Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik

Teil I: Eine Abschätzung der Ordnung der Automorphismengruppe

Von

HENNING STICHTENOTH

Einleitung. F sei ein algebraischer Funktionenkörper einer Variablen über einem algebraisch abgeschlossenen Körper K als Konstantenkörper. F habe die Charakteristik $p \geqq 0$ und das Geschlecht $g \geqq 2$. Dann ist die Automorphismengruppe G von F/K endlich.

Für $p = 0$ wurde die Endlichkeit von G von Hurwitz [4] gezeigt. In dieser Arbeit gab Hurwitz auch eine Abschätzung für die Ordnung von G an:

$$|G| \leqq 84(g-1) \quad (\text{bei } p = 0). \tag{0.1}$$

Diese Abschätzung ist scharf; es gibt Funktionenkörper der Charakteristik 0 von beliebig hohem Geschlecht, deren Automorphismengruppe die Ordnung $84(g-1)$ besitzt (Macbeath [7]).

H. L. Schmid [11] bewies die Endlichkeit von G im Fall $p > 0$, andere Beweise stammen von Iwasawa und Tamagawa [5] sowie von Rosenlicht [10]. Schmid gab für $p = 2$ Beispiele an, welche zeigen, daß die Abschätzung (0.1) bei Primzahlcharakteristik nicht allgemein gültig ist.

Nach Roquette [9] bleibt die Hurwitzsche Abschätzung (0.1) jedoch auch bei $p > 0$ unter der zusätzlichen Voraussetzung $g < p - 1$ richtig, abgesehen von einer Ausnahme. Diese Ausnahme tritt bei dem durch

$$y^p - y = x^2 \tag{0.2}$$

definierten Funktionenkörper $F = K(x, y)$ für $p \geqq 5$ auf. F hat das Geschlecht $g = \frac{1}{2}(p-1)$, seine Automorphismengruppe ist von der Ordnung $8g(g+1)(2g+1)$.

Mit denselben Mitteln wie bei Roquette läßt sich zeigen, daß die Abschätzung (0.1) auch noch für $g = p - 1$ gilt. Auch hier tritt jedoch bei $p \geqq 5$ wieder ein Ausnahmefall auf, nämlich der Körper $K(x, y)$ mit der definierenden Gleichung

$$y^p - y = x^3. \tag{0.3}$$

Seine Automorphismengruppe hat im Falle $p \equiv 1 \pmod 3$ die Ordnung $3g(g+1)$, im Fall $p \equiv -1 \pmod 3$ die Ordnung $3g(g+1)(g+2)$ (vgl. Stichtenoth [13], Satz 5 und 7).

In der vorliegenden Arbeit gebe ich eine Abschätzung für die Ordnung der Automorphismengruppe G eines algebraischen Funktionenkörpers einer Variablen vom Geschlecht $g \geqq 2$, dessen Konstantenkörper K algebraisch abgeschlossen ist und die Charakteristik $p > 0$ besitzt. Als wichtigstes Resultat beweise ich den

Hauptsatz. *Bis auf die unten angegebenen Ausnahmefälle läßt sich G abschätzen durch*

$$|G| < 16 \cdot g^4 .$$

Die Ausnahmen sind folgende: $F = K(x, y)$ mit der definierenden Relation[1])

$$y^{p^n} + y = x^{p^n+1}, \quad p^n \geqq 3 . \tag{0.4}$$

Hier gilt $g = \frac{1}{2} p^n(p^n - 1)$ und $|G| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$, d.h. $|G|$ ist etwas größer als $16 \cdot g^4$.

Die Idee zum Beweis des Hauptsatzes ist dieselbe wie bei Hurwitz [4] und bei Roquette [9]: Man betrachtet die Körpererweiterung F/F_G, wobei F_G der Fixkörper von G ist. Diese Erweiterung ist endlich und galoissch. Hat F_G das Geschlecht g_G, so besagt die Riemann-Hurwitzsche Geschlechtsformel (im folgenden zitiert als „Geschlechtsformel")

$$2g - 2 = |G|(2g_G - 2) + d . \tag{0.6}$$

d bedeutet dabei den Grad der Differente von F/F_G. Er hängt eng mit dem Verzweigungsverhalten der Stellen von F_G in F zusammen.

Wenn F_G nicht rational ist oder genügend viele Stellen in F/F_G verzweigen, liefert die Geschlechtsformel sehr schnell eine Abschätzung von $|G|$. Schwierigkeiten treten auf, wenn F_G rational ist und höchstens drei Stellen von F_G in F verzweigen. Es ist dann erforderlich, die Verzweigungsordnung e einer einzelnen Stelle $\mathfrak{p}$ von F in F/F_G abzuschätzen. e läßt sich deuten als Ordnung der Verzweigungsgruppe $G(\mathfrak{p}) = \{\sigma \in G \mid \sigma\mathfrak{p} = \mathfrak{p}\}$. Diese enthält als normale p-Sylowgruppe die erste Verzweigungsgruppe $G_1(\mathfrak{p})$.

In Satz 1 gebe ich eine Schranke für die Ordnung e_1 von $G_1(\mathfrak{p})$ an, nämlich

$$e_1 \leqq \frac{4p}{(p-1)^2} g^2 \quad (\text{falls } g \geqq p) . \tag{0.7}$$

---

[1]) LEOPOLDT [6] untersuchte die Automorphismengruppe des Fermatschen Funktionenkörpers $K(u, v)$, der definiert ist durch

$$u^k + v^k + 1 = 0, \quad k \geqq 4 . \tag{0.5}$$

Die Ordnung seiner Automorphismengruppe G liegt im allgemeinen in der Größenordnung $12 \cdot g$. Ausnahmen treten genau dann auf, wenn der Exponent k von der Form $p^n + 1$ ist. Dann ist die Ordnung von G größer als $16 \cdot g^4$, d.h. es muß der im Hauptsatz genannte Ausnahmefall vorliegen. Sind u, v Erzeugende des Fermatkörpers mit der Relation (0.5) und $k = p^n + 1$, so erhält man Erzeugende x, y welche (0.4) erfüllen, durch

$$x = \frac{b}{v - bu}, \quad y = ux - a .$$

Dabei sind a, b Elemente aus K mit der Eigenschaft

$$a^{p^n} + a = -1, \quad b^{p^n+1} = -1 .$$

Der Beweis dieser Abschätzung wird zurückgeführt auf die Bestimmung von $G_1(\mathfrak{p})$ im Spezialfall $F = K(x, y)$ mit der definierenden Gleichung

$$y^p - y = B(x), \tag{0.8}$$
$$B(x) \in K[x], \quad \operatorname{grad} B \geqq 2, \quad (p, \operatorname{grad} B) = 1.$$

$\mathfrak{p}$ bedeutet hier den Pol von x.

In Satz 2 wird die Ordnung e' von $G(\mathfrak{p})/G_1(\mathfrak{p})$ durch

$$e' \leqq 4g + 2 \tag{0.9}$$

abgeschätzt. Der Beweis des Hauptsatzes stützt sich dann im wesentlichen auf die Abschätzungen (0.7) und (0.9) sowie auf eine ausführliche Diskussion der Geschlechtsformel (0.6). Außerdem werden einzelne Tatsachen aus [13] benutzt.

In der demnächst erscheinenden Arbeit [13] werde ich eine Klasse von Funktionenkörpern untersuchen, die als Spezialfälle u.a. die Fälle (0.2), (0.3), (0.4) und (0.8) enthält. Dort werden insbesondere die Automorphismengruppen dieser Funktionenkörper explizit bestimmt.

Für die Anregung zu dieser Arbeit und viele wertvolle Hinweise bei ihrer Entstehung danke ich Herrn Prof Dr. P. Roquette sehr herzlich.

Bemerkung. Inzwischen wurde mir eine Arbeit von Singh[2]) bekannt, die sich mit demselben Thema befaßt. Singh gibt die Abschätzung

$$|G| \leqq \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right).$$

Für $p \leqq g \leqq \frac{1}{2}p^2$ ist diese Schranke etwas besser als die von mir gegebene, während sie für großes g schlechter wird, da sie das Geschlecht g in der 5. Potenz enthält.

1. Geschlechts- und Differentenformel. Grundlegend für die Abschnitte 2 und 3 sind die Riemann-Hurwitzsche Geschlechtsformel sowie der Zusammenhang zwischen der Differente einer Körpererweiterung und den höheren Verzweigungsgruppen der in dieser Erweiterung verzweigten Stellen. Diese Tatsachen sollen hier kurz zusammengestellt werden.

F^*/K sei ein algebraischer Funktionenkörper einer Variablen, K algebraisch abgeschlossen von der Charakteristik $p > 0$. Ist F/F^* eine endliche Körpererweiterung, so besteht zwischen den Geschlechtern g von F bzw. g^* von F^* die Beziehung

$$2g - 2 = [F : F^*] \cdot (2g^* - 2) + d. \tag{1.1}$$

Dabei ist d der Grad der Differente von F/F^* (vgl. Chevalley [1] S. 106, Kor. 2). d ist die Summe der Exponenten $d(\mathfrak{p})$, mit denen die in F/F^* verzweigten Stellen $\mathfrak{p}$ von F in der Differente dieser Erweiterung aufgehen. Die Formel (1.1) heißt Geschlechtsformel.

---

[2]) Balwant Singh, On the group of automorphisms of a function field of genus at least two. Die Arbeit wurde der Mathematischen Zeitschrift eingereicht.

