Über Funktionenkörper mit vielen Stellen vom Grad eins

Diplomarbeit
von
José Méndez Omaña

Angefertigt am Fachbereich Mathematik
der Technischen Universität Berlin
Berlin 1999

Inhaltsverzeichnis

Einleitung

"Um nun diese Ideen nach einem Prinzip mit systematischer
Präzision aufzählen zu können, müssen wir erstlich bemerken,
daß nur der Verstand es sei, aus welchem reine und transzendentale
Begriffe entspringen können, daß die Vernunft eigentlich gar keinen
Begriff erzeuge, sondern allenfalls nur den Verstandesbegriff von den
unvermeidlichen Einschränkungen einer möglichen Erfahrung frei mache
und ihn also über die Grenzen des Empirischen, doch aber in Verknüpfung
mit demselben zu erweitern suche."
Immanuel Kant, [39].

Riemann führte im Jahr 1857 in seiner Arbeit 'Theorie der Abel'schen Functionen' [64] den Begriff der Darstellung algebraischer Funktionen ein, der heute unter dem Namen Riemannsche Flächen bekannt ist. Algebraische Funktionen werden durch eine Gleichung $f(x,y) = 0$ mit $f(x,y) \in \mathbb{C}[x,y]$ definiert. Grundlage dieser Darstellung ist die Kompaktifizierung der komplexen Zahlen $\mathbb{C}$, die heute als Riemansche Zahlenkugel bekannt ist. Jeder Punkt x_0 auf dieser Zahlenkugel erzeugt ein Primideal bzw. ein maximales Ideal $< x - x_0 > \subset \mathbb{C}[x]$. Diese maximalen Ideale enthalten Nullstellen oder Polstellen einer rationalen Funktion $f \in \mathbb{C}(x)$ und aus diesem Grund werden sie als Stellen bezeichnet. Clebsch und Gordan (1863-66)[6] entwickelten im Anschluß an Riemanns Untersuchungen die Theorie in einem geometrischen Zusammenhang. Diese Darstellung führte zu der algebraisch-geometrischen Betrachtungsweise. Dedekind und Weber (1880) [10] begründeten die Theorie der algebraischen Funktionen unter Verwendung ausschließlich algebraischer Methoden. Der zugrundeliegende Begriff ist der Begriff des Ideals. Hensel und Landsberg [33] setzten die Entwicklung auf dem algebraischen Weg fort und legten der Theorie der algebraischen Funktionen einer Variablen den Divisorbegriff zugrunde. Diese Theorie wurde auf der Grundlage arithmetischer Untersuchungen von Kummer und Kronecker, sowie funktionentheoretischer Methoden von Weierstrass entwickelt und später durch eine allgemeinere Körpertheorie sowie durch die Bewertungstheorie unterbaut. Weil [95] übertrug das Wesentliche der funktionentheoretischen Ansätze ins rein Algebrai-

sche. Dieser Rückblick soll erklären, warum man in der Literatur die Begriffe des Primdivisors vom Grad eins, des maximalen Ideals eines Bewertungsringes, des rationalen Punktes und der Stelle synonym verwendet.
Die algebraischen Funktionen auf einer Riemannschen Fläche bilden einen Körper und aus diesem Grund spricht man in algebraischem Zusammenhang von einem algebraischen Funktionenkörper. Die Theorie der algebraischen Funktionenkörper bildet eine Brücke zwischen der Funktionentheorie, der algebraischen Geometrie und der algebraischen Zahlentheorie.
Wenn man nicht $\mathbb{C}$, sondern einen Körper k wie $\mathbb{Q}$ oder einen endlichen Körper als Ausgangspunkt für die Untersuchungen verwendet, entsteht eine Theorie, die in zahlentheoretischem bzw. algebraisch-geometrischem Zusammenhang von Bedeutung ist. Eine der interessantesten Fragen ist: Wie groß ist die Anzahl der Lösungen (α, β) der Gleichung $f(x, y) = 0$ mit $f(x, y) \in k[x, y]$, so daß $(\alpha, \beta) \in k \times k$? Der Grad einer Stelle gibt Auskunft darüber, ob man k oder eine Erweiterung von k betrachten muß. Im Falle der Stellen vom Grad eins betrachtet man k. Ein Funktionenkörper mit vielen Stellen vom Grad eins ist ein Körper, dessen definierende Gleichung viele Lösungen in $k \times k$ hat. Beschränkt man sich auf einen Teilring $R \subset k$ (z.B. $\mathbb{Z} \subset \mathbb{Q}$) so liegt nahe, daß es eine Verbindung mit der Theorie der Diophantischen Gleichungen gibt. Im Falle eines Zahlkörpers weiß man, daß es endlich viele Lösungen gibt, wie die Arbeiten von Faltings [17] und Wiles [97] zeigen. Ist k endlich, so ist die Anzahl der Lösungen offensichtlich endlich, die Frage ist nun die Bestimmung der Anzahl der Lösungen bzw. von Schranken für die Anzahl der Lösungen; die Beantwortung dieser Frage ist nicht trivial [50]. Im Folgenden wird die Gliederung der vorliegenden Arbeit erläutert:
In Kapitel 1 werden die Begriffe aus der allgemeinen Körpertheorie sowie aus der Theorie der endlichen Körper zusammengestellt, die später entweder verwendet werden oder einfach das Verständnis der Begriffe der Theorie der algebraischen Funktionenkörper erleichtern sollen. Im Abschnitt über algebraische Funktionenkörper wird, außer der Einführung von Notation und grundlegenden Definitionen, auf die Erzeugung der Funktionenkörper und auf ihre Darstellung, bzw. auf die Darstellung der Elemente des Funktionenkörpers eingegangen. Im letzten Abschnitt dieses Kapitels werden Grundbegriffe vorgestellt, die eine algebraisch-geometrische Interpretation der Ergebnise der Theorie der algebraischen Funktionenkörper ermöglichen.
Kapitel 2 führt die von uns verwendeten Begriffe der Bewertungstheorie ein, und zwar nur in diesem sehr beschränkten Umfang. Die Bewertungstheorie ermöglicht u.a. Aussagen über Teilbarkeit in Aussagen über eine Abbildung auf eine geordnete Gruppe zu übertragen. Anschließend wird der Begriff der Stelle vorgestellt.
In Kapitel 3 werden der Begriff des Divisors eines Funktionenkörpers definiert und

Aussagen über die Struktur der Menge der Divisoren eines Funktionenkörpers gemacht.

In Kapitel 4 wird der Satz von Riemann–Roch formuliert. Es handelt sich um die wichtigste Aussage der Theorie der algebraischen Funktionenkörper.

In Kapitel 5 werden grundlegende Begriffe, die bei der Untersuchung von Funktionenklassen von gegebenem Geschlecht verwendet werden, eingeführt und Gleichungen, die Funktionenkörper von gegebenem Geschlecht definieren, konstruiert. Da uns aber der Fall eines endlichen Konstantenkörpers interessiert, wird in Kapitel 6 eine Verallgemeinerung des Begriffes der Reduktion modulo p definiert, um u.a. die Übertragbarkeit aller vorher erstellten Gleichungen auf diesen Fall sicherzustellen.
In Kapitel 7 werden Schranken für die Anzahl der Primdivisoren vom Grad eins eines Funktionenkörpers und Methoden zur Konstruktion von Funktionenkörpern mit vielen Primdivisoren vom Grad eins vorgestellt.
Eines der Hauptziele dieser Arbeit ist eine Einführung in die Untersuchung von Klassen von Funktionenkörpern und der Anzahl der Primdivisoren vom Grad eins der Funktionenkörper einer Klasse. Es werden zwei klassische Probleme angesprochen und zwar die Untersuchung der Modulvarietät der Funktionenkörper von gegebenem Geschlecht über einem Körper k und die Bestimmung der Anzahl der rationalen Punkte einer Kurve (die Primdivisoren vom Grad eins des entsprechenden Funktionenkörpers).

Der gewählte Zugang zu diesen Problemen verwendet nur arithmetisch-algebraische Methoden und geringe technische Mittel. Abschließend wird anhand von Beispielen gezeigt, wie die entwickelte Theorie zur expliziten Konstruktion von Funktionenkörpern mit vielen Primdivisoren vom Grad eins angewandt werden kann, wie man experimentell mögliche Zusammenhänge zwischen der Modulvarietät elliptischer Kurven über $\mathbb{F}_{2^4}$, Konstantenkörpererweiterungen und der Anzahl der rationalen Punkten auf den Kurven erschließen kann.
Zum Schluß soll erwähnt werden, daß ein faszinierender Aspekt dieses Forschungsgebietes nicht nur das Aufwerfen von Fragen, wie die nach der eventuellen Existenz von Kurven, die mehr Punkte als der zugrundeliegende Raum haben, ist, sondern auch die Möglichkeit von Anwendungen auf das Gebiet der Informationsübertragungstechnologie (Codierungstheorie) und der Kryptographie [43].

Kapitel 1

Grundlagen

1.1 Körpertheorie

1.1. Definition. Ein algebraischer Funktionenkörper F/k (in einer Variablen) über einem Körper k ist eine Körpererweiterung F von k, so daß F eine endliche Erweiterung von $k(x)$ für ein über k transzendentes Element $x \in F$ ist.

Die in diesem Teilabschnitt vorgestellten Begriffe und Ergebnisse findet man in einigen Standardwerke der Algebra, Algebraischen Geometrie und der Theorie der algebraischen Funktionenkörper ([5, 8, 15, 16, 31, 54, 81, 92, 99]).
Ein algebraischer Funktionenkörper wird durch sukzessive Erweiterungen konstruiert. Die erste davon ist transzendent und besitzt eine Basis. Wir betrachten allgemein eine Körpererweiterung L/K. Eine endliche Menge $\{x_1, \ldots, x_n\} \subseteq L$ heißt algebraisch unabhängig über K, wenn es kein $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ gibt, so daß $f(x_1, \ldots, x_n) = 0$. Eine Transzendenzbasis von L/K ist ein maximales Element (bezüglich Inklusion) in der Menge aller über K algebraisch unabhängigen Mengen aus L. Die Kardinalität einer Transzendenzbasis heißt Transzendenzgrad von L/K.
Je zwei Transzendenzbasen haben die gleiche Kardinalität. Ist der Transzendenzgrad von L/K endlich und ist $\{x_1, \ldots, x_n\}$ eine Transzendenzbasis von L/K, dann ist der Körper $K(x_1, \ldots, x_n) \subseteq L$ isomorph zum Quotientenkörper des Polynomrings $K[X_1, \ldots, X_n]$ in n Variabeln über K.
Da ein algebraischer Funktionenkörper eine algebraische Erweiterung von $k(x)$ ist, erwähnen wir in diesem Zusammenhang einige Definitionen und Sätze:

1.2. Definition. Es sei ρ algebraisch über K. Das normierte irreduzible Polynom $m_\rho(t) \in K[t]$ mit $m_\rho(\rho) = 0$ heißt Minimalpolynom von ρ über K.

1.3. Proposition. *Es sei ρ algebraisch über K. Dann gilt:*

1. $[K(\rho) : K] = \deg(m_\rho)$,

2. $\{1, \rho, \ldots, \rho^{\deg(m_\rho)-1}\}$ *ist eine* K*-Basis von* $K(\rho)$.

Ein Körper K heißt algebraisch abgeschlossen, falls für jede algebraische Erweiterung L/K bereits $L = K$ gilt. Der Körper $\bar{K}$ heißt algebraischer Abschluß von K, falls $\bar{K}/K$ algebraisch und $\bar{K}$ algebraisch abgeschlossen ist.
Algebraisch abgeschlossene Körper sind immer unendlich. Endliche Körper sind also nicht algebraisch abgeschlossen. Der algebraische Abschluß eines endlichen Körpers besteht aus Einheitswurzeln.

1.4. Satz. *Zu jedem Körper* K *existiert ein algebraischer Abschluß* $\bar{K}$ *. Der Erweiterungskörper* $\bar{K}$ *ist bis auf* K*-Isomorphismus eindeutig definiert.*

Es gibt grundlegende Begriffe und strukturelle Aussagen der Theorie der algebraischen Funktionenkörper über einen Körper der Charakteristik $\chi(K)=p$, die die Existenz eines Elementes mit bestimmten Eigenschaften voraussetzen.
Es sei L/K eine Körpererweiterung. Ein über K algebraisches Element $x \in L$ heißt separabel über K, falls sein Minimalpolynom m_x über K separabel ist. Die Körpererweiterung L/K heißt separabel, falls L/K algebraisch und jedes $x \in L$ separabel über K ist. Eine nicht separable algebraische Körpererweiterung L/K heißt inseparabel.

1.5. Definition. Ein Element $x \in L$ heißt separierendes Element von L/K, falls L/K eine endliche separable Körpererweiterung ist. Wenn es ein separierendes Element von L/K gibt, dann heißt L/K eine separabel erzeugte Körpererweiterung.

Ein Element $x \in L$ heißt rein inseparabel über K, falls $m_x(t) = (t-x)^n$ für ein $n \in \mathbb{N}$ gilt. Eine Körpererweiterung L/K heißt rein inseparabel, falls L/K algebraisch und jedes Element aus L rein inseparabel über K ist.

1.6. Proposition. *Es sei* L/K *endlich mit* $\chi(K) = p$ *und rein inseparabel. Dann gilt:* $[L : K]$ *ist* p*-te Potenz.*

Unter den Strukturen, die in der Theorie der algebraischen Funktionenkörper eine herausragende Rolle spielen und bei denen separierende Elemente von Bedeutung sind, befindet sich eine Verallgemeinerung des klassischen Differentialbegriffs:

1.7. Definition. Es sei R ein Ring mit 1 und M ein R-Modul. Eine Abbildung $D : R \to M$ heißt Derivation, falls

$$D(a+b) = D(a) + D(b), \quad D(ab) = D(a)\, b + a\, D(b) \quad \forall a,\, b \in R$$

gilt.

Aus der Definition folgt, daß für $1 \in R$ gilt:
$D(1+1) = D(1) + D(1) = D(1 \cdot 1)$. Dies bedeutet: $D(1) = 0$.

1.8. Definition. Es seien L/K eine Körpererweiterung und $x \in L/K$ ein separierendes Element. Die eindeutig definierte Derivation $D_x : L \to L$ mit der Eigenschaft $D_x(x) \mapsto 1$ heißt Derivation bezüglich x.

Für die Abbildungskomposition im Falle einer Derivation verwenden wir folgende Bezeichnung: $D_x \circ D_y = D_x(D_y) = D_{xy}$
Ein bekanntes Beispiel für eine Derivation ist jede formale partielle Ableitung $\frac{\partial}{\partial x_i} : R \to R$ wobei $R[x_1, \dots, x_n]$ der Polynomring in n Unbestimmten über einem Ring R ist. Wenn M ein Vektorraum über einem Körper K ist, dann gilt: Es sei $x \in K^\times$. Aus $0 = D(xx^{-1}) = x^{-1}D(x) + xD(x^{-1})$ folgt, daß $D(x^{-1}) = -x^{-2}D(x)$. Schlüsse dieser Art begründen den ersten Teil der folgenden Aussage:

1.9. Proposition. *1. Es sei R ein Integritätsbereich mit Quotientenkörper K. Jede Derivation auf R hat eine eindeutige Erweiterung auf K.*

2. Es sei L/K eine algebraische separable Erweiterung. Jede Derivation auf K hat eine eindeutige Erweiterung auf L.

Bei der Konstruktion algebraischer Funktionenkörper sind zwei Erweiterungstypen von besonderer Bedeutung: Artin-Schreier-Erweiterungen und Kummer-Erweiterungen:

1.10. Definition. Es sei K ein Körper mit $\chi(K) = p$ und L/K eine zyklische Erweiterung vom Grad $[L : K] = n$. Es gelte $\mathrm{ggT}(p, n) = 1$ und K enthalte eine n-te Einheitswurzel (d.h. $T^n - 1$ zerfällt in lineare Faktoren in K[T]). Dann existiert ein Element $\rho \in L$ so daß $L = K(\rho)$ mit

$$\rho^n = c \in K, \text{ und } c \neq w^d \text{ für alle } w \in K \text{ und } d|n, d \geq 1$$

Eine Körpererweiterung mit diesen Eigenschaften heißt Kummer Erweiterung.

Die Automorphismen σ aus $\mathrm{Gal}(L/K)$ einer Kummer-Erweiterung werden durch $\sigma(\rho) = \xi \cdot \rho$ definiert, mit einer n-ten Einheitswurzel $\xi \in K$.
Wenn der Primkörper K der Charakteristik $\chi(K) = p$ ist und man eine nicht rein inseparable Erweiterung konstruieren will, verwendet man häufig Artin–Schreier–Erweiterungen:

1.11. Definition. Es sei K ein Körper mit $\chi(K) = p$ und L/K eine zyklische Erweiterung vom Grad $[L : K] = p$. Dann existiert ein Element $\rho \in L$, so daß $L = K(\rho)$ mit

$$\rho^p - \rho = c \in K, \text{ und } c \neq \rho^p - \rho \text{ für alle } \rho \in K.$$

Eine Körpererweiterung mit diesen Eigenschaften heißt Artin-Schreier-Erweiterung vom Grad p.

Die Automorphismen $\sigma \in Gal(L/K)$ einer Artin-Schreier Erweiterung werden durch $\sigma(\rho) = \rho + \nu$ definiert, mit $\nu \in \mathbb{Z}/p\mathbb{Z} \subseteq K$

1.2 Endliche Körper

Die Theorie der algebraischen Funktionenkörper über einem endlichen Körper $\mathbb{F}_q$ mit q Elementen hat große Bedeutung in theoretischer und praktischer Hinsicht. Funktionenkörper über einem endlichen Körper heißen globale Funktionenkörper. Globale Funktionenkörper haben eine weitgehende Analogie zu den algebraischen Zahlkörpern ([8, 32]). Für eine anwendungsorientierte Behandlung des Themas siehe [38, 52]. Es gibt einen Zusammenhang zwischen irreduziblen Polynomen und bestimmten Grundobjekten algebraischer Funktionenkörper, die wir später kennenlernen werden, den Primdivisoren eines algebraischen Funktionenkörpers. Aus diesem Grund stellen wir die folgende Definitionen und Sätze vor:

1.12. Lemma. *Es sei $\mathbb{F}_q = \mathbb{F}_{p^n}$ und $k \in \mathbb{Z}^{>0}$. Dann ist $t^{q^k} - t \in \mathbb{F}_q[t]$ das Produkt aller normierten irreduziblen Polynome $g \in \mathbb{F}_q[t]$ vom Grad d mit $d|k$.*

1.13. Proposition. *Ein normiertes Polynom $f \in \mathbb{F}_q[t]$ ist irreduzibel genau dann wenn $ggT(f(t), t^{q^j} - t) = 1$ für alle j mit $1 \leq j \leq \frac{\deg(f)}{2}$.*

Für einen Beweis siehe[61]

1.14. Definition. Die Möbius μ-Funktion $\mu : \mathbb{N} \to \mathbb{N}$ wird definiert durch:

$$\mu(x) = \begin{cases} 1 & \text{falls } x = 1 \\ (-1)^r & \text{wenn } x \text{ ein Produkt } r \text{ verschiedener Primzahlen ist} \\ 0 & \text{falls in } x \text{ ein quadratischer Faktor enthalten ist} \end{cases}$$

1.15. Satz. *$A_{m,q}$ bezeichne die Anzahl aller irreduziblen normierten Polynome vom Grad m in $\mathbb{F}_q[t]$. Dann gilt:*
(a) $q^m = \sum_{d|m} dA_{d,q}$.
(b) $A_{m,q} = \frac{1}{m} \sum_{d|n} \mu(d) q^{m/d}$.
(c) $A_{m,q} \geq 1$.
(d) $A_{m,q} \sim \frac{1/m}{q^m}$ für $m \to \infty$.

q^m ist die Anzahl der normierten Polynome m-ten Grades von $\mathbb{F}_q[t]$. Auf der Suche nach einem irreduziblen Polynom nach dem Zufallsprinzip, dürfte man nach etwa m Versuchen Erfolg haben. Zum Thema Faktorisierungsalgorithmen und Irreduzibilitätstests verweisen wir auf [60] und [38]

$\mathbb{F}_{q^n}$ ist ein $\mathbb{F}_q$-Vektorraum. Die Körpererweiterung $\mathbb{F}_{q^n}/\mathbb{F}_q$ ist eine Galois Erweiterung vom Grad n. Die Galoisgruppe ist zyklisch und wird durch den Frobenius-Automorphismus $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, definiert durch $\phi : \alpha \mapsto \alpha^q$, erzeugt. Diese Art von Erweiterungen kommen insbesondere vor, wenn man den Primkörper eines algebraischen Funktionenkörpers erweitert.

1.3 Algebraische Funktionenkörper

In diesem Abschnitt werden die für die Arbeit relevanten theoretischen Grundlagen über algebraische Funktionenkörper bereitgestellt und Notationen vereinbart. Für allgemeine Einführungen in die Theorie der algebraischen Funktionenkörper (einer Variablen) verweisen wir auf [8, 13, 15, 81], für detallierte Darstellungen werden [32] und [33] empfohlen. Hinsichtlich algorithmischer Aspekte verweisen wir auf [7, 34, 60, 61, 68, 77]. Es sei k ein Körper. Ein algebraischer Funktionenkörper F/k ist eine endlich erzeugte Erweiterung über k vom Transzendenzgrad $r \geq 1$. Man spricht von einem algebraischen Funktionenkörper in r Variablen. In dieser Arbeit betrachten wir nur endlich erzeugte Körpererweiterungen über k vom Transzendenzgrad eins. Für eine Einführung in die Theorie der algebraischen Funktionenkörper vom Transzendenzgrad zwei verweisen wir auf [8].

$$k \quad \text{sei ein vollkommener Körper}$$

Wie bereits erwähnt:
Ein algebraischer Funktionenkörper F/k (in einer Variablen) über einem Körper k ist eine Körpererweiterung F von k, so daß F eine endliche Erweiterung von $k(x)$ für ein über k transzendentes Element $x \in F$ ist.
Der Körper k wird Konstantenkörper genannt. Der algebraische Abschluß $\bar{k}$ von k in F hat endlichen Grad über k und wird der exakte Konstantenkörper von F/k genannt.
Künftig verwenden wir den Ausdruck Funktionenkörper anstelle von algebraischem Funktionenkörper. Wir gehen zunächst auf die Darstellung von Funktionenkörpern und dann auf die seiner Elementen ein:

1.16. Proposition. *Es seien k ein vollkommener Körper, x transzendent über k, ein irreduzibles Polynom $f \in k[x, y]$ mit $\deg_y(f) = n$, welches bezüglich y normiert und separabel ist, und $\rho \in \overline{k(x)}$ mit $f(x, \rho) = 0$. Dann gilt:*
$F = k(x, \rho)$ ist ein Funktionenkörper mit $n = [F : k(x)]$, und jeder Funktionenkörper F kann auf diese Weise durch eine geeignete Wahl von $x \in F$ separabel über $k(x)$ erzeugt werden. Ein solches x heißt separierendes Element von F/k.

1.17. Proposition. *Es seien k ein vollkommener Körper und F/k ein Funktionenkörper über k.*
(a) Es sei $z \in F$ so daß z keine p-te Potenz ist. Dann ist z ein separierendes Element für F/k. Insbesondere ist F/k separabel erzeugt.
(b) Es existieren $x, y \in F/k$, so daß $F = k(x,y)$.
(c) Für $n \geq 1$ ist die Menge $F^{p^n} := \{z^{p^n} | z \in F\}$ ein Teilkörper von F mit folgenden Eigenschaften:
(1) $k \subseteq F^{p^n} \subseteq F$ und F/F^{p^n} ist eine rein inseparable Körpererweiterung vom Grad p^n.
(2) Die Frobenius-Abbildung $\phi_n : F \to F$, definiert durch $\phi_n : z \mapsto z^{p^n}$, ist ein Isomorphismus von F auf F^{p^n}. Infolgedessen hat der Funktionenkörper F^{p^n}/k das gleiche Geschlecht wie F/k.
(3) Es sei $k \subseteq F_0 \subseteq F$, so daß F/F_0 rein inseparabel vom Grad $[F : F_0] = p^n$ ist. Dann ist $F_0 = F^{p^n}$.

Ein Element $z \in F$ ist ein separierendes Element von F/k, genau dann wenn $z \notin F^p$. Jedes transzendente Element x aus F/k kann als unabhängige Variable eingesetzt werden, um den Körper $k(x)$ zu konstruieren. Ist y ein weiteres transzendentes Element von F/k, so muß $f(x,y) = 0$ gelten, mit $f \in k[x,y]$ und f ist nicht das Nullpolynom $0 \in k[x,y]$. Da y transzendent ist, kann x nicht algebraisch unabhängig über $k(y)$ sein. Darüberhinaus gilt nach Konstruktion: $[F : k(y)] = [F : k(x,y)][k(x,y) : k(y)] \leq [F : k(x)][k(x,y) : k(y)] \leq \infty$
Wenn $f(x,y)k(x)[y]$ das in $k(x)[y]$ von f erzeugte Hauptideal ist, dann ist der Ring $k(x)[y]/f(x,y)k(x)[y]$ ein Integritätsbereich. Der entsprechende Quotientenring ist ein Körper. Das Element $\rho \in \overline{k(x)}$ mit $f(x,\rho) = 0$ wird formal durch die Bildung dieses Quotienten bestimmt. Es handelt sich um die $k(x)$-Algebra

$$k(x)[y]/f(x,y)k(x)[y] \;=\; k(x) + k(x)\rho + k(x)\rho^2 + \cdots + k(x)\rho^{n-1}$$

Wenn es ein Element $\xi \in F$ gibt, so daß $f(x,\xi) = 0$ über $k(x)$ dann sind die Funktionenkörper $F = k(x,\rho)$ und $F' = (x,\xi)$ isomorph.
Der Oberring $\mathfrak{o}_F := k[x,\rho]$ von $k[x]$ heißt endliche $k[x]$-Gleichungsordnung.
Die Abbildung von $k[x,y]$ nach $k[x,\rho]$, definiert durch $f(x,y) \mapsto f(x,\rho)$, ist ein Homomorphismus.
Jedes Element des Funktionenkörpers $F = k(x,\rho)$ kann als Polynom in ρ vom Grad kleiner als $\deg_y(f) = n$ dargestellt werden. Der Beweis dieser Behauptung ist eine einfache Anwendung des Divisionalgorithmus in $k(x)[\rho]$. Die folgende Aussage, sowie der entsprechende Beweis, werden, vor allem mit dem Ziel, einen Einblick in die Arithmetik algebraischer Funktionenkörper zu bieten, vorgestellt.

