Diedergruppe
und
Reziprozitätsgesetz

von

Jannis A. Antoniadis

Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3

Mathematisches Institut
der Universität Kreta
Iraklio, Kreta, Griechenland

MPI/SFB 85-31

1. Einleitung

Für ein normiertes irreduzibles Polynom $F(X)$ mit ganzen rationalen Koeffizienten bezeichnet $F_p(X)$ dasjenige Polynom, das man durch Reduktion der Koeffizienten von $F(X)$ modulo einer Primzahl p erhält.

Wenn für eine Primzahl p das Polynom $F_p(X)$ über dem Körper $\mathbb{F}_p$ der p Elemente in paarweise verschiedene lineare Polynome zerfällt, so sagt man, daß $F(X)$ vollzerlegt modulo p ist. Die Menge aller solcher p sei mit $Spl(F(X))$ bezeichnet. Jede Antwort auf die Frage, wie die zu $Spl(F(X))$ gehörenden Primzahlen bestimmt werden können, wird als höheres Reziprozitätsgesetz bezeichnet [15]. $Spl(F(X))$ läßt sich nach der Klassenkörpertheorie durch Kongruenzen modulo eines nur von $F(X)$ abhängigen Moduls bestimmen genau dann, wenn $F(X)$ abelsch ist [6].

In der vorliegenden Arbeit wird das höhere Reziprozitätsgesetz für eine Klasse von Polynomen mit Diedergruppe herausgestellt. Da die Zerfällungskörper dieser Polynome zyklische Erweiterungen imaginär-quadratischer Zahlkörper sind, benötigen wir einige Resultate aus der Theorie der komplexen Multiplikation, die im folgenden kurz zusammengefaßt werden [5],[13].
Sei $\Sigma = \mathbb{Q}(\sqrt{-d})$ ein imaginär-quadratischer Zahlkörper der Diskriminate $-d < 0$ und $R = R_f (f \in \mathbb{N} - \{0\})$ die Ordnung zum Führer f in Σ. Ist ein Element $\alpha = \frac{\alpha_1}{\alpha_2}$ aus der oberen Halbebene Idealbasisquotient eines Ideals $a_R = \{\alpha_1, \alpha_2\}$ der

Ringklasse k_R von R, so hängt der singuläre Wert $j(\alpha)$ nur von k_R ab. Man nennt daher $j(\alpha)$ die Ringklasseninvariante von k_R und schreibt

$$j(\alpha) = j(a_R) \quad \text{oder} \quad j(\alpha) = j(k_R).$$

Das Ringklassenpolynom

$$\Phi_f(X) = \prod_{k_R \in K_R} (X - j(k_R))$$

(K_R ist die Ringklassengruppe) der Ordnung R hat ganze rationale Koeffizienten und ist über Σ irreduzibel. Der Zerfällungskörper von $\Phi_f(X)$ über Σ ist der Ringklassenkörper modulo f über Σ :

$$N_f = \Sigma(j(k_R^{(1)}), j(k_R^{(2)}), \ldots, j(k_R^{(h_f)})),$$

wobei h_f die Ringklassenzahl modulo f bedeutet. Dabei gilt schon die einfachere Erzeugung

$$N_f = \Sigma(j(k_R))$$

mit irgendeiner Ringklasseninvarianten $j(k_R)$ zur Ordnung R.

Die Galoisgruppe $G(N_f/\Sigma)$ ist folgendermaßen kanonisch isomorph zur Ringklassengruppe K_R. Ist für jeden zum Führer f primen Primdivisor $\mathfrak{p}$ von Σ $\mathfrak{p}_R = \mathfrak{p} \cap R$ das zugehörige Ringideal, so entspricht die Ringklasse, in die das

$\mathfrak{p}_R$ gehört, dem Frobeniusautomorphismus

$$\left[\frac{N_f/\Sigma}{\mathfrak{p}}\right] .$$

Da das Ringklassenpolynom $\Phi_f(X)$ rationale Koeffizienten hat, erweist sich der Ringklassenkörper sogar als absolut galoissch. Die Galoisgruppe $G(N_f/\mathbb{Q})$ ensteht aus $G(N_f/\Sigma)$ durch Hinzunahme der Konjugation τ :

$$G(N_f/\mathbb{Q}) = G(N_f/\Sigma)\cdot\tau \cup G(N_f/\Sigma).$$

$\Phi_f(X) \in \mathbb{Z}[X]$ ist, wie schon gesagt, irreduzibel über Σ und damit über $\mathbb{Q}$ irreduzibel. Folglich bilden die Körper $\mathbb{Q}(j(\mathfrak{k}_R^{(\mu)}))$, $\mu = 1,2,\ldots,h_f$, ein volles System von zueinander über $\mathbb{Q}$ konjugierten Teilkörpern von N_f . Unter ihnen ist

$$K_0 = \mathbb{Q}(j(\mathfrak{k}_0)) = N_f \cap \mathbb{R}$$

der maximale reelle Teilkörper von N_f , wobei $\mathfrak{k}_0$ die Hauptringklasse von R bezeichnet.