Ab jetzt wird vorausgesetzt, daß F/F^* galoissch ist; U sei die zugehörige Galoisgruppe. $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ seien sämtliche Stellen von F^*, welche in F/F^* verzweigen; $\mathfrak{p}_j$ sei eine beliebige Fortsetzung von $\mathfrak{q}_j$ auf F $(1 \leqq j \leqq r)$, $e(\mathfrak{q}_j)$ die Verzweigungsordnung von $\mathfrak{p}_j$ über $\mathfrak{q}_j$ und $d(\mathfrak{q}_j)$ der Exponent von $\mathfrak{p}_j$ in der Differente von F/F^*. Weil F/F^* galoissch ist, hängen $e(\mathfrak{q}_j)$ bzw. $d(\mathfrak{q}_j)$ nur von $\mathfrak{q}_j$, nicht aber von der willkürlich gewählten Fortsetzung $\mathfrak{p}_j$ ab. Wegen der algebraischen Abgeschlossenheit des Konstantenkörpers treten keine Restklassengrade auf, und daher gibt es genau $|U|/e(\mathfrak{q}_j)$ verschiedene Fortsetzungen von $\mathfrak{q}_j$ auf F. Folglich läßt sich d ausdrücken durch

$$d = \sum_{j=1}^{r} \frac{|U|}{e(\mathfrak{q}_j)} d(\mathfrak{q}_j) = |U| \sum_{j=1}^{r} \frac{d(\mathfrak{q}_j)}{e(\mathfrak{q}_j)}. \tag{1.2}$$

Ich will nun den Exponenten $d(\mathfrak{p})$, mit dem eine Stelle $\mathfrak{p}$ von F in der Differente von F/F^* aufgeht, genauer bestimmen. Dazu betrachte ich die Reihe der Verzweigungsgruppen $U_i(\mathfrak{p})$ von $\mathfrak{p}$ in F/F^*. Diese sind folgendermaßen definiert:

$$U_0(\mathfrak{p}) = \{\sigma \in U \mid \sigma\mathfrak{p} = \mathfrak{p}\},$$
$$U_i(\mathfrak{p}) = \{\sigma \in U \mid \sigma\pi \equiv \pi (\mathrm{mod}\ \mathfrak{p}^{i+1})\} \quad \text{für} \quad i \geqq 1.$$

π ist dabei ein beliebiges Primelement für $\mathfrak{p}$ (Serre [12] S. 69f.). Es gilt

$$U_0(\mathfrak{p}) \supseteq U_1(\mathfrak{p}) \supseteq U_2(\mathfrak{p}) \supseteq \ldots,$$

und für genügend großes n ist $U_n(\mathfrak{p}) = 1$. Die Ordnung von $U_0(\mathfrak{p})$ ist gerade $e(\mathfrak{p})$, die Verzweigungsordnung von $\mathfrak{p}$ in F/F^*. Für $i \geqq 1$ sind die $U_i(\mathfrak{p})$ alle normal in $U_0(\mathfrak{p})$ und in $U_1(\mathfrak{p})$. Die erste Verzweigungsgruppe $U_1(\mathfrak{p})$ ist eine p-Gruppe, und $U_0(\mathfrak{p})$ ist semidirektes Produkt von $U_1(\mathfrak{p})$ mit einer zyklischen Gruppe H, deren Ordnung zu p teilerfremd ist (Serre [12] S. 75, Kor. 4). Insbesondere ist $U_0(\mathfrak{p})/U_1(\mathfrak{p})$ zyklisch von zu p teilerfremder Ordnung. $\mathfrak{p}$ heißt regulär verzweigt in F/F^*, falls $U_1(\mathfrak{p}) = 1$, andernfalls spricht man von irregulärer Verzweigung.

Der Exponent $d(\mathfrak{p})$ drückt sich mit Hilfe der Verzweigungsgruppen so aus (Serre [12] S. 72, Prop. 4):

$$d(\mathfrak{p}) = \sum_{i=0}^{\infty} (|U_i(\mathfrak{p})| - 1). \tag{1.3}$$

Diese Formel wird im folgenden als „Differentenformel" zitiert. Speziell bei regulärer Verzweigung besagt sie $d(\mathfrak{p}) = e(\mathfrak{p}) - 1$.

2. Die Gruppe $G(\mathfrak{p})$. In diesem Abschnitt ist F/K ein Funktionenkörper vom Geschlecht $g \geqq 1$. Hier werden elliptische Funktionenkörper also noch nicht ausgeschlossen. $\mathfrak{p}$ ist eine fest gewählte Stelle von F und $G(\mathfrak{p})$ die Gruppe aller Automorphismen von F/K, welche $\mathfrak{p}$ festlassen. Nach H. L. Schmid [11] und Iwasawa-Tamagawa [5] ist $G(\mathfrak{p})$ endlich. Ziel dieses Paragraphen ist es, die Ordnung $e = e(\mathfrak{p})$ von $G(\mathfrak{p})$ abzuschätzen.

F_0 sei der Fixkörper von $G(\mathfrak{p})$. Die Reihe der Verzweigungsgruppen von $\mathfrak{p}$ in F/F_0 bezeichne ich mit $G(\mathfrak{p}) = G_0(\mathfrak{p}) \supseteq G_1(\mathfrak{p}) \supseteq \ldots$, die zugehörigen Fixkörper mit F_0, $F_1, \ldots$, die Ordnung von $G_i(\mathfrak{p})$ mit e_i. Nach Abschnitt 1 ist e_1 die höchste Potenz

von p, welche in e aufgeht. Der Quotient e/e_1 werde mit e' bezeichnet. e_1 bzw. e' werden einzeln in Satz 1 bzw. Satz 2 abgeschätzt. Die hier gegebenen Schranken verbessern die schon von Iwasawa-Tamagawa gegebenen ([5] Theorem 1) und lassen sich nicht mehr verschärfen (siehe die Beispiele im Anschluß an Satz 1 und 2).

Satz 1. (a) *Ist F_1 nicht rational, so ist $e_1 \leqq g$.*

(b) *Ist F_1 rational und sind in F/F_1 außer $\mathfrak{p}$ noch weitere Stellen verzweigt, gilt* $e_1 \leqq \dfrac{p}{p-1} g$.

(c) *Ist F_1 rational und ist in F/F_1 nur $\mathfrak{p}$ verzweigt, so ist auch F_2 rational. In diesem Fall gilt* $e_1 \leqq \dfrac{4e_2}{(e_2-1)^2} g^2 \leqq \dfrac{4p}{(p-1)^2} g^2$.

Beweis. Ich betrachte die Erweiterung F/F_1 vom Grade e_1. Hat F_1 das Geschlecht g_1, so besagt die Geschlechtsformel (1.1):

$$2g - 2 = e_1(2g_1 - 2) + d. \tag{2.1}$$

Dabei bezeichnet d den Grad der Differente von F/F_1. Die Stelle $\mathfrak{p}$ ist in F/F_1 voll verzweigt, und da e_1 eine p-Potenz ist, haben die nullte und erste Verzweigungsgruppe von $\mathfrak{p}$ in F/F_1 die Ordnung e_1. Nach der Differentenformel (1.3) läßt sich demnach der Beitrag von $\mathfrak{p}$ zum Differentengrad abschätzen durch

$$d(\mathfrak{p}) \geqq 2e_1 - 2. \tag{2.2}$$

Im Fall (a) ist g_1 positiv. (2.1) und (2.2) ergeben sofort die Abschätzung

$$2g - 2 \geqq d \geqq d(\mathfrak{p}) \geqq 2e_1 - 2, \quad \text{also} \quad e_1 \leqq g.$$

Von jetzt an sei $g_1 = 0$. Dann vereinfacht sich (2.1) zu

$$2g - 2 = -2e_1 + d. \tag{2.3}$$

Im Fall (b) ist außer $\mathfrak{p}$ noch mindestens eine weitere Stelle $\mathfrak{q}$ von F_1 in F verzweigt. $e(\mathfrak{q})$ sei die Verzweigungsordnung von $\mathfrak{q}$, $d(\mathfrak{q})$ der Exponent einer Fortsetzung von $\mathfrak{q}$ in der Differente von F/F_1. Weil $e(\mathfrak{q})$ eine Potenz von p ist, folgt wieder aus der Differentenformel (1.3)

$$d(\mathfrak{q}) \geqq 2e(\mathfrak{q}) - 2.$$

(2.3) ergibt nun unter Beachtung von (1.2) und (2.2)

$$2g - 2 \geqq -2e_1 + d(\mathfrak{p}) + e_1 \frac{d(\mathfrak{q})}{e(\mathfrak{q})} \geqq -2e_1 + 2e_1 - 2 + 2e_1 \frac{e(\mathfrak{q}) - 1}{e(\mathfrak{q})},$$

$$g \geqq \frac{e(\mathfrak{q}) - 1}{e(\mathfrak{q})} e_1 \geqq \frac{p-1}{p} e_1.$$

Dies ist gerade die Behauptung von Satz 1 (b).

Ich betrachte nun die Situation (c), in der F_1 rational und nur $\mathfrak{p}$ in F/F_1 verzweigt ist. Zunächst beweise ich, daß auch F_2, der Fixpunktkörper von $G_2(\mathfrak{p})$, rational ist.

Der Differentengrad von F/F_1 sei d_1, der von F/F_2 sei d_2 und der von F_2/F_1 sei d^*. Wegen der Transitivitätseigenschaft der Differente (Serre [12], S. 60, Prop. 8) gilt

$$d_1 = d_2 + [F : F_2] d^* = d_2 + e_2 d^*. \tag{2.4}$$

Weil in F/F_1 nur $\mathfrak{p}$ verzweigt, sind die Grade d_1, d_2, d^* genau die Exponenten von $\mathfrak{p}$ in den einzelnen Differenten. Folglich ist wegen der Differentenformel (1.3)

$$d_1 = 2(e_1 - 1) + \sum_{i=2}^{\infty} (e_i - 1), \qquad d_2 = 2(e_2 - 1) + \sum_{i=2}^{\infty} (|H_i| - 1). \tag{2.5}$$

$H_0, H_1, \ldots$ ist hier die Reihe der Verzweigungsgruppen von $\mathfrak{p}$ in F/F_2. Da aber F_2 der Fixkörper von $G_2(\mathfrak{p})$ ist, stimmen für $i \geqq 2$ die Gruppen H_i und $G_i(\mathfrak{p})$ überein, d.h. die in (2.5) auftretenden Summen sind gleich:

$$d_1 - 2(e_1 - 1) = d_2 - 2(e_2 - 1).$$

Der Vergleich mit (2.4) ergibt

$$d^* = 2\frac{e_1}{e_2} - 2.$$

Die Geschlechtsformel für F_2/F_1 zeigt dann, daß F_2 vom Geschlecht 0, also rational ist.

