Unverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p.

Von *Hermann Ludwig Schmid* und *Ernst Witt* in Göttingen.

K sei ein algebraischer Funktionenkörper einer Unbestimmten vom Geschlecht g über einem algebraisch abgeschlossenen Konstantenkörper k der Charakteristik p. In einer kürzlich erschienenen Arbeit von H. Hasse und E. Witt [1]) wurde folgendes Ergebnis gewonnen:

Es existieren über K genau γ linear unabhängige zyklische Erweiterungskörper p-ten Grades, wobei γ als Rang einer gewissen invarianten Matrix eine der Zahlen 0 bis g ist.

Ist speziell k absolut algebraisch, so besagt dieses Resultat, wie wir zeigen werden: Es gibt genau p^γ Divisorenklassen C von K mit $C^p = 1$.

Wir verallgemeinern in der vorliegenden Arbeit diese Ergebnisse auf beliebigen Grad p^n $(n \geqq 1)$. Neben dem selbständigen Interesse, welches das vergleichende Studium der unverzweigten abelschen Körper einerseits und der Struktur der Divisorenklassengruppe endlicher Ordnung andererseits besitzt, hoffen wir, damit vielleicht einen kleinen Beitrag zur Lösung der Riemannschen Vermutung in Funktionenkörpern beliebigen Geschlechtes zu geben. Die Methode unserer Untersuchung entnehmen wir einer eben erschienenen Arbeit von E. Witt [2]). Wir gelangen zu folgenden Hauptsätzen:

I. *Der größte unverzweigte abelsche Erweiterungskörper vom Exponenten p^n über K hat den Grad $p^{n\gamma}$ und seine Gruppe ist vom Typus $(p^n, p^n, \ldots, p^n)$.* Dabei ist γ die oben erwähnte Zahl.

II. *Ist speziell k absolut algebraisch, so gibt es $p^{n\gamma}$ Divisorenklassen C von K mit $C^{p^n} = 1$. Die Gruppe dieser C ist vom Typus $(p^n, p^n, \ldots, p^n)$.*

Schließlich bemerken wir, daß γ genau dann kleiner als g ist, wenn es ein totales Differential in K (d. h. ein Differential einer Funktion aus K) gibt, das überall endlich ist — im klassischen Fall haben bekanntlich totale Differentiale stets Pole.

1. A sei eine n-reihige Matrix, b ein n-gliedriger Vektor aus einem algebraisch abgeschlossenen Körper k der Charakteristik p. Wir behaupten folgenden Satz:

---

[1]) H. Hasse und E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p, Mh. Math. Phys. **43** (1936). — Diese Arbeit zitieren wir mit H.-W.

[2]) 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.

Das Gleichungssystem

(1) $$Ax^p - x = b$$

hat stets eine Lösung.

Beweis. Simultane Transformationen $\bar{A} = SAS^{-p}$, $\bar{x} = Sx$, $\bar{b} = Sb$ mit einer regulären Matrix S aus k führen (1) in

(1a) $$\bar{A}\bar{x}^p - \bar{x} = \bar{b}$$

über[3]). Nach H.-W. kann durch passende Wahl von S stets erreicht werden, daß $\bar{A}$ oberhalb der Hauptdiagonale lauter Nullen hat. Man sieht sofort, daß sich $\bar{x}_1, \ldots, \bar{x}_n$ durch Auflösung von algebraischen Gleichungen so bestimmen lassen, daß $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$ das Gleichungssystem (1 a) befriedigt.

2. Nun sei K ein algebraischer Funktionenkörper einer Unbestimmten über einem algebraisch abgeschlossenen Konstantenkörper k der Charakteristik p. K habe das Geschlecht g.

An jeder Primstelle $\mathfrak{p}$ sei ein Element $\gamma^{\mathfrak{p}}$ aus der $\mathfrak{p}$-adischen Erweiterung $K_{\mathfrak{p}}$ vorgegeben, und zwar sollen unter diesen Elementen nur für endlich viele Stellen $\mathfrak{p}$ Hauptteile in der Entwicklung auftreten. Unter diesen Voraussetzungen beweisen wir den Satz:

Die Gleichungen

(2) $$\xi + \wp\xi^{\mathfrak{p}} = \gamma^{\mathfrak{p}}$$

lassen sich mit Elementen $\xi^{\mathfrak{p}}$ aus $K_{\mathfrak{p}}$ und einem Element ξ aus K lösen.

