Zur Divisorenklassengruppen-berechnung in globalen Funktionenkörpern

vorgelegt von
Diplom-Mathematiker
Florian Heß
aus Berlin

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation

Berlin 1999
D83

Promotionsausschuß:

Vorsitzender: Prof. Dr. A. Bobenko
Berichter: Prof. Dr. M. E. Pohst
Berichter: Prof. Dr. F. Grunewald

Tag der wissenschaftlichen Aussprache: 30. August 1999

Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern

vorgelegt von
Diplom-Mathematiker

Florian Heß

aus Berlin

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation

Promotionsausschuß:

Vorsitzender: Prof. Dr. A. Bobenko
Berichter: Prof. Dr. M. E. Pohst
Berichter: Prof. Dr. F. Grunewald

Tag der wissenschaftlichen Aussprache: 30. August 1999

Berlin 1999
D83

Inhaltsverzeichnis

Einleitung

Ein globaler Funktionenkörper F/k über dem endlichen Konstantenkörper k ist eine endliche Erweiterung des rationalen Funktionenkörpers $k(x)$. Neben dem Geschlecht zählt die Divisorenklassengruppe und speziell die von den Divisorenklassen vom Grad null erzeugte, endliche Klassengruppe zu den wichtigsten Invarianten von F/k.

In der Kryptographie werden endliche, abelsche Gruppen G verwendet, in denen das Gruppengesetz $a + b$ für $a, b \in G$ effizient, der diskrete Logarithmus $x \in \mathbb{Z}$ mit $ax = b$ aber nur sehr zeitaufwendig berechnet werden kann. Geeignete Gruppen G erhält man unter anderem mit der Punktgruppe elliptischer Kurven [31] und allgemeiner mit der Gruppe der k-rationalen Punkte der Jacobischen Varietät geeigneter hyperelliptischer Kurven über endlichen Körpern k [26]. Diese Gruppen sind isomorph zur Klassengruppe der entsprechenden elliptischen beziehungsweise hyperelliptischen globalen Funktionenkörper.

In der Codierungstheorie betrachtet man algebraisch-geometrische Codes, welche beispielsweise durch die Funktionswerte gewisser algebraischer Funktionen eines globalen Funktionenkörpers an Stellen vom Grad eins gegeben werden [55]. Ein solcher Code besitzt „gute“ Parameter, wenn die nach oben beschränkte Anzahl der Stellen vom Grad eins im Verhältnis zum Geschlecht groß ist. Funktionenkörpern mit vielen Stellen vom Grad eins erhält man bei beschränktem Geschlecht häufig durch die Betrachtung abelscher Erweiterungen [19]. Gemäß der Klassenkörpertheorie globaler Funktionenkörper stellt die Klassengruppe einen wichtigen Teil derjenigen Daten von F/k dar, mit Hilfe derer die abelschen Erweiterungen von F parametrisiert werden können. Dieser Ansatz wird in [3] verfolgt.

Unter Verwendung von globalen Funktionenkörpern mit vielen Stellen vom Grad eins lassen sich ferner Gitterkugelpackungen mit zumindest asymptotisch guter Dichte bei wachsendem Geschlecht und wachsender Dimension konstruieren [44]. Für eine Menge S von Stellen vom Grad eins werden hier S-Einheitengitter verwendet. Diese Gitter korrespondieren zu Untergruppen der Klassengruppe.

Bei der Berechnung der Klassenzahl, der Klassengruppe oder des L-Polynoms

eines globalen Funktionenkörpers lassen sich zwei grundsätzlich verschiedene Situationen unterscheiden: Die Betrachtung von Funktionenkörpern F/k des Geschlechts g über dem Konstantenkörper k mit q Elementen mit

(i) $q \to \infty$ und g fest, oder

(ii) q fest und $g \to \infty$.

In der Kryptographie betrachtet man meistens die Situation (i). Die Struktur der Punktgruppe elliptischer Kurven kann in polynomialer Laufzeit in $\log(q)$ berechnet werden [31, 49]. Durch die Verallgemeinerung dieser Methode wurde in [24] ein probabilistisches Verfahren für die Berechnung des L-Polynoms eines globalen Funktionenkörpers F/k mit in $\log(q)$ polynomialer, in g aber exponentieller Laufzeit erhalten.

Für die Situation (ii) gibt es in g subexponentielle, in $\log(q)$ aber exponentielle probabilistische Verfahren zur Bestimmung der Struktur der Klassengruppe für hyperelliptische Funktionenkörper [1] und für speziell reell-quadratische Funktionenkörper [53]. Wie in [39] bemerkt, scheint die Berechnung des L-Polynoms in Situation (ii) schwieriger zu sein.

Wir entwickeln in dieser Arbeit einen probabilistischen Algorithmus zur Berechnung der Klassengruppe beziehungsweise Divisorenklassengruppe eines globalen Funktionenkörpers F/k für die Situation (ii), dessen Laufzeit unter einer gewissen Annahme in g subexponentiell und in $\log(q)$ exponentiell ist, und verallgemeinern damit Methoden aus [50] und [53]. Wir gehen hierbei von einer Darstellung des Funktionenkörpers durch

$$F = k(x, \rho) \text{ mit } f(x, \rho) = 0$$

für ein in y normiertes und separables, irreduzibles Polynom $f(x, y) \in k[x, y]$ aus. Dieser Algorithmus wurde von uns im Computeralgebrasystem KASH, [25], implementiert und auf seine Anwendbarkeit überprüft. Damit ist es erstmals möglich, die Klassengruppe beziehungsweise Divisorenklassengruppe globaler Funktionenkörper mit $\deg_y\big(f(x, y)\big) \geq 3$ zu berechnen.

Unser Algorithmus basiert auf der Relationenmethode, die zuvor bereits in Einheiten- und Klassengruppenberechnungen verwendet wurde [7, 23, 50, 53]. Jede endliche, abelsche Gruppe kann als Faktorgruppe einer endlich erzeugten, freien abelschen Gruppe nach einer von den sogenannten Relationen erzeugten Untergruppe dargestellt werden. Die Idee für die Klassengruppenberechnung ist, als freie Erzeuger geeignet gewählte Divisoren vom Grad null zu verwenden und dann die durch diese Divisoren darstellbaren Hauptdivisoren, die Relationen, zu bestimmen.

Die Träger der die Klassengruppe erzeugenden Divisoren bilden die aus Stellen von F/k bestehende Faktorbasis S. Unter Verbesserung einer ähnlichen Schranke aus [53] weisen wir nach, daß es für $g > 0$ beispielsweise genügt, wenn die Faktorbasis die Stellen von F/k eines Grads kleiner gleich

$$\max\{\, \lceil 2\log_q(4g-2)\rceil,\ \lceil 2\log_q(2g)\rceil + 1 \,\}$$

enthält. Für die Relationensuche sind dann alle Hauptdivisoren mit Träger in S zu finden. Dazu entwickeln und verwenden wir Methoden für die Reduktion und für die Berechnung der Riemann-Roch-Räume von Divisoren. Mit Hilfe einer Approximation der Klassenzahl, die aus den Anzahlen der Stellen eines ähnlich wie zuvor beschränkten Grads berechnet wird, können wir schließlich testen, ob die volle Gruppe der Hauptdivisoren gefunden wurde.

Die Arbeit gliedert sich wie folgt:

Im ersten Kapitel stellen wir die theoretischen und algorithmischen Grundlagen für algebraische und speziell globale Funktionenkörper zusammen.

Im zweiten Kapitel geben wir eine konstruktive Fassung der Riemann-Roch-Theorie und beschreiben Algorithmen zur Bestimmung des Geschlechts, zur Reduktion von Divisoren und der Berechnung ihrer Riemann-Roch-Räume für allgemeine algebraische Funktionenkörper. Wir erweitern diese Methoden, so daß auch diskrete Bewertungen des Konstantenkörpers berücksichtigt werden können.

Im dritten Kapitel stellen wir die Grundlagen für L-Reihen globaler Funktionenkörper für Charaktere endlicher Ordnung der Divisorenklassengruppe zusammen und beweisen die benötigten Schranken für die Erzeugung der Klassengruppe und die Approximation der Klassenzahl mit Hilfe des Satzes von Hasse-Weil. Wir formulieren weiter eine Version des Satzes von Brauer-Siegel für globale Funktionenkörper und gehen auf Strukturaussagen über die Klassengruppe und die Beziehung der p-Torsion zu einem Differentialraum ein.

Im vierten Kapitel betrachten wir Glattheitseigenschaften, mit denen Ergebnisse über die Erfolgswahrscheinlichkeit der Relationensuche erhalten werden können. Die eigentlich benötigte, aufgrund der vorangegangenen Überlegungen plausible und heuristische unterstütze Aussage formulieren wir als Glattheitsannahme.

Im fünften Kapitel kommen wir zur Beschreibung des Klassengruppenverfahrens. Nach Erläuterung der allgemeinen Strategie beschreiben wir deterministische, in g exponentielle Techniken und eine probabilistische, unter der Glattheitsannahme in g subexponentielle Technik zur Relationensuche. Auf letzterer baut der in der Praxis eingesetzte Algorithmus auf, der anschließend formuliert wird.

Im sechsten Kapitel erwähnen wir Anwendungen des Klassengruppenverfahrens zur Bestimmung von Einheiten- und Idealklassengruppen und zur Berechnung des diskreten Logarithmus.

Im siebten Kapitel führen wir einige illustrative Beispiele an, die das Laufzeitverhalten und die Anwendbarkeit des Verfahrens unter Variation der wesentlichen Parameter q und g demonstrieren.

Ich möchte an dieser Stelle Herrn Prof. Dr. M. E. Pohst ganz herzlich für seine Hinweise, Unterstützung und die gute Zusammenarbeit während der Anfertigung dieser Arbeit danken.

Ferner danke ich Herrn Prof. Dr. F. Grunewald für die Übernahme des Koreferats, allen Mitgliedern der Kant-Gruppe, Dr. C. Fieker für die Durchsicht einer vorläufigen Fassung der Arbeit und Dr. R. Auer für einige Hinweise zur Verbesserung von KASH.

Darüber hinaus bedanke ich mich für die Förderung durch ein NaFöG-Stipendium bei den dafür zuständigen Personen.

Kapitel 1

Grundlagen

In diesem Kapitel werden die dieser Arbeit zugrundeliegenden Definitionen und theoretischen sowie algorithmischen Aussagen für algebraische Funktionenkörper bereitgestellt und Notationen vereinbart. Für die Theorie der algebraischen Funktionenkörper verweisen wir auf [11, 12, 13, 55], für algorithmische Aspekte auf [9, 36, 37, 50, 53].

1.1 Notation und Grundlagen

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 k_0 von k in F hat endlichen Grad über k und wird der exakte Konstantenkörper von F/k genannt. Ein globaler Funktionenkörper F/k liegt vor, wenn k ein endlicher Körper $\mathbb{F}_q$ ist.

Unter einer Stelle P von F/k verstehen wir das eindeutig bestimmte, maximale Ideal eines (diskreten) Bewertungsrings von F/k. Der zugehörige Bewertungsring werde mit $\mathfrak{o}_P$, die zugehörige exponentielle, surjektive Bewertung $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit v_P bezeichnet. Für jedes Element von k_0 liefert v_P den Wert null. Der Restklassenkörper von P ist der Körper $\mathfrak{o}_P/P$. Der Grad von P ist der Grad der (stets endlichen) Körpererweiterung von $\mathfrak{o}_P/P$ über k_0. Wir schreiben $\mathcal{P}l(F/k)$ für die Menge aller Stellen von F/k , $\mathcal{P}l^n(F/k)$ für die Menge der Stellen vom Grad n und $\mathcal{P}l^{\leq n}(F/k)$ für die Menge der Stellen vom Grad kleiner gleich n. Mittels des Grads von Stellen erhalten wir eine Abbildung $\deg : \mathcal{P}l(F/k) \longrightarrow \mathbb{Z}$. Gehen wir in diesen Definitionen vom Körper k zu einem Teilkörper $\tilde{k}$ von k_0 mit endlichem Index $[k_0 : \tilde{k}]$ über, so ändern sich Stellen, Bewertungen und Restklassenkörper nicht. Wir definieren den Grad über $\tilde{k}$ als $\deg_{\tilde{k}}(P) = [k_0 : \tilde{k}] \deg(P)$.

Die Gruppe $\mathcal{D}(F/k)$ der Divisoren von F/k wird als die von den Elementen aus $\mathcal{P}l(F/k)$ erzeugte, freie abelsche Gruppe definiert. Wir schreiben das Gruppengesetz additiv. Die Elemente von $\mathcal{D}(F/k)$ sind die Divisoren von F/k. Ein Divisor D ist also eine formale Summe $\sum_{P\in\mathcal{P}l(F/k)} n_P P$, in der fast alle n_p null sind. Der Exponent $v_P(D)$ einer Stelle P in D ist der Wert n_p, der Träger $\mathrm{supp}(D)$ eines Divisors D ist die Menge der Stellen P mit $v_P(D)\neq 0$. Einen durch eine einzige Stelle mit Exponent eins gegebenen Divisor nennen wir Primdivisor. Für Divisoren D_1, D_2 definieren wir $D_1 \leq D_2$, wenn $\leq$ exponentenweise gilt. Ein Divisor $D \geq 0$ heißt positiv.
Jeder Divisor läßt sich eindeutig als Differenz $D = (D)_0 - (D)_\infty$ positiver Divisoren schreiben, wobei $(D)_0$ Nullstellendivisor und $(D)_\infty$ Polstellendivisor von D genannt wird. Für eine Menge M von Divisoren oder Stellen von F/k bezeichnen wir mit $\langle M\rangle$ die von M erzeugte Untergruppe von $\mathcal{D}(F/k)$. Die Gradfunktion deg $(\deg_{\tilde{k}})$ wird additiv auf $\mathcal{D}(F/k)$ fortgesetzt, analog sprechen wir vom Grad eines Divisors. Die Menge der Divisoren vom Grad n bezeichnen wir mit $\mathcal{D}^n(F/k)$.
Schließlich definiert die Zuordnung $a \mapsto (a) := \sum_{P\in\mathcal{P}l(F/k)} v_P(a)P$ einen Homomorphismus $(\cdot) : F^\times \longrightarrow \mathcal{D}^0(F/k)$, dessen Bild aus den sogenannten Hauptdivisoren besteht und mit $\mathcal{P}(F/k)$ bezeichnet wird. Der Kern von $(\cdot)$ stimmt mit dem exakten Konstantenkörper k_0 von F/k überein. Den Nullstellen- beziehungsweise Polstellendivisor eines Hauptdivisors notieren wir in der Form $(a)_0$ beziehungsweise $(a)_\infty$.

Es sei D ein Divisor von F/k. Der Riemann-Roch-Raum $\mathcal{L}(D)$ von D wird definiert als

$$\mathcal{L}(D) := \{a \in F^\times \mid (a) \geq -D\} \cup \{0\}.$$

Hierbei handelt es sich um einen endlich-dimensionalen k-Vektorraum, dessen Dimension mit $\dim(D)$ notiert wird. Zur Angabe des Konstantenkörpers, über dem die Dimension gemessen wird, schreiben wir wie beim Grad gelegentlich $\dim_{\tilde{k}}(D)$. Für weitergehende Aussagen, insbesondere den Satz von Riemann-Roch und die Definition des Geschlechts g, sei auf [55] und Kapitel 2 verwiesen.

Die Menge aller Differentiale von F/k wird mit $\Omega(F/k)$ bezeichnet. Hierbei handelt es sich um einen eindimensionalen F-Vektorraum. Wie üblich verwenden wir die Abbildungen $d : F \longrightarrow \Omega(F/k)$ und $(\cdot) : \Omega(F/k) \longrightarrow \mathcal{D}(F/k)$. Es sei D ein Divisor von F/k. Wir bezeichnen den Differentialraum von D mit

$$\Omega(D) := \{\omega \in \Omega(F/k) \mid (\omega) \geq D\}.$$

Dies ist nur noch ein k-Vektorraum. Entsprechend der Exponenten $v_P\big((\omega)\big)$ heißen die in (ω) vorkommenden Stellen P Null- beziehungsweise Polstellen von ω

mit den Ordnungen $v_P\big((\omega)\big)$. Für diese und weitere Aussagen über Differentiale siehe [11, 13, 33, 55].

Die Divisorenklassengruppe $\mathcal{C}l(F/k)$ wird definiert als $\mathcal{D}(F/k)\,/\,\mathcal{P}(F/k)$, die Faktorgruppe der Gruppe aller Divisoren nach der Gruppe der Hauptdivisoren. Ihre Elemente heißen Divisorenklassen, das Bild eines Divisors D unter dem kanonischen Homomorphismus $[\cdot] : \mathcal{D}(F/k) \longrightarrow \mathcal{C}l(F/k)$ schreiben wir als $[D]$. Die Funktionen $\deg : \mathcal{D}(F/k) \longrightarrow \mathbb{Z}$ und $\dim : \mathcal{D}(F/k) \longrightarrow \mathbb{Z}$ faktorisieren durch $[\cdot]$, lassen sich also (vertreterweise) auch auf $\mathcal{C}l(F/k)$ definieren. Wir sprechen analog vom Grad beziehungsweise der Dimension einer Divisorenklasse über k. Die Divisorenklassen vom Grad n werden mit $\mathcal{C}l^n(F/k)$ bezeichnet. Speziell die Divisorenklassen vom Grad null bilden eine Untergruppe $\mathcal{C}l^0(F/k) = \mathcal{D}^0(F/k)\,/\,\mathcal{P}(F/k)$ von $\mathcal{C}l(F/k)$, die wir als Klassengruppe von F/k bezeichnen. Ihre Ordnung, eventuell unendlich, wird die Klassenzahl $h(F/k)$ von F/k genannt.

1.1. Proposition. *(i) Für die Divisorenklassengruppe gilt:*

$$\mathcal{C}l(F/k) \;\cong\; \mathcal{C}l^0(F/k) \oplus \mathbb{Z}.$$

(ii) Die Klassenzahl eines globalen Funktionenkörpers ist endlich.

Beweis. Der erste Teil folgt aus $\mathcal{C}l(F/k) \;\cong\; \mathcal{C}l^0(F/k) \dot{+} \langle\, [D]\,\rangle$, wobei D einen Divisor von F/k kleinsten, positiven Grads bezeichnet. Für die zweite Aussage siehe [55, S. 159]. □

Für einen globalen Funktionenkörper gibt es immer einen Divisor vom Grad eins, [48], [55, S. 164], der für diese Isomorphie herangezogen werden kann.

Es sei S eine Menge von Stellen von F/k. Ein Divisor, dessen Träger nur aus Stellen aus S besteht, wird S-glatt genannt. Die Gruppe der S-glatten Divisoren wird in Ergänzung zur bisherigen Notation mit $\mathcal{D}(S)$ bezeichnet. Analog setzen wir $\mathcal{D}^m(S) := \mathcal{D}^m(F/k) \cap \mathcal{D}(S)$ und $\mathcal{P}(S) := \mathcal{P}(F/k) \cap \mathcal{D}(S)$. Die Elemente von $F^\times$, deren Hauptdivisoren in $\mathcal{P}(S)$ liegen, werden S-Einheiten von F/k genannt. Die S-Einheiten und die S-glatten Hauptdivisoren bilden jeweils eine Untergruppe von $F^\times$ beziehungsweise $\mathcal{D}^0(S)$.

Für eine nicht-leere Stellenmenge S werde mit $\mathfrak{o}_S$ der Ring der an allen Stellen aus S ganzen Elemente von F/k bezeichnet, also der Ring derjenigen Elemente $a \in F$, für die $v_P(a) \geq 0$ für alle $P \in S$ gilt. Komplementär wird $\mathfrak{o}^S$ als der Ring der an allen Stellen außerhalb von S ganzen Elemente definiert. Es folgt aus [11, S. 58ff., S. 64], daß beide Ringe Dedekindringe sind. Ihre Idealgruppen werden mit $\mathfrak{I}_S$ beziehungsweise $\mathfrak{I}^S$ bezeichnet. Für $\mathfrak{o}^S$ gilt weiter, daß die Primideale aus $\mathfrak{I}^S$ eineindeutig und bewertungserhaltend mit den nicht in S befindlichen Stellen

korrespondieren, daß die Einheitengruppe $(\mathfrak{o}^S)^\times$ genau von den S-Einheiten von F/k gebildet wird und daß der Quotientenkörper von $\mathfrak{o}^S$ mit F übereinstimmt. Wir bezeichnen die Idealklassengruppe von $\mathfrak{o}^S$ mit $\mathcal{C}l(\mathfrak{o}^S)$ und ihre Ordnung, eventuell unendlich, mit $h(S)$. Die Idealklassengruppe ist eine Faktorgruppe der Divisorenklassengruppe: $\mathcal{C}l(\mathfrak{o}^S) \cong \mathcal{D}(F/k) \,/\, \big(\mathcal{D}(S) + \mathcal{P}(F/k)\big)$.

Zur Verknüpfung aller dieser Strukturen betrachten wir

1.2. Proposition. *Es sei $\phi : G \longrightarrow H$ ein Homomorphismus abelscher Gruppen und U eine Untergruppe von G. Man hat die kanonische exakte Sequenz*

$$0 \longrightarrow \ker\phi \cap U \longrightarrow \ker\phi \longrightarrow G/U \longrightarrow \phi(G)/\phi(U) \longrightarrow 0.$$

Beweis. Die durch ϕ induzierte Abbildung $G/U \longrightarrow \phi(G)/\phi(U)$ ist surjektiv, so daß die Exaktheit bei $\phi(G)/\phi(U)$ folgt. Ist $a \in G$ mit $\phi(a) \in \phi(U)$, so gibt es ein $u \in U$, so daß $a - u \in \ker\phi$ ist. Der Kern von $G/U \longrightarrow \phi(G)/\phi(U)$ besteht daher aus $\big(\ker\phi + U\big)/U \cong \ker\phi/\big(\ker\phi \cap U\big)$, so daß sich die Exaktheit an den anderen drei Stellen ergibt. □

Hieraus resultieren zwei Folgerungen:

1.3. Korollar. *Man hat eine kanonische exakte Sequenz*

$$\begin{aligned} 0 \longrightarrow \mathcal{D}^0(S) \,/\, \mathcal{P}(S) \longrightarrow \mathcal{C}l^0(F/k) \longrightarrow \mathcal{C}l(\mathfrak{o}^S) \\ \longrightarrow \deg\big(\mathcal{D}(F/k)\big) \,/\, \deg\big(\mathcal{D}(S)\big) \longrightarrow 0. \end{aligned}$$

Beweis. Hierfür wird $G := \mathcal{C}l(F/k)$, $H := \mathbb{Z}$, $\phi := \deg$ und $U := \big(\mathcal{D}(S) + \mathcal{P}(F/k)\big)/\mathcal{P}(F/k)$ gesetzt. Dann gilt $\ker\phi = \mathcal{C}l^0(F/k)$, $\ker\phi \cap U = \big(\mathcal{D}^0(S) + \mathcal{P}(F/k)\big)/\mathcal{P}(F/k) \cong \mathcal{D}^0(S) \,/\, \mathcal{P}(S)$, $G/U \cong \mathcal{D}(F/k) \,/\, \big(\mathcal{D}(S) + \mathcal{P}(F/k)\big) \cong \mathcal{C}l(\mathfrak{o}^S)$ und $\phi(G)/\phi(U) = \deg\big(\mathcal{D}(F/k)\big) \,/\, \deg\big(\mathcal{D}(S)\big)$. □

Aufgrund dieses Korollars definieren wir den *S-Regulator* durch

$$R(S) := \big(\mathcal{D}^0(S) : \mathcal{P}(S)\big).$$

Damit gilt dann die Formel

$$R(S)\, h(S) = \deg\big(\mathcal{D}(S)\big)\, h(F/k),$$

sofern außer $\deg\big(\mathcal{D}(S)\big)$ mindestens zwei der beteiligten Werte endlich sind, vgl. auch [3, S. 14], [43].

1.4. Korollar. *Es sei A ein S-glatter Divisor mit $\deg(A) > 0$. Dann hat man die kanonische exakte Sequenz*

$$0 \longrightarrow \mathcal{D}^0(S)/\mathcal{P}(S) \longrightarrow \mathcal{D}\,(S)/\,\big(\langle A\rangle + \mathcal{P}(S)\big) \longrightarrow \deg\big(\mathcal{D}(S)\big) \,/\, \deg(A)\mathbb{Z} \longrightarrow 0.$$

Beweis. Hierfür wird $G := \mathcal{D}(S)/\mathcal{P}(S)$, $H := \mathbb{Z}$, $\phi := \deg$ und $U := \big(\langle A\rangle + \mathcal{P}(S)\big) / \mathcal{P}(S)$ gesetzt. Dann gilt $\ker\phi = \mathcal{D}^0(S)/\mathcal{P}(S)$, $\ker\phi \cap U \cong \{0\}$, $G/U \cong \mathcal{D}(S)/\big(\langle A\rangle + \mathcal{P}(S)\big)$ und $\phi(G)/\phi(U) = \deg\big(\mathcal{D}(S)\big) / \deg(A)\mathbb{Z}$. □

Die Gradbewertung v_∞ zur „unendlichen" Stelle ∞ eines rationalen Funktionenkörpers $k(x)$ ist durch $v_\infty(f/g) := \deg(g) - \deg(f)$, $f, g \in k[x]$ definiert. Wir verwenden $\deg := -v_\infty$ dann auch für Elemente aus $k(x)$. Die Elemente nicht positiven Grads von $k(x)$ bilden den diskreten Bewertungsring $\mathfrak{o}_\infty$.

Für eine unitäre Ringerweiterung kommutativer Ringe $A \subseteq B$ definieren wir $\mathrm{Cl}(A, B)$ als den Ring der über A ganzalgebraischen Elemente von B.

1.2 Darstellung von Funktionenkörpern und Algorithmen

In diesem Abschnitt soll kurz auf die Darstellung von Funktionenkörpern und auf grundlegende Algorithmen Bezug genommen werden, die wir in dieser Arbeit benötigen werden.

Einen algebraischen Funktionenkörper F/k realisieren wir als den Quotientenkörper der „endlichen Gleichungsordnung" $k[x,y] \,/\, f(x,y)k[x,y]$, wobei $f(x,y) = y^n + a_1 y^{n-1} + \cdots + a_n \in k[x][y]$ ein irreduzibles Polynom ist, welches normiert und separabel in y ist. Eine solche Darstellung existiert für jeden algebraischen Funktionenkörper (einer Variablen) über einem vollkommenen Konstantenkörper k, [50, S. 2], [55, S. 128]. Das Element x wird dann ein separierendes Element von F/k genannt. Anders ausgedrückt gilt $F = k(x,\rho)$ mit $f(x,\rho) = 0$. Um Komplexitätsaussagen treffen zu können, definieren wir $C_f := \max\{\lceil \deg(a_i)/i \rceil \mid 1 \le i \le n\}$. Damit gilt $\deg \mathrm{disc}_y f(x,y) \le C_f n(n-1)$ (man sieht dies mit dem Differenzenprodukt unter Beachtung der Tatsache, daß ρ/x^{C_f} ganzalgebraisch über $\mathfrak{o}_\infty$ ist).

Für diese Darstellung betrachten wir insbesondere die ganzalgebraischen Abschlüsse $\mathrm{Cl}\big(k[x], F\big)$ und $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$. Wird S als die Menge der „unendlichen Stellen" von $F/k(x)$ gewählt, also die Menge der Stellen von F/k über der unendlichen Stelle ∞ von $k(x)$, so gilt $\mathfrak{o}^S = \mathrm{Cl}\big(k[x], F\big)$ und $\mathfrak{o}_S = \mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$. Außerdem hat man $S = \mathrm{supp}\big((x)_\infty\big)$. Weil $k[x]$ und $\mathfrak{o}_\infty$ Hauptidealringe sind, besitzen $\mathrm{Cl}\big(k[x], F\big)$ und $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ Ganzheitsbasen bestehend aus $[F : k(x)]$ Elementen, entsprechendes gilt für ihre Ideale. Solche Basen sind modulo unimodularer Transformationen über $k[x]$ oder $\mathfrak{o}_\infty$ eindeutig bestimmt. Die Norm $\mathrm{N}_{F/k(x)}(\mathfrak{a})$ eines (gebrochenen) Ideals $\mathfrak{a}$ von $\mathrm{Cl}\big(k[x], F\big)$ oder $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ wird als Determinante einer Übergangsmatrix einer Ganzheitsbasis zu einer Idealbasis von $\mathfrak{a}$ (modulo Einheiten von $k[x]$ oder $\mathfrak{o}_\infty$) definiert und ist multiplikativ.

In Algorithmen gehen wir davon aus, daß der Körper k berechenbar ist, daß also die Null und die Eins zu Verfügung stehen und daß mit vorgegebenen Elementen die Operationen $+, -, \cdot, /$ und die Abfrage auf Gleichheit ausgeführt werden können. Hiermit erhält man die Möglichkeit, auch in Polynomringen $k[x]$ und rationalen Funktionenkörpern $k(x)$ $+, -, \cdot, /, \mathrm{div}, =$ berechnen zu können (div soll Teilen mit eindeutigem Rest bedeuten). Bei Laufzeitangaben werden die benötigten Operationen und Zuweisungen in k sowie die Bitoperationen für entsprechende Rechnungen in $\mathbb{Z}$ gezählt.

Wir nehmen weiter an, daß Algorithmen zur Berechnung von Ganzheitsbasen der Ringe $\mathrm{Cl}\big(k[x], F\big)$ und $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$, zur Berechnung ihrer Primideale zu vorgegebenen Primelementen von $k[x]$ beziehungsweise $\mathfrak{o}_\infty$, eine Element- und Idealarithmetik für $\mathrm{Cl}\big(k[x], F\big)$ und $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ inklusive Idealfaktorisierung und Bewertungsberechnung bezüglich Primidealen zur Verfügung stehen. Dies ist beispielsweise für $k = \mathbb{F}_q$ oder $k =$ Zahlkörper der Fall, Implementierungen finden sich in [25]. Mindestens für die Bestimmung der Primideale beziehungsweise der Idealfaktorisierung werden hierbei insbesondere Faktorisierungsalgorithmen für Polynome über k (und über Erweiterungen von k) benötigt. Über das prinzipielle Vorgehen dieser Algorithmen geben [9, 17, 36, 37], und speziell für die Funktionenkörpersituation [50], Auskunft.

Im Fall globaler Funktionenkörper (also $k = \mathbb{F}_q$) wird in [8] gezeigt, daß der Aufwand zur Bestimmung der Ganzheitsbasis $\mathfrak{o}^S$ polynomial äquivalent zum Aufwand der Bestimmung des quadratfreien Anteils der Diskriminante von $f(x, y)$ als Polynom in y ist. Da diese Aufgabe wiederum polynomial im Grad der Diskriminante gelöst werden kann, erhalten wir insgesamt einen in C_f und n polynomialen Aufwand. Ohne an dieser Stelle auf die Details eingehen zu können, merken wir an, daß auch die anderen angeführten Algorithmen eine in C_f und n polynomiale Laufzeit benötigen, in welche aber noch der maximale Grad der in den Darstellungen der beteiligen Ideale auftretenden Polynome von $k[x]$ polynomial eingeht. Es ist speziell zu beachten, daß die Faktorisierung in $k[x]$ einen im Grad polynomialen Aufwand benötigt. Soll beispielsweise ein Potenzprodukt von Primidealen ausmultipliziert werden, so bringt dies einen Aufwand mit sich, welcher polynomial in C_f, n, der Anzahl und dem Grad der auftretenden Primpolynome ist. Die beiden letzten Werte fassen wir später in einer „Höhe“ zusammen.

Entsprechend Abschnitt 1.1 lassen sich die Stellen von F/k durch die Primideale von $\mathrm{Cl}\big(k[x], F\big)$ und $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ eineindeutig repräsentieren. Hier gilt die Beziehung $\deg(P) = |\deg(\mathrm{N}_{F/k(x)}(\mathfrak{p}))|$ für eine Stelle P von F/k und ein Primideal $\mathfrak{p}$ von $\mathrm{Cl}\big(k[x], F\big)$ oder $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$, welche dieselbe Bewertung auf F/k definieren. Für einen globalen Funktionenkörper sind wir damit in der Lage, alle Stellen eines vorgegebenen Grads m zu ermitteln, indem die Primidealfaktorisierungen

der Primpolynome des Grads $\leq m$ aus $k[x]$ in $\mathrm{Cl}\big(k[x], F\big)$ und die Primideale in $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ berücksichtigt werden.
Ist k der exakte Konstantenkörper von F/k, so kann die Bestimmung der Anzahl der Stellen vom Grad eins einer endlichen Konstantenkörpererweiterung F_r/k_r von F/k, $[k_r : k] = r$ und $F_r = Fk_r$ fast ohne Faktorisierungen erfolgen: Bis auf wenige Ausnahmen („Indexteiler“) genügt es aufgrund des Satzes von Kummer [37, S. 390], [55, S. 76], die Anzahl der Nullstellen von $f(x_0, y)$ für alle $x_0 \in k_r$ zu bestimmen, welche durch den Grad des ggT von $f(x_0, y)$ und $y^{q^r+1} - y$ gegeben ist. Man beachtet außerdem, daß dieser Grad für die Konjugierten von x_0 über k gleich bleibt, weil f Koeffizienten in k hat (nicht-konjugierte x_0 können mit einem zyklischen Erzeuger von $k_r^\times$ leicht aufgezählt werden).
Obwohl diese Methode gegenüber dem obigen Faktorisieren sehr effizient ist, zählt sie doch auch zu den „naiven“ Methoden, weil der Aufwand exponentiell in r ist. Für die Eigenschaften von Konstantenkörpererweiterungen siehe [55, S. 101ff., S. 163].

Später werden die Landau-Symbole verwendet: Es seien $g, h : \mathbb{R}^{>0} \longrightarrow \mathbb{R}$. Wir schreiben $g = O(h)$, wenn es $c, x_0 \in \mathbb{R}$ gibt, so daß $|g(x)| \leq c\, h(x)$ für alle $x \geq x_0$ gilt. Wir schreiben $g = o(h)$, wenn es für jedes $\varepsilon > 0$ ein $x_0 \in \mathbb{R}$ gibt, so daß $|g(x)| \leq \varepsilon\, h(x)$ für alle $x \geq x_0$ gilt.

1.3 Gitter und Basisreduktion

Für die Berechnung von Riemann-Roch-Räumen benötigen wir einen Reduktionsalgorithmus für Matrizen in $k(x)^{n\times n}$, welcher im Zusammenhang mit Gittern und der Basisreduktion in Funktionenkörpern zu sehen ist. Wir geben die wesentlichen Aussagen für den vereinfachten Fall der über einem Körper formaler Laurentreihen definierten Gitter wieder, wobei der Funktionenkörper selbst noch nicht auftritt. Dies geschieht in Abschnitt 2.5, wo Aussagen über die durch Funktionenkörper definierten Gitter zusammengefaßt werden. Es sei grundsätzlich auf die (etwas unterschiedliche) Darstellung in [50] verwiesen.

Wir bezeichnen mit $k((x^{-1}))$ den Körper der formalen Laurentreihen in x^{-1}. Der Grad eines Elements sei der Exponent der größten darin auftretenden x-Potenz. Für $v \in k((x^{-1}))^n$ bezeichnen wir mit $\deg(v)$ den Spaltengrad von v, also das Maximum der Grade der Einträge von v, und mit $\mathrm{hc}(v) \in k^n$ denjenigen Vektor, der aus den Koeffizienten der $\deg(v)$-ten Potenzen von x der Einträge von v entsteht (also die Koeffizienten der größten Potenzen, die anderen sind null).

Es seien nun $\Lambda \subseteq k((x^{-1}))^n$ ein freier $k[x]$-Modul des Rangs m und die $v_1, \ldots, v_m$ eine Basis von Λ. Wir setzen zusätzlich voraus, daß die Basiselemente $k((x^{-1}))$-

linear unabhängig sind (dies ist gleichbedeutend damit, daß Λ bezüglich deg diskret ist, daß es also immer nur endlich viele Vektoren mit beschränkten deg-Werten gibt). Λ ist dann ein „nicht-archimedisches“ *Gitter*. Das Maximum der Grade der Determinanten von $m \times m$-Teilmatrizen von $(v_j)_j$ ist eine Invariante von Λ, die wir als Gitterdiskriminante auffassen können. Unter einem Reduktionsschritt versteht man nun die Addition einer $k[x]$-Linearkombination der v_j zu einem v_i, $i \neq j$, so daß sich der Spaltengrad von v_i verkleinert. Hierbei handelt es sich um eine unimodulare Transformation. Die bezüglich der Spaltengrade aufsteigend sortierte Basis $v_1, \ldots, v_m$ von Λ wird *reduziert* genannt, wenn eine der folgenden, äquivalenten Bedingungen zutrifft:

1.5. Lemma. *Die folgenden Bedingungen sind äquivalent:*

(*i*) $\mathrm{hc}(v_1), \ldots, \mathrm{hc}(v_m)$ *sind linear unabhängig,*

(*ii*) $\deg(\sum_{i=1}^m \lambda_i v_i) = \max_{i=1}^m \deg(\lambda_i v_i)$ *für alle* $\lambda_i \in k[x]$, $1 \leq i \leq m$,

(*iii*) $\sum_{i=1}^m \deg(v_i)$ *ist gleich der Gitterdiskriminante,*

(*iv*) $v_1, \ldots, v_m$ *realisieren die sukzessiven Minima von* Λ.

Beweis. Zum Beweis siehe auch [50]. Die Situation in (*i*) stellt eine nur auf die führenden Terme gerichtete Sichtweise von (*ii*) und (*iii*) dar; die lineare Unabhängigkeit bedeutet, daß sich keine führenden Terme auslöschen können. Mit diesen Bemerkungen kann man sich die Äquivalenz von (*i*)-(*iii*) klar machen. Nummer (*iv*) folgt induktiv aus (*ii*). □

Diese Bedingungen bedeuten, daß kein Reduktionsschritt ausgeführt werden kann. Für eine nicht reduzierte Basis kann man also einen Reduktionsschritt ausführen, der die Summe der Grade der v_i verringert. Für diese Summe stellt die Gitterdiskriminante aber eine untere Schranke dar, so daß man nach endlich vielen Reduktionsschritten zu einer reduzierten Basis kommt. Hieraus ergibt sich der *Reduktionsalgorithmus*; man kann also immer eine reduzierte Basis konstruieren. Eine Matrix, deren Spalten ungleich null eine reduzierte Basis bilden, nennen wir reduziert.

Die Eigenschaft (*iii*) kann man als Orthogonalitätseigenschaft einer reduzierten Basis auffassen. Das Konzept der Orthogonalität läßt sich weiterverfolgen: Wir betrachten „orthogonale“ oder auch „isometrische“ Abbildungen des $k((x^{-1}))^n$, die durch unimodulare Matrizen $T \in k[[x^{-1}]]^{n \times n}$ mit Potenzreiheneinträgen gegeben werden: $v \mapsto Tv$. Für diese gilt $\deg(v) = \deg(Tv)$. Zwei Gitter Λ_1, Λ_2 heißen nun *isometrisch*, wenn es ein solches T mit $\Lambda_1 = T\Lambda_2$ gibt. Reduzierte Basen werden unter T in reduzierte Basen überführt. Zwei isometrische Gitter besitzen

dieselben sukzessiven Minima und dieselbe Gitterdiskriminante, wie man anhand von Lemma 1.5 erkennen kann. Wir definieren das *orthogonale Gitter* des Rangs m in $k((x^{-1}))^n$ mit den Invarianten $d_1 \geq \cdots \geq d_m \in \mathbb{Z}$ als das eindeutig bestimmte Gitter, welches eine Basis der Form $(x^{-d_j}\delta_{i,j})_i \in k((x^{-1}))^n$ für $1 \leq j \leq m$ besitzt. Es gilt nun der folgende „Klassifikationssatz“:

1.6. Lemma. *Es sei $\Lambda \subseteq k((x^{-1}))^n$ ein Gitter vom Rang m. Dann ist Λ zu genau einem orthogonalen Gitter in $k((x^{-1}))^n$ isometrisch.*

Beweis. Wir bemerken als erstes, daß $k[[x^{-1}]]$ ein euklidischer Ring für deg ist und daß Elemente kleineren Grads stets von Elementen größeren Grads geteilt werden. Man kann deswegen eine beliebige Basis von Λ durch $k[[x^{-1}]]$-unimodulare Zeilenoperationen in eine obere Dreiecksgestalt bringen, wobei die über der Diagonalen stehenden Einträge entweder null sind oder einen echt größeren Grad als die darunter stehenden Diagonaleinträge haben. Das von dieser Basis erzeugte Gitter Λ' ist ein zu Λ isometrisches Gitter. Wegen (i) aus Lemma 1.5 muß sich diese Basis von Λ' wegen der Isometrie zu Λ bereits in Diagonalgestalt befinden, wenn sie aus einer reduzierten Basis von Λ entsteht. Eine reduzierte Basis von Λ existiert jedoch stets.
Für die noch zu zeigende Eindeutigkeit kann man sich leicht überlegen, daß zwei verschiedene orthogonale Gitter nicht isometrisch sein können. □

Die für die spätere Anwendung benötigte Version dieses Lemmas liest sich wie folgt:

1.7. Korollar. *In dem $k(x)$-Vektorraum V seien ein $k[x]$-Modul M_1 und ein $\mathfrak{o}_\infty$-Modul M_2, beide frei vom Rang n, gegeben. Dann gibt es Basen $v_1, \ldots, v_n$ von M_1 und $b_1, \ldots, b_n$ von M_2, so daß*

$$(b_1, \ldots, b_n)N = (v_1, \ldots, v_n)$$

mit einer eindeutigen Matrix N der Gestalt $N = (x^{-d_j}\delta_{i,j})_{i,j} \in k(x)^{n\times n}$ und $d_1 \geq \cdots \geq d_n$ gilt. Die Basis $v_1, \ldots, v_n$ kann durch Anwendung des Reduktionsalgorithmus auf die Spalten einer Transformationsmatrix beliebiger Basen von M_1 und M_2 erhalten werden.