k sei die kleinste naturliche Zahl mit $k \geqq 3$ und $G_k(\mathfrak{p}) \neq G_2(\mathfrak{p})$. Ebenso wie $G_2(\mathfrak{p})$ ist auch $G_k(\mathfrak{p})$ normal in $G_1(\mathfrak{p})$. Nach der Theorie der p-Gruppen existiert ein Normalteiler G' von $G_1(\mathfrak{p})$, welcher zwischen $G_2(\mathfrak{p})$ und $G_k(\mathfrak{p})$ liegt und in $G_2(\mathfrak{p})$ den Index p hat (Huppert [3], S. 301, Satz 7.2.d). F' sei der Fixkörper von G'. Ich will das Geschlecht g' von F' berechnen.

d_2 sei wieder der Differentengrad von F/F_2, der von F/F' sei d' und der von F'/F_2 sei $\tilde{d}$. Ähnlich wie in (2.4) und (2.5) gelten hier die folgenden Beziehungen:

$$d_2 = d' + \frac{e_2}{p}\tilde{d}, \tag{2.6}$$

$$d_2 = k(e_2 - 1) + \sum_{i=k}^{\infty}(e_i - 1),$$

$$d' = k\left(\frac{e_2}{p} - 1\right) + \sum_{i=k}^{\infty}(e_i - 1).$$

Die dritte Gleichung ergibt sich daraus, daß G' zwischen $G_2(\mathfrak{p})$ und $G_k(\mathfrak{p})$ liegt. Aus (2.6) berechnet sich $\tilde{d}$ zu

$$\tilde{d} = k(p - 1).$$

Die Geschlechtsformel für F'/F_2 liefert nun

$$g' = \tfrac{1}{2}(k - 2)(p - 1). \tag{2.7}$$

Wegen $k \geqq 3$ ist F' nicht rational. F'/F_1 ist galoissch, weil G' normal in $G_1(\mathfrak{p})$ ist. $\mathfrak{p}'$ sei die von $\mathfrak{p}$ in F' induzierte Stelle, $G_1(\mathfrak{p}')$ die p-Sylowgruppe derjenigen Gruppe von Automorphismen von F'/K, welche $\mathfrak{p}'$ festlassen. Dann läßt sich $G_1(\mathfrak{p})/G'$ als Untergruppe von $G_1(\mathfrak{p}')$ auffassen.

F'/F_2 ist wegen $[G_2(\mathfrak{p}) : G'] = p$ zyklisch vom Grad p mit nur einer Verzweigungsstelle, nämlich $\mathfrak{p}'$. Ich wähle eine Erzeugende x von F_2/K, welche $\mathfrak{p}'$ als Pol hat. Nach Hasse [2] existiert eine Artin-Schreiersche Erzeugende y von F'/F_2, deren irreduzible Gleichung über $F_2 = K(x)$ die Gestalt

$$y^p - y = B(x) \tag{2.8}$$

hat. $B(x)$ ist dabei ein Polynom in x, dessen Grad zu p teilerfremd ist.

Funktionenkörper $F' = K(x, y)$ mit der definierenden Gleichung (2.8) werden in [13] genauer untersucht. Insbesondere wird dort die Gruppe $G_1(\mathfrak{p}')$ durch

$$|G_1(\mathfrak{p}')| \leqq \frac{4p}{(p-1)^2} g'^2 \tag{2.9}$$

abgeschätzt ([13], Satz 4). Nun ist $G_1(\mathfrak{p})/G'$ eine Untergruppe von $G_1(\mathfrak{p}')$, also

$$|G_1(\mathfrak{p})| \leqq |G'| \frac{4p}{(p-1)^2} g'^2 = \frac{4e_2}{(p-1)^2} g'^2 = e_2(k-2)^2 \tag{2.10}$$

unter Benutzung von (2.7).

Aus der Geschlechtsformel für F/F_2 folgt

$$2g - 2 \geqq -2e_2 + k(e_2 - 1)$$

und daher

$$k - 2 \leqq \frac{2g}{e_2 - 1}.$$

Setzt man dies in (2.10) ein, ergibt sich schließlich

$$e_1 \leqq \frac{4e_2}{(e_2-1)^2} g^2.$$

Der Beweis von Satz 1 ist damit beendet.

Bemerkungen. 1. Für $F = K(x, y)$ mit der definierenden Gleichung

$$y^{p^n} + y = x^{p^{kn}+1}$$

ist die Gruppe $G_1(\mathfrak{p})$ des Pols $\mathfrak{p}$ von x (x besitzt nur einen Pol) von der Ordnung

$$\frac{4e_2}{(e_2-1)^2} g^2.$$

Das wird in [13], Satz 5 bewiesen. In diesem Sinne läßt sich die Abschätzung von Satz 1 (c) nicht verbessern.

2. Im Beweis von Satz 1 habe ich die Endlichkeit von $G_1(\mathfrak{p})$ schon vorausgesetzt. Durch geringfügige Änderungen kann aber mit den gleichen Mitteln die Endlichkeit bewiesen werden. Der entscheidende Schritt beim Beweis der Endlichkeit ist nämlich der Nachweis, daß jede endliche Untergruppe von $G_1(\mathfrak{p})$ von beschränkter Ordnung ist (vgl. Iwasawa und Tamagawa [5]), und das wird in Satz 1 bewiesen.

Satz 2. *Die Ordnung e' von $G(\mathfrak{p})/G_1(\mathfrak{p})$ wird abgeschätzt durch*

$$e' \leqq 4g + 2.$$

Beweis. $G(\mathfrak{p})$ ist semidirektes Produkt von $G_1(\mathfrak{p})$ mit einer zyklischen Gruppe H. Beim Restklassenhomomorphismus $G(\mathfrak{p}) \to G(\mathfrak{p})/G_1(\mathfrak{p})$ wird H also isomorph abgebildet und besitzt die Ordnung e'. Der Fixkörper F_H von H habe das Geschlecht g_H. Die von $\mathfrak{p}$ verschiedenen Verzweigungsstellen von F_H in F/F_H seien $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, die Verzweigungsordnung von $\mathfrak{q}_j$ in F/F_H sei $e(\mathfrak{q}_j)$. Die Geschlechtsformel für F/F_H besagt

$$2g - 2 = e'(2g_H - 2) + d.$$

Der Grad d der Differente von F/F_H läßt sich hier leicht angeben, denn wegen $(e', p) = 1$ sind alle Stellen $\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r$ regulär verzweigt. Das bedeutet nach (1.2)

$$d = d(\mathfrak{p}) + e' \sum_{j=1}^{r} \frac{d(\mathfrak{q}_j)}{e(\mathfrak{q}_j)} = e' - 1 + e' \sum_{j=1}^{r} \frac{e(\mathfrak{q}_j) - 1}{e(\mathfrak{q}_j)}.$$

Einsetzen in die Geschlechtsformel gibt

$$2g - 1 = e'(2g_H - 1) + e' \sum_{j=1}^{r} \frac{e(\mathfrak{q}_j) - 1}{e(\mathfrak{q}_j)}. \tag{2.11}$$

Ist g_H positiv, folgt sofort $e' \leqq 2g - 1$. Im folgenden kann ich also $g_H = 0$ annehmen. (2.11) lautet dann

$$2g - 1 = e' \left(\sum_{j=1}^{r} \frac{e(\mathfrak{q}_j) - 1}{e(\mathfrak{q}_j)} - 1 \right). \tag{2.12}$$

Kein Summand ist dabei kleiner als $\frac{1}{2}$. Für $r \geqq 3$ folgt daher aus (2.12) die Abschätzung $e' \leqq 2(2g - 1)$. Dieselbe Abschätzung bleibt für $r = 2$ gültig, falls

$$\frac{e(\mathfrak{q}_1) - 1}{e(\mathfrak{q}_1)} + \frac{e(\mathfrak{q}_2) - 1}{e(\mathfrak{q}_2)} \geqq \frac{3}{2}.$$

Der Fall $r = 1$ oder $r = 0$ kann nicht vorkommen, denn die linke Seite von (2.12) ist positiv. Ordnet man $e(\mathfrak{q}_1)$ und $e(\mathfrak{q}_2)$ der Größe nach, so bleiben nur noch die folgenden Fälle zu diskutieren:

$$e(\mathfrak{q}_1) = 3, \quad e(\mathfrak{q}_2) = 5; \tag{2.13}$$

$$e(\mathfrak{q}_1) = 3, \quad e(\mathfrak{q}_2) = 4;$$
$$e(\mathfrak{q}_1) = 3, \quad e(\mathfrak{q}_2) = 3;$$
$$e(\mathfrak{q}_1) = 2, \quad e(\mathfrak{q}_2) \geqq 3;$$

$e(\mathfrak{q}_1) = e(\mathfrak{q}_2) = 2$ kann nicht auftreten, weil sonst aus (2.12) der Widerspruch $2g - 1 = 0$ folgte.

n sei das kleinste gemeinsame Vielfache von $e(\mathfrak{q}_1)$ und $e(\mathfrak{q}_2)$. Da H zyklisch ist, gibt es genau eine Untergruppe H_n von H mit der Ordnung n. Wäre H_n eine echte Untergruppe von H, so wäre in der Erweiterung F_n/F_H, wo F_n der Fixkörper von H_n ist, nur $\mathfrak{p}$ verzweigt. Eine galoissche Erweiterung des rationalen Funktionenkörpers F_H, deren Grad zu p teilerfremd ist, besitzt aber nach der Geschlechtsformel mindestens zwei verschiedene Verzweigungsstellen. Folglich ist $H_n = H$ und e' das kleinste gemeinsame Vielfache von $e(\mathfrak{q}_1)$ und $e(\mathfrak{q}_2)$. In den verschiedenen Fällen von (2.13) ergibt sich nun zusammen mit (2.12):

3,5:	$e' = 15,$	$g = 4,$
3,4:	$e' = 12,$	$g = 3,$
3,3:	$e' = 3,$	$g = 1,$
$2,2k$:	$e' = 2k,$	$g = k/2,$
$2,2k+1$:	$e' = 4k+2,$	$g = k.$

In jedem Falle gilt also $e' \leqq 4g + 2$.

