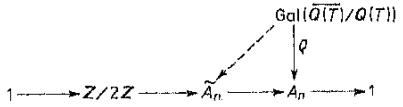
representation ϱ: $\mathrm{Gal}(\overline{Q(T)}/Q(T)) \to A_n$ with a trivial second Stiefel–Whitney class $\varrho^* w_2(\xi_n) \in H^2(\mathrm{Gal}(\overline{Q(T)}/Q(T)), Z/2Z)$. Here ξ_n denotes the real bundle over BA_n associated to the standard representation of the alternating group A_n into $SO_n(R)$. Since $\varrho^* w^2(A_n)$ can be viewed as the obstruction to the embedding problem given by the diagram



where $\tilde{A}_n$ denotes the universal central extension of A_n, the result follows.

References

[1] A. Arenas, *Un problema aritmético sobre las sumas de tres cuadrados*, Tesis doctoral. Univ. de Barcelona, 1985.

[2] A. Arenas and P. Bayer, *Arithmetic behaviour of the sums of three squares*, J. Number Theory 27 (1987), 273–284.

[3] L. E. Dickson, *History of the theory of numbers*, vol. II. Chelsea Pub. Comp., 1971.

[4] A. J. Earnest and J. S. Hsia, *Spinor norms of local integral rotations II*, Pacific J. Math. 61 (1975), 71–86.

[5] C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae, 1810. [English translation: Arthur A. Clarke, 1966, New Haven: Yale Univ. Press].

[6] R. Schulze-Pillot, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. 75 (1984), 283–299.

[7] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (4) (1984), 651–676.

[8] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. 97 (1973), 440–481.

[9] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, ibid. 36 (1935), 527–606. Gesammelte Abhand., Band 1, Springer, 1966.

[10] – *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1935), 83–86. Gesammelte Abhand., Band 1, Springer, 1966.

[11] N. Vila, *On central extensions of A_n as a Galois group over Q*, Arch. Math. 44 (1985), 424–437.

FACULTAT DE MATEMÀTIQUES
DPT. D'ÀLGEBRA I FONAMENTS
UNIVERSITAT DE BARCELONA
Gran Via de les Corts Catalanes 585
08007 Barcelona, Spain

Received on 17.6.1986
and in revised form on 5.2.1987 (1652)

ACTA ARITHMETICA
LI (1988)

Binäre quadratische Formen und Diederkörper

von

FRANZ HALTER-KOCH (Graz)

Gegenstand dieser Arbeit ist die Darstellung von Primzahlen durch ganzzahlige binäre quadratische Formen. Die Gauß'sche Theorie der Geschlechter gestattet es, zu entscheiden, ob eine Primzahl durch ein Geschlecht quadratischer Formen dargestellt wird oder nicht, aber sie erlaubt im allgemeinen keine Aussagen über die Darstellung durch individuelle Formen.

Die binären quadratischen Formen fester Diskriminante bilden bezüglich der Komposition eine zur Ringklassengruppe dieser Diskriminante isomorphe Gruppe, und jeder Satz über die Darstellung von Primzahlen durch eine Form dieser Diskriminante ist ein Satz über das Zerlegungsverhalten dieser Primzahl im Ringklassenkörper; umgekehrt ist auch jedes Zerlegungsgesetz für den Ringklassenkörper ein Darstellungssatz durch binäre quadratische Formen (auf Grund des Artin-Isomorphismus). Kann man nun auf andere als auf klassenkörpertheoretische Weise (etwa mittels einer Radikalerzeugung) ein Zerlegungsgesetz für den Ringklassenkörper herleiten, so hat man damit einen Darstellungssatz für Primzahlen durch binäre quadratische Formen hergeleitet. Auf diesem Prinzip beruhen viele der in den letzten Jahren publizierten Potenzrestkriterien für quadratische Einheiten, welche man auch als Darstellungssätze für Primzahlpotenzen durch binäre quadratische Formen deuten kann ([21, [15], [25], [14], [26], [12], [13]).

Verwendet man an Stelle des vollen Ringklassenkörpers nur einen Teilkörper desselben, so erhält man nicht mehr Darstellungssätze für individuelle Formen, aber doch noch Darstellungssätze für gewisse Mengen von Formenklassen, welche im Spezialfall absolut-abelscher Teilkörper gerade die Geschlechter sind. Eine in diesem Zusammenhang bereits mehrfach untersuchte Körperklasse ist die der Diederkörper 8. Grades ([21], [15], [20], [22]), da deren Radikalerzeugung leicht zu überblicken ist. Die daraus resultierenden Darstellungssätze für Primzahlen durch binäre quadratische Formen bestimmen die Klasse darstellender Formen bis auf 4. Potenzen in der Kompositionsklassengruppe ihrer Diskriminante.

In den zitierten Arbeiten wurden die Diederkörper 8. Grades immer nur in solchen Fällen verwendet, in denen die zugehörige Ringklassengruppe nur

eine durch 4 teilbare Invariante besitzt; nur in solchen Fällen ist nämlich eine eindeutige explizite Zuordnung zwischen dem Diederkörper und dem definierenden Charakter 4. Grades möglich. In der vorliegenden Arbeit befreie ich mich von dieser Einschränkung durch die systematische Verwendung von Charakteren; damit rücken einerseits die bisherigen Resultate in ein neues Licht, es gelingt aber auch, diese wesentlich zu verallgemeinern und eine Reihe neuer Darstellungssätze für Primzahlen durch binäre quadratische Formen herzuleiten.

Teile dieser Arbeit entstanden während eines Gastaufenthaltes an der Universite de Nancy I; Herrn Professor P. Kaplan danke ich für seine Gastfreundschaft und viele interessante Diskussionen zur Thematik dieser Arbeit.

1. Ein allgemeiner Darstellungssatz. Die in diesem Abschnitt eingeführten Bezeichnungen werde ich während der ganzen Arbeit beibehalten.

Sei Δ eine Diskriminante ganzzahliger binärer quadratischer Formen, also $\Delta \in \mathbf{Z} \setminus \{0, 1\}$, $\Delta \equiv 1 \bmod 4$ oder $\Delta \equiv 0 \bmod 4$, $\Delta = \Delta_0 f^2$ mit einer Fundamentaldiskriminante Δ_0, und sei $k_\Delta = \mathbf{Q}(\sqrt{\Delta})$. $\mathscr{C}(\Delta)$ sei die Klassengruppe ganzzahliger primitiver binärer (im Falle $\Delta < 0$ positiv definiter) quadratischer Formen der Diskriminante Δ; ich bezeichne mit $[a, b, c]$ die Klasse der Form $aX^2+bXY+cY^2$, es ist also $[a, b, c] \in \mathscr{C}(\Delta)$ genau dann, wenn $a, b, c \in \mathbf{Z}$, $(a, b, c) = 1$, $\Delta = b^2-4ac$, und $a > 0$, falls $\Delta < 0$. Stellt eine Klasse $A \in \mathscr{C}(\Delta)$ eine Zahl $\varkappa \in \mathbf{Z}$ primitiv dar, so schreibe ich $A \to \varkappa$.

$\mathscr{X}(\Delta)$ sei die Gruppe aller Geschlechtscharaktere $\varphi: \mathscr{C}(\Delta) \to \{\pm 1\}$ der Form $\varphi = \chi^2$ mit einem Charakter $\chi: \mathscr{C}(\Delta) \to C^\times$; $\mathscr{X}(\Delta)$ ist ein F_2-Vektorraum, und $\dim \mathscr{X}(\Delta)$ ist die Anzahl der durch 4 teilbaren Invarianten von $\mathscr{C}(\Delta)$.

Sei $\varphi: \mathscr{C}(\Delta) \to \{\pm 1\}$ ein Geschlechtscharakter, $\varphi \neq 1$; zu φ gehört ein k_Δ enthaltender biquadratischer Körper

$$K_\varphi = \mathbf{Q}(\sqrt{e_\varphi}, \sqrt{\tilde{e}_\varphi}) \supset k_\Delta$$

mit Fundamentaldiskriminanten e_φ, $\tilde{e}_\varphi$ und

$$e_\varphi \tilde{e}_\varphi = \Delta_0 \cdot (f_\varphi^0)^2$$

(f_φ^0 ist der Führer von K_φ/k_Δ), so daß gilt:

Für alle $Q \in \mathscr{C}(\Delta)$ und Primzahlen $p \nmid f_\varphi^0$ mit $Q \to p$ gilt für die Primteiler $\mathfrak{p}$ von p in k_Δ: Genau dann ist $\mathfrak{p}$ in K_φ zerlegt, wenn $\varphi(Q) = 1$. Insbesondere gilt für alle $\varkappa \in N$ mit $(\varkappa, 2\Delta) = 1$ und $Q \to \varkappa$:

$$\varphi(Q) = \left(\frac{e_\varphi}{\varkappa}\right) = \left(\frac{\tilde{e}_\varphi}{\varkappa}\right).$$

Die Deutung von φ als Artin-Charakter von K_φ/k_Δ liefert ein körpertheoretisches Kriterium für φ, zu $\mathscr{X}(\Delta)$ zu gehören:

Genau dann ist $\varphi \in \mathscr{X}(\Delta)$, wenn sich K_φ in einem über k_Δ zyklischen Diederkörper 8. Grades[1] L_φ einbetten läßt derart, daß für den Führer f_φ von L_φ/k_Δ gilt: $f_\varphi \mid f$.

Sei nun im folgenden $\varphi \in \mathscr{X}(\Delta)$ und L_φ ein über k_Δ zyklischer Diederkörper 8. Grades, sei f_φ der Führer von L_φ/k_Δ und $f_\varphi \mid f$. L_φ ist Teilkörper des Ringklassenkörpers modulo f über k_Δ (im "engeren" Sinne, d.h. mit klassenkörpertheoretischem Führer $f \cdot \infty$), und daher ist der Artincharakter χ_φ von L_φ/k_Δ auf $\mathscr{C}(\Delta)$ definiert,

$$\chi_\varphi: \mathscr{C}(\Delta) \to C^\times.$$

Es ist $\chi_\varphi^2 = \varphi$, und für $Q \in \mathscr{C}(\Delta)$, Primzahlen p mit $p \nmid f_\varphi$ und $Q \to p$ und Primteiler $\mathfrak{p}$ von p in k_Δ gilt; $\mathfrak{p}$ zerfällt in L_φ in ein Produkt von 1, 2 oder 4 Primfaktoren, je nachdem, ob $\chi_\varphi(Q) = \pm i$, -1 oder 1.

$\boldsymbol{P}(\Delta)$ sei die Menge aller Primzahlen p mit $p \nmid 2\Delta$, die von einer Klasse $Q \in \mathscr{C}(\Delta)^2$ dargestellt werden. Eine Primzahl p mit $p \nmid 2\Delta$ gehört offensichtlich genau dann zu $\boldsymbol{P}(\Delta)$, wenn p im Geschlechterkörper des Ringklassenkörpers modulo f von k_Δ voll-zerlegt ist [11]; dann ist p auch voll-zerlegt in K_φ für alle Geschlechtscharaktere $\varphi \neq 1$.

Für $p \in \boldsymbol{P}(\Delta)$ und $\varphi \in \mathscr{X}(\Delta)$ sei

$$\sigma_\varphi(p) = \begin{cases} 1, & \text{falls } \varphi = 1 \text{ oder } p \text{ in } L_\varphi \text{ voll-zerlegt ist,} \\ -1 & \text{sonst.} \end{cases}$$

Wegen $p \in \boldsymbol{P}(\Delta)$ ist $\sigma_\varphi(p)$ von der Wahl des Körpers L_φ unabhängig (das folgt aus dem unten stehenden Theorem, kann aber auch leicht direkt eingesehen werden).

Der Zusammenhang zwischen Diederkörpern 8. Grades und der Darstellung von Primzahlen durch binäre quadratische Formen kann nun wie folgt formuliert werden:

THEOREM. *Sei $A = A_0^2 \in \mathscr{C}(\Delta)^2$ eine Klasse im Hauptgeschlecht von $\mathscr{C}(\Delta)$, und sei $p \in \boldsymbol{P}(\Delta)$. Dann sind äquivalent:*

(i) *Es gibt ein $A' \in A \cdot \mathscr{C}(\Delta)^4$ mit $A' \to p$.*

(ii) *Für alle $\varphi \in \mathscr{X}(\Delta)$ ist $\sigma_\varphi(p) = \varphi(A_0)$.*

Bemerkung. Die Nebenklasse $A \cdot \mathscr{C}(\Delta)^4 \in \mathscr{C}(\Delta)/\mathscr{C}(\Delta)^4$ ist das Spinorgeschlecht von A im Sinne von [6]. Das Symbol $\sigma_\varphi(p)$ beschreibt das Spinorgeschlecht von $A \in \mathscr{C}(\Delta)$ mit $A \to p$ und kann daher als Spinorgeschlechtssymbol bezeichnet werden. Es ist eng verwandt mit den von L. Redei [31] und Y. Furuta [8] definierten Symbolen, jedoch ist keines der drei Symbole Spezialfall eines anderen; ihre genaue Beziehung zueinander habe ich an anderer Stelle ausführlich dargestellt [16].

---

[1] Unter einem Diederkörper 8. Grades verstehe ich einen galoisschen algebraischen Zahlkörper Ω, dessen Galoisgruppe $\mathrm{Gal}(\Omega/\mathbf{Q})$ eine Diedergruppe der Ordnung 8 ist.

Beweis des Theorems. Ist $A' = AB^4$ mit $B \in \mathcal{C}(\Delta)$ und $A' \to p$, so folgt $\sigma_\varphi(p) = \chi_\varphi(A')$ (Klassenkörper-Zerlegungsgesetz), also $\sigma_\varphi(p) = \chi_\varphi(A) = \varphi(A_0)$ für alle $\varphi \in \mathcal{X}(\Delta)$.

