Zyklische Körper und Algebren der Charakteristik
p vom Grad pn. Struktur diskret bewerteter
perfekter Körper mit vollkom...

Witt, Ernst

in: Journal für die reine und angewandte Mathematik | Journal für die reine und angewandte Mathematik | Article

126 - 140

Zyklische Körper und Algebren der Charakteristik p vom Grad p^n.

Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p.

Von *Ernst Witt* in Göttingen.

Merkwürdig ist der historische Weg bis zu dieser Arbeit: Er nimmt seinen Anfang bei Artins Untersuchungen über die reellen Körper, führt sodann durch ein Gebiet mit Primzahlcharakteristik, nämlich zuerst über die zyklischen Körper der Grade p und p^2 (Artin und Schreier), dann weiter über die zyklischen Körper vom Grad p^n (Albert, Witt), er geht dann durch das nichtkommutative Gebiet der zyklischen Algebren vom Grad p und p^n (H. L. Schmid), und endet schließlich wieder kommutativ mit Charakteristik 0, nämlich bei den Henselschen p-adischen Körpern (Hasse, F. K. Schmidt, Teichmüller, Witt) [1]).

Artin untersuchte die Körper der Charakteristik 0, die durch Adjunktion einer einzigen Zahl algebraisch abgeschlossen werden, und fand u. a., daß dies durch Adjunktion von $\sqrt{-1}$ geschehen kann. Um nun zu beweisen, daß ein algebraisch abgeschlossener Körper der Charakteristik p in bezug auf keinen Unterkörper von endlichem Grad ist, mußte gezeigt werden, daß bei Charakteristik p ein zyklischer Körper p-ten Grades immer enthalten ist in einem zyklischen Körper vom Grad p^2. Nebenresultate waren dabei die Artin-Schreiersche Normalform $x^p - x = a$ für die zyklischen Körper vom Grad p^2. Durch die Fortsetzung der hierfür entwickelten Methoden konnte Albert die zyklischen Körper vom Grad p^n schrittweise aufbauen. Es gelang mir, eine von speziellen Formeln freie Konstruktion anzugeben.

Inzwischen hatte H. L. Schmid die zyklischen Algebren p-ten Grades der Charakteristik p untersucht. Für diese Algebren $(\alpha, \beta]$ mit den Erzeugenden u, θ und den definierenden Relationen

$$u^p = \alpha, \quad \theta^p - \theta = \beta, \quad u\theta u^{-1} = \theta + 1$$

gelten die Regeln

$$(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta] \quad \text{und} \quad (\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

Für den Fall, daß der Grundkörper k aus Potenzreihen der Variablen t bestand, bewies Schmid die Residuenformel

$$(\alpha, \beta] \sim \left(t, \operatorname{Res} \frac{d\alpha}{\alpha} \beta\right].$$

Um entsprechende Resultate für Algebren vom Grad p^n zu erhalten, mußte zuerst meine sehr willkürliche Konstruktion für zyklische Körper vom Grad p^n wieder zweck-

[1]) Literaturangaben befinden sich auf S. 127.

mäßig normiert werden. Für p^2 fand Teichmüller eine Normierung. Eine andere wurde von Schmid gefunden und nach mühsamer Untersuchung auch für p^n. Für die entsprechend gebildeten zyklischen Algebren $(\alpha\,|\,\beta_0, \ldots, \beta_{n-1}]$ fand Schmid Regeln von der Form

$$(\alpha\,|\,\beta_i] \cdot (\alpha'\,|\,\beta_i] \sim (\alpha\alpha'\,|\,\beta_i] \quad \text{und} \quad (\alpha\,|\,\beta_i] \cdot (\alpha\,|\,\beta_i'] \sim (\alpha\,|\,s_i(\beta_j, \beta_j')]$$

mit gewissen Polynomen $s_i(x_j, y_j)$. Diese Polynome wurden zunächst für Charakteristik 0 definiert, und erst nach einem Beweis ihrer Ganzzahligkeit mod p genommen. Leider waren die Schmidschen Beweise durch Verwendung von Funktionen von vielen komplizierten Argumenten recht unübersichtlich.

Im Anschluß an die Schmidschen Untersuchungen machte ich die Entdeckung, daß die Verknüpfung $(x_i) + (y_i) = (s_i)$ mit Hilfe der Polynome $s_i(x_j, y_j)$ eine kommutative Gruppe der Vektoren $(x_i) = (x_0, x_1, \ldots)$ lieferte, die eng zusammenhing mit der Addition der p-adischen Zahlen $\Sigma\, x_i p^i$. Ausgehend von dieser Gruppe ließen sich jetzt die Schmidschen Resultate in vereinfachter Form herleiten. Ferner fand sich ein Analogon zur Residuenformel für den Grad p^n, wonach ich schon über ein Jahr lang gesucht hatte.

Die Gruppe der Vektoren mit Komponenten ξ_i aus dem Körper von p Elementen erwies sich wirklich als identisch mit der Additionsgruppe der ganzen p-adischen Zahlen $\Sigma\, x_i p^i$ mit passendem Vertreter x_i der Restklasse $\xi_i \bmod p$, und zwar waren nach einer Bemerkung von Hasse Vertreter x_i mit $x_i^p = x_i$ zu nehmen.

Da Teichmüller inzwischen auch eine neue Multiplikation der Vektoren fand, konnte er damit p-adische Körper mit beliebigem vollkommenen Restklassenkörper der Charakteristik p herstellen. Umgekehrt bewies Teichmüller den Satz, daß es in jedem diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper der Charakteristik p ein einziges Repräsentantensystem R mit der Eigenschaft $R^p = R$ gibt. Gestützt auf diesen Satz konnte er nun die Sätze von Hasse und F. K. Schmidt über die Struktur der diskret bewerteten perfekten Körper in neuer und viel einfacherer Form beweisen. Den verzweigten Fall konnte anschließend Hasse erledigen.

Auch diese Untersuchungen sind in dieser Arbeit aufgenommen worden, da sich unterdessen herausgestellt hat, daß alle Vektoroperationen gleichzeitig eingeführt werden können, und zwar in einer Weise, die jeden Nachweis von Rechengesetzen überflüssig macht. Außerdem werden dadurch die Beweise über die Struktur der diskret bewerteten perfekten Körper noch weiter vereinfacht.

Überraschend ist der enge Zusammenhang der Theorie der zyklischen Körper und Algebren der Charakteristik p vom Grad p^n mit der p-adischen Addition. Und noch mehr überrascht *die Erkenntnis, daß die Addition und Multiplikation der p-adischen Zahlen sich in einem Körper der Charakteristik p rational begründen läßt.*

Literaturverzeichnis.

1. A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Am. Math. Soc. **40** (1934).
2. E. Artin, Kennzeichnung des Körpers der reellen algebraischen Zahlen, Abh. Math. Sem. Hamburg **3** (1924).
3. E. Artin und O. Schreier, Über eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg **5** (1927).
4. H. Hasse und F. K. Schmidt, Die Struktur diskret bewerteter Körper, Crelle **170** (1934).
5. H. L. Schmid, Zyklische algebraische Funktionenkörper vom Grad p^n über endlichem Konstantenkörper der Charakteristik p, Crelle **175** (1936).
6. O. Teichmüller, Über die Struktur diskret bewerteter perfekter Körper, Gött. Nachr. 1936.
7. E. Witt, Der Existenzsatz für abelsche Funktionenkörper, Crelle **173** (1935). — Die Resultate dieser Arbeit werden mit W. I, 2; W. II; W. III usw. zitiert.
8. E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^l, Crelle **174** (1936).

1. Begründung einer Vektorrechnung.

p sei eine feste Primzahl. Für einen *Vektor*

$$x = (x_0, x_1, x_2, \ldots)$$

mit abzählbar vielen *Komponenten* x_n führen wir *Nebenkomponenten*

$$\text{(a)} \qquad x^{(n)} = x_0^{p^n} + p x_1^{p^{n-1}} + \cdots + p^n x_n$$

ein und bringen das auch gelegentlich in der Schreibweise

$$x = (x_0, x_1, x_2, \ldots \mid x^{(0)}, x^{(1)}, x^{(2)}, \ldots)$$

zum Ausdruck. Da sich umgekehrt x_n rekursiv als rationalzahliges Polynom in $x^{(0)}, \ldots, x^{(n)}$ aus den Gleichungen (a) berechnen läßt, ist ein Vektor x auch schon durch Angabe seiner Nebenkomponenten völlig bestimmt.

