Publ. I.R.M.A. Strasbourg, 1990, 413/S–21
Actes 21^{e} Séminaire Lotharingien, p. 46–54

Kettenbrüche und Divisoren in reell-quadratischen Erweiterungen von GF(q)[T]

von Andreas Guthmann in Kaiserslautern

Sei $p > 2$ eine Primzahl, q eine Potenz von p und $\mathbf{Z_T} = GF(q)[T]$ der Polynomring in der Unbestimmten T über $GF(q)$. Es ist bekannt, daß es viele Gemeinsamkeiten zwischen $\mathbf{Z_T}$ und dem Ring $\mathbf{Z}$ der ganzen Zahlen gibt und das soll auch durch unsere Bezeichnungen zum Ausdruck gebracht werden. Sei weiter $\mathbf{Q_T} = GF(q)(T)$ der Quotientenkörper von $\mathbf{Z_T}$. Dann ist $\mathbf{Q_T}$ nichtarchimedisch bewertet durch

$$\left|\frac{A}{B}\right| = q^{\operatorname{grad} A - \operatorname{grad} B} \text{ für } A,\ B \in \mathbf{Z_T}.$$

Bezeichnen wir mit $\mathbf{R_T}$ die Komplettierung von $\mathbf{Q_T}$ bezüglich $|\cdot|$, so ist $\mathbf{R_T}$ das Analogon der reellen Zahlen. Jedes $X \in \mathbf{R_T}$ hat eine eindeutige Darstellung in der Form

$$X = \sum_{\nu=n}^{-\infty} a_\nu T^\nu,\ a_\nu \in GF(q),\ a_n \neq 0,$$

und es ist $|X| = q^n$. Wir definieren außerdem das Signum von X durch $\operatorname{sgn} X = a_n$ und die größte ganze Funktion aus X durch $[X] := \sum_{\nu=n}^{0} a_\nu$. Ist $X = A/B \in \mathbf{Q_T}$, so gibt es $Q,\ R \in \mathbf{Z_T}$ mit $A = QB + R$ und $|R| < |B|$. Wie gewohnt sei dann $A \operatorname{div} B := [X] = Q$ und $A \bmod B := R$.
Im folgenden geben wir einen kleinen Überblick auf einige interessante Zusammenhänge zwischen Quadratwurzeln in $\mathbf{Z_T}$, deren Kettenbruchentwicklung und der Divisorentheorie in $GF(q)(T, \sqrt{D})$. Eine ausführliche Darstellung dieser Ergebnisse wird Gegenstand einer späteren Untersuchung seyn[5].

1. Kettenbrüche

Sei $D \in \mathbb{Z}_T$ mit $\operatorname{sgn} D = 1$ und $|D = q^{2m}$, $m \geq 1$. Dann gibt es bekanntlich[1, 3] ein $X \in \mathbb{R}_T$ mit $\operatorname{sgn} X = 1$, $|X| = q^m$ und $X^2 = D$. Wir setzen $\sqrt{D} := X$.
Die Berechnung von $\sqrt{D}$[3] geschieht am besten mit Hilfe des Newton-Verfahrens. Dazu sei $X_0 = T^m$ und $X_{n+1} = \frac{1}{2}(X_n + \frac{D}{X_n})$ und wie üblich findet man $\lim X_n = \sqrt{D}$. Für arithmetische Zwecke benötigt man aber oft nur $[\sqrt{D}]$, z.B. für Kettenbruchentwicklungen. Um $[\sqrt{D}]$ nur mit Operationen in $\mathbb{Z}_T$ zu berechnen, benutzt man ein diskretisiertes Newton-Verfahren: Sei wieder $X_0 = T^m$, aber nun $X_{n+1} = \frac{1}{2}(X_n + [\frac{D}{X_n}])$. Dann gibt es ein n mit $X_n = X_{n+1}$ und es ist $[\sqrt{D}] = X_n$. Einen Beweis findet man z.B. in [3].
Wir betrachten nun Kettenbrüche in $\mathbb{R}_T$. Sei $X_0 \in \mathbb{R}_T$ gegeben. Ist X_n vorgelegt und $X_n \neq [X_n]$, so setzen wir $X_{n+1} = \frac{1}{X_n - [X_n]}$, andernfalls bricht die Folge X ab. Auf diese Weise erhalten wir für alle $X_0 \in \mathbb{R}_T$ eine endliche oder unendliche Folge X. Es ist klar, daß X genau dann abbricht, wenn $X_0 \in \mathbb{Q}_T$ ist. Wir wollen hier von diesem Fall absehen.
Wir definieren nun drei weitere Folgen A, B und b durch $b_n = [X_n]$ für $n \geq 0$ und

