Zerfallende zyklische $\mathfrak{p}$-Algebren.

Von *Oswald Teichmüller* in Göttingen.

Diese Arbeit schließt sich unmittelbar an eine vorangehende von E. Witt[1]) an. Erst wird hier der Haupthilfssatz für den Beweis der Residuenformel (Satz 17 jener Arbeit) bewiesen, dann ergibt sich aus dem Beweis ein Kriterium für den Zerfall von Algebren $(\alpha \mid \beta]$.

Es handelt sich um folgenden

Hilfssatz. *Ist $k = C\{t\}$ der Potenzreihenkörper über dem vollkommenen Grundkörper C und enthalten die Potenzreihen $\beta_0, \ldots, \beta_{n-1}$ nur die Glieder mit negativen Potenzen von t:*

$$\beta_\nu = \sum_{i=-w_\nu}^{-1} b_{\nu i} t^i,$$

so gilt über k

$$(t \mid \beta] \sim 1.$$

Statt dessen beweisen wir gleich den etwas allgemeineren

Satz 1. *C sei ein vollkommener Unterkörper eines Körpers k der Charakteristik p. Für $\alpha \neq 0$ aus k bilden wir den Ring*

$$R = C\alpha + C\alpha^2 + \cdots.$$

Für $\beta_0, \ldots, \beta_{n-1}$ in R gilt dann

$$(\mathfrak{A}) \qquad (\alpha \mid \beta_0, \ldots, \beta_{n-1}] \sim 1.$$

Dieser Satz enthält offenbar den obigen Hilfssatz, man nehme $\alpha = t^{-1}$.

Satz 1 gelte schon für $n - 1$, wir beweisen ihn für n. Nach W. Satz 15 besagt unsere Induktionsvoraussetzung genau, daß $(\mathfrak{A})$ jedenfalls für $\beta_0 = 0$ gilt. Man beachte, daß so auch der Fall $n = 1$ mitgenommen wird.

Wir bemerken noch vorweg, daß für zwei Vektoren x und y aus R auch $x \pm y$ und $\wp x$ Komponenten aus R haben. Denn R ist ein Ring; daß R kein Einselement zu haben braucht, spielt keine Rolle.

Um nun $(\mathfrak{A})$ zu beweisen, zeigen wir zunächst

$$(\alpha \mid \alpha, 0, \ldots, 0] \sim 1;$$

hieraus wird sich später leicht die allgemeine Formel ergeben. Außerdem machen wir noch eine Fallunterscheidung, je nachdem $\alpha = \wp a$, $a \in k$, ist oder nicht.

Ist $\alpha = \wp a$, so sei entsprechend W. (20)

$$(\alpha, 0, \ldots, 0) = \wp(a, 0, \ldots, 0) + (0, \eta_1, \ldots, \eta_{n-1}),$$

---

[1]) E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p, dieser Band, S. 126, zitiert mit W.

dann sind die $\eta_1, \ldots, \eta_{n-1}$ in

$$R' = Ca + Ca^2 + \cdots,$$

und nach W. (22) und der Induktionsvoraussetzung haben wir

$$(a \mid \alpha, 0, \ldots, 0] \cong (a \mid 0, \eta_1, \ldots, \eta_{n-1}] \sim 1.$$

Weil für alle i des Primkörpers auch $\wp(a + i) = \alpha$ ist, gilt genau so

$$(a + i \mid \alpha, 0, \ldots, 0] \sim 1;$$

durch Multiplikation folgt

$$(\alpha \mid \alpha, 0, \ldots, 0] \sim 1,$$

weil doch $\prod_{i=0}^{p-1} (a + i) = \wp a = \alpha$ ist.