Summe, Differenz und Produkt zweier Vektoren erklären wir *nebenkomponentenweise*:

$$\text{(b)} \qquad x \mathbin{\dot{\pm}} y = (?, ?, \ldots \mid x^{(0)} \mathbin{\dot{\pm}} y^{(0)}, x^{(1)} \mathbin{\dot{\pm}} y^{(1)}, \ldots).$$

Wir wollen nun einige besondere Regeln für das Rechnen mit Vektoren herleiten. Dazu führen wir das *Verschiebungszeichen* V ein durch

$$\text{(1)} \qquad Vx = (0, x_0, x_1, \ldots).$$

Zur Abkürzung setzen wir noch

$$\text{(2)} \qquad \{u\} = (u, 0, 0, \ldots),$$

es ist also $V^i\{u\}$ ein Vektor, dessen i-te Komponente gleich u und dessen übrige Komponenten 0 sind. Aus (a) folgt

$$\text{(c)} \qquad (Vx)^{(n)} = p x^{(n-1)} \qquad (x^{(-1)} = 0)$$

oder ausführlich geschrieben

$$\text{(d)} \qquad Vx = (0, x_0, x_1, \ldots \mid 0, p x^{(0)}, p x^{(1)}, \ldots).$$

Es bestehen die Regeln

$$\text{(3)} \qquad V(x + y) = Vx + Vy$$

$$\text{(4)} \qquad (x_0, x_1, x_2, \ldots) = \sum_0^{r-1} V^i\{x\} + V^r(x_r, x_{r+1}, \ldots),$$

$$\text{(5)} \qquad \{u\}\,(x_0, x_1, x_2, \ldots) = (u x_0, u^p x_1, u^{p^2} x_2, \ldots),$$

wie man sofort durch Hinschreiben der n-ten Nebenkomponenten bestätigt. Es liegt nahe, die folgenden Bezeichnungen einzuführen:

$$\text{(6)} \qquad \begin{aligned} \mathbf{0} &= (0, 0, 0, \ldots) \\ \mathbf{1} &= (1, 0, 0, \ldots) \\ \boldsymbol{m} &= \mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}. \end{aligned}$$

Weiter wollen wir die fraglichen Komponenten $(x \mathbin{\dot{\pm}} y)_n$ des Vektors $x \mathbin{\dot{\pm}} y$ näher untersuchen. Dazu setzen wir

$$\text{(7)} \qquad x^p = (x_0^p, x_1^p, x_2^p, \ldots).$$

x^p ist also nicht etwa die p-te Potenz im Sinn der Vektormultiplikation; diese wird gar nicht vorkommen. Aus (a) folgt die *Rekursionsgleichung*

$$\text{(e)} \qquad x^{(n)} = x^{p\,(n-1)} + p^n x_n,$$

wobei natürlich $x^{p\,(n-1)}$ die $(n-1)$-te Nebenkomponente des Vektors x^p bedeutet und nicht etwa eine $p(n-1)$-te Potenz.

Wir bezeichnen allgemein mit

$$R[u, v, \ldots] \text{ und } G[u, v, \ldots]$$

den Ring aller rationalzahligen bzw. ganzzahligen Polynome in $u, v, \ldots$.

Aus (e) und (b) folgt die additive Kongruenz

$$p^n(x+y)^n \equiv (x+y)^{(n)} = x^{(n)} + y^{(n)} \equiv p^n x_n + p^n y_n \bmod R[x_0, y_0, \ldots, x_{n-1}, y_{n-1}],$$

also mit einem passenden Polynom f

$$(8) \qquad (x+y)_n = x_n + y_n + f(x_0, y_0, \ldots, x_{n-1}, y_{n-1}).$$

Bisher haben wir die Vektoroperationen nur *algebraisch* untersucht, und an keiner Stelle wurde benutzt, daß p eine Primzahl ist. Wir kommen jetzt auf die *arithmetischen* Eigenschaften zu sprechen, die aus der besonderen Gestalt der Gleichungen (a) fließen. Wir zeigen dazu das

Lemma. *Für zwei Vektoren x und y mögen die Hauptkomponenten in einem Integritätsbereich $\mathfrak{J}$ der Charakteristik 0 liegen. Dann sind für $r > 0$ die Kongruenzen*

$$x_\nu \equiv y_\nu \bmod p^r\mathfrak{J}$$

gleichwertig mit den Kongruenzen

$$x^{(\nu)} \equiv y^{(\nu)} \bmod p^{r+\nu}\mathfrak{J}.$$

Beweis. Für $\nu < n$ sei die Gleichwertigkeit schon erkannt, also dürfen wir annehmen, es sei $x_\nu \equiv y_\nu \bmod p^r\mathfrak{J}$. Wegen $x_\nu^p \equiv y_\nu^p \bmod p^{r+1}\mathfrak{J}$ folgt nach Induktionsnahme

$$x^{p(n-1)} \equiv y^{p(n-1)} \bmod p^{r+n}\mathfrak{J}.$$

Nun ist wegen (e)

$$(x^n - y^n) - (p^n x_n - p^n y_n) = x^{p(n-1)} - y^{p(n-1)} \equiv 0 \bmod p^{r+n}\mathfrak{J},$$

und daraus folgt die Gleichwertigkeit auch für $\nu = n$.

Satz 1. *$(x \dot{\pm} y)_n$ ist ein ganzzahliges Polynom in $x_0, y_0, \ldots, x_n, y_n$.*

In den beiden ersten Komponenten ist beispielsweise

$$x + y = \left(x_0 + y_0, x_1 + y_1 - \sum_1^{p-1} \frac{1}{p}\binom{p}{\nu} x_0^\nu y_0^{p-\nu}, \text{ usw.}\right)$$

$$x \cdot y = (x_0 y_0, x_1 y_0^p + x_0^p y_1 + p x_1 y_1, \text{ usw.})$$

Beweis. $x^{(n)}$ und $y^{(n)}$ liegen im Ring $\mathfrak{J} = G[x_0, y_0 \ldots, x_n, y_n]$. Nach (e) ist

$$x^{(n)} \equiv x^{p(n-1)} \text{ und } y^{(n)} \equiv y^{p(n-1)} \bmod p^n\mathfrak{J}.$$

Daher ist wegen (b)

$$(x \dot{\pm} y)^{(n)} = x^{(n)} \dot{\pm} y^{(n)} \equiv x^{p(n-1)} \dot{\pm} y^{p(n-1)} = (x^p \dot{\pm} y^p)^{(n-1)} \bmod p^n\mathfrak{J}.$$

Für $\nu < n$ sei der Satz schon bewiesen, also gilt $(x \dot{\pm} y)_\nu^p \equiv (x^p \dot{\pm} y^p)_\nu \bmod p\mathfrak{J}$. Das Lemma ergibt

$$(x \dot{\pm} y)^{p(n-1)} \equiv (x^p \dot{\pm} y^p)^{(n-1)} \bmod p^n\mathfrak{J}.$$

Wegen (e) ist

$$p^n(x \dot{\pm} y)_n = (x \dot{\pm} y)^{(n)} - (x \dot{\pm} y)^{p(n-1)} \equiv 0 \bmod p^n\mathfrak{J},$$

und daraus folgt der Satz auch für $\nu = n$.

Satz 2. *Es gilt komponentenweise $\boldsymbol{p}x \equiv Vx^p \bmod pG[x_i]$.*

Beweis. Nach (e), (c), (b), ist für die Nebenkomponenten

$$(\boldsymbol{p}x)^{(n)} = px^{(n)} \equiv px^{p(n-1)} = (Vx^p)^{(n)} \bmod p^{n+1}G[x_i],$$

aus dem Lemma folgt jetzt die Behauptung $(\boldsymbol{p}x)_n \equiv (Vx^p)_n \bmod pG[x_i]$.

2. Der Residuenvektor (α, β).

Zur Vorbereitung für die letzten Abschnitte müssen wir die folgenden Betrachtungen einschalten.