Wir setzen jetzt voraus, daß für ein $f \in \mathbb{N}-\{0\}$ die Erweiterung N_f/Σ zyklisch von der Ordnung h_f ist. Also ist die Erweiterung $N_f/\mathbb{Q}$ galoissch mit Galoisgruppe

$$G(N_f/\mathbb{Q}) = D_{2h_f} = \langle\sigma,\tau \mid \sigma^{h_f} = 1, \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau\rangle,$$

die Diedergruppe der Ordnung $2h_f$. Im folgenden ist es nötig,

die beiden Fälle "h_f gerade" und "h_f ungerade"zu unterscheiden. Im ersten Fall enthält N_f außer Σ noch genau zwei weitere quadratische Zahlkörper $K_1 = \mathbb{Q}(\sqrt{-d_1})$ und $K_2 = \mathbb{Q}(\sqrt{d_2})$ der Diskriminanten $-d_1 < 0$ und $d_2 > 0$, im zweiten Fall nur Σ .Das Hauptresultat dieser Arbeit ist folgender

Satz Für jede Primzahl p, welche die Diskriminante $\Delta(\Phi_f)$ des Ringklassenpolynoms Φ_f nicht teilt, gilt:

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = \begin{cases} \frac{h_f - 2}{2} a_2(p) + 1 + \left(\frac{d_2}{p}\right), & \text{falls } \mu_R \in k_0 \\ 0, & \text{falls } \mu_R \notin k_0, \end{cases}$$

wenn $h_f \equiv 0 \bmod 2$ und

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = \frac{h_f}{6}(a_1^2(p) + a_1(p)) - \frac{1}{2}\left(\frac{-d}{p}\right) + \frac{1}{2},$$

wenn $h_f \equiv 1 \bmod 2$.

Dabei bezeichnen $a_1(p)$ und $a_2(p)$ jeweils den p-ten Koeffizienten der Fourierentwicklung von Spitzenformen, die im nächsten Paragraphen via Theta-Reihen definiert werden und $\left(\frac{\cdot}{p}\right)$ das Legendresche Symbol.

Korollar Es gilt

$$\mathrm{Spl}(N_f/\mathbb{Q}) = \{p \in \mathbb{P} \mid p \nmid \Delta(\Phi_f),\ \left(\frac{d_2}{p}\right) = \left(\frac{-d_1}{p}\right) = 1 \text{ und } a_2(p) = 2\},$$

wenn h_f gerade

und

$$Spl(N_f/\mathbb{Q}) = \{p \in \mathbb{P} \mid p \nmid \Delta(\Phi_f),\ (\tfrac{-d}{p}) = 1 \text{ und } a_1(p) = 2\},$$

wenn h_f ungerade ist.

Zuletzt werden wir eine konstruktive Version des wohlbekannten Satzes von Deligne-Serre [4] für die hier betrachteten Erweiterungen erhalten.

Die vorliegende Arbeit wurde fertiggestellt während eines Aufenthalts am Max-Planck-Institut für Mathematik in Bonn. Dem Gastinstitut möchte ich an dieser Stelle für die herzliche Aufnahme danken.

2. Beweis des Satzes

Im folgenden bezeichnen

- p immer eine Primzahl, $\mathbb{P}$ die Menge aller Primzahlen,
- ζ die primitive h_f-te Einheitswurzel $e^{\frac{2\pi i}{h_f}}$,
- $\mathfrak{p}, \mathfrak{p}_2, \mathfrak{P}, P$ Primideale der jeweiligen Hauptordnungen $R_\Sigma, R_{K_2}, R_{K_0}, R_{N_f}$, die über p liegen,
- $f_\mathfrak{p}(K_0/\mathbb{Q}), e_p(N_f/\mathbb{Q})$ den Grad des Ideals $\mathfrak{P}$ in $K_0/\mathbb{Q}$ bzw. den Verzweigungsindex von P in $N_f/\mathbb{Q}$,
- $\mathbb{F}_p$ den Körper der p Elemente,
- F_p den Frobeniusautomorphismus für p in $N_f/\mathbb{Q}$, $p \nmid \Delta(\Phi_f)$,
- $G_z(P)$ bzw. $G_T(P)$ die Zerlegungs- bzw. Trägheitsgruppe für P über $\mathbb{Q}$, $p \nmid \Delta(\Phi_f)$,
- K_Z bzw. K_T den entsprechenden Zerlegungs- bzw. Trägheitskörper für P über $\mathbb{Q}$, $p \nmid \Delta(\Phi_f)$.

