Werk

Titel: Journal für die reine und angewandte Mathematik
Verlag: de Gruyter
Jahr: 1936
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN243919689_0175
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN243919689_0175

LOG Id: LOG_0013
LOG Titel: Zyklische algebraische Funktionenkörper vom Grade pn über endlichem Konstantenkörper der Charakteristik 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

Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p.

Von *Hermann Ludwig Schmid* in Göttingen.

Hasse hat die arithmetische und analytische Theorie der relativ-zyklischen algebraischen Funktionenkörper vom Grade p bei endlichem Konstantenkörper der Charakteristik p entwickelt [1]). Die Ausdehnung dieser Theorie auf beliebigen Grad p^n ($n \geqq 1$) setzt die Verallgemeinerung der Artin-Schreierschen Theorie der zyklischen Erweiterungen p-ten Grades über Körpern der Charakteristik p auf beliebigen Grad p^n voraus [2]). Inzwischen haben nun A. A. Albert und E. Witt den Erzeugungsmechanismus für beliebigen Grad p^n gefunden [3]) [4]). Beide arbeiten durchweg mit einer Zerlegung in n Schritte p-ten Grades.

Ich gebe in dieser Arbeit den Ansatz zu einer arithmetischen Theorie der relativ-zyklischen algebraischen Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p. Die dabei angewandten Methoden und erzielten Ergebnisse zeigen, daß die vorliegende Theorie durchaus nicht durch bloße Iteration der entsprechenden Tatsachen im Falle des Grades p gewonnen werden können. Insbesondere wird ihre Aufstellung erst durch eine Lösung des hier auftretenden Normierungsproblems ermöglicht.

Zusatz bei der Korrektur: Diese Arbeit war Besprechungsgrundlage in einer von E. Witt geleiteten Arbeitsgemeinschaft. Witt fand dabei eine neue Rechenoperation, für welche meine grundlegende Assoziativitätsrelation in eine gewöhnliche Assoziativität übergeht. Mit diesem neuen Kalkül lassen sich meine Resultate formal einfacher schreiben. Witt wird darauf in einer späteren Arbeit selbst zurückkommen.

1. Erzeugungsmechanismus und galoissche Gruppe.

Es sei K ein beliebiger Grundkörper der Charakteristik p. Z_ν sei ein über K zyklischer Körper vom Grade p^ν mit erzeugendem Automorphismus s_ν ($\nu = 1, 2, \ldots$). S_ν bezeichne die Spur von Z_ν nach K. c_ν sei ein festes Hilfselement aus Z_ν mit $S_\nu(c_\nu) = 1$. Der Operator $\wp$ habe die Bedeutung $\wp x = x^p - x$. Δ_ν sei der Operator $s_\nu - 1$. Mit diesen Bezeichnungen lauten die beiden Hauptsätze der Wittschen Erzeugung:

I. Hauptsatz. Enthält der Körper Z_ν den Körper $Z_{\nu-1}$, so besitzt Z_ν über $Z_{\nu-1}$ eine Erzeugung

[1]) H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, Journ. f. Math. 172 (1934). Im folgenden zitiert mit H I.

[2]) Artin-Schreier, Über eine Kennzeichnung der reell abgeschlossenen Körper, Abhandl. Math. Sem. Hamburg 5 (1927).

[3]) A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bulletin A. M. S. 40 (1934).

[4]) E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^l, Journ. f. Math. 174 (1936).

$$Z_\nu = Z_{\nu-1}(v_\nu) \qquad \nu = 2, 3, \ldots \tag{1}$$

mit

$$\wp v_\nu = z_{\nu-1}\,, \tag{2}$$

wo $z_{\nu-1}$ ein Element aus $Z_{\nu-1}$ ist, das der Relation

$$\Delta_{\nu-1} z_{\nu-1} = \wp c_{\nu-1} \tag{3}$$

genügt.

II. Hauptsatz. Für jedes $z_{\nu-1}$, also für jede Lösung der Gleichung (3) in $Z_{\nu-1}$, ist der durch (1), (2) definierte Körper Z_ν ein über K zyklischer Körper vom Grade p^ν, der $Z_{\nu-1}$ enthält. Ein erzeugender Automorphismus ist durch

$$s_\nu = (v_\nu \to v_\nu + c_{\nu-1})$$

gegeben.

Die Gleichung (3) stellt die Verallgemeinerung der für den Fall $n = 2$ von Artin-Schreier angegebenen Differenzengleichung

$$f(v_1 + 1) - f(v_1) = (v_1 + \beta_1)^{p-1} - v_1^{p-1} \tag{4}$$

dar. Dabei ist $\wp v_1 = \beta_1$. Man wähle einfach $c_1 = -v_1^{p-1}$ und $s_1 = (v_1 \to v_1 + 1)$.

Bemerkenswert ist, daß die Gleichung $\Delta z = \wp c$ stets Lösungen z besitzt. Dies besagt, daß sich die Körperkonstruktion unbeschränkt fortsetzen läßt, daß es also unter allen Umständen zyklische Körper beliebig hohen Grades p^n über K gibt, wenn es nur solche vom Grade p gibt.

Die Albertsche Erzeugungsart ergibt sich aus der Wittschen Erzeugung, indem man

$$c_\nu = (-1)^\nu \prod_{i=1}^{\nu} v_i^{p-1} \qquad (\nu = 1, 2, \ldots)$$

setzt [5]). Die in dieser Arbeit gegebene Lösung des Normierungsproblems zeigt, daß die Albertsche Wahl der Größen c_ν für den Aufbau einer arithmetischen Theorie ungeeignet ist. Wir wollen daher im folgenden die viel allgemeinere Wittsche Erzeugungsart verwenden. Wir werden uns die Freiheit in der Wahl der Hilfsgrößen c_ν (die nur der Bedingung $S_\nu(c_\nu) = 1$ genügen müssen) in möglichst vorteilhafter Weise zunutze machen.

Nach Wahl von c_ν ergibt sich z_ν aus der verallgemeinerten Differenzengleichung (3) nur bis auf Konstante (Elemente aus K) eindeutig [6]). z_ν werde im folgenden, dieser Freiheit entsprechend, beliebig, aber festbleibend ausgewählt. Auch über diese Wahl werden wir später noch entscheiden. Die allgemeinste Lösung von (3) ergibt sich dann in der Form $z_\nu + \beta_\nu$ mit β_ν aus K. So erhält man folgende Erzeugung des allgemeinsten Körpers Z_n:

(5)

$Z_1 = K(v_1)$	$\wp v_1 = \beta_1$	$\Delta_1 v_1 = 1$	
$Z_2 = Z_1(v_2)$	$\wp v_2 = z_1 + \beta_2$	$\Delta_2 v_2 = c_1$	$\Delta_1 z_1 = \wp c_1$
$Z_3 = Z_2(v_3)$	$\wp v_3 = z_2 + \beta_3$	$\Delta_3 v_3 = c_2$	$\Delta_2 z_2 = \wp c_2$
. . . . .	. . . . .	. . . . .	. . . . .
$Z_n = Z_{n-1}(v_n)$	$\wp v_n = z_{n-1} + \beta_n$	$\Delta_n v_n = c_{n-1}$	$\Delta_{n-1} z_{n-1} = \wp c_{n-1}$

Z_n ist also durch n Parameter $\beta_1, \beta_2, \ldots, \beta_n$ (Elemente aus K) erzeugbar.

[5]) Man beachte, daß für die Wurzeln einer normierten Gleichung $\wp v = \alpha$ die Spur $S(v^i) = 0$ ist für $0 \leqq i \leqq p-2$, während $S(v^{p-1}) = -1$ ist. Durch Zusammensetzen der Spur S_ν aus Teilspuren erkennt man, daß $S_\nu\left((-1)^\nu \prod_{i=1}^{\nu} v_i^{p-1}\right) = 1$ ist.

[6]) Wir setzen definitorisch $c_0 = 1$ und $z_0 = 0$.

Um in (5) eine echte Erweiterung vom Grade p^n zu erhalten, muß man

$$\beta_1 \neq \wp\beta_0$$

mit β_0 aus K wählen. Die Bedingungen

$$z_\nu + \beta_{\nu+1} \neq \wp z'_\nu$$

mit z'_ν aus Z_ν ($\nu = 1, 2, \ldots, n-1$) sind von selbst erfüllt, da die gegenteilige Annahme auf $S_\nu(c_\nu) = 0$ führen würde im Widerspruch zu $S_\nu(c_\nu) = 1$.

Wird der erzeugende Automorphismus $s_n = (v_n \to v_n + c_{n-1})$ der zyklischen galoisschen Gruppe $\mathfrak{Z}_n$ von Z_ν über K auf Z_ν über K angewandt ($\nu = 1, 2, \ldots, n$), so induziert er gerade den erzeugenden Automorphismus $s_\nu = (v_\nu \to v_\nu + c_{\nu-1})$ der zyklischen galoisschen Gruppe $\mathfrak{Z}_\nu$ von Z_ν über K. Wir können daher im folgenden den Index bei den Automorphismen s und den Operatoren Δ weglassen.