Wir betrachten formale Potenzreihen

$$\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots \qquad (a_m \neq 0)$$

in t mit Koeffizienten a_i aus einem Integritätsbereich $\mathfrak{J}$ der Charakteristik 0. β sei ein Vektor, dessen einzelne Komponenten β_ν wieder Potenzreihen [2]) sind:

$$\beta = (\beta_0, \beta_1, \ldots), \qquad \beta_\nu = \sum_{i > -\infty} b_{\nu i} t^i.$$

Für den von α und β abhängigen Vektor

$$(\mathrm{f}) \qquad (\alpha, \beta) = \left(?, ?, \ldots \,\middle|\, \mathrm{Res}\, \frac{d\alpha}{\alpha} \beta^{(0)}, \mathrm{Res}\, \frac{d\alpha}{\alpha} \beta^{(1)}, \ldots\right)$$

gelten nach (e) und (d) die Rechenregeln

$$(9) \qquad (\alpha\alpha', \beta) = (\alpha, \beta) + (\alpha', \beta),$$

$$(10) \qquad (\alpha, \beta + \beta') = (\alpha, \beta) + (\alpha, \beta'),$$

$$(11) \qquad (\alpha, V\beta) = V(\alpha, \beta).$$

Für später sprechen wir die unmittelbar aus (f) folgenden Tatsachen aus:

Satz 3. *Ist c ein Vektor mit lauter konstanten Komponenten, so gilt $(\alpha, \beta) \cdot c = (\alpha, \beta c)$. Es ist $(t, c) = c$. Enthalten alle Entwicklungen der β_ν nur Potenzen von t mit lauter positiven bzw. lauter negativen Exponenten, so ist $(t, \beta) = 0$.*

Wir zeigen nun den folgenden arithmetischen

Satz 4. *Für*

$$\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots \qquad (a_m \neq 0),$$

$$\beta = (\beta_0, \beta_1, \ldots) \quad \textit{mit} \quad \beta_\nu = \sum_{i > -\infty} b_{\nu i} t^i$$

sind die Komponenten $(\alpha, \beta)_n$ des Vektors (α, β) ganzzahlige Polynome in a_m^{-1}, a_i, $b_{\nu i}$.

Beweis. Es sei $\mathfrak{J} = G[a_m^{-1}, a_i, b_{\nu i}]$.

Wir führen zunächst den Beweis durch für den Fall $\alpha = t$. Zum Vektor β bilden wir die Vektoren β' und β'' mit den Komponenten

$$\beta'_\nu = \sum_{i > 0} b_{\nu i} t^i \quad \text{bzw.} \quad \beta''_\nu = \sum_{i < 0} b_{\nu i} t^i,$$

und führen damit die Vektoroperation Ω ein durch

$$\Omega\beta = \beta - \beta' - \beta''.$$

Mit den Koeffizienten von β liegen nach Satz 1 auch die Koeffizienten von $\Omega\beta$ in $\mathfrak{J}$. Sind die Komponenten $\beta_0, \ldots, \beta_{\nu-1}$ konstant, so auch die Komponenten $(\Omega\beta)_0, \ldots, (\Omega\beta)_\nu$. Nach (10) und Satz 3 ist

$$(t, \Omega\beta) = (t, \beta) - (t, \beta') - (t, \beta'') = (t, \beta),$$

und deshalb allgemein $(t, \beta) = (t, \Omega^n\beta)$. Für $\nu < n$ ist nun $(\Omega^n\beta)_\nu$ konstant; wie in Satz 3 gilt daher $(t, \Omega^n\beta)_\nu = (\Omega^n\beta)_\nu$. Somit liegt

$$(t, \beta)_\nu = (\Omega^n\beta)_\nu \qquad (\nu < n)$$

im Integritätsbereich $\mathfrak{J}$.

Nun sei α eine beliebige Potenzreihe. Wir können β_ν nach der neuen Variablen

---

[2]) Die Summationsbezeichnung $\sum_{i > -\infty}$ soll andeuten, daß in der Reihe nur endlich viele Glieder mit negativem Index i auftreten.

$t' = t^{1-m}\alpha$ entwickeln, und zwar liegen die neuen Koeffizienten $b'_{\nu i}$ wieder in $\mathfrak{Z}$. Nach dem vorhin Bewiesenen ist $(t', \beta)_n$ ganzzahliges Polynom in $b'_{\nu i}$, liegt also in $\mathfrak{Z}$. Nach (9) und (10) gilt die Zerlegung

$$(\alpha, \beta) = (m - 1) \cdot (t, \beta) + (t', \beta),$$

nach Satz 1 liegen daher die Komponenten des Vektors (α, β) ebenfalls in $\mathfrak{Z}$, w. z. b. w.

3. Vektoren bei Charakteristik p. Konstruktion von p-adischen Körpern.

Theoretisch brauchen wir nur die ganzzahligen Polynome $(x \dot{\pm} y)_n$ einfach anzugeben und können dann mit ihnen Summe, Differenz und Produkt von Vektoren erklären, ohne überhaupt von Nebenkomponenten zu reden. In diesem Sinn muß das bestehende Distributivgesetz $x(y + z) = xy + xz$ als Zusammenfassung von ganzzahligen Polynomidentitäten in x_i, y_i, z_i angesehen werden. Ähnlich ist es mit den anderen Gesetzen. Ebenso würde es genügen, wenn wir die ganzzahligen Polynome $(\alpha, \beta)_n$ einfach angeben. Die Formeln (1) bis (11) und die Sätze 1 bis 4 behalten dann ihre Gültigkeit.

Diesen Standpunkt nehmen wir nun ein und betrachten alles mod p:

Erklärung. *$x \dot{\pm} y$ ist ein Vektor, dessen Komponenten feststehende Polynome in x_i, y_i sind mit Koeffizienten aus dem Galoisfeld $GF(p)$ von p Elementen. Es gelten die Kommutativ-, Assoziativ- und Distributivgesetze.*

(α, β) ist ein Vektor, dessen Komponenten feststehende Polynome in $a_m^{-1}, a_i, b_{\nu i}$ sind mit Koeffizienten aus $GF(p)$.

Die Formeln (1) *bis* (11) *und Satz* 3 *bleiben bestehen. Ferner gilt jetzt*

$$(x \dot{\pm} y)^p = x^p \dot{\pm} y^p, \tag{12}$$

$$px = Vx^p \qquad \text{(Satz 2)}, \tag{13}$$

$$(V^i x) \cdot (V^j y) = V^{i+j}(x^{p^j} y^{p^i}). \tag{14}$$

Um (14) zu beweisen, dürfen wir erst x und y durch x^{p^i}, y^{p^j} ersetzen. Dann geht die Behauptung wegen (13) über in $(p^i x) \cdot (p^j y) = p^{i+j}(xy)$.

Nun sei $\mathfrak{k}$ ein **beliebiger Körper der Charakteristik p.** Wir betrachten Vektoren x mit Komponenten aus $\mathfrak{k}$. Diese bilden hinsichtlich der erklärten Vektorrechnung einen Ring $I(\mathfrak{k})$. Diesen Ring wollen wir nunmehr untersuchen.

Wir definieren folgendermaßen eine Bewertung der Vektoren:

Es werde $|x| = p^{-r}$ gesetzt, wenn x_r die erste von Null verschiedene Komponente des Vektors x ist; ferner $|0| = 0$. Aus (3) und (14) folgen dann sofort die beiden Regeln

$$|x + y| \leqq \text{Max}\,(|x|, |y|), \tag{15}$$

$$|xy| = |x| \cdot |y|. \tag{16}$$

Auf Grund dieser Bewertung dürfen wir von Konvergenz reden. Nach (4) gilt jetzt

$$(x_0, x_1, x_2, \ldots) = \sum_0^\infty V^i\{x_i\}. \tag{17}$$

Es ist ohne weiteres klar, daß jede konvergente Folge von Vektoren gegen einen Vektor konvergiert, d. h. daß der Ring $I(\mathfrak{k})$ perfekt ist.

Satz 5. *Im Ring $I(\mathfrak{k})$ ist ein Vektor $a = (a_0, a_1, \ldots)$ mit $a_0 \neq 0$ eine Einheit.*

Beweis. Setzen wir nämlich $1 - a\{a_0^{-1}\} = Vb$, so ist

$$a \cdot \{a_0^{-1}\} \sum_0^\infty (Vb)^i = (1 - Vb) \sum_0^\infty (Vb)^i = 1.$$

Jetzt sei $\mathfrak{k}$ ein **vollkommener Körper der Charakteristik p.** Wir haben dann für jeden Vektor aus dem Ring $I(\mathfrak{k})$ die Reihenentwicklung

$$(x_0, x_1, x_2, \ldots) = \sum_0^\infty p^i\{x^{p^{-i}}\}.$$

Wir wollen nun den Quotientenkörper $Q(\mathfrak{k})$ des Rings $I(\mathfrak{k})$ bilden. Da die in $Q(\mathfrak{k})$ gebildeten Reihen

$$\sum_{i>-\infty} p^i\{x^{p^{-i}}\} \tag{18}$$

offensichtlich einen Körper bilden, besteht $Q(\mathfrak{k})$ gerade aus allen Reihen (18). Wie immer, so läßt sich auch hier die Bewertung auf den Quotientenkörper fortsetzen.