$$A_{-1} = 1,\ A_0 = b_0,\ B_{-1} = 0,\ B_0 = 1$$

und

$$A_n = b_n A_{n-1} + A_{n-2},\ B_n = b_n B_{n-1} + B_{n-2} \text{ für } n \geq 1. \tag{1}$$

Die Quotienten $\frac{A_n}{B_n}$ heißen Näherungbrüche von X_0. Es gilt nämlich der

Approximationssatz:[4] Für $n \geq 0$ ist

$$\left| X_0 - \frac{A_n}{B_n} \right| = \frac{1}{|B_n||B_{n+1}|} = \frac{1}{|b_{n+1}||B_n|^2}.$$

Dieses Ergebnis zeigt, daß die Näherungsbrüche gute rationale Approximationen für X_0 liefern. Umgekehrt sind sie durch diese Eigenschaft charakterisiert und das ist der Inhalt des

Näherungsgesetzes:[4] Sei $X_0 \in \mathbb{R}_T \setminus \mathbb{Q}_T$ und für A, $B \in \mathbb{Z}_T{}^*$ gelte

$$\left| X_0 - \frac{A}{B} \right| < \frac{1}{|B|^2}.$$

Dann gibt es ein $n \geq 0$ mit $\frac{A}{B} = \frac{A_n}{B_n}$.

Wir werden nachher sehen, wie sich diese beiden Gesetze im Fall $X_0 = \sqrt{D}$ mit Hilfe der Divisoren in $\mathbb{Q}_T(\sqrt{D})$ deuten lassen.
Betrachten wir nun Kettenbruchentwicklungen von Quadratwurzeln. Wir wollen dabei stets

$$D \in \mathbb{Z}_T,\ |D| = q^{2m},\ m \geq 1,\ \operatorname{sgn} D = 1 \tag{2}$$

annehmen. Es sei dann X_0 in der Form

$$X_0 = \frac{\sqrt{D} + P_0}{Q_0} \text{ mit } P_0,\ Q_0 \in \mathbb{Z}_T,\ Q_0 \neq 0 \text{ und } Q_0 | D - P_0^2 \tag{3}$$

gegeben. Dann zeigt man leicht

$$X_n = \frac{\sqrt{D} + P_n}{Q_n},\ Q_n | D - P_n^2 \text{ für } n \geq 0$$

und man hat die Rekursionsformeln

$$P_{n+1} = b_n Q_n - P_n,\ Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n}.$$

Dabei ergibt sich b_n aus

$$b_n = [X_n] = ([\sqrt{D}] + P_n) \operatorname{div} Q_n,$$

so daß also $[\sqrt{D}]$ nur einmal berechnet werden muß. Es gilt die folgende wichtige Relation, die später eine Rolle spielen wird:

$$(Q_0 A_{n-1} - P_0 B_{n-1})^2 - D B_{n-1}^2 = (-1)^n Q_0 Q_n,\ n \geq 0. \tag{4}$$

