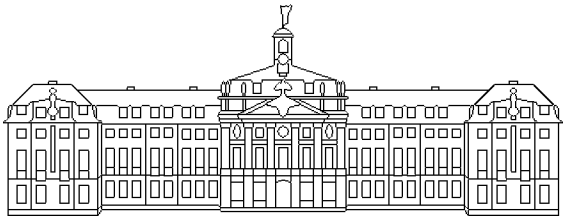
Reine Mathematik

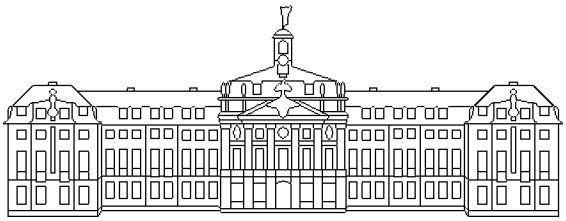


Raphael Richter

Kettenbrüche, L-Funktionen, Klassenzahlen und Geschlechtertheorie in quadratischen und biquadratischen Funktionenkörpern über $\mathbb{F}_p$

– Mai 2000 –

Reine Mathematik



Kettenbrüche, L-Funktionen, Klassenzahlen und Geschlechtertheorie in quadratischen und biquadratischen Funktionenkörpern über $\mathbb{F}_p$

Inaugural-Dissertation

zur Erlangung des Doktorgrades

der Naturwissenschaften im Fachbereich Mathematik und Informatik

der Mathematisch-Naturwissenschaftlichen Fakultät

der Westfälischen Wilhelms-Universität Münster

vorgelegt von

Raphael Richter

aus Menden

– Mai 2000 –

Dekan:	Prof. Dr. W. Lange
Erster Gutachter:	Prof. Dr. H. Lang
Zweiter Gutachter:	Prof. Dr. M. Peters
Tag der mündlichen Prüfungen:	
Tag der Promotion:	

Inhaltsverzeichnis

Einleitung

In seiner Dissertation [A] aus dem Jahre 1921 befaßte sich E. ARTIN mit quadratischen Erweiterungen des rationalen Funktionenkörpers $k := \mathbb{F}_p(X)$, wobei $p \neq 2$ eine Primzahl und $\mathbb{F}_p$ der Körper der Charakteristik p mit p Elementen ist. Er zeigte auf, daß sie ähnliche Strukturen wie quadratische Zahlkörper aufweisen.
In dem Buch *Zetafunktionen und quadratische Körper* ([Zag2]) veröffentlichte D. B. ZAGIER einen neuen Beweis für ein ursprünglich von F. HIRZEBRUCH (s. [Hir], S.241) stammendes Resultat. ZAGIER zeigte die Aussage von HIRZEBRUCH in der Form

Sei

$$\sqrt{p} = m_0 - \cfrac{1}{m_1 - \cfrac{1}{m_2 - \cfrac{1}{\ddots - \cfrac{1}{m_\rho - \cfrac{1}{m_1 - \cfrac{1}{\ddots}}}}}}$$

die negative Kettenbruchentwicklung der Quadratwurzel einer Primzahl $p \equiv 3\ (4)$ *mit* $p \neq 3$ *mit der minimalen Periode* ρ. *Für die Klassenzahl* $h(p)$ *im weiteren Sinne von* $\mathbb{Q}(\sqrt{p})$ *gelte* $h(p) = 1$. *Dann gilt für die Klassenzahl* $h(-p)$ *von* $\mathbb{Q}(\sqrt{-p})$

$$h(-p) = \frac{1}{3}\sum_{r=1}^{\rho} m_r - \rho.$$

(s.[Zag2], S.136)

Hierbei benutzte ZAGIER die Korrespondenz zwischen Idealklassen quadratischer Zahlkörper und Äquivalenzklassen binärer quadratischer Formen. Er erhielt die obige Formel durch die Betrachtung der engen Idealklasseneinteilung und zeigte auf, daß sie in Zusammenhang mit der negativen Kettenbruchentwicklung steht.
Im Jahre 1992 wurden die Methoden von ZAGIER von C. D. GONZÁLES in seinem Artikel *Class Numbers of Quadratic Function Fields and Continued Fractions* ([Gz]) erfolgreich auf reell-quadratische Funktionenkörper übertragen und führten zu einem *Hirzebruch-Analogon* für den Funktionenkörperfall. Hierbei benutzte er den von ARTIN entwickelten Kettenbruchalgorithmus für reell-quadratische Funktionenkörper und die Äquivalenz von Idealklassen im weiteren Sinn. Mit der Äquivalenz im engeren Sinn und seiner Übertragung auf Funktionenkörper beschäftigte sich R. FARWICK in seiner Diplomarbeit *Kettenbrüche und enge Klassen in reell quadratischen Funktionenkörpern über* $\mathbb{F}_p$ ([Far]), in welcher er die Aussagen von GONZÁLES auf die enge Klasseneinteilung übertrug.
Motiviert wurde er hierzu von der Arbeit *Real quadratic Function Fields* von D. R. HAYES ([H1]). HAYES stellte eine Möglichkeit vor, den Begriff der engen Äquivalenz in quadratischen Zahlkörpern auf quadratische Funktionenkörper zu übertragen und führte eine allgemeinere Kettenbruchentwicklung für Elemente eines reell-quadratischen Funktionenkörpers ein. Es gelang ihm mit der Untersuchung von SHINTANI-Sektoren ein zweites *Hirzebruch-Analogon* aus der Berechnung der Zeta-Funktion $Z(s, A)$ einer engen Idealklasse A an der Stelle $s = 0$ zu folgern.

Er bewies dieses letztendlich, indem er einige – für algebraische Zahlkörper bekannte – klassenkörpertheoretische Aussagen auf Funktionenkörper übertrug. Im Vordergrund stand hierbei das Zerlegungsverhalten ARTINscher L-Funktionen, welches für den Zahlkörperfall z.B. in [Nk], S.558ff. untersucht wurde.
Ziel der vorliegenden Arbeit ist es, ohne Benutzung klassenkörpertheoretischer Ergebnisse sowohl die *Hirzebruch-Analoga* von HAYES als auch allgemeinere Formeln für die Produkte zweier Klassenzahlen reell- bzw. imaginär-quadratischer Funktionenkörper herzuleiten.
Zu diesem Zweck übertragen wir die auf C. F. GAUSS zurückgehende von ZAGIER benutzte Geschlechtertheorie der engen Klasseneinteilung auf Funktionenkörper und bestimmen sämtliche Geschlechtscharaktere zur engen Klassengruppe.
Über die Betrachtung biquadratischer imaginärer bizyklischer und biquadratischer totalreeller Erweiterungen von k erhalten wir dann Formeln für das Produkt der Klassenzahlen zweier reell- bzw. imaginär-quadratischer Funktionenkörper. Wie im Zahlkörperfall können wir zeigen, daß diese auch im Funktionenkörperfall im wesentlichen den Werten von L-Funktionen zu Geschlechtscharakteren der engen Klassengruppe eines reell-quadratischen Funktionenkörpers an den Stellen 0 und 1 entsprechen.
Durch die vorangegangene explizite Angabe der Geschlechtscharaktere lassen sich diese Werte als Erweiterung der Ergebnisse von GONZÁLES, HAYES und FARWICK nun auch für mehrgeschlechtige und mehrklassige Funktionenkörper berechnen.
Um zu diesen Ergebnissen zu gelangen, werden wir wie folgt vorgehen.

Teil I der vorliegenden Arbeit stellt die Grundlagen aus der algebraischen Zahlentheorie bereit. Insbesondere werden hier die von ARTIN geprägten Begriffe reell- und imaginärquadratischer Funktionenkörper als Erweiterungen von k eingeführt und ihre wichtigsten Eigenschaften zusammengefaßt.

Der zweite Teil befaßt sich mit der allgemeinen Kettenbruchentwicklung in einer Komplettierung von k, welche auf HAYES zurückgeht. Ein Schwerpunkt liegt hier auf der Untersuchung der *engen Kettenbruchentwicklung* reduzierter Elemente eines reell-quadratischen Funktionenkörpers und ihrer Perioden. Mit ihrer Hilfe ist es z.B. möglich, die in Teil I definierte *positive Grundeinheit* eines reell-quadratischen Funktionenkörpers explizit zu berechnen.

In Teil III werden die *enge Äquivalenz* von Idealen und die enge Idealklassengruppe $C^+(K)$ definiert und Kriterien dafür hergeleitet, wann in reell- und imaginär-quadratischen Erweiterungen der enge mit dem weiten Äquivalenzbegriff zusammenfällt. Hier stellt man für imaginär-quadratische Funktionenkörper erhebliche Unterschiede zum Zahlkörperfall fest.
Es folgt die Konstruktion eines Isomorphismus zwischen den engen Idealklassen eines reell-quadratischen Funktionenkörpers $K = k(\sqrt{D})$ und den engen Äquivalenzklassen von Funktionen der Diskriminante D.
Nach der Einführung des auf ARTIN zurückgehenden quadratischen Restsymbols in $\mathbb{F}_p[X]$, welches wir für unsere Zwecke verallgemeinern, werden die Zeta- und L-Funktionen zu quadratischen Funktionenkörpern definiert und abschließend die ARTINschen Klassenzahlformeln zitiert.

Der zentrale Teil IV, welcher sich mit der Geschlechtertheorie der engen Klassengruppe beschäftigt, beginnt mit der Bestimmung der Anzahl ambiger Ideale und ambiger enger Klassen in reell- und imaginär-quadratischen Funktionenkörpern und somit der Anzahl der Geschlechter der engen Klassengruppe. Die bestehenden Analogien zum Zahlkörperfall legten die Vermutung nahe, die Geschlechtscharaktere im wesentlichen durch das quadratische

Restsymbol ausdrücken zu können, wie dies z.B. von C. L. SIEGEL in [Sie2] für quadratische Zahlkörper geschah. Das wird durch die explizite Angabe aller Geschlechtscharaktere der engen Klassengruppe in Kapitel 12 bestätigt.
Zieht man die Ergebnisse der Arbeit *Ambiguos Classes and 2-rank of Class Group of Quadratic Function Field* von X. ZHANG ([Zh]) heran, so gelingt es zudem, unter den Geschlechtscharakteren der engen Klassengruppe diejenigen auszuzeichnen, welche schon Charaktere der weiten Klassengruppe sind.

Der abschließende Teil V beschäftigt sich mit der Situation eines biquadratischen Funktionenkörpers $L = k(\sqrt{D_1}, \sqrt{D_1})$ über einem reell-quadratischen Körper $K = k(\sqrt{D_1 D_2})$ mit zwei teilerfremden normierten Polynomen $D_1, D_2 \in \mathbb{F}_p[X]$. Im Zahlkörperfall wird die Bestimmung der sogenannten *Relativklassenzahl* von L/K auf die Berechnung der Werte von L-Funktionen zu Geschlechtscharakteren der engen oder weiten Klassengruppe an der Stelle 1 zurückgeführt (vgl. dazu die Ausführungen in [Ha2]).
Im Funktionenkörperfall besteht die Berechnung des Produkts $h(D_1)h(D_2)$ der beiden quadratischen Teilkörper von L im wesentlichen aus der Ermittlung der Werte einer L-Funktion zu einem Geschlechtscharakter der engen Klassengruppe an den Stellen 0,1 und $\frac{\pi i}{\log p}$. Den Zahlkörper-Ansatz über Klassenfunktionen zu Vorzeichencharakteren aus [Mey] und [Lg] verfolgend, berechnen wir die Werte der L-Funktionen an diesen Stellen, indem wir die von HAYES verwendeten SHINTANI-Sektoren benutzen. Hier wird von uns jedoch eine veränderte Definition des *Eckenpaares eines Gitters* benutzt, um den Zusammenhang zur engen (bzw. negativen) Kettenbruchentwicklung herzustellen. Nach der Herleitung einer Formel für die *Kronecker-Grenzwerte* von Zeta-Funktionen zu einer engen Idealklasse, ist es abschließend möglich, das Produkt $h(D_1)h(D_2)$ zweier beliebiger quadratischer Körper $k(\sqrt{D_i})$ mit teilerfremden $D_1, D_2 \in \mathbb{F}_p[X]$ zu berechnen, für welche $K = k(\sqrt{D_1 D_2})$ ein reell-quadratischer Körper ist.
Zur Bestätigung der erhaltenen Formeln werden letztlich Beispiele sowohl für den einklassigen als auch für den mehrklassigen und mehrgeschlechtigen Fall angeführt.
Die dort gemachten Aussagen wurden zum einen vom Verfasser der vorliegenden Arbeit mit dem Computer-Algebra-System SIMATH 4.4 berechnet, welches an der Universität Saarbrücken entwickelt wurde. Zum anderen wurden sie aus Tabellen in [A] und [WZ] entnommen.

An dieser Stelle möchte ich mich ganz herzlich bei Herrn Prof. Dr. Heinrich Lang für die Auswahl des Themas, sein immer wieder motivierendes Interesse und die stete Gesprächsbereitschaft während der Entstehung dieser Arbeit bedanken.

Darüber hinaus geht mein Dank an das *Graduiertenkolleg Algebraische Geometrie und Zahlentheorie*, welches mich mit einem dreijährigen Stipendium finanziell unterstützte.

Schließlich danke ich noch allen Nicht-Mathematikern, die mich gerade in den letzten Monaten der Erstellung dieser Arbeit zwar oft mit Verständnislosigkeit aber immer wieder mit aufmunterndem Beistand unterstützt haben. Bei ihnen möchte ich mich mit den Worten des Zahlentheoretikers G. H. HARDY entschuldigen:

"Ich habe nie etwas gemacht, was 'nützlich' gewesen wäre. Für das Wohlbefinden der Welt hatte keine meiner Entdeckungen – ob im Guten oder Schlechten – je die geringste Bedeutung. Nach allen praktischen Maßstäben ist der Wert meines mathematischen Lebens gleich Null, und außerhalb der Mathematik ist es ohnehin trivial.

Ich habe nur eine Chance, dem Verdikt vollkommener Trivialität zu entgehen, und zwar dadurch, daß man mir zugesteht, etwas geschaffen zu haben, was sich zu schaffen lohnte. Daß ich etwas geschaffen habe, ist nicht zu bestreiten; die Frage ist nur, ob es etwas wert ist."

(GODFREY HAROLD HARDY, A Mathematician's Apology, Cambridge 1967)

Teil I
Grundlagen

In diesem Teil werden die theoretischen Grundlagen für die weiteren Teile der vorliegenden Arbeit zur Verfügung gestellt und bekannte Aussagen über reell- und imaginär-quadratische Funktionenkörper wiederholt.
Diese Aussagen basieren auf [A],[Sti],[Deu],[WZ],[Kor],[Ws] und [Schm2]. Sie stellen bekannte und zentrale Eigenschaften aus der Theorie algebraischer Funktionenkörper dar und werden daher an dieser Stelle weitgehend informell beschrieben.

1 Algebraische Funktionenkörper

1.1 Definition und Eigenschaften

1.1.1 Definition

Es sei p eine ungerade Primzahl, $\mathbb{F}_p$ der Körper der Charakteristik p mit p Elementen. Ein *algebraischer Funktionenkörper* K (in einer Variablen) über dem Konstantenkörper $\mathbb{F}_p$, $K/\mathbb{F}_p$, ist eine endlich-erzeugte Erweiterung von $\mathbb{F}_p$ vom Transzendenzgrad 1 über $\mathbb{F}_p$ und wird auch *algebraischer Kongruenzfunktionenkörper über $\mathbb{F}_p$* genannt.

Wie man weiß, existiert immer ein über $\mathbb{F}_p$ transzendentes Element $X \in K$, derart, daß K eine endlich-algebraische, separable Erweiterung von $k := \mathbb{F}_p(X)$, dem rationalen Funktionenkörper in der Variablen X über $\mathbb{F}_p$, ist und damit $[K : k] =: n < \infty$ gilt. Es sei von nun an X so gewählt.

Der Ganzheitsring von K, d.h. der ganz-algebraische Abschluß von $\mathbb{F}_p[X]$ in K, werde mit $\mathcal{O}_K$ bezeichnet. Bei diesem handelt es sich um einen Dedekind-Ring mit der Einheitengruppe $\mathcal{O}_K^*$.

1.2 Ideale

Die Menge $I(K)$ der *gebrochenen $\mathcal{O}_K$-Ideale* von K, d.h. der $\mathcal{O}_K-$Untermoduln $\mathfrak{a}$ von K, zu denen ein $d \in \mathcal{O}_K \backslash \{0\}$, existiert mit $d\mathfrak{a} \subseteq \mathcal{O}_K$, bildet bekanntlich eine multiplikative Gruppe mit der Menge $H(K)$ der *$\mathcal{O}_K$-Hauptideale* $\lambda\mathcal{O}_K = (\lambda)$ als Untergruppe ($\lambda \in K^*$).

Ein $\mathcal{O}_K$-Ideal $\mathfrak{a}$ heißt *ganz*, falls $\mathfrak{a} \subseteq \mathcal{O}_K$ gilt.

Zwei $\mathcal{O}_K$-Ideale $\mathfrak{a}, \mathfrak{b} \in I(K)$ heißen *äquivalent* ($\mathfrak{a} \sim \mathfrak{b}$), falls $\mathfrak{a} = (\lambda)\mathfrak{b}$ gilt mit einem $\lambda \in K^*$. Die aus dieser Relation hervorgehenden Äquivalenzklassen heißen *weite Äquivalenzklassen* (in Abgrenzung zu den in Kapitel 8.1 definierten *engen* Äquivalenzklassen).
Mit $C(K) = I(K)/H(K)$ wird dann die *weite Idealklasssengruppe* von K bzgl. $\mathcal{O}_K$ bezeichnet. Die Anzahl $h(K)$ der Elemente von $C(K)$ nennt man die *weite (Ideal-)Klassenzahl* von K. Für ein Ideal $\mathfrak{a} \in I(K)$ bezeichnen wir die zugehörige weite Idealklasse mit $[\mathfrak{a}]$.

2 Stellen

Zu den Stellen der algebraischen Funktionenkörper $K/\mathbb{F}_p$ und des rationalen Funktionenkörpers k fassen wir hier die Aussagen aus [Sti], [Nk] und [Schm2] zusammen.

Ist $\mathfrak{P}$ eine Stelle von $K/\mathbb{F}_p$ mit dem zugehörigen *Bewertungsring* $R_\mathfrak{P}$, dem *maximalen Ideal* $\mathfrak{m}_\mathfrak{P}$ und dem *Restklassenkörper* $\kappa_\mathfrak{P} := R_\mathfrak{P}/\mathfrak{m}_\mathfrak{P}$, dann ist der Grad von $\mathfrak{P}$ definiert als

$$f_\mathfrak{P} := \operatorname{grad}\mathfrak{P} := [\kappa_\mathfrak{P} : \mathbb{F}_p] < \infty.$$

Die *Norm* von $\mathfrak{P}$ ist definiert durch

$$N(\mathfrak{P}) := p^{f_\mathfrak{P}}.$$

Wir bezeichnen mit $v_\mathfrak{P}$ die zu $\mathfrak{P}$ gehörige (additive) normierte Bewertung von $K/\mathbb{F}_p$ und mit $\mathbb{P}_K$ die Menge der Stellen von K.

2.1 Unendliche Stellen

Es existiert eine unendliche Stelle von k über $\mathbb{F}_p$, welche wir mit ∞ bezeichnen. Für diese ist $f_\infty = 1$. Zu dieser gehört die (additive) Bewertung v_∞, welche gegeben ist durch $v_\infty(P(X)/Q(X)) = \operatorname{grad}Q(X) - \operatorname{grad}P(X)$ für Polynome $P, Q \in \mathbb{F}_p[X]$, $Q \neq 0$. Die zugehörige multiplikative Bewertung $|\cdot|$ ist gegeben durch

$$|Z| = \begin{cases} p^{\operatorname{grad}P - \operatorname{grad}Q}, & \text{falls } Z = \frac{P}{Q} \text{ mit } P, Q \in \mathbb{F}_p[X], Q \neq 0 \\ 0, & \text{falls } Z = 0. \end{cases}$$

Für den Bewertungsring

$$R_\infty := \{Z \in k \mid |Z| \leq 1\}$$

erhält man $R_\infty = \mathbb{F}_p[\frac{1}{X}]_{(\frac{1}{X})}$, die Lokalisierung nach dem Primideal $\mathfrak{m}_\infty := (X^{-1})$.

Ist nun $[K : k] = n \geq 1$, so ist die Zerlegung von ∞ gegeben durch

$$\infty = \infty_1^{e_1} \cdot \ldots \cdot \infty_r^{e_r},$$

wobei $\infty_1, \ldots, \infty_r$ die Fortsetzungen der unendlichen Stelle ∞ von k auf K sind, für welche die fundamentale Gleichung

$$n = \sum_{i=1}^{r} e_i f_{\infty_i}$$

mit $f_{\infty_i} = \operatorname{grad}\infty_i$ richtig ist.

2.2 Endliche Stellen

Die endlichen Stellen des rationalen Funktionenkörpers k über $\mathbb{F}_p$ sind eindeutig den normierten Primpolynomen $P \in \mathbb{F}_p[X]$, d.h. den normierten irreduziblen Polynomen über $\mathbb{F}_p$, zugeordnet. Jedem normierten Primpolynom $P \in \mathbb{F}_p[X]$ entspricht eine Stelle $\mathfrak{P}_P$ vom Grad $\operatorname{grad}\mathfrak{P}_P = \operatorname{grad}P$. Die zugehörige normierte Bewertung $v_{\mathfrak{P}_P}$ liefert für $Z = P^n Q_1/Q_2$ ($n \in \mathbb{Z}$, $Q_1, Q_2 \in \mathbb{F}_p[X]$, $Q_2 \neq 0$, $(P, Q_1 Q_2) = 1$) dann den Wert $v_{\mathfrak{P}_P}(Z) = n$. P ist dann Primelement für $\mathfrak{P}_P$, also gilt $v_{\mathfrak{P}_P}(P) = 1$.

Insgesamt hat man

$$\mathbb{P}_k = \{\mathfrak{P}_P \mid P \in \mathbb{F}_p[X] \text{ normiertes Primpolynom}\} \cup \{\infty\},$$

und die endlichen Stellen von $K/\mathbb{F}_p$ sind dann $\mathbb{P}_K \backslash \{\infty_1, \ldots, \infty_r\}$.

3 Die Komplettierung k_∞

3.1 Definition und Eigenschaften

3.1.1 Definition

Es bezeichne $(k_\infty, |\cdot|_\infty)$ die Komplettierung von $(k, |\cdot|)$ bezüglich der unendlichen Stelle ∞ des rationalen Funktionenkörpers k. Mit anderen Worten

(1) $k \subseteq k_\infty$, und $|\cdot|$ ist die Einschränkung von $|\cdot|_\infty$ auf k.

(2) k_∞ ist vollständig bezüglich $|\cdot|_\infty$, d.h. jede $|\cdot|_\infty$-Cauchy-Folge aus k_∞ konvergiert.

(3) k liegt dicht in k_∞.

Dann kann man k_∞ nach Sätzen aus der Bewertungstheorie (s. [Nk], S.132, [Sti], S. 143) schreiben als

$$k_\infty = \{\sum_{n=r}^{\infty} a_n \left(\frac{1}{X}\right)^n = \sum_{n=-\infty}^{r} a_n X^n \mid r \in \mathbb{Z},\ a_n \in \mathbb{F}_p,\ a_r \in \mathbb{F}_p^*\},$$

denn $\mathbb{F}_p$ bildet ein vollständiges Repräsentantensystem von $\kappa_\infty := R_\infty/\mathfrak{m}_\infty$.

Ist $Z := \sum_{n=-\infty}^{r} a_n X^n \in k_\infty^*$ mit $a_r \neq 0$, so ist

$$\begin{aligned} |Z|_\infty &= |\lim_{k\to\infty} \sum_{n=-k}^{r} a_n X^n| \\ &= \lim_{k\to\infty} |\sum_{n=-k}^{r} a_n X^n| \\ &= p^r, \end{aligned}$$

denn $|\cdot|_\infty$ setzt $|\cdot|$ stetig fort.

Da wir keine weiteren Absolutbeträge auf k bzw. k_∞ benutzen, werden wir auch die Fortsetzung $|\cdot|_\infty$ wieder mit $|\cdot|$ bezeichnen.

3.1.2 Definition

Für $Z = \sum_{n=-\infty}^{r} a_n X^n \in k_\infty^*$ mit $a_r \neq 0$ führen wir die folgenden Bezeichnungen ein:

(i) $\operatorname{grad} Z := r \in \mathbb{Z}$ sei definiert als der *Grad* von Z.

(ii) $\operatorname{sgn}(Z) := a_r \in \mathbb{F}_p^*$ nennen wir das *Signum von* Z und

(iii)
$$[Z] := \begin{cases} \sum_{n=0}^{r} a_n X^n, & \text{falls } r \geq 0, \\ 0, & \text{falls } r < 0 \end{cases} \in \mathbb{F}_p[X]$$
den *Polynomteil* oder auch *Hauptteil* von Z.

(iv) Ist $\operatorname{sgn} Z = 1$, so heißt Z *normiert*.

(v) Ist
$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{\pm 1\}$$
das Legendre-Symbol, so setzen wir dieses nach k_∞^* fort durch die Abbildung
$$\chi : k_\infty^* \to \{\pm 1\}$$
$$\chi(Z) := \left(\frac{\operatorname{sgn}(Z)}{p}\right)$$
für $Z \in k_\infty^*$.

(vi) Ein Element $Z \in k_\infty^*$ heiße *positiv*, falls $\chi(Z) = 1$ gilt.

4 Quadratische und biquadratische Erweiterungen von k

Der Großteil der vorliegenden Arbeit beschäftigt sich mit quadratischen und biquadratischen Erweiterungen des Körpers k, deren Eigenschaften basierend auf [A] und [Kor] hier zusammengefaßt werden sollen.

4.1 Definition und Eigenschaften

4.1.1 Definition

Ein algebraischer Funktionenkörper $K/\mathbb{F}_p$ heißt *quadratischer (Kongruenz-)Funktionenkörper über* $\mathbb{F}_p$, falls K eine quadratische Erweiterung von k ist mit
$$[K : k] = 2.$$

Wir betrachten also zu einer gegebenen Funktion $D \in \mathbb{F}_p[X]$ die quadratische Gleichung
$$Y^2 = D.$$

Im Falle, daß D ungeraden Grad besitzt oder $\operatorname{sgn} D$ ein quadratischer Nichtrest mod p ist, hat obige Gleichung offensichtlich keine Lösung in k_∞^*.
Ist jedoch $\operatorname{grad} D$ gerade und D positiv, so schreibt man
$$D = a^2 X^{2n} + a_{2n-1} X^{2n-1} + \ldots + a_0 = a^2 X^{2n}(1 + \Phi)$$
mit
$$\Phi = \frac{a_{2n-1}}{a^2} X^{-1} + \frac{a_{2n-2}}{a^2} X^{-2} + \ldots,$$

also $|\Phi| \leq p^{-1}$. Nach [A], S.159 kann man dann die Lösung Y der quadratischen Gleichung in k_∞^* darstellen durch

$$Y = aX^n \sum_{\nu=0}^{\infty} \binom{\frac{1}{2}}{\nu} \Phi^\nu,$$

wobei der Binomialkoeffizient mod p gelesen werden muß.
Wir schreiben von nun an $Y =: \sqrt{D}$, wobei das Vorzeichen ± 1 noch frei wählbar sei.
Ausgehend von diesen Beobachtungen definieren wir nun reell- und imaginär-quadratische Erweiterungen von k.

4.1.2 Definition

(i) Eine Erweiterung K/k von k heißt *reell-quadratisch*, wenn gilt:
$K = k(\sqrt{D})$ mit $D \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$, $\operatorname{grad} D$ gerade und D positiv.

(ii) K/k heißt *imaginär-quadratisch*, wenn gilt:

a) $K = k(\sqrt{D})$ mit $D \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$, $\operatorname{grad} D$ ungerade oder

b) $K = k(\sqrt{D})$ mit $D \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$, $\operatorname{grad} D$ gerade und D nicht positiv.

(iii) Ein Funktionenkörper L/k heißt *imaginärer biquadratischer bizyklischer Funktionenkörper*, falls L die Form $L = k(\sqrt{D_1}, \sqrt{D_2})$ hat, wobei $D_1 D_2 \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$ ist und ferner $K = k(\sqrt{D_1 D_2})$ ein reell-quadratischer Funktionenkörper und $k(\sqrt{D_1})$ und $k(\sqrt{D_2})$ zwei imaginär-quadratische Funktionenkörper mit $k(\sqrt{D_1}) \cap k(\sqrt{D_2}) = k$ sind.

(iv) Ein Funktionenkörper L/k heißt *total-reeller biquadratischer Funktionenkörper*, falls L die Form $L = k(\sqrt{D_1}, \sqrt{D_2})$ hat, wobei $D_1 D_2 \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$ ist und $k(\sqrt{D_1})$ und $k(\sqrt{D_2})$ zwei reell-quadratische Funktionenkörper mit $k(\sqrt{D_1}) \cap k(\sqrt{D_2}) = k$ sind.

4.1.3 Bemerkung

Es sei $g \in \mathbb{F}_p^*$ eine beliebige, aber von nun an fest gewählte Primitivwurzel mod p. Dann ist $\chi(g) = -1$, und es sei D in den obigen Fällen immer so gewählt, daß $\operatorname{sgn} D \in \{1, g\}$ gilt und D quadratfrei ist.
Im Fall (i) ($\sqrt{D} \in k_\infty$) sei ferner o.B.d.A. $\operatorname{sgn} \sqrt{D} = 1$.

4.1.4 Proposition

Für die Stelle ∞ von k gilt in den oben angeführten Fällen:

(i) Ist K/k eine reell-quadratische Erweiterung, so ist ∞ zerlegt in K, d.h. $\infty = \infty_1 \infty_2$ mit zwei verschiedenen unendlichen Stellen ∞_1 und ∞_2 von K.

(ii) a) Ist $K = k(\sqrt{D})/k$ mit $\operatorname{grad} D$ ungerade eine imaginär-quadratische Erweiterung, so ist ∞ verzweigt in K, d.h. $\infty = \infty_1^2$ in K mit einer unendlichen Stelle ∞_1 von K.

b) Ist $K = k(\sqrt{D})/k$, mit $\operatorname{grad} D$ gerade und nicht positiv, eine imaginär-quadratische Erweiterung, so ist ∞ träge in K, d.h. $\infty = \infty_1$ in K mit einer unendlichen Stelle ∞_1 von K.

(iii) Ist L/k ein imaginärer biquadratischer bizyklischer Funktionenkörper, so ist

$\infty = \infty_1^2\infty_2^2$ in L mit zwei verschiedenen unendlichen Stellen ∞_1 und ∞_2 von L, falls L erzeugt wird von zwei imaginär-quadratischen Körpern der Form (ii) a) und

$\infty = \infty_1\infty_2$ in L mit zwei verschiedenen unendlichen Stellen ∞_1 und ∞_2 von L, falls L erzeugt wird von zwei imaginär-quadratischen Körpern der Form (ii) b).

(iv) Ist L/k ein total-reeller biquadratischer Funktionenkörper, so ist $\infty = \infty_1\infty_2\infty_3\infty_4$ voll zerlegt in L, wobei $\infty_1, \ldots, \infty_4$ vier verschiedene unendliche Stellen von L sind.

Diese Aussagen findet man in [Kor], [H-R], [WZ],[Sti] und [A].

Ist $K = k(\sqrt{D})$ ein quadratischer Funktionenkörper, so gilt $\mathcal{O}_K = \mathbb{F}_p[X][\sqrt{D}]$ für den ganzen Abschluß $\mathcal{O}_K$ von $\mathbb{F}_p[X]$ in K.

Jedes $\mathcal{O}_K$-Ideal ist ein freier $\mathbb{F}_p[X]$-Untermodul vom Rang 2, d.h. es besitzt eine Basis (ω_1, ω_2) mit über $\mathbb{F}_p[X]$ linear unabhängigen $\omega_1, \omega_2 \in K$.

Bezüglich der Basis von ganzen Idealen eines quadratischen Funktionenkörpers findet man bei ARTIN ([A], S.164ff.) das

4.1.5 Lemma

Eine Teilmenge $(0) \neq \mathfrak{a} \subseteq \mathcal{O}_K$ ist genau dann ein ganzes Ideal von K, wenn es $\omega_1, \omega_2 \in K$ über $\mathbb{F}_p[X]$ der Form

$$\omega_1 = 2CS \quad \omega_2 = S(B + \sqrt{D}), \quad D = B^2 - 4AC$$

mit $A, B, C, S \in \mathbb{F}_p[X]$ gibt und $\mathfrak{a} =< \omega_1, \omega_2 >$ gilt.
Ein ganzes Ideal nennt man *primitiv*, falls $S = 1$ gewählt werden kann.
In obiger Basisdarstellung kann ferner $|B| < |C|$ angenommen werden. Eine Basis dieser Form nennt man *adaptierte* Basis. B, C und S sind dann bis auf einen Faktor aus $\mathbb{F}_p^*$ eindeutig bestimmt. Verlangt man weiterhin $\operatorname{sgn}(C) = 1$, so ist die adaptierte Darstellung eindeutig.

Die Körpererweiterung K/k ist galoissch mit Galoisgruppe $\{1, \sigma\}$, wobei σ der nicht-triviale k-Automorphismus von K ist, welcher $\sqrt{D}$ in $-\sqrt{D}$ überführt.
Zu einem Element $Z = A + B\sqrt{D} \in K$ mit $A, B \in k$ definieren wir das *konjugierte Element* $\overline{Z} := \sigma(Z) = A - B\sqrt{D}$ und die *Norm von* Z durch

$$N(Z) := Z\overline{Z} = A^2 - B^2D.$$

Ist speziell $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper, dann ist nach Proposition 4.1.4 die Stelle ∞ in K zerlegt ($\infty = \infty_1\infty_2$), und die Komplettierungen K_{∞_1} und K_{∞_2} bzgl. der unendlichen Stellen ∞_1 und ∞_2 sind isomorph zu k_∞. Wir können daher zwei Einbettungen e_1 und e_2 von K nach k_∞ definieren, wobei $\operatorname{sgn}(e_1(\sqrt{D})) = 1$ gelten soll. K läßt sich dann als dichter Unterkörper einbetten in die Produkt-k-Algebra $k_\infty \times k_\infty$ durch die Abbildung

$$e := e_1 \times e_2 : K \to k_\infty \times k_\infty$$
$$\alpha \mapsto \left(\alpha \atop \overline{\alpha}\right).$$

Wir setzen $P := k_\infty^* \times k_\infty$ und definieren die *Norm* eines Elements $x = \binom{x_1}{x_2} \in P$ durch $N(x) = x_1 \cdot x_2$ und die *Steigung* $S(x)$ durch $S(x) := \frac{x_2}{x_1}$.
Ist $Z \in K^*$, so definieren wir die *Steigung von* Z durch

$$S(Z) = \frac{\overline{Z}^2}{N(Z)} = \frac{\overline{Z}}{Z}.$$

Die spätere Untersuchung der engen Klasseneinteilung von Idealen führt uns zu Elementen $u \in K$ mit der Eigenschaft $\chi(N(u)) = 1$, mit denen wir uns zunächst beschäftigen wollen. Hier treffen wir auf weitere Unterschiede beim Vergleich des Zahlkörperfalls mit dem Funktionenkörperfall.

Ist es im Zahlkörperfall so, daß in imaginär-quadratischen Erweiterungen $\mathbb{Q}(\sqrt{d})$ von $\mathbb{Q}$ mit $0 > d \in \mathbb{Z}$ die Norm eines jeden Elements positiv ist (vgl. [Zag2], S. 91), so ergeben sich im Fall eines imaginär-quadratischen Funktionenkörpers einige Unterschiede. Die Aussagen über Elemente positiver Norm in quadratischen Funktionenkörpern faßt das folgende Lemma zusammen.

4.1.6 Lemma

(i) Ist K ein reell-quadratischer Funktionenkörper, so existiert ein Element $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$.

(ii) Ist K ein imaginär-quadratischer Funktionenkörper, so existiert kein Element $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$, falls

(1) $K = k(\sqrt{D})$, $\operatorname{grad} D$ ungerade, D normiert, quadratfrei und $\chi(-1) = 1$ oder

(2) $K = k(\sqrt{gD})$, $\operatorname{grad} D$ ungerade, D normiert, quadratfrei und $\chi(-1) = -1$ gilt.

In allen anderen imaginär-quadratischen Fällen findet man hingegen ein solches.

BEWEIS:

(i) Ist $p \neq 3$ und $\chi(-1) = 1$, so wählt man ein $h \in \mathbb{F}_p^{*^2}$ so, daß $\chi(h-1) = -1$ gilt.
Ausgehend von $p-1$, denn es ist $\chi(p-1) = \chi(-1) = 1$, sucht man den ersten Wert $p-k$ $(k < p)$, für den $\chi(p-k-1) = -1$ gilt.
Dieser liefert das gesuchte h.
Ist nun $\operatorname{grad} D = 2m$ und $h = b^2$, so setzt man $u := bX^m + \sqrt{D}$, und es gilt

$$N(u) = b^2 X^{2m} - D$$

mit $\chi(N(u)) = \chi(h-1) = -1$ wegen $|X^{2m}| = |D|$, $\operatorname{sgn} X^{2m} = \operatorname{sgn} D = 1$ und $h - 1 \neq 0$.
Ist hingegen $p = 3$ oder $p \neq 3$ und $\chi(-1) = -1$, so erhält man mit $u := \sqrt{D}$ sofort

$$\chi(N(u)) = \chi(-D) = \chi(-1) = -1$$

wegen $\chi(D) = 1$.

(ii) Befinden wir uns in Fall (1), so ist $N(u) = A^2 - B^2 D$ mit $u := A + B\sqrt{D}$ und

$$\chi(A^2 - B^2 D) = \begin{cases} \chi(A^2) = 1 & \text{falls } \operatorname{grad} A^2 > \operatorname{grad}(B^2 D) \text{ und} \\ \chi(-DB^2) = 1 & \text{falls } \operatorname{grad} A^2 < \operatorname{grad}(B^2 D), \end{cases}$$

da D ungeraden Grad besitzt und $\chi(-1) = 1$ gilt. Für alle $u \in \mathcal{O}_K$ gilt also $\chi(N(u)) = 1$. Dies erhält man auch in (2), indem man $\chi(-1) = -1$ ausnutzt und D durch gD ersetzt.
Es bleibt also zu zeigen, daß in allen übrigen Fällen immer ein $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$ zu finden ist.
Ist $K = k(\sqrt{gD})$ und $\chi(-1) = 1$, so ist $\sqrt{gD}$ wegen

$$\chi(N(\sqrt{gD})) = \chi(-gD) = -1$$

ein solches Element.
Ebenso $\sqrt{D}$ in $K = k(\sqrt{D})$, falls $\operatorname{grad} D$ ungerade und $\chi(-1) = -1$.
Ist hingegen $K = k(\sqrt{gD})$ mit $\operatorname{grad} D$ gerade und $\chi(-1) = -1$, so wählt man ein $h \in \mathbb{F}_p^*$ mit $\chi(h) = -1$ und $\chi(h-1) = 1$.
Ausgehend von $p-1$ (beachte: $\chi(p-1) = \chi(-1) = -1$) sucht man den ersten Wert $p-k$ $(k < p)$, für den $p - k - 1 \in \mathbb{F}_p^{*^2}$ gilt. Dieser liefert das gesuchte h.
Es gilt dann $\chi(hg - g) = -1$ und $hg = d^2 \in \mathbb{F}_p^{*^2}$. Ist $\operatorname{grad} D = 2m$, so setzt man $u := dX^m + \sqrt{gD}$, und es folgt

$$\chi(N(u)) = \chi(d^2 X^{2m} - gD) = \chi(d^2 - g) = \chi(hg - g) = -1,$$

da $|X^{2m}| = |D|$ und $\operatorname{sgn} D = 1$ gilt.
Somit existiert mit Ausnahme der Fälle (1) und (2) auch in jedem imaginär-quadratischen Körper ein Element $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$.

□

Weiterhin ist es für spätere Berechnungen wichtig, zu wissen, in welchen Körpern Elemente $\lambda \in \mathcal{O}_K$ existieren, deren Normen $N(\lambda) \in \mathbb{F}_p[X]$ ungeraden Grad besitzen.

4.1.7 Lemma

(i) Ist K ein reell-quadratischer Funktionenkörper, so existiert ein Element $\lambda \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$. Dieses kann sogar so gewählt werden, daß $\chi(N(\lambda)) = 1$ gilt.

(ii) Ist K ein imaginär-quadratischer Funktionenkörper, so unterscheidet man die folgenden Fälle:

(1) Ist $K = k(\sqrt{D})$ mit D normiert, quadratfrei und $\operatorname{grad} D$ ungerade, so existiert ein $\lambda \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$. Es gilt dann $\chi(N(\lambda)) = \chi(-1)$ für alle λ mit dieser Eigenschaft.

(2) Ist $K = k(\sqrt{gD})$ mit D normiert, quadratfrei und $\operatorname{grad} D$ ungerade, so existiert ein $\lambda \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$. Es gilt dann $\chi(N(\lambda)) = -\chi(-1)$ für alle λ mit dieser Eigenschaft.

(3) Ist $K = k(\sqrt{gD})$ mit D normiert, quadratfrei und $\operatorname{grad} D$ gerade, so existiert kein $\lambda \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$.

BEWEIS:

(i) Es sei $D = X^{2n} + \sum_{i=0}^{2n-1} a_i X^i$.
Ist $a_{2n-1} = 0$, so wähle $A := X^n + X^{n-1}$ und $B := 1$.
Dann ist $\mu := A + B\sqrt{D} \in \mathcal{O}_K$ mit

$$N(\mu) = A^2 - B^2 D = (X^n + X^{n-1})^2 - D = X^{2n} + 2X^{2n-1} + X^{2n-2} - X^{2n} - \sum_{i=0}^{2n-2} a_i X^i.$$

Es gilt also $\operatorname{grad} N(\mu) = 2n - 1$ und $\operatorname{sgn}(N(\mu)) = 2$. Man setzt nun

$$\lambda := \begin{cases} \mu, & \text{falls } \chi(2) = 1, \text{ und} \\ u\mu & \text{falls } \chi(2) = -1 \end{cases}$$

mit $u \in \mathcal{O}_K$ nach Lemma 4.1.6 so gewählt, daß $\chi(N(u)) = -1$ gilt. Dann ist $\chi(N(\lambda)) = 1$. Nach der Konstruktion im Beweis von Lemma 4.1.6 (i) besitzt $N(u)$ geraden Grad, d.h. mit $N(\mu)$ besitzt auch $N(u\mu)$ ungeraden Grad.
Ist jedoch $a_{2n-1} \neq 0$, so setzt man $A := X^n$ und $B := 1$.
Dann ist $\mu := A + B\sqrt{D} \in \mathcal{O}_K$ mit

$$N(\mu) = A^2 - B^2 D = X^{2n} - X^{2n} - a_{2n-1} X^{2n-1} - \sum_{i=0}^{2n-2} a_i X^i,$$

also $\chi(N(\mu)) = \chi(-a_{2n-1})$ und $\operatorname{grad} N(\mu) = 2n - 1$. Mit

$$\lambda := \begin{cases} \mu, & \text{falls } \chi(-a_{2n-1}) = 1 \text{ und} \\ u\mu, & \text{falls } \chi(-a_{2n-1}) = -1 \end{cases}$$

folgt wie oben die Behauptung.

(ii) (1) Ist $\operatorname{grad} D \equiv 1\ (2)$, so ist $\lambda := \sqrt{D}$ ein Element mit der Eigenschaft $\operatorname{grad} N(\lambda) = \operatorname{grad} -D = \operatorname{grad} D \equiv 1\ (2)$.
Ist $\lambda = A + B\sqrt{D} \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$, so ist

$$\chi(N(\lambda)) = \chi(A^2 - B^2 D) = \chi(-B^2 D) = \chi(-1),$$

da D normiert ist.

(2) In diesem Fall ist $\lambda := \sqrt{gD} \in \mathcal{O}_K$ ein Element mit der Eigenschaft $\operatorname{grad} N(\lambda) = \operatorname{grad}(-gD) = \operatorname{grad} D \equiv 1\ (2)$.
Ist $\lambda = A + B\sqrt{gD} \in \mathcal{O}_K$ mit $\operatorname{grad} N(\lambda) \equiv 1\ (2)$, so ist

$$\chi(N(\lambda)) = \chi(A^2 - gB^2 D) = \chi(-gB^2 D) = -\chi(-1),$$

da D normiert ist und $\chi(g) = -1$ gilt.

(3) Wäre $\lambda = A + B\sqrt{gD} \in \mathcal{O}_K$ ein Element mit der Eigenschaft $\operatorname{grad} N(\lambda) = \operatorname{grad}(A^2 - gB^2 D) \equiv 1\ (2)$, so müßten wegen $\operatorname{grad} D \equiv 0\ (2)$ die Grade von A^2 und $B^2 D$ gleich sein, und es müßte $\operatorname{sgn} A^2 = \operatorname{sgn} gB^2 D$ gelten. Letzteres ist aber unmöglich, denn aus $\chi(g) = -1$ folgt $\chi(A^2) = -\chi(gB^2 D)$.

□

4.2 Einheiten

Ein Element $\epsilon \in \mathcal{O}_K$ ist dann und nur dann eine Einheit des Rings $\mathcal{O}_K$, wenn $N(\epsilon) = c \in \mathbb{F}_p^*$ gilt.
Aus [A], S.196 und [Kor], S.3ff. bzw. dem DIRICHLETschen Einheitensatz (s. [Ws], S.207) zusammen mit Proposition 4.1.4 erhält man die folgenden Sätze, welche Aussagen über die Struktur der Einheitengruppen $\mathcal{O}_K^*$ quadratischer Erweiterungen K/k machen.

4.2.1 Satz

In imaginär-quadratischen Körpern (außer im Fall $D = g \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*^2}$) sind die trivialen Einheiten, d.h. die Elemente aus $\mathbb{F}_p^*$, die einzigen Einheiten. Ihre Anzahl ist $p - 1$.
Im Ring $\mathcal{O}_K$ der imaginär-quadratischen Erweiterung $K = k(\sqrt{g})$ haben alle Einheiten die Form $\epsilon = a + b\sqrt{g}$ mit $a, b \in \mathbb{F}_p$ und $(a, b) \neq (0, 0)$, ihre Anzahl ist also $p^2 - 1$.

4.2.2 Satz

Ist $K = k(\sqrt{D})$ eine reell-quadratische Erweiterung, so ist $\mathcal{O}_K^*$ das direkte Produkt von $\mathbb{F}_p^*$ mit einer unendlichen zyklischen Gruppe. Als Erzeuger dieser Gruppe kann man eine Einheit $\epsilon_0 \in \mathcal{O}_K^*$ so wählen, daß sie eine Einheit vom kleinsten Betrag größer als Eins ist und daß $N(\epsilon_0) \in \{1, g\}$ gilt.
Diese Einheit ist dann eindeutig bestimmt und werde die *Grundeinheit* oder *Fundamentaleinheit* von K genannt.
Ist also $\epsilon \in \mathcal{O}_K^*$, so gibt es ein $a \in \mathbb{F}_p^*$ und ein $k \in \mathbb{Z}$ mit

$$\epsilon = a\epsilon_0^k.$$

Der Wert $R_K := \operatorname{grad} \epsilon_0$ heißt der *Regulator von K*.
Wir wollen aber noch eine weitere Einheit von K auszeichnen.

4.2.3 Definition

Es sei ϵ_1 diejenige Einheit von K vom größten Betrag kleiner als 1 mit $N(\epsilon_1) = 1$.
Diese Einheit wird *positive Grundeinheit* genannt, und es ist offensichtlich

$$\epsilon_1 = \begin{cases} \epsilon_0^{-1}, & \text{falls } N(\epsilon_0) = 1, \\ g\epsilon_0^{-2}, & \text{falls } N(\epsilon_0) = g. \end{cases}$$

Ist dann $\mathcal{O}_K^{*+} := \{\epsilon \in \mathcal{O}_K^* \mid \chi(N(\epsilon)) = 1\}$, so gilt $\mathcal{O}_K^{*+} = \mathbb{F}_p^* \times < \epsilon_1 >$ und

$$|\mathcal{O}_K^*/\mathcal{O}_K^{*+}| = \begin{cases} 1, & \text{falls } N(\epsilon_0) = 1 \text{ und} \\ 2, & \text{falls } N(\epsilon_0) = g. \end{cases}$$

Teil II
Kettenbruchentwicklung

5 Allgemeine Kettenbruchentwicklung in Potenzreihenkörpern

In diesem Kapitel erweitern wir die von E. ARTIN benutzte Kettenbruchentwicklung im Potenzreihenkörper k_∞ (vgl. [A], S.190ff.). Er verwendete für seine Untersuchungen ausschließlich die Kettenbruchentwicklung mit Zähler 1, die sogenannte *Standard-Kettenbruchentwicklung*. Wir wollen die Definition der Kettenbruchentwicklungsarten dahingehend erweitern, daß wir für die Zähler beliebige Folgen aus $\mathbb{F}_p^*$ zulassen.

5.1 Definition und Eigenschaften

5.1.1 Definition

Es seien

$$\mathbb{K} := (\mathbb{F}_p^*)^{\mathbb{N}_0} = \{(\eta_r)_{r\in\mathbb{N}_0} \mid \eta_r \in \mathbb{F}_p^* \text{ für } r \in \mathbb{N}_0\},$$

$\eta \in \mathbb{K}$ und $Z \in k_\infty^*$.
Man definiert dann induktiv

$$Z_0^\eta := Z, \quad M_r^\eta := [Z_r^\eta], \quad Z_{r+1}^\eta := \frac{\eta_r}{Z_r^\eta - M_r^\eta} = T_r^\eta \circ Z_r^\eta \quad \text{für } r \geq 0,$$

wobei $T_r^\eta \circ Z_r^\eta$ die Schreibweise einer gebrochen-linearen Transformation ist mit

$$T_r^\eta := \begin{pmatrix} 0 & \eta_r \\ 1 & -M_r^\eta \end{pmatrix}.$$

Dieser Prozeß soll abbrechen, falls $Z_{r_0}^\eta = M_{r_0}^\eta$ für ein $r_0 \geq 0$ gilt; für $s > r_0$ seien dann $Z_s^\eta = M_s^\eta = 0$ gesetzt.
Ansonsten werde der Prozeß weitergeführt.

$$[M_0^\eta, M_1^\eta, \ldots]^\eta = M_0^\eta + \cfrac{\eta_0}{M_1^\eta + \cfrac{\eta_1}{M_2^\eta + \cfrac{\eta_2}{\ddots}}}$$

heißt die *Kettenbruchentwicklung (KBE) von Z bezüglich $\eta \in \mathbb{K}$* und

$$\alpha_r^\eta := [M_0^\eta, \ldots, M_r^\eta]^\eta = M_0^\eta + \cfrac{\eta_0}{M_1^\eta + \cfrac{\eta_1}{M_2^\eta + \cfrac{\eta_2}{\ddots + \cfrac{\eta_r}{M_r^\eta}}}}$$

der *r-te Näherungsbruch*, M_r^η der *r-te Partialbruch* und Z_r^η der *r-te vollständige Partialbruch von Z bezüglich $\eta \in \mathbb{K}$* und η die *KB-Entwicklungsart* (kurz KBE-Art).
Die Folge $\eta = (1)_{r\in\mathbb{N}_0}$ nennen wir die *Standard-KBE-Art* und $\eta = (-1)_{r\in\mathbb{N}_0}$ die *negative KBE-Art* mit den Bezeichnungen

$$M_r^+ := M_r^{((1))}, \quad M_r^- := M_r^{((-1))}.$$

5.1.2 Lemma

Es seien $Z \in k_\infty^*$ und $\eta \in \mathbb{K}$. Dann gilt $|M_r^\eta| > 1$ für alle $r \geq 1$ mit $Z_{r-1}^\eta \neq M_{r-1}^\eta$.

BEWEIS:

Ist $r \geq 1$ und $Z_{r-1}^\eta \neq M_{r-1}^\eta$, so gilt

$$|Z_{r-1}^\eta - M_{r-1}^\eta| = |Z_{r-1}^\eta - [Z_{r-1}^\eta]| < 1.$$

Man hat also

$$|M_r^\eta| = |Z_r^\eta| = \left| \frac{\eta_{r-1}}{Z_{r-1}^\eta - M_{r-1}^\eta} \right| > 1.$$

□

5.1.3 Lemma

Es seien $Z \in k_\infty^*$ und $\eta \in \mathbb{K}$. Definiert man dann induktiv

$$\mu_0 := 1 \quad \text{und} \quad \mu_{r+1} := \frac{1}{\eta_r \mu_r} \quad (r \geq 0),$$

so gilt $Z_r^+ = \mu_r Z_r^\eta$ und $M_r^+ = \mu_r M_r^\eta$ für $r \geq 0$.
Man erhält

$$\mu_{2j+1} = \prod_{i=0}^{j} \frac{\eta_{2i-1}}{\eta_{2i}} \quad \text{und} \quad \mu_{2j} = \prod_{i=0}^{j-1} \frac{\eta_{2i}}{\eta_{2i+1}}$$

mit $\eta_{-1} := 1$.