Wenn aber $\alpha \neq \wp a$ ist, so ist nach W. Satz 13

$$Z_n = k(\Theta_0, \ldots, \Theta_{n-1}) \quad \text{mit} \quad \wp\Theta = (\alpha, 0, \ldots, 0)$$

ein zyklischer Körper mit dem erzeugenden Automorphismus

$$\sigma\Theta = \Theta + 1.$$

Wir betrachten den Zwischenkörper

$$Z_1 = k(\Theta_0)$$

und in ihm den Ring

$$R' = C\Theta_0 + C\Theta_0^2 + \cdots.$$

Wieder sei

$$(\mathfrak{B}) \qquad (\alpha, 0, \ldots, 0) = \wp(\Theta_0, 0, \ldots, 0) + (0, \mathrm{H}_1, \ldots, \mathrm{H}_{n-1}),$$

die $\mathrm{H}_1, \ldots, \mathrm{H}_{n-1}$ liegen dann in R'. Nach Induktionsvoraussetzung gilt

$$(\mathfrak{C}) \qquad (\Theta_0 \mid \mathrm{H}_1, \ldots, \mathrm{H}_{n-1}] \sim 1.$$

Aus $(\mathfrak{B})$ folgt aber auch

$$Z_n = Z_1\left(\frac{(\alpha, 0, \ldots, 0)}{\wp}\right) = Z_1\left(\frac{(\mathrm{H}_1, \ldots, \mathrm{H}_{n-1})}{\wp}\right),$$

d. h. Z_n ist der kleinste Zerfällungskörper des Vektors $(\mathrm{H}_1, \ldots, \mathrm{H}_{n-1})$ aus Z_1. Indem man gemäß der Bemerkung nach W. Satz 15 die Algebra $(\Theta_0 \mid \mathrm{H}_1, \ldots, \mathrm{H}_{n-1}]$ als zyklische Algebra auffaßt, sieht man aus $(\mathfrak{C})$, daß $\Theta_0 = N_{Z_n/Z_1}\,\Xi$ Norm eines Elements von Z_n ist. Offenbar ist aber $\alpha = N_{Z_1/Z_0}\Theta_0$, mithin

$$\alpha = N_{Z_n/Z_0}\Xi.$$

Deshalb muß die zyklische Algebra $(\alpha \mid \alpha, 0, \ldots, 0]$ zerfallen.

Um nun $(\mathfrak{A})$ zu beweisen, bemerken wir zuerst, daß $(\alpha \mid \beta_0, \ldots, \beta_{n-1}]$ für $\beta_\nu \in R$ nach Induktionsvoraussetzung nur von β_0 abhängt und daß aus $\beta_0 + \beta_0' = \bar{\beta}_0$ folgt

$$(\alpha \mid \beta_0, \ldots, \beta_{n-1}] \times (\alpha \mid \beta_0', \ldots, \beta_{n-1}'] \sim (\alpha \mid \bar{\beta}_0, \ldots, \bar{\beta}_{n-1}].$$

Es genügt darum,

$$(\mathfrak{D}) \qquad (\alpha \mid c\alpha^r, 0, \ldots, 0] \sim 1 \qquad (c \in C,\ r > 0)$$

zu beweisen. $c = 0$ wäre trivial, es sei $c \neq 0$.

Ist r zu p prim, so ist

$$(\mathfrak{E}) \quad (\alpha \mid c\alpha^r, 0, \ldots, 0]^r \times \left(\sqrt[p^n]{c} \mid c\alpha^r, \ldots, 0\right]^{p^n} \sim (c\alpha^r \mid c\alpha^r, 0, \ldots, 0] \sim 1;$$

weil die p^n-te Potenz jeder unserer Algebren ~ 1 ist, ergibt sich daraus $(\mathfrak{D})$.

Ist aber $r = ps$, so kann ($\mathfrak{D}$) für s statt r schon als richtig angesehen werden, und ($\mathfrak{D}$) folgt dann aus

$$(c\alpha^{ps}, 0, 0, \ldots, 0) = \left(\sqrt[p]{c}\,\alpha^s, 0, \ldots, 0\right) + \wp\left(\sqrt[p]{c}\,\alpha^s, 0, \ldots, 0\right) + (0, \delta_1, \ldots, \delta_{n-1}), \quad \delta_\nu \in R.$$

Damit ist Satz 1 bewiesen. Nun soll für jedes feste $\alpha \neq 0$ aus einem beliebigen Körper k der Charakteristik p die additive Gruppe aller Vektoren β mit $(\alpha|\beta_0, \ldots, \beta_{n-1}] \sim 1$ bestimmt werden.