Beispiel. Der hyperelliptische Körper $K(x, y)$ sei durch

$$y^2 = x^{2g+1} - 1$$

definiert (p sei kein Teiler von $4g + 2$). Er hat das Geschlecht g. Durch

$$y \to \pm y, \quad x \to \alpha x, \quad \alpha^{2g+1} = 1$$

sind $4g + 2$ verschiedene Automorphismen gegeben, welche den Pol von x festlassen. Die in Satz 2 angegebene Schranke wird hier also angenommen.

3. Die volle Automorphismengruppe. Jetzt sei F/K ein Funktionenkörper vom Geschlecht $g \geqq 2$. Da K als algebraisch abgeschlossen vorausgesetzt wurde, ist die Automorphismengruppe G von F/K endlich. Den Fixkörper von G bezeichne ich mit F_G.

Satz 3. *Für die Ordnung von G gilt die Hurwitzsche Abschätzung*

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

Ausnahmen hiervon können höchstens in folgenden Fällen auftreten:

(1) *F_G ist rational, und es sind genau drei Stellen von F_G in F/F_G verzweigt. Zwei davon sind regulär verzweigt mit der Verzweigungsordnung 2, eine verzweigt irregulär (insbesondere ist also $p \neq 2$).*

(2) *F_G ist rational. Genau zwei Stellen von F_G sind in F/F_G verzweigt, und zwar beide irregulär.*

(3) *F_G ist rational. Genau eine Stelle von F_G ist in F/F_G verzweigt, und zwar irregulär.*

(4) *F_G ist rational. Genau zwei Stellen von F_G sind in F/F_G verzweigt, und zwar eine regulär, die andere irregulär.*

Beweis. Der Beweis ist eine Kopie des Hurwitzschen Beweises in Charakteristik 0. Das Geschlecht von F_G sei g_G. Dann besagt die Geschlechtsformel

$$2g - 2 = |G|(2g_G - 2) + d.$$

Der Grad d der Differente von F/F_G läßt sich folgendermaßen ausdrücken: $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ seien die sämtlichen Stellen von F_G, welche in F verzweigt sind; $e(\mathfrak{q}_j)$ sei die Verzweigungsordnung von $\mathfrak{q}_j$ und $d(\mathfrak{q}_j)$ der Exponent einer Fortsetzung von $\mathfrak{q}_j$ in der Differente von F/F_G. Ich setze

$$\delta_j = \frac{d(\mathfrak{q}_j)}{e(\mathfrak{q}_j)}, \qquad \delta = \sum_{j=1}^{r} \delta_j$$

und erhalte nach (1.2) aus der Geschlechtsformel

$$2g - 2 = |G|(2g_G - 2) + |G| \cdot \delta = |G|(2g_G - 2 + \delta). \tag{3.1}$$

Ist nun $g_G \geqq 2$, so folgt wegen $\delta \geqq 0$ sofort $|G| \leqq g - 1$. Für $g_G = 1$ ist wegen $g \geqq 2$ mindestens eine Stelle verzweigt. In diesem Fall ist $\delta \geqq \frac{1}{2}$, da $d(\mathfrak{q}_j) \geqq e(\mathfrak{q}_j) - 1$ gilt (nach (1.3)). Aus (3.1) folgt jetzt $|G| \leqq 4(g-1)$. Im folgenden sei also $g_G = 0$. Das bedeutet

$$2g - 2 = |G|(\delta - 2). \tag{3.2}$$

Insbesondere ist $\delta > 2$. Es sind einige Fälle zu unterscheiden:

(a) $r \geqq 5$: Dann ist $\delta \geqq \frac{5}{2}$, d.h. $|G| \leqq 4(g-1)$.

(b) $r = 4$: Jetzt ist wenigstens ein $\delta_j > \frac{1}{2}$, also mindestens $\frac{2}{3}$. Daher gilt $\delta - 2 \geqq \frac{1}{6}$ und $|G| \leqq 12(g-1)$.

(c) $r = 3$, $\delta_1 \leqq \delta_2 \leqq \delta_3$. Für $\delta_1 \geqq \frac{2}{3}$ ist $\delta_3 \geqq \frac{3}{4}$. Es folgt $|G| \leqq 24(g-1)$. Ist $\delta_1 = \frac{1}{2}$ und $\delta_2 \geqq \frac{3}{4}$, ergibt sich $|G| \leqq 40(g-1)$. Bei $\delta_1 = \frac{1}{2}$ und $\delta_2 = \frac{2}{3}$ folgt $\delta_3 \geqq \frac{6}{7}$ und damit $|G| \leqq 84(g-1)$. Für $\delta_1 = \delta_2 = \frac{1}{2}$ muß $\delta_3 > 1$ sein. Dann ist also $\mathfrak{q}_3$ irregulär verzweigt, und es liegt die in Satz 3 (1) beschriebene Situation vor. Analog sieht man, wenn nur eine oder zwei Stellen verzweigt sind, daß dann wenigstens eine Stelle irregulär verzweigen muß. Dies sind die in (2), (3) und (4) aufgeführten Möglichkeiten.

Der folgende Hauptsatz gibt auch in den durch Satz 3 nicht erfaßten Fällen eine Abschätzung für die Ordnung von G.

Hauptsatz. *F sei ein algebraischer Funktionenkörper einer Variablen über dem algebraisch abgeschlossenen Körper K. Das Geschlecht von F sei $g \geqq 2$, die Charakteristik sei $p > 0$. Dann läßt sich die Ordnung der Automorphismengruppe G von F/K abschätzen durch*

$$|G| < 16g^4,$$

abgesehen von einer Serie von Ausnahmefällen. In diesen Ausnahmefällen gibt es Elemente x, y in F, so daß $F = K(x, y)$ und die irreduzible Gleichung zwischen x und y von der Form

$$y^{p^n} + y = x^{p^n+1} \qquad (n \geqq 1,\ p^n \geqq 3)$$

ist. Dabei ist $g = \frac{1}{2} p^n(p^n - 1)$ und $|G| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$, d.h. $|G|$ ist etwas größer als $16g^4$.

In den Fällen (1) bis (3) von Satz 3 gelten sogar schärfere Abschätzungen:

$$|G| \leqq 24 \cdot g^2, \tag{1}$$

$$|G| \leqq 16 \cdot g^2, \tag{2}$$

$$|G| \leqq 16 \cdot g^3. \tag{3}$$

Beweis. Es sind nur noch die Fälle (1) bis (4) von Satz 3 zu untersuchen. Die Bezeichnungen aus dem Beweis von Satz 3 behalte ich bei.

Fall (1). Hier ist $\delta_1 = \delta_2 = \frac{1}{2}$, $\delta_3 = d(\mathfrak{q}_3)/e(\mathfrak{q}_3)$. Damit wird

$$\delta - 2 = \frac{d(\mathfrak{q}_3) - e(\mathfrak{q}_3)}{e(\mathfrak{q}_3)}. \tag{3.3}$$

Ich setze $e(\mathfrak{q}_3) = e = e_1 e'$, wobei e_1 die höchste in e aufgehende p-Potenz ist. Da $\mathfrak{q}_3$ irregulär verzweigt, gilt $e_1 \geqq p$. Der Exponent $d(\mathfrak{q}_3)$ läßt sich nach (1.3) wie folgt abschätzen:

$$d(\mathfrak{q}_3) \geqq e - 1 + e_1 - 1 .$$

Einsetzen in (3.3) ergibt

$$\delta - 2 \geqq \frac{e - 1 + e_1 - 1 - e}{e} = \frac{1}{e'}\left(1 - \frac{2}{e_1}\right) \geqq \frac{1}{e'}\left(1 - \frac{2}{p}\right) \geqq \frac{1}{3e'} \tag{3.4}$$

wegen $p \geqq 3$. Nach (3.2) und Satz 2 folgt

$$|G| \leqq 3e'(2g-2) \leqq 3(4g+2)(2g-2) < 24g^2 .$$

Fall (2). Jetzt sind genau zwei Stellen von F_G in F verzweigt, und zwar beide irregulär. Bei $p \geqq 3$ ergibt sich wie in (3.4):

$$\delta - 2 = \frac{d(\mathfrak{q}_1) - e(\mathfrak{q}_1)}{e(\mathfrak{q}_1)} + \frac{d(\mathfrak{q}_2) - e(\mathfrak{q}_2)}{e(\mathfrak{q}_2)} \geqq \frac{1}{3e'(\mathfrak{q}_1)} + \frac{1}{3e'(\mathfrak{q}_2)} \geqq \frac{2}{3(4g+2)}$$

und damit $|G| \leqq 3(2g+1)(2g-2) < 12g^2$.

Für $p = 2$ sei $e_i(\mathfrak{q}_j)$ die Ordnung der i-ten Verzweigungsgruppe einer Fortsetzung von $\mathfrak{q}_j$ $(j = 1, 2;\ i = 1, 2, 3, \ldots)$. Dann ist

$$\delta - 2 = \frac{d(\mathfrak{q}_1) - e(\mathfrak{q}_1)}{e(\mathfrak{q}_1)} + \frac{d(\mathfrak{q}_2) - e(\mathfrak{q}_2)}{e(\mathfrak{q}_2)} = \sum_{j=1}^{2} \frac{1}{e(\mathfrak{q}_j)} \left(e_1(\mathfrak{q}_j) - 2 + \sum_{i=2}^{\infty} (e_i(\mathfrak{q}_j) - 1) \right). \tag{3.5}$$

Es werden einige Fallunterscheidungen getroffen:

(a) $e_1(\mathfrak{q}_1) \geqq 4$ (analog für $e_1(\mathfrak{q}_2) \geqq 4$). Aus (3.5) folgt

$$\delta - 2 \geqq \frac{e_1(\mathfrak{q}_j) - 2}{e(\mathfrak{q}_1)} = \frac{1}{e'(\mathfrak{q}_1)}\left(1 - \frac{2}{e_1(\mathfrak{q}_1)}\right) \geqq \frac{1}{2e'(\mathfrak{q}_1)}$$

wegen $e_1(\mathfrak{q}_1) \geqq 4$. Satz 2 und Formel (3.2) liefern

$$|G| \leqq 2(4g+2)(2g-2) < 16g^2 .$$

(b) $e_1(\mathfrak{q}_1) = e_1(\mathfrak{q}_2) = 2$, $e_2(\mathfrak{q}_1) = e_2(\mathfrak{q}_2) = 1$. Dieser Fall ist nicht möglich, weil dann nach (3.5) der Widerspruch $\delta - 2 = 0$ folgte.