1.18. Proposition. *Es sei $F = k(x, \rho)$ ein Funktionenkörper über k, definiert durch $f(x, \rho) = 0$ mit $f \in k[x, y]$ und $\deg_y(f) = n$. Jedes Element $\xi \in F$ ist Wurzel einer Gleichung über $k(x)$ vom Grad höchstens n und falls $F = k(x, \rho) \cong F' = k(x, \xi)$ gilt, dann ist die Gleichung irreduzibel vom Grad n.*

Beweis. $1, \xi, \ldots, \xi^m$ sind Elemente aus $F = k(x, \rho)$ und die Menge $\{1, \rho, \ldots, \rho^{n-1}\}$ ist eine Basis des n-dimensionalen $k(x)$-Vektorraumes $[F : k(x)]$:

$$\begin{aligned} 1 &= 1 \\ \xi &= \mathrm{a}_{1,0} + \mathrm{a}_{1,1}\rho + \cdots + \mathrm{a}_{1,\mathrm{n}-1}\rho^{\mathrm{n}-1} \\ \xi^2 &= \mathrm{a}_{2,0} + \mathrm{a}_{2,1}\rho + \cdots + \mathrm{a}_{2,\mathrm{n}-1}\rho^{\mathrm{n}-1} \quad . \\ &\cdots\cdots\cdots \\ \xi^{\mathrm{n}} &= \mathrm{a}_{\mathrm{n},0} + \mathrm{a}_{\mathrm{n},1}\rho + \cdots + \mathrm{a}_{\mathrm{n},\mathrm{n}-1}\rho^{\mathrm{n}-1} \end{aligned}$$

$1, \xi, \ldots, \xi^n$ sind $n+1$ Elemente aus einem n-dimensionalen Vektorraums. Sie sind linear abhängig über $k(x)$: Es existieren $b_0, \ldots, b_n \in k(x)$ nicht alle gleich Null, so daß $b_0, b_1\xi + \cdots, b_n\xi^n = 0$. Wenn $F_1 = (x, \rho)$ $k(x)$-Isomorph zu $F_2 = (x, \xi)$ ist und ξ eine irreduzible Gleichung vom Grad m erfüllt, dann gilt $m \leq n$. Analog gilt $n \leq m$ und damit $m = n$.$\square$.

1.4 Funktionenkörper und algebraische Geometrie

In diesem Abschnitt gehen wir auf die geometrische Interpretation algebraischer Funktionenkörper ein. Für eine Einführung in die algebraische Geometrie wird auf [9, 21, 31, 63, 66, 94] verwiesen. Entsprechende Kapitel aus [26, 76] werden empfohlen. In [74] werden die Grundlagen der algebraischen Geometrie über einem vollkommenen Körper entwickelt. Diese ist eine wichtige Voraussetzung, wenn man globale Funktionenkörper betrachtet.

1.19. Definition. Es sei k ein Körper und $n \in \mathbb{Z}^{>0}$. Der n-dimensional affine Raum über k ist die Menge

$$\mathbf{A}^n(k) := \{P = (a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}.$$

P heißt Punkt in $\mathbf{A}^n(k)$ und die $a_1, \ldots, a_n$ heißen Koordinaten von P

Auf der Menge $\mathbf{A}^{n+1}(k)\backslash\{0, \ldots, 0\}$ wird eine Äquivalenzrelation definiert durch:

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$$

genau dann, wenn es ein Element $0 \neq \lambda \in k$ gibt so daß $b_i = \lambda a_i$ für $0 \leq i \leq n$. Für die Äquivalenzklasse von $(a_0, a_1, \ldots, a_n)$ bezüglich $\sim$ verwendet man die Bezeichnung $(a_0 : \ldots : a_n)$. Die Menge der so definierten Äquivalenzklassen heißt der n-dimensional projektive Raum $\mathbf{P}^n(k)$ über k:

$$\mathbf{P}^n(k) := \{P = (a_0 : \ldots : a_n) \mid a_0, \ldots, a_n \in k, \quad \text{nicht alle } a_i = 0\}$$

Man kann sich $\mathbf{P}^1(k)$ als $\mathbf{A}^1(k) \cup \{\infty\}$ vorstellen und $\mathbf{P}^2(k)$ als $\mathbf{A}^2(k) \cup \mathbf{P}^1(k)$ [76].

Es ist möglich eine Verbindung zwischen einem geometrischen Objekt und einem beliebigen kommutativen Ring herzustellen: Diese Verbindung heißt $\mathbf{Spec}\, R$.

1.20. Definition. Die Menge aller Primideale eines Ringes R heißt Spektrum von R. Die Bezeichnung ist $\mathbf{Spec}\, R$

1.21. Beispiel.

1. Im Ring $\mathbb{Z}$ ist $\mathbf{Spec}\,\mathbb{Z} = \{\langle 0\rangle\} \cup \{\langle p\rangle \mid p \text{ ist eine Primzahl}\}$.
2. Es sei k ein Körper, dann ist $\mathbf{Spec}\, k = \{\langle 0\rangle\}$.
3. Es sei k ein algebraisch abgeschlossener Körper und x transzendent über k. Wir betrachten den Ring $k[x]$. Dann ist
$\mathbf{Spec}\, k[x] = \{\langle 0\rangle\} \cup \{\langle x - \alpha\rangle \mid \alpha \in k\}$.
4. Es sei k ein algebraisch abgeschlossener Körper und x, y transzendent über k. Wir betrachten den Ring $k[x, y]$. Dann gilt:
$\mathbf{Spec}\, k[x, y] = \{\langle 0\rangle\} \cup \{\langle f\rangle \mid f \in k[x, y] \text{ irreduzibel und nicht konstant}\}$
$\cup \{\langle x - \xi, y - \rho\rangle \mid (\xi, \rho) \in \mathbf{A}^2(k)\}$
Beweis: Wir zeigen, daß alle Primideale $\mathfrak{p} \in k[x, y]$, die keine Hauptideale sind, der Form $\mathfrak{p} = \langle x - \xi, y - \rho\rangle$ sind. Es sei $f \in \mathfrak{p} \backslash \{0\}$ irreduzibel von minimalen Grad $deg_y\, f$. Da $\mathfrak{p}$ kein Hauptideal ist, existiert $g \in \mathfrak{p} \backslash \langle f\rangle$. Durch Anwendung des Euklidischen Algorithmus in $k(x)[y]$ erhält man ein Polynom $p \in k[x] \backslash \langle 0\rangle$ und $q, r \in k[x, y]$ mit $pg = qf + r$, wobei entweder $r = 0$ oder $deg_y\, r \langle deg_y\, f$. Aus den Voraussetzungen für f und weil $r = pg - qf \in \mathfrak{p}$ folgt $r = 0$. Weil $\langle f\rangle$ ein Primideal ist und $pg = qf \in \langle f\rangle$ sowie $g \notin \langle f\rangle$ gilt: $p \in \langle f\rangle$. Es ist also $\deg_y f \leq \deg_y p = 0$ und damit $f \in k[x]$. Da k algebraisch abgeschlossen und f irreduzibel ist, muß $f = x - \xi, \xi \in k$ ein Polynom vom Grad eins in x sein. Analog erhält man für y: $y - \rho, \rho \in k$ ist ein Polynom vom Grad eins. Dann gilt $\langle x - \xi, y - \rho\rangle = \mathfrak{p}$.$\square$
5. Die sogenannte arithmetische Fläche $\mathbf{Spec}\,\mathbb{Z}[x] = \{\langle 0\rangle\}$
$\cup \{\langle f\rangle \mid f \in \mathbb{Z}[x]\ \mathbb{Q}\text{-irreduzibel, primitiv und nicht konstant}\}$
$\cup \{\langle p\rangle \mid p \text{ ist eine Primzahl}\}$.
$\cup \{\langle p, f\rangle \mid p \text{ ist eine Primzahl}, f \in \mathbb{Z}[x] \mod p\text{-irreduzibel, normiert}\}$
f ist auch hier nicht konstant.

1.22. Definition. Es seien k ein Körper, L eine Erweiterung über k und der Teilring $k[x_1, \dots, x_n] \subset L$. Eine affine Varietät $\mathbf{V}$ über k ist die Menge $\mathbf{V} := \mathbf{Spec}\, k[x_1, \dots, x_n]$ der k-linearen Ringhomomorphismen von $k[x_1, \dots, x_n]$ in den algebraischen Abschluss $\bar{k}$ von k.

Diese zunächst zu abstrakt erscheinende Definition ist notwendig wenn man die Separabilität der Körpererweiterungen berücksichtigen muß. Die moderne Literatur auf diesem Gebiet benutzt in der Regel die Sprache der Schemata, auf die wir nicht eingehen. Ein affines Schema ist ein Objekt, das isomorph zu $\mathbf{Spec}\, R$, versehenen mit einer zusätzlichen Struktur, ist [31, 56]. Die Bedeutung der Darstellung einer Varietät als Spektrum eines Ringes findet man einfach erläutert in [63].

1.23. Definition. Der algebraische Funktionenkörper $K(\mathbf{V})$ einer affinen Varietät $\mathbf{V}$ über k ist der Quotientenkörper $K(\mathbf{V}) = k(x_1, \dots, x_n)$ von $k[x_1, \dots, x_n]$ über k. Der Teilring $k[x_1, \dots, x_n]$ von $K(\mathbf{V})$ heißt Ring der regulären Funktionen von $\mathbf{V}$.

Eine affine Varietät heißt separabel, falls ihr Funktionenkörper eine separable Erweiterung ist. Für eine affine separable Varietät läßt sich die angegebene Definition einer Varietät wie folgt formulieren:

Es sei k ein vollkommener Körper und es seien $f_1, \dots, f_s$ Polynome aus $k[x_1, \dots, x_n]$. Die Menge

$$\mathbf{V}(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in \mathbf{A}^n(k) \mid f_i(a_1, \dots, a_n) = 0\, \forall\, 1 \leq i \leq s\}.$$

heißt affine Varietät $\mathbf{V}(f_1, \dots, f_s)$, definiert durch $f_1, \dots, f_s$. Für konstruktive Ansätze wird diese Definition, zugrundegelegt [9].
Eine bestimmte Teilmenge einer über einem Körper k definierten Varietät ist von besonderem Interesse: Die Punkte deren Koordinaten Elemente aus k sind: Man betrachtet eine affine Varietät $\mathbf{V}(k)$. Die Menge

$$\mathbf{V}(k) := \mathbf{V} \cap \mathbf{A}^n(k) = \{P = (a_1, \dots, a_n) \in \mathbf{V} \mid \text{alle } a_i \in k\}$$

heißt Menge der k-rationalen Punkte von $\mathbf{V}$. In diesem Zusammenhang ergeben sich einige Fragen:
Was ist die Kardinalität dieser Menge? Besondere Bedeutung gewinnt diese Frage, wenn der Primkörper ein endlicher Körper ist. Eine weitere Frage ist: Wie definiert man Varietäten, die viele rationale Punkte enthalten? Hat diese Teilmenge einer Varietät eine Struktur?

Die ersten zwei Fragen sind Gegenstand dieser Arbeit. Nun betrachten wir weitere mit einer Varietät zusammenhängenden Strukturen: Es sei $k[X_1, \dots, X_n]$ der Polynomring in n unabhängigen Variablen über k. Das Ideal

$$I_k(\mathbf{V}) := \{f \in k[X_1, \dots, X_n] \mid f(x_1, \dots, x_n) = 0 \text{ für alle } x_1, \dots, x_n \in \mathbf{V}\}$$

heißt Ideal von $\mathbf{V}$.

Der Restklassenring $\Gamma = k[X_1, \dots, X_n]/I_k(\mathbf{V})$ heißt Koordinatenring der affinen Varietät $\mathbf{V}$.
$I_k(\mathbf{V})$ ist der Kern der Homomorphismen von $k[X_1, \dots, X_n]$ nach $k[x_1, \dots, x_n]$ definiert durch $f(X_1, \dots, X_n) \mapsto f(x_1, \dots, x_n)$. Dann ist

$$k[X_1, \dots, X_n]/I_k(\mathbf{V}) \cong k[x_1, \dots, x_n]$$

Da $k[x_1, \dots, x_n]$ ein Integritätsbereich ist, ist $I_k(\mathbf{V})$ ein Primideal, also ein Element aus $\mathbf{Spec}\, k[x_1, \dots, x_n]$.
Wir benötigen einen Begriff, der dazu dient die Varietäten zu charakterisieren, die mit den Funktionenkörpern einer Variablen in Verbindung stehen:
Die Dimension einer Varietät $\mathbf{V}$ ist der Transzendenzgrad ihres Funktionenkörpers.
Wir beschränken uns auf Varietäten der Dimension eins. Varietäten der Dimension eins heißen algebraische (affine) Kurven. Wir werden die Kurzform Kurve anstelle algebraischer affinen Kurve verwenden.
Ausgehend von einem Funktionenkörper kann man eine entsprechende Kurve definieren. Ein Funktionenkörper wird separabel erzeugt und das hat eine Eigenschaft der entsprechenden Kurve zur Folge. Wir definieren zunächst diese Eigenschaft:

1.24. Definition. Es seien k ein vollkommener Körper und $f \in k[x, y]$.

1. Ein Punkt $P \in \mathbf{V}(f)$ heißt singulär, falls
$$(f(P) = 0) \wedge (D_x f(P) = 0) \wedge (D_y f(P) = 0).$$
2. P heißt nicht-singulär, falls
$$(f(P) = 0) \wedge ((D_x f(P) \neq 0) \vee (D_y f(P) \neq 0)).$$
3. Eine Kurve heißt singulär, wenn alle Punkte $P \in \mathbf{V}(f)$ singulär sind.
4. Eine Kurve heißt nicht-singulär, wenn alle Punkte $P \in \mathbf{V}(f)$ nicht-singulär sind.

5. Ein Punkt $P \in \mathbf{V}(f)$ heißt gewöhnlicher Knotenpunkt, falls P ein singulärer Punkt ist und $D^2_{xy}f(P) \neq D_{xx}f(P)D_{yy}f(P)$

Nun sei $F = k(x, y)$ ein Funktionenkörper mit erzeugenden x, y und sei $G(X, Y) \in k[X, Y]$ ein irreduzibles Polynom mit $G(x, y) = 0$. Wir definieren die Menge

$$W := \{P \in \mathbf{A}^2(k) \cup \infty \mid G(P) = 0\}$$

Es sei $\mathbf{V}$ das nicht singuläre Modell von W; dann ist F isomorph zum Funktionenkörper von $\mathbf{V}$. D.h.: Es existiert eine nicht-singuläre affine Kurve $\mathbf{V}$ (eindeutig definiert bis auf Isomorphismus) mit Funktionenköper $K(\mathbf{V})$, der k-isomorph zu $F = k(x, y)$ ist.
Wenn man Varietäten klassifizieren oder bestimmte Eigenschaften untersuchen will, definiert man eine Äquivalenzrelation. Ein Klasseneinteilungskriterium ist:

1.25. Definition. Zwei Varietäten über k heißen birational äquivalent, falls die entsprechenden Funktionenkörper k-isomorph sind.

Kapitel 2

Bewertungen und Stellen

2.1 Bewertungen und Bewertungsringe

Die Bewertungstheorie kann als ein Zweig der topologischen Algebra betrachtet werden. Ein Körper mit einer Bewertung ist ein algebraisches System mit einer Metrik. Diese Einschränkung der algebraischen Freiheit erlaubt, strukturelle Eigenschaften feiner zu analysieren. Eine eingehende Behandlung der Bewertungstheorie findet man in [61]. Bei der Entwicklung der Theorie der algebraischen Funktionenkörper wird eine diskrete Bewertung verwendet. Es handelt sich um eine Abbildung auf eine geordnete, unendliche, abelsche Gruppe.

2.1. Definition. Eine abelsche Gruppe $(G, +)$ versehen mit einer binären Relation $>$, heißt geordnete Gruppe $(G, +, >)$ -im folgenden kurz G-, wenn für $\alpha, \beta, \gamma \in G$ genau eine der folgenden Relationen gilt:

1. $\alpha > \beta,\ \alpha = \beta,\ \beta > \alpha$
2. $\alpha > \beta, \beta > \gamma \Rightarrow \alpha > \gamma$
3. $\alpha > \beta, \delta \in G \Rightarrow \alpha + \delta > \beta + \delta$

Das neutrale Element von G wird mit 0 bezeichnet.

Wir fügen der Gruppe G ein Element ∞ hinzu. ∞ hat folgende Eigenschaften:

1. $\infty + \infty = \alpha + \infty = \infty + \alpha = \infty, \forall \alpha \in G$
2. $\alpha > \infty\ \forall \alpha \in G$

Wir beschränken uns auf die unendliche, geordnete, zyklische, abelsche Gruppe $\mathbb{Z}$:

2.2. Definition. Es sei K ein Körper. Eine diskrete Bewertung v eines Körpers K ist eine Abbildung

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

mit folgenden Eigenschaften für $x, y \in K$:

1. $v(x) = \infty \Longleftrightarrow x = 0$.
2. $v(xy) = v(x) + v(y)$ für alle $x, y \in K$.
3. $v(x + y) \geq \min(v(a), v(b))$
4. Es existiert $z \in K$ mit $v(z) = 1$
5. $v(a) = 0 \quad$ für alle $0 \neq a \in K$

Die Struktur (K, v) heißt bewerteter Körper. Aus 2. und 4. folgt, daß die Abbildung surjektiv ist. Die Eigenschaft $v(xy) = v(x) + v(y)$ besagt, daß $v : K^{\times} \to \mathbb{Z}$ ein Gruppenhomomorphismus ist.
Die Bewertung heißt trivial, wenn ihre einzigen Werte 0 und ∞ sind. Bewertungen mit der Eigenschaft $v(K) = \mathbb{Z} \cup \infty$, also mit der Eigenschaft 4., heißen normiert. Die Wertemenge $v(K^{\times}) \subseteq \mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Z}, +)$. Es ist $v(K^{\times}) = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. Die Bewertung v ist genau dann trivial, wenn $m = 0$ gilt. Ist v nicht trivial, dann kann man durch $v_{\infty}(x) := \frac{1}{m}v(x)$ mit $x \in K^{\times}$, $v_{\infty}(0) := \infty$ eine diskrete Bewertung auf K definieren. Das folgende Lemma ist von Bedeutung, wenn man die Bewertung eines Produktes von Elementen aus dem Körper berechnen will.

2.3. Lemma. *Es sei (K, v) ein bewerteter Körper, v eine diskrete Bewertung von K und $x, y \in K$, so daß $v(x) \neq v(y)$. Dann gilt: $v(x + y) = \min\{v(x), v(y)\}$.*

Um den Bewertungsbegriff zu veranschaulichen, betrachten wir ein Beispiel:

2.4. Beispiel. Es sei R ein ZPE-Ring, $Q(R)$ der entsprechende Quotientenring und $p \in R$ ein Primelement in R. Dann definiert man für $x \in Q(R)\backslash\{0\}$ von der Form $x = p^n \frac{x_1}{x_2}$ mit $p \not| x_1 x_2, \quad n \in \mathbb{Z}$, eine normierte diskrete Bewertung durch $v_p(x) = n$.

2.5. Satz. *Es sei (K, v) ein bewerteter Körper mit einer diskreten Bewertung v. Dann gilt:*

1. *$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ ist ein Ring.*

2. *$\mathcal{O}_v{}^* := \{x \in K \mid v(x) = 0\} =$*
   $\{x \in \mathcal{O} \mid$ es existiert ein $w \in \mathcal{O}$ mit $xw = 1\}$.

3. *$\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$ ist das einzige maximale Ideal von $\mathcal{O}_v$.*

4. *$\mathcal{O}_v$ ist ein Hauptidealring und ist genau dann kein Körper, wenn v nicht trivial ist.*

5. *Ein Element $x \in K$ ist ein Primelement von $\mathcal{O}_v$ genau dann, wenn $v(x) = 1$.*

Zum Beweis: Siehe [3].

2.6. Definition. Ein lokaler Hauptidealring $\mathcal{O}$, der kein Körper ist, heißt (diskreter) Bewertungsring eines Körpers K.

Das maximale Ideal $\mathfrak{m}_v$ des lokalen Ringes $\mathcal{O}$ ist $\mathfrak{m}_v = \mathcal{O} \backslash \mathcal{O}^*$ mit $\mathcal{O}^* := \{x \in \mathcal{O} \mid$ es existiert ein $w \in \mathcal{O}$ mit $xw = 1\}$. $\mathcal{O}^*$ heißt die Einheitengruppe von $\mathcal{O}$.
Ein (diskreter) Bewertungsring eines Funktionenkörpers F/k ist ein Ring $\mathcal{O} \subseteq F$ mit folgenden Eigenschaften:

1. $k \subset \mathcal{O} \subset F$, und

2. $x \in \mathcal{O}$ oder $x^{-1} \in \mathcal{O}$.

Wenn $\mathcal{O}$ ein Bewertungsring des Funktionenkörper F/k ist, dann gilt:

1. $\mathcal{O}$ ist ein lokaler Ring.

2. Es sei P das maximale Ideal von $\mathcal{O}$. Für $0 \neq x \in F$ gilt $x \in P \Longleftrightarrow x^{-1} \notin \mathcal{O}$.

3. P ist ein Hauptideal.

4. Falls $P = t\mathcal{O}$ gilt, dann hat jedes Element $0 \neq z \in F$ eine eindeutige Darstellung der Form $z = t^n u$ für $n \in \mathbb{Z}, u \in \mathcal{O}^*$.

Die Bewertungsringe des rationalen Funktionenkörpers $k(x)$ werden definiert durch

$$\mathcal{O}_{p(x)} := \{g/h \mid g, h \in k[x],\ h \neq 0,\ p(x) \nmid h\} \quad \text{für ein Primpolynom } p \in k[x]$$

und

$$\mathcal{O}_\infty := \{g/h \mid g, h \in k[x],\ h \neq 0,\ deg(g) \leq \deg(h)\}.$$

Der Oberring $\mathfrak{o}_{F,\infty} := \mathcal{O}_\infty[\rho]$ mit ρ ganz über $\mathcal{O}_\infty$, heißt unendliche Gleichungsordnung.

2.2 Stellen

Die folgende Definition ist grundlegend bei der Entwicklung der Theorie der algebraischen Funktionenkörper:

2.7. Definition. 1. Eine Stelle P des Funktionenkörpers F/k ist das maximale Ideal eines Bewertungsringes $\mathcal{O}$ von F/k. Jedes Element $t \in P$, so daß $P = t\mathcal{O}$, heißt ein Primelement für P.

2. $\mathcal{P}l(F/k) := \{P \mid P \text{ ist eine Stelle von } F/k\}$.

3. $\mathcal{O}_P$ heißt der Bewertungsring der Stelle P.

Eine Beschreibung der Stellen eines Funktionenkörpers auf einer bewertungstheoretischen Grundlage ist von praktischem Wert. Zu jeder Stelle $P \in \mathcal{P}l(F/k)$ definiert man eine Abbildung

$$v_P : F \to \mathbb{Z} \cup \infty.$$

wie folgt: Jedes Element $0 \neq x \in F$ hat eine eindeutige Darstellung $z = t^n u$ mit $u \in {\mathcal{O}_P}^*$ und $n \in \mathbb{Z}$. Man definiert $v_P\ (z) := n$ und $v_P(0) := \infty$.

Mit der definierten Bewertung erhalten wir die entsprechenden Bewertungsringe, bzw. Einheitengruppen und maximalen Ideale eines Funktionenkörpers F/k:

$$\mathcal{O}_P = \{x \in F \mid v_P(x) \geq 0\},$$

$${\mathcal{O}_P}^* = \{x \in F \mid v_P(x) = 0\},$$

$$P = \{x \in F \mid v_P(x) > 0\}.$$

2.8. Definition. Es sei $P \in \mathcal{P}l(F/k)$.

1. $F_P := \mathcal{O}_P/P$ heißt Restklassenkörper von P.

2. $\deg P := [F_P : k]$ heißt Grad von P.

Die Stellen eines Funktionenkörpers F/k entsprechen den irreduziblen Polynomen in $k(x)$. Falls der Konstantenkörper k unendlich ist, dann existieren unendlich viele Stellen vom Grad eins . Wenn k endlich ist, dann existieren unendlich viele irreduzible Polynome über k. Dies wird nach einer bekannten Schlußweise, die auf Euklid zurückgeht, gezeigt: Gäbe es $n < \infty$ irreduzible Polynome über k, dann wäre $f_r = f_1 \cdots f_n + 1$ ein Polynom vom Grad $d > 1$, so daß $f_i \not| f_r$. Dann enthält

f_r einen weitereren irreduziblen Faktor, im Widerspruch zur Annahme. Damit haben wir gezeigt, daß jeder Funktionenkörper unendlich viele Stellen hat.
Die Möbius μ-Funktion (1.14.) und der darauf basierende Satz 1.15. erhalten eine andere Interpretation: Es handelt sich um Aussagen über die Anzahl der Stellen von einem vorgegebenen Grad.
Die folgenden Definitionen und Sätze sind grundlegend, wenn man Erweiterungen eines Funktionenkörpers in Betracht zieht. Ein algebraischer Funktionenkörper kann immer als algebraische Erweiterung eines rationalen Funktionenkörpers betrachtet werden.
Es sei F ein Funktionenkörper über einem Konstantenkörper k und F' ein Funktionenkörper über einem Konstantenkörper k' so daß $F' \supset F$ eine algebraische Erweiterung ist und $k' \supset k$. Dann heißt F'/k' algebraische Erweiterung von F/k. Ist $k' \supset k$ eine algebraische Erweiterung, so heißt das Kompositum $F' = Fk'$ Konstantenkörpererweiterung von F/k.

2.9. Definition. Es sei F'/k' eine algebraische Erweiterung von F/k und sei $P \in \mathcal{P}l(F/k)$ und $Q \in \mathcal{P}l(F'/k')$ mit $P \subset Q$. Dann sagt man, daß Q über P liegt (in Zeichen: $Q \mid P$)

1. Die Zahl $e := e(Q \mid P) \in \mathbb{N}$ mit
$$v_Q(x) = e \cdot v_P(x) \quad \forall x \in F$$
heißt Verzweigungsindex von Q über P. $Q \mid P$ heißt verzweigt, falls $e(Q \mid P) > 1$ und unverzweigt, falls $e(Q \mid P) = 1$.

2. $f(Q \mid P) := [F'_Q : F_P]$ heißt Trägheitsgrad von Q über P.

Der Verzweigungsindex ist immer eine endliche Zahl. Der Trägheitsgrad kann endlich oder unendlich sein, in Abhängigkeit vom Grad der Körpererweiterung $[F' : F]$.

2.10. Definition. Es sei F'/k' eine algebraische Erweiterung von F/k und sei $P \in \mathcal{P}l(F/k)$ und $Q \in \mathcal{P}l(F'/k')$. Die Conorm $Con_{F'/F}(P)$ von P (bezüglich F'/F) wird definiert durch
$$Con_{F'/F}(P) := \sum_{Q|P} e(Q|P) \cdot Q,$$
wobei die Summe sich über alle $Q \in \mathcal{P}l(F'/k')$, die über P liegen, erstreckt.

2.11. Satz. *Es seien F'/k' eine endliche Erweiterung von F/k, $P \in \mathcal{P}l(F/k)$ und $P_1, \dots, P_m$ alle Stellen von F'/k', die über P liegen. Es sei $e_i := e(P_i \mid P)$ der Verzweigungsindex und $f_i := f(P_i \mid P)$ der Trägheitsgrad von $P_i \mid P$. Dann gilt*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

Um das Verzweigungsverhalten der Primdivisoren eines algebraischen Funktionenkörpers zu untersuchen, betrachten wir sie als Ideale.

2.12. Lemma. *Es sei k ein vollkommener Körper und $k[x][y]$ der Polynomring in zwei Unbekannten über k und ein irreduzibles Polynom*

$$f(x,y) = a_0(x)y^n + a_1(x)y^{n-1} + \cdots + a_{n-1}(x)y + a_n(x) \quad \in k[x][y]$$

dann gibt es Polynome $b(x,y), c(x,y)$ und $d(x) \neq 0$ aus $k[x][y]$ so daß

$$b(x,y) \cdot f(x,y) + c(x,y) \cdot f_y(x,y) = d(x)$$

wobei $f_y(x,y)$ die formale Ableitung nach y ist.