Beweis. Wir dürfen jedes $\gamma^{\mathfrak{p}}$ um dasselbe Element α aus K abändern. Diese Abänderungsmöglichkeit benutzen wir, um die $\gamma^{\mathfrak{p}}$ geeignet zu normieren.

Es sei $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ wie in H.-W. ein reguläres Primdivisorensystem, d. h. $\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g) = 1$. Für eine Primstelle $\mathfrak{p} \neq \mathfrak{p}_i$, für welche $\gamma^{\mathfrak{p}}$ den Nenner $\mathfrak{p}^r$ $(r > 0)$ hat, können wir ein α aus K so bestimmen, daß $\gamma^{\mathfrak{p}} - \alpha$ höchstens den Nenner $\mathfrak{p}^{r-1}$ hat und im übrigen nur die Hauptteile von $\gamma^{\mathfrak{p}_i} - \alpha$ $(i = 1, \ldots, g)$ verändert werden. Weil nämlich

$$\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}^r) - \dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}^{r-1}) = 1$$

ist, so gibt es ein Element α aus K, welches bei $\mathfrak{p}$ den genauen Nenner $\mathfrak{p}^r$ mit einem beliebig vorgeschriebenen Anfangskoeffizienten hat und sonst nur noch Pole an den Stellen $\mathfrak{p}_i$ besitzt. Nach dieser schrittweisen Abänderung besitzen die $\gamma^{\mathfrak{p}}$ höchstens noch an den Stellen $\mathfrak{p}_i$ $(i = 1, \ldots, g)$ Pole.

Hat $\gamma^{\mathfrak{p}_i}$ den Nenner $\mathfrak{p}_i^{r_i}$ $(r_i > 1)$, so können wir $\gamma^{\mathfrak{p}_i}$ wieder um ein Element α aus K so abändern, daß $\gamma^{\mathfrak{p}_i} - \alpha$ einen kleineren Nenner erhält, während sich an den Stellen $\mathfrak{p}_j$ $(j \neq i)$ die Hauptteile höchstens in den Gliedern erster Ordnung verändern und $\gamma^{\mathfrak{p}} - \alpha$ $(\mathfrak{p} \neq \mathfrak{p}_1, \ldots, \mathfrak{p}_g)$ nach wie vor keine Nenner hat. Wegen

$$\dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}_i^{r_i}) - \dim(\mathfrak{p}_1 \cdots \mathfrak{p}_g \mathfrak{p}_i^{r_i-1}) = 1$$

gibt es nämlich ein Element α aus K, das an der Stelle $\mathfrak{p}_i$ den genauen Nenner $\mathfrak{p}_i^{r_i}$ mit passendem Anfangskoeffizenten besitzt und sonst höchstens noch an den Stellen $\mathfrak{p}_j$ $(j \neq i)$ Pole erster Ordnung hat.

---

[3]) Unter S^p verstehen wir die Matrix, die aus S durch Potenzierung aller Elemente mit p entsteht. S^p ist also nicht etwa die p-te Potenz im Sinne des Matrizenprodukts; diese wird gar nicht vorkommen.

Damit haben wir erreicht, daß die neuen $\gamma^{\mathfrak{p}_i}$ $(i = 1, \ldots, g)$ höchstens den Nenner $\mathfrak{p}_i$ haben, während die übrigen $\gamma^{\mathfrak{p}}$ $(\mathfrak{p} \neq \mathfrak{p}_i)$ ganz sind.

Es sei $\pi_1, \ldots, \pi_g$ ein System von Primelementen an den Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_{\mathfrak{p}}$. Nach H.-W. existieren Elemente $v_1, \ldots, v_g$ aus K, welche die Entwicklungen

$$v_j = \frac{e_{ij}}{\pi_i^p} - \frac{a_{ij}}{\pi_i} + \cdots \qquad (i, j = 1, \ldots, g) \tag{3}$$

haben und an den übrigen Stellen ganz sind. Weiter sei

$$\gamma^{\mathfrak{p}_i} = \frac{b_i}{\pi_i} + \cdots$$

und $x = (x_1, \ldots, x_g)$ eine Lösung der Matrizengleichung

$$Ax^p - x = b,$$

wobei $A = (a_{ij})$ und $b = (b_i)$ gesetzt ist. Bilden wir das Element

$$\xi = \sum_{j=1}^{g} v_j x_j^p$$

aus K, so wird $\gamma^{\mathfrak{p}_i} + \xi + \wp \frac{x_i}{\pi_i}$ ganz. Für die übrigen Stellen $\mathfrak{p} \neq \mathfrak{p}_i$ bleibt $\gamma^{\mathfrak{p}} + \xi$ ganz. Also ist in jedem Falle