(c) $e_1(\mathfrak{q}_1) = e_1(\mathfrak{q}_2) = 2$, $e_2(\mathfrak{q}_1) = 2$ (oder $e_2(\mathfrak{q}_2) = 2$). Nun besagt (3.5)

$$\delta - 2 \geqq \frac{1}{e(\mathfrak{q}_1)} = \frac{1}{2e'(\mathfrak{q}_1)}$$

und damit $|G| \leqq 2e'(\mathfrak{q}_1)(2g-2) \leqq 2(4g+2)(2g-2) < 16g^2$.

Fall (3). Nur eine Stelle $\mathfrak{q}$ von F_G ist in F/F_G verzweigt. $\mathfrak{p}$ sei eine Fortsetzung von $\mathfrak{q}$ auf F. Es gibt zwei Möglichkeiten:

(a) $\mathfrak{p}$ ist invariant unter G, d.h. $G = G(\mathfrak{p})$. Ich setze $|G| = e = e_1 e'$ mit $e_1 = |G_1(\mathfrak{p})|$. Ist F_1, der Fixkörper von $G_1(\mathfrak{p})$, nicht rational, so folgt aus Satz 1 (a) und Satz 2

$$|G| = e_1 e' \leqq g(4g+2) .$$

Ist F_1 rational, so ist $G = G_1(\mathfrak{p})$. Andernfalls wäre nämlich F_1 eine galoissche Erweiterung des rationalen Funktionenkörpers F_G von zu p teilerfremdem Grad. Eine solche Erweiterung müßte aber mindestens an zwei Stellen verzweigen, wie die Geschlechtsformel zeigt. Es war jedoch angenommen worden, daß nur $\mathfrak{p}$ in F/F_G verzweigt. Demnach gilt nach Satz 1

$$|G| = e_1 \leqq 8g^2 .$$

(b) $\mathfrak{p}$ ist nicht invariant unter G. Bezeichnet e die Verzweigungsordnung von $\mathfrak{p}$ und d den Exponenten von $\mathfrak{p}$ in der Differente von F/F_G, so besagt (3.2):

$$|G| = \frac{2(g-1)e'e_1}{d - 2e} \leqq 2(g-1)(4g+2)e_1 < 8g^2 e_1 . \tag{3.6}$$

Falls F_1 nicht rational ist, ergibt Satz 1 (a) die Abschätzung $|G| < 8g^3$. Ist F_1 rational, aber $\mathfrak{p}$ nicht die einzige Verzweigungsstelle von F/F_1, dann liefert Satz 1 (b) zusammen mit (3.6) die Schranke $|G| < 16g^3$.

Schließlich sei F_1 rational und $\mathfrak{p}$ die einzige Verzweigungsstelle von F/F_1. Wegen $G(\mathfrak{p}) \neq G$ gibt es eine weitere Stelle $\mathfrak{p}'$ von F, welche über F_G verzweigt und unter G zu $\mathfrak{p}$ konjugiert ist. Diese Stelle muß in $F_{G(\mathfrak{p})}/F_G$ (hier ist $F_{G(\mathfrak{p})}$ der Fixkörper von $G(\mathfrak{p})$) mindestens von der Ordnung e_1 verzweigen. Aus (3.6) folgt nun

$$e_1 \leqq [F_{G(\mathfrak{p})}: F_G] = \frac{|G|}{e_1 e'} = \frac{2(g-1)}{d-2e} \leqq 2(g-1)$$

und damit $|G| < 8g^2 e_1 < 16g^3$.

Fall (4). Mit den gleichen Mitteln wie in den Fällen (1) bis (3) kommt man auch hier zu einer Abschätzung von $|G|$, und zwar in der Größenordnung g^5. Zum Beweis der im Hauptsatz aufgestellten Behauptungen sind jedoch weitere Fallunterscheidungen erforderlich.

Genau zwei Stellen von F_G verzweigen in F/F_G. Eine davon, etwa $\mathfrak{q}$, ist irregulär, die andere Stelle $\bar{\mathfrak{q}}$ ist regulär verzweigt. Die Verzweigungsordnung von $\bar{\mathfrak{q}}$ sei $\bar{e}$, die von $\mathfrak{q}$ sei e. Ich wähle eine Fortsetzung $\mathfrak{p}$ von $\mathfrak{q}$ fest aus; $G_1(\mathfrak{p})$ sei die erste Verzweigungsgruppe von $\mathfrak{p}$. Dann ist $e = e_1 e'$, wobei e_1 die Ordnung von $G_1(\mathfrak{p})$ und e' zu p teilerfremd ist. F_0 sei der Fixkörper von $G(\mathfrak{p})$ und F_1 der Fixkörper von $G_1(\mathfrak{p})$. Ich unterscheide die Fälle A.—E.:

A. F_1 ist nicht rational.

B. F_1 ist rational. In F/F_1 ist noch mindestens eine Stelle $\mathfrak{p}' \neq \mathfrak{p}$ verzweigt, welche in F_1/F_0 nicht verzweigt (d.h. die Einschränkung von $\mathfrak{p}'$ auf F_1 ist in F_1/F_0 unverzweigt).

C. F_1 ist rational, und in F/F_1 ist noch mindestens eine Stelle $\mathfrak{p}' \neq \mathfrak{p}$ verzweigt. $\mathfrak{p}'$ verzweigt auch in F_1/F_0.

D. F_1 ist rational. In F/F_1 ist nur $\mathfrak{p}$ verzweigt. Es gibt ein $\mathfrak{p}'$, welches unter G zu $\mathfrak{p}$ konjugiert ist, aber in F/F_0 nicht verzweigt.

E. F_1 ist rational. In F/F_1 ist nur $\mathfrak{p}$ verzweigt. Alle unter G zu $\mathfrak{p}$ konjugierten Stellen sind in F/F_0 verzweigt.

Bevor ich die einzelnen Fälle diskutiere, leite ich noch einen geschlossenen Ausdruck für die Ordnung von G her. Ist nämlich d der Exponent von $\mathfrak{p}$ in der Differente von F/F_G und

$$N = d\bar{e} - e\bar{e} - e,$$

dann ergibt (3.2) unmittelbar

$$|G| = \frac{2(g-1)\bar{e}e'e_1}{N}. \tag{3.7}$$

A. F_1 ist nicht rational, hat also das Geschlecht $g_1 \geqq 1$. Da $\mathfrak{p}$ in F/F_1 voll verzweigt, besagt die Geschlechtsformel für F/F_1

$$2g - 2 \geqq e_1(2g_1 - 2) + 2(e_1 - 1).$$

(Man beachte, daß der Exponent von $\mathfrak{p}$ in der Differente von F/F_1 nach (1.3) mindestens den Wert $2(e_1 - 1)$ hat, weil $\mathfrak{p}$ voll verzweigt und $[F : F_1]$ eine p-Potenz ist.) Damit folgt $e_1 \leqq g/g_1$. Die Faktorgruppe $G(\mathfrak{p})/G_1(\mathfrak{p})$ läßt sich als Automorphismengruppe von F_1/K auffassen, und dann folgt aus Satz 2 die Abschätzung $e' \leqq 4g_1 + 2$. Durch Einsetzen in (3.7) erhalte ich

$$|G| \leqq 2(g-1)(4g+2)(4g_1+2)\frac{g}{g_1} < 8g(g-1)(g+1)\left(4 + \frac{2}{g_1}\right) \leqq 16 \cdot 3g^3. \tag{3.8}$$

Für $g \geqq 3$ folgt hieraus $|G| < 16g^4$. Für $g = 2$ gilt aber wegen $e_1 \leqq g/g_1$ und $e_1 \geqq p$ sogar $e_1 = 2$ und $g_1 = 1$. Einsetzen in die erste Ungleichung von (3.8) liefert

$$|G| \leqq 2 \cdot 1 \cdot 10 \cdot 6 \cdot 2 = 240 < 256 = 16g^4.$$

B. F_1 ist rational. In F/F_1 ist noch mindestens eine Stelle $\mathfrak{p}' \neq \mathfrak{p}$ verzweigt, welche aber in F_1/F_0 nicht verzweigt. Dann verzweigen sogar mindestens e' von $\mathfrak{p}$ verschiedene Stellen von F_1 in F/F_1, und zwar mit derselben Verzweigungsordnung p^t wie $\mathfrak{p}'$. Die Geschlechtsformel für

F/F_1 gibt

$$2g-2 \geqq -2e_1 + 2(e_1-1) + \frac{e_1}{p^t}(2p^t-2)\cdot e',$$

$$g \geqq e_1 e' \left(1-\frac{1}{p^t}\right) \geqq \frac{1}{2} e_1 e'.$$

Aus (3.7) folgt jetzt

$$|G| \leqq 2(g-1)(4g+2)\cdot 2g < 16g^4.$$

Zur Untersuchung der Fälle C. und E. benötige ich ein einfaches Lemma.

Lemma. *L und M seien rationale Funktionenkörper über K und L eine zyklische Erweiterung von M vom Grad $n > 1$. Ist n nicht durch die Charakteristik p teilbar, dann sind genau zwei Stellen von M in L/M verzweigt, und zwar beide voll.*

Beweis. $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ seien die Stellen von M, welche in L/M verzweigen, $e(\mathfrak{q}_j)$ die Verzweigungsordnung von $\mathfrak{q}_j$. Da die Verzweigung regulär ist, hat der Exponent einer Fortsetzung von $\mathfrak{q}_j$ in der Differente von L/M den Wert $e(\mathfrak{q}_j)-1$. Ich setze $\delta_j = [e(\mathfrak{q}_j)-1]/e(\mathfrak{q}_j)$ und erhalte nach (1.2) aus der Geschlechtsformel

$$2 - \frac{2}{n} = \sum_{j=1}^{r} \delta_j. \tag{3.9}$$

Wegen $1 \leqq 2-(2/n) < 2$ und $\frac{1}{2} \leqq \delta_j < 1$ folgt sofort $r = 2$ oder $r = 3$. Insbesondere gilt auch für jede Zwischenerweiterung Z/M, daß mindestens zwei Stellen von M in Z/M verzweigen.