Wenn $b(x,y), c(x,y)$ und $d(x)$ keinen gemeinsamen Teiler $g(x)$ haben, dann ist $d(x)$ eindeutig bis auf einem konstanten Faktor aus k bestimmt. In diesem Fall heißt $d(x)$ die Gleichungsdiskriminante von $f(x,y)$. Die Nullstellen von $d(x)$ erzeugen Ideale, die verzweigt sein können. Man muß darüber hinaus das Verhalten von $d(x)$ untersuchen, wenn x einen unendlichen Wert annimmt.

Kapitel 3

Divisoren

3.1 Die Divisorengruppe

In diesem Abschnitt betrachten wir die Menge der Stellen in einem algebraischen Funktionenkörper F/k. Wir wollen diese Menge mit einer Struktur versehen, die grundlegend für Untersuchungen im Körper F/k ist. Eine frei erzeugte abelsche Gruppe ist eine von einer gegebenen Menge, als Basis bezeichnet, erzeugte abelsche Gruppe, in der, außer der sich aus den Gruppenaxiomen ergebenden Eigenschaften, keine weiteren nicht-trivialen Relationen zwischen ihren Elementen existieren. Die Elemente D einer so konstruierten Gruppe sind formale Summen von Elementen der Basis mit Koeffizienten aus $\mathbb{Z}$.

$$D = \sum_{x \in X} n_x x$$

Um die Gruppenoperation in der Gruppe G durchführen zu können, muß für die Elemente dieser Gruppe gelten: Nur endlich viele der Koeffizienten sind verschieden von Null.

3.1. Definition. Es sei $\mathcal{P}l(F/k)$ die Menge aller Stellen von F/k. Ein Divisor D von F/k ist ein Element aus der von den Elementen aus $\mathcal{P}l(F/k)$ (additiv geschrieben) frei erzeugten abelschen Gruppe $\mathcal{D}(F/k)$. Die Stellen selbst werden als Primdivisoren bezeichnet. Die Menge $\mathcal{P}(F/k)$ ist die Menge der Primdivisoren P von F/k.

Die Mengen $\mathcal{P}l(F/k)$ und $\mathcal{P}(F/k)$ sind per Definition gleich. Ein Divisor D von F/k ist also eine formale lineare Kombination von Primdivisoren $P \in \mathcal{P}(F/k)$ mit ganzen Koeffizienten

$$D = \sum_{P \in \mathcal{P}(F/k)} n_P P$$

wobei nur endlich viele n_P verschieden von Null sind. Wir reden künftig nur von Primdivisoren.

3.2. Definition. Der Träger des Divisors D ist die Menge $\text{supp}(D)$ der Primdivisoren, die Koeffizienten verschieden von Null haben.

Die Gruppenoperation in $\mathcal{D}(F/k)$ wird koeffizientenweise durchgeführt. Das heißt, wenn $D = \sum_{P\in\text{supp}(D)} n_P P$ und $D^* = \sum_{P\in\text{supp}(D^*)} n_P^* P$ zwei Elemente aus $\mathcal{D}(F/k)$ sind, dann ist

$$D + D^* = \sum_{P\in\text{supp}(D)\cup\text{supp}(D^*)} (n_P + n_P^*)P.$$

Das neutrale Element in der Divisorengruppe $\mathcal{D}(F/k)$ ist der Divisor D_0, dessen Koeffizienten alle gleich Null sind. Die Divisorengruppe hat eine weitere Struktur: Es seien $D, D' \in \mathcal{D}(F/k)$. Man kann diese zwei Divisoren koeffizientenweise vergleichen. Es ist $A \leq B$ genau dann, wenn $n_P \leq n'_P$ für alle $P \in \mathcal{P}(F/k)$.

3.3. Definition. $D \in \mathcal{D}(F/k)$ heißt positiv, wenn alle Koeffizienten größer oder gleich 0 sind. Es seien $A, D_i \in \mathcal{D}(F/k), i \in I$. Die Divisoren D_i mit der Eigenschaft $A \leq D_i$ heißen Vielfache von A.

Ein Divisor ist also positiv, wenn D größer oder gleich als das neutrale Element D_0 in $Div F/k$ ist.

Die bewertungstheoretische Betrachtungsweise der Divisorengruppe hat zur Folge, daß die Koeffizienten der Elemente $D \in \mathcal{D}(F/k)$ entsprechend dargestellt werden:

3.4. Definition. Für $Q \in \mathcal{P}(F/k)$ und $D = \sum_{P\in\text{supp}(D)} n_P P$ definiert man $v_Q(D) = n_Q$.

Im Umgang mit der Arithmetik der Divisorengruppe in einem Funktionenkörper muß dies berücksichtigt werden.

3.5. Beispiel. Wir betrachten die Divisoren $D_1 = 2P_1 - 3P_2 - P_3 - 5P_4$ und $D_2 = 3P_1 + 8P_3 + 5P_5$. Dann ist $D_1 + D_2 = 2P_1 - 3P_2 - P_3 - 5P_4$

3.6. Definition. Der Grad eines Divisors ist eine Abbildung $\deg : \mathcal{D}(F/k) \to \mathbb{Z}$ definiert durch $\deg D := \sum_{P\in\text{supp}(D)} v_P \cdot \deg P$.

Aus der Definition der Gruppenoperation in $\mathcal{D}(F/k)$ folgt, daß deg ein Homomorphismus ist. Um wichtige Strukturen in der Divisorengruppe zu untersuchen, betrachten wir Teilmengen von $\mathcal{D}(F/k)$. Da für ein Element $a \in F/k$ die diskrete

Bewertung $v_Q(a) \neq 0$ ist, für nur endlich viele Primdivisoren Q, kann man einen kanonischen Homomorphismus der Multiplikationsgruppe von F/k in $\mathcal{D}(F/k)$ definieren:
Jedem Element aus F/k ist eindeutig ein Element aus $\mathcal{D}(F/k)$ zugeordnet. Die Einheiten aus F/k werden auf den Nulldivisor D_0 abgebildet.

3.7. Definition. Es sei $0 \neq a \in F/k$ und N (bzw. M) die Menge der Nullstellen (bzw. Polstellen) von a in $\mathcal{P}l(F/k)$. Dann definieren wir

$$(a)_0 := \sum_{P \in Z} v_P(a)P$$

$(a)_0$ heißt der Nullstellendivisor von a. und

$$(a)_\infty := \sum_{P \in M} (-v_P(a))P.$$

$(a)_\infty$ heißt der Polstellendivisor von a Der Divisor $(a) := (a)_0 - (a)_\infty$ heißt Hauptdivisor von a. $\mathcal{H}(F/k) := \{(a) | 0 \neq a \in F/k\}$ ist die Menge aller Hauptdivisoren.

Aus dem Homomorphismus $(ay) = (a) + (y), 0 \neq a, y \in F/k$ folgt, daß $\mathcal{H}(F/k)$ eine Untergruppe von $\mathcal{D}(F/k)$ ist. Wir definieren eine Äquivalenzrelation in $\mathcal{D}(F/k)$:

3.8. Definition. Zwei Divisoren $D, D' \in \mathcal{D}(F/k)$ sind äquivalent
(in Zeichen: $D \sim D'$) wenn $D = D' + (a), a \in F \backslash \{0\}$. Einem $D \in \mathcal{D}(F/k)$ wird die Divisorenklasse $[D]$ zugeordnet.

Dies bedeutet insbesondere:$D - D' = (a)$. $D - D = 0 \in \mathcal{H}(F/k)$ bedeutet $D \sim D$ und für $D = D'' + (a)$ und $D' = D'' + (a')$ gilt $D - D' = (a) - (a')$. D.h. wenn $D \sim D''$ und $D' \sim D''$ gilt, dann gilt $D \sim D'$. Damit bestätigt man, daß es sich um eine Äquivalenzrelation handelt.

3.9. Definition. Die Faktorgruppe $\mathcal{C}l(F/k) := \mathcal{D}(F/k)/\mathcal{H}(F/k)$ heißt Divisorenklassengruppe. Ihre Elemente sind die Divisorenklassen.

Es gibt eine Klasse, die den Nulldivisor enthält und deswegen ist die Untergruppe $\mathcal{H}(F/k) \subseteq \mathcal{D}(F/k)$ selbst eine Klasse: Die Hauptdivisorenklasse. $\deg D$ ist ein Homomorphismus und infolgedessen gilt für die Elemente einer Divisorenklasse $[D]$, daß $degD = degD' + deg(a) = degD'$ wobei D' ein beliebiger Klassenvertreter ist. Alle Divisoren derselben Divisorenklasse haben den selben Grad. Man kann also vom Grad $\deg D$ einer Divisorenklasse $[D]$ sprechen. Hier ist D ein Klassenvertreter aus $[D]$.

3.10. Definition. Die Menge $\mathcal{D}^n(F/k)$ ist die Menge der Divisoren vom Grad n von F/k.
Die Menge $\mathcal{D}^{\leq n}(F/k)$ ist die Menge der Divisoren vom Grad kleiner gleich n von F/k.
Die Menge $\mathcal{C}l^n(F/k)$ ist die Menge der Divisorenklassen vom Grad n von F/k.
Die Anzahl der Elemente $h(F/k)$ von $\mathcal{C}l^0(F/k)$ wird als die Klassenzahl von F/k bezeichnet.

Es folgt eine wichtige Aussage über die Kardinalität einiger dieser Mengen im Fall, daß F/k ein Funktionenkörper über einem endlichen Konstantenkörper ist.

3.11. Satz. *Es sei F/k ein Funktionenkörper über einem endlichen Konstantenkörper. Zu einer beliebigen Zahl $0 \leq n \in \mathbb{Z}$ gilt:*
(i) $|\mathcal{D}^{\leq n}(F/k)|$ ist eine endliche Zahl.
(ii) $h(F/k)$ ist eine endliche Zahl.

Beweis. Siehe [81] ,V.1.3. Die positiven Divisoren einer Divisorenklasse $[D] \in \mathcal{C}l(F/k)$ sind von besonderer Bedeutung. Sie bilden einen Teilbereich dieser Divisorenklasse. Wenn D ein beliebiger positiver Divisor der Divisorenklasse $[D]$ ist, (a) das zugeordnete Element der Hauptdivisorenklasse und D' ein Klassenvertreter, dann ist $D = D' + (a)$ ein positiver Divisor und es gilt:

$$(a) = D - D'$$

Der Divisor D ist also genau dann positiv, wenn der zugeordnete Hauptdivisor (a) ein positiver Divisor mit $-D' \leq (a)$ ist. Die Elemente $a \in F/k$, deren zugeordnete Hauptdivisoren eine solche Ungleichung erfüllen, sind von herausragender Bedeutung in der Theorie der algebraischen Funktionenkörper.

3.12. Definition. Es sei $D \in \mathcal{D}(F/k)$. Wir definieren den Riemann-Roch-Raum $\mathcal{L}(D)$ des Divisors D

$$\mathcal{L}(D) := \{a \in F/k | -D \leq (a)\} \cup \{0\}$$

.

Wenn es einen positiven Divisor D' und einen Divisor D mit $D' = D + (a)$ gibt, folgt, daß (a) positiv ist und daß $\mathcal{L}(D)$ nicht nur aus der Nullfunktion besteht.

3.13. Lemma. *(i) $\mathcal{L}(D)$ ist ein k-Vektorraum*
(ii) Äquivalente Divisoren haben isomorphe Riemann-Roch-Räume

3.14. Definition. Es sei $D \in \mathcal{D}(F/k)$. Die Dimension $\dim D$ eines Divisors wird definiert als die Dimension des k-Vektorraumes $\mathcal{L}(D)$.

3.15. Proposition. *Für einen beliebigen Divisor $D \in \mathcal{D}(F/k)$ gilt:*

$$\dim D \leq \deg D + 1$$

Die folgende Definition spielt eine zentrale Rolle in der Theorie der algebraischen Funktionenkörper. Es handelt sich um die wichtigste Invariante eines Funktionenkörpers.

3.16. Definition. Das Geschlecht g eines algebraischen Funktionenkörpers wird definiert als

$$g := \max\{\deg A - \dim A\ + 1 | A \in \mathcal{D}(F/k)\}$$

3.17. Satz. *(Satz von Riemann) Es sei F/k ein algebraischer Funktionenkörper vom Geschlecht g.*
(i) Für jeden beliebigen Divisor $A \in \mathcal{D}(F/k)$ gilt

$$\dim A \geq \deg A + 1 - g.$$

(ii) Es existiert eine Zahl $c \in \mathbb{Z}$, die von F/k abhängt, mit der Eigenschaft: Wenn $\deg A \geq c$ gilt, dann ist

$$\dim A = \deg A + 1 - g.$$

Kapitel 4

Der Satz von Riemann - Roch

4.1 Weil-Differentiale

In der Menge $\mathcal{L}(D) := \{a \in F/k | -D \leq (a)\} \cup \{0\}$ sind die Elemente a aus dem Funktionenkörper F/k enthalten, dessen zugeordnete Hauptdivisoren (a) Vielfache eines vorgegebenen Divisors sind. Roch zeigte, wann die im Satz von Riemann formulierte Ungleichung in eine Gleichung übergeht.
Unsere Definition der Adele orientiert sich an der in [81] angegebenen.

4.1. Definition. Ein Adele von F/k ist eine Abbildung $\alpha : \mathcal{P}l(F/k) \to F$, definiert durch

$$P \mapsto \alpha_P$$

so daß $\alpha_P \in \mathcal{O}_P$ für fast alle $P \in \mathcal{P}l(F/k)$ Ein Adele ist ein Element des direkten Produkts $\prod_{P \in \mathcal{P}l(F/k)} F$

Die Menge

$$\mathcal{A}_F := \{\alpha | \alpha \text{ ist ein Adele von } F/k\}$$

ist der Adele-Raum $\mathcal{A}_F$ von F/k.
Der Adele-Raum $\mathcal{A}_F(A)$ eines Divisors A wird definiert als:

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F | -v_P(A) \leq v_P(\alpha) \text{ für fast alle } P \in \mathcal{P}(F/k)\} \subseteq \mathcal{A}_F$$

4.2. Definition. Ein *Weil-Differential* von F/k is eine k-lineare Abbildung $\omega : \mathcal{A}_F(A) \to k$, die auf der Menge $\mathcal{A}_F(A) + F$ für jeden Divisor $A \in \mathcal{D}(F/k)$ verschwindet. Die Menge

$$\Omega_F := \{\omega | \omega \text{ ist ein Weil-Differential von } F/k\}$$

ist das Modul der Weil-Differentiale Ω_F von F/k. Für $A \in \mathcal{D}(F/k)$ definiert man das Modul der Weil-Differentiale $\Omega_F(A)$ von A

$$\Omega_F(A) := \{\omega \in \Omega_F | \omega \text{ verschwindet auf } \mathcal{A}_F(A) + F\}$$

4.3. Definition. Es sei $x \in F/k$ und $\omega \in \Omega_F$. Wir definieren $x\omega : \mathcal{A}_F \to k$ durch

$$(x\omega)(\alpha) := \omega(x\alpha).$$

Aus dieser Definition folgt, daß Ω_F ein F-Vektorraum ist. Man zeigt, daß Ω_F ein eindimensionaler Vektorraum über F ist. Um eine Verbindung zwischen den Weil-Differentialen $\omega \neq 0$ und der Divisorengruppe herzustellen, betrachten wir (für festes ω) die Menge

$$M(\omega) := \{A \in \mathcal{D}(F/k) | \omega \text{ verschwindet auf } \mathcal{A}_F(A) + F\}$$

4.4. Lemma. *Es sei $0 \neq \omega \in \Omega_F$. Dann existiert ein eindeutig bestimmter Divisor $W \in M(\omega)$, so daß $A \leq W$ für alle $A \in M(\omega)$.*

4.5. Definition. Der Divisor (ω) eines Weil-Differentials $\omega \neq 0$ ist der eindeutig bestimmte Divisor von F/k mit folgenden Eigenschaften:

1. ω verschwindet auf $\mathcal{A}_F((\omega)) + F$.

2. Wenn ω auf $\mathcal{A}_F(A) + F$ verschwindet, dann gilt $A \leq (\omega)$.

Ein Divisor $W = (\omega)$ heißt kanonischer Divisor von F/k

4.6. Proposition. *(i)Für $0 \neq x \in F$ und $0 \neq \omega \in \Omega_F$ gilt:$(x\omega) = (x) + (w)$*
(ii)Je zwei kanonische Divisoren von F/k sind äquivalent.

Aus dieser Aussage folgt, daß die kanonischen Divisoren von F/k eine Divisorenklasse $[W]$ bilden. Diese Divisorenklasse ist natürlich in $\mathcal{C}l(F/k)$ enthalten und wird als kanonische Divisorenklasse bezeichnet.

4.2 Der Satz von Riemann - Roch

4.7. Satz. *Es sei A ein beliebiger Divisor und $W = (\omega)$ ein kanonischer Divisor von F/k. Dann gilt:*

$$\mathcal{L}(W - A) \cong \Omega_F(A)$$

Der k-Isomorphismus wird durch die Abbildung $\mu : x \mapsto x\omega$ definiert. Der folgende Satz ist der wichtigste Satz in der Theorie der algebraischen Funktionenkörper:

4.8. Satz. *Es sei W ein kanonischer Divisor von F/k. Für alle Divisoren $A \in \mathcal{D}(F/k)$ gilt*

$$\dim A = \deg A + 1 - g + \dim(W - A).$$

Mit Hilfe des Satzes von Riemann-Roch können sowohl das Geschlecht als auch die kanonischen Divisoren bzw. die kanonische Divisorenklasse charakterisiert werden. Wichtige Größen eines kanonischen Divisors werden ebenfalls mit Hilfe dieses Satzes charakterisiert.

4.9. Korollar. *Es sei W ein kanonischer Divisor. Es gilt*

$$\deg W = 2g - 2 \text{ und } \dim W = g.$$

4.10. Satz. *Es sei $A \in \mathcal{D}(F/k)$ mit $\deg A \geq 2g - 1$. Dann gilt*

$$\dim A = \deg A + 1 - g.$$

4.11. Satz. *Ein Divisor B ist kanonisch genau dann, wenn $\deg B = 2g - 2$ und $\dim B \geq g$*

In der Weierstraßschen Theorie der algebraischen Funktionen wird auf die besondere Rolle hingewiesen, die Elemente $x \in F/k$, die nur eine Polstelle haben, bei Aussagen über wichtige Eigenschaften des Körpers spielen.

4.12. Satz. *Es sei P ein Primdivisor von F/k. Zu jedem $n \geq 2g$ existiert ein Element $x \in F$ mit dem Poldivisor $(x)_\infty = nP$*

4.13. Definition. Es sei P ein Primdivisor von F/k. Eine ganze Zahl n heißt Polzahl von P genau dann wenn es ein Element $x \in F/k$ gibt, mit $(x)_\infty = nP$. Wenn es kein solches Element aus F/k gibt, dann bezeichnet man n als Lückenzahl.

4.14. Satz. *(Lückensatz von Weierstraß) Es sei F/k ein algebraischer Funktionenkörper vom Geschlecht $g > 0$ und P ein Primdivisor von F/k. Dann gibt es genau g Lückenzahlen $i_1, \ldots, i_g$ von P. Wir haben:*

$$i_1 = 1 \text{ und } i_g \leq 2g - 1$$

Diesem Satz kann man eine neue Definition des Geschlechts g eines algebraischen Funktionenkörpers entnehmen.
Eine bemerkenswerte Anwendung des Satzes von Riemann-Roch ist die folgende: Den kleinsten Erweiterungsgrad über dem rationalen Funktionenkörper eines algebraischen Funktionenkörpers F/k vom vorgegebenen Geschlecht g zu bestimmen. Dies entspricht der klassischen Fragestellung der Funktionentheorie: die kleinste Anzahl der Blätter der einer Funktion entsprechenden Riemannschen Fläche zu bestimmen.

4.3 Das Geschlecht eines algebraischen Funktionenkörpers

Es gibt verschiedene Arten, das Geschlecht eines algebraischen Funktionenköpers zu definieren. Dies steht im Zusammenhang mit der zu Grunde liegenden Theorie: Algebraische Topologie, Algebraische Geometrie, Funktionentheorie oder -wie in unserem Fall- die Theorie der algebraischen Funktionenkörper. Die verschiedene Begriffsbildungen lassen sich unter bestimmten Voraussetzungen von einem Gebiet auf das andere übertragen. Im vorigen Abschnitt wurde der Begriff des Geschlechtes g eines Funktionenkörpers F/k durch den Satz von Riemann-Roch charakterisiert. In der Praxis benötigt man Abschätzungen, die leicht zu ermitteln sind.

4.15. Proposition. *(Riemanns Ungleichung) Es sei $F = k(x, y)$. Dann gilt die folgende Abschätzung für das Geschlecht g des algebraischen Funktionenkörpers F/k:*

$$g \leq ([F : k(x)] - 1) \cdot ([F : k(y)] - 1).$$

Die folgende Abschätzung wird der algebraische Geometrie entnommen:

4.16. Proposition. *Es sei $F = k(x, y)$ ein algebraischer Funktionenköper über k und die irreduzible Gleichung in y über $k(x)$ habe die folgende Gestalt:*

$$f(x, y) = y^n + f_1(x)y^{n-1} + \cdots + f_n(x) = 0, \;\; f_i(x) \in k[x],\; deg_x f_j \leq j,\; 1 \leq j \leq n.$$

Dann gilt:

$$g \leq \frac{(n-1)(n-2)}{2}$$

Bei dieser häufig angewandten Abschätzung ist man daran interessiert, feststellen zu können, wann Gleichheit besteht. Dies ist der Fall, wenn die entsprechende Kurve nicht-singulär ist.
Der Satz von Riemann-Hurwitz gibt Auskunft über das Geschlecht g einer Körpererweiterung. Es sei $P \in \mathcal{D}(F/k)$ ein Primdivisor.

4.17. Satz. *(Riemann–Hurwitz-Geschlechtsbestimmungsformel) Es sei F/k ein algebraischer Funktionenkörper vom Geschlecht g, F'/F eine endliche separable Erweiterung von F/k, k' der Konstantenkörper von F' und g' das Geschlecht von F'/k'. Mit $P \in PF/k$ ein Primdivisor. Dann gilt:*

$$2g' - 2 \geq \frac{[F' : F]}{[k' : k]}(2g - 2) + \sum_{P \in PF/k} (e(P) - 1)$$

Das Gleichheitszeichen gilt genau dann wenn entweder
(i) $\chi(k) = 0$*; oder*
(ii) $\chi(k) = p$ *und* p *teilt kein Verzweigungsindex* e *für alle Primdivisoren von* F*.*

Beweis. Siehe [74] ,5.9

4.18. Beispiel. Es sei k ein Körper mit $\chi(k) \neq 7$. Der Funktionenkörper definiert durch die Gleichung $y^3 + x^3y + x$ ist unter dem Namen Kleins Quartik bekannt. Die Diskriminante ist $D(x) = 4x^9 + 27x^2$. Die möglichen Verzweigungspunkte sind dann $x = 0, \quad x = \infty$ und die Lösungen der Gleichung $x^7 = -27/4$. Da $\chi(k) \neq 7$ ist der Funktionenkörper nicht rational. Über den Primdivisor $P = x - 0$ liegt ein Primdivisor mit Verzweigungsindex $e = 3$. Über jeder der siebten Wurzeln von $-27/4$ liegen zwei Primdivisoren: einen davon mit $e = 2$ und der andere mit $e = 1$. Durch eine Substitution $z = 1/x$ könnte man den Primdivisor P_∞, der $x = \infty$ entspricht, untersuchen. Aus der Riemann–Hurwitz–Formel ersieht man, daß die Summe der Zahlen $e(P) - 1$ für die Primdivisoren über P_∞ eine gerade Zahl sein muß. Also es liegen über P_∞ zwei Primdivisoren mit Verzweigungsindex 2 und 1. Wenn man in Betracht zieht, daß ein algebraischer Funktionenkörper eine Erweiterung eines rationalen Funktionenkörpers, also eines Körpers vom Geschlecht 0, ist, erhalten wir:

$$2g - 2 = -2 * 3 + 2 + 2 + 7 * 1 + 1 = 4,$$

und damit ist $g = 3$.

Kapitel 5

Klassen von algebraischen Funktionenkörpern

Wir haben bisher Eigenschaften der Struktur eines algebraischen Funktionenkörpers betrachtet. In diesem Abschnitt stellen wir zunächst Definitionen und Ergebnise vor, die strukturerhaltende Abbildungen von Funktionenkörpern betreffen. Dies hängt mit folgender Fragestellung zusammen: Die Körpererweiterungen eines Körpers k, die über k den Transzendenzgrad 1 besitzen und durch eine endliche Anzahl von Elementen erzeugt werden, sind in Klassen einzuteilen, um dann Klassenvertreter mit einer möglichst einfachen definierenden Gleichung zu ermitteln.

5.1 Funktionenkörperhomomorphismen

Wir betrachten zwei Funktionenkörper F_1 und F_2 über k. Ein Funktionenkörperhomomorphismus $\phi : F_1 \to F_2$ heißt Einbettung von F_1 in F_2 über k, wenn $\phi(a) = a \; \forall a \in k$. ϕ ist injektiv und definiert einen Isomorphismus von F_1 auf einen Teilkörper $\phi(F_1) \subseteq F_2$. Eine surjektive Einbettung von F_1 in F_2 über k ist ein k-Isomorphismus.

Die $k(x)$-Isomorphie von zwei Funktionenkörpern über k setzt die Isomorphie voraus; es gibt aber auch nicht-$k(x)$-isomorphe Funktionenkörper die jedoch k-isomorph sind, wie das folgende Beispiel zeigt:

5.1. Beispiel. Es sei k ein beliebiger Körper, $k(T)/k$ eine einfache transzendente Erweiterung über k. Wir betrachten die irreduziblen Polynome $f_1(T, y) = y^2 - T$ und $f_2(T, y) = y^3 - T$ aus $k[T, y]$. Dann betrachten wir den Funktionenkörper $F_1 = k(T, \rho)$ mit $\rho \in \overline{k(T)}$ so daß $f_1(T, \rho) = 0$. Andererseits betrachten wir $F_2 = k(T, \xi)$, definiert durch $f_2(t, \xi) = 0$. Aus $\rho^2 = T$ bzw. $\xi^3 = T$ folgt $F_1 = k(\rho)$ bzw.

$F_2 = k(\xi)$, also $F_1 \cong k(T)$ und $F_2 \cong k(T)$ und infolgedessen $F_1 \cong F_2$. Dennoch sind F_1 und F_2 nicht $k(T)$-isomorph da $[F_1 : k(T)] = 2$ und $[F_2 : k(T)] = 3$.

Betrachtet man zwei $k(x)$-isomorphe Funktionenkörper $F = k(x, \rho)$ und $F' = k(z, \xi)$ so nennt man den Übergang von den erzeugenden Elementen x, ρ zu den erzeugenden Elementen z, ξ eine birationale Transformation.

5.2. Definition. Es k ein Körper und seien $F = k(x, \rho)$ und $F' = k(z, \xi)$ zwei $k(x)$-isomorphe Funktionenkörper über k. Eine Abbildung $\Phi : F \to F'$, definiert durch

$$\Phi : (x, \rho) \mapsto (z, \xi)$$

rational über F und so, daß eine Abbildung $\Phi^{-1} : F' \to F$ existiert, mit $\Phi^{-1} \circ \Phi = Id$

heißt birationale Transformation. Eine birationale Transformation ist ein $k(x)$-Isomorphismus. Birationale Transformationen konstruiert man durch die Wahl eines separierendes Elementes des Funktionenkörpers F und die Bestimmung eines algebraischen Elementes, das Wurzel einer Gleichung vom Grad $n = [F : k(x)]$ ist. Dies geschieht in endlich vielen Schritten wie es den Ausführungen von 1.3. zu entnehmen ist.