Ich nehme nun an, es sei $A' \in \mathcal{C}(\Delta)^2$ mit $A' \to p$, aber $A' \notin A \cdot \mathcal{C}(\Delta)^4$. Dann ist

$$A'A^{-1} = B^2 \in \mathcal{C}(\Delta)^2 \setminus \mathcal{C}(\Delta)^4$$

mit $B \in \mathcal{C}(\Delta)$, so daß $4 | \mathrm{ord}(B)$ und $B \notin \mathcal{C}(\Delta)^2$. Folglich existiert ein Charakter 4. Grades $\chi\colon \mathcal{C}(\Delta) \to \mathbb{C}^\times$ mit $\chi(B) = i$, und für $\varphi = \chi^2\colon \mathcal{C}(\Delta) \to \mathbb{C}^\times$ gilt:

$$\varphi \in \mathcal{X}(\Delta), \quad \chi_\varphi(B) = \pm i,$$

und

$$-1 = \chi_\varphi(B^2) = \chi_\varphi(A') \cdot \chi_\varphi(A)^{-1} = \sigma_\varphi(p) \cdot \varphi(A_0)^{-1}.$$

Daraus folgt aber $\varphi(A_0) \neq \sigma_\varphi(p)$. ∎

Korollar 1 und Zusatz. *Für φ, $\varphi' \in \mathcal{X}(\Delta)$ ist*

$$\sigma_\varphi \cdot \sigma_{\varphi'} = \sigma_{\varphi\varphi'}\colon \ P(\Delta) \to \{\pm 1\}.$$

Insbesondere kann man sich in Aussage (ii) *des Theorems auf ein Erzeugendensystem von $\mathcal{X}(\Delta)$ beschränken.*

Beweis. Sei $p \in P(\Delta)$ und $A_0 \in \mathcal{C}(\Delta)$ mit $A_0^2 \to p$. Dann folgt $\sigma_\varphi(p) = \varphi(A_0)$, $\sigma_{\varphi'}(p) = \varphi'(A_0)$, $\sigma_{\varphi\varphi'}(p) = (\varphi\varphi')(A_0) = \varphi(A_0) \cdot \varphi'(A_0)$ und daraus die Behauptung. ∎

Korollar 2. *Sei $A = A_0^2 \in \mathcal{C}(\Delta)^2$ eine Klasse im Hauptgeschlecht von $\mathcal{C}(\Delta)$, $\varkappa \in \mathbb{N}$ mit $(\varkappa, 2\Delta) = 1$, $p \in P(\Delta)$ und $A \to \varkappa^2 p$. Dann gilt für alle $\varphi \in \mathcal{X}(\Delta)$:*

$$\sigma_\varphi(p) = \left(\frac{e_\varphi}{\varkappa}\right) \cdot \varphi(A_0) = \left(\frac{\tilde{e}_\varphi}{\varkappa}\right) \cdot \varphi(A_0).$$

Beweis. Sei $Q = Q_0^2 \in \mathcal{C}(\Delta)^2$ mit $Q \to p$; dann folgt $A_0 Q_0^{-1} \to \varkappa$, also $\left(\frac{e_\varphi}{\varkappa}\right) = \varphi(A_0 Q_0^{-1})$ und damit $\left(\frac{e_\varphi}{\varkappa}\right) \cdot \varphi(A_0) = \varphi(Q_0) = \sigma_\varphi(p)$. ∎

Für die Anwendung des Theorems und der beiden Korollare ist es nötig, zu entscheiden, welche Geschlechtscharaktere φ zu $\mathcal{X}(\Delta)$ gehören, und nach dem eingangs Gesagten ist das äquivalent zum Problem der Einbettbarkeit von K_φ in einen Diederkörper unter Beschränkung des Führers; ferner ist eine (möglichst explizite) Formel zur Berechnung von σ_φ erforderlich. Diese Aufgaben werden in den beiden nächsten Paragraphen behandelt.

2. Berechnung von σ_φ. Ich behalte die in § 1 eingeführten Bezeichnungen bei und erhalte zunächst aus [9] das folgende Kriterium für einen Geschlechtscharakter, zu $\mathcal{X}(\Delta)$ zu gehören:

Proposition 1. *Für einen Geschlechtscharakter $\varphi\colon \mathcal{C}(\Delta) \to \{\pm 1\}$, $\varphi \neq 1$, sind äquivalent:*

(A) $\varphi \in \mathcal{X}(\Delta)$;

(B) *Es gibt eine Zahl $\alpha_\varphi \in Q(\sqrt{e_\varphi})$ mit folgenden Eigenschaften:*

1. $\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\alpha_\varphi) = \tilde{e}_\varphi h^2$ *mit* $h \in Q^\times$;

2. *für die Relativdiskriminante* $\mathfrak{d}(\alpha_\varphi)$ *von* $Q(\sqrt{\alpha_\varphi})/Q(\sqrt{e_\varphi})$ *gilt*

$$\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\mathfrak{d}(\alpha_\varphi)) \cdot e_\varphi \mid \Delta;$$

3. α_φ *ist ganz und ohne echten ganzrationalen Teiler.*

Die Zahl α_φ aus Proposition 1 ist die wichtigste Größe für die Berechnung von σ_φ; für eine quadratische Irrationalität α sei im folgenden stets α' die zu α konjugierte Zahl.

Proposition 2. *Sei $\varphi \in \mathcal{X}(\Delta)$, $\varphi \neq 1$; $\alpha_\varphi \in Q(\sqrt{e_\varphi})$ erfülle die Bedingungen* 1., 2. *und* 3. *von Proposition* 1. *Dann gilt:*

(i) *Für $p \in P(\Delta)$ und alle Primteiler* $\mathfrak{p}$ *von p in $Q(\sqrt{e_\varphi})$ ist*

$$\sigma_\varphi(p) = \left(\frac{\alpha_\varphi}{\mathfrak{p}}\right)$$

(*quadratisches Restsymbol modulo* $\mathfrak{p}$).

(ii) *Ist $\tilde{\alpha}_\varphi \in Q(\sqrt{\tilde{e}_\varphi})$ und $\xi \in Q(\sqrt{\tilde{e}_\varphi})$ mit*

$$\tilde{\alpha}_\varphi \xi^2 = (\sqrt{\alpha_\varphi} + \sqrt{\alpha_\varphi'})^2 = \alpha_\varphi + \alpha_\varphi' + h\sqrt{\tilde{e}_\varphi},$$

so gilt für $p \in P(\Delta)$ und alle Primteiler $\tilde{\mathfrak{p}}$ von p in $Q(\sqrt{\tilde{e}_\varphi})$:

$$\sigma_\varphi(p) = \left(\frac{\tilde{\alpha}_\varphi}{\tilde{\mathfrak{p}}}\right)$$

(*quadratisches Restsymbol modulo* $\tilde{\mathfrak{p}}$).

Beweis von Proposition 1 und 2. Sei zunächst $\varphi \in \mathcal{X}(\Delta)$, $\varphi \neq 1$. Dann ist $K_\varphi = Q(\sqrt{e_\varphi}, \sqrt{\tilde{e}_\varphi})$ in einen über k_Δ zyklischen Diederkörper 8. Grades L_φ einbettbar, so daß der Führer f_φ von L_φ/k_Δ f teilt. Nach [9] ist L_φ Normalkörper eines Körpers 4. Grades Λ_φ mit $Q(\sqrt{e_\varphi}) \subset \Lambda_\varphi \subset L_\varphi$, und für die Diskriminante $\partial(\Lambda_\varphi)$ von Λ_φ gilt:

$$\partial(\Lambda_\varphi) = \Delta_0 e_\varphi f_\varphi^2 \mid \Delta e_\varphi.$$

Sei $\alpha_\varphi \in Q(\sqrt{e_\varphi})$ ganz und ohne ganzrationalen Teiler mit $\Lambda_\varphi = Q(\sqrt{e_\varphi})(\sqrt{\alpha_\varphi})$; dann folgt

$$\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\alpha_\varphi) = \tilde{e}_\varphi h^2 \quad \text{mit } h \in Q^\times,$$

und

$$\partial(\Lambda_\varphi) = \pm e_\varphi^2 \cdot \mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\mathfrak{d}(\alpha_\varphi)),$$

also

$$\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\mathfrak{d}(\alpha_\varphi)) \cdot e_\varphi \mid \Delta,$$

d.h. α_φ hat die drei Eigenschaften aus Proposition 1 (B). Seien nun

$$\tilde{\alpha}_\varphi,\ \xi \in Q(\sqrt{\tilde{e}_\varphi}) \quad \text{mit } \tilde{\alpha}_\varphi \xi^2 = (\sqrt{\alpha_\varphi} + \sqrt{\alpha_\varphi'})^2 = \mathrm{Sp}_{Q(\sqrt{e_\varphi})/Q}(\alpha_\varphi) + h\sqrt{\tilde{e}_\varphi};$$

dann ist L_φ auch Normalkörper zu

$$\tilde{\Lambda}_\varphi = Q(\sqrt{e_\varphi})(\sqrt{\tilde{\alpha}_\varphi}),$$

und für $p \in P(\Delta)$ gilt: Genau dann ist $\sigma_\varphi(p) = 1$, wenn p in Λ_φ (bzw. $\tilde{\Lambda}_\varphi$) vollzerlegt ist. Ist $\mathfrak{p}$ bzw. $\tilde{\mathfrak{p}}$ ein Primteiler von p in $Q(\sqrt{e_\varphi})$ bzw. $Q(\sqrt{\tilde{e}_\varphi})$, so ist genau dann $\sigma_\varphi(p) = 1$, wenn $\mathfrak{p}$ in Λ_φ bzw. $\tilde{\mathfrak{p}}$ in $\tilde{\Lambda}_\varphi$ vollzerlegt ist, und das ist äquivalent zu $\left(\frac{\alpha_\varphi}{\mathfrak{p}}\right) = 1$ bzw. $\left(\frac{\tilde{\alpha}_\varphi}{\tilde{\mathfrak{p}}}\right) = 1$; damit ist Proposition 2 bewiesen.

Sei nun $\alpha_\varphi \in Q(\sqrt{e_\varphi})$, so daß Proposition 1(B) gilt, und sei $\Lambda_\varphi = Q(\sqrt{e_\varphi})(\sqrt{\alpha_\varphi})$. Dann ist Λ_φ nicht normal, und der zugehörige Normalkörper L_φ ist ein K_φ enthaltender, über k_Δ zyklischer, Diederkörper 8. Grades über Q. Ist f_φ der Führer von L_φ/k_Δ, so folgt wie oben:

$$\partial(\Lambda_\varphi) = \Delta_0 e_\varphi f_\varphi^2 = \pm e_\varphi^2 \cdot \mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\mathfrak{d}(\alpha_\varphi))$$

teilt

$$\Delta e_\varphi = \Delta_0 e_\varphi f^2,$$

also $f_\varphi \mid f$ und damit $\varphi \in \mathcal{X}(\Delta)$. ∎

Die Berechnung von $\sigma_\varphi(p)$ mittels Proposition 2 hat den Schönheitsfehler, daß die dazu benutzten quadratischen Restsymbole keine rationalen Symbole sind. Ein erster Schritt zur Beseitigung dieses Schönheitsfehlers ist die folgende unmittelbar einsichtige, aber oft nützliche Bemerkung.

ZUSATZ ZU PROPOSITION 2. *Die in Proposition 2 auftretenden quadratischen Restsymbole* $\left(\frac{\alpha_\varphi}{\mathfrak{p}}\right)$ *bzw.* $\left(\frac{\tilde{\alpha}_\varphi}{\tilde{\mathfrak{p}}}\right)$ *zur Berechnung von* $\sigma_\varphi(p)$ *sind von der Auswahl der* $\mathfrak{p} \mid p$ *bzw.* $\tilde{\mathfrak{p}} \mid p$ *unabhängig. Bei der Wahl von festen Einbettungen* $Q(\sqrt{e_\varphi}) \subset Q_p$ *bzw.* $Q(\sqrt{\tilde{e}_\varphi}) \subset Q_p$ *ist*

$$\left(\frac{\alpha_\varphi}{\mathfrak{p}}\right) = \left(\frac{\alpha_\varphi}{p}\right) \quad \text{bzw.} \quad \left(\frac{\tilde{\alpha}_\varphi}{\tilde{\mathfrak{p}}}\right) = \left(\frac{\tilde{\alpha}_\varphi}{p}\right)$$

(*mit gewöhnlichen Legendre-Symbolen in* Q_p).

Im folgenden leite ich für $\sigma_\varphi(p)$ einen rationalen Ausdruck her, welcher aus dem von Proposition 2 durch Anwendung des Reziprozitätsgesetzes in $Q(\sqrt{e_\varphi})$ entsteht und damit der Variabilität von $p \in P(\Delta)$ besser Rechnung trägt.

Sei also wieder $\varphi \in \mathcal{X}(\Delta)$, $\varphi \neq 1$, und habe $\alpha_\varphi \in Q(\sqrt{e_\varphi})$ die Eigenschaften aus Proposition 1(B). Dann hat die Primidealzerlegung von α_φ die Form

$$(\alpha_\varphi) = \mathfrak{y} \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \cdot \mathfrak{v}^2$$

mit paarweise nicht-konjugierten Primidealen 1. Grades $\mathfrak{q}_i \neq 2$ von $Q(\sqrt{e_\varphi})$ $(i = 1, \ldots, s)$; $\mathfrak{v}$ ist ein ganzes Ideal von $Q(\sqrt{e_\varphi})$, und es ist entweder $\mathfrak{y} = (1)$, oder $\mathfrak{y}$ ist ein Primteiler 1. Grades von 2 in $Q(\sqrt{e_\varphi})$. Ist $\mathcal{N}(\mathfrak{q}_i) = q_i$, so folgt

$$\tilde{e}_\varphi = u_\varphi \cdot q_1 \cdot \ldots \cdot q_s \quad \text{mit} \quad u_\varphi \in \{\pm 1, \pm 4, \pm 8\},$$

und genau dann ist $\mathfrak{y} \neq (1)$, wenn $u_\varphi = \pm 8$.

Sei λ_φ der Hecke'sche Idealcharakter von $Q(\sqrt{\alpha_\varphi})/Q(\sqrt{e_\varphi})$ (definiert auf den zu $\mathfrak{d}(\alpha_\varphi)$ primen Idealen von $Q(\sqrt{e_\varphi})$ mit Werten in $\{\pm 1\}$). Dann gilt für $p \in P(\Delta)$ und Primteiler $\mathfrak{p}$ von p in $Q(\sqrt{e_\varphi})$:

$$\sigma_\varphi(p) = \lambda_\varphi(\mathfrak{p}).$$

$\lambda_\varphi(\mathfrak{p})$ ist aber mittels Klassenkörpertheorie für $Q(\sqrt{\alpha_\varphi})/Q(\sqrt{e_\varphi})$ berechenbar!

Ist $p \in P(\Delta)$ und $\mathfrak{p}$ ein Primteiler von p in $Q(\sqrt{e_\varphi})$, so liegt $\mathfrak{p}$ im engeren Hauptgeschlecht von $Q(\sqrt{e_\varphi})$, also gibt es ein ganzes $\pi_\varphi \in Q(\sqrt{e_\varphi})$ ohne echten ganzrationalen Teiler, so daß

$$(\pi_\varphi) = \mathfrak{p}\mathfrak{c}^2$$

mit einem ganzen, zu $\mathfrak{d}(\alpha_\varphi)$ primen Ideal $\mathfrak{c}$ von $Q(\sqrt{e_\varphi})$ und $\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\pi_\varphi) > 0$. Damit folgt

$$\lambda_\varphi(\mathfrak{p}) = \lambda_\varphi((\pi_\varphi)) = \prod_{\mathfrak{w} \mid \mathfrak{d}(\alpha_\varphi) \cdot \infty} \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{w}}\right)$$

(siehe [5], "Exercises").

