Math. Z. 117, 157 – 163 (1970)

Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik

PETER ROQUETTE

Herrn Helmut Wielandt zum 60. Geburtstag am 19. 12. 1970 gewidmet

§ 1. Problemstellung

Es sei $F|K$ ein algebraischer Funktionenkörper einer Variablen mit algebraisch abgeschlossenem Konstantenkörper K der Charakteristik $p \geqq 0$. Wir setzen voraus, daß F ein Geschlecht

$$g \geqq 2$$

besitzt. Es ist wohlbekannt, daß dann die Automorphismengruppe G von $F|K$ *endlich* ist. Im Falle $p=0$ wurde dies von Hurwitz [5] bewiesen, während der Fall $p>0$ von H. L. Schmid [8] behandelt wurde. Es entsteht die Frage nach einer Abschätzung für die Ordnung von G.

Im Falle $p=0$ hat Hurwitz selbst in seiner oben zitierten Arbeit eine Abschätzung für die Ordnung $|G|$ gegeben, nämlich

$$|G| \leqq 84(g-1) \quad (\text{falls } p=0).$$

Diese Abschätzung ist scharf, denn der durch die homogene Gleichung

$$x^3 y + y^3 z + z^3 x = 0$$

definierte Funktionenkörper $F = K(x/z, y/z)$ besitzt das Geschlecht 3, und seine Automorphismengruppe G ist isomorph zur projektiven Gruppe $PSL(2, 7)$ der Ordnung 168. Vgl. dazu etwa Burnside [1], Chap. XIX, § 303.

Im Falle $p>0$ liegen die Verhältnisse zunächst anders. Schon die Beispiele von H. L. Schmid [8] zeigen, daß eine Abschätzung vom Hurwitzschen Typus für $p>0$ sicherlich nicht allgemein richtig ist. Eine nur von g und p abhängige Schranke für $|G|$ könnte man im Prinzip der Arbeit [6] von Iwasawa und Tamagawa entnehmen, jedoch ist diese viel zu grob und spiegelt nicht die wirklichen Verhältnisse wider.

In dieser Note wollen wir die Frage behandeln, unter welchen Voraussetzungen die Hurwitzsche Abschätzung auch im Falle $p>0$ richtig ist. Nach allgemeinen mathematischen Prinzipien ist zu erwarten, daß das sicherlich dann der Fall ist, wenn die Charakteristik p groß genug ist. Es bleibt zu präzisieren, was in diesem Zusammenhang unter „groß" zu verstehen ist. Wir werden den folgenden Satz beweisen:

Satz 1. *Die Hurwitzsche Abschätzung*

$$|G| \leqq 84(g-1)$$

ist richtig, falls $p=0$ *oder*

$$p > g+1;$$

ausgenommen ist dabei nur der Fall des durch die inhomogene Gleichung

$$y^2 = x^p - x$$

definierten hyperelliptischen Funktionenkörpers $F = K(x, y)$. *Im Ausnahmefall ist*

$$p = 2g+1, \quad |G| = 2p(p^2-1).$$

Es ist zu vermuten, daß die bei Charakteristik $p>0$ auftretenden Anomalien, welche die Gültigkeit der Hurwitzschen Ungleichung zerstören, nur in sehr speziellen Fällen auftreten. Insbesondere muß dann das Geschlecht g in bezug auf die Charakteristik p gewissen Kongruenzrelationen genügen, wenn man einmal vom hyperelliptischen Falle absieht. Eine genauere Klärung dieses Sachverhalts wäre sehr zu begrüßen; in diesem Sinne ist Satz 1 nur als ein vorläufiges Ergebnis in dieser Richtung zu betrachten.