5.3. Beispiel.

1. Wir betrachten den algebraischen Funktionenkörper $F = k(z, u)$, definiert durch die Gleichung $u^7 = \frac{z^3}{(1-z)}$. Es handelt sich um Kleins Quartik. Wir führen zunächst die Transformation $z = -y^2 x$ bzw. $y = u$ durch, damit erhalten wir:$-y^6 x^3 = (1 + y^2 x) y^7$. Durch Multiplikation mit $\frac{1}{y^6}$ erhalten wir: $y^3 + y^3 x + y = 0$. Dies ist eine Gleichung im zu $F = k(z, u)$ $k(z)$-isomorphen Funktionenkörper $F' = k(x, y)$. Ein Vorteil der ersten Darstellung des Funktionenkörpers ist, daß man leicht feststellen kann, daß wenn der Körper k der Charakteristik 7 ist, ein bestimmtes Verzweigungsverhalten auftritt.

2. Der Funktionenkörper $F = \mathbb{F}_3[x, \rho]$ vom Geschlecht 3, erzeugt durch die irreduzible, in y separable Gleichung $y^6 + y^4 + (2x^3 + x + 1)y^3 + y^2 + (x^3 + 2x + 1)y + x^6 + x^4 + x^2$, ist k-isomorph zum Funktionenkörper $F' = \mathbb{F}_3[x, \xi]$, erzeugt durch $y^3 + y + x^6 + x^4 + x^2$. Die Transformation wird durch die Wahl der unabhängigen Variable $x - y \in F$ definiert. Der Homomorphismus $\mathbb{F}_3[x, y] \mapsto F\mathbb{F}_3[x, \rho]$ und Rechnungen in der endlichen Ordnung $\mathfrak{o}_F := k[x, \rho]$ beanspruchen etwa zehn mal mehr Rechenzeit als die entsprechenden $\mathbb{F}_3[x, y] \mapsto \mathbb{F}_3[x, \xi]$ und $\mathfrak{o}'_F := k[x, \xi]$.

Bei einer birationalen Transformation wird immer von der, den Funktionenkörper definierenden, Gleichung $f(x,y)$ Gebrauch gemacht. Um die Rolle der Körperautomorphismen bei einer birationalen Tranformation zu veranschaulichen, führen wir ein aus [41] entnommenen Beispiel an:

5.4. Beispiel. Wir wählen $z = x^2$ und $y' = y$. Es sei $f(x,y) = f_1(x^2,y) + xf_2(x^2,y)$. Dann ist

$$x = -f_1(z,y')/f_2(z,y'),\ y = y'$$

Wie man sieht, gilt dies nicht, wenn der Funktionenkörper den Automorphismus $x \mapsto -x$, $y \mapsto y$ gestattet, denn in diesem Fall ist $f_2 = 0$, also ist x kein Element aus dem Funktionenkörper.

5.2 Normalgleichungen und Modulräume

In diesem Abschnitt widmen wir uns der Klassifizierung von algebraischen Funktionenkörpern.
Eine grobe Formulierung definiert einen Modulraum als eine algebraische Varietät, deren Punkte eindeutig der Menge der Isomorphieklassen von algebraisch-geometrischen Objekten zugeordnet werden. In unserem Fall handelt es sich um Isomorphieklassen von Funktionenkörpern. Die Formalisierung dieser Ideen führt in der Literatur zum Begriff eines darstellbaren Funktors. Wir werden jedoch diesen Begriff aus der kategoriellen Algebra nicht verwenden. Für eine entsprechende Darstellung verweisen wir auf [56, 30]. Wir folgen bei unserer Darstellung Ideen von Hensel/Landsberg [33] und Deuring [12]. Mit Riemann [64] wird allen k-isomorphen Funktionenkörpern vom Geschlecht g über k eine Klasse zugeordnet und man charakterisiert diese Klasse durch eine der in ihr enthaltenen definierenden Gleichungen.
Häufig untersucht man die Eigenschaften des durch eine gegebene Gleichung bestimmten Funktionenkörpers. Wir gehen hier den umgekehrten Weg: einen Körper,von dem das Geschlecht und eventuell auch eine spezielle Eigenschaft gegeben ist, durch eine Gleichung zu konstruieren. Dieser Ansatz ist nicht nur in theoretischer Hinsicht, sondern auch hinsichtlich praktischer Anwendungen von Bedeutung.

Im folgenden ist k ein algebraisch abgeschlossener Körper

Zunächst stellen wir einige Überlegungen über die Anzahl der Koeffizienten einer definierenden Gleichung für einen Funktionenkörper F/k vor:

5.5. Definition. Es sei $k[x,y]$ ein Polynomring in zwei Veränderlichen über k. Der maximale Grad eines bivariaten Polynoms $f \in k[x,y]$ ist die ganze Zahl $degmax\, f := \max\{\deg_x, \deg_y\}$

5.6. Definition. Es sei $k[x,y]$ ein Polynomring in zwei Veränderlichen über k. Wir definieren das allgemeine Polynom f vom maximalen Grad n: Es sei $f \in k[x,y]$ der Form:

$$f(x,y) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{i,j} x^i y^j$$

also

$$f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots\cdots\cdots +$$

$$a_{n0}x^n + a_{(n-1)1}x^{n-1}y + \cdots\cdots + a_{1(n-1)}xy^{n-1} + a_{0n}y^n$$

Die Kurve definiert durch $f(x,y) = 0$ heißt vom Grad n.

5.7. Bemerkung. Die Anzahl der Koeffizienten N ist $\frac{1}{2}(n+1)(n+2)$. Wenn man das Polynom normiert, erhält man $N = \frac{1}{2}(n+1)(n+2) - 1 = \frac{1}{2}n(n+3)$. Diese Zahl kann auch in der Form $3n + g - 1$ mit $g = \frac{(n-1)(n-2)}{2}$ geschrieben werden.

5.8. Bemerkung. Wenn man ν-mal spezialisiert $(x_i, y_i) \mapsto f(x_i, y_i), 1 \leq \nu$, erhält man ν Gleichungen:

$$f(x_1, y_1) = 0, \cdots, f(x_\nu, y_\nu) = 0.$$

Mit ihrer Hilfe läßt sich eine Anzahl von Koeffizienten a_{ik} durch die übrigen linear und homogen darstellen. Dies ist die algebraische Formulierung der geometrischen Gleichungstransformation, die man durchführt, wenn man Punkte auf einer Kurve kennt, bzw. die Bedingung, daß die Kurve durch bestimmte Punkte geht -mit den entsprechenden Einschränkungen- stellt.

Wir betrachten -nach Deuring [12]- folgende Menge:

5.9. Definition. Es sei $f \in k[x,y]$.

$$\mathbf{V}_{ng} := \{a_{i,j} \in k | 0 = f(x,y) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{i,j} x^i y^j\}$$

ist die Menge, in der die Kurven n-ten Grades vom Geschlecht g mit nur gewöhnlichen Knotenpunkten als einzigen Singularitäten, enthalten sind.

$\mathbf{V}_{ng}$ ist eine irreduzible Varietät. Die Dimension dieser Varietät ist $3n+g-1$ unter Berücksichtigung der Gleichung $g = \frac{(n-1)(n-2)}{2}$. In der Literatur spricht man von Severi-Varietäten im Zusammenhang mit dem Hilbert–Schema von Kurven vom Grad n. In [4] wird die Geometrie der Severi–Varietäten diskutiert. Es werden Kurven von gegebenem Grad und Geschlecht parametrisiert und eine rekursive Formel für die Anzahl der Kurven in $\mathbf{P}^2(\mathbb{C})$ von vorgegebenem Grad mit d gewöhnlichen Knotenpunkten und die durch eine bestimmte Anzahl von Punkten gehen angegeben.
Wir betrachten die Menge aller Funktionenkörper über k vom Geschlecht g über k und definieren eine Äquivalenzrelation: Zwei Funktionenkörper über k vom Geschlecht g über k sind äquivalent genau dann, wenn sie k-isomorph sind.

5.10. Definition. Die affine Varietät $\mathcal{M}_g(k)$ wird durch eine injektive Abbildung von $\mathcal{M}_g(k)$ in die Menge der Klassen von k-isomorphen Funktionenkörpern über k vom Geschlecht g über k definiert. $\mathcal{M}_g(k)$ heißt Modulvarietät der Funktionenkörper vom Geschlecht g über k. Die Koordinaten m eines Punktes aus $\mathcal{M}_g(k)$ heißen Moduln.

Wir wollen den Zusammenhang zwischen den Varietäten $\mathbf{V}_{ng}$ und $\mathcal{M}_g(k)$ nach Deuring [12] formalisieren. Dies geschieht unter Verwendung des Begriffes der algebraischen Korrespondenz, auf den wir ansonsten nicht eingehen werden. Für den Begriff der algebraischen Korrespondenz verweisen auf [15] oder [91]. Wir geben die im letzten Werk enthaltenen Definition wieder :

5.11. Definition. Es seien $\mathbf{V}_1$ und $\mathbf{V}_2$ zwei affine Varietäten über k von Dimension m bzw. n. Eine affine Varietät $\mathfrak{K}$ über k, definiert als

$$\mathfrak{K}(\mathbf{V}_1, \mathbf{V}_2) := \{(v_1, v_2) | v_1 \in \mathbf{V}_1, v_2 \in \mathbf{V}_2\}$$

heißt algebraische Korrespondenz, wenn sie durch ein System von homogenen Gleichungen (homogen sowohl in den v_1 als in den v_2)

$$f_i(v_{1,0}, \ldots, v_{1,m}, v_{2,0}, \ldots, v_{2,n}) = 0$$

definiert wird.

Von den Punkten v_2 wird gesagt, daß sie den Punkten v_1 in der Korrespondenz zugeordnet sind. Siehe [91]

5.12. Definition. Es sei $\mathfrak{K}(\mathbf{V}_{ng}, \mathcal{M}_g(k))$ eine algebraische Korrespondenz, die jeder nicht-singulären Kurve $C \in \mathbf{V}_{ng}$ einen Punkt $P(C) \in \mathcal{M}_g(k)$ eindeutig zuordnet, so daß zwei nicht-singuläre Kurven C_1 und C_2 genau dann k-isomorph sind, wenn $P(C_1) = P(C_2)$ ist. Die Gleichungen dieser Korrespondenz haben Koeffizienten in k. Dem durch die Kurve C definierten Funktionenkörper F/k wird durch $P(F/k) = P(C)$ ein Punkt $P(F/k) \in \mathcal{M}_g(k)$ zugeordnet.

Es sei $\mathcal{M}_g(k)$ eine Modulvarietät und F/k ein Funktionenkörper. Die Koordinaten m eines Punktes $P(F/k) \in \mathcal{M}_g(k)$ heißen Moduln von F/k.

5.13. Satz. *Es sei F/k ein Klassenvertreter aus $\mathcal{M}_g(k)$. F/k kann durch eine Gleichung*

$$f(x,y) = \sum_{i=0}^{\nu} \sum_{j=0}^{\mu} a_{i,j} x^i y^j$$

definiert werden, deren Gleichungskoeffizienten $a_{i,j}$ rationale Funktionen der Moduln mit Koeffizienten aus k sind. $f(x,y)$ heißt Normalgleichung für F/k.

Für einen Beweis siehe [12]. Normalgleichungen heißen auch kanonische Gleichungen. Wir werden uns darauf beschränken die Fälle der Funktionenkörper vom Geschlecht 0, 1, 2, 3 und 4 zu besprechen.

5.2.1 g=0

Es sei k ein Körper und $F = k(x,y)$ ein Funktionenkörper über k vom Geschlecht 0 über k. D ist ein Divisor aus $\mathcal{D}(F/k)$. Wegen $g = 0$ und mit 3.15. gilt $dim\, P \geq 1$. D.h. es existiert $x \in F/k$ und $x \notin k$, so daß $D = (x)_\infty$. Dann ist $deg\,(x)_0 = deg\,(x)_\infty = 1$ und damit $[F : k(x)] = 1$ also $F = k(x)$.
Die Funktionen x und y lassen sich mit Hilfe einer Funktion $t \in F$ mit $deg\,(t)_\infty = 1$ als rationale Funktionen von t darstellen und es ist also:

$$x = r(t), \quad y = r_1(t)$$

Analog für einen zweiten Funktionenkörper $F = k(z,u)$ vom Geschlecht $g = 0$:

$$z = R(\tau), \quad u = R_1(\tau),$$

wobei τ ebenfalls eine Funktion mit $deg\,(\tau)_\infty = 1$ des Körpers $F = k(z,u)$ ist. Da t und τ beide Funktionen mit $deg\,(t)_\infty = deg\,(\tau)_\infty = 1$ sind, so muß notwendig, wenn beide Funktionenkörper k-isomorph sind

$$t = \frac{\alpha\tau + \beta}{\gamma\tau + \delta} \qquad (\alpha\delta - \beta\gamma) \neq 0$$

sein; umgekehrt können zwei rationale Funktionenkörper durch eine derartige Substitution ineinander transformiert werden. Da hier drei Größen, nämlich die Verhältnise $\alpha : \beta : \gamma : \delta$ willkürlich bleiben, so folgt nicht nur, daß zwei beliebige Funktionenkörper vom Geschlecht Null in dieselbe Klasse fallen, sondern auch, daß die Zahl der Moduln gleich Null ist.

5.14. Satz. *Jeder algebraische Funktionenkörper vom Geschlecht Null hat unendlich viele Automorphismen, die von drei willkürlichen Parameter abhängen.*

5.2.2 g=1

5.15. Definition. Ein algebraischer Funktionenkörper F/k (k ist der exakte Konstantenkörper) heißt elliptischer Funktionenkörper falls gilt:
(i) F/k hat das Geschlecht $g = 1$
(ii) Es existiert ein Divisor $A \in \mathcal{D}(F/k)$ mit $\deg A = 1$

5.16. Bemerkung. Wenn k algebraisch abgeschlossen oder endlich ist, existiert immer ein Divisor $A \in \mathcal{D}(F/k)$ mit $\deg A = 1$.

Für die Theorie der elliptischen Funktionenkörper bzw. elliptischen Kurven wird auf [35], [76] und [74] hingewiesen. Wir betrachten die Varietät $\mathbf{V}_{3,1}(k)$. Die Dimension von $\mathbf{V}_{3,1}$ ist 9 . Das allgemeine Polynom f vom maximalen Grad $degmax\, f = 3$ ist

$$f(x,y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 +$$

$$a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3$$

Mit Hilfe des Satzes von Riemann wird die Normalgleichung bestimmt.
Es sei k ein Körper und F/k ein Funktionenkörper über k vom Geschlecht 1 über k. P ist ein Primdivisor aus $\mathcal{D}(F/k)$. Wegen $g = 1$ und mit 3.15. gilt $dim\, P \geq 1$. Nach 3.13. ist $dim\, P \leq 1$ und damit ist $dim\, P = 1$. Nach 3.15.(ii) ist dim P=(cP)=c für alle $c \geq 0$. Es sei die Menge $\{1, x\}$ eine Basis für $\mathcal{L}(2P)$. Dann ist $(x)_\infty = 2P$, weil wenn $(x)_\infty = P$ wäre, dann wäre F rational. Es folgt: $[F : k(x)] = 2$. Es sei $\{1, x, y\}$ eine Basis für $\mathcal{L}(3P)$. Dann ist $(y)_\infty = 3P$, und damit $y \notin k(x)$. Also $F/k = k(x, y)$. Die sieben Elemente $1, x, y, x^2, xy, x^3, y$ sind in $\mathcal{L}(6P)$ enthalten. Da $dim\,(6P) = 6$, existiert eine nicht-triviale Relation

$$a_{02}y^2 + a_{11}xy + a_{01}y = a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$$

mit $a_{02} \neq 0$ wegen $[F : k(x)] = 2$. Die Relation wäre sonst eine Gleichung ersten Grades in y, also rational. Analog ist $a_{30} \neq 0$. Im allgemeinen Polynom sind also $a_{03} = a_{12} = a_{21} = 0$. Nun multiplizieren wir die erhaltene Gleichung mit $a_{02}^3 a_{30}^2$; man erhält

$$a_{02}^4 a_{30}^2 y^2 + \cdots = a_{02}^3 a_{30}^3 x^3 + \cdots$$

Durch eine birationale Tranformation

$$u := a_{02}^2 a_{30} y \qquad z := a_{02} a_{30} x$$

ist $F = k(z, u)$ und man erhält die Normalgleichung über k, die nicht-singuläre Weierstrass-Gleichung:

$$f(z, u) = u^2 + b_{11}xu + b_{01}u + b_{30}z^3 + b_{20}b^2 + b_{10}z + a_{00}$$

bzw.

$$f(z, u) = u^2 + (b_{11}x + b_{01})u + b_{30}z^3 + b_{20}b^2 + b_{10}z + a_{00}$$

5.17. Bemerkung. Wenn $\chi(k) \neq 2$ oder $\chi(k) \neq 3$, kann die Normalform einfachere Formen annehmen, auf die wir später eingehen.

5.18. Definition. Es sei $F = k(x, y)$ ein Funktionenkörper, definiert durch die Weierstrass-Normalgleichung über k.

$$f(x, y) = y^2 + a_{11}xy + a_{01}y + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$$

Zu der Normalgleichung werden b_2, b_4, b_6, b_8, als rationale Funktionen der Ausgangskoeffizienten definiert:

$$\begin{aligned}
b_2 &= a_{11}^2 + 4a_{20} \\
b_4 &= 2a_{10} + a_{11}a_{01} \\
b_6 &= {a_{01}}^2 + 4a_{00} \\
b_8 &= {a_{11}}^2 a_{00} + 4a_{20}a_{00} - a_{11}a_{01}a_{10} + a_{2,0}{a_{01}}^2 - {a_{10}}^2 \\
c_4 &= {b_2}^2 - 24b_4 \\
c_6 &= -{b_2}^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -{b_2}^2 b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6 \\
j(F) &= {c_4}^3/\Delta
\end{aligned}.$$

$j(F)$ heißt j-Invariante von F/k. Δ heißt Gleichungsdiskriminante.

5.19. Bemerkung. Es besteht die folgende Relation: $12^3\Delta = {c_4}^3 - {c_6}^2$ und infolgedessen

$$j = 12^3 \frac{{c_4}^3}{{c_4}^3 - {c_6}^2}$$

12^3 wird als verschieden von Null auch im Fall $\chi(k) = 2$ und $\chi(k) = 3$ betrachtet.

5.20. Bemerkung. b_2, b_4, b_6, b_8 entstehen aus einer quadratischen Ergänzung, c_4, c_6 aus einer kubischen Ergänzung.

5.21. Satz. *Es seien F_1/k und F_2/k zwei Funktionenkörper über k. Wenn sie k-isomorph sind, dann ist $j(F_1/k) = j(F_2/k)$. Die Umkehrung gilt, falls k algebraisch abgeschlossen ist.*

Nach Konstruktion gilt $j(F/k) \in k$. $j(F/k)$ kann als Modul betrachtet werden. Die Varietät $\mathcal{M}_1(k)$ ist isomorph zur Menge $\mathbf{A}^1(k) \cup \{\infty\}$ und $j(F)$ ist die Koordinate auf $\mathcal{M}_1(k)$. Mit Ausnahme des unendlichen Punktes, in dem $\Delta = 0$ ist, entspricht jedem Punkt von $\mathcal{M}_1(k)$ eine k-isomorphe Klasse von Funktionenkörpern vom Geschlecht $g = 1$. Dies ist nicht der Fall, wenn der Konstantenkörper nicht algebraisch abgeschlossen ist.
Die Aussage von Satz 5.18. wird bewiesen, indem man die betreffenden Gleichungen angibt. Das heißt, ausgehend von einem Wert für j definiert man die entsprechende Gleichung. Dies erfordert eine Fallunterscheidung nach der Charakteristik $\chi(K)$ des Konstantenkörpers. Es entstehen verschiedene Isomorphieklassen wenn $\chi(K) = 2$ und wenn $\chi(K) \neq 2$. Da eine eingehende Behandlung viel Raum in Anspruch nehmen würde, verweisen wir auf die Literatur.[12, 35, 74]

5.22. Proposition. *Es sei $j \in \mathcal{M}_1(k)$. Es existiert ein Funktionenkörper F/k, der über $k(j)$ mit $j(F/k) = j$ definiert wird.*

Beweis[74]. Für $j \neq 0$ oder $j \neq 12^3$ definiert die folgende Gleichung

$$f(x,y) = y^2 + xy - x^3 + \frac{36}{j - 12^3}x + \frac{1}{j - 12^3}$$

einen elliptischen Funktionenkörper F/k mit $j(F/k) = j$ über einem Körper von beliebiger Charakteristik. Wenn $j = 0$ ist, wird der Funktionenkörper durch folgende Gleichung definiert:

$$f(x,y) = y^2 + y - x^3 + a_{00}$$

Im Fall $j = 12^3$ ist

$$f(x,y) = y^2 - x^3 + a_{10}x$$

die definierende Gleichung.□

5.2.3 g=2

5.23. Definition. Ein algebraischer Funktionenkörper F/k über k vom Geschlecht $g \geq 2$ über k, der einen rationalen Teilkörper $k(x) \subseteq F$ mit $[F : k(x)] = 2$ enthält, heißt hyperelliptisch.

5.24. Lemma. *(a) Ein algebraischer Funktionenkörper F/k vom Geschlecht $g \geq 2$ über k ist hyperelliptisch genau dann, wenn es einen Divisor $A \in \mathcal{D}(F/k)$ mit $\deg A = 2$ und $\dim(A) \geq 2$ gibt.*
(b) Jeder Funktionenkörper F/k vom Geschlecht $g = 2$ ist hyperelliptisch.

5.25. Proposition. *Es sei k ein vollkommener Körper der Charakteristik $\chi(k) \neq 2$.*
(a) Es sei F/k ein hyperelliptischer Funktionenkörper vom Geschlecht g. Es existieren $x, y \in F$ so daß $F = k(x, y)$ und

$$y^2 = f(x) \in k[x]$$

mit einem quadratfreien Polynom f(x) vom Grad $2g+1$ oder $2g+2$.
(b) Umgekehrt, falls $F = k(x, y)$ und $y^2 = f(x) \in k[x]$ mit einem quadratfreien Polynom $f(x)$ vom Grad $m \geq 4$, dann ist F/k ein hyperelliptischer Funktionenkörper vom Geschlecht

$$g = \begin{cases} \frac{m-1}{2} \text{ falls } m \cong 1 \mod 2, \\ \frac{m-2}{2} \text{ falls } m \cong 0 \mod 2. \end{cases}$$

(c) Es sei $F = k(x, y)$ mit $y^2 = f(x) \in k[x]$ wie in (a). Die in $F/k(x)$ verzweigten Primdivisoren $P \in \mathbb{P}_{k(x)}$ sind die folgenden:

alle Nullstellen von $f(x)$, falls $\deg f(x) \cong 0 \mod 2$,
alle Nullstellen von $f(x)$ und die Polstelle von x , falls $\deg f(x) \cong 1 \mod 2$.

Infolgedessen gilt: Wenn $f(x)$ in lineare Faktoren zerfällt, dann sind genau $2g+2$ Primdivisoren von $k(x)$ verzweigt in $F/k(x)$.

5.26. Bemerkung. Im Falle $\chi(k) = 2$ sind alle Primdivisoren in der quadratischen Erweiterung $F/k(x)$ wild verzweigt.

Wir widmen uns dem hyperelliptischen Fall vom Geschlecht 2. Für eine eingehende Behandlung des Themas verweisen auf die Originalarbeit von Igusa. [36] Wir betrachten die Varietät $\mathbf{V}_{6,2}(k)$. Die Dimension von $\mathbf{V}_{6,2}(k)$ ist 19. Für die definierende Gleichung eines hyperelliptischen Funktionenkörpers benötigt man jedoch viel weniger Koeffizienten. Wenn $\chi(k) \neq 2$ gibt es sechs Weierstrass-Punkte. Wir erhalten eine definierende Gleichung der Form:

$$f(x, y) = y^2 + \sum_{i=0}^{6} a_i x^{6-i}$$

also

$$y^2 = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2\cdot 2+2}) \;\; c \in k$$

und durch geeignete birationale Transformation erhalten wir für $\alpha_1, \cdots, \alpha_6$ die Werte $0, 1, \infty, \lambda_1, \lambda_2, \lambda_3$ und damit die Normalgleichung:

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

Im Falle $\chi(k) = 2$ benötigt man anstelle einer Kummer- eine Artin-Schreier-Erweiterung: $y^2 + y = f(x)$. Das erzeugende Element y ist bis auf Transformationen vom Typ: $y \to y + B(x)$ eindeutig definiert. Hier sind $u(x)$ und $B(x)$ rationale Funktionen von x. Es sei $(a)_\infty$ der Poldivisor der Funktion $f(x)$. Durch Anwendung des Satzes von Riemann-Hurwitz erhalten wir:

$$2 = \frac{[F : k(x)]}{[k : k]}(-2) + \sum_{P \in \operatorname{supp}((a)_\infty)} (v_P + 1)$$

also

$$6 = \sum_{P \in \operatorname{supp}((a)_\infty)} (v_P + 1)$$

Diese Gleichung hat drei verschiedene Lösungen:
(i) (1+1) + (1+1) + (1+1) = 6.
(ii) (3+1) + (1+1) = 6.
(iii) (5+1) = 6
Damit erhalten wir die Normalgleichungen für $\chi(k) = 2$:

$$(1) y^2 + y + \alpha x + \beta x^{-1} + \gamma(x-1)^{-1}$$

$$(2) y^2 + y + x^3 + \alpha x + \beta x^{-1}$$

$$(3) y^2 + y + x^5 + \alpha x^3$$

mit α, β, γ verschieden von Null im ersten Fall und $b \neq 0$ im zweiten Fall.

5.27. Bemerkung. Die Gleichung $y^2 + y + x^5 + \alpha x^3 + \beta x$ ist k-isomorph zum dritten Fall. Es werden eine lineare Transformation auf x und eine Tranformation auf y, die ein quadratisches Polynom in x verwendet, durchgeführt.

Wir benötigen eine allgemeine Normalgleichung, die über alle k einen hyperelliptischen Funktionenkörper definiert.
Wir erhalten die Normalgleichung durch Anwendung des Satzes von Riemann-Roch 4.8. Nach 4.9. gilt für jeden kanonischen Divisor $W \in \mathcal{D}(F/k)$: $\deg W = 2g - 2 = 2$ und $\dim W = g = 2$. Es sei P ein Weierstrass-Punkt. Nach 4.12. existiert zu jedem $n \geq 4$ ein $x \in F$ mit $(x)_\infty = nP$. Die sieben Elemente $x^2, x^3, x^4, y, xy, x^2y, xy^2$ sind in $\mathcal{L}(6P)$. Da $\dim(6P) = 6$, existiert eine nicht-triviale Relation mit Koeffizienten aus k:

$$a_{12}xy^2 + a_{01}y + a_{11}xy + a_{21}x^2y = a_{40}x^4 + a_{30}x^3 + a_{20}x^2$$

mit $a_{12} \neq 0$ und $a_{40} \neq 0$ bzw.:

$$f(x,y) = xy^2 + (1 + b_{11}x + b_{21}x^2)y + x^4 + b_{30}x^3 + b_{20}x^2$$

Die fünf fehlenden Weierstrass-Punkte sind die Nullstellen der Diskriminante der Normalgleichung, nämlich die Wurzel der Gleichung:

$$(1 + b_{11}x + b_{21}x^2)^2 - 4x^3(a_{20} + a_{30}x + x^2) = 0$$

5.28. Bemerkung. Es werden drei verschiedene Normalgleichungen, in Abhängigkeit von der Charakteristik $\chi(k)$ des Primkörpers, definiert. Dementsprechend kann die allgemeine Normalgleichung, wenn die Charakteristik berücksichtigt wird, in die jeweils andere transformiert werden.