Auf Grund der Normierung von α_φ ist

$$\mathfrak{d}(\alpha_\varphi) = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \cdot \prod_{\mathfrak{z} \mid 2} \mathfrak{z}^{s(\mathfrak{z})}$$

(mit geeigneten Exponenten $s(\mathfrak{z}) \geqslant 0$) und folglich

$$\prod_{\mathfrak{w} \mid \mathfrak{d}(\alpha_\varphi)} \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{w}}\right) = \prod_{j=1}^{s} \left(\frac{\pi_\varphi}{\mathfrak{q}_j}\right) \cdot \prod_{\substack{\mathfrak{z} \mid 2 \\ s(\mathfrak{z}) > 0}} \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right).$$

Im Falle $e_\varphi < 0$ ist $\prod_{\mathfrak{w} \mid \infty} \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{w}}\right) = 1$. Im Falle $e_\varphi > 0$ betrachte ich eine

feste Einbettung $Q(\sqrt{e_\varphi}) \subset \boldsymbol{R}$ und erhalte

$$\prod_{\mathfrak{w}\mid\infty}\left(\frac{\pi_\varphi,\alpha_\varphi}{\mathfrak{w}}\right)=(-1)^{S(\pi_\varphi,\alpha_\varphi)}$$

mit

$$S(\pi,\alpha)=\frac{\operatorname{sign}(\pi)-1}{2}\cdot\frac{\operatorname{sign}(\alpha)-1}{2}+\frac{\operatorname{sign}(\pi')-1}{2}\cdot\frac{\operatorname{sign}(\alpha')-1}{2}$$

also unter Beachtung von $\pi_\varphi\pi'_\varphi>0$ und $\operatorname{sign}(\alpha_\varphi\alpha'_\varphi)=\operatorname{sign}(\tilde{e}_\varphi)$:

$$\prod_{\mathfrak{w}\mid\infty}\left(\frac{\pi_\varphi,\alpha_\varphi}{\mathfrak{w}}\right)=1 \quad \text{genau dann, wenn } \pi_\varphi>0 \text{ oder } \tilde{e}_\varphi>0.$$

Damit ist bewiesen:

PROPOSITION 3. *Sei $\varphi\in\mathfrak{X}(\Delta)$, $\varphi\neq 1$; $\alpha_\varphi\in Q(\sqrt{e_\varphi})$ habe die Eigenschaften aus Proposition* 1(B); *sei die Diskriminante $\mathfrak{d}(\alpha_\varphi)$ von $Q(\sqrt{\alpha_\varphi})/Q(\sqrt{e_\varphi})$ von der Form*

$$\mathfrak{d}(\alpha_\varphi)=\mathfrak{q}_1\cdot\ldots\cdot\mathfrak{q}_s\cdot\prod_{\mathfrak{z}\mid 2}\mathfrak{z}^{s(\mathfrak{z})}$$

mit paarweise nicht-konjugierten Primidealen 1. *Grades $\mathfrak{q}_i\nmid 2$ und Exponenten $s(\mathfrak{z})\geqslant 0$. Sei $p\in P(\Delta)$ und $\pi_\varphi\in Q(\sqrt{e_\varphi})$ ganz und ohne echten ganzrationalen Teiler, so daß $\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\pi_\varphi)=pc^2$ mit $c\in N$, $(c,2\Delta)=1$; im Falle $e_\varphi>0$, $\tilde{e}_\varphi<0$ sei $\pi_\varphi>0$. Dann folgt:*

$$\sigma_\varphi(p)=\prod_{j=1}^{s}\left(\frac{\pi_\varphi}{\mathfrak{q}_j}\right)\cdot\prod_{\substack{\mathfrak{z}\mid 2\\ s(\mathfrak{z})>0}}\left(\frac{\pi_\varphi,\alpha_\varphi}{\mathfrak{z}}\right).$$

Besonders einfach ist der in den folgenden Anwendungen ausschließlich auftretende Fall, in welchem e_φ und $\tilde{e}_\varphi$ keinen ungeraden Primteiler gemeinsam haben, in dem also $(e_\varphi,\tilde{e}_\varphi)\mid 8$. In diesem Falle setze ich

$$e_\varphi^*=\prod_{j=1}^{s}q_j,$$

also $\tilde{e}_\varphi=ue_\varphi^*$; die q_j sind in $Q(\sqrt{e_\varphi})$ zerlegt, und nach fester Wahl von $\sqrt{e_\varphi}$ modulo e_φ^* ist

$$\prod_{j=1}^{s}\left(\frac{\pi_\varphi}{\mathfrak{q}_j}\right)=\left(\frac{\pi_\varphi}{e_\varphi^*}\right)$$

(Jacobi-Symbol). Sei nun

$$\pi_\varphi=\frac{M+N\sqrt{e'_\varphi}}{w}$$

mit $M,N\in\boldsymbol{Z}$, $(M,N)=1$, $M>0$, falls $e_\varphi>0$, $\tilde{e}_\varphi<0$, und

$$e'_\varphi=\begin{cases}e_\varphi,\ w\in\{1,2\},\ M+N\equiv w \bmod 2, & \text{falls } e_\varphi\equiv 1 \bmod 4,\\ \frac{1}{4}e_\varphi,\ w=1, & \text{falls } e_\varphi\equiv 0 \bmod 4.\end{cases}$$

Sei $\mathcal{N}_{Q(\sqrt{e_\varphi})/Q}(\pi_\varphi)=pH^2$ mit $H\in N$, also

$$M^2-e'_\varphi N^2=pw^2H^2;$$

dann ist nach fester Wahl von $\sqrt{e'_\varphi}$ modulo e_φ^*

$$\prod_{j=1}^{s}\left(\frac{\pi_\varphi}{\mathfrak{q}_j}\right)=\left(\frac{M+N\sqrt{e'_\varphi}}{e_\varphi^*}\right)\cdot\left(\frac{w}{e_\varphi^*}\right).$$

Der Normalkörper von $Q(\sqrt{M+N\sqrt{e'_\varphi}})$ ist ein Diederkörper 8. Grades über Q, und wegen

$$\left(\sqrt{M+N\sqrt{e'_\varphi}}+\sqrt{M-N\sqrt{e'_\varphi}}\right)^2=2(M+wH\sqrt{p})$$

ist dieser auch Normalkörper von $Q\left(\sqrt{2(M+wH\sqrt{p})}\right)$; daher folgt für alle $j\in\{1,\ldots,s\}$

$$\left(\frac{M+N\sqrt{e'_\varphi}}{q_j}\right)=\left(\frac{2}{q_j}\right)\cdot\left(\frac{M+wH\sqrt{p}}{q_j}\right)$$

und nach fester Wahl von $\sqrt{p}$ modulo e_φ^*:

$$\prod_{j=1}^{s}\left(\frac{\pi_\varphi}{\mathfrak{q}_j}\right)=\left(\frac{M+wH\sqrt{p}}{e_\varphi^*}\right)\cdot\left(\frac{2w}{e_\varphi^*}\right).$$

Damit ist bewiesen:

ZUSATZ ZU PROPOSITION 3. *Seien die Voraussetzungen von Proposition* 3 *erfüllt, und sei $(e_\varphi,\tilde{e}_\varphi)\mid 8$; e_φ^*, e'_φ, w, M und N seien wie eben definiert. Dann gilt bei fester Wahl von $\sqrt{e_\varphi}$ und $\sqrt{p}$ modulo e_φ^*:*

$$\sigma_\varphi(p)=\left(\frac{\pi_\varphi}{e_\varphi^*}\right)\cdot\prod_{\substack{\mathfrak{z}\mid 2\\ s(\mathfrak{z})>0}}\left(\frac{\pi_\varphi,\alpha_\varphi}{\mathfrak{z}}\right);$$

$$\left(\frac{\pi_\varphi}{e_\varphi^*}\right)=\left(\frac{M+N\sqrt{e'_\varphi}}{e_\varphi^*}\right)\cdot\left(\frac{w}{e_\varphi^*}\right)=\left(\frac{M+wH\sqrt{p}}{e_\varphi^*}\right)\cdot\left(\frac{2w}{e_\varphi^*}\right).$$

3. Einbettung in Diederkörper und explizite Formeln für die 2-Anteile von $\sigma_\varphi(p)$. In diesem Paragraphen gebe ich für die in Proposition 3 auftretenden

2-Anteile von $\sigma_\varphi(p)$,

$$\Gamma(\pi_\varphi, \alpha_\varphi) = \prod_{\substack{\mathfrak{z} \mid 2 \\ s(\mathfrak{z})>0}} \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right),$$

rationale Ausdrücke nach günstiger Wahl von α_φ an. Die dafür durchzuführenden Rechnungen erlauben es auch, ein explizites Kriterium dafür anzugeben, daß ein Geschlechtscharakter $\varphi \neq 1$ zu $\mathscr{X}(\Delta)$ gehört (Proposition 4).

Für einen Geschlechtscharakter φ: $\mathscr{C}(\Delta) \to \{\pm 1\}$, $\varphi \neq 1$, mögen e_φ, $\tilde{e}_\varphi$, f_φ^0 und K_φ die Bedeutung aus § 1 haben, und es sei $\tilde{e}_\varphi = u_\varphi e_\varphi^*$ mit $u_\varphi \in \{\pm 1, \pm 4, \pm 8\}$, $e_\varphi^* = q_1 \cdot \ldots \cdot q_s$ mit Primzahlen $q_j \equiv 1 \bmod 2$. Dann gilt:

PROPOSITION 4. *Sei* φ: $\mathscr{C}(\Delta) \to \{\pm 1\}$ *ein Geschlechtscharakter,* $\varphi \neq 1$. *Genau dann ist* $\varphi \in \mathscr{X}(\Delta)$, *wenn die beiden folgenden Bedingungen erfüllt sind:*

1. $\left(\frac{e_\varphi, \tilde{e}_\varphi}{p}\right) = 1$ *für alle* $p \in \boldsymbol{P} \cup \{\infty\}$.
2. $z_\varphi \cdot f_\varphi^0 \mid f$, *wobei*

$$z_\varphi = \begin{cases} 1, & \text{falls } 2 \nmid f_\varphi^0 \text{ und nicht } (e_\varphi, \tilde{e}_\varphi) \equiv (4, 5) \bmod 8 \\ & \text{oder } (e_\varphi, \tilde{e}_\varphi) \equiv (5, 4) \bmod 8, \\ 2 & \text{sonst.} \end{cases}$$

Bedingung 1. in Proposition 4 ist gleichwertig damit, daß K_φ in einen über k_Δ zyklischen Diederkörper 8. Grades L_φ einbettbar ist ([9], Satz 22); $\varphi \in \mathscr{X}(\Delta)$ ist nach § 1 gleichwertig damit, daß man L_φ so wählen kann, daß für den Führer f_φ von L_φ/k_Δ gilt: $f_\varphi \mid f$.

Proposition 4 kann somit angesehen werden als Kriterium für die Einbettbarkeit von K_φ in einen über k_Δ zyklischen Diederkörper 8. Grades L unter Beschränkung des Führers von L/k_Δ; als solches enthält es als Spezialfälle das klassische Kriterium von Rédei und Reichardt [32] und den scharfen Einbettungssatz von Perrin-Riou (für den hier betrachteten Fall ([30], Théorème 12).

Ich nehme nun an, es sei Bedingung 1 aus Proposition 4 erfüllt. Dann gibt es ein $\alpha \in \boldsymbol{Q}(\sqrt{e_\varphi})$, so daß $\mathscr{N}_{\boldsymbol{Q}(\sqrt{e_\varphi})/\boldsymbol{Q}}(\alpha) = \tilde{e}_\varphi h^2$ mit $h \in \boldsymbol{Q}^\times$. Definiert man $g_\varphi \in N$ durch

$$f = f_\varphi^0 \cdot g_\varphi,$$

so folgt:

Genau dann ist $\varphi \in \mathscr{X}(\Delta)$, wenn $f_\varphi \mid f$, und das ist nach der bereits in § 2 benutzten Diskriminantenformel für Diederkörper ([9], Satz 24) gleichwertig mit

$$\mathscr{N}\mathfrak{d}(\alpha) \mid \tilde{e}_\varphi g_\varphi^2$$

($\mathfrak{d}(\alpha)$ ist die Relativdiskriminante von $\boldsymbol{Q}(\sqrt{\alpha})/\boldsymbol{Q}(\sqrt{e_\varphi})$). Bedingung 2. aus Proposition 4 ist offensichtlich gleichwertig mit

$$z_\varphi \mid g_\varphi;$$

daher ist für den Beweis von Proposition 4 noch zu zeigen:

Genau dann gibt es ein $\alpha \in \boldsymbol{Q}(\sqrt{e_\varphi})$ mit $\mathscr{N}_{\boldsymbol{Q}(\sqrt{e_\varphi})/\boldsymbol{Q}}(\alpha) = \tilde{e}_\varphi h^2$ ($h \in \boldsymbol{Q}^\times$) und $\mathscr{N}\mathfrak{d}(\alpha) \mid \tilde{e}_\varphi g_\varphi^2$, wenn $z_\varphi \mid g_\varphi$.

Für die zu 2 primen Anteile von $\mathfrak{d}(\alpha)$ und g_φ ist das trivial; bezeichnet man mit $\mathfrak{d}_2(\alpha)$ den 2-Anteil von $\mathfrak{d}(\alpha)$, so bleibt zu beweisen:

PROPOSITION 4a. *Sei* φ: $\mathscr{C}(\Delta) \to \{\pm 1\}$ *ein Geschlechtscharakter,* $\varphi \neq 1$, *und sei*

$$\left(\frac{e_\varphi, \tilde{e}_\varphi}{p}\right) = 1 \quad \text{für alle } p \in \boldsymbol{P} \cup \{\infty\}.$$

Dann gilt:

1. *Ist* $\alpha \in \boldsymbol{Q}(\sqrt{e_\varphi})$, *so daß* $\mathscr{N}_{\boldsymbol{Q}(\sqrt{e_\varphi})/\boldsymbol{Q}}(\alpha) = \tilde{e}_\varphi h^2$ *mit* $h \in \boldsymbol{Q}^\times$, *so folgt* $z_\varphi^2 \cdot u_\varphi \mid \mathscr{N}\mathfrak{d}_2(\alpha)$.
2. *Es gibt ein ganzes* $\alpha_\varphi \in \boldsymbol{Q}(\sqrt{e_\varphi})$ *ohne echten ganzrationalen Teiler, so daß* $\mathscr{N}_{\boldsymbol{Q}(\sqrt{e_\varphi})/\boldsymbol{Q}}(\alpha_\varphi) = \tilde{e}_\varphi h^2$ *mit* $h \in \boldsymbol{Q}^\times$ *und* $\mathscr{N}\mathfrak{d}_2(\alpha) = \pm z_\varphi^2 u_\varphi$.

Der Beweis von Proposition 4a erfolgt nun getrennt für die verschiedenen Werte von e_φ und $\tilde{e}_\varphi$; dazu werde ich geeignete α_φ konstruieren und dabei auch die Zahlen $\Gamma(\pi_\varphi, \alpha_\varphi)$ berechnen.

Sei im folgenden φ: $\mathscr{C}(\Delta) \to \{\pm 1\}$ ein Geschlechtscharakter, $\varphi \neq 1$, und sei $\left(\frac{e_\varphi, \tilde{e}_\varphi}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$. Sei e bzw. $\tilde{e}$ der quadratfreie Kern von e_φ bzw. $\tilde{e}_\varphi$; dann ist auch $\left(\frac{e, \tilde{e}}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$.

Sei $\alpha \in \boldsymbol{Q}(\sqrt{e_\varphi})$, so daß $\mathscr{N}_{\boldsymbol{Q}(\sqrt{e_\varphi})/\boldsymbol{Q}}(\alpha) = \tilde{e}h^2$ mit $h \in \boldsymbol{Q}^\times$; ich kann o. E. annehmen, daß α ganz und ohne echten ganzrationalen Teiler ist und daß $h \in N$, $h \equiv 1 \bmod 2$ (diese Bedingungen kann ich durch Übergang von α zu $\alpha\gamma^2$ für geeignetes $\gamma \in \boldsymbol{Q}(\sqrt{e})$ erreichen, da $\mathfrak{d}(\alpha) = \mathfrak{d}(\alpha\gamma^2)$). Ich setze

$$\alpha = \frac{U + V\sqrt{e}}{v}$$

mit $U, V \in \boldsymbol{Z}$, $(U, V) = 1$, $v \in \{1, 2\}$, $v = 1$, falls $e \not\equiv 1 \bmod 4$; dann folgt

$$U^2 - eV^2 = \tilde{e}v^2 h^2.$$

α_φ werde ich aus obigem α durch geeignete Normierung erhalten.