Zuerst benötigen wir folgenden klassischen Dedekindschen

Satz 1 Sei $\Phi_f(X) = \prod_{i=1}^{r} h_i^{e_i}(x)$ die Zerlegung von $\Phi_f(x)$ in paarweise verschiedene irreduzible Faktoren über $\mathbb{F}_p$, $p \nmid \Delta(\Phi_f)$. Dann hat pR_{K_0} die Primidealzerlegung

$$pR_{K_0} = \mathfrak{P}_1^{\ell_1} \mathfrak{P}_2^{\ell_2} \cdots \mathfrak{P}_r^{\ell_r}$$

mit Graden $f_{K_i}(K_o/\mathbb{Q}) = \deg h_i(X)$, $i = 1,2,\ldots,r$.

Ist $H = \langle \tau \rangle$ die durch die Konjugation τ erzeugte Gruppe, so läßt sich $G = G(N_f/\mathbb{Q})$ in (rechte) Nebenklassen $H\sigma^i$, $i=0,\ldots,h-1$, zerlegen.

Nach [11], Seite 101, ist die Anzahl der Primideale in K_0, die pR_{K_0} teilen, gleich der Anzahl der Nebenklassenrepräsentanten (nach H) g, für welche die Inklusion $gG_Z(P)g^{-1} \subseteq H$ gilt.

Folglich ist die Anzahl der Wurzeln von $\Phi_f(x)$ in $\mathbb{F}_p$ gleich der Anzahl der Primideale ersten Grades in K_0, die pR_{K_0} teilen:

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = \#\{g \in \langle\sigma\rangle \mid gG_Z(P)g^{-1} \subseteq H\} \qquad (1)$$

<u>Hilfssatz 1</u> Für jedes $p \in \mathbb{P}$ mit $p \nmid \Delta(\Phi_f(x))$ gilt falls $h_f \equiv 0 \bmod 2$

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = \begin{cases} h_f, & \text{wenn } F_p = 1 \\ 0, & \text{wenn } F_p = \sigma^\mu,\ 1 \le \mu \le h_f - 1 \\ 2, & \text{wenn } F_p = \tau\sigma^\mu,\ 0 \le \mu \le h_f - 1,\ \mu \equiv 0 \bmod 2 \\ 0, & \text{wenn } F_p = \tau\sigma^\mu\ 0 \le \mu \le h_f - 1,\ \mu \equiv 1 \bmod 2 \end{cases}$$

und falls $h_f \equiv 1 \bmod 2$

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = \begin{cases} h_f, & \text{wenn } F_p = 1 \\ 0, & \text{wenn } F_p = \sigma^\mu, 1 \le \mu \le h_f - 1 \\ 1, & \text{wenn } F_p = \tau\sigma^\mu, 0 \le \mu \le h_f - 1 \end{cases}$$

<u>Beweis</u> Ist $F_p = 1$, also $G_Z(P) = \{1\}$, so gilt $gG_Zg^{-1} \subseteq H$ für jedes $g \in \langle\sigma\rangle$ und deswegen ist $\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = h_f$.
Sei $F_p = \sigma^\mu, 1 \le \mu \le h_f - 1$, d.h. $G_Z = \langle\sigma^\mu\rangle$ und folglich

gilt für jedes $g = \sigma^{\lambda}$, $0 \leq \lambda \leq h_f - 1$

$gG_Z(P)g^{-1} \not\subseteq H$, also $\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = 0$.

Sei nun $F_p = \tau\sigma^{\mu}$, $0 \leq \mu \leq h_f - 1$, also $G_Z(P) = \langle\tau\sigma^{\mu}\rangle$.