Einem beliebigen Element $s' = s^k$ ($k \bmod p^n$) der Gruppe $\mathfrak{Z}_n$ ordnen wir ein System von n Zahlen

$$(k_0, k_1, \ldots, k_{n-1}) \tag{6}$$

zu, entsprechend der p-adischen Darstellung von k:

$$k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1} + \cdots,$$

wobei die k_ν dem reduzierten Restsystem $0, 1, \ldots, p-1$ entnommen seien. Wir können dann sagen:

Jeder Automorphismus von Z_n über K ist umkehrbar eindeutig durch n Zahlen aus dem Primkörper von K charakterisiert. Die Zuordnung (6) hat folgende Bedeutung: Nach dem Fundamentalsatz der galoisschen Theorie entsprechen den Unterkörpern Z_ν von Z_n umkehrbar eindeutig Untergruppen $\mathfrak{U}_\nu$ von $\mathfrak{Z}_n$. Den Gruppen $\mathfrak{U}_\nu$ sind im Sinne von (6) die Zahlsysteme

$$(0, 0, \ldots, 0, k_\nu, k_{\nu+1}, \ldots, k_{n-1})$$

zugeordnet. Dabei ist $\mathfrak{Z}_n/\mathfrak{U}_\nu \cong \mathfrak{Z}_\nu$ und die Faktorgruppe $\mathfrak{U}_\nu/\mathfrak{U}_{\nu+1}$ isomorph zur galoisschen Gruppe von $Z_{\nu+1}$ über Z_ν. Ein Repräsentantensystem für $\mathfrak{U}_\nu/\mathfrak{U}_{\nu+1}$ im Sinne von (6) wird gerade durch die Koordinate k_ν geliefert.

2. Das Normierungsproblem.

Der Erzeugungsmechanismus (5) kann je nach Wahl der nichtinvarianten Hilfsgrößen c_ν und der sich daraus ergebenden Größen z_ν sehr verschiedenartig ausfallen. Diese Wahl geeignet zu treffen, soll das Normierungsproblem für die Körper Z_n heißen. Dafür muß in erster Linie bestimmend sein, daß sich nach getroffener Wahl die arithmetischen Eigenschaften eines Körpers Z_n einfach beschreiben lassen. Im einzelnen kann man fordern, daß sich die den Körper Z_n erzeugenden Größen z_ν aus (3) formal möglichst einfach ergeben oder daß sich die explizite Berechnung des Artin-Symbols einfach durchführen läßt oder daß die Rechenregeln für das Normenrestsymbol vernünftig lauten.

Wir geben nun anschließend eine Lösung des Normierungsproblems, die die aufgestellten Forderungen weitgehend befriedigt.

Wir setzen c_ν als Polynom von $v_1, v_2, \ldots, v_\nu$ und z_ν als Polynom von $v_1, v_2, \ldots, v_\nu$, $\beta_1, \beta_2, \ldots, \beta_\nu$ mit Koeffizienten aus dem Primkörper von K an:

$$c_\nu = c_\nu(v_1, v_2, \ldots, v_\nu), \qquad z_\nu = z_\nu(v_1, v_2, \ldots, v_\nu; \beta_1, \beta_2, \ldots, \beta_\nu).$$

Die Differenzengleichung (3) kann dann in der Form

$$(7)\quad z_\nu(v_1+1, v_2+c_1, \ldots, v_\nu+c_{\nu-1}; \beta_1, \beta_2, \ldots, \beta_\nu) - z_\nu(v_1, v_2, \ldots, v_\nu; \beta_1, \beta_2, \ldots, \beta_\nu)$$
$$= c_\nu(v_1+\beta_1, v_2+\beta_2+z_1, \ldots, v_\nu+\beta_\nu+z_{\nu-1}) - c_\nu(v_1, v_2, \ldots, v_\nu)$$
$$(\nu = 1, 2, \ldots, n-1)$$

geschrieben werden.

Es ist im folgenden von entscheidender Bedeutung, die Größen $v_1, v_2, \ldots, v_\nu; \beta_1, \beta_2, \ldots, \beta_\nu$ als Unbestimmte aufzufassen und die Gleichung (7) *im Körper der rationalen Zahlen zu lösen.* Wenn dann bei einer solchen Lösung die Koeffizienten von c_ν und z_ν keine unerlaubten (durch p teilbaren) Nenner besitzen, entspringt daraus eine Lösung von (7) im Körper Z_ν, indem man den Unbestimmten wieder die alte Bedeutung zurückgibt. Wir ersetzen formal die v_i durch x_i und die β_i durch y_i $(i = 1, 2, \ldots, \nu)$ und schreiben (7) in der Form

$$(7a)\quad z_\nu(x_1+1, x_2+c_1, \ldots, x_\nu+c_{\nu-1}; y_1, \ldots, y_\nu) - z_\nu(x_1, \ldots, x_\nu; y_1, \ldots, y_\nu)$$
$$= c_\nu(x_1+y_1, x_2+y_2+z_1, \ldots, x_\nu+y_\nu+z_{\nu-1}) - c_\nu(x_1, \ldots, x_\nu).$$

Natürlich sind in den Größen c_i und z_i ebenfalls die obigen Ersetzungen vorzunehmen. Der Koeffizientenbereich sei der Körper der rationalen Zahlen.

Nun sei $f_\nu(x_1, x_2, \ldots, x_\nu)$ ein beliebiges Polynom von $x_1, x_1, \ldots, x_\nu$ mit rationalen Koeffizienten. Wir zeigen dann, daß folgende Paare c_ν und z_ν eine Lösung von (7a) darstellen:

$$(8)\quad \boxed{\begin{aligned} c_\nu(x_1, \ldots, x_\nu) &= f_\nu(x_1+1, x_2+c_1, \ldots, x_\nu+c_{\nu-1}) - f_\nu(x_1, x_2, \ldots, x_\nu) - f_\nu(1, 0, \ldots, 0) \\ z_\nu(x_1, \ldots, x_\nu; y_1, \ldots, y_\nu) &= f_\nu(x_1+y_1, x_2+y_2+z_1, \ldots, x_\nu+y_\nu+z_{\nu-1}) - f_\nu(x_1, x_2, \ldots, x_\nu) \\ &\quad - f_\nu(y_1, y_2, \ldots, y_\nu) \end{aligned}}$$

(8) ist ein rekursives System zur Berechnung von c_ν und z_ν [7]). Wir stellen zunächst einige Eigenschaften dieser Größen fest. Es ist, kurz geschrieben,

$$(9)\qquad c_\nu(0) = 0 \quad \text{und} \quad z_\nu(0; y) = z_\nu(x; 0) = 0.$$

Zwischen c_ν und z_ν besteht der Zusammenhang

$$(10)\qquad c_\nu(x_1, x_2, \ldots, x_\nu) = z_\nu(x_1, x_2, \ldots, x_\nu; 1, 0, 0, \ldots, 0).$$

z_ν ist ein in den Variablen x und y symmetrisches Polynom, d. h. es gilt, kurz geschrieben,

$$(11)\qquad z_\nu(x; y) = z_\nu(y; x).$$

Schließlich genügt z_ν einer additiven Assoziativitätsrelation, die in den Unbestimmten ξ_i, η_i, ζ_i $(i = 1, 2, \ldots, \nu)$ geschrieben so lautet [8]):

$$(12)\quad \begin{aligned} &z_\nu(\xi_1+\eta_1, \xi_2+\eta_2+z_1(\xi_1; \eta_1), \ldots, \xi_\nu+\eta_\nu+z_{\nu-1}(\xi_1, \ldots, \xi_{\nu-1}; \eta_1, \ldots, \eta_{\nu-1}); \zeta_1, \zeta_1, \ldots, \zeta_\nu) \\ &\qquad + z_\nu(\xi_1, \xi_2, \ldots, \xi_\nu; \eta_1, \eta_2, \ldots, \eta_\nu) \\ &= z_\nu(\eta_1+\zeta_1, \eta_2+\zeta_2+z_1(\eta_1; \zeta_1), \ldots, \eta_\nu+\zeta_\nu+z_{\nu-1}(\eta_1, \ldots, \eta_{\nu-1}; \zeta_1, \ldots, \zeta_{\nu-1}); \xi_1, \xi_2, \ldots, \xi_\nu) \\ &\qquad + z_\nu(\eta_1, \eta_2, \ldots, \eta_\nu; \zeta_1, \zeta_2, \ldots, \zeta_\nu). \end{aligned}$$

---

[7]) Der Sinn des Lösungsansatzes (8) ist folgender: Wäre $S_\nu(c_\nu) = 0$, so könnte man wegen der Vertauschbarkeit der Operatoren $\wp$ und Δ Lösungen der Gleichung $\Delta z_\nu = \wp c_\nu$ in der Form $c_\nu = \Delta f_\nu$ und $z_\nu = \wp f_\nu$ mit f_ν aus Z_ν erhalten. Wegen $S_\nu(c_\nu) = 1$ ist dies aber in Z_ν unmöglich. Faßt man aber v_i und β_i als Unbestimmte auf und rechnet im Körper der rationalen Zahlen, so bleibt der Formalismus $\Delta \wp f_\nu = \wp \Delta f_\nu$ erhalten. Daß es über diesen Umweg möglich ist, eine Lösung c_ν, z_ν von (7) in z_ν mit $S_\nu(c_\nu) = 1$ zu bekommen, werden wir sofort sehen. Der Ansatz (8) kann als additives Faktorensystem aufgefaßt werden.

[8]) Die additive Assoziativitätsrelation ist eine Folge der Tatsache, daß z_ν als additives Faktorensystem geschrieben ist.