Ist $r = 2$, so ergibt (3.9) weiter $\delta_1 = \delta_2 = (n-1)/n$ und damit die Behauptung des Lemmas.

Den Fall $r = 3$ will ich zum Widerspruch führen. Es sei $\delta_1 \leqq \delta_2 \leqq \delta_3$. Wegen $\delta_1 + \delta_2 + \delta_3 < 2$ gibt es nur folgende Möglichkeiten:

(a) $\delta_1 = \frac{1}{2}$, $\delta_2 = \frac{2}{3}$, $\frac{2}{3} \leqq \delta_3 \leqq \frac{4}{5}$,

(b) $\delta_1 = \delta_2 = \frac{1}{2}$, δ_3 beliebig.

Im Fall (a) untersuche ich nur den Fall $\delta_3 = \frac{4}{5}$ (die beiden Fälle $\delta_3 = \frac{3}{4}$ bzw. $\frac{2}{3}$ lassen sich ebenso behandeln). (3.9) ergibt für n den Wert $n = 60$. Z sei der Zwischenkörper zwischen L und M mit $[L:Z] = 30$ (Z ist eindeutig bestimmt, weil L/M zyklisch ist). In Z/M ist dann keine Stelle verzweigt, denn die Verzweigungskörper der drei Verzweigungsstellen haben in L den Index 2, 3 bzw. 5 und sind daher Oberkörper von Z. Andererseits existieren aber in jeder Zwischenerweiterung Z/M mindestens zwei Verzweigungsstellen. Das ist ein Widerspruch.

Im Fall (b) wähle ich Z als den Zwischenkörper vom Index 2 in L. Ist Z echt größer als M, dann ist in Z/M nur die Stelle $\mathfrak{q}_3$ von M verzweigt. Ist aber $Z = M$, dann folgt $n = 2$, und aus (3.9) ergibt sich der Widerspruch $1 = \frac{3}{2}$. Das Lemma ist damit bewiesen.

C. F_1 ist rational. In F/F_1 ist noch eine Stelle $\mathfrak{p}' \neq \mathfrak{p}$ verzweigt, und $\mathfrak{p}'$ verzweigt auch in F_1/F_0. Weil F_1/F_0 eine zyklische Erweiterung rationaler Funktionenkörper vom Grad e' ist, verzweigt $\mathfrak{p}'$ nach dem Lemma voll in F_1/F_0. Daher existiert eine zyklische Untergruppe H in $G(\mathfrak{p}) \cap G(\mathfrak{p}')$ von der Ordnung e'. Der zugehörige Fixkörper F_H ist nicht rational. Sind nämlich $\mathfrak{r}$ bzw. $\mathfrak{r}'$ die von $\mathfrak{p}$ bzw. $\mathfrak{p}'$ in F_0 induzierten Stellen, so verzweigen alle Fortsetzungen von $\mathfrak{r}$ und $\mathfrak{r}'$ in F_H/F_0 irregulär (in F/F_H findet nur reguläre Verzweigung statt). Daher ist der Grad der Differente von F_H/F_0 mindestens $2e_1 = 2[F_H : F_0]$. Die Geschlechtsformel für F_H/F_0 zeigt, daß F_H positives Geschlecht hat. Die Geschlechtsformel für F/F_H ergibt $2g-2 \geqq 2e'-2$, weil hier mindestens zwei Stellen voll verzweigen, und damit $e' \leqq g$. Durch Einsetzen in (3.7) folgt nun unter Beachtung von Satz 1 (b)

$$|G| \leqq 2(g-1)(4g+2)\cdot g \cdot \frac{p}{p-1} \cdot g < 16g^4.$$

D. F_1 ist rational, und nur $\mathfrak{p}$ ist in F/F_1 verzweigt. Es gibt eine unter G zu $\mathfrak{p}$ konjugierte Stelle $\mathfrak{p}'$, welche in F/F_0 nicht verzweigt. Unter diesen Voraussetzungen folgt, daß $\mathfrak{p}'$ in F_0/F_G seine volle Verzweigungsordnung e erhält. Das bedeutet nach (3.7)

$$e \leqq [F_0 : F_G] = \frac{|G|}{e} \leqq 2\bar{e}(g-1). \tag{3.10}$$

Der in (3.7) auftretende Nenner N läßt sich wie folgt abschätzen:

$$N = d\bar{e} - e\bar{e} - e \geqq d\bar{e} - e\bar{e} - 2\bar{e}(g-1) = \bar{e}(d - e - 2(g-1)). \tag{3.11}$$

Die Geschlechtsformel für F/F_1 besagt:

$$2(g-1) = -2e_1 + (d - e_1(e'-1)) = d - e - e_1, \quad d - e - 2(g-1) = e_1.$$

Einsetzen in (3.11) ergibt $N \geqq e_1\bar{e}$. Damit erhalte ich aus (3.7):

$$|G| \leqq \frac{2(g-1)\bar{e}e'e_1}{e_1\bar{e}} = 2e'(g-1) \leqq 8(g+1)(g-1) < 16g^4.$$

E. F_1 ist rational. In F/F_1 ist nur $\mathfrak{p}$ verzweigt. Alle unter G zu $\mathfrak{p}$ konjugierten Stellen sind in F/F_0 verzweigt.

Ich kann $e' \geqq 2$ annehmen, weil sonst $G = G(\mathfrak{p}) = G_1(\mathfrak{p})$ folgt. In diesem Fall ist die Abschätzung $16g^4$ ohnehin richtig. Nach dem Lemma sind in F_1/F_0 genau zwei Stellen, und zwar beide voll, verzweigt. Eine davon ist $\mathfrak{p}$, die andere muß die Einschränkung einer zu $\mathfrak{p}$ unter G konjugierten Stelle $\mathfrak{p}'$ auf F_0 sein. Weil alle diese Stellen über F_0, aber nicht über F_1 verzweigen, induzieren sie alle dieselbe Stelle auf F_1. Es folgt, daß alle unter G zu $\mathfrak{p}$ konjugierten Stellen $\mathfrak{p}' \neq \mathfrak{p}$ untereinander in $G_1(\mathfrak{p})$ konjugiert sind. Insbesondere gibt es genau e_1 solche Stellen. Die volle Gruppenordnung ist demnach gegeben durch

$$|G| = |G(\mathfrak{p})|(e_1+1) = e_1e'(e_1+1). \tag{3.12}$$

Mit F_2 bezeichne ich den Fixpunktkörper von $G_2(\mathfrak{p})$. Nach Satz 1 (c) ist F_2 rational. Mit $q = [F:F_2]$ gilt die Abschätzung von Satz 1 (c):

$$e_1 \leqq \frac{4q}{(q-1)^2}\, g^2. \tag{3.13}$$

Nun wähle ich eine Stelle $\mathfrak{p}' \neq \mathfrak{p}$, welche unter G zu $\mathfrak{p}$ konjugiert ist. Sie verzweigt in F/F_0 mit dem Exponenten e'. Daher ist $H = G(\mathfrak{p}) \cap G(\mathfrak{p}')$ zyklisch von der Ordnung e'. Da $\mathfrak{p}$ und $\mathfrak{p}'$ konjugiert sind, existiert ein Automorphismus $\omega' \in G$ mit $\omega'\mathfrak{p}' = \mathfrak{p}$. Wegen $\omega'\mathfrak{p} \neq \mathfrak{p}$ gibt es ein $\lambda \in G_1(\mathfrak{p})$ mit $\lambda\omega'\mathfrak{p} = \mathfrak{p}'$. Ich setze $\omega = \lambda\omega'$ und erhalte

$$\omega\mathfrak{p} = \mathfrak{p}', \quad \omega\mathfrak{p}' = \mathfrak{p}.$$

Es folgt $\omega^2 \in H$ und $\omega^{-1}H\omega = H$. Weil H zyklisch ist, gibt es eine ganze Zahl s, so daß für jedes $\sigma \in H$ gilt

$$\omega^{-1}\sigma\omega = \sigma^s.$$

Zur Bestimmung von s betrachte ich den Verzweigungscharakter χ: $G(\mathfrak{p}) \to K^\times$, wobei $K^\times$ die multiplikative Gruppe von K ist. χ ist folgendermaßen definiert (Serre [12], S. 74 f.): Für ein $\mathfrak{p}$-Primelement π und ein $\sigma \in G(\mathfrak{p})$ ist

$$\frac{\sigma\pi}{\pi} \equiv \chi(\sigma) \pmod{\mathfrak{p}}.$$

Allgemeiner gilt für beliebiges $z \in F^\times$

$$\frac{\sigma z}{z} \equiv \chi(\sigma)^{v_\mathfrak{p}(z)} \pmod{\mathfrak{p}}. \tag{3.14}$$

Dabei bedeutet $v_\mathfrak{p}$ die zu $\mathfrak{p}$ gehörige normierte additive Bewertung von F. Der Kern von χ ist gerade $G_1(\mathfrak{p})$. Die Einschränkung von χ auf H ist wegen $H \cap G_1(\mathfrak{p}) = 1$ ein treuer Charakter von H.