$$\gamma^{\mathfrak{p}} + \xi = \wp \xi^{\mathfrak{p}}.$$

3. Wir betrachten im Sinne der Arbeit von E. Witt[2]) Vektoren $(\alpha_1, \ldots, \alpha_n)$ mit Elementen aus K. Es handelt sich also nicht etwa um gewöhnliche lineare Vektoren; diese werden von nun an nicht mehr vorkommen. Wir nennen einen solchen Vektor **zerfallend,** wenn

$$(\alpha_1, \ldots, \alpha_n) = \wp(\beta_1, \ldots, \beta_n)$$

mit Elementen $\beta_1, \ldots, \beta_n$ aus K ist. Wir nennen $(\alpha_1, \ldots, \alpha_n)$ **unverzweigt,** wenn an jeder Stelle

$$(\alpha_1, \ldots, \alpha_n) = \wp(\beta_1^{\mathfrak{p}}, \ldots, \beta_n^{\mathfrak{p}})$$

mit Elementen $\beta_1^{\mathfrak{p}}, \ldots, \beta_n^{\mathfrak{p}}$ aus $K_{\mathfrak{p}}$ ist. Es gilt folgender

Erweiterungssatz. *Jeder unverzweigte Vektor* $(\alpha_1, \ldots, \alpha_{n-1})$ *läßt sich zu einem unverzweigten Vektor* $(\alpha_1, \ldots, \alpha_{n-1}, \xi)$ *fortsetzen.*

Beweis. Nach Voraussetzung ist für jede Stelle $\mathfrak{p}$

$$(\alpha_1, \ldots, \alpha_{n-1}) = \wp(\beta_1^{\mathfrak{p}}, \ldots, \beta_{n-1}^{\mathfrak{p}}).$$

Man sieht sofort durch Induktion nach n: An denjenigen Stellen, an denen die α_ν ganz sind, müssen auch die $\beta_\nu^{\mathfrak{p}}$ ganz sein. Das Gleichungssystem

$$(\alpha_1, \ldots, \alpha_{n-1}, \xi) = \wp(\beta^{\mathfrak{p}}, \ldots, \beta_{n-1}^{\mathfrak{p}}, \xi^{\mathfrak{p}})$$

ist gleichwertig mit einem System

$$\xi - \wp \xi^{\mathfrak{p}} = \gamma^{\mathfrak{p}},$$

wo die $\gamma^{\mathfrak{p}}$ ganz rational von den α_ν und $\beta_\nu^{\mathfrak{p}}$ abhängen, folglich nur für endlich viele Stellen $\mathfrak{p}$ Hauptteile besitzen. In 2 haben wir die Lösbarkeit eines solchen Systems schon nachgewiesen.

4. Bezeichnen wir zerfallende bzw. unverzweigte Vektoren der Länge n mit $\mathfrak{z}_n$ bzw. $\mathfrak{u}_n$, so folgt, ähnlich wie in der Kummerschen Theorie, daß der Gruppenindex $(\mathfrak{u}_n : \mathfrak{z}_n)$ gleich dem Grad des größten abelschen unverzweigten Körpers vom Exponenten p^n ist.

Für die Matrix $A = (a_{ij})$ aus (3) sei γ der Rang von $AA^p \cdots A^{p^{g-1}}$. In H.-W. wurde festgestellt, daß der größte abelsche unverzweigte Körper vom Exponenten p den Grad p^γ hat. Wir behaupten hier folgenden Satz:

Der größte abelsche unverzweigte Körper vom Exponenten p^n hat den Grad $p^{n\gamma}$.

Beweis. Es sei A eine Gruppe und B eine Untergruppe. T sei eine homomorphe Abbildung, bei welcher genau die Untergruppen A_1 bzw. B_1 in 1 übergehen mögen. Dann gilt

$$(A : B) = (TA : TB) \cdot (A_1 : B_1).$$

Dieses gruppentheoretische Prinzip wenden wir auf $(\mathfrak{u}_n : \mathfrak{z}_n)$ an. Unter T verstehen wir Weglassung der letzten Komponente. Dabei geht nach unserem Erweiterungssatz $\mathfrak{u}_n$ in jeden beliebigen Vektor $\mathfrak{u}_{n-1}$ über; es ist klar, daß dabei $\mathfrak{z}_n$ in jeden beliebigen Vektor $\mathfrak{z}_{n-1}$ übergeht. Streichen wir bei denjenigen Vektoren, die bei unserer Abbildung in Null übergehen, die vorderen $n-1$ Nullen, so entstehen gerade die Gruppen $\mathfrak{u}_1$ bzw. $\mathfrak{z}_1$. Also gilt

$$(\mathfrak{u}_n : \mathfrak{z}_n) = (\mathfrak{u}_{n-1} : \mathfrak{z}_{n-1}) \cdot (\mathfrak{u}_1 : \mathfrak{z}_1). \tag{4}$$