Sei $p \in P(\Delta)$ (dann ist p insbesondere voll-zerlegt in $K_\varphi = Q(\sqrt{e}, \sqrt{\tilde{e}})$, und die Primteiler von p in den quadratischen Teilkörpern von K_φ liegen im jeweiligen engeren Hauptgeschlecht); sei $\mathfrak{p}$ ein Primteiler von p in $Q(\sqrt{e})$ und $\pi_\varphi \in Q(\sqrt{e})$ ganz und ohne echten ganzrationalen Teiler mit

$$(\pi_\varphi) = \mathfrak{p}\mathfrak{c}^2,$$

einem ganzen, zu 2Δ primen Ideal $\mathfrak{c}$ von $Q(\sqrt{e})$ und $\mathcal{N}_{Q(\sqrt{e})/Q}(\pi_\varphi) > 0$. Ich setze

$$\pi_\varphi = \frac{M + N\sqrt{e}}{w}$$

mit $M, N \in Z$, $(M, N) = 1$, $w \in \{1, 2\}$, und $w = 1$, falls $e \not\equiv 1 \bmod 4$; dann ist

$$M^2 - eN^2 = w^2 H^2 p$$

mit $H \in N$, $H \equiv 1 \bmod 2$.

Für die Berechnung von $\mathfrak{d}_2(\alpha)$ benutze ich im folgenden stets [15], Lemma 2.

3.1. $e \equiv \tilde{e} \equiv 1 \bmod 4$. Es ist $z_\varphi = 1$, $u_\varphi = \pm 1$, $v = 1$, $\alpha \equiv U + V \bmod 4$, ich normiere α so, daß $\alpha \equiv 1 \bmod 4$, und setze dann $\alpha_\varphi = \alpha$. Es folgt $\mathfrak{d}_2(\alpha_\varphi) = 1$ und

$$\Gamma(\pi_\varphi, \alpha_\varphi) = 1.$$

3.2. $e \equiv 1 \bmod 8$, $\tilde{e} \equiv 3 \bmod 4$. Es ist $z_\varphi = 1$, $u_\varphi = \pm 4$, $v = 1$, $U \equiv 0 \bmod 2$, $V \equiv 1 \bmod 2$, also $\alpha \equiv 1 \bmod 2$ und $\alpha \not\equiv 1 \bmod 4$. Sei $(2) = \mathfrak{z}\mathfrak{z}'$ in $Q(\sqrt{e})$ und $(\alpha - 1) = \mathfrak{z}\mathfrak{z}'^c$ mit $c \geqslant 1$. Aus $\mathcal{N}_{Q(\sqrt{e})/Q}(\alpha - 1) = (U-1)^2 - V^2 e \equiv 0 \bmod 8$ folgt $c \geqslant 2$, also $\mathfrak{d}_2(\alpha) = \mathfrak{z}^2$, $\mathcal{N}\mathfrak{d}_2(\alpha) = 4$. Ich setze $\alpha_\varphi = \alpha$. Aus $\mathcal{N}_{Q(\sqrt{e})/Q}(\pi_\varphi) \equiv 1 \bmod 2$ folgt $w = 1$ und $M + N \equiv 1 \bmod 2$. Zur Berechnung von $\Gamma(\pi_\varphi, \alpha_\varphi) = \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right)$ identifiziere ich $Q(\sqrt{e})_\mathfrak{z}$ mit Q_2 durch Wahl eines $t \in Z_2$ mit $t^2 = e$, $t \equiv 1 \bmod 4$. Auf Grund der Normierung von α_φ ist $U + Vt \equiv 3 \bmod 4$, $U - Vt \equiv 1 \bmod 4$, und aus $\left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right) = \left(\frac{M + Nt, U + Vt}{2}\right)$ folgt

$$\Gamma(\pi_\varphi, \alpha_\varphi) = (-1)^{(M+N-1)/2}.$$

3.3. $e \equiv 5 \bmod 8$, $\tilde{e} \equiv 3 \bmod 4$. Es ist $z_\varphi = 2$, $u_\varphi = \pm 4$, $v = 1$ und wie eben $\alpha \equiv 1 \bmod 2$, $\alpha \not\equiv 1 \bmod 4$. Die prime Restklassengruppe modulo 4 in $Q(\sqrt{e})$ ist vom Typ (3, 2, 2), und Basiselemente werden repräsentiert durch ω, -1 und $\sqrt{e}$, wobei $\omega \not\equiv 1$, $\omega^3 \equiv 1 \bmod 4$ [10]. Daher ist α quadratischer Nichtrest modulo 4, $\mathfrak{d}_2(\alpha) = (2^2)$ und $\mathcal{N}\mathfrak{d}_2(\alpha) = 2^4 = \pm z_\varphi^2 u_\varphi$. Ich setze $\alpha_\varphi = \alpha$. $\theta = \left(\frac{\cdot, \alpha_\varphi}{2}\right)$ ist ein quadratischer Charakter mit Führer 2^2 auf $Q_2(\sqrt{e})^\times$;

da $Q_2(\sqrt{\alpha_\varphi})/Q_2$ nicht galoissch ist, ist θ bei $(\sqrt{e} \to -\sqrt{e})$ nicht invariant. 2 ist Primelement von $Q_2(\sqrt{e})$, also induziert θ einen bei $(\sqrt{e} \to -\sqrt{e})$ nicht invarianten quadratischen Charakter auf der primen Restklassengruppe modulo 4 von $Q(\sqrt{e})$, d.h. $\theta(\omega) = 1$, $\theta(-1) = 1$, und wegen

$$\left(\frac{\sqrt{e}, \alpha_\varphi}{\mathfrak{z}}\right) = -\left(\frac{\sqrt{e}, \alpha'_\varphi}{\mathfrak{z}}\right)$$

kann ich durch Auszeichnung von α_φ vor α'_φ $\theta(\sqrt{e}) = 1$ erreichen. Daraus folgt

$$\Gamma(\pi_\varphi, \alpha_\varphi) = (-1)^{(M+N-1)/2}, \quad \text{falls } w = 1.$$

Im Falle $w = 2$ ist $\pi_\varphi^3 = M' + N'\sqrt{e}$ mit

$$M' = \tfrac{1}{8} M(M^2 + 3N^2 e), \quad N' = \tfrac{1}{8} N(3M^2 + N^2 e),$$

und

$$\Gamma(\pi_\varphi, \alpha_\varphi) = \left(\frac{\pi_\varphi^3, \alpha_\varphi}{\mathfrak{z}}\right) = (-1)^{(M'+N'-1)/2}.$$

3.4. $e \equiv 1 \bmod 4$, $\tilde{e} \equiv 2 \bmod 4$. In diesem Falle ist $z_\varphi = 1$, $u_\varphi = \pm 8$, $v = 2$, und aus $\left(\frac{e, \tilde{e}}{2}\right) = 1$ folgt $e \equiv 1 \bmod 8$, also $(2) = \mathfrak{z}\mathfrak{z}'$ in $Q(\sqrt{e})$. Sei $\mathfrak{z} | \alpha$, $\mathfrak{z}' \nmid \alpha$; dann folgt $\mathfrak{z}^2 \nmid \alpha$, also $\mathfrak{z}^3 | \mathfrak{d}_2(\alpha)$ und $2^3 | \mathcal{N}\mathfrak{d}_2(\alpha)$. Ich normiere nun α so, daß $\alpha \equiv 1 \bmod \mathfrak{z}'^2$, und setze $\alpha_\varphi = \alpha$. Dann folgt $\mathfrak{d}_2(\alpha_\varphi) = \mathfrak{z}^3$, also $\mathcal{N}\mathfrak{d}_2(\alpha_\varphi) = 8$. Zur Berechnung von $\Gamma(\pi_\varphi, \alpha_\varphi) = \left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right)$ identifiziere ich $Q(\sqrt{e})_\mathfrak{z}$ mit Q_2 durch Wahl eines $t \in Z_2$ mit $t^2 = e$, $t \equiv 1 \bmod 4$. Auf Grund der Normierung von α_φ ist $U + Vt \equiv 0 \bmod 4$, $U - Vt \equiv 2 \bmod 8$, und für $Z = (U + Vt)/4$ gilt

$$Z \equiv \frac{U - Vt}{2} \cdot \frac{U + Vt}{4} \bmod 4,$$

also

$$Z \equiv \frac{U^2 - V^2 e}{8} \equiv \frac{\tilde{e}}{2} \bmod 4.$$

Damit folgt

$$\left(\frac{\pi_\varphi, \alpha_\varphi}{\mathfrak{z}}\right) = \left(\frac{M + Nt, 2Z}{2}\right) = \left(\frac{2}{M + Nt}\right) \cdot (-1)^{(M+Nt-1)(z-1)/4},$$

also

$$\Gamma(\pi_\varphi, \alpha_\varphi) = \left(\frac{2}{M+Nt}\right)\cdot(-1)^{(M+N-1)(t-2)/8}$$

mit $t \equiv \frac{1}{2}(e+1) \bmod 8$.

3.5. $e \equiv 3 \bmod 4$. In diesem Falle ist $(2) = \mathfrak{z}^2$ in $Q(\sqrt{e})$, $v = w = 1$, und aus $\left(\frac{e, \tilde{e}}{2}\right) = 1$ folgt $\tilde{e} \not\equiv 3 \bmod 4$. Es sind nun die folgenden Fälle zu unterscheiden:

(a) $V \equiv 0 \bmod 4$: $\tilde{e} \equiv 1 \bmod 8$, $\mathfrak{d}_2(\alpha) = 1$.
(b) $V \equiv 2 \bmod 4$: $\tilde{e} \equiv 5 \bmod 8$, $\mathfrak{d}_2(\alpha) = \mathfrak{z}^2$.
(c) $U \equiv V \equiv 1 \bmod 2$: $\tilde{e} \equiv 2 \bmod 4$, $\mathfrak{d}_2(\alpha) = \mathfrak{z}^5$.
(d) $U \equiv 0$, $V \equiv 1 \bmod 2$: $\tilde{e} \equiv 1 \bmod 4$, $\mathfrak{d}_2(\alpha) = \mathfrak{z}^4$.

In jedem Falle folgt $z_\varphi^2 u_\varphi | \mathcal{N}\mathfrak{d}_2(\alpha)$.

Im Falle $\tilde{e} \equiv 1 \bmod 4$ lehrt 3.2 (unter Vertauschung von e und $\tilde{e}$ und unter Berücksichtigung der Diskriminantenformeln für Diederkörper [9], Satz 24) die Existenz eines $\alpha_\varphi \in Q(\sqrt{e})$, so daß $\mathcal{N}_{Q(\sqrt{e})/Q}(\alpha_\varphi) = \tilde{e}h^2$ mit $h \in Q^\times$ und $\mathfrak{d}_2(\alpha_\varphi) | \mathfrak{z}^2$; ich brauche daher im folgenden den Fall (d) nicht mehr weiter zu betrachten.

In den Fällen (a), (b) und (c) ist $\mathcal{N}\mathfrak{d}_2(\alpha) = \pm z_\varphi^2 u_\varphi$, und $\alpha_\varphi \in \{\pm\alpha, \pm\alpha'\}$ leistet das Gewünschte. Nun noch zur Berechnung von $\Gamma(\pi_\varphi, \alpha_\varphi)$!

3.5a. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 1 \bmod 8$. Wegen $\mathfrak{d}_2(\alpha_\varphi) = 1$ ist auch

$$\Gamma(\pi_\varphi, \alpha_\varphi) = 1.$$

3.5b. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 5 \bmod 8$. Wegen $\mathfrak{d}_2(\alpha_\varphi) = \mathfrak{z}^2$ ist $\theta = \left(\frac{\cdot, \alpha_\varphi}{\mathfrak{z}}\right)$ ein quadratischer Charakter auf der primen Restklassengruppe modulo $\mathfrak{z}^2$ von $Q(\sqrt{e})$, welche von der Restklasse von $\sqrt{e}$ erzeugt wird; daraus folgt:

$$\Gamma(\pi_\varphi, \alpha_\varphi) = (-1)^N.$$

3.5c. $e \equiv 3 \bmod 4$, $\tilde{e} \equiv 2 \bmod 4$. Wegen $\mathfrak{d}_2(\alpha_\varphi) = \mathfrak{z}^5$ ist $\theta = \left(\frac{\cdot, \alpha_\varphi}{\mathfrak{z}}\right)$ ein quadratischer Charakter auf der primen Restklassengruppe modulo $\mathfrak{z}^5$ von $Q(\sqrt{e})$. Zu dessen Berechnung (als Normrestsymbol der Erweiterung $Q(\sqrt{\alpha_\varphi})/Q(\sqrt{e})$) normiere ich α_φ durch $U \equiv V \equiv 1 \bmod 4$ und erhalte die folgenden Charakterwerte $\theta(\xi)$ auf den Repräsentanten ξ der Basiselemente der primen Restklassengruppen modulo $\mathfrak{z}^5$ [10]:

$e \equiv 3 \bmod 8$	$\xi = -1$	$\xi = \sqrt{e}$	$\xi = -1+2\sqrt{e}$
$U \equiv V \bmod 8$	-1	-1	1
$U \not\equiv V \bmod 8$	-1	1	1

$e \equiv -1 \bmod 8$	$\xi = \sqrt{e}$	$\xi = 5$	$\xi = -1+2\sqrt{e}$
$U \equiv V \bmod 8$	1	-1	1
$U \not\equiv V \bmod 8$	-1	-1	1

Genau dann ist $U \equiv V \bmod 8$, wenn $e+\tilde{e} \equiv 1 \bmod 16$ (wegen $\left(\frac{e, \tilde{e}}{2}\right) = 1$ ist stets $e+\tilde{e} \equiv 1 \bmod 8$). Aus $p \in P(\Delta) \subset P(64e\tilde{e})$ folgt $p \equiv M^2 - eN^2 \equiv 1 \bmod 8$, und damit erhält man die gesuchten Charakterwerte in den einzelnen Fällen:

$$\Gamma(\pi_\varphi, \alpha_\varphi) = \begin{cases} (-1)^{(e+\tilde{e}-1)/8}\cdot\left(\frac{2s}{M+N}\right), & \text{falls } M \equiv 0 \bmod 2, \\ \left(\frac{2s}{M+N}\right), & \text{falls } M \equiv 1 \bmod 2 \end{cases}$$

mit

$$s = \begin{cases} 1, & \text{falls } e \equiv -1 \bmod 8, \\ -1, & \text{falls } e \equiv 3 \bmod 8. \end{cases}$$