§ 2. Der Beweisansatz

Ist $\mathfrak{p}$ eine Stelle von F, so bezeichnen wir mit $G(\mathfrak{p})$ den Stabilisator von $\mathfrak{p}$ in der Automorphismengruppe G. Man kann $G(\mathfrak{p})$ als die Verzweigungsgruppe von $\mathfrak{p}$ über dem Fixkörper F^G von G in F auffassen. Die Ordnung $|G(\mathfrak{p})|$ ist gleich der Verzweigungsordnung $e(\mathfrak{p})$ von $\mathfrak{p}$ über F^G. Wenn $e(\mathfrak{p})$ zu p teilerfremd ist, so liegt reguläre (zahme) Verzweigung vor; dann ist $G(\mathfrak{p})$ zyklisch, und $\mathfrak{p}$ kommt in der Differente $\mathfrak{D}^G$ von $F|F^G$ mit der Vielfachheit $e(\mathfrak{p})-1$ vor. Insbesondere ist dies der Fall, wenn $p=0$; hierauf stützt sich der Hurwitzsche Beweis [5], der auf einer Abschätzung des Grades d^G von $\mathfrak{D}^G$ beruht. In der Tat ergibt eine Inspektion des Hurwitzschen Beweises aus dem Jahre 1892, daß er wörtlich gültig bleibt im Falle $p>0$, unter der Voraussetzung, daß $|G(\mathfrak{p})| \not\equiv 0 \bmod p$ für alle Stellen $\mathfrak{p}$ von F. Wir haben also den

Satz 2 (Hurwitz). *Wenn* $|G(\mathfrak{p})| \not\equiv 0 \bmod p$ *für alle Stellen* $\mathfrak{p}$ *von* F, *so gilt*

$$|G| \leqq 84(g-1).$$

Demnach ergibt sich der Satz 1 unmittelbar aus dem folgenden

Satz 3. *Es sei* $p>0$. *Wenn es eine Stelle* $\mathfrak{p}$ *von* F *gibt mit* $|G(\mathfrak{p})| \equiv 0 \bmod p$, *so ist*

$$p \leqq g+1;$$

ausgenommen ist dabei nur der Fall des durch die Gleichung

$$y^2 = x^p - x$$

definierten hyperelliptischen Funktionenkörpers $F = K(x, y)$.

Der Ausnahmefall wird in § 4, anschließend an den Beweis von Satz 3, diskutiert werden.

§ 3. Beweis von Satz 3

Es sei $\mathfrak{p}$ eine Stelle von F mit $|G(\mathfrak{p})| \equiv 0 \bmod p$. Nach dem Satz von Sylow [10] gibt es eine Untergruppe $H \subset G(\mathfrak{p})$ der Ordnung p. Es sei F^H der Fixkörper von H und g^H sein Geschlecht; ferner sei d^H der Grad der Differente $\mathfrak{D}^H$ von $F|F^H$. Dann gilt die Hurwitzsche Geschlechtsformel

$$2g-2=(2g^H-2)\,p+d^H. \tag{1}$$

Vgl. dazu etwa Hasse [4], S. 462. Es handelt sich zunächst darum, den Differentengrad d^H abzuschätzen.

Im folgenden durchlaufe $\mathfrak{q}$ die Menge der über F^H verzweigten Stellen von F. Es gibt mindestens eine solche Verzweigungsstelle, nämlich $\mathfrak{p}$. (Denn wegen $H \subset G(\mathfrak{p})$ wird $\mathfrak{p}$ durch H festgelassen.) Der Differentengrad d^H setzt sich nun zusammen aus Beiträgen $d^H(\mathfrak{q})$, die den Verzweigungsstellen $\mathfrak{q}$ entsprechen:

$$d^H=\sum_{\mathfrak{q}} d^H(\mathfrak{q}).$$

Hierbei stellt sich $d^H(\mathfrak{q})$ gemäß der Hilbertschen Verzweigungstheorie wie folgt dar:

Da H die Primzahlordnung p besitzt, so ist $\mathfrak{q}$ über F^H *voll* verzweigt, d.h. H ist die Verzweigungsgruppe von $\mathfrak{q}$ über F^H. Allgemein bezeichnet man mit $H_i(\mathfrak{q})$ die i-te Verzweigungsgruppe von $\mathfrak{q}$ in H, bestehend aus denjenigen $\sigma \in H$, für welche

$$w_{\mathfrak{q}}(\sigma\pi-\pi) \geqq i+1,$$

unter π ein Primelement für $\mathfrak{q}$ verstanden. ($w_{\mathfrak{q}}$ bezeichnet die zu $\mathfrak{q}$ gehörige additive, normierte Bewertung von F.) Die $H_i(\mathfrak{q})$ bilden eine absteigende Reihe von Untergruppen von H, die sich auf 1 zusammenziehen. Da nun H die Primzahlordnung p besitzt, so gibt es einen Index $m=m(\mathfrak{q})$ derart, daß

$$H_m(\mathfrak{q})=H, \qquad H_{m+1}(\mathfrak{q})=1.$$

Es ist dann

$$w_{\mathfrak{q}}(\sigma\pi-\pi)=m(\mathfrak{q})+1$$

für jeden Automorphismus $\sigma \neq 1$ aus H. Die Hilbertsche Verzweigungstheorie lehrt nun, daß

$$d^H(\mathfrak{q})=(m(\mathfrak{q})+1)\,(p-1).$$

Vgl. z.B. [9], S. 72, Prop. 4.

Hierbei ist

$$m(\mathfrak{q}) \geqq 1$$

weil nämlich irreguläre Verzweigung vorliegt.

Es ergibt sich:

$$d^H=\sum_{\mathfrak{q}}(m(\mathfrak{q})+1)\,(p-1) \geqq 2r(p-1),$$

wobei r die Anzahl der Verzweigungsstellen $\mathfrak{q}$ bedeutet. Zusammen mit der Geschlechtsformel (1) erhalten wir daraus:

$$2g-2 \geqq (2g^H-2)\,p+2r(p-1). \tag{2}$$

Wie bereits oben gesagt, ist dabei $r \geqq 1$, denn $\mathfrak{p}$ selbst ist verzweigt über F^H.

Wenn $g^H \geqq 1$, so ist $2g^H-2 \geqq 0$ und wir erhalten

$$2g-2 \geqq 2(p-1)$$
$$g \geqq p.$$

Nun sei $g^H=0$. Die Ungleichung (2) lautet jetzt:

$$2g-2 \geqq -2p+2r(p-1).$$

Wenn hierin $r \geqq 2$, so folgt

$$2g-2 \geqq -2p+4(p-1)$$
$$g+1 \geqq p.$$

Es bleibt also der Fall zu diskutieren, daß $r=1$, d.h. daß $\mathfrak{p}$ die *einzige* über F^H verzweigte Stelle ist. Es ist jetzt

$$\begin{aligned} d^H &= (m(\mathfrak{p})+1)(p-1) \\ 2g-2 &= -2p+(m(\mathfrak{p})+1)(p-1). \end{aligned} \tag{3}$$

Hieraus folgt zunächst $m(\mathfrak{p}) \geqq 2$, denn sonst wäre $m(\mathfrak{p})=1$ und aus (3) folgte $g=0$, was unserer eingangs angegebenen Voraussetzung widerspricht. Wenn $m(\mathfrak{p}) \geqq 3$, so folgt aus (3):

$$2g-2 \geqq -2p+4(p-1)$$
$$g+1 \geqq p.$$

Es bleibt also der Fall zu diskutieren, daß $m(\mathfrak{p})=2$. Nach (3) bedeutet das:

$$g=\frac{p-1}{2}.$$

Wegen $g^H=0$ ist F^H rational über K. Es sei y eine Erzeugende von F^H über K. Wir können und wollen y so wählen, daß y die Stelle $\mathfrak{p}$ als Pol besitzt. Da $\mathfrak{p}$ verzweigt ist über F^H, so ist $\mathfrak{p}$ die *einzige* Polstelle von y. Wir haben nun die folgende Situation:

(i) *F ist Galoissche Erweiterung p-ten Grades eines rationalen Funktionenkörpers $K(y)$.*

(ii) *Der Pol von y ist verzweigt in F, und zwar ist er die einzige Stelle, die in der Erweiterung $F|K(y)$ verzweigt ist.*

(iii) $g=\frac{p-1}{2}$.