Beweis. Man betrachtet das von den Spalten einer Basistransformationsmatrix M beliebiger b_i und v_i aufgespannte Gitter, wendet Lemma 1.6 an und erhält unimodulare Matrizen $T \in \mathfrak{o}_\infty^{n\times n}$ und $R \in k[x]^{n\times n}$ mit $N = TMR$ wie gefordert. Zu beachten ist, daß $T \in \mathfrak{o}_\infty^{n\times n}$ wegen $M \in k(x)^{n\times n}$ gilt. Die letzte Aussage ergibt sich speziell aus dem Beweis von Lemma 1.6. □

1.8. Beispiel. Wir betrachten die (in Hermite-Normalform befindliche) Matrix

$$\begin{pmatrix} x^3 - x & x^2 - 2 \\ 0 & x \end{pmatrix}.$$

Diese Matrix ist nicht reduziert, weil die Summe der Spaltengrade 5 und der Determinantengrad 4 beträgt. Wir subtrahieren das x-fache der zweiten Spalte von der ersten Spalte und erhalten die reduzierte Matrix

$$\begin{pmatrix} x & x^2 - 2 \\ -x^2 & x \end{pmatrix}.$$

Zur Berechnung der Normalform negieren wir die letzte Zeile, vertauschen sie mit der ersten Zeile und ziehen von der jetzt letzten Zeile das $1/x$-fache der ersten Zeile ab. Daraus ergibt sich

$$\begin{pmatrix} x^2 & -x \\ 0 & x^2 - 1 \end{pmatrix}.$$

Nun wird das $x/(x^2 - 1)$-fache der letzten Zeile zur ersten Zeile addiert und die letzte Zeile mit $x^2/(x^2 - 1)$ skaliert. Daraus erhält man das Endergebnis

$$\begin{pmatrix} x^2 & 0 \\ 0 & x^2 \end{pmatrix}.$$

1.9. Bemerkung. Bei dem Reduktionsalgorithmus handelt es sich um eine verallgemeinerte Polynomdivision, operierend auf Spalten. Entsprechend kann man ihn auch als eine Gröbnerreduktion interpretieren. Für Funktionenkörper übernimmt der Reduktionsalgorithmus die Rolle, die der LLL-Algorithmus im Zahlkörperfall spielt.

Kapitel 2

Konstruktive Riemann-Roch-Theorie

Das Hauptziel dieses Kapitels ist, einen Algorithmus zur Bestimmung des Riemann-Roch-Raums $\mathcal{L}(D)$ eines Divisors D eines algebraischen Funktionenkörpers F/k anzugeben. Wir benutzen dafür eine idealtheoretische Fassung der Riemann-Roch-Theorie, in deren Rahmen der Satz von Riemann-Roch relativ leicht bewiesen werden kann. Alle Strukturen sind hierbei einer direkten, algorithmischen Behandlung zugänglich. Darauf aufbauend geben wir Methoden zur Divisorreduktion und zur erweiterten Riemann-Roch-Raum-Berechnung an, ziehen einen Vergleich zur Geometrie der Zahlen für globale Funktionenkörper und betrachten als Anwendungen die Bestimmung von Differentialräumen und das explizite Rechnen in der Divisorenklassengruppe.

Zur Vertiefung dieser Methoden verwenden wir im letzten, vergleichsweise umfangreichen Abschnitt zusätzlich diskrete Bewertungen des Konstantenkörpers und beweisen Aussagen über die Struktur ganzalgebraischer Abschlüsse und über Teilräume von Riemann-Roch-Räumen, deren Elemente zusätzliche Bewertungsbedingungen erfüllen. Anwendungen hiervon liegen beispielsweise in der Reduktion algebraischer Funktionenkörper nach diskreten Bewertungen des Konstantenkörpers im Sinne von [13, S. 187ff.]. Auf diese Ergebnisse werden wir jedoch im weiteren Verlauf der Arbeit nicht zurückgreifen.

Die in den Abschnitten 2.1 und 2.3 ausgeführten Gedanken wurden in ähnlicher Form bereits in [48] verwendet, eine neuere Darstellung läßt sich in [27] finden.

In diesem Kapitel bezeichnet F/k einen algebraischen Funktionenkörper mit einem separierenden Element x, $S := \operatorname{supp}\big((x)_\infty\big)$ und $n := [F : k(x)]$, vgl. Abschnitt 1.2.

2.1 Basen der k-Räume $\mathcal{L}(D)$

Das Hauptergebnis dieses Abschnitts ist der folgende Satz zusammen mit seinem konstruktiven Beweis:

2.1. Satz. *Für jeden Divisor D von F/k gibt es eindeutig bestimmte, ganzrationale Zahlen $d_1 \geq \cdots \geq d_n$ und Elemente $v_1, \ldots, v_n \in F$, so daß die Menge*

$$\{\, x^j v_i \mid 1 \leq i \leq n,\, 0 \leq j \leq d_i + r\}$$

für alle $r \in \mathbb{Z}$ eine k-Basis von $\mathcal{L}\big(D + r(x)_\infty\big)$ darstellt. Die Elemente $v_1, \ldots, v_n$ sind $k(x)$-linear unabhängig.

Wir bemerken, daß die obigen d_i und v_i nicht nur dem Divisor D zugeordnet sind, sondern auch von dem Konstantenkörper k und dem separierenden Element x abhängen; die Abhängigkeit besteht genauer vom Polynomring $k[x] \subseteq F$. Zur späteren Bezugnahme definieren wir die d_i als die $k[x]$-*Invarianten* von D, geschrieben $|D|_i$ (wenn die Vorgabe von $k[x]$ klar ist).

Um einen konstruktiven Beweis dieses Satzes geben zu können, übersetzen wir die obige Situation in einen idealtheoretischen Kontext:

2.2. Proposition. (*i*) *Es besteht eine natürliche, Bewertungen erhaltende Bijektion zwischen der Menge der Stellen von F/k und der Menge der Primideale von $\mathfrak{o}^S$ und von $\mathfrak{o}_S$,*

(*ii*) *durch diese Bijektion wird ein Isomorphismus der Gruppe der Divisoren von F/k auf das direkte Produkt $\mathfrak{I}^S \times \mathfrak{I}_S$ der Idealgruppen induziert, $D \mapsto (D^S, D_S)$.*

(*iii*) *Wenn D einen Divisor bezeichnet und D^S, D_S die zugehörigen Ideale in $\mathfrak{I}^S$ und $\mathfrak{I}_S$ sind, dann gilt $\mathcal{L}(D) = (D^S)^{-1} \cap (D_S)^{-1}$.*

Beweis. Wir verweisen auf Abschnitt 1.1, S. 3 unten. Für (*iii*) sei $\mathfrak{p}$ ein Primideal von $\mathfrak{o}^S$, P die zugehörige Stelle von F/k und r die genaue Potenz, mit der $\mathfrak{p}$ in D^S aufgeht. Also ist $r = v_P(D)$ erfüllt. Weil $\mathfrak{o}^S$ ein Dedekindring ist, gilt $a \in (D^S)^{-1}$ genau dann, wenn $a \in F$ und $v_P(a) \geq -r$ ist. Analoges trifft für $(D_S)^{-1}$ zu, so daß $\mathcal{L}(D) = (D^S)^{-1} \cap (D_S)^{-1}$ folgt. □

2.3. Bemerkung. Es sei D ein durch (D^S, D_S) dargestellter Divisor. Dann wird $D + r(x)_0$ durch $(x^r D^S, D_S)$ und $D + r(x)_\infty$ durch $(D^S, x^{-r} D_S)$ dargestellt.

Wegen Proposition 2.2, (*iii*) sind wir nun an der Beziehung von $(D^S)^{-1}$ und $(D_S)^{-1}$ in F interessiert. Die Ideale in $\mathfrak{I}^S$ und $\mathfrak{I}_S$ sind freie $k[x]$- beziehungsweise $\mathfrak{o}_\infty$-Moduln vom Rang n, wir können daher Basen $v_1, \ldots, v_n \in (D^S)^{-1}$ und $b_1, \ldots, b_n \in (D_S)^{-1}$ von $(D^S)^{-1}$ und $(D_S)^{-1}$ wählen. Weil F ein $k(x)$-Vektorraum der Dimension n ist, existiert darüber hinaus eine Matrix $M \in k(x)^{n\times n}$, so daß $(b_1, \ldots, b_n)\, M = (v_1, \ldots, v_n)$ gilt. Wir sehen, daß M eindeutig bis auf Multiplikation mit einem unimodularen $R \in \mathfrak{o}_\infty^{n\times n}$ von links und einem unimodularen $T \in k[x]^{n\times n}$ von rechts ist, denn je zwei Basen von $(D^S)^{-1}$ oder $(D_S)^{-1}$ unterscheiden sich um zwei solche Transformationen. Korollar 1.7 paßt genau auf diese Situation, wir können damit nun einen Beweis für Satz 2.1 geben:

Beweis von Satz 2.1. Wir fixieren ein D und beweisen zunächst die Existenz. Durch Wahl einer Basisübergangsmatrix M für $(D^S)^{-1}$ und $(D_S)^{-1}$ wie oben und durch Anwendung von Korollar 1.7 sehen wir, daß es Idealbasen $(v_i)_i$ von $(D^S)^{-1}$ und $(b_i)_i$ von $(D_S)^{-1}$ gibt, welche zueinander diagonal liegen mit einer eindeutigen Transformationsmatrix $(x^{-d_i}\delta_{i,j})_{i,j}$, in anderen Worten $x^{-d_i}b_i = v_i$ mit eindeutigen ganzrationalen Zahlen $-d_i$ für $1 \le i \le n$.
Es sei nun $r \in \mathbb{Z}$ beliebig. Der Divisor $D + r(x)_\infty$ wird gemäß Bemerkung 2.3 durch das Paar $(D^S, x^{-r}D_S)$ von Idealen eindeutig dargestellt. Die Idealbasen von $(D^S)^{-1}$ und $x^r(D_S)^{-1}$ sind $(v_i)_i$ wie vorher und $(b'_i)_i$ mit $b'_i = x^r b_i$. Diese befinden sich bereits in diagonaler Lage. Wir betrachten nun den Schnitt von $(D^S)^{-1}$ mit $x^r(D_S)^{-1}$: Das Element $z = \sum_{i=1}^n \lambda_i v_i$ mit beliebigen $\lambda_i \in k[x]$ liegt in $(D^S)^{-1}$. Weil auf der anderen Seite $z = \sum_{i=1}^n \lambda_i x^{-d_i-r} b'_i$ gilt, sieht man, daß für die Bedingung $z \in x^r(D_S)^{-1}$ notwendig und hinreichend ist, daß $\lambda_i x^{-d_i-r} \in \mathfrak{o}_\infty$ gilt. Dies bedeutet aber, daß $\deg \lambda_i \le d_i + r$ ist. Aufgrund dieser Beobachtung und der $k(x)$-linearen Unabhängigkeit der v_i ergibt sich die Aussage von Satz 2.1 über die Basis.
Als nächstes beweisen wir die letzte Aussage: Die $k(x)$-lineare Unabhängigkeit von Elementen v_i wie im Satz folgt aus der Basiseigenschaft der $x^j v_i$ für alle $r \in \mathbb{Z}$. Denn wenn es eine Relation $\sum_{i=1}^n \lambda_i v_i = 0$ mit $\lambda_i \in k[x]$ nicht alle null geben würde, dann wären die Elemente $x^j v_i$ k-linear abhängig.
Zu zeigen bleibt die Eindeutigkeit jedweder d_i, die Satz 2.1 zusammen mit beliebigen v_i genügen. Wir behaupten, daß erstens $v_1, \ldots, v_n$ eine Idealbasis von $(D^S)^{-1}$ und zweitens $x^{d_1}v_1, \ldots, x^{d_n}v_n$ eine Idealbasis von $(D_S)^{-1}$ darstellen. Weil es für jedes $g \in (D^S)^{-1}$ ein $r \in \mathbb{Z}$ gibt, so daß $g \in \mathcal{L}\big(D + r(x)_\infty\big)$ gilt, können wir g durch die v_i darstellen, und die erste Behauptung ist klar. Für die zweite Behauptung merken wir an, daß es für jedes $g \in (D_S)^{-1}$ ein $h \in k[x]$ gibt, so daß $g \in \mathcal{L}\big(D + (h)_0\big)$ ist. Wenn wir $r := \deg h$ setzen, gilt $r(x)_\infty = (h)_\infty$ und außerdem $D + (h)_0 = D + r(x)_\infty + (h)$, so daß die Elemente $h^{-1}x^j v_i$ mit $1 \le i \le n$, $0 \le j \le d_i + r$ eine k-Basis von $\mathcal{L}\big(D + (h)_0\big)$ darstellen (man beachte

$\mathcal{L}\big(D+(a)\big) = a^{-1}\mathcal{L}(D)$ für $a \in F^\times$). Wir sehen also, daß g durch eine $\mathfrak{o}_\infty$-lineare Kombination der $x^{d_i}v_i$ dargestellt werden kann, was zu beweisen war.
Weil nun die Basen $v_1, \ldots, v_n$ von $(D^S)^{-1}$ und $x^{d_1}v_1, \ldots, x^{d_n}v_n$ von $(D_S)^{-1}$ in diagonaler Lage zueinander sind, schließen wir auf die Eindeutigkeit der d_i durch die Eindeutigkeitsaussage von Korollar 1.7. □

Aus dem Beweis ergibt sich speziell die Gleichung

$$-\sum_{i=1}^{n} |D|_i = \deg(\det M), \tag{2.4}$$

wobei M wie zuvor die Transformationsmatrix einer Basis von $(D_S)^{-1}$ zu einer Basis von $(D^S)^{-1}$ ist.

Es ist klar, daß es eine Verbindung zwischen den $k[x]$-Invarianten eines Divisors D, dem Geschlecht und der Dimension des exakten Konstantenkörpers von F/k über k geben sollte.

2.5. Korollar. *Es bezeichne g das Geschlecht von F/k, und es sei k_0 der exakte Konstantenkörper von F/k. Für die $k[x]$-Invarianten $|D|_i$ eines Divisors D gilt dann*

$$\sum_{i=1}^{n} |D|_i = \deg_k D + [k_0 : k](1-g) - n.$$

Beweis. Wir wählen $r \in \mathbb{Z}$ groß genug, so daß der Divisor $D + r(x)_\infty$ nicht speziell ist, [55, S. 33], und daß $r \geq |D|_i$ für alle $1 \leq i \leq n$ gilt. Aufgrund des Satzes von Riemann-Roch wissen wir dann, daß $\dim_k(D + r(x)_\infty) = \deg_k(D + r(x)_\infty) + [k_0 : k](1-g)$ ist. Mittels Satz 2.1 bestätigen wir auf der anderen Seite die Gleichungen $\dim_k(D + r(x)_\infty) = \sum_{i=1}^{n}(|D|_i + r + 1) = rn + n + \sum_{i=1}^{n} |D|_i$. Wegen $\deg_k(D + r(x)_\infty) = \deg_k D + rn$ erhalten wir das gewünschte Resultat durch Gleichsetzen. □

Das letzte Ergebnis erlaubt eine anschauliche Interpretation der Invarianten g und $[k_0 : k]$ des Funktionenkörpers F/k und des Grads eines Divisors D (für ein festes, separierendes Element x): Durch diese wird nämlich der „Abstand“ der den Divisor darstellenden Ideale D^S und D_S in F beschrieben. Bei wachsendem Grad entfernen sich D^S und D_S voneinander, wohingegen sich $(D^S)^{-1}$ und $(D_S)^{-1}$ annähern (so daß Überlappung entsprechend der Größe des Grads von D eintritt).

Für den Beweis des Korollars haben wir den Satz von Riemann-Roch verwendet. Wir geben später einen konstruktiven Beweis des Satzes von Riemann-Roch an, welcher auf der geeigneten Reformulierung dieses Korollars aufbaut. Dies wird

Korollar 2.10 sein, für welches wir einen alternativen Beweis verwenden, ohne den Satz von Riemann-Roch vorauszusetzen.

Als Anwendung erhalten wir die folgende Schranke für das Geschlecht, vgl. [55, S. 132], [18, S. 201], [33, S. 169]:

2.6. Korollar. *Der algebraische Funktionenkörper F/k mit dem exakten Konstantenkörper k_0 sei durch eine Gleichung $f(x,y)=0$ mit einem in y normierten und separablen, irreduziblen Polynom $f(x,y)\in k[x,y]$ gegeben. Dann gilt für das Geschlecht von F/k*

$$g \le \frac{C_f(n-1)n - 2(n-[k_0:k])}{2[k_0:k]}.$$

Ist $C_f = 1$ und $k_0 = k$, so erhält man daraus

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

Beweis. Es sei $\rho \in F$ mit $f(x,\rho)=0$. Wir betrachten Gleichungsordnungen $k[x,\rho]$ von $\mathfrak{o}^S$ und $\mathfrak{o}_\infty[\rho/x^{C_f}]$ von $\mathfrak{o}_S$ (ρ/x^{C_f} ist ganzalgebraisch über $\mathfrak{o}_\infty$). Für die Transformationsmatrix der Basen haben wir dann

$$(1, x^{-C_f}\rho, \ldots, x^{-C_f(n-1)}\rho^{n-1})(x^{C_f(i-1)}\delta_{i,j})_{i,j} = (1,\rho,\ldots,\rho^{n-1}).$$

Die Summe der Grade der hierin auftretenden x-Potenzen bildet wegen (2.4) eine obere Schranke für die Summe der negierten $k[x]$-Invarianten des Nulldivisors. Mit Korollar 2.5 erhalten wir dann: $n + [k_0:k](g-1) \le C_f n(n-1)/2$, woraus sich durch Umstellen der Ungleichung die Aussage ergibt. □

Man vergleiche diese Schranke für das Geschlecht mit der Schranke für den Diskriminantengrad $\deg \operatorname{disc}_y f(x,y) \le C_f n(n-1)$ aus Abschnitt 1.2.

2.2 Riemann-Roch-Raum-Berechnung I

In diesem Abschnitt soll das Basisverfahren zur Berechnung des Riemann-Roch-Raums eines Divisors beschrieben werden. Wir setzen die Maximalordnungen $\mathfrak{o}^S$ und $\mathfrak{o}_S$ als berechnet voraus (vgl. Abschnitt 1.2). Die *Höhe* eines Divisors D wird als die Summe der Grade des Pol- und Nullstellendivisors von D definiert:

$$h(D) := \deg_k(D)_0 + \deg_k(D)_\infty.$$

Es gibt nun zwei wesentliche Arten der Darstellung eines Divisors D. Wie bisher verwendet kann D durch zwei Ideale D^S und D_S repräsentiert werden, von

denen wir im Hinblick auf Proposition 2.2, (*iii*) aber besser nur die Inversen verwenden. Diese Darstellung soll *Idealdarstellung* heißen. Die andere Darstellung ist einfach diejenige als Summe von Stellen beziehungsweise als Potenzprodukt von Primidealen. Wir nennen sie die *freie Darstellung*. Die Divisorarithmetik wird für Divisoren in freier Darstellung exponentenweise und für Divisoren in Idealdarstellung mit Idealarithmetik durchgeführt, wobei in beiden Fällen für Divisoren D_1, D_2 wegen Abschnitt 1.2 ein in C_f, n und $\max\{\, h(D_1),\, h(D_2)\,\}$ polynomialer Aufwand entsteht (die Größe der Exponenten geht bei der freien Darstellung allerdings nur logarithmisch ein). Durch Ausmultiplizieren der Primideale in einer freien Darstellung kann man die Ideale D^S und D_S der Idealdarstellung bestimmen. Umgekehrt müssen diese beiden Ideale aber faktorisiert werden, um die im Divisor aufgehenden Stellen und ihre Exponenten zu erhalten. Dieser Darstellungswechsel erfordert in beiden Richtungen nach Abschnitt 1.2 ebenfalls eine polynomiale Laufzeit in C_f, n und $h(D)$. Durch die Verwendung von Hauptidealen kann man so auch Hauptdivisoren in freier Darstellung von Elementen aus $F^\times$ bestimmen.

Die Berechnung eines Riemann-Roch-Raums besteht aus der Berechnung seiner Basis. Wir stützen uns dabei auf Satz 2.1 und unterscheiden Basen in kurzer (durch v_i, d_j gegebener) und langer (durch $x^j v_i$ gegebener) Darstellung.

2.7. Algorithmus. *(Riemann-Roch-Raum-Berechnung I)*

Eingabe: *Ein Divisor D des algebraischen Funktionenkörpers F/k.*

Ausgabe: *Eine k-Basis von $\mathcal{L}(D)$ in kurzer oder langer Darstellung.*

1. *(Basen) Bestimme $k[x]$- beziehungsweise $\mathfrak{o}_\infty$-Basen $v'_1, \ldots, v'_n$ und $b'_1, \ldots, b'_n$ der Ideale $(D^S)^{-1}$ und $(D_S)^{-1}$.*

2. *(Trafo) Bestimme $M \in k(x)^{n\times n}$ mit $(b'_1, \ldots, b'_n)M = (v'_1, \ldots, v'_n)$.*

3. *(Schnitt) Bestimme die gesuchte Basis $v_1, \ldots, v_n$ mit den $k[x]$-Invarianten d_j durch Anwendung des Reduktionsalgorithmus auf die Spalten von M gemäß Korollar 1.7 und Satz 2.1.*

4. *(Ende) Ausgabe der Basis von Satz 2.1 in kurzer oder langer Darstellung. Terminiere.*

2.8. Bemerkung. Der Algorithmus benötigt insgesamt eine in C_f, n und $h(D)$ polynomiale Laufzeit: Die Größe der Einträge der Matrix M im zweiten Schritt ist nämlich polynomial in C_f, n und $h(D)$. Folglich erfordert der Reduktionsalgorithmus ebenfalls polynomiale Zeit in C_f, n und $h(D)$.

Wenn man Riemann-Roch-Räume zu Divisoren kleiner Höhe, also ungefähr in der Größenordnung von n oder C_f, berechnen möchte, eignet sich Algorithmus 2.7 gut. Gerade im Zusammenhang mit der Divisorenklassengruppe globaler Funktionenkörper kann es aber vorkommen, daß die Exponenten des Divisors in freier Darstellung bei kleinen Stellengraden in der Größenordnung q^g liegen, wobei q die Elementanzahl von k und g das Geschlecht von F/k ist. Dies bedeutet dann einen entsprechend der Bemerkung exponentiellen Zeitaufwand für Algorithmus 2.7. Die Diskussion dieser Problematik wird in Abschnitt 2.6 fortgeführt.

2.9. Beispiel. Zur Demonstration der Methode betrachten wir ein möglichst einfaches Beispiel: Wir wählen $k = \mathbb{Q}$, $f(x,y) = y^2 - x^3 - 1$ und $F = k(x,\rho)$ mit $f(x,\rho) = 0$, also einen elliptischen Funktionenkörper. Man rechnet leicht nach, daß $\mathfrak{o}_F := \mathrm{Cl}(k[x],F) = k[x,\rho]$ gilt. Für die Bestimmung von $\mathfrak{o}_{F,\infty} := \mathrm{Cl}(\mathfrak{o}_\infty,F)$ beachtet man, daß ρ/x^2 ganzalgebraisch über $\mathfrak{o}_\infty$ ist. Das zugehörige Minimalpolynom ist $f_\infty(y) = y^2 - (x^3+1)/x^4 \in \mathfrak{o}_\infty[y]$, und hierfür gilt auch $\mathrm{Cl}(\mathfrak{o}_\infty,F) = \mathfrak{o}_\infty[\rho/x^2]$. Man sieht damit, daß $\mathbb{Q}$ der exakte Konstantenkörper ist und das Geschlecht eins beträgt. Wir wollen das von $x-2$ erzeugte Hauptideal in $\mathfrak{o}_F$ faktorisieren. Nach dem Satz von Kummer faktorisieren wir dazu $f(x,y) \bmod (x-2)k[x,y]$ in der Form $y^2 - 9 = (y-3)(y+3)$ und erhalten $(x-2)\mathfrak{o}_F = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1 = (x-2)\mathfrak{o}_F + (\rho-3)\mathfrak{o}_F$ und $\mathfrak{p}_2 = (x-2)\mathfrak{o}_F + (\rho+3)\mathfrak{o}_F$. Daraus schließen wir, daß es über der durch $x-2$ definierten Stelle von $k(x)$ vom Grad 1 zwei unverzweigte Stellen P_1 beziehungsweise P_2 von F/k vom Grad 1 gibt, an denen x den Wert 2 und ρ den Wert 3 beziehungsweise -3 annimmt. Wir untersuchen nun die Zerlegung der unendlichen Stelle ∞ von $k(x)$ in F. Dazu muß $(1/x)\mathfrak{o}_{F,\infty}$ faktorisiert werden, weil $1/x$ ein Primelement von ∞ ist. Wieder mit dem Satz von Kummer und wegen $f_\infty(x,y) \equiv y^2 \bmod (1/x)\mathfrak{o}_\infty[y]$ gilt $(1/x)\mathfrak{o}_\infty = \mathfrak{p}_3^2$ mit $\mathfrak{p}_3 = (\rho/x^2)\mathfrak{o}_{F,\infty}$. Die unendliche Stelle von $k(x)$ besitzt also genau eine, verzweigte Fortsetzung vom Grad 1 auf F, die ebenfalls mit ∞ bezeichnet wird. Man kann daher auch sagen, daß x den Grad 2 und ρ den Grad 3 hat.
Nun soll schließlich der Riemann-Roch-Raum von $D = 3\infty - P_1$, also der Schnitt $\mathfrak{p}_1 \cap \mathfrak{p}_3^{-3}$, berechnet werden. Eine $k[x]$-Basis von $\mathfrak{p}_1$ wird durch $(\alpha_1,\alpha_2) = (x-2, \rho-3)$ und eine $\mathfrak{o}_\infty$-Basis von $\mathfrak{p}_3^{-3}$ durch $(\beta_1,\beta_2) = (x^3/\rho)\,(1,\rho/x^2)$ gegeben. Daraus folgt die Basisbeziehung

$$\begin{aligned}(\alpha_1,\alpha_2) &= (\beta_1,\beta_2)\begin{pmatrix} 0 & (x^3+1)/x^5 \\ 1/x & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & x^2 \end{pmatrix}\begin{pmatrix} x-2 & -3 \\ 0 & 1 \end{pmatrix} \\ &= (\beta_1,\beta_2)\begin{pmatrix} 0 & (x^3+1)/x^3 \\ (x-2)/x & -3/x \end{pmatrix}.\end{aligned}$$

Die Matrix ist bereits reduziert, so daß die $k[x]$-Invarianten von D beide null

sind und eine Basis des Riemann-Roch-Raums durch $x-2, y-3$ gegeben wird. Anschaulich gesprochen besteht $\mathcal{L}(D)$ aus den Elementen von $\mathfrak{p}_1$, deren Grad durch 3 beschränkt ist, so daß das Ergebnis mit der obigen Bemerkung über die Grade im Einklang steht.

2.3 Der Satz von Riemann-Roch

Unter Benutzung der idealtheoretischen Sprache aus Abschnitt 2.1 wollen wir nun einen kurzen, konstruktiven Beweis des Satzes von Riemann-Roch 2.13 und eine Definition des Geschlechts geben. Wir nehmen an, daß wir uns in der Situation genau nach dem Beweis von Satz 2.1 befinden. Korollar 2.5 wird dann passend wie folgt reformuliert:

2.10. Korollar. *Für einen algebraischen Funktionenkörper F/k gibt eine Konstante $c_{k,x} \in \mathbb{Z}$, abhängig vom Konstantenkörper k und vom gewählten separierenden Element x, so daß für die $k[x]$-Invarianten eines Divisors D gilt:*

$$\sum_{i=1}^{n} |D|_i \;=\; \deg_k D + c_{k,x} - n.$$

Beweis. Für zwei Ideale $\mathfrak{a}, \mathfrak{b}$ von $\mathfrak{o}^S$ oder $\mathfrak{o}_S$ ist der Grad der Determinante einer Übergangsmatrix einer Basis von $\mathfrak{a}$ zu einer von $\mathfrak{ab}$ durch $\deg\big(\mathrm{N}_{F/k(x)}(\mathfrak{b})\big)$ gegeben. Für einen zusätzlichen Divisor E von F/k stimmt die Summe $-\sum_{i=1}^{n} |D+E|_i$ wegen (2.4) mit dem Grad der Determinante einer Übergangsmatrix einer Basis von $(D_S E_S)^{-1}$ zu einer Basis von $(D^S E^S)^{-1}$ überein, analoges gilt für $-\sum_{i=1}^{n} |D|_i$. Durch Zusammensetzen erhält man daher den Ausdruck $-\sum_{i=1}^{n} |D+E|_i = -\sum_{i=1}^{n} |D|_i + \deg\big(\mathrm{N}_{F/k(x)}(E_S)\big) - \deg\big(\mathrm{N}_{F/k(x)}(E^S)\big)$. Weil für den Divisor E die Gleichung $\deg_k(E) = \deg\big(\mathrm{N}_{F/k(x)}(E^S)\big) - \deg\big(\mathrm{N}_{F/k(x)}(E_S)\big)$ gilt, ergibt sich daraus die Formel

$$\sum_{i=1}^{n} |D+E|_i = \deg_k E + \sum_{i=1}^{n} |D|_i.$$

Wegen dieser Formel kann $c_{k,x}$ unter Verwendung des Nulldivisors durch $c_{k,x} := \sum_{i=1}^{n} |0|_i + n$ definiert werden. □

Die Summe der $k[x]$-Invarianten eines Divisors ist also gleich seinem Grad plus einer nur von k, x und dem Funktionenkörper F/k abhängigen Konstante. Wir können nun die Summe der nicht-negativen $|D|_i$ gemäß Satz 2.1 (für $r = 0$) ungefähr als Dimension von $\mathcal{L}(D)$ auffassen. Zum Beweis des Satzes von Riemann-Roch 2.13 werden wir zeigen, daß es einen zu D *dualen* Divisor D^* gibt, dessen

nicht-negative $|D^*|_i$ ungefähr mit den negativen $|D|_i$ übereinstimmen. Dies bedeutet dann $\dim_k D - \dim_k D^* \approx \sum_{i=1}^n |D|_i = \deg_k D +$ Konstante, welches bereits die Riemann-Roch-Gleichung bis auf die gewissen Ungenauigkeiten darstellt.

Um nun die Existenz eines solchen D^* zu zeigen, benutzen wir komplementäre Ideale, komplementäre Divisoren und ihre grundlegenden Eigenschaften, vgl. [27, S. 88ff.]: Es sei A ein Hauptidealring, K der Quotientenkörper, L/K eine separable Körpererweiterung vom Grad n und B der ganze Abschluß von A in L. Wenn $\mathfrak{a}$ ein (gebrochenes) Ideal von B ist, so ist $\mathfrak{a}^\# := \{\alpha \in L \,|\, \mathrm{Tr}_{L/K}(\alpha\mathfrak{a}) \subseteq A\}$ das *komplementäre* Ideal zu $\mathfrak{a}$. Wenn $a_1, \ldots, a_n \in \mathfrak{a}$ eine A-Basis von $\mathfrak{a}$ ist, dann gibt es $a_1^\#, \ldots, a_n^\# \in \mathfrak{a}^\#$ mit $\mathrm{Tr}_{L/K}(a_i^\# a_j) = \delta_{i,j}$ für $1 \le i, j \le n$, und diese bilden eine A-Basis von $\mathfrak{a}^\#$. Wenn $\mathfrak{b}$ ein weiteres Ideal von B ist, haben wir $(\mathfrak{ab})^\# = \mathfrak{a}^\#\mathfrak{b}^{-1}$. Wieder in unserer Funktionenkörpersituation sei der Divisor D durch $(\mathfrak{a}, \mathfrak{b})$ dargestellt. Der *$k(x)$-komplementäre* Divisor $D^\#$ zu D wird als der durch $\big(((\mathfrak{a}^{-1})^\#)^{-1}, ((\mathfrak{b}^{-1})^\#)^{-1}\big)$ dargestellte Divisor definiert. Wir merken an, daß diese Definition tatsächlich nur von dem rationalen Funktionenkörper $k(x)$ und nicht von x selbst abhängt. Ähnlich wie oben gilt die Identität $(D + E)^\# = D^\# - E$ für Divisoren D und E. Der *Differentendivisor* $\mathcal{D}_{F/k(x)}$ von $F/k(x)$ ist gleich dem $k(x)$-komplementären Divisor des Nulldivisors. Zuletzt definieren wir den zu einem Divisor D *(k,x)-dualen Divisor* D^* durch $D^\# - 2(x)_\infty$.

Die nächsten Aussagen bilden die Grundlage des Satzes von Riemann-Roch:

2.11. Lemma. *Für die $k[x]$-Invarianten des zu D $k(x)$-komplementären Divisors $D^\#$ gilt für alle $1 \le i \le n$:*

$$|D^\#|_i \;=\; -|D|_i.$$

Beweis. Wir kürzen $\mathfrak{a} = (D^S)^{-1}$ und $\mathfrak{b} = (D_S)^{-1}$ ab. $D^\#$ wird dann durch $(\mathfrak{a}^\#)^{-1}$ und $(\mathfrak{b}^\#)^{-1}$ dargestellt. Wie in Abschnitt 2.1 seien $a_1, \ldots, a_n$ eine $k[x]$-Basis von $\mathfrak{a}$ und $b_1, \ldots, b_n$ eine $\mathfrak{o}_\infty$-Basis von $\mathfrak{b}$, so daß $b_i = x^{|D|_i} a_i$ für $1 \le i \le n$ gilt. Es genügt, $b_i^\# = x^{-|D|_i} a_i^\#$ zu beweisen: Es gibt $\lambda_{i,j} \in k(x)$, so daß $a_j^\# = \sum_{i=1}^n \lambda_{i,j} b_i^\#$ gilt. Damit erhalten wir $\lambda_{i,j} = \mathrm{Tr}_{F/k(x)}(a_j^\# b_i) = x^{|D|_i}\mathrm{Tr}_{F/k(x)}(a_j^\# a_i) = x^{|D|_i}\delta_{i,j}$, wobei die erste und die letzte Gleichheit aufgrund der Dualbasiseigenschaft und die zweite Gleichheit wegen $b_i = x^{|D|_i} a_i$ folgen. □

2.12. Lemma. *Für jeden Divisor D von F/k und seinen (k,x)-dualen Divisor D^* gilt die Gleichung*

$$\dim_k D \;=\; \deg_k D + c_{k,x} + \dim_k D^*.$$

Beweis. Wir können $\sum_{|D|_i \ge 0}(|D|_i + 1) + \sum_{|D|_i \le -1}(|D|_i + 1) = \sum_{i=1}^n |D|_i + n = \deg_k D + c_{k,x}$ wegen Korollar 2.10 schreiben. Nach Satz 2.1 ist die Dimension $\dim_k D$ gleich der obigen, ersten Summe. Wegen Lemma 2.11 und Satz 2.1

sehen wir, daß die $k[x]$-Invarianten von D^* mit $|D^*|_i = -|D|_i - 2$ übereinstimmen. Aufsummieren für die Dimension von D^* ergibt bereits $\dim_k D^* = \sum_{|D^*|_i \geq 0}(|D^*|_i + 1) = -\sum_{|D|_i \leq -1}(|D|_i + 1)$, was das Negative der obigen, zweiten Summe ist. □

Der Divisor D^* kann wegen dem zuvor gesagten als $D^* = W_{k,x} - D$ geschrieben werden, wobei wir $W_{k,x}$ als $\mathcal{D}_{F/k(x)} - 2(x)_\infty$ definieren. Weiter sei l die Dimension des exakten Konstantenkörpers k_0 von F/k über k. Mit Lemma 2.12 erkennen wir nun, daß $c_{k,x}$ von l geteilt wird und daß (Nulldivisor einsetzen) $c_{k,x} \leq l$ gilt. Wir definieren schließlich das *Geschlecht* von F/k durch $g := 1 - c_{k,x}/l$ und erhalten

2.13. Satz (Riemann-Roch). *Die Menge der Divisoren W von F/k, für die die Gleichung*

$$\dim_k D \;=\; \deg_k D + l(1-g) + \dim_k(W - D)$$

mit beliebigen Divisoren D gilt, bildet eine nicht-leere Divisorenklasse von F/k. Ihre Elemente W, die kanonischen Divisoren, werden exakt durch $\dim_k W = lg$ und $\deg_k W = 2l(g-1)$ unter allen Divisoren von F/k charakterisiert.

Beweis. Die Divisoren $W_{k,x}$ sind kanonische Divisoren, weil sie der geforderten Gleichung wegen des vorangegangenen Lemmas für alle Divisoren D genügen. Außerdem hängt die Definition des Geschlechts nicht von k oder x ab, weil für Divisoren D großen positiven Grads $\dim_{k_0}(W_{k,x} - D) = 0$, folglich $1 - g = \dim_{k_0} D - \deg_{k_0} D$ gilt, und die rechte Seite ist sicherlich von x unabhängig. Wenn W_1 obige Gleichung für alle Divisoren D erfüllt, haben wir $\dim_k W_1 = lg$ und $\deg_k W_1 = 2l(g-1)$, wie man durch Einsetzen des Nulldivisors und W_1 für D sehen kann. Wenn für W_2 die Gleichungen $\dim_k W_2 = lg$ und $\deg_k W_2 = 2l(g-1)$ gelten, dann ist $\dim_k(W_1 - W_2) = l$ und $\deg_k W_1 - W_2 = 0$, so daß W_1 und W_2 derselben Divisorenklasse angehören. Dies zeigt die letzte Aussage sowie, daß die kanonischen Divisoren tatsächlich eine Divisorenklasse bilden. □

2.4 Eigenschaften der $k[x]$-Invarianten

In diesem Abschnitt soll auf weitere Eigenschaften der $k[x]$-Invarianten eines Divisors D von F/k eingegangen werden. Gilt $\dim_k(W - D) > 0$ für einen kanonischen Divisor W, so wird D *speziell* genannt.

2.14. Lemma. *Ein Divisor D von F/k ist nicht speziell genau dann, wenn für seine $k[x]$-Invarianten $|D|_i \geq -1$ gilt.*

Beweis. Für den (k,x)-dualen Divisor D^* von D gilt $\dim_k(W-D) = \dim_k D^* = -\sum_{|D|_i \le -1}(|D|_i+1)$ (wie im Beweis von Lemma 2.12). Daraus folgt die Gültigkeit der Aussage. □

2.15. Lemma. *Für die $k[x]$-Invarianten eines Divisors D von F/k gilt:*

$$0 \le |D|_1 - |D|_n \le l(1+g).$$

Beweis. Die erste Ungleichung ist klar, weil die $|D|_i$ per Definition in i monoton fallen. Durch Addition von Vielfachen von $(x)_\infty$ zu D ändert sich die Varianz $|D|_1 - |D|_n$ der $k[x]$-Invarianten nicht (siehe Satz 2.1), so daß wir $|D|_1 = 0$, folglich $\dim_k D > 0$ annehmen können. Es sei D^* der (k,x)-duale Divisor zu D. Aus $\dim_k D^* = 0$ folgt $0 \ge |D|_i \ge -1$ für alle $1 \le i \le n$ wegen Lemma 2.14, und die Aussage ist wahr. Wir nehmen nun an, daß $\dim_k D^* > 0$ ist und benutzen die Tatsache [55, S. 34], daß $\dim_k A + \dim_k B \le l + \dim_k(A+B)$ für Divisoren A und B mit $\dim_k A > 0$ und $\dim_k B > 0$ gilt. Entsprechend dem Vorgehen im Beweis von Lemma 2.12 haben wir $\dim_k D = \sum_{|D|_i \ge 0}(|D|_i+1) \ge |D|_1 + 1$ und $\dim_k D^* = -\sum_{|D|_i \le -1}(|D|_i+1) \ge -|D|_n - 1$. Wegen $D + D^* = W_{k,x}$ erhalten wir durch Aufsummieren und unter Beachtung der zitierten Ungleichung, daß $|D|_1 + 1 - |D|_n - 1 \le \dim_k D + \dim_k D^* \le l + lg$ gilt, womit der Beweis vollständig erbracht ist. □

2.5 Verbindung zur Gittertheorie in globalen Funktionenkörpern

In diesem Abschnitt wollen wir die Relevanz der $k[x]$-Invarianten eines Divisors D für die Geometrie der Zahlen eines globalen Funktionenkörpers F/k mit separierendem Element x erläutern. Zu diesem Zweck wiederholen wir kurz einige Begriffe und Aussagen aus [50] (in etwas veränderter Form). Die durch einen Funktionenkörper gegebenen Gitter sind im allgemeinen nicht mehr über $k((x^{-1}))$ wie die Gitter von Abschnitt 1.3 definiert, sondern beispielsweise über Puiseuxreihenkörpern. Wir gehen hierauf nicht weiter ein, merken aber an, daß die Gittertheorie aus Abschnitt 1.3 hier analog gilt.

Wir wechseln vom logarithmischen Längenmaß deg zu einem Absolutbetrag mittels der Beziehung $\log_q|\cdot| = \deg(\cdot)$: Im rationalen Funktionenkörper $k(x)$ definieren wir den Absolutbetrag eines $\lambda \in k(x)$ durch $|\lambda| = q^{-v_\infty(\lambda)}$, wobei q die (endliche) Anzahl der Elemente von k ist. Die Menge der Stellen über ∞ wird als $S = \{P_0, P_1, \ldots, P_s\}$ geschrieben, und wir bezeichnen mit v_i beziehungsweise $|\cdot|_i$ die zu P_i gehörige, surjektive exponentielle Bewertung beziehungsweise den Absolutbetrag, so daß $|\alpha|_i = q^{-v_i(\alpha)}$ für beliebiges $\alpha \in F^\times$ gilt. Es sei nun D ein

Divisor von F/k. Wir definieren c_i als den Exponenten von P_i in D und e_i als den Verzweigungsindex von P_i über ∞. Auf dem $k(x)$-Vektorraum F existiert eine ultrametrische, $|\cdot|$-lineare Norm $\|\cdot\|_D$ definiert durch $\|\alpha\|_D = \max_{i=0}^{s} q^{-c_i/e_i}|\alpha|_i^{1/e_i}$. Der freie $k[x]$-Modul $(D^S)^{-1}$ ist diskret bezüglich $\|\cdot\|_D$ und wird das zu D (und k, x) gehörige *Gitter* Λ_D genannt. Für diese Gitter haben wir den üblichen Begriff der sukzessiven Minima.
Eine Basis $\omega_1, \ldots, \omega_n$ von Λ_D, geordnet nach aufsteigenden $\|\cdot\|_D$-Werten, wird *schwach reduziert* genannt, wenn $\lceil \log_q \|\sum_{i=1}^n \lambda_i\omega_i\|_D \rceil = \max_{i=1}^n \lceil \log_q \|\lambda_i\omega_i\|_D \rceil$ für alle $\lambda_i \in k[x]$, $(1 \le i \le n)$ gilt. Sie heißt *reduziert*, wenn $\|\sum_{i=1}^n \lambda_i\omega_i\|_D = \max_{i=1}^n \|\lambda_i\omega_i\|_D$ für alle $\lambda_i \in k[x]$, $(1 \le i \le n)$ gilt. Es ist klar, daß reduzierte Basen auch schwach reduziert sind. Man kann nun beweisen, daß reduzierte Basen die sukzessiven Minima von Λ_D realisieren und daß es (im Fall der zahmen Verzweigung der Stellen von S über ∞) reduzierte Basen für alle Λ_D gibt [50]. Die Berechnung reduzierter Gitterbasen erfolgt im zahm verzweigten Fall mit dem Reduktionsalgorithmus aus [50]. Hierfür werden Approximationen der Gitterelemente in der Form von Puiseuxreihenentwicklungen verwendet.