Satz 6. *Für einen vollkommenen Körper $\mathfrak{k}$ ist der Quotientenkörper $Q(\mathfrak{k})$ des Ringes $I(\mathfrak{k})$ aller Vektoren aus $\mathfrak{k}$ ein diskret bewerteter perfekter Körper der Charakteristik 0. $Q(\mathfrak{k})$ ist unverzweigt, d. h. (p) ist ein Primideal in $I(\mathfrak{k})$. Der Restklassenkörper $I(\mathfrak{k})/(p)$ ist mit $\mathfrak{k}$ isomorph.*

Diskrete Bewertung bedeutet dabei: die vorkommenden Beträge haben *nur* den Häufungspunkt 0.

4. Struktur diskret bewerteter perfekter Körper.

Diesen Abschnitt schalten wir ein, um eine Übersicht über alle diskret bewerteten perfekten Körper $\mathfrak{k}$ mit vollkommenem Restklassenkörper $\mathfrak{k}$ der Charakteristik p zu gewinnen.

Es sei k ein bewerteter perfekter Körper. Für den Betrag mögen die Regeln (15) und (16) gelten. Die vorkommenden Beträge sollen nur den Häufungspunkt 0 haben. Die Elemente a mit $|a| \leqq 1$ (ganze Elemente) bilden einen Integritätsbereich $\mathfrak{J}$. Die Elemente b mit $|b| < 1$ bilden in $\mathfrak{J}$ ein Primideal, wegen der Diskretheit der Bewertung ist es ein Hauptideal (π). Der Restklassenkörper $\mathfrak{k} = \mathfrak{J}/(\pi)$ sei ein vollkommener Körper der Charakteristik p. Da für eine Primzahl $q \neq p$ sicher $q \not\equiv 0 \bmod \pi$, also erst recht $q \not\equiv 0$ in k ist, hat k entweder die Charakteristik p oder die Charakteristik 0.

Für die Beweise der nachfolgenden Sätze 7 und 9 machen wir zwei Feststellungen:

(g) Für ganze Elemente a und b folgt aus $a \equiv b \bmod \pi^r$ $(r > 0)$ die Kongruenz $a^{p^n} \equiv b^{p^n} \bmod \pi^{r+n}$ $(n \geqq 0)$.

(h) Sind die Komponenten der Vektoren x und y ganz, so folgt aus den Kongruenzen $x_\nu \equiv y_\nu \bmod \pi^r$ $(r > 0)$ die Kongruenz $x^{(n)} \equiv y^{(n)} \bmod \pi^{r+n}$ $(n \geqq 0)$.

Weil nämlich $\binom{p}{i} \equiv 1$ oder $0 \bmod \pi$ ist, folgt zunächst $a^p \equiv b^p \bmod \pi^{r+1}$ und dann durch n-malige Iteration die Behauptung (g). Hiermit läßt sich aus der Gleichung (a) unmittelbar die andere Behauptung (h) ablesen. —

Mit einem Repräsentantensystem R aus $\mathfrak{J} \bmod \pi$ läßt sich jedes Element aus k auf genau eine Weise in eine Reihe

$$\sum_{i>-\infty} r_i \pi^i \qquad (r_i \text{ aus } R) \tag{19}$$

entwickeln.

Wir zeigen nun nach Teichmüller:

Satz 7. *Es gibt in $\mathfrak{J}$ ein einziges Repräsentantensystem R mit der Eigenschaft $R^p = R$. Es ist multiplikativ abgeschlossen. Wenn k die Charakteristik p hat, so ist R ein mit $\mathfrak{k}$ isomorpher Körper.*

Beweis. $\mathfrak{a}$ sei eine feste Restklasse $\bmod \pi$. Wir wählen aus jeder Restklasse $\mathfrak{a}^{p^{-\nu}}$ $(\nu \geqq 0)$ ein beliebiges Element a_ν, und behaupten: $a_\nu^{p^\nu}$ konvergiert für $\nu \to \infty$, und zwar gegen eine Zahl a aus $\mathfrak{a}$, und weiter, a hängt nicht ab von der besonderen Auswahl der a_ν.

Es folgt nämlich $a_{\nu+1}^{p} \equiv a_\nu \bmod \pi$, also $a_{\nu+1}^{p^{\nu+1}} \equiv a_\nu^{p^\nu} \bmod \pi^{\nu+1}$, und hieraus folgt die Konvergenz. Weil jedes $a_\nu^{p^\nu}$ in $\mathfrak{a}$ liegt, muß auch der Grenzwert a darin liegen. a_ν' seien die Elemente einer zweiten Auswahl. Wegen $a_\nu' \equiv a_\nu \bmod \pi$ ist $a_\nu'^{p^\nu} \equiv a_\nu^{p^\nu} \bmod \pi^{\nu+1}$, und für die Grenzwerte folgt $a' = a$.

Konstruieren wir für jede Restklasse $\mathfrak{a}$ die zugehörige Zahl a, so bilden diese Zahlen ein Repräsentantensystem R. Es sei $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. Dann liegt $a_\nu b_\nu = c_\nu$ in $\mathfrak{a}^{p^{-\nu}}\mathfrak{b}^{p^{-\nu}} = \mathfrak{c}^{p^{-\nu}}$, und wegen $a^{p^\nu} b^{p^\nu} = c^{p^\nu}$ folgt für die Grenzwerte $ab = c$. Daher ist R multiplikativ abgeschlossen, und wegen $\mathfrak{k}^p = \mathfrak{k}$ ist $R^p = R$. Wenn k die Charakteristik p hat, so folgt analog aus $\mathfrak{a} + \mathfrak{b} = \mathfrak{c}$ die Gleichung $a + b = c$, also ist R ein mit $\mathfrak{k}$ isomorpher Körper.

Umgekehrt sei R' ein Repräsentantensystem mit $R'^p = R$. Es sei a_ν' der Repräsentant aus $\mathfrak{a}^{p^{-\nu}}$, dann ist $a_\nu'^{p^\nu} = a_0'$, also der Grenzwert $a = a_0'$, d. h. es ist $R = R'$.

Aus diesem Satz in Verbindung mit (19) folgt

Satz 8. *Ein diskret bewerteter perfekter Körper k der Charakteristik p mit einem vollkommenen Restklassenkörper $\mathfrak{k}$ der Charakteristik p ist mit einem Potenzreihenkörper einer Variablen über $\mathfrak{k}$ isomorph.*

Nunmehr habe k die Charakteristik 0. Es sei $(p) = (\pi^e)$, wegen $p \equiv 0 \bmod \pi$ ist $e > 0$.

Satz 9. *Jedem Vektor*

$$\mathfrak{x} = (\mathfrak{x}_0, \mathfrak{x}_1, \ldots)$$

aus $I(\mathfrak{k})$ werde die ganze Zahl

$$\xi = \sum_0^\infty x_i^{p^{-i}} p^i$$

aus k zugeordnet, wobei $x_i^{p^{-i}}$ der Repräsentant von $\mathfrak{x}_i^{p^{-i}}$ in dem Repräsentantensystem R mit $R^p = R$ ist.

Aus $\mathfrak{x} \dot{\pm} \mathfrak{y} = \mathfrak{z}$ folgt dann $\xi \dot{\pm} \eta = \zeta$.

Beweis. Es werde $\mathfrak{x}^{p^{-n}} = (\mathfrak{x}_0^{p^{-n}}, \mathfrak{x}_1^{p^{-n}}, \ldots)$ und $x^{p^{-n}} = (x_0^{p^{-n}}, x_1^{p^{-n}}, \ldots)$ gebildet, wobei $x_i^{p^{-n}}$ wieder in R liegen und $\mathfrak{x}_i^{p^{-n}}$ repräsentieren soll. — Nach (a) ist

$$x^{p^{-n}(n)} = \sum_0^n x^{p^{-i}} p^i,$$

also

$$\lim x^{p^{-n}(n)} = \xi.$$

Aus $\mathfrak{x} \dot{\pm} \mathfrak{y} = \mathfrak{z}$ folgt $\mathfrak{x}^{p^{-n}} \dot{\pm} \mathfrak{y}^{p^{-n}} = \mathfrak{z}^{p^{-n}}$, und hieraus $(x^{p^{-n}} \dot{\pm} y^{p^{-n}})_\nu \equiv z_\nu^{p^{-n}} \bmod \pi$. Nach (b) und (h) ergibt sich für die Nebenkomponenten

$$x^{p^{-n}(n)} \dot{\pm} y^{p^{-n}(n)} = (x^{p^{-n}} \dot{\pm} y^{p^{-n}})^{(n)} \equiv z^{p^{-n}(n)} \bmod \pi^{n+1}.$$

Für die Grenzwerte ist daher $\xi \dot{\pm} \eta = \zeta$, w. z. b. w.