Bekannt ist außerdem[4], daß die Kettenbruchentwicklung von $X_0 = \frac{\sqrt{D}+P_0}{Q_0}$ periodisch ist, d.h. es gibt $k \geq 0$, $l \geq 1$, so daß $X_{k+nl+i} = X_{k+i}$ für alle $n \geq 0$, $i \geq 0$ gilt. Ist X_0 reduziert, d.h. gilt $|\frac{-\sqrt{D}+P_0}{Q_0}| < 1 < |\frac{\sqrt{D}+P_0}{Q_0}|$, so ist der Kettenbruch rein periodisch, also $k = 0$. Man zeigt leicht, daß X_0 genau dann reduziert ist, wenn

$$|\sqrt{D} - P_0| \leq q^{-2}|\sqrt{D}| \text{ und } |P_0 - \sqrt{D}| < |Q_0| < |\sqrt{D}|$$

erfüllt sind. So ist z.B. $\sqrt{D} + [\sqrt{D}]$ reduziert.

2. Divisoren in $\mathbf{Q}_T$ und $\mathbf{Q}_T(\sqrt{D})$

Sei $P \in \mathbb{Z}_T$ ein Primpolynom. Jedes $X \in \mathbf{Q}_T$ läßt sich eindeutig in der Form $X = P^a \frac{U}{V}$ schreiben, mit $U,\ V \in \mathbb{Z}_T$, $a \in \mathbb{Z}$, $(P, UV) = 1$. Durch die Definition $w_P(x) := a$ erhalten wir so eine Bewertung w_P auf $\mathbf{Q}_T$. Der entsprechende Absolutbetrag ist $|X|_P = q^{-w_P(X)}$. Eine weitere Bewertung w_∞ erhalten wir durch $w_\infty(\frac{U}{V}) := \operatorname{grad} V - \operatorname{grad} U$ und entsprechend $|\frac{U}{V}|_\infty = |\frac{U}{V}| = q^{\operatorname{grad} U - \operatorname{grad} V}$ für $U,\ V \in \mathbb{Z}_T$.
Es ist bekannt[6], daß durch die w_P und w_∞ alle Bewertungen (genauer: alle Äquivalenzklassen von Bewertungen) von $\mathbf{Q}_T$ gefunden sind. Die Menge der Bewertungen von $\mathbf{Q}_T$ bezeichnen wir mit $W(\mathbf{Q}_T)$.

Jeder Bewertung $w \in W(\mathbf{Q}_T)$ wird nun formal ein Primdivisor $\mathcal{P}_w$ zugeordnet. Wir schreiben $\mathcal{P}_w = \mathcal{P}_P$, falls $w = w_P$ und $\mathcal{P}_w = \infty$, falls $w = w_\infty$. Die Menge der Primdivisoren von $\mathbf{Q}_T$ bezeichnen wir mit $P(\mathbf{Q}_T)$ und die von ihnen erzeugte freie abelsche Gruppe heißt *Divisorengruppe* $Div(\mathbf{Q}_T)$ von $\mathbf{Q}_T$.
Ist $\mathcal{P}_w \in P(\mathbf{Q}_T)$, so sei $R_w = \{X \in \mathbf{Q}_T | w(X) \geq 0\}$ und $I_w = \{X \in \mathbf{Q}_T | w(X) > 0\}$. Dann ist $K_w = R_w/I_w$ ein endlicher Körper, der Restklassenkörper der Bewertung w und der Grad von K_w über GF(q) heißt auch Grad $\deg(\mathcal{P}_w)$ des zu w gehörenden Primdivisors $\mathcal{P}_w$; Offenbar ist $\deg(\mathcal{P}_w) = \text{grad}(P)$, falls $w = w_P$ und $\deg(\infty) = 1$. Für einen beliebigen Divisor $\mathcal{D} \in Div(\mathbf{Q}_T)$, etwa $\mathcal{D} = \prod_w \mathcal{P}_w^{e_w}$ (nur endlich viele $e_w \neq 0$), definieren wir $\deg(\mathcal{D}) = \sum e_w \deg(\mathcal{P}_w)$. Die Divisoren vom Grad 0 bilden eine Untergruppe $Div_0(\mathbf{Q}_T)$ von $Div(\mathbf{Q}_T)$.
Jedes $X \in \mathbf{Q}_T$ definiert einen Divisor $(X) \in Div_0(\mathbf{Q}_T)$ gemäß