2.16. Satz. *Es sei D ein Divisor von F/k und Λ_D das zugehörige Gitter bezüglich k, x. Die schwach reduzierten Basen $\omega_1, \ldots, \omega_n$ von Λ_D entsprechen genau den Elementen $v_1, \ldots, v_n \in F$ aus Satz 2.1. Weiterhin stehen die $k[x]$-Invarianten $|D|_i$ und die Absolutbeträge $\|\omega_i\|_D$ (dies sind die sukzessiven Minima von Λ_D im Fall einer reduzierten Basis) in der Beziehung*

$$|D|_i = -\lceil \log_q \|\omega_i\|_D \rceil.$$

Beweis. Es sei D ein Divisor von F/k und $r \in \mathbb{Z}$. Wir merken als erstes an, daß für $\alpha \in F$ die Bedingungen $\alpha \in \mathcal{L}(D + r(x)_\infty)$ und $\alpha \in \Lambda_D \wedge \log_q \|\alpha\|_D \le r$ äquivalent sind, wie eine leichte Rechnung zeigt.
Es seien $\omega_1, \ldots, \omega_n$ schwach reduziert und $t_i := -\lceil \log_q \|\omega_i\|_D \rceil$. Für beliebiges $\alpha = \sum_{i=1}^n \lambda_i\omega_i$ mit $\lambda_i \in k[x]$ und $r \in \mathbb{Z}$ erhält man wegen der schwachen Reduziertheit der ω_i die folgenden Äquivalenzen:

$$\begin{aligned} \alpha \in \mathcal{L}(D + r(x)_\infty) &\Leftrightarrow \log_q \|\alpha\|_D \le r \\ &\Leftrightarrow \lceil \log_q \|\lambda_i\omega_i\|_D \rceil \le r, \text{ für } 1 \le i \le n, \\ &\Leftrightarrow \deg \lambda_i \le t_i + r, \text{ für } 1 \le i \le n. \end{aligned}$$

Die Eindeutigkeitseigenschaft der $k[x]$-Invarianten von D aus Satz 2.1 ergibt, daß $|D|_i = t_i$ ist und daß die ω_i die Eigenschaft der v_i aus Satz 2.1 besitzen.
Es bleibt zu zeigen, daß beliebige Elemente v_i des Satzes 2.1 schwach reduziert sind. Dafür sei $\alpha = \sum_{i=1}^n \lambda_i v_i$ beliebig und $r \in \mathbb{Z}$ minimal, so daß $\alpha \in \mathcal{L}(D + r(x)_\infty)$ ist. Wegen Satz 2.1 haben wir $\lambda_i v_i \in \mathcal{L}(D + r(x)_\infty)$. Die am Anfang des

Beweises erwähnte Äquivalenz zeigt nun, daß $\log_q \|\alpha\|_D \leq r$ und $\log_q \|\lambda_i v_i\|_D \leq r$ für alle $1 \leq i \leq n$ gilt. Wegen der Minimalität von r erhalten wir daher $r = \lceil \log_q \|\alpha\|_D \rceil \leq \max_{i=1}^{n} \lceil \log_q \|\lambda_i v_i\|_D \rceil \leq r$. □

2.6 Divisorreduktion

Wir knüpfen an die Situation des Abschnitts 2.2 an. Zur Vereinfachung der Notation betrachten wir Grade und Dimensionen nun über dem exakten Konstantenkörper k_0 und setzen $k = k_0$ voraus.

2.17. Definition. Es sei A ein Divisor mit $\deg(A) \geq 1$. Der Divisor $\widetilde{D}$ heißt *maximalreduziert entlang* A, wenn $\widetilde{D} \geq 0$ und $\dim(\widetilde{D} - rA) = 0$ für alle $r \geq 1$ gilt. Die Menge der entlang A maximalreduzierten Divisoren wird mit $\mathcal{D}_{\mathrm{red}}^{\max}(F/k, A)$ bezeichnet. Es sei $m \geq \deg(A)$. Der Divisor $\widetilde{D}$ heißt *m-minimalreduziert entlang* A, wenn $\widetilde{D} \geq 0$, $\dim(\widetilde{D}) \leq m$ und $\dim(\widetilde{D} + rA) > m$ für alle $r \geq 1$ gilt. Die Menge der entlang A m-minimalreduzierten Divisoren wird mit $\mathcal{D}_{\mathrm{red}}^{m}(F/k, A)$ bezeichnet. Die Darstellung eines Divisors D als $D = \widetilde{D} + rA - (a)$ mit einem entlang A maximalreduzierten (m-minimalreduzierten) Divisor $\widetilde{D}$, $r \in \mathbb{Z}$, $a \in F^{\times}$ (und $m \geq \deg(A)$) nennen wir eine *Maximalreduktion (m-Minimalreduktion) von D entlang A*.

Die Eigenschaft eines Divisors, reduziert zu sein, ist zwar an sich nicht besonders interessant, spielt aber wegen ihrer Verwendung bei Berechnungen mit der Divisorenklassengruppe eine wichtige Rolle. Wir bemerken die folgenden weiteren Eigenschaften, wobei das Geschlecht von F/k mit g bezeichnet sei: Für entlang A maximalreduzierte Divisoren $\widetilde{D}$ gilt $\dim(\widetilde{D}) \leq \deg(A)$ und $\deg(\widetilde{D}) < g + \deg(A)$. Für entlang A m-minimalreduzierte Divisoren $\widetilde{D}$ gilt $\deg(\widetilde{D}) < g + m$.

Für eine m-Minimalreduktion $D = \widetilde{D}_1 + rA - (a)$ haben alle weiteren m-Minimalreduktionen den gleichen Grad und werden durch $\widetilde{D}_2 := (b) + \widetilde{D}_1$ für $b \in \mathcal{L}(\widetilde{D}_1)$ gebildet. Analoges gilt für die Maximalreduktionen. Man sieht daher, daß die m-Minimal- und Maximalreduktionen entlang A mittels einer Basis von $\mathcal{L}(\widetilde{D}_1)$ in eine 1-1-Beziehung zu den Punkten des projektiven Raums $\mathbb{P}^{\dim(\widetilde{D}_1)}(k)$ gesetzt werden können (in der algebraischen Geometrie werden diese auch „vollständige lineare Reihen“ genannt). Aus diesen Überlegungen folgt

2.18. Proposition. *Es sei A ein Divisor mit* $\deg(A) = 1$. *Die Maximalreduktion eines Divisors D entlang A ist dann eindeutig. Anders ausgedrückt: Für jede Divisorenklasse $[D]$ gibt es genau einen entlang A maximalreduzierten Divisor $\widetilde{D}$ und ein eindeutig bestimmtes $r \in \mathbb{Z}$ mit $[D] = [\widetilde{D} + rA]$.*

Beweis. Wir berechnen $[D-rA]$ mit dem maximal möglichen, eindeutig bestimmten $r \in \mathbb{Z}$, so daß $\dim\big([D-rA]\big) = 1$ ist. Die Klasse $[D-rA]$ enthält einen einzigen, positiven Divisor $\widetilde{D}$, welcher entlang A maximalreduziert ist. Damit ist $\widetilde{D}+rA$ ein eindeutiger Repräsentant von $[D]$. Die Eindeutigkeit von (a) ergibt sich wegen $(a) = \widetilde{D}+rA-D$. □

Ähnlich wie im Beweis der Proposition wollen wir nun die Schritte für eine Reduktion von Divisoren in freier Darstellung erläutern. Dies wird bei der Berechnung von Riemann-Roch-Räumen von Divisoren großer Höhe oder großen Grads eine wirksame Hilfe sein.

Vorgegeben sei ein beliebiger Divisor A kleiner Höhe und kleinen Grads; beispielsweise ein Primdivisor vom Grad eins, falls existent. Einen Divisor D mit großen Exponenten schöpfen wir mittels A aus. Dies soll heißen, daß wir ein (möglichst) großes Vielfaches von A von D subtrahieren, so daß $D-rA$ noch eine Dimension größer null besitzt. Hierbei kann r für einen Divisor negativen Grads selbst negativ sein. Mit diesem Vorgehen können wir erreichen, daß $\widetilde{D} = (a)+D-rA$ für $a \in \mathcal{L}(D-rA)$ ein entlang A maximalreduzierter, ein m-minimalreduzierter oder nur ein im Grad beschränkter, positiver Divisor wird. Speziell hat man dann $D = \widetilde{D}+rA-(a)$ und $\mathcal{L}(D) = a \cdot \mathcal{L}(\widetilde{D}+rA)$.
Wir machen zwei Beobachtungen: Erstens, ist a bekannt, so bestimmt man daraus $\widetilde{D}$ in Idealdarstellung, um Faktorisierung zu vermeiden. Zweitens, die Berechnung von a und $\widetilde{D}$ ist weiterhin schwierig, da $h(D-rA)$ im allgemeinen nicht klein im Vergleich zu $h(D)$ ist. Die hier explizit verwendete Darstellung von D durch $\widetilde{D}$ nennen wir *Elementarreduktion entlang* A, über die Wahl von r verfügen wir später. Die Elementarreduktion sollte also nur für Divisoren kleiner Höhe ausgeführt werden.

Es gibt nun eindeutige Divisoren $D_0, \ldots, D_m$, so daß $D = \sum_{i=0}^{m} 2^i D_i$ gilt und die Exponenten in den D_i betraglich eins sind. Die Anzahl der in D_i auftretenden Stellen sollte nicht zu groß sein. Wir evaluieren diese Summe nach dem Hornerschema, wobei vor jeder Multiplikation eine Elementarreduktion durchgeführt wird. Mit $\widetilde{D}_{m+1} := 0$ nehmen wir für $-1 \le j < m$ induktiv an, daß

$$D = 2^{m-j}\widetilde{D}_{m-j} + \sum_{i=0}^{m-j-1} 2^i D_i + A \sum_{i=m-j}^{m} 2^i r_i - \sum_{i=m-j}^{m} 2^i (a_i)$$

gilt. Durch eine Elementarreduktion von $2\,\widetilde{D}_{m-j} + D_{m-j-1}$ erhalten wir die Darstellung $2\,\widetilde{D}_{m-j} + D_{m-j-1} = \widetilde{D}_{m-j-1} + r_{m-j-1}A - (a_{m-j-1})$ desselbigen. Durch Einsetzen dieses Ausdrucks sieht man, daß die Darstellung von D mit j auch für

$j+1$ gilt. Daraus ergibt sich für $j = m$:

$$D = \widetilde{D}_0 + A\sum_{i=0}^{m} 2^i r_i - \sum_{i=0}^{m} 2^i(a_i) \tag{2.19}$$

Die Größe der Exponenten von D geht jetzt nur noch logarithmisch ein. Problematisch bleibt weiterhin die Anzahl der in den einzelnen D_i auftretenden Stellen. Hier summiert man die Stellen aus D_i sukzessive auf und erhält nach jedem Schritt Teildivisoren in Idealdarstellung, auf die man die Elementarreduktion anwendet. Die Anzahl der Stellen geht dann zwar weiterhin linear in die Laufzeit ein, das Anwachsen der Höhen wird jedoch vermieden. Wir schreiben also $D_i = D_i' + l_i A - \sum_{j=1}^{t}(b_{i,j})$, wobei t die Anzahl der in D auftretenden Stellen und D_i' reduziert ist, setzen dies in $\sum_{i=0}^{m} 2^i D_i$ ein und wenden das Vorgehen für (2.19) auf $\sum_{i=0}^{m} 2^i D_i'$ an. Zusammenfassend erhält man:

$$D = \widetilde{D}_0 + A\sum_{i=0}^{m} 2^i(r_i + l_i) - \sum_{i=0}^{m} 2^i\left((a_i) + \sum_{j=1}^{t}(b_{i,j})\right) \tag{2.20}$$

Wir kommen auf die Wahl von r in der Elementarreduktion zu sprechen. Man kann zwei Strategien unterscheiden, wobei weitere denkbar sind: Gradreduktion und Maximalreduktion entlang A. Die Gradreduktion liefert einen im Grad beschränkten, positiven Divisor $\widetilde{D}$, wohingegen die Maximalreduktion einen entlang A maximalreduzierten Divisor $\widetilde{D}$ ergibt. Bei der Gradreduktion bestimmt man also $D - rA$ mit einem maximalen $r \in \mathbb{Z}$, so daß $g \leq \deg(D - rA) < g + \deg(A)$ gilt. Dann hat man auf jeden Fall positive, eventuell relativ große Dimension, und für die reduzierten Divisoren $\widetilde{D}$ gilt ebenfalls $g \leq \deg(\widetilde{D}) < g + \deg(A)$. Diese Reduktion ist nicht eindeutig. Bei der Maximalreduktion bestimmt man wie im Beweis der Proposition 2.18 $D - rA$ mit einem maximalen $r \in \mathbb{Z}$, so daß $0 < \dim(D - rA) \leq \deg(A)$ gilt. Dann hat man $\deg(\widetilde{D}) < g + \deg(A)$, der Grad kann also auch kleiner als g sein. Für einen Divisor A vom Grad eins ist diese Reduktion eindeutig. Beide Reduktionsarten stimmen für vorgelegte Divisoren häufig überein.

Wir fassen das Vorgehen in einem Algorithmus zusammen:

2.21. Algorithmus. *(Divisorreduktion)*

Eingabe: *Divisoren A, D des algebraischen Funktionenkörpers F/k, wobei D in freier Darstellung und $\deg(A) > 0$ ist, und eine Strategie für die Elementarreduktion.*

Ausgabe: *Ein positiver Divisor $\widetilde{D}$ mit $\deg(\widetilde{D}) < g + \deg(A)$, in Idealdarstellung gegeben, ein $r \in \mathbb{Z}$ und Elemente $a_i, b_{i,j} \in F^\times$, so daß $D = \widetilde{D} + rA - \sum_{i=0}^{m} 2^i\big((a_i) + \sum_{j=1}^{t}(b_{i,j})\big)$ mit $t := |\mathrm{supp}(D)|$ gilt.*

1. *(Zerlegung von D) Berechne $m \in \mathbb{Z}$ und Divisoren $D_0, \ldots, D_m$, deren Exponenten betraglich eins sind und für die $D = \sum_{i=0}^{m} 2^i D_i$ gilt.*

2. *(Trägerreduktion) Für jedes $i := 0, \ldots, m$ wird D_i' sukzessive in Idealdarstellung aufgebaut, wobei nach jeder Addition beziehungsweise Subtraktion eines Primdivisors von D_i eine Elementarreduktion erfolgt. Dies liefert $D_i = D_i' + l_i A - \sum_{j=1}^{t}(b_{i,j})$.*

3. *(Exponentenreduktion) Es sei $\widetilde{D}_{m+1} := 0$. Berechne für $j := -1, \ldots, m-1$ einen Divisor $\widetilde{D}_{m-j-1}$ in Idealdarstellung, ein $r_{m-j-1} \in \mathbb{Z}$ und $a_{m-j-1} \in F$ mittels der Elementarreduktion angewendet auf $2\,\widetilde{D}_{m-j} + D'_{m-j-1}$, so daß $2\,\widetilde{D}_{m-j} + D'_{m-j-1} = \widetilde{D}_{m-j-1} + r_{m-j-1}A - (a_{m-j-1})$ gilt.*

4. *(Ende) Setze $\widetilde{D} := \widetilde{D}_0$ und $r := \sum_{i=0}^{m} 2^i(r_i + l_i)$. Ausgabe von $\widetilde{D}$, r und $a_i, b_{i,j}$. Terminiere.*

2.22. Bemerkung. Die Größe der Exponenten geht logarithmisch und die Anzahl der Stellen von D linear in die Laufzeit ein. Letzteres gilt, weil die Höhe der D_i' wegen der Reduktion in Abhängigkeit von $\deg(A)$ ständig beschränkt wird. Insgesamt gibt es also $\alpha, \beta \in \mathbb{R}^{>0}$, so daß Algorithmus 2.21 eine Laufzeit $\leq \beta \log(h(D))\,|\mathrm{supp}(D)|\,(nC_f \deg(A)d)^{\alpha}$ benötigt, wobei d der maximale Grad der in D auftretenden Stellen ist. Die Elementarreduktion läßt sich in der Praxis besonders günstig für $A = (x)_\infty$ durchführen.

2.23. Bemerkung. Wird ein Divisor A mit $\deg(A) = 1$ gewählt und als Strategie für die Elementarreduktion die Maximalreduktion verwendet, so liefert Algorithmus 2.21 für jeden Divisor D die eindeutige Maximalreduktion von D entlang A (weil im letzten Schritt eine Maximalreduktion durchgeführt wird). Man kann so eindeutige Repräsentanten für Divisorenklassen berechnen. Wählt man im Fall eines globalen Funktionenkörpers über dem exakten Konstantenkörper mit q Elementen ein A größeren Grads, so erhält man maximal $(q^{\deg(A)}-1)/(q-1)$ Möglichkeiten für eine Maximalreduktion $\widetilde{D}$, also eine „beschränkte“ Mehrdeutigkeit.

2.24. Bemerkung. Die Berechnung aller m-Minimalreduktionen eines Divisors D entlang A wird ebenfalls auf Algorithmus 2.21 zurückgeführt. Man bestimmt zunächst die Maximalreduktion $D = \widetilde{D} + rA + (a)$ und sucht dann (binäre Suche möglich) das maximale j mit $\dim(\widetilde{D} + jA) \leq m$, wobei $0 \leq j \leq \lfloor (g + m - 1 - \deg(\widetilde{D}))/\deg(A) \rfloor$ gilt. Man erhält damit einen Vertreter der m-Minimalreduktionen modulo Hauptdivisoren, die anderen ergeben sich entsprechend der Bemerkungen vor Proposition 2.18. Im Fall eines globalen Funktionenkörpers lassen sich die einzelnen m-Minimalreduktionen sogar direkt aufzählen, ihre Anzahl beträgt nämlich maximal $(q^m - 1)/(q - 1)$, $q = |k|$.

2.7 Riemann-Roch-Raum-Berechnung II

Mit Hilfe der Divisorreduktion des vorigen Abschnitts und der Beziehung $\mathcal{L}(D) = a \cdot \mathcal{L}(\widetilde{D} + rA)$ für $D = \widetilde{D} + rA - (a)$ können wir nun Riemann-Roch-Räume auch für „große“ Divisoren berechnen. Dazu beachten wir zwei Dinge: Enthält der Divisor D große Exponenten, hat dabei aber einen kleinen Grad, so sollte die Berechnung von $\mathcal{L}(\widetilde{D} + rA)$ mit der Divisorreduktion $D = \widetilde{D} + rA - (a)$ kein Problem darstellen, weil die Dimension ebenfalls klein ist. Bei großem Grad von D ist aber auch die Dimension groß, die Angabe einer Basis könnte Schwierigkeiten bereiten. Doch auch dies stellt nach Satz 2.1 kein Problem dar, wenn $A = (x)_\infty$ gilt. Die Basiselemente können in diesem Fall parametrisch angegeben werden. Daraus ergibt sich

2.25. Algorithmus. *(Riemann-Roch-Raum-Berechnung II)*

Eingabe: *Ein Divisor D des algebraischen Funktionenkörpers F/k.*

Ausgabe: *Eine k-Basis von $\mathcal{L}(D)$ in kurzer Darstellung wie in Satz 2.1, wobei die Basiselemente v_i durch Potenzprodukte von Elementen aus $F^\times$ gegeben sind.*

1. *(Reduktion) Führe unter Verwendung von $A = (x)_\infty$ und der Gradreduktion eine Divisorreduktion von D gemäß Algorithmus 2.21 durch, wir erhalten $\widetilde{D}$, $r \in \mathbb{Z}$ und $a \in F^\times$ mit $D = \widetilde{D} + rA - (a)$, wobei a das Potenzprodukt der a_i und $b_{i,j}$ ist.*

2. *(Riemann-Roch) Berechne mittels Algorithmus 2.7 eine Basis von $\mathcal{L}(\widetilde{D})$ in kurzer Darstellung, gegeben durch $v'_1, \ldots, v'_n$ und $d'_1, \ldots, d'_n$.*

3. *(Ende) Setze $v_j := av'_j$, $d_j := d'_j + r$ für $j := 1, \ldots, n$. Ausgabe von $v_1, \ldots, v_n$ und $d_1, \ldots, d_n$. Terminiere.*

2.26. Bemerkung. Gemäß Bemerkung 2.22 ist der Aufwand für diesen Algorithmus von derselben Form wie der für Algorithmus 2.21.

2.8 Weitere Methoden zur Berechnung von Riemann-Roch-Räumen

Wir wollen in diesem Abschnitt alternative Formen der Berechnung von Riemann-Roch-Räumen diskutieren beziehungsweise erwähnen.

Aufgrund von Satz 2.16 läßt sich der Riemann-Roch-Raum eines Divisors auch aus einer reduzierten Basis des Gitters Λ_D und seinen sukzessiven Minima bestimmen. Zu den Vorteilen dieser Methode: Eine reduzierte Basis enthält mehr Information als eine schwach reduzierte Basis, und zwar die Information über das Verzweigungsverhalten der Stellen über ∞. Die Folge hiervon ist, daß Satz 2.1 nun für „verallgemeinerte" Divisoren $D+r(x)_\infty$ mit $r \in \mathbb{R}$ und rationalen $k[x]$-Invarianten ausgesprochen werden kann. Wir bemerken, daß sich dies günstig auf die Maximalreduktion von Divisoren entlang $(x)_\infty$ auswirkt (das gesuchte r ist nun nämlich rational, so daß auch Teildivisoren von $(x)_\infty$ spezifiziert werden können).
Zu den Nachteilen zählt, daß die Gitterreduktion Approximationen verwendet. Um korrekte Ergebnisse zu erhalten, ist daher die Verwendung einer ausreichenden Präzision beziehungsweise die Durchführung einer Fehleranalyse unerläßlich. Abgesehen von Präzisionsfragen ist die Gittermethode von der mathematischen und von der programmiertechnischen Seite her aufwendiger. Während nur im Fall der zahmen Verzweigung Puiseuxreihenentwicklungen zur Verfügung stehen, werden ansonsten allgemeinere P-adische beziehungsweise Hamburger-Noether Reihen benötigt. Schließlich dürfte es Probleme bereiten, bei der Riemann-Roch-Raum-Berechnung auch diskrete Bewertungen des Konstantenkörpers zu berücksichtigen. Dies ist bei der hier beschriebenen, symbolischen Methode möglich und wird in Abschnitt 2.10 behandelt.

Zur Riemann-Roch-Raum-Berechnung und zu ihren Anwendungen, siehe nächster Abschnitt, gibt es ferner Methoden, die von der Seite der algebraischen Geometrie inspiriert werden [6, 20, 57, 58]. Diese basieren auf dem Brill-Noether Algorithmus und verwenden ebenfalls Reihenentwicklungen.

2.9 Anwendungen

Der Satz von Riemann-Roch dominiert die gesamte Theorie der algebraischen Funktionenkörper (einer Variablen). Entsprechend umfangreich sind die Anwendungsgebiete konstruktiver Verfahren der Riemann-Roch-Theorie. Wir wollen ein paar Beispiele erwähnen.

Die Konstruktion *algebraisch-geometrischer Codes* kann mit Hilfe von Basen von Riemann-Roch-Räumen und auch von Basen von Divisoren zugeordneten Differentialräumen erfolgen, vgl. [55].

Die Berechnung von *Differentialräumen* $\Omega(D)$ selbst kann ebenfalls auf die Berechnung von Riemann-Roch-Räumen zurückgeführt werden. Der Funktionenkörper F/k über dem vollkommenen Körper k werde durch $f(x,y) = 0$ definiert, wobei $f(x,y) \in k[x,y]$ in y normiert, separabel und irreduzibel ist. Wir deu-

ten das Vorgehen nur grob an. Durch Anwendung des Differentialoperators d auf $f(x,y) = 0$ erhält man nach den Differentiationsregeln eine F-lineare Relation zwischen dy und dx:

$$dy = -\frac{f_x}{f_y} dx,$$

wobei der Nenner ungleich null nach Voraussetzung an $f(x,y)$ ist (f_x und f_y sind die partiellen Ableitungen nach x und y). Ein beliebiges Element a von F läßt sich als rationale Funktion in x, y darstellen. Durch Anwenden von d auf a in dieser Darstellung und unter Beachtung der Relation zwischen x und y erhält man dann ein $b \in F$ mit $da = b\,dx$. Man weiß, daß sich jedes Differential als $b\,dx$ für ein $b \in F$ darstellen läßt. Der Divisor des Differentials $b\,dx$ ist $(b\,dx) = (b) + (dx)$, wobei $(dx) = \mathcal{D}_{F/k(x)} - 2(x)_\infty$ gilt, siehe [55, S. 156 (3.16)]. Den Differentendivisor können wir wie üblich leicht mit Hilfe der Spurenmatrizen berechnen [9, S. 203, 4.8.18]. Insgesamt sind wir also in der Lage, den Divisor eines beliebigen Differentials zu bestimmen. Andererseits sieht man auch, daß für einen Divisor D die Ungleichung $(b\,dx) \geq D$ genau dann gilt, wenn $(b) + (dx) - D \geq 0$ ist. Diese Äquivalenz liefert einen k-Vektorraumisomorphismus $\Omega(D) \longrightarrow \mathcal{L}((dx) - D)$, mit dessen Hilfe wir dann schließlich eine k-Basis von $\Omega(D)$ berechnen können.

Eine weitere, wichtige Anwendung liegt in der Möglichkeit, in der *Divisorenklassengruppe* eines algebraischen Funktionenkörpers explizit zu rechnen. Sind zwei Divisorenklassen $[D_1]$ und $[D_2]$ gegeben, so gilt trivialerweise $[D_1] + [D_2] = [D_1 + D_2]$ und $k[D_1] = [kD_1]$. Es stellt sich aber die Frage, wann zwei Klassen gleich beziehungsweise wann eine Klasse die Hauptklasse ist. Gleichheit von $[D_1]$ und $[D_2]$ gilt genau dann, wenn $\deg(D_1) = \deg(D_2)$ und $\dim(D_1 - D_2) > 0$ ist, und dieser „Hauptdivisortest“ kann mit den beschriebenen Methoden in einfacher und effizienter Weise durchgeführt werden. Wir merken zusätzlich an, daß wegen Bemerkung 2.23 auch eindeutige Repräsentanten selektiert werden können.

Schließlich spielt die Riemann-Roch-Raum-Berechnung bei der Erzeugung von Relationen für die *Klassengruppenberechnung* eines globalen Funktionenkörpers eine zentrale Rolle. Darauf kommen wir aber in Kapitel 5 noch eingehend zu sprechen.

2.10 Zusätzliche Bewertungsbedingungen

In den vorangegangenen Abschnitten haben wir diskrete Bewertungen des Konstantenkörpers, falls vorhanden, unberücksichtigt gelassen. Dies soll nun wiederum in einer idealtheoretischen Weise nachgeholt werden. Die Ergebnisse dieses Abschnitts werden konstruktiv, aber theoretisch dargestellt; wir geben keine ex-

pliziten Algorithmen an. Es werden Methoden der Theorie der Moduln über Dedekindringen Verwendung finden, für die wir beispielsweise auf [10] verweisen.

2.10.1 Ein weiterer Grundring

Es sei R ein Dedekindring und k der Quotientenkörper von R. Der *Inhalt* $\mathrm{cont}(g)$ eines Polynoms $g \in k[x]$ wird definiert als der größte gemeinsame Teiler der von den Koeffizienten von g erzeugten Hauptideale. Es handelt sich hierbei um ein (gebrochenes) Ideal von R. Diese Definition wird auf ganz $k(x)$ durch die Setzung $\mathrm{cont}(g/h) := \mathrm{cont}(g)/\mathrm{cont}(h)$ für $g, h \in k[x]$ ausgedehnt. Die Inhaltsfunktion besitzt drei Eigenschaften:

(i) $\mathrm{cont}(g) = \{0\} \Leftrightarrow g = 0$,

(ii) $\mathrm{cont}(gh) = \mathrm{cont}(g)\mathrm{cont}(h)$,

(iii) $\gcd\big(\mathrm{cont}(g), \mathrm{cont}(h)\big) \,|\, \mathrm{cont}(g+h)$ für alle $g, h \in k(x)$.

Man sagt, eine rationale Funktion habe ganzen Inhalt, wenn ihr Inhalt ein ganzes Ideal von R ist.

Unter Verwendung eines *festen*, separierenden Elements x erweitern wir nun R nach $k(x) \subseteq F$, indem wir $R\langle x\rangle$ als den Ring der rationalen Funktionen mit ganzem Inhalt definieren. Dieser Ring wird die Rolle eines weiteren Grundrings analog wie $k[x]$ und $\mathfrak{o}_\infty$ spielen.

2.27. Proposition. *Der Ring $R\langle x\rangle$ ist ein Hauptidealring und die Idealgruppen von R und $R\langle x\rangle$ sind isomorph unter $\mathfrak{a} \mapsto R\langle x\rangle\mathfrak{a}$. Die Umkehrabbildung hiervon ist $\mathfrak{b} \mapsto \mathfrak{b} \cap k$.*

Beweis. Es sei $\mathfrak{a}$ ein Ideal von R mit Erzeugern $a_0, \ldots, a_n \in \mathfrak{a}$. Das Ideal $R\langle x\rangle\mathfrak{a}$ stellt ein von $a := a_n x^n + \cdots + a_0$ erzeugtes Hauptideal $R\langle x\rangle a$ dar, weil $\mathrm{cont}(a) = \mathfrak{a}$ gilt und die Inhalte aller Elemente von $R\langle x\rangle\mathfrak{a}$ durch $\mathfrak{a}$ teilbar sind. Im Bildbereich von $\mathfrak{a} \mapsto R\langle x\rangle\mathfrak{a}$ liegen also nur Hauptideale.
Es sei $b \in R\langle x\rangle$. Für jedes $\lambda \in \mathrm{cont}(b)$ haben wir $\lambda/b \in R\langle x\rangle$, folglich $\lambda \in R\langle x\rangle b$, so daß $\mathrm{cont}(b) \subseteq R\langle x\rangle b$ gilt. Weil $R\langle x\rangle\mathrm{cont}(b)$ ein Hauptideal ist und einen Erzeuger desselben Inhalts wie b wegen des vorangegangenen Absatzes besitzt, sind beide Erzeuger assoziiert (unterscheiden sich nur um Einheiten) und es gilt $R\langle x\rangle\mathrm{cont}(b) = R\langle x\rangle b$. Im Bildbereich von $\mathfrak{a} \mapsto R\langle x\rangle\mathfrak{a}$ liegen also alle Hauptideale von $R\langle x\rangle$.
Die Abbildung $\mathfrak{a} \mapsto R\langle x\rangle\mathfrak{a}$ ist sicherlich multiplikativ, additiv und inklusionserhaltend. Nach den beiden letzten Absätzen erhalten wir eine Isomorphie der Idealgruppe von R zur Gruppe der Hauptideale von $R\langle x\rangle$. Die Abbildung $\mathfrak{b} \mapsto \mathfrak{b} \cap k$ ist für Hauptideale $\mathfrak{b}$ von $R\langle x\rangle$ dann tatsächlich die Umkehrabbildung.

Es bleibt zu zeigen, daß jedes ganze Ideal $\mathfrak{b}$ von $R\langle x\rangle$ ein Hauptideal ist. Wir setzen $\mathfrak{a} := \sum_{b\in\mathfrak{b}} \mathrm{cont}(b)$. Dies ist ein ganzes Ideal von R und es gilt $R\langle x\rangle\mathfrak{a} = \mathfrak{b}$, weshalb $\mathfrak{b}$ ein Hauptideal sein muß. □

Wir merken an, daß jedes Ideal $\mathfrak{a}$ von R wegen des Chinesischen Restsatzes als die Summe zweier Hauptideale dargestellt werden kann. Daher sieht man, daß sich jedes Ideal von $R\langle x\rangle$ bereits durch ein einzelnes Element von R oder ein Polynom in $R[x]$ vom Grad eins erzeugen läßt.

Eine *Gaußsche* Bewertung auf $k(x)$ ensteht aus einer diskreten Bewertung von k, welche wir zuerst auf $k[x]$ als das Minimum der Bewertungen der Koeffizienten eines gegebenen Polynoms definieren, und danach auf $k(x)$ als Differenz der Bewertung des Zählers und der Bewertung des Nenners einer rationalen Funktion fortsetzen.

Die Primideale von R definieren diskrete Bewertungen von k und wir bemerken, daß $R\langle x\rangle$ auch als Ring derjenigen rationalen Funktionen von $k(x)$ beschrieben werden kann, deren Gaußsche Bewertungen für alle Primideale von R sämtlich nicht negativ sind.

2.28. Beispiel. Die Elemente $a \in \mathbb{Z}\langle x\rangle$, $a \neq 0$ lassen sich in der Form $a = cf/g$ normieren, wobei $f, g \in \mathbb{Z}[x]$ teilerfremde Polynome des Inhalts eins sind, g einen positiven Leitkoeffizienten besitzt und $c \in \mathbb{Z}^{\geq 1}$ ist. Bewertungen von a lassen sich dann an c ablesen, denn f/g ist eine Einheit in $\mathbb{Z}\langle x\rangle$. Ähnliches kann man auch im Fall geeigneter Hauptidealringe R tun.

2.10.2 Der ganze Abschluß von $R\langle x\rangle$ in F

Der ganze Abschluß von $R\langle x\rangle$ im Funktionenkörper F ist ein freier $R\langle x\rangle$-Modul des Rangs n, weil wir uns gemäß Proposition 2.27 in der Situation eines endlich erzeugten, torsionsfreien Moduls über einem Hauptidealring befinden. Eine Ganzheitsbasis von $\mathrm{Cl}\big(R\langle x\rangle, F\big)$ kann im Prinzip mittels des *Round-2*-Algorithmus berechnet werden (welcher beispielsweise in [9] und [17] beschrieben wird). Wir gehen hierauf aber nicht näher ein.

2.29. Beispiel. Für $R = \mathbb{Z}$ und $k = \mathbb{Q}$ betrachten wir den durch $f(x, y) = y^2 - 4x^3 - 1$ erzeugten Funktionenkörper $F = k(x, \rho)$ mit $f(x, \rho) = 0$. Wir suchen $\mathrm{Cl}\big(\mathbb{Z}\langle x\rangle, F\big)$. Unter Verwendung der Spur und Norm beliebig angesetzter Elemente sieht man wie im Fall quadratischer Zahlkörper, daß wegen der Gestalt von f $\mathrm{Cl}\big(\mathbb{Z}\langle x\rangle, F\big) = \mathbb{Z}\langle x\rangle[(1+\rho)/2]$ gilt.

2.10.3 Zusätzliche Bedingungen an Elemente aus $\mathcal{L}(D)$

Im Abschnitt 2.1 haben wir $\mathcal{L}(D)$ als den Schnitt von Idealen $(D^S)^{-1}$ und $(D_S)^{-1}$ von $\mathfrak{o}^S$ beziehungsweise $\mathfrak{o}_S$ betrachtet. Durch Schnittbildung von $\mathcal{L}(D)$ mit einem passend gewählten Ideal $\mathfrak{a}$ von $\mathrm{Cl}\big(R\langle x\rangle, F\big)$ können wir zusätzlich erreichen, daß die Fortsetzungen Gaußscher Bewertungen von $k(x)$ auf F auf den Elementen des Durchschnitts vorgegebene Mindestwerte überschreiten.

2.30. Lemma. *Es sei D ein Divisor von F/k und $\mathfrak{a}$ ein Ideal von $\mathrm{Cl}(R\langle x\rangle, F)$. Dann ist $\mathcal{L}(D) \cap \mathfrak{a}$ ein R-Modul. Es gibt Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_l$ von R und Elemente $u_1, \ldots, u_l \in F$ mit $l := \dim_k D$, so daß gilt:*

$$\mathcal{L}(D) \cap \mathfrak{a} = \mathfrak{b}_1 u_1 \dotplus \ldots \dotplus \mathfrak{b}_l u_l.$$

Beweis. Weil $\mathcal{L}(D)$ ein k-Vektorraum, $\mathfrak{a}$ ein $R\langle x\rangle$-Modul und $k \cap R\langle x\rangle = R$ ist, sehen wir, daß $\mathcal{L}(D) \cap \mathfrak{a}$ ein R-Modul ist. Nun sei $v_1, \ldots, v_l$ eine k-Basis von $\mathcal{L}(D)$ und $z_1, \ldots, z_n$ eine $R\langle x\rangle$-Basis von $\mathfrak{a}$. Es gibt eine Matrix $M \in R[x]^{n\times l}$ und einen gemeinsamen Nenner $d \in R[x]$ mit

$$(z_1, \ldots, z_n) d^{-1} M = (v_1, \ldots, v_l).$$

Zur Bestimmung des Schnitts $\mathcal{L}(D) \cap \mathfrak{a}$ verwenden jetzt wir eine Reihe von äquivalenten Bedingungen. Es sei $\mathfrak{d}$ das Ideal von R mit $\mathfrak{d}R\langle x\rangle = dR\langle x\rangle$ und $a = (v_1, \ldots, v_l)\lambda$ mit $\lambda = (\lambda_i)_i \in k^l$. Dann gilt

$$\begin{aligned} a \in \mathcal{L}(D) \cap \mathfrak{a} &\Leftrightarrow d^{-1} M\lambda \in R\langle x\rangle^n, \\ &\Leftrightarrow M\lambda \in \mathfrak{d}R\langle x\rangle^n. \end{aligned}$$

Wir ersetzen nun jede Zeile von M durch mehrere, aber endlich viele neue Zeilen, und erhalten eine neue Matrix M': Fixiere eine Zeile $\left(\sum_i \gamma_{i,j} x^i\right)_j \in k[x]^{1\times l}$ mit $\gamma_{i,j} \in k$. Diese wird durch $(\gamma_{i,j})_{i,j}$ ersetzt, wobei hierin noch Nullzeilen gestrichen werden. Wir haben dann $M' \in R^{m\times l}$ mit $m \geq l$, denn M und M' haben l k-linear unabhängige Spalten. Die letzte, obige Bedingung für λ liest sich nun

$$a \in \mathcal{L}(D) \cap \mathfrak{a} \Leftrightarrow M'\lambda \in \mathfrak{d}^m.$$

Bezeichnen wir den von den Zeilen von M' erzeugten R-Modul mit V. Durch Berechnung der relativen Hermite-Normalform, siehe beispielsweise [10], für die Zeilen von M' erhalten wir Ideale $\mathfrak{b}'_1, \ldots, \mathfrak{b}'_l$ und unabhängige Zeilen $s_1, \ldots, s_l \in k^{1\times l}$, so daß $V = \mathfrak{b}'_1 s_1 \dotplus \ldots \dotplus \mathfrak{b}'_l s_l$ gilt. Es seien S die Matrix bestehend aus den Zeilen $s_1, \ldots, s_l$, $s'_1, \ldots, s'_l$ die Spalten von S^{-1} und definiere $\mathfrak{b}_i := \mathfrak{d}/\mathfrak{b}'_i$ für alle $1 \leq i \leq l$. Die Äquivalenzenkette läßt sich damit wie folgt weiterführen:

$$\begin{aligned} a \in \mathcal{L}(D) \cap \mathfrak{a} &\Leftrightarrow v\lambda \in \mathfrak{d}, \quad (v \in V), \\ &\Leftrightarrow \lambda \in \mathfrak{b}_1 s'_1 \dotplus \ldots \dotplus \mathfrak{b}_l s'_l. \end{aligned}$$

Die Basiselemente u_i erhält man also durch $u_i = (v_1, \ldots, v_l)s'_i$ für $1 \leq i \leq l$. □

2.10.4 Schnitt von $\mathrm{Cl}\big(k[x], F\big)$- mit $\mathrm{Cl}\big(R\langle x\rangle, F\big)$-Idealen

Es sei $\mathfrak{a}$ ein Ideal von $\mathrm{Cl}\big(k[x], F\big)$ und $\mathfrak{b}$ ein Ideal von $\mathrm{Cl}\big(R\langle x\rangle, F\big)$. In diesem Abschnitt soll die Struktur und eine Möglichkeit zur Berechnung von $\mathfrak{a} \cap \mathfrak{b}$ beschrieben werden. Wir zitieren eine Proposition, die üblicherweise „Euklidischer Schritt“ in Matrix-Normalform-Berechnungen über Dedekindringen genannt wird.

2.31. Proposition. *Es seien v_1, v_2 linear unabhängige Elemente eines k-Vektorraums V und $\mathfrak{a}_1, \mathfrak{a}_2$ Ideale von R. Dann gibt es $\lambda \in \mathfrak{a}_1/(\mathfrak{a}_1 + \mathfrak{a}_2) \subseteq R$ und $\mu \in \mathfrak{a}_2/(\mathfrak{a}_1 + \mathfrak{a}_2) \subseteq R$ mit $\lambda + \mu = 1$, so daß gilt:*

$$\mathfrak{a}_1 v_1 \dot{+} \mathfrak{a}_2 v_2 = (\mathfrak{a}_1 + \mathfrak{a}_2)(\lambda v_1 + \mu v_2) \dot{+} (\mathfrak{a}_1 \cap \mathfrak{a}_2)(v_1 - v_2).$$

Beweis. Siehe beispielsweise [10]. □

Das folgende Lemma entspricht dem Korollar 1.7.