Gilt für $g = \sigma^{\lambda}$, $0 \leq \lambda \leq h_f - 1$ $gG_Z(P)g^{-1} \subseteq H$, so muß $\sigma^{2\lambda-\mu}\tau$ Element von H sein, was aber genau dann erfüllt ist, wenn $2\lambda-\mu \equiv 0 \bmod h_f$. Die letzte Kongruenz aber hat, wegen der Einschränkungen für λ und μ, $2\lambda - \mu = 0$ oder $2\lambda - \mu = h_f$ zur Folge, also $\lambda = \frac{\mu}{2}$ oder $\lambda = \frac{h_f+\mu}{2}$. (2)

Für gerade Klassenzahl gibt es 2 ganzrationale λ oder kein λ, je nachdem $\mu \equiv 0 \bmod 2$ oder $\mu \equiv 1 \bmod 2$ ist, für ungerade Klassenzahl gibt es immer ein ganzrationales λ.

<u>Hilfssatz 2</u> Für jedes $p \in \mathbb{P}$, $p \nmid \Delta(\Phi_f)$, gelten:

(i) $F_p = 1$ genau dann, wenn $(\frac{-d}{p}) = 1$ und $\mathfrak{p}_R \in k_0$.

(ii) $F_p = \sigma^{\mu}$, $1 \leq \mu \leq h_f-1$, genau dann, wenn $(\frac{-d}{p}) = 1$ und $\mathfrak{p}_R \notin k_0$.

(iii) $F_p = \tau\sigma^{\mu}$, $0 \leq \mu \leq h_f-1$ genau dann, wenn $(\frac{-d}{p}) = -1$.

<u>Beweis</u> (i) $F_p = 1$ ist äquivalent zu

$f_{\mathfrak{p}}(\Sigma/\mathbb{Q}) = 1$ und $f_p(N_f/\Sigma) = 1$,

was aber nach der Klassenkörpertheorie äquivalent zu

$(\frac{-d}{p}) = 1$ und $\mathfrak{p}_R \in k_0$ ist.

(ii) $F_p = \sigma^{\mu}$, $\mu = 1,2,\ldots,h_f-1$, ist äquivalent zu

$\Sigma \subseteq K_Z \subsetneq N_f$, also zu $f_{\mathfrak{p}}(\Sigma/\mathbb{Q}) = 1$ und $f_p(N_f/\Sigma) > 1$,

was aber auch gleichbedeutend mit $(\frac{-d}{p}) = 1$ und

$\mathfrak{p}_R \notin k_0$ ist.

(iii) $F_p = \tau\sigma^\mu, 0 \leq \mu \leq h_f-1$, ist äquivalent dazu, daß Σ in K_Z nicht enthalten ist, was aber auch gleich bedeutend mit $(\frac{-d}{p}) = -1$ ist.

Ist nun die Ringklassenzahl h_f gerade, so existieren die Körper K_1 und K_2 mit den zugehörigen Galoisgruppen $\langle\sigma^2,\sigma\tau\rangle$ und $\langle\sigma^2,\tau\rangle$. Es gilt $-d_1d_2 = -df_1^2$ mit f_1 ganzrational. Nach dem Führer-Diskriminanden-Satz der Klassenkörpertheorie teilt nun f_1 den Führer f. Es läßt sich leicht folgern, daß die Voraussetzung $(\frac{-d}{p}) = 1$ und $\mathfrak{p}_R \in k_0$ äquivalent zu $(\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1$ und $\mathfrak{p}_R \in k_0$ ist, denn der Fall $(\frac{d_2}{p}) = (\frac{-d_1}{p}) = -1$ widerspricht $\mathfrak{p}_R \in k_0$.

Ist $(\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1$ und $\mathfrak{p} \notin k_0$, so folgt $(\frac{-d}{p}) = 1$ und $\mathfrak{p} \notin k_0$, was nach den Hilfssätzen 1 und 2 $\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = 0$ zur Folge hat.

Hilfssatz 3 Sei h_f gerade. Dann gilt für jedes $p \in \mathbb{P}$, $p \nmid \Delta(\Phi_f(x))$

(i) $F_p = \tau\sigma^\mu, 0 \leq \mu \leq h_f-1$, $\mu \equiv 0 \bmod 2$ genau dann, wenn $(\frac{d_2}{p}) = 1$ und $(\frac{-d_1}{p}) = -1$.

(ii) $F_p = \tau\sigma^\mu, 0 \leq \mu \leq h_f-1$, $\mu \equiv 1 \bmod 2$ genau dann, wenn $(\frac{d_2}{p}) = -1$ und $(\frac{-d_1}{p}) = 1$.

Beweis (i) Da nach Voraussetzung μ gerade ist, ist $\langle\tau\sigma^\mu\rangle$ Untergruppe von $\langle\sigma^2,\tau\rangle$ und folglich $K_2 \subseteq K_Z$, also $f_{\mathfrak{p}_2}(K_2/\mathbb{Q}) = 1$, was $(\frac{d_2}{p}) = 1$ zur Folge hat.