Setzen wir zur Abkürzung

$$g_\nu(\xi, \eta, \zeta) = z_\nu(\xi_1 + \eta_1, \xi_2 + \eta_2 + z_1(\xi_1; \eta_1), \ldots, \xi_\nu + \eta_\nu + z_{\nu-1}(\xi_1, \ldots, \xi_{\nu-1}; \eta_1, \ldots, \eta_{\nu-1}); \zeta_1, \zeta_2, \ldots, \zeta_\nu),$$

so können wir (12) kurz so schreiben:

$$g_\nu(\xi, \eta, \zeta) + z_\nu(\xi; \eta) = g_\nu(\eta, \zeta, \xi) + z_\nu(\eta; \zeta).$$

Beweis. Wir schreiben z_ν in der Form (8). Dann ersehen wir sofort die Richtigkeit von (12) für $\nu = 1$. Wir nehmen an, (12) sei für $\nu = 1, 2, \ldots, k-1$ schon bewiesen. Soll dann (12) auch für $\nu = k$ gelten, so muß die Richtigkeit folgender Identität gezeigt werden:

$$\begin{aligned}
&f_k(\xi_1+\eta_1+\zeta_1, \xi_2+\eta_2+\zeta_2+z_1(\xi_1;\eta_1)+g_1(\xi,\eta,\zeta), \ldots, \xi_k+\eta_k+\zeta_k+z_{k-1}(\xi_1,\ldots,\xi_{k-1};\eta_1,\ldots,\eta_{k-1})+g_{k-1}(\xi,\eta,\zeta))\\
&-f_k(\xi_1+\eta_1, \xi_2+\eta_2+z_1(\xi_1,\eta_1), \ldots, \xi_k+\eta_k+z_{k-1}(\xi_1,\ldots,\xi_{k-1};\eta_1,\ldots,\eta_{k-1}))-f_k(\zeta_1,\zeta_2,\ldots,\zeta_k)\\
&+f_k(\xi_1+\eta_1, \xi_2+\eta_2+z_1(\xi_1,\eta_1), \ldots, \xi_k+\eta_k+z_{k-1}(\xi_1,\ldots,\xi_{k-1};\eta_1,\ldots,\eta_{k-1}))-f_k(\xi_1,\xi_2,\ldots,\xi_k)-f_k(\eta_1,\eta_2,\ldots,\eta_k)\\
&=f_k(\xi_1+\eta_1+\zeta_1, \xi_2+\eta_2+\zeta_2+z_1(\eta_1;\zeta_1)+g_1(\eta,\zeta,\xi), \ldots, \xi_k+\eta_k+\zeta_k+z_{k-1}(\eta_1,\ldots,\eta_{k-1};\zeta_1,\ldots,\zeta_{k-1})+g_{k-1}(\eta,\zeta,\xi))\\
&-f_k(\eta_1+\zeta_1, \eta_2+\zeta_2+z_1(\eta_1;\zeta_1), \ldots, \eta_k+\zeta_k+z_{k-1}(\eta_1,\ldots,\eta_{k-1};\zeta_1,\ldots,\zeta_{k-1}))-f_k(\xi_1,\xi_2,\ldots,\xi_k)\\
&+f_k(\eta_1+\zeta_1, \eta_2+\zeta_2+z_1(\eta_1;\zeta_1), \ldots, \eta_k+\zeta_k+z_{k-1}(\eta_1,\ldots,\eta_{k-1};\zeta_1,\ldots,\zeta_{k-1}))-f_k(\eta_1,\eta_2,\ldots,\eta_k))-f_k(\zeta_1,\zeta_2,\ldots,\zeta_k).
\end{aligned}$$

Nach Wegheben der gleichen Glieder bleibt noch zu beweisen:

$$f_k(\xi_1+\eta_1+\zeta_1, \xi_2+\eta_2+\zeta_2+z_1(\xi_1;\eta_1)+g_1(\xi,\eta,\zeta),\ldots) = f_k(\xi_1+\eta_1+\zeta_1, \xi_2+\eta_2+\zeta_2+z_1(\eta_1;\zeta_1)+g_1(\eta,\zeta,\xi),\ldots).$$

Dies ist aber nach Induktionsannahme eine koordinatenweise Identität. Damit ist die Assoziativitätsrelation bewiesen.

Ersetzen wir in (12) die η_i durch x_i und die ξ_i durch y_i $(i = 1, 2, \ldots, \nu)$, ζ_1 durch 1, die übrigen ζ_i durch 0, so geht unter Beachtung von (10) und (11) die Assoziativitätsrelation (12) direkt in die Identität (7a) über. Damit ist unsere Behauptung, daß die in (8) definierten Größen c_ν und z_ν eine Lösung von (7a) darstellen, bewiesen.

Wir werden nun eine Lösung von (7) in der Form (8) bekommen, wenn Polynome f_ν so existieren, daß in (8) c_ν und z_ν lauter mod p ganze Koeffizienten erhalten. Wir geben mit den Polynomen

$$f_\nu(x_1, x_2, \ldots, x_\nu) = -\left(\frac{x_\nu^p}{p} + \frac{x_{\nu-1}^{p^2}}{p^2} + \cdots + \frac{x_1^{p^\nu}}{p^\nu}\right) \tag{13}$$

für diese Frage einen Existenzbeweis. Dazu brauchen wir folgenden

Hilfssatz. *$P(x_1, x_2, \ldots, x_n)$ sei ein Polynom in den n Unbestimmten $x_1, x_2, \ldots, x_n$ mit ganz-rationalen Koeffizienten. Dann gilt für jede natürliche Zahl $k \geqq 1$ die Polynomkongruenz*

$$P(x_1, x_2, \ldots, x_n)^{p^k} - P(x_1^p, x_2^p, \ldots, x_n^p)^{p^{k-1}} \equiv 0 \bmod p^k. \tag{14}$$

Beweis. (14) ist für $k = 1$ richtig. Allgemein beweisen wir die Gültigkeit von (14) durch Induktion nach k unter Berücksichtigung des auch für Polynome A, B von mehreren Variablen mit ganz-rationalen Koeffizienten gültigen Satzes aus der Zahlentheorie: Aus

$$A \equiv B \bmod p^k.$$

folgt

$$A^p \equiv B^p \bmod p^{k+1}.$$

Wir setzen einfach $A = P(x_1, x_2, \ldots, x_n)^{p^k}$ und $B = P(x_1^p, x_2^p, \ldots, x_n^p)^{p^{k-1}}$.

Dieser Hilfssatz wird uns leicht den angekündigten Existenzbeweis liefern. Wir

behaupten also, daß

$$-c_\nu = \frac{(x_\nu + c_{\nu-1})^p - x_\nu^p}{p} + \frac{(x_{\nu-1} + c_{\nu-2})^{p^2} - x_{\nu-1}^{p^2}}{p^2} + \cdots + \frac{(x_1+1)^{p^\nu} - x_1^{p^\nu} - 1}{p^\nu}$$

(15) und

$$-z_\nu = \frac{(x_\nu + y_\nu + z_{\nu-1})^p - x_\nu^p - y_\nu^p}{p} + \frac{(x_{\nu-1} + y_{\nu-1} + z_{\nu-2})^{p^2} - x_{\nu-1}^{p^2} - y_{\nu-1}^{p^2}}{p^2} + \cdots + \frac{(x_1+y_1)^{p^\nu} - x_1^{p^\nu} - y_1^{p^\nu}}{p^\nu}$$

$$(\nu = 1, 2, \ldots)$$

Polynome mit ganz-rationalen Koeffizienten sind. Wegen (10) genügt es, diese Behauptung für z_ν nachzuweisen.

Für $\nu = 1$ ist die Behauptung richtig. Wir nehmen an, wir hätten z_ν für $\nu = 1, 2, \ldots, k$ schon als Polynom mit ganz-rationalen Koeffizienten erkannt, und wollen die gleiche Eigenschaft für z_{k+1} nachweisen. Wir führen ein Äquivalenzzeichen „$\sim$" mit folgender Bedeutung ein: Für zwei Polynome g und h soll $g \sim h$ bedeuten, daß $g - h$ ein Polynom mit ganz-rationalen Koeffizienten ist. Dann gilt einerseits

$$-z_{k+1} = \frac{(x_{k+1} + y_{k+1} + z_k)^p - x_{k+1}^p - y_{k+1}^p}{p} + \cdots$$

$$\sim \frac{z_k^p}{p} + \frac{(x_k + y_k + z_{k-1})^{p^2} - x_k^{p^2} - y_k^{p^2}}{p^2} + \cdots + \frac{(x_1+y_1)^{p^{k+1}} - x_1^{p^{k+1}} - y_1^{p^{k+1}}}{p^{k+1}}.$$

Andererseits ist nach der Induktionsannahme

$$-\frac{z_k^p}{p} \sim \frac{1}{p} z_k(x_1^p, x_2^p, \ldots, x_k^p;\ y_1^p, y_2^p, \ldots, y_k^p)$$

$$\sim \frac{1}{p}\left[\frac{(x_k^p + y_k^p + z_{k-1}(x_1^p, \ldots, x_{k-1}^p; y_1^p, \ldots, y_{k-1}^p))^p - x_k^{p^2} - y_k^{p^2}}{p} + \cdots + \frac{(x_1^p + y_1^p)^{p^k} - x_1^{p^{k+1}} - y_1^{p^{k+1}}}{p^k}\right].$$

Wir werden also $z_{k+1} \sim 0$ nachgewiesen haben, wenn wir die Richtigkeit folgender Äquivalenzbeziehung gezeigt haben:

$$\frac{(x_k + y_k + z_{k-1})^{p^2}}{p^2} + \frac{(x_{k-1} + y_{k-1} + z_{k-2})^{p^3}}{p^3} + \cdots + \frac{(x_1+y_1)^{p^{k+1}}}{p^{k+1}}$$

$$\sim \frac{(x_k^p + y_k^p + z_{k-1}(x_1^p, \ldots, x_{k-1}^p; y_1^p, \ldots, y_{k-1}^p))^p}{p^2}$$

$$+ \frac{(x_{k-1}^p + y_{k-1}^p + z_{k-2}(x_1^p, \ldots, x_{k-2}^p; y_1^p, \ldots, y_{k-2}^p))^{p^2}}{p^3} + \cdots + \frac{(x_1^p + y_1^p)^{p^k}}{p^{k+1}}.$$

Diese Äquivalenzbeziehung ist aber nach unserem Hilfssatz gliedweise erfüllt. Also ist auch z_{k+1} ein Polynom mit ganz-rationalen Koeffizienten.