2.32. Lemma. *Es sei $M \in k(x)^{n\times n}$ regulär. Dann gibt es ein $U \in R\langle x\rangle^{n\times n}$ und ein $V \in k[x]^{n\times n}$ mit $\det U \in R\langle x\rangle^{\times}$ und $\det V \in k^{\times}$, so daß $UMV \in k[x]^{n\times n}$ diagonal ist.*

Beweis. Wir nehmen an, daß M sich in unterer triangulärer Gestalt befindet. Dies kann beispielsweise dadurch erreicht werden, daß M in die untere Spalten-Hermite-Normalform gebracht wird (bezüglich eines gemeinsamen Nenners, $k[x]$ ist Euklidisch).
Wir beweisen die Diagonalisierbarkeit von M zuerst für $n = 2$ und setzen voraus, daß sich $M \in k[x]^{2\times 2}$ mit gemeinsamen Nenner $h \in k[x]$ tatsächlich in unterer Spalten-Hermite-Normalform befindet. Wir führen jetzt eine induktive Schlußweise über endlich viele $j \in \mathbb{Z}^{\geq 1}$ für geeignet konstruierte Ideale $\mathfrak{a}_j, \mathfrak{c}_j$ von $R\langle x\rangle$, Elemente $a_j, c_j, d_j \in k[x]$ und $R\langle x\rangle$-Moduln $U_j := \mathfrak{a}_j(a_j, 0) + \mathfrak{c}_j(c_j, d_j)$ durch. Für $j = 1$ sei $\mathfrak{a}_1 := \mathfrak{c}_1 := R\langle x\rangle$ und

$$\begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix} := M.$$

Durch die nachfolgende Konstruktion weisen wir die Existenz eines $r \in \mathbb{Z}^{\geq 1}$ nach, für welches $c_r = 0$ gilt und ein $T \in k[x]^{2\times 2}$ mit $\det(T) \in k^{\times}$ und $U_r = U_1 T$ existiert. Wir können dann $a' \in k[x]$, und analog c', als das Produkt von a_r und einem Erzeuger von $\mathfrak{a}_r$ definieren. Damit gilt dann

$$U_r = R\langle x\rangle(a', 0) + R\langle x\rangle(0, c') = U_1 T.$$

Weil sich zwei Basen von U_r durch eine $R\langle x\rangle$-unimodulare Transformation unterscheiden, sehen wir schließlich, daß die Diagonalmatrix $M' \in k[x]^{2\times 2}$ mit a', c' auf der Diagonalen durch $R\langle x\rangle$-unimodulare Zeilen- und $k[x]$-unimodulare Spaltenoperationen aus M wie gewünscht hervorgeht. Für den eingangs definierten gemeinsamen Nenner $h \in k[x]$ gibt es ein $h' \in k[x]$, so daß $hh' \in R\langle x\rangle^\times$ gilt. Es genügt daher, M mit h' zu multiplizieren, anstatt durch h zu dividieren, womit der Beweis für $n = 2$ abgeschlossen wäre.
Die angekündigte Konstruktion erfolgt nun derart, daß für geeignete Matrizen $T_{j+1} \in k[x]^{2\times 2}$ mit $\det(T_{j+1}) \in k^\times$ die Bedingungen

$$c_j \neq 0, \qquad \deg c_j < \deg d_j, \tag{2.33}$$

$$\deg(d_{j+1}) = \deg(c_j), \qquad U_{j+1} = U_j T_{j+1} \tag{2.34}$$

erfüllt sind. Ohne Einschränkung gilt (2.33) für $j = 1$, weil sich M voraussetzungsgemäß in Hermite-Normalform befindet.
Wenn die obigen Werte für ein $j \in \mathbb{Z}^{\geq 1}$ definiert sind und (2.33) gilt, bestimmen wir die nächsten Werte für $j+1$ wie folgt: Es sei $\mathfrak{d}_{1,j} := \mathfrak{a}_j\, a_j/c_j \cap k$ und $\mathfrak{d}_{2,j} := \mathfrak{c}_j \cap k$. Damit haben wir

$$U_j = \mathfrak{d}_{1,j} R\langle x\rangle (c_j, 0) + \mathfrak{d}_{2,j} R\langle x\rangle (c_j, d_j).$$

Proposition 2.31 zeigt, daß

$$\mathfrak{d}_{1,j}(c_j, 0) + \mathfrak{d}_{2,j}(c_j, d_j) = (\mathfrak{d}_{1,j} + \mathfrak{d}_{2,j})(\lambda_j c_j + \mu_j c_j, \mu_j d_j) + (\mathfrak{d}_{1,j} \cap \mathfrak{d}_{2,j})(0, d_j)$$

für geeignete $\lambda_j, \mu_j \in R$ mit $\lambda_j + \mu_j = 1$ und daher auch

$$U_j = (\mathfrak{d}_{1,j} + \mathfrak{d}_{2,j}) R\langle x\rangle (c_j, \mu_j d_j) + (\mathfrak{d}_{1,j} \cap \mathfrak{d}_{2,j}) R\langle x\rangle (0, d_j)$$

gilt. Mit der Polynomdivision $\mu_j d_j = \gamma_j c_j + r_j$, $\deg(r_j) < \deg(c_j)$ definieren wir

$$\begin{aligned}
&\mathfrak{a}_{j+1} := (\mathfrak{d}_{1,j} \cap \mathfrak{d}_{2,j}) R\langle x\rangle, \quad \mathfrak{c}_{j+1} := (\mathfrak{d}_{1,j} + \mathfrak{d}_{2,j}) R\langle x\rangle, \\
&a_{j+1} := d_j, \quad d_{j+1} := c_j, \quad c_{j+1} := r_j, \\
&T_{j+1} := \begin{pmatrix} -\gamma_j & 1 \\ 1 & 0 \end{pmatrix}.
\end{aligned}$$

Im Fall $c_{j+1} \neq 0$ sind die Bedingungen (2.33) und (2.34) damit erfüllt. Aufgrund der Gradbedingung (2.33) gilt jedoch notwendigerweise nach einer endlichen Anzahl r von Schritten wie gewünscht $c_r = 0$ und $U_r = U_1 T$ mit $T := \prod_{j=2}^{r} T_j$.
Es sei nun schließlich $n > 2$ und $M \in k(x)^{n\times n}$ in unterer Dreiecksgestalt. Durch die Diagonalisierung von 2×2 Teilmatrizen von M, die durch die Schnitte der

Zeilen i, n und Spalten i, n für $i = n-1, \ldots, 1$ erhalten werden, können wir alle Elemente bis auf das letzte Element der n-ten Zeile von M zu null machen. Indem dies auch für die anderen Zeilen durchgeführt wird, läßt sich M vollständig diagonalisieren. □

Wir merken an, daß sogar erreicht werden kann, daß die Einträge von M einen Grad von höchstens eins besitzen. Im Fall eines Hauptidealrings R können sie sogar selbst als eins gewählt werden.

2.35. Satz. *Es sei $\mathfrak{a}$ ein Ideal von $\mathrm{Cl}\big(R\langle x\rangle, F\big)$, $\mathfrak{b}$ ein Ideal von $\mathrm{Cl}\big(k[x], F\big)$. Dann ist $\mathfrak{a} \cap \mathfrak{b}$ ein $R[x]$-Modul und es gibt Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ von R und eine Basis $w_1, \ldots, w_n$ von $\mathfrak{b}$, so daß gilt:*

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}_1[x]w_1 \dotplus \ldots \dotplus \mathfrak{a}_n[x]w_n.$$

Die Idealklasse des Produkts der $\mathfrak{a}_j$ in R ist eine Invariante von $\mathfrak{a} \cap \mathfrak{b}$ (verallgemeinerte Steinitz-Klasse).

Beweis. Der Schnitt $R\langle x\rangle \cap k[x]$ ist gleich $R[x]$. $\mathfrak{a}$ ist ein $R\langle x\rangle$-Modul und $\mathfrak{b}$ ist ein $k[x]$-Modul, beide sind frei vom Rang n. Daher ist $\mathfrak{a} \cap \mathfrak{b}$ ein $R[x]$-Modul und es gibt eine reguläre Matrix $M \in k(x)^{n\times n}$, welche eine Basis von $\mathfrak{a}$ (geschrieben als Zeile) in eine Basis von $\mathfrak{b}$ transformiert. Wegen Lemma 2.32 können wir die Basis von $\mathfrak{a}$ und die Basis von $\mathfrak{b}$ so wählen, daß M diagonal ist. Die Koeffizienten einer $k[x]$-Linearkombination der Basiselemente von $\mathfrak{b}$ werden durch M in eine $k(x)$-Linearkombination der Basiselemente von $\mathfrak{a}$ transformiert. Multipliziert mit den Diagonaleinträgen müssen diese in $R\langle x\rangle$ liegen, was auch durch Idealzugehörigkeitsbedingungen wie oben mit den $\mathfrak{a}_j$ unter Beachtung von Proposition 2.27 ausgedrückt werden kann. Schließlich gilt $\prod_{j=1}^{n} \mathfrak{a}_j = \det M^{-1} R\langle x\rangle \cap k$ und $\det M$ ist modulo Multiplikation mit Einheiten aus $R\langle x\rangle$ oder aus $k[x]$ eindeutig definiert, weshalb auch die Steinitz-Klasse eindeutig bestimmt ist. □

2.10.5 Der ganze Abschluß von $R[x]$ in F

Weil es sich bei $R[x]$ nicht um einen Dedekindring handelt, kann man den Round-2-Algorithmus nicht ohne weiteres zur Bestimmung von $\mathrm{Cl}\big(R[x], F\big)$ heranziehen. Unter Benutzung der Einheitsideale und mit der Beobachtung, daß $\mathrm{Cl}\big(R[x], F\big) = \mathrm{Cl}\big(k[x], F\big) \cap \mathrm{Cl}\big(R\langle x\rangle, F\big)$ gilt, stellt Satz 2.35 die Struktur von $\mathrm{Cl}\big(R[x], F\big)$ als $R[x]$-Modul klar und gibt darüber hinaus eine Methode zur Bestimmung einer „Pseudo“-Basis an.

2.36. Korollar. *Es gibt Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ von R und $k(x)$-linear unabhängige Elemente $v_1, \ldots, v_n \in F$, so daß der Ring der $R[x]$-ganzen Elemente von F die direkte Summe*

$$\mathrm{Cl}\big(R[x], F\big) = \mathfrak{a}_1[x]v_1 \dotplus \ldots \dotplus \mathfrak{a}_n[x]v_n$$

ist. Die Idealklasse des Produkts der $\mathfrak{a}_j$ in R ist die (verallgemeinerte) Steinitz-Klasse von $\mathrm{Cl}\big(R[x], F\big)$.

Das Korollar zeigt außerdem, daß $\mathrm{Cl}\big(R[x], F\big)$ projektiv ist, weil die Ideale $\mathfrak{a}_j$ und $\mathfrak{a}_j[x]$ invertierbar sind. Für $R[x]$-Moduln ist dies im allgemeinen nicht der Fall, typische Beispiele stellen gerade die nicht invertierbaren Ideale von $R[x]$ dar, beispielsweise $\mathfrak{p}[x] + R[x]x$, $\mathfrak{p}$ ein Primideal von R. Einen anderen Beweis für den Fall eines Hauptidealrings R findet man in [13, S. 192].

2.37. Beispiel. Für den Funktionenkörper in Beispiel 2.29 ist $1, (1+\rho)/2$ auch eine $k[x]$-Basis für $\mathrm{Cl}\big(k[x], F\big)$, so daß man $\mathrm{Cl}\big(\mathbb{Z}[x], F\big) = \mathbb{Z}[x, (1+\rho)/2]$ hat.

2.10.6 Parametrische Basen von $\mathcal{L}(D) \cap \mathfrak{a}$

Satz 2.1 zeigt die Existenz einer parametrischen Basis von $\mathcal{L}(D)$, durch die Basen für alle $\mathcal{L}\big(D + r(x)_\infty\big)$, $(r \in \mathbb{Z})$ leicht angegeben werden können. Lemma 2.30 zeigt, wie eine Basis für $\mathcal{L}(D) \cap \mathfrak{a}$ erhalten werden kann. Es soll nun geklärt werden, wie parametrische Basen für $\mathcal{L}\big(D + r(x)_\infty\big) \cap \mathfrak{a}$ angegeben werden können. Das Hauptproblem liegt darin, daß der Reduktionsalgorithmus in Korollar 1.7 Spalten beliebig mit Elementen aus $k^\times$ skalieren muß und dadurch Ganzheitseigenschaften verloren gehen, die in Lemma 2.30 zurückgewonnen werden. Wir benötigen eine Proposition über die Ergänzung von Riemann-Roch-Basen:

2.38. Proposition. *Es seien $v_1, \ldots, v_n \in F$ und $d_1, \ldots, d_n \in \mathbb{Z}$ für D wie in Satz 2.1 und es sei $w_1, \ldots, w_n$ eine beliebige Idealbasis von $(D^S)^{-1}$. Wähle ganzrationale Zahlen s_j, so daß $w_j \in \mathcal{L}\big(D - s_j(x)_\infty\big)$ für $1 \le j \le n$ gilt. Dann gibt es eindeutig bestimmte $l_1, \ldots, l_n \in \mathbb{Z}$ mit der Eigenschaft, daß die Vereinigungen $A_r \cup B_r$ der beiden Familien von Mengen*

$$\begin{aligned} A_r &= \{\ x^i w_j \mid 0 \le i \le s_j + r,\ 1 \le j \le n\ \}, \\ B_r &= \{\ x^i v_j \mid \max\{0, l_j + r\} \le i \le d_j + r,\ 1 \le j \le n\ \} \end{aligned}$$

disjunkt sind und k-Basen von $\mathcal{L}\big(D + r(x)_\infty\big)$ für alle $r \in \mathbb{Z}$ ergeben.

Beweis. Daß die l_j eindeutig bestimmt sind, sofern sie existieren, folgt aus der Basiseigenschaft von $A_r \dot\cup B_r$ für großes r und weil die v_i $k[x]$-linear unabhängig sind. $A_r \cup B_r \subseteq \mathcal{L}(D + r(x)_\infty)$ ergibt sich aus der Wahl der s_j und d_j.

Weil es sich bei $\mathcal{L}\big(D + r(x)_\infty\big)$ um einen Vektorraum handelt, kann A_r durch geeignete Wahl von Elementen $x^i v_j$ zu einer Basis ergänzt werden. Es seien $t_{i,j} \in k[x]$ mit $v_j = \sum_{i=1}^n t_{i,j} w_i$. Wir sehen jetzt, daß sich $x^c v_j$, $0 \le c \le d_j + r$, wegen der Koeffizientenschranken genau dann im Erzeugnis von A_r befindet, wenn $c + \deg(t_{i,j}) \le s_i + r$ für alle $1 \le i \le n$ gilt. Erhöht man das maximale c dieser Eigenschaft um eins, so liegt $x^c v_j$ nicht mehr im Erzeugnis von A_r. Daran erkennt man, daß $l_j := \min\{s_i - \deg(t_{i,j}) \mid 1 \le i \le n\} + 1$ für $1 \le j \le n$ das Gewünschte leistet. □

2.39. Satz. *Es sei D ein Divisor von F/k und $\mathfrak{a}$ ein Ideal von $\mathrm{Cl}(R\langle x\rangle, F)$. Es gibt ganzrationale Zahlen l_0, r_0, s_ν, Ideale $\mathfrak{a}_\nu, \mathfrak{b}_j$ von R und Elemente w_ν, u_j von F für $1 \le \nu \le n$ und $1 \le j \le l_0$, so daß für alle $r \ge r_0$*

$$\mathcal{L}\big(D + r(x)_\infty\big) \cap \mathfrak{a} \quad = \sum_{\substack{1 \le \nu \le n \\ 0 \le i \le s_\nu + r}} \mathfrak{a}_\nu \, x^i \, w_\nu \quad + \quad \sum_{1 \le j \le l_0} \mathfrak{b}_j \, x^{r - r_0} \, u_j$$

gilt, wobei alle Summen direkt sind.

Beweis. Wir definieren die w_j und $\mathfrak{a}_j$ wie in Satz 2.35 bezüglich des Schnitts $\mathfrak{a} \cap (D^S)^{-1}$ und übernehmen ansonsten die Notation von Proposition 2.38 und ihrem Beweis. Es sei weiter $r_0 \in \mathbb{Z}$ mit $s_j + r_0 \ge 0$ und $l_j + r_0 \ge 0$ für alle $1 \le j \le n$. Wir betrachten beliebige $r \ge r_0$ und setzen $r' := r - r_0$, $s'_j := s_j + r - r'$, $l'_j := l_j + r - r'$ und $d'_j := d_j + r - r'$, so daß $s'_j, l'_j \ge 0$ für alle $1 \le j \le n$ gilt. Mit diesen Bezeichnungen haben wir

$$\begin{aligned} A_r &= \{\, x^i w_j \mid 0 \le i \le s'_j + r',\ 1 \le j \le n \,\}, \\ B_r &= \{\, x^i v_j \mid l'_j + r' \le i \le d'_j + r',\ 1 \le j \le n \,\}. \end{aligned}$$

Wir wollen die Elemente von B_r „parametrisch“ modulo der Elemente von A_r reduzieren: Durch geeignetes Subtrahieren entfernen wir die Terme der Form $x^\mu w_j \in A_r$ aus den $x^i v_j = \sum_{\nu=1}^n x^i t_{\nu,j} w_\nu \in B_r$ und erhalten die Aussage: Es gibt $v_{i,j} := \sum_{\nu=1}^n x^{s'_\nu + 1} \gamma_{\nu,i,j} w_\nu$, $\gamma_{\nu,i,j} \in k[x]$ für $1 \le \nu, j \le n$ und $l'_j \le i \le d'_j$, so daß die Differenzen $x^{r'}(x^i v_j - v_{i,j})$ im Erzeugnis von A_r liegen und $A_r \,\dot\cup\, B'_r$ mit

$$B'_r := \{\, x^{r'} v_{i,j} \mid 1 \le j \le n, l'_j \le i \le d'_j \,\}$$

eine k-Basis von $\mathcal{L}\big(D + r(x)_\infty\big)$ für alle $r \ge r_0$ bildet. Wir bemerken, daß die $v_{i,j}$ beziehungsweise $\gamma_{\nu,i,j}$ von r unabhängig sind.
Für ein beliebiges Element $a \in \mathcal{L}\big(D + r(x)_\infty\big)$ gibt es ein $h_j \in k[x]$ mit $\deg(h_j) \le$

$s'_j + r'$ und $\lambda_{i,j} \in k$ für $1 \leq j \leq n$ und $l'_j \leq i \leq d'_j$, so daß a durch

$$\begin{aligned} a &= \sum_{j=1}^{n} h_j w_j \; + \; x^{r'} \sum_{i,j} \lambda_{i,j} v_{i,j} \\ &= \sum_{\nu=1}^{n} h_\nu w_\nu \; + \; \sum_{\nu=1}^{n} x^{s'_\nu + r' + 1} \left(\sum_{i,j} \lambda_{i,j} \gamma_{\nu,i,j} \right) w_\nu \end{aligned}$$

eindeutig dargestellt wird. Man beachte, daß die beiden Summen keine Terme der Form $x^\mu w_\nu$ gemeinsam haben. Nach Satz 2.35 gilt nun

$$a \in \mathfrak{a} \;\; \Leftrightarrow \;\; h_\nu \in \mathfrak{a}_\nu[x] \;\text{ und }\; \sum_{i,j} \lambda_{i,j} \gamma_{\nu,i,j} \in \mathfrak{a}_\nu[x], \;\; (1 \leq \nu \leq n).$$

Die auf der rechten Seite stehende, zweite Bedingung ist unabhängig von r. Die $\lambda_{i,j}$, die diese Bedingung erfüllen, bilden einen endlich erzeugten, torsionsfreien R-Modul, dessen Basis man ähnlich dem Vorgehen im Beweis von Satz 2.30 und wie in [17, S. 78ff.] bestimmen kann. Hieraus ergibt sich die zu beweisende Aussage. □

2.10.7 Anwendungen

Anwendungen der Ergebnisse dieses Abschnitts ergeben sich, wenn bei Spezialisierungen von x im Funktionenkörper Ganzheitsbedingungen beachtet werden sollen, beispielsweise, wenn die Restklassenkörper Zahlkörper sind und man durch die Restbildung ganzalgebraische Elemente beziehungsweise Minimalpolynome mit ganzen Koeffizienten erhalten möchte.
Ein anderes Einsatzgebiet ergibt sich mit der Reduktion eines Funktionenkörpers nach einer diskreten Bewertung (einem Primideal) des Konstantenkörpers, es sei auf [13, S. 187ff.] verwiesen. Man betrachtet für gewöhnlich nur reguläre Primideale oder Primideale guter Reduktion. Der obige Ansatz ist jedoch völlig allgemeingültig und kann somit für beliebige diskrete Bewertungen beziehungsweise Primideale angewendet werden. Durch die Betrachtung des Dedekindrings R (und nicht nur des Bewertungsrings einer diskreten Bewertung) werden die Berechnungen simultan für alle Primideale von R ausgeführt.
Abschließend sei bemerkt, daß die Klassenzahl von $\mathrm{Cl}\big(R\langle x\rangle, F\big)$ nach dem Irreduzibilitäts- und Trägheitssatz aus [13, S. 187ff.] endlich ist.

Kapitel 3

Divisorenklassengruppen

In diesem Kapitel werden die für die Klassengruppenberechnung relevanten theoretischen Aussagen zusammengestellt. Die wichtigsten Ergebnisse sind die Herleitung einer Schranke an die Grade der für die Erzeugung der Klassengruppe benötigten Stellen und die Angabe einer Formel für die Approximation der Klassenzahl.

F/k bezeichnet einen globalen Funktionenkörper über dem exakten, endlichen Konstantenkörper k mit dem Geschlecht g. Die Charakteristik von k sei p, die Elementanzahl q. In einem fest gewählten, algebraischen Abschluß $\bar{F}$ von F sei k_r die Erweiterung von k vom Grad r und F_r/k_r mit $F_r = Fk_r$ die Konstantenkörpererweiterung von F/k vom Grad r.

3.1 Grundlagen

3.1.1 L-Reihen und Satz von Hasse-Weil

Unter einem Charakter χ endlicher Ordnung einer abelschen Gruppe G verstehen wir einen Homomorphismus $G \longrightarrow \mathbb{C}^\times$, dessen Kern endlichen Index in G besitzt. Der Hauptcharakter $\chi = 1$ ist der Charakter endlicher Ordnung von G mit $\ker \chi = G$.

3.1. Definition. Die zu einem Charakter χ endlicher Ordnung der Divisorenklassengruppe $\mathcal{C}l(F/k)$ definierte formale Potenzreihe

$$L(\chi, t) := \sum_{D \geq 0} \chi([D]) \cdot t^{\deg D}$$

heißt die L-Reihe von χ. Die Summe erstreckt sich hierbei über alle positiven Divisoren. Für $\chi = 1$ spricht man von der Zeta-Funktion von F/k, die wir mit $\zeta_{F/k}(t)$ bezeichnen.

Es sei bemerkt, daß sich die Analogie zum Zahlkörperfall mit $t = q^{-s}$ ergibt. Wegen der Orthogonalitätsrelationen sind mitunter Fallunterscheidungen notwendig. Hierfür definieren wir $\rho_\chi := 1$, wenn χ eingeschränkt auf $\mathcal{C}l^0(F/k)$ der Hauptcharakter ist, und $\rho_\chi := 0$ andernfalls.

3.2. Satz. (*i*) *Eine L-Reihe $L(\chi, t)$ erfüllt die Funktionalgleichung*

$$L(\chi, t) = \chi([W])\, q^{g-1}\, t^{2g-2}\, L(\overline{\chi}, 1/(qt)),$$

wobei W einen kanonischen Divisor bezeichnet.

(*ii*) *Eine L-Reihe $L(\chi, t)$ besitzt die folgenden Darstellungen (als formale Potenzreihen):*

$$L(\chi,t) = \prod_{P \in \mathcal{P}l(F/k)} \left(1 - \chi([P]) \cdot t^{\deg P}\right)^{-1} \tag{3.3}$$

$$= \left((1-t)(1-qt)\right)^{-\rho_\chi} \prod_{i=1}^{2(g-1+\rho_\chi)} (1 - \omega_i(\chi) \cdot t) \tag{3.4}$$

$$= \exp\left(\sum_{r=1}^{\infty} N_r(\chi) \cdot \frac{t^r}{r}\right), \tag{3.5}$$

wobei die $\omega_i(\chi) \in \mathbb{C}^\times$ ganzalgebraische Zahlen sind und

$$N_r(\chi) := \sum_{\deg(P) \mid r} \deg(P) \cdot \chi([P])^{r/\deg(P)} \tag{3.6}$$

$$= \rho_\chi(q^r + 1) - \sum_{i=1}^{2(g-1+\rho_\chi)} \omega_i(\chi)^r \tag{3.7}$$

gilt.

Beweis. Teil (*i*), Teil (*ii*) (3.3) und (3.4) folgen aus [12, S. 59–67] mit $t = q^{-s}$. Man vergleiche auch [33, S. 48ff.] und [55, S. 158ff.].
Der Beweis von (3.5) erfolgt durch Anwendung von log und exp auf die davor stehenden Darstellungen, wobei mit formalen Potenzreihen gerechnet wird. Aus (3.3) ergibt sich:

$$\begin{aligned} L(\chi,t) &= \exp\left(-\sum_P \log\left(1 - \chi([P]) \cdot t^{\deg P}\right)\right) \\ &= \exp\left(\sum_P \sum_{r=1}^{\infty} \left(\chi([P]) \cdot t^{\deg P}\right)^r / r\right) \\ &= \exp\left(\sum_{r=1}^{\infty} t^r / r \sum_{\deg(P)\,|\,r} \deg(P) \cdot \chi([P])^{r/\deg(P)}\right). \end{aligned}$$

Aus (3.4) ergibt sich:

$$\begin{aligned} L(\chi,t) &= \exp\left(\rho_\chi \sum_{r=1}^{\infty}\left(t^r+(qt)^r\right)/r \;-\; \sum_{i=1}^{2(g-1+\rho_\chi)}\sum_{r=1}^{\infty}(\omega_i(\chi)\cdot t)^r/r\right) \\ &= \exp\left(\sum_{r=1}^{\infty} t^r/r\left(\rho_\chi(q^r+1) \;-\; \sum_{i=1}^{2(g-1+\rho_\chi)}\omega_i(\chi)^r\right)\right). \end{aligned}$$

Durch Koeffizientenvergleich erhält man (3.5), (3.6) und (3.7). □

3.8. Korollar. *Es sei χ ein Charakter endlicher Ordnung von $\mathcal{C}l(F/k)$. Durch $\chi^* := \chi \circ \mathrm{N}_{F_r/F}$ wird ein Charakter endlicher Ordnung auf $\mathcal{C}l(F_r/k_r)$ definiert, für den $N_d(\chi^*) = N_{rd}(\chi)$ für alle $d \in \mathbb{Z}^{\geq 1}$, $\rho_{\chi^*} = \rho_\chi$ und $\omega_i(\chi^*) = \omega_i(\chi)^r$ für alle $1 \leq i \leq 2(g-1+\rho_\chi)$ mit geeigneter Sortierung gilt.*

Beweis. Der zurückgezogene Charakter χ^* ist von endlicher Ordnung, weil sein Bild endlich ist. Eine Stelle P von F/k mit $\deg(P) \mid r$ wird in F_r/k_r in $\deg(P)$ Stellen des Grads eins zerlegt. Hieraus ergibt sich $N_1(\chi^*) = N_r(\chi)$. Indem dies für $\chi^{**} := \chi^* \circ \mathrm{N}_{F_{dr}/F_r}$ angewendet und die Transitivität der Norm beachtet wird, sieht man $N_d(\chi^*) = N_1(\chi^{**}) = N_{rd}(\chi)$. In dieser Gleichung steht wegen (3.7) auf beiden äußeren Seiten eine Summe von $2g+2$ d-ten Potenzen für alle $d \in \mathbb{Z}^{\geq 1}$, die nach den Newton-Relationen bis auf Vertauschung übereinstimmen müssen. Weil die $\omega_i(\chi)$ beziehungsweise $\omega_i(\chi^*)$ ungleich null sind, folgt $\rho_{\chi^*} = \rho_\chi$ und $\omega_i(\chi^*) = \omega_i(\chi)^r$ nach geeigneter Sortierung. □

Für den Hauptcharakter $\chi = 1$ schreiben wir statt $N_r(\chi)$ auch $N_r(F/k)$ und statt $\omega_i(\chi)$ auch $\omega_i(F/k)$. Man sieht, daß $N_r(F/k)$ gleich der Anzahl der Stellen vom Grad eins in der Konstantenkörpererweiterung F_r/k_r ist.

Das Zählerpolynom der Zeta-Funktion von F/k (Fall $\chi = 1$) in (3.4) wird das L-Polynom von F/k genannt. Das L-Polynom enthält einige wichtige Informationen über den Funktionenkörper F/k. Es erfüllt eine Funktionalgleichung, die man leicht aus der für L-Reihen ableitet, und kann als charakteristisches Polynom eines Frobeniusendomorphismus aufgefaßt werden (die Koeffizienten müssen dazu in ihrer Reihenfolge vertauscht werden). Wir benötigen für unsere Zwecke nur den folgenden

3.9. Satz. *Für das L-Polynom $L(t)$ von F/k gilt:*

$$L(1) = q^g L(1/q) = h(F/k).$$

Beweis. Siehe [55, S. 166] □

Der folgende Satz gehört neben dem Satz von Riemann-Roch zu den wichtigsten Sätzen über globale Funktionenkörper:

3.10. Satz (Hasse-Weil). *Für einen Charakter χ endlicher Ordnung der Divisorenklassengruppe $\mathcal{C}l(F/k)$ gilt:*

$$|\omega_i(\chi)| = q^{1/2}, \quad \text{für } 1 \leq i \leq 2(g-1+\rho_\chi).$$

Beweis. In [55, S. 169ff.] und [33, S. 59ff.] wird die Aussage für den Hauptcharakter $\chi = 1$ nach der Methode von Bombieri und Stepanov bewiesen. Der Originalbeweis findet sich in [59].
Für andere Charaktere $\chi \neq 1$ endlicher Ordnung benötigt man Klassenkörpertheorie: Mit [2, S. 70ff.] gibt es eine (eindeutige) endliche, abelsche und an allen Stellen unverzweigte Erweiterung E_χ/F, so daß $\mathcal{C}l(F/k)\,/\ker\chi$ unter dem Artinsymbol isomorph zur Galoisgruppe $\mathrm{Gal}(E_\chi/F)$ ist. Es sei k_1 der exakte Konstantenkörper von E_χ. Die benötigte und hieraus folgende Aussage ist, daß der Relativgrad $f(P'|P)$, [55, S. 110], für eine Stelle P' von E_χ/k_1 über der Stelle P von F/k mit der Ordnung von $[P]$ in $\mathcal{C}l(F/k)\,/\ker\chi$ übereinstimmt. Entsprechend der Überlegungen aus [22, S. 217, Thm. 6, i)] und [12, S. 148ff.] (vgl. auch [34, S. 547ff.]) ist die Zeta-Funktion von E_χ/k_1 dann das Produkt der L-Reihen zu Charakteren χ' von $\mathcal{C}l(F/k)$ mit $\ker\chi \subseteq \ker\chi'$:

$$\zeta_{E_\chi/k_1}\left(t^{[k_1:k]}\right) \;=\; \prod_{\ker\chi\subseteq\ker\chi'} L(\chi',t).$$

Daher findet man die $\omega_i(\chi)^{[k_1:k]}$ unter den $\omega_j(E_\chi/k_1)$, für die die Betragsaussage mit $q^{[k_1:k]}$ statt q bereits bewiesen ist. □

Wegen Satz 3.2, (3.7) hat dieser Satz eine unmittelbare Auswirkung auf die Zahlen $N_r(\chi)$ und alle sich daraus ergebenden Größen. Wir erhalten beispielsweise eine „effektive“ Version des Primdivisorsatzes:

3.11. Satz. *Für die Anzahl $\pi_r(F/k)$ der Stellen des Grads r von F/k gilt:*

(*i*) $\pi_r(F/k) = (1/r)\sum_{d|r}\mu(r/d)N_d(F/k)$, *wobei μ die Möbius-Funktion bezeichnet.*

(*ii*) *Man hat die folgende, explizite Abschätzung*

$$|\pi_r(F/k) - \frac{q^r}{r}| < (7g+2)\cdot\frac{q^{r/2}}{r}.$$

(*iii*) *Ist $g > 0$, so gilt $\pi_{r_1}(F/k) \geq 1$ für jedes $r \in \mathbb{Z}^{\geq 1}$ mit $r \geq 2\log_q(2g)$ und mindestens einem $r_1|r$.*

Beweis. Für (i) und (ii) siehe [55, S. 178–180]. (iii) beweisen wir wie folgt: Es sei $r \in \mathbb{Z}^{\geq 1}$ mit $N_r(F/k) > 0$. Also gibt es eine Stelle vom Grad eins in F_r/k_r, und diese Stelle rührt von einer Stelle P von F/k mit $r_1 := \deg(P) \,|\, r$ her. Aufgrund von Satz 3.10 und Satz 3.2, (3.7) gilt $N_r(F/k) > 0$ für alle $r \in \mathbb{Z}^{\geq 1}$ mit $q^r + 1 > 2gq^{r/2}$, welches mindestens dann gilt, wenn $r \geq 2\log_q(2g)$ ist. □

In F/k existiert also immer eine Stelle vom Grad kleiner gleich $\lceil 2\log_q(2g) \rceil$. Wir merken an, daß diese Schranke noch verbessert werden kann, beispielsweise mit dem Trick von Serre [55, S. 180].

Aus dem voranstehenden Satz und [28] erhalten wir die asymptotische Aussage:

3.12. Lemma. *Es sei $\varepsilon > 0$. F/k durchlaufe eine Folge von globalen Funktionenkörpern mit festem q und $g \to \infty$. Für die Anzahl der Stellen P von F/k mit $\deg(P) \leq m$ und $m \geq (2+\varepsilon)\log_q(g)$ gilt*

$$\sum_{j=1}^{m} \pi_j(F/k) = \frac{q}{q-1} \cdot q^m/m \cdot \big(1 + o(1)\big).$$

Beweis. Mit Satz 3.11 erhält man $\sum_{j=1}^{m} \pi_j(F/k) = \sum_{j=1}^{m} q^j/j + O(mgq^{m/2})$. Mit der Methode aus [28] ergibt sich für den Hauptterm $\sum_{j=1}^{m} q^j/j = q^m/m \,\big(q/(q-1) + O(1/m)\big)$. Nach Ausklammern von q^m/m ist der zuerst genannte Fehlerterm gleich $m^2 g/q^{m/2}$ und strebt nach Voraussetzung an m gegen null. Insgesamt folgt daraus die Aussage. □

Eine andere, unmittelbare Folgerung aus Satz 3.9 zusammen mit Satz 3.10 ist das „Brauer-Siegel“-ähnliche Resultat:

3.13. Korollar. *Für die Klassenzahl von F/k gelten die Abschätzungen:*

$$(q^{1/2} - 1)^{2g} \leq h(F/k) \leq (q^{1/2} + 1)^{2g}.$$

Hierdurch wird jedoch das asymptotische Verhalten von $h(F/k)/q^g$, an dem man häufig interessiert ist, nicht besonders genau beschrieben.

3.1.2 Struktur der Klassengruppe

Für eine abelsche Gruppe G und $d \in \mathbb{Z}$ bezeichnen wir die Untergruppe der d-Torsionselemente mit $G[d] := \{\, g \in G \,|\, dg = 0 \,\}$.

Es sei $\bar{k}$ der algebraische Abschluß von k in $\bar{F}$. Wir betrachten die Konstantenkörpererweiterung $F\bar{k}/\bar{k}$:

3.14. Satz. *Für $\ell \in \mathbb{Z}^{\geq 1}$ mit $p \nmid \ell$ ist $\mathcal{C}l^0(F\bar{k})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, für $r \in \mathbb{Z}^{\geq 1}$ ist $\mathcal{C}l^0(F\bar{k})[p^r] \cong (\mathbb{Z}/p^r\mathbb{Z})^{\sigma(F/k)}$, wobei $\sigma(F/k)$ die Hasse-Witt-Invariante von F/k bezeichnet. Für diese gilt $0 \leq \sigma(F/k) \leq g$.*

Beweis. Für die erste Aussage mit ℓ siehe [14]. Für die zweite Aussage und mehr über die Hasse-Witt-Invariante siehe [54]. □

Bei diesem Satz handelt es sich ebenso wie bei Satz 3.10 eigentlich um eine für abelsche Varietäten allgemein gültige Aussage, vgl. [32]. Für asymptotische Aussagen bei wachsender, aber endlicher Konstantenkörpererweiterung siehe [42].

Wir schließen aus diesem Satz, daß die Klassengruppe $\mathcal{C}l^0(F/k)$ von F/k (endliches k !) in Elementarteilergestalt ein Produkt von $2g$ zyklischen Gruppen ist und daß es ein Erzeugendensystem von maximal $2g$ Divisorenklassen gibt.

3.2 Beschränkte Erzeugung

Jede Divisorenklasse $[D]$ wird durch Divisoren D modulo Hauptdivisoren dargestellt, und jeder solche Divisor setzt sich seinerseits aus Stellen zusammen. Unter allen Divisoren der Klasse $[D]$ gibt es nun natürlich solche, bei denen das Maximum der Grade der beteiligten Stellen minimal wird. Diese Zahl nennen wir den Minimalgrad $\mathrm{md}\big([D]\big)$ von $[D]$. Der Minimalgrad der Klasse des Nulldivisors wird als null definiert.

3.15. Proposition. *Für $g > 0$ gibt es einen Divisor D vom Grad eins mit Minimalgrad $\mathrm{md}\big([D]\big) \leq \lceil 2\log_q(2g) \rceil + 1$.*

Beweis. Setze $r := \lceil 2\log_q(2g) \rceil$. Nach Satz 3.11, *(iii)* gibt es eine Stelle P_1 vom Grad $r_1 \,|\, r$ und eine Stelle P_2 vom Grad $r_2 \,|\, (r+1)$. Weil r_1 und r_2 teilerfremd sind, gibt es $l_1, l_2 \in \mathbb{Z}$ mit $l_1 r_1 + l_2 r_2 = 1$. Hieraus erhält man mit $A_1 := l_1 P_1 + l_2 P_2$ einen Divisor der gesuchten Art. □

Es sei angemerkt, daß es üblicherweise Stellen vom Grad eins gibt, die man für A_1 verwenden kann. Der Fall $g = 0$ wird hier und in folgenden Abschätzungen nur wegen der log-Ausdrücke ausgeschlossen. Wir wollen nun Aussagen über die Minimalgrade von Erzeugendensystemen von $\mathcal{C}l^0(F/k)$ herleiten.

3.16. Satz. *Es sei χ ein Charakter endlicher Ordnung von $\mathcal{C}l(F/k)$, dessen Einschränkung auf $\mathcal{C}l^0(F/k)$ nicht den Hauptcharakter ergibt. Gilt für die Anzahl der Stellen vom Grad eins von F_r/k_r*

$$N_r(F/k) > (g-1)2q^{r/2},$$

so existiert eine Stelle P von F/k vom Grad kleiner gleich r mit

$$\chi\big([P]\big) \neq 1.$$

Diese Ungleichung gilt immer für $r \in \mathbb{Z}^{\geq 1}$ mit $q^r \geq (2g-1)2q^{r/2}$, also insbesondere, wenn $r \geq 2\log_q(4g-2)$ für $g > 0$ ist.

Beweis. Wir ziehen Satz 3.2, (3.6) und (3.7) heran: Weil die Charakterwerte Einheitswurzeln sind, gilt $N_r(F/k) \geq |N_r(\chi)|$ für alle $r \in \mathbb{Z}^{\geq 1}$, und im Fall der Ungleichheit gibt es eine Stelle P eines Grads kleiner gleich r von F/k mit $\chi\big([P]\big) \neq 1$. Nach Satz 3.10 gilt $|\sum_{i=1}^{2g-2} \omega_i(\chi)^r| \leq (g-1)2q^{r/2}$. Durch Umstellen sieht man nun, daß die im Satz angegebenen Abschätzungen $N_r(F/k) > |N_r(\chi)|$ erzwingen. □

3.17. Satz. *Es sei A_1 ein Divisor vom Grad eins von F/k und $r \in \mathbb{Z}^{\geq 1}$ wie in Satz 3.16. Es sei weiter $S := \mathcal{P}l^{\leq r}(F/k) \cup \operatorname{supp}(A_1)$. Dann gilt*

$$\mathcal{D}^0(S)\,/\mathcal{P}(S) \;\cong\; \mathcal{C}l^0(F/k).$$

Beweis. $\mathcal{C}l(F/k)$ ist das (innere) direkte Produkt von $\mathcal{C}l^0(F/k)$ und der von $[A_1]$ erzeugten Gruppe. Wir können daher jeden Charakter χ von $\mathcal{C}l^0(F/k)$ auf $\mathcal{C}l(F/k)$ durch $\chi\big([A_1]\big) = 1$ fortsetzen. Nach Satz 3.16 gibt es einen Divisor D mit $\operatorname{md}\big([D]\big) \leq r$ und $\chi\big([D]\big) \neq 1$, sofern χ auf $\mathcal{C}l^0(F/k)$ nicht trivial war. Wir setzen $[D'] := [D] - \deg(D)[A_1]$ und beobachten, daß $[D'] \in \big(\mathcal{D}^0(S) + \mathcal{P}(F/k)\big)/\mathcal{P}(F/k) \cong \mathcal{D}^0(S)/\mathcal{P}(S)$ und $\chi\big([D']\big) \neq 1$ gilt. Die Charaktergruppe von $G := \mathcal{C}l^0(F/k)/H$, wobei H die von allen solchen $[D']$ erzeugte Untergruppe bezeichnet, kann demnach nur aus dem Hauptcharakter bestehen, so daß G (aufgrund der Dualität) trivial ist, also $H = \mathcal{C}l^0(F/k)$ gilt. Weil H wegen der Erzeugung isomorph zu einer Untergruppe von $\mathcal{D}^0(S)/\mathcal{P}(S)$ ist, ergibt sich die zu beweisende Aussage. □

3.18. Korollar. *Mit $r_0 \in \mathbb{Z}^{\geq 1}$ werde das Maximum des Minimalgrads eines Divisors A_1 vom Grad eins von F/k und einem r wie in Satz 3.16 bezeichnet. Die Klassengruppe $\mathcal{C}l^0(F/k)$ besitzt dann ein Erzeugendensystem $[D_1], \ldots, [D_l]$, bestehend aus maximal $2g$ Elementen, mit*

$$\operatorname{md}\big([D_i]\big) \;\leq\; r_0 \quad \text{für} \quad 1 \leq i \leq l.$$

Für den Minimalgrad jeder Klasse $[D]$ von $\mathcal{C}l(F/k)$ gilt daher $\operatorname{md}\big([D]\big) \leq r_0$.