5.29. Definition. Es sei $f(x,y) = xy^2 + (1 + a_{11}x + a_{21}x^2)y + x^4 + a_{30}x^3 + a_{20}x^2$ die allgemeine Normalgleichung für hyperelliptische Funktionenkörper vom Geschlecht 2. Man definiert:

$$\begin{aligned}
J_2(F) &= a_{11}^2 a_{21}^2 \\
J_4(F) &= a_{11}^5 a_{21} + a_{11}^4 a_{21}^2 a_{30} + a_{11}^3 a_{21}^2(a_{21}a_{20} + 1) + a_{11}^2 a_{21}^2 a_{20}^2 + a_{11}a_{21}^3(a_{21}a_{20} + 1). \\
J_6(F) &= a_{11}^8 + a_{11}^6 a_{21}^2 a_{30}^2 + a_{11}^4 a_{21}^2(a_{21}a_{20} + 1)^2 + a_{11}^2 a_{21}^2 a_{20}^4 + a_{21}^4(a_{21}a_{20} + 1)^2, \\
J_8(F) &= 2^{-2}(J_2J_6 - J_4^2), \\
J_{10}(F) &= a_{11}^7 a_{20} + a_{11}^6(a_{21}^3 a_{20} + a_{30}) + a_{11}^5(a_{21}^4 a_{20} a_{30} + a_{21}^3 a_{30} + a_{21}a_{20} + 1) + \\
&a_{11}^4(a_{21}^5 a_{20}^2 + a_{21}^4 a_{30}^2 + a_{21}^3 + a_{20}^2) a_{11}^3 a_{21}(a_{21}a_{20} + 1)^3 + (a_{21}a_{20} + 1)^4.
\end{aligned}$$

Die $J_i(F)$, $i \in \{2,4,6,8,10\}$. heißen arithmetische Invarianten J_i von F/k.

Die Invarianten der Funktionenkörper vom Geschlecht 2 heißen auch Igusa–Invarianten. Die arithmetischen Invarianten sind in der angegebenen Darstellung für Körper der Charakteristik $\chi(k) = 2$ gültig. Wenn $\chi(k) \neq 2$, können die arithmetischen Invarianten anders definiert werden. Man kann jedoch, wie im Falle der Normalgleichungen, von einer Darstellung zur anderen übergehen.
Das Analogon zur Aussage über die Bedeutung der Invariante $j(F)$ im elliptischen Fall ist:

5.30. Satz. *Es sei k ein vollkomener Körper und seien F_1/k und F_2/k zwei hyperelliptische Funktionenkörper vom Geschlecht 2 über k. Genau dann, wenn F_1/k und F_2/k k-isomorph sind, gilt $J_i(F_1) = J_i(F_2)$, für $i \in \{2,4,6,8,10\}$.*

5.31. Bemerkung. Nach Konstruktion gilt $J_i(F) \in k$. Die $J_i(F)$ können als Moduln betrachtet werden.

5.32. Proposition. *Es sei $\mathcal{M}_2(k)$ die Modulvarietät der Funktionenkörper vom Geschlecht 2 über k. Die Elemente*

$$\frac{J_4}{J_2^2}, \frac{J_6}{J_2^3}, \frac{J_{10}}{J_2^5},$$

aus $\mathcal{M}_2(k)$ sind algebraisch unabhängig. Damit ist $\dim(\mathcal{M}_2(k) = 3$

5.33. Proposition. *Es seien $J_i \in \mathcal{M}_2(k)$. Es existiert ein Funktionenkörper F/k, definiert über $k(J_i)$ mit $J_i(F/k) = j$*

Die Aussage von Satz 5.13 wird bewiesen, indem man die betreffenden Gleichungen angibt. Wir werden uns hier darauf beschränken, beispielhaft einen Fall zu behandeln. Wir betrachten die Normalgleichung für $\chi(k) = 2$ vom Typ:

$$y^2 + y + x^5 + \alpha x^3$$

Es gilt

$$\alpha^{10} = \frac{J_8^{\frac{5}{4}}}{J_{10}}$$

Für Untersuchungen auf dem Gebiet der expliziten Konstruktion von Kurven bzw. Funktionenkörpern vom Geschlecht 2 verweisen wir auf [48, 49, 53]. Für Anwendungen sowie weitere konstruktive Untersuchungen verweisen wir auf[42, 34, 62]

5.2.4 g=3

In diesem Abschnitt untersuchen wir nicht hyperelliptische algebraische Funktionenkörper vom Geschlecht drei. Der hyperelliptische Fall wird von der angegebenen Definition im Fall $g = 2$ erfaßt.
Wir betrachten die Varietät $\mathbf{V}_{4,3}(k)$. Die Dimension von $\mathbf{V}_{4,3}(k)$ ist 14.

$$\mathbf{V}_{4,3}(k) := \{a_{i,j} \in k | 0 = f(x,y) = \sum_{i=0}^{4} \sum_{j=0}^{4} a_{i,j} x^i y^j\}$$

Da wir nicht-hyperelliptische Funktionenkörper betrachten, gibt es keinen Divisor $A \in \mathcal{D}(F/k)$ mit $\deg A = 2$.

5.34. Satz. *Es sei F/k ein nicht-hyperelliptischer Funktionenkörper vom Geschlecht $g = 3$. Es existiert ein Divisor $A \in \mathcal{D}(F/k)$ mit* $\deg A = 3$ *und* $\dim(A) \geq 2$

Beweis. Die Funktionenkörper vom Geschlecht $g \geq 2$ werden durch kanonische Divisoren erzeugt (siehe [5]). Es sei W ein kanonischer Divisor. Es gilt $\deg W = 4$ und $dim A = 4 + 1 - 3 = 2$. Da ein Divisor D vom Grad eins existiert und der Funktionenkörper nicht hyperelliptisch ist, gilt $W = A + D$ und A ist ein Divisor vom Grad drei.□

Ausgehend von der Existenz eines Divisors $A \in \mathcal{D}(F/k)$ mit $\deg A = 3$ und $\dim(A) \geq 2$ und da $g = 3 = (4-1)(4-2)/2$ gilt, erhalten wir unter Verwendung elementarsymmetrischer Funktionen eine Normalgleichung der Form:

$$f(x,y) = b_{00} + b_{10}x + b_{20}x^2 + b_{30}x^3 + b_{40}x^4 +$$

$$b_{01}y + b_{11}xy + b_{21}x^2y + b_{03}y^3$$

bzw.

$$f(x,y) = y^3 + (a_{21}x^2 + a_{11}x + a_{01})y +$$

$$x^4 + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$$

wobei die Koeffizienten der Form $b_{i2}y^2$ durch eine birationale Transformation eliminiert wurden. Bei der Transformation wurde durch drei dividiert und infolgedessen hat diese Normalform eine schlechte Reduktion $\mod 3$. Setzen wir $a(x) = a_{21}x^2 + a_{11}x + a_{01}$ und $b(x) = x^4 + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$ so erhalten wir für die Diskriminante der Gleichungsordnung den Ausdruck: $\Delta = 4a(x)^3 + 27b(x)^2$. Aus diesem Ausdruck wird ersichtlich, daß diese Normalform nicht allgemein gültig ist, wenn der Konstantenkörper k der Charakteristik $\chi(k) = 2, 3$ ist. Im allgemeinen wissen wir, daß wir bei einer Reduktion modulo eines Primdivisors des Konstantenkörpers, nur für endlich viele Primdivisoren des Konstantenkörpers einen Funktionenkörper vom Geschlecht $g < 3$ erwarten können. Ein globaler Funktionenkörper $F/\mathbb{F}_5$, definiert durch $y^3 + (x^2 + x + 1)y + x^4 + x^3 + x^2 + x + 1$, ist vom Geschlecht 1 über $\mathbb{F}_5$

Die Dimension von $\mathcal{M}_g(k)$ ist gleich $3g - 3 + \epsilon$ für $g > 1$ wobei ϵ die Parameterzahl der Automorphismengruppe von F/k ist und für $g > 2$ $\epsilon = 0$ gilt, wenn der Funktionenkörper hinreichend allgemein ist [12, 31]. Dies wurde bereits von Riemann [64] bewiesen. Einen weiteren Beweis findet man in [56]. Auf die Automorphismen über k werden wir nicht eingehen und verweisen auf [78, 79] für eine Behandlung der Automorphismengruppe eines Funktionenkörpers von Primzahlcharakteristik. Explizite Ausdrücke analog zu den j- bzw. Igusa–Invarianten sind für $g \geq 3$ noch unbekannt. Die Dimension von $\mathcal{M}_g(k)$ kann auf der Grundlage der bis jetzt vorgestellten Theorie errechnet werden: Die Dimension der Severi-Varietät $\mathbf{V}_{4,3}(k)$ ist 14. Betrachtet man die entsprechende Gleichung als nicht-normiert, so ist 15 die Anzahl ihrer Koeffizienten. Der Funktionenkörper wird durch die kanonische Klasse $[W]$ erzeugt und $\dim W = 3$. Also kann der Funktionenkörper durch drei Funktionen x_1, x_2, x_3 erzeugt werden. Jede dieser Funktionen läßt eine Transformation der Form

$$t_i = \frac{\alpha x_i + \beta}{\gamma x_i + \delta} \qquad (\alpha\delta - \beta\gamma) \neq 0$$

zu. Dann sind $3 \cdot 3 = 9$ Konstanten nicht-wesentlich für Definition des Funktionenkörpers. Wir erhalten

$$\dim \mathbf{V}_{4,3}(k) + 1 - 9 = 15 - 9 = \quad 6 \quad = 3 \cdot 3 - 3 = \dim \mathcal{M}_3(k)$$

5.2.5 g=4

Wir betrachten die Varietät $\mathbf{V}_{6,4}(k)$. Die Dimension von $\mathbf{V}_{6,4}(k)$ ist 21.

$$\mathbf{V}_{6,4}(k) := \{a_{i,j} \in k | 0 = f(x,y) = \sum_{i=0}^{6} \sum_{j=0}^{6} a_{i,j} x^i y^j\}$$

Da wir nicht-hyperelliptische Funktionenkörper betrachten, gibt es keinen Divisor $A \in \mathcal{D}(F/k)$ mit $\deg A = 2$.

5.35. Satz. *Es existieren zwei verschiedene Arten nicht-hyperelliptischer Funktionenkörper vom Geschlecht 4. Die erste enthält eine Divisorenklasse vom Grad drei und der Dimension zwei und die andere enthält zwei Divisorenklassen vom Grad drei und der Dimension zwei.*

Beweis. Der Funktionenkörper wird von der kanonischen Klasse erzeugt. Es sei W ein kanonischer Divisor. Es gilt $\deg W = 6$.
(a) Es existieren zwei verschiedene Divisoren A_1, A_2 mit $A_1 + A_2 = W$, jeweils vom Grad drei. Durch Anwendung des Satzes von Riemann–Roch und da $\dim W = g = 4$ gilt $\dim A_1 = 3 + 1 - 4 + \dim(W - A_1) = 2$. Analog gilt $\dim A_2 = 2$. Die zugeordnete Divisorenklassen sind $[A_1]$ und $[A_2]$.
(b) Wir betrachten den Fall $A_1 = A_2$. Es gilt $\dim A_1 = 2$ und $\deg A_1 = 3$. $\square$.
Wir erhalten zwei verschiedene Normalgleichungen. Wenn es zwei verschiedene Divisorenklassen vom Grad drei gibt, dann existieren zwei Funktionen x, y vom Grad drei, die als unabhängige Variabeln gewählt werden können. Wählt man o.B.d.A. x als unabhängige Variable, so ist y Wurzel einer Gleichung dritten

Grades. Die Normalgleichung ist also eine Gleichung dritten Grades in beiden Variablen:

$$f(x,y) = y^3 + (a_{32}x^3 + a_{22}x^2 + a_{12}x + a_{02})y^2 +$$

$$(a_{31}x^3 + a_{21}x^2 + a_{11}x + a_{01})y + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}.$$

Wenn es nur eine Divisorenklasse vom Grad drei gibt und da $\deg W = 6$ erhalten wir unter Verwendung elementarsymmetrischer Funktionen eine Normalgleichung der Form

$$f(x,y) = y^3 + (a_{4,1}x^4 + a_{31}x^3 + a_{21}x^2 + a_{11}x + a_{01})y +$$

$$x^6 + a_{50}x^5 + a_{40}x^4 + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}.$$

wobei die Koeffizienten der Form $a_{i2}y^2$ durch eine birationale Transformation eliminiert wurden. Setzen wir $a(x) = a_{4,1}x^4 + a_{31}x^3 + a_{21}x^2 + a_{11}x + a_{01}$ und $b(x) = x^6 + a_{50}x^5 + x^4 + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$ so erhalten wir für die Diskriminante der Gleichungsordnung den Ausdruck: $\Delta = 4a(x)^3 + 27b(x)^2$. Es handelt sich um eine ganze rationale Funktion zwölften Grades. Aus diesem Ausdruck wird ersichtlich, daß diese Normalform nicht allgemein gültig ist, wenn der Konstantenkörper k der Charakteristik $\chi(k) = 2, 3$ ist. Mit der gleichen Methode wie im Fall $g = 3$ gilt:

$$\dim \mathbf{V}_{4,4}(k) - 6 = 15 - 6 = \quad 9 \quad = 3 \cdot 4 - 3 = \dim \mathcal{M}_4(k)$$

Wenn die Divisorenklassen zusammenfallen, dann hat die Normalgleichung 12 Koeffizienten. Die erzeugenden Elemente x, y lassen folgende Transformationen zu:

$$t = \frac{\alpha x + \beta}{\gamma x + \delta} \qquad (\alpha\delta - \beta\gamma) \neq 0$$

und

$$\tau = \frac{my}{(\gamma x + \delta)^2} \quad m \in \mathbb{Z}$$

Damit reduziert sich die Anzahl der wesentlichen Koeffizienten auf $12 - 4 = 8$ und die Invarianten der Normalgleichung bilden eine Untervarietät der Dimension 8 von $\mathcal{M}_4(k)$.

Kapitel 6

Reduktion nach Primdivisoren des Konstantenkörpers

In diesem Kapitel gehen wir folgender Frage nach: Es sei F/k ein Funktionenkörper, der als Primkörper den Körper $\mathbb{Q}$ enthält. Wie ändert sich die Struktur des Funktionenkörpers, wenn der Primkörper $\mathbb{Q}$ durch einen Primkörper k der Charakteristik $\chi(k) = p$, p eine Primzahl, ersetzt wird?
Wir geben hier im wesentlichen Ergebnisse von Deuring [11] wieder. Beweise der hier vorgestellten Sätze findet man im eben zitierten Artikel oder in [15] ,III.6.

6.1. Definition. Ein noetherscher, faktorieller Integritätsring mit 1, in dem jedes von Null verschiedene Primideal ein maximales Ideal ist, heißt Dedekindring.

Es sei k ein vollkommener Körper, x transzendent über k, und ein irreduzibles Polynom $f \in k[x][y]$ mit $\deg_y(f) = n$, welches bezüglich y normiert und separabel ist. f erzeuge den Funktionenkörper F/k. Der Konstantenkörper k enthalte einen Dedekindring R, von dem k der Quotientenkörper ist. O.b.d.A. gelte: Die Koeffizienten $a_i(x)$ von f sind Elemente aus $R[x]$[15]. Es ist hervorzuheben, daß der Gleichungsring $k[x,y]/f(x,y)k[x,y]$ weder ein ZPE- noch ein Dedekindring ist [61].

6.2. Definition. Es sei P ein Primdivisor des Konstantenkörpers k. Die Reduktion modulo P ist eine Abbildung $\tilde{(\cdot)} : R \to R/P$, definiert durch $t \mapsto t + P$.

6.3. Bemerkung.

1. Es sei $k = \mathbb{Q}$ und $R = \mathbb{Z}$. Dann ist $(\tilde{f}) : \mathbb{Z} \to \mathbb{Z}/P$ und man erhält eine Gleichung $\tilde{f}$ mit Koeffizienten in $\mathbb{Z}_p[x]$.

2. Es sei k_1 ein Körper und $k = k_1(x)$ und $R = k_1[x]$. Die Reduktion modulo $P = x - x_0$, mit $x_0 \in k_1$, bedeutet die Anwendung des Einsetzungshomomorphismus $\Phi(x_0)$, also $x = x_0$.

Es sei also R/P der Restklassenkörper von R bezüglich P. Man ersetzt alle Koeffizienten in dem Polynom $f \in R[x]$ durch die entsprechenden Restklassen aus R/P und erhält ein Polynom $\tilde{f} \in R/P[x]$.

6.4. Satz. *Es sei k ein vollkommener Körper, x transzendent über k, und ein irreduzibles Polynom $f \in k[x][y]$ mit $\deg_y(f) = n$, welches bezüglich y normiert und separabel ist. f erzeuge den Funktionenkörper F/k. Es gibt nur endlich viele Primdivisoren P von k, für welche f im Restklassenkörper $\tilde{k}$ mod P oder in einer Erweiterung $\tilde{k_r}$ reduzibel oder auch nur inseparabel wird.*

Nun gehen wir auf die Merkmale der erhaltenen Struktur $\widetilde{F/k}$ ein, bzw. betrachten wir strukturerhaltende Eigenschaften der Abbildung Reduktion modulo P:

6.5. Satz. *Es sei F/k ein Funktionenkörper vom Geschlecht g über k und $\widetilde{F/k}$ der aus F/k durch Reduktion modulo P erhaltene Funktionenenkörper vom Geschlecht $\tilde{g}$. Es gilt:*

$$\tilde{g} \leq g$$

Der Vergleich von g und $\tilde{g}$ wird mit Hilfe des Satzes von Riemann-Hurwitz durchgeführt.
Nun benötigen wir einige Definitionen und Ergebnisse aus Kapitel 2: Wir betrachten den Bewertungsring $\mathcal{O}_P$ des Primdivisors P. Jedes Element $0 \neq a \in F/k$ hat eine eindeutige Darstellung $a = t^n u, \quad t$ ist ein Primelement für P und $u \in {\mathcal{O}_P}^*$. Ein Element $a \in F/k$ ist ein Primelement von $\mathcal{O}_P$ genau dann, wenn $v_P(a) = 1$.

6.6. Satz. *Es sei F/k ein Funktionenkörper vom Geschlecht g über k, $A, B \in \mathcal{D}(F/k)$ und $\widetilde{F/k}$ vom gleichen Geschlecht g über $\tilde{k}$. In dem Fall kann man jedem Divisor $A \in \mathcal{D}(F/k)$ einen Divisor $\tilde{A} \in \mathcal{D}(\widetilde{F/k})$ zuordnen, so daß Folgendes gilt:*

1. $\widetilde{A+B} = \tilde{A} + \tilde{B}$
2. $\deg A = \deg \tilde{A}$
3. $\widetilde{(a)} = (\tilde{a}) \qquad \forall a \in F/k$ *so daß* $v_P(a) = 1$

Der Satz besagt, daß die Abbildung Reduktion modulo P $\tilde{(\cdot)}$ ein Homomorphismus, sowohl der Gruppe $\mathcal{D}(F/k)$ in die Gruppe $\mathcal{D}(\widetilde{F/k})$, als auch der Divisorenklassengruppe $\mathcal{C}l(F/k)$ in die Divisorenklassengruppe $\mathcal{C}l(\widetilde{F/k})$ ist.

6.7. Satz. *Es sei F/k ein Funktionenkörper vom Geschlecht g über k und $\widetilde{F/k}$ vom Geschlecht $\tilde{g}$ über $\tilde{k}$ mit $\tilde{g} = g$. Es sei $[W]$ die kanonische Klasse von F/k und $\widetilde{[W]}$ die kanonische Klasse in $\widetilde{F/k}$. Es gilt:*

$$\widetilde{[W]} = [\tilde{W}]$$

6.8. Satz. *Es sei F/k ein Funktionenkörper und $\widetilde{F/k}$ der aus F/k durch Reduktion modulo P erhaltene Funktionenkörper. Ist $\tilde{x}$ separierend für $\widetilde{F/k}$ so ist es x für F/k.*

Zusammenfassend: Es sei F/k ein Funktionenkörper vom Geschlecht g über k. Für fast alle Primdivisoren P des Konstantenkörpers k ist $\tilde{k}$ der Konstantenkörper von $\widetilde{F/k}$ und das Geschlecht ist gleich g. Wenn das Geschlecht von $\widetilde{F/k}$ kleiner als g ist, spricht man von einer schlechten Reduktion modulo P.

6.9. Beispiel. Wir betrachten Kleins Quartik, definiert durch $f(y,z) = z^3 + y^3z + y$ über $\mathbb{Q}$. Durch eine birationale Transformation erhalten wir die Gleichung: $g(z,u) = u^7 - \frac{z^3}{(1-z)}$. Der Funktionenkörper, definiert durch $f(y,z)$, ist vom Geschlecht 3. Reduziert man modulo 7, so erhält man einen Funktionenkörper vom Geschlecht 0. $f(y,z)$, reduziert modulo 2, definiert einen Funktionenkörper vom Geschlecht 3.

Kapitel 7

Über die Anzahl der Primdivisoren vom Grad Eins

Es sei F/k ein globaler Funktionenkörper. Wie wir aus 3.11. wissen, gibt es zu jedem $n \in \mathbb{Z}$ höchstens endlich viele positive Divisoren vom Grad n, also positive Elemente aus der Menge $\mathcal{D}^n(F/k)$ wenn der Konstantenkörper k endlich ist. Infolgedessen ist die Anzahl der Primdivisoren vom Grad eins endlich.
Man betrachtet Lösungen $(x_0, y_0) \in k \times k$ der den globalen Funktionenkörper definierenden Gleichung $f(x, y) = 0$, mit $f \in k[x][y]$. Wir erinnern an die Definition 1.74.: Es sei k ein Körper und $\mathbf{V}$ eine affine Varietät der Dimension 1 über k. Die Menge

$$\mathbf{V}(k) = \mathbf{V} \cap \mathbf{A}^2(k) = \{P = (a_1, a_2) \in \mathbf{V} \mid \text{alle } a_i \in k\}$$

heißt Menge der k-rationalen Punkte von $\mathbf{V}$. Die Betrachtung des Beispiels 1.71.4. vermittelt uns eine Vorstellung über die Gestalt der Primdivisoren vom Grad eins in ihrer Darstellung als maximale Ideale im $\mathbf{Spec}\, k[x, y]$.
Die Primdivisoren eines Funktionenkörpers sind per Definition (3.1.) die Stellen des Funktionenkörpers, so daß man alternativ von den Stellen vom Grad eins eines Funktionenkörpers oder von den rationalen Punkten auf einer Kurve sprechen kann. In der Literatur begegnet man allen drei Bezeichnungen.

7.1. Definition. Es sei F/k ein globaler Funktionenkörper vom Geschlecht g über $k = \mathbb{F}_q$.

1. $N_{F/k}$ ist die Anzahl der Primdivisoren P vom Grad eins des globalen Funktionenkörpers F/k.

2. $N_q(g)$ ist die maximale Anzahl der Primdivisoren vom Grad eins für die Klasse der Funktionenkörper vom Geschlecht g über $k = \mathbb{F}_q$.

3. Ein globaler Funktionenkörper F/k heißt optimal, falls $N_{F/k} = N_q(g)$.

Daraus ersieht man die Untersuchungsfelder: Bestimmung der Zahlen $N_{F/k}$ und $N_q(g)$ bzw. entsprechender Schranken und Bestimmung oder Konstruktion von Funktionenkörpern, die möglichst optimal sind. Dies bestimmt die Gliederung der ersten drei Unterabschnitte dieses Kapitels: Als erstes werden obere Schranken für $N_q(g)$ eingeführt und in diesem Rahmen wird definiert, wann ein globaler Funktionenkörper als Funktionenkörper mit vielen Stellen vom Grad eins bezeichnet wird. Danach wird eine elementare Methode zur expliziten Bestimmung der Anzahl der Primdivisoren vom Grad eins vorgestellt und zuletzt werden wir über verschiedene Ansätze zur Bestimmung oder Konstruktion von globalen Funktionenkörper mit vielen Primdivisoren vom Grad eins berichten.

7.1 Obere Schranken

Die Potenzreihe

$$\zeta_{F/k}(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{Z}[[t]] \subseteq \mathbb{C}((t))$$

mit $A_n := |\{A \in \mathcal{D}(F/k) \mid A \geq 0 \text{ und } \deg A = n\}|$ wird als die Zeta-Funktion $\zeta_{F/k}(t)$ des Funktionenkörpers F/k bezeichnet. $\mathbb{C}((t))$ ist die Menge der Potenzreihen in der Unbestimmten t über $\mathbb{C}$. Die entsprechende L-Reihe des Funktionenkörpers $F/\mathbb{F}_q$ ist:

$$L_{F/\mathbb{F}_q}(t) := (1-t)(1-qt)\zeta_{F/\mathbb{F}_q}(t)$$

$L_{F/\mathbb{F}_q}(t)$ ist, als Polynom betrachtet, vom Grad kleiner oder gleich $2g$
Ein Ergebnis von Hasse für elliptische Funktionenkörper wurde von Weil verallgemeinert. Es handelt sich um das Analogon der Riemannsche Vermutung für Funktionenkörper [96]:

7.2. Satz. *(Hasse–Weil) Für die Kehrwerte der Wurzeln $\alpha_i, \dots, \alpha_{2g}$ von $L_{F/\mathbb{F}_q}(t)$ gilt:*

$$|\alpha_i| = q^{1/2} \qquad \textit{für} \qquad 1 \leq i \leq 2g$$

Für einen Beweis siehe [81],V.2.
Aus dem Satz von Hasse–Weil folgt eine Abschätzung für die Anzahl der Primdivisoren vom Grad eins $N_q(g)$ eines Funktionenkörpers $F/\mathbb{F}_q$ vom Geschlecht g:

$$|N_q(g) - (q+1)| \leq 2gq^{\frac{1}{2}} \tag{7.3}$$

Diese Abschätzung heißt Hasse–Weil–Schranke. Damit erhalten wir eine obere Abschätzung:

$$N_q(g) \leq q + 1 + 2gq^{\frac{1}{2}} \tag{7.4}$$

Es ist hervorzuheben, daß die Hasse–Weil Schranke sowie andere Schranken für die Anzahl der Primdivisoren vom Grad eins eines globalen Funktionenkörpers nur von der Kardinalität des Konstantenkörpers und vom Geschlecht g des Funktionenkörpers abhängt.
Die Hasse–Weil–Schranke ist im allgemeinen eine gute Abschätzung, d.h.: Es existieren globale Funktionenkörper, die sie erreichen. Man kann jedoch genauere obere Schranken angeben. Z.B. wenn q kein Quadrat ist, dann gilt:

$$N_q(g) \leq q + 1 + \lfloor 2gq^{\frac{1}{2}} \rfloor$$

Serre bewies in [70], daß die Hasse–Weil–Schranke verbessert werden kann:

$$N_q(g) \leq q + 1 + g\lfloor 2q^{\frac{1}{2}} \rfloor \tag{7.5}$$

Dieser Ausdruck heißt **Serre–Schranke**.