Damit ist gezeigt, daß die Reihen $\sum_0^\infty Rp^i$ $(R^p = R)$ einen zu $I(\mathfrak{k})$ isomorphen Ring $\mathfrak{J}'$ bilden. Folglich bilden die Reihen $\sum_{i>-\infty} Rp^i$ einen zu $Q(\mathfrak{k})$ isomorphen Körper k'.

Wie jedes Element aus $\mathfrak{J}$ läßt sich auch π^e/p in eine Reihe

$$\frac{\pi^e}{p} = \sum_{i=0}^{e-1} \sum_{j=0}^{\infty} r_{ij} p^j \pi^i = \sum_{i=0}^{e-1} g_i \pi^i$$

entwickeln mit r_{ij} aus $R^p = R$, bzw. g_i aus $\mathfrak{F}'$. Mit π^e/p muß auch g_0 prim zu p sein. Es ist also $k = k'(\pi)$, wobei π einer Eisensteinschen Gleichung e-ten Grades genügt.

Satz 10. *Ein diskret bewerteter perfekter Körper der Charakteristik 0 mit einem vollkommenen Restklassenkörper $\mathfrak{k}$ der Charakteristik p enthält einen invariant bestimmten Unterkörper k', der zum Körper $Q(\mathfrak{k})$ von Satz 6 isomorph ist. Ist $(p) = (\pi^e)$ mit einem Primelement π aus k, so ist $k = k'(\pi)$, wo π einer Eisensteinschen Gleichung e-ten Grades genügt.*

Während die Sätze 8 und 10 die Struktur der diskret bewerteten perfekten Körper mit vollkommenem Restklassenkörper $\mathfrak{k}$ aufdecken, kann uns Satz 9 dazu dienen, gegebenenfalls das Rechnen mit Vektoren zurückzuführen auf das Rechnen mit ganzen p-adischen Zahlen.

5. Zyklische und abelsche Körper der Charakteristik p vom Exponenten p^n.

Es sei k ein beliebiger Körper der Charakteristik p. Wir wollen seine zyklischen Oberkörper vom Grad p^n, allgemeiner seine abelschen Oberkörper vom Exponenten p^n untersuchen.

Dazu rechnen wir mit Vektoren x mit Komponenten aus k, und zwar nur mod V^n, d. h. wir rechnen nur mit Vektoren

$$x = (x_0, x_1, \ldots, x_{n-1})$$

der Länge n.

Wir gehen jetzt genau nach derselben Methode vor wie in der Arbeit W. I, nur daß wir alle dort bewiesenen Sätze über Körperzahlen hier entsprechend für Vektoren aussprechen.

Mit $\sigma, \tau, \ldots$ seien die Automorphismen des galoisschen (separablen) Körpers K/k bezeichnet. Für einen Vektor $C = (C_0, C_1, \ldots)$ mit C_i aus K erklären wir

$$C^\sigma = \sigma C = (\sigma C_0, \sigma C_1, \ldots)$$
$$\mathrm{Sp}\, C = \sum_\sigma \sigma C = (\mathrm{Sp}\, C_0, *, \ldots).$$

Ist also C_0 eine Zahl, deren Spur nicht verschwindet, so gibt es nach Satz 5 einen zu Sp C reziproken Vektor. Es bestehen die Regeln

$$\sigma(A + B) = \sigma A + \sigma B, \qquad (AB)^\sigma = A^\sigma B^\sigma.$$

Jedem σ sei ein Vektor A_σ zugeordnet. Der Satz W. I, 2 kann mitsamt seinem Beweis fast ungeändert übernommen werden:

Satz 11. *Bestehen die Relationen $A_\sigma + \sigma A_\tau = A_{\sigma\tau}$, so gibt es einen solchen Vektor B, daß $A_\sigma = (1 - \sigma)\, B$ gilt.*

Zum Beweis nehmen wir den oben konstruierten Vektor C. Wie man leicht nachrechnet, kann $B = \dfrac{1}{\mathrm{Sp}\, C} \sum_\tau A_\tau\, \tau C$ gewählt werden.

Übrigens gelten auch hier die Sätze W. I, 1 und W. I, 3.

Ebenso wie für Zahlen a vorteilhaft die Bezeichnung $\wp a = a^p - a$ eingeführt wurde, setzen wir für Vektoren

$$\wp x = x^p - x = (x_0^p, x_1^p, \ldots, x_{n-1}^p) - (x_0, x_1, \ldots, x_{n-1}).$$

Es besteht die Regel

$$\wp(x + y) = \wp x + \wp y.$$

Die Lösungen von $\wp x = 0$ sind genau die Vektoren mit Komponenten aus dem Primkörper.

Wir nennen nun die Vektoren α von der Form $\wp\beta$ zerfallend, und schreiben dafür auch $\alpha \sim 0$.

1. Der Zerfall von $(0, \alpha_1, \ldots, \alpha_{n-1})$ ist gleichwertig mit dem Zerfall von $(\alpha_1, \ldots, \alpha_{n-1})$.

Denn ist $(0, \alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_0, \beta_1, \ldots, \beta_{n-1})$, so liegt β_0 im Primkörper. Wird die Gleichung $0 = \wp(\beta_0, 0 \ldots, 0)$ abgezogen, so bleibt

$$(0, \alpha_1, \ldots, \alpha_{n-1}) = \wp(0, \beta_1, \ldots, \beta_{n-1}),$$

und diese Gleichung ist nach (4) gleichwertig mit $(\alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_1, \ldots, \beta_{n-1})$.

2. Im algebraisch abgeschlossenen Körper $\bar{k}$ zerfällt jeder Vektor.

Denn in $\bar{k}$ darf man $\alpha_0 = \wp a$ setzen, und wegen

$$(20) \quad (\wp a, \alpha_1, \ldots, \alpha_{n-1}) \sim (\wp a, \alpha_1, \ldots, \alpha_{n-1}) - \wp(a, 0, \ldots, 0) = (0, \alpha_1', \ldots, \alpha_{n-1}')$$

braucht jetzt nur noch der Zerfall des kürzeren Vektors $(\alpha_1', \ldots, \alpha_{n-1}')$ nachgewiesen zu werden.

Im Körper k können wir jedenfalls sagen, daß die Komponenten θ_i einer Lösung $\theta = (\theta_0, \ldots, \theta_{n-1})$ der Gleichung $\wp\theta = \alpha$ algebraische Zahlen sind. $K = K(\theta_0, \ldots, \theta_{n-1})$ ist also ein Zerfällungskörper des Vektors α. Jede weitere Lösung unterscheidet sich von θ nur um einen Vektor aus dem Primkörper, daher liegen in K sämtliche Lösungen. K ist also charakterisiert als kleinster Zerfällungskörper des Vektors α und muß daher galoissch sein. Die sämtlichen Lösungen θ der Gleichung $\wp\theta = \alpha$ sollen mit $\frac{1}{\wp}\alpha$ bezeichnet werden.

Wir sind nun im Stande, sämtliche Überlegungen und Sätze aus W. III (und W. II) fast wörtlich zu übertragen. Es ist dabei zu beachten, daß an Stelle von Zahlen immer Vektoren der Länge n zu nehmen sind, und statt einer Anwendung von W. I muß hier der vorhin bewiesene Satz 11 herangezogen werden. Auf diese Weise gelangen wir zu den Ergebnissen:

Satz 12. *Es sei ω eine additive Gruppe von Vektoren der Länge n, die alle zerfallenden Vektoren $\wp\alpha$ enthält, so daß $\omega/\wp\alpha$ endlich ist. Dann ist die galoissche Gruppe von $k\left(\frac{1}{\wp}\omega\right)/k$ zur Gruppe $\omega/\wp\alpha$ isomorph.*

Zu jedem abelschen Körper K/k vom Exponenten p^n gibt es genau eine solche Gruppe $\omega/\wp\alpha$, daß $K = k\left(\frac{1}{\wp}\omega\right)$ gilt.