Wir haben jetzt bewiesen, daß die Elemente

(16)
$$c_\nu = -\frac{(v_\nu + c_{\nu-1})^p - v_\nu^p}{p} - \frac{(v_{\nu-1} + c_{\nu-2})^{p^2} - v_{\nu-1}^{p^2}}{p^2} - \cdots - \frac{(v_1+1)^{p^\nu} - v_1^{p^\nu} - 1}{p^\nu},$$

$$z_\nu = -\frac{(v_\nu + \beta_\nu + z_{\nu-1})^p - v_\nu^p - \beta_\nu^p}{p} - \frac{(v_{\nu-1} + \beta_{\nu-1} + z_{\nu-2})^{p^2} - v_{\nu-1}^{p^2} - \beta_{\nu-1}^{p^2}}{p^2} - \cdots - \frac{(v_1+\beta_1)^{p^\nu} - v_1^{p^\nu} - \beta_1^{p^\nu}}{p^\nu}$$

Lösungen der Differenzengleichung (7) im Körper Z_ν sind. Die p-Potenzen im Nenner stehen dabei nur formal da. Um die Brauchbarkeit der Elemente c_ν und z_ν aus (16) für den Erzeugungsmechanismus (5) zu zeigen, ist es nur noch notwendig, $S_\nu(c_\nu) = 1$ nachzuweisen. $S_1(c_1) = 1$ ist evident. Wegen

$$-c_\nu = \frac{(v_\nu + c_{\nu-1})^p - v_\nu^p}{p} + \cdots = v_\nu^{p-1} c_{\nu-1} + \cdots$$

folgt $S_\nu(c_\nu) = -S_\nu(v_\nu^{p-1} c_{\nu-1}) = S_{\nu-1}(c_{\nu-1}) = 1$ durch Induktion.

Nach diesem Existenzsatz hat es einen Sinn, das Normierungsproblem in folgender Weise zu entscheiden:

Für den Erzeugungsmechanismus (5) *sollen nur solche* c_ν *(mit* $S_\nu(c_\nu) = 1$*) und* z_ν *Verwendung finden, die sich in der Form* (8) *darstellen lassen.* c_ν und z_ν seien im folgenden in diesem Sinne beliebig, aber festbleibend ausgewählt. Durch diese Entscheidung ist auch die noch willkürliche additive Konstante in z_ν festgelegt. c_ν und z_ν besitzen die Eigenschaften (9) bis (12).

Mit dieser Normierung wird sich die Theorie des Artin- und des Normenrestsymbols einfach darstellen lassen.

Wird im folgenden mit den Elementen c_ν und z_ν in der Form (8) gerechnet, so müssen natürlich die v_i und β_i $(i = 1, 2, \ldots, \nu)$ wieder als Unbestimmte aufgefaßt und es muß im Körper der rationalen Zahlen gerechnet werden, ohne daß dies dann jedesmal wieder vermerkt wird.

Da für die Erzeugung eines Körpers Z_2 besonders einfache Verhältnisse vorliegen, wollen wir über diesen Fall noch die folgenden Einzelheiten anfügen.

Der Lösungsansatz (8) lautet für $\nu = 1$:

$$c_1(x_1) = f_1(x_1 + 1) - f_1(x_1) - f_1(1),$$
$$z_1(x_1; y_1) = f_1(x_1 + y_1) - f_1(x_1) - f_1(y_1).$$

Der Existenzbeweis wurde mit $f_1 = \frac{x_1^p}{p}$ geführt. Damit ergibt sich:

$$-c_1 = \frac{(x_1 + 1)^p - x_1^p - 1}{p} = \sum_{\mu=1}^{p-1} \frac{1}{p}\binom{p}{\mu} x_1^\mu$$

und

$$-z_1 = \frac{(x_1 + y_1)^p - x_1^p - y_1^p}{p} = \sum_{\mu=1}^{p-1} \frac{1}{p}\binom{p}{\mu} x_1^\mu y^{p-\mu}$$

Wegen $-\frac{1}{p}\binom{p}{\mu} \equiv \frac{(-1)^\mu}{\mu} \bmod p$ sehen wir, daß die Normierung der Erzeugung eines Körpers Z_2 mit folgenden abbrechenden Logarithmusreihen vorgenommen werden kann:

$$c_1(v_1) = \sum_{\mu=1}^{p-1} \frac{(-1)^\mu}{\mu} v_1^\mu \quad \text{und} \quad z_1(v_1, \beta_1) = \beta_1^p \sum_{\mu=1}^{p-1} \frac{(-1)^\mu}{\mu} \left(\frac{v_1}{\beta_1}\right)^\mu.$$

Wir können für f_1 auch $\binom{x_1}{p}$ setzen. Damit ergibt sich

$$c_1 = \binom{x_1 + 1}{p} - \binom{x_1}{p} = \binom{x_1}{p-1} \quad \text{und} \quad z_1 = \binom{x_1 + y_1}{p} - \binom{x_1}{p} - \binom{y_1}{p} = \sum_{\mu=1}^{p-1} \binom{x_1}{\mu}\binom{y_1}{p-\mu}.$$

Mit $c_1(v_1) = \binom{v_1}{p-1}$ ist also $z_1(v_1, \beta_1) = \sum_{\mu=1}^{p-1} \binom{v_1}{\mu}\binom{\beta_1}{p-\mu}$ eine Lösung der Differenzengleichung [9]).

Wegen $\binom{v_1}{p-1} = 1 - (v_1 + 1)^{p-1}$ ergibt sich hieraus eine Lösung der Artin-

[9]) Diese Lösung hat O. Teichmüller angegeben.

Schreierschen Differenzengleichung, indem man v_1 durch $v_1 - 1$ ersetzt. Es ist also

$$f = -\sum_{\mu=1}^{p-1} \binom{v_1 - 1}{\mu} \binom{\beta_1}{p - \mu}$$

eine Lösung von (4).

Die Assoziativitätsrelation bekommt für $\nu = 1$ die einfache Gestalt:

$$z_1(\xi, \eta) + z_1(\xi + \eta, \zeta) = z_1(\eta, \zeta) + z_1(\eta + \zeta, \xi).$$

3. Zerlegungs- und Verzweigungstheorie.

Jetzt setzen wir K als algebraischen Funktionenkörper einer Unbestimmten über endlichem Konstantenkörper mit $q = p^l$ Elementen voraus. $\mathfrak{p}$ sei ein Primdivisor von K vom Grade m.

Der Körper Z_n sei durch (5) mit der durch uns getroffenen Normierung erzeugt. Die Elemente $\beta_1, \beta_2, \ldots, \beta_n$ seien durch zulässige Substitutionen

$$v_\nu \to v_\nu + \beta_\nu^{(0)} \qquad (\nu = 1, 2, \ldots, n)$$

mit $\beta_\nu^{(0)}$ aus K auf die Form

$$(17) \quad \beta_\nu \cong \frac{\mathfrak{g}_\nu}{\mathfrak{p}^{\lambda_\nu}} \qquad \left(\lambda_\nu \geqq 0; \quad \begin{array}{l} (\lambda_\nu, p) = 1 \text{ und } \mathfrak{g}_\nu \text{ prim zu } \mathfrak{p}, \text{ falls } \lambda_\nu > 0; \\ \mathfrak{g}_\nu \text{ ganz für } \mathfrak{p}, \text{ falls } \lambda_\nu = 0. \end{array}\right)$$

gebracht [10]). Da z_ν nach (8) ein Polynom in den x und y mit Koeffizienten aus dem Primkörper von K ist, können wir sofort feststellen:

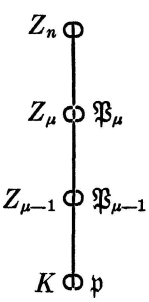
Der Primdivisor $\mathfrak{p}$ bleibt dann und nur dann im Körper Z_n unverzweigt, wenn

$$\lambda_1 = 0, \quad \lambda_2 = 0, \ldots, \lambda_n = 0$$

ist. Eine Verzweigung von $\mathfrak{p}$ in Z_n tritt also dann und nur dann ein, wenn von den in (17) erklärten Exponenten mindestens ein $\lambda_\nu > 0$ ist. Und zwar gilt genauer:

Ist in der Reihe $\lambda_1, \lambda_2, \ldots, \lambda_n$ der erste von Null verschiedene (also positive) Exponent λ_μ, so tritt eine Verzweigung nicht nur beim Übergang von $Z_{\mu-1}$ nach Z_μ, sondern auch bei allen folgenden Schritten von Z_ν nach $Z_{\nu+1}$ $(\nu = \mu, \mu + 1, \ldots, n)$ ein.