BEWEIS:

Wir beweisen $Z_r^+ = \mu_r Z_r^\eta$ durch vollständige Induktion nach r.
Für $r = 0$ gilt $Z = Z_0^+ = Z_0^\eta = \mu_0 Z_0^\eta$ und ebenso $M_0^+ = \mu_0 M_0^\eta$.
Es sei nun $Z_r^+ = \mu_r Z_r^\eta$ und $M_r^+ = \mu_r M_r^\eta$ vorausgesetzt. Dann gilt

$$Z_{r+1}^+ = \frac{1}{Z_r^+ - M_r^+} = \frac{1}{\mu_r Z_r^\eta - \mu_r M_r^\eta} = \frac{1}{\mu_r \eta_r} Z_{r+1}^\eta = \mu_{r+1} Z_{r+1}^\eta.$$

Zum Beweis der Produktdarstellung durch vollständige Induktion nach j verifiziert man zunächst $\mu_1 = \frac{1}{\eta_0}$ und $\mu_0 = 1$ für $j = 0$.
Für den Schritt $j \mapsto j+1$ nutzt man die Gleichungen

$$\mu_{2j+2}\mu_{2j+1} = \frac{1}{\eta_{2j+1}} \quad \text{und} \quad \mu_{2j}\mu_{2j+1} = \frac{1}{\eta_{2j}}$$

aus und benutzt die Induktionsvoraussetzung. □

5.1.4 Folgerung

Sind M_r^+ für $r \geq 0$ die Partialbrüche der Standard-KBE und M_r^- die Partialbrüche der negativen KBE eines Elements $Z = Z_0^+ \in k_\infty^*$, so gilt

$$M_r^+ = (-1)^r M_r^-.$$

BEWEIS:

Ist $\eta := (-1)_{r\geq 0}$, so erhält man mit Lemma 5.1.3

$$\mu_r = \begin{cases} -1, & \text{falls } r \text{ ungerade,} \\ 1, & \text{falls } r \text{ gerade,} \end{cases}$$

was die Behauptung liefert. □

5.2 Äquivalenz in k_∞^*

5.2.1 Definition

Es seien

$$\begin{aligned} \mathrm{GL}(2;\mathbb{F}_p[X]) &:= \{T \in \mathrm{Mat}(2;\mathbb{F}_p[X]) \mid \det T \in \mathbb{F}_p^*\} \text{ und} \\ \mathrm{SL}(2;\mathbb{F}_p[X]) &:= \{T \in \mathrm{GL}(2;\mathbb{F}_p[X]) \mid \chi(\det T) = 1\}. \end{aligned}$$

Zwei Elemente $F, G \in k_\infty^*$ heißen *äquivalent* ($F \sim G$), falls $\alpha, \beta, \gamma, \delta \in \mathbb{F}_p[X]$ existieren mit $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2;\mathbb{F}_p[X])$ und

$$F = \frac{\alpha G + \beta}{\gamma G + \delta} = T \circ G.$$

F und G heißen *eng äquivalent* ($F \sim_+ G$), falls $F = T \circ G$ mit $T \in \mathrm{SL}(2;\mathbb{F}_p[X])$ erfüllt ist.

5.2.2 Definition

Es seien $\eta \in \mathbb{K}$ und $Z \in k_\infty^*$. Dann definieren wir induktiv

$$P_0^\eta := 1, \;\; Q_0^\eta := 0, \;\; P_1^\eta := M_0^\eta, \;\; Q_1^\eta := 1$$

und

$$\begin{aligned} P_{r+1}^\eta &:= P_r^\eta M_r^\eta + \eta_{r-1} P_{r-1}^\eta \\ Q_{r+1}^\eta &:= Q_r^\eta M_r^\eta + \eta_{r-1} Q_{r-1}^\eta \end{aligned}$$

für $r \geq 1$ mit den Partialbrüchen M_r^η der KBE von $Z = Z_0^\eta$ bezüglich η.

Für $r \geq 0$ seien T_r^η die Matrizen aus Definition 5.1.1. Wegen $\det T_r^\eta = -\eta_r$ handelt es sich hierbei um Elemente von $\mathrm{GL}(2;\mathbb{F}_p[X])$.
Dann wird für $r \geq 1$ mit

$$T := T_{r-1}^\eta \cdot \ldots \cdot T_0^\eta \in \mathrm{GL}(2;\mathbb{F}_p[X])$$

die Matrix $S_r^\eta \in \mathrm{GL}(2;\mathbb{F}_p[X])$ definiert durch

$$S_r^\eta := (\eta_0 \cdot \ldots \cdot \eta_{r-1}) T^{-1}.$$

5.2.3 Lemma

Es seien $\eta \in \mathbb{K}$ und $Z \in k_\infty^*$. Dann sind die folgenden Aussagen richtig:

(i) Es gilt

$$P_1^\eta Q_0^\eta - P_0^\eta Q_1^\eta = -1$$

und

$$P_r^\eta Q_{r-1}^\eta - P_{r-1}^\eta Q_r^\eta = (-1)^r(\eta_0 \cdot \ldots \cdot \eta_{r-2})$$

für $r \geq 2$.

(ii) Es gilt

$$S_r^\eta = \begin{pmatrix} P_r^\eta & \eta_{r-1}P_{r-1}^\eta \\ Q_r^\eta & \eta_{r-1}Q_{r-1}^\eta \end{pmatrix} = \begin{pmatrix} M_0^\eta & \eta_0 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} M_{r-1}^\eta & \eta_{r-1} \\ 1 & 0 \end{pmatrix}$$

für $r \geq 1$.

(iii) Es ist

$$\begin{aligned} |P_r^\eta| &= |M_0^\eta \cdot \ldots \cdot M_{r-1}^\eta| \\ |Q_r^\eta| &= |M_1^\eta \cdot \ldots \cdot M_{r-1}^\eta| \end{aligned}$$

und $|P_r^\eta| > |Q_r^\eta| > |Q_{r-1}^\eta|$ für $r \geq 1$.

(iv) Ist $r \geq 1$, so gilt

$$\alpha_{r-1}^\eta = \frac{P_r^\eta}{Q_r^\eta}.$$

(v) Für alle $Z \in k_\infty^*$, $r \in \mathbb{N}_0$ und $\eta \in \mathbb{K}$ ist

$$Z = S_r^\eta \circ Z_r^\eta$$

mit $S_r^\eta \in \mathrm{GL}(2; \mathbb{F}_p[X])$ aus Definition 5.2.2, also $Z \sim Z_r^\eta$.

(vi) Ist $\eta = ((-1))_{r \in \mathbb{N}_0}$ die negative KBE, so gilt

$$Z \sim_+ Z_r^- .$$

BEWEIS:

(i) Diese Aussagen zeigt man durch eine einfache vollständige Induktion nach r.

(ii) Für die Matrizen T_i^η ($i \in \{0, \ldots, r-1\}$) aus Definition 5.1.1 zeigt man durch vollständige Induktion nach r, daß

$$T_{r-1}^\eta \cdot \ldots \cdot T_0^\eta = (-1)^r \begin{pmatrix} \eta_{r-1}Q_{r-1}^\eta & -\eta_{r-1}P_{r-1}^\eta \\ -Q_r^\eta & P_r^\eta \end{pmatrix} =: T$$

mit $\det T = (-1)^r(\eta_0 \cdot \ldots \cdot \eta_{r-1})$ richtig ist.
Man hat dann

$$S_r^\eta = (\eta_0 \cdot \ldots \cdot \eta_{r-1}) \cdot \frac{1}{\det T} \begin{pmatrix} P_r^\eta & \eta_{r-1}P_{r-1}^\eta \\ Q_r^\eta & \eta_{r-1}Q_{r-1}^\eta \end{pmatrix} = \begin{pmatrix} M_0^\eta & \eta_0 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} M_{r-1}^\eta & \eta_{r-1} \\ 1 & 0 \end{pmatrix}$$

mit $\det S_r^\eta = \det T$.

(iii) Diese Aussagen zeigen wir wiederum durch vollständige Induktion nach $r \geq 1$. Für $r = 1$ folgt $|P_1^\eta| = |M_0^\eta|$ und $|Q_1^\eta| = 1$ (leeres Produkt) aus Definition 5.2.2. Für den Schritt $r \to r+1$ benutzt man die Tatsache $|M_r^\eta| > 1$ für $r \geq 1$ aus Lemma 5.1.2. Daraus erhält man

$$|P_{r+1}^\eta| = |P_r^\eta M_r^\eta + \eta_{r-1} P_{r-1}^\eta| \overset{\text{I.V.}}{=} |M_0^\eta \cdot \ldots \cdot M_r^\eta + \eta_{r-1} M_0^\eta \cdot \ldots \cdot M_{r-1}^\eta| \overset{|M_r^\eta|>1}{=} |M_0^\eta \cdot \ldots \cdot M_r^\eta|$$

und analog $|Q_{r+1}^\eta| = |M_1^\eta \cdot \ldots \cdot M_r^\eta|$.
Hieraus folgt nun insbesondere $|P_r^\eta| > |Q_r^\eta| > |Q_{r-1}^\eta|$ für alle $r \geq 1$.

(iv) Wir zeigen

$$\frac{P_r^\eta}{Q_r^\eta} = [M_0^\eta, \ldots, M_{r-1}^\eta] = \alpha_{r-1}^\eta$$

mit vollständiger Induktion nach $r \geq 1$.
Für $r = 1$ erhält man $\frac{P_1^\eta}{Q_1^\eta} = M_0^\eta$.
Für den Induktionsschritt betrachtet man das Produkt

$$\begin{pmatrix} M_0^\eta & \eta_0 \\ 1 & 0 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} M_1^\eta & \eta_1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} M_r^\eta & \eta_r \\ 1 & 0 \end{pmatrix}}_{=: \begin{pmatrix} P & P' \\ Q & Q' \end{pmatrix}} = \begin{pmatrix} P_{r+1}^\eta & \eta_r P_r^\eta \\ Q_{r+1}^\eta & \eta_r Q_r^\eta \end{pmatrix}.$$

Hier gilt $\frac{P}{Q} = [M_1^\eta, \ldots, M_r^\eta]$ nach Induktionsvoraussetzung, und es ist

$$P_{r+1}^\eta = M_0^\eta P + \eta_0 Q, \;\; Q_{r+1}^\eta = P.$$

Es folgt dann mit

$$\frac{P_{r+1}^\eta}{Q_{r+1}^\eta} = M_0^\eta + \frac{\eta_0}{\frac{P}{Q}} = M_0^\eta + \frac{\eta_0}{[M_1^\eta, \ldots, M_r^\eta]} = \alpha_r^\eta$$

die Behauptung.

(v) Für $r \geq 1$ gilt $S_r^\eta \in \mathrm{GL}(2; \mathbb{F}_p[X])$, und aus der Definition 5.1.1 erhält man

$$Z_r^\eta = (T_{r-1}^\eta \cdot \ldots \cdot T_0^\eta) \circ Z,$$

also ist $Z = S_r^\eta \circ Z_r^\eta$, d.h. $Z \sim Z_r^\eta$.

(vi) Für $\eta = ((-1))_{r \in \mathbb{N}_0}$ ist $\det S_r^\eta = (-1)^{2r} = 1$, also $S_r^- \in \mathrm{SL}(2; \mathbb{F}_p[X])$ für alle $r \geq 1$. Daraus folgt $Z \sim_+ Z_r^-$.

□

Analogien zur Kettenbruchentwicklung im Körper der reellen Zahlen bezüglich abbrechender Kettenbruchentwicklungen und der Konvergenz endlicher Kettenbrüche (vgl. z.B. [Zag2], S.126) zeigt der folgende Satz auf.

5.2.4 Satz

(i) Die KBE von $Z \in k_\infty^*$ bezüglich $\eta \in \mathbb{K}$ bricht ab

$$\Leftrightarrow \quad Z \in k^* = \mathbb{F}_p(X)^*.$$

(ii) Ist $Z \in k_\infty^*$, $\eta \in \mathbb{K}$ und $|\ \cdot\ |$ der Absolutbetrag auf k_∞^*, so gilt

$$|\ |-\lim_{r\to\infty}\alpha_r^\eta = |\ |-\lim_{r\to\infty}\frac{P_{r+1}^\eta}{Q_{r+1}^\eta} = Z.$$

BEWEIS:

Man führt die Rechnungen in [A], S. 190ff. mod $\mathbb{F}_p^*$ durch und nutzt für Teil (ii) zusätzlich Lemma 5.2.3 (iv) aus. □

Haben wir bisher allgemein Elemente $Z \in k_\infty^*$ betrachtet, so beschränken wir uns bei unseren weiteren Untersuchungen nun auf Elemente $Z \in K\backslash k$, wobei $K = k(\sqrt{D}) \subset k_\infty$ ein reell-quadratischer Funktionenkörper sei. D.h. bei $D \in \mathbb{F}_p[X]$ handelt es sich um ein normiertes quadratfreies Polynom von geradem Grad.

5.3 (Artin-)Reduzierte Elemente

Wir führen neben dem von ARTIN benutzten Reduziertheitsbegriff (vgl. [A], S. 192) auf $K\backslash k$ einen strengeren Reduziertheitsbegriff ein, der in Zusammenhang mit der engen Äquivalenz von Elementen steht.

5.3.1 Definition

Ein $Z \in K\backslash k$ heißt *Artin-reduziert* (A-red.), falls

$$|\overline{Z}| < 1 < |Z|.$$

Z heiße *reduziert*, falls Z A-red. ist und zusätzlich $\operatorname{sgn} Z \in \{1, g\}$ gilt.

5.3.2 Lemma

Es seien $Z \in K\backslash k$ A-red., $\eta \in \mathbb{K}$ beliebig und Z_r^η für $r \geq 0$ die vollständigen Partialbrüche von Z bezüglich η. Dann gilt

$$|\overline{Z_{r+1}^\eta}| = |Z_r^\eta|^{-1},$$

und es ist Z_r^η A-red. für alle $r \geq 0$.

BEWEIS:

Wir beweisen die Aussage durch vollständige Induktion nach $r \geq 0$.
Für $r = 0$ ist $|\overline{Z_0^\eta} - [Z_0^\eta]| = |Z_0^\eta|$, denn es gilt $|\overline{Z_0^\eta}| < 1 < |Z_0^\eta| = |[Z_0^\eta]|$, da $Z = Z_0^\eta$ A-red. ist. Weiterhin gilt

$$Z_1^\eta = \frac{\eta_0}{Z_0^\eta - [Z_0^\eta]}, \quad \text{also} \quad \overline{Z_1^\eta} = \frac{\eta_0}{\overline{Z_0^\eta} - [Z_0^\eta]},$$

da $\eta_0, [Z_0^\eta] \in k$. Daraus folgt

$$|\overline{Z_1^\eta}| = \left|\frac{\eta_0}{\overline{Z_0^\eta} - [Z_0^\eta]}\right| = |Z_0^\eta|^{-1}.$$

Setzt man nun Z_r^η als A-red. voraus, so gilt $|\overline{Z_r^\eta} - [Z_r^\eta]| = |Z_r^\eta| > 1$ und $|Z_r^\eta - [Z_r^\eta]| < 1$, denn es ist $|Z_r^\eta| > 1 > |\overline{Z_r^\eta}|$.

Daraus erhält man

$$|\overline{Z_{r+1}^{\eta}}| = \left| \frac{\eta_r}{\overline{Z_r^{\eta}} - [Z_r^{\eta}]} \right| = |Z_r^{\eta}|^{-1} < 1$$

und

$$|Z_{r+1}^{\eta}| = \left| \frac{\eta_r}{Z_r^{\eta} - [Z_r^{\eta}]} \right| > 1,$$

also die Artin-Reduziertheit von Z_{r+1}^{η}. □

Ist $Z \in K\backslash k$ reduziert, so hängt die Reduziertheit der vollständigen Partialbrüche Z_r^{η} offensichtlich stark von der gewählten KBE-Art η ab. Wir definieren nun eine KBE-Art mit der Eigenschaft, daß alle vollständigen Partialbrüche eines reduzierten Elements Z wieder reduziert sind.

5.3.3 Definition

Es sei $Z \in K\backslash k$. Dann ist die *enge KBE* von Z mit der *engen KBE-Art* η wie folgt definiert:

$$Z_0^{\eta} := Z, \quad M_r^{\eta} := [Z_r^{\eta}] \quad Z_{r+1}^{\eta} := \frac{\eta_r}{Z_r^{\eta} - M_r^{\eta}}$$

mit

$$\eta_r := \begin{cases} \operatorname{sgn}(Z_r^{\eta} - M_r^{\eta}), & \text{falls } \chi(M_r^{\eta} - Z_r^{\eta}) = 1, \\ g \cdot \operatorname{sgn}(Z_r^{\eta} - M_r^{\eta}), & \text{falls } \chi(M_r^{\eta} - Z_r^{\eta}) = -1. \end{cases}$$

Wir kennzeichnen die enge KBE mit einem hochgestellten Sternchen ($Z_r^{\eta} =: Z_r^*$).

5.3.4 Lemma

Ist $Z \in K\backslash k$, so gilt:

(i) $Z \sim_+ Z_r^*$ für alle $r \geq 0$,

(ii) $\operatorname{sgn} Z_r^* \in \{1, g\}$ für alle $r \geq 1$.

BEWEIS:

Diese Aussagen folgen sofort aus der Definition 5.3.3. □

5.3.5 Lemma

Ist $Z \in K\backslash k$ Artin-reduziert, so gilt

(i) Z_r^* ist reduziert für $r \geq 1$,

(ii) $\chi(\overline{Z_{r+1}^*}) = \chi(Z_r^*)$ für alle $r \geq 0$.

BEWEIS:

(i) Nach Lemma 5.3.2 ist Z_r^* A-red. für alle $r \geq 1$. Mit Lemma 5.3.4 (ii) folgt dann die Reduziertheit von Z_r^* für $r \geq 1$.

(ii) Diese Aussage liest man sofort an der Darstellung

$$Z_{r+1}^* = \frac{\eta_r}{Z_r^* - M_r^*}$$

ab, indem man ausnutzt, daß die Partialbrüche Z_r^* für $r \geq 0$ A-red. sind.

□

5.3.6 Satz

Es seien $Z \in K\backslash k$ und $\eta \in \mathbb{K}$ beliebig. Dann gilt

(i) Es existieren $r_0 \geq 0$ und $\nu \in \mathbb{N}$ mit

$$\frac{Z_{\nu+r}^{\eta}}{Z_r^{\eta}} \in \mathbb{F}_p^*$$

für alle $r \geq r_0$.

(ii) Z ist A-red. genau dann, wenn in (i) $r_0 = 0$ wählbar ist.

(iii) Zu jedem $Z \in K\backslash k$ existiert ein A-red. W mit $Z \sim W$.

(iv) Zu jedem $Z \in K\backslash k$ existiert ein red. W mit $Z \sim_+ W$.

BEWEIS:

(i) Dies erhält man wie in [A], S. 193/194, indem alle Rechnungen wiederum mod $\mathbb{F}_p^*$ geschehen müssen.

(ii) Die Äquivalenz zeigt sich ebenfalls durch Übertragung der Aussagen von [A], S. 193/194 auf die allgemeine Kettenbruchentwicklung.

(iii) In (i) ist $Z_{r_0}^{\eta}$ A-red., und nach Lemma 5.2.3 (v) gilt $Z \sim Z_{r_0}^{\eta}$.

(iv) Nach Lemma 5.3.4 (ii) gilt $\operatorname{sgn}(Z_r^*) \in \{1, g\}$ für alle $r \geq 1$ mit den vollständigen Partialbrüchen Z_r^* der engen KBE-Art.
Nach (iii) existiert ein r_0, so daß $Z_{r_0}^*$ A-red. ist, und wegen Lemma 5.3.4 (i) gilt $Z \sim_+ Z_{r_0}^*$. Daraus folgt die Behauptung mit $W := Z_{r_0}^*$.

□

5.4 Perioden

Basierend auf der Aussage (i) des Satzes 5.3.6 lassen sich nun verschiedene Perioden von Kettenbruchentwicklungen Artin-reduzierter Elemente definieren.

5.4.1 Definition

Es sei $Z \in K\backslash k$ A-red. und $\eta \in \mathbb{K}$. Dann heißt

(1) $\rho_\eta(Z) := \min\{\rho \geq 1 \mid \frac{Z_{\rho+k}^{\eta}}{Z_k^{\eta}} = 1 \text{ für alle } k \geq 0\} \in \mathbb{N} \cup \{\infty\}$
die *Periode*,

(2) $\mu_\eta(Z) := \min\{\mu \geq 1 \mid \frac{Z_{\mu+k}^{\eta}}{Z_k^{\eta}} \in \mathbb{F}_p^{*^2} \text{ für alle } k \geq 0\} \in \mathbb{N} \cup \{\infty\}$
die *Quadratperiode* und

(3) $\nu_\eta(Z) := \min\{\nu \geq 1 \mid \frac{Z_{\nu+k}^{\eta}}{Z_k^{\eta}} \in \mathbb{F}_p^* \text{ für alle } k \geq 0\} \in \mathbb{N}$
die *Quasiperiode* der KBE von Z bezüglich $\eta \in \mathbb{K}$.

Die Endlichkeit der Quasiperiode in (3) folgt direkt aus Satz 5.3.6.

5.4.2 Lemma

Es sei $Z \in K\backslash k$ A-red. Dann gilt

(i) $\nu_\eta(Z)|\mu_\eta(Z)$, falls $\mu_\eta(Z) \in \mathbb{N}$.

(ii) $\nu_\eta(Z)|\rho_\eta(Z)$, falls $\rho_\eta(Z) \in \mathbb{N}$.

(iii) $\mu_\eta(Z)|\rho_\eta(Z)$, falls $\eta_r \in \mathbb{F}_p^{*^2}$ für alle $r \geq 0$ und $\mu_\eta(Z), \rho_\eta(Z) \in \mathbb{N}$.

BEWEIS:

(i) Es sei $Z \in K\backslash k$ A-red. und $\mu_\eta(Z) = l\nu_\eta(Z)+r$ mit eindeutig bestimmten $l \geq 1$, $0 \leq r \leq \nu_\eta(Z) - 1$. Nach Definition von $\mu_\eta(Z)$ gilt

$$\frac{Z^\eta_{\mu_\eta(Z)+k}}{Z^\eta_k} = b \in \mathbb{F}_p^{*^2} \quad \text{für alle } k \geq 0.$$

Daraus ergibt sich

$$Z^\eta_0 = b^{-1}Z^\eta_{\mu_\eta(Z)} = b^{-1}Z^\eta_{l\nu_\eta(Z)+r} = b^{-1}aZ^\eta_r \quad \text{mit } a \in \mathbb{F}_p^*,$$

da $\nu_\eta(Z)$ die Quasiperiode ist. Es folgt also $r = 0$ oder $\nu_\eta(Z) - 1 < r$. Letzteres ist wegen $0 \leq r \leq \nu_\eta(Z) - 1$ nicht möglich, also gilt $r = 0$ und $\nu_\eta(Z)|\mu_\eta(Z)$.

(ii) Analog zu (i) mit $b = 1$.

(iii) Analog zu (i) mit $b = 1$ und $a \in \mathbb{F}_p^{*2}$.

□

5.4.3 Satz

Es seien $\eta, \zeta \in \mathbb{K}$ und $Z, W \in K\backslash k$ mit $Z = bW$ und $b \in \mathbb{F}_p^*$. Setzt man $\eta_{-1} = \zeta_{-1} = 1$, so gilt

$$\frac{Z^\zeta_r}{W^\eta_r} = b^{(-1)^r} \prod_{i=0}^{r} (\zeta_{i-1}\eta_{i-1}^{-1})^{(-1)^{r-i}} \in \mathbb{F}_p^* \quad \text{für alle } r \geq 0.$$

BEWEIS:

Der Beweis erfolgt mit einer Induktion nach r.

Für $r = 0$ verifiziert man $\frac{Z^\zeta_0}{W^\eta_0} = \frac{Z}{W} = b \in \mathbb{F}_p^*$.

Für den Schritt $r \mapsto r + 1$ benutzt man die Darstellung

$$Z^\zeta_{r+1} = \frac{\zeta_r}{Z^\zeta_r - [Z^\zeta_r]} \overset{\text{I.V.}}{=} \zeta_r\eta_r^{-1} \prod_{i=0}^{r} (\zeta_{i-1}\eta_{i-1}^{-1})^{(-1)^{r-i+1}} b^{(-1)^{r+1}} W^\eta_{r+1},$$

und das war die Behauptung. □

5.4.4 Korollar

a) Ist $Z \in K\backslash k$ A-red., so ist die Quasi-Periode $\nu_\eta(Z)$ unabhängig von der KBE-Art $\eta \in \mathbb{K}$, so daß wir von nun an $\nu(Z)$ für die Quasiperiode von Z bezüglich irgendeiner KBE-Art schreiben können.

b) Ist $Z \in K\backslash k$ A-red., so gilt

$$\nu(Z) = \nu(bZ)$$

für alle $b \in \mathbb{F}_p^*$.

c) Ist $Z \in k_\infty^*$, und sind $\zeta, \eta \in \mathbb{K}$, so gilt $|Z_r^\zeta| = |Z_r^\eta|$ für alle $r \geq 0$.

d) Ist $\eta \in \mathbb{K}$ eine konstante Folge, $Z \in K\backslash k$ A-red. und $\nu(Z)$ ungerade, dann ist $\rho_\eta(Z)$ endlich, und es gilt

$$\frac{\rho_\eta(Z)}{\nu(Z)} \in \{1, 2\}.$$

e) Ist $\eta \in \mathbb{K}$ eine konstante Folge, $Z \in K\backslash k$ A-red. und periodisch mit ungerader Periode $\rho_\eta(Z)$, so gilt $\nu = \rho_\eta(Z)$.

BEWEIS:

a) Diese Aussage folgt aus Satz 5.4.3 mit $b = 1$.

b) Dies folgt sofort aus der Aussage des Satzes 5.4.3.

c) Dies zeigt man wie in a).

d) Für diese Aussage nutzt man aus, daß $Z_\nu^\eta = bZ_0^\eta$ mit $\nu := \nu(Z)$ ist und setzt $W = Z_0^\eta$ in Satz 5.4.3. Man erhält

$$\frac{Z_{2\nu}^\eta}{Z_\nu^\eta} = b^{(-1)^\nu},$$

da η eine konstante Folge ist. Wegen $\nu \equiv 1\ (2)$ hat man $Z_{2\nu}^\eta = b^{-1}Z_\nu^\eta = Z_0^\eta$, also $\frac{\rho_\eta(Z)}{\nu} \in \{1, 2\}$. Hierbei ist $\rho_\eta(Z) = \nu$ im Fall $b = 1$.

e) Ist $\rho_\eta(Z)$ ungerade, so muß wegen $\nu(Z)|\rho_\eta(Z)$ auch $\nu(Z)$ ungerade sein. Nach d) kann dann nur der Fall $\nu(Z) = \rho_\eta(Z)$ auftreten, und es folgt die Behauptung. □

5.4.5 Definition

Für $\zeta, \eta \in \mathbb{K}$ definiert man

$$\zeta \simeq \eta \quad \Leftrightarrow \quad \chi(\zeta_r) = \chi(\eta_r) \text{ für alle } r \geq 0.$$

5.4.6 Satz

Sind $\zeta, \eta \in \mathbb{K}$ mit $\zeta \simeq \eta$ und $Z = bW \in K\backslash k$ mit $b \in \mathbb{F}_p^*$, so gilt

$$\chi(Z_r^\zeta) = \chi(b)\chi(W_r^\eta) \quad \text{für alle } r \geq 0.$$

BEWEIS:

Wegen $\chi(b) = \chi(b^{-1})$ für alle $b \in \mathbb{F}_p^*$ und $\chi(\zeta_r\eta_r^{-1}) = 1$ folgt die Aussage direkt aus Satz 5.4.3. □

5.4.7 Korollar

Sind unter den Voraussetzungen von Satz 5.4.6 zusätzlich $Z, W \in K\backslash k$ A-red., so gilt

$$\mu_\zeta(Z) = \mu_\eta(W).$$

BEWEIS:

Das Korollar folgt aus Satz 5.4.6 und der Definition der Quadratperiode. □

5.4.8 Satz

Sei $Z \in K\backslash k$ A-red., $\nu := \nu(Z)$, $a := \frac{Z_\nu^\eta}{Z_0^\eta} \in \mathbb{F}_p^*$ und $\eta \in \mathbb{K}$ mit $\chi(\eta_r) = \chi(\eta_{\nu+r})$ für alle $r \geq 0$. Dann gilt

$$Z_{l\nu+k}^\eta = a^l q_{l,k} Z_k^\eta \quad \text{für alle } l \geq 0, k \geq 0 \text{ mit gewissen } q_{l,k} \in \mathbb{F}_p^{*^2},$$

d.h.

$$\chi\left(\frac{Z_{l\nu+k}^\eta}{Z_k^\eta}\right) = \chi(a)^l$$

für alle $l, k \geq 0$.

BEWEIS:

Für $l = 0$ ist die Aussage des Satzes trivial.

Wir zeigen:

$$(*) \quad Z_{l\nu+k}^\eta = a\tilde{q}_{l,k} Z_{(l-1)\nu+k}^\eta$$

für alle $l \geq 1$, $k \geq 0$ mit einer Induktion nach l. Wir wissen, daß $Z_\nu^\eta = aZ_0^\eta$ gilt. Definiert man $(\tilde{\zeta}_r)_{r\geq 0} := (\eta_{\nu+r})_{r\geq 0}$ und $\tilde{\eta} := \eta$, so folgt aus Satz 5.4.3 mit $Z = Z_\nu^\eta$, $W = Z_0^\eta$ und $b = a$:

$$\frac{Z_k^{\tilde{\zeta}}}{W_k^{\tilde{\eta}}} = \frac{Z_{\nu+k}^\eta}{Z_k^\eta} = a^{(-1)^k} \prod_{i=0}^{k} (\eta_{\nu+i}\eta_i^{-1})^{k-i}.$$

Hier gilt $\prod_{i=0}^{k}(\eta_{\nu+i}\eta_i^{-1})^{k-i} \in \mathbb{F}_p^{*2}$ nach Voraussetzung. Ist k ungerade, so schreibt man $a^{-1} = aa^{-2}$ und zieht das Quadrat a^{-2} mit in das Produkt. Dies liefert die Aussage für $l = 1$.

Der Schritt $l \to l+1$ verläuft analog. Man setzt $Z_{l\nu+k}^\eta = aq_{l,k} Z_{(l-1)\nu+k}^\eta$ voraus und definiert $(\tilde{\zeta}_r)_{r\geq 0} := (\eta_{l\nu+r})_{r\geq 0}$, $(\tilde{\eta}_r)_{r\geq 0} := (\eta_{(l-1)\nu+r})_{r\geq 0}$. Daraus erhält man die Induktionsbehauptung und somit $(*)$ durch Anwendung von Satz 5.4.3 auf $\tilde{\zeta}, \tilde{\eta}$ und $Z = Z_{l\nu+k}^\eta$, $b = aq_{l,k}$, $W = Z_{(l-1)\nu+k}^\eta$. Es ist dann

$$\frac{Z_{l\nu+k}^\eta}{Z_k^\eta} = \underbrace{\frac{Z_{l\nu+k}^\eta}{Z_{(l-1)\nu+k}^\eta} \cdot \frac{Z_{(l-1)\nu+k}^\eta}{Z_{(l-2)\nu+k}^\eta} \cdot \ldots \cdot \frac{Z_{1+k}^\eta}{Z_k^\eta}}_{l \text{ Faktoren}} = a^l q_{l,k}$$

mit gewissen $q_{l,k} \in \mathbb{F}_p^{*^2}$, indem man gegebenenfalls $a^{-1} = aa^{-2}$ einfließen läßt. □

5.4.9 Korollar

Sind $Z \in K\backslash k$ A-red., $\nu := \nu(Z)$, $\eta \in \mathbb{K}$ mit $\chi(\eta_r) = \chi(\eta_{\nu+r})$ für alle $r \geq 0$ und $\mu_\eta := \mu_\eta(Z)$, so gilt

(i)
$$\frac{\mu_\eta}{\nu} \in \{1, 2\},$$
d.h. insbesondere $\mu_\eta < \infty$, und

(ii)
$$\frac{\mu_\eta}{\nu} = 2 \quad \Leftrightarrow \quad \frac{Z^\eta_{l\nu}}{Z^\eta_{(l-1)\nu}} \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*^2} \quad \text{für alle } l \geq 1.$$

BEWEIS:

(i) Nach Satz 5.4.8 ist
$$\chi(\frac{Z^\eta_{2\nu+k}}{Z^\eta_k}) = 1 \quad \text{für alle } k \geq 0,$$
d.h. $\mu_\eta \leq 2\nu$, und beide Werte sind endlich. Aus Lemma 5.4.2 folgt $\nu | \mu_\eta$, also $\frac{\mu_\eta}{\nu} \in \{1, 2\}$.

(ii) Die Äquivalenz erhält man folgendermaßen:

"$\Rightarrow$" Es sei $\mu_\eta > \nu$. Mit $a := \frac{Z^\eta_\nu}{Z^\eta_0}$ ist $\chi(a) = -1$. Für beliebiges $l \geq 1$ gilt dann
$$\frac{Z^\eta_{l\nu}}{Z^\eta_{(l-1)\nu}} = \frac{Z^\eta_{l\nu}}{Z^\eta_0} \frac{Z^\eta_0}{Z^\eta_{(l-1)\nu}} = a^l a^{-(l-1)} \tilde{q}_l = a\tilde{q}_l$$
mit einem $\tilde{q}_l \in \mathbb{F}_p^{*^2}$, was die Behauptung war.

"$\Leftarrow$" Wäre $\mu_\eta = \nu$, so würde schon $\frac{Z^\eta_\nu}{Z^\eta_0} \in \mathbb{F}_p^{*^2}$ gelten, was einen Widerspruch zur Voraussetzung mit $l = 1$ herbeiführt.

□

6 Funktionen der Diskriminante D

6.1 Definition und Eigenschaften

6.1.1 Definition

Es seien $A, B, C \in \mathbb{F}_p[X]$ teilerfremd und $D = B^2 - 4AC$ quadratfrei.
Dann nennt man
$$W = \{A, B, C\} = \frac{B + \sqrt{D}}{2C}$$
eine *Funktion der Diskriminante D.*
Es sei
$$F(D) := \{W \mid W \text{ ist Funktion der Diskriminante } D\}.$$
Diese Elemente kann man als die 'positiven' Lösungen der Gleichung
$$F(-1, Y) = 0,$$
also als quadratische Irrationalitäten ansehen, wobei $F(X, Y) := AX^2 + BXY + CY^2$ eine binäre quadratische Form der Diskriminante D über $\mathbb{F}_p[X]$ ist.

6.1.2 Satz

(i) Ist $F \in F(D)$ und $F \sim G$, so ist auch $G \in F(D)$.

Insbesondere gilt dann:

Ist $\eta \in \mathbb{K}$ und $Z \in F(D)$, so existieren zu jedem $r \geq 0$ geeignete A_r^η, B_r^η und $C_r^\eta \in \mathbb{F}_p[X]$ mit $D = (B_r^\eta)^2 - 4A_r^\eta C_r^\eta$, so daß für den vollständigen Partialbruch Z_r^η von Z bezüglich der KBE η gilt:

$$Z_r^\eta = \frac{B_r^\eta + \sqrt{D}}{2C_r^\eta}.$$

(ii) Es gibt nur endlich viele (A-)reduzierte Funktionen in $F(D)$.

(iii) Ist $\eta \in \mathbb{K}$ beliebig und $Z \in F(D)$ (A-)red., so gilt

$$|M_r^\eta| = |Z_r^\eta| \leq |\sqrt{D}|$$

für alle $r \geq 0$.

BEWEIS:

(i) s. [A], S. 176.

(ii) s. [A], S. 194. ARTIN zeigte die Endlichkeit der A-red. Funktionen quadratfreier Diskriminante D, woraus sofort die Endlichkeit der red. Funktionen aus $F(D)$ folgt.

(iii) Es ist

$$|M_r^\eta| = |Z_r^\eta| \overset{|Z_r^\eta|>1>|\overline{Z_r^\eta}|}{=} |Z_r^\eta - \overline{Z_r^\eta}| = \left|\frac{\sqrt{D}}{C_r^\eta}\right|$$

nach (i) mit $C_r^\eta \in \mathbb{F}_p[X]$. Es ist also $|C_r^\eta| \geq 1$, woraus die Behauptung folgt.

□

6.2 Zykel

Ausgehend von Satz 5.3.6 (iv) und den Aussagen (i) und (ii) des Satzes 6.1.2 wird nun gezeigt, daß die Anzahl der engen Äquivalenzklassen von Funktionen $F \in F(D)$ endlich ist. Hierzu wird die enge KBE aus Definition 5.3.3 benutzt.

6.2.1 Bemerkung

Betrachtet man die enge KBE eines reduzierten Elements $Z \in F(D)$, so ist jeder vollständige Partialbruch Z_r^* $(r \geq 0)$ der KBE nach Satz 6.1.2 (i) wieder ein Element von $F(D)$ und nach Lemma 5.3.5 (i) auch reduziert.

Da es wegen Satz 6.1.2 (ii) nur endlich viele reduzierte Elemente in $F(D)$ gibt, und durch die Wahl der Folge $\eta \in \mathbb{K}$ der Nachfolger durch den Vorgänger eindeutig bestimmt ist, erhält man ausgehend von einem reduzierten $Z = Z_0^*$ ein sogenanntes *Zykel* $\{Z_0^*, \ldots, Z_{\lambda-1}^*\}$ von λ reduzierten Elementen.

Man nennt dieses Zykel das *zu Z gehörige Zykel* reduzierter Elemente. Die Zahl $\lambda \geq 1$ ist demnach die Periode der engen KBE von $Z = Z_0^*$.

Ist Z nicht reduziert, so weiß man aus Satz 5.3.6, daß es einen vollständigen Partialbruch $Z^*_{r_0}$ $(r_0 > 0)$ in der engen KBE von Z gibt, welcher reduziert ist. Man nennt dann das zu $Z^*_{r_0}$ gehörige Zykel reduzierter Elemente das *von Z erzeugte Zykel* reduzierter Elemente.

6.2.2 Folgerung

Ist $Z \in F(D)$ reduziert und $\lambda \geq 1$ die Länge des von Z erzeugten Zykels, so gilt

$$\lambda = \rho_*(Z) = \mu_-(Z) = \mu_*(Z).$$

BEWEIS:

Es sei $\eta \in \mathbb{K}$ die enge KBE-Art, $Z \in F(D)$ reduziert, $\rho_*(Z)$ die Periode und $\mu_*(Z)$ die Quadratperiode der engen KBE von Z. Ferner sei $\mu_-(Z)$ die Quadratperiode der negativen KBE von Z.
Aus Satz 5.4.6 mit $b = 1$ zusammen mit $((-1))_{r\geq 0} \simeq \eta$ erhält man

$$Z^-_k = b_k Z^*_k \quad (b_k \in \mathbb{F}_p^{*^2})$$

und

$$\mu_*(Z) \overset{5.4.7}{=} \mu_-(Z) = \min\{\mu \geq 1 \mid \frac{Z^-_\mu}{Z^-_0} \in \mathbb{F}_p^{*^2}\}$$

$$\overset{5.3.4\,(ii)}{=} \min\{\mu \geq 1 \mid \frac{Z^*_\mu}{Z^*_0} = 1\} = \min\{\mu \geq 1 \mid \frac{Z^*_{\mu+k}}{Z^*_k} = 1 \text{ für alle } k \geq 0\} = \rho_*(Z) = \lambda.$$

An der Stelle, an welcher Lemma 5.3.4 (ii) eingeht, muß beachtet werden, daß sich Z^*_0 und Z^*_μ wegen $\operatorname{sgn} Z^*_\mu \in \{1, g\}$ höchstens um einen Faktor aus $\mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$ unterscheiden können, falls sie nicht schon gleich sind. In diesem speziellen Fall müssen sie demnach schon gleich sein. Sind sie dies aber einmal, so auch bei jedem μ-ten Mal wieder. □

6.2.3 Satz

Zwei reduzierte Funktionen $W, W' \in F(D)$ sind genau dann eng äquivalent, wenn sie zum selben Zykel gehören.

BEWEIS:

"$\Leftarrow$" Liegen W und W' im selben Zykel, so sind sie offensichtlich eng äquivalent.

"$\Rightarrow$" Es seien W, W' zwei reduzierte Funktionen mit

$$W = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \circ W' = \frac{\alpha W' + \beta}{\gamma W' + \delta},$$

$\alpha, \beta, \gamma, \delta \in \mathbb{F}_p[X]$ und $\alpha\delta - \beta\gamma \in \mathbb{F}_p^{*^2}$. Wir betrachten zunächst drei Fälle:

(1) $\gamma = 0$.
Dann sind $\alpha, \delta \in \mathbb{F}_p^*$ und $\alpha\delta \in \mathbb{F}_p^{*^2}$. Aus $W = \frac{\alpha}{\delta} W' + \frac{\beta}{\delta}$ folgt

$$|\beta| = |\delta\overline{W} - \alpha\overline{W'}| \leq \max\{|\overline{W}|, |\overline{W'}|\} < 1,$$

da $\alpha, \delta \in \mathbb{F}_p^*$ und W, W' reduziert sind. Man erhält daraus $\beta = 0$ und $\alpha W' = \delta W$, d.h. insbesondere $\alpha \cdot \operatorname{sgn} W' = \delta \cdot \operatorname{sgn} W$. Wegen $\alpha\delta \in \mathbb{F}_p^{*^2}$ und $\operatorname{sgn} W, \operatorname{sgn} W' \in \{1, g\}$ ist dann $\alpha = \delta$. Daraus folgt aber $W = W'$. W und W' liegen also im selben Zykel.

(2) $\beta = 0, \gamma \neq 0$.
Dann folgt wieder $\alpha, \delta \in \mathbb{F}_p^*$ mit $\alpha\delta \in \mathbb{F}_p^{*^2}$.
Ist $\gamma \neq 0$, so gilt wegen $|W'| > 1$ und $\delta \in \mathbb{F}_p^*$

$$|\gamma W' + \delta| = |\gamma W'|.$$

Mit $\beta = 0$ und $\alpha \in \mathbb{F}_p^*$ würde dann $|W| \leq 1$ folgen, was ein Widerspruch zur Reduziertheit von W ist.
Somit gilt auch $\gamma = 0$, woraus nach (1) wieder $W = W'$ folgt.

(3) $\beta\gamma \neq 0$.
Wir zeigen zunächst

$$(*) \quad |\delta| < |\gamma| \quad \text{oder} \quad |\alpha| < |\beta|.$$

Wir können o.E. annehmen, daß $\alpha\delta \neq 0$ ist, denn sonst ist die Behauptung $(*)$ offensichtlich. Es gilt

$$(**) \quad |\alpha\delta| = |\beta\gamma|,$$

denn sonst würde aus

$$1 = |\alpha\delta - \beta\gamma| = \max\{|\alpha\delta|, |\beta\gamma|\}$$

folgen, daß ($|\alpha\delta| = 0$ und $|\beta\gamma| = 1$) oder ($|\alpha\delta| = 1$ und $|\beta\gamma| = 0$) gelten würde, ein Widerspruch zu $\alpha\delta \neq 0 \neq \beta\gamma$.
Nehmen wir nun an, es wären $|\delta| \geq |\gamma|$ und $|\alpha| \geq |\beta|$. Mit $(**)$ wären dann schon $|\delta| = |\gamma|$ und $|\beta| = |\alpha|$. Wir hätten also wegen $|W'| > 1 > |\overline{W'}|$

$$\left|\frac{\alpha}{\gamma}\right| = \left|\frac{\beta}{\delta}\right| = \left|\frac{\alpha\overline{W'} + \beta}{\gamma\overline{W'} + \delta}\right|$$

$$= |\overline{W}| < 1 < |W|$$

$$= \left|\frac{\alpha W' + \beta}{\gamma W' + \delta}\right| = \left|\frac{\alpha W'}{\gamma W'}\right| = \left|\frac{\alpha}{\gamma}\right|,$$

was ein Widerspruch ist. Damit ist $(*)$ gezeigt.
Es wird sich weiterhin zeigen, daß man den Fall $|\alpha| < |\beta|$ auf den Fall $|\delta| < |\gamma|$ zurückspielen kann:
Gilt nämlich $|\alpha| < |\beta|$, so gilt auch $|\alpha| < |\gamma|$, denn aus $\alpha = 0$ folgt dies wegen $\gamma \neq 0$ sofort. Aus $\delta = 0$ folgt $1 = |\beta\gamma|$, also $|\alpha| < |\beta| = |\gamma|$. Ist hingegen $\alpha\delta \neq 0$, so ist wieder $|\alpha\delta| = |\beta\gamma|$ und somit

$$(***) \quad \left|\frac{\delta}{\gamma}\right| = \left|\frac{\beta}{\alpha}\right| > 1.$$

Unter Ausnutzung von $|\overline{W'}| < 1$ erhält man

$$\left|\frac{\gamma}{\alpha}\right| > |\overline{W}| \left|\frac{\gamma}{\alpha}\right| = \left|\frac{\alpha\overline{W'} + \beta}{\gamma\overline{W'} + \delta}\right| \left|\frac{\gamma}{\alpha}\right| = \left|\frac{\overline{W'} + \frac{\beta}{\alpha}}{\overline{W'} + \frac{\delta}{\gamma}}\right| \overset{(***)}{=} \left|\frac{\frac{\beta}{\alpha}}{\frac{\delta}{\gamma}}\right| = 1,$$

und somit $|\alpha| < |\gamma|$.

Betrachtet man nun statt $W = T \circ W'$ mit $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2; \mathbb{F}_p[X])$ die Gleichung $W' = T^{-1} \circ W$, so ist

$$T^{-1} = \left(\begin{smallmatrix} \tilde{\alpha} & \tilde{\beta} \\ \tilde{\gamma} & \tilde{\delta} \end{smallmatrix}\right) = (\det T)^{-1} \left(\begin{smallmatrix} \delta & -\beta \\ -\gamma & \alpha \end{smallmatrix}\right),$$

und es gilt $|\tilde{\delta}| = |\alpha| < |\gamma| = |\tilde{\gamma}|$. Man braucht also im Fall $\beta\gamma \neq 0$ nur den Fall $|\delta| < |\gamma|$ zu untersuchen, was wir nun tun werden. Es gilt

$$W - \frac{\alpha}{\gamma} = \frac{\alpha W' + \beta}{\gamma W' + \delta} - \frac{\alpha}{\gamma} = \frac{-\det T}{(\gamma W' + \delta)\gamma}.$$

Ist $|\delta| < |\gamma|$, so erhält man daraus

$$\left| W - \frac{\alpha}{\gamma} \right| = \frac{1}{|(\gamma W' + \delta)\gamma|} \overset{|\delta| \leq |\gamma|}{=} \frac{1}{|\gamma|^2 |W'|^2} < 1.$$

Weiterhin gilt

$$\left| [W] - \frac{\alpha}{\gamma} \right| = \left| [W] - W + W - \frac{\alpha}{\gamma} \right| \leq \max\{|[W] - W|, |W - \frac{\alpha}{\gamma}|\} < 1.$$

Wendet man nun nach Definition 5.3.3 einen engen KBE-Schritt auf das Element $W = W_0^*$ an, so erhält man

$$W_1^* = \left(\begin{smallmatrix} 0 & \eta_0 \\ 1 & -[W] \end{smallmatrix}\right) \circ W = \left(\begin{smallmatrix} 0 & \eta_0 \\ 1 & -[W] \end{smallmatrix}\right) \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \circ W'$$

$$= \underbrace{\left(\begin{smallmatrix} \gamma\eta_0 & \delta\eta_0 \\ \alpha - \gamma[W] & \beta - \delta[W] \end{smallmatrix}\right)}_{=: \left(\begin{smallmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{smallmatrix}\right)} \circ W'$$

mit $\eta_0 \in \mathbb{F}_p^*$ und $|\gamma_1| = |\gamma[W] - \alpha| = |\gamma||[W] - \frac{\alpha}{\gamma}| < |\gamma|$.
Ist nun $\beta_1\gamma_1 = 0$, so gilt nach (1) und (2) $W_1^* = W'$. Da W und W_1^* aber offensichtlich im selben Zykel liegen, ist das dann die Behauptung.
Ist hingegen $\beta_1\gamma_1 \neq 0$, so kann man wiederum nach (3) folgern, daß entweder $|\delta_1| < |\gamma_1|$ oder $|\alpha_1| < |\beta_1|$ gilt. Wegen $|\alpha_1| = |\gamma|$ und $|\beta_1| = |\delta|$ stünde letzteres im Widerspruch zu $|\delta| < |\gamma|$, also haben wir erneut den Fall $|\delta_1| < |\gamma_1|$.
Definieren wir nun induktiv

$$W_0^* = W, \;\; T_0 = T, \;\; T_r := \left(\begin{smallmatrix} 0 & \eta_{r-1} \\ 1 & -[W_{r-1}^*] \end{smallmatrix}\right) T_{r-1}, \;\; T_i = \left(\begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix}\right) \quad (i \geq 1),$$

mit den η_i aus der engen KBE von Definition 5.3.3, so liegen sämtliche W_r^* im selben Zykel. Die Behauptung ist demnach gezeigt, falls irgendwann $\beta_i\gamma_i = 0$ gilt. Dies wird aber aufgrund der Ungleichung

$$|\gamma| > |\gamma_1| > |\gamma_2| > \ldots$$

eintreten, denn wegen $\gamma_i \in \mathbb{F}_p[X]$ muß schließlich $\gamma_n = 0$ sein für ein $n \in \mathbb{N}$.

□

6.2.4 Folgerung und Definition

(i) Zwei nicht notwendig reduzierte Elemente $Z, W \in F(D)$ sind genau dann eng äquivalent, wenn sie dasselbe Zykel erzeugen.

(ii) Definiert man für ein reduziertes Element $W \in K\backslash k$

$$\mathrm{Aut}(W) := \{T \in \mathrm{SL}(2; \mathbb{F}_p[X]) \mid T \circ W = W\},$$

so gilt

$$\mathrm{Aut}(W) = \{a \cdot (S^*_{\rho_*})^k \mid k \in \mathbb{Z},\ \ a \in \mathbb{F}_p^*\},$$

wobei $\rho_* := \rho_*(W)$ die Periode der engen KBE von W und $S^*_{\rho_*}$ die Matrix aus Definition 5.2.2 ist.

(iii) Es gibt nur endlich viele enge Äquivalenzklassen von Funktionen der Diskriminante D. Ihre Anzahl entspricht der Anzahl der disjunkten Zykel reduzierter Elemente aus $F(D)$.

BEWEIS:

(i) Dies folgt aus 5.3.6 (iv) und 6.2.3.

(ii) "$\supset$" Ist $W \in F(D)$ reduziert und ρ_* die Periode der engen KBE von W, so gilt nach Lemma 5.2.3 (v)

$$W = S^*_{\rho_*} \circ W^*_{\rho_*} = S^*_{\rho_*} \circ W,$$

also auch $W = a(S^*_{\rho_*})^k \circ W$ für alle $a \in \mathbb{F}_p^*$, $k \in \mathbb{Z}$.
Somit ist $a(S^*_{\rho_*})^k \in \mathrm{Aut}(W)$.

"$\subset$" Es sei $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{Aut}(W)$ für ein reduziertes $W \in K\backslash k$. Ist $\beta\gamma = 0$, so folgt aus dem Beweis des Satzes 6.2.3

$$T = aE = a(S^*_{\rho_*})^0$$

für ein $a \in \mathbb{F}_p^*$, also $T \in \{a(S^*_{\rho_*})^k \mid a \in \mathbb{F}_p^*,\ k \in \mathbb{Z}\}$.
Ist hingegen $\beta\gamma \neq 0$, so gilt entweder $|\delta| < |\gamma|$ oder $|\alpha| < |\beta|$.
Im ersten Fall liefert der Beweis des Satzes 6.2.3 ein $n \in \mathbb{N}$ und ein $a \in \mathbb{F}_p^*$ mit

$$T^*_{n-1} \cdot \ldots \cdot T^*_0 \cdot T = aE.$$

Aus Lemma 5.2.3 (ii) erhalten wir $T^*_{n-1} \cdot \ldots \cdot T^*_0 = (S^*_n)^{-1}$, also ist $T = a \cdot (S^*_n)$.
Außerdem ist

$$W = T \circ W = a(S^*_n) \circ W = W^*_n,$$

demnach muß $n \equiv 0 \mod \rho_*$ sein. Insgesamt folgt also

$$S^*_n = (S^*_{\rho_*})^k$$

für ein $k \in \mathbb{Z}$ und damit die Behauptung.
Im Fall $|\alpha| < |\beta|$ erhielten wir

$$T^*_{n-1} \cdot \ldots \cdot T^*_0 \cdot T^{-1} = aE,$$

d.h. $T = a^{-1}(S^*_n)^{-1}$, und die Behauptung folgt mit derselben Schlußweise wie im Fall $|\delta| < |\gamma|$.