Wir behaupten, daß in dieser Situation der in Satz 3 genannte Ausnahmefall vorliegt.

Aus (i) folgt: F ist Artin-Schreier-Erweiterung von $K(y)$. Das heißt: Es gibt eine Erzeugende x von $F|K(y)$ derart, daß

$$x^p - x = f(y) \in K(y).$$

Aus (ii) folgt: Die Artin-Schreier-Erzeugende x kann so gewählt werden, daß $f(y)$ nur einen einzigen Pol besitzt, nämlich den Pol von y. Das bedeutet: $f(y) \in K[y]$ ist ein Polynom in y. (Für die hier und im folgenden verwendeten Tatsachen über Artin-Schreier-Erweiterungen rationaler Funktionenkörper verweisen wir auf [4].) Außerdem kann angenommen werden, daß der Grad von $f(y)$ teilerfremd zu p ist.

Die Theorie der Artin-Schreier-Erweiterungen rationaler Funktionenkörper lehrt nun, daß sich das Geschlecht g von F durch die Formel

$$g = \frac{(\operatorname{grad}(f)-1)(p-1)}{2} \tag{4}$$

berechnet. Vergleich mit (iii) zeigt jetzt:

$$\operatorname{grad}(f) = 2.$$

Also ist f ein quadratisches Polynom:

$$f(y) = a y^2 + b y + c$$

mit $a, b, c \in K$ und $a \neq 0$.

Nach Ersetzung von y durch $\sqrt{a} \cdot y$ können wir annehmen, es sei $a = 1$. Nach weiterer Ersetzung von y durch $y + b/2$ können wir ferner annehmen, daß $b = 0$. Beachte, daß $p > 2$ zufolge (iii). Die definierende Relation für x über $K(y)$ lautet jetzt:

$$x^p - x = y^2 + c.$$

Es sei $\gamma \in K$ eine Lösung der Gleichung $\gamma^p - \gamma = c$. Wir ersetzen x durch $x - \gamma$ und erhalten somit eine Gleichung der Form

$$x^p - x = y^2$$

$$F = K(x, y).$$

Es liegt also tatsächlich der Ausnahmefall vor.

§ 4. Diskussion des Ausnahmefalles

Wir nehmen jetzt an, daß $F = K(x, y)$ gegeben ist durch die definierende Relation

$$y^2 = x^p - x. \tag{5}$$

Zunächst wollen wir das Geschlecht g von F bestimmen.

Wenn $p=2$, so besagt (5), daß $x=(y+x)^2$; also ist $F=K(y+x)$ rational und mithin $g=0$. Wenn $p>2$, so fassen wir F als Artin-Schreier-Erweiterung von $K(y)$ auf und entnehmen der bereits oben zitierten Formel (4), daß

$$g=\frac{p-1}{2}.$$

Unsere Voraussetzung $g\geqq 2$ besagt also $p\geqq 5$.