Beweis. $\mathcal{C}l^0(F/k)$ besitzt ein Erzeugendensystem mit wie oben beschränkten Minimalgraden nach dem vorangegangenen Satz. Diese Beschränkung des Minimalgrads gilt weiter für jede Klasse $[D]$ von $\mathcal{C}l(F/k)$, insbesondere für jedes maximal $2g$-elementige Erzeugendensystem von $\mathcal{C}l^0(F/k)$, welches nach Satz 3.14 existiert. □

3.19. Bemerkung. Man beachte, daß für $g > 0$ allgemein

$$r_0 \leq \max\{\, \lceil 2\log_q(4g-2)\rceil,\ \lceil 2\log_q(2g)\rceil + 1\,\}$$

erreicht werden kann.

Ein ähnliches Ergebnis wurde bereits in [53, S. 145ff.] nach der analogen Methode von [4] für Zahlkörper bewiesen. Die obige Schranke ist jedoch etwas schärfer, und der Beweis ist wesentlich kürzer.

3.3 Approximation der Klassenzahl

Die Klassenzahl kann „analytisch“ approximiert werden. Wir wollen die hierfür benötigte Formel mit explizitem Fehlerterm angeben und die Verbindung zu einem Eulerprodukt erklären.

3.20. Satz. *Für die Klassenzahl $h(F/k)$ und $r_0 \in \mathbb{Z}^{\geq 0}$ gilt:*

$$\left| \log\bigl(h(F/k)\,/\,q^g\bigr) + \sum_{r=1}^{r_0} \frac{q^{-r}}{r} \sum_{i=1}^{2g} \omega_i(F/k)^r \right| \leq \frac{2g}{q^{1/2}-1} \cdot \frac{q^{-r_0/2}}{r_0+1}.$$

Beweis. Es sei x ein separierendes Element von F/k. Der Quotient der Zetafunktion von F/k und der Zetafunktion von $k(x)/k$ ergibt gerade das L-Polynom $L(t)$ von F/k. Ferner wissen wir, daß $N_r(F/k) = q^r + 1 - \sum_{i=1}^{2g} \omega_i(F/k)^r$ und daß $N_r(k(x)/k) = q^r + 1$ gilt. Anhand von Satz 3.2, Gleichung (3.5) ergibt sich daher $L(t) = \exp\bigl(-\sum_{r=1}^{\infty} t^r/r \sum_{i=1}^{2g} \omega_i(F/k)^r\bigr)$. Weil die Reihe im exp-Argument für $t = q^{-1}$ absolut konvergiert und der Wert des L-Polynoms nach Satz 3.9 dort gleich $h(F/k)/q^g$ ist, stimmt ihr Grenzwert mit $\log\bigl(h(F/k)/q^g\bigr)$ überein. Der Fehlerterm ergibt sich dann durch folgende Rechnung:

$$\begin{aligned}
\left| \sum_{r=r_0+1}^{\infty} \frac{q^{-r}}{r} \sum_{i=1}^{2g} \omega_i(F/k)^r \right| &\leq \frac{2g}{r_0+1} \sum_{r=r_0+1}^{\infty} \frac{r_0+1}{r} q^{-r/2} \\
&\leq \frac{2g q^{-\frac{r_0+1}{2}}}{r_0+1} \sum_{r=0}^{\infty} (q^{-1/2})^r \leq \frac{2g}{q^{1/2}-1} \cdot \frac{q^{-r_0/2}}{r_0+1}.
\end{aligned}$$

□

3.21. Bemerkung. Wegen $\sum_{i=1}^{2g} \omega_i(F/k)^r = q^r + 1 - N_r(F/k)$ sind zur Approximation der Klassenzahl die Werte $N_r(F/k)$ zu bestimmen, vgl. S. 7.

Unter Verwendung von Satz 3.2, (3.3) können wir wie eben im Beweis den Quotienten der Zetafunktionen bilden und erhalten in Analogie zur Zahlkörpersituation, [5], [23, S. 26ff.], nach Sortierung der Faktoren ein Eulerprodukt

$$\prod_{r=1}^{\infty} \prod_{P_0 \in \mathcal{P}l^r(k(x)/k)} (1-t^r) \prod_{P \in \mathcal{P}l^r(F/k)} (1-t^r)^{-1}.$$

Man kann zeigen, daß dieses Produkt für $t = q^{-1}$ gegen $h(F/k)/q^g$ konvergiert und daß die Partialprodukte bis $r = r_0$ mit dem exp-Wert obiger Partialsummen bis $r = r_0$ übereinstimmen. Wir benötigen diese Aussagen im folgenden aber nicht weiter.

Die obige Restgliedabschätzung ergab sich vergleichsweise leicht aus der einfachen Abschätzung der $\omega_i(F/k)$ mit Satz 3.10 und ist für den angestrebten Verwendungszweck ausreichend. Schärfere Abschätzungen lassen sich eventuell mit der Oesterlé-Schranke erzielen, vgl. [3, S. 48].

Mit Satz 3.20 ist man auch in der Lage, das Größenverhältnis der Klassenzahl zum Wert q^g asymptotisch zu untersuchen. Wir erhalten das folgende Äquivalent zum Satz von Brauer-Siegel für Zahlkörper:

3.22. Satz. *Es sei $\varepsilon > 0$. F/k durchlaufe eine Folge von globalen Funktionenkörpern mit festem q und $g \to \infty$. Wir nehmen an, daß F/k einen rationalen Teilkörper $k(x)$ mit $n = n(g) := [F : k(x)]$ besitzt. Dann gilt*

$$\left|\log\left(h(F/k)\,/\,q^g\right)\right| \;\le\; \big(1+o(1)\big)\cdot(n-1)\cdot\log\big((2+\varepsilon)\log_q(g)\big)\,.$$

Beweis. Wir wählen $r_0 \in \mathbb{Z}$ mit $2\log_q(g) \le r_0 \le (2+\varepsilon)\log_q(g)$, was für hinreichend großes g möglich ist, und wenden Satz 3.20 an. Der Fehlerterm $2g/\big((q^{1/2}-1)q^{r_0/2}(r_0+1)\big)$ strebt dabei wegen der Wahl von r_0 für $g \to \infty$ gegen null. Wir betrachten nun den Approximationswert für $\log(h(F/k)/q^g)$ aus Satz 3.20. Die Anzahl der Stellen vom Grad eins von F_r/k_r läßt sich nach oben beschränken durch $N_r(F/k) \le n(q^r+1)$, weil über jeder Stelle von $k_r(x)/k_r$ höchstens n Stellen von F_r/k_r liegen. Mit $\left|\sum_{i=1}^{2g}\omega_i(F/k)^r\right| = \left|N_r(F/k)-(q^r+1)\right| \le (n-1)\,(q^r+1)$ erhält man

$$\left|\sum_{r=1}^{r_0} q^{-r}/r \sum_{i=1}^{2g}\omega_i(F/k)^r\right| \;\le\; (n-1)\sum_{r=1}^{r_0} q^{-r}(q^r+1)/r.$$

Unter Beachtung von $\sum_{r=1}^{r_0} 1/r = \big(1+o(1)\big)\log(r_0)$ und weil die geometrische Reihe beschränkt ist, läßt sich diese Summe durch $\big(1+o(1)\big)(n-1)\log(r_0)$ abschätzen, wobei mit $o(1)$ von n unabhängige Funktionen bezeichnet werden,

die für $g \to \infty$ nach null streben. Weil der Fehlerterm gegen null geht, erhält man insgesamt $\bigl|\log(h(F/k)/q^g)\bigr| \leq \bigl(1+o(1)\bigr)(n-1)\log(r_0)$, woraus die Behauptung wegen $r_0 \leq (2+\varepsilon)\log_q(g)$ folgt. □

Dieser Satz besagt also, daß der Quotient $h(F/k)/q^g$ nur relativ schwach wachsen (oder fallen) kann, sofern die Erweiterungsgrade n genügend schwach mit g wachsen. Auf ähnliche Weise wie eben kann man allgemeiner zeigen, daß $h(F/k)/q^g$ nie exponentiell in g fällt, und daß $h(F/k)/q^g$ exponentiell in g wächst, wenn beispielsweise die Anzahl der Stellen vom Grad eins asymptotisch groß wird. Dazu sei auf [40] verwiesen.

3.4 Cartier-Operator, p-Torsion der Klassengruppe und Hasse-Witt-Invariante

In diesem Abschnitt bezeichnet F/k einen algebraischen Funktionenkörper über dem exakten Konstantenkörper k, wobei k entweder der endliche Körper mit q Elementen oder der algebraische Abschluß eines solchen ist. Die p-Torsion der Klassengruppe $\mathcal{C}l^0(F/k)$ ist isomorph zu einem $\mathbb{F}_p$-Vektorraum von Differentialen. Aufgrund dieser Isomorphie und unter Benutzung des Cartier-Operators lassen sich sowohl der p-Rang der Klassengruppe als auch die Hasse-Witt-Invariante von F/k bestimmen. Dies soll im folgenden erläutert werden.

Zusätzlich zu den in Abschnitt 1.1 gegebenen Definitionen und Aussagen über Differentiale benötigen wir die folgenden: Der Raum der holomorphen Differentiale, also derjenigen Differentiale ohne Polstellen, wird mit $\Omega^1(F/k) := \Omega(D)$, D der Nulldivisor von F/k, bezeichnet. Anhand des Satzes von Riemann-Roch überlegt man sich leicht, daß $\dim\bigl(\Omega^1(F/k)\bigr) = g$ gilt. Ein Differential ω heißt exakt, wenn $\omega = da$ für ein $a \in F$ gilt. Ein Differential ist von der dritten Gattung, wenn seine Polstellen mit der Ordnung eins auftreten. Der Raum dieser Differentiale wird mit $\Omega^3(F/k)$ bezeichnet. In Charakteristik $p > 0$ bestehen die Differentiationskonstanten $a \in F$ mit $da = 0$ genau aus den p-ten Potenzen F^p. Für $a, x \in F$ und x separierend ist die p-te Ableitung $d^p a/dx^p = 0$, so daß es sich bei der $(p-1)$-ten Ableitung um eine p-te Potenz handelt.
Ein wichtiger Teilraum von $\Omega^3(F/k)$ ergibt sich mit den logarithmischen Differentialen, welche Differentiale der Form $(1/a)\,da$ mit $a \in F^\times$ sind. Dieser Raum wird mit $\Omega^{\log}(F/k)$ bezeichnet. Durch $a \mapsto (1/a)\,da$ erhält man nämlich einen Homomorphismus $F^\times \longrightarrow \Omega^{\log}(F/k)$, dessen Kern $(F^\times)^p$ ist. Man weiß, daß $v_P(a) \equiv 0 \bmod p$ genau dann gilt, wenn $v_P\bigl(((1/a)\,da)\bigr) \geq 0$ ist (für das Residuum gilt zum Beispiel $\mathrm{res}_P\bigl((1/a)\,da\bigr) \equiv \deg(P)\,v_P(a) \bmod p$). Für diese und weitere Aussagen über Differentiale siehe [11, 13, 33, 55].

Die Verbindung zur p-Torsion der Klassengruppe wird nun wie folgt hergestellt:

3.23. Satz. *Es sei $[D] \in \mathcal{C}l^0(F/k)[p]$. Dann ist $pD = (a)$ für ein $a \in F^\times$. Die Abbildung*

$$\mathcal{C}l^0(F/k)[p] \longrightarrow \Omega^1(F/k) \cap \Omega^{\log}(F/k), \quad [D] \mapsto (1/a)\, da$$

ist ein Isomorphismus (von $\mathbb{F}_p$-Vektorräumen).

Beweis. Wir verweisen auf [51, S. 41]. □

Aufgrund dieses Satzes sind wir an der Bestimmung von $\Omega^1(F/k) \cap \Omega^{\log}(F/k)$ interessiert. Den Raum $\Omega^1(F/k)$ können wir mit Abschnitt 2.9 berechnen. Zur Bestimmung der hierin enthaltenen logarithmischen Differentiale wird der Cartier-Operator eingesetzt.

3.24. Definition. Es sei x ein separierendes Element von F/k. Der Cartier-Operator C von F/k wird wie folgt definiert:

$$C : \Omega(F/k) \longrightarrow \Omega(F/k), \quad C(\omega) := \left(-d^{p-1}(\omega/dx)/dx^{p-1}\right)^{1/p} dx,$$

wobei unter der $(1/p)$-ten Wurzel die $(p-1)$-te Ableitung von $\omega/dx \in F$ gebildet wird. Man kann zeigen [29, S. 307ff.], daß diese Definition nicht von der Wahl des separierenden Elements x abhängt. Zur Berechnung der Werte $C(\omega)$ beachten wir Abschnitt 2.9 und die Tatsache, daß $a \mapsto a^p$ mit $a \in F$ ein injektiver, $\mathbb{F}_p$-linearer Ringhomomorphismus ist. Für eine $k(x)$-Basis $a_1, \ldots, a_n$ von F gibt es ein $M \in k(x)^{n\times n}$, so daß für beliebiges $a = (a_i)_i \lambda$ mit $\lambda \in k(x)^{n\times 1}$

$$a^p = (a_1, \ldots, a_n) M \lambda^p$$

gilt, wobei λ^p aus λ durch p-Potenzierung der Koeffizienten entsteht. Weil die $a_1^p, \ldots, a_n^p$ wegen $F^p \cap k(x) = k(x)^p$ linear unabhängig über $k(x)$ sind, ist M invertierbar und man kann leicht nach λ auflösen.

3.25. Satz. *Es sei $\omega \in \Omega(F/k)$.*

(*i*) *Der Cartier-Operator ist $\mathbb{F}_p$-linear,*

(*ii*) *$C(z^p\omega) = zC(\omega)$ für jedes $z \in F$. C ist also $(1/p)$-linear und C^n ist $\mathbb{F}_{p^n}$-linear.*

(*iii*) *Ist ω an einer Stelle holomorph, so ist $C(\omega)$ an derselben Stelle ebenfalls holomorph.*

(*iv*) *$C(\omega) = 0$ gilt genau dann, wenn ω exakt ist,*

(v) *$C(\omega) = \omega$ gilt genau dann, wenn ω logarithmisch ist.*

Beweis. Wir verweisen auf [29, S. 307ff.]. Die beiden letzten Eigenschaften werden dort nur für $F\bar{k}/\bar{k}$ formuliert, behalten hier aber ihre Gültigkeit (für $\omega = a\,dx$ bedeutet $C(\omega) = \omega$ per Definition $a^p = -d^{p-1}a/dx^{p-1}$, die dortige Schlußweise wird nicht benötigt). Vergleiche auch [2, S. 29ff.]. □

Die Kombination der beiden vorangegangenen Sätze zusammen mit Aussagen über p- beziehungsweise $(1/p)$-lineare Abbildungen (vgl. [21], [51]) ergibt nun den folgenden Satz, den wir [45] entnehmen:

3.26. Satz. *Es sei F/k ein globaler Funktionenkörper über dem exakten Konstantenkörper k der Charakteristik p.*

(i) *Es gilt*

$$\Omega^1(F/k) \cap \Omega^{\log}(F/k) \;=\; \ker\big((1-C)\,|\,\Omega^1(F/k)\big),$$

wobei $\Omega^1(F/k)$ als $\mathbb{F}_p$-Vektorraum aufgefaßt wird.

(ii) *Es sei $\omega_1, \ldots, \omega_g$ eine k-Basis von $\Omega^1(F/k)$ und $C^g(\omega_i) = \sum_{j=1}^{g} d_{j,i}\omega_j$ mit einer Matrix $(d_{i,j})_{i,j} \in k^{g\times g}$. Dann gilt*

$$\sigma(F/k) \;=\; \operatorname{rank}\big((d_{i,j})_{i,j}\big).$$

Mit diesem Satz läßt sich die Berechnung des p-Rangs der Klassengruppe nach (i) und der Hasse-Witt-Invariante nach (ii) auf lineare Algebra zurückführen. Im Vergleich zum später vorgestellten, allgemeinen Verfahren der Klassengruppenberechnung kann man hiermit Funktionenkörper mit wesentlich höherem Geschlecht und größerem Konstantenkörper behandeln. Für ein Beispiel verweisen wir auf den Abschnitt 7.6.

Wir bemerken ferner, daß Satz 3.23 zur effizienten Berechnung diskreter Logarithmen in der p-Torsion verwendet werden kann [46] und daß das charakteristische Polynom von C^n, $|k| = q = p^n$, unter einer weiteren Voraussetzung mit dem L-Polynom von F/k modulo p (nach Umkehrung der Reihenfolge der Koeffizienten) übereinstimmt [30, 45], vgl. auch [54].

Im Hinblick auf die spätere Bestimmung von S-Einheiten des globalen Funktionenkörpers F/k betrachten wir schließlich noch den Homomorphismus $(\mathfrak{o}^S)^\times \to \Omega^3(-D) \cap \Omega^{\log}(F/k)$, $a \mapsto (1/a)\,da$ für endliches $S \subseteq \mathcal{P}l(F/k)$ mit $|S| > 1$ und $D := \sum_{P\in S} P$. Diesen letzteren Raum können wir wie oben mit Hilfe des Cartier-Operators berechnen und ähnlich wie in [2, S. 29ff.] lassen sich dann für $\omega \in \Omega^3(-D) \cap \Omega^{\log}(F/k)$ sogar Elemente $b \in F^\times$ mit $\omega = (1/b)\,db$ bestimmen. Es scheint allerdings nicht möglich zu sein, hieraus brauchbare Informationen über die (unbekannten) S-Einheiten zu gewinnen.

Kapitel 4

Glattheitseigenschaften

In diesem Kapitel bezeichnet F/k einen globalen Funktionenkörper vom Geschlecht g über dem exakten Konstantenkörper k mit q Elementen.

Wir stellen Untersuchungen über die Anzahl positiver, glatter Divisoren an, wobei wir hierfür sowohl eine exakte Formel als auch eine asymptotische untere Schranke angeben werden. Im letzten Abschnitt wird die Glattheitsannahme formuliert, die wir für die Komplexitätsuntersuchungen des nächsten Kapitels benötigen.

Glattheitsaussagen für globale Funktionenkörper scheinen in der Literatur bis auf den rationalen und reell-quadratischen Fall bisher nicht betrachtet worden zu sein, siehe hierfür [35, 53].

4.1 Glattheitsfunktion

Die bisherige Glattheitsdefinition für einen Divisor wird wie folgt erweitert:

4.1. Definition. Es seien $n, m \in \mathbb{Z}^{\geq 0}$. Ein positiver Divisor D von F/k heiße (n,m)-glatt, wenn $\deg D \leq n$ und $\deg P \leq m$ für alle Primdivisoren $P \leq D$ gilt. Die Anzahl aller (n,m)-glatten Divisoren wird mit $\Psi_{F/k}(n,m)$ bezeichnet.

Man sieht, daß $\Psi_{F/k}(0,m) = \Psi_{F/k}(n,0) = 1$ gilt, da der Nulldivisor mitgezählt wird. Für den folgenden Satz beachte man $\binom{n}{m} := 0$ für $0 \leq n < m$ und $\binom{n}{0} := 1$ für $n \in \mathbb{Z}$.

4.2. Satz. *Für alle $n, m \in \mathbb{Z}^{\geq 0}$ gilt:*

(*i*)
$$\Psi_{F/k}(n,m) \;=\; \sum_{1j_1+\cdots+mj_m \leq n} \prod_{i=1}^{m} \binom{\pi_i(F/k) + j_i - 1}{j_i}.$$

(*ii*) *Mit* $N_{F/k}(n,m) := \sum_{0<d\le m,\ d|n} d\pi_d(F/k)$ *gilt*

$$n\Psi_{F/k}(n,m) = \sum_{j=0}^{n-1} \big(1 + N_{F/k}(n-j,m)\big)\, \Psi(j,m).$$

Beweis. Teil (*i*) ergibt sich wie folgt: Jeder (n,m)-glatte Divisor kann eindeutig durch m Summen von j_i (nicht unbedingt verschiedenen) Stellen des Grads i für $1 \le i \le m$ dargestellt werden (leere Summen mitgedacht). Für jedes solche i gibt es genau $\binom{\pi_i(F/k)+j_i-1}{j_i}$ dieser j_i-elementigen Summen (Anzahl der Kombinationen j_i-ter Ordnung von $\pi_i(F/k)$ Elementen mit Wiederholung, siehe [41, S. 465]).
Der Teil (*ii*) ist komplizierter: Wir setzen

$$S(n,m) := \sum_{\substack{D\ (n,m)\text{-glatt}\\ D\neq 0}} \deg(D)$$

und evaluieren diesen Ausdruck auf zwei verschiedene Weisen. Indem wir $S(n,m)$ als Summe aller möglichen Grade j multipliziert mit der Anzahl der (n,m)-glatten Divisoren vom Grad j schreiben, erhalten wir einerseits

$$\begin{aligned} S(n,m) &= \sum_{j=1}^{n} j \cdot \big(\Psi_{F/k}(j,m) - \Psi_{F/k}(j-1,m)\big) \\ &= n\cdot\Psi_{F/k}(n,m) - \sum_{j=0}^{n-1} \Psi_{F/k}(j,m) \end{aligned} \tag{4.3}$$

durch Zusammenfassung der Ψ-Terme. Andererseits können wir die Grade $\deg(D)$ aber auch in ihre P-Beiträge aufteilen und nach diesen sortiert aufsummieren. Die folgenden Summationen erstrecken sich über jeweils alle freien Parameter ($l, d \in \mathbb{Z}$ und $P \in \mathcal{P}l(F/k)$):

$$\begin{aligned} S(n,m) &= \sum_{\substack{D\ (n,m)\text{-glatt}\\ 0<lP\le D}} \deg(P) \;=\; \sum_{\substack{\deg(P)\le m\\ 0<l\deg(P)\le n}} \deg P \cdot \sum_{\substack{D\ (n,m)\text{-glatt}\\ lP\le D}} 1 \\ &= \sum_{\substack{\deg(P)\le m\\ 0<l\deg(P)\le n}} \deg(P)\cdot\Psi_{F/k}(n-l\deg(P),m) \\ &= \sum_{j=1}^{n} \Psi_{F/k}(n-j,m) \sum_{\substack{0<d\le m\\ d|j}} d\pi_d(F/k) \\ &= \sum_{j=0}^{n-1} \Psi_{F/k}(j,m)\cdot N_{F/k}(n-j,m). \end{aligned} \tag{4.4}$$

Durch Gleichsetzen von (4.3) und (4.4) ergibt sich die Formel in (*ii*). □

4.5. Bemerkung. Die Berechnung von $\Psi_{F/k}(n,m)$ kann mit Satz 4.2, Teil (ii) ganz praktikabel erfolgen, wohingegen sich Teil (i) dafür nicht besonders eignet. Zur Auflösung der Rekursion berechnet man die Werte $\Psi_{F/k}(j,m)$ für $0 \le j \le n$ und hat dann einen Aufwand von $O(n^2)$ Operationen, die Kenntnis von $N_{F/k}(j,m)$ vorausgesetzt. Für den Fall, daß $m \le g$ relativ groß im Verhältnis zu g ist, stellt letzteres das eigentliche Problem der Berechnung dar, weil dafür die Werte von $\pi_j(F/k)$ beziehungsweise $N_j(F/k)$ bekannt sein müssen. Wir bemerken, daß $N_{F/k}(n,m) = N_m(F/k) = q^m + 1 - \sum_{i=1}^{2g} \omega_i(F/k)^m$ für $n \le m$ gilt. Wenn $\Psi_{F/k}(n,m)$ nur approximiert werden soll, berechnet man $\pi_j(F/k)$ für ein paar kleine j und setzt für die anderen $\pi_j(F/k) \approx q^j/j$. Vorteilhaft wirkt sich hier der Umstand aus, daß die Abweichungen von $\pi_j(F/k)$ von q^j/j wegen Teil (ii) für größere j immer weniger vom Gesamtwert von $\Psi_{F/k}(n,m)$ ausmachen.

4.2 Untere Schranken

Es sollen nun asymptotische Aussagen über $\Psi_{F/k}(n,m)$ bewiesen werden.

4.6. Proposition. *Es sei F/k ein globaler Funktionenkörper des Geschlechts g und $\varepsilon \ge 1/2$. Für die Anzahl der (n,m)-glatten Divisoren von F/k mit $n, m \in \mathbb{Z}^{\ge 1}$ und $m \ge 2\log_q\big(2(g+\varepsilon)\big)$ gilt dann*

$$\Psi_{F/k}(n,m) \;\ge\; q^n / \exp\Big(\Big(\Big\lfloor \frac{n}{m} \Big\rfloor + 1 \Big) \; \big(\log(n) + g/\varepsilon \big) + 2\log\big(2(g+\varepsilon)\big) \Big) .$$

Beweis. Wir setzen $n = rm + b$ mit $0 \le b < m$. Die Rekursion in Satz 4.2, (ii) wird durch die ausschließliche Betrachtung der Terme für $j = \max\{n-m, 0\}$ aufgelöst: $\Psi_{F/k}(n,m) \ge n^{-1}(1 + N_{F/k}(m,m))\Psi_{F/k}(n-m,m)$ usw. und im letzten Schritt $\Psi_{F/k}(b,m) \ge n^{-1}(1 + N_{F/k}(b,b))$. Wir erhalten insgesamt

$$\Psi_{F/k}(n,m) \ge (1/n)^{r+1}(1 + N_{F/k}(m,m))^r (1 + N_{F/k}(b,b)). \tag{4.7}$$

Zu beachten ist im folgenden $N_{F/k}(m,m) \ge q^m - 2gq^{m/2}$ und $2gq^{-m/2} \le g/(g+\varepsilon)$ wegen $m \ge 2\log_q\big(2(g+\varepsilon)\big)$ nach Voraussetzung. Wenn auch $b \ge 2\log_q(2(g+\varepsilon))$ ist, haben wir mit Ausklammern von q durch Berücksichtigung aller Terme des Produkts (4.7):

$$\Psi_{F/k}(n,m) \ge (1/n)^{r+1} q^n (1 - g/(g+\varepsilon))^{r+1}. \tag{4.8}$$

Gilt andernfalls $b < 2\log_q(2(g+\varepsilon))$, so ergibt sich mit $q^b \le 2(g+\varepsilon)^2$ und $(1 + N_{F/k}(b,b)) \,/\, q^b \ge 2(g+\varepsilon)^{-2}$, indem der letzte Term des Produkts (4.7) fortgelassen wird:

$$\Psi_{F/k}(n,m) \ge (1/n)^{r+1} q^n (1 - g/(g+\varepsilon))^r (2(g+\varepsilon))^{-2}. \tag{4.9}$$

Wir erhalten daraus die Behauptung in beiden Fällen für $g = 0$ und für $g > 0$ wegen $\log(1 - 1/x) \geq -1/(x-1)$ für $x > 1$ angewendet auf $1 - g/(g+\varepsilon) = 1 - 1/(1+\varepsilon/g)$ mit $x = 1 + \varepsilon/g$. □

4.10. Satz. *Es seien $\beta, \varepsilon_0 \in \mathbb{R}^{>0}$ mit $\beta < 1$ und q eine Primpotenz. Dann gibt es $\gamma, \delta \in \mathbb{R}$, so daß für jeden globalen Funktionenkörper F/k vom Geschlecht g über dem exakten Konstantenkörper mit q Elementen die Ungleichung*

$$\Psi_{F/k}(n,m) \;\geq\; q^n \cdot \exp\big(-u\,(\log(u) + \log(\log(u)) + \gamma)\big)$$

für $u := n/m$ und alle $n, m \in \mathbb{Z}^{\geq \delta}$ mit

$$\begin{aligned} n^\beta \;&\geq\; m, \\ \min\{\, m, u \,\} \;&\geq\; (2+\varepsilon_0)\log_q(3g+1) \end{aligned}$$

gilt.

Beweis. Der Beweis basiert auf dem Vorgehen von [38] für den Fall $\mathbb{Z}$, vgl. [52]. Nach Voraussetzung gilt $u > 1$ für $m \geq 1$, so daß wir $b := (1 - 1/\log(u))m$ definieren können. Die nachfolgenden Abschätzungen erfordern eine gewisse Mindestgröße der Parameter n, m, u, b, die wir mittels dem nur von β, ε_0, q abhängigen δ sicherstellen. Für den Anfang sei also $\delta \geq 1$, wir werden es mehrfach vergrößern. Wir bemerken als erstes, daß mit $\delta \to \infty$ auch $u \to \infty$ wegen der Voraussetzungen gilt. Wir vergrößern δ, so daß $b \geq 1$ erfüllt ist.
Bis zum Beweisende bezeichnen wir nun mit D die Divisoren, die eine Summe von $\lfloor u \rfloor$ nicht notwendigerweise verschiedenen Stellen eines Grads $> b$ und $\leq m$ sind und setzen $d := \deg(D)$. Damit gilt $b\lfloor u \rfloor < d \leq m\lfloor u \rfloor \leq n$, und man erhält die untere Abschätzung

$$\Psi_{F/k}(n,m) \;\geq\; \sum_D \Psi_{F/k}(n-d, \lfloor b \rfloor), \tag{4.11}$$

weil die Träger der D und der durch $\Psi_{F/k}(n-d, \lfloor b \rfloor)$ gezählten Divisoren disjunkt sind. Wir schätzen nun die $\Psi_{F/k}(n-d, \lfloor b \rfloor)$ und danach die Summe nach unten ab. Die folgenden Ungleichungen werden dazu benötigt:

$$m^{(1-\beta)/\beta} \;\leq\; u, \tag{4.12}$$

welche aus den Voraussetzungen folgt, und

$$\begin{aligned} (n-d)/b \;&\leq\; \big\lfloor (n-d)/\lfloor b \rfloor \big\rfloor + 1 \\ &\leq\; 2(n-d)/b + 1 \qquad \leq \quad 2(n/b - \lfloor u \rfloor) + 1 \\ &\leq\; 2\big((1 - 1/\log(u))^{-1} u - u + 1\big) + 1 \\ &\leq\; 3u/\log(u), \end{aligned} \tag{4.13}$$

welche für alle Divisoren D gilt (für die zweite Abschätzung verwenden wir $b\lfloor u\rfloor < d$ wie oben, und für die letzte Abschätzung ist eine ausreichende Vergrößerung von δ und damit u erforderlich).
Wenn $n-d=0$ ist, so gilt $\Psi_{F/k}(n-d,\lfloor b\rfloor)=1$. Andernfalls wenden wir Proposition 4.6 mit $\varepsilon := (g+1)/2$ an. Dies ist zulässig aufgrund der Voraussetzungen an m und n. Unter Verwendung der Ungleichungen

$$2\log_q(2(g+\varepsilon)) = 2\log_q(3g+1) \le u$$

nach Voraussetzung,

$$\log(n-d) = \log((n-d)/b) + \log(b) \le \log(u) + \log(m)$$

wegen (4.13) für ausreichend großes δ und wegen $b \le m$ nach Definition von b, und

$$\log(m) \le \beta/(1-\beta)\log(u)$$

wegen (4.12) erhält man dann mit Proposition 4.6 und (4.13)

$$\begin{aligned}
\Psi_{F/k}(n-d,\lfloor b\rfloor) &\ge q^{n-d}/\exp\left(\left(\left\lfloor\tfrac{n-d}{\lfloor b\rfloor}\right\rfloor+1\right)(\log(n-d)+2)+2\log(3g+1)\right)\\
&\ge q^{n-d}/\exp\left((3u/\log(u))\,(\log(u)+\log(m)+2)+u\right)\\
&\ge q^{n-d}/\exp(cu), \qquad (4.14)
\end{aligned}$$

nach ausreichend großer Wahl von δ mit einer nur von β,ε_0,q abhängigen Konstante $c\in\mathbb{R}^{>0}$. Diese Ungleichung gilt für alle Divisoren D (auch für $n-d=0$). Wir wenden uns jetzt der Abschätzung der Summe in (4.11) zu. Wegen (4.14) bekommt (4.11) die Gestalt

$$\Psi_{F/k}(n,m) \;\ge\; q^n\cdot\exp(-cu)\cdot\sum_D q^{-d}. \qquad (4.15)$$

Auf die Summe über alle D greifen wir mittels

$$\sum_D q^{-d} \;=\; \left(\sum_{b<\deg(P)\le m} q^{-\deg(P)}\right)^{\lfloor u\rfloor}/\lfloor u\rfloor! \qquad (4.16)$$

zu, wobei sich die rechte Summe über alle Stellen P mit $b<\deg(P)\le m$ erstreckt (die $\lfloor u\rfloor$-Potenz bildet die Summe aller Werte q^{-d} unter Beachtung der Reihenfolge, weshalb durch $\lfloor u\rfloor!$ dividiert wird).
Nach wieder nur von β,ε_0,q abhängiger Vergrößerung von δ können wir aufgrund der Definition von b annehmen, daß wegen Satz 3.11, (ii) $q^{-j}\pi_j(F/k)\ge 1/m-(7g+2)q^{-b/2}/b$ für $b<j\le m$ gilt und daß wegen $m/b\to 1$ für $\delta\to\infty$ und wegen

$(2+\varepsilon_0)\log_q(3g+1) \le m$ nach Voraussetzung $(7g+2)mq^{-b/2}/b \le 1/2$ erfüllt ist. Unter Beachtung von $m - b = m/\log(u)$ erhalten wir:

$$\begin{aligned} \sum_{b<\deg(P)\le m} q^{-\deg(P)} &= \sum_{b<j\le m} q^{-j}\pi_j(F/k) \\ &\ge (m-b)\left(1/m - (7g+2)q^{-b/2}/b\right) \\ &\ge \log(u)^{-1}\cdot\left(1-(7g+2)mq^{-b/2}/b\right) \\ &\ge (2\log(u))^{-1}. \end{aligned} \tag{4.17}$$

Wegen $\lfloor u\rfloor! \le \exp(\lfloor u\rfloor \log(\lfloor u\rfloor))$ ergibt sich aus (4.17), (4.16) und (4.15):

$$\Psi_{F/k}(n,m) \;\ge\; q^n/\exp\bigl(u\,(\log(u)+\log(\log(u))+\gamma)\bigr)$$

für δ und γ, wobei γ die Summe der Konstanten $\log(2)$ aus (4.17) und c aus (4.14) ist. □

4.3 Glattheitsannahme für reduzierte Divisoren

4.18. Definition. Es sei S eine nicht-leere Teilmenge von $\mathcal{P}l(F/k)$. Für einen S-glatten Divisor A mit $\deg(A) \ge 1$ und $m \ge \deg(A)$ werden die S-glatten, entlang A maximal- beziehungsweise m-minimalreduzierten Divisoren mit $\mathcal{D}^{\max}_{\mathrm{red}}(S,A) := \mathcal{D}^{\max}_{\mathrm{red}}(F/k,A)\cap\mathcal{D}(S)$ beziehungsweise $\mathcal{D}^{m}_{\mathrm{red}}(S,A) := \mathcal{D}^{m}_{\mathrm{red}}(F/k,A)\cap\mathcal{D}(S)$ bezeichnet. Ihre Anzahlen erhalten wir mit „$N_{\mathrm{red}}()$“ statt „$\mathcal{D}_{\mathrm{red}}()$“.

Für spätere Komplexitätsanalysen benötigen wir die folgende Annahme über die Mindestanzahl glatter, minimalreduzierter Divisoren.

4.19. Glattheitsannahme. *Es seien $\alpha,\beta \in (0,1)$, $\alpha<\beta$. F/k durchlaufe eine Folge von Funktionenkörpern mit festem q und $g\to\infty$. Wir setzen voraus, daß F/k einen rationalen Teilkörper $k(x)$ mit $[F:k(x)] = O(1)$ besitzt. Es sei A ein Divisor von F/k mit $\deg(A) = O(1)$ und S die Menge aller Stellen von F/k eines Grads kleiner gleich m, wobei $n^\alpha \le m \le n^\beta$ mit $n := g+\deg(A)-1$ gelte. Dann nehmen wir an:*

$$N^{\deg(A)}_{\mathrm{red}}(S,A) \ge q^n/\exp\bigl(u\log(u)\bigr)^{(1+o(1))}.$$

Es handelt sich bei dieser Annahme also um Satz 4.10, ausgesprochen für zusätzlich entlang A $\deg(A)$-minimalreduzierte Divisoren, allerdings unter spezielleren Bedingungen. Wegen [55, S. 33, I.6.10] erscheint es plausibel (man kann auch Vergleichbares beweisen), daß ein zufällig gewählter positiver Divisor „kleinen“ Grads auch eine „kleine“ Dimension besitzt. Mit Annahme 4.19 übertragen wir diese Eigenschaft auf S-glatte Divisoren. Im Zahlkörperfall wird übrigens eine ähnliche Annahme ausgesprochen, vgl. [7].

Kapitel 5

Das Klassengruppenverfahren

In diesem Kapitel wird das Verfahren der Klassengruppenberechnung eines globalen Funktionenkörpers F/k des Geschlechts $g > 0$ über dem exakten Konstantenkörper k mit q Elementen beschrieben.

Unter der Berechnung der Klassengruppe $\mathcal{C}l^0(F/k)$ von F/k verstehen wir die Berechnung ihrer Struktur als endliche abelsche Gruppe

$$\mathcal{C}l^0(F/k) \cong \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}$$

mit $1 \leq c_1 \mid \ldots \mid c_m$ zusammen mit Divisoren $D_1, \ldots, D_m$ vom Grad null, deren Klassen den Erzeugern der zyklischen Faktoren entsprechen. Die ganze Divisorenklassengruppe $\mathcal{C}l(F/k)$ erhält man unter Hinzunahme eines Divisors A_1 vom Grad eins mit Proposition 1.1 in der Form

$$\mathcal{C}l(F/k) \cong \mathbb{Z} \times \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}.$$

Die Komplexitätsbetrachtungen konzentrieren sich auf die Situation $g \to \infty$, wobei alle sonstigen Größen als von g abhängig betrachtet und die O- beziehungsweise o-Aussagen gleichmäßig für jeden Funktionenkörper gelten werden, sofern das Geschlecht nur groß genug ist. Die erste, grundsätzliche Forderung ist $q = O(1)$. Wir setzen weiter voraus, daß F/k einen rationalen Teilkörper $k(x)$ mit $[F : k(x)] = O(1)$ besitzt. Die explizite Darstellung von F/k kann dann mit einem in y normierten und separablen, irreduziblen Polynom $f \in \tilde{k}[x, y]$ erfolgen, wobei $\tilde{k}$ einen Teilkörper von k bezeichnet und $\deg_y(f) = O(1)$ gilt. Die O- beziehungsweise o-Konstanten sind daher stets von g, F/k und $C_f = C_f(g)$ unabhängig.

Das Verfahren stützt sich im wesentlichen auf Methoden zur Berechnung des Geschlechts von F/k, der Stellen von F/k eines beliebigen, aber nicht zu großen Grads, der Riemann-Roch-Räume von Divisoren und der Hauptdivisoren (in freier Darstellung) von Elementen von F/k.

5.1 Prinzipielle Vorgehensweise

In diesem Abschnitt wird das dem Klassengruppenverfahren zugrundeliegende Prinzip als Berechnung spezieller S-Einheiten dargestellt und ein Rumpfalgorithmus angegeben. Wir beginnen mit

5.1. Satz (S-Einheiten). *Für eine endliche, nicht-leere Menge $S \subseteq \mathcal{P}l(F/k)$ von Stellen und $s := |S| - 1$ ist*

$$(\mathfrak{o}^S)^\times \;\cong\; \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}^s.$$

Beweis. $\mathcal{D}^0(S)$ ist frei vom Rang s. Die (nicht kanonische) Isomorphie ergibt sich, weil $\mathcal{P}(S)$ aufgrund der Endlichkeit der Klassenzahl endlichen Index in $\mathcal{D}^0(S)$ hat und weil es exakt die Elemente von $k^\times$ sind, deren Hauptdivisoren das Nullelement repräsentieren. Siehe auch [43]. □

Es genügen bereits endliche Mengen S, um $\mathcal{D}^0(S)/\mathcal{P}(S) \cong \mathcal{C}l^0(F/k)$ zu erhalten. In Satz 3.17 beziehungsweise Bemerkung 3.19 werden genauer Schranken für die Grade der dafür benötigten Stellen angegeben, so daß wir ein geeignetes S explizit bestimmen können. Die Klassengruppenberechnung läßt sich deswegen auf die Berechnung der entsprechenden S-Einheiten beziehungsweise ihrer Hauptdivisoren reduzieren. Allgemein sehen wir eine S-Einheitengruppe für endliches, nicht leeres S als berechnet an, wenn eine Basis bestehend aus Elementen von $(\mathfrak{o}^S)^\times$ für den freien Teil wie in Satz 5.1 bestimmt worden ist. Analoges gilt für die freie Gruppe $\mathcal{P}(S)$. Die Berechnung der Klassengruppe aus der S-Einheitengruppe beziehungsweise aus $\mathcal{P}(S)$ wird mit dem folgenden Lemma erreicht:

5.2. Lemma. *Für ein endliches $S = \{P_0, \ldots, P_s\}$ mit $s \geq 1$ seien Hauptdivisoren $(\alpha_1), \ldots, (\alpha_l)$ von S-Einheiten gegeben. Die von diesen Hauptdivisoren erzeugte Untergruppe von $\mathcal{P}(S)$ sei U. Durch Berechnung der Smith-Normalform der Matrix $M := (v_{P_i}(\alpha_j))_{i,j}$ erhalten wir den Rang m und Diagonalelemente $c_1 \,|\, \ldots \,|\, c_m$ von M und einen explizit gegebenen Isomorphismus*

$$\mathcal{D}(S)/U \;\cong\; \mathbb{Z}^{s+1-m} \times \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}.$$

Der maximal mögliche Rang der Matrix M ist s. Genau in diesem Fall hat U endlichen Index in $\mathcal{D}^0(S)$ und die Einschränkung der obigen Isomorphie ergibt

$$\mathcal{D}^0(S)/U \;\cong\; \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}.$$

Beweis. Die erste Isomorphieaussage ist an sich klar und folgt aus der Gestalt der Smith-Normalform von M: Bei ihrer Berechnung werden die $P_0, \ldots, P_s$ unimodular zu Divisoren $D_1, \ldots, D_{s+1}$ transformiert, so daß die ersten m Divisoren

D_i die Ordnung c_i und die restlichen $s+1-m$ unendliche Ordnung in $\mathcal{D}(S)/U$ haben. Per Definition entsprechen diese D_i unter dem Isomorphismus den Erzeugern der obigen zyklischen Faktoren. Der maximale Rang von M ist s, weil $\mathcal{P}(S)$ und $\mathcal{D}^0(S)$ Rang s haben. In diesem Fall hat nur D_{s+1} unendliche Ordnung in $\mathcal{D}(S)/U$. Weil die anderen endliche Ordnung haben, müssen sie den Grad null haben, sie bilden daher eine Basis von $\mathcal{D}^0(S)$, woraus sich die zweite Isomorphieaussage ergibt. Es sei angemerkt, daß der Grad von D_{s+1} gleich dem größten gemeinsamen Teiler der Grade der Stellen aus S ist, weil alle D_i zusammen eine Basis von $\mathcal{D}(S)$ bilden. □

Wir wenden uns jetzt der Berechnung der speziell für die Klassengruppe benötigten S-Einheitengruppe zu. Die folgende Namensgebung hat sich eingebürgert:

5.3. Definition. Eine Faktorbasis S ist eine endliche, nicht-leere Teilmenge von $\mathcal{P}l(F/k)$. S ist vollständig, wenn $\mathcal{D}^0(S)/\mathcal{P}(S) \cong \mathcal{C}l^0(F/k)$ gilt. Zu vorgegebener Faktorbasis S nennen wir die Hauptdivisoren von S-Einheiten auch Relationen.

