overline{\mathfrak{R}}$ über $\mathfrak{k}$ zyklischer Körper der Grade $p, p^2, \ldots$, und dementsprechend auch nur je einen einzigen Turm $\overline{K}$ bzw. $\overline{L}$ über $k$ bzw. $l$ zyklischer Körper der Grade $p, p^2, \ldots$. Für $\overline{\mathfrak{R}}$ und $\overline{K}$ kann dabei $S = Q = P^f$ gesetzt werden (Artin-Automorphismus).

Die $L$ zugeordnete Gruppe $\omega$ in $l$ ist dann die Gruppe *aller* $\omega \neq 0$ aus $l$, für die $l(\sqrt[p^n]{\omega})$ unverzweigt über $l$ ist, also die Gruppe der *$p^n$-primären* Elemente aus $l$. Der zuletzt ausgesprochene Satz gibt also eine explizite Bestimmung dieser Gruppe, und zwar mit Hinblick auf die Potenzregel (1) in Form einer Kongruenzcharakterisierung.

Überdies ergibt sich eine explizite Bestimmung des zugehörigen *Artin-Symbols* $\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}$. Dieses ist definiert durch

$$\Theta^Q = \Theta \cdot \left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}, \quad \text{wo } \Theta^{p^n} = \omega.$$

Führt man die gewonnene Potenzdarstellung

$$\Theta = \zeta^{\xi}\alpha \qquad (\alpha \neq 0 \text{ in } l)$$

mit

$$\xi^P = \xi + \gamma, \quad \gamma \text{ ganz in } k,$$

ein, so hat man

$$\xi^Q = \xi^{P^f} = \xi + \gamma + \gamma^P + \cdots + \gamma^{P^{f-1}} = \xi + \mathrm{Sp}\,\gamma,$$

also

$$\Theta^Q = \zeta^{\xi^Q}\alpha = \zeta^{\xi}\alpha \cdot \zeta^{\mathrm{Sp}\,\gamma} = \Theta \cdot \zeta^{\mathrm{Sp}\,\gamma},$$

d. h.

$$\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n} = \zeta^{\mathrm{Sp}\,\gamma}.$$

---

[6]) Den Hinweis auf diese einfache Schlußführung an Stelle meines ursprünglichen komplizierteren Beweises verdanke ich E. Witt.

Wir haben also:

*Ist*

$$\omega = \zeta^{p^n \xi} \alpha^{p^n} \qquad \begin{Bmatrix} \xi \text{ ganz in } \overline{K} \\ \alpha \neq 0 \text{ in } l \end{Bmatrix}$$

*eine $p^n$-primäre Zahl aus $l$ und dabei*

$$\xi^P = \xi + \gamma,$$

*so ist das zugehörige Artin-Symbol durch*

$$\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n} = \zeta^{S\mathfrak{p}\,\gamma}$$

*gegeben.*

Faßt man $l$ als $\mathfrak{p}$-adische Erweiterung eines die $p^n$-ten Einheitswurzeln enthaltenden algebraischen Zahlkörpers $\Lambda$ für einen Primteiler $\mathfrak{p}$ von $p$ auf, so hat man eine Kongruenzcharakterisierung der für $\mathfrak{p}$ $p^n$-primären $\omega$ aus $\Lambda$ und eine darauf gegründete explizite Bestimmung des Artin-Symbols $\left(\frac{\omega}{\mathfrak{p}}\right)_{p^n}$ in $\Lambda$.

---

Eingegangen 7. Mai 1936.