$$(X) = \prod_{w \in W(\mathbf{Q}_T)} \mathcal{P}_w^{w(X)}.$$

Ist etwa $X = \prod_P P^{e_P}$ mit $e_P \in \mathbb{Z}$ die kanonische Primfaktorzerlegung und $\text{grad}\, X = n$, so ist $(X) = \infty^{-n} \prod (P)^{e_P}$. Die Divisoren (X) heißen Hauptdivisoren und bilden eine Untergruppe $Div_H(\mathbf{Q}_T)$ von $Div_0(\mathbf{Q}_T)$.

Nun sei wieder $D \in \mathbb{Z}_T$, $\text{sgn}\, D = 1$, $|D| = q^{2m}$, $m \geq 1$ und D quadratfrei in $\mathbb{Z}_T$. Wir betrachten dann den Körper $\mathrm{K} = \mathbf{Q}_T(\sqrt{D})$, der durch Adjunktion einer Wurzel des irreduziblen Polynoms $F(X) = X^2 - D \in \mathbb{Z}_T[X]$ aus $\mathbf{Q}_T$ entsteht. Die über $\mathbb{Z}_T$ ganzen Elemente aus K bilden einen Integritätsbereich R. Es gilt

$$\mathrm{K} = \mathbf{Q}_T \oplus \mathbf{Q}_T \sqrt{D},\ \mathrm{R} = \mathbb{Z}_T[\sqrt{D}] = \mathbb{Z}_T \oplus \mathbb{Z}_T \sqrt{D}.$$

K hat einen Automorphismus $'$ der ein Element $X = A + B\sqrt{D} \in \mathrm{K}$ auf sein Konjugiertes $X' := A - B\sqrt{D}$ abbildet. Die Norm von X ist $N(X) := XX' = A^2 - B^2 D$.
Man erhält nun alle Primdivisoren von K, indem man die Primdivisoren von $\mathbf{Q}_T$ fortsetzt. Sei dazu $P \in \mathbb{Z}_T$ prim, w_P die entsprechende Bewertung und $\mathbf{Q}_{T,P}$ die Komplettierung von $\mathbf{Q}_T$ bezüglich w_P. Zunächst sei P kein Teiler von D und die Kongruenz $X^2 \equiv D \bmod P$ lösbar. Nach dem Henselschen Lemma zerfällt dann das Polynom F in $\mathbf{Q}_{T,P}$ in zwei Linearfaktoren: $F(X) = (X - \sqrt{D})(X + \sqrt{D})$ mit $\sqrt{D} \in \mathbf{Q}_{T,P}$. Entsprechend gibt es zwei Fortsetzungen von w_P nach K, die wir mit $w_{P,1}$ und $w_{P,2}$ bezeichnen. Für $X = A + B\sqrt{D} \in \mathrm{K}$ ist dann

$$w_{P,1}(X) := w_P(X) = w_P(A + B\sqrt{D}),\ w_{P,2}(X) := w_P(X') = w_P(A - B\sqrt{D}),$$

wobei die w_P in $\mathbf{Q}_{T,P}$ bestimmt sind. Solchen Bewertungen w entsprechen zwei Primdivisoren $\mathcal{P}_w$ und $\mathcal{P}_{w'}$ vom Grad 1.
Nun sei die Kongruenz $X^2 \equiv D \bmod P$ nicht lösbar. Dann ist $\mathbf{Q}_{T,P}(\sqrt{D})$ eine Erweiterung vom Grad 2 von $\mathbf{Q}_{T,P}$ und für $X = A + B\sqrt{D} \in \mathrm{K}$ ist