(iii) Über die enge KBE erzeugt jede Funktion $F \in F(D)$ nach (i) ein eindeutig bestimmtes Zykel reduzierter Funktionen. Wegen 5.3.5 (i) und Satz 6.2.3 zerfällt die Menge der reduzierten Funktionen in disjunkte Zykel, ihre Anzahl ist demnach die Anzahl der engen Äquivalenzklassen von Funktionen der Diskriminante D.

□

7 Berechnung von Grundeinheiten

7.1 Berechnung der Fundamentaleinheit

Mit Hilfe der Standard-KBE des Elements $Z = \sqrt{D}$ ist es nach [W] und [WZ] möglich, die Fundamentaleinheit ϵ_0 und damit auch den Regulator $R_K = \operatorname{grad} \epsilon_0$ des reell-quadratischen Körpers $K = k(\sqrt{D})$ zu berechnen.
Der in [WZ], S.270 angegebene Algorithmus zur Berechnung einer Fundamentaleinheit beruht auf den Ausführungen von ARTIN in [A], S.196ff. Hierbei ist es notwendig, einmal die Quasi-Periode der Standard-KBE von $\sqrt{D}$ zu durchlaufen. Die Fundamentaleinheit setzt sich dann aus den Polynomen P_ν^+ und Q_ν^+ aus 5.2.2 zusammen.

Ähnliche Ergebnisse erhält man hinsichtlich der Berechnung der *positiven* Grundeinheit von K, wenn man die enge KBE eines reduzierten Elements $Z \in F(D)$ benutzt.

7.2 Berechnung der positiven Grundeinheit

Die nun folgenden Sätze erlauben es uns, mit Hilfe der engen KBE eines reduzierten Elements $Z \in F(D)$ – bis auf einen Faktor aus $\mathbb{F}_p^*$ – die positive Grundeinheit ϵ_1 von K zu berechnen.

7.2.1 Satz

Es sei $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper. Dann ist die enge KBE eines reduzierten Elements $Z \in F(D)$ periodisch von der Form

$$[\overline{M_0^*, M_1^*, \ldots, M_{\nu-1}^*, M_\nu^*, \ldots, M_{\rho_*-1}^*}].$$

Hier ist ν die Quasi-Periode und $\rho_* = \mu_*$ die Periode bzw. Quadratperiode der engen KBE.

Es gilt

$$N(P_\nu^* - Q_\nu^* Z) \in \mathbb{F}_p^*,$$

also $\epsilon := P_\nu^* - Q_\nu^* Z \in \mathcal{O}_K^*$ mit den Bezeichnungen aus Definition 5.2.2. Ist $\frac{Z_\nu}{Z} = c \in \mathbb{F}_p^*$, so gilt

$$\epsilon^{-1} = (-1)^\nu (\eta_0 \cdot \ldots \cdot \eta_{\nu-1})^{-1} (c Q_\nu^* Z + \eta_{\nu-1} Q_{\nu-1}^*).$$

Weiterhin ist $\frac{\rho_*}{\nu} \in \{1, 2\}$.
Im Fall $\nu \neq \rho_*$ ist $M_\nu^* = g^{\pm 1} M_0^*$ und $\chi(N(P_\nu^* - Q_\nu^* Z)) = -1$.
Ist hingegen $\nu = \rho_*$, so gilt $\chi(N(P_\nu^* - Q_\nu^* Z)) = 1$.

BEWEIS:

Es sei $\eta \in \mathbb{K}$ die enge KBE-Art und $Z \in K\backslash k$ reduziert. Es seien $\nu := \nu(Z)$ die Quasiperiode und $\mu_*(Z)$ die Quadratperiode der engen KBE-Art. Aus der Definition 5.3.3 folgt $\chi(\eta_r) = \chi(-1)$ für alle $r \geq 0$, d.h. insbesondere $\chi(\eta_r) = \chi(\eta_{\nu+r})$ für alle $r \geq 0$. Die Voraussetzungen des Korollars 5.4.9 sind demnach erfüllt. Nach Korollar 5.4.9 (i) ist somit $\mu_*(Z)$ endlich, und es gilt

$$\frac{\mu_*(Z)}{\nu(Z)} \in \{1, 2\}.$$

Wegen Folgerung 6.2.2 ist ferner $\mu_*(Z) = \rho_*(Z)$, was die Aussagen über die Perioden bestätigt.
Wir zeigen nun $N(P_\nu^* - Q_\nu^* Z) \in \mathbb{F}_p^*$.
Es sei also $Z_\nu^* = cZ$. Wie im Beweis des Lemmas 5.2.3 (v) gilt dann

$$Z = \frac{P_\nu^* Z_\nu^* + \eta_{\nu-1} P_{\nu-1}^*}{Q_\nu^* Z_\nu^* + \eta_{\nu-1} Q_{\nu-1}^*} = \frac{P_\nu^* cZ + \eta_{\nu-1} P_{\nu-1}^*}{Q_\nu^* cZ + \eta_{\nu-1} Q_{\nu-1}^*}.$$

Definiert man

$$S := \begin{pmatrix} cP_\nu^* & \eta_{\nu-1} P_{\nu-1}^* \\ cQ_\nu^* & \eta_{\nu-1} Q_{\nu-1}^* \end{pmatrix} = S_\nu^* \cdot \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$$

mit der Matrix $S_\nu^* \in \mathrm{GL}(2; \mathbb{F}_p[X])$ aus Definition 5.2.2, so gilt $S \circ Z = Z$, also

$$S \begin{pmatrix} Z \\ 1 \end{pmatrix} = (cQ_\nu^* Z + \eta_{\nu-1} Q_{\nu-1}^*) \begin{pmatrix} Z \\ 1 \end{pmatrix}.$$

Mit $\epsilon' := cQ_\nu^* Z + \eta_{\nu-1} Q_{\nu-1}^*$ gilt dann $|\epsilon'| > 1$, denn es ist $|Z| > 1$ und $|Q_\nu^*| > |Q_{\nu-1}^*|$ nach Lemma 5.2.3 (iii). Aus Lemma 5.2.3 (i) und (ii) folgt weiterhin

$$N(\epsilon') = \det S = c \det S_\nu^* = c(-1)^\nu (\eta_0 \cdot \ldots \cdot \eta_{\nu-1}).$$

Somit handelt es sich bei ϵ' um eine Einheit von $\mathcal{O}_K$, welche die quadratische Gleichung

$$\epsilon'^2 - \epsilon'(cP_\nu^* + \eta_{\nu-1} Q_{\nu-1}^*) = c\eta_{\nu-1}(Q_\nu^* P_{\nu-1}^* - P_\nu^* Q_{\nu-1}^*)$$

erfüllt. Es gilt also

$$\epsilon'(\epsilon' - cP_\nu^* - \eta_{\nu-1} Q_{\nu-1}^*) = c\epsilon'(Q_\nu^* Z - P_\nu^*) = -\det S,$$

woraus

$$\epsilon'(P_\nu^* - Q_\nu^* Z) = \frac{1}{c} \det S = \frac{1}{c} N(\epsilon') = (-1)^\nu (\eta_0 \cdot \ldots \cdot \eta_{\nu-1})$$

folgt. Es ist also $\epsilon := (P_\nu^* - Q_\nu^* Z) \in \mathcal{O}_K^*$ mit

$$\epsilon^{-1} = (-1)^\nu (\eta_0 \cdot \ldots \cdot \eta_{\nu-1})^{-1} (cQ_\nu^* Z + \eta_{\nu-1} Q_{\nu-1}^*),$$

$N(\epsilon) = c^{-1}(-1)^\nu (\eta_0 \cdot \ldots \cdot \eta_{\nu-1})$ und $|\epsilon| < 1$ gefunden. Da sowohl Z_ν^* als auch Z reduziert sind, also $\operatorname{sgn} Z, \operatorname{sgn} Z_\nu^* \in \{1, g\}$ gilt, können sie sich – wenn überhaupt – höchstens um den Faktor $g^{\pm 1} \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$ unterscheiden, d.h. es ist $c \in \{1, g^{\pm 1}\}$.
Hieraus und aus der Definition der engen KBE folgt sofort, daß im Falle $c = 1$, also $\nu = \rho_*$, $\epsilon = P_\nu^* - Q_\nu^* Z \in \mathcal{O}_K^{*+}$ gilt.
Andernfalls, nämlich im Fall $c = g^{\pm 1}$, ist $\chi(N(P_\nu^* - Q_\nu^* Z)) = -1$ und $\epsilon^2 \in \mathcal{O}_K^{*+}$.

□

7.2.2 Satz

Ist $Z \in F(D)$ reduziert und $\rho_* := \rho_*(Z)$ die Periode der engen KBE von Z, so ist $(P^*_{\rho_*} - Q^*_{\rho_*} Z)$ bis auf einen Faktor aus $\mathbb{F}_p^*$ die positive Grundeinheit ϵ_1 von K.

BEWEIS:

Es ist zu zeigen:
Ist $\epsilon = U + V\sqrt{D} \in \mathcal{O}_K^*$ mit $|\epsilon| < 1$ und $\chi(N(\epsilon)) = 1$, so gibt es ein $i \geq 1$ und ein $a \in \mathbb{F}_p^*$ mit $\epsilon = a(P^*_{\rho_*} - Q^*_{\rho_*} Z)^i$.
Sei also $\epsilon \in \mathcal{O}_K^*$ mit $|\epsilon| < 1$ und $\chi(N(\epsilon)) = 1$.
Gesucht ist dann eine Matrix $S = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2; \mathbb{F}_p[X])$ mit

$$S \begin{pmatrix} Z \\ 1 \end{pmatrix} = \epsilon \begin{pmatrix} Z \\ 1 \end{pmatrix}.$$

Für diese Matrix muß gelten

$$S = \frac{1}{Z - \overline{Z}} \left(\begin{smallmatrix} Z & \overline{Z} \\ 1 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \overline{\epsilon} \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & -\overline{Z} \\ -1 & Z \end{smallmatrix}\right),$$

also

$$S = \frac{1}{Z - \overline{Z}} \left(\begin{smallmatrix} Z\epsilon - \overline{Z\epsilon} & -Z\overline{Z}(\epsilon - \overline{\epsilon}) \\ \epsilon - \overline{\epsilon} & -\overline{Z}\epsilon + Z\overline{\epsilon} \end{smallmatrix}\right).$$

Ist $Z = \frac{B + \sqrt{D}}{2C}$ und $\epsilon = U + V\sqrt{D}$, so erhält man

$$S = \left(\begin{smallmatrix} U + VB & -2VA \\ 2CV & U - VB \end{smallmatrix}\right),$$

da $D = B^2 - 4AC$ gilt.
Diese Matrix erfüllt

$$S \circ Z = \frac{(U + VB)(B + \sqrt{D}) - 4ACV}{V(B + \sqrt{D})2C + (U - VB)2C} \overset{D = B^2 - 4AC}{=} \frac{(U + V\sqrt{D})(B + \sqrt{D})}{2C(U + V\sqrt{D})} = \frac{B + \sqrt{D}}{2C} = Z,$$

und wegen $\chi(N(\epsilon)) = 1$ und

$$\det S = U^2 - V^2 B^2 + 4ACV^2 \overset{D = B^2 - 4AC}{=} U^2 - V^2 D = N(\epsilon)$$

gilt $S \in \mathrm{Aut}(Z)$. Nach Folgerung 6.2.4 existieren $a \in \mathbb{F}_p^*$ und $k \in \mathbb{Z}$ mit $S = a(S^*_{\rho_*})^k$.
Es gilt aber

$$S^*_{\rho_*} \begin{pmatrix} Z \\ 1 \end{pmatrix} = (Q^*_{\rho_*} Z + \eta_{\rho_* - 1} Q^*_{\rho_* - 1}) \begin{pmatrix} Z \\ 1 \end{pmatrix}$$

und somit

$$S \begin{pmatrix} Z \\ 1 \end{pmatrix} = a(Q^*_{\rho_*} Z + \eta_{\rho_* - 1} Q^*_{\rho_* - 1})^k \begin{pmatrix} Z \\ 1 \end{pmatrix}$$

mit $|Q^*_{\rho_*} Z + \eta_{\rho_* - 1} Q^*_{\rho_* - 1}| > 1$, woraus

$$\epsilon = a(Q^*_{\rho_*} Z + \eta_{\rho_* - 1} Q^*_{\rho_* - 1})^k$$

folgt. Wegen $|\epsilon| < 1$ muß demnach $k < 0$ sein. Mit denselben Schlüssen wie im Beweis des vorhergehenden Satzes zeigt man

$$\epsilon^{-1} = a^{-1}(-1)^{k\nu}(\eta_0 \cdot \ldots \cdot \eta_{\rho_* - 1})^{-k}(P^*_{\rho_*} - Q^*_{\rho_*} Z)^k,$$

d.h.

$$\epsilon = b(P^*_{\rho_*} - Q^*_{\rho_*} Z)^{-k}$$

mit $b := a(-1)^{k\nu}(\eta_0 \cdot \ldots \cdot \eta_{\rho_* - 1})^k \in \mathbb{F}_p^*$. Für $i := -k \geq 1$ ist dies die Behauptung. □

7.2.3 Beispiel

Wir betrachten ein allgemeines quadratisches Polynom $D \in \mathbb{F}_p[X]$, welches kein volles Quadrat ist. Dieses hat die Form $D = X^2 + aX + b$ mit $\frac{1}{4}a^2 - b \neq 0$. Nach Kapitel 4 ist dann

$$\sqrt{D} = X + \frac{1}{2}a + \ldots, \quad [\sqrt{D}] = X + \frac{1}{2}a.$$

Die Elemente $Z := \frac{1}{2}(\sqrt{D} + [\sqrt{D}])$ und $\frac{g}{2}(\sqrt{D} + [\sqrt{D}])$ sind demnach reduziert. Es gilt

$$[Z_0^*] = [Z] = X + \frac{1}{2}a \quad \text{und} \quad \operatorname{sgn}([Z] - Z) = \frac{1}{4}(\frac{1}{4}a^2 - b) \neq 0$$

wegen $[\sqrt{D}]^2 - D = ([\sqrt{D}] + \sqrt{D})([\sqrt{D}] - \sqrt{D}) = \frac{1}{4}a^2 - b$.

Wir unterscheiden zwei Fälle:

(i) $\frac{1}{4}a^2 - b \in \mathbb{F}_p^{*2}$.

Dann ist der erste Schritt der engen KBE gegeben durch

$$Z_1^* = \frac{\frac{1}{4}(b - \frac{1}{4}a^2)}{\frac{1}{2}(\sqrt{D} - [\sqrt{D}])} = \frac{1}{2}(\sqrt{D} + [\sqrt{D}]) = Z_0^*,$$

also $Z = \overline{[[\sqrt{D}]]}^*$ die enge KBE von Z mit $\nu(Z) = \mu_*(Z) = \rho_*(Z) = 1$. Ebenso ist dann $W = \overline{[g[\sqrt{D}]]}^*$ die enge KBE von W.

Man errechnet aus der KBE von Z, daß $P_1^* = [\sqrt{D}]$ und $Q_1^* = 1$ gilt und erhält nach Satz 7.2.2 mit

$$\epsilon_1 := (P_1^* - Q_1^* Z) = \frac{1}{2}([\sqrt{D}] - \sqrt{D}) = \overline{Z} \qquad (N(\epsilon_1) = \frac{1}{4}(\frac{1}{4}a^2 - b))$$

bis auf einen Faktor aus $\mathbb{F}_p^*$ die positive Grundeinheit von K.

(ii) $\frac{1}{4}a^2 - b \notin \mathbb{F}_p^{*2}$.

Dann ist

$$Z_1^* = gZ_0^* = W \quad \text{und} \quad Z_2^* = Z_0^*,$$

also $Z = \overline{[[\sqrt{D}], g[\sqrt{D}]]}^*$ die enge KBE von Z mit $\nu(Z) = 1$, $\mu_*(Z) = \rho_*(Z) = 2$.

Hier ist

$$P_2^* = P_1^* M_1^* + \eta_0 P_0^* = g[\sqrt{D}]^2 + \frac{g}{4}(b - \frac{1}{4}a^2)$$

und

$$Q_2^* = Q_1^* M_1^* + \eta_0 Q_0^* = g[\sqrt{D}],$$

also ist hier wiederum nach Satz 7.2.2

$$\begin{aligned} \epsilon_1 &= g[\sqrt{D}]^2 + \frac{g}{4}(b - \frac{1}{4}a^2) - \frac{g}{2}[\sqrt{D}]^2 - \frac{g}{2}[\sqrt{D}]\sqrt{D} \\ &= g\left(\frac{1}{2}([\sqrt{D}] - \sqrt{D})\right)^2 = g\overline{Z}^2 \end{aligned}$$

bis auf einen Faktor aus $\mathbb{F}_p^*$ die positive Grundeinheit von K.

Teil III
Klassenzahlformeln

8 Idealklassen

8.1 Enge Äquivalenz

Wir führen nun analog zum Zahlkörperfall für einen quadratischen Funktionenkörper den Begriff der *engen Äquivalenz* von Idealen ein, einen strengeren Äquivalenzbegriff als den in 1.2 eingeführten. Am Schluß des Kapitels definieren wir eine Bijektion zwischen den engen Äquivalenzklassen von gebrochenen Idealen eines reell-quadratischen Funktionenkörpers und den Äquivalenzklassen reduzierter Funktionen der Diskriminante D.

8.1.1 Definition

Zwei Ideale $\mathfrak{a}$ und $\mathfrak{b} \in I(K)$ heißen *eng äquivalent* ($\mathfrak{a} \sim_+ \mathfrak{b}$), falls ein $\lambda \in K^*$ mit $\chi(N(\lambda)) = 1$ existiert mit

$$\mathfrak{a} = (\lambda)\mathfrak{b}.$$

8.1.2 Folgerung

Wie die weiten, so bilden auch die engen Äquivalenzklassen eine Gruppe bezüglich der Ideal-Multiplikation, die *enge Idealklassengruppe* $C^+(K) = I(K)/H^+(K)$ von $\mathcal{O}_K$ mit

$$H^+(K) := \{(\lambda) \mid \chi(N(\lambda)) = 1\},$$

der *engen Hauptidealgruppe*.
Aus der Endlichkeit der *weiten Klassenzahl* $h(K) = |C(K)|$ (s. z.B. [A], S. 180/194) folgt sofort die Endlichkeit der *engen Klassenzahl* $h^+(K) := |C^+(K)|$. Diese ergibt sich auch später aus der Isomorphie $(F(D)/\sim_+) \simeq (I(K)/\sim_+)$ und Satz 6.2.4 (iii).
Statt $h(k(\sqrt{D}))$ bzw. $h^+(k(\sqrt{D}))$ benutzen wir später auch die Bezeichnungen $h(D)$ bzw. $h^+(D)$.

Zunächst wollen wir uns mit der Frage beschäftigen, wann der enge mit dem weiten Äquivalenzbegriff zusammenfällt.

Hier untersuchen wir zunächst den reell-quadratischen Fall.

8.2 Der Äquivalenzindex eines reell-quadratischen Funktionenkörpers

8.2.1 Definition

Ist K ein reell-quadratischer Funktionenkörper, so heißt

$$Q_K := 3 - |\mathcal{O}_K^*/\mathcal{O}_K^{*+}| = \begin{cases} 1, & \text{falls ein } \epsilon \in \mathcal{O}_K^* \text{ existiert mit } \chi(N(\epsilon)) = -1 \\ 2, & \text{falls } \chi(N(\epsilon)) = 1 \text{ für alle } \epsilon \in \mathcal{O}_K^*. \end{cases}$$

der *Äquivalenzindex* von K. Diese Bezeichnung basiert auf dem

8.2.2 Lemma

Es sei K ein reell-quadratischer Funktionenkörper. Dann sind äquivalent:

(i) Es existiert ein $\epsilon \in \mathcal{O}_K^*$ mit $\chi(N(\epsilon)) = -1$.

(ii) $Q_K = 1$.

(iii) Die enge Äquivalenz fällt mit der weiten Äquivalenz zusammen.

(iv) Es gilt $N(\epsilon_0) = g$ für die Grundeinheit ϵ_0 von K.

BEWEIS:

(i) $\Leftrightarrow$ (ii) ist klar.

(i) $\Rightarrow$ (iii) Es sei $\mathfrak{a} \sim \mathfrak{b}$. Dann existiert ein $\lambda \in K$ mit $\mathfrak{a} = (\lambda)\mathfrak{b}$.
Ist $\chi(N(\lambda)) = 1$, so ist $\mathfrak{a} \sim_+ \mathfrak{b}$. Ist jedoch $\chi(N(\lambda)) = -1$, so gilt

$$\mathfrak{a} = (\lambda)\mathfrak{b} = (\epsilon\lambda)\mathfrak{b}$$

mit einem $\epsilon \in \mathcal{O}_K^*$ und $\chi(N(\epsilon)) = -1$.
Es ist $\chi(N(\epsilon\lambda)) = 1$ und wiederum $\mathfrak{a} \sim_+ \mathfrak{b}$, die engen und weiten Äquivalenzklassen fallen demnach zusammen.

(iii) $\Rightarrow$ (iv) Wäre $N(\epsilon_0) = 1$ für die Grundeinheit $\epsilon_0 \in \mathcal{O}_K^*$, so würde für alle $\epsilon \in \mathcal{O}_K^*$ gelten $\chi(N(\epsilon)) = 1$. Ist $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$, so ist $\mathfrak{a} \sim (u)\mathfrak{a}$ für alle ganzen $\mathfrak{a} \in I(K)$. Fallen die engen und weiten Klassen zusammen, so folgt auch $\mathfrak{a} \sim_+ (u)\mathfrak{a}$, d.h. es existiert ein $\mu' \in K^*$ mit $\chi(N(\mu')) = 1$ und $\mathfrak{a} = (\mu' u)\mathfrak{a}$. Demnach gilt $\mu' u \in \mathcal{O}_K^*$ und $\chi(N(\mu' u)) = -1$, denn $\chi(N(u)) = -1$. Ein Widerspruch zu $\chi(N(\epsilon)) = 1$ für alle $\epsilon \in \mathcal{O}_K^*$.

(iv) $\Rightarrow$ (i) Es ist $\chi(N(\epsilon_0)) = -1$.

□

8.2.3 Lemma

Sind im reell-quadratischen Fall enge und weite Äquivalenzklassen verschieden, so zerfällt jede weite Äquivalenzklasse A in zwei disjunkte enge Äquivalenzklassen A' und uA', wobei $u \in K^*$ ein nach Lemma 4.1.6 (i) in jedem reell-quadratischen Funktionenkörper existierendes Element mit $\chi(N(u)) = -1$ ist. Zusammenfassend gilt also

$$h(K) = \frac{1}{Q_K} h^+(K).$$

BEWEIS:

Es sei $A := [\mathfrak{a}] = \{\mathfrak{b} \in I(K) \mid \mathfrak{b} \sim \mathfrak{a}\}$ eine weite Äquivalenzklasse. Ist dann $u \in K^*$ so gewählt, daß $\chi(N(u)) = -1$ gilt, so ist

$$A = A' \cup uA' \quad \text{und} \quad A' \cap uA' = \emptyset$$

mit $A' := \{\mathfrak{b} \in I(K) \mid \mathfrak{b} \sim_+ \mathfrak{a}\}$.
Ist $\mathfrak{c} \in A' \cup uA'$, so gilt trivialerweise $\mathfrak{c} \in A$. Ist andererseits $\mathfrak{c} \in A$, also $\mathfrak{c} \sim \mathfrak{a}$, so gilt entweder $\mathfrak{c} \sim_+ \mathfrak{a}$, also $\mathfrak{c} \in A'$, oder es existiert ein $\lambda \in K^*$ mit $\chi(N(\lambda)) = -1$

und $\mathfrak{c} = \lambda\mathfrak{a} = u\frac{\lambda}{u}\mathfrak{a}$ mit $\frac{\lambda}{u}\mathfrak{a} \in A'$, also $\mathfrak{c} \in uA'$. Wäre $A' \cap uA' \neq \emptyset$, so müßte – wie schon im Beweis (iii) $\Rightarrow$ (iv) des vorangegangenen Lemmas – ein $\epsilon \in \mathcal{O}_K^*$ existieren mit $\chi(N(\epsilon)) = -1$, was aber nicht sein kann, da enge und weite Klassen verschieden sind, demnach sind A' und uA' disjunkt. □

8.3 Enge und weite Äquivalenz in imaginär-quadratischen Funktionenkörpern

8.3.1 Bemerkung

Da nach Satz 4.2.1 in imaginär-quadratischen Erweiterungen von k (mit Ausnahme des Falles $K = k(\sqrt{g})$) die trivialen Einheiten, nämlich die Elemente aus $\mathbb{F}_p^*$ die einzigen Einheiten sind, sind hier wegen $\chi(N(\epsilon)) = 1$ für alle $\epsilon \in \mathcal{O}_K^*$ die enge und weite Klassenzahl genau dann verschieden, wenn es ein Element $u \in \mathcal{O}_K$ gibt mit $\chi(N(u)) = -1$.

Im Fall $D = g$ haben nach Proposition 4.2.1 die Einheiten $\epsilon \in \mathcal{O}_K$ die Form $\epsilon = a + b\sqrt{g} \in \mathcal{O}_K^*$ mit $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p \backslash (0, 0)$. Unter diesen kann man immer Einheiten mit $\chi(N(\epsilon)) = -1$ finden, was zur Folge hat, daß enge und weite Klassen zusammenfallen. Dies sieht man wie folgt ein.

Im Fall $\chi(-1) = 1$ ist offensichtlich $\epsilon := \sqrt{g}$ eine Einheit mit $\chi(N(\epsilon)) = \chi(-g) = -1$.

Ist hingegen $\chi(-1) = -1$, so wählt man wie im Beweis des Lemmas 4.1.6 ein $h \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$ mit $\chi(h - 1) = 1$. Da g eine Primitivwurzel mod p ist, existiert ein $k \in \mathbb{N}$ mit $h = g^{2k+1}$. Mit $\epsilon := 1 + g^k\sqrt{g}$ gilt dann

$$\chi(N(\epsilon)) = \chi(1 - (g^k)^2 g) = \chi(1 - g^{2k+1}) = \chi(1 - h) \overset{\chi(-1)=-1}{=} -\chi(h - 1) = -1.$$

Man erhält somit die

8.3.2 Folgerung

In den Bezeichnungen von Lemma 4.1.6 gilt $h^+(K) = h(K)$ genau in den Fällen (ii) (1) und (2) und im Fall $D = g$. In allen anderen imaginär-quadratischen Fällen gilt $h^+(K) = 2h(K)$.

BEWEIS:

Dies folgt sofort aus Lemma 4.1.6 (ii) in Verbindung mit Bemerkung 8.3.1.

□

8.4 Orientierte Basen

Analog zum klassischen Fall führen wir den Begriff der orientierten Basis ein. Dieser wird wie schon bei [Zag2] im Zahlkörperfall auch für die Konstruktion einer Bijektion zwischen $F(D)/\sim_+$ und $C^+(K)$ im Funktionenkörper ausschlaggebend sein.

8.4.1 Definition

Eine $\mathbb{F}_p[X]$-Basis $(\omega_1, \omega_2) \in K^2$ eines Ideals $\mathfrak{a} \in I(K)$ heißt *orientiert*, falls

$$\chi(\overline{\omega_1}\omega_2 - \omega_1\overline{\omega_2}) = 1$$

gilt.

8.4.2 Satz

Jedes Ideal $\mathfrak{a} \in I(K)$ besitzt eine orientierte Basis.

BEWEIS:

Ist $(\omega_1, \omega_2) \in K^2$ eine nicht-orientierte Basis von $\mathfrak{a}$, so ist

$$\begin{pmatrix} \omega_1^* \\ \omega_2^* \end{pmatrix} := \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

eine orientierte Basis, falls $a \in \mathbb{F}_p^*$ mit $\chi(a) = -1$ ist.
Denn es gilt $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{GL}(2; \mathbb{F}_p[X])$ mit $\chi(\det T) = -1$. □

8.4.3 Lemma

Es seien $(\omega_1, \omega_2), (\omega_1', \omega_2') \in K^2$ Basen von $\mathfrak{a} \in I(K)$, von denen die Basis (ω_1, ω_2) orientiert sei.
Es sei weiterhin $T \in \mathrm{GL}(2; \mathbb{F}_p[X])$ die Übergangsmatrix mit $\left(\begin{smallmatrix} \omega_1' \\ \omega_2' \end{smallmatrix}\right) = T \left(\begin{smallmatrix} \omega_1 \\ \omega_2 \end{smallmatrix}\right)$. Dann gilt

$$(\omega_1', \omega_2') \text{ ist eine orientierte Basis von } \mathfrak{a} \quad \Leftrightarrow \quad T \in \mathrm{SL}(2; \mathbb{F}_p[X]).$$

BEWEIS:

Es ist

$$\overline{\omega_1'}\omega_2' - \omega_1'\overline{\omega_2'} = \det \left(\begin{smallmatrix} \overline{\omega_1'} & \omega_1' \\ \overline{\omega_2'} & \omega_2' \end{smallmatrix}\right) = \det \left(T \left(\begin{smallmatrix} \overline{\omega_1} & \omega_1 \\ \overline{\omega_2} & \omega_2 \end{smallmatrix}\right)\right) = (\det T)(\overline{\omega_1}\omega_2 - \omega_1\overline{\omega_2}),$$

woraus die Behauptung folgt. □

8.4.4 Lemma

(i) Ist $(\omega_1, \omega_2) \in K^2$ eine Basis von $\mathfrak{a}$, so ist für $\lambda \in K^*$ das Tupel $(\lambda\omega_1, \lambda\omega_2) \in K^2$ eine Basis von $\lambda\mathfrak{a}$.

(ii) Ist (ω_1, ω_2) eine orientierte Basis des Ideals $\mathfrak{a} \in I(K)$ und $\lambda \in K^*$. Dann gilt

$$\chi(N(\lambda)) = 1 \quad \Leftrightarrow \quad (\lambda\omega_1, \lambda\omega_2) \text{ ist orientierte Basis von } \lambda\mathfrak{a}.$$

(iii) Ist (ω_1, ω_2) eine nicht-orientierte Basis von $\mathfrak{a} \in I(K)$ und $\lambda \in K^*$, so gilt

$$\chi(N(\lambda)) = -1 \quad \Leftrightarrow \quad (\lambda\omega_1, \lambda\omega_2) \text{ ist orientierte Basis von } \lambda\mathfrak{a}.$$

BEWEIS:

Zu (i) vergleiche man [A], S. 173 (6). Die Aussagen (ii) und (iii) folgen in Verbindung mit (i) und der Multiplikativität von χ unmittelbar aus

$$\overline{\lambda\omega_1}\lambda\omega_2 - \lambda\omega_1\overline{\lambda\omega_2} = N(\lambda)(\overline{\omega_1}\omega_2 - \omega_1\overline{\omega_2}).$$

□

8.5 Idealnorm

8.5.1 Definition

Ist $\mathfrak{a} =< \omega_1, \omega_2 >$ ein gebrochenes Ideal von K, so heißt der Wert

$$N(\mathfrak{a}) := a_{\omega_1,\omega_2} \frac{\overline{\omega_1}\omega_2 - \omega_1\overline{\omega_2}}{\sqrt{D}} \in k^*$$

die *Norm* von $\mathfrak{a}$, wobei $a_{\omega_1,\omega_2} \in \mathbb{F}_p^*$ so gewählt sei, daß $\operatorname{sgn}(N(\mathfrak{a})) = 1$ gilt.

Daß $N(\mathfrak{a}) \in k^*$ für jedes $\mathfrak{a} \in I(K)$ gilt, liegt an der Eigenschaft $\overline{N(\mathfrak{a})} = N(\mathfrak{a})$, da es sich bei K/k um eine Galois-Erweiterung vom Grad 2 handelt. Aus dem selben Grund würde $\frac{\omega_1}{\omega_2} \in k$ aus $N(\mathfrak{a}) = 0$ folgen, was aufgrund der $\mathbb{F}_p[X]$-linearen Unabhängigkeit von ω_1 und ω_2 nicht möglich ist.

Ist $\mathfrak{a} =< 2CS, S(B + \sqrt{D}) >$ ein ganzes Ideal in adaptierter Basisdarstellung, so erhält man

$$N(\mathfrak{a}) = \frac{S^2C}{\operatorname{sgn}(S^2C)} \in \mathbb{F}_p[X].$$

Im Fall eines Hauptideals $(\alpha) = (X + Y\sqrt{D})$ mit $X, Y \in k$ gilt

$$N((\alpha)) = \frac{N(\alpha)}{\operatorname{sgn} N(\alpha)} = \frac{X^2 - Y^2D}{\operatorname{sgn}(X^2 - Y^2D)}.$$

8.5.2 Lemma

Ist $\mathfrak{a} \in I(K)$, und definiert man das zu $\mathfrak{a}$ *konjugierte Ideal* $\overline{\mathfrak{a}}$ durch $\overline{\mathfrak{a}} := \{\overline{\alpha} \mid \alpha \in \mathfrak{a}\}$, so gilt

$$\mathfrak{a}\overline{\mathfrak{a}} = (N(\mathfrak{a}))$$

und

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$$

für alle $\mathfrak{b} \in I(K)$.

BEWEIS:

s. [A], S.168. □

8.5.3 Folgerung

Ist $A^+ = [\mathfrak{a}]^+ \in C^+(K)$ (bzw. $A = [\mathfrak{a}] \in C(K)$) eine (enge) Idealklasse, so ist die inverse Klasse $(A^+)^{-1}$ bzw. A^{-1} gegeben durch $[\overline{\mathfrak{a}}]^{(+)}$.

BEWEIS:

Dies folgt sofort aus Lemma 8.5.2. □

8.5.4 Lemma

Ist $\mathfrak{p}$ ein Primideal von K, so existiert genau ein normiertes Primpolynom $P \in \mathbb{F}_p[X]$ mit $\mathfrak{p} \mid (P)$. Für dieses Polynom P gilt dann $N(\mathfrak{p}) = P$ bzw. $N(\mathfrak{p}) = P^2$, je nachdem, ob die Kongruenz $X^2 \equiv D \mod P$ lösbar ist oder nicht.

BEWEIS:

s. [A], S. 169/70. □

8.5.5 Lemma

Ist $\mathfrak{a} \in I(K)$ ein gebrochenes Ideal und $\lambda \in \mathfrak{a}$, so gilt

$$\frac{N(\lambda)}{N(\mathfrak{a})} \in \mathbb{F}_p[X].$$

BEWEIS:

Ist $\mathfrak{a} \in I(K)$, so existiert ein $d \in \mathcal{O}_K \backslash \{0\}$ mit $d\mathfrak{a} \subseteq \mathcal{O}_K$. Ist $\lambda \in \mathfrak{a}$, so gilt $d\mathfrak{a} \mid (d\lambda)$, und beide Ideale sind ganz. Es existiert also ein $\mathfrak{b} \subseteq \mathcal{O}_K$ mit $d\mathfrak{a}\mathfrak{b} = (d\lambda)$ und

$$N((d))N(\mathfrak{a})N(\mathfrak{b}) = N((d))N((\lambda)).$$

Da $\mathfrak{b} \subseteq \mathcal{O}_K$ und $N((\lambda)) = aN(\lambda)$ für ein $a \in \mathbb{F}_p^*$ gilt, ist dann

$$\frac{N((\lambda))}{N(\mathfrak{a})} = \frac{aN(\lambda)}{N(\mathfrak{a})} = N(\mathfrak{b}) \in \mathbb{F}_p[X].$$

□

8.6 Konstruktion einer Bijektion zwischen $C^{(+)}(K)$ und $F(D)/\sim_{(+)}$

Wie zu Beginn angekündigt, wollen wir nun eine Bijektion zwischen den (engen) Idealklassen eines reell-quadratischen Funktionenkörpers $K = k(\sqrt{D})$ und den (engen) Äquivalenzklassen von Funktionen der Diskriminante D konstruieren.
Die schon in der Überschrift gebrauchte Bezeichnung $\sim_{(+)}$ bzw. $C^{(+)}(K)$ wird hier benutzt, um zu verdeutlichen, daß wir sowohl die weite als auch die enge Äquivalenz von Idealklassen bzw. Funktionen der Diskriminante D betrachten. Die eingeklammerten Bemerkungen – vor allem im Beweis des Satzes 8.6.3 – beziehen sich dann immmer auf die Betrachtung der engen Klasseneinteilung.

Wir betrachten die Abbildung

$$\varphi : I(K) \to K^*/\sim_{(+)}$$

mit $\varphi(\mathfrak{a}) = \varphi(<\omega_1, \omega_2>) := [\frac{\omega_2}{\omega_1}]$, wobei $(\omega_1, \omega_2) \in K^2$ eine (orientierte) Basis von $\mathfrak{a} \in I(K)$ sei.
Obige Abbildung ist wohldefiniert, d.h. unabhängig von der Wahl der Basis von $\mathfrak{a}$, denn es gilt das

8.6.1 Lemma

Sind (ω_1, ω_2), $(\omega_1^*, \omega_2^*) \in K^2$ zwei Basen von $\mathfrak{a} \in I(K)$ mit

$$\begin{pmatrix} \omega_1^* \\ \omega_2^* \end{pmatrix} = T \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

und $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2; \mathbb{F}_p[X])$, so ist

$$\omega^* := \frac{\omega_2^*}{\omega_1^*} = \left(\begin{smallmatrix} \delta & \gamma \\ \beta & \alpha \end{smallmatrix}\right) \circ \omega$$

mit $\omega := \frac{\omega_2}{\omega_1}$, also $\omega^* \sim \omega$.

BEWEIS:

$$\omega^* = \frac{\omega_2^*}{\omega_1^*} = \frac{\gamma\omega_1 + \delta\omega_2}{\alpha\omega_1 + \beta\omega_2} = \frac{\gamma + \delta\frac{\omega_2}{\omega_1}}{\alpha + \beta\frac{\omega_2}{\omega_1}}.$$

□

Hieraus ergibt sich sofort die

8.6.2 Folgerung

Sind (ω_1, ω_2), $(\omega_1^*, \omega_2^*) \in K^2$ zwei orientierte Basen von $\mathfrak{a} \in I(K)$, so ist $\omega^* \sim_+ \omega$, denn die Übergangsmatrix zwischen zwei orientierten Basen ist ein Element von $\mathrm{SL}(2; \mathbb{F}_p[X])$.

8.6.3 Satz

φ induziert eine Abbildung

$$\Phi : C^{(+)}(K) \to F(D)/\sim_{(+)}$$

mit $\Phi([< \omega_1, \omega_2 >]) := [\frac{\omega_2}{\omega_1}]$.
Diese Abbildung ist bijektiv, und ist $u \in \mathcal{O}_K$ ein Element mit $\chi(N(u)) = -1$, so ist

$$\Psi : F(D)/\sim_{(+)} \to C^{(+)}(K)$$

$$\left[W = \frac{B + \sqrt{D}}{2C}\right] \mapsto [u_W < 2C, B + \sqrt{D} >]$$

mit

$$u_W := \begin{cases} 1, & \text{falls } (2C, B + \sqrt{D}) \text{ orientiert,} \\ u, & \text{falls } (2C, B + \sqrt{D}) \text{ nicht orientiert.} \end{cases}$$

ihre Umkehrabbildung.
Das Element u_W werde natürlich nur für den Fall $\Psi : F(D)/\sim_+ \to C^+(K)$ benutzt.

BEWEIS:

Zunächst ist zu zeigen, daß für zwei (orientierte) Basen (ω_1, ω_2), $(\omega_1', \omega_2') \in K^2$ mit $< \omega_1, \omega_2 > \sim_{(+)} < \omega_1', \omega_2' >$ auch $\frac{\omega_2}{\omega_1} \sim_{(+)} \frac{\omega_2'}{\omega_1'}$ gilt.
Es gibt also ein $\lambda \in K^*$ $(\chi(N(\lambda)) = 1)$ mit

$$< \omega_1, \omega_2 > < \omega_1', \omega_2' >^{-1} = (\lambda).$$

Aus Lemma 8.4.4 (i) folgt dann, daß $(\lambda\omega_1', \lambda\omega_2')$ eine Basis von $< \omega_1, \omega_2 >$ ist, welche im Fall $\chi(N(\lambda)) = 1$ nach Lemma 8.4.4 (ii) orientiert ist. Aus Lemma 8.6.1 bzw. Folgerung 8.6.2 ergibt sich dann

$$\frac{\omega_2}{\omega_1} \sim_{(+)} \frac{\omega_2'}{\omega_1'}.$$

Für die Wohldefiniertheit der Umkehrabbildung ist folgende Implikation zu zeigen:

$$W' \sim_{(+)} W \quad \Rightarrow \quad u_{W'} < 2C', B' + \sqrt{D} > \sim_{(+)} u_W < 2C, B + \sqrt{D} > .$$

Dazu sei

$$W' = \frac{\alpha W + \beta}{\gamma W + \delta} = \frac{\alpha(B + \sqrt{D}) + \beta 2C}{\gamma(B + \sqrt{D}) + \delta 2C}$$

mit $T := \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2; \mathbb{F}_p[X])$ bzw. $\in \mathrm{SL}(2; \mathbb{F}_p[X])$. Definiert man

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} := \frac{u_{W'}(B' + \sqrt{D})}{\alpha(B + \sqrt{D}) + \beta 2C} \begin{pmatrix} \gamma(B + \sqrt{D}) + \delta 2C \\ \alpha(B + \sqrt{D}) + \beta 2C \end{pmatrix} = u_{W'} \begin{pmatrix} 2C' \\ B' + \sqrt{D} \end{pmatrix}$$

und

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} := \left(\begin{smallmatrix} \delta & \gamma \\ \beta & \alpha \end{smallmatrix}\right) \begin{pmatrix} u_W \cdot 2C \\ u_W(B + \sqrt{D}) \end{pmatrix},$$

so ist (ω_1', ω_2') eine (orientierte) Basis von $u_{W'} < 2C', B' + \sqrt{D} >$ und (ω_1, ω_2) eine (orientierte) Basis von $u_W < 2C, B + \sqrt{D} >$ mit

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \frac{u_{W'} u_W^{-1}(B' + \sqrt{D})}{\alpha(B + \sqrt{D}) + \beta 2C} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Mit $\lambda := \frac{u_{W'} u_W^{-1}(B' + \sqrt{D})}{\alpha(B + \sqrt{D}) + \beta 2C}$ folgt aus Lemma 8.4.4 (ii) im Falle der Orientiertheit der Basen die Eigenschaft $\chi(N(\lambda)) = 1$ und somit

$$< \omega_1', \omega_2' > \sim_{(+)} < \omega_1, \omega_2 > .$$

Weiterhin gilt

$$\Phi(\Psi([\frac{B + \sqrt{D}}{2C}])) = \Phi([u_W < 2C, B + \sqrt{D} >]) = \left[\frac{u_W(B + \sqrt{D})}{u_W 2C}\right] = \left[\frac{B + \sqrt{D}}{2C}\right].$$

Zur Surjektivität von Ψ sei $\mathfrak{a} =< \omega_1, \omega_2 >$ ein Ideal mit einer (orientierten) Basis $(\omega_1, \omega_2) \in K^2$. Dann definieren wir

$$C := \frac{a_{\omega_1,\omega_2} N(\omega_1)}{N(\mathfrak{a})},\ A := \frac{a_{\omega_1,\omega_2} N(\omega_2)}{N(\mathfrak{a})} \text{ und } B := \frac{a_{\omega_1,\omega_2}(\omega_1 \overline{\omega_2} + \overline{\omega_1}\omega_2)}{N(\mathfrak{a})}$$

mit $a_{\omega_1,\omega_2} \in \mathbb{F}_p^*$ wie in Definition 8.5.1. Es gilt dann

$$B^2 - 4AC = \frac{(\omega_1 \overline{\omega_2} - \overline{\omega_1}\omega_2)^2}{N(\mathfrak{a})^2} = D.$$

Da wegen Lemma 8.5.5 $A, C \in \mathbb{F}_p[X]$ gilt, folgt aus $B^2 - 4AC = D \in \mathbb{F}_p[X]$ auch $B \in \mathbb{F}_p[X]$. Weiterhin rechnet man nach, daß

$$\frac{B + \sqrt{D}}{2C} = \frac{\omega_2}{\omega_1}$$

ist.
Um $\Psi([\frac{B+\sqrt{D}}{2C}]) = [< \omega_1, \omega_2 >]$ zu zeigen, stellen wir zunächst fest, daß die Basis $(2C, B + \sqrt{D})$ wegen $\operatorname{sgn}\sqrt{D} = 1$ genau dann orientiert ist, wenn $\chi(C) = 1$ gilt.
In unserem Fall gilt

$$\chi(C) = \chi(N(\omega_1))\chi(a_{\omega_1,\omega_2})\chi(N(\mathfrak{a})) = \chi(N(\omega_1))\chi(a_{\omega_1,\omega_2}) = \chi(N(\omega_1)),$$

denn $a_{\omega_1,\omega_2} \in \mathbb{F}_p^{*2}$ nach Definition 8.5.1 und aufgrund der Orientiertheit der Basis (ω_1, ω_2).

Es ist also $\Psi([\frac{B+\sqrt{D}}{2C}]) = [\mathfrak{a}] = [u_W < 2C, B+\sqrt{D} >]$ mit

$$u_W = \begin{cases} u, & \text{falls } \chi(N(\omega_1)) = -1 \text{ und} \\ 1, & \text{falls } \chi(N(\omega_1)) = 1. \end{cases}$$

Es gilt weiterhin

$$< \omega_1, \omega_2 >= (\frac{N(\mathfrak{a})}{2a_{\omega_1,\omega_2}\overline{\omega_1}}) < 2C, B+\sqrt{D} >$$

mit

$$\chi(\frac{N(\mathfrak{a})}{2a_{\omega_1,\omega_2}\overline{\omega_1}}) = \chi(N(\omega_1)),$$

wie man leicht nachrechnet.
Also ist in beiden oben genannten Fällen $\mathfrak{a} \sim_{(+)} < \omega_1, \omega_2 >$, was noch zu zeigen war.
□

Diese Isomorphie bietet uns nun neben Lemma 8.2.2 für den reell-quadratischen Funktionenkörper ein weiteres Hilfsmittel zur Charakterisierung, wann enge und weite Äquivalenzklassen von Idealen $\in I(K)$ bzw. Funktionen der Diskriminante D zusammenfallen.

8.6.4 Satz

Für einen reell-quadratischen Funktionenkörper $K = k(\sqrt{D})$ sind die folgenden Aussagen äquivalent:

(i) Die engen und weiten Äquivalenzklassen von Funktionen der Diskriminante D bzw. von Idealen aus $I(K)$ fallen zusammen.

(ii) Es gilt $\mu_*(W) = 2\nu(W)$ für alle reduzierten Funktionen $W \in F(D)$.

(iii) Zu jeder reduzierten Funktion $W \in F(D)$ existiert ein $T \in \mathrm{GL}(2; \mathbb{F}_p[X])\backslash\mathrm{SL}(2; \mathbb{F}_p[X])$ mit $W = T \circ W$.

BEWEIS:
(i) $\Rightarrow$ (ii) Sei $W \in F(D)$ reduziert. Dann ist auch

$$W' := \begin{cases} gW, & \text{falls sgn } W = 1, \\ g^{-1}W, & \text{falls sgn } W = g \end{cases}$$

reduziert, und es gilt $W \sim W'$, denn

$$W' = \begin{pmatrix} g^{\pm 1} & 0 \\ 0 & 1 \end{pmatrix} \circ W.$$

Wegen (i) gilt auch $W' \sim_+ W$, d.h. W und W' liegen nach Satz 6.2.3 im selben Zykel reduzierter Elemente. Da W und W' sich nur um den Faktor $g^{\pm 1}$ unterscheiden, muß $W' = W_0^* = W$ oder $W' = W_\nu^*$ gelten. Wegen $W \neq W'$ und $g^{\pm 1} \in \mathbb{F}_p^*\backslash\mathbb{F}_p^{*^2}$ folgt dann aus Satz 5.4.9 $\frac{\mu_*}{\nu} = 2$ mit der Quadratperiode μ_* der engen KBE auf Definition 5.3.3.

(ii) $\Rightarrow$ (iii) Sei $W \in F(D)$. In der engen KBE von W ist $W_\nu^* \neq W$ nach Voraussetzung, also gilt $W_\nu^* = W'$, es existiert demnach ein $S \in \mathrm{SL}(2;\mathbb{F}_p[X])$ mit $W_\nu^* = S \circ W$, also

$$W = \underbrace{\begin{pmatrix} g^{\pm 1} & 0 \\ 0 & 1 \end{pmatrix}}_{=:S'} S \circ W,$$

was mit $T := S'S \in \mathrm{GL}(2;\mathbb{F}_p[X])\backslash\mathrm{SL}(2;\mathbb{F}_p[X])$ die Behauptung ist.

(iii) $\Rightarrow$ (i) Aufgrund der Isomorphie $F(D)/\sim_{(+)} \simeq I(K)/\sim_{(+)}$ reicht es, die Aussage $W \sim Z \;\Rightarrow\; W \sim_+ Z$ für alle $W, Z \in F(D)$ zu zeigen.
Sei also $W \sim Z$, d.h. es existiert ein $S \in \mathrm{GL}(2;\mathbb{F}_p[X])$ mit $W = S \circ Z$. Ist $S \in \mathrm{SL}(2;\mathbb{F}_p[X])$, so sind wir fertig. Ist $S \notin \mathrm{SL}(2;\mathbb{F}_p[X])$, so weiß man nach Voraussetzung, daß eine Matrix $T \in \mathrm{GL}(2;\mathbb{F}_p[X])\backslash\mathrm{SL}(2;\mathbb{F}_p[X])$ existiert mit $W = T \circ W = TS \circ Z$ und $TS \in \mathrm{SL}(2;\mathbb{F}_p[X])$, es gilt also $W \sim_+ Z$.

□

8.6.5 Beispiel

Es sei $D = X^2 + aX + b$ mit $\frac{1}{4}a^2 - b \neq 0$ wie in Beispiel 7.2.3 gewählt. ARTIN stellte fest, daß durch $Z_c = c([\sqrt{D}] + \sqrt{D})$ $(c \in \mathbb{F}_p^*)$ alle Artin-reduzierten Funktionen gegeben sind (s. [A], S.195).
Daraus folgt sofort, daß es nur zwei reduzierte Funktionen in K gibt, nämlich die Funktionen $Z = Z_{\frac{1}{2}}$ und $W = Z_{\frac{g}{2}}$ aus Beispiel 7.2.3. Denn für diese ist $\operatorname{sgn} Z, \operatorname{sgn} W \in \{1, g\}$, und sie sind offensichtlich im weiteren Sinne äquivalent. Es gilt somit $h(K) = 1$.
Aus Satz 8.6.4 zusammen mit den Beobachtungen in 7.2.3 erhält man nun, daß in K enge und weite Äquivalenzklassen von Funktionen genau dann zusammenfallen, wenn $\frac{1}{4}a^2 - b \notin \mathbb{F}_p^{*2}$ gilt. Denn dann bestehen für die beiden einzigen reduzierten Funktionen $Z, W \in K$ die Verhältnisse $\mu_*(Z) = \rho_*(Z) = 2\nu(Z)$ und $\mu_*(W) = \rho_*(W) = 2\nu(W)$. Es gilt demnach 8.6.4 (ii).
In diesem Fall ist $h^+(K) = h(K) = 1$. Man hat

$$Z = S_1^* \circ gZ = S_1^* \circ W = S_1^* \cdot \begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix} \circ Z,$$

d.h. $Z \sim_+ W$, und mit

$$T := S_1^* \cdot \left(\begin{smallmatrix} g & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2;\mathbb{F}_p[X])\backslash\mathrm{SL}(2;\mathbb{F}_p[X])$$

ist eine Matrix T der in (iii) beschriebenen Form mit Fixpunkt Z gefunden.
Ist hingegen $\frac{1}{4}a^2 - b \in \mathbb{F}_p^{*2}$, so gilt $h^+(K) = 2h(K) = 2$.

8.6.6 Definition

Ein Ideal $\mathfrak{a} \in I(K)$ heißt *(Artin-)reduziert*, wenn es eine Basis (ω_1, ω_2) besitzt, deren zugehörige Funktion $\frac{\omega_2}{\omega_1} \in F(D)$ (Artin-)reduziert ist.

Aus der Endlichkeit der (Artin-)reduzierten Funktionen aus $F(D)$ (s. Satz 6.1.2) zusammen mit der oben definierten Bijiektion folgt sofort der

8.6.7 Satz

Es gibt nur endlich viele (A-)red. Ideale, und jedes Ideal $\mathfrak{a}$ ist (eng) äquivalent zu einem (A-)red. Ideal.

Insbesondere haben wir nach Satz 6.2.4 (iii) erneut gezeigt, daß die (enge) Klassenzahl $h^{(+)}(K)$ endlich ist.

8.6.8 Lemma

Ein Ideal $\mathfrak{a} =< 2C, B+\sqrt{D} >$ ist A-red. genau dann, wenn $|N(\mathfrak{a})| = |4C| = |C| < |\sqrt{D}|$ gilt.

BEWEIS:

"$\Leftarrow$" Dies folgt aus der Reduziertheitsbedingung in [A], S. 194.