Dies ergibt sich sofort aus der Hilbertschen Theorie und aus der eindeutigen Bestimmtheit der Unterkörper Z_ν von Z_n. Es sei $\mathfrak{p} = \Pi \mathfrak{P}_{\mu-1}$, $\mathfrak{P}_{\mu-1} = \mathfrak{P}_\mu^p$ (siehe Figur!). Dann ist der Trägheitskörper von $\mathfrak{p}$ für Z_n über K gleich $Z_{\mu-1}$, der Trägheitskörper von $\mathfrak{P}_\mu$ für Z_n über Z_μ daher gleich dem Kompositum $Z_{\mu-1} \times Z_\mu = Z_\mu$. Daraus folgt, daß $\mathfrak{P}_\mu$ beim Übergang von Z_μ nach $Z_{\mu+1}$ verzweigt ist, w. z. b. w.



Ist insbesondere also schon $\lambda_1 > 0$, so tritt Vollverzweigung $\mathfrak{p} = \mathfrak{P}^{p^n}$ ein. Daraus folgt sofort ohne Rechnung der kürzlich von Tannaka bewiesene Satz [11]):

Es gibt unendlich viele Körper Z_n, in welchen endlich viele vorgegebene Primdivisoren $\mathfrak{p}_j$ voll verzweigt sind. (Analogon zum Grunwaldschen Existenztheorem).

Man braucht nur β_1 so zu wählen, daß für die endlich vielen Primdivisoren $\mathfrak{p}_j$ die Exponenten $\lambda_1^{(j)} > 0$ werden. Dies ist aber stets möglich.

Eine zur Verzweigungstheorie analoge Tatsache können wir auch im unverzweigten Falle feststellen:

---

[10]) Siehe H I.

[11]) T. Tannaka, Zyklische Zerfällungskörper der einfachen Ringe über dem algebraischen Funktionenkörper, Sci. Rep. Tohoku Univ. (1) **24** (1935).

Tritt beim Übergang von $Z_{\mu-1}$ nach Z_μ zum ersten Male Trägheit ein ($\mathfrak{P}_{\mu-1} = \mathfrak{P}_\mu$), so gilt dies auch für alle folgenden Schritte, soweit sie überhaupt unverzweigt sind.

Zum Beweis braucht man nur im vorigen Beweis den Begriff „Trägheitskörper" durch „Zerlegungskörper" zu ersetzen.

Durch diese Feststellungen werden die zunächst denkbaren 3^n Möglichkeiten für die Zerlegung von $\mathfrak{p}$ in Z_n auf $\binom{n+2}{2}$ Möglichkeiten reduziert. Man beherrscht hiernach die Zerlegungstheorie vollkommen, wenn man noch die Frage entscheiden kann, ob im unverzweigten Falle $\mathfrak{p}$ in Z_n voll zerlegt ist oder nicht. Eine Antwort hierauf geben wir mit Hilfe der im folgenden zu entwickelnden Theorie des Artin-Symbols.

4. Das Artin-Symbol.

Der Primdivisor $\mathfrak{p}$ sei im Körper Z_n unverzweigt. In diesem Falle können wir den Artin-Automorphismus

$$F = \left(\frac{Z_n}{\mathfrak{p}}\right) = s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\}}$$

einführen. Für ihn gilt

$$z^F \equiv z^{\mathfrak{N}\mathfrak{p}} \bmod \mathfrak{p}$$

für alle für $\mathfrak{p}$ ganzen z aus Z_n.

Diesem Automorphismus sind vermöge (6) umkehrbar eindeutig n Elemente des Primkörpers von K

$$\left[\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right]_\nu \qquad (\nu = 1, 2, \ldots, n) \tag{18}$$

zugeordnet, die der Beziehung

$$\left\{\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\} = \sum_{\nu=0}^{n-1} \left[\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right]_\nu p^{\nu-1} \tag{19}$$

genügen. Der Verschiebungssatz für das Artin-Symbol, angewandt auf Z_ν über K ($\nu = 1, 2, \ldots, n-1$), ergibt sofort

$$\left[\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right]_\nu = \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right]_\nu.$$

Die Reihe (18) können wir also abändern in

$$\left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right],$$

wobei wir ohne Mißverständnis die Klammerindizes weglassen können. (19) schreibt sich jetzt in der Form

$$\left\{\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\} = \sum_{\nu=1}^{n} \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] p^{\nu-1}.$$

Insbesondere ist

$$\left\{\frac{\beta_1}{\mathfrak{p}}\right\} = \left[\frac{\beta_1}{\mathfrak{p}}\right] \equiv \frac{P^{fm} - 1}{P - 1} \beta_1 \bmod \mathfrak{p}$$ [12])

[12]) P bedeutet den Operator $Px = x^p$.

das in HI eingeführte Symbol und

$$\left\{\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right\} = \left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\} + \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] p^{\nu-1}. \tag{20}$$

Die eckigen Klammersymbole können wir nun rekursiv berechnen. Es gilt unter Berücksichtigung von $\Delta v_\nu = c_{\nu-1}$, von (20) und von

$$S_\nu(c) = \frac{s^{p^\nu} - 1}{s - 1} c_\nu = 1$$

die Beziehung

$$\begin{aligned}
\left(s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right\}} - 1\right) v_\nu &= \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1} \\
&= \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\} + \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] p^{\nu-1}} - 1}{s - 1} c_{\nu-1} \\
&= \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1} + s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} \frac{s^{\left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] p^{\nu-1}} - 1}{s - 1} c_{\nu-1} \\
&= \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1} + \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} \cdot \frac{s^{p^{\nu-1}} - 1}{s - 1} c_{\nu-1} \\
&= \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1} + \left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right].
\end{aligned}$$

Nun ist

$$\left(s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right\}} - 1\right) v_\nu \equiv v_\nu^{\mathfrak{P}\mathfrak{p}} - v_\nu \equiv \frac{P^{fm} - 1}{P - 1} z_{\nu-1} + \left\{\frac{\beta_\nu}{\mathfrak{p}}\right\} \bmod \mathfrak{p}.$$

Also ergibt sich folgende Rekursionsformel [13]):

$$\boxed{\left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] \equiv \left\{\frac{\beta_\nu}{\mathfrak{p}}\right\} + \frac{P^{fm} - 1}{P - 1} z_{\nu-1} - \frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1} \bmod \mathfrak{p}.} \tag{21}$$

Soweit gilt alles für beliebige Normierung. Jetzt wollen wir unsere spezielle Normierung benutzen und die Rekursionsformel (21) weiter auswerten.

Wird die rechte Seite von (21) explizit ausgerechnet und dabei jedes v auf einen Grad kleiner als p reduziert (wie dies nach dem Erzeugungsmechanismus (5) stets möglich ist), so müssen sich natürlich alle Glieder mit v aus Invarianzgründen wegheben. Führen wir die Bezeichnungen

$$\left(\frac{P^{fm} - 1}{P - 1} z_{\nu-1}\right)_{v=0} = \zeta_{\nu-1} \quad \text{und} \quad \left(\frac{s^{\left\{\frac{\beta_1, \beta_2, \ldots, \beta_{\nu-1}}{\mathfrak{p}}\right\}} - 1}{s - 1} c_{\nu-1}\right)_{v=0} = \gamma_{\nu-1}$$

ein, wobei also das Nullsetzen erst nach Gradreduktion vorgenommen werden darf, so können wir (21) so schreiben:

$$\left[\frac{\beta_1, \beta_2, \ldots, \beta_\nu}{\mathfrak{p}}\right] \equiv \left\{\frac{\beta_\nu}{\mathfrak{p}}\right\} + \zeta_{\nu-1} - \gamma_{\nu-1} \bmod \mathfrak{p}. \tag{21a}$$

Es entsteht nun das Problem, die rechte Seite von (21a) einfacher zu gestalten und zwar

[13]) Witt hat unabhängig von dieser Arbeit ebenfalls die Möglichkeit dieser Rekursion erkannt.

so, daß mod $\mathfrak{p}$ ihre Zugehörigkeit zum Primkörper von K evident wird. Wir beschränken uns auf die Vereinfachung des Gliedes $\zeta_{\nu-1}$, da $\gamma_{\nu-1}$ bei der Charakterisierung des Vollzerfallens, auf die es uns nachher ankommt, ersichtlich Null wird. Es gilt

$$\begin{aligned}\zeta_{\nu-1} &= \sum_{k=0}^{fm-1} z_{\nu-1}(v_1^{p^k}, v_2^{p^k}, \ldots, v_{\nu-1}^{p^k}; \beta_1^{p^k}, \beta_2^{p^k}, \ldots, \beta_{\nu-1}^{p^k})_{v=0} \\ &= \sum_{k=0}^{fm-1} f_{\nu-1}(v_1^{p^k} + \beta_1^{p^k}, \ldots, v_{\nu-1}^{p^k} + \beta_{\nu-1}^{p^k} + z_{\nu-2}(v_1^{p^k}, \ldots, v_{\nu-2}^{p^k}; \beta_1^{p^k}, \ldots, \beta_{\nu-2}^{p^k}))_{v=0} \\ &\quad - \sum_{k=0}^{fm-1} f_{\nu-1}(v_1^{p^k}, v_2^{p^k}, \ldots, v_{\nu-1}^{p^k})_{v=0} - \sum_{k=0}^{fm-1} f_{\nu-1}(\beta_1^{p^k}, \beta_2^{p^k}, \ldots, \beta_{\nu-1}^{p^k}).\end{aligned}$$