$$w_P(X) := \frac{1}{2} w_P(XX') = \frac{1}{2} w_P(A^2 - B^2 D)$$

die (einzige) Fortsetzung von w_P nach K. Der zugehörige Primdivisor $\mathcal{P}_w$ hat den Grad 2. Es bleibt noch der Fall $P|D$ übrig. Hier gibt es eine Fortsetzung von w_P und der Primdivisor hat den Grad 2.
Schließlich betrachten wir noch die Fortsetzungen $w_{\infty,1}$ und $w_{\infty,2}$ des gewöhnliches Absolutbetrags. Hier haben wir

$$w_{\infty,1}(X) := w_\infty(x),\ W_{\infty,2}(X) := w_\infty(X'),$$

und die entsprechenden Primdivisoren ∞_1 und ∞_2 haben den Grad 1.
Mit $W(\mathrm{K})$ bezeichnen wir die Menge der Bewertungen von K, mit $P(\mathrm{K})$ die Menge der Primdivisoren und mit $Div(\mathrm{K})$ die Divisorengruppe von K. Wir haben wie üblich die Untergruppen $Div_0(\mathrm{K})$ der Divisoren vom Grad 0 und $Div_H(\mathrm{K})$ der Hauptdivisoren (X), die für $X \in \mathrm{K}$ wieder durch

$$(X) := \prod_{w \in W(\mathrm{K})} \mathcal{P}_w^{w(X)}$$

definiert sind. Hauptdivisoren haben natürlich den Grad 0. Dazu ein Beispiel. Sei $\eta \in \mathrm{R}$ die Fundamentaleinheit[1], etwa $\eta = A + B\sqrt{D}$. Dann ist $N(\eta) = \eta\eta' = A^2 - B^2 D \in GF(q)$ und aus $|\eta| = q^a$, $a \geq 1$, folgt $|\eta'| = q^{-a}$ und der Hauptdivisor $(\eta) \in Div_H(\mathrm{K})$ hat die Gestalt $\infty_1^{-a}\infty_2^a$.
Ein Divisor $\mathcal{D} = \prod_w \mathcal{P}_w^{e_w}$ heißt ganz, falls alle $e_w \geq 0$ sind. Sind $\mathcal{D}$, $\mathcal{E} \in Div(\mathrm{K})$, so nennen wir $\mathcal{D}$ ein Vielfaches von $\mathcal{E}$, wenn $\mathcal{D}/\mathcal{E}$ ganz ist. Eine Funktion $Z \in \mathrm{K}$ ist ein Vielfaches von $\mathcal{D}$, wenn $(Z)/\mathcal{D}$ ganz ist.
Die Vielfachen $Z \in \mathrm{K}$ von $\mathcal{D}^{-1}$ bilden einen $GF(q)$–Vektorraum endlicher Dimension, den wir mit $\mathrm{L}(\mathcal{D})$ bezeichnen. Seine Dimension heißt auch Dimension $\dim(\mathcal{D})$ von $\mathcal{D}$. Mit diesen Bezeichnungen gilt nun der wichtige

Satz von Riemann-Roch:

$$\dim(\mathcal{D}) = \deg(\mathcal{D}) + \dim\left(\frac{\mathcal{W}}{\mathcal{D}}\right) - g + 1. \tag{5}$$

Darin ist g das Geschlecht von K (für $|D| = q^{2m}$ ist $g = m - 1$) und $\mathcal{W}$ ein kanonischer Divisor vom Grad $2g - 2$. Wegen $\mathrm{L}(\mathcal{D}) = \{0\}$ für $\deg(\mathcal{D}) < 0$ haben wir als Spezialfall von (5)

$$\dim(\mathcal{D}) = \deg(\mathcal{D}) - g + 1,\ \text{falls}\ \deg(\mathcal{D}) \geq 2g - 1 \tag{6}$$

und, wenn $|D| = q^4$ ist, sogar

$$\dim(\mathcal{D}) = \deg(\mathcal{D}),\ g = 1,\ \deg(\mathcal{D}) \geq 1. \tag{7}$$