Andererseits ist $\langle\tau\sigma^{\mu}\rangle$ nicht Untergruppe von $\langle\sigma\rangle$, womit Σ nicht in K_Z enthalten ist. Folglich gilt $f_{\mathfrak{p}}(\Sigma/\mathbb{Q}) \neq 1$, d.h. $f_{\mathfrak{p}}(\Sigma/\mathbb{Q}) = 2$, also $(\frac{-d}{p}) = -1$.

Seien jetzt $(\frac{d_2}{p}) = 1$ und $(\frac{-d_1}{p}) = -1$. Daraus folgt, daß in K_Z K_2, aber nicht Σ enthalten ist, und äquivalent dazu, daß $G_Z(P)$ Untergruppe von $\langle\sigma^2,\tau\rangle$, aber nicht von $\langle\sigma\rangle$ ist. Da $G_Z(P)$ zyklisch ist und für jedes $v \in \mathbb{Z}$, $0 \leq v < h_f$, $\tau\sigma^{v} = \sigma^{-v}\tau$ gilt, enthält das Erzeugende der Zerlegungsgruppe unbedingt τ und eventuell eine gerade Potenz von σ. Deshalb ist $F_p = \tau\sigma^{\mu}$, $0 \leq \mu \leq h_f-1$ und $\mu \equiv 0 \bmod 2$. (ii) kann man ähnlich beweisen.

Es ist noch zu bemerken, daß $(\frac{d_2}{p}) = (\frac{-d_1}{p}) = -1$ $(\frac{-d}{p}) = 1$ und $\mathfrak{p}_R \notin k_0$ zur Folge hat, womit der Beweis des folgenden Satzes vervollständigt wird.

Satz 2 (i) Ist h_f gerade, so ist

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x)=0\} = \begin{cases} h_f, & \text{wenn } (\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1 \text{ und } \mathfrak{p}_R \in k_0, \\ 0, & \text{wenn } (\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1 \text{ und } \mathfrak{p}_R \notin k_0 \\ 2, & \text{wenn } (\frac{d_2}{p}) = 1 \text{ und } (\frac{-d_1}{p}) = -1 \\ 0, & \text{wenn } (\frac{d_2}{p}) = -1 \end{cases}$$

(ii) Ist h_f ungerade, so ist

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x)=0\} = \begin{cases} h_f, & \text{wenn } (\frac{-d}{p}) = 1 \text{ und } \mathfrak{p}_R \in k_0, \\ 0, & \text{wenn } (\frac{-d}{p}) = 1 \text{ und } \mathfrak{p}_R \notin k_0 \\ 1, & \text{wenn } (\frac{-d}{p}) = -1 \end{cases}$$

Dabei ist $p \in \mathbb{P}$, $p \nmid \Delta(\Phi_f(x))$.

Im weiteren wird hier versucht,eine Aussage mit Hilfe der Fourierkoeffizienten gewisser Spitzenformen zu gewinnen.Bekanntlich existiert eine Bijektion zwischen der Gesamtheit der Äquivalenzklassen von positiv-definiten binären quadratischen Formen der Diskriminante $-df^2$ und der Ringklassengruppe modulo f über Σ.

Für jedes $j(0 \leq j \leq h_f-1)$ sei $g_{k_j}(x,y)$ ein Repräsentant derjenigen Äquivalenzklasse , der die Ringklasse k_j entspricht. Sei jetzt k_1 ein Erzeugendes der Ringklassengruppe modulo f über Σ, $k_j = k_1^j$. Die einzigen ambigen Klassen sind k_0 und $k_{h_f/2}$. Bezeichne nun $A_{k_j}(n)$ die Anzahl der eigentlichen Darstellungen von n durch die quadratische Form $g_{k_j}(x,y)$. Die Gültigkeit des folgenden Resultates ist wohlbekannt [16]:

Hilfssatz 4 Für jede Primzahl p , $p \nmid df$, gelten:

$$\text{(i)} \quad \frac{1}{2} A_{k_0}(p) + \frac{1}{2} A_{k_{h_f/2}}(p) + \sum_{k \in K-\{k_0, k_1, \bar{k}_1\}} A_k(p) = 1 + \left(\frac{-d}{p}\right)$$

(ii) Höchstens eine der $A_k(p)$ ist nicht gleich Null.