3.6. $e \equiv 2 \bmod 4$, $\tilde{e} \equiv 1 \bmod 4$. Wegen $\left(\frac{e, \tilde{e}}{2}\right) = 1$ ist $\tilde{e} \equiv 1 \bmod 8$, und aus $u_\varphi = \pm 1$, $z_\varphi = 1$ folgt $z_\varphi^2 u_\varphi | \mathcal{N}\mathfrak{d}_2(\alpha)$. Die Überlegungen aus 3.4 (unter Vertauschung von e und $\tilde{e}$ und unter Beachtung der Diskriminantenformeln für Diederkörper) lehren, daß man α_φ so wählen kann, daß $\mathfrak{d}_2(\alpha_\varphi) = 1$, also $\mathcal{N}\mathfrak{d}_2(\alpha_\varphi) = \pm z_\varphi^2 u_\varphi$, und damit folgt

$$\Gamma(\pi_\varphi, \alpha_\varphi) = 1.$$

3.7. $e \equiv 2 \bmod 4$, $\tilde{e} \equiv 3 \bmod 4$. Es ist $u_\varphi = \pm 4$, $z_\varphi = 2$, und in $Q(\sqrt{e})$ ist $(2) = \mathfrak{z}^2$; aus $\tilde{e} \equiv 3 \equiv U^2 - 2V^2 \bmod 4$ folgt $U \equiv V \equiv 1 \bmod 2$, $\alpha \equiv 1 + \sqrt{e} \bmod \mathfrak{z}^2$, also ist α quadratischer Nichtrest modulo $\mathfrak{z}^2$, $\mathfrak{d}_2(\alpha) = \mathfrak{z}^4$, und ich setze $\alpha_\varphi = \alpha$. Aus $p \in P(\Delta)$ folgt $p \equiv M^2 + 2N^2 \equiv 1 \bmod 8$, also $M \equiv 1$, $N \equiv 0 \bmod 2$. $\theta = \left(\frac{\cdot, \alpha_\varphi}{\mathfrak{z}}\right)$ ist ein quadratischer Charakter auf $Q(\sqrt{e})_\mathfrak{z}^\times$ mit Führer $\mathfrak{z}^4$, also gilt $\theta(-1) = -1$. Da -1 und $1+\sqrt{e}$ eine Basis der primen Restklassengruppe modulo $\mathfrak{z}^4$ in $Q(\sqrt{e})$ repräsentieren [10], folgt

$$\Gamma(\pi_\varphi, \alpha_\varphi) = (-1)^{(M+N-1)/2}.$$

3.8. $e \equiv \tilde{e} \equiv 2 \bmod 4$. Es ist $u_\varphi = \pm 8$, $z_\varphi = 2$, und in $Q(\sqrt{e})$ ist $(2) = \mathfrak{z}^2$; aus $\tilde{e} \equiv U^2 - eV^2 \bmod 8$ folgt $U \equiv 0$, $V \equiv 1 \bmod 2$, also $\mathfrak{z} | \alpha$, $\mathfrak{z}^2 \nmid \alpha$ und daher

$\mathfrak{d}_2(\alpha) = \mathfrak{z}^5$, $\mathcal{N}\mathfrak{d}_2(\alpha) = \pm z_\varphi^2 u_\varphi$. Ich setze $\alpha_\varphi = \alpha$. Genau dann ist $e \equiv \tilde{e} \bmod 8$, wenn $U \equiv 2 \bmod 4$. Aus $p \in \boldsymbol{P}(\Delta)$ folgt $p \equiv M^2 + 2N^2 \equiv 1 \bmod 8$, also $M \equiv 1$, $N \equiv 0 \bmod 2$. $\theta = \left(\frac{\cdot, \alpha_\varphi}{\mathfrak{z}}\right)$ ist ein quadratischer Charakter auf $\boldsymbol{Q}(\sqrt{e})_{\mathfrak{z}}^{\times}$ mit Führer $\mathfrak{z}^5$, also folgt $\theta(5) = -1$, und die Berechnung von θ als Normrestsymbol für $\boldsymbol{Q}(\sqrt{\alpha_\varphi})/\boldsymbol{Q}(\sqrt{e})$ liefert:

$$\theta(-1) = \begin{cases} 1, & \text{falls } \tilde{e} \equiv 2 \bmod 8, \\ -1, & \text{falls } \tilde{e} \equiv -2 \bmod 8. \end{cases}$$

Daraus folgt nun

$$\Gamma(\pi_\varphi, \alpha_\varphi) = \begin{cases} \left(\frac{2\varepsilon}{|M|}\right), & \text{falls } N \equiv 0 \bmod 4, \\ \left(\frac{2\varepsilon}{3|M|}\right), & \text{falls } N \equiv 2 \bmod 4 \end{cases}$$

mit

$$\varepsilon = \begin{cases} 1, & \text{falls } e \equiv 2 \bmod 8, \\ -1, & \text{falls } e \equiv -2 \bmod 8. \end{cases}$$

4. Darstellung von Primzahlen durch ambige Formen im Hauptgeschlecht (Beispiele). Ich gebe nun eine Reihe von Anwendungen der entwickelten Theorie und der abgeleiteten expliziten Formeln auf die Darstellung von Primzahlen durch konkrete binäre quadratische Formen, insbesondere für den Fall ambiger Formen im Hauptgeschlecht. Die behandelten Beispiele haben dabei exemplarischen und nicht enzyklopädischen Charakter. Eine Reihe von Einzelresultaten der neueren Literatur wird verallgemeinert und im Rahmen der dargestellten Theorie neu bewiesen. Die in den ersten Abschnitten eingeführten Bezeichnungen werden auch im Beispielteil beibehalten.

4a. Der Charakter $\left(\frac{-1}{\cdot}\right)$ und das rationale biquadratische Reziprozitätsgesetz. Sei $m \in N$ quadratfrei, $m \geqslant 2$ und $m = U^2 + V^2$ mit $U, V \in N$, $U \equiv 1 \bmod 2$. Ich setze

$$m^* = \begin{cases} m, & \text{falls } m \equiv 1 \bmod 4, \\ m/2, & \text{falls } m \equiv 2 \bmod 4 \end{cases}$$

und

$$\Delta = \begin{cases} -4m, & \text{falls } m \equiv 1 \bmod 8, \\ -16m, & \text{falls } m \equiv 5 \bmod 8, \\ -64m, & \text{falls } m \equiv 2 \bmod 4. \end{cases}$$

Dann ist $\varphi\colon \mathscr{C}(\Delta) \to \{\pm 1\}$, definiert durch $\varphi(Q) = \left(\frac{-1}{\varkappa}\right)$ für $Q \in \mathscr{C}(\Delta)$, $\varkappa \in N$ mit $Q \to \varkappa$ und $(\varkappa, \Delta) = 1$, ein Geschlechtscharakter von $\mathscr{C}(\Delta)$, und nach Proposition 4 ist

$$\varphi \in \mathscr{X}(\Delta), \qquad \{e_\varphi, \tilde{e}_\varphi\} = \{-1, m\}.$$

Sei $\varepsilon(m) \in \boldsymbol{Q}(\sqrt{m})$ ganz und ohne echten ganzrationalen Teiler, so daß

$$\mathcal{N}_{\boldsymbol{Q}(\sqrt{m})/\boldsymbol{Q}}(\varepsilon(m)) = -h^2$$

mit $h \in N$, $(h, 2m) = 1$. Setzt man $e_\varphi = m$, so zeigen die Rechnungen von § 3, daß man $\alpha_\varphi = \varepsilon(m)$ oder $\alpha_\varphi = -\varepsilon(m)$ wählen kann. Für $p \in \boldsymbol{P}(\Delta)$ ist $p \equiv 1 \bmod 4$, also in jedem Falle

$$\sigma_\varphi(p) = \left(\frac{\alpha_\varphi}{p}\right) = \left(\frac{\varepsilon(m)}{p}\right)$$

(Legendre-Symbol nach fester Wahl von $\sqrt{m}$ modulo p). Bei Wahl von $e_\varphi = -1$ zeigen die Rechnungen von 3.5, daß man $\alpha_\varphi = U + V\sqrt{-1}$ wählen kann, und für $p \in \boldsymbol{P}(\Delta)$,

$$p = M^2 + N^2 \quad \text{mit } M, N \in \boldsymbol{Z},\ N \equiv 0 \bmod 2,$$

folgt aus den Propositionen 2 und 3:

$$\sigma_\varphi(p) = \left(\frac{U + V\sqrt{-1}}{p}\right) = \left(\frac{M + N\sqrt{-1}}{m^*}\right) \cdot \Gamma_2 = \left(\frac{M + \sqrt{p}}{m^*}\right) \cdot \left(\frac{2}{m^*}\right) \cdot \Gamma_2$$

mit

$$\Gamma_2 = \begin{cases} 1, & \text{falls } m \equiv 1 \bmod 4, \\ \left(\frac{2}{M+N}\right), & \text{falls } m \equiv 2 \bmod 4. \end{cases}$$

Aus dem Vergleich der beiden Formeln für $\sigma_\varphi(p)$ erhält man

$$\left(\frac{\varepsilon(m)}{p}\right) = \left(\frac{U + V\sqrt{-1}}{p}\right),$$

und daraus folgt unmittelbar:

Satz 1. *Seien $m, m_1, \ldots, m_d \in N$ quadratfreie Zahlen, $m \geqslant 2$, $m_i \geqslant 2$, und seien $m, m_1, \ldots, m_d$ Summe zweier Quadrate. Sei $\boldsymbol{Q}(\sqrt{m}) = \boldsymbol{Q}(\sqrt{m_1 \cdot \ldots \cdot m_d})$, seien $\varepsilon(m) \in \boldsymbol{Q}(\sqrt{m})$, $\varepsilon(m_i) \in \boldsymbol{Q}(\sqrt{m_i})$ mit $\mathcal{N}\varepsilon(m) = -h^2$, $\mathcal{N}\varepsilon(m_i) = -h_i^2$ mit $h, h_i \in N$, $(h, 2m) = (h_i, 2m_i) = 1$. Sei $p \in \boldsymbol{P}$ mit $\left(\frac{-1}{p}\right) = \left(\frac{\pi}{p}\right) = 1$ für alle Prim-*

teiler π *von* $m_1 \cdot \ldots \cdot m_d$. *Dann folgt*

$$\left(\frac{\varepsilon(m)}{p}\right) = \prod_{i=1}^{d} \left(\frac{\varepsilon(m_i)}{p}\right).$$

Spezialfälle von Satz 1 findet man in [34] und [7].

Bevor ich nun die Anwendungen auf binäre quadratische Formen studiere, ziehe ich noch weitere Folgerungen aus dem Vergleich der verschiedenen Formeln für $\sigma_\varphi(p)$. Ich setze dazu

$$\varepsilon(m) = R + S\sqrt{m}$$

mit $R, S \in \boldsymbol{Z}$, also $R^2 - S^2 m = -h^2$ wie oben, und

$$m^* = U^{*2} + V^{*2}$$

mit $U^*, V^* \in N$, $U^* \equiv 1 \bmod 2$. Sei $h' \in \boldsymbol{Z}$ mit $hh' \equiv 1 \bmod m^*$; dann folgt

$$\left(\frac{M + N\sqrt{-1}}{m^*}\right) = \left(\frac{M + NRh'}{m^*}\right) = \left(\frac{MU^* \pm NV^*}{m^*}\right),$$

da $Rh'U^* \equiv \pm V^* \bmod m^*$ und $\left(\frac{U^*}{m^*}\right) = \left(\frac{m^*}{U^*}\right) = 1$ (auf das Vorzeichen kommt es in obigem Legendre-Symbol nicht an!). Damit ist bewiesen:

Satz 2. *Sei* $m \in N$ *quadratfrei,* $m \geqslant 2$, $m = U^2 + V^2$ *mit* $U, V \in N$, $U \equiv 1 \bmod 2$. *Im Falle* $m \equiv 2 \bmod 4$ *sei* $m^* = m/2 = U^{*2} + V^{*2}$ *mit* $U^*, V^* \in N$, $U^* \equiv 1 \bmod 2$. *Sei* p *eine Primzahl mit*

$$\left(\frac{-1}{p}\right) = \left(\frac{\pi}{p}\right) = 1$$

für alle Primteiler π *von* m, *und sei*

$$p = M^2 + N^2 \quad \text{mit } M, N \in N,\ N \equiv 0 \bmod 2.$$

Sei $\varepsilon(m) \in \boldsymbol{Q}(\sqrt{m})$ *ganz und ohne echten ganzrationalen Teiler, so daß* $N_{\boldsymbol{Q}(\sqrt{m})/\boldsymbol{Q}}(\varepsilon(m)) = -h^2$ *mit* $h \in N$, $(h, 2m) = 1$. *Dann folgt*

$$\left(\frac{\varepsilon(m)}{p}\right) = \begin{cases} \left(\frac{MU + NV}{m}\right), & \text{falls } m \equiv 1 \bmod 4, \\ \left(\frac{MU^* + NV^*}{m^*}\right)\cdot\left(\frac{2}{M+N}\right), & \text{falls } m \equiv 2 \bmod 4. \end{cases}$$

Spezialfälle von Satz 2 stehen in [23]; der Fall $m = 2$ liefert

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{2}{M+N}\right)$$

(siehe [1] und [34]).

Ist $m = q$ eine Primzahl, so gilt nach [33] (vgl. auch [24]):

$$\left(\frac{\varepsilon(q)}{p}\right) = \left(\frac{p}{q}\right)_4 \cdot \left(\frac{q}{p}\right)_4;$$

anderseits ist nach Satz 2

$$\left(\frac{\varepsilon(q)}{p}\right) = \left(\frac{MU + NV}{q}\right)$$

($p = M^2 + N^2$, $q = U^2 + V^2$). Der Vergleich der beiden Formeln liefert einen Beweis des rationalen biquadratischen Reziprozitätsgesetzes von K. Burde [4] (für einen Beweis mit indefiniten binären Formen siehe [19] und [6]).

Ich gebe hier einen weiteren Beweis des rationalen biquadratischen Reziprozitätsgesetzes, indem ich die Formel

$$\sigma_\varphi(p) = \left(\frac{p}{q}\right)_4 \cdot \left(\frac{q}{p}\right)_4$$

direkt nachrechne. Nach Korollar 2 zum Theorem in § 1 genügt es, zu zeigen:

Ist

$$I = \begin{cases} [1, 0, q], & \text{falls } q \equiv 1 \bmod 8, \\ [1, 0, 4q], & \text{falls } q \equiv 5 \bmod 8 \end{cases}$$

die Hauptklasse von $\mathscr{C}(-4q)$ bzw. $\mathscr{C}(-16q)$ und $\varkappa \in N$ mit $I \to \varkappa^2 p$, so folgt

$$\left(\frac{q}{\varkappa}\right) = \left(\frac{p}{q}\right)_4 \cdot \left(\frac{q}{p}\right)_4.$$

Es gilt allgemeiner:

Satz 3. *Seien* $m, P \in N$, $m \equiv P \equiv 1 \bmod 4$, $(m, P) = 1$, *und sei*

$$\varkappa^2 P = x^2 + kmy^2$$

mit $\varkappa \in N$, $(\varkappa, 2mP) = 1$, $x, y \in N$, $(x, y) = 1$ *und* $k \in \{1, 2\}$. *Dann folgt*

$$\left(\frac{km}{P}\right)_4 \cdot \left(\frac{P}{km}\right)_4 = \begin{cases} \left(\frac{-1}{\varkappa}\right)\cdot\left(\frac{2}{m}\right)^y, & \text{falls } k = 1, \\ \left(\frac{-1}{\varkappa}\right)\cdot(-1)^{y/2}, & \text{falls } k = 2. \end{cases}$$

Für den Fall $m, P \in \boldsymbol{P}$ stehen die Aussagen von Satz 3 in [18], § 13; die dort gegebenen (elementaren, nur das quadratische Reziprozitätsgesetz benutzenden) Beweise behalten auch im allgemeinen Fall Gültigkeit, so daß ich hier auf deren Wiederholung verzichten kann.

Ich komme nun zur Anwendung der hergeleiteten Formeln für $\sigma_\varphi(p)$ auf

die Darstellung von Primzahlen durch binäre quadratische Formen. Um aus den nachstehend formulierten Darstellungskriterien die in der Literatur aufscheinenden zu folgern, hat man lediglich die verschiedenen oben angeführten Formeln für $\sigma_\varphi(p)$ einzutragen.