3. Die Regulatorgruppe und Kettenbrüche in $Q_T(\sqrt{D})$

Sei $U(K) := \langle \infty_1, \infty_2 \rangle$ die von den Divisoren ∞_1 und ∞_2 erzeugte Untergruppe von $Div(K)$. Außerdem seien $U_0(K) := U(K) \cap Div_0(K)$ und $U_H(K) := U(K) \cap Div_H(K)$. Dann gilt natürlich $U_H(K) \leq U_0(K) \leq U(K)$ und die Faktorgruppe

$$reg(K) := U_0(K)/U_H(K)$$

nennen wir die *Regulatorgruppe* von K. Sie ist eine endliche, zyklische Gruppe[8], und wegen $U_0(K) = \langle \Lambda \rangle$ mit $\Lambda := \infty_1^{-1}\infty_2$ ist $|reg(K)|$ die kleinste positive Zahl r, für die Λ^r ein Hauptdivisor ist. Wenn $\eta \in R$ wieder die Fundamentaleinheit bedeutet und $|\eta| = q^n$ ist, so folgt $r = n$.
Das Problem besteht nun darin, ob und wie in der Regulatorgruppe effektiv gerechnet werden kann. Wir werden sehen, daß es im Fall $g = 1$ ($|D| = q^4$) einen sehr einfachen Algorithmus dafür gibt. Zunächst untersuchen wir aber noch einige Zusammenhänge zwischen den Vektorräumen $L(\Lambda^{-n}\infty_1^a)$ und Kettenbrüchen.
Wir definieren eine Abbildung $\kappa : \mathbb{N}_0 \to \mathbb{N}_0$ durch

$$\kappa(n) := \min\{a \geq 0 | L(\infty_1^a \Lambda^{-n}) \neq \{0\}\}. \tag{8}$$

Ist $X \in L(\infty_1^a \Lambda^{-n})$, so folgt $(X) = \infty_1^{-a}\Lambda^n \mathcal{G} = \infty_1^{-a-n}\infty_2^n \mathcal{G}$ mit einem ganzen Divisor $\mathcal{G}$, und es ist sogar $X \in R$, also ganz algebraisch.
Nun ist $\deg(\infty_1^a \Lambda^{-n}) = a$ und daher $\kappa(n) \leq 2g - 1$ nach dem Riemann-Rochschen Satz in der Form (6). Kann der Fall $\kappa(n) \leq g$ eintreten? Darüber geben die folgenden beiden Sätze Auskunft:

Satz 1: Sei $n \in \mathbb{N}$, $\kappa(n) \leq g$ und $X = A + B\sqrt{D} \in R$ eine zugehörige Funktion.
Dann ist $\frac{A}{B}$ ein Näherungsbruch von $\sqrt{D}$.

Der Beweis kann mit Hilfe des Näherungsgesetzes geführt werden. Die Umkehrung folgt aus dem Approximationssatz:

Satz 2: Sei $\frac{A}{B}$ ein Näherungsbruch in der Kettenbruchentwicklung von $\sqrt{D}$ mit $|A| = q^s$.
Ist $X = A + B\sqrt{D}$, so gilt

$$(X) = \infty_1^{-a}\Lambda^n \mathcal{G},\ \mathcal{G} \text{ ganz},\ n \in \mathbb{N}_0,\ a + n = s \text{ und } 0 \leq a \leq g.$$

Man kann in diesen beiden Sätzen die divisoriellen Analoga des Approximationssatzes und des Näherungsgesetzes sehen.