Für den Rest dieses Abschnitts gehen wir davon aus, daß eine Methode zur Verfügung steht, die unter Eingabe einer noch zu bestimmenden Faktorbasis S der Reihe nach Relationen $(\alpha_1), (\alpha_2), \ldots$ produziert, für die es ein (uns unbekanntes) $l \in \mathbb{Z}^{\geq 1}$ gibt, so daß die ersten l Relationen (α_j) die Gruppe der S-glatten Hauptdivisoren $\mathcal{P}(S)$ (mit großer Wahrscheinlichkeit) erzeugen. Wir nennen diesen Prozeß *Relationensuche*. Wie dies bei spezieller Wahl von S zu bewerkstelligen ist, wird später erklärt. Die Bestimmung beliebiger S-Einheiten läßt sich im übrigen dann auf diesen speziellen Fall zurückführen.

Wir wählen jetzt eine vollständige Faktorbasis S. Die Idee ist dann die folgende: Die (α_j) werden der Reihe nach abgearbeitet und mit Lemma 5.2 (evtl. blockweise) ausgewertet, bis der Index der von den (α_j) erzeugten Gruppe U in $\mathcal{D}^0(S)$ endlich wird. Nun stellt sich die Frage, ob bereits $U = \mathcal{P}(S)$ gilt. Wir wissen aufgrund der Voraussetzung an S, daß der uns bekannte Index $(\mathcal{D}^0(S) : U)$ ein ganzzahliges Vielfaches der Klassenzahl $h(F/k) = (\mathcal{D}^0(S) : \mathcal{P}(S))$ ist. Mittels Satz 3.20 können wir die Klassenzahl aber auch approximieren und den Fehler abschätzen.

5.4. Lemma. *Es sei* $\bar{h} \in \mathbb{R}^\times$ *und* $I(\bar{h}) := \{x \in \mathbb{R} \mid 2^{-1/2} < x/\bar{h} < 2^{1/2}\}$. *Für jedes* $h \in I(\bar{h})$ *gilt dann* $h\mathbb{Z} \cap I(\bar{h}) = \{h\}$.

Beweis. Man kann ohne Einschränkung $\bar{h} > 0$ annehmen. Es sei $ah \in I(\bar{h})$ mit $a \in \mathbb{Z}^{>0}$. Durch Logarithmieren ergibt sich: $|\log(a)| = |\log(ah) - \log(h)| \leq |\log(ah) - \log(\bar{h})| + |\log(\bar{h}) - \log(h)| < \log(2)$, also $a = 1$. □

Unter Verwendung einer Approximation $\bar{h}$ der Klassenzahl $h(F/k)$, die so genau ist, daß $h(F/k) \in I(\bar{h})$ gilt, fahren wir mit der Auswertung weiterer (α_j) fort, bis $(\mathcal{D}^0(S) : U) \in I(\bar{h})$ erfüllt ist. Dann haben wir aufgrund des Lemmas $(\mathcal{D}^0(S) : U) = h(F/k)$, deswegen auch $U = \mathcal{P}(S)$, und sind fertig. Wir fassen das Vorgehen in einem Algorithmus zusammen:

5.5. Algorithmus. *(Klassengruppenverfahren)*

Eingabe: *Ein globaler Funktionenkörper F/k des Geschlechts $g > 0$ über dem endlichen Körper k mit q Elementen.*

Ausgabe: *Struktur und Erzeuger von $\mathcal{C}l^0(F/k)$.*

1. *(Erzeugungsschranke) Bestimme eine für die Erzeugung der Klassengruppe ausreichende obere Schranke $m_E = r \in \mathbb{Z}^{\geq 1}$ für die Grade der hierfür benötigten Stellen und einen Divisor A_1 vom Grad eins mittels Satz 3.17 und Proposition 3.15 durch die Berechnung der ersten Werte von $N_r(F/k)$ bis maximal* $\max\{\lceil 2\log_q(4g-2)\rceil, \lceil 2\log_q(2g)\rceil + 1\}$.

2. *(Approximation von $h(F/k)$) Berechne eine Approximation $\bar{h}$ der Klassenzahl $h(F/k)$ mittels Satz 3.20 unter Verwendung der Werte $N_r(F/k)$ bis $m_P \leq 2\log_q\big(3g/(q^{1/2}-1)\big)$, so daß der Fehlerterm kleiner* $\log(2)/2$ *wird.*

3. *(Vollständige Faktorbasis) Erstelle eine für die Relationensuche geeignete Faktorbasis S, die die Stellen von F/k eines Grads kleiner gleich m_E und den Träger von A_1 enthält.*

4. *(Relationensuche) Unter Verwendung von Lemma 5.2 und Lemma 5.4 wird die Relationensuche für S (blockweise) solange durchgeführt, bis eine Untergruppe U von $\mathcal{P}(S)$ von endlichem Index bekannt ist, für die $(\mathcal{D}^0(S) : U) \in I(\bar{h})$ gilt.*

5. *(Ende) Es gilt nun $U = \mathcal{P}(S)$. Unter Verwendung von Lemma 5.2 werden die für die Klassengruppenberechnung erforderlichen Daten bestimmt. Terminiere.*

5.6. Bemerkung. Die maximale Anzahl der in den Schritten 1 und 2 zu betrachtenden Stellen ist $O(g^2\log(g))$, so daß der Gesamtaufwand hierfür unter Beachtung von Abschnitt 1.2 und der Voraussetzungen am Anfang dieses Kapitels polynomial in gC_f ist. Die Kosten für Schritt 3 bis 5 ergeben sich im wesentlichen aus der Strategie der verwendeten Relationensuche und werden später untersucht. Die Abschätzung für m_P in Schritt 2 ergibt sich aus dem Fehlerterm in Satz 3.20 mit $2/\log(2) < 3$.

In der Praxis können die zu verwendenden, vollständigen Faktorbasen bei größerem g und q und damit auch M aus Lemma 5.2 relativ groß werden, so daß die Berechnung der Smith-Normalform zu aufwendig wird. In dieser Situation hilft in gewissem Rahmen eine Variation von Algorithmus 5.5: In Schritt 3 verzichten wir auf die Forderung, daß S vollständig sein soll. Das Abbruchkriterium in Schritt 4 wird nur mit der oberen Schranke beibehalten und liefert nicht notwendigerweise das gewünschte Ergebnis. Es ist jetzt nämlich möglich, daß nur eine Faktorgruppe von $\mathcal{D}^0(S)/U$ zu einer Untergruppe der Klassengruppe isomorph ist. Zur Erkennung beziehungsweise Behebung dieser Situation werden vor Schritt 5 Wurzeltests durchgeführt.

Bei den *Wurzeltests* handelt es sich um das folgende Vorgehen: Mit U sei eine Untergruppe von $\mathcal{P}(S)$ von endlichem Index bezeichnet. Mit Hilfe der letzten Isomorphie in Lemma 5.2 betrachten wir eine Auswahl solcher Divisoren $D \in \mathcal{D}^0(S)$, deren Klassen in $\mathcal{D}^0(S)/U$ eine Primzahlordnung l besitzen. Zusammen mit der Nullklasse bilden letztere einen $\mathbb{F}_l$-Vektorraum. Genau dann gilt $U = \mathcal{P}(S)$, wenn keiner der Divisoren D für keines der möglichen l ein Hauptdivisor ist. Wir testen dies für alle D (modulo $\mathbb{F}_l^\times$), und falls ein Hauptdivisor D gefunden wurde, können wir U erweitern beziehungsweise den Index von U in $\mathcal{P}(S)$ um l verkleinern, und beginnen mit den Tests für l von vorne. Der Aufwand dieser Berechnungen wird vom l-Rang der Gruppe $\mathcal{D}^0(S)/\mathcal{P}(S)$ dominiert. Schlimmstenfalls sind daher wegen Satz 3.14 mindestens $(l^{2g}-1)/(l-1)$ Wurzeltests für l durchzuführen, so daß das Verfahren im allgemeinen exponentiell in g ist. $\mathcal{D}^0(S)/\mathcal{P}(S)$ ist aber häufig zyklisch (oder ein Produkt weniger zyklischer Gruppen), so daß die Durchführung von Wurzeltests in diesem Fall recht effizient ist. Es sei angemerkt, daß die auftretenden Exponenten sehr groß werden können und daher Algorithmus 2.25 für die Hauptidealtests unentbehrlich ist. Vgl. auch [3, S. 16], [50, S. 54].

In der obigen Situation können wir nun mit den Wurzeltests aus $\mathcal{D}^0(S)/U$ die Untergruppe $\mathcal{D}^0(S)/\mathcal{P}(S)$ selbst erhalten. Wenn ihre Ordnung in $I(\bar{h})$ liegt, handelt es sich um die Klassengruppe, ansonsten um eine echte Untergruppe. Unter Verwendung einer nicht vollständigen Faktorbasis können wir also die von ihr erzeugte Untergruppe der Klassengruppe mit Hilfe der Wurzeltests (in unter Umständen exponentieller Zeit in g) berechnen.

Im Zahlkörperfall wird eine Methode für Wurzeltests basierend auf dem Cebotarevschen Dichtigkeitssatz zur Umgehung der $(l^{\mathrm{Rang}}-1)/(l-1)$-vielen Einzelschritte eingesetzt. Wie in [50, S. 55] beschrieben, ist dieses Verfahren im Funktionenkörperfall in der Praxis nicht effizient durchführbar. Dies liegt daran, daß Stellen eines Grads m mit $l \mid q^m - 1$ betrachtet werden müssen, und solche m sind häufig sehr groß (nicht selten $m = l-1$). Es sei schließlich auf die Analogie dieser Methode zur Tate-Lichtenbaum Paarung aus [16], siehe auch [15], hingewiesen.

5.2 Relationensuche

In diesem Abschnitt soll eine Übersicht über die Strategien zur Suche von Relationen gegeben werden. Wir fixieren dafür eine Faktorbasis $S = \{P_0, \ldots, P_s\}$ mit $s \geq 1$ und einen S-glatten Divisor A mit $\deg(A) \geq 1$.

Die allgemeine Form der *Relationensuche* besteht in der sukzessiven Berechnung der Schnitte $\big(\mathcal{L}(D)\big) \cap \mathcal{P}(S)$ für S-glatte Divisoren D, welche nach einer gewissen Strategie zu erzeugen sind. Die später berechneten Relationen entstehen im Prinzip alle auf diese Weise.

Mit den vorausgesetzten Möglichkeiten ist die Berechnung dieser Schnitte prinzipiell möglich. Man beschränkt sich sinnvollerweise auf Divisoren nicht-negativen Grads. Die Berechnung von $\mathcal{L}(D)$ erfolgt mit den Methoden des ersten Kapitels, danach kann (und offenbar muß) man für die Elemente von $\mathcal{L}(D)$ multiplikativ modulo Konstanten einzeln überprüfen, ob es sich um S-Einheiten handelt. Der Aufwand der Schnittberechnung ist damit a priori exponentiell im Grad der Divisoren D.

Es lassen sich drei allgemeine Situationen beziehungsweise Strategieansätze unterscheiden:

1.) Divisoren vom Grad null

Für die Schnittberechnung werden S-glatte Divisoren D vom Grad null verwendet. In diesem Fall gilt entweder $\dim(D) = 0$ oder $\dim(D) = 1$, und bei $\dim(D) = 1$ hat man eine S-Einheit gefunden. Die Wahrscheinlichkeit für $\dim(D) = 1$ bei zufälliger Wahl von D sollte ungefähr bei $1/h(F/k)$ liegen. Dieser Ansatz entspricht einem *Rechnen in abelschen Gruppen.*

2.) Divisoren eines kleinen Grads

Für die Schnittberechnung werden hier S-glatte Divisoren D eines kleinen Grads und positiver Dimension verwendet, die beispielsweise durch Divisorreduktion erhalten werden können. Ein $a \in \mathcal{L}(D)$ ist genau dann S-glatt, wenn $(a) + D$ S-glatt ist. Weil $(a) + D$ mit D kleinen Grad besitzt, besteht hierfür eine *Glattheitswahrscheinlichkeit.* Bei geeigneter Wahl von S fällt diese höher als $1/h(F/k)$ aus.

3.) Divisoren großen Grads

Es werden S-glatte Divisoren D mit großem Grad und großer Dimension verwendet, beispielsweise so groß, daß ein komplettes Erzeugendensystem der S-Einheiten in $\mathcal{L}(D)$ zu finden ist. Man könnte diesen Ansatz als *Direktberechnung von S-Einheiten* bezeichnen. Er ist unbrauchbar, weil wir nicht

in der Lage sind, die (relativ wenigen) S-Einheiten unter den sehr vielen Elementen von $\mathcal{L}(D)$ zu finden.

In der Schwierigkeit der Berechnung des Schnitts $\big(\mathcal{L}(D)\big) \cap \mathcal{P}(S)$ einer additiven mit einer multiplikativen Struktur ist also wegen 3.) ein grundlegendes Problem der Klassengruppenberechnung zu sehen. Zur Schnittberechnung bei großem Divisorgrad erwähnen wir deshalb zwei, leider vergebliche Ansätze, die auf notwendigen Bedingungen für die Glattheit eines Elements von $\mathcal{L}(D)$ beruhen: Es sei $a_1, \ldots, a_m$ eine Basis von $\mathcal{L}(D)$. Der erste Ansatz besteht darin, die Normen $\mathrm{N}_{F/k(x)}(a)$ von Elementen $a = \sum \lambda_i a_i \in \mathcal{L}(D)$ parametrisch auszurechnen und auf entsprechende Glattheit zu testen. Hierbei wird stark vereinfachend die Frage aufgeworfen, für welche Spezialisierungen der λ_i ein Polynom $h \in k[\lambda_1, \ldots, \lambda_m, x]$ nur aus Linearfaktoren besteht. Dies ist genau dann der Fall, wenn ein spezialisiertes h eine ausreichend hohe Potenz von $x^q - x$ teilt.
Der zweite Ansatz besteht darin, das durch a definierte, logarithmische Differential $(1/a)da$ parametrisch als Linearkombination der logarithmischen Differentiale der S-Einheiten wie am Ende von Abschnitt 3.4 darzustellen. In beiden Fällen erhält man dann jedoch nicht-lineare Gleichungen und Ungleichungen in großer Anzahl oder mit vielen freien Variablen (m ist groß), deren Lösung unter den gegebenen Umständen nicht mehr sinnvoll beziehungsweise möglich ist.

Es bleiben die Ansätze 1.) und 2.), auf die man sich stützen kann. Ansatz 1.) führt zu im Prinzip deterministischen Algorithmen, wohingegen 2.) einen probabilistischen Algorithmus liefert. Die folgenden Teilabschnitte geben einen Überblick über diese Methoden, bevor der probabilistische Ansatz dann eingehend behandelt wird.

5.2.1 Deterministische Methoden

Zur Berechnung unabhängiger Relationen beziehungsweise S-Einheiten kann man zwei Methoden unterscheiden.

Für die erste beschränken wir uns entsprechend 1.) auf die Betrachtung von Divisoren in $\mathcal{D}^0(S)$ und wollen herausfinden, welche davon in $\mathcal{P}(S)$ liegen. Wir können speziell die unabhängigen Divisoren $D_i := \deg(P_0)P_i - \deg(P_i)P_0$ für $1 \leq i \leq s$ betrachten. Für jedes solche i gibt es ein $m \in \mathbb{Z}$ mit $1 \leq m \leq (q^{1/2}+1)^{2g}$, so daß mD_i ein Hauptdivisor ist. Wir berechnen unabhängige S-Einheiten, indem wir für jedes m und jedes i testen, ob mD_i ein Hauptdivisor ist. Die einzelnen Tests sind mit Algorithmus 2.25 effizient zu bewerkstelligen. Zur Reduzierung des Aufwands in m kann man speziell beispielsweise die Baby-Step-Giant-Step Methode, vgl. [9, S. 235ff.], verwenden. Der Aufwand bleibt allerdings wegen der Schranke für m exponentiell in g.

Mit der eben beschriebenen, ersten Methode der Berechnung unabhängiger Relationen und den Wurzeltests aus Abschnitt 5.1 kann man also bereits $\mathcal{P}(S)$ und damit die Klassengruppe für eine vollständige Faktorbasis S deterministisch berechnen. Der Aufwand ist aber exponentiell in g. Allgemeiner können unter Verwendung von Divisoren vom Grad null und des Hauptdivisortests Techniken zum Berechnen der Struktur einer abelschen Gruppe von „innen“ heraus eingesetzt werden.

Die zweite Methode zur Berechnung unabhängiger Relationen verwendet bereits Divisorreduktion. Zu einer Folge von speziell oder zufällig gewählten S-glatten Divisoren D_i, $i = 1, 2, \ldots$ berechnen wir entlang A maximalreduzierte Divisoren $\widetilde{D}_i$ mit $D_i = \widetilde{D}_i + rA - (a_i)$. Weil diese reduzierten Divisoren positiv und von einem Grad kleiner $g + \deg(A)$ sind, ist ihre Anzahl endlich. Folglich gibt es j_1, j_2, so daß $\widetilde{D}_{j_1} = \widetilde{D}_{j_2}$ gilt, und in diesem Fall haben wir mit a_{j_1}/a_{j_2} eine S-Einheit gefunden. Wählen wir speziell $A = P_0$ und $D_{i,j} = i \deg(P_0)P_j$ für $1 \leq j \leq s$, so erhalten wir auf diese Weise für jedes j eine S-Einheit, deren Hauptdivisor von der Form $m_j \left(\deg(P_0)P_j - \deg(P_j)P_0\right)$ analog wie oben ist. Weil es mindestens $h(F/k)$ viele entlang A maximalreduzierte Divisoren gibt, ist der Aufwand dieser Berechnungen ebenfalls exponentiell in g.

Es sei an dieser Stelle auf die Verbindung der beiden Methoden zur Berechnung von Dirichlet-Einheiten [36, S. 48ff.], zur Relationenerzwingung [56, S. 46ff.] und zur Relationenerzeugung durch Idealreduktion [47] im Zahlkörperfall hingewiesen.

5.2.2 Probabilistische Methode

Die prinzipielle Verfahrensweise der probabilistischen Methode ist die folgende: Zu einem zufällig gegebenen Divisor D berechnen wir einen positiven Divisor $\widetilde{D}$ mittels Divisorreduktion, so daß $D = \widetilde{D} + rA - (a)$ gilt, ähnlich der zuvor beschriebenen Methode der reduzierten Divisoren. Ist $\widetilde{D}$ S-glatt, so hat man mit a eine Relation gefunden. Man stützt sich also bei dieser Methode nicht mehr auf die Gleichheit zweier $\widetilde{D}$, sondern auf ihre Glattheitswahrscheinlichkeit, und erhält ein Verfahren, welches eine wesentlich bessere Laufzeit als die zuvor beschriebenen Methoden hat. Die probabilistische Methode und ihre Erfolgswahrscheinlichkeit werden im nächsten Abschnitt eingehend beschrieben.

5.3 Probabilistische Methode

In diesem Abschnitt wird die probabilistische Methode der Relationensuche beschrieben, auf die wir uns im Klassengruppenverfahren hauptsächlich stützen.

Die Beschreibung bleibt theoretisch, so daß in dem darauffolgenden Abschnitt die Vorgehensweise in der Praxis erläutert wird. Insbesondere untersuchen wir jetzt das asymptotische Verhalten für $g \to \infty$, wobei ähnlich wie in [7] vorgegangen wird, vgl. auch [53].

5.3.1 Situation und Strategie der Relationensuche

Mit $S = \{P_0, \ldots, P_s\}$, $s \geq 1$ bezeichnen wir wieder eine Faktorbasis und mit A einen positiven, S-glatten Divisor, $\deg(A) \geq 1$.

Die von A erzeugte Untergruppe von $\mathcal{D}(S)$ ist $\langle A \rangle$. Wir betrachten die Projektion $pr_{S,A} : \mathcal{D}(S) \longrightarrow \mathcal{D}(S)/\langle A \rangle$. Ihre Einschränkung auf $\mathcal{D}^m(S)$ ist für alle $m \in \mathbb{Z}$ injektiv, aber nicht unbedingt surjektiv. Wir bemerken insbesondere, daß $\mathcal{P}(S)$ ein isomorphes Bild in $\mathcal{D}(S)/\langle A \rangle$ besitzt.

Wenn A ein Primdivisor ist, sieht man unmittelbar, daß $\mathcal{D}(S)/\langle A \rangle \cong \mathbb{Z}^s$ gilt. Im allgemeinen erhält man einen Epimorphismus in der folgenden Weise: Wir dividieren A durch den größten gemeinsamen Teiler der Exponenten von A und erhalten einen „primitiven“ Divisor D_0. Durch unimodulare Ergänzung erhalten wir weiter Divisoren $D_1, \ldots, D_s$, so daß $S' := \{D_0, \ldots, D_s\}$ eine Basis von $\mathcal{D}(S)$ ist. Mit dieser Basis ergibt sich die Isomorphie $\mathcal{D}(S)/\langle D_0 \rangle \cong \mathbb{Z}^s$ und der angekündigte Epimorphismus $\mathcal{D}(S)/\langle A \rangle \longrightarrow \mathcal{D}(S)/\langle D_0 \rangle \cong \mathbb{Z}^s$.

Durch diese Abbildungen erhalten wir zusammenfassend ein ebenfalls epimorphes $\lambda_{S,A} : \mathcal{D}(S) \longrightarrow \mathbb{Z}^s$. Das isomorphe Bild von $\mathcal{P}(S)$ unter $\lambda_{S,A}$ in $\mathbb{Z}^s$ bezeichnen wir mit $\Lambda_{S,A}$. Die Berechnung von $\mathcal{P}(S)$ kann damit auf die Berechnung von $\Lambda_{S,A}$ zurückgeführt werden. Wegen Korollar 1.4 angewendet auf D_0 statt A wissen wir, daß $(\mathbb{Z}^s : \Lambda_{S,A}) \leq \deg(A) h(F/k)$ gilt. Das Bild von $\mathcal{D}_{\mathrm{red}}^{\deg(A)}(S, A)$ unter $\lambda_{S,A}$ wird schließlich mit $\Lambda_{S,A}^{\mathrm{red}}$ bezeichnet.

Für die Berechnung von Bildern und Urbildern unter $\lambda_{S,A}$ benötigen wir zusätzlich eine Beschränktheitseigenschaft von $\lambda_{S,A}$ im Hinblick auf $g \to \infty$. Wir fordern, daß die Grade der P_i aus S polynomial in g und daß der Grad von A, die Anzahl der in A vorkommenden Stellen sowie die betragliche Summe ihrer Exponenten in A alle $O(1)$ sind. Wenn wir dann die Basis S' nicht „absichtlich schlecht“ wählen, können wir von folgendem ausgehen: Es sei $T \in \mathbb{Z}^{(s+1)\times(s+1)}$ die unimodulare Transformationsmatrix mit $(D_0, \ldots, D_s) = (P_0, \ldots, P_s)T$. Es gibt ein positives $c_0 = O(1)$, so daß für die Maximumnormen $c_0^{-1}\|v\|_\infty \leq \|Tv\|_\infty \leq c_0\|v\|_\infty$ für alle $v \in \mathbb{Z}^{s+1}$ gilt. Die Basen S und S' sollen sich also nicht zu sehr „unterscheiden“. Diese Forderungen lassen sich beispielsweise dann erfüllen, wenn A ein Primdivisor vom Grad eins oder die Differenz zweier Primdivisoren aus S ist. Weil der Grad der Körpererweiterung $F/k(x)$ nach Voraussetzung $O(1)$ ist, können diese Forderungen auch für $A = (x)_\infty$ erfüllt werden.

5.7. Bemerkung. Es gilt $|\Lambda_{S,A}^{\mathrm{red}}| \geq N_{\mathrm{red}}^{\deg(A)}(S,A)/\deg(A)$, weil sich zwei entlang A $\deg(A)$-minimalreduzierte Divisoren nicht um ein Vielfaches von A, eventuell aber um ein Vielfaches von D_0 unterscheiden. Weiter ist für jedes $v \in \Lambda_{S,A}^{\mathrm{red}}$ nach der obigen Beschränktheitsforderung $\|v\|_\infty < c_0\big(g + \deg(A)\big)$ erfüllt. Außerdem bemerken wir noch einmal, daß wir $(\mathbb{Z}^s : \Lambda_{S,A}) \leq \deg(A)h(F/k)$ haben.

5.8. Definition. Die Relationenabbildung $r_{S,A}$ wird definiert als

$$r_{S,A} : \Lambda_{S,A}^{\mathrm{red}} \times \Lambda_{S,A} \longrightarrow \mathbb{Z}^s, \quad (v_1, v_2) \mapsto v_1 + v_2$$

und für ihre Umkehrung betrachten wir ($2^{\Lambda_{S,A}}$ ist die Potenzmenge von $\Lambda_{S,A}$)

$$u_{S,A} : \mathbb{Z}^s \longrightarrow 2^{\Lambda_{S,A}}, \quad u_{S,A}(v) := \{\, v_2 \in \Lambda_{S,A} \mid r_{S,A}(v_1, v_2) = v \text{ für } v_1 \in \Lambda_{S,A}^{\mathrm{red}} \,\}.$$

Unter der Relationensuche verstehen wir nun spezieller die sukzessive Berechnung von Bildern unter $u_{S,A}$. Dies kommt der Aufgabe gleich, alle entlang A $\deg(A)$-minimalreduzierten und S-glatten Divisoren $\widetilde{D}$ mit $D = \widetilde{D} + rA - (a)$ für die Divisoren $D \in \lambda_{S,A}^{-1}(v)$ zu bestimmen. Letztere unterscheiden sich voneinander nur durch Vielfache von D_0.
Den Aspekten 1.) und 2.) aus Abschnitt 5.2 wird durch die Verwendung der entlang A $\deg(A)$-minimalreduzierten Divisoren Rechnung getragen, denn dadurch bleiben die auftretenden Dimensionen klein.

5.9. Algorithmus. *(Berechnung von $u_{S,A}$)*

Eingabe: *Die Divisoren A, $D_0, \ldots, D_s$ und ein $v \in \mathbb{Z}^s$.*

Ausgabe: *Die Menge $R_v \subseteq \Lambda_{S,A}$ mit $u_{S,A}(v) = R_v$.*

1. *(Divisoren mod A berechnen) Berechne den Divisor $D := \sum_{i=1}^{s} v_i D_i$, wobei die v_i die Koeffizienten von v sind. Berechne die Divisoren $D_i' := D + iD_0$ für $i := 0, \ldots, \deg(A)/\deg(D_0) - 1$.*

2. *(Reduzierte Divisoren) Berechne mit Algorithmus 2.21 und Bemerkung 2.24 alle entlang A $\deg(A)$-minimalreduzierten Divisoren $\widetilde{D}_{i,j}$ mit $D_i' := \widetilde{D}_{i,j} + r_{i,j}A - (a_{i,j})$.*

3. *(Glattheit) Berechne die Menge J der Indizes (i,j), für die $\widetilde{D}_{i,j}$ ein S-glatter Divisor ist. Setze $R_v := \{\, v - \lambda_{S,A}(\widetilde{D}_{i,j}) \mid (i,j) \in J \,\}$.*

4. *(Ende) Ausgabe von R_v. Terminiere.*

5.10. Bemerkung. Die Anzahl der entlang A $\deg(A)$-minimalreduzierten Divisoren $\widetilde{D}_{i,j}$ im zweiten Schritt beträgt maximal $\deg(A)(q^{\deg(A)}-1)/(q-1)$ wegen Bemerkung 2.24. Die ersten beiden Schritte benötigen damit einen Aufwand $O(1)\log\big(\|v\|_\infty\big)(gC_f)^{O(1)}s$, nach den Voraussetzungen an S, A, T und wegen Bemerkung 2.22. Für die Glattheitstests ist zu beachten, daß die $\widetilde{D}_{i,j}$ positive Divisoren eines Grads kleiner gleich $g+\deg(A)$ in Idealdarstellung sind. Unter Verwendung von Faktorisierungen der $\widetilde{D}_{i,j}$ beziehungsweise ihrer Normen und mit Hilfe einer Ordnung für die unter Stellen aus S liegenden Stellen von $k(x)$ kann man den Glattheitstest in einer Laufzeit von $O(1)(gC_f)^{O(1)}\log(s)$ durchführen, indem die berechneten Stellen in der Faktorbasis (binär) gesucht werden, und erhält dabei die freie Darstellung von $\widetilde{D}_{i,j}$. Damit ist die Gesamtlaufzeit von Algorithmus 5.9 $O(1)\log\big(\|v\|_\infty\big)(gC_f)^{O(1)}s$ (die ersten beiden Schritte bleiben bestimmend für den s-Anteil).

Nach Festlegung der Situation für die Relationensuche und der Beschreibung, wie sie für einzelne $v \in \mathbb{Z}^s$ durchzuführen ist, kommen wir nun zur Strategie der Erzeugung dieser Vektoren. Mit $l_{S,A} := \deg(A)^2(q^{1/2}+1)^{4g}$ definieren wir hierfür zwei Quader $Q_{S,A}$, $Q_{S,A}^{\mathrm{red}} \subseteq \mathbb{Z}^s$ durch

$$\begin{aligned} Q_{S,A} &:= [\,0,\, l_{S,A}\,]^s \cap \mathbb{Z}^s, \\ Q_{S,A}^{\mathrm{red}} &:= \big[\,-c_0\big(g+\deg(A)\big),\, l_{S,A}+c_0\big(g+\deg(A)\big)\,\big]^s \cap \mathbb{Z}^s. \end{aligned}$$

Die in Algorithmus 5.5, Schritt 4 durchzuführende Relationensuche besteht nun einfach in der *zufälligen* (und *gleichverteilten*) Erzeugung von Vektoren $v \in Q_{S,A}^{\mathrm{red}}$ als Eingabe für Algorithmus 5.9, und zwar solange, bis ein Erzeugendensystem von $\Lambda_{S,A}$ beziehungsweise $\mathcal{P}(S)$ gefunden wurde (dies kann mit den Methoden des Abschnitts 5.1 getestet werden).

5.3.2 Erfolgswahrscheinlichkeit

Durch die sukzessive Berechnung von $u_{S,A}$ erhält man also eine (eventuell leere) Folge von Vektoren aus $\Lambda_{S,A}$ beziehungsweise eine Folge von Elementen aus $\mathcal{P}(S)$. Wir wenden uns jetzt der Frage zu, inwiefern Vektoren aus $\Lambda_{S,A}\backslash U$ für ein echtes Teilgitter U von $\Lambda_{S,A}$ durch die Berechnung von $u_{S,A}$ für Vektoren des Quaders $Q_{S,A}^{\mathrm{red}}$ erhalten werden können.

5.11. Lemma. *Für $l \to \infty$ seien $s = o(l^{1/2})$, $s \geq 1$, und $Q_l := [0,l]^s$ ein Quader im $\mathbb{Z}^s$. Für jedes Gitter Λ vom Rang s im $\mathbb{Z}^s$ mit $d(\Lambda) := (\mathbb{Z}^s : \Lambda) \leq l^{1/2}$ gilt:*

$$|\Lambda \cap Q_l| \;=\; \frac{1+o(1)}{d(\Lambda)} \cdot |Q_l|. \tag{5.12}$$

Für jedes echte Teilgitter U eines solchen Gitters Λ gilt:

$$|(\Lambda\backslash U)\cap Q_l| \;\geq\; \frac{1+o(1)}{2\,d(\Lambda)}\cdot|Q_l|. \tag{5.13}$$

Wenn zusätzlich U den Rang s hat und eine Basis in Q_l besitzt, so gilt:

$$(\Lambda : U) \;\leq\; (s^{1/2}l)^s/d(\Lambda) \;\leq\; (s^{1/2}l)^s. \tag{5.14}$$

Beweis. Wir betrachten eine Basis von Λ in Hermite-Normalformgestalt und bezeichnen mit $d_i \in \mathbb{Z}^{\geq 1}$ die Einträge auf den Stufen. Dann haben wir $\big|d_i\mathbb{Z}\cap[0,l]\big| = \lfloor l/d_i\rfloor + 1$ und unter Beachtung der Stufengestalt der Basis ergibt sich, daß $|\Lambda\cap Q_l| = \prod_{i=1}^{s}\big(\lfloor l/d_i\rfloor+1\big)$ ist. Aus dieser Gleichung erhalten wir wegen $d_i \leq d(\Lambda) \leq l^{1/2}$:

$$(l+l^{1/2})^s\,/\,d(\Lambda) \;\;\geq\;\; |\Lambda\cap Q_l| \;\;\geq\;\; l^s\,/\,d(\Lambda). \tag{5.15}$$

Nun haben wir $(l+l^{1/2})^s\,/\,|Q_l| \leq (1+l^{-1/2})^s = 1+o(1)$ und ähnlich $l^s\,/\,|Q_l| = 1+o(1)$ wegen $s = o(l^{1/2})$ und weil allgemein $(1+1/x)^x \to e$ für $x\to\infty$ gilt. Aus (5.15) ergibt sich damit (5.12).
Ist r der Rang von U, so gibt es $\nu_j, w_{\nu_j} \in \mathbb{Z}^{\geq 1}$, so daß die Stufenelemente von U durch $w_{\nu_j}d_{\nu_j}$ gegeben werden und $|U\cap Q_l| \leq \prod_{j=1}^{r}\big(\lfloor l/(w_{\nu_j}d_{\nu_j})\rfloor+1\big)$ gilt. Hieraus erhalten wir für $r<s$

$$|U\cap Q_l| \;\;\leq\;\; (l+1)^{s-1} \tag{5.16}$$

und für $r=s$ wegen $|U\cap Q_l| \leq d(\Lambda)^{-1}\prod_{j=1}^{s}\big(l/w_{\nu_j}+d_{\nu_j}\big)$ und weil mindestens ein $w_{\nu_j}\geq 2$ ist:

$$|U\cap Q_l| \;\;\leq\;\; \big(l+2l^{1/2}\big)^s\,/\,\big(2d(\Lambda)\big). \tag{5.17}$$

Hat U nicht vollen Rang, so gilt nach (5.15) und (5.16)

$$\begin{aligned}|(\Lambda\backslash U)\cap Q_l| &\geq l^s/d(\Lambda) - (l+1)^{s-1}\\ &= \big((1+1/l)^{-s} - d(\Lambda)/(l+1)\big)\;|Q_l|\,/\,d(\Lambda)\\ &= \big(1+o(1)\big)\;|Q_l|\,/\,d(\Lambda).\end{aligned}$$

Hat U Rang s, so gilt nach (5.15) und (5.17)

$$\begin{aligned}|(\Lambda\backslash U)\cap Q_l| &\geq l^s/d(\Lambda) - (l+2l^{1/2})^s\,/\,\big(2d(\Lambda)\big)\\ &= l^s\big(2-(1+2l^{-1/2})^s\big)\,/\,\big(2d(\Lambda)\big)\\ &= l^s\big(1+o(1)\big)\,/\,\big(2d(\Lambda)\big).\end{aligned}$$

Mit $l^s/|Q_l| = 1+o(1)$ ergibt sich die Ungleichung (5.13) in beiden Fällen.
Die letzte Aussage (5.14) über den Index von U folgt mit der Abschätzung der Determinante einer aus s unabhängigen Vektoren von U in Q_l gebildeten Matrix mit Hilfe der Hadamard-Schranke. □

5.18. Lemma. *Für $g \to \infty$ sei $s = o\big(l_{S,A}^{1/2}\big)$, $s \geq 1$. Mit $R'_v := \Lambda_{S,A}^{\mathrm{red}} \times \big(\Lambda_{S,A} \cap Q_{S,A}\big)$ gilt:*

$$r_{S,A}(R'_v) \;\subseteq\; Q_{S,A}^{\mathrm{red}},$$

$$\big|r_{S,A}(R'_v)\big| \;\geq\; \frac{\big(1+o(1)\big)\, N_{\mathrm{red}}^{\deg(A)}(S,A)}{\deg(A)^2\, h(F/k)} \cdot \big|Q_{S,A}^{\mathrm{red}}\big|.$$

Beweis. Die Aussage $r_{S,A}(R'_v) \subseteq Q_{S,A}^{\mathrm{red}}$ folgt aus Bemerkung 5.7. Wir beachten nun drei Aussagen: Erstens, $h(F/k) \leq (q^{1/2}+1)^{2g}$ nach Korollar 3.13; zweitens, $r_{S,A}$ ist in jedem Argument injektiv; drittens, wegen $s = o(l_{S,A}^{1/2})$ gilt $|Q_{S,A}| = (1+o(1))\,|Q_{S,A}^{\mathrm{red}}|$. Mit Lemma 5.11, (5.12) angewendet auf $\Lambda_{S,A}$ und den Quader $Q_{S,A}$ erhalten wir damit, daß das Bild $r_{S,A}(R'_v)$ für jede feste Wahl eines $v_1 \in \Lambda_{S,A}^{\mathrm{red}}$ $(1+o(1))\,|Q_{S,A}^{\mathrm{red}}| \,/\, (\deg(A) h(F/k))$ Elemente enthält. Wegen Bemerkung 5.7 vervielfältigt sich diese Anzahl um mindestens $N_{\mathrm{red}}^{\deg(A)}(S,A)/\deg(A)$, wenn man $v_1 \in \Lambda_{S,A}^{\mathrm{red}}$ variiert, und daraus ergibt sich die obige Abschätzung. □

5.19. Lemma. *Es seien $\alpha, \beta \in (0,1)$ und $n := g + \deg(A) - 1$. Für $g \to \infty$ gilt bei Wahl der speziellen Faktorbasis $S := \mathcal{P}l^{\leq m}(F/k)$ mit $n^\alpha \leq m \leq n^\beta$ und $u := n/m$ sowie unter der Glattheitsannahme 4.19:*

$$\frac{N_{\mathrm{red}}^{\deg(A)}(S,A)}{\deg(A)^2\, h(F/k)} \;\geq\; \exp\big(-u\log(u)\big)^{(1+o(1))}.$$

Beweis. Der Faktor $\deg(A)^2$ wird von dem $(1+o(1))$ aufgenommen, so daß man sich auf die Betrachtung des Quotienten $N_{\mathrm{red}}^{\deg(A)}(S,A) \,/\, h(F/k)$ beschränken kann. Wegen Satz 3.22 mit den Voraussetzungen an F/k über die Existenz eines rationalen Teilkörpers und der Glattheitsannahme 4.19 ergibt sich die Behauptung für $N_{\mathrm{red}}^{\deg(A)}(S,A) \,/\, h(F/k)$, indem man beachtet, daß die Fehlerterme ebenfalls in den $(1+o(1))$-Ausdruck aufgenommen werden können. □

5.20. Proposition. *Es seien $p_0, p_1 \in \mathbb{R}^{>0}$ mit $p_0 + p_1 = 1$ und bezeichne V einen Algorithmus, der mit einer Wahrscheinlichkeit von p_1 das Ergebnis „wahr“ liefert.*

(*i*) *Die erwartete Mindestanzahl von Ausführungen von V, um genau r-mal das Ergebnis „wahr“ zu erhalten, beträgt r/p_1.*

(*ii*) *Die Wahrscheinlichkeit, in $\lfloor p_1^{-1} \rfloor$ Ausführungen von V mindestens einmal das Ergebnis „wahr“ zu erhalten, strebt mit $p_1 \to 0$ gegen $1 - 1/e$.*

(*iii*) *Es gibt ein $k_0 = k_0(p_1) \in \mathbb{R}^{\geq 2}$, so daß die Wahrscheinlichkeit, nach $k_0 r$ Ausführungen von V mindestens r-mal das Ergebnis „wahr“ zu erhalten, mit $r \to \infty$ gegen 1 strebt.*

Beweis. Wir bezeichnen mit X_r die Mindestanzahl von Ausführungen von V, welche genau r-mal „wahr“ liefern. Es gilt also $X_r = w$, wenn die letzte und davor beliebige $r-1$ von insgesamt w Ausführungen von V den „wahr“-Wert ergeben. Dies tritt folglich mit einer Wahrscheinlichkeit von

$$p(X_r = w) = \binom{w-1}{r-1} p_1^r \, p_0^{w-r}$$

ein. Für den Erwartungswert von X_r ergibt sich damit

$$\begin{aligned} E(X_r) &= \sum_{w=0}^{\infty} w\, p(X_r = w) = \sum_{w=r}^{\infty} w \binom{w-1}{r-1} p_1^r \, p_0^{w-r} \\ &= \frac{p_1^r}{(r-1)!} \sum_{w=r}^{\infty} w(w-1)\cdots(w-r+1)\, p_0^{w-r} \\ &= \frac{p_1^r}{(r-1)!} \cdot \frac{d^r}{dx^r}(1-x)^{-1}\big|_{x=p_0} = \frac{p_1^r}{(r-1)!} \cdot \frac{r!}{(1-p_0)^{r+1}} \\ &= r/p_1, \end{aligned}$$

womit Teil (i) bewiesen wäre. Für Teil (ii) beachtet man, daß die Wahrscheinlichkeit, keinmal den Wert „wahr“ zu erhalten, $(1-p_1)^{\lfloor p_1^{-1} \rfloor}$ beträgt, welches für $p_1 \to 0$ gegen $1/e$ strebt.
Zum Beweis von Teil (iii) wird ein $k_0 \in \mathbb{R}^{\geq 2}$ mit $p_0^{k_0-1} e k_0 < 1$ gewählt und $w := k_0 r$ gesetzt. Wir betrachten die Wahrscheinlichkeit $p(X_r \leq w)$, in w Ausführungen von V mindestens r-mal den Wert „wahr“ zu erhalten:

$$p(X_r \leq w) \;=\; \sum_{j=r}^{w} \binom{w}{j} p_1^j \, p_0^{w-j}.$$

Für die Komplementärwahrscheinlichkeit folgt unter Verwendung der Stirlingschen Formel in der Form $\log(n!) = n(\log(n) - 1 + o(1))$

$$\begin{aligned} p(X_r > w) &= \sum_{j=0}^{r-1} \binom{k_0 r}{j} (1-p_0)^j \, p_0^{k_0 r - j} \\ &\leq r\, p_0^{(k_0-1)r} \binom{k_0 r}{r} \leq r\, p_0^{(k_0-1)r} \, (k_0 r)^r / r! \\ &\leq \left(p_0^{k_0-1} e k_0\right)^r e^{o(r)} \end{aligned}$$

welches für wachsendes r nach Wahl von k_0 gegen null strebt. □

5.21. Lemma. *Für $g \to \infty$ berechnet man mit den Voraussetzungen von Lemma 5.19 ein Erzeugendensystem von $\Lambda_{S,A}$, bestehend aus $q^{m+o(1)}$ Elementen,*

nach erwartungsgemäß $u^{u(1+o(1))}\,q^m$ Anwendungen von Algorithmus 5.9 auf zufällig (und gleichverteilt) gewählte Vektoren aus $Q_{S,A}^{\mathrm{red}}$ mit gegen 1 strebender Wahrscheinlichkeit.