Für $g > (q - q^{\frac{1}{2}})/2$ gibt es eine bessere Abschätzung für $N_q(g)$ als die durch die Serre–Schranke zur Verfügung gestellten. In einer Arbeit von 1981 [37] wurde die als **Ihara–Schranke** bezeichnete Ungleichung bewiesen:

$$N_q(g) \leq q + 1 + \lfloor \frac{\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g}{2} \rfloor. \tag{7.6}$$

Die Grundidee läst sich wie folgt grob skizzieren: Es wird angenommen, daß $N_{F/\mathbb{F}_q}$ groß ist. Dann liegen die Werte der Wurzeln $\alpha_i, \ldots, \alpha_{2g}$ von $L_{F/\mathbb{F}_q}(t)$ in einer kleinen Umgebung von $-q^{\frac{1}{2}}$ in $\mathbb{C}$. Die Werte der ${\alpha_i}^2$ befinden sich infogedessen in einer kleinen Umgebung von q, so daß $N_{F/\mathbb{F}_{q^2}}$ klein ist. Es gilt jedoch $N_{F/\mathbb{F}_q} \leq N_{F/\mathbb{F}_{q^2}}$. Unter Verwendung der Cauchy-Schwarz-Ungleichung erhält man die Ihara–Schranke. Aus der Ihara–Schranke erhält man eine asymptotische Schranke:

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g} \leq \left(2q + \frac{1}{4}\right)^{1/2} - \frac{1}{2}.$$

Wenn q ein Quadrat ist, dann gilt $A(q) \geq q^{1/2} - 1$. Drinfeld und Vladut zeigten:

$$A(q) \leq q^{1/2} - 1$$

Diese Abschätzung heißt **Drinfeld–Vladut–Schranke**.

7.7. Beispiel. Wir betrachten Kleins Quartic über $\mathbb{F}_4$, also den Funktionenkörper definiert durch $y^3 + x^3y + x \in \mathbb{F}_4[x][y]$. Das Geschlecht dieses Funktionenkörpers ist $g = 3$. Die Serre–Schranke für $N_4(3)$ hat den Wert 17. Die Ihara–Schranke für $N_4(3)$ hat den Wert 14. Für Kleins Quartic über $\mathbb{F}_8$ hat die Serre–Schranke für $N_8(3)$ den Wert 24. Die Ihara–Schranke für $N_8(3)$ hat den Wert 25.

Iharas Methode wurde von Drinfeld und Vladut in [14] und von Serre verallgemeinert. Serre führte in [70] die Idee der Anwendung von *expliziten Formeln* ein. Der folgender Satz führt zu besseren Ergebnisse wenn das Geschlecht groß im Verhältnis zu q ist.

7.8. Proposition. *Es seien $c_1, \dots, c_m \in \mathbb{R}$, die folgende Bedingungen erfüllen:*

1. *$c_r \geq 0$ für $r = 1, \dots, m$ und nicht alle $c_r = 0$.*
2. *Es sei $\lambda_m(t) := \sum_{r=1}^{m} c_r t^r$ und $f_m(t) := 1 + \lambda_m(t) + \lambda_m(t^{-1})$. Damit definieren wir: $f_m(t) \geq 0$ für alle $t \in \mathbb{C}$ mit $|t| = 1$.*

Dann gilt:

$$N_q(g) \leq \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1.$$

Für einen Beweis siehe [81] ,V.3.3.
Eine Umformung dieses Ergebnisses ist

$$(N_q(g) - 1)\lambda_m(q^{-1/2}) - \lambda_m(q^{1/2}) \leq g \tag{7.9}$$

Die rechte Seite von 7.9 wurde für alle $f_m(t) \geq 0$ für alle $t \in \mathbb{C}$ mit $|t| = 1$ von Oesterlé in einem bei Serre eingereichten unveröffentlichten Manuskript maximiert. Eine Darstellung dieser Ideen findet man in [67]. Wir bieten eine Skizze des Resultates in Anlehnung an Auer [2]:
Es sei $\Phi_m : [\frac{\pi}{m+1}, \frac{\pi}{m}] \to [0, 1]$, $m \in \mathbb{N}$, definiert durch

$$\phi \mapsto -\frac{\cos \frac{m+1}{2}\phi}{\cos \frac{m-1}{2}\phi}.$$

Die Ableitung dieser Abbildung ist

$$\Phi'_m(\phi) = (\sin m\phi + m \sin \phi)/(2\cos^2 \frac{m-1}{2}\phi).$$

Damit ist Φ ein isotoner Homöomorphismus. Dann wird eine Abbildung

$$\vartheta_q : [q + 1, \infty) \to [0, 1)$$

stückweise definiert:
Es sei $N \in \mathbb{R}$ so daß $N \geq q+1$ und $2 \leq m \in \mathbb{Z}$ sei die einzige Zahl so daß $N \in [q^{m/2}+1, q^{(m+1)/2}+1)$. Wir setzen

$$u := \frac{1}{q^{1/2}} \frac{q^{(m+1)/2} - N + 1}{N - 1 - q^{(m-1)/2}} \in (0, 1].$$

und definieren $\vartheta_q(N) := \cos(\Phi_m^{-1}(u))$. Aus dem Verhalten der Ableitung dieser Funktion folgt, daß $\vartheta_q(N)$ ein isotoner Homeomorphismus ist. Zuletzt betrachten wir die Abbildung $\gamma_q : [q+1, \infty) \to [0, \infty)$ definiert durch

$$\gamma_q : N \mapsto 1 + \frac{N(q^{1/2}\vartheta_q(N) - 1)}{q - 2q^{1/2}\vartheta_q(N) + 1}.$$

γ_q ist isoton auf $[q^2+1, \infty)$. Dies gilt weil $\vartheta_q(q^2+1) = 1/2^{1/2} \geq 1/q^{1/2}$. Man zeigt daß

$$\gamma_q(N) = (N - q - 1)/2q^{1/2} \quad \text{für} \quad N \in [q+1, q^{3/2}+1] \tag{7.10}$$

und

$$\gamma_q(N) = 1/4q(N - q^2 - 1 + \tag{7.11}$$

$$\sqrt{(8q+1)N^2 - (18q^2+16q+2)N + q^4 + 8q^3 + 18q^2 + 8q + 1})$$

für $N \in [q3/2+1, q^2+1]$. Es gilt also: γ_q ist auf $[q+1, q^2+1]$ streng monoton fallend.

7.12. Satz. *(Oesterlé) Es sei $N_{F/\mathbb{F}_q} \geq q+1$. Dann gilt:*

$$g \geq \gamma_q(N_{F/\mathbb{F}_q}).$$

Für $q \geq 3$ ist $\gamma_q(N_{F/\mathbb{F}_q})$ das Maximum der linken Seite der Ungleichung 7.9 für alle $f_m(t) \geq 0$ für alle $t \in \mathbb{C}$ mit $|t| = 1$. Im Fall $q = 2$ gilt diese Aussage nicht immer.

Für einen Beweis siehe [82].
Man definiert unter Verwendung der Umkehrfunktion von γ_q:

$$\bar{N}_q := \gamma_q^{-1} : [0, \infty) \to [q+1, \infty)$$

Es gilt dann

$$N_q(g) \leq \bar{N}_q \quad \text{für alle } g \in \mathbb{Z}^{\geq 0} \tag{7.13}$$

Diese Abschätzung heißt **Oesterlé –Schranke**. Diese Abschätzung ist die genaueste wenn das Geschlecht g groß in Verhältnis zu q ist. Aus der Gleichung (7.10) folgt, daß für $g \in [0, (q - q^{1/2})/2]$ die Oesterlé–Schranke mit der Hasse–Weil–Schranke übereinstimmt. Aus (7.11) und für $g \in \left[\frac{1}{2}(q - q^{1}2), (\frac{q}{2})^{1/2}(q-1)\right]$ erhält man die Ihara–Schranke. Wir betrachten zwei bedeutende Beispiele:

7.14. Beispiel. 1. Wir vergleichen die Abschätzungen für $N_3(5)$:

(a) Die Hasse–Weil–Schranke hat den Wert 21.

(b) Die Serre–Schranke hat den Wert 19.

(c) Die Ihara–Schranke hat den Wert 15.

(d) Die Oesterlé –Schranke hat den Wert 14.

Ein herausragendes Ergebnis ist, daß die oberen Schranken nicht in jedem Fall erreicht werden können. K. Lauter zeigte in [46] die Unmöglichkeit der Existenz eines Funktionenkörpers $F/\mathbb{F}_3$ vom Geschlecht 5 mit $N_{F/\mathbb{F}_3} = 14$.

2. Wir betrachten Kleins Quartik über $\mathbb{F}_4$, also den Funktionenkörper, definiert durch $y^3 + x^3y + x \in \mathbb{F}_4[x][y]$. Das Geschlecht dieses Funktionenkörpers ist $g = 3$.

(a) Die Serre–Schranke für $N_4(3)$ hat den Wert 17.

(b) Die Ihara–Schranke für $N_4(3)$ hat den Wert 14.

(c) Die Oesterlé –Schranke für $N_4(3)$ beträgt 14.

Die entsprechenden Abschätzungen für Kleins Quartik über $\mathbb{F}_8$ sind:

(a) Die Serre–Schranke für $N_8(3)$ hat den Wert 24.

(b) Die Ihara–Schranke für $N_8(3)$ hat den Wert 25.

(c) Die Oesterlé –Schranke für $N_8(3)$ hat den Wert 24.

Eine elementare Betrachtung läßt die Schwierigkeiten bei der Bestimmung von $N_q(g)$ deutlich werden:
In einem geometrischen Zusammenhang ist folgendes zu bemerken: q ist die Kardinalität des 1-dimensionalen affinen Raums $\mathbf{A}^1(\mathbb{F}_q)$, $q+1$ ist die Kardinalität des projektiven Raums $\mathbf{P}^1(\mathbb{F}_q)$ und q^2+q+1 ist die Kardinalität des projektiven Raums $\mathbf{P}^2(\mathbb{F}_q) = \mathbf{A}^2(\mathbb{F}_q) \cup \mathbf{P}^1(\mathbb{F}_q)$. Wenn $\mathbf{V}$ eine affine Varietät vom Geschlecht g über $\mathbb{F}_q$ ist, dann ist die Bestimmung von $N_q(g)$ gleichbedeutend mit der Bestimmung einer Schranke für die Kardinalität der Menge der $\mathbb{F}_q$-rationalen Punkte:

$$|\,\mathbf{V}(\mathbb{F}_q)| = |\,\mathbf{V} \cap \mathbf{A}^2(k)| \leq N_q(g)$$

Betrachten wir im obigen Beispiel die Serre–Schranke für $N_4(3)$. Ihr Wert ist 17. Die Anzahl der rationalen Punkte einer Varietät $\mathbf{V}(\mathbb{F}_4)$ vom Geschlecht 3 über $\mathbb{F}_4$ ist $|\mathbf{V} \cap \mathbf{A}^2(\mathbb{F}_4)|$ und $|\mathbf{A}^2(\mathbb{F}_4)| = 16$. Infolgedessen hat eine Kurve, die die Serre–Schranke erreicht, einen Punkt mehr als der zugrundeliegende affine Raum. Es ist zu vermuten, daß wenn das Geschlecht größer wird, die Schwierigkeiten, eine Varietät zu finden, die eine vorgegebene Schranke erreicht, zunehmen. Im Fall des Beispiels 7.14.1 stellt man fest, daß $|\mathbf{A}^2(\mathbb{F}_3)| = 9$ und theoretisch 14 rationale Punkte existieren könnten. Der projektive Raum $\mathbf{P}^2(\mathbb{F}_3)$ enthält 13 Punkte. Die Varietät hätte einen Punkt mehr als der zugrundeliegende projektive Raum. Der Beweis der Unmöglichkeit der Existenz einer solchen Varietät ist allerdings nicht trivial. Es gibt in der Tat nur zwei bewiesene Beispiele: Das oben erwähnte [46] und ein weiteres von Serre [71]:
Es existiert keine Kurve vom Geschlecht $g = 7$ über $\mathbb{F}_2$ die 11 rationale Punkte hat, wobei 11 die entsprechende Oesterlé –Schranke ist. In diesem Fall konnte Serre die Oesterlé –Schranke verbessern und (mit Hilfe einer Grad 2 Erweiterung des elliptischen Funktionenkörpers mit 5 Punkten, definiert durch $y^2 + y + x^3 + x \in \mathbb{F}_2[x][y]$, in der genau eine Stelle vom Grad 5 verzweigt ist) eine Kurve mit 10 Punkten finden. Der projektive Raum $\mathbf{P}^2(\mathbb{F}_2)$ enthält 7 Punkte. Für globale rationale Funktionenkörper bestimmte Serre:

$$N_q(0) = q + 1.$$

Für die Klasse der globalen, elliptischen Funktionenkörper, sowie für die Klasse der globalen, hyperelliptischen Funktionenkörper wurden $N_q(1)$ und $N_q(2)$ ebenfalls von Serre bestimmt [69]. Die Bestimmung von $N_q(g)$ für $g \geq 3$ durch explizite Formeln ist bis heute nicht gelungen.
Ein weiteres Ergebnis von Serre ist [71]:

7.15. Satz. *Es sei $F/\mathbb{F}_q$ ein Funktionenkörper vom Geschlecht g. Falls $N_q(g) = q + 1 + g\lfloor 2q^{\frac{1}{2}} \rfloor$ gilt, dann ist $g = 1$ oder $g = 2$.*

Für globale Funktionenkörper von Geschlecht $g \geq 3$, die eine zusätzliche Bedingung erfüllen, erhält man das folgende Ergebnis:

7.16. Proposition. *Es sei $F/\mathbb{F}_q$ ein Funktionenkörper vom Geschlecht $g \geq 3$ mit $N_q(g) < q + 1 + g\lfloor 2q^{\frac{1}{2}} \rfloor$. Dann gilt: $N_q(g) \leq q - 1 + g\lfloor 2q^{\frac{1}{2}} \rfloor$.*

Wir widmen uns jetzt der Frage: Wann bezeichnet man einen globalen Funktionenkörper als Funktionenkörper mit vielen Stellen vom Grad eins? In 7.1.3 wurden optimale Funktionenköper definiert: Für sie gilt $N_{F/\mathbb{F}_q} = N_q(g)$. Funktionenkörper mit einer Anzahl von Primdivisoren vom Grad eins, die die Hasse-Weil–Schranke erreichen, werden besonders gekennzeichnet:

7.17. Definition. Ein globaler Funktionenkörper F/k vom Geschlecht g heißt maximal, falls $N_{F/k} = q + 1 + 2gq^{1/2}$.

7.18. Bemerkung. Aus der Definition folgt, daß ein globaler Funktionenkörper F maximal ist, wenn $g = 0$ oder wenn $\mathbb{F}_{q^2}$ der Konstantenkörper ist.

Wenn ein globaler Funktionenkörper $F/\mathbb{F}_q$ maximal ist, kann man eine obere Schranke für das Geschlecht g von $F/\mathbb{F}_q$ angeben.

7.19. Proposition. *Es sei $F/\mathbb{F}_q$ ein maximaler, globaler Funktionenkörper vom Geschlecht g. Dann gilt:*

$$g \leq (q - q^{\frac{1}{2}})/2.$$

Aus diesem Satz folgt, daß ein globaler Funktionenkörper nicht maximal sein kann, wenn das Geschlecht groß im Vergleich zu q ist.
Rück und Stichtenoth [65] zeigten, daß der Hermitesche Funktionenkörper (d.h. der Funktionenkörper definiert durch eine Gleichung $H(x, y) = y^q + y - x^{q+1}$ mit $H(x, y) \in \mathbb{F}_{q^2}$) der einzige (bis auf $\mathbb{F}_{q^2}$-isomorphismen) maximale, globale Funktionenkörper über $\mathbb{F}_{q^2}$ vom Geschlecht $g = (q - 1)q/2$ ist.

7.20. Satz. *(Fuhrmann und Torres) Es sei $F/\mathbb{F}_q$ ein maximaler Funktionenkörper. Dann gilt:*

$$\textit{Entweder } g = (q - q^{\frac{1}{2}})/2 \ \textit{ oder } \ g \leq (q^{\frac{1}{2}} - 1)^2/4.$$

Für einen Beweis dieses Satzes siehe [20]. Für eine eingehende Behandlung maximaler Funktionenkörper verweisen wir auf [19]. Die Serre–Schranke und der Satz von Fuhrmann–Torres ergeben:

7.21. Korollar. *Es sei $F/\mathbb{F}_q$ ein globaler Funktionenkörper. Wenn q ein Quadrat mit $q \geq 16$ ist und $(q - q^{\frac{1}{2}})/2 \neq g \geq (q^{\frac{1}{2}} - 1)^2/4$, dann gilt:*

$$N_{F/k} \leq q - 1 + 2gq^{1/2}.$$

Wenn $g \leq 50$ ist in vielen Fällen die Ihara–Schranke, die genauere obere Schranke für $N_q(g)$. Da die Drinfeld–Vladut–Schranke in etwa das $1/2^{1/2}$-fache der asymptotischen Ihara–Schranke beträgt wird ein Intervall

$$[N_q(g)/2^{1/2}, N_q(g)]$$

als Maßstab vereinbart [87]: Ein globaler Funktionenkörper wird als Funktionenkörper mit vielen Stellen vom Grad eins bezeichnet, wenn

$$N_{F/\mathbb{F}_q} \in [N_q(g)/2^{1/2}, N_q(g)]$$

Abschließend gehen wir auf den Fall $g = 3$, bei dem es ein Ergebnis von K. Lauter gibt. Wir widergeben ihr Resultat [1, 44]:
Sei $m(q) := 3\lfloor 2sqrt(q)\rfloor$ die Serre–Schranke für den Betrag der Frobenius-Spur $q+1-N_{F/\mathbb{F}_q} = sum_{i=1}^{6}\alpha_i$ eines globalen Funktionenkoerpers $F/\mathbb{F}_q$ vom Geschlecht 3. Für jedes q existiert dann ein Funktionenkörper $F/\mathbb{F}_q$ vom Geschlecht $g = 3$ über $\mathbb{F}_q$ und es gilt

$$|N_{F/\mathbb{F}_q} - (q+1)| \geq m(q) - 3.$$

Mit anderen Worten, der sogenannte Defekt $m(q)$ beträgt -für alle q- höchstens 3. (Für Geschlecht 1 bzw. 2 ist dieser Defekt ebenfalls durch 2 bzw. 3 beschränkt, doch hat Serre die Vermutung geäussert, daß der Defekt für genügend großes (festes) Geschlecht g, etwa $g > 10$, stets unbeschraenkt ist.) Bis auf den genauen Wert für den Defekt war Lauters Ergebnis für $g = 3$ sicher Serre bereits bekannt (s. seine Arbeiten), und sie konnte eben nicht das ämbiguity of signProblem lösen, auf das Serre seinerzeit hingewiesen hatte. Wir gehen auf dieses Problem nicht ein. Es wird deshalb erwähnt, um auf die Schwierigkeiten auf dem Gebiet hinzuweisen. Es ist von Bedeutung, weil es daran nach wie vor die allgemeine Bestimmung von $N_q(3)$ scheitert. Stattdessen wird für jedes q die Existenz eines Funktionenkörpers vom Geschlecht 3 mit entweder sehr vielen oder sehr wenigen rationalen Punkten gesichert.

7.2 Ein Satz von Kummer

Wir stellen ein elementares Verfahren zur expliziten Ermittlung der Primdivisoren vom Grad eins eines globalen Funktionenkörpers vor. Die Grundlage dieses Verfahrens ist ein Satz von E. Kummer. Wir verwenden die Notation von Kapitel 6 und weisen insbesondere auf die Bemerkung 6.3.2. hin.

7.22. Satz. *(Kummer)Es sei F ein Funktionenkörper und $F' = F(y)$ eine algebraische Erweiterung mit y ganz über $\mathcal{O}_P$ und $\varphi(T) \in \mathcal{O}_P[T]$ das Minimalpolynom von y über F. Darüber hinaus sei*

$$\tilde{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i}$$

die Faktorisierung von $\tilde{\varphi}(T)$ in irreduzible Faktoren über $\tilde{F}$ (d.h.: Die γ_i sind irreduzible, normierte, paarweise verschiedene Polynome in $\tilde{F}[T]$ und $\epsilon_i \geq 1$). Man wähle normierte Polynome $\varphi_i(T) \in \mathcal{O}_P[T]$ mit der Eigenschaft

$$\tilde{\varphi}(T) = \gamma_i(T) \quad und \quad \deg \varphi_i(T) = \gamma_i(T).$$

Dann existieren Primdivisoren P_i von F' für die gilt:

$$P_i \mid P, \quad \varphi_i(y) \in P_i \quad f(P_i \mid P) \geq \deg \gamma_i(T).$$

und $P_i \neq P_j$ für $i \neq j$. Nimmt man an, daß mindestens eine der beiden folgenden Prämissen erfüllt wird

1. $\epsilon_i = 1$ *für* $i = 1, \dots, r$,
2. $\{1, y, \dots, y^{n-1}\}$ *ist eine Ganzheitsbasis für* P.

Dann existiert genau ein Primdivisor P_i mit $P_i \mid P$ und $\varphi(y) \in P_i$, für $1 \leq i \leq r$. Die Primdivisoren $P_1, \dots, P_r$ sind alle Primdivisoren von F', die über P liegen und man erhält

$$Con_{F'/F}(P) = \sum_{i=1}^{r} \epsilon_i P_i,$$

d.h. $\epsilon_i = e(P_i \mid P)$. Der Restklassenkörper $F'_{P_i} = \mathcal{O}_{P_i}/P_i$ ist isomorph zu $\tilde{F}[T]/(\gamma_i(T))$, und infolgedessen $f(P_i \mid P) = \deg \gamma_i(T)$.

Beweis. Siehe [81] ,III.3.7. Ein Fall des Satzes von Kummer ist für praktische Berechnungen von besonderer Bedeutung:

7.23. Korollar. *Es sei $\varphi(T) = T^n + f_{n-1}(x)T^{n-1} + \ldots + f_0(x) \in K(x)[T]$ ein irreduzibles Polynom über den rationalen Funktionenkörper $K(x)$. Wir betrachten den Funktionenkörper $K(x,y)/K$, wobei y die Gleichung $\varphi(y) = 0$ erfüllt und ein Element $\alpha \in K$ mit der Eigenschaft $f_j(\alpha) \neq \infty$ für alle j mit $0 \leq j \leq n-1$. Wir verwenden die Bezeichnung P_α für den Primdivisor von $K(x)$, die Nullstelle von $x - \alpha$ in $K(x)$. Man setzt voraus, daß das Polynom*

$$\varphi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + \ldots + f_0(\alpha) \in K[T]$$

folgende Faktorisierung im Polynomring $K[T]$:

$$\varphi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)$$

mit irreduziblen, normierten, paarweise verschiedenen Polynomen $\psi_i(T) \in K[T]$. Dann erhalten wir:

1. *Zu jedem $i = 1, \dots, r$ existiert ein eindeutig bestimmter Primdivisor P_i von $K(x,y)$ so daß $x - \alpha \in P_i$ und $\psi_i(y) \in P_i$. Das Element $x - \alpha$ ist ein Primelement von P_i (d.h. $e(P_i \mid P_\alpha) = 1$), und der Resklassenkörper von P_i ist isomorph zu $K[T]/(\psi_i(T))$. Dann gilt: $f(P_i \mid P) = \deg \psi_i(T)$.*

2. *Falls* $\deg \psi_i(T) = 1$ *für mindestens ein* $i \in \{1, \dots, r\}$, *dann ist* K *der exakte Konstantenkörper von* $K(x, y)$.

3. *Falls* $\varphi_\alpha(T)$ $n = \deg \varphi(T)$ *verschiedene Wurzeln in* K *hat, dann existiert zu jedem* β *mit* $\varphi_\alpha(\beta) = 0$ *ein eindeutig bestimmter Primdivisor* $P_{\alpha,\beta}$ *von* $K(x, y)$ *so daß*

$$x - \alpha \in P_{\alpha,\beta} \quad \textit{und} \quad y - \beta \in P_{\alpha,\beta}.$$

   $P_{\alpha,\beta}$ *ist ein Primdivisor von* $K(x, y)$ *vom Grad 1.*

Beweis. Wir setzen $F := K(x)$ und $F' := K(x, y)$. Die Annahme $f_j(\alpha) \neq \infty$ besagt, daß y ganz über $\mathcal{O}_{P_\alpha}$, und das Polynom $\varphi_\alpha(T)$ ist $\tilde{\varphi}(T)$. Wir nehmen also $\epsilon_i = 1$ für $i = 1, \dots, r$ an und mit dem Satz von Kummer folgt die Behauptung.$\square$.

7.24. Beispiel. Wir betrachten Kleins Quartik über $\mathbb{F}_8$ und beispielsweise den Primdivisor $P = x - 1$. Wir führen eine Reduktion modulo P durch und betrachten $f(x, y) \mod (x-1)\mathbb{F}_8[x, y]$. Nach 6.3.2 erhalten wir das Polynom $\widetilde{f(x, y)} = y^3 + y + 1$. Die Faktorisierung dieses Polynoms über $\mathbb{F}_8$ mit einem erzeugenden ω für die zyklische Erweiterung $\mathbb{F}_8/\mathbb{F}_2$ ergibt:

$$\widetilde{f(x, y)} = (x + \omega)(x + \omega^2)(x + \omega^4)$$

Aus diesem Ergebnis läßt sich schließen, daß über dem Primdivisor $P = x - 1$ von $\mathbb{F}_8(x)$ vom Grad eins drei unverzweigte Primdivisoren vom Grad eins vom Funktionenkörper $F' = \mathbb{F}_8(x, \rho)$ mit $f(x, \rho) = 0$ existieren. Diese Primdivisoren sind: $P_1 = (x-1, \rho-\omega), P_2 = (x-1, \rho-\omega^2), P_3 = (x-1, \rho-\omega^4)$. Durch Reduktion modulo P für alle Primdivisoren P von $\mathbb{F}_8(x)$ und anschließende Aufzählung ermittelt man $N_{F'/\mathbb{F}_8} = 24$. Wir wir aus 7.14.3. wissen, beträgt der Wert der Oesterlé–Schranke für $N_8(3)$ 24. Das ist einer der Gründe für die Bedeutung dieses Funktionenkörpers

Eine algorithmische Darstellung des Satzes von Kummer ist:

7.25. Algorithmus. *(Berechnung der Primdivisoren vom Grad 1)*

Eingabe: *Die definierende Gleichung eines Funktionenkörpers* $F/\mathbb{F}_q$.

Ausgabe: *Die Primdivisoren vom Grad 1 von* $F/\mathbb{F}_q$.

1. *(Primdivisoren für die Reduktion) Bestimme die Elemente* N *des Konstantenkörpers, die Nullstellen der Ordnungsdiskriminante sind. Bilde die Menge* R *der Primdivisoren vom Grad eins von* $\mathbb{F}_q(x)$, *so daß für alle* $x - \alpha_i \in R$ *mit* $1 \leq i \leq q$ *die Bedingung* $\alpha_i \notin N$ *erfüllt ist.*

2. *(Reduktion modulo P) Führe die Reduktion modulo P für jedes $P \in R$ durch.*

3. *(Faktorisierung) Faktorisiere das Bild der Reduktion modulo P.*

4. *(Ende) Ausgabe der Primdivisoren vom Grad 1 von $F/\mathbb{F}_q$. Terminiere.*

7.3 Methoden

In diesem Abschnitt berichten wir über verschiedene Ansätze, die angewandt werden, um Funktionenkörper mit vielen Primdivisoren vom Grad eins zu konstruieren, bzw. zu ermitteln. Die einzelnen Methoden können nicht im Rahmen dieser Arbeit diskutiert werden. Entsprechende Literaturhinweise begleiten jedoch die Vorstellung der Methoden. Die Zuordnung erfolgt nach der zugrundeliegenden Theorie bzw. Ansatz und orientiert sich an der von van der Geer und van der Vlugt angegebenen Einteilung [87].