Man sieht durch Induktion sofort, daß

$$\left[v_i^{p^{k-1}} + \beta_i^{p^{k-1}} + z_{i-1}(v_1^{p^{k-1}}, \ldots, v_{i-1}^{p^{k-1}}; \beta_1^{p^{k-1}}, \ldots, \beta_{i-1}^{p^{k-1}})\right]_{v=0} = (v_i^{p^k})_{v=0}$$
$$(i = 1, 2, \ldots, \nu - 1).$$

Also ergibt sich

$$\begin{aligned}\zeta_{\nu-1} = f_{\nu-1}(v_1^{p^{fm-1}} + \beta_1^{p^{fm-1}}, \ldots, v_{\nu-1}^{p^{fm-1}} + \beta_{\nu-1}^{p^{fm-1}} + z_{\nu-2}(v_1^{p^{fm-1}}, \ldots; \beta_1^{p^{fm-1}}, \ldots))_{v=0} \\ - \sum_{k=0}^{fm-1} f_{\nu-1}(\beta_1^{p^k}, \ldots, \beta_{\nu-1}^{p^k}).\end{aligned}$$

Nun ist

$$\begin{aligned}&\left[v_i^{p^{fm-1}} + \beta_i^{p^{fm-1}} + z_{i-1}(v_1^{p^{fm-1}}, \ldots, v_{i-1}^{p^{fm-1}}; \beta_1^{p^{fm-1}}, \ldots, \beta_{i-1}^{p^{fm-1}})\right]_{v=0} \\ &\qquad = \frac{P^{fm} - 1}{P - 1}\beta_i + \sum_{k=0}^{fm-1} z_{i-1}(v_1^{p^k}, \ldots, v_{i-1}^{p^k}; \beta_1^{p^k}, \ldots, \beta_{i-1}^{p^k})_{v=0} \\ &\qquad = \frac{P^{fm} - 1}{P - 1}\beta_i + \zeta_{i-1} \qquad (i = 1, 2, \ldots;\ \zeta_0 = 0).\end{aligned}$$

Setzen wir dies in $\zeta_{\nu-1}$ ein, so erhalten wir

$$\boxed{\zeta_\nu = f_\nu\left(\frac{P^{fm} - 1}{P - 1}\beta_1, \frac{P^{fm} - 1}{P - 1}\beta_2 + \zeta_1, \ldots, \frac{P^{fm} - 1}{P - 1}\beta_\nu + \zeta_{\nu-1}\right) - \sum_{k=0}^{fm-1} f_\nu(\beta_1^{p^k}, \beta_2^{p^k}, \ldots, \beta_\nu^{p^k}).} \tag{22}$$

Beachten wir, daß die Konjugierten von β_i mod $\mathfrak{p}$

$$\beta_i, \beta_i^p, \beta_i^{p^2}, \ldots, \beta_i^{p^{fm-1}}$$

sind, so erkennen wir rekursiv aus (22), daß ζ_ν ein für jedes i in den Konjugierten von β_i symmetrischer Ausdruck ist, der demnach mod $\mathfrak{p}$ im Primkörper liegen muß.

Die notwendige und hinreichende Bedingung für das Vollzerlegtsein eines Primdivisors $\mathfrak{p}$ von K in Z_n lautet jetzt nach (21a) und (22) so:

$$\left\{\frac{\beta_\nu}{\mathfrak{p}}\right\} + \zeta_{\nu-1} \equiv 0 \bmod \mathfrak{p} \qquad (\nu = 1, 2, \ldots, n).$$

Dies sind n nur von den β_i abhängige Kongruenzen.

5. Das Normenrestsymbol.

Um die Multiplikationsregeln für zwei zyklische Körper verschiedenen Grades aufstellen zu können, müssen wir unsere über c_ν und z_ν getroffene Normierung noch etwas verschärfen:

Es sollen in (8) nur solche Polynome f_ν verwendet werden, welche die Eigenschaften

$$f_\nu(x_1, \ldots, x_\nu) = f_{\nu-r+1}(x_r, \ldots, x_\nu) + f_\nu(x_1, \ldots, x_{r-1}, 0, \ldots, 0) \tag{23}$$
$$(1 \leqq r \leqq \nu;\ \nu = 1, 2, \ldots, n-1)$$

erfüllen.

Die für den Existenzbeweis verwendeten Polynome $f_\nu = -\sum_{i=1}^{\nu} \frac{x_\nu^{p^{\nu-i+1}}}{p^{\nu-i+1}}$ besitzen offenbar auch die zusätzliche Eigenschaft (23). Aus (23) resultieren für z_ν die Eigenschaften

$$(23\,a)\quad \begin{aligned} &z_\nu(0, 0, \ldots, 0, x_r, x_{r+1}, \ldots, x_\nu; y_1, \ldots, y_\nu) = z_{\nu-r+1}(x_r, \ldots, x_\nu; y_r, \ldots, y_\nu)\\ &z_\nu(x_1, \ldots, x_\nu; 0, 0, \ldots, 0, y_r, y_{r+1}, \ldots, y_\nu) = z_{\nu-r+1}(x_r, \ldots, x_\nu; y_r, \ldots, y_\nu)\,. \end{aligned}$$

Wir definieren die zyklischen Algebren

$$H_n = K(u; v_1, v_2, \ldots, v_n) = (\alpha; \beta_1, \beta_2, \ldots, \beta_n] \text{ mit}$$

$$\begin{aligned} &\wp v_1 = \beta_1 && u^{p^n} = \alpha\\ &\wp v_2 = z_1 + \beta_2 &&\\ &\cdots\cdots\cdots && uv_n u^{-1} = v_n + c_{n-1}\\ &\wp v_n = z_{n-1} + \beta_n && \end{aligned}$$

und mit der für c_i und z_i von uns getroffenen verschärften Normierung. Es sei $\beta_1 \neq \wp\beta^{(0)}$ mit $\beta^{(0)}$ aus K. H_n ist dann vom Grade p^n.

In geläufiger Weise sei das Normenrestsymbol

$$\left(\frac{\alpha, Z_n}{\mathfrak{p}}\right)$$

aus der $\mathfrak{p}$-Invariante von H_n definiert. Dem Gruppenelement $\left(\frac{\alpha, Z_n}{\mathfrak{p}}\right)$ sei durch die Festsetzung

$$\left(\frac{\alpha, Z_n}{\mathfrak{p}}\right) = s^{\left\{\frac{\alpha; \beta_1, \ldots, \beta_n}{\mathfrak{p}}\right\}}$$

das spezielle Normenrestsymbol

$$\left\{\frac{\alpha; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\} \bmod p^n$$

und diesem weiter das isomorphe multiplikative Symbol

$$\left(\frac{\alpha; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right) = \exp\left(\frac{2\pi i}{p^n}\left\{\frac{\alpha; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\}\right)$$

zugeordnet. Entsprechend sei für das Artin-Symbol

$$\left(\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right) = \exp\left(\frac{2\pi i}{p^n}\left\{\frac{\beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right\}\right).$$

Außer dem vorderen Zerlegungssatz

$$\left(\frac{\alpha\alpha'; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right) = \left(\frac{\alpha; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right)\left(\frac{\alpha'; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right)$$

gelten für das Normenrestsymbol auch hintere Zerlegungssätze, die jetzt in den entsprechenden Algebrenregeln hergeleitet werden sollen. Bei ihrem Beweis werden die Assoziativitätsrelation, die Symmetrieeigenschaft und die Eigenschaft (23a) von z_ν eine hervorragende Rolle spielen.