Beweis. Wir stellen die Beobachtung voran, daß die Größe s der Faktorbasis S nach Lemma 3.12 durch $q^{m+o(1)}$ beschränkt wird. Wegen Lemma 5.18 und 5.19 kann daher $u^{-u(1+o(1))}$ als untere Schranke für die Wahrscheinlichkeit aufgefaßt werden, ein Element von $\Lambda_{S,A}$ durch zufällige Wahl eines Vektors aus $Q_{S,A}^{\mathrm{red}}$ und Anwendung von Algorithmus 5.9 zu erhalten. Mit Proposition 5.20, (ii) erhalten wir daher für ausreichend großes g nach $u^{u(1+o(1))}$ Versuchen eine Relation mit einer Wahrscheinlichkeit größer 1/2. Bezeichne U ein (von bisher gefundenen Relationen aufgespanntes) echtes Teilgitter von $\Lambda_{S,A}$. Wenn eine Relation v gefunden wird, so können wir wegen Lemma 5.11, (5.13) mit einer Wahrscheinlichkeit von beispielsweise mindestens 1/3 davon ausgehen, daß $v \in \Lambda_{S,A}\backslash U$ ist. Wenn der Rang von U kleiner als s ist, kann man für die Wahrscheinlichkeit $v \in \Lambda_{S,A}\backslash\mathbb{Q}\cdot U$ sogar die gleiche untere Schranke annehmen. Wir wenden Proposition 5.20, (i), (iii) mit dem Algorithmus $V :=$ „ $u^{u(1+o(1))}$-malige Anwendung von Algorithmus 5.9 auf zufällige Vektoren aus $Q_{S,A}^{\mathrm{red}}$ “ an, wobei „wahr“ bedeuten soll, daß eine neue, ggf. den Rang vergrößernde Relation gefunden wurde. Die Wahrscheinlichkeit p_1 beträgt dann entsprechend obigem mindestens 1/6. Nach erwartungsgemäß $6s$ Anwendungen von V erhält man ein U mit endlichem Index in $\Lambda_{S,A}$ und nach weiteren, erwartungsgemäß $O(sg)$ Anwendungen wegen Lemma 5.11, (5.14) sogar ein Erzeugendensystem von $\Lambda_{S,A}$, denn der Index verringert sich immer um einen Faktor von mindestens 2. Weil die konstanten Faktoren und selbst g in den $o(1)$-Ausdruck im Exponenten übernommen werden können, ergibt sich die Aussage des Lemmas mit Proposition 5.20. □

5.3.3 Komplexität

Zur Minimierung der Anwendungen von Algorithmus 5.9 in Lemma 5.21 gilt es nun $m = m(n)$ so zu bestimmen, daß der Aufwand asymptotisch möglichst klein wird. Im Exponenten findet sich hier bis auf den $(1+o(1))$-Faktor ein Ausdruck der Form $(n/m)\log(n/m) + cm$. Man kann sich überlegen, daß dieser Ausdruck asymptotisch für $m = \big(\beta + o(1)\big)\sqrt{n\log(n)}$ mit einem geeigneten, festen $\beta \in \mathbb{R}^{>0}$ minimiert wird und dort den Wert $\big((2\beta)^{-1} + c\beta + o(1)\big)\sqrt{n\log(n)}$ besitzt. Hieraus ergibt sich unter Minimierung des Vorfaktors $\beta = 1/\sqrt{2c}$ und $(2\beta)^{-1} + c\beta = \sqrt{2c}$. Wir stoßen somit auf die für komplexitätstheoretische Aussagen häufig benötigte Funktion

$$L(a,x) := \exp\big(\sqrt{x\log(x)}\big)^a.$$

5.22. Satz. *Mit der Glattheitsannahme 4.19 und unter Verwendung einer geeigneten Faktorbasis bestehend aus*

$$L\big(1/\sqrt{2\log(q)} + o(1),\, g\big)$$

Stellen berechnet man ein Erzeugendensystem des Gitters $\Lambda_{S,A}$ asymptotisch derselben Größe

$$L\big(1/\sqrt{2\log(q)} + o(1),\, g\big)$$

durch

$$L\big(\sqrt{2\log(q)} + o(1),\, g\big)$$

Anwendungen von Algorithmus 5.9 auf zufällig und gleichverteilt gewählte Vektoren aus $Q_{S,A}^{\mathrm{red}}$ mit gegen 1 strebender Wahrscheinlichkeit.

Beweis. Folgt mittels der obigen Minimierung des Faktors $(2\beta)^{-1} + c\beta$ und $c = \log(q)$, Lemma 5.21 und unter Beachtung von $\deg(A) = O(1)$. □

Bei diesem Satz handelt es sich im Prinzip um die komplexitätsbestimmende Kernaussage über das Verhalten der probabilistischen Relationensuche.

Nach der Berechnung des (wahrscheinlichen) Erzeugendensystems in Schritt 4 von Algorithmus 5.5 mit der beschriebenen Methode müssen allerdings noch die Struktur und Erzeugende der Klassengruppe mit Lemma 5.2 in Schritt 5 bestimmt werden, wobei sich dieser und der von Algorithmus 5.9 gelieferte Anteil an der Gesamtkomplexität als nicht unerheblich erweist. Der Aufwand für die Berechnung der Faktorbasis in Schritt 3 leistet hingegen keinen besonderen Beitrag.

5.23. Satz. *Für festes $k = \mathbb{F}_q$ durchlaufe F/k eine Folge globaler Funktionenkörper des Geschlechts g mit $g \to \infty$, die durch in y normierte und separable, irreduzible Polynome $f(x,y) \in k[x,y]$ mit $\deg_y(f) = O(1)$ gegeben werden. Die Klassengruppe kann dann unter der Glattheitsannahme 4.19 in einer erwarteten Laufzeit von*

$$C_f^{O(1)} \cdot L\big(5\sqrt{\log(q)/6} + o(1),\, g\big)$$

mit gegen 1 strebender Wahrscheinlichkeit berechnet werden.

Beweis. Die Vorberechnungen der Schritte 1 und 2 in Algorithmus 5.5 sind nach Bemerkung 5.6 polynomial in C_f und g. Weil die Schranke m vergleichsweise groß gewählt wird, ist Schritt 1 in diesem Fall sogar überflüssig. Wir setzen $m := \beta\sqrt{g\log(g)}$ mit einem noch zu bestimmenden $\beta \in \mathbb{R}^{>0}$. Für die Größe s der Faktorbasis $S = \mathcal{P}l^{\leq m}(F/k)$ gilt damit $s = q^{m+o(1)}$, und diese Anzahl in C_f polynomialer Operationen wird für ihre Berechnung benötigt. Die Verwendung von Lemma 5.21 erfordert danach $u^{u(1+o(1))}q^m$ Aufrufe von Algorithmus 5.9, was eine

Laufzeit von $(C_f)^{O(1)}u^{u(1+o(1))}q^{2m}$ entsprechend Bemerkung 5.10 ergibt. Schließlich gilt es Lemma 5.2 nach Umrechnung der gefundenen Relationen aus $\Lambda_{S,A}$ in Divisoren anzuwenden. Hierin dominiert die Berechnung der Smith-Normalform, analog wie in [53, S. 202] setzen wir einen Aufwand von $q^{5(m+o(1))}$ für die $q^{m+o(1)}$ Relationen an (der Wert für die Faktorbasiserzeugung verschwindet gegenüber diesen Größen). Wenn der Rang nicht s ist oder die Determinante nicht in dem Intervall $I(\bar{h})$ liegt, endet der Algorithmus ergebnislos, was aber wegen Lemma 5.21 nur mit gegen null gehender Wahrscheinlichkeit eintritt.
Mit der Berechnung der Smith-Normalform erhält man auch die die Klassengruppe zyklisch erzeugenden Divisoren. Zur Vermeidung von Koeffizientenexplosion in ihren Exponenten beachtet man die folgende Reduktionsmöglichkeit: Ohne Einschränkung kann $\deg(A) = 1$ und $\deg(D_i) = 0$ für $1 \leq i \leq s$, Bemerkung 5.6 und Schritt 1 in Algorithmus 5.5, gewählt werden. A ist dann an den Relationen nicht beteiligt, weil diese als Hauptdivisoren den Grad null haben, und die Exponenten von in den D_i dargestellten Divisoren können modulo $h(F/k)$ reduziert werden.
Für den Gesamtaufwand ergibt sich insgesamt

$$(C_f)^{O(1)}\, L\big(1/(2\beta) + 2\log(q)\beta + o(1),\, g\big) \;+\; L\big(5\beta\log(q) + o(1),\, g\big),$$

welches für $\beta := 1/\sqrt{6\log(q)}$ (bei nicht zu stark wachsendem C_f) minimiert wird. □

Dieses Laufzeitergebnis stimmt mit dem für reell-quadratische Funktionenkörper aus [53] überein.

5.4 Praktische Vorgehensweise

Nach den vorangegangenen, theoretischen Ausführungen soll in diesem Abschnitt auf die praktische Durchführung der Klassengruppenberechnung eingegangen werden, wobei wir für die Relationensuche die probabilistische Methode verwenden. In den Algorithmen werden nun insbesondere auch praktische Erfahrungen berücksichtigt.

5.4.1 Erzeugung der Faktorbasis

Die Wahl der Faktorbasis spielt eine entscheidende Rolle für die Relationensuche. Bei den beschriebenen, deterministischen Methoden sollte sie vollständig und möglichst klein sein, wohingegen für die probabilistische Methode ein ausgewogenes Verhältnis von Größe und Glattheitswahrscheinlichkeit wie in Satz 5.22

benötigt wird und sich die Vollständigkeit aufgrund der Schranken bei ausreichend großem Geschlecht von selbst einstellt.

Bei der probabilistischen Methode ist man genauer am Minimum des Produkts der Anzahl der Stellen der Faktorbasis und dem Inversen der Glattheitswahrscheinlichkeit interessiert, um die Anzahl der Versuche der Relationensuche zu minimieren. Zusätzlich gilt es auch noch die Kosten für die Smith-Normalform-Berechnung in Lemma 5.2 zu berücksichtigen.

Für die Divisorreduktion benutzen wir standardmäßig $A = (x)_\infty$, da diese dann besonders effizient ausgeführt werden kann. Die Wahl eines anderen Divisor A in Schritt 3.1 unten mit kleinem Grad bleibt jedoch möglich und ist beispielsweise bei relativ großem $[F : k(x)]$ im Verhältnis zu g sinnvoll, weil damit reduzierte Divisoren zu großer Dimension bei der Relationensuche ausgeschlossen werden.

Für die Praxis hat sich insgesamt das folgende Vorgehen als brauchbar erwiesen (Schritt 3 in Algorithmus 5.5 wird ersetzt):

...

3.1. (Reduktionsdivisor) Wähle $A = (x)_\infty$ *und setze* $n := g + \deg(A) - 1$.

3.2. (Stellenzahl exakt) Es sei r_1 *das Maximum der Schranken für die Erzeugung der Klassengruppe* m_E *und für die Approximation der Klassenzahl* m_P *aus Schritt 1 und 2. Berechne* $\widetilde{\pi}_r := \pi_r(F/k)$ *für* $1 \le r \le r_1$.

3.3. (Stellenzahl approximiert) Setze $\widetilde{\pi}_r := q^r/r$ *für* $r_1 < r \le n^{0.7}$.

3.4. (Minimum finden) Finde $1 \le m_H \le n^{0.7}$, *für welches der Wert*

$$g^2\,[F : k(x)]^5\,\big(\Psi_{F/k}(n,n)/\Psi_{F/k}(n,m_H)\big)\left(\sum_{r=1}^{m_H}\widetilde{\pi}_r\right) + \left(\sum_{r=1}^{m_H}\widetilde{\pi}_r\right)^3$$

minimal, aber ungleich null wird. Die Berechnung der $\Psi_{F/k}$*-Werte erfolgt mit Satz 4.2,* (ii) *und mit den* $\widetilde{\pi}_r$ *anstelle der exakten, aber unbekannten* $\pi_r(F/k)$.

3.5. (Schranke anpassen) Setze $m_B := \max\{m_H, m_E\}$.

3.6. (Faktorbasis erzeugen) Berechne

$$S := \mathcal{P}l^{\le m_B}(F/k) \cup \operatorname{supp}(A_1) \cup \operatorname{supp}\big((x)_\infty\big) \cup \operatorname{supp}(A).$$

Wir erwarten eine Glattheitswahrscheinlichkeit von $p_{S,A} := \Psi_{F/k}(n,m_B)\,/\,\Psi_{F/k}(n,n)$.

...

Der Wert in Schritt 3.4 stellt keine exakte Angabe der benötigten Kosten dar, liefert aber in der Praxis im Bereich $q < 10$ und $g < 10$ ganz brauchbare Schranken m_B. Für größere q und g muß man meist kleinere m_B verwenden, so daß unter Umständen auch Wurzeltests, wie nach Algorithmus 5.5 beschrieben, notwendig werden. Für Beispiele sei auf Kapitel 7 verwiesen.

5.4.2 Relationensuche

Bei der probabilistischen Relationensuche verzichten wir gegenüber der Beschreibung in Abschnitt 5.3.1 auf die Verwendung der D_i, deren Nutzen eher theoretisch war, und arbeiten direkt mit den Stellen P_i der Faktorbasis (in Algorithmus 5.24 wird die Bezeichnung D_i für andere Divisoren verwendet).

Für die Praxis hat sich insgesamt das folgende Vorgehen als brauchbar erwiesen, wobei Schritt 4 in Algorithmus 5.5 ersetzt wird:

5.24. Algorithmus. *(Relationensuche)*

Eingabe: *Ein globaler Funktionenkörper F/k des Geschlechts $g > 0$ über dem endlichen Körper k mit q Elementen, eine Faktorbasis S, ein S-glatter Divisor A mit $\deg(A) > 0$, eine Approximation $\bar{h}$ der Klassenzahl wie in Algorithmus 5.5, sowie die erwartete Glattheitswahrscheinlichkeit $p_{S,A}$.*

Ausgabe: *Ein Erzeugendensystem einer Untergruppe U von $\mathcal{P}(S)$ mit dem Index $(\mathcal{D}^0(S) : U) \in I(\bar{h})$.*

1. *(Initialisierung) Schreibe $S := \{P_0, \ldots, P_s\}$ und setze $W := 1$. Wähle für jedes $0 \leq i \leq s$ ein zufälliges $P \in S$ und definiere $D_i := -P_i + P - rA$ mit einem maximalen $r \in \mathbb{Z}$, so daß $\dim(D_i) > 0$ ist. Setze weiter $RV := 0$ (Anzahl Relationenversuche), $R := 0$ (Anzahl der gefundenen Relationen), $RV_0 := 0$, $R_0 := 0$, $\Delta RV := \max\{10\lceil p_{S,A}^{-1}\rceil, 20\}$, $\Delta R := \max\{\lceil |S|/10\rceil, 10\}$, $S_R := 1$ (Rangzuwachs pro Relationenzuwachs), $R_{RV} := 1$ (Relationen pro Relationenversuche), $i := 0$.*

2. *(Schleife über i) Nach Schritt 8 wird zu Schritt 2 gesprungen.*

3. *(Nächstes Element) Wenn $\mathcal{L}(D_i)$ multiplikativ modulo $k^\times$ kein bisher nicht verwendetes Element enthält, wird ein neues D_i erzeugt: Setze $D_i := -P_i +$ (Summe von W zufällig gewählten Stellen aus S mit zufälligen Exponenten in $[1, W]$) $- rA$, mit einem maximalen $r \in \mathbb{Z}$, so daß $\dim(D_i) > 0$ ist. Wähle für a ein bisher nicht verwendetes Element von $\mathcal{L}(D_i)$ und setze $RV := RV + 1$.*

4. *(Relation gefunden?) Überprüfe, ob mit a eine Relation gefunden wurde. Wenn ja, speichere a für die spätere Auswertung und setze $R := R + 1$.*

5. *(Glattheitstest) Wenn $RV - RV_0 \geq \Delta RV$ ist, so werden die folgenden Teilschritte ausgeführt:*

   5.1. *Setze $R_{RV} := R/RV$.*

   5.2. *(Faktorbasis vergrößern?) Wenn $R_{RV} \leq p_{S,A}/100$ ist, wird die Faktorbasis um die Stellen des nächsthöheren Grads, als wie bisher verwendet, erweitert, $p_{S,A}$ wird angepaßt und die neu dazugekommenen D_j und ΔRV werden wie in der Initialisierung berechnet. Andernfalls wird $\Delta RV := \max\{10\lceil 1/R_{RV}\rceil, 20\}$ gesetzt.*

   5.3. *Setze $RV_0 := RV$.*

6. *(Relationen-Test) Wenn $R - R_0 \geq \Delta R$ ist, so werden die folgenden Teilschritte ausgeführt:*

   6.1. *(Relationen auswerten) Die Relationen werden wie in Lemma 5.2 ausgewertet und U als das von ihnen erzeugte Teilgitter gesetzt.*

   6.2. *(Endlicher Index) Folgendes wird für endlichen Index $(\mathcal{D}^0(S) : U)$ getan: Wenn $(\mathcal{D}^0(S) : U) \in I(\bar{h})$ ist, so wird die Schleife 2 verlassen. Wenn der Index und W mit den letzten $\max\{\lceil |S|/10\rceil, 10\}$ Relationen unverändert geblieben ist, wird $W := \min\{W + 1, |S|, 10\}$ gesetzt und alle D_j werden wie in Schritt 3 neu berechnet. Schließlich wird $\Delta R := \lceil 2R_{RV}|S|/[F : k(x)]\rceil$ gesetzt.*

   6.3. *(Nicht endlicher Index) Wenn der Index noch nicht endlich war, so wird das folgende getan: Es sei Δr der Rangzuwachs mit den letzten ΔR Relationen. Setze $S_R := (\Delta r/\Delta R + S_R)/2$. Wenn $S_R < 0.2$ ist und der Rang und W mit den letzten $\max\{|S|/10, 10\}$ Relationen unverändert geblieben ist, dann sei $W := \min\{W + 1, |S|, 10\}$, alle D_j werden wie in Schritt 3 neu berechnet, und es wird $\Delta R := \max\{\lceil |S|/10\rceil, 10\}\rceil$ gesetzt. Andernfalls sei*

   $$\Delta R := \lceil \min\{\, 3S_R\Delta R,\ 2R_{RV}|S|(|S| - \operatorname{rank}(U))/(S_R[F : k(x)])\,\}\rceil.$$

7. *(Nächstes i) Wenn in Schritt 4 eine Relation gefunden wurde, setze $i := i + 1$. Wenn $i > s$ ist, dann setze $i := 0$.*

8. *(Ende Schleife über i) Gehe zu Schritt 2.*

9. *(Ende) Die Relationensuche ist abgeschlossen. Ausgabe der gefundenen Relationen und U. Terminiere.*

Bemerkungen:

Wegen der beschränkten Größe der in Schritt 1 und 3 erzeugten Divisoren D_i treffen die Komplexitätsüberlegungen der vorangegangenen Abschnitte streng genommen nicht mehr auf Algorithmus 5.24 zu. In der Praxis erweist sich dieses Vorgehen jedoch als günstig, weil die Berechnung der Riemann-Roch-Räume zügiger vonstatten geht und die auftretenden Relationen ebenfalls eine beschränkte Größe besitzen.

Wenn $A \neq (x)_\infty$ ist, verwendet man statt der Maximalreduktion in Schritt 1 und 3 praktischerweise nur die Gradreduktion aus Abschnitt 2.6, welche schneller zu bestimmen ist und in der Regel dasselbe Ergebnis liefert.

Für die Ausführung von Schritt 4 bietet es sich an, die Norm $\mathrm{N}_{F/k(x)}(a)$ zu betrachten. Der Nenner ist nach den Voraussetzungen an S und A S-glatt. Eine gute Vorauswahl S-glatter Elemente a erhält man daher, falls $S = \mathcal{P}l^{\leq m_B}(F/k)$ ist, wenn zuerst getestet wird, ob der Zähler der Norm nur aus Primpolynomen eines Grads $\leq m_B$ besteht. Dies kann effizient durchgeführt werden.

Die Schritte 5.1-5.3 beruhen auf der Erfahrung, daß die Relationensuche mitunter für sehr kleine Faktorbasen beziehungsweise sehr kleines q und g nicht genügend Relationen finden kann, so daß eine Vergrößerung notwendig ist. Dies tritt allerdings nur selten ein. Will man die Relationensuche bei großem g mit fester Faktorbasisgröße durchführen, sollte man diese Schritte nicht berücksichtigen.

Das Vorgehen der Schritte 6.1-6.3 realisiert die folgende Strategie: Die Relationen werden, durch ΔR gesteuert, zu Beginn der Relationensuche häufig und später immer seltener ausgewertet, sofern das Rangwachstum ausreichend gut ausfällt. Hierdurch spart man sich die allzu häufige Berechnung der Smith-Normalform in Lemma 5.2, die bei größeren Faktorbasen ziemlich teuer wird. Schließlich erfolgt die Auswertung der Relationen dann auch, wenn aufgrund des bisherigen Rangwachstums ein voller Rang erwartet werden kann. Wenn das Rangwachstum jedoch schlecht ist, werden die Relationen immer häufiger ausgewertet und gegebenenfalls dann W erhöht. In die Anzahl ΔR der zu findenden Relationen bis zur nächsten Auswertung geht zusätzlich das Verhältnis des Aufwands, eine Relation zu finden, zum Aufwand der Smith-Normalform-Berechnung ein: Ist die Smith-Normalform-Berechnung verhältnismäßig teuer, so werden relativ viele Relationen bis zur nächsten Auswertung gesucht, und umgekehrt.

Für Beispiele sei auf das Kapitel 7 verwiesen.

Kapitel 6

Anwendungen

In diesem Kapitel wird auf Anwendungen der Klassengruppenberechnung globaler Funktionenkörper eingegangen: Wir beschreiben die Berechnung von Bildern und Urbildern unter der Isomorphie der Divisorenklassengruppe zur berechneten, endlich erzeugten, abelschen Gruppe und die sich daraus ergebende Möglichkeit zur Berechnung diskreter Logarithmen, S-Einheiten und Idealklassengruppen der Dedekindringe $\mathfrak{o}^S$, für beliebige, nicht-leere endliche Stellenmengen S.

Die Voraussetzungen von Kapitel 5 werden übernommen.

6.1 Eindeutige Klassendarstellung

Wie beschrieben liegt die Struktur der Klassengruppe nach der Klassengruppenberechnung als endliche abelsche Gruppe in Elementarteilergestalt $\mathcal{C}l^0(F/k) \cong \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}$ vor. Urbilder unter diesem Isomorphismus sind leicht zu berechnen, weil zusätzlich konkrete, den zyklischen Faktoren entsprechende Divisoren gegeben sind. Es stellt sich nun die Frage, wie das Bild einer beliebigen Divisorenklasse $[D] \in \mathcal{C}l^0(F/k)$ unter diesem Isomorphismus zu bestimmen ist. Gesucht ist also eine eindeutige Darstellung von $[D]$ in den erzeugenden Divisoren. Wenn dies geklärt ist, erhält man unter Hinzunahme eines Divisors vom Grad eins mit Proposition 1.1 dann auch die in beiden Richtungen berechenbare Isomorphie der ganzen Divisorenklassengruppe $\mathcal{C}l(F/k) \cong \mathbb{Z} \times \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}$.

Wir gehen von einer freien Darstellung (S. 16) von D mit $\deg(D) = 0$ aus. Um die eindeutige Klassendarstellung zu finden, geht man sehr ähnlich wie bei der Relationensuche vor. Unter Verwendung der Faktorbasis S aus der Klassengruppenberechnung bestimmt man zufällig gewählte S-glatte Divisoren D' (nicht zu großer Höhe) und betrachtet die Maximalreduktionen von $D + D'$ entlang A, also $D + D' = \widetilde{D} + rA - (a)$. Wenn eines dieser $\widetilde{D}$ S-glatt ist, hat man eine Darstellung

von D durch einen S-glatten Divisor $\widetilde{D} + rA - D'$ modulo einem Hauptdivisor gefunden. Wegen $[\widetilde{D} + rA - D'] \in \big(\mathcal{D}^0(S) + \mathcal{P}(F/k)\big) \,/\, \mathcal{P}(F/k) \cong \mathcal{D}^0(S)/\mathcal{P}(S)$ berechnet man dann leicht die gesuchte Darstellung mit Lemma 5.2. Die Erfolgswahrscheinlichkeit dieses probabilistischen Vorgehens stimmt mit der Wahrscheinlichkeit überein, bei der probabilistischen Relationensuche eine Relation zu finden, so daß ein subexponentieller Aufwand erwartet werden kann.

Mit der Klassendarstellung lassen sich Fragestellungen bezüglich der Divisorenklassengruppe in den Kontext explizit gegebener, endlich erzeugter abelscher Gruppen übersetzen. Im folgenden nehmen wir an, daß die erforderlichen Algorithmen für endlich erzeugte abelsche Gruppen und Homomorphismen zwischen ihnen zur Verfügung stehen.

6.2 Diskreter Logarithmus

Für zwei Divisorenklassen $[D_1], [D_2]$ vom Grad null ist der diskrete Logarithmus von $[D_1]$ bezüglich $[D_2]$ eine modulo der Ordnung von $[D_2]$ bestimmte Zahl $r \in \mathbb{Z}$, für die $[D_1] = r[D_2]$ gilt. Indem man nun die Klassendarstellung von $[D_1]$ und $[D_2]$ bestimmt, läßt sich das Problem der Berechnung des diskreten Logarithmus von $[D_1]$ bezüglich $[D_2]$ in das analoge Problem in $\mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}$ übersetzen, wo es leicht wegen der *bekannten* Größen c_i gelöst werden kann.

6.3 Einheiten und Idealklassengruppe des Dedekindrings $\mathfrak{o}^S$

S sei eine beliebige, nicht-leere endliche Menge von $s+1$ Stellen von F/k. Es stellt sich die Frage nach der Berechnung der Einheitengruppe und der Idealklassengruppe des Rings der außerhalb S ganzen Elemente $\mathfrak{o}^S$. Auch dieses kann mit Hilfe der Klassendarstellung in die Situation endlich erzeugter abelscher Gruppen übertragen werden.

Wir verwenden dazu den Homomorphismus $\phi_S : \mathcal{D}(S) \longrightarrow \mathcal{C}l(F/k)$, für den nämlich $\ker \phi_S = \mathcal{P}(S)$ und $\operatorname{coker} \phi_S = \mathcal{C}l(F/k)/\phi_S\big(\mathcal{D}(S)\big) \cong \mathcal{C}l(\mathfrak{o}^S)$ gilt (man vergleiche mit dem Beweis von Korollar 1.3). Mit Hilfe der Klassendarstellung erhalten wir für ϕ_S einen explizit gegebenen Homomorphismus $\phi'_S : \mathbb{Z}^{s+1} \longrightarrow \mathbb{Z} \times \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_m\mathbb{Z}$ und können dessen Kern und Kokern berechnen. Aus den Hauptdivisoren $\mathcal{P}(S)$ lassen sich mittels Riemann-Roch-Raum-Berechnung schließlich fundamentale S-Einheiten von $(\mathfrak{o}^S)^\times$ in Potenzproduktdarstellung gewinnen.

Kapitel 7

Beispiele

Wir betrachten nun Beispiele für die Berechnung von Klassengruppen globaler Funktionenkörper F/k. Im ersten Abschnitt berechnen wir neben der Divisorenklassengruppe auch die Einheiten- und Idealklassengruppe von $\mathfrak{o}^S = \mathrm{Cl}(k[x], F)$ für die Beispiele zur Einheitenberechnung aus [50] und für einige weitere Beispiele. In den darauf folgenden Abschnitten betrachten wir zufällig gewählte Funktionenkörper mit entweder großer Elementanzahl q des exakten Konstantenkörpers oder großem Geschlecht g, eine Tabelle mit hyperelliptischen Funktionenkörpern und speziell konstruierte Funktionenkörper mit vielen Stellen vom Grad eins. Den Abschluß bildet ein Beispiel zur Bestimmung des p-Rangs der Klassengruppe sowie der Hasse-Witt-Invariante von F/k.

Alle Berechnungen wurden mit dem Computeralgebrasystem KASH, [25], auf einer SGI Origin 2000 durchgeführt.

Die Tabelleneinträge gliedern sich in Kästen des folgenden Inhalts:

Der erste Kasten enthält immer die Werte q und g, die laufende Nummer des Beispiels, die Klassenzahl $h(F/\mathbb{F}_q)$ und die Struktur der Klassengruppe $\mathcal{C}l^0(F/\mathbb{F}_q)$, sowie die Berechnungszeit T in Sekunden.

In den Abschnitten 7.1 und 7.5 folgen zusätzlich der S_0-Regulator $R(S_0)$, die Idealklassenzahl $h(S_0)$ und die Struktur der Idealklassengruppe $\mathcal{C}l(\mathfrak{o}^{S_0})$ des Rings $\mathfrak{o}^{S_0}$ für $S_0 := \mathrm{supp}\big((x)_\infty\big)$.

Danach wird die definierende Gleichung $f(x, \rho) = 0$ des Funktionenkörpers, der Grad n und die Konstante C_f zur Koeffizientengröße angegeben.

Im letzten Kasten werden die wesentlichen Parameter des Klassengruppenverfahrens aufgelistet. Für einen Divisor $A = \sum_{i=1}^{r} c_i P_i$ schreiben wir hier $A \sim \big(c_1, \deg(P_1); \ldots; c_r, \deg(P_r)\big)$. Die anderen Werte entsprechen bei gleicher Bezeichnung den Werten aus Algorithmus 5.5 und den Algorithmen in Abschnitt 5.4: m_E

ist die Schranke für die Erzeugung der Faktorbasis, m_P ist die Schranke für die Approximation der Klassenzahl, m_H ist die Schranke, für die die kürzeste Laufzeit erwartet wird. m_B ist die dann tatsächlich für die Faktorbasis S verwendete Schranke. Für die Anzahl RV der Versuche, eine Relation zu finden, geben wir den erwarteten ($=_?$) und den tatsächlichen Wert an. RR bezeichnet die Anzahl der benötigten Riemann-Roch-Raum-Berechnungen, R die Anzahl der gefundenen Relationen. W ist schließlich die Exponentenschranke für die zufällig gewählten Divisoren der Relationensuche.
Für keines der Beispiele ist eine Vergrößerung der Faktorbasis während der Berechnung erforderlich. Außerdem gilt immer $\mathrm{supp}(A_1) \subseteq S$.

Auf die Angabe von Divisoren, Idealen und S-Einheiten verzichten wir aus Platzgründen.

7.1 Vergleich mit Beispielen aus der Einheitenberechnung

Die folgenden Beispiele sind [50, S. 64ff.] entnommen. Man beachte, daß dort die Grade der „unendlichen“ Stellen mit in den Regulator aufgenommen werden. Die Laufzeiten haben sich teilweise erheblich verbessert.

$q = 3, \quad g = 3$	1
$h(F/\mathbb{F}_3) = 76, \quad \mathcal{C}l^0(F/\mathbb{F}_3) \cong 2 \times 38.$	$T = 1.4\,s$
$R(S_0) = 19, \quad h(S_0) = 4, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 2 \times 2.$	
$F := \mathbb{F}_3(x,\rho): \quad \rho^3 + (2x+1)\rho^2 + (2x^3+x^2+x+1)\rho + x^2 + 2 = 0.$	$n = 3, \quad C_f = 2$
$A = (x)_\infty \sim (1,1;2,1).$	
$m_E = 2, \quad m_P = 4, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 11, \quad RV =_? 16.$	
$RR = 26, \quad RV = 47, \quad R = 36 \quad \longrightarrow \quad R/RV = 0.77, \quad \lvert S\rvert/R = 0.31.$	
$W = 1.$	

$q = 3, \quad g = 2$	2
$h(F/\mathbb{F}_3) = 16, \quad \mathcal{C}l^0(F/\mathbb{F}_3) \cong 2 \times 8.$	$T = 0.7\,s$
$R(S_0) = 4, \quad h(S_0) = 4, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 4.$	
$F := \mathbb{F}_3(x,\rho): \quad \rho^3 + (x^2+2)\rho^2 + (2x^2+2)\rho + 2 = 0.$	$n = 3, \quad C_f = 2$
$A = (x)_\infty \sim (1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 3, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 5, \quad RV =_? 12.$	
$RR = 7, \quad RV = 14, \quad R = 10 \quad \longrightarrow \quad R/RV = 0.71, \quad \lvert S\rvert/R = 0.5.$	
$W = 1.$	

$q = 5, \quad g = 1$	3
$h(F/\mathbb{F}_5) = 3, \quad \mathcal{C}l^0(F/\mathbb{F}_5) \cong 3.$	$T = 0.6\,s$
$R(S_0) = 1, \quad h(S_0) = 3, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 3.$	
$F := \mathbb{F}_5(x,\rho): \quad \rho^3 + (x^2+2x+2)\rho^2 + (x+2)\rho + 2 = 0.$	$n = 3, \quad C_f = 2$
$A = (x)_\infty \sim (1,1;1,2).$	
$m_E = 1, \quad m_P = 2, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 4, \quad RV =_? 17.$	
$RR = 5, \quad RV = 31, \quad R = 10 \quad \longrightarrow \quad R/RV = 0.32, \quad \lvert S\rvert/R = 0.4.$	
$W = 1.$	

$q = 25, \quad g = 0$	4
$h(F/\mathbb{F}_{25}) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_{25}) \cong 1.$	$T = 1.5\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{25}(x,\rho): \quad \rho^3 + (3x+4)\rho^2 + 2\rho + 1 = 0.$	$n = 3, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;2,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 26, \quad RV =_? 124.$	
$RR = 39, \quad RV = 39, \quad R = 39 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.67.$	
$W = 1.$	

$q = 7, \quad g = 0$	5
$h(F/\mathbb{F}_7) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_7) \cong 1.$	$T = 0.6\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_7(x,\rho): \quad \rho^3 + (2x+3)\rho^2 + 1 = 0.$	$n = 3, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;2,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 8, \quad RV =_? 25.$	
$RR = 17, \quad RV = 17, \quad R = 17 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.47.$	
$W = 1.$	

$q = 49, \quad g = 2$	6
$h(F/\mathbb{F}_{49}) = 3600, \quad \mathcal{C}l^0(F/\mathbb{F}_{49}) \cong 2 \times 2 \times 30 \times 30.$	$T = 15\,s$
$R(S_0) = 2, \quad h(S_0) = 1800, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 2 \times 30 \times 30.$	
$F := \mathbb{F}_{49}(x,\rho): \quad \rho^4 + 2\rho^3 + (2x^2+3x+4)\rho + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;3,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 70, \quad RV =_? 1823.$	
$RR = 71, \quad RV = 787, \quad R = 124 \quad \longrightarrow \quad R/RV = 0.16, \quad \lvert S\rvert/R = 0.56.$	
$W = 1.$	

$q = 11, \quad g = 2$	7
$h(F/\mathbb{F}_{11}) = 268, \quad \mathcal{C}l^0(F/\mathbb{F}_{11}) \cong 2 \times 134.$	$T = 2.5\,s$
$R(S_0) = 268, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{11}(x,\rho): \quad \rho^3 + (8x^2+x)\rho^2 + (6x^2+3x+3)\rho + 8 = 0.$	$n = 3, \quad C_f = 2$
$A = (x)_\infty \sim (1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 21, \quad RV =_? 66.$	
$RR = 21, \quad RV = 81, \quad R = 40 \quad \longrightarrow \quad R/RV = 0.49, \quad \lvert S\rvert/R = 0.53.$	
$W = 1.$	

$q = 13, \quad g = 1$	8
$h(F/\mathbb{F}_{13}) = 16, \quad \mathcal{C}l^0(F/\mathbb{F}_{13}) \cong 4 \times 4.$	$T = 2\,s$
$R(S_0) = 4, \quad h(S_0) = 4, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 4.$	
$F := \mathbb{F}_{13}(x,\rho): \quad \rho^3 + (10x^2+7x+1)\rho^2 + (2x^2+8x+5)\rho + 7 = 0.$	$n = 3, \quad C_f = 2$
$A = (x)_\infty \sim (1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 16, \quad RV =_? 52.$	
$RR = 16, \quad RV = 101, \quad R = 21 \quad \longrightarrow \quad R/RV = 0.21, \quad \lvert S\rvert/R = 0.76.$	
$W = 1.$	

$q = 17, \quad g = 1$	9
$h(F/\mathbb{F}_{17}) = 16, \quad \mathcal{C}l^0(F/\mathbb{F}_{17}) \cong 16.$	$T = 1.8\,s$
$R(S_0) = 16, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{17}(x,\rho): \quad \rho^3 + 2\rho^2 + (6x^2+14x+6)\rho + 10x^2 + 10x + 1 = 0.$	$n = 3, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;1,2).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 17, \quad RV =_? 84.$	
$RR = 19, \quad RV = 162, \quad R = 40 \quad \longrightarrow \quad R/RV = 0.25, \quad \lvert S\rvert/R = 0.43.$	
$W = 1.$	

$q = 9, \quad g = 0$	10
$h(F/\mathbb{F}_9) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_9) \cong 1.$	$T = 1.2\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_9(x,\rho): \quad \rho^4 + 2\rho^3 + (2x+1)\rho^2 + 2\rho + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (2,1;2,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 10, \quad RV =_? 89.$	
$RR = 16, \quad RV = 16, \quad R = 16 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.63.$	
$W = 1.$	

$q = 5, \quad g = 0$	11
$h(F/\mathbb{F}_5) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_5) \cong 1.$	$T = 1.2\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_5(x,\rho): \quad \rho^4 + (2x+3)\rho^3 + \rho^2 + (3x+2)\rho + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 6, \quad RV =_? 32.$	
$RR = 10, \quad RV = 10, \quad R = 10 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.6.$	
$W = 1.$	

$q = 25, \quad g = 0$	12
$h(F/\mathbb{F}_{25}) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_{25}) \cong 1.$	$T = 2.9\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{25}(x,\rho): \quad \rho^4 + 2\rho^3 + (3x+2)\rho^2 + \rho + 2 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (2,1;2,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 26, \quad RV =_? 411.$	
$RR = 54, \quad RV = 54, \quad R = 54 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.48.$	
$W = 1.$	

$q = 25, \quad g = 0$	13
$h(F/\mathbb{F}_{25}) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_{25}) \cong 1.$	$T = 2.8\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{25}(x,\rho): \quad \rho^4 + (2x+3)\rho^3 + \rho^2 + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;3,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 26, \quad RV =_? 411.$	
$RR = 40, \quad RV = 40, \quad R = 40 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.65.$	
$W = 1.$	

$q = 25, \quad g = 0$	14
$h(F/\mathbb{F}_{25}) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_{25}) \cong 1.$	$T = 3.8\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{25}(x,\rho): \quad \rho^4 + (2x+3)\rho^3 + (x+1)\rho^2 + (4x+3)\rho + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 26, \quad RV =_? 411.$	
$RR = 39, \quad RV = 39, \quad R = 39 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.67.$	
$W = 1.$	

$q = 49, \quad g = 0$	15
$h(F/\mathbb{F}_{49}) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_{49}) \cong 1.$	$T = 11\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_{49}(x,\rho): \quad \rho^4 + (2x+3)\rho^3 + (3x+2)\rho^2 + (4x+5)\rho + 1 = 0.$	$n = 4, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;1,1;1,1;1,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 50, \quad RV =_? 960.$	
$RR = 129, \quad RV = 129, \quad R = 129 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.39.$	
$W = 1.$	

$q = 5, \quad g = 0$	16
$h(F/\mathbb{F}_5) = 1, \quad \mathcal{C}l^0(F/\mathbb{F}_5) \cong 1.$	$T = 1.3\,s$
$R(S_0) = 1, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_5(x,\rho): \quad \rho^5 + (2x+3)\rho^2 + 3\rho + 1 = 0.$	$n = 5, \quad C_f = 1$
$A = (x)_\infty \sim (2,1;3,1).$	
$m_E = 1, \quad m_P = 0, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 6, \quad RV =_? 72.$	
$RR = 19, \quad RV = 19, \quad R = 19 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.32.$	
$W = 1.$	

Die folgendenen Beispiele haben größeres Geschlecht und benötigen wie zuvor nur eine relativ geringe Laufzeit:

$q = 3, \quad g = 10$	17
$h(F/\mathbb{F}_3) = 52584, \quad \mathcal{C}l^0(F/\mathbb{F}_3) \cong 2 \times 2 \times 13146.$	$T = 44\,s$
$R(S_0) = 1, \quad h(S_0) = 52584, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 2 \times 2 \times 13146.$	
$F := \mathbb{F}_3(x,\rho): \quad \rho^5 + x\rho + x^6 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A = (x)_\infty \sim (5,1).$	
$m_E = 6, \quad m_P = 5, \quad m_H = 4 \quad \longrightarrow \quad m_B := 6, \quad \lvert S\rvert = 192, \quad RV =_? 697.$	
$RR = 265, \quad RV = 495, \quad R = 238 \quad \longrightarrow \quad R/RV = 0.48, \quad \lvert S\rvert/R = 0.81.$	
$W = 1.$	

$q = 11, \quad g = 6$	18
$h(F/\mathbb{F}_{11}) = 1847040, \quad \mathcal{C}l^0(F/\mathbb{F}_{11}) \cong 2 \times 923520.$	$T = 25\,s$
$R(S_0) = 1, \quad h(S_0) = 1847040, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 2 \times 923520.$	
$F := \mathbb{F}_{11}(x,\rho): \quad \rho^4 + x^2\rho + x^5 + x + 1 = 0.$	$n = 4, \quad C_f = 2$
$A = (x)_\infty \sim (4,1).$	
$m_E = 2, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 71, \quad RV =_? 5583.$	
$RR = 362, \quad RV = 2701, \quad R = 109 \quad \longrightarrow \quad R/RV = 0.04, \quad \lvert S\rvert/R = 0.65.$	
$W = 1.$	

$q = 19, \quad g = 7$	19
$h(F/\mathbb{F}_{19}) = 1336199119, \quad \mathcal{C}l^0(F/\mathbb{F}_{19}) \cong 1336199119.$	$T = 62\,s$
$R(S_0) = 1, \quad h(S_0) = 2672398238, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 2672398238.$	
$F := \mathbb{F}_{19}(x,\rho): \quad \rho^4 + \rho^3 + x^2\rho + x^6 + x + 1 = 0.$	$n = 4, \quad C_f = 2$
$A = (x)_\infty \sim (2,2).$	
$m_E = 2, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 224, \quad RV =_? 11112.$	
$RR = 679, \quad RV = 4018, \quad R = 436 \quad \longrightarrow \quad R/RV = 0.11, \quad \lvert S\rvert/R = 0.51.$	
$W = 1.$	

$q = 9, \quad g = 6$	20
$h(F/\mathbb{F}_9) = 417956, \quad \mathcal{C}l^0(F/\mathbb{F}_9) \cong 2 \times 208978.$	$T = 234\,s$
$R(S_0) = 417956, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^{S_0}) \cong 1.$	
$F := \mathbb{F}_9(x,\rho): \quad \rho^5 + x\rho^3 + x^5 + x^2 + 1 = 0.$	$n = 5, \quad C_f = 1$
$A = (x)_\infty \sim (1,1;1,2;1,2).$	
$m_E = 3, \quad m_P = 2, \quad m_H = 3 \quad \longrightarrow \quad m_B := 3, \quad \lvert S\rvert = 327, \quad RV =_? 3150.$	
$RR = 450, \quad RV = 8599, \quad R = 700 \quad \longrightarrow \quad R/RV = 0.081, \quad \lvert S\rvert/R = 0.47.$	
$W = 1.$	

7.2 Großes Geschlecht

Es folgen Beispiele, in denen das Geschlecht für jeden Konstantenkörper so groß gewählt wird, daß wir eine ungefähre Vorstellung über die Grenzen des Verfahrens beziehungsweise der verwendeten Implementierung erhalten können.