Wir wollen nun die Automorphismengruppe G von F bestimmen. F ist nach (5) eine quadratische Erweiterung des rationalen Funktionenkörpers $K(x)$, also hyperelliptisch. Folglich ist $K(y)$ der *einzige* rationale Teilkörper vom Index 2 in F; er wird erzeugt durch die Quotienten ganzer Differentiale von F (vgl. z.B. [2], Chap. IV, § 9). Insbesondere folgt: die Automorphismengruppe G von F bildet $K(x)$ auf sich ab, wird also dargestellt durch gebrochen lineare Transformationen der Form

$$x\to\frac{Ax+B}{Cx+D} \tag{6}$$

mit $A, B, C, D\in K$ und $AD-BC\neq 0$. Der Kern dieser Darstellung ist die Galoisgruppe von $F|K(x)$; diese besitzt die Ordnung 2. Bedeutet daher G_0 die Gruppe der von G in $K(x)$ induzierten Automorphismen, so ist

$$|G|=2\,|G_0|.$$

G_0 permutiert die in F verzweigten Stellen von $K(x)$. Aus (5) folgt, daß dies genau die Nullstellen und der Pol von x^p-x sind, d.h. die $p+1$ Stellen

$$x\to\infty,\quad x\to a\quad\text{mit}\quad a\in Z/p.$$

Hierbei bedeutet Z/p den in K enthaltenen Primkörper mit p Elementen.

Eine lineare Transformation der Form (6) permutiert genau dann die angegebenen $p+1$ Stellen, wenn $A, B, C, D\in Z/p$ (bis auf einen gemeinsamen Faktor, der herausgekürzt werden kann). Diese Automorphismen bilden die projektive Gruppe $PGL(2, p)$. Es folgt:

$$G_0\subset PGL(2, p).$$

Wir behaupten, daß hier das $=$-Zeichen steht. $PGL(2, p)$ wird erzeugt durch die Automorphismen

$$x\to x+1,\quad x\to-\frac{1}{x},\quad x\to ax$$

mit $0\neq a\in Z/p$. Es ist zu zeigen, daß jeder dieser erzeugenden Automorphismen in G_0 liegt; d.h. daß er sich fortsetzen läßt zu einem Automorphismus von F. Aus der definierenden Relation (5) entnimmt man nun unmittelbar, daß eine solche Fortsetzung in den einzelnen Fällen gegeben wird durch:

$$y\to y,\quad y\to\frac{y}{x^{(p+1)/2}},\quad y\to\sqrt{a}\cdot y.$$

Es gilt also in der Tat:

$$G_0 = PGL(2, p).$$

Also:

$$|G| = 2\,|G_0| = 2p(p^2-1).$$

§ 5. Bemerkung

Der bereits in § 1 erwähnte Funktionenkörper der durch

$$x^3 y + y^3 z + z^3 x = 0$$

gegebenen ebenen projektiven Kurve besitzt auch bei Primzahlcharakteristik $p \neq 2, 3, 7$ das Geschlecht 3, und seine Automorphismengruppe hat die Ordnung $168 = 84(3-1)$.

Literatur

1. Burnside, W.: Theory of groups of finite order, 2nd ed. Cambridge: Dover Publ. 1911.
2. Chevalley, C.: Introduction to the theory of algebraic functions of one variable. New York: Amer. Math. Soc. 1951.
3. Hasse, H.: Zahlentheorie, 2. Aufl. Berlin: Akademie-Verlag 1963.
4. – Theorie der relativ zyklischen algebraischen Funktionenkörper. Crelles J. **172**, 37–54 (1934).
5. Hurwitz, A.: Über algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. **41**, 403–442 (1893).
6. Iwasawa, K., Tamagawa, T.: On the group of automorphisms of a function field. J. Math. Soc. Japan **3**, 137–147 (1951); **4**, 100–101, 203–204 (1952).
7. Roquette, P.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers. Arch. der Math. **3**, 343–350 (1952).
8. Schmid, H. L.: Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. Crelles J. **179**, 5–15 (1938).
9. Serre, J. P.: Corps locaux. Paris: Hermann 1962.
10. Wielandt, H.: Ein Beweis für die Existenz der Sylowgruppen. Arch. der Math. **10**, 401–402 (1959).

Prof. Peter Roquette
Mathematisches Institut
der Universität
D-6900 Heidelberg

(Eingegangen am 25. Juni 1970)