Neben H_n betrachten wir die zyklische Algebra

$$H'_{n-k} = K(u'; v'_1, v'_2, \ldots, v'_{n-k}) = (\alpha'; \beta'_1, \beta'_2, \ldots, \beta'_{n-k}]$$

vom Grade p^{n-k} $(0 \leqq k < n)$ mit

$$\begin{aligned} &\wp v'_1 = \beta'_1 && (u')^{p^{n-k}} = \alpha'\\ &\wp v'_2 = z_1 + \beta'_2 &&\\ &\cdots\cdots\cdots && u' v'_{n-k} (u')^{-1} = v'_{n-k} + c_{n-k-1}\,.\\ &\wp v'_{n-k} = z_{n-k-1} + \beta'_{n-k} && \end{aligned}$$

Wir bilden

$$H_n \times H'_{n-k} = K(u; v_1, v_2, \ldots, v_n \mid u'; v'_1, v'_2, \ldots, v'_{n-k}),$$

wobei die gestrichenen Operatoren mit den ungestrichenen vertauschbar sind. Wir führen folgende Transformation der Operatoren aus:

$$\text{(24)}\quad \begin{aligned} &1.\ \ \bar{u} = u;\ \bar{v}_i = v_i \text{ für } i = 1, 2, \ldots, k \\ &\quad \bar{v}_{k+1} = v_{k+1} + v'_1 \\ &\quad \bar{v}_{k+2} = v_{k+2} + v'_2 + z_1(v_{k+1}; v'_1) \\ &\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\quad \bar{v}_n = v_n + v'_{n-k} + z_{n-k-1}(v_{k+1}, \ldots, v_{n-1}; v'_1, \ldots, v'_{n-k-1}). \\ &2.\ \ \bar{u}' = u'(u^p)^{-1};\ \bar{v}'_j = v'_j \quad (j = 1, 2, \ldots, n-k). \end{aligned}$$

Über die neuen Operatoren stellen wir in mehreren Schritten fest:

a) *Die Transformationsgleichungen* (24) *sind nach den ursprünglichen Operatoren auflösbar. Es ist also*

$$K(u; v_1, v_2, \ldots, v_n \mid u'; v'_1, v'_2, \ldots, v'_{n-k}) = K(\bar{u}; \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n \mid \bar{u}'; \bar{v}'_1, \bar{v}'_2, \ldots, \bar{v}'_{n-k}).$$

b) *Es ist*

$$K(\bar{u}'; \bar{v}'_1, \bar{v}'_2, \ldots, \bar{v}'_{n-k}) = \left(\frac{\alpha'}{\alpha}; \beta'_1, \beta'_2, \ldots, \beta'_{n-k}\right].$$

c) *Es gilt*

$$\text{(25)}\quad \wp\bar{v}_i = z_{i-1}(\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{i-1}; \bar{\beta}_1, \bar{\beta}_2, \ldots, \bar{\beta}_{i-1}) + \bar{\beta}_i \qquad (i = 1, 2, \ldots, n)$$

mit

$$\bar{\beta}_i = \beta_i \text{ für } i = 1, 2, \ldots, k$$

und

$$\bar{\beta}_i = \beta_i + \beta'_{i-k} + z_{i-k-1}(\beta_{k+1}, \ldots, \beta_{i-1}; \beta'_1, \ldots, \beta'_{i-k-1}) \quad \text{für} \quad i = k+1, k+2, \ldots, n.$$

Beweis. Für $i = 1, 2, \ldots, k$ ist (25) evident. Soll (25) auch für $i = k+1$, $k+2, \ldots, n$ gelten, so muß folgende Identität erfüllt sein:

$$\begin{aligned} &z_{i-1}(\bar{v}_1, \ldots, \bar{v}_{i-1}; \bar{\beta}_1, \ldots, \bar{\beta}_{i-1}) + z_{i-k-1}(\beta_{k+1}, \ldots, \beta_{i-1}; \beta'_1, \ldots, \beta'_{i-k-1}) \\ &= z_{i-1}(v_1, \ldots, v_{i-1}; \beta_1, \ldots, \beta_{i-1}) + z_{i-k-1}(v'_1, \ldots, v'_{i-k-1}; \beta'_1, \ldots, \beta'_{i-k-1}) \\ &+ z_{i-k-1}(v_{k+1} + \beta_{k+1} + z_k(v_1, \ldots; \beta_1, \ldots), \ldots; v'_1 + \beta'_1, \ldots, v'_{i-k-1} + \beta'_{i-k-1} + z_{i-k-2}(v'_1, \ldots; \beta'_1, \ldots)) \\ &\qquad - z_{i-k-1}(v_{k+1}, \ldots, v_{i-1}; v'_1, \ldots, v'_{i-k-1}). \end{aligned} \tag{26}$$

Nun beachten wir die Assoziativitätsrelation (12) und die Eigenschaft (23a) von z_ν. In (12) ersetzen wir ν durch $i-k-1$ und geben den Unabhängigen ξ, η, ζ folgende Werte:

$$\xi_j = v'_j, \quad \eta_i = \beta'_j, \quad \zeta_j = \beta_{k+j} \qquad (j = 1, 2, \ldots, i-k-1).$$

Dann geht (12) über in

$$\begin{aligned} &z_{i-k-1}(\beta'_1 + \beta_{k+1}, \ldots, \beta'_{i-k-1} + \beta_{i-1} + z_{i-k-2}(\beta'_1, \ldots; \beta_{k+1}, \ldots); v'_1, \ldots, v'_{i-k-1}) \\ &\qquad + z_{i-k-1}(\beta'_1, \ldots, \beta'_{i-k-1}; \beta_{k+1}, \ldots, \beta_{i-1}) \\ &= z_{i-k-1}(v'_1 + \beta'_1, \ldots, v'_{i-k-1} + \beta'_{i-k-1} + z_{i-k-2}(v'_1, \ldots, \beta'_1, \ldots); \beta_{k+1}, \ldots, \beta_{i-1}) \\ &\qquad + z_{i-k-1}(v'_1, \ldots, v'_{i-k-1}; \beta'_1, \ldots, \beta'_{i-k-1}). \end{aligned} \tag{27a}$$

Ersetzen wir in (12) ν durch $i-1$ und geben den Unabhängigen ξ, η, ζ die Werte

$\xi_j = v_j$ für $j = 1, 2, \ldots, i-1$,
$\eta_j = 0$, $\zeta_j = \beta_j$ für $j = 1, 2, \ldots, k$,
$\eta_j = v'_{j-k}$, $\zeta_j = \beta_j + \beta'_{j-k} + z_{j-k-1}(\beta_{k+1}, \ldots, \beta'_1, \ldots)$ für $j = k+1, k+2, \ldots, i-1$,

so geht (12) unter Beachtung von (23a) über in

$$\begin{aligned} &z_{i-1}(\bar{v}_1, \ldots, \bar{v}_{i-1}; \bar{\beta}_1, \ldots, \bar{\beta}_{i-1}) + z_{i-k-1}(v_{k+1}, \ldots, v_{i-1}; v_1', \ldots, v_{i-k-1}') \\ &\qquad = z_{i-1}(\beta_1, \ldots, \beta_k, v_1' + \beta_{k+1} + \beta_1', \ldots; v_1, \ldots, v_{i-1}) \\ &+ z_{i-k-1}(v_1', \ldots, v_{i-k-1}'; \beta_{k+1} + \beta_1', \ldots, \beta_{i-1} + \beta_{i-k-1}' + z_{i-k-2}(\beta_{k+1}, \ldots; \beta_1', \ldots)). \end{aligned} \tag{27b}$$

Ersetzen wir in (12) ν wieder durch $i-1$ und geben den Unabhängigen ξ, η, ζ die Werte

$$\begin{aligned} &\xi_j = 0 \text{ für } j = 1, 2, \ldots, k, \\ &\xi_j = v_{j-k}' + \beta_{j-k}' + z_{j-k-1}(v_1', \ldots; \beta_1', \ldots) \text{ für } j = k+1, k+2, \ldots, i-1, \\ &\eta_j = \beta_j, \zeta_j = v_j \text{ für } j = 1, 2, \ldots, i-1, \end{aligned}$$

so geht (12) unter Beachtung von (23a) über in

$$\begin{aligned} &z_{i-1}(\beta_1, \ldots, \beta_k, v_1' + \beta_1' + \beta_{k+1}, \ldots; v_1, \ldots, v_{i-1}) \\ &+ z_{i-k-1}(v_1' + \beta_1', \ldots, v_{i-k-1}' + \beta_{i-k-1}' + z_{i-k-2}(v_1', \ldots; \beta_1', \ldots); \beta_{k+1}, \ldots, \beta_{i-1}) \\ &= z_{i-k-1}(v_{k+1} + \beta_{k+1} + z_k(v_1, \ldots; \beta_1, \ldots), \ldots; v_1' + \beta_1', \ldots) \\ &\qquad + z_{i-1}(v_1, \ldots, v_{i-1}; \beta_1, \ldots, \beta_{i-1}). \end{aligned} \tag{27c}$$

Die Summation von (27a), (27b) und (27c) gibt gerade die Identität (26). Damit ist die Richtigkeit von (26) erwiesen.

d) *Es gilt*

$$\bar{u}\,\bar{v}_i\,\bar{u}^{-1} = \bar{v}_i + c_{i-1}(\bar{v}_1, \ldots, \bar{v}_{i-1}) \qquad (i = 1, 2, \ldots, n). \tag{28}$$

Aus (25) und (28) folgt dann

$$K(\bar{u}; \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n) = (\alpha; \bar{\beta}_1, \bar{\beta}_2, \ldots, \bar{\beta}_n].$$

(28) ist für $i \leqq k$ trivial. Soll (28) auch für $i > k$ richtig sein, so muß die Identität

$$\begin{aligned} &z_{i-k-1}(v_{k+1} + c_k, \ldots, v_{i-1} + c_{i-2}; v_1', \ldots, v_{i-k-1}') - z_{i-k-1}(v_{k+1}, \ldots, v_{i-1}; v_1', \ldots, v_{i-k-1}') \\ &\qquad = c_{i-1}(\bar{v}_1, \ldots, \bar{v}_{i-1}) - c_{i-1}(v_1, \ldots, v_{i-1}) \end{aligned} \tag{28a}$$

erfüllt sein. (28a) folgt aber unter Beachtung von (23a) sofort aus (7), wenn wir in (7)

$$\nu = i-1, \beta_j = 0 \text{ für } j \leqq k \text{ und } \beta_j = v_{j-k}' \text{ für } j = k+1, k+2, \ldots, i-1$$

setzen.