Wir wollen nun zusehen, wie sich insbesondere die zyklischen Körper Z vom Grade p^n darstellen. Es ist $Z = k\left(\frac{1}{\wp}\beta\right)$ mit einem einzigen Vektor β der Länge n, und dabei darf $p^{n-1}\beta$ nicht zerfallen. Nun ist

$$(21) \qquad p\beta = V\beta^p = V\beta + \wp V\beta \sim V\beta,$$

also darf $V^{n-1}\beta$, d. h. β_0 nicht zerfallen. Ist θ eine Lösung von $\wp\theta = \beta$, so erhalten wir durch Anwendung der Automorphismen von Z/k auf θ genau p^n verschiedene, d. h. alle Lösungen dieser Gleichung. Daher gibt es einen Automorphismus σ mit $\sigma\theta = \theta + 1$. Wegen $\sigma^{p^{n-1}}\theta = \theta + p^{n-1} \neq \theta$ hat σ die Ordnung p^n.

Satz 13. *Ist $\beta = (\beta_0, \ldots, \beta_{n-1})$ ein Vektor mit $\beta_0 \neq \wp a$, so entsteht aus k durch Adjunktion einer Lösung $\theta = (\theta_0, \ldots, \theta_{n-1})$ der Gleichung $\wp\theta = \beta$ ein zyklischer Körper $Z = k\left(\frac{1}{\wp}\beta\right)$ vom Grad p^n.*

Umgekehrt läßt sich jeder zyklische Körper vom Grad p^n in dieser Weise darstellen. Durch $\sigma\theta = \theta + 1$ wird ein erzeugender Automorphismus von Z definiert.

6. Zyklische Algebren der Charakteristik p vom Grad p^n.

Wir werden jetzt die zyklischen Algebren vom Grad p^n über einem beliebigen Körper k der Charakteristik p behandeln.

Es sei $\alpha \neq 0$ eine Zahl und $\beta = (\beta_0, \ldots, \beta_{n-1})$ ein Vektor der Länge n aus k. Mit

$$(\alpha, \beta] = (\alpha \mid \beta_0, \ldots, \beta_{n-1}]$$

bezeichnen wir den **hyperkomplexen Ring**

mit der Erzeugenden u, den untereinander vertauschbaren Erzeugenden $\theta_0, \ldots, \theta_{n-1}$ und den definierenden Relationen $u^{p^n} = \alpha$, $\wp\theta = \beta$, $u\theta u^{-1} = \theta + 1$.

Dabei ist $\theta = (\theta_0, \ldots, \theta_{n-1})$ und $u\theta u^{-1} = (u\theta_0 u^{-1}, \ldots, u\theta_{n-1}u^{-1})$ gesetzt.

Die Transformation mit u liefert also einen Automorphismus des kommutativen Teilringes $k(\theta_0, \ldots, \theta_{n-1})$, und wegen

$$u^{p^{n-1}}\theta u^{-p^{n-1}} = \theta + \boldsymbol{p}^{n-1} \neq \theta, \quad u^{p^n}\theta u^{-p^n} = \theta + \boldsymbol{p}^n = \theta$$

hat dieser Automorphismus die Ordnung p^n.

Machen wir mit einer Zahl $\gamma \neq 0$ und einem Vektor δ aus k die simultanen Substitutionen

$$u' = \gamma u, \quad \alpha' = \alpha\gamma^{p^n}$$
$$\theta' = \theta + \delta, \quad \beta' = \beta + \wp\delta,$$

so gehen alle bisherigen Gleichungen in die entsprechenden Gleichungen für die gestrichenen Größen über. Daher gilt die Isomorphie

$$(\alpha, \beta] \cong (\alpha\gamma^{p^n}, \beta + \wp\delta]. \tag{22}$$

Satz 14. *Das eben erklärte System $(\alpha, \beta]$ ist einfach und normal und hat den Grad p^n.*

Beweis. Wir berufen uns auf einen allgemeinen Satz aus der Theorie hyperkomplexer Systeme: Ein System S über einem Körper k ist einfach und normal, wenn das mit dem algebraisch abgeschlossenen Körper $\bar{k}$ erweiterte System $\bar{S}$ einfach ist (und umgekehrt). Im Körper $\bar{k}$ haben wir aber wegen (22) mit $\gamma = \alpha^{p-n}$ und $\delta = -\frac{1}{\wp}\beta$ die Isomorphie $(\alpha, \beta] \cong (1, 0]$. Wir müssen also zeigen, daß das System $(1, 0]$ einfach ist und den Rang p^{2n} hat.

Der kommutative Teilring $k(\theta_0, \ldots, \theta_{n-1})$ wird durch die Gleichungen $\theta^p - \theta = 0$, d. h. durch $\theta_i^p = \theta_i$ bestimmt, daher ist $k(\theta_0, \ldots, \theta_{n-1}) = \sum_1^{p^n} k\, e_i$ mit Idempotenten e_i. Die Transformation mit u liefert eine Permutation der e_i von der Ordnung p^n, also eine zyklische. Wir können somit den Ring $(1, 0]$ auch darstellen durch die Basis

$$e_\sigma u^\tau \ (\sigma, \tau \bmod p^n) \text{ vom Rang } p^{2n}$$

und die Rechenregeln

$$u^{p^n} = 1; \quad e_\sigma^2 = e_\sigma, \quad e_\sigma e_\tau = 0 \ (\sigma \neq \tau), \quad (\Sigma e_\sigma = 1), \quad u e_\sigma u^{-1} = e.$$

Im Ring $(1, 0]$ sei nun $\mathfrak{A}$ ein Ideal, das ein Element $A = \sum_{\sigma,\tau} a_{\sigma,\tau} e_\sigma u^\tau \neq 0$ enthält, es sei etwa $a_{s,t} \neq 0$. Eine leichte Rechnung ergibt

$$\sum_\varrho u^\varrho e_s a_{s,t}^{-1} A u^{-t} e_s u^{-\varrho} = 1,$$

also ist $\mathfrak{A} = (1)$, d. h. der Ring $(1, 0]$ ist einfach, w. z. b. w.

Nunmehr zeigen wir einige grundlegende Algebrenregeln:

Satz 15. *Es gilt* $(\alpha \mid 0, \beta_1, \ldots, \beta_{n-1}] \sim (\alpha \mid \beta_1, \ldots, \beta_{n-1}]$.

Beweis. Für den kommutativen Teilring $k(\theta_0, \ldots, \theta_{n-1})$ der linksstehenden Algebra L gilt

$$\wp(\theta_0, \theta_1, \ldots, \theta_{n-1}) = (0, \beta_1, \ldots, \beta_{n-1}),$$

also ist $\theta_0^p = \theta_0$. Wird die Gleichung $\wp(\theta_0, 0, \ldots, 0) = 0$ abgezogen, so bleibt

$$\wp(0, \theta_1, \ldots, \theta_{n-1}) = (0, \beta_1, \ldots, \beta_{n-1}),$$

also ist

$$(\alpha) \qquad \wp(\theta_1, \ldots, \theta_{n-1}) = (\beta_1, \ldots, \beta_{n-1}).$$

Aus

$$u^p(\theta_0, \theta_1, \ldots, \theta_{n-1})\, u^{-p} = (\theta_0, \theta_1, \ldots, \theta_{n-1}) + \boldsymbol{p}$$

folgt

$$(\beta) \qquad u^p(\theta_1, \ldots, \theta_{n-1})\, u^{-p} = (\theta_1, \ldots, \theta_{n-1}) + \mathbf{1}.$$

e_i ($i \bmod p$) seien die p Idempotente des Ringes $k(\theta_0)$, sie werden bei Transformation mit u zyklisch vertauscht, $ue_iu^{-1} = e_{i+1}$. Es gilt die Zerlegung

$$k(\theta_0, \ldots, \theta_{n-1}) = \sum_{i \bmod p} e_i k(\theta_1, \ldots, \theta_{n-1}),$$

also

$$L = \sum_i \sum_\nu e_i k(\theta_1, \ldots, \theta_{n-1})\, u^\nu,$$

folglich

$$e_0 L e_0 = \sum_{\nu \equiv 0(p)} e_0 k(\theta_1, \ldots, \theta_{n-1})\, u^\nu.$$

Nach der hyperkomplexen Theorie ist $L \sim e_0 L e_0$. Der Ring $e_0 L e_0$ enthält e_0 als Einselement, er wird erzeugt von

$$e_0 u^p;\ e_0\theta_1, \ldots, e_0\theta_{n-1},$$

und nach (α), (β) bestehen die Relationen

$$(e_0u^p)^{p^{n-1}} = e_0\alpha,\quad \wp(e_0\theta_1, \ldots, e_0\theta_{n-1}) = (e_0\beta_1, \ldots, e_0\beta_{n-1}),$$
$$e_0u^p \cdot (e_0\theta_1, \ldots, e_0\theta_{n-1}) \cdot e_0u^{-p} = (e_0\theta_1, \ldots, e_0\theta_{n-1}) + (e_0, \ldots, 0).$$

Da die rechtsstehende Algebra $R = (\alpha \mid \beta_1, \ldots, \beta_{n-1}]$ durch genau entsprechende Relationen definiert ist, ist die Isomorphie $e_0 L e_0 \cong R$ und damit die Ähnlichkeit $L \sim R$ nachgewiesen.