"$\Rightarrow$" Existiert eine Basis $(2C', B'+\sqrt{D})$ von $\mathfrak{a}$, deren zugehörige Funktion reduziert ist, so gilt $|C'| < |\sqrt{D}|$. Es ist aber weiterhin

$$\begin{pmatrix} 2C \\ B+\sqrt{D} \end{pmatrix} = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \begin{pmatrix} 2C' \\ B'+\sqrt{D} \end{pmatrix}$$

mit $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2; \mathbb{F}_p[X])$. Hieraus folgt

$$|N(< 2C, B+\sqrt{D} >)| = |C'| < |\sqrt{D}|.$$

□

8.6.9 Lemma

Ist $F \in \mathbb{F}_p[X]$, so existiert in jeder (engen oder auch weiten) Idealklasse ein ganzes Ideal $\mathfrak{a}$ mit $(\mathfrak{a}, (F)) = 1$.

BEWEIS:

Es genügt zu zeigen, daß in jeder (engen) Idealklasse ein Ideal $\mathfrak{a} =< 2C, B+\sqrt{D} >$ mit $D = B^2 - 4AC$, $A, B, C \in \mathbb{F}_p[X]$ und $(C, F) = 1$ existiert.
Es sei zunächst $\mathfrak{a} =< 2C, B+\sqrt{D} >$ ein ganzes Ideal, welches aufgrund der Isomorphie $I(K)/\sim_{(+)} \simeq C^{(+)}(K)$ in jeder (engen) Äquivalenzklasse existiert.
Ist nun $(C, F) = 1$, so auch $(\mathfrak{a}, (F)) = 1$, und das Lemma ist bewiesen.
Ist hingegen $(C, F) \neq 1$, so zeigen wir, daß es Elemente $\alpha, \beta, \gamma, \delta \in \mathbb{F}_p[X]$ gibt, so daß $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2; \mathbb{F}_p[X])$ gilt und mit

$$\omega' := T \circ \frac{B+\sqrt{D}}{2C} = \frac{B_1+\sqrt{D}}{2C_1}$$

das Polynom

$$(*) \quad C_1 = (\det T)^{-1}(A\gamma^2 + B\gamma\delta + C\delta^2), \quad \text{(vgl. [A], S. 176)}$$

die Eigenschaft $(C_1, F) = 1$ hat.
Setzt man

$$\gamma := \prod_{\substack{P|F \\ P\nmid C}} P, \qquad \delta := \prod_{\substack{P|F \\ P|C, P\nmid A}} P,$$

wobei P die Primteiler von F durchlaufe, so gilt $(\gamma, \delta) = 1$, d.h. zu $\gamma, \delta \in \mathbb{F}_p[X]$ existieren Elemente $\alpha, \beta \in \mathbb{F}_p[X]$ mit $\alpha\delta - \beta\gamma = 1$.
Es ist dann $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2; \mathbb{F}_p[X])$. Ist

$$T \circ \frac{B + \sqrt{D}}{2C} = \frac{B_1 + \sqrt{D}}{2C_1},$$

so bleibt noch $(C_1, F) = 1$ zu zeigen. Denn dann hat man

$$\mathfrak{a}' := < 2C_1, B_1 + \sqrt{D} > \sim_+ \mathfrak{a},$$

mit $(\mathfrak{a}', (F)) = 1$.
Dazu sei $P \in \mathbb{F}_p[X]$ ein Primteiler von F.

(i) Gilt $P \nmid C$, so gilt $P \mid \gamma$ und $P \nmid \delta$. Also wird $A\gamma^2 + B\gamma\delta$ von P geteilt, nicht aber $C\delta^2$. Es folgt $P \nmid C_1$ aus $(*)$.

(ii) Gilt $P \mid C$, aber $P \nmid A$, so gilt $P \mid \delta$, $P \nmid \gamma$.
Daraus folgt $P \nmid A\gamma^2$, aber $P \mid (B\gamma\delta + C\delta^2)$ und somit wieder $P \nmid C_1$ nach $(*)$.

(iii) Werden sowohl A als auch C von P geteilt, so kann dies nicht für B gelten, denn D ist quadratfrei (beachte: $D = B^2 - 4AC$). Es gilt also $P \nmid B\gamma\delta$, aber $P \mid (A\gamma^2 + C\delta^2)$, woraus wieder $P \nmid C_1$ folgt.

□

9 Zeta- und L-Funktionen quadratischer Funktionenkörper

In [A] leitete ARTIN Formeln für die weite Klassenzahl quadratischer Funktionenkörper her. Er benutzte hierfür ein quadratisches Restsymbol in $\mathbb{F}_p[X]$, welches ein Analogon zum Legendre-Symbol in $\mathbb{Z}$ darstellt. Wir erweitern in diesem Kapitel zunächst das Restsymbol, welches von ARTIN nur für normierte Polynome im Nenner definiert wurde, auf beliebige Primpolynome. Zum Schluß des Kapitels werden die ARTINschen Aussagen zu den Zeta-Funktionen und den L-Funktionen quadratischer Funktionenkörper zusammengefaßt und die im Kapitel 12 benötigten Formeln für die weiten Klassenzahlen zitiert.

9.1 Das quadratische Restsymbol

9.1.1 Definition

Das *Restsymbol* in $\mathbb{F}_p[X]$ definieren wir für beliebige $D \in \mathbb{F}_p[X]$ und irreduzible Polynome $P \in \mathbb{F}_p[X]$ durch

$$\left[\frac{D}{P}\right] = \begin{cases} 0, & \text{falls } P \mid D, \\ 1, & \text{falls } P \nmid D \text{ und } X^2 \equiv D \mod P \text{ lösbar}, \\ -1, & \text{falls } P \nmid D \text{ und } X^2 \equiv D \mod P \text{ nicht lösbar}. \end{cases}$$

Dieses Symbol ist das $\mathbb{F}_p[X]$-Analogon des Legendre-Symbols $\left(\frac{d}{p}\right)$ für Zahlen $d \in \mathbb{Z}$ und Primzahlen p und liefert Aussagen über das Zerlegungsverhalten von Primfunktionen in quadratischen Funktionenkörpern.

9.1.2 Lemma

Es sei $D \in \mathbb{F}_p[X]$ quadratfrei und $P \in \mathbb{F}_p[X]$ irreduzibel und normiert. Dann gilt:

$\left[\frac{D}{P}\right] = 0 \quad \Leftrightarrow \quad (P) = \mathfrak{p}^2$ in $\mathcal{O}_K$ verzweigt mit $\mathfrak{p} = (P, \sqrt{D})$.

$\left[\frac{D}{P}\right] = 1 \quad \Leftrightarrow \quad (P) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_K$ m. $\mathfrak{p} \neq \overline{\mathfrak{p}}$ zerlegt mit $\mathfrak{p} = (P, B + \sqrt{D})$ $(B^2 \equiv D \mod P)$.

$\left[\frac{D}{P}\right] = -1 \quad \Leftrightarrow \quad (P) = \mathfrak{p} = (P, P\sqrt{D})$ in $\mathcal{O}_K$ träge.

In den ersten beiden Fällen ist $N(\mathfrak{p}) = P$, im letzten Fall gilt $N(\mathfrak{p}) = P^2$.

BEWEIS:

[A], S. 171 und Lemma 8.5.4. □

Setzt man dieses Restsymbol kanonisch im Nenner auf alle $N \in \mathbb{F}_p[X]$ fort, so erhält man ein Funktionenkörper-Analogon zum Jacobi-Symbol für teilerfremde ganze Zahlen.

9.1.3 Satz

Für teilerfremde $M, N \in \mathbb{F}_p[X]$ und $N = P_1 \cdot \ldots \cdot P_r$ mit irreduziblen Polynomen $P_i \in \mathbb{F}_p[X]$ schreiben wir

$$\left[\frac{M}{N}\right] := \prod_{i=1}^{r} \left[\frac{M}{P_i}\right].$$

Dieses Symbol besitzt folgende Eigenschaften:

(i) $\left[\frac{M_1}{N}\right]\left[\frac{M_2}{N}\right] = \left[\frac{M_1 M_2}{N}\right]$.

(ii) $M_1 \equiv M_2 \mod N \Rightarrow \left[\frac{M_1}{N}\right] = \left[\frac{M_2}{N}\right]$.

(iii) Aus $N_1 \equiv N_2 \mod M$ folgt i.a. nicht $\left[\frac{M}{N_1}\right] = \left[\frac{M}{N_2}\right]$.

(iv) $\left[\frac{\zeta}{M}\right] = \chi(\zeta)^{\operatorname{grad} M}$ für $\zeta \in \mathbb{F}_p^*$ und $M \in \mathbb{F}_p[X]$.
(*Ergänzungssatz*)

(v) Es ist
$$\left[\frac{M}{N}\right] = \left[\frac{N}{M}\right] \chi(-1)^{\operatorname{grad} M \cdot \operatorname{grad} N} \chi(M)^{\operatorname{grad} N} \chi(N)^{\operatorname{grad} M}$$
für teilerfremde $M, N \in \mathbb{F}_p[X]$.
(*Reziprozitätsgesetz*)

(vi) Ist $M \in \mathbb{F}_p[X] \backslash \mathbb{F}_p[X]^2$, und durchläuft N ein vollständiges primes Restsystem mod M, so gilt
$$\sum_{(N,M)=1} \left[\frac{N}{M}\right] = 0.$$

BEWEIS:

Bis auf (iii) finden sich alle Beweise in [A], S. 204ff.
Hier liefert aber schon

$$\left[\frac{X}{X-1}\right] = 1 \neq -1 = \left[\frac{X}{2X-1}\right]$$

im Fall $p = 3$ ein Beispiel für die gemachte Aussage.
ARTIN bewies (i),(ii) und (iv)-(vi) für das Restsymbol mit normierten Polynomen im Nenner. Sie gelten aber nach Definition 9.1.1 auch für nicht-normierte Polynome. Lediglich beim Reziprozitätsgesetz (v) müssen im Vergleich mit dem in [A] genannten die Faktoren $\chi(M)^{\operatorname{grad} N}$ und $\chi(N)^{\operatorname{grad} M}$ ergänzt werden. Ansonsten verlaufen alle Beweise wie in [A]. □

9.1.4 Definition

Für $n \geq 0$ und quadratfreies $D \in \mathbb{F}_p[X]$ definiert man

$$\sigma_n(D) := \sum_{|F|=p^n} \left[\frac{D}{F}\right],$$

wobei über alle normierten Funktionen $F \in \mathbb{F}_p[X]$ summiert wird.

9.1.5 Proposition

(i) Ist $D \in \mathbb{F}_p[X]$ quadratfrei und $D \neq g$, so gilt $\sigma_n(D) = 0$ für alle $n \geq \operatorname{grad} D$.

(ii) Ist $\zeta \in \mathbb{F}_p^*$ mit $\chi(\zeta) = -1$, so gilt

$$\sigma_n(\zeta D) = (-1)^n \sigma_n(D)$$

für alle $n \geq 0$.

(iii) Ist $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper, so gilt

$$\sum_{n=0}^{\operatorname{grad} D - 1} \sigma_n(D) = 0.$$

BEWEIS:

Diese Aussagen werden sämtlich in [A], S. 206 und 210ff. bewiesen. □

Wie aus Satz 9.1.3 (iii) zu ersehen, gilt für zwei normierte modulo einer Funktion $M \in \mathbb{F}_p[X]$ kongruente Funktionen $N_1, N_2 \in \mathbb{F}_p[X]$ i.a. nicht $\left[\frac{M}{N_1}\right] = \left[\frac{M}{N_2}\right]$.

In speziellen Fällen werden wir jedoch eine Funktion mit dieser Eigenschaft benötigen. Die folgende auf $\mathbb{F}_p[X]$ definierte Funktion leistet unter einer unerheblichen Zusatzvoraussetzung das Verlangte.

9.1.6 Definition

Für $D \in \mathbb{F}_p[X]$ definieren wir die Funktion ψ_D auf $\mathbb{F}_p[X]$ durch

$$\psi_D(M) := \left[\frac{(-1)^{\operatorname{grad} D} D}{M}\right]$$

für $M \in \mathbb{F}_p[X]$.

9.1.7 Lemma

Ist $D \in \mathbb{F}_p[X]$ normiert, so gilt

$$\psi_D(M) = \psi_D(N)$$

für alle $M, N \in \mathbb{F}_p[X]$ mit $M \equiv N \mod D$ und $\chi(M) = \chi(N)$.

BEWEIS:

Sind $M \equiv N \mod D$ und $\chi(M) = \chi(N)$, so gilt

$$\begin{aligned}
\psi_D(M) &= \left[\frac{(-1)^{\operatorname{grad} D} D}{M}\right] \\
&\overset{9.1.3\,(\mathrm{iv})}{=} \chi(-1)^{\operatorname{grad} D \cdot \operatorname{grad} M} \left[\frac{D}{M}\right] \\
&\overset{9.1.3\,(\mathrm{v}),\ D \text{ norm.}}{=} \chi(-1)^{\operatorname{grad} D \cdot \operatorname{grad} M \cdot 2} \chi(M)^{\operatorname{grad} D} \left[\frac{M}{D}\right] \overset{9.1.3\,(\mathrm{ii})}{=} \chi(M)^{\operatorname{grad} D} \left[\frac{N}{D}\right] \\
&\overset{9.1.3\,(\mathrm{v})}{=} \chi(M)^{\operatorname{grad} D} \chi(N)^{\operatorname{grad} D} \chi(-1)^{\operatorname{grad} D \cdot \operatorname{grad} N} \left[\frac{D}{N}\right] = \left[\frac{(-1)^{\operatorname{grad} D} D}{N}\right],
\end{aligned}$$

was die Behauptung war. □

9.2 Zeta- und L-Funktionen quadratischer Funktionenkörper

9.2.1 Definition

Die *Zeta-Funktion* $Z_K(s)$ eines quadratischen Funktionenkörpers $K = k(\sqrt{D})$ wird definiert durch

$$\begin{aligned}
Z_K(s) &:= \sum_{\mathfrak{a}} \frac{1}{|N(\mathfrak{a})|^s} \\
&= \sum_{A \in C(K)} \sum_{\mathfrak{a} \in A} \frac{1}{|N(\mathfrak{a})|^s} = \sum_{A \in C(K)} Z(s, A)
\end{aligned}$$

mit

$$Z(s, A) := \sum_{\mathfrak{a} \in A} \frac{1}{|N(\mathfrak{a})|^s}.$$

Hierbei durchläuft $\mathfrak{a}$ alle ganzen $\mathcal{O}_K$-Ideale, bzw. alle ganzen Ideale aus der weiten Idealklasse $A \in C(K)$.

9.2.2 Satz

Es gilt

$$Z_K(s) = \sum_{\mathfrak{a}} \frac{1}{|N(\mathfrak{a})|^s} = \prod_{\mathfrak{p}} \left(1 - \frac{1}{|N(\mathfrak{p})|^s}\right)^{-1},$$

wobei $\mathfrak{p}$ alle Primideale von K durchlaufe. Sowohl die Reihe als auch das Produkt konvergieren absolut und gleichmäßig auf $\operatorname{Re} s \geq 1+\delta$ $(\delta > 0)$, ebenso wie die Reihe $Z(s, A) = \sum_{\mathfrak{a} \in A} \frac{1}{|N(\mathfrak{a})|^s}$ für $A \in C(K)$.

BEWEIS:

Wir zeigen zunächst die absolute und gleichmäßige Konvergenz des Produkts auf $\operatorname{Re} s \geq 1 + \delta$ mit $\delta > 0$. Die Gleichheit von Reihe und Produkt und die Konvergenz der Reihe zeigt man dann wie im Zahlkörperfall, indem man die eindeutige Primidealzerlegung im Dedekindring $\mathcal{O}_K$ benutzt.
Ist $\mathfrak{p}$ nach Lemma 8.5.4 ein Teiler der normierten Primfunktion P, so ist $|N(\mathfrak{p})| \geq |P|$, und zu jedem P gehören höchstens zwei Primideale.
Für $\operatorname{Re} s \geq 1 + \delta$ ist demnach

$$\sum_{\mathfrak{p}} \left|\frac{1}{|N(\mathfrak{p})|^s}\right| \leq \sum_{\substack{P \\ P \text{ normiert}}} \frac{2}{|P|^{\operatorname{Re} s}} < 2 \sum_{\substack{F \\ \operatorname{sgn} F = 1}} \frac{1}{|F|^{1+\delta}}.$$

Sortiert man nun nach Graden der Funktionen F, so erhält man jeweils p^ν Funktionen $F \in \mathbb{F}_p[X]$ vom Grad ν mit $\operatorname{sgn}(F) = 1$, und es ergibt sich die Abschätzung

$$\sum_{\mathfrak{p}} \left|\frac{1}{|N(\mathfrak{p})|^s}\right| < 2 \sum_{\nu=0}^{\infty} \frac{p^\nu}{p^{\nu(1+\delta)}} = 2 \sum_{\nu=0}^{\infty} p^{-\nu\delta} < \infty,$$

was die Behauptung war.
Die Reihe $Z(s, A)$ ist für jedes $A \in C(K)$ eine Teilreihe von $Z_K(s)$. Sie konvergiert also ebenfalls gleichmäßig absolut auf $\operatorname{Re} s \geq 1 + \delta$ für $\delta > 0$. □

Die folgenden Sätze fassen diejenigen ARTINschen Aussagen über die Zeta-Funktionen, die L-Funktionen und die Berechnung der weiten Klassenzahlen quadratischer Funktionenkörper zusammen, welche wir in Teil V benutzen werden. Zu den Beweisen sei auf [A], S.207ff. verwiesen.

9.2.3 Satz

Die Zetafunktion $Z_K(s)$ eines quadratischen Zahlkörpers $K = k(\sqrt{D})$ besitzt die Darstellung

$$Z_K(s) = Z_k(s) L_D(s)$$

mit

$$Z_k(s) = \frac{1}{1 - p^{-(s-1)}}$$

und

$$\begin{aligned} L_D(s) &= \sum_{(D,F)=1} \left[\frac{D}{F}\right] |F|^{-s} = \prod_{(D,P)=1} \left(1 - \left[\frac{D}{P}\right] |P|^{-s}\right)^{-1} \\ &= \sum_{n=0}^{\infty} \frac{\sigma_n(D)}{p^{ns}}. \end{aligned}$$

Die Summen erstrecken sich dabei über normierte Funktionen aus $\mathbb{F}_p[X]$. Aus Proposition 9.1.5 (i) erhält man demnach

$$Z_K(s) = \frac{1}{1-p^{-(s-1)}} \sum_{n=0}^{\operatorname{grad} D-1} \frac{\sigma_n(D)}{p^{ns}}.$$

Ist $K = k(\sqrt{g})$, $D = g \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$, so ist $\sigma_n(g) = p^n(-1)^n$, also

$$Z_K(s) = \frac{1}{1-p^{-(s-1)}} \frac{1}{1+p^{-(s-1)}} = \frac{1}{1-p^{-2(s-1)}}$$

und

$$L_g(s) = \frac{1}{1+p^{-(s-1)}}.$$

9.2.4 Satz

Die Funktion $Z_K(s)$ ist periodisch mit der Periode $\frac{2\pi i}{\log p}$ und holomorph auf ganz $\mathbb{C}$ bis auf einfache Pole an den Stellen $s = 1 + \frac{2\pi i k}{\log p}$ $(k \in \mathbb{Z})$ mit den Residuen

$$\lim_{s\to 1}(s-1)Z_K(s) = \frac{1}{\log p} L_D(1) = \frac{1}{\log p} \sum_{n=0}^{\operatorname{grad} D-1} \frac{\sigma_n(D)}{p^n}.$$

Ist $K = k(\sqrt{D})$ eine reell-quadratische Erweiterung und $K' = k(\sqrt{gD})$, so gilt

$$Z_K(s + \frac{\pi i}{\log p}) = \frac{1-p^{-(s-1)}}{1+p^{-(s-1)}} Z_{K'}(s).$$

Ferner liegen die Nullstellen der Funktion $Z_K(s)$ bei $s = \frac{2k\pi i}{\log p}$ und die der Funktion $Z_{K'}(s)$ bei $s = \frac{(2k+1)\pi i}{\log p}$ für $k \in \mathbb{Z}$.

9.3 Klassenzahlformeln

9.3.1 Satz

(i) Ist $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper, $\epsilon_0 \in \mathcal{O}_K^*$ seine Grundeinheit, $R_K = \operatorname{grad} \epsilon_0$ sein Regulator und Q_K sein Äquivalenzindex, so gilt für die Klassenzahlen $h(K)$ und $h^+(K)$ die Identität

$$h(K) = \frac{1}{Q_K} h^+(K) = -\frac{1}{R_K} \sum_{n=1}^{\operatorname{grad} D-1} n\sigma_n(D).$$

(ii) Ist $K = k(\sqrt{D})$ ein imaginär-quadratischer Funktionenkörper, so ist

$$h(K) = \sum_{n=0}^{\operatorname{grad} D-1} \sigma_n(D) = L_D(0).$$

9.3.2 Satz

Es sei $K = k(\sqrt{D})$ ein quadratischer Funktionenkörper und (im reellen Fall) R_K sein Regulator.
Definiert man

$$\kappa := \begin{cases} 2, & \text{falls } D = g, \\ \frac{2\sqrt{|D|}}{p+1}, & \text{falls } D \neq g \text{ und } \operatorname{grad} D \text{ gerade } (K \text{ imaginär}), \\ \sqrt{\frac{|D|}{p}}, & \text{falls } \operatorname{grad} D \text{ ungerade } (K \text{ imaginär}) \text{ und} \\ \frac{\sqrt{|D|}}{(p-1)R_K}, & \text{falls } \operatorname{grad} D \text{ gerade } (K \text{ reell}), \end{cases}$$

so gilt

$$h(D) := h(K) = \kappa L_D(1).$$

Teil IV
Geschlechtertheorie

In diesem Teil der Arbeit wird ein Großteil der Ergebnisse von ZAGIER zur Geschlechtertheorie im Zahlkörper aus [Zag2], S.108ff. auf quadratische Funktionenkörper übertragen. Ein zentraler Punkt ist hierbei die vollständige Bestimmung aller Geschlechtscharaktere quadratischer Funktionenkörper.
Wie ZAGIER betrachten auch wir nur die Geschlechter der engen Klassengruppe.
Ergebnisse hinsichtlich der weiten Klasseneinteilung findet man bei ZHANG ([Zh]), welcher ambige weite Klassen und den 2-Rang der weiten Klassengruppe von quadratischen Funktionenkörpern untersuchte. Diese Aussagen werden wir an späterer Stelle noch einmal aufgreifen und um einige Ergebnisse, welche wir aus den Untersuchungen der engen Klassen für die weiten Klassen erhalten, ergänzen.

10 Ambige Ideale und Idealklassen

10.1 Definition und Eigenschaften

10.1.1 Definition

Es sei $K = k(\sqrt{D})$ ein quadratischer Funktionenkörper.
Eine enge Idealklasse $A \in C^+(K)$ heißt *ambig*, falls $A = \overline{A}$.

Ein Ideal $\mathfrak{a} \in I(K)$ heißt *ambig*, falls $\mathfrak{a}$ ganz ist und $\mathfrak{a} = \overline{\mathfrak{a}}$ gilt.

Wir nennen eine ambige Klasse A *regulär*, wenn sie ein ambiges Ideal enthält, ansonsten heiße sie *irregulär*.

10.1.2 Lemma

(i) Ist
$$D = g^j P_1 \cdot \ldots \cdot P_s$$
mit $j \in \{0,1\}$ die Zerlegung der quadratfreien Funktion D in normierte Primpolynome P_i für $i = 1, \ldots, s$, und demnach $P_i = \mathfrak{p}_i^2$ in $K = k(\sqrt{D})$, so gibt es genau 2^s primitive ambige Ideale gegeben durch
$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{p}_s^{\alpha_s} \quad (\alpha_i \in \{0,1\}).$$

(ii) Ist $A \in C^+(K)$ eine reguläre ambige Klasse, so enthält A ein primitives ambiges Ideal.

BEWEIS:

(i) Ist $\mathfrak{a}$ ein ganzes primitives ambiges Ideal, so ist $\mathfrak{a}$ zunächst einmal durch kein Primideal $\mathfrak{p} = (P)$ mit P träge teilbar, denn sonst wäre $\mathfrak{a}$ wegen $P|\mathfrak{a}$ nicht primitiv. Es sei also
$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{r_i} \prod_{j=1}^{l} \mathfrak{q}_j^{s_j}$$
mit $\mathfrak{p}_i$ $(i = 1, \ldots, k)$ verzweigt und $\mathfrak{q}_j$ $(j = 1, \ldots, l)$ zerlegt.

Dann muß wegen

$$\mathfrak{a} = \overline{\mathfrak{a}} = \prod_{i=1}^{k} \overline{\mathfrak{p}_i}^{r_i} \prod_{j=1}^{l} \overline{\mathfrak{q}_j}^{s_j}$$

$s_j = 0$ für $j = 1, \ldots, l$ gelten, denn sonst würden ein $j \in \{1, \ldots, l\}$ und ein Primpolynom $P \in \mathbb{F}_p[X]$ existieren mit $(P) = \mathfrak{q}_j \overline{\mathfrak{q}_j} | \mathfrak{a} = \overline{\mathfrak{a}}$, was wieder aufgrund der Primitivität von $\mathfrak{a}$ nicht möglich ist. Aus dem selben Grund können die verzweigten Primideale $\mathfrak{p}_i$ für $i = 1, \ldots, k$ auch höchstens in der ersten Potenz in $\mathfrak{a}$ aufgehen, d.h. es muß $r_i \leq 1$ gelten für alle $i \in \{1, \ldots, k\}$, was die Behauptung war.

(ii) Ist $A \in C^+(K)$ regulär, so enthält A ein ambiges Ideal $\mathfrak{a} \subsetneq \mathcal{O}_K$. Ist $\mathfrak{a}$ nicht primitiv, etwa $\mathfrak{a} = (S)\mathfrak{b}$ mit einem primitiven Ideal $\mathfrak{b} \subsetneq \mathcal{O}_K$ und $S \in \mathbb{F}_p[X]$, so ist $\mathfrak{b} = (\frac{1}{S})\mathfrak{a} \in A$ wegen $\chi(N(\frac{1}{S})) = \chi(\frac{1}{S^2}) = 1$. A enthält also ein primitives Ideal.

□

10.1.3 Lemma

Ist $\mu \in K^*$ mit $N(\mu) = 1$, so existiert ein Element $\lambda \in \mathcal{O}_K$ mit

$$\mu = \frac{\lambda}{\overline{\lambda}}.$$

In dieser Darstellung ist der Wert $\chi(N(\lambda)) \in \{\pm 1\}$ eindeutig bestimmt.

BEWEIS:

Ist $\mu = -1$ und $K = k(\sqrt{g^j D})$ mit $j \in \{0, 1\}$, so leistet $\lambda := \sqrt{g^j D}$ das Verlangte.
Ist hingegen $\mu \neq -1$, so wählt man $F \in \mathbb{F}_p[X]$ so, daß $\lambda := F \cdot (\mu + 1) \in \mathcal{O}_K$ gilt.
Es ist dann

$$\frac{\lambda}{\overline{\lambda}} = \frac{\mu + 1}{\overline{\mu} + 1} = \mu \frac{\mu + 1}{\mu\overline{\mu} + \mu} = \mu \frac{\mu + 1}{\mu + 1} = \mu.$$

Ist λ' ein weiteres Element mit $\mu = \frac{\lambda'}{\overline{\lambda'}}$, so gilt $\lambda\overline{\lambda'} = \overline{\lambda}\lambda' = A \in k$, d.h. es ist $\chi(N(\lambda)) = \chi(A^2 \cdot N(\lambda')^{-1}) = \chi(N(\lambda'))$. Daher ist $\chi(N(\lambda))$ zu gegebenem μ mit $N(\mu) = 1$ eindeutig bestimmt. □

Es stellt sich nun die Frage, ob es überhaupt enge ambige Klassen ohne ambiges Ideal (also irreguläre ambige Klassen) gibt.
In quadratischen Zahlkörpern $\mathbb{Q}(\sqrt{d})$ ist dies nicht der Fall, dort enthält jede enge ambige Klasse auch ein ambiges Ideal (s. [Zag2], S.117), ist also regulär.
Im reell- bzw. imaginär-quadratischen Funktionenkörpern können aber auch irreguläre enge ambige Klassen auftreten.
Für den reell-quadratischen Fall läßt sich diesbezüglich feststellen:

10.1.4 Satz

Es sei K ein reell-quadratischer Funktionenkörper mit der Grundeinheit $\epsilon_0 \in \mathcal{O}_K^*$. Dann sind äquivalent:

(i) Es existiert eine irreguläre ambige Klasse.

(ii) Es gilt $\chi(-1) = 1$, $N(\epsilon_0) = 1$ und $\chi(\epsilon_0) = 1$.

BEWEIS:

"$\Leftarrow$" Um zu beweisen, daß unter den obigen Voraussetzungen eine irreguläre ambige Klasse existiert, nutzt man aus, daß es nach Lemma 4.1.6 im reell-quadratischen Körper immer ein Element $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$ gibt.
$A_0 := [(u)]$ ist dann wegen $A_0^2 = [(u^2)] = 1$ ambig. Enthielte diese ambige Idealklasse ein ambiges Ideal $\mathfrak{a}$, so wäre $\mathfrak{a} = (u)(\mu)$ mit $\chi(N(\mu)) = 1$ und

$$(\overline{u})(\overline{\mu}) = (u)(\mu).$$

Es würde demnach ein $\epsilon \in \mathcal{O}_K^*$ existieren mit

$$\overline{u\mu}\epsilon = u\mu,$$

und hierbei wäre dann notwendigerweise $N(\epsilon) = 1$.
Betrachtet man

$$u\overline{u}\mu\overline{\mu}\epsilon = N(u)N(\mu)\epsilon = u^2\mu^2$$

mit $\chi(N(u)) = -1 = -\chi(N(\mu))$, so folgt aus dieser Gleichung $\chi(\epsilon) = -1$.
Nach Satz 4.2.2 besitzt ϵ die Darstellung $\epsilon = a \cdot \epsilon_0^k$ mit $a \in \mathbb{F}_p^*$ und $k \in \mathbb{Z}$.
Wegen $N(\epsilon) = 1 = a^2 N(\epsilon_0)^k = a^2$ ist $a = \pm 1$, also $\epsilon = \pm\epsilon_0^k$.
Aus $\chi(\epsilon_0) = 1$ und $\chi(-1) = 1$ erhält man dann

$$\chi(\epsilon) = \chi(\pm\epsilon_0^k) = \chi(\pm 1)\chi(\epsilon_0)^k = 1.$$

Dies ist ein Widerspruch zu $\chi(\epsilon) = -1$. A_0 enthält also kein ambiges Ideal.

"$\Rightarrow$" Für diese Richtung beweisen wir, daß in den Fällen $N(\epsilon_0) = g$ bzw. $N(\epsilon_0) = 1$ und $\chi(-1) = -1$ bzw. $\chi(-1) = 1$ und $\chi(\epsilon_0) = -1$ jede ambige Klasse auch ein ambiges Ideal enthält.
Ist $A = \overline{A}$ eine ambige Klasse und $\mathfrak{a} \in A$ ganz, dann existiert ein $\alpha \in K$ mit $\chi(N(\alpha)) = 1$ und

$$(\alpha)\mathfrak{a} = \overline{\mathfrak{a}}.$$

Es muß also $N((\alpha)) = c^2 N(\alpha) = 1$ sein mit einem $c \in \mathbb{F}_p$. Nach Lemma 10.1.3 existiert dann ein $\rho \in \mathcal{O}_K$ mit

$$c\alpha = \frac{\rho}{\overline{\rho}}.$$

Wir unterscheiden nun die folgenden Fälle:

I. Ist $\chi(N(\rho)) = 1$, so ist

$$(\alpha)\mathfrak{a} = \left(c^{-1}\frac{\rho}{\overline{\rho}}\right)\mathfrak{a} = \left(\frac{\rho}{\overline{\rho}}\right)\mathfrak{a} = \overline{\mathfrak{a}},$$

d.h. $(\rho)\mathfrak{a} = (\overline{\rho})\overline{\mathfrak{a}} \in A$ ist ein ambiges Ideal.

II. Ist $\chi(N(\rho)) = -1$, so betrachten wir noch einmal drei Fälle:
(1) Ist $N(\epsilon_0) = g$ so definiert man $\mu := \epsilon_0\rho$ und erhält

$$\left(\frac{\mu}{\overline{\mu}}\right)\mathfrak{a} = (cg^{-1}\epsilon_0^2\alpha)\mathfrak{a} = (\alpha)\mathfrak{a} = \overline{\mathfrak{a}},$$

weshalb $(\mu)\mathfrak{a} = (\overline{\mu})\overline{\mathfrak{a}}$ wegen $\chi(N(\mu)) = 1$ ein ambiges Ideal in A ist.

(2) Ist $\chi(-1) = -1$, so definieren wir $\mu := \rho\sqrt{D}$ und erhalten somit wieder $(\frac{\mu}{\overline{\mu}}) = (-\alpha) = (\alpha)$, was uns wie im Fall (1) das Ideal $(\mu)\mathfrak{a}$ als ambiges Ideal in A liefert.

(3) Ist $\chi(-1) = 1$, aber $\epsilon_0 = \frac{\lambda}{\overline{\lambda}}$ mit $\chi(N(\lambda)) = \chi(\epsilon_0) = -1$, so wählt man $\mu := \lambda\rho$. Es gilt $(\frac{\mu}{\overline{\mu}}) = (\epsilon_0\alpha) = (\alpha)$ und $(\mu)\mathfrak{a} \in A$ ist ambig.

□

10.1.5 Lemma

Ist K ein quadratischer Funktionenkörper und $A_0 \in C^+(K)$ eine irreguläre enge ambige Klasse, so erhält man alle irregulären engen ambigen Klassen in der Form A_0A, wobei A alle regulären engen ambigen Klassen durchläuft.

BEWEIS:

Ist $A_1 \neq A_0$ und A_1 eine irreguläre enge ambige Klasse, dann existieren Ideale $\mathfrak{a}_0 \in A_0$ und $\mathfrak{a}_1 \in A_1$ mit

$$(\alpha_0)\mathfrak{a}_0 = \overline{\mathfrak{a}_0}, \quad (\alpha_1)\mathfrak{a}_1 = \overline{\mathfrak{a}_1}$$

und $\chi(N(\alpha_i)) = 1$, aber

$$\alpha_i = d_i\frac{\lambda_i}{\overline{\lambda_i}}$$

mit $d_i \in \mathbb{F}_p^*$ und $\chi(N(\lambda_i)) = -1$ für $i = 0, 1$. Wäre nämlich $\chi(N(\lambda_i)) = 1$ für ein $i \in \{0, 1\}$, so enthielte die Klasse A_i das ambige Ideal $(\lambda_i)\mathfrak{a}_i$. Nun gilt aber

$$\mathfrak{a}_0\mathfrak{a}_1(\alpha_0\alpha_1) = \overline{(\mathfrak{a}_0\mathfrak{a}_1)},$$

womit man $\mathfrak{a}_0\mathfrak{a}_1(\lambda_0\lambda_1)$ als ambiges Ideal der Klasse A_0A_1 identifiziert hätte. Es ist also $A := A_0A_1$ eine reguläre ambige Klasse, d.h. es gilt $A_1 = A_0^{-1}A = A_0A$. Verschiedene reguläre ambige Klassen A liefern ferner auch durch A_0A verschiedene irreguläre ambige Klassen. Enthielte nämlich A_0A ein ambiges Ideal $\mathfrak{a}_0\mathfrak{a}$ mit $\mathfrak{a}_0 \in A_0$ und $\mathfrak{a} \in A$, so würde ein $\alpha \in \mathcal{O}_K$ mit $\chi(N(\alpha)) = 1$ und ein ambiges Ideal $\mathfrak{a}' \in A$ existieren mit

$$\overline{\mathfrak{a}_0\mathfrak{a}} = \overline{\mathfrak{a}_0}(\overline{\alpha})\overline{\mathfrak{a}'} = \mathfrak{a}_0(\alpha)\mathfrak{a}'.$$

Demnach wäre wegen $\mathfrak{a}' = \overline{\mathfrak{a}'}$ das Ideal $(\alpha)\mathfrak{a}_0 \in A_0$ ambig, was nicht sein kann. □

10.2 Die Anzahl der ambigen Klassen im reell-quadratischen Funktionenkörper

10.2.1 Satz

Es sei $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper mit einem normierten und quadratfreien $D = P_1 \cdot \ldots \cdot P_s$ von geradem Grad. Dann gibt es genau 2^{s-1} enge ambige Klassen.

BEWEIS:

Im Fall $N(\epsilon_0) = g$ mit $\chi(g) = -1$ fallen enge und weite Klassen zusammen. Man weiß dann nach [Zh], S. 427, daß es 2^{s-1} ambige Klassen gibt.

Es sei $N(\epsilon_0) = 1$ und $\epsilon_0 = \frac{\lambda}{\overline{\lambda}}$ mit $\lambda \in \mathcal{O}_K$. Ist nun $(\mu) = (\overline{\mu})$ mit $\mu \in \mathcal{O}_K\backslash\{0\}$ ein ambiges Hauptideal, so existiert ein $\epsilon \in \mathcal{O}_K^*$ mit $N(\epsilon) = 1$ und $\mu = \epsilon\overline{\mu}$. Nach Satz

4.2.2 und wegen $N(\epsilon) = 1$ kann man ϵ schreiben als $\epsilon = \pm\epsilon_0^k$ mit einem $k \in \mathbb{Z}$ und der Grundeinheit ϵ_0 von K. Es folgt

$$\frac{\mu}{\overline{\mu}} = \pm\epsilon_0^k = \pm\frac{\lambda^k}{\overline{\lambda}^k}$$

mit $k \in \mathbb{Z}$. Es ist dann

$$\frac{\mu}{\lambda^k} = \pm\frac{\overline{\mu}}{\overline{\lambda}^k}.$$

Da $\mu \in \mathcal{O}_K$ gelten soll ist demnach $(\mu) = (F\lambda^k)$ oder $(\mu) = (F\lambda^k\sqrt{D})$ mit einem $F \in \mathbb{F}_p[X]$ und $k \in \mathbb{N}$.
Wegen $\epsilon_0 = \frac{\lambda}{\overline{\lambda}}$ ist $(\lambda) = (\overline{\lambda})$ und somit $(\lambda^2) = (N(\lambda))$.
Wegen $\lambda \in \mathcal{O}_K$ gilt $N(\lambda) \in \mathbb{F}_p[X]$. (1) und $(\sqrt{D})$ sind offensichtlich – da D quadratfrei ist – primitive ambige Hauptideale. Wird zusätzlich $\lambda \in \mathcal{O}_K$ so gewählt, daß es durch kein Polynom $F \in \mathbb{F}_p[X]$ teilbar ist, so ist auch (λ) ein primitives ambiges Hauptideal, welches von (1) und $(\sqrt{D})$ verschieden ist. Wäre nämlich $(\lambda) = (1)$, so wäre $\lambda \in \mathcal{O}_K^* = \mathbb{F}_p^* \times < \epsilon_0 >$, also

$$\epsilon_0 = \frac{\lambda}{\overline{\lambda}} = \frac{a\epsilon_0^k}{a\epsilon_0^{-k}} = \epsilon_0^{2k}$$

für ein $a \in \mathbb{F}_p^*$ und ein $k \in \mathbb{Z}$. Dies ist aber ein Widerspruch zu $|\epsilon_0| > 1$. Wäre $(\lambda) = (\sqrt{D})$, so würden ein $a \in \mathbb{F}_p^*$ und ein $k \in \mathbb{Z}$ existieren mit $\lambda = a\epsilon_0^k\sqrt{D}$, also

$$\frac{\lambda(-\sqrt{D})}{\overline{\lambda}\sqrt{D}} = -\epsilon_0 = \epsilon_0^{2k},$$

wiederum ein Widerspruch. Zu $(\lambda\sqrt{D})$ hingegen existiert ein Polynom $F \in \mathbb{F}_p[X]$ und ein primitives ambiges Hauptideal (α) mit $\alpha \in \mathcal{O}_K$ und $(\lambda\sqrt{D}) = (F)(\alpha)$. Wie oben zeigt man $(\alpha) \notin \{(1), (\sqrt{D}), (\lambda)\}$.
Ist also (μ) ein **primitives** ambiges Hauptideal, so gilt $(\mu) \in \mathfrak{A} := \{(1), (\sqrt{D}), (\lambda), (\alpha)\}$.
Es handelt sich somit bei $\mathfrak{A}$ um die Menge aller primitiven ambigen Hauptideale.
Für unsere Zwecke bestimmen wir nun noch die Menge $\mathfrak{A} \cap H^+(K)$ und unterscheiden dazu die folgenden Fälle.

(i) Ist $\chi(-1) = 1 = \chi(\epsilon_0) = \chi(N(\lambda))$, so gilt $\chi(N(\sqrt{D})) = \chi(-D) = 1$ und $\chi(N(\alpha)) = \chi(N(\lambda\sqrt{D})) = 1$, also $\mathfrak{A} \subset H^+(K)$.

(ii) Ist $\chi(-1) = 1$, aber $\chi(\epsilon_0) = -1 = \chi(N(\lambda))$, so ist $\mathfrak{A} \cap H^+(K) = \{(1), (\sqrt{D})\}$, da weder (λ) noch $(\lambda\sqrt{D}) = (F)(\alpha)$ in der engen Hauptidealklasse liegen.

(iii) Ist $\chi(-1) = -1$ und $\chi(\epsilon_0) = 1$, so ist $\mathfrak{A} \cap H^+(K) = \{(1), (\lambda)\}$.

(iv) Gilt schließlich $\chi(-1) = -1 = \chi(\epsilon_0)$, so ist $\mathfrak{A} \cap H^+(K) = \{(1), (\alpha)\}$.

Ist A nun eine reguläre ambige Klasse, so enthält A wegen Lemma 10.1.2 (ii) ein primitives ambiges Ideal $\mathfrak{a}_0$.
In den obigen Bezeichnungen existieren dann paarweise verschiedene primitive ambige Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \subset \mathcal{O}_K$ und Polynome $F_1, F_2, F_3 \in \mathbb{F}_p[X]$ mit

$$\begin{aligned} (\sqrt{D})\mathfrak{a}_0 &= (F_1)\mathfrak{a}_1, \\ (\lambda)\mathfrak{a}_0 &= (F_2)\mathfrak{a}_2 \text{ und} \\ (\alpha)\mathfrak{a}_0 &= (F_3)\mathfrak{a}_3. \end{aligned}$$

Daß die $\mathfrak{a}_i$ für $i \in \{0, \ldots, 3\}$ paarweise verschieden sind, führt man wie oben darauf zurück, daß $\mathfrak{A}$ aus paarweise verschiedenen Elementen besteht.
Benutzt man die Aussagen (i)-(iv) über die Menge $\mathfrak{A} \cap H^+(K)$, so erhält man, daß in diesen Fällen für die Menge Amb(A) der primitiven ambigen Ideale aus A gilt

$$\mathrm{Amb}(A) = \begin{cases} \{\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3\} & \text{im Fall (i),} \\ \{\mathfrak{a}_0, \mathfrak{a}_1\} & \text{im Fall (ii),} \\ \{\mathfrak{a}_0, \mathfrak{a}_2\} & \text{im Fall (iii) und} \\ \{\mathfrak{a}_0, \mathfrak{a}_3\} & \text{im Fall (iv).} \end{cases}$$

Nach Lemma 10.1.2 (i) gibt es 2^s primitive ambige Ideale. Diese verteilen sich demnach im Fall (i) auf 2^{s-2} reguläre ambige Klassen. Nach Satz 10.1.4 und Lemma 10.1.5 gibt es demnach 2^{s-1} ambige Klassen insgesamt (mit den 2^{s-2} irregulären).
In den Fällen (ii)-(iv) enthält nach Satz 10.1.4 und Lemma 10.1.2 (ii) jede ambige Klasse ein primitives ambiges Ideal.
D.h. die 2^s primitiven ambigen Ideale verteilen sich auf genau 2^{s-1} ambige Klassen, was die Behauptung war. □

10.3 Die Anzahl der ambigen Klassen im imaginär-quadratischen Funktionenkörper

Nun ist es nicht so, daß, wie im Zahlkörperfall, die Anzahl der ambigen Klassen im imaginär-quadratischen Körper derjenigen im reell-quadratischen Körper entspricht.
Wie wir bereits feststellten, gibt es imaginär-quadratische Funktionenkörper, in denen die engen und weiten Äquivalenzklassen nicht zusammenfallen, anders als in Zahlkörpern.
Es wird gezeigt, daß in den imaginär-quadratischen Körpererweiterungen von k, in denen die Stelle ∞ verzweigt ist und in denen kein Element $u \in \mathcal{O}_K$ existiert mit $\chi(N(u)) = -1$ (dies entspricht im wesentlichen den Eigenschaften imaginär-quadratischer Zahlkörper), die Anzahl der engen ambigen Klassen der Anzahl im reell-quadratischen Körper entspricht, diese in allen anderen Fällen hingegen doppelt so groß ist.

10.3.1 Satz

Es sei K ein imaginär-quadratischer Funktionenkörper, d.h. $K = k(\sqrt{gD})$ bzw. $K = k(\sqrt{D})$ mit $\operatorname{grad} D$ ungerade und $D = P_1 \cdot \ldots \cdot P_s \in \mathbb{F}_p[X]$ normiert und quadratfrei. Dann unterscheidet man die folgenden Fälle:

(i) Ist $\chi(-1) = 1$, so gilt:

  (1) Ist $K = k(\sqrt{gD}) \neq k(\sqrt{g})$, so ist jede ambige Klasse regulär. Es gibt 2^s (reguläre) ambige Klassen.

  (2) Ist $K = k(\sqrt{D})$ mit $\operatorname{grad} D \equiv 1\ (2)$, so ist wiederum jede ambige Klasse regulär. In diesem Fall gibt es jedoch 2^{s-1} ambige Klassen.

(ii) Ist $\chi(-1) = -1$, so gilt:

  (1) Ist $K = k(\sqrt{gD}) \neq k(\sqrt{g})$ mit $\operatorname{grad} D$ gerade, so existiert eine irreguläre ambige Klasse, es existieren 2^{s-1} reguläre ambige Klassen, demnach gibt es 2^s ambige Klassen insgesamt.

(2) Ist $K = k(\sqrt{gD})$ mit $\operatorname{grad} D$ ungerade, so gibt es keine irregulären ambigen Klassen, und die Anzahl der (regulären) ambigen Klassen beträgt 2^{s-1}.

(3) Ist $K = k(\sqrt{D})$ mit $\operatorname{grad} D \equiv 1\ (2)$, so enthält wieder jede ambige Klasse ein ambiges Ideal. Es gibt 2^s (reguläre) ambige Klassen.

(iii) Ist $K = k(\sqrt{g})$, so gibt es genau eine enge Idealklasse. Diese ist ambig und regulär. Dieser Fall fügt sich also nahtlos (für den Fall $s = 0$) in (i)(1) und (ii)(1) ein.

BEWEIS:

Ist $A = \overline{A} \in C^+(K)$ ambig und $\mathfrak{a} \in A$ ein ganzes Ideal, so existiert ein $\alpha \in \mathcal{O}_K$ mit $\chi(N(\alpha)) = 1$ und $(\alpha)\mathfrak{a} = \overline{\mathfrak{a}}$. Es ist dann $N((\alpha)) = c^2 N(\alpha) = 1$, also

$$c\alpha = \frac{\rho}{\overline{\rho}}$$

mit $\rho \in \mathcal{O}_K$ nach Lemma 10.1.3.

(i) Es sei $\chi(-1) = 1$.

(1) Ist $\chi(N(\rho)) = 1$, so ist wegen $\left(\frac{\rho}{\overline{\rho}}\right) = (\alpha)$ das Ideal $(\rho)\mathfrak{a} = (\overline{\rho})\overline{\mathfrak{a}}$ ein ambiges Ideal in A. Ist hingegen $\chi(N(\rho)) = -1$, so ist $\beta := \rho\sqrt{gD}$ ein Element mit $\chi(N(\beta)) = 1$, es gilt $\left(\frac{\beta}{\overline{\beta}}\right) = (\alpha)$. Es ist dann $(\beta)\mathfrak{a} = (\overline{\beta})\overline{\mathfrak{a}}$ ein ambiges Ideal in A. Somit enthält jede ambige Klasse ein primitives ambiges Ideal.
Ist also $(\mu) = (\overline{\mu})$ ein ambiges Hauptideal mit $\chi(N(\mu)) = 1$, so muß gelten

$$\frac{\mu}{\overline{\mu}} = \pm 1,$$

da im imaginären Körper (mit Ausnahme von $K = k(\sqrt{g})$) die Einheiten gerade die Elemente aus $\mathbb{F}_p^*$ sind.
Es folgt also $(\mu) = (F)$ oder $(\mu) = (F\sqrt{gD})$ mit einem $F \in \mathbb{F}_p[X]$. Wegen $\chi(N(F\sqrt{gD})) = -1$ gilt $(F\sqrt{gD}) \notin H^+(K)$, d.h. es gibt insbesondere kein nicht-triviales primitives ambiges Hauptideal. Das einzige primitive ambige Hauptideal ist demnach das Ideal (1). Da jede ambige Klasse nach Lemma 10.1.2 (ii) ein primitives ambiges Ideal enthält, folgt daraus nach Lemma 10.1.2 (i) die Existenz von 2^s ambigen Klassen, welche sämtlich regulär sind.

(2) Daß es keine irregulären ambigen Klassen gibt, beruht auf der Tatsache, daß es kein Element $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$ gibt (Lemma 4.1.6). Es gilt also $\chi(N(\rho)) = 1$. Demnach ist wie schon in (i)(1) $(\rho)\mathfrak{a} = (\overline{\rho})\overline{\mathfrak{a}}$ ein ambiges Ideal in A.
Ferner ist $(\sqrt{D})$ ein primitives ambiges Hauptideal, es existieren daher 2^{s-1} (reguläre) ambige Klassen.

(ii) Sei nun $\chi(-1) = -1$.

(1) Wird $A_0 := [(u)]$ mit $u \in \mathcal{O}_K$ so gewählt, daß $\chi(N(u)) = -1$ ist, so ist A_0 eine irreguläre ambige Klasse.
Denn andernfalls würde ein $\alpha \in \mathcal{O}_K$ existieren mit $\chi(N(\alpha)) = 1$ und $(u)(\alpha) = (\overline{u\alpha})$, also würde $u\alpha = \overline{u\alpha}\epsilon = \pm\overline{u\alpha}$ gelten. Daraus würde $u\alpha = F$ oder $u\alpha = F\sqrt{gD}$ mit einem $F \in \mathbb{F}_p[X]$ folgen, was aber wegen

$$\chi(N(u\alpha)) = -1 \neq 1 = \chi(F^2) = \chi(F^2(-gD))$$

nicht sein kann.
In diesem Fall ist $(\sqrt{gD})$ ein nicht-triviales primitives ambiges Hauptideal. Es existieren daher nach Lemma 10.1.2 (i) und (ii) genau 2^{s-1} reguläre ambige Klassen. Wegen Lemma 10.1.5 gibt es dann zusammen 2^s ambige Klassen.

(2) Daß es keine irreguläre ambige Klasse gibt, erhält man analog zu (i) (2), wobei $(\sqrt{gD})$ ein nicht-triviales enges ambiges Hauptideal ist.
D.h. die Anzahl der ambigen Klassen beträgt auch hier 2^{s-1}.

(3) Wieder nach den Überlegungen im Beweis des Satzes 10.1.4 II. (2) ist jede ambige Klasse regulär, jedoch ist (1) das einzige ambige Hauptideal, wonach die Anzahl der (regulären) ambigen Klassen 2^s beträgt.

(iii) Nach [A], S. 184, ist $h(k(\sqrt{g})) = 1$.
Wegen Folgerung 8.3.2 ist dann auch $h^+(K) = 1$. Es existiert demnach genau eine enge Idealklasse, nämlich die enge Hauptidealklasse, welche offensichtlich ambig und regulär ist.

□

11 Geschlechter und Geschlechtscharaktere

11.1 Die Struktur der engen Idealklassengruppe

11.1.1 Definition

Ein Charakter $\psi : C^+(K) \to \mathbb{C}^*$ heißt ein *Geschlechtscharakter von* $C^+(K)$, falls ψ reellwertig ist. Wir bezeichnen mit $\mathfrak{G}^+(K)$ die Menge der Geschlechtscharaktere von $C^+(K)$.

Ein Geschlechtscharakter ψ von $C^+(K)$ werde ein *echter* Geschlechtscharakter von $C^+(K)$ genannt, wenn es sich bei ihm nicht um einen Charakter von $C(K)$ handelt, d.h. wenn gilt

$$\psi([(\lambda)]) = -1 \quad \text{für } \lambda \in K^* \text{ mit } \chi(N(\lambda)) = -1.$$

Zwei Klassen $A_1, A_2 \in C^+(K)$ gehören zu demselben *Geschlecht*

$\Leftrightarrow$ $\psi(A_1) = \psi(A_2)$ für alle $\psi \in \mathfrak{G}^+(K)$.

$\Leftrightarrow$ $A_1 = A^2 A_2$ für ein $A \in C^+(K)$.

Es ist also

$$G^+(K) = \text{Gruppe der Geschlechter} \simeq C^+(K)/C^+(K)^2 \simeq \mathfrak{G}^+(K).$$

In Abgrenzung dazu bezeichnen wir mit $\mathfrak{G}(K) \subseteq \mathfrak{G}^+(K)$ die Gruppe der Geschlechtscharaktere von $C(K)$ und analog mit $G(K)$ die Gruppe der Geschlechter von $C(K)$.