1. *Klassenkörpertheoretische Methode.* Die Konstruktion globaler Funktionenkörper mit vielen Primdivisoren vom Grad eins unter Verwendung der Klassenkörpertheorie, insbesondere von Strahlklassenkörpern, geht auf Serre zurück. In 4.1. wurde der Adele-Raum $\mathcal{A}_F$ eines Funktionenkörpers definiert. Bei dieser Methode konstruiert man abelsche Erweiterungen des Funktionenkörpers F/k, die bestimmte Strukturen im Adele-Raum berücksichtigen. Ein Merkmal der konstruierten Funktionenkörper ist das vorgegebene Verzweigungsverhalten. Die Methode wurde von Serre [69], Schoof [67], Lauter [47], Niederreiter und Xing [57] und Auer [2] u.a. angewandt.

   Eine weitere Methode verwendet Drinfeld- Module vom Rang 1. Die Methode wurde von Niederreiter und Xing [58] eingeführt. Für eine Einführung in die Theorie der Drinfeld-Module siehe [25]. Wenn man Erweiterungen eines rationalen Funktionenkörpers betrachtet, kann man gute explizite Ergebnisse erreichen.

2. *Faserprodukte von Artin – Schreier – Erweiterungen* Die Definition eines Faserproduktes findet man in [31],II.3.3. Ausgehend von einem Funktionenkörper $F/\mathbb{F}_q$ betrachtet man bei dieser Methode Artin-Schreier-Erweiterungen F_f über $F/\mathbb{F}_q$ definiert durch $F_f = F(\alpha)$, wobei α eine Lösung einer Gleichung $\alpha^p - \alpha = f$ ist und f aus einer bestimmten Teilmenge $L \subseteq \mathcal{L}(D)$ des Funktionenkörpers $\mathbb{F}_q(x)$ für einen geeigneter Divisor D ist. Die Faserprodukte sind ganz verzweigte Erweiterungen von F und aus diesem Grund erwartet man viele Primdivisoren vom Grad eins. G. van der

Geer und M. van der Vlugt [88], [90],[89], [86], Shabat [72] und Stichtenoth [80] u.a. haben diese Methode angewandt.

3. *Funktionenkörpertürme* Es handelt sich um eine Kombination von Artin-Schreier- und Kummer-Erweiterungen oder Körperkomposita von Kummer-Erweiterungen. Die Funktionenkörper werden explizit angegeben. Funktionenkörpertürme werden z.B. von Garcia und Stichtenoth [23], Niederreiter und Xing [57], Özbudak und Stichtenoth [59] und Thomas [82] behandelt.

4. *Weitere Methoden*

   (a) Formeln für $N_q(1)$ und $N_q(2)$ [70].

   (b) *Explizite Kurven* Es gibt explizite Funktionenkörper, dessen Eigenschaften weitgehend bekannt sind: Kleins Quartik, Hermitesche Funktionenkörper und Kummer- bzw. Artin-Schreier-Erweiterungen. Man sucht nach Polynomen $f(x) \in \mathbb{F}_q[x]$, für die eine Artin-Schreier-Erweiterung

   $$\sum_{i=0}^{m} a_i y^{p^i} = f(x) \qquad \chi(\mathbb{F}_q) = p, \quad a_0, a_m \neq 0$$

   viele Primdivisoren vom Grad eins hat. Computerorientierte Untersuchungen ermöglichen auch empirische Versuche mit dem Ziel, explizite Kurven zu bestimmen. Referenzen auf dem Gebiet der explizit definierten Funktionenkörper sind u.a.: [22], [28], [27], [71], [98].

   (c) *Quotientenkörper* Hermitesche Funktionenkörper sind die Grundlage für die Konstruktion dieser Funktionenkörper. Siehe [28] und [24] u.a.

   (d) *Deligne−Lustig−Kurven* Die Suzuki und die Ree Kurven sind Verallgemeinerungen der Hermiteschen Kurven bzw. Funktionenkörper. Die Deligne-Lusztig-Kurven umfassen diese Typen von Funktionenkörpern. Von Bedeutung bei diesem Ansatz ist die Untersuchung der Automorphismengruppe. Die Deligne-Lusztig-Varietäten wurden, im Zusammenhang mit der Codierungstheorie, von Hansen eigeführt: [29]. Die Methode wird in [45] von Lauter angewandt und erläutert.

   (e) *Elliptische modulare Kurven.* Man betrachtet nicht einzelne elliptische Kurven sondern die Menge aller Isomorphismusklassen elliptischer Kurven und definiert damit eine algebraische Kurve. Aus der Untersuchung von Funktionen und Differentialformen auf dieser Varietät lassen sich Aussagen über die Eigenschaften elliptischer Kurven ableiten. Analog untersucht man Kurven vom Geschlecht $g \geq 2$. Eine Einführung in die Theorie der modularen elliptischen Kurven findet man in [75]. Die Methode wurde u.a. in [90] angewandt. In diesem Artikel wird auch der Zusammenhang der Untersuchungen auf dem Gebiet der Kurven mit vielen rationalen Punkten mit der Codierungstheorie besonders hervorgehoben.

7.4 Normalformen-Untersuchung

In theoretischer Hinsicht untersucht dieser Ansatz den Zusammenhang zwischen der Anzahl der Primdivisoren vom Grad eins $N_{F/k}$ bzw. den Schranken für $N_q(g)$ und der Severi–Varietät $\mathbf{V}_{ng}$ sowie der Modulvarietät $\mathcal{M}_g(k)$ über $\mathbb{F}_q$. Ein Hauptmerkmal dieser Methode ist die Konstruktion der definierenden Gleichung des Funktionenkörpers und läßt sich unter die expliziten Untersuchungen einordnen. Es ist im allgemeinen keine Methode um Funktionenkörper mit vielen Primdivisoren vom Grad eins zu konstruieren, sondern eine Methode um ganze Klassen von Funktionenkörpern zu untersuchen. Auf dieser Grundlage kann man, unter anderem, Funktionenkörper von vorgegebenem Geschlecht konstruieren und nach der Untersuchung der Anzahl ihrer Primdivisoren vom Grad eins, dann durch eine geignete Konstantenkörpererweiterung neue Funktionenkörper mit vielen Primdivisoren vom Grad eins konstruieren.
Ein wichtiger Aspekt ist, daß eine Normalform Schranken für den Grad in beiden Variablen bietet. Auf dieser Grundlage kann man andere Methoden anwenden, um gezielt Funktionenkörper mit vielen Primdivisoren vom Grad eins zu konstruieren. Man hat eine Schranke für den Grad eines Divisors des zugrundeliegenden rationalen Funktionenkörpers und eine Grundform für die anschließende Erweiterung. Durch geeignete Wahl des Divisors und der restlichen Koeffizienten läßt sich das Verzweigungsverhalten festlegen. Eine andere Möglichkeit ist die Konstruktion von Gleichungen durch Erzeugung eines Zufallspolynoms im rationalen Funktionenkörper, die als Koeffizienten in die Normalform eingesetzt werden. Die Methode ist geeignet, um Informationen für Datenbanken von Funktionenkörpern hinsichtlich codierungstheoretischer- bzw. kryptographischer Anwendungen zu ermitteln. Unter Berücksichtigung der Punkte der Varietät $\mathcal{M}_g(k)$ kann man die Anzahl und den Wert der Koeffizienten der definierenden Gleichung einschränken. Dadurch entstehen Fragen des Typs: Haben elliptische Kurven über $\mathbb{F}_{2^r}$ mit der j-Invariante 0 mehr rationale Punkte als elliptische Kurven mit anderen j-Invarianten? . Die analoge Frage bezüglich der Igusa–Invarianten ist auch von Bedeutung. Die Grenzen der Methode liegen darin, daß es in diesem Zusammenhang noch zahlreiche ungelöste Fragen gibt.

Kapitel 8

Anwendung

8.1 Algebraisch-geometrische Goppa Codes

Die Codierungstheorie ist eine der interessantesten Anwendungsgebiete der Theorie der globalen Funktionenkörper. In diesem Abschnitt bieten wir eine elementare Einführung in die Codierungstheorie. Darüber hinaus zeigen wir an einem Beispiel, wie man einen algebraisch-geometrischen Goppa–Code konstruiert. Für eine Einführung in die algebraisch-geometrische Codierungstheorie verweisen wir auf [26, 93, 85, 51, 55, 81, 83]. Ein algorithmischer Ansatz, insbesondere zum Thema Decodierung findet man in [18, 73].
Unter $\mathbb{F}_q^n$ verstehen wir den n-dimensionalen $\mathbb{F}_q$-Vektorraum. Die Elemente $a \in \mathbb{F}_q^n$ sind n-Tupel $a = (a_1, \dots, a_n)$, $a_i \in \mathbb{F}_q$.

8.1. Definition. Ein Code C (über das Alphabet $\mathbb{F}_q$) ist ein linearer Unterraum von $\mathbb{F}_q^n$. n ist die Länge von C und k ist die Dimension von C als $\mathbb{F}_q$-Vektorraum. Ein $[n,k]_q$ Code ist ein Code der Länge n und Dimension k. Die Elemente aus C heißen Wörter.

Der Vektorraum $\mathbb{F}_q^n$ wird mit einer Metrik d (Hamming–Abstand) versehen:

8.2. Definition. Für $a, b \in \mathbb{F}_q^n$ ist

$$d(a,b) := |\{i | 1 \le i \le n, \quad a_i \ne b_i\}|$$

. Das Gewicht $w(a)$ wird definiert als

$$w(a) := d(a,0) = |\{i | 1 \le i \le n, \quad a_i \ne 0\}|$$

.

8.3. Definition. Ein $[n, k]_q$Code C als linearer Unterraum von $\mathbb{F}_q^n$ in dem die Metrik d definiert ist, wird als linearer Code C mit Parametern $[n, k, d]_q$ bezeichnet.

Die Effektivität eines fehlerkorrigierenden Codes wird anhand der Informationsrate k/n von C gemessen. Aus den Definitionen folgt, daß

$$d = min\{w(a)|a \in C,\ a \neq 0\}$$

Diese Metrik wird als minimaler Abstand bezeichnet und wird verwendet um die Effektivität eines fehlerkorrigierenden Codes zu messen. Als Untervektorraum besitzt C eine $\mathbb{F}_q$-Basis. Eine $k \times n$ Matrix, die als Zeilen k Basiselemente von C enthält, wird als erzeugende Matrix von C bezeichnet. In der folgenden Definition bezeichnet $<,>$ das kanonische Skalarprodukt in $\mathbb{F}_q^n$.

8.4. Definition. Es sei C ein linearen Code. Der duale Code $C^\perp$ wird definiert als

$$C^\perp := \{b \in \mathbb{F}_q^n|\quad < a, b >= 0,\ \ \forall a \in C\}$$

Die Parameter eines dualen Codes $C^\perp$ sind $[n, n-k, d']_q$. d' ist nicht notwendig gleich d.

8.5. Definition. Eine erzeugende Matrix H von $C^\perp$ heißt Prüfmatrix von C.

$C^\perp$ ist ein $[n, n-k, d']_q$ Code und infolgedessen ist die Prüfmatrix von C eine $n-k \times n$ Matrix vom Rang $n-k$. Die Prüfmatrix ermöglicht eine Aussage über die Zugehörigkeit eines Wortes zum Code C, nämlich

$$C = \{u \in \mathbb{F}_q^n | H \cdot u^t = 0\}$$

hier bezeichnet u^t die Transponierte von u. Der Bestimmung der Parameter eines Codes wird in der Codierungstheorie grosse Bedeutung beigemessen. Man ist an Unterräume von $\mathbb{F}_q^n$ von einer großen Dimension im Verhältnis zur Dimension des gesamten Raumes interessiert. In diesen Unterräumen sollte auch d im Verhältnis zu n groß sein. Es gibt obere und untere Schranken für die Parameter eines $[n, k, d]_q$ Codes mit vorgegebenen Metrik d. Einige dieser Schranken berücksichtigen die Charakteristik des zugrundeliegenden Körpers andere nicht. Ein einfaches Beispiel ist die $Singleton--Schranke$:

8.6. Proposition. *Es sei C ein linearer $[n, k, d]_q$ Code und H seine Prüfmatrix. Es gilt: $n - k \geq d - 1$.*

Beweis. $r = n - k$ ist der Rang von H, also die maximale Anzahl an linear unabhängigen Zeilen.□
Eine untere Schranke für die Informationsrate n/k eines Codes ist die Gilbert-Varshamov-Schranke. Eine Arbeit von Tsfasman et al.[84] zeigte, daß diese Schranke, unter Verwendung von Codes über ein Alphabet mit mehr als 49 Elementen, übertroffen werden kann. Codes, die auf globale Funktionenkörpern basieren, werden (algebraisch)- geometrische Goppa–Codes genannt.

Es sei $F/\mathbb{F}_q$ ein globaler Funktionenkörper vom Geschlecht g . Wir betrachten $P_1, \ldots P_n$ Primdivisoren vom Grad Eins von $F/\mathbb{F}_q$ und bilden den Divisor $D = P_1 + \cdots + P_n$. Es sei $G \in \mathcal{D}(F/k)$. $\mathrm{supp}(G)$ bestehe aus Primdivisoren vom Grad Eins und es gelte $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \emptyset$.

8.7. Definition. Der geometrischer Goppa–Code $C_{\mathcal{L}}(D, G)$ für die Divisoren D, G wird definiert als

$$C_{\mathcal{L}}(D, G) := \{x(P_1), \ldots , x(P_n)|x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

Die Parameter $[n, k, d]_q$ von $C_{\mathcal{L}}(D, G)$ lassen folgende Abschätzung zu:

8.8. Proposition. *Es sei $C_{\mathcal{L}}(D, G)$ ein $[n, k, d]_q$ Code. Es gilt*

$$k = dimG - dim(G - D) \text{ und } d \geq d^* = n - deg(G)$$

Der Parameter d^* wird als der designierte Minimalabstand bezeichnet. Wir führen die Codes $C_\Omega(D, G)$ ein. Diese sind die Codes, die von Goppa zuerst eingeführt wurden.

8.9. Definition. Der Code $C_\Omega(D, G)$ für die Divisoren D, G ist die Abbildung $\alpha^* : \Omega(G - D) \to \mathbb{F}_q^n$ definiert durch

$$\alpha^*(\Omega) := (Res_{P_1}(\omega), \ldots , Res_{P_n}(\omega)) \subseteq \mathbb{F}_q^n$$

8.1.1 Konstruktion eines Goppa–Codes

Codes über $\mathbb{F}_{2^r}$ sind in der Praxis von besonderer Bedeutung weil die Implementierung der zugrundeliegenden Arithmetik effizient ist. Wir konstruieren einen Code über $\mathbb{F}_{64}$ Dies wird in zwei Schritten geschehen: Als erster Schritt konstruieren wir einen Funktionenkörper (bzw. eine Kurve) mit vielen Primdivisoren vom Grad eins ($\mathbb{F}_{64}$-rationalen Punkte). Hier wird insbesondere die Bedeutung der expliziten Berechnung der Primdivisoren vom Grad eins eines Funktionenkörpers deutlich.

I. Wir betrachten den Körper $\mathbb{F}_6 4$ mit einem primitiven Element ω für die multiplikative Gruppe. Dann wählen wir den Divisor $D = 2P_1 + 2P_2 + 2P_3$ von $\mathbb{F}_{64}(x)$ mit $P_1 = x, P_2 = x + \omega^{21}, P_3 = x + \omega^{42}$. Die entsprechende rationale Funktion ist $f(x) = x^6 + x^4 + x^2$. Wir kontruieren die Artin–Schreier–Erweiterung $f(x,y) = y^2 + y + f(x)$. Die Kurve enthält 81 $\mathbb{F}_6 4$-rationale Punkte und ist vom Geschlecht 1. Da die Oesterlé –Schranke für $N_{64}(1)$ den Wert 81 hat, ist der entsprechende Funktionenkörper optimal. Die $\mathbb{F}_{64}$-rationalen Punkte sind in der folgenden Liste enthalten: $P_i = (\alpha, \beta)$ mit $\alpha, \beta \in \mathbb{F}_{64}$ stellt die gemeinsame Nullstelle von $x - \alpha$ und $y - \beta$ dar. Für den nicht im Endlichen liegenden Punkt verwenden wir die projektive Schreibweise $P_\infty = (\alpha, \beta, \gamma)$ mit $\alpha, \beta, \gamma \in \mathbb{F}_{64}$.

$$
\begin{array}{ll}
P_\infty = (0,1,0) & P_2 = (0,0) \\
P_3 = (0,1) & P_4 = (w^3, w^{11}) \\
P_5 = (\omega^3, \omega^{23}) & P_6 = (\omega^5, \omega^{36}) \\
P_7 = (\omega^5, \omega^{45}) & P_8 = (\omega^6, \omega^{22}) \\
P_9 = (\omega^6, \omega^{46}) & P_{10} = (\omega^9, \omega^{47}) \\
P_{11} = (\omega^9, \omega^{61}) & P_{12} = (\omega^{10}, \omega^9) \\
P_{13} = (\omega^{10}, \omega^2 7) & P_{14} = (\omega^{12}, \omega^{29}) \\
P_{15} = (\omega^{12}, \omega^{44}) & P_{16} = (\omega^{13}, \omega^{55}) \\
P_{17} = (\omega^{13}, \omega^{62}) & P_{18} = (\omega^{15}, \omega^{11}) \\
P_{19} = (\omega^{15}, \omega^{23}) & P_{20} = (\omega^{17}, \omega^9) \\
P_{21} = (\omega^{17}, \omega^{27}) & P_{22} = (\omega^{18}, \omega^{31}) \\
P_{23} = (\omega^{18}, \omega^{59}) & P_{24} = (\omega^{19}, \omega^{47}) \\
P_{25} = (\omega^{19}, \omega^{61}) & P_{26} = (\omega^{20}, \omega^{18}) \\
P_{27} = (\omega^{20}, \omega^{54}) & P_{28} = (\omega^{21}, 0) \\
P_{29} = (\omega^{21}, 1) & P_{30} = (\omega^{24}, \omega^{25}) \\
P_{31} = (\omega^{24}, \omega^{58}) & P_{32} = (\omega^{26}, \omega^{47}) \\
P_{33} = (\omega^{26}, \omega^{61}) & P_{34} = (\omega^{27}, \omega^{36}) \\
P_{35} = (\omega^{27}, \omega^{45}) & P_{36} = (\omega^{30}, \omega^{22}) \\
P_{37} = (\omega^{30}, \omega^{46}) & P_{38} = (\omega^{31}, \omega^{37}) \\
P_{39} = (\omega^{31}, \omega^{43}) & P_{40} = (\omega^{33}, \omega^{37}) \\
P_{41} = (\omega^{33}, \omega^{43}) & P_{42} = (\omega^{34}, \omega^{18}) \\
P_{43} = (\omega^{34}, \omega^{54}) & P_{44} = (\omega^{36}, \omega^{55}) \\
P_{45} = (\omega^{36}, \omega^{62}) & P_{46} = (\omega^{38}, \omega^{31}) \\
P_{47} = (\omega^{38}, \omega^{59}) & P_{48} = (\omega^{39}, \omega^{37}) \\
P_{49} = (\omega^{39}, \omega^{43}) & P_{50} = (\omega^{40}, \omega^{36}) \\
P_{51} = (\omega^{40}, \omega^{45}) & P_{52} = (\omega^{41}, \omega^{55}) \\
P_{53} = (\omega^{41}, \omega^{62}) & P_{54} = (\omega^{42}, 0) \\
P_{55} = (\omega^{42}, 1) & P_{56} = (\omega^{45}, \omega^{18}) \\
P_{56} = (\omega^{45}), \omega^{54}) & P_{58} = (\omega^{47}, \omega^{50}) \\
P_{59} = (\omega^{47}, \omega^{53}) & P_{60} = (\omega^{48}, \omega^{50})
\end{array}
$$

$P_{61} = (\omega^{48}, \omega^{53})$ $P_{62} = (\omega^{51}, \omega^{50})$
$P_{63} = (\omega^{51}, \omega^{53})$ $P_{64} = (\omega^{52}, \omega^{31})$
$P_{65} = (\omega^{52}, \omega^{59})$ $P_{66} = (\omega^{54}, \omega^{9})$
$P_{67} = (\omega^{54}, \omega^{27})$ $P_{68} = (\omega^{55}, \omega^{25})$
$P_{69} = (\omega^{55}, \omega^{58})$ $P_{70} = (\omega^{57}, \omega^{25})$
$P_{71} = (\omega^{5}7, \omega^{58})$ $P_{72} = (\omega^{59}, \omega^{29})$
$P_{73} = (\omega^{5}9, \omega^{44})$ $P_{74} = (\omega^{60}, \omega^{29})$
$P_{75} = (\omega^{6}0, \omega^{44})$ $P_{76} = (\omega^{61}, \omega^{22})$
$P_{77} = (\omega^{61}, \omega^{46})$ $P_{78} = (\omega^{62}, \omega^{11})$
$P_{79} = (\omega^{62}, \omega^{23})$ $P_{80} = (1, \omega^{21})$
$P_{81} = (1, \omega^{42})$
T= 20 ms

II. Wir definieren den Code $C_{\mathcal{L}}(D, G)$. Der Divisor D wird definiert als $D = P_2 + \cdots + P_{81}$ also die Summe über alle endlichen rationale Punkte. Die Länge n des definierten Codes ist 80. Der Divisor G wird definiert als $G = 23P_\infty$ mit $0 < m < 80$. Die Parameter des Codes sind $[80, 23, d \geq 80 - 23]_{64}$. Eine Basis für den Riemann–Roch–Raum $\mathcal{L}(23P_\infty)$ ist:
$\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}, (x^3 + x^2 + y), (x^4 + x^3 + xy), (x^5 + x^4 + x^2y), (x^6 + x^5 + x^3y), (x^7 + x^6 + x^4y), (x^8 + x^7 + x^5y), (x^9 + x^8 + x^6y), (x^{10} + x^9 + x^7y), (x^{11} + x^{10} + x^8y), (x^{12} + x^{11} + x^9y), (x^{13} + x^{12} + x^{10}y)\}$ Und damit ist die erzeugende Matrix eine 23×80 Matrix. Jede Zeile enthält die Werte der Funktionen aus dem Riemann–Roch–Raum an den P_i Punkten.

8.2 Beispiele

Sämtliche Berechnungen wurden mit dem Computeralgebrasystem KASH[40] auf eine Intel P3 mit 500 Mhz und 500 RAM durchgeführt.

8.2.1 Ein rationaler Funktionenkörper

Wir betrachten folgende Primdivisoren vom Grad eins des rationalen Funktionenkörpers $\mathbb{F}_9(x)$:
$P_1 = x - 0$, $P_2 = x - 1$, $P_3 = x - 2$. Wir bilden den Divisor $D = 2P_1 + 2P_2 + 2P_3$. Diesem Divisor entspricht die rationale Funktion $f(x) = x^6 + x^4 + x^2$. Dann konstruieren wir eine Erweiterung $y^3 + a(x)y + f(x)$. Durch eine geeignete Wahl von $a(x)$, und zwar $a(x) = x^2 + x + 1$, bestimmen wir das Verzweigungsverhalten: Die Diskriminante ist $D(x) = (x + 2)^4$. Durch Anwendung der Riemann–Hurwitz–Formel erhalten wir:
$2g = -2 \cdot 6 + (3 - 1) + (3 - 1) + (3 - 1) + (3 - 1) + (3 - 1) + 2 = 0$. Wobei

die Stelle P_∞ durch einen Beitrag eines Summanden $3 - 1 = 2$ berücksichtigt wurde. Die folgende Tabelle enthält Daten über $N_{F/\mathbb{F}_9}$. Die letzte Zeile enthält die Rechenzeiten für die Bestimmung der Primdivisoren vom Grad eins.

q =	9
Serre–Schranke	10
Oesterlé–Schranke	10
Ihara–Schranke	10
$N_{F/\mathbb{F}_q}$	10
T=	10ms

Es wird darauf hingewiesen, daß die Wahl des Koeffizienten $a(x) = x + 1$ zu einem Funktionenkörper vom Geschlecht 2 führt. Dieser Funktionenkörper enthält wenige Primdivisoren vom Grad eins: 13 von 21 möglichen nach Oesterlé. Die Artin–Schreier–Erweiterung, die durch die Wahl von $a(x) = 1$ konstruiert wird, ist vom Geschlecht 3 und wird später behandelt.

8.2.2 $\mathcal{M}_1(\mathbb{F}_4)$ und $N_{F/\mathbb{F}_{4^r}}$

Zur Tabelle eins: Wir betrachten die Modulvarietät $\mathcal{M}_1(\mathbb{F}_4)$. Ihre Elemente werden in der ersten Spalte der Tabelle eingetragen. In der zweiten Spalte werden die definierenden Gleichungen der elliptischen, globalen Funktionenkörper über $\mathbb{F}_4$ bis auf $\mathbb{F}_4$-Isomorphismen eingetragen. Die folgenden Spalten enthalten die Einträge: Die erste Zeile bezeichnet den exakten Konstantenkörper $\mathbb{F}_{4^r}$ mit $4 \leq 4^r \leq 2048$. Die folgenden Zeilen enthalten die entsprechende Anzahl $N_{F/\mathbb{F}_{4^r}}$ der Primdivisoren vom Grad eins. Das Ablesen des Eintrags in der ersten Zeile ermöglicht einen Vergleich von $N_{F/\mathbb{F}_{4^r}}$ mit $|\mathbf{P}^1(\mathbb{F}_{q^r})| = q^r + 1$.

Die zur Klasse der Funktionenkörper vom Geschlecht 1 über $\mathbb{F}_4$ gehörenden Schranken werden in der Tabelle 2 aufgeführt. Die Oesterlé– Schranke berücksichtigt den Satz von Fuhrmann–Torres.