Wir können jetzt zeigen, daß jede Algebra $(\alpha, \beta]$ einer *zyklischen Algebra* ähnlich ist. Wenn nämlich $\beta_0 \neq \wp a$ ist, so ist nach Satz 13 $k\left(\frac{1}{\wp}\beta\right)$ ein zyklischer Körper vom Grad p^n, und mit dem dort angegebenen Automorphismus σ ist in der üblichen Schreibweise für zyklische Algebren offenbar

$$(\alpha, \beta] \sim \left(\alpha, k\left(\frac{1}{\wp}\beta\right), \sigma\right).$$

Ist dagegen $\beta_0 = \wp a$, so ist nach (20) $\beta \sim (0, \beta_1', \ldots, \beta_{n-1}')$, wegen (22) und Satz 15 ist also

$$(\alpha \mid \beta_0, \beta_1, \ldots, \beta_{n-1}] \sim (\alpha \mid 0, \beta_1', \ldots, \beta_{n-1}'] \sim (\alpha \mid \beta_1', \ldots, \beta_{n-1}'].$$

Wird diese Reduktionsmethode mehrfach angewandt, so kommen wir schließlich auf den vorhin behandelten Fall zurück, bzw. auf eine Algebra vom Rang 1.

Satz 16. *Es gelten die Regeln*

$$(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta],$$
$$(\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

Beweis. Die Algebra $(\alpha, \beta] \cdot (\alpha', \beta']$ wird erzeugt von den Größen

$$\begin{cases} u, \theta & \text{mit } u^{p^n} = a, \quad \wp\theta = \beta, \quad u\theta u^{-1} = \theta + \mathbf{1}, \\ u', \theta' & \text{mit } u'^{p^n} = \alpha', \quad \wp\theta' = \beta', \quad u'\theta'u'^{-1} = \theta' + \mathbf{1}. \end{cases}$$

Dabei sind die Größen der ersten Zeile vertauschbar mit denen der zweiten.

Die Algebra wird aber auch erzeugt von den Größen

$$\begin{cases} v = uu', & \mathsf{H} = \theta \text{ mit } v^{p^n} = \alpha\alpha', \quad \wp\mathsf{H} = \beta, \; v\mathsf{H}v^{-1} = \mathsf{H} + \mathbf{1}, \\ v' = u', & \mathsf{H}' = \theta' - \theta \text{ mit } v'^{p^n} = \alpha', \; \mathsf{H}' = \beta' - \beta, \; v'\mathsf{H}'v'^{-1} = \mathsf{H}' + \mathbf{1}. \end{cases}$$

Dabei werden wieder die Größen der ersten Zeile vertauschbar mit denen der zweiten.

Infolgedessen gilt die Regel

$$(\alpha, \beta] \cdot (\alpha', \beta'] \sim (\alpha\alpha', \beta] \cdot (\alpha', \beta' - \beta].$$

Nun ist nach Satz 15 $(\alpha, 0] \sim 1$. Für $\beta = \beta'$ folgt daher die erste zu beweisende Regel $(\alpha, \beta] \cdot (\alpha', \beta] \sim (\alpha\alpha', \beta]$. Für $\alpha = 1$ ergibt sich hieraus $(1, \beta] \sim 1$. Setzen wir $\alpha' = \alpha^{-1}$ und $\beta' = 0$, so folgt $(\alpha, \beta] \sim (\alpha^{-1}, -\beta]$. Ersetzen wir die Größen α', β' durch α^{-1} und β', so erhalten wir die zweite zu beweisende Regel

$$(\alpha, \beta] \cdot (\alpha, \beta'] \sim (\alpha, \beta + \beta'].$$

7. Residuenformel für Algebren über einem Potenzreihenkörper.

In diesem Abschnitt sollen die Algebren $(\alpha, \beta]$ über einem speziellen Körper k untersucht werden.

C sei ein vollkommener Körper der Charakteristik p. Wir betrachten den Körper k aller Potenzreihen

$$\sum_{i>-\infty} c_i t^i, \qquad c_i \text{ aus } C.$$

Der im Abschnitt 2 eingeführte konstante Vektor (α, β) werde entsprechend auch für Vektoren β der Länge n eingeführt, so daß (α, β) ebenso lang wie β ist.

Satz 17. *Es besteht die* **Residuenformel** [3])

$$(\alpha \,|\, \beta] \sim (t \,|\, (\alpha, \beta)].$$

Beweis. Wir setzen den Quotienten $(\alpha \,|\, \beta] \cdot (t \,|\, (\alpha, \beta)]^{-1} = q(\alpha, \beta)$. Es gelten nach (9), (10) und Satz 16 die Regeln

$$(\alpha) \qquad q(\alpha\alpha', \beta) \sim q(\alpha, \beta) \cdot q(\alpha', \beta),$$

$$(\beta) \qquad q(\alpha, \beta + \beta') \sim q(\alpha, \beta) \cdot q(\alpha, \beta').$$

Enthalten alle Entwicklungen der β_ν nur Potenzen von t mit lauter positiven Exponenten, so konvergiert $\sum_0^\infty \beta^{p^h}$ komponentenweise gegen einen Vektor B. Wegen $\beta = \wp(-B)$ ist in diesem Fall $(t \,|\, \beta] \sim 1$.

Wenn alle Entwicklungen der β_ν nur Potenzen von t mit lauter negativen Exponenten enthalten, so ist ebenfalls $(t, \beta] \sim 1$, wie in einer nachfolgenden Arbeit von Teichmüller (dieser Bd. S. 141) bewiesen wird. (Dort wird benützt, daß C vollkommen ist.)

Zum Vektor β bilden wir wie im Beweis von Satz 4 die Vektoren β', β'' und $\Omega\beta = \beta - \beta' - \beta''$. Es folgt aus Satz 16 und den eben ausgeführten Tatsachen

$$(t \,|\, \Omega\beta] \sim (t \,|\, \beta] \cdot (t \,|\, \beta']^{-1} \cdot (t \,|\, \beta'']^{-1} \sim (t \,|\, \beta],$$

allgemeiner $(t \,|\, \beta] \sim (t \,|\, \Omega^n \beta]$. Es ist aber nach dem Beweis von Satz 4, weil wir es hier mit Vektoren der Länge n zu tun haben, $\Omega^n \beta = (t, \beta)$. Damit haben wir zunächst $q(t, \beta) \sim 1$ nachgewiesen.

---

[3]) Das sich für $p = 2$ ergebende Resultat

$$(t \,|\, \sum_i b_{0i} t^i, \sum_i b_{1i} t^i] \sim (t \,|\, b_{00}, b_{10} + \sum_{i>0} b_{0i} b_{0,-i}]$$

fand ich bereits im Januar 1935 durch sehr komplizierte nichtkommutative Rechnungen, bei denen nur das Ergebnis zufällig einfach erschien.

Nun sei $\alpha = a_m t^m + a_{m+1} t^{m+1} + \cdots (a_m \neq 0)$. Für die neue Variable $t' = t^{1-m}\alpha$ ist wieder $q(t', \beta) \sim 1$, folglich ist nach (α) und (β)

$$q(\alpha, \beta) \sim q(t, \beta)^{m-1} \cdot q(t', \beta) \sim 1, \text{ w. z. b. w.}$$

8. Berechnung der Invariante einer Algebra.

K_f sei der unverzweigte p-adische Körper mit dem Restklassenkörper C_f von p^f Elementen. k_f sei der Potenzreihenkörper mit C_f als Konstantenkörper. Derjenige Automorphismus von K_f, k_f bzw. C_f, der die Restklassen mod p, die Konstanten bzw. die Elemente in die p-te Potenz erhebt, werde einheitlich mit P bezeichnet. Ebenso soll die Spur über K_f/K_1, k_f/k_1, C_f/C_1 einheitlich mit Sp bezeichnet werden.