Die Theta-Funktion,welche der quadratischen Form $g_k(x,y)$ entspricht, ist durch

$$\Theta_j(\omega) = \frac{1}{2} \sum_{n=0}^{\infty} A_{k_j}(n) e^{2\pi i \omega n} \quad (\mathrm{Im}(\omega) > 0) \quad \text{definiert.}$$

Die Funktionen $F_1(\omega) = \Theta_0(\omega) - \Theta_1(\omega) = \sum_{n=0}^{\infty} a_1(n)q^n$ für h_f ungerade und $F_2(\omega) = \Theta_0(\omega) - \Theta_{h_f/2}(\omega) = \sum_{n=0}^{\infty} a_2(n)q^n$ für h_f gerade sind nach [7] normierte Spitzenformen zur Kongruenzgruppe $\Gamma_0(df^2)$ vom Gewicht Eins und Charakter $(\frac{-d}{p})$. Mit Hilfe der obigen Überlegungen ergibt sich nun:

Hilfssatz 5 Es gilt

$$a_1(p) = \begin{cases} 2, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p = g_0(x,y) \\ -1, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p_R \in k_1 \cup \bar{k}_1 \\ 0, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p_R \notin k_1 \cup \bar{k}_1 \cup k_0 \\ 0, \text{ wenn } (\frac{-d}{p}) = -1 \end{cases}$$

und

$$a_2(p) = \begin{cases} 2, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p = g_0(x,y) \\ -2, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p = g_{h_f/2}(x,y) \\ 0, \text{ wenn } (\frac{-d}{p}) = 1 \text{ und } p_R \notin k_0 \cup k_{h_f/2} \\ 0, \text{ wenn } (\frac{-d}{p}) = -1, \end{cases}$$

wobei $p \in \mathbb{P}$ mit $p \nmid df$ ist.

Aus dem Satz 2 sowie den Hilfssätzen 4 und 5 ergibt sich die Richtigkeit unseres in der Einleitung aufgestellten Resultates.

3. Der Satz von Deligne-Serre

Hier wird vorausgesetzt, daß die Ringklassenzahl gerade ist, $h_f = 2\ell, \ell \in \mathbb{Z}$. Folglich läßt sich die Galoisgruppe $G = G(N_f/\mathbb{Q}) = D_{2h_f}$ in $\ell + 3$ Konjugationsklassen zerlegen.

Dementsprechend gibt es $\ell + 3$ irreduzible Darstellungen, von denen 4 linear und $\ell - 1$ zweidimensional sind:

$$\rho_j(\sigma) = \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix}, \quad \rho_j(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad j = 1,2,\ldots,\ell - 1.$$

Seien jetzt

$$P_1 = \{p \in \mathbb{P} \mid p \nmid f, \ (\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1 \text{ und } \mathfrak{p}_R \in k_0\}$$

$$P_2 = \{p \in \mathbb{P} \mid p \nmid f, \ (\frac{d_2}{p}) = (\frac{-d_1}{p}) = 1 \text{ und } \mathfrak{p}_R \notin k_0\}$$
$$\cup \{p \in \mathbb{P} \mid p \nmid f, \ (\frac{d_2}{p}) = (\frac{-d_1}{p}) = -1\}$$

$$P_3 = \{p \in \mathbb{P} \mid p \nmid f, \ (\frac{d_2}{p}) = 1 \text{ und } (\frac{-d_1}{p}) = -1\}$$
$$\cup \{p \in \mathbb{P} \mid p \nmid f, \ (\frac{d_2}{p}) = -1 \text{ und } (\frac{-d_1}{p}) = 1\},$$

$$P_4 = \{p \in \mathbb{P} \mid p \nmid f, \ p \mid d \text{ und } \mathfrak{p}_R \in k_0\} \text{ und}$$

$$P_5 = \{p \in \mathbb{P} \mid p \nmid f, \ p \mid d \text{ und } \mathfrak{p}_R \in k_{h_f/2} = k_1^{\ell}\}.$$