Fall 1: $m \equiv 1 \bmod 8$, $\Delta = -4m$: $I = [1, 0, m] \in \mathscr{C}(\Delta)$ ist die Hauptklasse, und für $\varkappa \in N$, $(\varkappa, 2m) = 1$ und $p \in P(-4m)$ gilt:

$$\text{Aus } I \to \varkappa^2 p \text{ folgt } \left(\frac{-1}{\varkappa}\right) = \sigma_\varphi(p).$$

Ich betrachte nun die Form

$$A = \left[2, 2, \frac{1+m}{2}\right] \in \mathscr{C}(-4m).$$

Genau dann ist $A \in \mathscr{C}(-4m)^2$, wenn m nur Primteiler $q \equiv 1 \bmod 8$ besitzt; in diesem Falle ist $m = 2f^2 - g^2$ mit $f, g \in N$ und $A = A_0^2$ mit $A_0 = [f, 2g, 2f]$ und

$$\varphi(A_0) = \left(\frac{-1}{f}\right) = \left(\frac{2}{m}\right)_4 \cdot \left(\frac{m}{2}\right)_4$$

(siehe [18], Théorème 2). Für $\varkappa \in N$ mit $(\varkappa, 2m) = 1$ und $p \in P(-4m)$ gilt:

$$\text{Aus } A \to \varkappa^2 p \text{ folgt } \left(\frac{-1}{\varkappa}\right) \cdot \left(\frac{2}{m}\right)_4 \cdot \left(\frac{m}{2}\right)_4 = \sigma_\varphi(p).$$

Man beachte noch, daß genau dann $A \to \varkappa^2 p$ gilt, wenn $I \to 2\varkappa^2 p$.

Sei nun $m = q$ eine Primzahl. Dann hat $\mathscr{C}(-4q)$ eine zyklische 2-Komponente, $\# \mathscr{C}(-4q) = 4s$, und $2 | s$ genau dann, wenn $\left(\frac{2}{q}\right)_4 \cdot \left(\frac{q}{2}\right)_4 = 1$ [19]; φ ist der einzige Geschlechtscharakter von $\mathscr{C}(-4q)$, und für $p \in P(-4q)$ $\left(\text{d.h. } \left(\frac{-1}{p}\right) = \left(\frac{q}{p}\right) = 1\right)$ und $Q \in \mathscr{C}(-4q)$ mit $Q \to p$ gilt:

$$Q \in \mathscr{C}(-4q)^4 \text{ genau dann, wenn } \sigma_\varphi(p) = 1$$

(vgl. [20]; [22], Theorem 1); ferner gilt:

$$I \to p^s \text{ genau dann, wenn } \sigma_\varphi(p) = 1$$

(vgl. [14], Potenzrestkriterium 10).

Für eine beliebige Klasse $C = [k, m, n] \in \mathscr{C}(-4q)^2$ mit $q = kf^2 - g^2$ $(f, g \in N)$ ist $C = [f, 2g, kf]^2$, und für eine Primzahl p mit $C \to p$ folgt $\sigma_\varphi(p) = \left(\frac{-1}{f}\right) = \left(\frac{f}{q}\right)$ und damit die allgemeine Form des rationalen biquadratischen Reziprozitätsgesetzes von E. Brown [2].

Fall 2: $m \equiv 5 \bmod 8$, $\Delta = -16m$. $I = [1, 0, 4m]$ und $A = [4, 0, m]$ liegen im Hauptgeschlecht von $\mathscr{C}(\Delta)$, und ich zeige zunächst $A = A_0^2$ mit $A_0 = [(1+m)/2, 4, 8]$. Dazu betrachte ich den kanonischen Epimorphismus θ: $\mathscr{C}(-16m) \to \mathscr{C}(-4m)$, definiert durch $\theta([a, 2b, 4c]) = [a, b, c]$ mit $\operatorname{Kern}(\theta) = \{I, A\}$. Wegen $\theta(A_0) = [(1+m)/2, 2, 2]$ ist $A_0^2 \in \{I, A\}$, und aus $\left(\frac{1+m}{2}\right)^2 = 4 \cdot \left(\frac{1-m}{2}\right)^2 + m \cdot 1^2$ folgt $A_0^2 = A$. Wegen $(1+m)/2 \equiv 3 \bmod 4$ ist $\varphi(A_0) = -1$, und daher gilt:

Für $p \in P(\Delta)$, $\varkappa \in N$ mit $(\varkappa, 2m) = 1$ und $\varkappa^2 p = x^2 + my^2$ mit $x, y \in Z$, $(x, y) = 1$, folgt

$$\left(\frac{-1}{\varkappa}\right) \cdot (-1)^y = \sigma_\varphi(p)$$

(vgl. auch Satz 3). Ist insbesondere $m = q$ eine Primzahl, so folgt $\# \mathscr{C}(-16q) = 4s$ mit $s \equiv 1 \bmod 2$, und für $p \in P(\Delta)$ (d. h. $\left(\frac{-1}{p}\right) = \left(\frac{q}{p}\right) = 1$) folgt

$$p^s = x^2 + qy^2, \quad (-1)^y = \sigma_\varphi(p)$$

mit $x, y \in Z$, $(x, y) = 1$ (siehe [20], [3]; im Spezialfall $q = 5$ folgt [29], Theorem 1).

Fall 3: $m \equiv 2 \bmod 4$, $\Delta = -64m$. Ich setze $m = 2m^*$ und betrachte die vier Klassen

$$I = [1, 0, 32m^*], \qquad A = [32, 0, m^*],$$
$$B = [4, 4, 1+8m^*], \qquad AB = [32, 32, 8+m^*],$$

welche eine Untergruppe vom Typ (2, 2) von $\mathscr{C}(\Delta)$ bilden.

Wegen $B \to (1+2m^*)^2$ ist $B = B_0^2$ mit $B_0 \in \mathscr{C}(\Delta)$, so daß $B_0 \to 1+2m^* \equiv 3 \bmod 4$, also

$$\varphi(B_0) = -1.$$

Sei $p \in P(\Delta)$ und $\varkappa \in N$ mit $(m, \varkappa) = 1$, so daß

$$\varkappa^2 p = x^2 + 8m^* y^2$$

mit $x, y \in Z$, $(x, y) = 1$. Dann gilt:

$$I \to \varkappa^2 p, \quad \text{falls } y \equiv 0 \bmod 2,$$
$$B \to \varkappa^2 p, \quad \text{falls } y \equiv 1 \bmod 2,$$

also

$$\sigma_\varphi(p) = \left(\frac{-1}{\varkappa}\right) \cdot (-1)^y.$$

Genau dann ist $A \in \mathcal{C}(\Delta)^2$, wenn m^* nur Primteiler $q \equiv 1 \bmod 8$ besitzt; ist dann $m^* = f^2 - 2g^2$ mit $f, g \in N$, $g \equiv 0 \bmod 4$, so folgt $A = A_0^2$ mit $A_0 = [f, 16g, 32f]$, also

$$\varphi(A_0) = \left(\frac{-1}{f}\right) = \left(\frac{2}{m^*}\right)_4 \cdot \left(\frac{m^*}{2}\right)_4$$

nach [18], Théorème 2.

Sei nun wieder $p \in \boldsymbol{P}(\Delta)$ und $\varkappa \in \boldsymbol{N}$ mit $(m, \varkappa) = 1$, so daß

$$\varkappa^2 p = 8x^2 + m^* y^2$$

mit $x, y \in \boldsymbol{Z}$, $(x, y) = 1$. Dann gilt:

$$A \to \varkappa^2 p, \quad \text{falls } x \equiv 0 \bmod 2,$$

$$AB \to \varkappa^2 p, \quad \text{falls } x \equiv 1 \bmod 2,$$

also

$$\sigma_\varphi(p) = \left(\frac{-1}{\varkappa}\right) \cdot (-1)^y \cdot \left(\frac{2}{m^*}\right)_4 \cdot \left(\frac{m^*}{2}\right)_4.$$

Ist speziell $m^* = q$ eine Primzahl, $q \equiv 1 \bmod 8$, so ist die 2-Komponente von $\mathcal{C}(-128q)$ vom Typ $(2^\tau, 4)$ mit $\tau \geqslant 2$, und es ist $\tau > 2$ genau dann, wenn $\left(\frac{2}{q}\right)_4 = 1$ [19]. Dann folgen [25], Case 1.3, [28], Theorem 1, und unter Benutzung von Satz 1 folgt auch [28], Theorem 2.

4b. Der Fall $\Delta = 4PP'$ mit $P \equiv 1 \bmod 8$, $P' \equiv 3 \bmod 4$ und $\varphi = \left(\frac{P}{\cdot}\right)$.

Seien $P, P' \in \boldsymbol{Z} \setminus \{0, 1\}$ quadratfrei, $(P, P') = 1$, $P \equiv 1 \bmod 8$, $P' \equiv 3 \bmod 4$, $\left(\frac{P, P'}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$ und

$$\Delta = 4PP'.$$

Dann ist $\varphi\colon \mathcal{C}(\Delta) \to \{\pm 1\}$, definiert durch $\varphi(Q) = \left(\frac{P}{\varkappa}\right) = \left(\frac{P'}{\varkappa}\right)$ für $Q \in \mathcal{C}(\Delta)$, $\varkappa \in N$ mit $(\varkappa, \Delta) = 1$ und $Q \to \varkappa$, ein Geschlechtscharakter von $\mathcal{C}(\Delta)$, und nach Proposition 4 ist $\varphi \in \mathcal{X}(\Delta)$. Es ist $\{e_\varphi, \tilde{e}_\varphi\} = \{P, 4P'\}$, und man erhält aus dem Zusatz zu Proposition 3 und aus 3.2 bzw. 3.5a die folgenden Formeln für $\sigma_\varphi(p)$:

(a) $e = P$, $\tilde{e} = P'$: Sei $p \in \boldsymbol{P}(\Delta)$, $M^2 - PN^2 = H^2 p$ mit $H \in N$, $H \equiv 1 \bmod 2$, $M, N \in \boldsymbol{N}$, $(M, N) = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M + N\sqrt{P}}{|P'|}\right) \cdot \Gamma_2 = \left(\frac{M + H\sqrt{p}}{|P'|}\right)\left(\frac{2}{|P'|}\right) \cdot \Gamma_2$$

mit

$$\Gamma_2 = (-1)^{(M+N-1)/2}.$$

(b) $e = P'$, $\tilde{e} = P$: Sei $p \in \boldsymbol{P}(\Delta)$, $M'^2 - P'N'^2 = H'^2 p$ mit $H' \in N$, $H' \equiv 1 \bmod 2$, $M', N' \in N$, $(M', N') = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M' + N'\sqrt{P'}}{|P|}\right) = \left(\frac{M' + H'\sqrt{p}}{|P|}\right).$$

Ich betrachte die Klassen

$$I = [1, 0, -PP'], \quad A = [2, 2, (1 - PP')/2]$$

und im Falle $P > 0$ außerdem noch

$$B = [P, 0, -P'], \quad AB = [2P, 2P, (P - P')/2].$$

Genau dann ist $A \in \mathcal{C}(\Delta)^2$, wenn PP' nur Primteiler $q \equiv \pm 1 \bmod 8$ besitzt; dann ist $-PP' = 2f'^2 - g^2$ mit $f, g \in N$, $A = A_0^2$, wobei $A_0 = [f, 2g, 2f']$ und $\varphi(A_0) = \left(\frac{P}{f}\right)$.

Im Falle $P > 0$ ist genau dann $B \in \mathcal{C}(\Delta)^2$, wenn P nur Primteiler $q \equiv 1 \bmod 4$ besitzt; dann ist $B = B_0^2$ und $\varphi(B_0) = \left(\frac{P'}{P}\right)_4$ (Beweis wie [18], Lemme 1).

Seien im folgenden $P = t$ und $-P' = t'$ Primzahlen. Dann erhält man aus § 1, Korollar 2 und obigen Formeln für $\sigma_\varphi(p)$ zunächst die Aussagen von [29], Theorem 5 (für $q \equiv 1 \bmod 4$, $r \equiv 1 \bmod 8$) sowie eine Reihe damit verwandter Resultate. Darüber hinaus verdient der Fall

$$t \equiv t' \equiv 1 \bmod 8$$

besondere Beachtung; in diesem Fall ist nämlich die 2-Komponente von $\mathcal{C}(\Delta)$ vom Typ $(2^\tau, 2^{\tau'})$ mit $\tau, \tau' \geqslant 2$, und es gibt genau einen von φ verschiedenen Geschlechtscharakter von $\mathcal{C}(\Delta)$, nämlich φ', definiert durch

$$\varphi'(Q) = \left(\frac{-1}{\varkappa}\right) \quad \text{für } Q \in \mathcal{C}(\Delta), \varkappa \in N$$

mit $(\varkappa, \Delta) = 1$ und $Q \to \varkappa$ (dieser wurde in § 4a eingehend untersucht). Ich betrachte insbesondere den Fall $\tau = \tau' = 2$ (siehe [18], Prop. C_1, für notwendige und hinreichende Bedingungen) und setze $\#\mathcal{C}(\Delta) = 16s$ mit $s \equiv 1 \bmod 2$. Dann ist $\mathcal{X}(\Delta) = \langle \varphi, \varphi' \rangle$ und $\mathcal{C}(\Delta)^{2s} = \{I, A, B, AB\}$ mit $I = [1, 0, tt']$, $A = [2, 2, (1 + tt')/2]$, $B = [t, 0, t']$ und $AB = [2t, 2t, (t + t')/2]$; sind $A_0, B_0 \in \mathcal{C}(\Delta)$ mit $A_0^2 = A$, $B_0^2 = B$, und ist $tt' = 2f^2 - g^2$ mit $f, g \in N$, so

folgt

$$\varphi(A_0) = \left(\frac{t}{f}\right), \quad \varphi(B_0) = \left(\frac{t'}{t}\right)_4$$

wie oben und

$$\varphi'(A_0) = \left(\frac{-1}{f}\right), \quad \varphi'(B_0) = \left(\frac{t}{t'}\right)_4 \cdot \left(\frac{t'}{t}\right)_4$$

nach [18], p. 349. Sei nun p eine Primzahl mit $\left(\frac{-1}{p}\right) = \left(\frac{t}{p}\right) = \left(\frac{t'}{p}\right) = 1$ (also $p \in \boldsymbol{P}(\Delta)$); dann folgt $Q \to p^s$ für genau ein $Q \in \{I, A, B, AB\}$; ist $Q = Q_0^2$, so folgt aus dem Theorem in § 1

$$\varphi(Q_0) = \sigma_\varphi(p), \quad \varphi'(Q_0) = \sigma_{\varphi'}(p).$$

Die Formeln für $\sigma_\varphi(p)$ sind oben angegeben. $\sigma_{\varphi'}(p)$ berechnet man nach § 4a wie folgt: Sei $p = m^2 + n^2$ mit $m, n \in N$, $n \equiv 0 \bmod 2$ und $tt' = U^2 + V^2$ mit $U, V \in N$, $V \equiv 0 \bmod 2$; dann ist

$$\sigma_{\varphi'}(p) = \left(\frac{U + V\sqrt{-1}}{p}\right) = \left(\frac{m + n\sqrt{-1}}{tt'}\right) = \left(\frac{m + \sqrt{p}}{tt'}\right) = \left(\frac{\varepsilon(tt')}{p}\right)$$

mit $\varepsilon(tt') \in \boldsymbol{Q}(\sqrt{tt'})$, so daß $N_{\boldsymbol{Q}(\sqrt{tt'})/\boldsymbol{Q}}(\varepsilon(tt')) = -h^2$, $h \in N$, $(h, p) = 1$.