Nach H.-W. ist $(\mathfrak{u}_1 : \mathfrak{z}_1) = p^\gamma$. Durch Induktion sei schon gezeigt, daß $(\mathfrak{u}_{n-1} : \mathfrak{z}_{n-1}) = p^{(n-1)\gamma}$ ist. Aus (4) folgt dann

$$(\mathfrak{u}_n : \mathfrak{z}_n) = p^{n\gamma},$$

w. z. b. w.

5. Wir beweisen folgende **Hauptsätze:**

I. *Die Gruppe $\mathfrak{A}_n$ des größten abelschen unverzweigten Körpers vom Exponenten p^n über K ist direktes Produkt von zyklischen Gruppen der Ordnung p^n.*

II. *Ist speziell k absolut algebraisch, so hat die Gruppe der Divisorenklassen vom Exponenten p^n den Grad $p^{n\gamma}$ und ist Produkt von γ zyklischen Gruppen der Ordnung p^n.*

Wir schicken folgende allgemeine gruppentheoretische Bemerkung voraus: Jede abelsche Gruppe $\mathfrak{A}$ mit endlich vielen Erzeugenden ist als freie abelsche Gruppe mit den Erzeugenden

$$x_1, \ldots, x_r; \quad y_1, \ldots, y_s; \quad z_1, \ldots, z_t$$

und den definierenden Relationen

$$y_i^{p^{\nu_i}} = 1, \quad z_i^{e_i} = 1 \qquad (e_i \not\equiv 0 \bmod p)$$

darstellbar. Die Elemente x_i sind von unendlicher Ordnung. In diesen Bezeichnungen ist die

Ordnung der größten Faktorgruppe $\mathfrak{A}_1$ vom Exponenten p gleich

$$p^{r+s}$$

und die

Ordnung der größten Faktorgruppe $\mathfrak{A}_n$ vom Exponenten p^n gleich

$$p^{nr + \sum\limits_{\nu_i \geqq n} n + \sum\limits_{\nu_i < n} \nu_i}. \tag{5}$$

Beweis von **I.** $\mathfrak{A} = \mathfrak{A}_n$ sei die galoissche Gruppe des größten abelschen unverzweigten Körpers vom Exponenten p^n. Es folgt $r = 0$ und $t = 0$ und alle $\nu_i \leqq n$. Da $\mathfrak{A}_1$ die Ordnung p^γ hat, ist $s = \gamma$. Da $\mathfrak{A}_n$ die Ordnung $p^{n\gamma}$ hat, folgt $\nu_i \geqq n$, also alle $\nu_i = n$, w. z. b. w.

Beweis von **II.** Es sei $K = k(x, y)$ mit der erzeugenden Gleichung $f(x, y) = 0$. Ferner sei

$$(\alpha_1^{(i)}, \ldots, \alpha_n^{(i)}) \qquad (i = 1, \ldots, p^{n\gamma})$$

ein Vertretersystem der unverzweigten Vektoren modulo den zerfallenden Vektoren. k' sei ein endlicher Körper, der

1. die Koeffizienten von f

2. die Koeffizienten von $\alpha_k^{(i)}$ in ihrer Darstellung als rationale Ausdrücke in x und y

enthält. Wir setzen $K' = k'(x, y)$. K_n' sei der größte abelsche unverzweigte Körper vom Exponenten p^n über K'. Dann ergeben sich die in nachstehender Zeichnung angeführten Körper.

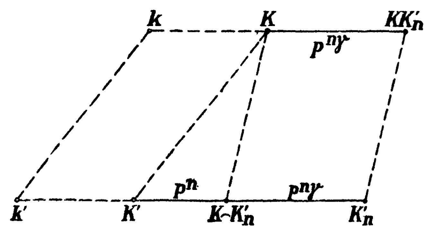

Fig. 1.

Dabei ist das Kompositum KK_n' der größte abelsche unverzweigte Körper vom Exponenten p^n über K und der Durchschnitt $K \frown K_n'$ der größte unverzweigte Körper, der aus K' durch Konstantenerweiterung entsteht; er hat über K' den Grad p^n.