11.1.2 Bemerkung

Das Einselement von $G^+(K)$, das sogenannte Hauptgeschlecht, besteht aus den Quadraten der Idealklassen, $C^+(K)^2$.

Ein Ideal $\mathfrak{a}$ gehört demnach zum Hauptgeschlecht genau dann, wenn $\mathfrak{a} = (\lambda)\mathfrak{b}^2$ für ein Ideal $\mathfrak{b}$ und ein Element $\lambda \in K^*$ mit $\chi(N(\lambda)) = 1$ gilt.
Es sei $Sq : C^+(K) \to C^+(K)$ die Abbildung, die eine Idealklasse auf ihr Quadrat schickt. Dann hat man die exakte Sequenz

$$0 \to I \to C^+(K) \stackrel{Sq}{\to} C^+(K) \to C^+(K)/C^+(K)^2 \to 0$$

mit $I = \mathrm{Kern}(Sq)$.
Da alle Gruppen endlich sind, folgt $|I| = |C^+(K)/C^+(K)^2|$, und für $A \in C^+(K)$ hat man wegen $A^{-1} = \overline{A}$

$$A \in I \quad \Leftrightarrow \quad A^2 = 1 \quad \Leftrightarrow \quad A = \overline{A}.$$

Speziell kann man schreiben:

$$C^+(K) =< A_1, \ldots, A_t, B_1, \ldots, B_e >$$

mit $A_i^{2^{e_i}} = 1$ und $B_i^{q_i} = 1$, wobei $q_i = p_i^{f_i}$ für gewisse nicht notwendig verschiedene ungerade $p_i \in \mathbb{P}$ und $e_i, f_i \in \mathbb{N}_0$ gilt. t ist dann die Zahl der geraden Invarianten der engen Idealklassengruppe.
Da die $B_i = B_i^{2\frac{q_i+1}{2}}$ Quadrate sind, gilt

$$C^+(K)^2 =< A_1^2, \ldots, A_t^2, B_1, \ldots, B_e >,$$

und somit

$$G^+(K) = C^+(K)/C^+(K)^2 =< A_1^{2^{e_1-1}}, \ldots, A_t^{2^{e_t-1}} >=< X_1, \ldots, X_t \mid X_i^2 = 1 > .$$

Man erhält also $h^+(K) = \prod_{i=1}^{t} 2^{e_i} \prod_{i=1}^{e} p_i^{f_i}$ und $|C^+(K)^2| = h^+(K) \cdot 2^{-t}$, also insbesondere $2^t | h^+(K)$, und es ist

$$\#G^+(K) = 2^t = \#\{X \in C^+(K) \mid X^2 = 1\}.$$

Die Anzahl der Geschlechter entspricht also der Anzahl der engen ambigen Idealklassen.

Die Zahl t wird auch der *2-Rang der engen Idealklassengruppe* genannt.

Bevor wir die (echten) Geschlechtscharaktere der einzelnen Körper explizit bestimmen, wollen wir noch einige Aussagen über die Charakterisierung der Geschlechter anführen, welche in [Zag2], S. 109/110, ihr Analogon im Hinblick auf den Zahlkörperfall finden.

11.1.3 Satz

a) Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ gehören zu demselben Geschlecht

$$\Leftrightarrow \quad \text{Es existiert ein } \lambda \in K^*, \ \chi(N(\lambda)) = 1 \text{ mit } N(\mathfrak{a}) = N((\lambda)\mathfrak{b}).$$

b) Ein normiertes Polynom $F \in \mathbb{F}_p[X]$ ist genau dann Norm eines Elements aus K, wenn F die Norm eines ganzen Ideals aus dem Hauptgeschlecht ist.

BEWEIS:

a)"$\Rightarrow$" Gehören $\mathfrak{a}$ und $\mathfrak{b}$ zu demselben Geschlecht, so gilt nach obigen Aussagen $\mathfrak{a} = (\mu)\mathfrak{c}^2\mathfrak{b}$ mit einem Ideal $\mathfrak{c}$ aus K und $\mu \in K$ mit $\chi(N(\mu)) = 1$. Dann ist

$$N(\mathfrak{a}) = N((\mu))N(\mathfrak{c})^2N(\mathfrak{b}) = N((\mu N(\mathfrak{c}))\mathfrak{b}) = N((\lambda)\mathfrak{b})$$

mit $\lambda := \mu N(\mathfrak{c})$, und wir erhalten die Behauptung.

"$\Leftarrow$" Gilt hingegen $N(\mathfrak{a}) = N((\lambda)\mathfrak{b})$ und $\chi(N(\lambda)) = 1$, so ist zu zeigen, daß $\mathfrak{a}$ im Geschlecht von $\mathfrak{b}$ liegt.
Indem man $\mathfrak{a}$ durch $\mathfrak{a}(\lambda^{-1})\mathfrak{b}^{-1}$ ersetzt, reicht es zu zeigen, daß gilt

$$(*) \qquad N(\mathfrak{a}) = 1 \quad \Rightarrow \quad \exists \text{ ganzes Ideal } \mathfrak{b} \text{ mit } \mathfrak{a} = \frac{\mathfrak{b}}{\overline{\mathfrak{b}}}$$

Dies impliziert dann die Behauptung, denn nach Lemma 8.5.2 ist

$$\frac{\mathfrak{b}}{\overline{\mathfrak{b}}} = (N(\mathfrak{b}))^{-1}\mathfrak{b}^2,$$

und dieses Ideal gehört offensichtlich zum Hauptgeschlecht.
Um die Implikation $(*)$ zu beweisen, betrachten wir die Primidealzerlegung von

$$\mathfrak{a} = \left(\prod_i \mathfrak{p}_i^{a_i}\overline{\mathfrak{p}_i}^{b_i}\right)\left(\prod_j \mathfrak{q}_j^{c_j}\right) \quad (a_i, b_i, c_j \in \mathbb{Z}),$$

wobei $N(\mathfrak{p}_i) = P_i$ eine zerlegte Primfunktion sei und $\mathfrak{q}_j$ diejenigen Primfaktoren mit $\mathfrak{q}_j = \overline{\mathfrak{q}_j}$, d.h. $N(\mathfrak{q}_j) = Q_j^2$ mit Q_j träge oder $N(\mathfrak{q}_j) = Q_j$ verzweigt. Es folgt dann aus

$$1 = N(\mathfrak{a}) = \prod_i P_i^{a_i+b_i}\prod_j Q_j^{c_j}$$

und der eindeutigen Primfaktorzerlegung in $\mathbb{F}_p[X]$, daß $a_i + b_i = 0$ und $c_j = 0$ für alle i, j gelten muß, und somit haben wir die Implikation $(*)$ mit

$$\mathfrak{b} := \prod_{a_i>0} \mathfrak{p}_i^{a_i}\prod_{b_i>0}\overline{\mathfrak{p}_i}^{b_i}$$

bewiesen.

b)"$\Leftarrow$" Ist $F = N(\mathfrak{a})$ mit $\mathfrak{a}$ im Hauptgeschlecht, so ist F normiert. Weiter ist $\mathfrak{a} = (\mu)\mathfrak{c}^2$ für ein Ideal $\mathfrak{c} \in I(K)$. Wegen $\chi(N(\mu)) = 1$ gilt dann

$$F = N((\mu N(\mathfrak{c}))) = aN(\mu)N(\mathfrak{c})^2$$

mit einem $a \in \mathbb{F}_p^{*2}$.
Ist $a = c^2$ mit $c \in \mathbb{F}_p^*$, so gilt $F = N(\lambda)$ mit $\lambda := c\mu N(\mathfrak{c})$.

"$\Rightarrow$" Ist andererseits $F = N(\lambda) \in \mathbb{F}_p[X]$ normiert mit $\lambda \in K^*$, so schreibt man $(\lambda) = \frac{\mathfrak{a}}{\mathfrak{b}}$, wobei $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde ganze Ideale aus K sind.
Wegen $N(\mathfrak{b})|N(\mathfrak{a})$ (beachte: $F = N(\lambda) \in \mathbb{F}_p[X]$) und $(\mathfrak{a}, \mathfrak{b}) = 1$ folgt $\overline{\mathfrak{b}}|\mathfrak{a}$, also $\mathfrak{a} = \overline{\mathfrak{b}}\mathfrak{c}$ mit einem ganzen $\mathfrak{c}$. Dann ist

$$F = N(\lambda) \overset{\operatorname{sgn} N(\lambda)=1}{=} N((\lambda)) = N(\frac{\mathfrak{a}}{\mathfrak{b}}) = N(\frac{\overline{\mathfrak{b}}\mathfrak{c}}{\mathfrak{b}}) = N(\mathfrak{c}),$$

was die Behauptung war. Denn $\mathfrak{c}$ liegt wegen a) im Hauptgeschlecht.

□

11.2 L-Funktionen zu Geschlechtscharakteren

11.2.1 Definition

Es sei $\psi : C^+(K) \to \{\pm 1\}$ ein Geschlechtscharakter der engen Idealklassen.
Dann definieren wir für $s \in \mathbb{C}$ mit $\operatorname{Re} s > 1$

$$L_\psi(s) := \sum_{\mathfrak{a}} \frac{\psi(\mathfrak{a})}{|N(\mathfrak{a})|^s},$$

die L-Reihe zum Charakter ψ. In der Reihe wird über alle ganzen Ideale von K summiert. Es ist dann

$$L_\psi(s) = \prod_{\mathfrak{p}} \left(1 - \frac{\psi(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1}$$

für $\operatorname{Re} s > 1$ absolut konvergent, wobei das Produkt über alle Primideale von K läuft. Die Konvergenz der Summe und des Produkts zeigt man wie die der Zeta-Funktion in Kapitel 9.2.

Ist $h^+(K)$ die enge Klassenzahl von K, so läßt sich $L_\psi(s)$ auch in der Form

$$L_\psi(s) = \sum_{i=1}^{h^+(K)} \psi(\mathfrak{a}_i) Z(s, A_i)$$

mit der Zetafunktion

$$Z(s, A_i) := \sum_{\mathfrak{a} \in A_i} \frac{1}{|N(\mathfrak{a})|^s}$$

zur engen Idealklasse $A_i \in C^+(K)$ darstellen, wobei $\mathfrak{a}_i$ jeweils ein beliebiger ganzer Vertreter der engen Idealklasse A_i ist.

Im folgenden soll es darum gehen, die Geschlechtscharaktere in den verschiedenen quadratischen Erweiterungen von k explizit durch die in Kapitel 9.1 eingeführten Restsymbole auszudrücken und eine Zerlegungsformel für die zugehörige L-Reihe aufzustellen, wie dies auch in [Zag2], S. 111/112 für die quadratischen Zahlkörper geschehen ist.

11.3 Bestimmung der verschiedenen Geschlechtscharaktere im reell-quadratischen Funktionenkörper

11.3.1 Satz

Ist $D = P_1 \cdot \ldots \cdot P_s$ ein normiertes quadratfreies Polynom geraden Grades aus $\mathbb{F}_p[X]$, so existieren im reell-quadratischen Funktionenkörper $K = k(\sqrt{D})$ genau 2^{s-1} Geschlechter bzw. Geschlechtscharaktere.

BEWEIS:

Die Behauptung folgt aus Bemerkung 11.1.2 in Verbindung mit Satz 10.2.1. □

11.3.2 Satz

Ist $D = P_1 \cdot \ldots \cdot P_s$ ein quadratfreies normiertes Polynom aus $\mathbb{F}_p[X]$ von geradem Grad, $K = k(\sqrt{D})$ und $D = D_1 D_2$ eine Zerlegung von D in ein Produkt zweier normierter Polynome

$D_1, D_2 \in \mathbb{F}_p[X]$, dann definiert man

$$\tilde{\psi}(\mathfrak{p}) := \begin{cases} \psi_{D_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1 \\ \psi_{D_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

mit ψ_{D_i} aus Definition 9.1.6. Setzt man diese Abbildung durch

$$\tilde{\psi}(\mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_k^{n_k}) = \tilde{\psi}(\mathfrak{p}_1)^{n_1} \cdot \ldots \cdot \tilde{\psi}(\mathfrak{p}_k)^{n_k} \quad (\mathfrak{p}_i \text{ prim}, n_i \in \mathbb{Z})$$

auf beliebige gebrochene Ideale fort, so ist $\tilde{\psi}$ ein Geschlechtscharakter von $C^+(K)$.
Für die L-Reihe zu $\tilde{\psi}$ gilt

$$L_{\tilde{\psi}}(s) = L_{\psi_{D_1}}(s) L_{\psi_{D_2}}(s)$$

mit

$$L_{\psi_{D_i}}(s) = \sum_{(D_i, F)=1} \psi_{D_i}(F)|F|^{-s} = \sum_{n=0}^{\infty} \frac{\sigma_n((-1)^{\operatorname{grad} D_i} D_i)}{p^{ns}} = L_{(-1)^{\operatorname{grad} D_i} D_i}(s).$$

Es besteht eine bijektive Korrespondenz zwischen den Geschlechtscharakteren von K und den Zerlegungen $D = D_1 D_2$ als Produkt von zwei normierten Funktionen. Hierbei werden Zerlegungen $D = D_1 D_2$ und $D = D_2 D_1$ als gleich angesehen, und es ist $D = 1 \cdot D = D \cdot 1$ als Zerlegung erlaubt.
Ist $\tilde{\psi}$ der zur Zerlegung $D = 1 \cdot D$ gehörige Charakter, so gilt

$$L_{\tilde{\psi}}(s) = Z_K(s) = Z_k(s) L_D(s).$$

BEWEIS:

Daß $\tilde{\psi}$ wohldefiniert ist, sieht man wie folgt ein:
Es ist $N(\mathfrak{p}) = P^f$ für ein $f \in \{1, 2\}$ mit einem normierten Primpolynom $P \in \mathbb{F}_p[X]$.
Zu zeigen ist, daß

$$\psi_{D_1}(N(\mathfrak{p})) = \psi_{D_2}(N(\mathfrak{p}))$$

für $P \nmid D_1 D_2$ gilt.

i) Ist P träge, d.h. $(P) = \mathfrak{p}$ in K, so ist $N(\mathfrak{p}) = P^2$ und beide Symbole haben den Wert 1.

ii) Ist P zerlegt, d.h. $(P) = \mathfrak{p}\mathfrak{p}'$ in K, so ist $N(\mathfrak{p}) = N(\mathfrak{p}') = P$ und

$$\left[\frac{D_1 D_2}{N(\mathfrak{p})}\right] = 1 = \psi_{D_1}(N(\mathfrak{p})) \psi_{D_2}(N(\mathfrak{p})),$$

denn es gilt $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \mod 2$ wegen $\operatorname{grad} D_1 D_2 \equiv 0 \mod 2$. Beide Symbole sind demnach gleich, da sie nur die Werte ± 1 annehmen.

Da $\tilde{\psi}$ aufgrund der Definition multiplikativ ist, bleibt nur noch nachzuweisen, daß es sich auch um einen Charakter der engen Idealklassen handelt, d.h. daß

$$\tilde{\psi}((\lambda)) = 1 \quad \text{für alle } \lambda \in K^* \text{ mit } \chi(N(\lambda)) = 1$$

gilt. Hier können wir $\lambda \in \mathcal{O}_K$ annehmen, da sich jedes $\lambda \in K$ mit $\chi(N(\lambda)) = 1$ darstellen läßt in der Form $\lambda = \frac{\lambda_1}{\lambda_2}$ mit $\lambda_1, \lambda_2 \in \mathcal{O}_K$ und $\chi(N(\lambda_1)) = \chi(N(\lambda_2)) = 1$.
Hier beachte man, daß es immer ein $u \in \mathcal{O}_K$ mit $\chi(N(u)) = -1$ gibt.

(i) Wir betrachten zunächst den Fall, daß ein $i \in \{1,2\}$ existiert, so daß $N(\lambda)$ bzw. λ zu D_i teilerfremd ist.
Dann folgt
$$\tilde{\psi}((\lambda)) = \psi_{D_i}(N((\lambda)))$$
mit $N((\lambda)) = a \cdot N(\lambda)$ für ein geeignetes $a \in \mathbb{F}_p^{*^2}$.
Es ist also $\psi_{D_i}(a \cdot N(\lambda)) = 1$ zu zeigen. Dazu sei $\lambda = A + B\sqrt{D_1 D_2}$. Es ist dann
$$\psi_{D_i}(a(A^2 - B^2 D_1 D_2)) = \psi_{D_i}(aA^2) = 1$$
nach Lemma 9.1.7, denn $aN(\lambda) \equiv aA^2 \mod D_i$ und $\chi(aN(\lambda)) = 1 = \chi(aA^2)$ wegen $a \in \mathbb{F}_p^{*^2}$.

(ii) Sei nun $\lambda \in \mathcal{O}_K$ beliebig mit $\chi(N(\lambda)) = 1$, und
$$(\lambda) = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \mathfrak{a}$$
mit $\mathfrak{p}_i | D_1 D_2$ und $(\mathfrak{a}, D_1 D_2) = 1$.
Für jedes $j \in \{1, \ldots, r\}$ wählen wir nun ein ganzes Ideal $\mathfrak{a}_j$ in der engen Idealklasse von $\mathfrak{p}_j^{-1}$, das zu $D_1 D_2$ teilerfremd ist (dies ist möglich nach Lemma 8.6.9). Dann ist $\mathfrak{p}_j \mathfrak{a}_j$ ein zu D_1 oder D_2 teilerfremdes enges Hauptideal, d.h. von der Form $\mathfrak{p}_j \mathfrak{a}_j = (\mu_j)$ mit $\chi(N(\mu_j)) = 1$, und es gilt
$$\tilde{\psi}(\mathfrak{p}_j \mathfrak{a}_j) = 1$$
nach (i). Weiterhin haben wir
$$(\lambda) = (\mathfrak{p}_1 \mathfrak{a}_1) \cdot \ldots \cdot (\mathfrak{p}_r \mathfrak{a}_r) \cdot \underbrace{(\mathfrak{a} \mathfrak{a}_1^{-1} \cdot \ldots \cdot \mathfrak{a}_r^{-1})}_{\text{zu } D_1 D_2 \text{ teilerfremdes enges Hauptideal}},$$
woraus wieder $\tilde{\psi}((\lambda)) = 1$ nach (i) folgt.

Aus (i) und (ii) erhält man, daß $\tilde{\psi}$ ein Geschlechtscharakter der engen Idealklassen ist.

Die Identität der L-Reihen zeigt man folgendermaßen:
Es ist
$$L_{\tilde{\psi}}(s) = \prod_P \prod_{\mathfrak{p}|P} \left(1 - \frac{\tilde{\psi}(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1},$$
und wir betrachten die folgenden Fälle:

<u>1.Fall:</u> $\left[\frac{D_1 D_2}{P}\right] = 1$, $(P) = \mathfrak{p}\overline{\mathfrak{p}}$ in K und $N(\mathfrak{p}) = P \nmid D_i$ $(i = 1,2)$.

Dann ist
$$\tilde{\psi}(\mathfrak{p}) = \tilde{\psi}(\overline{\mathfrak{p}}) = \psi_{D_1}(P) = \psi_{D_2}(P)$$
und damit
$$\prod_{\mathfrak{p}|P} \left(1 - \frac{\tilde{\psi}(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} = \left(1 - \frac{\psi_{D_1}(P)}{|P|^s}\right)^{-1} \left(1 - \frac{\psi_{D_2}(P)}{|P|^s}\right)^{-1}.$$

2.Fall: $[\frac{D_1D_2}{P}] = -1$, $(P) = \mathfrak{p}$, $N(\mathfrak{p}) = P^2$, $\tilde{\psi}(\mathfrak{p}) = 1$ und $\psi_{D_1}(P) = -\psi_{D_2}(P)$.

Dann folgt

$$\prod_{\mathfrak{p}|P}\left(1-\frac{\tilde{\psi}(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} = \left(1-\frac{1}{|P|^{2s}}\right)^{-1} = \left(1-\frac{1}{|P|^s}\right)^{-1}\left(1+\frac{1}{|P|^s}\right)^{-1}$$

$$= \left(1-\frac{\psi_{D_1}(P)}{|P|^s}\right)^{-1}\left(1-\frac{\psi_{D_2}(P)}{|P|^s}\right)^{-1}.$$

3.Fall: $[\frac{D_1D_2}{P}] = 0$, $(P) = \mathfrak{p}^2$, $N(\mathfrak{p}) = P$.
Es sei o.E. $\psi_{D_1}(P) = 0$, dann ist $\tilde{\psi}(\mathfrak{p}) = \psi_{D_2}(P)$, da D_1D_2 quadratfrei ist.

Es gilt

$$\prod_{\mathfrak{p}|P}\left(1-\frac{\tilde{\psi}(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} = \left(1-\frac{\psi_{D_2}(P)}{|P|^s}\right)^{-1}$$

$$= \left(1-\frac{\psi_{D_1}(P)}{|P|^s}\right)^{-1}\left(1-\frac{\psi_{D_2}(P)}{|P|^s}\right)^{-1}.$$

Die Fälle 1-3 liefern dann die behauptete Formel.

Es bleibt zu zeigen, daß sämtliche so entandenen Geschlechtscharaktere verschieden sind, denn dann hat man sämtliche 2^{s-1} Geschlechtscharaktere durch obige Konstruktion gefunden.
Dazu sei ψ_i der der Zerlegung $D = P_iP_1\cdot\ldots\cdot P_{i-1}P_{i+1}\cdot\ldots\cdot P_s$ zugeordnete Charakter. Für eine allgemeine Zerlegung $D = D_1D_2$ mit $D_2 = P_{i_1}\cdot\ldots\cdot P_{i_m}$ ist dann der entsprechende Charakter $\tilde{\psi}$ gleich $\psi_{i_1}\cdot\ldots\cdot\psi_{i_m}$. Mit anderen Worten, die Charaktere, die wir konstruiert haben, bilden eine Gruppe

$$G = <\psi_1, \ldots, \psi_s>$$

mit den Relationen $\psi_i^2 = 1$ und $\psi_1\cdot\ldots\cdot\psi_s = 1$. Wir müssen nun nur noch zeigen, daß der zu einer Zerlegung $D = D_1D_2$ gehörige Charakter $\tilde{\psi}$ genau dann der triviale Charakter ist, wenn $D_1 = 1$ oder $D_2 = 1$ gilt.
Dies ist jedoch der Fall, da für $D_1 \neq 1 \neq D_2$ sowohl $L_{\psi_{D_1}}(s)$ als auch $L_{\psi_{D_2}}(s)$ nach Satz 9.2.3 in $s = 1$ holomorph sind, $\tilde{\psi}$ also nicht der triviale Charakter sein kann. Denn sonst wäre

$$L_{\tilde{\psi}}(s) = Z_K(s) = Z_k(s)L_D(s)$$

und hätte nach Satz 9.2.4 einen Pol 1. Ordnung bei $s = 1$.

□

11.3.3 Lemma

Es sei $D = D_1D_2$ eine Zerlegung eines normierten $D \in \mathbb{F}_p[X]\backslash\mathbb{F}_p[X]^2$ mit $\operatorname{grad} D \equiv 0\ (2)$ in zwei Polynome $D_1, D_2 \in \mathbb{F}_p[X]$ mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 1\ (2)$. Ist ψ_1 der zu dieser Zerlegung gehörige Geschlechtscharakter, so handelt es sich bei ψ_1 um einen *echten* Geschlechtscharakter von $C^+(K)$.

Sind jedoch D_1 und D_2 Polynome von geradem Grad, so ist der zu dieser Zerlegung gehörige Geschlechtscharakter ψ_2 auch schon ein reeller Charakter von $C(K)$, d.h. es gilt $\psi_2((\lambda)) = 1$ für *alle* $\lambda \in K$.

Echte Geschlechtscharaktere kann es also nur dann geben, wenn D von einer Primfunktion ungeraden Grades geteilt wird, ihre Anzahl beträgt dann 2^{s-2}.

BEWEIS:

Die Behauptung ist bewiesen, wenn wir zeigen, daß für alle $\lambda \in K$ mit $\chi(N(\lambda)) = -1$ $\psi_1((\lambda)) = -1$ und $\psi_2((\lambda)) = 1$ gilt.
Wir können wie im Beweis des vorigen Satzes o.E. annehmen, daß es sich bei dem Element $\lambda := A + B\sqrt{D}$ um ein Element von $\mathcal{O}_K$ handelt mit $((\lambda), D_1) = 1$. Es ist hier $N((\lambda)) = aN(\lambda) = a(A^2 - B^2 D_1 D_2)$ mit einem $a \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$ nach Definition 8.5.1.
Betrachten wir ψ_1 als den zur Zerlegung $D_1 D_2$ gehörigen Geschlechtscharakter, so ist $\operatorname{grad} D_1$ ungerade, und es gilt

$$\begin{aligned}
\psi_1((\lambda)) &= \psi_{D_1}((\lambda)) = \left[\frac{-D_1}{a(A^2 - B^2 D_1 D_2)}\right] \\
&\overset{9.1.3\,(\mathrm{iv})}{=} \chi(-1)^{\operatorname{grad}(A^2 - B^2 D_1 D_2)} \left[\frac{D_1}{a(A^2 - B^2 D_1 D_2)}\right] \\
&\overset{9.1.3\,(\mathrm{iv}),(\mathrm{v})}{=} \chi(-1)^{2\cdot\operatorname{grad}(A^2 - B^2 D_1 D_2)} \chi(a)^{\operatorname{grad} D_1} \left[\frac{A^2 - B^2 D_1 D_2}{D_1}\right] \\
&\overset{9.1.3\,(\mathrm{ii})}{=} \chi(a)^{\operatorname{grad} D_1} \left[\frac{A^2}{D_1}\right] \\
&\overset{\chi(a)=-1,\ \operatorname{grad} D_1 \text{ ung.}}{=} -\left[\frac{A^2}{D_1}\right] = -1.
\end{aligned}$$

Im Fall ψ_2 ist $\operatorname{grad} D_1$ gerade, und wir erhalten

$$\begin{aligned}
\psi_2((\lambda)) &= \left[\frac{D_1}{a(A^2 - B^2 D_1 D_2)}\right] \overset{9.1.3\,(\mathrm{v})}{=} \left[\frac{a(A^2 - B^2 D_1 D_2)}{D_1}\right] \\
&\overset{9.1.3\,(\mathrm{ii}),(\mathrm{iii})}{=} \chi(a)^{\operatorname{grad} D_1} \left[\frac{A^2}{D_1}\right] \overset{\operatorname{grad} D_1 \text{ gerade}}{=} 1.
\end{aligned}$$

□

11.4 Bestimmung der verschiedenen Geschlechtscharaktere im imaginär-quadratischen Funktionenkörper

Bei der Untersuchung der Geschlechtscharaktere in imaginär-quadratischen Funktionenkörpern halten wir uns an die Fallunterscheidung von Satz 10.3.1. Wir erhalten den

11.4.1 Satz

In den Bezeichnungen und mit den Fallunterscheidungen des Satzes 10.3.1 existieren in den Fällen (i)(1), (ii)(1), (ii)(3) und (iii) genau 2^s Geschlechter bzw. Geschlechtscharaktere. In allen übrigen Fällen beträgt ihre Anzahl 2^{s-1}.

BEWEIS:

Dies folgt aus Bemerkung 11.1.2 in Verbindung mit Satz 10.3.1. □

Der folgende Satz zeigt, daß man tatsächlich in den Fällen (i)(1), (ii)(1) und (ii)(3) zu jeder Zerlegung von D zwei verschiedene Geschlechtscharaktere erhält.

11.4.2 Satz

(i) (1) Es sei $D = P_1 \cdot \ldots \cdot P_s$ ein normiertes quadratfreies Polynom, und es gelte $\chi(-1) = 1$. Ferner sei $K = k(\sqrt{gD})$. Dann existieren zu jeder Zerlegung $D = D_1 D_2$ in zwei normierte Polynome $D_1, D_2 \in \mathbb{F}_p[X]$ zwei verschiedene Geschlechtscharaktere von $C^+(K)$. Diese erhält man, indem man die auf Primidealen $\mathfrak{p}$ von K definierten Abbildungen

$$\tilde{\psi}_1(\mathfrak{p}) := \begin{cases} \psi_{gD_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{D_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

und

$$\tilde{\psi}_2(\mathfrak{p}) := \begin{cases} \psi_{D_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{gD_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

wie in Satz 11.3.2 multiplikativ auf alle gebrochenen Ideale fortsetzt. Die sämtlichen so entstehenden Geschlechtscharaktere sind verschieden, und für die zugehörigen L-Reihen erhält man die Zerlegungen

$$L_{\tilde{\psi}_1}(s) = L_{\psi_{gD_1}}(s) L_{\psi_{D_2}}(s) \quad L_{\tilde{\psi}_2}(s) = L_{\psi_{D_1}}(s) L_{\psi_{gD_2}}(s).$$

(2) Es sei $K = k(\sqrt{D})$ mit einem normierten quadratfreien Polynom $D = P_1 \cdot \ldots \cdot P_s$ von ungeradem Grad. Gilt noch zusätzlich $\chi(-1) = 1$, so existiert zu jeder Zerlegung $D = D_1 D_2$ mit normierten Polynomen $D_1, D_2 \in \mathbb{F}_p[X]$ ein Geschlechtscharakter von $C^+(K)$. Diesen erhält man, indem man die auf den Primidealen $\mathfrak{p}$ von K definierte Abbildung

$$\tilde{\psi}(\mathfrak{p}) := \begin{cases} \psi_{D_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{D_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

wie in Satz 11.3.2 auf alle gebrochenen Ideale fortsetzt.

(ii) (1) Es sei $\chi(-1) = -1$ und $D = P_1 \cdot \ldots \cdot P_s$ ein normiertes quadratfreies Polynom geraden Grades und $K := k(\sqrt{gD})$. Dann gibt es zu jeder Zerlegung $D = D_1 D_2$ in zwei normierte Polynome zwei Geschlechtscharaktere auf $C^+(K)$. Diese erhält man wie in (i)(1).

(2) Ist $\chi(-1) = -1$, $D = P_1 \cdot \ldots \cdot P_s$ ein normiertes quadratfreies Polynom ungeraden Grades und $K = k(\sqrt{gD})$, so existiert zu jeder Zerlegung $D = D_1 D_2$ in normierte Polynome mit $\operatorname{grad} D_1 \equiv 1\ (2)$ und $\operatorname{grad} D_2 \equiv 0\ (2)$ ein Geschlechtscharakter auf $C^+(K)$. Dieser ist analog zu (i) (2) gegeben durch die Fortsetzung der auf den Primidealen $\mathfrak{p}$ von K definierten Abbildung

$$\tilde{\psi}(\mathfrak{p}) := \begin{cases} \psi_{D_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{D_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1. \end{cases}$$

(3) Ist $D = P_1 \cdot \ldots \cdot P_s$ ein quadratfreies und normiertes Polynom ungeraden Grades, $K = k(\sqrt{D})$, und gilt zusätzlich $\chi(-1) = -1$, so existieren zu jeder Zerlegung $D = D_1 D_2$ zwei verschiedene Geschlechtscharaktere von $C^+(K)$. Diese erhält man, indem man die auf den Primidealen $\mathfrak{p}$ von K definierten Abbildungen

$$\tilde{\psi}_1(\mathfrak{p}) := \begin{cases} \psi_{gD_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{D_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

und

$$\tilde{\psi}_2(\mathfrak{p}) := \begin{cases} \psi_{D_1}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_1) = 1, \\ \psi_{gD_2}(N(\mathfrak{p})), & \text{falls } (N(\mathfrak{p}), D_2) = 1 \end{cases}$$

auf alle gebrochenen Ideale wie in Satz 11.3.2 fortsetzt.

Sämtliche L-Reihen aus (i)(2)-(ii)(3) zerlegen sich analog zu (i)(1).

BEWEIS:

(i) (1) Hinsichtlich der Wohldefiniertheit von $\tilde{\psi}_1$ und $\tilde{\psi}_2$ verläuft der Fall des trägen Primideals P mit $N(\mathfrak{p}) = P^2$ wie im Beweis des Satzes 11.3.2.
Ist $N(\mathfrak{p}) = P$ zerlegt, so ist hier

$$\left[\frac{gD_1D_2}{N(\mathfrak{p})}\right] = \psi_{gD_1}(N(\mathfrak{p}))\psi_{D_2}(N(\mathfrak{p})) = \psi_{D_1}(N(\mathfrak{p}))\psi_{gD_2}(N(\mathfrak{p}))$$

zu zeigen. Wegen $\chi(-1) = 1$ gilt aber

$$\begin{aligned} \left[\frac{gD_1D_2}{N(\mathfrak{p})}\right] &= \left[\frac{gD_1}{N(\mathfrak{p})}\right]\left[\frac{D_2}{N(\mathfrak{p})}\right] \\ &= \left[\frac{g(-1)^{\operatorname{grad} D_1}D_1}{N(\mathfrak{p})}\right]\left[\frac{(-1)^{\operatorname{grad} D_2}D_2}{N(\mathfrak{p})}\right] \\ &= \psi_{gD_1}(N(\mathfrak{p}))\psi_{D_2}(N(\mathfrak{p})). \end{aligned}$$

Es bleibt der Nachweis der Eigenschaft

$$\tilde{\psi}_i((\lambda)) = 1 \quad \text{für } i = 1,2 \text{ und } \lambda \in \mathcal{O}_K \text{ mit } \chi(N(\lambda)) = 1.$$

Daß dies richtig ist beruht darauf, daß nach Lemma 4.1.7 (ii) (2) und (3) das Polynom $N(\lambda) = A^2 - gB^2D \in \mathbb{F}_p[X]$ sowohl im Fall $\operatorname{grad} D \equiv 0$ (2) als auch im Fall $\operatorname{grad} D \equiv 1$ (2) immer geraden Grad besitzt, falls $\chi(N(\lambda)) = 1$ gelten soll.
Sei also o.B.d.A. $\tilde{\psi}_1$ betrachtet und λ zu D_1 teilerfremd. Dann ist wieder $N((\lambda)) = aN(\lambda)$ mit $a \in \mathbb{F}_p^{*2}$ und

$$\tilde{\psi}_1(aN(\lambda)) = \left[\frac{g(-1)^{\operatorname{grad} D_1}D_1}{aN(\lambda)}\right]$$

$$\overset{\operatorname{grad} N(\lambda) \equiv 0(2)}{=} \psi_{D_1}(aN(\lambda)) \overset{9.1.7}{=} \psi_{D_1}(aA^2) = 1.$$

Denn D_1 ist normiert, und es gilt

$$\chi(aN(\lambda)) = 1 = \chi(aA^2) \quad \text{sowie} \quad aN(\lambda) \equiv aA^2 \mod D_1.$$

Das Zerlegungsverhalten der L-Reihen zeigt man sowohl hier als auch in den Punkten (i)(2)-(ii)(3) wie im reell-quadratischen Fall (vgl. Satz 11.3.2) und führt die Tatsache, daß die so gefundenen Geschlechtscharaktere paarweise verschieden sind, ebenso auf diese Untersuchungen zurück.

(2) Die Wohldefiniertheit zeigt man wie in (i)(1) unter Ausnutzung der Voraussetzung $\chi(-1) = 1$. Weiterhin gilt $\psi_{D_i}(aN(\lambda)) = \psi_{D_i}(aA^2) = 1$ mit den selben Schlußweisen wie unter (i)(1).

(ii) (1) Für die Wohldefiniertheit nutzt man die Tatsache aus, daß $\operatorname{grad} D \equiv 0\ (2)$, also $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2\ (2)$ gilt. Daraus erhält man

$$\left[\frac{gD_1D_2}{N(\mathfrak{p})}\right] = \left[\frac{g(-1)^{\operatorname{grad} D_1}D_1}{N(\mathfrak{p})}\right]\left[\frac{(-1)^{\operatorname{grad} D_2}D_2}{N(\mathfrak{p})}\right] = \psi_{gD_1}(N(\mathfrak{p}))\psi_{D_2}(N(\mathfrak{p})).$$

Der Nachweis der restlichen Eigenschaften verläuft wie in (i)(1), denn in diesem Fall haben nach Lemma 4.1.7 (ii) (3) die Normen **aller** Elemente $\lambda \in \mathcal{O}_K$ geraden Grad.

(2) Die Wohldefiniertheit der Abbildung $\tilde{\psi}$ zeigt man mit $\operatorname{grad} D_1 \equiv 1\ (2)$ und $\chi(g)^{\operatorname{grad} D_1} = \chi(-1)^{\operatorname{grad} D_1} = -1$. Denn unter diesen Voraussetzungen gilt

$$\left[\frac{gD_1D_2}{N(\mathfrak{p})}\right] = \left[\frac{(-1)^{\operatorname{grad} D_1}D_1}{N(\mathfrak{p})}\right]\left[\frac{(-1)^{\operatorname{grad} D_2}D_2}{N(\mathfrak{p})}\right] = \psi_{D_1}(N(\mathfrak{p}))\psi_{D_2}(N(\mathfrak{p})).$$

Die Charaktereigenschaften folgen wie in (i)(2) aus Lemma 9.1.7.

(3) Die Wohldefiniertheit folgt wie in (ii)(2) aus $\chi(g)^{\operatorname{grad} D_i} = \chi(-1)^{\operatorname{grad} D_i}$ für $i = 1, 2$. Es ist nämlich

$$\begin{aligned}\psi_{gD_1}(N(\mathfrak{p}))\psi_{D_2}(N(\mathfrak{p})) &= \psi_{D_1}(N(\mathfrak{p}))\psi_{gD_2}(N(\mathfrak{p})) \\ &= \left[\frac{g(-1)^{\operatorname{grad} D_1}(-1)^{\operatorname{grad} D_2}D_1D_2}{N(\mathfrak{p})}\right] \\ &= \left[\frac{D_1D_2}{N(\mathfrak{p})}\right].\end{aligned}$$

Wie in (i)(1) erkennt man weiter, daß es wegen Lemma 4.1.7 (ii) (1) kein Element $\lambda \in \mathcal{O}_K$ mit der Eigenschaft $\chi(N(\lambda)) = 1$ gibt, für welches $\operatorname{grad} N(\lambda) \equiv 1\ (2)$ gilt. Die Behauptung folgt dann mit Lemma 9.1.7 durch analoge Schlußweisen.

□

Bezüglich der echten Geschlechtscharaktere in imaginär-quadratischen Funktionenkörpern erhalten wir ähnliche Ergebnisse wie im reell-quadratischen Fall.
In den Fällen 11.4.2 (i)(2) und (ii)(2) existieren keine Elemente negativer Norm, d.h. weite und enge Klassen fallen zusammen.
In allen anderen Fällen läßt sich wie im reell-quadratischen Fall die Existenz echter Geschlechtscharaktere daran festmachen, ob D durch ein Primpolynom ungeraden Grades teilbar ist oder nicht.

11.4.3 Lemma

Ist D in den Fällen 11.4.2 (i)(1), (ii)(1) oder (ii)(3) durch ein Primpolynom ungeraden Grades teilbar, so befinden sich unter den 2^s Geschlechtscharakteren 2^{s-1} echte.

Diese sind im Fall (i)(1) und $\operatorname{grad} D$ gerade ebenso wie im Fall (ii)(1) genau diejenigen, die zu einer Zerlegung $D = D_1 D_2$ mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 1\ (2)$ gehören.

Im Fall (i)(1) und $\operatorname{grad} D \equiv 1\ (2)$ und in (ii)(3) sind dies in den Bezeichnungen von 11.4.2 jeweils die Charaktere $\tilde{\psi}_1$ mit $\operatorname{grad} D_1 \equiv 0\ (2)$.

BEWEIS:

Es sei $\lambda := A + B\sqrt{g^j D} \in \mathcal{O}_K$ $(j \in \{0,1\})$ ein Element mit

$$\chi(N(\lambda)) = \chi(A^2 - g^j B^2 D) = -1.$$

Dann ist $N((\lambda)) = aN(\lambda)$ für ein $a \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$. Wir betrachten die Fälle (i)(1), (ii)(1) und (ii)(3) getrennt:

(i)(1) In diesem Fall gilt

$$\operatorname{grad} N(\lambda) = \operatorname{grad}(A^2 - gB^2 D) \equiv \operatorname{grad} D\ (2)$$

wegen $\chi(-1) = 1$.
Es sei zunächst $\operatorname{grad} D \equiv 0\ (2)$ und $D = D_1 D_2$ eine Zerlegung von D mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 0\ (2)$. Dann kann man wie oben o.E. $(N(\lambda), D_1) = 1$ annehmen, und man erhält

$$\tilde{\psi}_1((\lambda)) = \left[\frac{gD_1}{aN(\lambda)}\right] = 1 = \left[\frac{D_1}{aN(\lambda)}\right] = \tilde{\psi}_2((\lambda))$$

nach Satz 9.1.3, da wegen $\operatorname{grad} D_1 \equiv \operatorname{grad} N(\lambda) \equiv 0\ (2)$ Zähler und Nenner beliebig vertauschbar sind und auch die Faktoren aus $\mathbb{F}_p^*$ ohne Veränderung des Vorzeichens aus den Restsymbolen ausgeklammert werden können.
Ist jedoch $D = D_1 D_2$ mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 1\ (2)$, so gilt

$$\tilde{\psi}_1((\lambda)) = \left[\frac{-gD_1}{aN(\lambda)}\right] \overset{\operatorname{grad} N(\lambda) \equiv 0\ (2)}{=} \left[\frac{D_1}{aN(\lambda)}\right]$$
$$\overset{\operatorname{grad} N(\lambda) \equiv 0\ (2)}{=} \left[\frac{aN(\lambda)}{D_1}\right] = -1$$

nach Satz 9.1.3.
Denn es ist $\operatorname{grad} D_1 \equiv 1\ (2)$, $a \in \mathbb{F}_p^* \backslash \mathbb{F}_p^{*2}$, und es gilt $N(\lambda) \equiv A^2 \mod D_1$. Dies zeigt man analog auch für $\tilde{\psi}_2$.
Ist $\operatorname{grad} D$ ungerade und $D = D_1 D_2$ mit $\operatorname{grad} D_1 \equiv 1\ (2)$ und $\operatorname{grad} D_2 \equiv 0\ (2)$, so zeigt man mit denselben Schlüssen

$$\tilde{\psi}_1((\lambda)) = -1 = -\tilde{\psi}_2((\lambda)).$$

(ii)(1) Dieser Fall verläuft analog zu (i)(1) $(\operatorname{grad} D \equiv 0\ (2))$, wenn man benutzt, daß $\operatorname{grad} N(\lambda) \equiv 0\ (2)$ für **alle** $\lambda \in \mathcal{O}_K$ gilt.

(ii)(3) Aus der Darstellung $N(\lambda) = A^2 - B^2 D$ erhält man wegen $\chi(-1) = -1$, daß für alle $\lambda \in \mathcal{O}_K$ mit $\chi(N(\lambda)) = -1$ auch $\operatorname{grad} N(\lambda) \equiv 1\ (2)$ gelten muß. Somit ist auch dieser Fall auf (i)(1) $(\operatorname{grad} D \equiv 1\ (2))$ zurückzuführen.

□

Für die imaginär-quadratischen Funktionenkörper $k(\sqrt{D})$ bzw. $k(\sqrt{gD}) \neq k(\sqrt{g})$ mit einem normierten quadratfreien $D \in \mathbb{F}_p[X]$ erhält man für die Fälle $\chi(-1) = 1$ und $\chi(-1) = -1$ nun zusammenfassend die Tabellen 1 und 2.

Tabelle 1: Imaginär-quadratische Körper mit $\chi(-1) = 1$

$\chi(-1) = 1$:	I	II	III	IV
Körper	$k(\sqrt{gD})$	$k(\sqrt{gD})$	$k(\sqrt{gD})$	$k(\sqrt{D})$
grad D	gerade		ungerade	
$\exists\ P$, grad P ungerade, $P \mid D$?	nein	ja	ja	ja
$\exists\ u,\ \chi(N(u)) = -1$?	ja ($\sqrt{gD}$)	ja ($\sqrt{gD}$)	ja ($\sqrt{gD}$)	nein
irreguläre enge ambige Klassen	keine			
$\#G^+(K)$	2^s	2^s	2^s	2^{s-1}
$\#G(K)$	2^s	2^{s-1}	2^{s-1}	2^{s-1}
Anzahl enger ambiger Hauptideale	1			2
Charaktere der Zerlegungen	$\psi_{gD_1}\psi_{D_2}$ $\psi_{D_1}\psi_{gD_2}$			$\psi_{D_1}\psi_{D_2}$
grad $N(\mu)$ m. $\chi(N(\mu)) = 1$	gerade			
$h^+(K)$ ungerade $\Leftrightarrow$	nie			$s = 1$
$h(K)$ ungerade $\Leftrightarrow$	nie		$s = 1$	
$\frac{h^+(K)}{h(K)}$	2			1

Tabelle 2: Imaginär-quadratische Körper mit $\chi(-1) = -1$

$\chi(-1) = -1$:	I	II	III	IV
Körper	$k(\sqrt{gD})$	$k(\sqrt{gD})$	$k(\sqrt{gD})$	$k(\sqrt{D})$
grad D	gerade		ungerade	
$\exists\ P$, grad P ungerade, $P \mid D$?	nein	ja	ja	ja
$\exists\ u,\ \chi(N(u)) = -1$?	ja (vgl. 4.1.6)	ja (vgl. 4.1.6)	nein	ja ($\sqrt{D}$)
irreguläre enge ambige Klassen	ja		keine	
$\#G^+(K)$	2^s	2^s	2^{s-1}	2^s
$\#G(K)$	2^s	2^{s-1}	2^{s-1}	2^{s-1}
Anzahl enger ambiger Hauptideale	2			1
Charaktere der Zerlegungen	$\psi_{gD_1}\psi_{D_2}$ $\psi_{D_1}\psi_{gD_2}$		$\psi_{D_1}\psi_{D_2}$	$\psi_{gD_1}\psi_{D_2}$ $\psi_{D_1}\psi_{gD_2}$
grad $N(\mu)$ m. $\chi(N(\mu)) = 1$	gerade			gerade
$h^+(K)$ ungerade $\Leftrightarrow$	nie		$s = 1$	nie
$h(K)$ ungerade $\Leftrightarrow$	nie		$s = 1$	
$\frac{h^+(K)}{h(K)}$	2		1	2

Die Aussagen über die Anzahl der Geschlechter in der weiten Idealklassengruppe und über die weite Klassenzahl wurden der Tabelle I aus [Zh], S. 427 entnommen.
Die Ergebnisse über die Geschlechter und die ambigen Klassen bezüglich der engen Klasseneinteilung im reell-quadratischen Funktionenkörper $K = k(\sqrt{D})$ mit der Grundeinheit $\epsilon_0 \in \mathcal{O}_K^*$ fasst die Tabelle 3 zusammen.

Tabelle 3: Enge Geschlechter in reell-quadratischen Körpern

	I	II	III	IV	V
$N(\epsilon_0)$	g	1			
$\chi(-1)$		1	-1	1	-1
$\chi(\epsilon_0)$		1		-1	
irreguläre enge ambige Klassen	keine	ja	keine		
Anzahl enger ambiger Hauptideale	2	4	2		
$\#G^+(K)$	2^{s-1}				
Q_K	1	2			
$h^+(K)$ ungerade $\Leftrightarrow$	$s=1$	nie			

Vergleicht man wiederum die Aussagen über die engen Klassen mit denen von ZHANG über die weiten Klassen, so ergibt sich wie schon im imaginär-quadratischen Fall ein Zusammenhang dazu, ob D durch ein Polynom ungeraden Grades teilbar ist oder nicht.

Tabelle 4: Enge und weite Geschlechter in reell-quadratischen Körpern

	I	II	III
$N(\epsilon_0)$	g	1	1
$\exists\ P$, grad P ungerade, $P \mid D$?	nein	nein	ja
$\#G(K)$	2^{s-1}	2^{s-1}	2^{s-2}
$\frac{\#G^+(K)}{\#G(K)}$	1	1	2
$h(K)$ ungerade $\Leftrightarrow$	$s=1$	nie	$s=2$

Als Ergänzung zu den Ergebnissen von ZHANG haben wir somit nach 11.3.3 und 11.4.3 auch sämtliche Geschlechtscharaktere zur weiten Klasseneinteilung bestimmt.

11.4.4 Lemma

Ist $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper, so sind die Geschlechtscharaktere zur weiten Klasseneinteilung genau die in Satz 11.3.2 definierten, welche zu einer Zerlegung $D = D_1 D_2$ mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 0\ (2)$ gehören.

Ist $K = k(\sqrt{g^j D})$ $(j \in \{0, 1\})$ ein imaginär-quadratischer Funktionenkörper, so sind die Geschlechtscharaktere zur weiten Klasseneinteilung im Fall 11.4.2 (i)(1) ($\operatorname{grad} D$ gerade) und (ii)(1) genau die, welche zu einer Zerlegung $D = D_1 D_2$ mit $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 0\ (2)$ gehören. In den Fällen (i)(1) ($\operatorname{grad} D$ ungerade) und (ii)(3) sind dies die Geschlechtscharaktere $\tilde{\psi}_2$ mit $\operatorname{grad} D_1 \equiv 0\ (2)$, und in den Fällen (i)(2) und (ii)(2) sind sämtliche angegebenen Charaktere genau die Geschlechtscharaktere zur weiten Idealklasseneinteilung.

Teil V
Klassenzahl-Produktformeln

12 Klassenzahl-Produkte als Werte von $L_{\tilde{\psi}}(s)$

In diesem Kapitel werden wir Formeln für das Produkt von Klassenzahlen zweier quadratischer Funktionenkörper aufstellen.
Unsere Vorgehensweise ähnelt derjenigen im Zahlkörperfall zur Berechnung der sogenannten *Relativklassenzahl* biquadratischer Zahlkörper. Hierzu vergleiche man z.B. die Ausführungen in [Ha2]. Wir untersuchen im wesentlichen den Quotienten aus der Zeta-Funktion eines biquadratischen Funktionenkörpers $L = k(\sqrt{D_1}, \sqrt{D_2})$ ($D_1, D_2 \in \mathbb{F}_p[X]$ teilerfremd, $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2$ (2) und $\chi(D_1) = \chi(D_2)$) und der Zeta-Funktion des reell-quadratischen Unterkörpers $K = k(\sqrt{D_1 D_2})$ von L. Dieser Quotient erweist sich in vielen Fällen als L-Funktion zu einem Geschlechtscharakter der engen Klassengruppe von K.
Zur Herleitung der Formeln für das Produkt der Klassenzahlen $h(D_1)h(D_2)$ wird es daher nötig werden, gewisse Werte von L-Funktionen zu Geschlechtscharakteren der engen Idealklassengruppe zu bestimmen.
Wir beschreiben zunächst die zugrundeliegende Ausgangssituation.

12.1 Situation

Wir betrachten ein normiertes quadratfreies Polynom $D \in \mathbb{F}_p[X]$ von geradem Grad und zu diesem eine Zerlegung $D = D_1 D_2$ in zwei teilerfremde normierte Funktionen. $K = k(\sqrt{D_1 D_2})$ ist dann ein reell-quadratischer Funktionenkörper.
Dieser sei von nun an immer so gewählt, daß $Q_K = 2$ gilt, also enge und weite Klasseneinteilung verschieden sind.
Nun wählen wir $D_1' \in \{D_1, gD_1\}$ und $D_2' \in \{D_2, gD_2\}$ so, daß $L = k(\sqrt{D_1'}, \sqrt{D_2'})$ mit den Teilkörpern $k_1 = k(\sqrt{D_1'})$, $k_2 = k(\sqrt{D_2'})$ und $K = k(\sqrt{D_1' D_2'}) = k(\sqrt{D_1 D_2})$ zu einem in 4.1.2 (iii) beschriebenen imaginären biquadratischen bizyklischen Funktionenkörper oder einem total-reellen biquadratischen Funktionenkörper wie in 4.1.2 (iv) wird.