Natürlich ist $(\alpha|\wp\gamma] \sim 1$. Ferner gilt nach dem soeben bewiesenen Satze $(\alpha|\alpha, 0, \ldots, 0] \sim 1$. (Für das oben auftretende C kann man z. B. den Primkörper nehmen.) Wie bei ($\mathfrak{E}$) folgt daraus für $(r, p) = 1$

$$(\alpha|c^{p^n}\alpha^r, 0, \ldots, 0]^r\,(c|c^{p^n}\alpha^r, 0, \ldots, 0]^{p^n} \sim (c^{p^n}\alpha^r|c^{p^n}\alpha^r, 0, \ldots, 0] \sim 1,$$
$$(\alpha|c^{p^n}\alpha^r, 0, \ldots, 0] \sim 1.$$

Wir behaupten nun, daß damit schon im wesentlichen die gesuchte additive Gruppe aufgefunden ist:

Satz 2. *Ist* $(\alpha|\beta] \sim 1$, *so ist* β *von der Form*

$$(\mathfrak{F})\qquad \beta = \wp\gamma + \sum_{r=1}^{p-1} V^{n-1}(c_{n-1,r}^{p}\alpha^r) + \sum_{\substack{r=1\\ p\nmid r}}^{p^2-1} V^{n-2}(c_{n-2,r}^{p^2}\alpha^r, 0) + \cdots + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} (c_{0,r}^{p^n}\alpha^r, 0, \ldots, 0).$$

Ist dieser Satz schon für Vektoren mit $n-1$ Komponenten richtig, so genügt es offenbar, aus $(\alpha|\beta] \sim 1$ eine Darstellung

$$\beta_0 = \wp c_0 + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} c_r^{p^n}\alpha^r$$

zu folgern, dann wird nämlich durch

$$(\beta_0, \ldots, \beta_{n-1}) = \wp(c_0, 0, \ldots, 0) + \sum_{\substack{r=1\\ p\nmid r}}^{p^n-1} (c_r^{p^n}\alpha^r, 0, \ldots, 0) + (0, \beta_1', \ldots, \beta_{n-1}')$$

ein Vektor $(\beta_1', \ldots, \beta_{n-1}')$ mit $n-1$ Komponenten definiert, für den auch $(\alpha|\beta'] \sim 1$ gilt und der darum schon die Struktur ($\mathfrak{F}$) haben muß.

Wenn α in k eine p-te Potenz sein sollte: $\alpha = \delta^p$, so gilt

$$(\alpha|\beta] \sim (\delta|\beta]^p \sim (\delta|\boldsymbol{p}\beta] \sim (\delta|V\beta^p] \sim (\delta|V\beta^p - \wp V\beta] \sim (\delta|V\beta];$$

aus $(\alpha|\beta_0, \ldots, \beta_{n-1}] \sim 1$ folgt also $(\delta|\beta_0, \ldots, \beta_{n-2}] \sim 1$; weil hier nur eine Algebra vom Grad p^{n-1} auftritt, gilt schon eine Darstellung

$$\beta_0 = \wp c' + \sum_{\substack{r=1\\ p\nmid r}}^{p^{n-1}-1} c_r^{p^{n-1}}\delta^r,$$

aus ihr folgt

$$\beta_0 = \beta_0^p - \wp\beta_0 = \wp(c'^p - \beta_0) + \sum_{\substack{r=1\\ p\nmid r}}^{p^{n-1}-1} c_r^{p^n}\alpha^r.$$

Dies gilt für $n > 1$; ist $n = 1$ und $\alpha = \delta^p$, so ist einfach

$$\beta_0 = \wp(-\beta_0) + \left(\frac{\beta_0}{\delta}\right)^p \alpha.$$

Nun sei α keine p-te Potenz. Wir betrachten die beiden Algebren

$$A = (\alpha|\beta] = k[u, \Theta_\nu], \quad u^{p^n} = \alpha, \quad \wp\Theta = \beta, \quad u\Theta u^{-1} = \Theta + 1$$

und

$$A^{(0)} = (\alpha\,|\,0] = k[u, \Theta_\nu^{(0)}], \quad u^{p^n} = \alpha, \quad \wp\Theta^{(0)} = 0, \quad u\Theta^{(0)}u^{-1} = \Theta^{(0)} + 1.$$

Sie sollen ähnlich sein, also müssen sie durch einen Isomorphismus i. b. a. k ineinander übergehen; dieser Isomorphismus kann sogar so gewählt werden, daß die kommutativen Unterkörper $k(u)$ von $A^{(0)}$ und von A einander entsprechen. Wir denken uns also A und $A^{(0)}$ als dieselbe Algebra mit demselben u darin.