Ich wähle eine Erzeugende x des rationalen Funktionenkörpers F_2, welche $\mathfrak{p}'$ als Nullstelle und $\mathfrak{p}$ als Pol besitzt. Der Divisor von x hat dann die Form

$$x \cong \frac{\mathfrak{p}' \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_{q-1}}{\mathfrak{p}^q}. \tag{3.15}$$

Die Nullstellen von x sind alle einfach, weil über F_2 nur $\mathfrak{p}$ verzweigt. Da F_2 als Fixkörper von

$G_2(\mathfrak{p})$ galoissch über F_0 ist und H die Stellen $\mathfrak{p}$ und $\mathfrak{p}'$ festläßt, folgt $\sigma x = ax$ für $\sigma \in H$. Dabei ist a ein Element von $K^\times$. Vergleich mit (3.14) ergibt

$$\sigma x = \chi(\sigma)^{-q} \cdot x \quad (\sigma \in H).$$

Folglich liegt $x^{e'}$ in F_H, dem Fixkörper von H. Wegen der Teilerfremdheit von $q = [F : K(x)]$ und $e' = [F : F_H]$ ist x eine Kummersche Erzeugende von F/F_H (d.h. $F = F_H(x)$, und die irreduzible Gleichung für x über F_H lautet $x^{e'} = w \in F_H$). Da F_H invariant unter ω ist ($\omega^{-1} H \omega = H$), bleibt auch ωx eine Kummersche Erzeugende von F/F_H. Die Stellen $\mathfrak{p}$ und $\mathfrak{p}'$ werden unter ω vertauscht; ωx ist also nach (3.15) ein $\mathfrak{p}$-Primelement, und es gilt für $\sigma \in H$

$$\sigma(\omega x) = \chi(\sigma) \cdot \omega x, \quad \omega^{-1} \sigma \omega x = \chi(\sigma) \cdot x.$$

Vergleicht man das mit $\omega^{-1} \sigma \omega = \sigma^s$ und $\sigma^s x = \chi(\sigma^{-sq}) \cdot x$ und beachtet, daß χ auf H ein treuer Charakter ist, so folgt

$$-sq \equiv 1 \pmod{e'}. \tag{3.16}$$

ω^2 liegt in der abelschen Gruppe H, also

$$\sigma = \omega^{-1}(\omega^{-1} \sigma \omega)\, \omega = \omega^{-1} \sigma^s \omega = \sigma^{s^2}.$$

Das bedeutet $s^2 \equiv 1 \pmod{e'}$. Zusammen mit (3.16) heißt das $s \equiv -q \pmod{e'}$, also

$$\omega^{-1} \sigma \omega = \sigma^{-q} \tag{3.17}$$

für jedes $\sigma \in H$, und weiter

$$q^2 \equiv 1 \pmod{e'}. \tag{3.18}$$

Mit (3.12), (3.13) und (3.18) sind die wesentlichen Hilfsmittel zur Abschätzung der Ordnung von G bereitgestellt.

Die Zahl $r = (q^2 - 1)/e'$ ist nach (3.18) ganz. Damit besagt (3.12):

$$|G| = e_1 e'(e_1 + 1) \leqq \frac{4q(q^2-1)g^2}{r(q-1)^2} \cdot \left(\frac{4qg^2}{(q-1)^2} + 1 \right), \tag{3.19}$$

$$|G| \leqq \frac{16}{r} \cdot \left(\frac{q}{q-1} \right)^2 \cdot \frac{q+1}{q-1} \cdot g^4 + \frac{4q}{r} \cdot \frac{q+1}{q-1} \cdot g^2.$$

Ich behandle zuerst den Fall $r \geqq 2$.

Für $q = p$ ist F eine zyklische Erweiterung von $K(x)$ vom Grad p, in welcher nur der Pol von x verzweigt. Dann existiert ein Element y, so daß $F = K(x, y)$ ist und die irreduzible Gleichung von y über $K(x)$ die Gestalt

$$y^p - y = B(x)$$

hat, wo $B(x)$ ein Polynom in x ist (Hasse [2]). Die Automorphismengruppe eines solchen Funktionenkörpers untersuche ich genauer in [13]. Wegen $G \neq G(\mathfrak{p})$ und $e' < p^2 - 1$ lassen sich x und y dann so normieren, daß ihre irreduzible Gleichung von der Form

$$y^p + y = x^m, \quad m \geqq 2, \quad p \equiv -1 \pmod{m}, \quad m < p \tag{3.20}$$

ist ([13], Satz 7 und 5). Die Ordnung von G ist in dem Fall kleiner als $16g^4$ ([13], Satz 7).

Im folgenden kann ich $q \geqq p^2$ annehmen (weiterhin ist $r \geqq 2$). Für $p \geqq 3$ gilt $q \geqq 9$, also besagt (3.19)

$$|G| \leqq 8 \cdot \left(\frac{9}{8} \right)^2 \cdot \frac{5}{4} \cdot g^4 + 5 \cdot \frac{q}{2} \cdot g^2. \tag{3.21}$$

Der Faktor bei g^4 ist kleiner als 13, und aus der Geschlechtsformel für F/F_2 folgt

$$2g - 2 \geqq -2q + 3(q-1),$$

weil F_2 der Fixkörper von $G_2(\mathfrak{p})$ ist. Das bedeutet $9 \leqq q \leqq 2g + 1$, mithin $5 \leqq g + 1$ und $q/2 \leqq g + 1$. Nun ergibt (3.21)

$$|G| \leqq 13 \cdot g^4 + (g+1)^2 \cdot g^2 < 16 \cdot g^4.$$

Für $p = 2$ ist r als Teiler von $q^2 - 1$ ungerade. Ist $r \geqq 3$ und $q \geqq 8$ oder $r \geqq 5$ und $q = 4$, dann folgt genauso die Abschätzung $|G| < 16g^4$. Es bleibt daher außer dem Fall $r = 1$ (d.h. $e' = q^2 - 1$) nur noch die Möglichkeit $p = 2$, $q = 4$, $e' = \frac{1}{3}(q^2 - 1) = 5$ zu diskutieren. Ich werde zeigen, daß dieser letzte Fall gar nicht auftritt und daß im Falle $e' = q^2 - 1$ der im Hauptsatz genannte Ausnahmefall $F = K(x, y)$ mit der irreduziblen Gleichung $y^q + y = x^{q+1}$ vorliegt (dabei wird x eventuell um einen Faktor aus K abgeändert).

Zunächst sei $e' = q^2 - 1$. Ich betrachte die Erweiterung $F/K(x^{e'})$. Hier sind genau der Pol $\mathfrak{p}$ und die Nullstellen $\mathfrak{p}', \mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$ von x verzweigt, und zwar voll bzw. mit der Verzweigungsordnung $e' = q^2 - 1$. Das liegt daran, daß in $K(x)/K(x^{e'})$ genau die Nullstelle und der Pol von x verzweigen, während über $F_2 = K(x)$ nur noch $\mathfrak{p}$ verzweigt ist. $K(x^{e'})$ ist in F_H enthalten, weil x eine Kummersche Erzeugende von F über F_H ist. Wegen $q = [F_H : K(x^{e'})] < e'$ müssen also die Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$ auch noch über F_H verzweigen. Zusammen mit $\mathfrak{p}$ und $\mathfrak{p}'$ sind das dann alle Verzweigungsstellen von F/F_H.

Der Automorphismus ω läßt F_H invariant und permutiert daher die Verzweigungsstellen von F/F_H. Weil dabei $\mathfrak{p}$ und $\mathfrak{p}'$ vertauscht werden, werden die Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$ untereinander permutiert. Ich bilde

$$y = \frac{x}{\omega x}. \tag{3.22}$$

Nach (3.15) hat y den Divisor

$$y \cong \frac{\mathfrak{p}'^{q+1}}{\mathfrak{p}^{q+1}}, \tag{3.23}$$

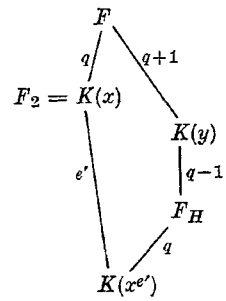
weil sich die Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$ gegen $\omega\mathfrak{p}_1, \ldots, \omega\mathfrak{p}_{q-1}$ wegkürzen. Folglich ist $[F : K(y)] = q + 1$, und wegen $[F : K(x)] = q$ folgt $F = K(x, y)$.

H ist zyklisch von der Ordnung $q^2 - 1$. Demnach existiert eine Untergruppe der Ordnung $q + 1$, nämlich die Menge aller $\sigma \in H$ mit $\sigma^{q+1} = 1$. Von diesen Automorphismen wird y festgelassen:

$$\sigma y = \frac{\sigma x}{\sigma\omega x} = \frac{\chi(\sigma^{-q})x}{\omega\sigma^{-q}x} \quad \text{(vgl. (3.17))}$$

$$= \frac{\chi(\sigma^{-q})x}{\chi(\sigma^{q^2})\omega x} = \chi(\sigma^{q+1})^{-q} y = y.$$

$K(y)$ liegt daher im Fixpunktkörper dieser Gruppe der Ordnung $q + 1$, d.h. $K(y)$ ist der genaue Fixkörper. Das folgende Diagramm verdeutlicht die Lage der einzelnen Körper zueinander; außerdem sind die jeweiligen Körpergrade angegeben.



$\mathfrak{p}_i$ sei eine der Stellen $\mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$. In $F_H/K(x^{e'})$ verzweigt $\mathfrak{p}_i$ höchstens von der Ordnung $q - 1$, weil $\mathfrak{p}_i$ und $\mathfrak{p}'$ Fortsetzungen derselben Stelle von $K(x^{e'})$ sind und $\mathfrak{p}'$ über F_H voll verzweigt. In $K(y)/F_H$ ist $\mathfrak{p}_i$ unverzweigt, denn hier verzweigen $\mathfrak{p}$ und $\mathfrak{p}'$ voll und $K(y)$ ist rational. Diese beiden Stellen sind daher die einzigen Verzweigungsstellen in $K(y)/F_H$, wie die Geschlechtsformel zeigt. In $F/K(x^{e'})$ hat $\mathfrak{p}_i$ die Verzweigungsordnung $q^2 - 1$. Daher ist $\mathfrak{p}_i$ über $K(y)$ voll verzweigt, d.h. in $F/K(y)$ sind genau die $q + 1$ Stellen $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}_1, \ldots, \mathfrak{p}_{q-1}$ verzweigt, und zwar alle voll.

Die Geschlechtsformel für $F/K(y)$ ergibt nun

$$2g-2=-2(q+1)+(q+1)q.$$

Folglich hat F das Geschlecht

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

Ich will das irreduzible Polynom zwischen x und y aufstellen. x^{q+1} liegt in $K(y)$, da x eine Kummersche Erzeugende von F/F_H ist. x^{q+1} hat nur $\mathfrak{p}$ als Pol, ebenso y. Das bedeutet

$$x^{q+1}=A(y), \tag{3.24}$$

wo $A(y)$ ein Polynom aus $K[y]$ vom Grad q ist. Es wird sich herausstellen, daß $A(y)$ die Gestalt $A(y)=ay^q+by$ mit $a, b\neq 0$ hat.

Für eine ganze Zahl t sei $L(\mathfrak{p}^t)$ die Menge aller Elemente von F, welche nur $\mathfrak{p}$ als Pol haben, und zwar höchstens von der Polordnung t. Der Vektorraum $L(\mathfrak{p}^t)$ hat endliche Dimension über K.