Über dem Körper k_f gibt es p^n verschiedene Algebren vom Grade p^n, die alle auf die zyklische Gestalt

$$(t^m, k_{nf}/k_f, P^f)$$

gebracht werden können, und welche durch die **Invariante** $\frac{m}{p^n} \bmod 1$ charakterisiert werden. Wir wollen zeigen, wie die Invariante einer Algebra $(\alpha, \beta]$ berechnet werden kann.

Satz 18. *Es werde der Potenzreihe* $\alpha = \mathfrak{a}^m t_m + \mathfrak{a}_{m+1} t^{m+1} + \cdots$ *des Körpers* k_f *mit Koeffizienten* $\mathfrak{a}_\nu$ *aus dem Galoisfeld* C_f *eine Potenzreihe* $\mathsf{A} = A_m t^m + A_{m+1} t^{m+1} + \cdots$ *mit Koeffizienten* A_ν *aus dem p-adischen Körper* K_f *derart zugeordnet, daß* A_ν *in der Restklasse* $\mathfrak{a}_\nu$ mod p *liegt. Entsprechend werde komponentenweise auch dem Vektor* $(\beta_0, \ldots, \beta_{n-1})$ *ein Vektor* $(\mathsf{B}_0, \ldots, \mathsf{B}_{n-1})$ *zugeordnet.*

Die Invariante der Algebra

$$(\alpha\,|\,\beta_0, \ldots, \beta_{n-1}]$$

lautet dann

$$\operatorname{Sp} \operatorname{Res} \frac{d\mathsf{A}}{\mathsf{A}} \left(\frac{\mathsf{B}_0^{p^n-1}}{p^n} + \frac{\mathsf{B}_1^{p^n-1}}{p^{n-1}} + \cdots + \frac{\mathsf{B}_{n-1}}{p} \right) \text{ mod } 1.$$

Beweis. Wie in Satz 9 ordnen wir jedem Vektor $\mathfrak{x} = (\mathfrak{x}_0, \ldots, \mathfrak{x}_{n-1})$ mit Komponenten $\mathfrak{x}_\nu$ aus dem Galoisfeld C_f die Restklasse $\xi = \sum_0^{n-1} \mathfrak{x}_i^{p^{-i}} p^i \bmod p^n$ zu. Dabei soll $\mathfrak{x}_i^{p^{-i}}$ im multiplikativen Repräsentantensystem des Körpers K_f liegen und die Restklasse $\mathfrak{x}_i^{p^{-i}} \bmod p$ darstellen. Bei dieser additiven Zuordnung geht $P\mathfrak{x}$ über in $P\xi$, ebenso geht Sp $\mathfrak{x}$ über in Sp ξ.

Wir betrachten zunächst Algebren $(t, \mathfrak{x}]$ mit konstantem Vektor $\mathfrak{x}$. Wenn $(t, \mathfrak{x}]$ zerfällt, so ist t Norm einer Zahl des zyklischen unverzweigten Körpers $k_f\left(\frac{1}{\wp}\mathfrak{x}\right)/k_f$, daher ist der betreffende Körpergrad 1, und es ist $\mathfrak{x} = (P-1)\mathfrak{y}$, also Sp $\mathfrak{x} = 0$. Deshalb werden die Algebren $(t, \mathfrak{x}]$ homomorph abgebildet auf Sp $\mathfrak{x}$. Ist umgekehrt Sp $\mathfrak{x} = 0$, so ist nach Satz 13 $\mathfrak{x} = (P-1)\mathfrak{y}$, und die Algebra $(t, \mathfrak{x}]$ zerfällt. Die Abbildung der Algebren $(t, \mathfrak{x}]$ auf Sp $\mathfrak{x}$ bzw. auf Sp ξ mod p^n ist infolgedessen eine Isomorphie.

Damit ist gezeigt, daß die Invariante der Algebra $(t, \mathfrak{x}]$ gleich $\frac{c}{p^n}$ Sp ξ mod 1 ist, wobei die Restklasse c mod p^n nicht von $\mathfrak{x}$ abhängt:

$$(t, \mathfrak{x}] \sim (t^{c \operatorname{Sp} \xi}, k_{nf}/k_f, P^f).$$

Zur Berechnung von c wählen wir speziell einen Vektor $\mathfrak{x}$ mit $\operatorname{Sp}\mathfrak{x} = 1$, d. h. mit $\operatorname{Sp}\xi \equiv 1 \bmod p^n$. Die Algebra $(t, \mathfrak{x}]$ mit den Relationen

$$u^{p^n} = t, \quad (P-1)\theta = \mathfrak{x}, \quad u\theta u^{-1} = \theta + 1$$

hat dann den Exponenten p^n. Daher ist $k_f(\theta)/k_f$ ein unverzweigter Körper vom Grad p^n, also $k_f(\theta) = k_{nf}$. Wegen

$$(P^f - 1)\theta = \frac{P^f - 1}{P - 1}(P-1)\theta = \frac{P^f - 1}{P-1}\mathfrak{x} = \operatorname{Sp}\mathfrak{x} = 1 \quad \text{oder} \quad P^f\theta = \theta + 1$$

können die Relationen für $(t, \mathfrak{x}]$ auch in der Form

$$u^{p^n} = t^1, \quad k_f(\theta) = k_{nf}, \quad u\theta u^{-1} = P^f\theta$$

geschrieben werden, dies sind aber gerade die Relationen für die Algebra $(t^1, k_{nf}/k_f, P^f)$. Damit ist $c \equiv 1 \bmod p^n$ nachgewiesen, und es ist allgemein gezeigt, daß die Algebra $(t, \mathfrak{x}]$ die Invariante $\frac{1}{p^n}\operatorname{Sp}\xi \bmod 1$ hat.

Aus der Restklasse $\mathfrak{x}_i \bmod p$ des Körpers K_f werde ein beliebiges Element X_i gewählt und der Vektor

$$X = (X_0, \ldots, X_{n-1} \mid X^{(0)}, \ldots, X^{(n-1)})$$

gebildet. Wird beachtet, daß für einen multiplikativen Repräsentanten r die Gleichung $\operatorname{Sp} r^p = \operatorname{Sp} r$ besteht, so folgt

$$\xi = \operatorname{Sp}\sum_0^{n-1} x_i^{p^{-i}} p^i = \operatorname{Sp}\sum_0^{n-1} x_i^{p^{n-i-1}} p^i \equiv \operatorname{Sp}\sum_0^{n-1} X_i^{p^{n-i-1}} p^i = \operatorname{Sp} X^{(n-1)} \bmod p^n.$$

Nun betrachten wir eine beliebige Algebra $(\alpha, \beta]$ und bilden gemäß Satz 18 A und B. Wird $\operatorname{Res}\frac{d\mathsf{A}}{\mathsf{A}}\mathsf{B}^{(i)} = X^{(i)}$ gesetzt und mit $\mathfrak{x}_i$ die Restklasse $X_i \bmod p$ bezeichnet, so ist nach Satz 17 $(\alpha, \beta] \cong (t, \mathfrak{x}]$. Die Invariante von $(\alpha, \beta]$ ist daher

$$\frac{1}{p^n}\operatorname{Sp} X^{(n-1)} = \frac{1}{p^n}\operatorname{Sp}\operatorname{Res}\frac{d\mathsf{A}}{\mathsf{A}}\mathsf{B}^{(n-1)} \bmod 1,$$

und dies war gerade zu beweisen.

9. Analogon zum Residuensatz.

Für einen algebraischen Funktionenkörper k der Charakteristik p mit vollkommenem Konstantenkörper teilen wir ohne Beweis noch folgendes mit:

Ist $\alpha \neq 0$ eine Zahl und β ein Vektor aus k, so werde an jeder Stelle $\mathfrak{p}$ der im Abschnitt 2 eingeführte Vektor (α, β) gebildet. Die Abhängigkeit von $\mathfrak{p}$ deuten wir durch einen Index an. Es gilt dann das Analogon zum Residuensatz

$$\sum_{\mathfrak{p}} (\alpha, \beta)_{\mathfrak{p}} = 0.$$

Der Beweis dieser Relation verläuft im Prinzip genau wie der übliche Beweis des Residuensatzes: Reduktion auf Geschlecht Null durch Spurbildung im Kleinen, und bei Geschlecht Null durch Zerlegung in Partialbrüche,

Die Relation $\sum_{\mathfrak{p}} = 0$ kann auch als Verallgemeinerung der Tatsache angesehen werden, daß die Summe der $\mathfrak{p}$-Invarianten einer Algebra $\equiv 0 \bmod 1$ ist.

Göttingen, 22. 6. 1936.

Eingegangen 29. August 1936.