Bis auf die ersten beiden und das vierte Beispiel wurde durchweg $A = A_1$ für eine gute Glattheitswahrscheinlichkeit verwendet. Als Schranke für die Faktorbasis wurde häufig ein kleinerer Wert als m_E gewählt, so daß am Ende der Klassengruppenberechnung Wurzeltests erforderlich waren. Wegen der Strukturen der Klassengruppen benötigten diese nur einen Bruchteil der gesamten Berechnungszeit.

$q = 2, \quad g = 50$	21
$h(F/\mathbb{F}_2) = 1743271585380988, \quad \mathcal{C}l^0(F/\mathbb{F}_2) \cong 1743271585380988.$	$T = 8749\,s$
$F := \mathbb{F}_2(x,\rho): \quad \rho^2 + (x+1)\rho + x^{101} + x + 1 = 0.$	$n = 2, \quad C_f = 51$
$A = (x)_\infty \sim (2,1).$	
$m_E = 14, \quad m_P = 12, \quad m_H = 12 \quad \longrightarrow \quad m_B := 10, \quad \lvert S\rvert = 250, \quad RV =_? 83985.$	
$RR = 79940, \quad RV = 98342, \quad R = 1057 \quad \longrightarrow \quad R/RV = 0.011, \quad \lvert S\rvert/R = 0.24.$	
$W = 5.$	

$q = 3, \quad g = 30$	22
$h(F/\mathbb{F}_3) = 205217259503652, \quad \mathcal{C}l^0(F/\mathbb{F}_3) \cong 2 \times 102608629751826.$	$T = 13450\,s$
$F := \mathbb{F}_3(x,\rho): \quad \rho^2 + (x+1)\rho + x^{62} + x + 1 = 0.$	$n = 2, \quad C_f = 31$
$A = (x)_\infty \sim (1,2).$ $m_E = 8, \quad m_P = 7, \quad m_H = 7 \quad \longrightarrow \quad m_B := 6, \quad \lvert S\rvert = 230, \quad RV =_? 74270.$ $RR = 80377, \quad RV = 130973, \quad R = 1127 \quad \longrightarrow \quad R/RV = 0.0086, \quad \lvert S\rvert/R = 0.2.$ $W = 5.$	

$q = 5, \quad g = 19$	23
$h(F/\mathbb{F}_5) = 16563730252090, \quad \mathcal{C}l^0(F/\mathbb{F}_5) \cong 16563730252090.$	$T = 6234\,s$
$F := \mathbb{F}_5(x,\rho): \quad \rho^3 + x\rho + x^{21} + x + 1 = 0.$	$n = 3, \quad C_f = 7$
$A \sim (1,1).$ $m_E = 5, \quad m_P = 4, \quad m_H = 5 \quad \longrightarrow \quad m_B := 4, \quad \lvert S\rvert = 219, \quad RV =_? 63731.$ $RR = 106132, \quad RV = 126754, \quad R = 909 \quad \longrightarrow \quad R/RV = 0.0072, \quad \lvert S\rvert/R = 0.24.$ $W = 4.$	

$q = 7, \quad g = 14$	24
$h(F/\mathbb{F}_7) = 1322299613348, \quad \mathcal{C}l^0(F/\mathbb{F}_7) \cong 2 \times 661149806674.$	$T = 1461\,s$
$F := \mathbb{F}_7(x,\rho): \quad \rho^5 + (x+1)\rho + x^8 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A = (x)_\infty \sim (5,1).$ $m_E = 4, \quad m_P = 3, \quad m_H = 4 \quad \longrightarrow \quad m_B := 3, \quad \lvert S\rvert = 148, \quad RV =_? 102364.$ $RR = 14923, \quad RV = 90844, \quad R = 468 \quad \longrightarrow \quad R/RV = 0.0052, \quad \lvert S\rvert/R = 0.32.$ $W = 2.$	

$q = 13, \quad g = 10$	25
$h(F/\mathbb{F}_{13}) = 206665304791, \quad \mathcal{C}l^0(F/\mathbb{F}_{13}) \cong 206665304791.$	$T = 1888\,s$
$F := \mathbb{F}_{13}(x,\rho): \quad \rho^5 + (x+1)\rho + x^6 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A \sim (1,1).$ $m_E = 3, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 111, \quad RV =_? 10848.$ $RR = 19116, \quad RV = 20802, \quad R = 395 \quad \longrightarrow \quad R/RV = 0.019, \quad \lvert S\rvert/R = 0.28.$ $W = 2.$	

$q = 17, \quad g = 10$	26
$h(F/\mathbb{F}_{17}) = 2231475497166, \quad \mathcal{C}l^0(F/\mathbb{F}_{17}) \cong 2231475497166.$	$T = 17771\,s$
$F := \mathbb{F}_{17}(x,\rho): \quad \rho^5 + (x+1)\rho + x^6 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A \sim (1,1).$ $m_E = 2, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 168, \quad RV =_? 33990.$ $RR = 49690, \quad RV = 52399, \quad R = 666 \quad \longrightarrow \quad R/RV = 0.013, \quad \lvert S\rvert/R = 0.25.$ $W = 2.$	

$q = 23, \quad g = 10$	27
$h(F/\mathbb{F}_{23}) = 37953554676269, \quad \mathcal{C}l^0(F/\mathbb{F}_{23}) \cong 37953554676269.$	$T = 11602\,s$
$F := \mathbb{F}_{23}(x,\rho): \quad \rho^5 + (x+1)\rho + x^6 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A \sim (1,1).$	
$m_E = 2, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 322, \quad RV =_? 81501.$	
$RR = 148690, \quad RV = 154883, \quad R = 1113 \quad \longrightarrow \quad R/RV = 0.0072, \ \lvert S\rvert/R = 0.29.$	
$W = 2.$	

$q = 25, \quad g = 10$	28
$h(F/\mathbb{F}_{25}) = 147510773172045, \ \mathcal{C}l^0(F/\mathbb{F}_{25}) \cong 3 \times 3 \times 3 \times 5463361969335.$	$T = 69ks$
$F := \mathbb{F}_{25}(x,\rho): \quad \rho^5 + (x+1)\rho + x^6 + x + 1 = 0.$	$n = 5, \quad C_f = 2$
$A \sim (1,1).$	
$m_E = 2, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 375, \quad RV =_? 47170.$	
$RR = 93274, \quad RV = 1544153, \quad R = 1053 \ \longrightarrow \ R/RV = 0.00068, \quad \lvert S\rvert/R = 0.36.$	
$W = 5.$	

7.3 Großer Konstantenkörper

In den folgenden Beispielen betrachten wir einen festen Funktionenkörper und nehmen Konstantenkörpererweiterungen vor. Wir beobachten, daß die Größe der Faktorbasis exponentiell im Grad der Konstantenkörpererweiterung zunimmt, so daß dem Verfahren hier schnell Grenzen gesetzt werden.

$q = 2, \quad g = 4$	29
$h(F/\mathbb{F}_2) = 10, \quad \mathcal{C}l^0(F/\mathbb{F}_2) \cong 10.$	$T = 1\,s$
$F := \mathbb{F}_2(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 5, \quad m_P = 6, \quad m_H = 2 \quad \longrightarrow \quad m_B := 5, \quad \lvert S\rvert = 18, \quad RV =_? 18.$	
$RR = 37, \quad RV = 40, \quad R = 40 \quad \longrightarrow \quad R/RV = 1, \quad \lvert S\rvert/R = 0.45.$	
$W = 1.$	

$q = 4, \quad g = 4$	30
$h(F/\mathbb{F}_4) = 280, \quad \mathcal{C}l^0(F/\mathbb{F}_4) \cong 280.$	$T = 2.6\,s$
$F := \mathbb{F}_4(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 3, \quad m_P = 3, \quad m_H = 2 \quad \longrightarrow \quad m_B := 3, \quad \lvert S\rvert = 38, \quad RV =_? 55.$	
$RR = 98, \quad RV = 148, \quad R = 111 \quad \longrightarrow \quad R/RV = 0.75, \quad \lvert S\rvert/R = 0.34.$	
$W = 1.$	

$q = 8, \quad g = 4$	31
$h(F/\mathbb{F}_8) = 4090, \quad \mathcal{C}l^0(F/\mathbb{F}_8) \cong 4090.$	$T = 3.5\,s$
$F := \mathbb{F}_8(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 2, \quad m_P = 2, \quad m_H = 1 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 42, \quad RV =_? 147.$	
$RR = 214, \quad RV = 251, \quad R = 186 \quad \longrightarrow \quad R/RV = 0.74, \quad \lvert S\rvert/R = 0.23.$	
$W = 2.$	

$q = 16, \quad g = 4$	32
$h(F/\mathbb{F}_{16}) = 114800, \quad \mathcal{C}l^0(F/\mathbb{F}_{16}) \cong 5 \times 22960.$	$T = 19\,s$
$F := \mathbb{F}_{16}(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 2, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 2, \quad \lvert S\rvert = 172, \quad RV =_? 436.$	
$RR = 680, \quad RV = 703, \quad R = 575 \quad \longrightarrow \quad R/RV = 0.82, \quad \lvert S\rvert/R = 0.3.$	
$W = 2.$	

$q = 64, \quad g = 4$	33
$h(F/\mathbb{F}_{64}) = 20041000, \quad \mathcal{C}l^0(F/\mathbb{F}_{64}) \cong 5 \times 35 \times 114520.$	$T = 15\,s$
$F := \mathbb{F}_{64}(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 76, \quad RV =_? 3919.$	
$RR = 428, \quad RV = 2399, \quad R = 302 \quad \longrightarrow \quad R/RV = 0.13, \quad \lvert S\rvert/R = 0.25.$	
$W = 3.$	

$q = 256, \quad g = 4$	34
$h(F/\mathbb{F}_{256}) = 5470220000, \quad \mathcal{C}l^0(F/\mathbb{F}_{256}) \cong 5 \times 5 \times 5 \times 43761760.$	$T = 111\,s$
$F := \mathbb{F}_{256}(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 320, \quad RV =_? 15520.$	
$RR = 1181, \quad RV = 7868, \quad R = 1230 \quad \longrightarrow \quad R/RV = 0.16, \quad \lvert S\rvert/R = 0.26.$	
$W = 2.$	

$q = 512, \quad g = 4$	35
$h(F/\mathbb{F}_{512}) = 76440901630, \quad \mathcal{C}l^0(F/\mathbb{F}_{512}) \cong 76440901630.$	$T = 562\,s$
$F := \mathbb{F}_{512}(x,\rho): \quad \rho^2 + (x+1)\rho + x^9 + x^3 + 1 = 0.$	$n = 2, \quad C_f = 5$
$A = (x)_\infty \sim (2,1).$	
$m_E = 1, \quad m_P = 1, \quad m_H = 1 \quad \longrightarrow \quad m_B := 1, \quad \lvert S\rvert = 566, \quad RV =_? 44660.$	
$RR = 2163, \quad RV = 25730, \quad R = 2279 \quad \longrightarrow \quad R/RV = 0.089, \quad \lvert S\rvert/R = 0.25.$	
$W = 2.$	

7.4 Hyperelliptische Funktionenkörper

Wir betrachten eine Familie von hyperelliptischen Funktionenkörpern F/k für $k = \mathbb{F}_3$, welche durch

$$y^2 = f(x)$$

mit einem normierten, irreduziblen Polynom $f(x) \in k[x]$, $\deg\big(f(x)\big) \leq 13$ gegeben werden. Ist $\deg\big(f(x)\big)$ gerade, so erhalten wir reell-quadratische, andernfalls imaginär-quadratische Erweiterungen $F/k(x)$ mit „Primdiskriminante“.

Die Tabelle gliedert sich wie folgt: d bezeichnet den Grad von $f(x)$. In der mit $f(x)$ überschriebenen Spalte stehen die Anzahlen der Primpolynome $f(x)$ des Grads d. Danach folgen das Geschlecht g, das Minimum $h_{\min}$, Maximum $h_{\max}$ und arithmetische Mittel h' der Klassenzahlen. Die Spalte $Cl : f(x)$ beinhaltet Einträge $a : b$, wobei a die Anzahl der Isomorphietypen der nicht zyklischen Klassengruppen $\mathcal{C}l^0(F/k)$ und b die Anzahl der zugehörigen $f(x)$ bedeutet. Bis auf Grad 12 sind die nicht zyklischen Klassengruppen das Produkt zweier zyklischer Faktoren, wobei der erste Faktor in den meisten Fällen $\mathbb{Z}/3\mathbb{Z}$ ist. Die Berechnung der einzelnen Klassengruppen nahm durchschnittlich $4.5s$ in Anspruch.

d	$f(x)$	g	$h_{\min}$	$h_{\max}$	h'	$Cl : f(x)$	
1	3	0	1	1	1.0	0 : 0	
2	3	0	1	1	1.0	0 : 0	
3	8	1	1	7	4.0	0 : 0	
4	18	1	2	6	4.0	0 : 0	
5	48	2	3	29	14.1	0 : 0	
6	116	2	3	35	15.0	0 : 0	
7	312	3	9	111	50.4	0 : 0	
8	810	3	12	136	58.5	1 : 6	(3×12)
9	2184	4	21	387	172.2	10 : 43	
10	5880	4	33	513	200.6	5 : 78	
11	16104	5	49	1291	607.3	41 : 198	
12	44220	5	86	1714	711.8	41 : 838	
						1 : 3	$(3 \times 3 \times 18)$
13	122640	6	155	4217	2029.9	186 : 1722	

7.5 Viele Stellen vom Grad eins

Wir betrachten nun speziell konstruierte Funkionenkörper, welche viele Stellen vom Grad eins besitzen. Die ersten beiden Beispiele wurden uns von R. Auer und G. Pirsic mitgeteilt und weisen die maximal mögliche Anzahl $N_1(F/k)$ auf,

das dritte Beispiel haben wir einer Tabelle von [19] entnommen. Ein besonders aufälliges Verhalten des Klassengruppenverfahren läßt sich hier nicht beobachten.

$q = 4, \quad g = 13, \quad N_1(F/k) = 33$	36
$h(F/\mathbb{F}_4) = 96486886125, \quad \mathcal{C}l^0(F/\mathbb{F}_4) \cong 3 \times 3 \times 21 \times 21 \times 21 \times 105 \times 105 \times 105.$	$T = 1178\,s$
$R(S_0) = 1, \quad h(S_0) = 96486886125,$ $\mathcal{C}l(\mathfrak{o}^S) \cong 3 \times 3 \times 21 \times 21 \times 21 \times 105 \times 105 \times 105.$	
$F := \mathbb{F}_4(x,\rho):$ $\rho^8 + (x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)\rho^4 + (x^{10} + x^9 + x^3 + x^2)\rho^2 +$ $(x^{10} + x^9 + x^8 + x^6 + x^5 + x^4)\rho + x^{22} + wx^{20} + wx^{18} + wx^{16} + x^{15} +$ $w^2x^{12} + x^{11} + wx^{10} + x^9 + wx^8 + x^6 + x^5 + x^4 = 0,$ $w^2 + w + 1 = 0.$	$n = 8, \quad C_f = 3$
$A = (x)_\infty \sim (8, 1).$ $m_E = 5, \quad m_P = 4, \quad m_H = 1 \quad \longrightarrow \quad m_B := 5, \quad \lvert S\rvert = 345, \quad RV =_? 1286.$ $RR = 397, \quad RV = 1051, \quad R = 644 \quad \longrightarrow \quad R/RV = 0.61, \quad \lvert S\rvert/R = 0.54.$ $W = 1.$	

$q = 2, \quad g = 9, \quad N_1(F/k) = 12$	37
$h(F/\mathbb{F}_2) = 135200, \quad \mathcal{C}l^0(F/\mathbb{F}_2) \cong 260 \times 520.$	$T = 997\,s$
$R(S_0) = 135200, \quad h(S_0) = 1, \quad \mathcal{C}l(\mathfrak{o}^S) \cong 1.$	
$F := \mathbb{F}_2(x,\rho):$ $\rho^{12} + (x^2+x+1)\rho^{10} + (x^2+x+1)\rho^9 + (x^4+x^2+1)\rho^8 + (x^6+x^5+x^4+$ $x^3+x^2+x)\rho^6 + (x^6+x^5+x^3+x+1)\rho^5 + (x^6+x^5+x^3+x^2)\rho^4 + (x^6+$ $x^5+x^3+x+1)\rho^3 + (x^4+x^2+1)\rho^2 + (x^4+x^2+1)\rho + x^2 + x + 1 = 0.$ $n = 12, \quad C_f = 1$	
$A = (x)_\infty \sim (1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1;1,1).$ $m_E = 8, \quad m_P = 8, \quad m_H = 2 \quad \longrightarrow \quad m_B := 8, \quad \lvert S\rvert = 83, \quad RV =_? 112.$ $RR = 249, \quad RV = 252, \quad R = 196 \quad \longrightarrow \quad R/RV = 0.78, \quad \lvert S\rvert/R = 0.42.$ $W = 3.$	

$q = 9, \quad g = 7, \quad N_1(F/k) = 36$	38
$h(F/\mathbb{F}_9) = 86704128, \quad \mathcal{C}l^0(F/\mathbb{F}_9) \cong 16 \times 48 \times 336 \times 336.$	$T = 88\,s$
$R(S_0) = 48, \quad h(S_0) = 1806336, \quad \mathcal{C}l(\mathfrak{o}^S) \cong 16 \times 336 \times 336.$	
$F := \mathbb{F}_9(x,\rho):$ $\rho^4 + (-x^5 + x^4 - x^3 + x^2)\rho^2 + x^8 - x^6 + x^5 + x^4 + x^3 + x^2 = 0.$ $n = 4, \quad C_f = 3$	
$A = (x)_\infty \sim (2,1;2,1).$ $m_E = 3, \quad m_P = 2, \quad m_H = 2 \quad \longrightarrow \quad m_B := 3, \quad \lvert S\rvert = 256, \quad RV =_? 834.$ $RR = 314, \quad RV = 792, \quad R = 470 \quad \longrightarrow \quad R/RV = 0.59, \quad \lvert S\rvert/R = 0.54.$ $W = 1.$	

7.6 p-Rang der Klassengruppe und Hasse-Witt-Invariante

Zum Abschluß betrachten wir ein Beispiel für die Berechnung des p-Rangs der Klassengruppe und der Hasse-Witt-Invariante eines globalen Funktionenkörpers mit Hilfe des Cartier-Operators, wie in Abschnitt 3.4 beschrieben.

Es sei $k = \mathbb{F}_q$ mit $q = 5^{12} = 244140625$ und F/k der durch

$$f(x, y) = y^4 - x^2y + 3x^{18} + 2$$

definierte globale Funktionenkörper vom Geschlecht $g = 23$.

Die Berechnung der k-Basis der holomorphen Differentiale $\Omega^1(F/k)$ benötigt $17s$. Danach wird die Darstellungsmatrix $(d_{i,j})_{i,j} \in k^{g \times g}$ des Cartier-Operators wie in Satz 3.26 in $82s$ berechnet.

Für den p-Rang der Klassengruppe gilt

$$\dim_{\mathbb{F}_p} \mathcal{C}l^0(F/k)[p] = 4,$$

die Hasse-Witt-Invariante beträgt

$$\sigma(F/k) = 15.$$

Hierfür wurde schließlich eine Zeit von $1.3s$ beziehunsgweise $1.8s$ in Anspruch genommen.

Wir bemerken, daß dieses Beispiel sicherlich außerhalb der Reichweite des allgemeinen Verfahrens der Klassengruppenberechnung liegt. Außerdem wird klar, daß die Berechung diskreter Logarithmen in $\mathcal{C}l^0(F/k)[p]$ in der Tat sehr effizient durchgeführt werden kann.

Symbolverzeichnis

(a)	Hauptdivisor von $a \in F^\times$	2
$(a)_0$	Nullstellendivisor des Hauptdivisors (a)	2
$(a)_\infty$	Polstellendivisor des Hauptdivisors (a)	2
$[D]$	Divisorenklasse von D	3
$(D)_0$	Nullstellendivisor des Divisors D	2
$(D)_\infty$	Polstellendivisor des Divisors D	2
$\langle M \rangle$	Untergruppe von $\mathcal{D}(F/k)$, die von einer Menge M von Divisoren erzeugt wird	2
$\dot{+}$	Innere direkte Summe	32
A	Divisor	56, 62
A_1	Divisor vom Grad eins	44
χ	Charakter endlicher Ordnung der Divisorenklassengruppe	39
$\mathrm{cont}(h)$	Inhalt einer rationalen Funktion $h \in k(x)$	30
C	Cartier-Operator	49
C_f	Koeffizientengröße des F/k erzeugenden Polynoms $f(x, y)$	5
$\mathcal{C}l(F/k)$	Divisorenklassengruppe von F/k	3
$\mathcal{C}l^n(F/k)$	Menge der Divisorenklassen vom Grad n von F/k	3
$\mathcal{C}l(\mathfrak{o}^S)$	Idealklassengruppe von $\mathfrak{o}^S$	4
$\mathrm{Cl}(A, B)$	Ring der über A ganzalgebraischen Elemente von B	5
c_0	$c_0 = O(1)$ mit $c_0^{-1}\|v\|_\infty \leq \|Tv\|_\infty \leq c_0\|v\|_\infty$	65
deg	Grad eines Divisors über dem exakten Konstantenkörper k_0	1
$\deg_{\tilde{k}}$	Grad eines Divisors über dem Konstantenkörper $\tilde{k}$	1
$\dim(D)$	Dimension des Riemann-Roch-Raums $\mathcal{L}(D)$ über dem exakten Konstantenkörper k_0	2

$\dim_{\tilde{k}}(D)$	Dimension des Riemann-Roch-Raums $\mathcal{L}(D)$ über dem Konstantenkörper $\tilde{k}$	2
D, D_i	Divisoren	2, 65
D^*	(k,x)-dualer Divisor zu D	18, 20
$\|D\|_i$	$k[x]$-Invarianten des Divisors D	12
$\mathcal{D}_{F/k(x)}$	Differentendivisor der Erweiterung $F/k(x)$	19
$\mathcal{D}(F/k)$	Gruppe der Divisoren von F/k	2
$\mathcal{D}^n(F/k)$	Menge der Divisoren vom Grad n von F/k	2
$\mathcal{D}(S)$	Gruppe der S-glatten Divisoren	3
$\mathcal{D}^m(S)$	Menge der S-glatten Divisoren vom Grad m	3
D^S	Das dem Divisor D zugeordnete Ideal von $\mathfrak{I}^S$	12
D_S	Das dem Divisor D zugeordnete Ideal von $\mathfrak{I}_S$	12
$\mathcal{D}^{\max}_{\mathrm{red}}(F/k,A)$	Menge der entlang A maximalreduzierten Divisoren von F/k	23
$\mathcal{D}^m_{\mathrm{red}}(F/k,A)$	Menge der entlang A m-minimalreduzierten Divisoren von F/k	23
$\mathcal{D}^{\max}_{\mathrm{red}}(S,A)$	Menge der entlang A maximalreduzierten S-glatten Divisoren	56
$\mathcal{D}^m_{\mathrm{red}}(S,A)$	Menge der entlang A m-minimalreduzierten S-glatten Divisoren	56
e_i	Verzweigungsindex einer Stelle P_i über ∞	22
$\bar{F}$	Algebraischer Abschluß von F	39
F/k	Algebraischer Funktionenkörper	1
F_r/k_r	Konstantenkörpererweiterung vom Grad r	7, 39
g	Geschlecht eines Funktionenkörpers F/k	2, 14, 20
$h(D)$	Höhe des Divisors D	15
$h(F/k)$	Klassenzahl von F/k	3
$h(S)$	Ordnung der Idealklassengruppe von $\mathfrak{o}^S$	4
$I(\bar{h})$	Intervall um eine Approximation der Klassenzahl	59
$\mathfrak{I}_S$	Idealgruppe von $\mathfrak{o}_S$	3
$\mathfrak{I}^S$	Idealgruppe von $\mathfrak{o}^S$	3
k	Konstantenkörper	1
k_0	Exakter Konstantenkörper	1
k_r	Erweiterung des endlichen Konstantenkörpers k vom Grad r	7, 39
$\bar{k}$	Algebraischer Abschluß von k in $\bar{F}$	43

$\lambda_{S,A}$	Divisorabbildung	65
$\Lambda_{S,A}$	Relationengitter	65
$l_{S,A}$	Quaderkantenlänge	67
$\Lambda_{S,A}^{\mathrm{red}}$	Bild von $\mathcal{D}_{\mathrm{red}}^{\deg(A)}(S,A)$ unter $\lambda_{S,A}$	65
$L(\chi,t)$	L-Reihe von χ	39
$\mathcal{L}(D)$	Riemann-Roch-Raum des Divisors D	2
$\mathrm{md}\big([D]\big)$	Minimalgrad von $[D]$	44
m_B	Verwendete Schranke für die Faktorbasis	74
m_E	Schranke für die Erzeugung der Faktorbasis	60
m_H	Heuristische Schranke für die Faktorbasis	74
m_P	Schranke für die Approximation der Klassenzahl	60
n	Erweiterungsgrad $[F:k(x)]$ oder Schranke für Stellen	5, 11, 51, 69, 74
$\mathrm{N}_{F/k(x)}$	Norm von F nach $k(x)$	5
$\mathrm{N}_{F_r/F}$	Norm von F_r nach F	41
$N_{\mathrm{red}}^{\max}(S,A)$	Anzahl der entlang A maximalreduzierten S-glatten Divisoren	56
$N_{\mathrm{red}}^{m}(S,A)$	Anzahl der entlang A m-minimalreduzierten S-glatten Divisoren	56
$N_r(\chi)$	Charaktersumme r-ten Grads	40
$N_r(F/k)$	Charaktersumme r-ten Grads für den Hauptcharakter $\chi = 1$	7, 41
$\omega_i(\chi)$	Reziproke Nullstellen von $L(\chi,t)$	40
$\omega_i(F/k)$	Reziproke Nullstellen von $\zeta_{F/k}(t)$	41
$\Omega(F/k)$	Raum aller Differentiale von F/k	2
$\Omega(D)$	Differentialraum des Divisors D	2
$O()$, $o()$	Landau-Symbole	7
$\mathfrak{o}_S$	Ring der an allen Stellen aus S ganzen Elemente	3
$\mathfrak{o}^S$	Ring der an allen Stellen außerhalb S ganzen Elemente	3
$(\mathfrak{o}^S)^\times$	Einheitengruppe von $\mathfrak{o}^S$, die S-Einheiten	4
$\pi_r(F/k)$	Anzahl der Stellen des Grads r von F/k	42
$\Psi_{F/k}(n,m)$	Anzahl aller (n,m)-glatten Divisoren	51
p	Endliche Charakteristik des Körpers k	39, 48
$p_{S,A}$	Glattheitswahrscheinlichkeit	74
P, P_i	Stellen von F/k	1, 21

$\mathcal{P}(F/k)$	Gruppe der Hauptdivisoren von F/k	2
$\mathcal{P}l(F/k)$	Menge aller Stellen von F/k	1
$\mathcal{P}l^n(F/k)$	Menge der Stellen vom Grad n von F/k	1
$\mathcal{P}l^{\leq n}(F/k)$	Menge der Stellen vom Grad kleiner gleich n von F/k	1
$\mathcal{P}(S)$	Gruppe der Hauptdivisoren von S-Einheiten	3
q	Elementanzahl des endlichen Körpers k	39, 48
$Q_{S,A}$	Quader in $\mathbb{Z}^s$	67
$Q_{S,A}^{\mathrm{red}}$	Quader in $\mathbb{Z}^s$	67
$r_{S,A}$	Relationenabbildung	66
R	Dedekindring	30
$R(S)$	S-Regulator	4
$R\langle x\rangle$	Ring der rationalen Funktionen mit ganzem Inhalt	30
$\sigma(F/k)$	Hasse-Witt-Invariante von F/k	44
$\mathrm{supp}(D)$	Träger des Divisors D	2
S	Nicht-leere Menge von Stellen von F/k.	5, 11, 59
v_P	Exponentielle, surjektive Bewertung von $F \longrightarrow \mathbb{Z}\cup\{\infty\}$ an der Stelle P	1
$v_P(D)$	Exponent der Stelle P im Divisor D	2
x	Separierendes Element	1
$\zeta_{F/k}(t)$	Zeta-Funktion des Funktionenkörpers F/k	39

Literaturverzeichnis

[1] L. Adleman, J. DeMarrais, M.-D. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, Proceedings of the First Symposium on Algorithmic Number Theory, ANTS-I (Ithaca, NY) (L. Adleman et. al., ed.), LNCS 877, Springer-Verlag, Berlin - Heidelberg - New York, 1994, pp. 28–40.

[2] E. Artin und J. Tate, *Class field theory*, Benjamin, New York, 1968.

[3] R. Auer, *Ray class fields of global function fields with many rational places*, Dissertation, Carl-von-Ossietzky-Universität, Oldenburg, 1999.

[4] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380.

[5] E. Bach, *Improved approximations for Euler products*, CMS Conf. Proc. **15** (1995), 13–28.

[6] D. Le Brigand und J. J. Risler, *Algorithme de Brill-Noether et codes de Goppa*, Bull. Soc. Math. France **116** (1988), 231–253.

[7] J. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Semin. Theor. Nombres, Prog. Math. **91** (1990), 27–41.

[8] A. L. Chistov, *The complexity of constructing the ring of integers of a global field*, Soviet Math. Dokl. **39** (1989), 597–600.

[9] H. Cohen, *A course in algebraic number theory*, 3rd corr. printing, GTM 138, Springer-Verlag, Berlin - Heidelberg - New York, 1996.

[10] H. Cohen, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), 1681–1699.

[11] P. M. Cohn, *Algebraic numbers and algebraic functions*, Chapman & Hall, London, 1991.

[12] M. Deuring, *Lectures on the theory of algebraic functions of one variable*, LNM 314, Springer-Verlag, Berlin - Heidelberg - New York, 1973.

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

[14] G. Frey, *On the structure of the class group of a function field*, Arch. Math. **33** (1979), 33–40.

[15] G. Frey, M. Müller und H.-G. Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, Preprint, 1998.

[16] G. Frey und H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[17] C. Friedrichs, *Berechnung relativer Ganzheitsbasen mit dem Round-2-Algorithmus*, Diplomarbeit, Technische Universität Berlin, 1997.

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

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

[20] G. Haché, *Computation in algebraic function fields for effective construction of algebraic-geometric codes*, Applied algebra, algebraic algorithms and error-correcting codes, AAECC-11 (Paris) (G. Cohen et al., ed.), LNCS 948, Springer-Verlag, Berlin - Heidelberg - New York, 1995, pp. 262–278.

[21] H. Hasse und E. Witt, *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p*, Monatsh. Math. Phys. **43** (1936), 477–492.

[22] H. Heilbronn, *Zeta-functions and L-functions*, Algebraic Number Theory (J. W. S. Cassels & A. Fröhlich, ed.), Academic Press, London, 1967, pp. 204–230.

[23] F. Heß, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, Technische Universität Berlin, 1996.

[24] M.-D. Huang, D. Ierardi, *Counting points on curves over finite fields*, J. Symbolic Comp. **25** (1998), 1–21.

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

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

[27] H. Koch, *Zahlentheorie*, Vieweg Verlag, Braunschweig, 1997.

[28] M. Kruse, H. Stichtenoth, *Ein Analogon zum Primzahlsatz für algebraische Funktionenkörper*, manuscripta math. **69** (1990), 219–221.

[29] S. Lang, *Elliptic functions*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.

[30] J. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, Trans. Amer. Math. Soc. **45** (1965), 245–264.

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

[32] J. S. Milne, *Abelian varieties*, Arithmetic Geometry (Storrs, Connecticut) (G. Cornell & J. H. Silverman, ed.), Springer-Verlag, Berlin - Heidelberg - New York, 1986, pp. 103–150.

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

[34] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin - Heidelberg - New York, 1992.

[35] D. Panario, X. Gourdon und Ph. Flajolet, *An analytic approach to smooth polynomials over finite fields*, Proceedings of the Third Symposium on Algorithmic Number Theory, ANTS-III (Portland, Oregon) (J. Buhler, ed.), LNCS 1423, Springer-Verlag, Berlin - Heidelberg - New York, 1998, pp. 226–236.

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

[37] M. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, 1st paperback ed., Cambridge University Press, Cambridge, 1997.

[38] C. Pomerance, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory (R. Tijdeman & H. Lenstra, ed.), Mathematisch Centrum, Tract 154, Amsterdam, 1982, pp. 89–139.

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

[40] H.-G. Quebbemann, *Estimates of regulators and class numbers in function fields*, J. reine angew. Math. **419** (1991), 79–87.

[41] F. Reinhard und H. Soeder, *dtv-Atlas zur Mathematik Band 2*, Deutscher Taschenbuch Verlag, München, 1990.

[42] M. Rosen, *The asymptotic behavior of the class group of a function field over a finite field*, Arch. Math. **24** (1973), 287–296.

[43] M. Rosen, *S-units and S-class group in algebraic function fields*, J. Algebra **26** (1973), 98–108.

[44] M. Rosenbloom, M. Tsfasman, *Multiplicative lattices in global fields*, Invent. math. **101** (1990), 687–696.

[45] H.-G. Rück, *Class groups and L-series of function fields*, J. Number Th. **22** (1986), 177–189.

[46] H.-G. Rück, *On the discrete logarithm in the divisor class group of curves*, Preprint, 1997.

[47] E. Scheid, *Ein neuer Algorithmus zur Berechnung der Klassenzahl algebraischer Zahlkörper*, Diplomarbeit, Universität des Saarlandes, 1993.

[48] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeit. **33** (1931), 1–32.

[49] R. Schoof, *Elliptic curves over finite fields and the computation of square roots*, Math. Comp. **44** (1985), 483–494.

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

[51] J. P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Sympos. Internat. Topologia Algebraica (Mexico City), 1956, pp. 24–53.

[52] M. Seysen, *A probabilistic factorization algorithm with quadratic forms of negative discriminant*, Math. Comp. **48** (1987), 757–780.

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

[54] H. Stichtenoth, *Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers*, Arch. Math. **33** (1979), 357–360.

[55] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin - Heidelberg - New York, 1993.

[56] J. Graf v. Schmettow, *Beiträge zur Klassengruppenberechnung*, Dissertation, Heinrich-Heine Universität Düsseldorf, 1991.

[57] E. Volcheck, *Computing in the Jacobian of a plane algebraic curve*, Proceedings of the First Symposium on Algorithmic Number Theory, ANTS-I (Ithaca, NY) (L. Adleman et. al., ed.), LNCS 877, Springer-Verlag, Berlin - Heidelberg - New York, 1994, pp. 221–233.

[58] E. Volcheck, *Addition in the Jacobian of a curve over a finite field*, Computational Number Theory (Oberwolfach), conference manuscript, 1995.

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

Zusammenfassung

Es sei F/k ein algebraischer Funktionenkörper, gegeben durch

$$F = k(x, \rho) \text{ mit } f(x, \rho) = 0$$

für ein in y normiertes und separables, irreduzibles Polynom $f(x, y) \in k[x, y]$.

Wir beschreiben eine konstruktive Fassung der Riemann-Roch-Theorie, die es uns gestattet, das Geschlecht g von F/k und Riemann-Roch-Räume $\mathcal{L}(D)$ von Divisoren D mit Techniken der algorithmischen algebraischen Zahlentheorie zu berechnen. Wir geben ferner einen wichtigen Algorithmus zur Divisorreduktion an und entwickeln Methoden, mit denen zusätzlich diskrete Bewertungen von k berücksichtigt werden können.

Es sei $k = \mathbb{F}_q$ der exakte Konstantenkörper des globalen Funktionenkörpers F/k. Die Divisorenklassengruppe ist die Gruppe aller Divisorenklassen von F/k. Die Klassengruppe $\mathcal{C}l^0(F/k)$ ist die endliche Gruppe der Divisorenklassen vom Grad null. Ihre Ordnung ist die Klassenzahl $h(F/k)$.

Für eine Menge S von Stellen P von F/k mit $\deg(P) \leq m$ beweisen wir mit Hilfe des Satzes von Hasse-Weil untere Schranken für m, so daß $\mathcal{C}l^0(F/k)$ durch die Klassen der Divisoren vom Grad null mit Träger in S erzeugt wird. Diese Schranken sind von der Form $O\big(\log(g)\big)$ bei festem q. Weiter geben wir eine Formel für die Approximation von $h(F/k)$ bis auf einen festen, multiplikativen Fehler an, für welche die Anzahlen der Stellen eines Grads ebenfalls $O\big(\log(g)\big)$ benötigt werden, und formulieren eine Version des Satzes von Brauer-Siegel für globale Funktionenkörper.

Wir betrachten Glattheitseigenschaften. Ein Divisor D ist (n, m)-glatt, wenn $\deg(D) \leq n$ gilt und sein Träger nur aus Stellen eines Grads $\leq m$ besteht. Wir beweisen verschiedene Aussagen über die Anzahl solcher Divisoren und formulieren eine Glattheitsannahme.

Das Hauptergebnis ist das Klassengruppenverfahren zur Berechnung der Klassengruppe beziehungsweise Divisorenklassengruppe von F/k. Dieses stützt sich auf die Relationenmethode, für die wir bei festem q deterministische, in g aber exponentielle Techniken und eine probabilistische, unter der Glattheitsannahme in g subexponentielle Technik entwickeln. Die vorhergehenden Ergebnisse werden hier eingesetzt. Wir beschreiben Anwendungen dieses Verfahrens zur Einheiten- und Idealklassengruppenberechnung und zur Bestimmung diskreter Logarithmen.

Den Abschluß bilden einige illustrative Beispiele, die das Laufzeitverhalten und die Anwendbarkeit des Verfahrens unter Variation der wesentlichen Parameter q und g demonstrieren.