Damit erhält man nun das folgende explizite Kriterium:

$I \to p^s$ genau dann, wenn $\sigma_\varphi(p) = \sigma_{\varphi'}(p) = 1$;

$A \to p^s$ genau dann, wenn $\sigma_\varphi(p) = \left(\frac{t}{f}\right)$, $\sigma_{\varphi'}(p) = \left(\frac{-1}{f}\right)$;

$B \to p^s$ genau dann, wenn $\sigma_\varphi(p) = \left(\frac{t'}{t}\right)_4$, $\sigma_{\varphi'}(p) = \left(\frac{t}{t'}\right)_4 \cdot \left(\frac{t'}{t}\right)_4$;

$AB \to p^s$ sonst.

4c. Der Fall $\Delta = 16PP'$ mit $P \equiv 5 \bmod 8$, $P' \equiv 3 \bmod 4$ und $\varphi = \left(\frac{P}{\cdot}\right)$. Seien $P, P' \in Z \setminus \{0, 1\}$ quadratfrei, $(P, P') = 1$, $P \equiv 5 \bmod 8$, $P' \equiv 3 \bmod 4$, $\left(\frac{P, P'}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$ und $\Delta = 16PP'$.

Dann ist φ: $\mathscr{C}(\Delta) \to \{\pm 1\}$, definiert durch

$$\varphi(Q) = \left(\frac{P}{\varkappa}\right) = \left(\frac{P'}{\varkappa}\right) \quad \text{für } Q \in \mathscr{C}(\Delta), \varkappa \in N$$

mit $(\varkappa, \Delta) = 1$ und $Q \to \varkappa$, ein Geschlechtscharakter von $\mathscr{C}(\Delta)$, und nach Proposition 4 ist $\varphi \in \mathscr{X}(\Delta)$. Es ist $\{e_\varphi, \tilde{e}_\varphi\} = \{P, 4P'\}$, und man erhält aus

dem Zusatz zu Proposition 3 und aus 3.3 bzw. 3.5b die folgenden Formeln für $\sigma_\varphi(p)$:

(a) $e = P$, $\tilde{e} = P'$: Sei $p \in \boldsymbol{P}(\Delta)$, $M^2 - PN^2 = H^2 p$ mit $H \in N$, $H \equiv 1 \bmod 2$, $M, N \in N$, $(M, N) = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M + N\sqrt{P}}{|P'|}\right) \cdot \Gamma_2 = \left(\frac{M + H\sqrt{p}}{|P'|}\right) \cdot \left(\frac{2}{|P'|}\right) \cdot \Gamma_2$$

mit

$$\Gamma_2 = (-1)^{(M+N-1)/2}.$$

(b) $e = P'$, $\tilde{e} = P$: Sei $p \in \boldsymbol{P}(\Delta)$, $M'^2 - P'N'^2 = H'^2 p$ mit $H' \in N$, $H' \equiv 1 \bmod 2$, $M', N' \in N$, $(M', N') = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M' + N'\sqrt{P'}}{|P|}\right) \cdot \Gamma_2' = -\left(\frac{M' + H'\sqrt{p}}{|P|}\right) \cdot \Gamma_2'$$

mit

$$\Gamma_2' = (-1)^{N'}.$$

Ich betrachte die Klassen

$$I = [1, 0, -4PP'], \quad A = [4, 0, -PP']$$

und im Falle $P > 0$ außerdem noch

$$B = [P, 0, -4P'], \quad AB = [4P, 0, -P'].$$

I und A liegen im Hauptgeschlecht; es ist

$$A = A_0^2 \quad \text{mit } A_0 = [(1 - PP')/2, 4, 8]$$

(vgl. § 4a, Fall 2), also

$$\varphi(A_0) = \left(\frac{\frac{1}{2}(1 - PP')}{P}\right) = \left(\frac{2}{P}\right) = -1.$$

Im Falle $P > 0$ ist genau dann $B \in \mathscr{C}(\Delta)^2$, wenn P nur Primteiler $q \equiv 1 \bmod 4$ besitzt; dann ist $B = B_0^2$ mit $B_0 \in \mathscr{C}(\Delta)$, und $\varphi(B_0) = \left(\frac{P'}{P}\right)_4$ (Beweis wie [18], Lemme 1).

Sind $P = t$ und $-P' = t'$ Primzahlen, so folgen aus § 1, Korollar 2 und obigen Formeln für $\sigma_\varphi(p)$ die Aussagen von [29], Theorem 5 (für $q \equiv 1 \bmod 4$, $r \equiv 5 \bmod 8$) sowie eine Reihe damit verwandter Resultate.

Im folgenden soll wiederum der Fall, daß $\Delta < 0$ und die 2-Komponente von $\mathscr{C}(\Delta)$ vom Typ (4, 4) ist, besonders herausgestellt werden. Seien dazu $P = t \equiv 5 \bmod 8$ und $-P' = t' \equiv 1 \bmod 4$ Primzahlen mit $\left(\frac{t'}{t}\right) = 1$; dann lie-

gen die 4 Klassen

$$I = [1, 0, 4tt'], \quad A = [4, 0, tt'],$$
$$B = [t, 0, 4t'], \quad AB = [4t, 0, t']$$

im Hauptgeschlecht von $\mathscr{C}(-16tt')$; also ist die 2-Komponente von $\mathscr{C}(-16tt')$ genau dann vom Typ (4, 4), wenn die 2-Komponente von $\mathscr{C}(-4tt')$ vom Typ (4, 2) ist, und das ist genau dann der Fall, wenn

$$\left(\frac{t}{t'}\right)_4 = -1, \quad \text{falls } t' \equiv 1 \bmod 8,$$
$$\left(\frac{t}{t'}\right)_4 \cdot \left(\frac{t'}{t}\right)_4 = 1, \quad \text{falls } t' \equiv 5 \bmod 8$$

[18], Prop. B_3', B_4': Seien diese Bedingungen erfüllt, und sei $\#\mathscr{C}(-16tt') = 16s$ mit $s \equiv 1 \bmod 2$; dann ist $\mathscr{C}(\Delta)^{2s} = \{I, A, B, AB\}$ und $\mathscr{X}(\Delta) = \langle \varphi, \varphi' \rangle$ mit dem Geschlechtscharakter φ' von $\mathscr{C}(\Delta)$, definiert durch

$$\varphi'(Q) = \left(\frac{-1}{\varkappa}\right) \quad \text{für } Q \in \mathscr{C}(\Delta),\ \varkappa \in N$$

mit $(\varkappa, \Delta) = 1$ und $Q \to \varkappa$ (siehe § 4a). Sind $A_0, B_0 \in \mathscr{C}(-16tt')$ mit $A_0^2 = A$, $B_0^2 = B$, so erhält man die folgenden Charakterwerte:

$t' \equiv 1 \bmod 8$	A_0	B_0
φ	-1	$\left(\frac{t'}{t}\right)_4$
φ'	-1	$-\left(\frac{t'}{t}\right)_4$

$t' \equiv 5 \bmod 8$	A_0	B_0
φ	-1	$-\left(\frac{t'}{t}\right)_4$
φ'	1	-1

(die φ-Werte wurden oben berechnet, $\varphi'(A_0) = \left(\frac{-1}{\frac{1}{2}(1+tt')}\right)$, und $\varphi'(B_0)$ berechnet man nach der Methode von [18], p. 320, unter Beachtung von $\varphi'(B_0) = \left(\frac{t}{\varkappa}\right) \cdot \left(\frac{t'}{\varkappa}\right)$, falls $B \to \varkappa^2$). Ist nun p eine Primzahl mit $\left(\frac{-1}{p}\right) = \left(\frac{t}{p}\right) = \left(\frac{t'}{p}\right) = 1$, so folgt $Q \to p^s$ für genau ein $Q \in \{I, A, B, AB\}$, und das Theorem aus § 1 liefert gemeinsam mit den obigen Rechnungen und den Formeln für $\sigma_\varphi(p)$, $\sigma_{\varphi'}(p)$ explizite arithmetisch Kriterien dafür, welche der vier Formen p^s darstellt, auf deren Ausformulierung ich hier verzichte (vgl. § 4b).

4d. Der Fall $\Delta = PP'$ mit $P \equiv P' \equiv 1 \bmod 4$ und $\varphi = \left(\frac{P}{\cdot}\right)$. Seien $P, P' \in \mathbf{Z}\setminus\{0, 1\}$ quadratfrei, $(P, P') = 1$, $P \equiv P' \equiv 1 \bmod 4$, $\left(\frac{P, P'}{p}\right) = 1$ für alle $p \in \mathbf{P} \cup \{\infty\}$ und $\Delta = PP'$.

Dann ist $\varphi\colon \mathscr{C}(\Delta) \to \{\pm 1\}$, definiert durch

$$\varphi(Q) = \left(\frac{P}{\varkappa}\right) = \left(\frac{P'}{\varkappa}\right) \quad \text{für } \varkappa \in N$$

mit $(\varkappa, 2\Delta) = 1$ und $Q \to \varkappa$, ein Geschlechtscharakter von $\mathscr{C}(\Delta)$, und nach Proposition 4 ist $\varphi \in \mathscr{X}(\Delta)$. Es ist $\{e_\varphi, \tilde{e}_\varphi\} = \{P, P'\}$, und ich erhalte aus dem Zusatz zu Proposition 3 und aus 3.1 die folgenden Formeln für $\sigma_\varphi(p)$:

Sei $p \in \mathbf{P}(\Delta)$, $M^2 - PN^2 = H^2 p$ mit $H \in N$, $H \equiv 1 \bmod 2$, $M, N \in \mathbf{N}$, $(M, N) = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M + N\sqrt{P}}{|P'|}\right) = \left(\frac{M + H\sqrt{p}}{|P'|}\right) \cdot \left(\frac{2}{|P'|}\right).$$

Der Homomorphismus $\theta\colon \mathscr{C}(4\Delta) \to \mathscr{C}(\Delta)$, definiert durch

$$\theta([a, 2b, 4c]) = [a, b, c],$$

induziert einen Isomorphismus der 2-Sylow gruppen von $\mathscr{C}(4\Delta)$ und $\mathscr{C}(\Delta)$, und daher kann ich die Geschlechtscharaktere von $\mathscr{C}(4\Delta)$ und $\mathscr{C}(\Delta)$ miteinander identifizieren. Für $Q \in \mathscr{C}(4\Delta)$ und $\varkappa \in N$ mit $(\varkappa, 2\Delta) = 1$ gilt:

Aus $Q \to \varkappa$ folgt $\theta(Q) \to \varkappa$;

$Q \to 4\varkappa$ genau dann, wenn $\theta(Q) \to \varkappa$.

Neben der Hauptklasse $I = [1, 0, -PP'] \in \mathscr{C}(4\Delta)$ betrachte ich im Falle $P > 0$ die Klasse $A = [P, 0, -P'] \in \mathscr{C}(4\Delta)$. Genau dann ist $A \in \mathscr{C}(4\Delta)^2$, wenn P nur Primteiler $q \equiv 1 \bmod 4$ besitzt; dann ist $A = A_0^2$ mit $A_0 \in \mathscr{C}(4\Delta)$, und $\varphi(A_0) = \left(\frac{P'}{P}\right)_4$ ([18], Lemme 1).

Sind P und $-P'$ Primzahlen, so erhält man mit Hilfe der expliziten Formeln für $\sigma_\varphi(p)$ aus § 1, Korollar 2 die Aussagen von [29], Theorem 5 (im Falle $q \equiv 3 \bmod 4$).

Sind entweder P und P' oder P und $-P'$ Primzahlen, so ist die 2-Komponente von $\mathscr{C}(\Delta)$ zyklisch; ist p eine Primzahl mit $\left(\frac{P}{p}\right) = \left(\frac{P'}{p}\right) = 1$ bzw. $\left(\frac{P}{p}\right) = \left(\frac{-P'}{p}\right) = 1$ und $Q \in \mathscr{C}(\Delta)$ mit $Q \to p$, so ist $Q \in \mathscr{C}(\Delta)^4$ genau dann, wenn $\sigma_\varphi(p) = 1$ (siehe [22], Theorems 4, 6).

4e. Der Fall $\Delta = 8PP'$ mit $P \equiv 1 \bmod 8$ und $\varphi = \left(\frac{P}{\cdot}\right)$. Seien $P, P' \in \boldsymbol{Z} \setminus \{0, 1\}$ quadratfrei, $(P, P') = 1$, $P \equiv 1 \bmod 8$, $\left(\frac{P, 2P'}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$, und sei $\Delta = 8PP'$.

Dann ist $\varphi\colon \mathscr{C}(\Delta) \to \{\pm 1\}$, definiert durch

$$\varphi(Q) = \left(\frac{P}{\varkappa}\right) = \left(\frac{2P'}{\varkappa}\right) \quad \text{für } \varkappa \in N$$

mit $(\varkappa, \Delta) = 1$, $Q \to \varkappa$, ein Geschlechtscharakter von $\mathscr{C}(\Delta)$, und nach Proposition 4 ist $\varphi \in \mathscr{X}(\Delta)$. Ich erhalte $\{e_\varphi, \tilde{e}_\varphi\} = \{P, 8P'\}$, und aus dem Zusatz zu Proposition 3 folgen mittels 3.4 bzw. 3.6 die nachstehenden Formeln für $\sigma_\varphi(p)$:

(a) $e = P$, $\tilde{e} = 2P'$: Sei $p \in \boldsymbol{P}(\Delta)$, $M^2 - PN^2 = H^2 p$ mit $H \in N$, $H \equiv 1 \bmod 2$, $M, N \in N$, $(M, N) = 1$; dann folgt:

$$\sigma_\varphi(p) = \left(\frac{M + N\sqrt{P}}{|P'|}\right) \cdot \Gamma_2 = \left(\frac{M + H\sqrt{p}}{|P'|}\right) \cdot \left(\frac{2}{|P'|}\right) \cdot \Gamma_2$$

mit

$$\Gamma_2 = \left(\frac{2}{M + Nt}\right) \cdot (-1)^{(M+N-1)(P'-1)/4}.$$

(b) $e = 2P'$, $\tilde{e} = P$: Sei $p \in \boldsymbol{P}(\Delta)$, $M'^2 - 2P'N'^2 = H'^2 p$ mit $H' \in N$, $H' \equiv 1 \bmod 2$, $M', N' \in N$, $(M', N') = 1$; dann folgt

$$\sigma_\varphi(p) = \left(\frac{M' + N'\sqrt{2P'}}{|P|}\right) = \left(\frac{M' + H'\sqrt{p}}{|P|}\right).$$

Ich betrachte die Klassen

$$I = [1, 0, -2PP'], \quad A = [2, 0, -PP']$$

und im Falle $P > 0$ außerdem noch

$$B = [P, 0, -2P'], \quad AB = [2P, 0, -P'].$$

Genau dann ist $A \in \mathscr{C}(\Delta)^2$, wenn PP' nur Primteiler $q \equiv \pm 1 \bmod 8$ besitzt; dann ist $-PP' = f^2 - 2g^2$ mit $f, g \in N$, und $A = A_0^2$ mit $A_0 = [f, 4g, 2f]$, $\varphi(A_0) = \left(\frac{P}{f}\right)$.

Im Falle $P > 0$ ist genau dann $B \in \mathscr{C}(\Delta)^2$, wenn P nur Primteiler $q \equiv 1, 3 \bmod 8$ besitzt; dann ist $B = B_0^2$ mit $B_0 \in \mathscr{C}(\Delta)$, so daß $\varphi(B_0) = \left(\frac{2P'}{P}\right)_4$ (Beweis wie [18], Lemme 2).