Jetzt sei $\mathfrak{A}$ die Divisorenklassengruppe von K', also $r = 1$ und daher $s = \gamma$. Nach der Klassenkörpertheorie hat $\mathfrak{A}_1$ die Ordnung $p^{\gamma+1}$ und $\mathfrak{A}_n$ die Ordnung $p^{n(\gamma+1)}$ [4]). Ein Vergleich mit (5) ergibt $\nu_i \geqq n$. Daher wird die in $\mathfrak{A}$ größte Untergruppe $\mathfrak{U}_n$ vom Exponenten p^n von den Elementen $y_i^{\nu_i - n}$ erzeugt. $\mathfrak{U}_n$ hat die Ordnung $p^{n\gamma}$ und ist vom Typus $(p^n, p^n, \ldots, p^n)$.

Nun kann $\mathfrak{U}_n$ bei Erweiterung von k' zu k nicht größer werden. Einerseits läge nämlich jede etwa neu hinzukommende Divisorenklasse schon in einer endlichen Konstantenerweiterung von K'. Andererseits erfüllt auch eine endliche Erweiterung k'' von k' die an k' gestellten Forderungen und führt daher zur selben Anzahl $p^{n\gamma}$. Es kann also keine neue Divisorenklasse hinzukommen. Also ist $\mathfrak{U}_n$ gleich der gesuchten Gruppe in K.

Insbesondere ist damit für $n = 1$ die in der Einleitung erwähnte Ergänzung der Arbeit H.-W. hinsichtlich Divisorenklassen der Ordnung p bewiesen.

6. Wir beweisen den Satz:

Es gibt $g - \varrho$ linear unabhängige überall endliche totale Differentiale in K, wobei ϱ der Rang der Matrix $A = (a_{ij})$ ist.

Es sei $d\alpha$ ein totales überall endliches Differential in K. Wir dürfen α additiv um eine p-te Potenz aus K abändern. Wir zeigen dann, daß wir infolge dieser Abänderungsmöglichkeit α stets in die Form

$$(6) \qquad \alpha = \sum_{j=1}^{g} c_j v_j \qquad (c_j \text{ aus } k)$$

mit den in (3) eingeführten Elementen v_j bringen können.

---

[4]) E. Witt, Der Existenzsatz für abelsche Funktionenkörper, Journ. f. Math. **173** (1935).

Zunächst beseitigen wir analog wie oben in 2 die Hauptteile von α an den Stellen $\mathfrak{p} \neq \mathfrak{p}_i$ auf Kosten der Hauptteile an den Stellen $\mathfrak{p}_i$ $(i = 1, \ldots, g)$. Dann sorgen wir dafür, daß α höchstens den Nenner $(\mathfrak{p}_1 \cdots \mathfrak{p}_g)^p$ hat. Weil $d\alpha$ keine Hauptteile besitzt, muß an den Stellen $\mathfrak{p}_i$ des regulären Systems

$$\alpha \equiv \frac{c_i}{\pi_i^p} \bmod \mathfrak{p}_i^0$$

sein. Dann hat aber die Differenz

$$\alpha - \sum_{j=1}^{g} c_j v_j$$

höchstens den Nenner $\mathfrak{p}_1 \cdots \mathfrak{p}_g$, ist also konstant. Also können wir α tatsächlich in die Form (6) bringen.

Damit nun

$$\frac{d\alpha}{d\pi_i} = \frac{d}{d\pi_i} \sum_j c_j v_j \equiv \sum_j \frac{a_{ij} c_j}{\pi_i^2} \bmod \mathfrak{p}_i^0$$

ganz ist, muß

$$\sum_{j=1}^{g} a_{ij} c_j = 0$$

sein. Dies trifft für $g - \varrho$ unabhängige α zu.

Verschiedene α von der Form (6) liefern aber verschiedene Differentiale. Denn aus $d\alpha = 0$ folgt $\alpha = \beta^p$ mit β aus K[4]). β hat dann höchstens den Nenner $\mathfrak{p}_1 \cdots \mathfrak{p}_g$, ist also konstant; also ist auch α konstant und dann nach (6) notwendig $\alpha = 0$.

Die in der Einleitung erwähnte Tatsache ergibt sich daraus, daß für γ als Rang von $AA^p \cdots A^{p^{g-1}}$ stets $\gamma \leqq \varrho$ gilt und daß aus $\varrho = g$ auch $\gamma = g$ folgt.

Eingegangen 29. August 1936.