4. Der Fall $|D| = q^4$

Der Satz von Riemann-Roch lautet hier

$$\dim(\mathcal{D}) = \deg(\mathcal{D}) \text{ falls } \deg(\mathcal{D}) \geq 1. \tag{9}$$

Wir betrachten die Kettenbruchentwicklung von $X_0 = \sqrt{D} + [\sqrt{D}]$. Da X_0 reduziert ist, gibt es ein kleinstes positives r mit $X_r = X_0$. Setzen wir wieder $X_n = (\sqrt{D} + P_n)/Q_n$, so gibt es auch ein minimales s mit $1 \leq s \leq r$ und $|Q_s| = 1$. Es gilt dann

$$|Q_n| = q,\ 1 \leq n \leq s-1,\ |b_n| = |X_n| = q,\ 1 \leq n \leq s-1$$
$$|A_n| = q^{n+2},\ 0 \leq n \leq s-1,\ |B_n| = q^n,\ 0 \leq n \leq s-1.$$

Schließlich ist auch noch $|\operatorname{reg}(\mathrm{K})| = s+1$, da $A_{s-1} + B_{s-1}\sqrt{D}$ bis auf Normierung die Fundamentaleinheit von R ist. Es sei nun

$$C_n := A_{n-1} - [\sqrt{D}]B_{n-1} + B_{n-1}\sqrt{D},\ n \geq 0.$$

Aus (4) folgt dann $N(C_n) = C_n C_n' = (-1)^n Q_n$ und weiter

$$(C_n) = \infty_1^{-n-1}\infty_2^n(Q_n) = \infty_1^{-1}\Lambda^n(Q_n) \text{ für } 1 \leq n \leq s-1,$$
$$(C_s) = \infty_1^{-s-1}\infty_2^{s+1} = \Lambda^{s+1},$$
$$(C_{s+1}) = \infty_1^{-s-3}\infty_2^{s+2}(Q_1) = \infty_1^{-1}\Lambda^{s+2}(Q_1).$$

Man beachte, daß dabei aufgrund von (9) der Divisor (Q_n) für $1 \leq n \leq s-1$ bzw. ∞_2 im Fall $n = s$ eindeutig bestimmt ist. Wir zeigen nun, daß mit Hilfe des Riemann-Rochschen Satzes die Gruppenstruktur von reg(K) auf die Primpolynome Q_n (genauer: die Divisoren (Q_n)) übertragen werden kann, so daß

$$Q_n \circ Q_l = Q_{n+l}$$

gilt. Der Einfachheit halber betrachten wir nur den Fall $n + l \leq s-1$, die Modifikationen für $n + l \geq s$ sind unschwer durchzuführen[5].
Wir bemerken wie oben, daß es wegen $\deg(\infty_1\Lambda^{-n}) = 1$ und (9) genau eine Funktion $C \in \mathrm{R}$ gibt, mit

$$\mathrm{L}(\infty_1\Lambda^{-n}) = \langle C \rangle.$$

Dem Divisor $\Lambda^{-n} \in U_0(\mathrm{K})$ ist also (bis auf einen Faktor aus $GF(q)$) für $n \leq s-1$ genau ein Primpolynom Q_n zugeordnet und die Gruppenstruktur von $U_0(\mathrm{K})$ legt eine Multiplikation der Q_n nahe. Der Kürze halber werden wir nur den Divisor (Q_{n+l}), d.h. das Primpolynom Q_{n+l} nur bis auf eine multiplikative Konstante bestimmen.
Wir nehmen also $\operatorname{sgn} Q_n = \operatorname{sgn} Q_l = 1$ und $n + l \leq s-1$ an und betrachten die Divisoren

$$(C_n C_l) = \infty_1^{-n-l-2}\infty_2^{n+l}(Q_n)(Q_l) = \infty_1^{-2}\Lambda^{n+l}(Q_n)(Q_l)$$

und

$$\mathcal{D} := \infty_1^{-1}(Q_n Q_l).$$

Wegen $\deg(\mathcal{D}) = 1$ gibt es genau ein $X \in \mathrm{K}$, das Vielfaches von $\mathcal{D}^{-1}$ ist, also

$$(X) = \infty_1 (Q_n Q_l)^{-1} \mathcal{G}, \tag{10}$$

mit einem ganzen Divisor $\mathcal{G}$, der alsdann vom Grad 1 ist. Es folgt nun

$$(C_n C_l)(X) = \infty_1^{-1} \Lambda^{n+l} \mathcal{G},$$

und weil $\mathcal{G}$ einzig und $(C_{n+l}) = \infty_1^{-1} \Lambda^{n+l}(Q_{n+l})$ ist