Hier sind wegen $\operatorname{grad} D_1' \equiv \operatorname{grad} D_2'$ (2) die folgenden Fälle möglich:

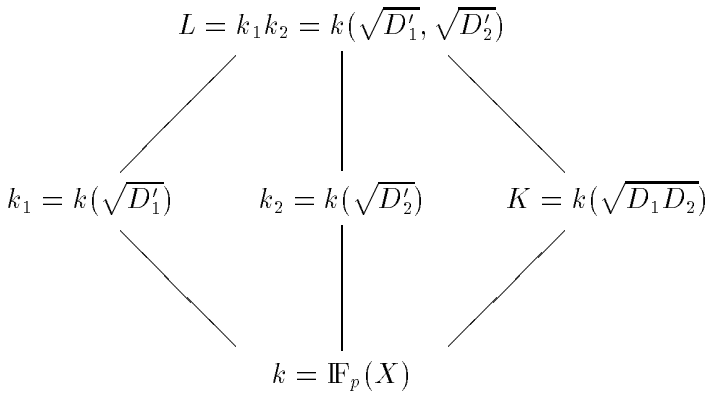
(1) $\operatorname{grad} D_1' \equiv \operatorname{grad} D_2' \equiv 0$ (2) und $D_i' = gD_i$ für $i = 1, 2$. (L imaginär)

(2) $\operatorname{grad} D_1' \equiv \operatorname{grad} D_2' \equiv 1$ (2) und $D_i' = gD_i$ für $i = 1, 2$. (L imaginär)

(3) $\operatorname{grad} D_1' \equiv \operatorname{grad} D_2' \equiv 1$ (2) und $D_i' = D_i$ für $i = 1, 2$. (L imaginär)

(4) $\operatorname{grad} D_1' \equiv \operatorname{grad} D_2' \equiv 0$ (2) und $D_i' = D_i$ für $i = 1, 2$. (L total-reell)

Es ergibt sich die folgende Situation:



12.2 Zeta- und L-Funktionen reell-quadratischer Funktionenkörper K mit $Q_K = 2$

Es sei K ein reell-quadratischer Funktionenkörper mit der Grundeinheit $\epsilon_0 \in \mathcal{O}_K^*$ und der positiven Grundeinheit $\epsilon_1 \in \mathcal{O}_K^*$. Es gelte $N(\epsilon_0) = 1$. Dann sind die enge und weite Klasseneinteilung verschieden, d.h. es gilt $Q_K = 2$.
Nach Lemma 8.2.3 und der Darstellung der Zeta-Funktion aus Kapitel 9.2 ist $Z_K(s)$ dann darstellbar in der Form

$$Z_K(s) = \sum_{\tilde{A} \in C(K)} Z(s, \tilde{A}) = \frac{1}{2} \sum_{A \in C^+(K)} (Z(s, A) + Z(s, uA)),$$

wobei $\tilde{A}$ die weiten Idealklassen, A die engen Idealklassen durchläuft und $u \in \mathcal{O}_K$ ein Element mit $\chi(N(u)) = -1$ ist. Über die Zetafunktion

$$Z(s, A) = \sum_{\mathfrak{a} \in A} \frac{1}{|N(\mathfrak{a})|^s}$$

der engen Idealklasse A kann man folgende Aussagen treffen:

12.2.1 Lemma

Ist $A \in C^+(K)$ eine enge Idealklasse, so gilt

$$Z(s, A) = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \\ \chi(N(\alpha))=1}}{}' \frac{1}{|N(\alpha)|^s}$$

und

$$Z(s, uA) = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \\ \chi(N(\alpha))=-1}}{}' \frac{1}{|N(\alpha)|^s},$$

wobei $\mathfrak{a}$ ein beliebiger ganzer Vertreter der Klasse A und u ein Element mit $\chi(N(u)) = -1$ ist.
Der Strich an der Summe zeigt an, daß jeweils genau ein Element jeder Bahn der Operation von $\epsilon_1^{\mathbb{Z}}$ auf $\mathfrak{a} \cap \{x \in K^* \mid \chi(N(x)) = 1\}$ gewählt werden soll.

Ist $S(\alpha) := \frac{\overline{\alpha}}{\alpha}$ die schon in 4.1.5 definierte Steigung eines Elements $\alpha \in K^*$ und

$$S(\epsilon_1, \epsilon_1^2) := \{\alpha \in K^* \mid |S(\epsilon_1)| \leq |S(\alpha)| < |S(\epsilon_1^2)|\},$$

so erhält man

$$Z(s, A) = |N(\mathfrak{a})|^s \sum_{\mathfrak{b} \in A} \frac{1}{|N(\mathfrak{ab})|^s} = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \cap S(\epsilon_1, \epsilon_1^2) \\ \chi(N(\alpha))=1}} \frac{1}{|N(\alpha)|^s}$$

und ebenso

$$Z(s, uA) = |N(\mathfrak{a})|^s \sum_{\mathfrak{b} \in A} \frac{1}{|N(\mathfrak{ab})|^s} = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \cap S(\epsilon_1, \epsilon_1^2) \\ \chi(N(\alpha))=-1}} \frac{1}{|N(\alpha)|^s}.$$

BEWEIS:

Es sei $A \in C^+(K)$ und $\mathfrak{a}$ ein beliebiger ganzer Vertreter der Klasse A^{-1}.
Ist dann $\mathfrak{b} \in A$, so ist $\mathfrak{ab} = (\alpha)$ mit $\alpha \in K$ und $\chi(N(\alpha)) = 1$.
Ist umgekehrt (α) durch $\mathfrak{a}$ teilbar, so ist $(\alpha) = \mathfrak{ab}$ mit $\mathfrak{b} \in A$. $\mathfrak{ab}$ durchläuft also alle durch $\mathfrak{a}$ teilbaren Hauptideale (α) mit $\chi(N(\alpha)) = 1$, wenn $\mathfrak{b}$ die Ideale aus A durchläuft.
Weiterhin ist $(\alpha) = (\beta)$ mit $\chi(N(\alpha)) = \chi(N(\beta))$ genau dann, wenn α und β *positiv assoziiert* sind, d.h. wenn eine Einheit $\epsilon \in \mathcal{O}_K^{*+}$ existiert mit $\alpha = \epsilon\beta$. Jedes $\epsilon \in \mathcal{O}_K^{*+}$ hat aber nach 4.2.3 eine Darstellung $\epsilon = a\epsilon_1^k$ mit $a \in \mathbb{F}_p^*$ und $k \in \mathbb{Z}$, wobei ϵ_1 die positive Grundeinheit von K ist.
Wegen $|S(\epsilon_1)| > 1$ ist $|S(\epsilon_1)| < |S(\epsilon_1^2)|$. Ist also $\alpha' \in K^*$, so gibt es zu diesem Element genau $p-1$ positiv assoziierte Elemente $\alpha_i \in K^*$ $(i = 1, \ldots, p-1)$ mit

$$|S(\epsilon_1)| \leq |S(\alpha_i)| < |S(\epsilon_1^2)|.$$

Da sich je zwei Elemente $\alpha_i, \alpha_j \in K^*$ nur um einen Faktor aus $\mathbb{F}_p^*$ unterscheiden, gilt $|N(\alpha_i)| = |N(\alpha_j)|$ für alle $i, j \in \{1, \ldots, p-1\}$.
Die Menge

$$S(\epsilon_1, \epsilon_1^2) := \{\alpha \in K^* \mid |S(\epsilon_1)| \leq |S(\alpha)| < |S(\epsilon_1^2)|\}$$

bildet demnach einen Fundamentalbereich für die Operation von $\epsilon_1^{\mathbb{Z}}$ auf K^*. Man erhält also zusammenfassend

$$Z(s, A) = |N(\mathfrak{a})|^s \sum_{\mathfrak{b} \in A} \frac{1}{|N(\mathfrak{ab})|^s} = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \cap S(\epsilon_1, \epsilon_1^2) \\ \chi(N(\alpha))=1}} \frac{1}{|N(\alpha)|^s}.$$

Analog zeigt man

$$Z(s, uA) = |N(\mathfrak{a})|^s \sum_{\mathfrak{b} \in uA} \frac{1}{|N(\mathfrak{ab})|^s} = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\substack{\alpha \in \mathfrak{a} \cap S(\epsilon_1, \epsilon_1^2) \\ \chi(N(\alpha))=-1}} \frac{1}{|N(\alpha)|^s}.$$

Nach Folgerung 8.1.2 gilt $A^{-1} = \overline{A}$. Da aufgrund der Definition von $Z(s, A)$ dann offensichtlich $Z(s, A) = Z(s, \overline{A}) = Z(s, A^{-1})$ gilt, kann das Ideal $\mathfrak{a}$ auch aus A gewählt werden. □

12.2.2 Definition

Es sei X^+ irgendein Fundamentalbereich der Operation von $\epsilon_1^{\mathbb{Z}}$ auf K^*, z.B. $X^+ = S(\epsilon_1, \epsilon_1^2)$, $A \in C^+(K)$ eine enge Idealklasse und $\mathfrak{a} \in A$ ein beliebiger ganzer Vertreter von A. Dann definieren wir die L-Funktion zu A durch

$$L(s,A) := Z(s,A) - Z(s,uA) = \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\alpha \in \mathfrak{a} \cap X^+} \frac{\chi(N(\alpha))}{|N(\alpha)|^s}.$$

Weiterhin sei

$$L_0(s,A) := \frac{|N(\mathfrak{a})|^s}{p-1} \sum_{\alpha \in \mathfrak{a} \cap X^+} \frac{1}{|N(\alpha)|^s}.$$

Die Zeta-Funktion $Z(s,A)$ läßt sich demnach darstellen in der Form

$$Z(s,A) = \frac{1}{2}(L_0(s,A) + L(s,A)),$$

und für die L-Funktionen der engen Geschlechtscharaktere ψ gilt

$$L_\psi(s) = \begin{cases} \frac{1}{2}\sum_{i=1}^{h^+(K)} \psi(\mathfrak{a}_i) L(s,A_i), & \text{falls } \psi \text{ ein } \textit{echter} \text{ Charakter von } C^+(K) \text{ ist} \\ \\ \frac{1}{2}\sum_{i=1}^{h^+(K)} \psi(\mathfrak{a}_i)(Z(s,A_i) + Z(s,uA_i)) & \text{sonst.} \end{cases}$$

12.3 Die Zetafunktion eines biquadratischen Funktionenkörpers

Über die Zetafunktion $Z_L(s)$ von $L = k_1 k_2$ mit $k_i = K(\sqrt{D_i'})$ $(i = 1,2)$ wollen wir nun eine Formel für das Produkt der Klassenzahlen $h(D_1')h(D_2')$ herleiten.

12.3.1 Definition

Es wird $Z_L(s)$ für $\operatorname{Re} s > 1$ definiert durch

$$Z_L(s) := \prod_{\mathfrak{P}} (1 - \frac{1}{|N(\mathfrak{P})|^s})^{-1}.$$

Diese Funktion ist die Zetafunktion des Körpers $L = k(\sqrt{D_1'}, \sqrt{D_2'})$. Das Produkt verläuft hier über alle Primideale $\mathfrak{P} \subset \mathcal{O}_L$.
Das Zerlegungsverhalten der Primideale von K nach L läßt sich nun durch das Zerlegungsverhalten der Primelemente von k nach k_1 bzw. k_2 beschreiben.

12.3.2 Satz

Ist in der Situation 12.1 $Z_L(s)$ die Zetafunktion des Körpers $L = k(\sqrt{D_1'}, \sqrt{D_2'})$, so gilt

$$Z_L(s) = Z_K(s) L_\psi(s) = Z_K(s) \prod_{\mathfrak{p}} \left(1 - \frac{\psi(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1}$$

mit der Zetafunktion $Z_K(s)$ zum reell-quadratischen Unterkörper K von L.

Das Produkt läuft über alle Primideale $\mathfrak{p}$ von K und $\psi : I(K) \to \mathbb{R}$ ist auf Primidealen $\mathfrak{p} \subset \mathcal{O}_K$ definiert durch

$$\psi(\mathfrak{p}) = \begin{cases} 0, & \text{falls } \mathfrak{p} \text{ verzweigt in } L, \\ 1, & \text{falls } \mathfrak{p} \text{ (voll) zerlegt in } L, \text{ und} \\ -1, & \text{falls } \mathfrak{p} \text{ träge in } L. \end{cases}$$

Die Abbildung ψ werde multiplikativ auf alle gebrochenen Ideale durch

$$\psi(\mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_k^{n_k}) = \psi(\mathfrak{p}_1)^{n_1} \cdot \ldots \cdot \psi(\mathfrak{p}_k)^{n_k} \quad (\mathfrak{p}_i \text{ prim}, n_i \in \mathbb{Z})$$

fortgesetzt.

Liegt in der Situation 12.1 Fall (2) vor und gilt $\chi(-1) = -1$ oder ist im Fall (3) $\chi(-1) = 1$, so handelt es sich bei ψ um den nach 11.3.2 zur Zerlegung $D = D_1 D_2$ gehörigen echten Geschlechtscharakter, und es ist

$$L_\psi(s) = L_{\psi_{D_1}}(s) L_{\psi_{D_2}}(s).$$

Im Fall (4) des total-reellen biquadratischen Körpers L ist ψ der zur Zerlegung $D = D_1 D_2$ gehörige Charakter, welcher aber schon ein Element von $\mathfrak{G}(K)$, also kein echter Geschlechtscharakter von $C^+(K)$ ist.

In allen anderen Fällen ist ψ kein Geschlechtscharakter der engen Idealklassen, aber es gilt

$$L_\psi(s + \frac{\pi i}{\log p}) = L_{\tilde{\psi}}(s) = L_{\psi_{D_1}}(s) L_{\psi_{D_2}}(s),$$

wobei $\tilde{\psi}$ der zur Zerlegung $D = D_1 D_2$ gehörige Charakter ist.

BEWEIS:

Es ist

$$\begin{aligned} Z_L(s) &= \prod_{\mathfrak{P} \in L} \left(1 - \frac{1}{|N(\mathfrak{P})|^s}\right)^{-1} \\ &= \prod_{\mathfrak{p} \in K} \prod_{\mathfrak{P} | \mathfrak{p}} \left(1 - \frac{1}{|N(\mathfrak{P})|^s}\right)^{-1} \\ &= \prod_{\mathfrak{p} \text{ verzw.}} \left(1 - \frac{1}{|N(\mathfrak{p})|^s}\right)^{-1} \prod_{\mathfrak{p} \text{ zerl.}} \left(1 - \frac{1}{|N(\mathfrak{p})|^s}\right)^{-2} \prod_{\mathfrak{p} \text{ träge}} \left(1 - \frac{1}{|N(\mathfrak{p})|^{2s}}\right)^{-1} \\ &= Z_K(s) \prod_{\mathfrak{p} \in K} \left(1 - \frac{\psi(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} \end{aligned}$$

nach Umsortieren der Faktoren. Da es aufgrund der Teilerfremdheit von D_1 und D_2 keine in L verzweigten Primideale von K gibt, nimmt ψ nur die Werte ± 1 an.
Um die Aussagen über ψ zu beweisen und die Zerlegung der L-Funktion nachzuweisen, zeigen wir

$$(*) \qquad \psi(\mathfrak{p}) = \psi'(\mathfrak{p}) := \begin{cases} \left[\frac{D_1'}{N(\mathfrak{p})}\right], & \text{falls } (N(\mathfrak{p}), D_1') = 1, \\ \left[\frac{D_2'}{N(\mathfrak{p})}\right], & \text{falls } (N(\mathfrak{p}), D_2') = 1. \end{cases}$$

Im Fall (1) gilt dann nämlich $\psi'(\mathfrak{p}) = \left[\frac{g}{N(\mathfrak{p})}\right] \tilde{\psi}(\mathfrak{p})$, wenn $\tilde{\psi}$ der zu der Zerlegung $D = D_1 D_2$ gehörige Geschlechtscharakter ist. Dann ist ψ kein Geschlechtscharakter mehr. Denn nach Lemma 4.1.7 (i) existiert ein Element $\lambda \in \mathcal{O}_K$ mit $\chi(N(\lambda)) = 1$ und $\operatorname{grad} N(\lambda) \equiv 1$ (2). Hierfür gilt dann nämlich $\psi'((\lambda)) = -1$. Dies gilt ebenso im Fall (2), falls $\chi(-1) = 1$ oder im Fall (3), falls $\chi(-1) = -1$ ist. In den anderen Fällen ist offensichtlich $\psi' = \tilde{\psi}$, also ψ' und dann auch ψ ein Geschlechtscharakter von $C^+(K)$. In den Fällen (2) mit $\chi(-1) = -1$ und (3) mit $\chi(-1) = 1$ handelt es sich hierbei sogar um einen echten Geschlechtscharakter dieser Klassengruppe.

Um $(*)$ zu beweisen, reicht es - da ψ und ψ' nur die Werte ± 1 annehmen - zu zeigen, daß

$$\psi(\mathfrak{p}) = 1 \quad \Leftrightarrow \quad \psi'(\mathfrak{p}) = 1$$

für alle Primideale $\mathfrak{p}$ von K gilt.
Dazu sei $\mathfrak{p} \cap \mathbb{F}_p[X] = (P)$. Nach 8.5.4 ist dann $N(\mathfrak{p}) = P^f$ mit einem $f \in \{1, 2\}$.

"$\Rightarrow$" Ist $\psi(\mathfrak{p}) = 1$, so können nur die folgenden drei Fälle auftreten:

1) P ist träge in K, also $f = 2$, woraus aber sofort $\psi'(\mathfrak{p}) = 1$ folgt.
2) P ist verzweigt in K. Dann muß P aber wegen $\psi(\mathfrak{p}) = 1$ in genau einem $k_i = k(\sqrt{D_i'})$ zerlegt sein. Es folgt $f = 1$ und $P \nmid D_i'$, also $\psi'(\mathfrak{p}) = \left[\frac{D_i'}{P}\right] = 1$.
3) P ist in beiden k_i zerlegt. Dann ist $f = 1$ und $\psi'(\mathfrak{p}) = 1$ offensichtlich.

"$\Leftarrow$" Ist $\psi'(\mathfrak{p}) = 1$, so betrachten wir wieder drei Fälle hinsichtlich des Zerlegungsverhaltens von (P) in K.

1) Ist P träge, also $f = 2$, so folgt

$$\left[\frac{D_1 D_2}{P}\right] = -1 = \left[\frac{D_1'}{P}\right] \cdot \left[\frac{D_2'}{P}\right],$$

eines der beiden Symbole $\left[\frac{D_i'}{P}\right]$ für $i = 1, 2$ muß also den Wert 1 haben. Dann folgt aber $\psi(\mathfrak{p}) = 1$, denn $\mathfrak{p}$ muß dann in L zerlegt sein.

2) Ist P verzweigt in K, so gilt $P | D_i$ für ein $i \in \{1, 2\}$, aber $P \nmid D_j$ für $j \neq i$, da D_1 und D_2 teilerfremd sind. Wegen $\psi'(\mathfrak{p}) = 1$ gilt dann $\left[\frac{D_j'}{P}\right] = 1$, d.h. P ist in k_j zerlegt, woraus wieder $\psi(\mathfrak{p}) = 1$ folgt.
3) Ist P zerlegt in K und $\psi'(\mathfrak{p}) = 1$, so ist P in beiden k_i zerlegt. Nach bekannten Sätzen aus der algebraischen Zahlentheorie (s. z.B. [Sti], S. 121) ist dann P in L voll zerlegt, zerfällt also in L in vier verschiedene Primideale. Man erhält $\psi(\mathfrak{p}) = 1$.

Damit ist $(*)$ bewiesen. Wir haben weiterhin gezeigt, daß

$$\begin{aligned} L_\psi(s) = \prod_{\mathfrak{p} \in K} \left(1 - \frac{\psi(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} &= \prod_{P \in \mathbb{F}_p[X]} \prod_{\mathfrak{p} | P} \left(1 - \frac{\psi(\mathfrak{p})}{|N(\mathfrak{p})|^s}\right)^{-1} \\ &= L_{D_1'}(s) L_{D_2'}(s) \end{aligned}$$

gilt. Dies folgt wie im Beweis des Satzes 11.3.2. Für die Fälle (2) mit $\chi(-1) = -1$, (3) mit $\chi(-1) = 1$ und (4) gilt somit

$$L_\psi(s) = L_{D_1'}(s) L_{D_2'}(s) = L_{\psi_{D_1}}(s) L_{\psi_{D_2}}(s) = L_{\tilde{\psi}}(s).$$

Wegen $L_D(s+\frac{\pi i}{\log p}) = L_{gD}(s)$ (vgl. Satz 9.2.3) ist in allen anderen Fällen

$$\begin{aligned} L_{\tilde{\psi}}(s+\frac{\pi i}{\log p}) &= L_{\psi_{D_1}}(s+\frac{\pi i}{\log p})L_{\psi_{D_2}}(s+\frac{\pi i}{\log p}) = L_{g(-1)^{\operatorname{grad} D_1}D_1}(s)L_{g(-1)^{\operatorname{grad} D_2}D_2}(s) \\ &= \begin{cases} L_{gD_1}(s)L_{gD_2}(s) & \text{in (1)}, \\ L_{gD_1}(s)L_{gD_2}(s) & \text{in (2) mit } \chi(-1)=1 \text{ und} \\ L_{D_1}(s)L_{D_2}(s) & \text{in (3) mit } \chi(-1)=-1, \end{cases} \end{aligned}$$

denn im letzten Fall ist $\chi(-g)=1$.

□

12.3.3 Satz

Es liege die zu Anfang des Kapitels 12.1 beschriebene Situation vor. Dann erhält man für die Fälle 12.1 (1)-(4) die folgenden Formeln für das Produkt der Klassenzahlen $h(D_1')h(D_2')$:

(1) Ist $\tilde{\psi}$ der zur Zerlegung $D=D_1D_2$ gehörige Geschlechtscharakter, und ist $D_1 \neq 1 \neq D_2$, so gilt

$$h(gD_1)h(gD_2) = L_{\tilde{\psi}}\left(\frac{\pi i}{\log p}\right).$$

Ist $\tilde{\psi}$ der zur Zerlegung $D = 1 \cdot D$ gehörige Geschlechtscharakter, also der triviale Charakter, so ist $L_{\tilde{\psi}}(s) = Z_K(s)$, und es gilt

$$h(gD) = (p+1)L_{\tilde{\psi}}(\frac{\pi i}{\log p}).$$

(2) Ist $\tilde{\psi}$ der zur Zerlegung $D=D_1D_2$ gehörige Geschlechtscharakter, und sind D_1, D_2 normiert und von ungeradem Grad, so ist

$$h(gD_1)h(gD_2) = L_{\tilde{\psi}}\left(\frac{(1+\chi(-1))\pi i}{2\log p}\right).$$

(3) Auch hier gilt mit dem Geschlechtscharakter $\tilde{\psi}$ zur Zerlegung $D=D_1D_2$

$$h(D_1)h(D_2) = L_{\tilde{\psi}}\left(\frac{(1-\chi(-1))\pi i}{2\log p}\right).$$

(4) Ist $\tilde{\psi}$ wie in (1) der zur Zerlegung $D=D_1D_2$ mit $D_1 \neq 1 \neq D_2$ gehörige Geschlechtscharakter, so gilt

$$h(D_1)h(D_2) = \frac{|\sqrt{D}|}{(p-1)^2}\frac{1}{R_1R_2}L_{\tilde{\psi}}(1)$$

mit den Regulatoren R_1, R_2 der reell-quadratischen Körper $k(\sqrt{D_1})$ und $k(\sqrt{D_2})$.

BEWEIS:

Es sei $\tilde{\psi}$ der zur Zerlegung $D = D_1 D_2$ gehörige Geschlechtscharakter von $C^+(k(\sqrt{D}))$.

(1) Ist $\tilde{\psi}$ nicht der triviale Charakter, so ist nach Satz 12.3.2

$$L_{\tilde{\psi}}(s + \frac{\pi i}{\log p}) = L_{gD_1}(s) L_{gD_2}(s).$$

Mit Satz 9.3.1 (ii) gilt dann für $s = 0$

$$L_{\tilde{\psi}}(\frac{\pi i}{\log p}) = L_{gD_1}(0) L_{gD_2}(0) = h(gD_1) h(gD_2),$$

was die Behauptung war.

Ist $\tilde{\psi}$ speziell der zur Zerlegung $D = 1 \cdot D$ gehörige Geschlechtscharakter, so gilt

$$L_{\tilde{\psi}}(s + \frac{\pi i}{\log p}) = Z_K(s + \frac{\pi i}{\log p}) \overset{\text{Satz 9.2.4}}{=} \frac{1 - p^{-(s-1)}}{1 + p^{-(s-1)}} Z_{k(\sqrt{gD})}(s)$$

und wegen

$$Z_{k(\sqrt{gD})}(0) = -\frac{1}{p-1} L_{gD}(0) \overset{9.3.1\ \text{(ii)}}{=} -\frac{1}{p-1} h(gD)$$

erhält man die Behauptung.

(2) Nach Satz 12.3.2 ist

$$L_{gD_1}(0) L_{gD_2}(0) = \begin{cases} L_{\tilde{\psi}}(\frac{\pi i}{\log p}), & \text{falls } \chi(-1) = 1, \\ L_{\tilde{\psi}}(0), & \text{falls } \chi(-1) = -1, \end{cases}$$

und mit der Formel für die Werte von $L_{gD_i}(s)$ an der Stelle $s = 0$ aus Satz 9.3.1 folgt die Behauptung wie in (1).

(3) Man argumentiert wie in (2), indem man

$$L_{D_1}(0) L_{D_2}(0) = \begin{cases} L_{\tilde{\psi}}(\frac{\pi i}{\log p}), & \text{falls } \chi(-1) = -1, \\ L_{\tilde{\psi}}(0), & \text{falls } \chi(-1) = 1 \end{cases}$$

ausnutzt.

(4) Nach Satz 9.3.2 gilt

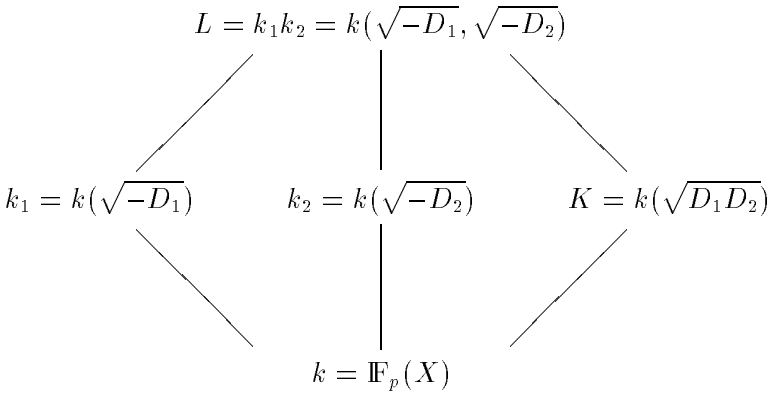
$$L_{\tilde{\psi}}(1) = L_{D_1}(1) L_{D_2}(1) = \frac{h(D_1) h(D_2) (p-1)^2 R_1 R_2}{\sqrt{|D_1|}\sqrt{|D_2|}},$$

wobei R_i für $i = 1, 2$ die Regulatoren der reell-quadratischen Körper $k(\sqrt{D_i})$ sind. Daraus folgt die genannte Formel für $h(D_1) h(D_2)$.

□

12.3.4 Bemerkung

Die beiden Fälle, in denen es sich bei ψ schon um einen Geschlechtscharakter der engen Idealklassen handelt, lassen sich für $\chi(-1) = \pm 1$ in folgendem Körperturm zusammenfassen:



Hier sieht man wegen $\operatorname{grad} D_1 \equiv \operatorname{grad} D_2 \equiv 1\ (2)$ sofort, daß dies genau die Fälle sind, bei denen in den imaginär-quadratischen Erweiterungen k_1 und k_2 kein Element $u \in \mathcal{O}_{k_i}$ existiert mit $\chi(N(u)) = -1$, wie wir schon in 4.1.6 bemerkten.

Die Herleitung von expliziten Formeln für das Produkt obiger Klassenzahlen läuft also nach 11.2.1 und 12.2.2 auf die Berechnung der Werte der Zeta-Funktionen $Z(s, A)$ bzw. der L-Funktionen $L(s, A)$ zu einer engen Idealklasse A an den Stellen $s = 0$, $s = 1$ und $s = \frac{\pi i}{\log p}$ hinaus.

13 Gitter in $k_\infty \times k_\infty$

Die Berechnung der Werte der Funktionen $Z(s, A)$ und $L(s, A)$ an den Stellen $s = 0$ und $s = \frac{\pi i}{\log p}$ führen wir unter Zuhilfenahme der Darstellungen in 12.2.2 auf die Einbettung e aus 4.1.5 von K^* in $P = k_\infty^* \times k_\infty$ zurück und betrachten zu diesem Zweck zunächst einmal Gitter in $k_\infty \times k_\infty$.
Wir folgen hier der Vorgehensweise von HAYES in [H1], passen aber an einigen Stellen die Definitionen an unsere Definition der Reduziertheit von Elementen bzw. an die enge KBE-Art an, so daß sich Abweichungen bei den Berechnungen ergeben.

13.1 Definition und Eigenschaften

13.1.1 Definition

Ein *Gitter* Λ in $k_\infty \times k_\infty$ ist ein $\mathbb{F}_p[X]$-Untermodul von $k_\infty \times k_\infty$ vom Rang 2.
Ein Gitter wird demnach erzeugt über $\mathbb{F}_p[X]$ von zwei k_∞-linear unabhängigen Vektoren $\rho = \binom{\rho_1}{\rho_2}, \tau = \binom{\tau_1}{\tau_2} \in k_\infty^2$.

Wir schreiben dann

$$\Lambda = [\rho, \tau] = \mathbb{F}_p[X]\rho + \mathbb{F}_p[X]\tau$$

und nennen das Gitter *zerstreut*, wenn für jedes $0 \neq \lambda = \binom{\lambda_1}{\lambda_2} \in \Lambda$ gilt: $\lambda_1 \neq 0 \neq \lambda_2$.

Weiterhin definieren wir das *Volumen von* Λ durch $\mathrm{Vol}(\Lambda) := |V(\Lambda)|$ durch

$$V(\Lambda) := \det \begin{pmatrix} \rho_1 & \rho_2 \\ \tau_1 & \tau_2 \end{pmatrix}.$$

Ein Paar von Basisvektoren (ρ, τ) von Λ heißt *orientiert*, falls $\chi(V([\rho, \tau])) = 1$ gilt.
In diesem Abschnitt wollen wir uns ausschließlich mit zerstreuten Gittern befassen, auch wenn diese Eigenschaft nicht immer explizit hervorgehoben wird.

13.1.2 Lemma

(i) Ist Λ' ein Untergitter eines Gitters Λ, so ist $\#(\Lambda/\Lambda') = \frac{\mathrm{Vol}(\Lambda')}{\mathrm{Vol}(\Lambda)}$.

(ii) Sind $\rho, \tau \in k_\infty \times k_\infty$ zwei Vektoren mit $|S(\rho)| < |S(\tau)|$, so ist $\Lambda = [\rho, \tau]$ ein Gitter mit dem Volumen $\mathrm{Vol}(\Lambda) = |\rho_1 \tau_2|$.

(iii) Sind (ρ, τ) und (ρ', τ') Basen eines Gitters Λ, von denen (ρ, τ) orientiert ist, und ist $T \in \mathrm{GL}(2; \mathbb{F}_p[X])$ die Übergangsmatrix mit $\binom{\rho'}{\tau'} = T \binom{\rho}{\tau}$. Dann gilt

$$(\rho', \tau') \text{ ist orientiert} \quad \Leftrightarrow \quad T \in \mathrm{SL}(2; \mathbb{F}_p[X]).$$

BEWEIS:
Zu (i) und (ii) s. [H1], (2.5) und Lemma 2.6.
Die Aussage (iii) zeigt man wie in Lemma 8.4.3. □

13.1.3 Proposition

Ist $K = k(\sqrt{D}) \subset k_\infty$ ein reell-quadratischer Funktionenkörper, $\mathfrak{a} =< \omega_1, \omega_2 >$ ein ganzes Ideal von K und

$$\Lambda_\mathfrak{a} = e(\mathfrak{a}) := [\begin{pmatrix} \omega_2 \\ \overline{\omega_2} \end{pmatrix}, \begin{pmatrix} \omega_1 \\ \overline{\omega_1} \end{pmatrix}],$$

so ist $\Lambda_\mathfrak{a}$ ein (zerstreutes) Gitter in k_∞^2 mit

$$\mathrm{Vol}(\Lambda_\mathfrak{a}) = |N(\mathfrak{a})||\sqrt{D}|.$$

Das angegebene Basispaar von $\Lambda_\mathfrak{a}$ ist genau dann orientiert, wenn die Basis (ω_1, ω_2) von $\mathfrak{a}$ orientiert ist.

BEWEIS:
Wir wissen aus Lemma 4.1.5, daß jedes gebrochene Ideal $\mathfrak{a}$ ein freier $\mathbb{F}_p[X]$-Untermodul von K vom Rang 2 ist.
Besitzt $\mathfrak{a}$ die Basis (ω_1, ω_2), so ist $\Lambda_\mathfrak{a} := e(\mathfrak{a})$ ein (aufgrund der Eigenschaft der Abbildung e zerstreutes) Gitter in k_∞^2 mit

$$\mathrm{Vol}(\Lambda_\mathfrak{a}) = |N(\mathfrak{a})||\sqrt{D}|$$

nach Definition der Norm des ganzen Ideals $\mathfrak{a}$.
Die Aussage über die Orientiertheit folgt sofort mit

$$V(\Lambda_\mathfrak{a}) = \overline{\omega_1}\omega_2 - \omega_1\overline{\omega_2}$$

aus der Definition 8.4.1 der Orientiertheit der Basis (ω_1, ω_2) von $\mathfrak{a}$. □

13.2 Eckenpaare

13.2.1 Definition

Ein geordnetes Paar von Basis-Vektoren $(\rho,\tau) \in k_\infty^2 \times k_\infty^2$ eines Gitters Λ heißt ein *Eckenpaar von* Λ, falls folgende Bedingungen erfüllt sind:

(i) $\operatorname{sgn} \frac{\rho_1}{\tau_1} \in \{1, g\}$.

(ii) $\left|\frac{\rho_1}{\tau_1}\right| > 1 > \left|\frac{\rho_2}{\tau_2}\right|$.

(iii) (ρ,τ) ist orientiert.

Jede Komponente eines Eckenpaares von Λ nennt man *Ecke von* Λ.

13.2.2 Bemerkung

(i) Die Definition der Eckenpaare entspricht nicht ganz der Definition 6.1 aus [H1], S.214. Sie wurde angepaßt an die Reduziertheit von Elementen, die später für die Anwendung der engen KBE gebraucht wird.

Dies hat, wie man sehen wird, Konsequenzen für die Vorzeichen der Elemente in den folgenden Berechnungen.

(ii) Es sei $\mathfrak{a} =< \omega_1, \omega_2 >$ ein ganzes Ideal aus $I(K)$. Die Basis (ω_1, ω_2) sei orientiert und der Basisquotient $\frac{\omega_2}{\omega_1} \in F(D)$ sei reduziert.

Ist dann $\Lambda_\mathfrak{a} = e(\mathfrak{a}) = [\rho,\tau]$ wie in Proposition 13.1.3, so ist (ρ,τ) ein Eckenpaar des Gitters $\Lambda_\mathfrak{a}$.

Weitere Eigenschaften von Eckenpaaren erhalten wir aus dem folgenden Satz.

13.2.3 Satz

Ist $(\rho,\tau) \in k_\infty^2 \times k_\infty^2$ ein Eckenpaar von Λ, so gilt:

(i) $|S(\tau)| > |S(\rho)|$.

(ii) Das Paar (ρ,τ) ist schon durch einen seiner Vektoren eindeutig bestimmt.

(iii) Es existiert ein Vektor $\kappa \in k_\infty^2$, so daß (τ,κ) wieder ein Eckenpaar von Λ ist.

(iv) Ist (ρ^*,τ^*) ein Eckenpaar von Λ mit

$$|S(\rho)| \leq |S(\rho^*)| < |S(\tau)|,$$

so existieren $c, d \in \mathbb{F}_p^*$ mit $(c\rho^*, d\tau^*) = (\rho,\tau)$.

BEWEIS:

(i) Diese Ungleichung folgt sofort aus der Definition des Eckenpaares.

(ii) Seien (ρ,τ) und (ρ,τ^*) zwei Eckenpaare von Λ. Dann ist die Übergangsmatrix S von einem zum anderen Eckenpaar aufgrund der Orientiertheit ein Element von $\mathrm{SL}(2;\mathbb{F}_p[X])$ der Form $S=\left(\begin{smallmatrix}1 & 0\\ A & \zeta\end{smallmatrix}\right)$ mit $A\in\mathbb{F}_p[X]$ und $\zeta\in\mathbb{F}_p^{*^2}$.
Es ist also

$$\tau^* = A\rho+\zeta\tau.$$

Wegen $|\rho_1|>|\tau_1^*|$ und $|\rho_1|>|\tau_1|$ muß demnach $A=0$ sein, also $\tau^*=\zeta\tau$.
Weiterhin gilt $\operatorname{sgn}\frac{\rho_1}{\tau_1},\operatorname{sgn}\frac{\rho_1}{\tau_1^*}=\operatorname{sgn}\left(\zeta^{-1}\frac{\rho_1}{\tau_1}\right)\in\{1,g\}$. Wegen $\zeta\in\{1,g^{-1},g\}$ muß $\zeta=1$ gelten, denn die beiden Vorzeichen unterscheiden sich wenn, dann höchstens durch einen quadratischen Nichtrest. Das kann aber wegen $S\in\mathrm{SL}(2;\mathbb{F}_p[X])$ nicht sein, woraus die Behauptung folgt.
Ein ähnliches Argument – man nutzt $|\rho_2|<|\tau_2|$ aus – zeigt, daß auch ρ durch τ eindeutig bestimmt ist.

(iii) Es sei $\kappa\in k_\infty^2$ definiert durch

$$\eta\kappa = \rho-\left[\frac{\rho_1}{\tau_1}\right]\tau,$$

wobei $\eta\in\mathbb{F}_p^*$ gewählt werde wie in Definition 5.3.3, nämlich $\eta=-a$ bzw. $\eta=-ag$ mit $a=\operatorname{sgn}\left(\left[\frac{\rho_1}{\tau_1}\right]-\frac{\rho_1}{\tau_1}\right)$, je nachdem, ob a ein quadratischer Rest oder ein quadratischer Nichtrest mod p ist.
Dies entspricht dem ersten Schritt der engen KBE von $\frac{\rho_1}{\tau_1}$, und es gilt

$$\frac{\tau_1}{\kappa_1}=\frac{\eta}{\frac{\rho_1}{\tau_1}-\left[\frac{\rho_1}{\tau_1}\right]},$$

also

1) $\operatorname{sgn}\left(\frac{\tau_1}{\kappa_1}\right)\in\{1,g\}$ und
2) $\left|\frac{\tau_1}{\kappa_1}\right|>1>\left|\frac{\tau_2}{\kappa_2}\right|$,

da (ρ,τ) ein Eckenpaar war.
Weiterhin ist

$$\begin{pmatrix}\tau\\ \kappa\end{pmatrix}=\begin{pmatrix}0 & 1\\ \frac{1}{\eta} & -\frac{1}{\eta}\left[\frac{\rho_1}{\tau_2}\right]\end{pmatrix}\begin{pmatrix}\rho\\ \tau\end{pmatrix}=:S\begin{pmatrix}\rho\\ \tau\end{pmatrix}$$

mit der Übergangsmatrix $S\in\mathrm{GL}(2;\mathbb{F}_p[X])$. Diese ist schon ein Element von $\mathrm{SL}(2;\mathbb{F}_p[X])$, da $-\frac{1}{\eta}$ nach Wahl von $\eta\in\mathbb{F}_p^*$ ein quadratischer Rest mod p ist. Dies beweist die Orientiertheit von (τ,κ), woraus man zusammen mit 1) und 2) schließt, daß es sich bei (τ,κ) um ein Eckenpaar von Λ handelt.

(iv) Man wähle $c\in\mathbb{F}_p^*$ so, daß $\operatorname{sgn}\frac{c\rho_1^*}{\tau_1}\in\{1,g\}$ gilt und das Untergitter $[c\rho^*,\tau]$ von Λ orientiert ist. $(\tilde\rho,\tilde\tau):=(c\rho^*,c\tau^*)$ ist wieder ein Eckenpaar von Λ, und $\Lambda_1:=[\rho,\tilde\tau]$, $\Lambda_2:=[\tilde\rho,\tau]$ sind Untergitter von Λ mit $|S(\rho)|=|S(\tilde\rho)|<|S(\tilde\tau)|$ und $|S(\tilde\rho)|=|S(\rho)|<|S(\tau)|$. Es gilt also $\mathrm{Vol}(\Lambda_1)=|\rho_1\tilde\tau_2|$ und $\mathrm{Vol}(\Lambda_2)=|\tilde\rho_1\tau_2|$ nach Lemma 13.1.2.
Aus ebendiesem Lemma folgt auch

$$\mathrm{Vol}(\Lambda)=|\rho_1\tau_2|=|\tilde\rho_1\tilde\tau_2|,$$

sowie

$$l_1 := \#\,(\Lambda/\Lambda_1) = \frac{\mathrm{Vol}(\Lambda_1)}{\mathrm{Vol}(\Lambda)} = \left|\frac{\tilde{\tau}_2}{\tau_2}\right| \quad \text{und}$$

$$l_2 := \#\,(\Lambda/\Lambda_2) = \frac{\mathrm{Vol}(\Lambda_2)}{\mathrm{Vol}(\Lambda)} = \left|\frac{\tau_2}{\tilde{\tau}_2}\right|.$$

Dies sind zwei ganze Zahlen ≥ 1 mit $l_1 l_2 = 1$, also $l_1 = l_2 = 1$.
Man erhält $\Lambda = \Lambda_1 = \Lambda_2$ und damit die Ungleichungen $|\tau_2| = |\tilde{\tau}_2| > |\tilde{\rho}_2|$ sowie $|\tilde{\rho}_1| = |\rho_1| > |\tau_1|$. Es ist also $(\tilde{\rho}, \tau)$ ein Eckenpaar von $\Lambda = \Lambda_2$, somit gilt $\tilde{\rho} = \rho$, d.h. es existiert ein $c \in \mathbb{F}_p^*$ mit $\rho = c\rho^*$.
Nach (iii) existieren zu τ und τ^* zwei Elemente $\kappa, \kappa^* \in k_\infty^2$, so daß (τ, κ) und (τ^*, κ^*) wieder Eckenpaare von Λ sind.
Kann man nun $|S(\tau)| \leq |S(\tau^*)| < |S(\kappa)|$ zeigen, so kann man die vorangegangenen Berechnungen für ρ^* ebenso auf τ^* anwenden und erhält ein $d \in \mathbb{F}_p^*$ mit $d\tau^* = \tau$.
Wäre also $|S(\tau^*)| < |S(\tau)|$, so könnte man wegen

$$|S(\rho)| \leq |S(\rho^*)| < |S(\tau^*)| < |S(\tau)|$$

wie oben zeigen, daß ein $e \in \mathbb{F}_p^*$ existiert mit $e\tau^* = \rho = c\rho^*$, was aufgrund der linearen Unabhängigkeit von τ^* und ρ^* aber nicht sein kann.
Wäre $|S(\kappa)| \leq |S(\tau^*)|$ richtig, so wären wegen

$$|S(\rho)| \leq |S(\rho^*)| < |S(\tau)| < |S(\kappa)| \leq |S(\tau^*)|$$

auch τ und ρ linear abhängig. Denn mit obigen Schlußweisen für ρ^* nun angewandt auf τ erhält man in diesem Fall ein $e \in \mathbb{F}_p^*$ mit $e\tau = \rho^* = c^{-1}\rho$.
Es muß also

$$|S(\tau)| \leq |S(\tau^*)| < |S(\kappa)|$$

gelten, und diese Ungleichung liefert uns ein $d \in \mathbb{F}_p^*$ mit $d\tau^* = \tau$.

□

13.2.4 Proposition

Ist $K \subset k_\infty$ ein reell-quadratischer Funktionenkörper und $\epsilon_1 \in \mathcal{O}_K^*$ die positive Grundeinheit von K, so operiert $\epsilon_1^{\mathbb{Z}}$ mittels der Multiplikation

$$\alpha * x := \begin{pmatrix} \alpha x_1 \\ \overline{\alpha} x_2 \end{pmatrix}$$

für $x \in k_\infty^2$ und $\alpha \in K$ auf den Ecken eines Gitters Λ, d.h. ist $\Lambda = [\rho, \tau]$, so ist mit (ρ, τ) auch $(\rho^*, \tau^*) := (\epsilon_1 * \rho, \epsilon_1 * \tau)$ wieder ein Eckenpaar von Λ, und zwar mit der Eigenschaft $|S(\rho)| < |S(\epsilon_1 * \rho)|$.

BEWEIS:

Ist $(\rho, \tau) \in k_\infty^2 \times k_\infty^2$ eine Ecke und $(\rho^*, \tau^*) := (\epsilon_1 * \rho, \epsilon_1 * \tau)$, so gilt

(i) $\mathrm{sgn}\left(\frac{\epsilon_1\rho_1}{\epsilon_1\tau_1}\right) = \mathrm{sgn}\left(\frac{\rho_1}{\tau_1}\right) \in \{1, g\}$.

(ii) $\left|\frac{\epsilon_1\rho_1}{\epsilon_1\tau_1}\right| = \left|\frac{\rho_1}{\tau_1}\right| > 1 > \left|\frac{\rho_2}{\tau_2}\right| = \left|\frac{\overline{\epsilon_1}\rho_2}{\overline{\epsilon_1}\tau_2}\right|$ und

(iii) $\chi(\epsilon_1\rho_1\overline{\epsilon_1}\tau_2 - \overline{\epsilon_1}\rho_2\epsilon_1\tau_1) = \chi(N(\epsilon_1))\chi(V([\rho, \tau])) = 1$.

(ρ^*, τ^*) ist also wieder ein Eckenpaar. Ferner ist $|S(\rho^*)| = |S(\epsilon_1)S(\rho)| > |S(\rho)|$, da $|S(\epsilon_1)| > 1$ wegen $|N(\epsilon_1)| < 1$ ist. □

13.2.5 Proposition

Ist $\mathfrak{a} = < \omega_1, \omega_2 >$ ein ganzes Ideal von K mit einer orientierten Basis $(\omega_1, \omega_2) \in K^{*2}$, dessen Basisquotient $\frac{\omega_2}{\omega_1} \in F(D)$ reduziert ist, und ist $\Lambda_\mathfrak{a} = [\gamma^{(0)}, \gamma^{(1)}]$, so ist nach Bemerkung 13.2.2 (ii) das Tupel $(\gamma^{(0)}, \gamma^{(1)}) \in k_\infty^2 \times k_\infty^2$ ein Eckenpaar.
Durch sukzessive Anwendung von Satz 13.2.3 (iii) erhält man somit eine Menge von Ecken $\{\gamma^{(i)} \mid i \in \mathbb{N}_0\}$ mit $|S(\gamma^{(i)})| > |S(\gamma^{(j)})|$ für $i > j$.
Es gibt dann ein $\delta = \delta(\mathfrak{a})$ und zu jedem $r \in \mathbb{N}_0$ ein $c_r \in \mathbb{F}_p^*$ mit

$$\epsilon_1 * \gamma^{(r)} = c_r \cdot \gamma^{(r+\delta)}.$$

BEWEIS:

Zusammen mit Proposition 13.2.4 folgt dies aus Satz 13.2.3 (i) und (iv). □

13.2.6 Lemma

Entsteht aus einem Eckenpaar $(\gamma^{(0)}, \gamma^{(1)}) \in k_\infty^2 \times k_\infty^2$ eine Menge von Ecken wie in Proposition 13.2.5, und ist $\epsilon_1 * \gamma^{(0)} = c_0 \cdot \gamma^{(\delta)}$, so ist δ die minimale Periode der engen Kettenbruchentwicklung von $\frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$.

BEWEIS:

Nach Bemerkung 6.2.1 ist die Periode der engen KBE von $\frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$ endlich. Es sei daher $n > 0$ so gewählt, daß

$$\frac{\gamma_1^{(n)}}{\gamma_1^{(n+1)}} = \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$$

gilt.
Man hat dann also mit $Z_0^* := \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$ die Identität

$$Z_0^* = \tilde{S}_n^* \circ Z_0^*.$$

Hierbei ist die Matrix $\tilde{S}_n^*$ das Inverse der Matrix $S_n^* \in \mathrm{SL}(2; \mathbb{F}_p[X])$ aus Folgerung 6.2.4 (ii), die aus der engen KBE von Z_0^* hervorgeht.
Sei also $\eta \in \mathbb{K}$ die enge KBE-Art. Dann besitzt die Matrix $\tilde{S}_n^*$ die Darstellung

$$\tilde{S}_n^* = (\eta_0 \cdot \ldots \cdot \eta_{n-1})^{-1} T_{n-1}^* \cdot \ldots \cdot T_0^*$$

mit

$$T_i^* := \begin{pmatrix} 0 & \eta_i \\ 1 & -\left[\frac{\gamma_1^{(i)}}{\gamma_1^{(i+1)}}\right] \end{pmatrix}.$$

Schreibt man $Z_i^* := \frac{\gamma_1^{(i)}}{\gamma_1^{(i+1)}}$, so erhält man

$$\begin{aligned} T_i^* \begin{pmatrix} Z_i^* \\ 1 \end{pmatrix} &= \begin{pmatrix} \eta_i \\ Z_i^* - [Z_i^*] \end{pmatrix} \\ &= (Z_i^* - [Z_i^*]) \begin{pmatrix} Z_{i+1}^* \\ 1 \end{pmatrix} \\ &= \eta_i \frac{\gamma_1^{(i+2)}}{\gamma_1^{(i+1)}} \begin{pmatrix} Z_{i+1}^* \\ 1 \end{pmatrix} \end{aligned}$$

für alle $0 \leq i \leq n-1$.
Insgesamt folgt wegen $Z_0^* = Z_n^*$ die Identität

$$\tilde{S}_n^* \begin{pmatrix} Z_0^* \\ 1 \end{pmatrix} = (\eta_0 \cdot \ldots \cdot \eta_{n-1})^{-1} \prod_{i=0}^{n-1} (\eta_i \frac{\gamma_1^{(i+2)}}{\gamma_1^{(i+1)}}) = \frac{\gamma_1^{(n+1)}}{\gamma_1^{(1)}} \begin{pmatrix} Z_0^* \\ 1 \end{pmatrix}.$$

Man hat also mit $\epsilon := \frac{\gamma_1^{(n+1)}}{\gamma_1^{(1)}} = \frac{\gamma_1^{(n)}}{\gamma_1^{(0)}}$ einen Eigenwert von $\tilde{S}_n^* \in \mathrm{SL}(2; \mathbb{F}_p[X])$ gefunden. Dieses ϵ ist daher eine Einheit aus $\mathcal{O}_K$ mit $\chi(N(\epsilon)) = 1$. Ferner ist $\epsilon * \gamma^{(0)} = \gamma^{(n)}$ und

$$|S(\epsilon)| = \left|\frac{\overline{\epsilon}}{\epsilon}\right| = \left|\frac{S(\gamma^{(n+1)})}{S(\gamma^{(1)})}\right| > 1,$$

also existiert nach 4.2.3 eine ganze Zahl $k \geq 1$ und ein $c \in \mathbb{F}_p^*$ mit $\epsilon = c \cdot \epsilon_1^k$ und $n = k\delta$, δ ist somit die minimale Periode der engen KBE-Art von Z_0^*. □

13.2.7 Korollar

Ist δ die minimale Periode der engen KBE des reduzierten Elements $\frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$, so ist

$$\epsilon = \frac{\gamma_1^{(\delta)}}{\gamma_1^{(0)}}$$

bis auf einen Faktor aus $\mathbb{F}_p^*$ die positive Grundeinheit von K.

BEWEIS:
Nach Lemma 13.2.6 besitzt die Matrix $(S_\delta^*)^{-1}$ aus Folgerung 6.2.4 (ii) den Eigenwert $\frac{\gamma_1^{(\delta)}}{\gamma_1^{(0)}}$. Dieser ist nach Satz 7.2.2 bis auf einen Faktor aus $\mathbb{F}_p^*$ identisch mit $(P_\delta^* - Q_\delta^* \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}})$.
Somit handelt es sich bei $\frac{\gamma_1^{(\delta)}}{\gamma_1^{(0)}}$ bis auf einen Faktor aus $\mathbb{F}_p^*$ um die Grundeinheit des Körpers K. □

13.2.8 Beispiel

Wir verifizieren die Ergebnisse von Beispiel 7.2.3 anhand des Korollars 13.2.7.
Zu diesem Zweck wählen wir

$$\mathfrak{a} := < 2, \sqrt{D} + [\sqrt{D}] >, \quad \text{also} \quad \Lambda_\mathfrak{a} = \left[\begin{pmatrix} [\sqrt{D}] + \sqrt{D} \\ [\sqrt{D}] - \sqrt{D} \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right].$$

Bei der Basis von $\Lambda_\mathfrak{a}$ handelt es sich nach den Ausführungen in Beispiel 7.2.3 um ein Eckenpaar.
Nach einer kurzen Rechnung erhält man:

(i) $\frac{1}{4}a^2 - b \in \mathbb{F}_p^{*2}$: Hier ist $\rho_* = 1$, also

$$\epsilon = \frac{\gamma_1^{(1)}}{\gamma_1^{(0)}} = \frac{2}{\sqrt{D} + [\sqrt{D}]} = 2(\frac{1}{4}a^2 - b)^{-1}(\sqrt{D} - [\sqrt{D}]) \quad \text{mit } N(\epsilon) = 4,$$

denn $\gamma_1^{(1)} = 2$. Dies ist in der Tat bis auf einen Faktor die positive Grundeinheit von K, wie wir schon in Beispiel 7.2.3 bemerkten.