e) *Die Operatoren $\bar{v}_i$ $(i = 1, 2, \ldots, n)$ sind mit dem Operator $\bar{u}'$ vertauschbar.*

Dazu müssen wir zeigen, daß

$$(u^{p^k})\,\bar{v}_i(u^{p^k})^{-1} = (u')\,\bar{v}_i(u')^{-1}. \tag{29}$$

(29) beweisen wir mit Hilfe der sofort ersichtlichen Tatsache:

$$(u^{p^k})\,v_j(u^{p^k})^{-1} = v_j \text{ für } j \leqq k$$

und

$$(u^{p^k})\,v_j(u^{p^k})^{-1} = v_j + c_{j-k-1}(v_{k+1}, \ldots, v_{j-1}) \text{ für } k < j \leqq i.$$

Damit geht über (29) in

$$\begin{aligned} &c_{i-k-1}(v_{k+1}, \ldots, v_{i-1}) + z_{i-k-1}(v_{k+1}+1, \ldots, v_{i-1} + c_{i-k-2}(v_{k+1}, \ldots, v_{i-2}); v_1', \ldots, v_{i-k-1}') \\ &= c_{i-k-1}(v_1', \ldots, v_{i-k-1}') + z_{i-k-1}(v_{k+1}, \ldots, v_{i-1}; v_1'+1, \ldots, v_{i-k-1}' + c_{i-k-2}(v_1', \ldots, v_{i-k-2})). \end{aligned} \tag{29a}$$

(29a) entsteht aber durch Subtraktion zweier Relationen (7) mit $\nu = i-k-1$. Wir ersetzen einfach das eine Mal

$$v_j \text{ durch } v_{j+k}, \quad \beta_j \text{ durch } v_j',$$

und das andere Mal

$$v_j \text{ durch } v_j', \quad \beta_j \text{ durch } v_{j+k}, \quad (j = 1, 2, \ldots, i-k-1).$$

Aus a) bis e) zusammen folgern wir:

$$K(\bar{u}; \bar{v}_1, \ldots, \bar{v}_n \mid \bar{u}'; \bar{v}_1', \ldots, \bar{v}_{n-k}) = (\alpha; \bar{\beta}_1, \ldots, \bar{\beta}_n] \times \left(\frac{\alpha'}{\alpha}; \beta_1', \ldots, \beta_{n-k}'\right].$$

Für $\alpha = \alpha'$ ergibt sich daher die grundlegende Algebrenregel:

(30) $$\boxed{\begin{array}{l}(\alpha; \beta_1, \beta_2, \ldots, \beta_n] \times (\alpha; \beta_1', \beta_2', \ldots, \beta_{n-k}'] \\ \sim (\alpha; \beta_1, \ldots, \beta_k, \beta_{k+1} + \beta_1', \beta_{k+2} + \beta_2' + z_1(\beta_{k+1}; \beta_1'), \ldots, \beta_n + \beta_{n-k}' + z_{n-k-1}(\beta_{k+1}, \ldots; \beta_1', \ldots)].\end{array}}$$

Insbesondere gilt für die Multiplikation zweier Algebren vom gleichen Grade ($k = 0$):

(30a) $$\boxed{(\alpha; \beta_1, \ldots, \beta_n] \times (\alpha; \beta_1', \ldots, \beta_n'] \sim (\alpha; \beta_1 + \beta_1', \beta_2 + \beta_2' + z_1(\beta_1; \beta_1'), \ldots, \beta_n + \beta_n' + z_{n-1}(\beta_1, \ldots; \beta_1', \ldots)].}$$ [14])

Setzen wir in (30) $\beta_{k+1} = \beta_{k+2} = \cdots = \beta_n = 0$ und ändern in den β_i' die Bezeichnungen, so entsteht aus (30) wegen (9) die Regel:

(30b) $$\boxed{(\alpha; \beta_1, \beta_2, \ldots, \beta_k, 0, 0, \ldots, 0]_n \times (\alpha; \beta_{k+1}, \beta_{k+2}, \ldots, \beta_n] \sim (\alpha; \beta_1, \beta_2, \ldots, \beta_n].}$$

Der angefügte Index n soll andeuten, daß die Algebra vom Grade p^n ist.

Durch Iteration von (30b) erhalten wir schließlich die Regel:

(30c) $$\boxed{(\alpha; \beta_1, \beta_2, \ldots, \beta_n] \sim (\alpha; \beta_1, 0, \ldots, 0]_n \times (\alpha; \beta_2, 0, \ldots, 0]_{n-1} \times \cdots \times (\alpha; \beta_n]_1.}$$

Es entsteht nun die Frage der Transformation der Algebra H_n auf eine unverzweigte Darstellung für die Stelle $\mathfrak{p}$. Diese Frage ist für $n = 1$ durch die Formel

$$(\alpha, \beta]_{\mathfrak{p}} = \left(\pi, \ \operatorname{Res} \beta \frac{d\alpha}{\alpha}\right]_{\mathfrak{p}} \qquad (\pi \text{ Primelement zu } \mathfrak{p})$$

gelöst. Unter Berücksichtigung unseres Ergebnisses in der Verzweigungstheorie lehrt die Regel (30b), daß jede verzweigte Algebra H_n, falls sie nicht selbst schon vollverzweigt ist, als Produkt einer vollverzweigten Algebra H_{n-k} und einer unverzweigten Algebra H_n dargestellt werden kann. Zusammen mit der Regel (30c) besagt dies, daß wir uns bei der Aufsuchung einer unverzweigten Darstellung auf die Untersuchung des vollverzweigten Typus

$$(\alpha; \beta, 0, 0, \ldots, 0]$$

beschränken können.

Das in meiner Dissertation [15]) aufgestellte *Reziprozitätsgesetz der Potenzreste* ist auf Körper Z_n verallgemeinerungsfähig. Es ist unter Benutzung der Produktformel

$$\prod_{\mathfrak{p}} \left(\frac{\alpha; \beta_1, \beta_2, \ldots, \beta_n}{\mathfrak{p}}\right) = 1$$

rein formal herleitbar.

$\beta_1, \beta_2, \ldots, \beta_n$ und $\beta_1', \beta_2', \ldots, \beta_n'$ seien die erzeugenden Parameter der Körper Z_n und Z_n' mit den Führern $\mathfrak{f}$ und $\mathfrak{f}'$. Die Divisoren von β_ν und β_ν' ($\nu = 1, 2, \ldots, n$) werden so zerlegt:

---

[14]) Hier müssen wir auch noch $\beta_1 + \beta_1' + \wp\beta_1^{(0)}$ mit $\beta_1^{(0)}$ aus K voraussetzen. (30a) gilt natürlich auch ohne die verschärfte Normierung.

[15]) H. L. Schmid, Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper, Math. Zeitschr. **40** (1935).

$$\beta_\nu \cong \mathfrak{b}_\nu\, \mathfrak{c}'_\nu \quad \text{mit} \quad \begin{cases} (\mathfrak{b}_\nu, \mathfrak{f}') = 1 \\ \mathfrak{c}'_\nu \text{ nur aus Primteilern von } \mathfrak{f}' \text{ zusammengesetzt,} \end{cases}$$

$$\beta'_\nu \cong \mathfrak{b}'_\nu\, \mathfrak{c}_\nu \quad \text{mit} \quad \begin{cases} (\mathfrak{b}'_\nu, \mathfrak{f}) = 1 \\ \mathfrak{c}_\nu \text{ nur aus Primteilern von } \mathfrak{f} \text{ zusammengesetzt.} \end{cases}$$

Man zeigt dann leicht beitragsweise:

$$\left\{\frac{\beta_1, \ldots, \beta_n}{\prod_{\nu=1}^{n} \mathfrak{b}'_\nu}\right\} - \left\{\frac{\beta'_1, \ldots, \beta'_n}{\prod_{\nu=1}^{n} \mathfrak{b}_\nu}\right\} = \sum_{\mathfrak{p} \nmid \mathfrak{f}} \left\{\frac{\prod_{\nu=1}^{n} \beta'_\nu;\ \beta_1, \ldots, \beta_n}{\mathfrak{p}}\right\} - \sum_{\mathfrak{p} \nmid \mathfrak{f}'} \left\{\frac{\prod_{\nu=1}^{n} \beta_\nu;\ \beta'_1, \ldots, \beta'_n}{\mathfrak{p}}\right\}.$$

Mit der Produktformel ergibt sich dann ohne weiteres:

$$\left(\frac{\beta_1, \ldots, \beta_n}{\prod_{\nu=1}^{n} \mathfrak{b}'_\nu}\right)\left(\frac{\beta'_1, \ldots, \beta'_n}{\prod_{\nu=1}^{n} \mathfrak{b}_\nu}\right)^{-1} = \prod_{\mathfrak{p} \mid \mathfrak{f}'} \left(\frac{\prod_{\nu=1}^{n} \beta_\nu;\ \beta'_1, \ldots, \beta'_n}{\mathfrak{p}}\right) \prod_{\mathfrak{p} \mid \mathfrak{f}} \left(\frac{\prod_{\nu=0}^{n} \beta'_\nu;\ \beta_1, \ldots, \beta_n}{\mathfrak{p}}\right)^{-1}.$$

Eingegangen 6. Januar 1936.