$$\mathcal{G} = (Q_{n+l}),$$

und somit ist Q_{n+l} bis auf eine multiplikative Konstante bestimmt.
Die Aufgabe besteht also nur noch darin, ein $X \in \mathrm{K}$ zu finden, das die Form (10) hat. Die Bedingungen lauten:

$$|X| = q^{-1}, \ |X|_{Q_n,1} = |X|_{Q_l,1} = q.$$

Zunächst berechne man ein $Y \in \mathbb{Z}_T$ mit $Y^2 \equiv D \bmod Q_n Q_l$. Dann ist

$$Y \equiv -\sqrt{D} \bmod Q_n Q_l, \ |Y| = q,$$

wobei das Vorzeichen der Wurzel noch geeignet gewählt werden muß . Dann sei

$$X := \frac{Q_n Q_l + Y - \sqrt{D}}{Q_n Q_l}.$$

Dann ist (X) ein Vielfaches des Divisors $\infty_1 (Q_n Q_l)^{-1}$ und es folgt

$$H = \frac{(Q_n Q_l + Y)^2 - D}{Q_n Q_l} \in \mathbb{Z}_T$$

und somit $H = Q_{n+l}$, bis auf Normierung.

Abschließend folgen noch einige ergänzende Anmerkungen. Bezeichnen wir mit h die Idealklassenzahl von R, so gilt nach Artin[1]

$$h|\operatorname{reg}(\mathrm{K})| = q + 2 + \sigma_1,$$

wobei σ_1 eine gewisse Charaktersumme ist, für die aus der Riemannschen Vermutung im Fall $g = 1$ die Abschätzung

$$|\sigma_1| \leq 2\sqrt{q}$$

folgt. Dies zeigt, daß

$$h|\operatorname{reg}(\mathrm{K})| \sim q, \text{ für } q \to \infty$$

ist (das Analogon der Brauer-Siegel-Formel), und daß $|\mathrm{reg}(K)|$ im Allgemeinen so groß wie q werden kann. Die genaue Ordnung r und die Gruppenstruktur von reg(K) kann mit Hilfe des Shanksschen Algorithmus[9] in $O(\sqrt{r})$ Schritten bestimmt werden.
Anwendungen der Regulatorgruppe sind z.B. Primzahltests (nach dem Vorbild von Goldwasser-Kilian[2]) und Primfaktorzerlegung nach Lenstra[7]. Man erhält hier einen Algorithmus, dessen Laufzeit etwa der ECM-Methode von Lenstra entspricht.

Literatur

[1] Artin, E., Quadratische Körper im Gebiet der höheren Kongruenzen I, Math. Zeitschrift **19**, 153-206(1924)

[2] Goldwasser,S., Kilian,J., Almost All Primes Can be Quickly Certified, Proc. 18. STOC, Berkeley 1986.

[3] Guthmann,A., Konstruktive Arithmetik in GF(q)[T] I, Preprint 1988.

[4] Guthmann,A., Konstruktive Arithmetik in GF(q)[T] II, Preprint 1988.

[5] Guthmann,A., Konstruktive Arithmetik in GF(q)[T] IV, in Vorbereitung.

[6] Hasse,H., Number Theory, Springer 1980.

[7] Lenstra, H.W. Jr., Factoring Integers with Elliptic Curves, Ann. of Math. **126**, 649-673(1987).

[8] Schmidt,F.K., Analytische Zahlentheorie in Körpern der Charakteristik p, Math. Zeitschrift **33**, 1-32(1931).

[9] Shanks,D., Class Number, a Theory of Factorization, and Genera, Proc. Symp. Pure Math. **20**, 415-440(1971).

Anschrift des Autors:

Andreas Guthmann
Fachbereich Mathematik
Universität Kaiserslautern
Pfaffenbergstr. 95
D-6750 Kaiserslautern