(ii) $\frac{1}{4}a^2 - b \notin \mathbb{F}_p^{*2}$: Hier ist, wie schon gesehen, $\eta_0 = g\frac{1}{4}(b - \frac{1}{4}a^2)$ und $\rho_* = 2$.
Aus $Z_1^* = gZ_0^* = \frac{g}{2}(\sqrt{D} + [\sqrt{D}])$ errechnet man $\gamma_1^{(2)} = \frac{2}{gZ_0^*}$, $\eta_1 = \eta_0$ und somit

$$\epsilon = \frac{\gamma_1^{(2)}}{\gamma_1^{(0)}} = \frac{2}{g(Z_0^*)^2} = (g(\frac{1}{4}(b - \frac{1}{4}a^2))^2)^{-1}\overline{Z_0^*}^2 = g^{-1}((\frac{1}{4}(b - \frac{1}{4}a^2))^{-1}([\sqrt{D}] - \sqrt{D}))^2.$$

Ein Vergleich mit den Ergebnissen aus Beispiel 7.2.3 bestätigt die Berechnungen.

14 Sektor-L-Funktionen

14.1 Definition und Eigenschaften

Ausgehend von der Einbettung P von K^* in k_∞^2 (s. 4.1.5) definieren wir nun die *Sektor-L-Funktionen*, über die wir die Berechnung der L-Funktionen $L_0(s, A)$ und $L(s, A)$ vollziehen werden.

14.1.1 Definition

Sind $\rho, \tau \in P$ mit $|S(\rho)| < |S(\tau)|$ gegeben, so heißt

$$X(\rho, \tau) := \{\alpha \in P \mid |S(\rho)| \leq |S(\alpha)| < |S(\tau)|\}$$

der *Sektor zu ρ und τ* in P und

$$L(s; \rho, \tau) := \frac{\mathrm{Vol}([\rho, \tau])^s}{p-1} \sum_{\lambda \in X(\rho,\tau) \cap [\rho,\tau]} \frac{\chi(N(\lambda))}{|N(\lambda)|^s}$$

die *Sektor-L-Funktion zum Gitter* $[\rho, \tau]$.
Weiterhin definieren wir

$$L_0(s; \rho, \tau) := \frac{\mathrm{Vol}([\rho, \tau])^s}{p-1} \sum_{\lambda \in X(\rho,\tau) \cap [\rho,\tau]} \frac{1}{|N(\lambda)|^s}.$$

14.1.2 Bemerkung

Ist X_P^+ ein Fundamentalbereich für die Operation von $\epsilon_1^{\mathbb{Z}}$ auf P und $[\rho, \tau] = \Lambda_\mathfrak{a}$ für ein $\mathfrak{a} \in A \in C^+(K)$, so lassen sich $L(s, A)$ und $L_0(s, A)$ nach Proposition 13.1.3 schreiben als

$$L(s, A) = |\sqrt{D}|^{-s} \frac{\mathrm{Vol}(\Lambda_\mathfrak{a})}{p-1} \sum_{\lambda \in X_P^+ \cap \Lambda_\mathfrak{a}} \frac{\chi(N(\lambda))}{|N(\lambda)|^s}$$

und

$$L_0(s, A) = |\sqrt{D}|^{-s} \frac{\mathrm{Vol}(\Lambda_\mathfrak{a})}{p-1} \sum_{\lambda \in X_P^+ \cap \Lambda_\mathfrak{a}} \frac{1}{|N(\lambda)|^s}.$$

Ließen sich nun Vektoren $\rho, \tau \in P$ mit $\Lambda_\mathfrak{a} = [\rho, \tau]$ finden, für welche zudem $X(\rho, \tau) = X_P^+$ ein Fundamentalbereich der gewünschten Form wäre (etwa $\rho \in P$ beliebig und $\tau = \epsilon_1 * \rho$), so hätte man

$$L(s, A) = |\sqrt{D}|^{-s} L(s; \rho, \tau)$$

bzw.

$$Z(s,A) = \frac{1}{2}|\sqrt{D}|^{-s}(L_0(s;\rho,\tau) + L(s;\rho,\tau)).$$

Diese Wahl für ρ und τ ist aber i.a. nicht möglich.
Wie wir später zeigen werden, ist es jedoch immer möglich, $L(s,A)$ und $L_0(s,A)$ und somit auch $Z(s,A)$ als Summe gewisser Sektor-L-Funktionen ausdrücken.
Somit wäre dann die Berechnung der Werte von $Z(s,A)$ auf die Berechnung der Werte der Sektor-L-Funktionen $L(s;\rho,\tau)$ und $L_0(s;\rho,\tau)$ zurückgeführt.
Grundlegend hierfür ist offensichtlich die Beschreibung der Menge $X(\rho,\tau) \cap [\rho,\tau]$ für ein Gitter $[\rho,\tau]$, welche Inhalt des nun folgenden Lemmas ist.

14.1.3 Lemma

Es seien $\rho = \binom{\rho_1}{\rho_2}, \tau = \binom{\tau_1}{\tau_2} \in P$, $\Lambda := [\rho,\tau]$ ein Gitter in $k_\infty \times k_\infty$ und (ρ,τ) ein Eckenpaar von Λ. Es sei $X(\rho,\tau)$ der zugehörige Sektor zu ρ und τ in P und

$$l_1 := \operatorname{grad}\frac{\rho_1}{\tau_1}, \quad l_2 := -\operatorname{grad}\frac{\rho_2}{\tau_2}.$$

Dann sind l_1 und l_2 zwei positive ganze Zahlen. Ist $\lambda := A\rho + B\tau$ mit $A, B \in \mathbb{F}_p[X]$, so gilt

$$\lambda = \begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix} \in \Lambda \cap X(\rho,\tau)$$

genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

(1) $-l_2 < \operatorname{grad} B - \operatorname{grad} A < l_1$.

(2) $\operatorname{grad} A = \operatorname{grad} B + l_2$ und $\operatorname{sgn} A\rho_2 \neq -\operatorname{sgn} B\tau_2$.

(3) $B \neq 0$ und $\operatorname{grad} A > \operatorname{grad} B + l_2$.

(4) $B = 0$.

In allen vier Fällen gilt $\operatorname{sgn}\lambda_1 = \operatorname{sgn} A\rho_1$, und für $\operatorname{sgn}\lambda_2$ erhält man:

(1) $\operatorname{sgn}\lambda_2 = \operatorname{sgn} B\tau_2$

(2) $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2 + \operatorname{sgn} B\tau_2$ und

(3)&(4) $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2$.

BEWEIS:

Daß es sich bei l_1 und l_2 um ganze Zahlen mit $l_1, l_2 \geq 1$ handelt, erhält man aus der Eigenschaft $\left|\frac{\rho_1}{\tau_1}\right| > 1 > \left|\frac{\rho_2}{\tau_2}\right|$, denn (ρ,τ) ist ein Eckenpaar von Λ.
Es gilt

$$\begin{aligned} |S(\rho)| \leq |S(\lambda)| \quad &\Leftrightarrow \quad 1 \leq |\tfrac{\rho_1}{\rho_2}S(\lambda)| = |\tfrac{\rho_1}{\rho_2}S(A\rho + B\tau)| \\ &\Leftrightarrow \qquad |A + B\tfrac{\tau_2}{\rho_2}| \geq |A + B\tfrac{\tau_1}{\rho_1}|. \end{aligned}$$

Diese Ungleichung gilt im Fall $B = 0$ für alle $A \in \mathbb{F}_p[X]$.

Für $B \neq 0$ ist sie äquivalent zu

$$\left|\frac{A}{B} + \frac{\tau_2}{\rho_2}\right| \geq \left|\frac{A}{B} + \frac{\tau_1}{\rho_1}\right|.$$

Wegen

$$\left|\frac{\tau_2}{\rho_2}\right| > 1 > \left|\frac{\tau_1}{\rho_1}\right|$$

gilt dies für jede Wahl von A und $B \neq 0$ außer für die Paare (A,B) mit $\left|\frac{A}{B}\right| = \left|\frac{\tau_2}{\rho_2}\right|$ (also $\operatorname{grad} A - \operatorname{grad} B = l_2$) und $\operatorname{sgn}\frac{A}{B} = -\operatorname{sgn}\frac{\tau_2}{\rho_2}$.

Die Ungleichung $|S(\lambda)| < |S(\tau)|$ ist nach ähnlichen Folgerungen wie oben äquivalent zu $A \neq 0$ und

$$\left|\frac{B}{A} + \frac{\rho_2}{\tau_2}\right| < \left|\frac{B}{A} + \frac{\rho_1}{\tau_1}\right|.$$

Da $|\frac{\rho_2}{\tau_2}| < 1 < |\frac{\rho_1}{\tau_1}|$ gilt, ist dies genau dann richtig, wenn

$$(*) \qquad \left|\frac{B}{A}\right| < \left|\frac{\rho_1}{\tau_1}\right|,$$

also genau dann, wenn $\operatorname{grad} B - \operatorname{grad} A < l_1$ ist.
Faßt man diese Aussagen zusammen, so erhält man

$$\lambda = A\rho + B\tau \in \Lambda \cap X(\rho,\tau)$$

genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

(1) Es ist $\operatorname{grad} A - \operatorname{grad} B < l_2$ und $\operatorname{grad} B - \operatorname{grad} A < l_1$, also $-l_2 < \operatorname{grad} B - \operatorname{grad} A < l_1$ oder

(2) Es gilt $\operatorname{grad} A - \operatorname{grad} B = l_2$, aber $\operatorname{sgn}\frac{A}{B} \neq -\operatorname{sgn}\frac{\tau_2}{\rho_2}$. (Hier gilt $(*)$ wegen $\operatorname{grad} B - \operatorname{grad} A = -l_2 < l_1$.)

(3) Es ist $\operatorname{grad} A - \operatorname{grad} B > l_2$, womit automatisch wieder $(*)$ aufgrund der Ungleichung $\operatorname{grad} B - \operatorname{grad} A < -l_2 < l_1$ erfüllt ist.

(4) Es gilt $B = 0$.

Zu den Werten $\operatorname{sgn}\lambda_1$ und $\operatorname{sgn}\lambda_2$ stellt man folgendes fest:
In allen Fällen haben wir $|A\rho_1| > |B\tau_1|$ und somit $\operatorname{sgn}\lambda_1 = \operatorname{sgn} A\rho_1$.
Bezüglich des Vorzeichens von λ_2 gilt es, die Fälle (1) bis (4) getrennt zu betrachten.

(1) Hier ist $|A\rho_2| < |B\tau_2|$, d.h. $\operatorname{sgn}\lambda_2 = \operatorname{sgn} B\tau_2$.

(2) Es gilt $|A\rho_2| = |B\tau_2|$ und $\operatorname{sgn} A\rho_2 \neq -\operatorname{sgn} B\tau_2$. Für das Vorzeichen von λ_2 muß demnach $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2 + \operatorname{sgn} B\tau_2$ gelten.

(3)&(4) Hier haben wir $|A\rho_2| > |B\tau_2|$, also $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2$.

□

14.1.4 Satz

Unter den Voraussetzungen und mit den Bezeichnungen des Lemmas 14.1.3 lassen sich die Sektor-L-Funktionen $L(s;\rho,\tau)$ und $L_0(s;\rho,\tau)$ für $\operatorname{Re} s > 1$ darstellen durch

$$L(s;\rho,\tau) = \frac{\chi(\frac{\rho_2}{\tau_2})}{1-pU^2}\left(U^{-l_2} - (pU)^{l_2}\right)$$

und

$$L_0(s;\rho,\tau) = \left(\frac{(p-1)}{1-(pU)^2} \cdot \frac{(pU)^{l_1} + (pU)^{l_2} - pU - 1}{pU-1} + \frac{(p-2)(pU)^{l_2}}{1-(pU)^2} + \frac{(p-1)(pU)^{l_2}}{1-pU^2} \cdot \frac{pU^2}{1-p^2U^2} + \frac{U^{-l_2}}{1-pU^2} \right)$$

mit $U := p^{-s}$.

BEWEIS:

Wir benutzen die Bedingungen (1)-(4) aus Lemma 14.1.3 und schreiben

$$L(s;\rho,\tau) = \frac{1}{p-1} \sum_{i=1}^{4} L_i(s)$$

mit den Funktionen

$$L_i(s) = |V(\Lambda)|^s \sum_{\substack{\lambda \in \Lambda \cap X(\rho,\tau) \\ \lambda \text{ erf. Bedingung } (i)}} \frac{\chi(N(\lambda))}{|N(\lambda)|^s}$$

bzw.

$$L_0(s;\rho,\tau) = \frac{1}{p-1} \sum_{i=1}^{4} L_i^0(s)$$

mit

$$L_i^0(s) = |V(\Lambda)|^s \sum_{\substack{\lambda \in \Lambda \cap X(\rho,\tau) \\ \lambda \text{ erf. Bedingung } (i)}} \frac{1}{|N(\lambda)|^s}.$$

Hierzu bemerken wir zunächst, daß

$$\chi(N(\lambda)) = \chi(\lambda_1)\chi(\lambda_2)$$

und

$$|N(\lambda)| = |A\rho_1 + B\tau_1||A\rho_2 + B\tau_2|$$

gilt.

Wir betrachten nun die einzelnen Fälle (1)-(4), wobei wir die Aussagen des Lemmas 14.1.3 zugrundelegen.

(1) In diesem Fall ist $|\frac{\rho_2}{\tau_2}| < |\frac{B}{A}| < |\frac{\rho_1}{\tau_1}|$, also gilt $\operatorname{sgn} N(\lambda) = \operatorname{sgn}(A\rho_1 B\tau_2)$ und $|N(\lambda)| = |A\rho_1||B\tau_2|$.
Es folgt $\chi(N(\lambda)) = \chi(\rho_1\tau_2)\chi(A)\chi(B)$ und $|N(\lambda)| = |\rho_1\tau_2||A||B| = |V(\Lambda)||A||B|$ nach Lemma 13.1.2.
Damit erhält man

$$L_1(s) = \sum_k L_1(k,s) \quad (-l_2 < k < l_1)$$

mit

$$L_1(k,s) = \chi(\rho_1\tau_2) \sum_{A,B} \frac{\chi(AB)}{|A|^s|B|^s} = \chi(\rho_1\tau_2) \sum_{n \geq 0} p^{-ns} p^{-(n+|k|)s} \sum_{A,B} \chi(AB),$$

wobei die innere Summation über alle Tupel (A,B) mit $\operatorname{grad} A = n$ und $\operatorname{grad} B = n+k$ für $k \geq 0$ und andererseits über diejenigen mit $\operatorname{grad} B = n$ und $\operatorname{grad} A = n + |k|$ läuft.
Da jedes Paar führender Koeffizienten ungleich Null als $(\operatorname{sgn} A, \operatorname{sgn} B)$ für genau $p^{2n+|k|}$ Paare auftritt, hat die Summe, falls χ nicht der Hauptcharakter ist, für jedes k den Wert 0. Es ist dann also $L_1(s) = 0$.
Ist jedoch χ der Hauptcharakter – diesen Fall benötigen wir für die Berechnung von $L_0(s;\rho,\tau)$ – so ist

$$\sum_{A,B} \chi(AB) = (p-1)^2 p^{2n+|k|},$$

und somit

$$L_1(k,s) = (p-1)^2 p^{(1-s)|k|} \cdot \sum_{n=0}^{\infty} p^{(2-2s)n} = \frac{(p-1)^2 (pU)^{|k|}}{1-(pU)^2}$$

für $\operatorname{Re} s > 1$. In dieser Halbebene erhält man dann zusammen

$$\begin{aligned} L_1^0(s) &= \frac{(p-1)^2}{1-(pU)^2} \left(\sum_{k=0}^{l_1-1} (pU)^k + \sum_{k=0}^{l_2-1} (pU)^k - 1 \right) \\ &= \frac{(p-1)^2}{1-(pU)^2} \frac{(pU)^{l_1} + (pU)^{l_2} - pU - 1}{pU-1}. \end{aligned}$$

(2) In diesem Fall gilt $\operatorname{sgn} \lambda_1 = \operatorname{sgn} A\rho_1$ und $\operatorname{sgn} \lambda_2 = \operatorname{sgn} A\rho_2 + \operatorname{sgn} B\tau_2$ nach Lemma 14.1.3 (2). Es ist dann $\chi(N(\lambda)) = \chi(A\rho_1)\chi(\operatorname{sgn} A\rho_2 + \operatorname{sgn} B\tau_2)$. Weiterhin ist $|\frac{A}{B}| = |\frac{\tau_2}{\rho_2}|$ nach Lemma 14.1.3 (2), aber $\operatorname{sgn} A\rho_2 \neq -\operatorname{sgn} B\tau_2$. Es gilt also $|A\rho_2 + B\tau_2| = |B\tau_2|$. Wegen $l_1 > -l_2 = \operatorname{grad} B - \operatorname{grad} A$ ist auch $|A\rho_1| > |B\tau_1|$. Man erhält $|N(\lambda)| = |A\rho_1||B\tau_2| = |V(\Lambda)||A||B|$ wie schon in (1). Es ist dann

$$\begin{aligned} L_2(s) &= \chi(\rho_1\rho_2) \sum_{\substack{A,B \\ \operatorname{grad} A = \operatorname{grad} B + l_2}} \frac{\chi(A)\chi(\operatorname{sgn} A + \operatorname{sgn} B\frac{\tau_2}{\rho_2})}{|A|^s |B|^s} \\ &= \chi(\rho_1\rho_2) \sum_{n \geq 0} p^{-(n+l_2)s} p^{-ns} p^{2n+l_2} \sum_{\substack{\zeta,\mu \neq 0 \\ \mu+\zeta \neq 0}} \chi(\mu)\chi(\mu+\zeta). \end{aligned}$$

Für die letzte Summe ergibt sich

$$\begin{aligned} \sum_{\substack{\mu,\zeta \neq 0 \\ \mu+\zeta \neq 0}} \chi(\mu)\chi(\zeta+\mu) &= \sum_{\mu \neq 0} \chi(\mu) \sum_{\substack{\zeta \neq 0 \\ \mu+\zeta \neq 0}} \chi(\mu+\zeta) \\ &= \sum_{\mu \neq 0} \chi(\mu) \Big(\underbrace{\sum_{\mu+\zeta \neq 0} \chi(\mu+\zeta)}_{=0} - \chi(\mu) \Big) \\ &= -\sum_{\mu \neq 0} 1 = -(p-1) = 1-p. \end{aligned}$$

Die Reihe über n konvergiert absolut für $\operatorname{Re} s > 1$, und man erhält nach Anwendung der geometrischen Reihe die Darstellung

$$L_2(s) = \chi(\rho_1\rho_2) \frac{(1-p)(pU)^{l_2}}{1-p^2U^2}$$

in dieser Halbebene.

Ist hier χ der Hauptcharakter, so ist

$$\sum_{\substack{\mu,\zeta\neq 0\\ \mu+\zeta\neq 0}} \chi(\mu)\chi(\zeta+\mu) = (p-1)(p-2),$$

und es folgt sofort

$$L_2^0(s) = \frac{(p-1)(p-2)(pU)^{l_2}}{1-(pU)^2}$$

für $\operatorname{Re} s > 1$.

(3) Hier ist $\operatorname{sgn}\lambda_1 = \operatorname{sgn} A\rho_1$, $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2$ und $|\frac{B}{A}| < |\frac{\rho_2}{\tau_2}| < |\frac{\rho_1}{\tau_1}|$ nach Lemma 14.1.3 (3).

Es ist demnach $\chi(N(\lambda)) = \chi(A\rho_1)\chi(A\rho_2) = \chi(\rho_1\rho_2)$, $|A\rho_1 + B\tau_1| = |A\rho_1|$ und $|A\rho_2 + B\tau_2| = |A\rho_2|$. Daraus folgt

$$|N(\lambda)| = |A\rho_1||A\rho_2| = |\rho_1\tau_2||\frac{\rho_2}{\tau_2}||A|^2 = p^{-l_2}|V(\Lambda)||A|^2,$$

woraus man

$$L_3(s) = \chi(\rho_1\rho_2)p^{sl_2} \sum_{\substack{A,B\\ \operatorname{grad} A>\operatorname{grad} B+l_2}} \frac{1}{|A|^{2s}}$$

erhält.

Setzt man $n := \operatorname{grad} A$ und $m := \operatorname{grad} B$, so ergibt sich für die obige Summe nach Berücksichtigung der Anzahl der vorkommenden Funktionen

$$\begin{aligned}
\sum_{\substack{A,B\\ \operatorname{grad} A>\operatorname{grad} B+l_2}} \frac{1}{|A|^{2s}} &= \sum_{n>m+l_2} (p-1)^2 p^{n+m} p^{-2ns} \\
&= (p-1)^2 \sum_{m\geq 0} (p^2U^2)^m \sum_{n\geq 0} (pU^2)^{l_2+1+n} \\
&= (p-1)^2 \sum_{m\geq 0} (p^2U^2)^m \left(\frac{(pU^2)^{l_2+1}}{1-pU^2}\right) \\
&= (p-1)^2 \frac{(pU^2)^{l_2}}{1-pU^2}\frac{pU^2}{1-p^2U^2}
\end{aligned}$$

für $\operatorname{Re} s > 1$, denn dafür konvergieren alle auftretenden Reihen absolut. Zusammenfassend hat man dann wegen $p^{sl_2} = U^{-l_2}$

$$L_3(s) = \chi(\rho_1\rho_2)\frac{(p-1)^2(pU)^{l_2}}{1-pU^2}\cdot\frac{pU^2}{1-p^2U^2}$$

und

$$L_3^0(s) = \frac{(p-1)^2(pU)^{l_2}}{1-pU^2}\cdot\frac{pU^2}{1-p^2U^2}.$$

(4) Wegen $B = 0$, $\operatorname{sgn}\lambda_1 = \operatorname{sgn} A\rho_1$ und $\operatorname{sgn}\lambda_2 = \operatorname{sgn} A\rho_2$ ist in diesem Fall $\chi(N(\lambda)) = \chi(\rho_1\rho_2)$ und $|N(\lambda)| = p^{-l_2}|V(\Lambda)||A|^2$. Wir erhalten

$$L_4(s) = \chi(\rho_1\rho_2)p^{sl_2} \sum_{A\in\mathbb{F}_p[X]} \frac{1}{|A|^{2s}}.$$

Für die Summe auf der rechten Seite der Gleichung erhält man

$$\begin{aligned}\sum_{A\in\mathbb{F}_p[X]} \frac{1}{|A|^{2s}} &= (p-1)\sum_{n\geq 0} p^n p^{-2ns} = (p-1)\sum_{n\geq 0} p^{(1-2s)n} \\ &= (p-1)\sum_{n\geq 0}(pU^2)^n = \frac{p-1}{1-pU^2}\end{aligned}$$

in der Halbebene $\operatorname{Re} s > \frac{1}{2}$, denn die Reihen konvergieren dort absolut.
Es folgt

$$L_4(s) = \chi(\rho_1\rho_2)\frac{(p-1)U^{-l_2}}{1-pU^2} = \chi(\rho_1\rho_2)L_4^0(s).$$

Setzt man (1)-(4) in die Formel für $L(s,\rho,\tau)$ bzw. $L_0(s;\rho,\tau)$ ein, so erhält man endlich

$$\begin{aligned}L(s,\rho,\tau) &= \chi(\rho_1\rho_2)\frac{1}{p-1}\left(\frac{(1-p)(pU)^{l_2}}{1-p^2U^2} + \frac{(p-1)^2(pU)^{l_2}}{1-pU^2}\frac{pU^2}{1-p^2U^2} + \frac{(p-1)U^{-l_2}}{1-pU^2}\right) \\ &= \frac{\chi(\rho_1\rho_2)}{1-pU^2}\left(U^{-l_2} - (pU)^{l_2}\right)\end{aligned}$$

und

$$\begin{aligned}L_0(s;\rho,\tau) &= \frac{1}{p-1}\left(\frac{(p-1)^2}{1-(pU)^2}\cdot\frac{(pU)^{l_1}+(pU)^{l_2}-pU-1}{pU-1}\right. \\ &\quad \left. + \frac{(p-1)(p-2)(pU)^{l_2}}{1-(pU)^2} + \frac{(p-1)^2(pU)^{l_2}}{1-pU^2}\cdot\frac{pU^2}{1-p^2U^2} + \frac{(p-1)U^{-l_2}}{1-pU^2}\right).\end{aligned}$$

Es bleibt also nur noch zu zeigen, daß $\chi(\rho_1\rho_2) = \chi(\frac{\rho_2}{\tau_2})$ gilt.

Diese Aussage erhält man aus der Tatsache, daß es sich bei (ρ,τ) um ein Eckenpaar handelt. Es gilt nämlich

$$1 \overset{13.2.1\text{ (iii)}}{=} \chi(\rho_1\tau_2 - \tau_1\rho_2) = \chi(\rho_1\rho_2)\chi\left(\frac{\tau_2}{\rho_2} - \frac{\tau_1}{\rho_1}\right) = \chi(\rho_1\rho_2)\chi\left(\frac{\tau_2}{\rho_2}\right),$$

denn es ist $\left|\frac{\tau_2}{\rho_2}\right| > 1 > \left|\frac{\tau_1}{\rho_1}\right|$ wegen 13.2.1 (ii).
Daraus erhält man schließlich $\chi(\rho_1\rho_2) = \chi\left(\frac{\rho_2}{\tau_2}\right)$. □

14.2 Die Berechnung spezieller Werte von $L(s,A)$ und $Z(s,A)$

14.2.1 Satz

Es sei A eine enge Idealklasse und $\mathfrak{a} \in A$ ein ganzes Ideal. Dieses sei so gewählt, daß es eine Basis besitzt, so daß $\Lambda_\mathfrak{a} = [\gamma^{(0)}, \gamma^{(1)}]$ ein Gitter mit einem Eckenpaar $(\gamma^{(0)}, \gamma^{(1)})$ ist. Ferner sei $Z = Z_0^* := \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$.

Sind dann M_r^* für $r \geq 0$ die Partialbrüche der engen KBE-Art und $\delta := \rho_*$ die Periode der engen KBE von Z, so ist

$$L(s,A) = U^m \frac{1}{1-pU^2}\left[P(\frac{1}{pU},A) - P(U,A)\right]$$

mit

$$P(U,A) = \sum_{r=1}^{\delta} \chi\left(\frac{\gamma_2^{(r)}}{\gamma_2^{(r+1)}}\right)(pU)^{\operatorname{grad}\frac{\gamma_1^{(r-1)}}{\gamma_1^{(r)}}} = \sum_{r=1}^{\delta} \chi(M_{r-1}^*)(pU)^{\operatorname{grad} M_{r-1}^*}$$

und $m = \frac{\operatorname{grad} D}{2}$. Weiterhin gilt

$$L_0(s,A) = \frac{U^m}{(1-pU)^2}\left((p-1)\delta - \frac{p(U-1)^2 P_0(U,A) + (1-pU)^2 P_0(\frac{1}{pU},A)}{1-pU^2}\right)$$

mit

$$P_0(U,A) = \sum_{r=1}^{\delta}(pU)^{\operatorname{grad} M_{r-1}^*}.$$

BEWEIS:

Es sei $\mathfrak{a} =< \omega_1, \omega_2 > \in A$ ein ganzes Ideal mit einer orientierten Basis (ω_1, ω_2), deren Basisquotient $\frac{\omega_2}{\omega_1}$ reduziert ist. $\Lambda_\mathfrak{a} = [\gamma^{(0)}, \gamma^{(1)}]$ sei sein zugehöriges Gitter.
Offensichtlich ist dann der Sektor $X(\gamma^{(0)}, \epsilon_1 * \gamma^{(0)})$ ein Fundamentalbereich für die Operation von ϵ_1 auf P. Dieser läßt sich nach Proposition 13.2.5 und Lemma 13.2.6 darstellen als Vereinigung kleinerer Sektoren in der Form

$$X(\gamma^{(0)}, \epsilon_1 * \gamma^{(0)}) = X(\gamma^{(0)}, c_0^{-1}\epsilon_1 * \gamma^{(0)}) = \bigcup_{r=1}^{\delta} X(\gamma^{(r-1)}, \gamma^{(r)}),$$

wobei die $\gamma^{(r-1)}, \gamma^{(r)}$ jeweils Eckenpaare (insbesondere Basen) von $\Lambda_\mathfrak{a}$ sind und das $c_0 \in \mathbb{F}_p^*$ wie in Lemma 13.2.6 gewählt sei. Nach Definition der Sektoren ist diese Vereinigung disjunkt und läßt nach Bemerkung 14.1.2 für die L-Funktionen $L(s,A)$ und $L_0(s,A)$ die Darstellungen

$$L(s,A) = |\sqrt{D}|^{-s}\frac{\operatorname{Vol}(\Lambda_\mathfrak{a})}{p-1}\sum_{\lambda \in X(\gamma^{(0)}, \epsilon_1 * \gamma^{(0)}) \cap \Lambda_\mathfrak{a}} \frac{\chi(N(\lambda))}{|N(\lambda)|^s} = |\sqrt{D}|^{-s}\sum_{r=1}^{\delta} L(s; \gamma^{(r-1)}, \gamma^{(r)})$$

und

$$L_0(s,A) = |\sqrt{D}|^{-s}\sum_{r=1}^{\delta} L_0(s; \gamma^{(r-1)}, \gamma^{(r)})$$

zu.
Zur Berechnung der Sektor-L-Funktionen $L(s; \gamma^{(r-1)}, \gamma^{(r)})$ für $r \geq 1$ nehmen wir Lemma 14.1.3 und Satz 14.1.4 zu Hilfe.
Für $r \geq 1$ und $\gamma^{(r-1)}$ und $\gamma^{(r)}$ schreiben wir $Z_{r-1}^* = \frac{\gamma_1^{(r-1)}}{\gamma_1^{(r)}}$ für die vollständigen Partialbrüche und $M_{r-1}^* = [Z_{r-1}^*]$ für die Partialbrüche, die aus der engen KBE von $Z := Z_0^* = \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$ hervorgehen.
Wie in Satz 14.1.3 definieren wir für $r \geq 1$ die Werte

$$l_1(r) := \operatorname{grad} Z_{r-1}^* \quad \text{und} \quad l_2(r) := -\operatorname{grad}\overline{Z_{r-1}^*}.$$

Aus Lemma 5.3.2 (i) erhalten wir dann

$$l_1(r) = \operatorname{grad} M^*_{r-1} = l_2(r+1)$$

für alle $r \geq 1$. Aus Satz 14.1.4 folgt

$$L(s;\gamma^{(r-1)},\gamma^{(r)}) = \frac{\chi(\overline{Z^*_{r-1}})}{1-pU^2}\left(U^{-l_2(r)} - (pU)^{l_2(r)}\right).$$

Schreibt man

$$P(U,A) := \sum_{r=1}^{\delta} \chi(\overline{Z^*_{r-1}})(pU)^{l_2(r)} \overset{\delta \text{ Periode}}{=} \sum_{r=1}^{\delta} \chi(\overline{Z^*_r})(pU)^{l_1(r)},$$

und benutzt die Gleichung

$$\chi(\overline{Z^*_r}) = \chi(Z^*_{r-1}) = \chi(M^*_{r-1}),$$

die aus Lemma 5.3.5 in Verbindung mit der Reduziertheit von Z^*_r folgt, so erhält man die Formel

$$L(s,A) = \frac{U^m}{1-pU^2}\left(P(\frac{1}{pU},A) - P(U,A)\right)$$

mit

$$P(U,A) = \sum_{r=1}^{\delta} \chi(M^*_{r-1})(pU)^{\operatorname{grad} M^*_{r-1}}$$

und $m = \frac{\operatorname{grad} D}{2}$, denn in diesem Fall ist $U^m = |\sqrt{D}|^{-s}$. Ebenso erhält man mit

$$P_0(U,A) := \sum_{r=1}^{\delta}(pU)^{l_2(r)} = \sum_{r=1}^{\delta}(pU)^{l_1(r)}$$

die Formel

$$\begin{aligned}
L_0(s,A) &= \frac{U^m}{(1-pU)^2}\sum_{r=1}^{\delta}\left(\frac{(p-1)(pU+1)}{pU+1} - \frac{(p-1)((pU)^{l_1}+(pU)^{l_2})}{1+pU}\right.\\
&\quad \left. + \frac{(p-2)(pU)^{l_2}(1-pU)}{1+pU} + \frac{(p-1)(pU)^{l_2}(1-pU)pU^2}{(1-pU^2)(1+pU)} + \frac{U^{-l_2}(1-pU)^2}{1-pU^2}\right)\\
&= \frac{U^m}{(1-pU)^2}\left((p-1)\delta + \frac{P_0(U,A)((-2(p-1)+(p-2)(1-pU))(1-pU^2)}{(1+pU)(1-pU^2)}\right.\\
&\quad \left. + \frac{(p-1)(1-pU)pU^2 + (1-pU)^2(1+pU)P_0(\frac{1}{pU},A)}{(1+pU)(1-pU^2)}\right)\\
&= \frac{U^m}{(1-pU)^2}\left((p-1)\delta - \frac{p(U-1)^2P_0(U,A) + (1-pU)^2P_0(\frac{1}{pU},A)}{1-pU^2}\right).
\end{aligned}$$

□

14.2.2 Lemma

Ist $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper und $A \in C^+(K)$, so läßt sich $L(s,A)$ zu einer auf ganz $\mathbb{C}$ holomorphen Funktion von s fortsetzen und erfüllt die Funktionalgleichung

$$L(1-s,A) = p^{1-2s} p^{m(2s-1)} L(s,A)$$

mit $m := \frac{\operatorname{grad} D}{2}$.
Ist $U := p^{-s}$, so handelt es sich bei $L(s,A)$ um ein Polynom in $\mathbb{Z}[U]$, d.h. insbesondere gilt

$$L(1-n,A) \in \mathbb{Z}$$

für alle $n \geq 1$.

BEWEIS:

Die Funktion

$$L(s,A) = \frac{U^m}{1-pU^2}\left(P(\frac{1}{pU},A) - P(U,A)\right)$$

besitzt offensichtlich höchstens bei $s = \frac{1}{2} + \frac{\pi i k}{\log p}$ für $k \in \mathbb{Z}$ isolierte Singularitäten. Wegen

$$\begin{aligned}
\lim_{s \to \frac{1}{2}+\frac{\pi i k}{\log p}} (s - (\frac{1}{2} + \frac{\pi i k}{\log p}))L(s,A) &= \lim_{s \to \frac{1}{2}+\frac{\pi i k}{\log p}} \left(\frac{(s - (\frac{1}{2} + \frac{\pi i k}{\log p}))p^{-sm}}{1-p^{1-2s}}\right) \\
&\quad \cdot \lim_{s \to \frac{1}{2}+\frac{\pi i k}{\log p}} (P(\frac{1}{p^{1-s}},A) - P(p^{-s},A)) \\
&= \frac{p^{-\frac{1}{2}m}}{2\log p}(P((-1)^k p^{-\frac{1}{2}},A) - P((-1)^k p^{-\frac{1}{2}},A)) \\
&= 0
\end{aligned}$$

sind diese sämtlich hebbar, $L(s,A)$ ist also als Funktion von s in die ganze komplexe Ebene holomorph fortsetzbar.
Beim Übergang $s \mapsto 1-s$ geht $U = p^{-s}$ über in $p^{s-1} = \frac{1}{pU}$, das bedeutet

$$\begin{aligned}
L(1-s,A) &= \frac{(pU)^{-m}}{1-\frac{1}{pU^2}}(P(U,A) - P(\frac{1}{pU},A)) \\
&= \frac{pU^2(pU)^{-m}}{1-pU^2}(P(\frac{1}{pU},A) - P(U,A)) \\
&= p^{1-2s}p^{-m}p^{2sm}\frac{U^m}{1-pU^2}(P(\frac{1}{pU},A) - P(U,A)) \\
&= p^{1-2s}p^{m(2s-1)}L(s,A),
\end{aligned}$$

und entspricht der behaupteten Funktionalgleichung.
In den Bezeichnungen des Satzes 14.2.1 ist

$$P(U,A) = \sum_{r=1}^{\delta} \chi(M_{r-1}^*)(pU)^{\operatorname{grad} M_{r-1}^*},$$

also

$$P(\frac{1}{pU},A) = \sum_{r=1}^{\delta} \chi(M_{r-1}^*)U^{-\operatorname{grad} M_{r-1}^*}.$$

Daraus folgt

$$P(\frac{1}{pU},A)-P(U,A)=\sum_{r=1}^{\delta}\chi(M_{r-1}^*)U^{-\operatorname{grad}M_{r-1}^*}(1-(pU^2)^{\operatorname{grad}M_{r-1}^*}).$$

Nach Proposition 6.1.2 (iii) ist $\operatorname{grad}M_{r-1}^*\leq m$, und zusammen mit $\operatorname{grad}M_{r-1}^*\geq 1$ erhält man

$$\begin{aligned}L(s,A) &= \frac{U^m}{1-pU^2}\left(P(\frac{1}{pU},A)-P(U,A)\right)\\ &= \sum_{r=1}^{\delta}\chi(M_{r-1}^*)U^{m-\operatorname{grad}M_{r-1}^*}\underbrace{\left(\frac{1-(pU^2)^{\operatorname{grad}M_{r-1}^*}}{1-pU^2}\right)}_{\in\mathbb{Z}[U]}\in\mathbb{Z}[U].\end{aligned}$$

Ist $s=n\geq 1$, so hat man also $p^{-(1-s)}=p^{n-1}$, was bedeutet, daß $L(1-n,A)$ für $n\geq 1$ nur ganzzahlige Werte annimmt. □

14.2.3 Satz

Es sei $A\in C^+(K)$ und $\mathfrak{a}=<\omega_1,\omega_2>\in A$ ein ganzes Ideal mit einer orientierten Basis (ω_1,ω_2), deren Basisquotient $\frac{\omega_2}{\omega_1}$ reduziert ist. Dann ist $\Lambda_{\mathfrak{a}}=[\gamma^{(0)},\gamma^{(1)}]$ mit einem Eckenpaar $(\gamma^{(0)},\gamma^{(1)})$. Es sei ferner $Z:=Z_0^*=\frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$. Dann erhält man die Formeln

$$L(1,A)=p^{1-m}\sum_{r=1}^{\rho_*}\chi(M_{r-1}^*)\frac{|M_{r-1}^*|-1}{p-1}=p^{1-m}L(0,A)$$

und

$$L(\frac{\pi i}{\log p},A)=(-1)^m\sum_{r=1}^{\rho_*}(-1)^{\operatorname{grad}M_{r-1}^*}\chi(M_{r-1}^*)\frac{|M_{r-1}^*|-1}{p-1},$$

wobei M_{r-1}^* für $r\geq 1$ die Partialbrüche und ρ_* die Periode der engen KBE von Z sind.

BEWEIS:

Ist $U=p^{-s}$ und $s=0$, so folgt $U=1$. Eingesetzt in die Formel aus Satz 14.2.1 erhält man dann mit $\delta=\rho_*$ die Identität

$$\begin{aligned}L(0,A) &= \frac{1}{1-p}\left(\sum_{i=1}^{\rho_*}\chi(M_{r-1}^*)-\sum_{i=1}^{\rho_*}\chi(M_{r-1}^*)p^{\operatorname{grad}M_{r-1}^*}\right)\\ &= \sum_{i=1}^{\rho_*}\chi(M_{r-1}^*)\frac{|M_{r-1}^*|-1}{p-1},\end{aligned}$$

und die Aussage für $L(1,A)$ folgt dann aus der Funktionalgleichung aus Lemma 14.2.2. Für $s=\frac{\pi i}{\log p}$ ist $U=-1$. Abermaliges Einsetzen in die Formel aus Satz 14.2.1 liefert die Behauptung. □

Über Satz 14.2.3 läßt sich die Brücke schlagen zum klassischen, d.h. zum Zahlkörperfall. Hier führt (vgl. [Zag2], S. 126ff.) die Untersuchung der engen Idealklassen zu Aussagen, welche sich am einfachsten mit Hilfe der negativen Kettenbruchentwicklung ausdrücken lassen.

In unserem Fall stellt man zum einen fest, daß sich in der Formel des Satzes 14.2.3 die Periode ρ_* der engen Kettenbruchentwicklung durch die Quadratperiode μ_- der negativen KBE des Elements Z ersetzen läßt.
Zum anderen bleibt die Formel gültig, wenn man die Partialbrüche M^*_{r-1} der engen KBE durch die Partialbrüche M^-_{r-1} der negativen KBE von Z ersetzt.
Dies sieht man wie folgt ein:

Die Gleichung $\rho_* = \mu_-$ wurde schon in 6.2.2 hergeleitet. Daß die Grade der Partialbrüche M^*_{r-1} und M^-_{r-1} gleich sind, liegt daran, daß sie sich wegen Lemma 5.1.3 höchstens um einen Faktor aus $\mathbb{F}_p^*$ unterscheiden. Es bleibt also zu zeigen, daß

$$\chi(M^*_r) = \chi(M^-_r)$$

für alle $r \geq 0$ richtig ist.

Für $r \geq 0$ sei dazu $M^+_r = \mu_r M^*_r$ mit den $\mu_r \in \mathbb{F}_p^*$, welche man nach Lemma 5.1.3 aus der engen KBE erhält.
Aus Folgerung 5.1.4 folgt dann zunächst

$$\chi(M^-_r) = \chi((-1)^r M^+_r) = \chi(-1)^r \chi(\mu_r M^*_r).$$

Unter Verwendung von Lemma 5.1.3 erhält man für ungerade $r \geq 1$

$$\chi(\mu_r) = \chi\left(\prod_{i=0}^{\frac{r-1}{2}} \frac{\eta_{2i-1}}{\eta_{2i}}\right) \overset{\chi(\eta)=\chi(\eta^{-1})}{=} \chi\left(\prod_{i=0}^{r-1} \eta_i\right) = \chi(-1)^r,$$

denn es ist $\eta \simeq (-1)_{r\geq 0}$.
Ist r hingegen gerade, so ergibt sich mit denselben Schlußweisen

$$\chi(\mu_r) = \chi\left(\prod_{i=0}^{\frac{r}{2}-1} \frac{\eta_{2i-1}}{\eta_{2i}}\right) = \chi\left(\prod_{i=0}^{r-1} \eta_i\right) = \chi(-1)^r.$$

Damit ist $\chi(M^-_r) = \chi(-1)^{2r}\chi(M^*_r) = \chi(M^*_r)$, und wir haben bewiesen:

14.2.4 Folgerung

Unter den Voraussetzungen des Satzes 14.2.3 gilt

$$L(0, A) = \sum_{i=1}^{\mu_-} \chi(M^-_{r-1}) \frac{|M^-_{r-1}| - 1}{p-1} = p^{m-1} L(1, A)$$

und

$$L(\frac{\pi i}{\log p}, A) = (-1)^m \sum_{r=1}^{\mu_-} (-1)^{\operatorname{grad} M^-_{r-1}} \chi(M^-_{r-1}) \frac{|M^-_{r-1}| - 1}{p-1},$$

wobei μ_- die Quadratperiode und M^-_{r-1} die Partialbrüche der negativen KBE des Elements $Z = \frac{\gamma_1^{(0)}}{\gamma_1^{(1)}}$ aus Satz 14.2.3 sind.

Benutzt man auch für die Darstellung der Funktion $L_0(s, A)$ die Periode und die Partialbrüche der negativen KBE wie in 14.2.4, so erhält man den

14.2.5 Satz

Sind Z_{r-1}^-, M_{r-1}^- und μ_- für $r \geq 1$ wie in Folgerung 14.2.4 gewählt, so besitzt die Funktion $L_0(s,A)$ die Darstellung

$$L_0(s,A) = \frac{U^m}{(1-pU)^2}\left((p-1)\mu_- - \frac{p(U-1)^2 P_0(U,A)}{1-pU^2} + \frac{(1-pU)^2 P_0(\frac{1}{pU},A)}{1-pU^2}\right)$$

mit

$$P_0(U,A) = \sum_{r=1}^{\mu_-}(pU)^{\operatorname{grad} M_{r-1}^-}.$$

Als Funktion von s ist sie auf ganz $\mathbb{C}$ holomorph mit Ausnahme einfacher Pole an den Stellen $s = 1 + \frac{2\pi i}{\log p}$ für $n \in \mathbb{Z}$ mit den Residuen

$$a_{-1}(K) := \frac{p-1}{p^m \log p} R_K,$$

welche nur von K, nicht aber von der engen Idealklasse A abhängen. Ist

$$L_0(s,A) = \frac{a_{-1}(K)}{s-1} + a_0(A) + a_1(A)(s-1) + \ldots$$

die Laurent-Entwicklung von $L_0(s,A)$ in $s=1$, so erhält man für $a_0(A)$ die Formel

$$a_0(A) = p^{1-m}\sum_{r=1}^{\mu_-}\frac{|M_{r-1}^-|-1}{p-1} - \frac{(p-1)}{2p^m}\left(2(m-1)R_K + \sum_{r=1}^{\mu_-}(\operatorname{grad} M_{r-1}^-)^2\right).$$

Die Werte von $L_0(s,A)$ an den Stellen $s=0$ und $s = \frac{\pi i}{\log p}$ sind gegeben durch

$$L_0(0,A) = 0 \quad \text{und} \quad L_0(\frac{\pi i}{\log p}, A) = \frac{(-1)^m}{(p+1)^2}\left(4p\sum_{r=1}^{\mu_-}(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1} + 2W(p-1)\right),$$

wobei die Zahl $W \in \mathbb{N}_0$ definiert ist durch

$$W := \#\{M_{r-1}^- \mid r \in \{1,\ldots,\mu_-\},\ \operatorname{grad} M_{r-1}^- \text{ ungerade}\}.$$

BEWEIS:

Die Funktion $L_0(s,A)$ besitzt offensichtlich isolierte Singularitäten an den Stellen $z_k := \frac{1}{2} + \frac{\pi i k}{\log p}$ und $s_k := 1 + \frac{2\pi i k}{\log p}$ $(k \in \mathbb{Z})$. Daß die Singularitäten in den Stellen z_k $(k \in \mathbb{Z})$ sämtlich hebbar sind, sieht man wie in Lemma 14.2.2. Bei den s_k $(k \in \mathbb{Z})$ handelt es sich jedoch um Pole erster Ordnung. Dies sieht man wie folgt ein:
Die Funktion $(1-pU)^2 L_0(s,A)$ hat wegen $P_0(\frac{1}{p},A) = \mu_-$ eine Nullstelle bei $U = \frac{1}{p}$, d.h. bei $L_0(s,A)$ handelt es sich um eine rationale Funktion von U mit $(1-pU)$ im Nenner. Ist also $L_0(s,A) = F(U)$ und setzen wir $l_1(r) := \operatorname{grad} M_{r-1}^-$, so ist das Residuum von F in $U = \frac{1}{p}$ gegeben durch

$$\begin{aligned}
\operatorname{Res}(F(U), U=\frac{1}{p}) &= \lim_{U\to\frac{1}{p}}\frac{U^m(U-\frac{1}{p})}{1-pU}\lim_{U\to\frac{1}{p}}\frac{(p-1)\mu_-(1-pU^2) - p(U-1)^2 P_0(U,A)}{(1-pU)(1-pU^2)} \\
&\overset{\text{L'Hospital}}{=} \frac{-1}{p^{1+m}}\cdot\frac{-2\mu_- 2p(\frac{1}{p}-1)P_0(\frac{1}{p},A) - p(\frac{1}{p}-1)^2\sum_{r=1}^{\mu_-} l_1(r)p^{l_1(r)}(\frac{1}{p})^{l_1(r)-1}}{1-\frac{1}{p}} \\
&= \frac{1-p}{p^{1+m}}\sum_{r=1}^{\mu_-} l_1(r) = \frac{1-p}{p^{1+m}}\sum_{r=1}^{\mu_-}(-\operatorname{grad}\overline{Z_{r-1}^-}),
\end{aligned}$$

denn es ist

$$\sum_{r=1}^{\mu_-} \operatorname{grad} M_{r-1}^- = \sum_{r=1}^{\mu_-} \operatorname{grad} Z_{r-1}^- \overset{5.3.2}{=} \sum_{r=1}^{\mu_-} -\operatorname{grad} \overline{Z_r^-} \overset{\mu_- \text{ Qu.-Per.}}{=} \sum_{r=1}^{\mu_-} -\operatorname{grad} \overline{Z_{r-1}^-}.$$

Weiterhin gilt

$$\begin{aligned} \frac{1-p}{p^{1+m}} \sum_{r=1}^{\mu_-} -\operatorname{grad} \overline{Z_{r-1}^-} &= \frac{1-p}{p^{1+m}} \sum_{r=1}^{\mu_-} (\operatorname{grad} \gamma_2^{(r)} - \operatorname{grad} \gamma_2^{(r-1)}) = \frac{1-p}{p^{1+m}} \operatorname{grad} \left(\frac{\gamma_2^{(\mu_-)}}{\gamma_2^{(0)}} \right) \\ &\overset{13.2.7}{=} \frac{1-p}{p^{1+m}} \operatorname{grad} \overline{\epsilon_1}, \end{aligned}$$

denn nach 6.2.2 ist $\mu_- = \rho_* = \delta$ aus 13.2.7. Es ist nun

$$\operatorname{Res}(L_0(s,A), s=1) = \frac{-p}{\log p} \operatorname{Res}(F(U), U = \frac{1}{p}),$$

woraus die Behauptung über das Residuum von $L_0(s,A)$ an der Stelle $s=1$ folgt, wenn man noch die Gleichung

$$\operatorname{grad} \overline{\epsilon_1} \overset{Q_K=2}{=} \operatorname{grad} \epsilon_0 = R_K$$

einbringt. Das Residuum hängt somit nicht von der Klasse A, sondern lediglich vom Körper K ab. Wir bezeichnen es fortan mit $a_{-1}(K)$.
Ist also $L_0(s,A) = \frac{a_{-1}(K)}{s-1} + a_0(A) + a_1(A)(s-1) + \ldots$ die Laurententwicklung von $L_0(s,A)$ in $s=1$, so kann man den Wert $a_0(A) = \lim_{s \to 1} \left(L_0(s,A) - \frac{a_{-1}(K)}{s-1} \right)$ berechnen. Dazu sei $s > 1$ reell. Mit F wie oben gilt

$$\begin{aligned} a_0(A) &= \lim_{s \to 1} \left(L_0(s,A) - \frac{a_{-1}(K)}{s-1} \right) \\ &= \lim_{U \to \frac{1}{p}} \left(F(U) + \frac{a_{-1}(K) \log p}{\log pU} \right), \end{aligned}$$

denn es ist $\frac{1}{s-1} = -\frac{\log p}{\log pU}$ für $U = p^{-s}$ und reelles $s > 1$. Wir haben also

$$\begin{aligned} a_0(A) &= \lim_{U \to \frac{1}{p}} \left(\frac{U^m}{(1-pU)^2} \left((p-1) \cdot \mu_- - \frac{p(U-1)^2 P_0(U,A)}{1-pU^2} \right) + \frac{(p-1)R_K}{p^m \log pU} \right) + \frac{p^{1-m} P_0(1,A)}{p-1} \\ &= \lim_{U \to \frac{1}{p}} \left(\frac{U^m}{(1-pU)^2} \left(\frac{p(U-1)^2 (P_0(U,A) - \mu_-)}{pU^2 - 1} \right) + \frac{(p-1)R_K}{p^m \log pU} \right) + \frac{p^{1-m}(P_0(1,A) - \mu_-)}{p-1}, \end{aligned}$$

woraus nach Multiplikation mit p^m folgt

$$\begin{aligned} p^m a_0(A) - p \frac{P_0(1,A) - \mu_-}{p-1} &= \lim_{U \to \frac{1}{p}} \left(\frac{(pU)^m (pU-p)^2 (P_0(U,A) - \mu_-)}{(1-pU)^2((pU)^2 - p)} + \frac{(p-1)R_K}{\log pU} \right) \\ &\overset{x := pU}{=} \lim_{x \to 1} \left(\frac{f(x)}{x-1} + \frac{(p-1)R_K}{\log x} \right) \end{aligned}$$

mit

$$f(x) := \frac{x^m (x-p)^2}{x^2 - p} \cdot \frac{P_0(\frac{x}{p}, A) - \mu_-}{x-1}.$$

Es ist aber

$$\frac{P_0(\frac{x}{p},A)-\mu_-}{x-1}=\sum_{r=1}^{\mu_-}\frac{1-x^{\operatorname{grad} M^-_{r-1}}}{1-x}=\sum_{r=1}^{\mu_-}\sum_{i=0}^{\operatorname{grad} M^-_{r-1}-1}x^i,$$

demnach

$$f(1)=\frac{(1-p)^2}{1-p}\sum_{r=1}^{\mu_-}\operatorname{grad} M_{r-1}=\frac{(1-p)^2}{1-p}\sum_{r=1}^{\mu_-}-\operatorname{grad}\overline{Z^-_{r-1}}=-(p-1)R_K$$

mit denselben Schlüssen wie oben.
Die Funktion $\frac{1}{\log x}$ läßt sich bekanntlich darstellen in der Form

$$\frac{1}{\log x}=\frac{1}{x-1}+\frac{1}{2}+h(x),$$

wobei h eine in 1 stetige Funktion mit $h(1)=0$ ist. Daraus folgt

$$\begin{aligned}p^m a_0(A)-p\frac{P_0(1,A)-\mu_-}{p-1} &= \lim_{x\to 1}\left(\frac{f(x)}{x-1}+\frac{(p-1)R_K}{\log x}\right)\\ &= \lim_{x\to 1}\left(\frac{f(x)-f(1)}{x-1}+\frac{(p-1)R_K}{2}\right)=f'(1)+\frac{(p-1)R_K}{2}.\end{aligned}$$

Für $f'(1)$ berechnet man

$$\begin{aligned}f'(x)|_{x=1} &= \left(\frac{x^m(x-p)^2}{x^2-p}\right)'\sum_{r=1}^{\mu_-}\sum_{i=0}^{\operatorname{grad} M^-_{r-1}-1}x^i\Bigg|_{x=1}+\sum_{r=1}^{\mu_-}\sum_{i=0}^{\operatorname{grad} M^-_{r-1}-1}(i+1)x^i\left(\frac{x^m(x-p)^2}{x^2-p}\right)\Bigg|_{x=1}\\ &= R_K\cdot\frac{(mx^{m-1}(x-p)^2+2(x-p)x^m)(x^2-p)-2x(x^m(x-p)^2)}{(x^2-p)^2}\Bigg|_{x=1}\\ &\quad+\sum_{r=1}^{\mu_-}\frac{(\operatorname{grad} M^-_{r-1}-1)\operatorname{grad} M^-_{r-1}}{2}(1-p)\\ &= m(1-p)+\frac{1-p}{2}\sum_{r=1}^{\mu_-}(\operatorname{grad} M^-_{r-1})^2+(p-1)\frac{R_K}{2}\\ &= (p-1)(\frac{R_K}{2}-mR_K-\frac{1}{2}\sum_{r=1}^{\mu_-}(\operatorname{grad} M^-_{r-1})^2).\end{aligned}$$

Setzen wir dies in die letzte Gleichung ein und formen nach $a_0(A)$ um, so gilt

$$\begin{aligned}a_0(A) &= \frac{p^{1-m}}{p-1}(P_0(1,A)-\mu_-)-\frac{p-1}{2p^m}(2(m-1)R_K+\sum_{r=1}^{\mu_-}(\operatorname{grad} M^-_{r-1})^2)\\ &= p^{1-m}\sum_{r=1}^{\mu_-}\frac{|M^-_{r-1}|-1}{p-1}-\frac{(p-1)}{2p^m}\left(2(m-1)R_K+\sum_{r=1}^{\mu_-}(\operatorname{grad} M^-_{r-1})^2\right).\end{aligned}$$

Da es sich bei $L_0(s,A)$ um eine rationale Funktion von $U=p^{-s}$ handelt, ist sie periodisch mit der Periode $\frac{2\pi i}{\log p}$, und somit sind mit $s=1$ auch alle $s=1+\frac{2\pi ik}{\log p}$ einfache Pole mit demselben Residuum wie an der Stelle $s=1$. Der Wert von

$L_0(s,A)$ an der Stelle $s=0$ ist gegeben durch den Wert von $F(U)$ an der Stelle $U=1$, und man sieht leicht, daß $F(1)=L_0(0,A)=0$ gilt.
$s=\frac{\pi i}{\log p}$ entspricht dem Wert $U=-1$, und es folgt

$$\begin{aligned}
L_0(\frac{\pi i}{\log p},A) &= \frac{(-1)^m}{(p+1)^2}\left((p-1)\mu_- + \frac{4p\sum_{r=1}^{\mu_-}(-p)^{\operatorname{grad} M_{r-1}^-}}{p-1} - \frac{(p+1)^2\sum_{r=1}^{\mu_-}(-1)^{\operatorname{grad} M_{r-1}^-}}{p-1}\right)\\
&= \frac{(-1)^m}{(p+1)^2}\left((p-1)\mu_- + \frac{4p\left(\sum_{r=1}^{\mu_-}(-p)^{\operatorname{grad} M_{r-1}^-} - (-1)^{\operatorname{grad} M_{r-1}^-}\right)}{p-1}\right.\\
&\quad \left. - \frac{(p-1)^2\sum_{r=1}^{\mu_-}(-1)^{\operatorname{grad} M_{r-1}^-}}{p-1}\right)\\
&= \frac{(-1)^m}{(p+1)^2}\left(4p\sum_{r=1}^{\mu_-}(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1} + (p-1)\sum_{r=1}^{\mu_-}\left(1-(-1)^{\operatorname{grad} M_{r-1}^-}\right)\right)\\
&= \frac{(-1)^m}{(p+1)^2}\left(4p\sum_{r=1}^{\mu_-}(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1} + 2W(p-1)\right)
\end{aligned}$$

mit

$$W := \#\{M_{r-1}^- \mid r\in\{1,\dots,\mu_-\},\ \operatorname{grad} M_{r-1}^- \text{ ungerade}\}.$$

□

Nun lassen sich die vorangegangenen Beobachtungen zu Feststellungen über die Zeta-Funktion $Z(s,A)$ einer engen Idealklasse zusammenfassen.