Genauso wie in [1] läßt sich nun das entsprechende

$$A_p = \frac{1}{e} \sum_{r \in G_T} \rho(F_p r) \ , \ e = e_p(N_f/\mathbb{Q}) \qquad \rho = \rho_1, \ G_T = G_T(P)$$

zu

$$A_p = \rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \text{ falls } \ p \in P_1 \ ,$$

$$A_p = \rho(\sigma^\mu) = \begin{pmatrix} \zeta^\mu & 0 \\ 0 & \zeta^{-\mu} \end{pmatrix} , \ \text{ falls } \ p \in P_2,$$

$$A_p = \rho(\tau\sigma^\mu) = \begin{pmatrix} 0 & \zeta^{-\mu} \\ \zeta^\mu & 0 \end{pmatrix}, \text{ falls } \ p \in P_3 \ ,$$

$$A_p = \frac{1}{2}(\rho(1) + \rho(\tau\sigma^\mu)) = \frac{1}{2} \begin{pmatrix} 1 & \zeta^{-\mu} \\ \zeta^\mu & 1 \end{pmatrix} , \text{ falls } \ p \in P_4,$$

$$A_p = \frac{1}{2}(\rho(\sigma^\ell) + \rho(\sigma^\ell\tau\sigma^\mu)) = \frac{1}{2}\begin{pmatrix} -1 & -\zeta^{-\mu} \\ -\zeta^\mu & -1 \end{pmatrix} \ , \text{ falls } \ p \in P_5$$

berechnen.

ρ ist bekanntlich eine monomiale Darstellung [3], Seite 339, also induziert von einer linearen Darstellung ρ' der zyklischen Untergruppe $G(N_f/\Sigma) = \langle\sigma\rangle$. ρ' ist als Darstellung des Ringklassenkörpers modulo f via Artinsches Reziprozitätsgesetz aufzufassen. Da ρ' nicht trivial ist, folgt nun

$$A_p = \frac{1}{e} \sum_{r \in G_T} \rho'(F_p r) = \frac{1}{e} \rho'(F_p) \sum_{r \in G_T} \rho'(r) = 0$$

für jede Primzahl p, die f teilt. Das Eulerprodukt der

entsprechenden Artinschen L-Reihe $L(s,\rho,N_f/\mathbb{Q})$ ist

$$L(s,\rho,N_f/\mathbb{Q}) = \prod_{p\in\mathbb{P}} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - A_p Np^{-s} \right)^{-1}$$

$$= \prod_{p\in P_1} (1 - 2p^{-s} + p^{-2s})^{-1} \prod_{p\in P_2} (1-2\cos \frac{2\pi\mu}{h_f} p^{-s} + p^{-2s})^{-1}$$

$$\prod_{p\in P_3} (1 - p^{-2s})^{-1} \prod_{p\in P_4} (1 - p^{-s})^{-1} \prod_{p\in P_5} (1 + p^{-s})^{-1}.$$

Sei χ der Charakter der Ringklassengruppe modulo f, welcher der Darstellung ρ' entspricht und

$$F(\omega) = \sum_{i=0}^{h_f-1} \chi(k_1^i)\Theta_i(\omega) = \sum_{n=1}^{\infty} a(n)q^n \quad , q = e^{2\pi i\omega}, \mathrm{Im}(\omega)>0.$$

Es läßt sich leicht nachweisen, daß $a(1) = 1$, $a(mn) = a(m)a(n)$ für $(m,n) = 1$, $a(p)a(p^r) = a(p^{r+1}) + (\frac{-d}{p})a(p^{r-1})$ für $p\nmid df$, $r\geq 1$ und $a(p)a(p^r) = a(p^{r+1})$ für $p|df$, also daß $F(\omega)$ eine <u>normierte neue Form</u> zu $\Gamma_0(df^2)$ vom Gewicht Eins und Charakter $(\frac{-d}{p})$ ist. Sei $L_F(s) = \sum_{n=1}^{\infty} a(m)m^{-s}$ die Dirichletsche Reihe, die der normierten neuen Form, via eine Mellintransformation, entspricht. Da $F(\omega)$ Eigenfunktion aller Hecke-Operatoren ist, läßt sich $L_F(s)$ in folgendes Eulerprodukt entwickeln:

$$L_F(s) = \prod_{p\nmid df} (1-a(p)p^{-s} + (\frac{-d}{p})p^{-2s})^{-1} \prod_{p|df} (1-a(p)p^{-s})^{-1}.$$

Beachte man nun noch, daß $a(p) = 0$ wenn p/f und $a(p) = \pm 1$ für $p \nmid f$ aber p/d, je nachdem $\mathfrak{p}_R \in k_0$ oder $\mathfrak{p}_R \in k^{\ell} = k_{h_f/2}$,

so ergibt sich endlich die Aussage des Delinge-Serreschen Satzes, nämlich die Gleichheit

$$L_F(s) = L(s,\rho,N_f/\mathbb{Q}) \ .$$

Ähnlich kann man die obere Relation beweisen für den Fall einer ungeraden Ringklassenzahl h_f .