Die Tabelle 3 enthält die zur Tabelle 1 entsprechende Werte für $2048 \leq 4^r \leq 32768$.

j	$F/\mathbb{F}_4$	**q=**4	8	16	32	64	128	256	512	1024
0	y^2+y+x^3	9	9	9	33	81	129	225	513	1089
0	$y^2+y+x^3+\omega$	1	9	9	33	81	129	225	513	1089
0	y^2+y+x^3+x	5	5	25	25	65	145	225	545	1025
0	$y^2+y+x^3\omega x$	5	9	17	33	65	129	257	513	1089
0	$y^2+y+x^3+x+\omega$	5	5	25	25	65	145	225	545	1025
0	$y^2+y+x^3+\omega x+\omega$	5	9	17	33	65	129	257	513	1089
0	$y^2+\omega y+x^3$	3	9	21	33	57	129	273	513	993
0	$y^2+\omega y+x^3+\omega$	7	9	13	33	73	129	273	513	1057
1	y^2+xy+x^3+1	8	4	16	44	56	116	288	508	968
1	$y^2+xy+x^3+\omega x^2+1$	2	4	16	44	56	116	288	508	968
ω	$y^2+xy+x^3+\omega$	4	8	16	32	72	128	240	512	1072
ω	$y^2+xy+x^3+\omega x^2+\omega$	6	8	16	32	72	128	240	512	1072

Tabelle 1 $\mathcal{M}_1(\mathbb{F}_{4^r})$ und $N_{F/\mathbb{F}_{4^r}}$ mit $4 \leq 4^r \leq 1024$.

q=	4	8	16	32	64	128	256	512	1024
Serre–Schranke	9	14	25	44	81	151	289	558	1089
Oesterlé–Schranke	9	14	25	44	81	151	289	558	1089
Ihara–Schranke	9	17	33	65	129	257	513	1025	2049

Tabelle 2 $N_{4^r}(1)$ mit $4 \leq 4^r \leq 1024$.

j	$F/\mathbb{F}_4$	**q=**2048	4096	8192	16384	32768
0	y^2+y+x^3	2049	3969	8193	16641	32769
0	$y^2+y+x^3+\omega$	2049	3969	8193	16641	32769
0	y^2+y+x^3+x	1985	4225	8065	16385	33025
0	$y^2+y+x^3\omega x$	2049	4097	8193	16129	32769
0	$y^2+y+x^3+x+\omega$	1985	4225	8065	16385	33025
0	$y^2+y+x^3+\omega x+\omega$	2049	4097	8193	16129	32769
0	$y^2+\omega y+x^3$	2049	4161	8193	16257	32769
0	$y^2+\omega y+x^3+\omega$	2049	4033	8193	16257	32769
1	y^2+xy+x^3+1	2116	4144	8012	16472	33044
1	$y^2+xy+x^3+\omega x^2+1$	2116	4144	8012	16472	33044
ω	$y^2+xy+x^3+\omega$	2048	4032	8320	16576	32896
ω	$y^2+xy+x^3+\omega x^2+\omega$	2048	4032	8320	16576	32896

Tabelle 3 $\mathcal{M}_1(\mathbb{F}_{4^r})$ und $N_{F/\mathbb{F}_{4^r}}$ mit $2048 \leq 4^r \leq 32768$.

Serre–Schranke	2139	4225	8374	16641	33131
Oesterlé–Schranke	2139	4225	8374	16641	33131
Ihara–Schranke	4097	8193	16385	32769	65537

Tabelle 4 $N_{4^r}(1)$ mit $2048 \leq 4^r \leq 32768$

8.2.3 $\mathcal{M}_1(\mathbb{F}_9)$ und $N_{F/\mathbb{F}_9}$

Es sei $k = \mathbb{F}_9$ mit ω als erzeugendes Element der multiplikativen Gruppe. Wir konstruieren einen elliptischen Funktionenkörper mit vielen Primdivisoren vom Grad eins unter der Voraussetzung $j = 0$. Wir betrachten die Weierstrass-Normalgleichung

$$f(x, y) = y^2 + a_{11}xy + a_{01}y + a_{30}x^3 + a_{20}x^2 + a_{10}x + a_{00}$$

Aus der Definition und der Wahl von j folgt, daß $a_{11} = a_{20} = 0$ gilt. Wir erhalten

$$f_1(x, y) = y^2 + a_{01}y + a_{30}x^3 + a_{10}x + a_{00}$$

Die restlichen Koeffizienten bestimmen wir durch die Wahl des Divisors $D = P_1 + P_2 + P_3$ von $\mathbb{F}_9(x)$ mit $P_1 = x + 1$, $P_2 = x + \omega^5$, und $P_3 = x + \omega^7$. Die entsprechende rationale Funktion ist $f(x) = x^3 + x + 2$. Dann setzen wir $a_{01} = 1 + \omega^5 + \omega^7 = 0$. Der Funktionenkörper $F/\mathbb{F}_9$ wird definiert durch

$$g(x, y) = y^2 + x^3 + x + 2$$

Der Wert der Oesterlé–Schranke für $N_9(1)$ beträgt 16, genau so wie die Serre–Schranke. Der Funktionenkörper ist optimal. Die 16 Primdivisoren vom Grad eins sind in der folgenden Liste enthalten.

$$\begin{array}{ll}
P_1 =< 1/x, y > & P_2 =< x, y+1 > \\
P_3 =< x, y+2 > & P_4 < x+\omega, y+\omega^2 > \\
P_5 =< x+\omega, y+\omega^6 > & P_6 =< x+\omega^2, y+1 > \\
P_7 =< x+\omega^2, y+2 > & P_8 =< x+\omega^3, y+\omega^2 > \\
P_9 < x+\omega^3, y\omega^6, 1] > & P_{10} =< x+2, y+\omega^2 > \\
P_{11} =< x+2, y+\omega^6 > & P_{12} =< x+\omega^5, y > \\
P_{13} =< x+\omega^6, y+1 > & P_{14} =< x+\omega^6, y+2 > \\
P_{15} =< x+\omega^7, y > & P_{16} =< x+1, y >
\end{array}$$

T= 0 ms

8.2.4 Stellen vom Grad eins in einem Funktionenkörper vom Geschlecht 3

In 8.2.1. wurde die Artin–Schreier–Erweiterung definiert durch $y^3 + y + x^6 + x^4 + x^2$ konstruiert. Die folgende Tabelle enthält Information über die Anzahl der Primdivisoren vom Grad eins. Die letzte Zeile enthält die Rechenzeiten für die Bestimmung der Primdivisoren vom Grad eins.

q =	3	9	27	81	243	729
Serre–Schranke	13	28	58	136	337	892
Oesterlé–Schranke	10	28	58	136	337	892
Ihara–Schranke	11	28	77	225	667	1995
$N_{F/\mathbb{F}_q}$	4	28	28	28	244	892
T=	10ms	10ms	10ms	10ms	30ms	70ms

8.2.5 Stellen vom Grad eins in Funktionenkörpern vom Geschlecht 4

Wir untersuchen einige Funktionenkörper aus der Klasse der Funktionenkörper $F/\mathbb{F}_q$ vom Geschlecht $g = 4$ über $\mathbb{F}_q$ der Charakteristik $\chi(\mathbb{F}_q) \neq 3$. Aus dieser Klasse untersuchen wir nicht-hyperelliptische Funktionenkörper. Die Funktionenkörper werden unter Verwendung der Normalgleichung $f(x, y) = y^3 + a(x)y + b(x) \in \mathbb{F}_q[x][y]$, d.h.:

$$y^3 + (\alpha_4 x^4 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0)y+$$

$$\beta_6 x^6 + \beta_5 x^5 + \beta_4 x^4 + \beta_3 x^3 + \beta_2 x^2 + \beta_1 x + \beta_0$$

definiert. Die Koeffizienten $a(x), b(x) \in \mathbb{F}_q[x]$ wurden durch ein Zufallsverfahren ermittelt. Anschließend wurde der Funktionenkörper erzeugt und es wurde überprüft, ob der erzeugte Funktionenkörper tatsächlich vom Geschlecht 4 über $\mathbb{F}_q$ war.

Die Tabelleneinträge gliedern sich in Zeilen des folgenden Inhalts:
Die erste Zeile enthält die Zahl q für $F/\mathbb{F}_q$.
Die zweite Zeile enthält den Koeffizient $a(x)$.
Die dritte Zeile enthält den Koeffizient $b(x)$.
Die vierte Zeile enthält die Diskriminante $D(x)$
Die fünfte Zeile enthält den Wert der Serre–Schranke.
Die sechste Zeile enthält den Wert der Oesterlé–Schranke. Die Oesterlé–Schranke wurde berechnet unter Berücksichtigung des Satzes von Fuhrmann und Torres.

Die siebte Zeile enthält den Wert der Ihara–Schranke. Wenn die Bedingung $4 > (q - \sqrt{q})/2$ nicht erfüllt ist, wurde dieser Wert nicht berechnet und die entsprechende Zeile ist nicht vorhanden.

Die achte Zeile enthält die Anzahl N_F der Stellen vom Grad Eins.

Die neunte Zeile enthält die Rechenzeit zur Ermittlung von $N_{F/\mathbb{F}_q}$ in Stunden.

Beispiele für q= 33554467 $q = 33554467$ ist die erste Primzahl, die größer als $2^{25} = 33554432$ ist. Der Wert der Ihara-Schranke für $N_33554467(4)$ ist 100 663 406 und ist nicht von Bedeutung.

$q = 33554467$	8.2.2.1.
$a(x) = x^4 + x^3 + x^2 + x$	
$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	
$D(x) = (x^3 + 33282346x^2 + 24715938x + 29249769) \cdot (x^9 + 26249775x^8 + 26195902x^7 + 24116111x^6 + 2399780x^5 + 25066306x^4 + 21096667x^3 + 25986416x^2 + 15686156x + 31364908)$	
Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 556 807
T: 1,45 h	

$q = 33554467$	8.2.2.2.
$a(x) = 0$	
$b(x) = x^6 + 1292070x^5 + 18711310x^4 + 18432739x^3 + 14315760x^2 + 18477431x + 20134528$	
$D(x) = (x + 1397342)^2(x + 15300519)^2(x + 19325562)^2 \cdot (x + 19660032)^2(x^2 + 12717549x + 796723)^2$	
Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 557 224
T: 1,12 h	

$q = 33554467$	8.2.2.3.
$a(x) = x^4 + 16138128x^3 + 3993324x^2 + 13893386x + 14611664$	
$b(x) = 33554466x^6 + 5845628x^5 + 3075458x^4 + 7964993x^3 +$ $24535299x^2 + 7797542x + 1687823$	
$D(x) = (x + 24346622)\cdot$ $(x^4 + 4176210x^3 + 16675382x^2 + 9074360x + 32855866)\cdot$ $(x^7 + 24908793x^6 + 963236x^5 + 15688741x^4 +$ $31329143x^3 + 17187855x^2 + 4636760x + 16399092)$ $4636760x + 16399092)$	

Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 557 449
T: 1,55 h	

$q = 33554467$	8.2.2.4.
$a(x) = x^4 + 26160794x^3 + 19492933x^2 + 8870081x + 1742865$ $b(x) = 33554466x^5 + 8287531x^4 + 3239123x^3 + 3599574x^2 +$ $28183624x + 14236150$	
$D(x) = (x + 9135113)(x + 12347687)(x + 31047334)\cdot$ $(x^9 + 25952248x^8 + 29751591x^7 + 5954051x^6 +$ $30180092x^5 + 9825062x^4 + 2257977x^3 +$ $29701278x^2 + 7122003x + 1410830)$	

Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 559 699
T: 1,45 h	

$q = 33554467$	8.2.2.5.
$a(x) = x^4 + 4870727x^3 + 15220770x^2 +$ $16867445x + 18950748$ $b(x) = 33554466x^6 + 24128110x^5 + 8860585x^4 +$ $16212979x^3 + 25450461x^2 + 11641003x$	
$D(x) = (x^2 + 2042897x + 11046527)\cdot$ $(x^{10} + 6521032x^9 + 4007832x^8 + 21949651x^7 +$ $26506876x^6 + 21178319x^5 + 12395560x^4 +$ $29867907x^3 + 27636436x^2 + 361604x + 19908565)$	

Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 561 509
T: 1,47 h	

$q = 33554467$	8.2.2.6.
$a(x) = x^4 + 32074157x^3 + 25445488x^2 + 20862568x + 11681747$	
$b(x) = x^6 + 2147784x^5 + 11974097x^4 + 31096792x^3 + 31298351x^2 + 20527247x + 3948781$	
$D(x) = (x + 18321109) \cdot (x^2 + 24770749x + 31475922) \cdot (x^3 + 18456041x^2 + 32262066x + 4549261) \cdot (x^6 + 29294954x^5 + 7652165x^4 + 5182492x^3 + 11687727x^2 + 20661288x + 23011941)$	

Serre-Schranke für $N_q(4) =$	33 600 808
Oesterlé-Schranke für $N_q(4) =$	33 566 053
$N_{F/\mathbb{F}_q}(4) =$	33 553 156
T: 1,55 h	

Symbolverzeichnis

(a)	Hauptdivisor von $a \in F^\times$	21
$(a)_0$	Nullstellendivisor des Hauptdivisors (a)	21
$(a)_\infty$	Polstellendivisor des Hauptdivisors (a)	21
$\mathcal{A}_F(A)$	Adele-Raum eines Divisors A	25
$\mathbf{A}^n(k)$	Der n-dimensional affine Raum über einem Körper k	7
$\chi(K)$	Charakteristik des Körpers K	2
$\mathcal{C}l(F/k)$	Divisorklassengruppe von F/k	21
$\mathcal{C}l^n(F/k)$	Menge der Divisorklassen vom Grad n von F/k	22
$Con_{F'/F}(P)$	Conorm von P bezüglich F'/F	17
$\deg P$	Grad von der Stelle P	16
$\deg D$	Grad vom Divisor D bzw. von der Klasse $[D]$	20,21
$\deg_y(f)$	Grad eines Polynoms $f(x,y)$ bezüglich y	5
$\dim D$	Dimension des Riemann-Roch-Raums $\mathcal{L}(D)$	23

$\mathbf{P}^n(k)$	Der n-dimensional projektive Raum über einem Körper k	8
q	Elementanzahl des endlichen Körpers $\mathbb{F}_q$	4
$\tilde{(\cdot)}$	Reduktion modulo P	47
$\mathbf{Spec}\, R$	Spektrum von dem Ring R	8
$\mathrm{supp}(D)$	Träger des Divisors D	20
$\mathbf{V}$	Affine Varietät über einem Körper	9
$\mathbf{V}(f_1, \dots, f_s)$	Affine Varietät definiert durch die Polynome $f_1, \dots, f_s$	9
$\mathbf{V}(k)$	Menge der k-rationalen Punkte einer Varietät $\mathbf{V}$ über k	9
$\mathbf{V}_{ng}$	Menge der Kurven vom Grad n und Geschlecht g	35
v	Diskrete Bewertung eines Körpers	14
v_P	Diskrete Bewertung eines Funktionenkörpers an der Stelle P	16
W	Kanonischer Divisor von F/k	26
x	Separierendes Element	5
$\zeta_{F/k}(t)$	Zeta-Funktion des Funktionenkörpers F/k	52

Literaturverzeichnis

[1] R. Auer. Private Mitteilung.

[2] R. Auer. *Ray Class Fields of Global Function Fields with Many Rational Places.* Dissertation, Carl-von-Ossietzky-Universität Oldenburg, 1999.

[3] R. Brüske, F. Ischebeck, F. Vogel. *Kommutative Algebra.* B. I.-Wissenschaftsverlag, Mannnheim, 1989.

[4] L. Caporaso, J. Harris. Counting plane curves of any genus, *Invent. math.* **131** (1998), 345–392.

[5] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable.* AMS Math. Surveys, New York, 1951.

[6] A. Clebsh, P. Gordan. *Theorie der abelschen Functionen.* B.G. Teubner, Leipzig, 1866.

[7] H. Cohen. *A course in Algebraic Number Theory.* 3rd corr. printing, GTM 138. Springer-Verlag, Berlin - Heidelberg - New York, 1996.

[8] P. M. Cohn. *Algebraic Numbers and Algebraic Functions.* Chapman & Hall, London, 1991.

[9] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms.* UTM. Springer-Verlag, Berlin - Heidelberg - New York, 1992.

[10] R. Dedekind, H. Weber. Theorie der algebraischen Functionen einer Veränderlichen, *J. reine angew. Math.* **92** (1882), 181–290.

[11] M. Deuring. Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers, *Math. Zeit.* **47** (1941), 643–654.

[12] M. Deuring. Zur Theorie der Moduln algebraischer Funktionenkörper, *Math. Zeit.* **47** (1941), 34–45.

[13] M. Deuring. *Lectures on the Theory of Algebraic Functions of One Variable.* LNM 314. Springer-Verlag, Berlin - Heidelberg - New York, 1973.

[14] V. Drinfeld, S.G. Vladut. The number of points of an algebraic curve, *Funct. Anal. and Appl.* **17** (1983), 53–54.

[15] M. Eichler. *Einführung in die Theorie der algebraischen Zahlen und Funktionen.* Birkhäuser Verlag, Basel, 1963.

[16] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* GTM 150. Springer-Verlag, Berlin - Heidelberg - New York, 1995.

[17] G. Faltings. Endlichkeitssätze für abelsche Varietäten über zahlkörper, *Invent. Math.* **73** (1983), 349–366.

[18] G.-L. Feng, T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. Inform. Theory* **39** (1993), 37–45.

[19] R. Fuhrmann, A. Garcia und F. Torres. On maximal curves, *J. Number Th.* **67** (1997), 29–51.

[20] R. Fuhrmann, F. Torres. The genus of curves over finite fields with many rational points, *Manuscr. Math.* **89** (1996), 103–106.

[21] W. Fulton. *Algebraic curves.* Benjamin, New York, 1969.

[22] A. Garcia, H. Stichtenoth. A class of polynomials over finite fields. Preprint 1998.

[23] A. Garcia, H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attainning the drinfeld-vladut bound, *Inv. Math.* **121** (1995), 211–222.

[24] A. Garcia, H. Stichtenoth und C.P. Xing. On subfields of the Hermitian function field. Preprint 1998.

[25] D. Goos. *Basic Structures of Function Field Arithmetic.* Springer-Verlag, Berlin - Heidelberg - New York, 1991.

[26] V. Goppa. *Geometry and Codes.* Kluwer Academic Publishers, Boston, 1988.

[27] G. Haché,D. Le Brigand. Effective construction of algebraic geometry codes, *IEEE Trans. Info. Th.* **41** (1995), 1615–1628.

[28] J. Hansen. Group codes and algebraic curves. *Mathematica Gottingensis, Schriftenreihe SFB Geometrie und Analysis, Heft 9* (1987).

[29] J. Hansen. Deligne-lusztig varieties and group codes. In *Proceedings from the Conference at Luminy*, Seiten 63–81, 1991.

[30] J. Harris, I. Morrison. *Moduli of curves.* GTM 187. Springer-Verlag, Berlin - Heidelberg - New York, 1998.

[31] R. Hartschorne. *Algebraic Geometry.* Springer-Verlag, Berlin - Heidelberg - New York, 1977.

[32] H. Hasse. *Zahlentheorie.* Akademie Verlag, Berlin, 1963.

[33] K. Hensel, G. Landsberg. *Theorie der algebraischen Funktionen einer Variabeln.* B.G. Teubner, Leipzig, 1902.

[34] F. Heß. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* Dissertation, Technische Universität Berlin, 1999.

[35] D. Husemöller. *Elliptic curves.* Springer-Verlag, Berlin - Heidelberg - New York, 1987.

[36] J. Igusa. Arithmetic Variety of Moduli for Genus Two, *Annals of Mathematics* **72** (1960), 612–649.

[37] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28** (1981), 721–724.

[38] D. Jungnickel, H. Niederreiter. *Finite fields: structute and arithmetics.* B. I.-Wissenschaftsverlag, Mannnheim, 1993.

[39] I. Kant. *Kritik der reinen Vernunft.* 1781.

[40] Kant-Gruppe. *KASH.* `http://www.math.tu-berlin.de/~kant`, 1999.

[41] O.-H. Keller. *Vorlesungen über algebraische Geometrie.* Akademische Verlagsgesellschaft, Leipzig, 1974.

[42] N. Koblitz. Hyperelliptic cryptosystems, *J. Cryptology* **1** (1989), 139–150.

[43] N. Koblitz. *Algebraic Aspects of Cryptography.* Springer-Verlag, Berlin - Heidelberg - New York, 1998.

[44] K. Lauter. Aus einem in Luminy gehaltenen Vortrag über die Anzahl von rationalen Punkten für Geschlecht 3.

[45] K. Lauter. Deligne-Lusztig curves as ray class fields. `http://www.mpim-bonn.mpg.de/html/preprints/`.

[46] K. Lauter. Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points . `http://www.mpim-bonn.mpg.de/html/preprints/`.

[47] K. Lauter. Ray class field constructions of curves over finite fields with many rational points. In H. Cohen, Hrsg., *Algorithmic Number Theory*, LNCS 1122, Seiten 187–195, Talence 1996, 1996. Springer-Verlag, Berlin - Heidelberg - New York.

[48] F. Leprevost. Famille de courbes des genre 2 munies d'une classe de diviseurs rationnels d'ordre 13., *C. R. Acad. Sci., Paris,Ser.I 313* **7** (1991), 451–454.

[49] F. Leprevost. Famille de courbes des genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 or 21., *C. R. Acad. Sci., Paris,Ser.I 313* **11** (1991), 771–774.

[50] Y. Manin. What is the Maximum Number of Points on a Curve over $\mathbb{F}_2$?, *J. Fac. Sci. Univ. Tokyo* **28** (1981), 715–720.

[51] A. Menezes. *Aplications of Finite Fields.* Kluwer Academic Publishers, Boston, 1993.

[52] A. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, Boston, 1993.

[53] J.-P. Mestre. Courbes de Weil et courbes supersingulieres. Semin. Theor. Nombres, Univ. Bordeaux I 1984-1985, Exp. No.23, 1985.

[54] K. Meyberg. *Algebra 1,2.* Carl Hanser Verlag, München, Wien, 1975.

[55] C. Moreno. *Algebraic curves over finite fields.* Cambridge University Press, Cambridge, 1991.

[56] D. Mumford. *Geometric invariant theory.* Springer-Verlag, Berlin - Heidelberg - New York, 1982.

[57] H. Niederreiter, C.P. Xing. Cyclotomic function fields, Hilbert class fields and global function fields with many rational places, *Acta Arith.* **79** (1997), 59–76.

[58] H. Niederreiter, C.P. Xing. Drinfeld modules of rank 1 and algebraic curves with many rational points, *Acta Arith.* **81** (1997), 81–100.

[59] F. Özbudak, H Stichtenoth. Curves with many points and configurations of hyperplanes over finite fields. Preprint 1998.

[60] M. E. Pohst. *Computational algebraic number theory.* DMV-Seminar 21. Birkhaeuser, Basel-Boston-Berlin, 1993.

[61] M. E. Pohst und H. Zassenhaus. *Algorithmic Algebraic Number Theory.* Cambridge University Press, Cambridge, 1st paperback Auflage, 1997.

[62] B. Poonen. Computational aspects of curves of genus at least 2. In H. Cohen, Hrsg., *Proceedings of the Second Symposium on Algorithmic Number Theory, ANTS-II*, LNCS 1122, Seiten 283–306, Talence, France, 1996. Springer-Verlag, Berlin - Heidelberg - New York.

[63] M. Reid. *Undergraduate Algebraic Geometry.* London Mathematical Society Student Texts,12. Cambridge University Press, Cambridge, 1988.

[64] B. Riemann. Theorie der Abelschen Funktionen, *J. reine angew. Math.* **54** (1857), –.

[65] H.-G. Rück, H. Stichtenoth. A characterization of Hermitian function fields over finite fields, *J. reine angew. Math.* **457** (1994), 185–188.

[66] I. R. Schafarewitsch. *Basic Algebraic Geometry.* Springer-Verlag, Berlin - Heidelberg - New York, 1977.

[67] R. Schoof. Algebraic curves and coding theory. UTM 336, Univ. of Trento, 1990.

[68] M. Schörnig. *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern.* Dissertation, Technische Universität Berlin, 1996.

[69] J.-P. Serre. *Nombre de points des courbes algébriques sur* $\mathbb{F}_q$, Band 22. Séminaire de Théorie des Nombres de Bordeaux, 1982/83.

[70] J.-P. Serre. Sur le nombre de points rationnels d'une courbe algebrique sur une corp fini., *C.R. Acad. Sci. Paris* **296** (1983), 397–402.

[71] J.-P. Serre. *Rational points on curves over finite fields. Notes of Lectures.* Harvard University, 1985.

[72] V. Shabat. Unpublisched manuscript. University of Amsterdam, 1997/98.

[73] M. Shokrollahi, H. Wasserman. Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. Inform. Theory* **39** (1993), 37–45.

[74] J. Silverman. *The Arithmetic of Elliptic Curves.* GTM. Springer-Verlag, Berlin - Heidelberg - New York, 1986.

[75] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* GTM. Springer-Verlag, Berlin - Heidelberg - New York, 1994.

[76] J. Silverman, J. Tate. *Rational points on Elliptic Curves.* UTM. Springer-Verlag, Berlin - Heidelberg - New York, 1986.

[77] A. Stein. *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern.* Dissertation, Universität des Saarlandes, 1996.

[78] H. Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik Teil I, *Arch. Math.* **24** (1973), 527–544.

[79] H. Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik Teil II, *Arch. Math.* **24** (1973), 615–631.

[80] H. Stichtenoth. Algebraic-geometric codes associated to Artin-Schreier extensions of $\mathbb{F}_q(z)$. In *Proc. 2nd Int. Workshop on Alg. and Comb. Coding Theory*, Seiten 203–206, Leningrad, 1990.

[81] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin - Heidelberg - New York, 1993.

[82] M. Thomas. *Türme und Pyramiden algebraischer Funktionenkörper.* Dissertation, Universität GH Essen., 1997.

[83] M. Tsfasman, S.G.Vladut. *Algebraic-Geometric Codes.* Kluwer Academic Publishers, Boston, 1971.

[84] M. Tsfasman, S.G.Vladut und T. Zink. On Goppa codes which are better than the Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.

[85] G. van der Geer, J.H. van Lint. Introduction to coding theory and algebraic geometry. DMV Seminar 12, Birkhäuser, 1988.

[86] G. van der Geer, M. van der Vlugt. Constructing curves over finite fields with many points by solving linear equations. Report W 97-29, Leiden University 1997.

[87] G. van der Geer, M. van der Vlugt. Tables of curves with many points. regelmäßig aktualisierte Tabelle unter `http://www.wins.uva.nl/~geer`.

[88] G. van der Geer, M. van der Vlugt. Curves over finite fields of characteristic 2 with many rational points, *C.R. Acad. Sci. Paris* **317** (1993), 593–597.

[89] G. van der Geer, M. van der Vlugt. Quadratic forms, generalized hamming weights of codes and curves with many points, *J. Number Th.* **59** (1996), 20–36.

[90] G. van der Geer, M. van der Vlugt. How to construct curves over finite fields with many points. In F. Catanese, Hrsg., *Arithmetic geometry (Cortona 1994)*, Seiten 169–189, Cambridge, 1997. Cambridge University Press.

[91] B. van der Waerden. *Einführung in die algebraische Geometrie.* Springer-Verlag, Berlin - Heidelberg - New York, 1939.

[92] B. van der Waerden. *Algebra I,II.* Springer-Verlag, Berlin - Heidelberg - New York, 1971.

[93] J. van Lint. *Introduction to Coding Theory.* Springer-Verlag, Berlin - Heidelberg - New York, 1982.

[94] R. Walker. *Algebraic Curves.* Dover, New York, 1950.

[95] A. Weil. Zur algebraischen Theorie der algebraischen Funktionen, *J. reine angew. Math.* **179** (1938), 129–133.

[96] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann, Paris, 1948.

[97] A. Wiles. Modular elliptic curves and Fermat's Last Theorem, *Ann. Math, II. Ser. 141* **3** (1995), 443–551.

[98] M. Wirtz. *Konstruktion und Tabellen linearer Codes.* Dissertation, Westfälische Wilhelms-Universität Münster, 1991.

[99] O. Zariski, P. Samuel. *Commutative Algebra I.* Van Nostrand, Princeton, New Jersey, 1958.

Hiermit erkläre ich, daß ich die vorliegende Arbeit
selbständig verfaßt und keine anderen als die
angegebenen Quellen und Hilfsmittel verwendet habe.
Berlin, den 28.11.1999

Ich möchte an dieser Stelle Herrn Prof. Dr. M. Pohst ganz herzlich
für die Überlassung des Themas dieser Arbeit sowie für seine
Unterstützung und Hinweise danken.
Mein besonderer Dank gilt meiner Mutter. Ihr ist diese Arbeit dankend
gewidmet.