Ich betrachte insbesondere den Raum $L(\mathfrak{p}^{2g-1})$. Die Elemente

$$x^iy^j \quad \text{mit} \quad i,j\geqq 0, \quad i+j\leqq q-2 \tag{3.25}$$

liegen alle in $L(\mathfrak{p}^{2g-1})$. Nach (3.15) hat nämlich x den Nenner $\mathfrak{p}^q$, während y den Nenner $\mathfrak{p}^{q+1}$ hat (3.23). Demnach besitzt x^iy^j den Nenner $\mathfrak{p}^{iq+j(q+1)}$. Diese Polordnung läßt sich wie folgt abschätzen:

$$\begin{aligned} iq+j(q+1) &\leqq (i+j)(q+1)\leqq (q-2)(q+1) \quad \text{nach (3.25)}\\ &< q(q-1)-1=2g-1. \end{aligned}$$

Durch (3.25) sind genau $[q(q-1)]/2=g$ verschiedene Elemente definiert. Weil ihre Polordnungen paarweise verschieden sind und $L(\mathfrak{p}^{2g-1})$ nach dem Riemann-Rochschen Satz die Dimension g hat (Chevalley [1], S. 32, Kor. zu Theorem 6), bilden sie eine Basis dieses Raumes. Der Unterraum $L(\mathfrak{p}^{q+1})$ wird dann offenbar von $1, x, y$ aufgespannt.

τ sei ein Automorphismus aus $G_2(\mathfrak{p})$, der Gruppe von $F/K(x)$. Dieser Automorphismus läßt $\mathfrak{p}$ fest und bildet daher $L(\mathfrak{p}^{q+1})$ in sich ab. Insbesondere gilt

$$\tau y=cy+P_\tau(x).$$

Dabei ist $P_\tau(x)$ ein Polynom in x vom Grad 0 oder 1. Der Koeffizient c verschwindet nicht, weil auch τy die Polordnung $q+1$ hat. Aus $\tau^q=1$ folgt $c^q=1$ und damit $c=1$. Wegen

$$P_{\tau\tau'}(x)=P_\tau(x)+P_{\tau'}(x)$$

bilden die Polynome $P_\tau(x)$ eine additive Gruppe. Daher wird durch

$$A^*(y)=\prod_{\tau\in G_2(\mathfrak{p})}(y+P_\tau(x)) \tag{3.26}$$

ein additives Polynom in y über $K(x)$ definiert. $A^*(y)$ hat den Grad q und ist unter allen Automorphismen von $F/K(x)$ invariant, liegt also in $K(x)$. Weil das irreduzible Polynom zwischen x und y bis auf einen konstanten Faktor eindeutig bestimmt ist, folgt durch Vergleich von (3.24) und (3.26)

$$A(y)=d\cdot A^*(y)+d'$$

mit $d\neq 0$. Der Summand d' verschwindet, weil $A(y)$ und $A^*(y)$ die gemeinsame Nullstelle $\mathfrak{p}'$ haben. Mithin ist auch $A(y)$ ein additives Polynom.

Ich setze $q=p^n$ und erhalte aus (3.24)

$$x^{q+1}=a_ny^{p^n}+a_{n-1}y^{p^{n-1}}+\cdots+a_ky^{p^k}+\cdots+a_0y. \tag{3.27}$$

Auf der rechten Seite steht gerade $A(y)$. Die Koeffizienten a_n und a_0 verschwinden nicht, weil $F/K(x)$ den Grad p^n hat und separabel ist.

Als nächstes zeige ich, daß die Koeffizienten $a_{n-1}, \ldots, a_1$ in (3.27) verschwinden. Dazu betrachte ich die Wirkung des Automorphismus ω auf (3.27).

ω bildet F_H in sich ab, und weil $K(y)$ der einzige Oberkörper von F_H vom Grad $q-1$ über

F_H ist, bleibt auch $K(y)$ invariant unter ω. Die Stellen $\mathfrak{p}$ und $\mathfrak{p}'$ werden von ω vertauscht, d.h.

$$\omega y = f/y$$

mit $f \neq 0$. Zusammen mit $\omega x = x/y$ (vgl. (3.22)) ergibt (3.27)

$$\text{(3.28)} \qquad x^{q+1} = y^{q+1}(a_n f^{p^n} y^{-p^n} + \cdots + a_k f^{p^k} y^{-p^k} + \cdots) =$$
$$= a_0 f y^{p^n} + \cdots + a_k f^{p^k} y^{p^n - p^k + 1} + \cdots + a_n f^{p^n} y .$$

Der Koeffizientenvergleich von (3.27) und (3.28) zeigt $a_k = 0$ für $1 \leqq k \leqq n-1$, d.h.

$$x^{q+1} = a_n y^q + a_0 y , \qquad a_n , a_0 \neq 0 .$$

Weil K algebraisch abgeschlossen ist, gibt es Elemente a, b in K mit $a^{q-1} = a_0^{-1} a_n$, $b^{q+1} = a_0^{-1} a$. Ich setze $y^* = ay$ und $x^* = bx$ und erhalte

$$y^{*q} + y^* = a(a^{q-1} y^q + y) = a_0^{-1} a (a_n y^q + a_0 y) = b^{q+1} x^{q+1} = x^{*q+1} .$$

Es gilt also $F = K(x^*, y^*)$ mit

$$\text{(3.29)} \qquad y^{*q} + y^* = x^{*q+1} .$$

Den durch (3.29) definierten Funktionenkörper untersuche ich in [13] genauer. Er hat das Geschlecht $g = \frac{1}{2} q(q-1)$, also $g \geqq 2$ für $q \geqq 3$ ([13], Satz 1). Seine Automorphismengruppe hat die Ordnung

$$|G| = q^3(q^3+1)(q^2-1) > q^4(q-1)^4 = 16 g^4$$

([13], Satz 7).

Der Beweis des Hauptsatzes ist damit außer für den Fall $p = 2$, $q = 4$, $e' = 5$, der vorhin ausgelassen wurde, geführt. Dieser Fall läßt sich ganz ähnlich wie der Fall $e' = q^2 - 1$ behandeln:

Jetzt ist $H = G(\mathfrak{p}) \cap G(\mathfrak{p}')$ von der Ordnung 5 und $[F_H : K(x^5)] = 4$. In $F/K(x^5)$ verzweigen außer $\mathfrak{p}$ genau die Stellen $\mathfrak{p}'$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, und zwar mit der Verzweigungsordnung 5. In F/F_H verzweigt eine Stelle entweder gar nicht oder voll, weil diese Erweiterung galoissch von Primzahlgrad ist. Es folgt, daß in F/F_H genau die Stellen $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ verzweigen. und zwar alle voll. Wie im Fall $e' = q^2 - 1$ folgt, daß der Automorphismus ω die Stellen $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ permutiert. Daher hat $y = x/\omega x$ den Divisor

$$y \cong \frac{\mathfrak{p}'^5}{\mathfrak{p}^5} .$$

y liegt im Fixkörper von H, denn für $\sigma \in H$ gilt

$$\sigma y = \frac{\sigma x}{\sigma \omega x} = \frac{\chi(\sigma)^{-4} x}{\omega \sigma^{-4} x} = \chi(\sigma)^{-4-16} y = y .$$

Folglich ist $F_H = K(y)$.

Nun läßt sich der Beweis wie bei $e' = q^2 - 1$ weiterführen. Nach eventueller Normierung von x und y kommt man zu $F = K(x, y)$ mit der definierenden Gleichung

$$y^4 + y = x^5 .$$

Für diesen Körper gilt jedoch $e' = 15 \neq 5$ ([13], Satz 5); also tritt der Fall $p = 2$, $q = 4$, $e' = 5$ gar nicht auf. Damit ist der Beweis des Hauptsatzes beendet.

Bemerkung. Bei (3.20) habe ich die erst in [13] bewiesene Tatsache benutzt, daß im Fall $e' < p^2 - 1$ der durch

$$y^p - y = B(x)$$

definierte Funktionenkörper $K(x, y)$ eine Automorphismengruppe der Ordnung $|G| < 16 g^4$ hat. Für $p \geqq 11$ bekommt man diese Abschätzung direkt aus (3.19) (vgl. (3.21)).

Literaturverzeichnis

[1] C. CHEVALLEY, Introduction to the theory of algebraic functions of one variable. New York 1951.
[2] H. HASSE, Theorie der relativ zyklischen algebraischen Funktionenkörper. J. Reine Angew. Math. **172**, 37–54 (1934).
[3] B. HUPPERT, Endliche Gruppen I. Berlin-Heidelberg-New York 1967.
[4] A. HURWITZ, Über algebraische Gebilde mit eindeutigen Transformationen in sich. Math. Ann. **41**, 403–442 (1893).
[5] K. IWASAWA and T. TAMAGAWA, On the group of automorphisms of a function field. J. Math. Soc. Japan **3**, 137–147 (1951); **4**, 100–101 und 203–204 (1952).
[6] H. W. LEOPOLDT, Über die Automorphismengruppe des Fermatkörpers. Erscheint demnächst in J. Reine Angew. Math.
[7] A. M. MACBEATH, On a theorem of Hurwitz. Proc. Glasgow Math. Ass. **5**, 90–96 (1961).
[8] P. ROQUETTE, Über die Automorphismengruppe eines algebraischen Funktionenkörpers. Arch. Math. **3**, 343–350 (1952).
[9] P. ROQUETTE, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. **117**, 157–163 (1970).
[10] M. ROSENLICHT, Automorphisms of function fields. Trans. Amer. Math. Soc. **79**, 1–11 (1955).
[11] H. L. SCHMID, Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. J. Reine Angew. Math. **179**, 5–15 (1938).
[12] J. P. SERRE, Corps locaux. Paris 1962.
[13] H. STICHTENOTH, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. Teil II: Ein spezieller Typ von Funktionenkörpern. Erscheint demnächst im Arch. Math.

Eingegangen am 15. 5. 1972

Anschrift des Autors:
Henning Stichtenoth
Lehrstuhl VI für Mathematik
Universität Mannheim (WH)
68 Mannheim
Schloß