Von besonderer Einfachheit sind die folgenden drei Fälle, in denen die 2-Komponente von $\mathscr{C}(\Delta)$ zyklisch ist:

1. $P = -q$ mit einer Primzahl $q \equiv 7 \bmod 8$, $P' = 1$: In diesem Falle ist $\varphi(A_0) = \left(\frac{-q}{f}\right) = \left(\frac{2}{f}\right) = (-1)^{(q+1)/8}$; aus § 1, Korollar 2 und den Formeln für $\sigma_\varphi(p)$ erhält man in diesem Falle [29], Theorem 2 (für $q \equiv 7 \bmod 8$).

2. $P = r$ mit einer Primzahl $r \equiv 1 \bmod 8$, $P' = 1$: In diesem Falle ist $\varphi(A_0) = \varphi(B_0) = (-1)^{(r-1)/8}$, und $\#\{I, A, B, AB\} = 2$ ([19], § 3).

3. $P = r$ mit einer Primzahl $r \equiv 1 \bmod 8$, $P' = -1$: In diesem Falle ist $A = B$, $I = AB$ und $\varphi(A_0) = \left(\frac{2}{r}\right)_4$ ([19], § 4).

Liege einer der Fälle 1., 2., 3. vor, und sei p eine Primzahl mit $\left(\frac{P}{p}\right) = \left(\frac{2P'}{p}\right) = 1$; dann gibt es ein $Q \in \mathscr{C}(\Delta)$ mit $Q \to p$, und genau dann ist $Q \in \mathscr{C}(\Delta)^4$, wenn $\sigma_\varphi(p) = 1$; mit Hilfe der expliziten Formeln für $\sigma_\varphi(p)$ folgen daraus [22], Theorems 2, 3 und 5; in [22], Theorem 5, ist die Bedingung $e+f \equiv 1 \bmod 8$ inkorrekt und zu ersetzen durch $\left(\frac{-1}{p}\right)^{(r-1)/8} \cdot \left(\frac{2}{e+f}\right) = 1$.

Abschließend betrachte ich noch einmal den bereits in § 4a erwähnten Fall von Formen der Diskriminante $-128q$ mit einer Primzahl $q \equiv 1 \bmod 8$, so daß $\left(\frac{2}{q}\right)_4 = 1$. In diesem Falle ist $\#\mathscr{C}(-128q) = 16s$ mit $s \equiv 1 \bmod 2$, die 2-Komponente von $\mathscr{C}(-128q)$ ist vom Typ (4, 4), und

$$\mathscr{C}(-128q)^{2s} = \{\tilde{I}, \tilde{A}, \tilde{B}, \tilde{A}\tilde{B}\}$$

mit

$$\tilde{I} = [1, 0, 32q], \qquad \tilde{A} = [32, 0, q],$$
$$\tilde{B} = [4, 4, 1+8q], \qquad \tilde{A}\tilde{B} = [32, 32, 8+q].$$

Es ist $\mathscr{X}(-128q) = \langle \varphi_q, \varphi' \rangle$ wobei $\varphi_q(Q) = \left(\frac{q}{\varkappa}\right)$, $\varphi'(Q) = \left(\frac{-1}{\varkappa}\right)$ für $Q \in \mathscr{C}(-128q)$, $\varkappa \in N$ mit $(\varkappa, 2q) = 1$ und $Q \to \varkappa$, $\tilde{I} = \tilde{I}^2$, $\tilde{A} = \tilde{A}_0^2$ $\tilde{B} = \tilde{B}_0^2$ mit $\tilde{A}_0, \tilde{B}_0 \in \mathscr{C}(-128q)$, und aus § 4a folgt

$$\varphi'(\tilde{A}_0) = \left(\frac{2}{q}\right)_4 \cdot \left(\frac{q}{2}\right)_4 = (-1)^{(q-1)/8}, \qquad \varphi'(\tilde{B}_0) = -1.$$

Zur Berechnung von $\varphi_q(\tilde{A}_0)$, $\varphi_q(\tilde{B}_0)$ betrachte ich den kanonischen Epimorphismus $\theta\colon \mathscr{C}(-128q) \to \mathscr{C}(-8q)$, definiert durch $\theta([a, 4b, 16c]) = [a, b, c]$, nach welchem φ_q faktorisiert. Wegen $\theta(\tilde{A}_0)^2 = [2, 0, q]$ und $\theta(\tilde{B}_0)^2 = [1, 0, 2q]$ folgt aus obigen Rechnungen

$$\varphi_q(\tilde{B}_0) = 1, \qquad \varphi_q(\tilde{A}_0) = \left(\frac{2}{q}\right)_4 = -1.$$

Ist nun p eine Primzahl mit $p \equiv 1 \bmod 8$ und $\left(\frac{q}{p}\right) = 1$, so folgt $Q \to p^s$ für genau ein $Q \in \{\tilde{I}, \tilde{A}, \tilde{B}, \tilde{A}\tilde{B}\}$, und zwar für jenes, für welches $Q = Q_0^2$ mit $\varphi_q(Q_0) = \sigma_{\varphi_q}(p)$ und $\varphi'(Q_0) = \sigma_{\varphi'}(p)$ (nach dem Theorem in § 1), und mit Hilfe des Zusatzes zu Proposition 2 folgt das Theorem in [27].

4f. Der Fall $\Delta = 128PP'$ mit $P \equiv 3 \bmod 4$, $P' \equiv 1 \bmod 2$ und $\varphi = \left(\frac{P}{\cdot}\right)$. Seien $P, P' \in \mathbf{Z} \setminus \{0, 1\}$ quadratfrei, $(2P, P') = 1$, $P \equiv 3 \bmod 4$, $\left(\frac{P, 2P'}{p}\right) = 1$ für alle $p \in \boldsymbol{P} \cup \{\infty\}$, und sei $\Delta = 128PP'$.

Dann ist $\varphi\colon \mathscr{C}(\Delta) \to \{\pm 1\}$, definiert durch $\varphi(Q) = \left(\frac{P}{\varkappa}\right) = \left(\frac{2P'}{\varkappa}\right)$ für $\varkappa \in N$ mit $(\varkappa, \Delta) = 1$ und $Q \to \varkappa$, ein Geschlechtscharakter von $\mathscr{C}(\Delta)$, und nach Proposition 4 ist $\varphi \in \mathscr{X}(\Delta)$. Ich erhalte $\{e_\varphi, \tilde{e}_\varphi\} = \{P, 8P'\}$ und explizite Formeln für $\sigma_\varphi(p)$ aus den Propositionen 2 und 3 (samt Zusatz) und aus 3.5c und 3.7, auf deren Angabe ich hier verzichte.

Wie in § 4a, Fall 3, betrachte ich die vier Klassen

$$I = [1, 0, -32PP'], \qquad A = [32, 0, -PP'],$$

$$B = [4, 4, 1-8PP'], \qquad AB = [32, 32, 8-PP'].$$

Es ist $B = B_0^2$ mit $B_0 = [1-2PP', 8, 16]$; sei $l \in N$ mit $B_0 \to 1-2PP' + lP > 0$. Dann folgt

$$\varphi(B_0) = \left(\frac{P}{1-2PP'+lP}\right) = -\left(\frac{1-2PP'+lP}{P}\right) = -1.$$

Genau dann ist $A \in \mathscr{C}(\Delta)^2$, wenn PP' nur Primteiler $q \equiv \pm 1 \bmod 8$ besitzt; dann ist $-PP' = f^2 - 2g^2$ mit $f, g \in N$, $g \equiv 0 \bmod 4$, und $A = A_0^2$ mit $A_0 = [f, 16g, 32f]$ und folglich $\varphi(A_0) = \left(\frac{P}{f}\right)$.

Für $\varkappa \in N$ mit $(\varkappa, 2PP') = 1$ gilt:

Aus $\varkappa = x^2 - 8PP'y^2$ mit $x, y \in N$, $(x, y) = 1$, folgt $I \to \varkappa$, falls $y \equiv 0 \bmod 2$, und $B \to \varkappa$, falls $y \equiv 1 \bmod 2$;

aus $\varkappa = 8x^2 - PP'y^2$ mit $x, y \in N$, $(x, y) = 1$ folgt $A \to \varkappa$, falls $x \equiv 0 \bmod 2$, und $AB \to \varkappa$, falls $x \equiv 1 \bmod 2$.

Ist $P = -q$ mit einer Primzahl $q \equiv 1 \bmod 8$ und $P' = 1$, so folgt

$$\varphi(A_0) = \left(\frac{-q}{f}\right) = \left(\frac{2}{f}\right) = (-1)^{(q-1)/8},$$

und mit Hilfe von § 1, Korollar 2 und den explizitien Formeln für $\sigma_\varphi(p)$ erhält man [29], Theorem 2 (im Falle $q \equiv 1 \bmod 8$).

Ist entweder $P = -q$ mit einer Primzahl $q \equiv 5 \bmod 8$, $P' = 1$ oder $P = q$ mit einer Primzahl $q \equiv 3 \bmod 8$, $P' = -1$, so ist $\mathscr{C}(\Delta)$ vom Typ (2, 4), also $\# \mathscr{C}(\Delta) = 8s$ mit $s \equiv 1 \bmod 2$. Ist p eine Primzahl mit $p \equiv 1 \bmod 8$, $\left(\frac{q}{p}\right) = 1$, so folgt

$$p^s = x^2 + 8qy^2$$

mit $x, y \in \mathbf{Z}$, $(x, y) = 1$, und aus dem Theorem in § 1 und den expliziten Formeln für $\sigma_\varphi(p)$ folgen arithmetische Kriterien für die Parität von y (siehe [20] für den Fall $q \equiv 3 \bmod 8$).

Literatur

[1] P. Barrucand, H. Cohn, *Note on primes of type x^2+32y^2, class number and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

[2] E. Brown, *Biquadratic reciprocity laws*, Proc. Amer. Math. Soc. 37 (1973), 374–476.

[3] — *A theorem on biquadratic reciprocity*, ibid. 30 (1971), 220–222.

[4] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), 175–184.

[5] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[6] D. R. Estes, G. Pall, *Spinor Genera of Binary Quadratic Forms*, J. Number Theory 5 (1973), 421–432.

[7] Y. Furuta, *Norms of units of quadratic fields*, J. Math. Soc. Japan 11 (1959), 139–145.

[8] — *A prime decomposition symbol for a non abelian central extension which is abelian over a bicyclic biquadratic field*, Nagoya Math. J. 79 (1980), 79–109.

[9] F. Halter-Koch, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe*, J. Number Theory 3 (1971), 412–443.

[10] — *Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern*, ibid. 4 (1972), 70–77.

[11] — *Geschlechtertheorie der Ringklassenkörper*, J. Reine Angew. Math. 250 (1971), 107–108.

[12] — *An Artin character and representations of primes by binary quadratic forms III*, Manuscripta Math. 51 (1985), 163–169.

[13] — *On the quartic character of certain quadratic units and representations of primes by binary quadratic forms*, Rocky Mountain J. Math. 16 (1986), 95–102.

[14] — *Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten*, Manuscripta Math. 54 (1986), 453–492.

[15] F. Halter-Koch, P. Kaplan, K. S. Williams, *An Artin character and representations of primes by binary quadratic forms II*, ibid. 37 (1982), 357–381.

[16] F. Halter-Koch, *Binary Quadratic Forms, Dihedral Fields and Decomposition Laws*, Proc. Conf. on Alg. Number Theory, Kyoto 1986.

[17] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Physika-Verlag, Würzburg 1965.

[18] P. Kaplan, *Sur le 2-groupe des classes d'ideaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), 313–363.

[19] — *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan 25 (1973), 596–608.

[20] — *Representations of prime numbers by classes of binary quadratic forms*, Proc. Intern. Symp. on Alg. Number Theory, Kyoto 1976.

[21] P. Kaplan, K. S. Williams, *An Artin character and representations of primes by binary quadratic forms*, Manuscripta Math. 33 (1981), 339–356.
[22] P. Kaplan, K. S. Williams, Y. Yamamoto, *An application of dihedral fileds to representations of primes by binary quadratic forms*, Acta Arith. 44 (1984), 407–413.
[23] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), 42–48.
[24] – *On some special quadratic reciprocity laws*, Acta Arith. 21 (1972), 367–377.
[25] P. A. Leonard, K. S. Williams, *The quadratic and quartic character of certain quadratic units II*, Rocky Mountain J. Math. 9 (1979), 683–692.
[26] – – *The Quartic Characters of Certain Quadratic Units*, J. Number Theory 12 (1980), 106–109.
[27] – – *A representation problem involving binary quadratic forms*, Arch. Math. 36 (1981), 53–56.
[28] – – *An Observation on Binary Quadratic Forms of Discriminant* $-32q$, Abh. Math. Inst. der Univ. Hamburg 53 (1983), 39–40.
[29] J. B. Muskat, *On Simultaneous Representations of Primes by Binary Quadratic Forms*, J. Number Theory 19 (1984), 263–282.
[30] B. Perrin-Riou, *Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne*, Ann. Inst. Fourier 30 (1980), 19–33.
[31] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. Reine Angew. Math. 180 (1939), 1–43.
[32] L. Rédei, H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, ibid. 170 (1933), 69–74.
[33] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2-Du^2=-4$, Math. Zeitschr. 39 (1934), 95–111.
[34] H. C. Williams, *The quadratic character of a certain quadratic surd*, Utilitas Math. 5 (1974), 49–55.
[35] – *Note on a result of Barrucand and Cohn*, J. Reine Angew. Math. 285 (1976), 218–220.
[36] Y. Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. 21 (1984), 1–22.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
Halbärthgasse 1/1
A-8010 Graz

Eingegangen am 24.10.1986
und in revidierter Form am 23.3.1987 (1684)

ACTA ARITHMETICA
LI (1988)

A generalization of Bombieri's prime number theorem to algebraic number fields

by

JÜRGEN G. HINZ (Marburg)

1. Introduction. For many important problems in the theory of numbers we need some information about the average distribution of primes in arithmetic progressions. It is convenient to introduce the classical device of "weighting" the primes with von Mangoldt's function $\Lambda(m)$. Let

$$\psi(y; q, l) = \sum_{\substack{m \leqslant y \\ m \equiv l \bmod q}} \Lambda(m). \tag{1.1}$$

We ask for inequalities of type ($A > 0$ arbitrary but fixed)

$$\sum_{q \leqslant Q = Q(x)} \max_{y \leqslant x} \max_{(l,q)=1} \left| \psi(y; q, l) - \frac{y}{\varphi(q)} \right| \ll x(\log x)^{-A}. \tag{1.2}$$

The first attempt to obtain a "non-trivial" estimate of this kind was made by Renyi. He showed that (1.2) is true with $Q = x^a$ for some small positive a. Subsequent refinements of Bombieri [1] enable us to take $Q = x^{1/2}(\log x)^{-B}$ for some $B = B(A) > 0$. A slightly weaker result has been derived independently by A. I. Vinogradov [18], using a different method. Gallagher [4] later introduced major simplifications in Bombieri's arguments. More recently Vaughan [17] developed an ingenious new method which differs significantly from all approaches used previously and which gives a still simpler proof by essentially elementary means.

The main advantage of Bombieri's theorem becomes clear, if we note that the classical prime number theorem of Page, Siegel and Walfisz only leads to the limit $Q = (\log x)^C$ for the moduli q in (1.2). Moreover, Bombieri's bound Q is as good, apart from the logarithmic factor, as one can obtain on the assumption of the generalized Riemann hypothesis.

Many important applications of (1.2) are to be found in the literature. The major results are too well known to need elaboration. In the sequel, let K be an algebraic number field of finite degree $n = r_1 + 2r_2$ (in the usual notation) over the rationals with discriminant d. Z_K will denote the ring of integers in K.