14.2.6 Satz

Es sei $A\in C^+(K)$ eine enge Idealklasse. Dann ist die Zetafunktion $Z(s,A)$ eine rationale Funktion in $U=p^{-s}$. Diese ist holomorph auf ganz $\mathbb{C}$ mit Ausnahme einfacher Pole an den Stellen $s=1+\frac{2\pi ik}{\log p}$ für $k\in\mathbb{Z}$ mit den Residuen

$$\operatorname{Res}(Z(s,A), s=1+\frac{2\pi ik}{\log p}) = \frac{(p-1)}{2\log p}\cdot\frac{R_K}{|\sqrt{D}|}.$$

Es sei $b_{-1}(K) := \operatorname{Res}(Z(s,A), s=1)$. Ist dann

$$Z(s,A) = \frac{b_{-1}(K)}{s-1} + b_0(A) + b_1(A)(s-1) + \dots$$

die Laurententwicklung von $Z(s,A)$ um $s=1$, so erhält man den Wert $b_0(A)$ durch

$$\begin{aligned}
b_0(A) &= \lim_{s\to 1}\left(Z(s,A) - \frac{b_{-1}(K)}{s-1}\right) = \frac{1}{2}(a_0(A)+L(1,A))\\
&= \frac{1}{2}p^{1-m}\left(\sum_{r=1}^{\mu_-}(1+\chi(M_{r-1}^-))\frac{|M_{r-1}^-|-1}{p-1}\right) - \frac{p-1}{4p^m}((2(m-1)R_K + \sum_{r=1}^{\mu_-}(\operatorname{grad} M_{r-1}^-)^2)
\end{aligned}$$

mit den Bezeichnungen aus Satz 14.2.5. Für die Zetafunktion $Z_K(s)$ gilt also

$$\lim_{s\to 1}(s-1)Z_K(s) = \frac{h^+(K)(p-1)R_K}{2\log p|\sqrt{D}|},$$

was die in 9.3.1 und 9.3.2 angeführten ARTINschen Aussagen für den reell-quadratischen Fall mit $Q_K = 2$ bestätigt.

BEWEIS:

Die Aussagen folgen aus Satz 14.2.5, 14.2.1 und den Darstellungen

$$Z(s, A_i) = \frac{1}{2}(L_0(s, A_i) + L(s, A_i)) \quad \text{bzw.} \quad Z_K(s) = \sum_{i=1}^{h^+(K)} Z(s, A_i)$$

mit den engen Idealklassen $A_i \in C^+(K)$ für $i = 1, \ldots, h^+(K)$. □

14.2.7 Bemerkung

In Analogie zum quadratischen Zahlkörperfall kann man die Formel für den Wert $b_0(A)$ zu einer engen Idealklasse A durchaus als KRONECKER-*Grenzformel* auffassen.
Erste Formeln dieser Art für den Fall eines imaginär-quadratischen Zahlkörpers findet man bei L. KRONECKER in [Kron].
Spezielle Formen und Anwendungen der KRONECKER-Grenzformeln in imaginär-quadratischen Zahlkörpern finden sich bei SIEGEL in [Sie1], S. 1-17 und ZAGIER in [Zag1], S. 156-160.
Im Jahre 1917 benutzte E. HECKE die Formeln von KRONECKER, um zu Ergebnissen im reell-quadratischen Zahlkörperfall zu kommen (s. [He]). Beschäftigten sich KRONECKER und HECKE ausschließlich mit der weiten Klasseneinteilung, so wandte MEYER in [Mey] zum ersten Mal die Methoden von HECKE auf die Zetafunktion einer engen Idealklasse an. Haben alle Einheiten positive Norm, so ist jede weite Idealklasse $\tilde{A}$ (wie auch im Funktionenkörperfall) die Vereinigung zweier enger Idealklassen A und ΘA, wobei Θ die enge Idealklasse aller Hauptideale (α) mit $N(\alpha) < 0$ ist. Es gilt dann $b_0(A) + b_0(\Theta A) = b_0(\tilde{A})$ für die Kronecker-Grenzwerte der Idealklassen.
MEYER berechnete die Differenz $b_0(A) - b_0(\Theta A)$. Bei dieser handelt es sich um den Wert der L-Funktion zur engen Idealklasse A an der Stelle 1. Daß sich diese Differenz im reell-quadratischen Zahlkörperfall mit Hilfe der negativen Kettenbruchentwicklung eines reduzierten Elements ausdrücken läßt, stellte ZAGIER fest und führte dies in [Zag1] aus.
Dies entspricht genau den Ergebnissen, welche im Fall $Q_K = 2$ aus 14.2.6 und 14.2.3 für den Funktionenkörperfall folgen. Es gilt nämlich

$$L(1, A) = b_0(A) - b_0(uA) = p^{1-m} \sum_{r=1}^{\mu^-} \frac{|M_{r-1}^-| - 1}{p - 1}$$

in den Bezeichnungen von 14.2.3 und 14.2.4.
D.h. auch hier läßt sich die Differenz $b_0(A) - b_0(uA)$ mit Hilfe der Partialbrüche der negativen KBE eines reduzierten Elements ausdrücken.
Erste KRONECKERsche Grenzformeln für weite Idealklassen in reell-quadratischen Funktionenkörpern findet man (allerdings ohne Beweis) in [Gz], S. 58.
Wie wir im nächsten Kapitel sehen werden, spielen sowohl die Kronecker-Grenzwerte $b_0(A)$ als auch die Differenzen $b_0(A) - b_0(uA)$ zu $A \in C^+(K)$ eine große Rolle bei der Berechnung des Produkts der Klassenzahlen zweier quadratischer Funktionenkörper.

15 Klassenzahl-Produktformeln mit negativer Kettenbruchentwicklung

15.1 Der allgemeine Fall

Da wir die Werte der L-Funktionen zu den engen Idealklassen an den Stellen $s = 0$ und $s = \frac{\pi i}{\log p}$ bestimmt haben, können wir die Produkte der Klassenzahlen imaginär- und reell-quadratischer Funktionenkörper der Fälle 12.3.3 (1)-(4) anhand der negativen KBE der Quotienten aus Basiselementen geeigneter Vertreter der engen Idealklassen bestimmen.

Dazu sei $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper, $h^+(K)$ seine enge Klassenzahl und $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_{h^+(K)}\}$ ein Vertretersystem der Idealklassen aus ganzen reduzierten Idealen von K. Es seien $\mathfrak{a}_i =< \omega_1^{(i)}, \omega_2^{(i)} >$ so gewählt, daß die Basen $(\omega_1^{(i)}, \omega_2^{(i)})$ orientiert und die Quotienten $Z^{(i)} := \frac{\omega_2^{(i)}}{\omega_1^{(i)}} \in F(D)$ reduziert sind.

Betrachten wir nun eine der engen Idealklassen $A_i \in C^+(k(\sqrt{D}))$ und den zugehörigen reduzierten Vertreter $Z^{(i)} \in F(D)$, so läßt sich – da wir $Q_K = 2$ voraussetzen wollen – ein Vertreter der Klasse uA_i leicht bestimmen.

15.1.1 Lemma

Es sei $Q_K = 2$ und $Z^{(i)} \in F(D)$ ein wie oben bestimmter reduzierter Vertreter der engen Idealklasse A_i.
Dann ist

$$\tilde{Z}^{(i)} := \begin{cases} gZ^{(i)}, & \text{falls } \operatorname{sgn} Z^{(i)} = 1, \\ g^{-1}Z^{(i)}, & \text{falls } \operatorname{sgn} Z^{(i)} = g \end{cases} \in F(D)$$

ein reduzierter Vertreter der Klasse uA_i.

Weiterhin gilt

$$\mu_-(Z^{(i)}) = \mu_-(\tilde{Z}^{(i)}), \quad \operatorname{grad} M_{r-1}^{(i)^-} = \operatorname{grad} \tilde{M}_{r-1}^{(i)^-} \quad \text{und} \quad \chi(M_{r-1}^{(i)^-}) = -\chi(\tilde{M}_{r-1}^{(i)^-}) \ \ (r \geq 1)$$

für die Partialbrüche $M_{r-1}^{(i)^-}$ und $\tilde{M}_{r-1}^{(i)^-}$ der negativen KBE von $Z^{(i)}$ und $\tilde{Z}^{(i)}$.

BEWEIS:

Zunächst stellt man fest, daß $Z^{(i)} \sim \tilde{Z}^{(i)}$ gilt.
Besitzt $Z^{(i)} \in F(D)$ die Darstellung $Z^{(i)} = \frac{B+\sqrt{D}}{2C}$ mit der über die Funktion Ψ in 8.6.3 zugeordneten Idealklasse $[u^j < 2C, B + \sqrt{D} >]$, so wird dem Element $\tilde{Z}^{(i)}$ die Idealklasse $[u^{1-j} < 2Cg^{-1}, B + \sqrt{D} >]$ mit $j \in \{0, 1\}$ zugeordnet, je nachdem, ob die zustandekommenden Basen orientiert sind oder nicht.
Dies zeigt, daß $\tilde{Z}^{(i)}$ einen Vertreter von uA_i bildet, falls $Z^{(i)}$ ein Vertreter der Klasse A_i ist.
Die Gleichungen $\chi(M_{r-1}^{(i)^-}) = -\chi(\tilde{M}_{r-1}^{(i)^-})$ und $\operatorname{grad} M_{r-1}^{(i)^-} = \operatorname{grad} \tilde{M}_{r-1}^{(i)^-}$ erhält man sofort aus Satz 5.4.6 mit $b = g$, und die Identität $\mu_-(Z^{(i)}) = \mu_-(\tilde{Z}^{(i)})$ folgt aus Korollar 5.4.7. □

Die Produktformeln aus Satz 12.3.3 (1)-(4) erhalten somit die folgende Form:

15.1.2 Satz

Es sei $K = k(\sqrt{D})$ ein reell-quadratischer Funktionenkörper mit $Q_K = 2$, und $Z^{(i)}$ für $i \in \{1, \dots, h^+(K)\}$ wie zu Beginn des Kapitels gewählt. Dann gilt:

(1) Ist $D = D_1 D_2$ mit $D_1 \neq 1 \neq D_2$ eine Zerlegung von D in zwei normierte Polynome von geradem Grad und $\tilde{\psi}$ der nach 11.3.2 zu dieser Zerlegung gehörige Geschlechtscharakter, so gilt für das Produkt der Klassenzahlen der imaginär-quadratischen Körper

$$h(gD_1)h(gD_2) = \frac{(-1)^m}{(p+1)^2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) \left(2p \sum_{r=1}^{\mu_-(Z^{(i)})} (-1)^{\operatorname{grad} M_{r-1}^{(i)-}} \frac{|M_{r-1}^{(i)-}| - 1}{p-1} + W(p-1) \right)$$

mit

$$W := \#\{M_{r-1}^- \mid r \in \{1, \dots, \mu_-\},\ \operatorname{grad} M_{r-1}^- \text{ ungerade}\}$$

und $m := \frac{\operatorname{grad} D}{2}$.

Für den Körper $k(\sqrt{gD})$ gilt

$$h(gD) = \frac{(-1)^m}{p+1} \sum_{i=1}^{h^+(K)} \left(2p \sum_{r=1}^{\mu_-(Z^{(i)})} (-1)^{\operatorname{grad} M_{r-1}^{(i)-}} \frac{|M_{r-1}^{(i)-}| - 1}{p-1} + W(p-1) \right).$$

(2) Ist $D = D_1 D_2$ eine Zerlegung von D in zwei normierte Polynome ungeraden Grades mit zugehörigem Charakter $\tilde{\psi}$, so gilt

$$h(gD_1)h(gD_2) = \frac{1}{2}(-\chi(-1))^m \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) \sum_{r=1}^{\mu_-(Z^{(i)})} \chi(M_{r-1}^{(i)-})(-\chi(-1))^{\operatorname{grad} M_{r-1}^{(i)-}} \frac{|M_{r-1}^{(i)-}| - 1}{p-1},$$

wobei alle Bezeichnungen wie in (1) gewählt seien.

(3) Unter den Voraussetzungen von Punkt (2) gilt

$$h(D_1)h(D_2) = \frac{1}{2}(\chi(-1))^m \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) \sum_{r=1}^{\mu_-(Z^{(i)})} \chi(M_{r-1}^{(i)-})(\chi(-1))^{\operatorname{grad} M_{r-1}^{(i)-}} \frac{|M_{r-1}^{(i)-}| - 1}{p-1}.$$

(4) Für das Produkt der Klassenzahlen der reell-quadratischen Körper gilt

$$\begin{aligned} h(D_1)h(D_2) \;=\; & \frac{1}{2(p-1)^2 R_1 R_2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) \left(p \sum_{r=1}^{\mu_-(Z^{(i)})} (1 + \chi(M_{r-1}^{(i)-})) \frac{|M_{r-1}^{(i)-}| - 1}{p-1} \right. \\ & \left. - \frac{(p-1)}{2} \left(2(m-1)R_K + \sum_{r=1}^{\mu_-(Z^{(i)})} (\operatorname{grad} M_{r-1}^{(i)-})^2 \right) \right), \end{aligned}$$

wobei R_i die Regulatoren von $k(\sqrt{D_i})$ sind und R_K derjenige von K.

BEWEIS:

(1) Nach Satz 12.3.3 (1) gilt für den Fall $D = D_1D_2$ mit $D_1 \neq 1 \neq D_2$ die Identität

$$h(gD_1)h(gD_2) = L_{\tilde{\psi}}(\frac{\pi i}{\log p}).$$

Ist $Q_K = 2$, so ist

$$L_{\tilde{\psi}}(\frac{\pi i}{\log p}) = \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) Z(\frac{\pi i}{\log p}, A_i) = \frac{1}{2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i)(Z(s, A_i) + Z(s, uA_i)),$$

nach Definition 11.2.1, da es sich bei $\tilde{\psi}$ wegen Lemma 11.3.3 lediglich um einen Geschlechtscharakter der weiten Idealklassen handelt.
Setzt man

$$Z(s, A_i) = \frac{1}{2}(L_0(s, A_i) + L(s, A_i))$$

in diese Formel ein, so erhält man

$$L_{\tilde{\psi}}(\frac{\pi i}{\log p}) = \frac{1}{4} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i)(L_0(s, A_i) + L_0(s, uA_i) + L(s, A_i) + L(s, uA_i)).$$

Aus Folgerung 14.2.4 und Lemma 15.1.1 folgt

$$L(\frac{\pi i}{\log p}, A_i) = (-1)^m \left(\sum_{r=1}^{\mu_-(Z^{(i)})} \chi(M_{r-1}^{(i)-})(-1)^{\operatorname{grad} M_{r-1}^{(i)-}} \frac{|M_{r-1}^{(i)-}| - 1}{p-1} \right) = -L(\frac{\pi i}{\log p}, uA_i)$$

und $L_0(\frac{\pi i}{\log p}, A_i) = L_0(\frac{\pi i}{\log p}, uA_i)$.
Es ist also

$$L_{\tilde{\psi}}(\frac{\pi i}{\log p}) = \frac{1}{2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) L_0(\frac{\pi i}{\log p}, A_i),$$

und aus der Formel für $L_0(\frac{\pi i}{\log p}, A)$ aus Satz 14.2.5 folgt die Behauptung.

Die Formel für $h(gD)$ erhält man auch in diesem Fall analog, indem man $\tilde{\psi}$ durch den trivialen Charakter ersetzt und die Gleichung

$$h(gD) = (p+1) L_{\tilde{\psi}}(\frac{\pi i}{\log p})$$

aus Satz 12.3.3 (1) benutzt.

(2) Nach Lemma 11.3.3 handelt es sich bei $\tilde{\psi}$ in diesem Fall um einen echten Geschlechtscharakter von $C^+(K)$, der wegen 11.2.1 die Darstellung

$$L_{\tilde{\psi}}(s) = \frac{1}{2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) L(s, A_i)$$

zuläßt. Für $\chi(-1) = -1$ folgt dann aus 12.3.3 (2) die Identität

$$\begin{aligned} h(gD_1)h(gD_2) &= \frac{1}{2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) L(0, A_i) \\ &\overset{14.2.4}{=} \frac{1}{2} \sum_{i=1}^{h^+(K)} \tilde{\psi}(\mathfrak{a}_i) \sum_{r=1}^{\mu_-(Z^{(i)})} \chi(M_{r-1}^{(i)-}) \frac{|M_{r-1}^{(i)-}| - 1}{p-1}. \end{aligned}$$

Für $\chi(-1)=1$ ist analog zum Beweis von (1)

$$\begin{aligned} h(gD_1)h(gD_2) &= \frac{1}{2}\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)L(\frac{\pi i}{\log p},A_i) \\ &\overset{14.2.4}{=} \frac{1}{2}(-1)^m\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)\sum_{r=1}^{\mu_-(Z^{(i)})}\chi(M_{r-1}^{(i)-})(-1)^{\operatorname{grad} M_{r-1}^{(i)-}}\frac{|M_{r-1}^{(i)-}|-1}{p-1}, \end{aligned}$$

und das war die Behauptung.

(3) Der Beweis dieser Aussage verläuft vollständig analog zu Punkt (2).

(4) Nach Satz 12.3.3 (4) ist

$$h(D_1)h(D_2)=\frac{p^m}{(p-1)^2R_1R_2}L_{\tilde{\psi}}(1)$$

mit den Regulatoren R_i der Körper $k(\sqrt{D_i})$ und der L-Funktion zum nichttrivialen Geschlechtscharakter $\tilde{\psi}$, welche man in der Form

$$L_{\tilde{\psi}}(s)=\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)Z(s,A_i)$$

schreiben kann. Da das Residuum von $Z(s,A_i)$ in $s=1$, wie wir in 14.2.6 zeigten, nicht von der engen Idealklasse A_i abhängt und $\tilde{\psi}$ nicht der triviale Charakter ist, gilt

$$\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)\frac{b_{-1}(K)}{s-1}=\frac{b_{-1}(K)}{s-1}\underbrace{\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)}_{=0}=0$$

mit den Bezeichnungen des Satzes 14.2.6. Wir können demnach folgern

$$\begin{aligned} \lim_{s\to 1}L_{\tilde{\psi}}(s) &= \lim_{s\to 1}\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)\left(Z(s,A_i)-\frac{b_{-1}(K)}{s-1}\right) \\ &\overset{14.2.6}{=} \sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)b_0(A_i), \end{aligned}$$

also

$$h(D_1)h(D_2)=\frac{p^m}{(p-1)^2R_1R_2}\sum_{i=1}^{h^+(K)}\tilde{\psi}(\mathfrak{a}_i)b_0(A_i),$$

woraus nach Einsetzen der Formel für $b_0(A_i)$ aus 14.2.6 die Behauptung folgt. □

15.2 Der Fall $h(K)=1$

Gilt zusätzlich zu den Voraussetzungen des Satzes 15.1.2 noch $h(K)=1$, so sind wir in der Lage, einen festen Vertreter der Klasse $\mathcal{O}_K=(1)=<\omega_1,\omega_2>$ zu wählen und anhand der

negativen KBE des Basisquotienten das Produkt der Klassenzahlen der gewünschten Körper zu berechnen.

Hierzu sei $\mathcal{O}_K$ in der Basisdarstellung $\mathcal{O}_K =< 2, \sqrt{D} + [\sqrt{D}] >$ gewählt. Wie man leicht sieht, handelt es sich hierbei um eine orientierte Basis von $\mathcal{O}_K$ mit dem Basisquotienten $Z := \frac{\sqrt{D}+[\sqrt{D}]}{2}$, der wegen $\operatorname{sgn}\sqrt{D} = 1$ und $|Z| > 1 > |\overline{Z}|$ reduziert ist.

Mit der negativen KBE dieses Elements lassen sich nun die Produkte der oben beschriebenen Klassenzahlen explizit berechnen.

Hierbei ist jedoch zu bemerken, daß aus der Tabelle 4 auf S. 71 folgt, daß die weite Klassenzahl des reell-quadratischen Körpers nur dann ungerade sein kann, wenn D ein Produkt zweier Primpolynome ungeraden Grades oder D selbst eine Primfunktion geraden Grades ist.
Aufgrund der Voraussetzung $h(K) = 1$ kann es also keine nicht-triviale Zerlegung $D = D_1 D_2$ von D in zwei Polynome $D_1, D_2 \in \mathbb{F}_p[X]$ mit $\operatorname{grad} D_i \equiv 0\ (2)$ geben.
Außerdem kann der Fall $h(K) = 1$ in Zusammenhang mit $Q_K = 2$ nur dann auftreten, wenn D ein Produkt zweier Primfunktionen $P_1 P_2$ mit $\operatorname{grad} P_1 \equiv \operatorname{grad} P_2 \equiv 1\ (2)$ ist, denn für D prim und von geradem Grad gilt $Q_K = 1$ nach [A], S. 198. Die Aussagen des Satzes 15.1.2 (1) mit $D_1 \neq 1 \neq D_2$ und (4) sind demnach unter der Voraussetzung $h(K) = 1$ leer, brauchen also hier nicht betrachtet zu werden.

15.2.1 Satz

Es sei D ein quadratfreies normiertes Polynom mit $\operatorname{grad} D$ gerade, und es gelte $h(K) = 1$ für die weite Klassenzahl des Körpers $K = k(\sqrt{D})$. Ferner sei $Q_K = 2$ und $Z := \frac{[\sqrt{D}]+\sqrt{D}}{2}$. Sind M_r^- für $r \geq 0$ die Partialbrüche der negativen KBE von Z und $\mu_-(Z)$ die Quadratperiode, so gilt:

(1) Die Klassenzahl des imaginär-quadratischen Körpers $k(\sqrt{gD})$ erhält man in der Form

$$h(gD) = \frac{(-1)^m}{p+1}\left(4p\sum_{r=1}^{\mu_-(Z)}(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1} + 2W(p-1)\right)$$

mit

$$W := \#\{M_{r-1}^- \mid r \in \{1,\ldots,\mu_-(Z)\},\ \operatorname{grad} M_{r-1}^- \text{ ungerade}\}$$

und $m := \frac{\operatorname{grad} D}{2}$.

(2) Ist $D = D_1 D_2$ eine Zerlegung von D in zwei normierte Polynome ungeraden Grades, so gilt $h^+(D) = 2$, und es ist

$$h(gD_1)h(gD_2) = (-\chi(-1))^m \sum_{r=1}^{\mu_-(Z)}\chi(M_{r-1}^-)(-\chi(-1))^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1},$$

wobei alle Bezeichnungen wie in (1) gewählt seien.

(3) Unter den Voraussetzungen von Punkt (2) gilt

$$h(D_1)h(D_2) = (\chi(-1))^m \sum_{r=1}^{\mu_-(Z)}\chi(M_{r-1}^-)(\chi(-1))^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1}.$$

BEWEIS:

(1) Man erhält

$$h(gD) = \frac{(-1)^m}{p+1}\left(4p\sum_{r=1}^{\mu_-(Z)}(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1} + 2W(p-1)\right)$$

mit

$$W := \#\{M_{r-1}^- \mid r \in \{1,\dots,\mu_-(Z)\},\ \operatorname{grad} M_{r-1}^- \text{ ungerade}\}$$

direkt aus Satz 15.1.2 (1).

(2) In diesem Fall kann D nur ein Produkt zweier Primpolynome ungeraden Grades sein. Ist $\chi(-1) = -1$, so gilt mit Satz 15.1.2 (2) und Lemma 15.1.1

$$h(gD_1)h(gD_2) = \sum_{r=1}^{\mu_-(Z)}\chi(M_{r-1}^-)\frac{|M_{r-1}^-|-1}{p-1}.$$

Ist hingegen $\chi(-1) = 1$, so ist mit derselben Begründung

$$h(gD_1)h(gD_2) = (-1)^m\sum_{r=1}^{\mu_-(Z)}\chi(M_{r-1}^-)(-1)^{\operatorname{grad} M_{r-1}^-}\frac{|M_{r-1}^-|-1}{p-1}.$$

(3) Der Beweis verläuft analog zu den Ausführungen in (2).

□

15.2.2 Bemerkung

An dieser Stelle ist zu bemerken, daß sich die von HAYES bewiesenen Theoreme 8.9 und 8.14 aus [H1], S.232f. hier sofort aus 15.2.1 (1)-(3) folgern lassen.
Für die Formel von HAYES sind in 15.2.1 (1) die Quadratperiode der negativen KBE-Art durch die Quasiperiode der Standard-KBE-Art, und die Partialbrüche M_{r-1}^- der negativen KBE von Z durch die Partialbrüche der Standard-KBE von $2Z$ zu ersetzen. Dies führt auf die selben Werte, wenn man ausnutzt, daß sich wegen Satz 5.4.3 weder durch Multiplikation von Z mit einem Faktor aus $\mathbb{F}_p^*$ noch durch Verwendung einer anderen KBE-Art an den Graden der Partialbrüche etwas ändert.
Weiterhin gilt auch

$$\nu(2Z) \overset{5.4.4}{=} \nu(Z) = \mu_*(Z) \overset{6.2.2}{=} \mu_-(Z) \overset{5.4.7}{=} \mu_-(2Z),$$

denn wäre $\nu(Z) \neq \mu_*(Z)$, so wäre $\frac{Z_\nu^*}{Z} = g^{\pm 1}$ nach Korollar 5.4.9 (ii), denn Z und Z_ν^* sind reduziert. Das würde aber $Z \sim_+ Z_\nu^* = \tilde{Z}$ mit $\tilde{Z}$ aus 15.1.1 bedeuten, was wegen $Q_K = 2$ nicht sein kann, denn dann würden die Klassen $\mathcal{O}_K$ und $u\mathcal{O}_K$ zusammenfallen.
Mit denselben Begründungen erhält man Theorem 8.14 von HAYES im Fall $\chi(-1) = -1$ aus 15.2.1 (2) und im Fall $\chi(-1) = 1$ aus (3), wenn man bemerkt, daß der Wert $\chi((-1)^{r-1}A_r^S)$ bei HAYES dem Wert $\chi(M_{r-1}^-)$ nach Folgerung 5.1.4 entspricht. Der Faktor $\chi(2)$ bei HAYES entspringt nach 5.4.6 aus der Verwendung von $2Z$ statt Z für die Standard-KBE-Art anstelle der negativen KBE-Art.

16 Beispiele

16.1 Der Fall $h(K) = 1$

Wir wollen zusätzlich zu den Beispielen von HAYES (s. [H1], S.234f.) die in Kapitel 16 hergeleiteten Formeln noch an allgemeineren Fällen verifizieren.

(a) Es sei $p = 3$ und $P(X) = X^3 - X - 1 \in \mathbb{F}_3[X]$. Dann können wir $g = 2 = -1$ wählen, und es gilt $h(XP) = 1$, $h(P) = 1$ nach [A], S. 232/233 und $h(gP) = h(-P) = 7$ wegen $h(D) + h(gD) = 2(p+1)$ für kubische $D \in \mathbb{F}_p[X]$ (s. [A], S. 230).

Wir wollen diese Ergebnisse anhand der negativen KBE des Elements $Z = (\sqrt{D} + [\sqrt{D}])/2$ verifizieren. Man berechnet zunächst $[\sqrt{D}] = X^2 + 1$ und dann

$$Z = \frac{X^2 + 1 + \sqrt{D}}{2} = [\overline{X^2 + 1, X + 2, X, X + 2}]^-.$$

Die Periode, und somit auch die Quadratperiode der negative KBE ist also $\rho_- = \mu_- = 4$. Da XP zwei Primfaktoren ungeraden Grades besitzt, gilt $Q_K = 2$, also $h^+(XP) = 2$. Es gibt somit zwei enge Idealklassen $\mathcal{O}_K$ und $u\mathcal{O}_K$ und zwei Geschlechtscharaktere: den trivialen und den zu XP gehörigen echten Geschlechtscharakter ψ mit $\psi(\mathcal{O}_K) = 1$ und $\psi(u\mathcal{O}_K) = -1$.

Wir erhalten wegen $\chi(-1) = -1$ die Formeln

$$h(-X)h(-P) \overset{h(-X)=1}{=} h(-P) = \sum_{r=1}^{4} \chi(M_{r-1}^-) \frac{|M_{r-1}^-| - 1}{2} = 4 + 1 + 1 + 1 = 7$$

und

$$h(X)h(P) = h(P) = (-1)^2 \sum_{r=1}^{4} \chi(M_{r-1}^-)(-1)^{\operatorname{grad} M_{r-1}^-} \frac{|M_{r-1}^-| - 1}{2} = (4 - 1 - 1 - 1) = 1.$$

Dies bestätigt unsere Aussagen 15.2.1 (2) und (3).

Natürlich läßt sich auch die Klassenzahl $h(-XP)$ berechnen, welche nach [A], S. 233 den Wert 6 haben muß.

In 15.2.1 (1) gilt $W = 3$, und somit

$$h(-XP) = \frac{(-1)^2}{4} \left(12 \sum_{r=1}^{4} (-1)^{\operatorname{grad} M_{r-1}^-} \frac{|M_{r-1}^-| - 1}{2} + 12 \right) = \frac{1}{4}(12(4-1-1-1)+12) = 6.$$

(b) Das Beispiel unter (a) wurde von D. R. HAYES schon mit Formeln verifiziert, in denen die Standard-KBE des Elements $\sqrt{D} + [\sqrt{D}]$ benutzt wurde. Er berechnete die Ausdrücke lediglich für Primfunktionen geraden Grades – hier gilt jedoch immer $Q_K = 1$ – und für $D = XP$ mit einem Primpolynom P ungeraden Grades.

Basierend auf den Ausführungen in [A] implementierten B. WEIS (s. [W],[WZ]) und A. STEIN (s. [St1]) für das Computer - Algebra - System SIMATH Algorithmen zur Berechnung der Grundeinheit, des Regulators und der Klassenzahl eines reell-quadratischen Funktionenkörpers.

Tabellen, welche auf diesen Berechnungen beruhen, findet man in [WZ], S. 275ff.

Diese basieren sämtlich auf der Standard-KBE Artin-reduzierter Elemente, lassen sich jedoch unter Zuhilfenahme des Lemmas 5.1.3 auf beliebige KBE-Arten umschreiben, so daß es möglich wird, die verschiedenen Perioden der engen oder negativen KBE reduzierter Elemente und deren Partialbrüche zu berechnen.

Von der Vielzahl an Beispielen mit $h(D) = 1$ und $Q_K = 2$, in denen die Funktion D in 15.2.1 (2) nicht durch X teilbar ist, sei hier eines herausgegriffen.

Für $p = 3$ seien $P_1(X) := X^3 + 2X^2 + 2X + 2$ und $P_2(X) := X^3 + X^2 + 2X + 1 \in \mathbb{F}_3[X]$. Wir betrachten das Polynom $D = P_1 P_2$ vom Grad 6.

Der reell-quadratische Körper $K := k(\sqrt{D})$ hat nach [WZ], S.281 die Klassenzahl $h(K) = 1$. Nach [A], S.232 gilt $h(P_1) = 5$ und $h(P_2) = 3$.

Unter Zuhilfenahme von an die negative KBE angepaßten Algorithmen berechnet man die negative KBE des Elements $Z_0^- = Z := \frac{1}{2}(\sqrt{D} + [\sqrt{D}])$.

Man erhält

r	1	2	3	4
Z_{r-1}^-	$\frac{1}{2}(\sqrt{D} + X^3)$	$\frac{\sqrt{D}+X^3}{2X^2+2}$	$\frac{\sqrt{D}+X^3+2X}{2X^2+2}$	$\frac{1}{2}(\sqrt{D} + X^3) = Z_0^-$
M_{r-1}^-	X^3	X	X	X^3

Es ist also $Z = [\overline{X^3, X, X}]^-$ mit $\mu_-(Z) = \rho_-(Z) = \nu(Z) = 3$.

Wegen $p = 3$ ist $\chi(-1) = -1$, und wir stellen mit Satz 15.2.1 (3) fest, daß

$$(-1)^3 \sum_{r=1}^{3} \chi(M_{r-1}^-)(-1)^{\operatorname{grad} M_{r-1}^-} \frac{|M_{r-1}^-| - 1}{p-1} = -(1 \cdot (-1)\frac{27-1}{3-1} + (-1) + (-1)) = -(-15) = 15$$

gilt, womit die Formel an diesem Beispiel verifiziert wurde.

16.2 Der Fall $h(K) > 1$

Zwei letzte Beispiele seien dem mehrklassigen mehrgeschlechtigen Fall gewidmet, der unsere besondere Aufmerksamkeit bekommen soll, da es hier nötig wird, die Werte der Geschlechtscharaktere für die verschiedenen Idealklassen auszurechnen.

16.2.1 Der Fall $\#G^+(K) = 2$

Es sei $p = 3$ und

$$D(X) = X^6 + X^4 + X^2 + 2 = (X^3 + 2X + 2)(X^3 + 2X + 1) = D_1 D_2 \in \mathbb{F}_3[X]$$

mit $h(D_1 D_2) = 3$ (s. [WZ], S.282), $h(D_1) = 1$ und $h(D_2) = 7$ (s. [A], S.232).
Mit Hilfe der Implementierungen von B. Weis kann man nun, da es drei weite Idealklassen gibt, Vertreter $\mathfrak{a}_1, \mathfrak{a}_2$ und $\mathfrak{a}_3$ in Form von ganzen Idealen mit orientierten Basen berechnen,

deren zugehörige Basisquotienten reduziert sind. Da D zwei Primfaktoren ungeraden Grades enthält, gilt $Q_K = 2$, also $h^+(K) = 6$.
Es gibt also genau einen nicht-trivialen Geschlechtscharakter ψ, nämlich denjenigen, der zu der Zerlegung $D = D_1 D_2$ gehört. Bei diesem handelt es sich nach Lemma 11.3.3 um einen echten Geschlechtscharakter von $C^+(K)$. Auch die Werte $\psi(A_i)$ für $i = 1, 2, 3$ lassen sich nach 11.3.2 mit der Norm der Idealvertreter einfach berechnen.
Es ist

Klasse	$A_1 = \mathcal{O}_K$	A_2	A_3
Vertreter	$< 2, X^3 + 2X + \sqrt{D} >$	$< 2(X^2+1), X^3 + X + 1 + \sqrt{D} >$	$< 2(X^2 + X + 2), X^3 + X + \sqrt{D} >$
$\psi(A_i) =$	1	$\left[\frac{X^3+2X+2}{X^2+1}\right] = -1$	$\left[\frac{X^3+2X+2}{X^2+X+2}\right] = -1$

Wir haben demnach nur noch die negative KBE der Elemente

$$Z^{(1)} := \frac{1}{2}(X^3 + 2X + \sqrt{D}), \quad Z^{(2)} := \frac{1}{2}\frac{X^3 + X + \sqrt{D}}{X^2 + 1} \text{ und } \quad Z^{(3)} := \frac{1}{2}\frac{X^3 + X + \sqrt{D}}{X^2 + X + 2}$$

zu berechnen. Man erhält

$$\begin{aligned} Z^{(1)} &= [\overline{X^3 + 2X}]^-, \\ Z^{(2)} &= [\overline{X, X+2, X+1}]^- \text{ und} \\ Z^{(3)} &= [\overline{X+2, X, X+1}]^-, \end{aligned}$$

also $\mu_-(Z^{(1)}) = \rho_-(Z^{(1)}) = 1$ und $\mu_-(Z^{(2)}) = \mu_-(Z^{(3)}) = 3$.
Es seien nun $A^+_{2i-1} := A_{2i-1}$ und $A^+_{2i} := uA_{2i-1}$ für $i = 1, 2, 3$ die Elemente von $C^+(K)$. Da $\tilde{Z}^{(i)} := gZ^{(i)}$ nach 15.1.1 ein Vertreter von A^+_{2i} ist und somit

$$\sum_{r=1}^{\mu_-(Z^{(i)})} \chi(M^{(i)\,-}_{r-1})(-1)^{\operatorname{grad} M^{(i)}_{r-1}} \frac{|M^{(i)\,-}_{r-1}| - 1}{p-1} = -\sum_{r=1}^{\mu_-(\tilde{Z}^{(i)})} \chi(\tilde{M}^{(i)\,-}_{r-1})(-1)^{\operatorname{grad} \tilde{M}^{(i)}_{r-1}} \frac{|\tilde{M}^{(i)\,-}_{r-1}| - 1}{p-1}$$

gilt, haben wir nach 15.1.2 (3) wegen $\psi(A_i^+) = -\psi(uA_i^+)$ die Identität

$$\begin{aligned} h(D_1)h(D_2) &= \frac{1}{2}(-1)^3 \sum_{i=1}^{3} 2 \left(\chi(M_0^{(1)\,-})(-1)^{\operatorname{grad} M_0^{(1)}} \frac{|M_0^{(1)}| - 1}{p-1} \right. \\ &\quad - \sum_{r=1}^{3} \chi(M^{(2)\,-}_{r-1})(-1)^{\operatorname{grad} M^{(2)}_{r-1}} \frac{|M^{(2)\,-}_{r-1}| - 1}{p-1} \\ &\quad \left. - \sum_{r=1}^{3} \chi(M^{(3)\,-}_{r-1})(-1)^{\operatorname{grad} M^{(3)}_{r-1}} \frac{|M^{(3)\,-}_{r-1}| - 1}{p-1} \right) \\ &= -(-13 - \sum_{r=1}^{3}(-1) - \sum_{r=1}^{3}(-1)) = 7, \end{aligned}$$

was unsere Aussagen bestätigt.
Zuletzt möchten wir noch ein Beispiel anführen, in welchem nicht nur echte Geschlechtscharaktere zu berechnen sind.

16.2.2 Der Fall $\#G(K) = 4$

Als Beispiel für eine nicht-triviale Zerlegung der Art 15.1.2 (1) sei $p = 11$ und

$$D(X) := X^4 + 10X + 8 = (X+9)(X+5)(X^2+8X+8) = P_1P_2P_3 \in \mathbb{F}_{11}[X].$$

Wieder kann $g = -1$ gewählt werden.
Man berechnet $h(D) = 2$ und $h^+(D) = 4$, da D zwei Linearfaktoren enthält. Nach Folgerung 10.2.1 sind sämtliche engen Klassen ambig, es gibt somit vier Geschlechtscharaktere und unter ihnen nach 11.3.3 zwei echte. Diese sind genau diejenigen, welche zu den Zerlegungen $P_1(P_2P_3)$ und $P_2(P_1P_3)$ gehören. Sie seien mit ψ_{13} und ψ_{23} bezeichnet. Weiterhin seien ψ_0 der triviale und ψ_1 der zur Zerlegung $(P_1P_2)P_3$ gehörige Charakter. Ist $u \in \mathcal{O}_K$ ein Element mit $\chi(N(u)) = -1$, z.B. $u := \sqrt{D}$, so berechnet man

Klassen	A_1	A_2	A_3	A_4
Vertreter	$\mathfrak{a} =< 2, X^2 + \sqrt{D} >$	$(u)\mathfrak{a}$	$\mathfrak{b} =< 2(X+8), X^2 + 10 + \sqrt{D} >$	$(u)\mathfrak{b}$
$\psi_1(A_i)$	1	1	-1	-1
$\psi_{13}(A_i)$	1	-1	1	-1
$\psi_{23}(A_i)$	1	-1	-1	1

Für die reduzierten Basisquotienten $Z^{(1)} := \frac{X^2+\sqrt{D}}{2}$ und $Z^{(2)} := \frac{X^2+10+\sqrt{D}}{2X+5}$ von $\mathfrak{a}$ und $\mathfrak{b}$ gilt

$$Z^{(1)} = \overline{[X^2, 4X+10, 7X+5, 2X+1, 7X+5, 4X+10]}^-,$$

also $\mu_-(Z^{(1)}) = \rho_-(Z^{(1)}) = 6$, und

$$Z^{(2)} = [\underbrace{X+3, 7X+8, 3X+4, 9X+7, 3X+4, 7X+8, X+3}_{\mu_-(Z^{(2)})=7}, ...]^-,$$

denn es ist $Z_7^{(2)\,-} = 5Z^{(2)}$ und $5 = 4^2 \in \mathbb{F}_{11}^{*2}$.
Nach [A], S.230 ist $h(gP_1P_2)h(gP_3) = 4$. Dies wollen wir nun mit der Formel 15.1.2 (1) für diese Zerlegung verifizieren. Wir benutzen dazu den Charakter ψ_1, dessen Werte wir für die Idealklassen schon bestimmt haben, und erhalten wieder unter Anwendung von 15.1.1 die Gleichung

$$\begin{aligned} h(gP_1P_2)h(gP_3) &= \frac{1}{12^2}\left(4 \cdot 11 \cdot \sum_{r=1}^{6}(-1)^{\operatorname{grad} M_{r-1}^{(1)}} \frac{|M_{r-1}^{(2)\,-}| - 1}{11-1} + 2 \cdot 5(11-1)\right. \\ &\quad \left. -4 \cdot 11 \sum_{r=1}^{7}(-1)^{\operatorname{grad} M_{r-1}^{(2)}} \frac{|M_{r-1}^{(2)\,-}| - 1}{11-1} + 2 \cdot 7(11-1)\right) \\ &= \frac{1}{12^2}\left((44 \cdot (12-5) + 100) - (44 \cdot (-7) + 140)\right) = \frac{576}{144} = 4. \end{aligned}$$

Bei diesem Beispiel findet auch die Formel 15.1.2 (4) Anwendung.
Nach [A] gilt $h(D) = 1$ für quadratische D, d.h. $h(P_1P_2)h(P_3) = 1$. Für die Regulatoren R_1 und R_2 der Körper $k(\sqrt{P_1P_2})$ und $k(\sqrt{P_3})$ gilt ebenfalls $R_1 = R_2 = 1$.
Weiterhin kann man die positive Grundeinheit ϵ_1 mit Satz 7.2.2 berechnen und erhält

$$\epsilon_1 = (8X^7 + 2X^6 + 3X^5 + X^4 + 3X^3 + 3X + 3) - (8X^5 + 2X^4 + 3X^3 + 5X^2 + 5X + 10)\sqrt{D},$$

und damit $R_K = 7$. Setzt man dies in die Formel 15.1.2 (4) ein, so ergibt sich

$$\begin{aligned} h(P_1P_2)h(P_3) &= \frac{1}{200}\,(11(24+2+2) - 5(2\cdot 7 + (4+1+1+1+1+1)) \\ &\quad +11\cdot 6 - 5(14+9) - 11\cdot 10 + 5(14+7) - 11(2+2) + 5(14+7)) \\ &= \frac{1}{200}(308 - 115 + 66 - 115 - 110 + 105 - 44 + 105) = 1. \end{aligned}$$

Dies liefert eine Bestätigung unserer Aussagen.

Literatur

[A] ARTIN, E.: *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, in: *The collected papers of Emil Artin*, Addison-Wesley, Festschrift (1965), 153-246.

[Deu] DEURING, M.: *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Mathematics 314, Berlin 1973.

[Far] FARWICK, R.: *Kettenbrüche und enge Klassen in reell quadratischen Funktionenkörpern über $\mathbb{F}_p$*, Diplomarbeit WWU Münster 1994.

[Gz] GONZÁLES, C.: *Class Numbers of Quadratic Function Fields and Continued Fractions*, Journal of Number Theory 40 (1992), 38-59.

[Ha1] HASSE, H.: *Zahlentheorie*, 3. berichtigte Auflage, Akademie-Verlag, Berlin 1969.

[Ha2] HASSE, H.: *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952.

[H1] HAYES, D.R.: *Real Quadratic Function Fields*, CMS Conference Proceedings Vol. 7 (1987), 203-236.

[He] HECKE, E.: *Über die Kroneckersche Grenzformel für reelle quadratische Körper und die Klassenzahl relativ-abelscher Körper*, Verhandl. d. Naturforschenden Gesell. i. Basel 28 (1917), 363-372.

[Hir] HIRZEBRUCH, F.: *Hilbert Modular Surfaces*, L'Enseignement Mathématique 19 (3-4) (1973), 183-281.

[H-R] HOFFSTEIN, J.; ROSEN, M.: *Average values of L-series in function fields*, Journal f.d. reine und angewandte Mathematik 426 (1992), 117-150.

[Kor] KORTE, U.: *Binäre quadratische Formen über Zahlkörpern und Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper*, Dissertation WWU Münster 1981.

[Kron] KRONECKER, L.: *Zur Theorie der elliptischen Modulfunktionen*, Werke IV, 347-495 und V, 1-132.

[Lg] LANG, H.: *Über die Klassenzahlen eines imaginären bizyklischen biquadratischen Zahlkörpers und seines reell-quadratischen Teilkörpers; Teil I*, Journal f.d. reine und angewandte Mathematik 262 (1973), S. 18-40.

[Mey] MEYER, C.: *Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag Berlin 1957.

[Nk] NEUKIRCH, J.: *Algebraische Zahlentheorie*, Springer-Verlag Berlin 1992.

[R] ROSEN, M.: *S-Units and S-Class Group in Algebraic Function Fields*, Journal of Algebra 26 (1973), 98-108.

[Schm1] SCHMIDT, F.K.: *Die Theorie der Klassenkörper über einem Körper algebraischer Funktionen in einer Unbestimmten und mit endlichem Koeffizientenbereich*, Sitzungsbericht der phys.-med. Sozietät zu Erlangen 62 (1930), 267-284.

[Schm2] SCHMIDT, F.K.: *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeitschrift 33 (1931), 1-32.

[Sie1] SIEGEL, C.L.: *Lectures on Advanced Analytic Number Theory*, Tata Institute Bombay 1961.

[Sie2] SIEGEL, C.L.: *Analytische Zahlentheorie I, II*, Vorlesungen Göttingen 1963/64.

[St1] STEIN, A.: *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern*, Dissertation Universität Saarbrücken 1996.

[Sti] STICHTENOTH, H., *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin 1993.

[W] WEIS, B.: *Zur Berechnung der Einheitengruppe und der Klassengruppen in quadratischen Kongruenzfunktionenkörpern*, Diplomarbeit Saarbrücken 1986.

[WZ] WEIS, B.; ZIMMER, H.G.: *Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen*, Mitt. Math. Ges. Hamburg, Sond XII, 2 (1991), 261-286.

[Ws] WEISS, E.: *Algebraic Number Theory*, McGraw-Hill, New York 1963.

[Zag1] ZAGIER, D.B.: *A Kronecker limit formula for real quadratic fields*, Math. Ann. 213 (1975), 153-184.

[Zag2] ZAGIER, D.B.: *Zetafunktionen und quadratische Körper*, Springer-Verlag, Berlin 1981.

[Zh] ZHANG, X.: *Ambiguous Classes and 2-rank of Class Group of Quadratic Function Field*, Journal of China University of Science and Technology 17, No. 4 (1987), 425-430.

Lebenslauf

Raphael Richter, geboren am 23. Februar 1969 in Menden

Familienstand: verheiratet

Vater: Klaus Max Erich Richter
Mutter: Christa Maria Richter, geb. Finger

Schulbildung

08/1975-07/1979	Besuch der Grundschule St. Josef in 58710 Menden-Lendringsen
08/1979-06/1988	Besuch des privaten, staatlich anerkannten Walburgisgymnasiums mit Abiturabschluß am 9. Juni 1988 in 58706 Menden

Ersatzdienst

08/1988-04/1990	Zivildienst an der westfälischen Schule für Körperbehinderte in Hemer

weitere Ausbildungen

11/1984-06/1987	Ausbildung zum nebenamtlichen Kirchenmusiker der Region Ruhrgebiet Ost (C-Examen)

Studium

04/1990	Beginn des Studiums der Mathematik und kath. Theologie für das Lehramt Sek II/I an der WWU Münster
04/1992	Abschluß des Grundstudiums in Erziehungswissenschaft im Rahmen des Lehramtsstudiengangs Sek II
04/1992	Zwischenprüfung im Fach Mathematik
09/1992	Abschluß des Grundstudiums in kath. Theologie (Sek II)
10/1992	Beginn des zusätzlicher Studiengangs Mathematik Diplom mit Nebenfach Mathematische Logik nach Einstufung in das 3. Semester
11/1994	Vordiplom im Fach Mathematik mit Nebenfach Mathematische Logik
05/1997	Diplom im Fach Mathematik mit Nebenfach Mathematische Logik am 5. Mai 1997 an der WWU Münster
im WS1997	Beginn des Promotionsstudiengangs Mathematik und Umschreibung Lehramtsstudiengang auf Mathematik mit den Nebenfächern Informatik und Italienisch (Sek II)

Sonstige schul- und studienbegleitende Tätigkeiten

10/1987-04/1992	Beschäftigung als nebenamtlicher Kirchenmusiker in der St. Nikolaus-Gemeinde in Balve-Beckum und der St. Paulus-Gemeinde in Menden
10/1992-04/1996	studentische Hilfskraft am mathematischen Institut der WWU Münster
seit 07/1997	wissenschaftliche Hilfskraft am mathematischen Institut der WWU Münster

Beginn der Dissertation

Die Dissertation wurde im Juli 1997 am Fachbereich Mathematik und Informatik der WWU Münster begonnen und von Prof. Dr. Heinrich Lang betreut.