4. Schlußbemerkungen

(i) Ist speziell $h_f = 4$, so läßt sich die erste Gleichheit des in dieser Arbeit bewiesenen Satzes einheitlich so formulieren:

$$\#\{x \in \mathbb{F}_p \mid \Phi_f(x) = 0\} = 1 + \left(\frac{d_2}{p}\right) + a_2(p) \ ,$$

was das Hauptresultat in [1] war, das als Spezialfall ein früheres Resultat von Moreno [12] enthält.

(ii) Chowla und Cowles [2] haben zuerst das höhere Reziprozitätsgesetz für das Polynom

$$f(x) = 4x^3 - 4x^2 + 1$$

bewiesen und zwar unter Benutzung der Tatsache, daß alle elliptischen Kurven über $\mathbb{Q}$ mit Führer 11 sich durch Modulfunktionen für $\Gamma_0(11)$ parametrisieren lassen [14], was bekanntlich ein spezieller (bewiesener) Fall der Taniyama-Weil-Vermutung ist.

Hiramatsu [8] gibt einen anderen Beweis desselben Resultates im Sinne der Klassenkörpertheorie.

Er bemerkte, daß der Zerlegungskörper von $f(x)$ über $\mathbb{Q}$ mit dem Strahlklassenkörper modulo 2 von $\Sigma = \mathbb{Q}(\sqrt{-11})$ übereinstimmt. Da der Strahlklassenkörper modulo 2 mit dem Ringklassenkörper modulo 2 über Σ identisch ist, stellt dieses Resultat auch einen Spezialfall unseres Satzes dar. Hiramatsu und Mimura [9] haben das höhere Reziprozitätsgesetz des Hilbertschen

Klassenkörpers über einem imaginär-quadratischen Zahlkörper $\Sigma = \mathbb{Q}(\sqrt{-d})$, allerdings nur für den Fall $d \in \mathbb{P}$, $d \equiv -1(8)$ bewiesen. Für eine Verallgemeinerung des Chowla-Cowleschen Resultates in Richtung der Theorie der elliptischen Kurven siehe [10].

Literatur

[1] J.A. Antoniadis, Höhere Reziprozitätsgesetze und Modulformen vom Gewicht Eins, J. reine angew. Math. (erscheint demnächst).

[2] S. Chowla, M. Cowles, On the coefficients c_m in the expansion $x\prod_1^\infty(1-x^n)^2(1-x^{11n})^2 = \sum_1^\infty c_n x^n$, J. reine angew. Math 292(1977), 115-116.

[3] C.W. Curtis, I. Reiner, Representation theory of finite groups and associative Algebras, Interscience, N. York 1962.

[4] P. Deligne, J.-P. Serre, Formes modulaires des Poids 1, Ann. Sci. Ecole Norm. Sup., 4 serie, 7 (1974), 507-530.

[5] M. Deuring, Die Klassenkörper der komplexen Multiplikation, Enzykl. der Math. Wissenschaften, Band I, 2. Teil C, Stuttgart 1958.

[6] D. Garbanati, Class field summarized, Rocky Mt. J. Math. 11 (1981), 195-225.

[7] E. Hecke, Theorie der elliptischen Modulfunktionen, Math. Ann. 97 (1926), 210-242.

[8] T. Hiramatsu, Higher Reciprocity Laws and Modular Forms of Weight One, Commentarii Mathematici Universitatis Sancti Pauli 31 (1982), 75-85.

[9] T. Hiramatsu, Y. Mimura, The modular equation and modular forms of weight one, Manuskript.

[10] H. Ito, A remark on a theorem of Chowla-Cowles, J. reine angew. Math. 332 (1982), 151-155.

[11] G.J. Janusz, Algebraic Number Fields, New York 1973.

[12] C.J. Moreno, The Higher Reciprocity Laws: An Example, J. Number Theory 12 (1980), 57-70.

[13] R. Schertz, Eine Neubegründung der Weberschen Resultate über die singulären Werte der Modulfunktionen $f, f_1, f_2, \gamma_2, \gamma_3$ und der Beweis der beiden Weberschen Vermutungen, Dissertation, Köln 1971.

[14] A.J. Van der Poorten, The polynomial x^3+x^2+x-1 and elliptic curves of Conductor 11, Seminaire Delange-Pisot-Poitou (Théorie des nombres), 18°anneé, 1976/77, n°17, 17-01 ~ 17-07.

[15] B.F. Wyman, What is a reciprocity law? Am. Math. Mo. 79 (1972), 571-586.

[16] D. Zagier, Zetafunktionen und quadratische Körper, Berlin-Heidelberg-New York 1981.