Aus $u\Theta_0 u^{-1} = \Theta_0 + 1$ und $u\Theta_0^{(0)}u^{-1} = \Theta_0^{(0)} + 1$ folgt

$$\Theta_0 - \Theta_0^{(0)} = y \in k(u),$$

denn y ist mit u vertauschbar und $k(u)$ ist maximalkommutativ. Es sei

$$y = \sum_{r=0}^{p^n-1} c_r u^r = \sum_{s=0}^{p-1} \left(\sum_{h=0}^{p^{n-1}-1} c_{hp+s}(u^p)^h \right) u^s, \quad c_r \in k.$$

Betrachten wir nun die Subalgebra $k[u, \Theta_0^{(0)}]$ als einfache und normale Algebra über ihrem Zentrum $k(u^p)$, so ist nach einem früheren Ergebnis von Witt [2])

$$(\mathfrak{G}) \qquad \beta_0 = \wp(\Theta_0^{(0)} + y) = \wp\Theta_0^{(0)} + \mathfrak{f}\mathfrak{p}_u y = \sum_{r=0}^{p^n-1} c_r^p u^{pr} - \sum_{h=0}^{p^{n-1}-1} c_{hp} u^{hp}.$$

Um den rechtsstehenden Ausdruck auszuwerten, zerspalten wir y folgendermaßen:

$$y = \sum_{\nu=0}^{n} s_\nu; \qquad s_\nu = \sum_{\substack{t=1\\ p\nmid t}}^{p^{n-\nu}-1} c_{tp^\nu} u^{tp^\nu} \quad (\nu = 0, \ldots, n-1), \qquad s_n = c_0.$$

Wir fassen also die $c_r u^r$ nach der in r steckenden p-Potenz zusammen. Dann geht ($\mathfrak{G}$) über in

$$(\mathfrak{H}) \qquad \beta_0 = (s_0 + \cdots + s_{n-1} + s_n)^p - s_1 - \cdots - s_n = (s_0^p - s_1) + (s_1^p - s_2) + \cdots$$
$$+ (s_{n-2}^p - s_{n-1}) + (s_{n-1}^p + s_n^p - s_n).$$

β_0 liegt aber in k. Wir sehen also, daß man y nicht ganz beliebig vorschreiben darf, sondern daß wir darauf achten müssen, daß bei Entwicklung der rechten Seite von ($\mathfrak{H}$) nach Potenzen von u ein Element von k erscheint. $s_{n-1}^p + s_n^p - s_n = \wp c_0 + s_{n-1}^p$ liegt schon in k, aber die übrigen Glieder $s_\nu^p - s_{\nu+1}$ $(\nu = 0, 1, \ldots, n-2)$ enthalten u-Potenzen mit genau durch $p^{\nu+1}$ teilbarem Exponenten, sie müssen also alle verschwinden. Das heißt

$$s_0^p = s_1, \quad s_1^p = s_2, \ldots, \quad s_{n-2}^p = s_{n-1},$$
$$\beta_0 = \wp c_0 + s_{n-1}^p$$

oder

$$\beta_0 = \wp c_0 + s_0^{p^n} = \wp c_0 + \sum_{\substack{t=1\\ p\nmid t}}^{p^n-1} c_t^{p^n} \alpha^t, \qquad \text{w. z. b. w.}$$

Wir haben damit T. Satz 8 auf zyklische p-Algebren vom Grad p^n übertragen. Dagegen macht die Übertragung des (mehr besagenden) Satzes 7 noch Schwierigkeiten. Ich hoffe, sie durch eine Verallgemeinerung meiner Normierung [3]) für p^2 auf p^n beheben zu können.

---

[2]) Veröffentlicht in: O. Teichmüller, p-Algebren, Deutsche Mathematik 1 (1936), Satz 7. Zitiert mit T.

[3]) O. Teichmüller, Multiplikation zyklischer Normalringe, Deutsche Mathematik 1 (1936), § 15: Zyklische Normalringe vom Rang p^2.

Eingegangen 29. August 1936