

Über Bernoullische Zahlen in reel-quadratischen Zahlkörpern

von

HEINRICH LANG (Köln)

I. Einleitung. Es sei Ω ein reel-quadratischer Zahlkörper mit der Diskriminante $d_\Omega > 0$. Bezeichnet dann $\zeta(s|\mathfrak{A})$ die Zetafunktion einer absoluten Idealklasse \mathfrak{A} von Ω und $L(s|\mathfrak{A}_+)$ die L -Funktion einer Idealklasse \mathfrak{A}_+ im engeren Sinne [10], so sind für natürliche Argumente $k \geq 2$ die Werte

$$(1.1) \quad B(k|\mathfrak{A}_k) = \begin{cases} \frac{4(4h)!d_\Omega^{2h}}{(2\pi)^{4h}\sqrt{d_\Omega}} \zeta(2h|\mathfrak{A}), & \text{falls } k = 2h \text{ gerade ist,} \\ \frac{4(4h+2)!d_\Omega^{2h+1}}{(2\pi)^{4h+2}\sqrt{d_\Omega}} L(2h+1|\mathfrak{A}_+), & \text{falls } k = 2h+1 \text{ ungerade ist,} \end{cases}$$

rationale Zahlen [2], [7], [8], [11], [13], [14]. Nach E. Hecke [6] sind diese rationalen Zahlen $B(k|\mathfrak{A}_k)$ — nach geeigneter Normierung — als ein Analogon der gewöhnlichen Bernoullischen Zahlen B_m anzusehen. So bleibt insbesondere die Frage zu beantworten, ob für diese *Bernoullischen Zahlen in reel-quadratischen Zahlkörpern* eine ähnliche Charakterisierung der Nenner und eine entsprechende Partialbruchzerlegung besteht, wie sie im Satz von v. Staudt und Clausen für die gewöhnlichen Bernoullischen Zahlen formuliert wird.

In [9] ist versucht worden, die möglichen Nenner von $B(2h|\mathfrak{A}_{2h})$ genauer zu beschreiben, wobei sich die dort durchgeführten Beweise ohne Schwierigkeiten auch auf die Untersuchung von $B(2h+1|\mathfrak{A}_{2h+1})$ übertragen lassen, und es wurde bewiesen: Ist G_{2h} Hauptnenner der Zahlen $\binom{4h}{m} B_{4h-m} B_m$, so ist $G_{2h} B(2h|\mathfrak{A}_{2h})$ eine ganz-rationale Zahl. Im folgenden soll untersucht werden, wann Primteiler der Diskriminante d_Ω und der Komponenten u, v der normpositiven Grundeinheit $\varepsilon_+ = \frac{1}{2}(u + v\sqrt{d_\Omega}) > 1$, $N(\varepsilon_+) = 1$, von Ω im Nenner von $B(k|\mathfrak{A}_k)$ auftreten. Für den Fall, daß $2h+1 = p$ eine Primzahl ist, gelangt man für diese Primzahl p sogar zu einer genauen Partialbruchzerlegung von $B(k|\mathfrak{A}_k)$.

II. Höhere Dedekindsche Summen. Bei der Bildung der oben in (1.1) eingeführten Werte $B(k|\mathfrak{A}_k)$ spielen die höheren Dedekindschen Summen eine wesentliche Rolle. Es seien daher zunächst ihre Grundeigenschaften referiert [1], [3], [9]. Die gewöhnlichen Bernoullischen Zahlen B_m sind durch die Potenzreihenentwicklung

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} B_m \frac{x^m}{m!} \quad (|x| < 2\pi)$$

gegeben. Mit ihnen definiert man die mit der Periode 1 periodischen Bernoullischen Funktionen $P_m(x)$ durch

$$P_m(x) = \sum_{r=0}^m \binom{m}{r} B_r (x - [x])^{m-r},$$

wobei im Fall $m = 1$ noch $P_1(0) = 0$ festgesetzt wird.

Sind d und $c \neq 0$ zwei teilerfremde ganz-rationale Zahlen, so werden die höheren Dedekindschen Summen vermöge

$$(2.1) \quad S_{2k}^{(m)}(d, c) = \sum_{j \bmod c} P_{2k-m} \left(\frac{j}{c} \right) P_m \left(\frac{dj}{c} \right) \quad (k = 2, 3, 4, \dots; 0 \leq m \leq 2k)$$

erklärt. Evident gilt für sie

$$(2.2) \quad S_{2k}^{(m)}(d, c) = S_{2k}^{(m)}(d^*, c) \quad \text{für} \quad d \equiv d^* \pmod{c}.$$

In den Fällen $m = 0$ und $m = 2k$ läßt sich die Summation in (2.1) durchführen, und man hat

$$(2.3) \quad S_{2k}^{(0)}(d, c) = S_{2k}^{(2k)}(d, c) = \operatorname{sgn} c \frac{B_{2k}}{c^{2k-1}}.$$

Für $c = 1$ folgt aus der Definition (2.1) sofort

$$(2.4) \quad S_{2k}^{(m)}(0, 1) = B_{2k-m} B_m.$$

Ist auch noch $d \neq 0$, so gilt für $m = 2k - 1$ das von T. M. Apostol [1] aufgestellte einfache Reziprozitätsgesetz

$$\begin{aligned} 2k(d c^{2k-1} \operatorname{sgn} c S_{2k}^{(2k-1)}(d, c) + c d^{2k-1} \operatorname{sgn} d S_{2k}^{(2k-1)}(c, d)) \\ = (2k-1) B_{2k} + \sum_{r=0}^{2k} \binom{2k}{r} (-1)^r c^{2k-r} d^r B_{2k-r} B_r. \end{aligned}$$

Wählt man darin speziell $c = d = 1$ und beachtet, daß

$$(2.5) \quad B_m = 0 \quad \text{für} \quad m \geq 3 \quad \text{und} \quad m \equiv 1 \pmod{2}$$

ist, so erhält man mit Hilfe von (2.2) und (2.4) die schon L. Euler bekannte Relation

$$(2.6) \quad \sum_{r=0}^k \binom{2k}{2r} B_{2k-2r} B_{2r} = -(2k-1) B_{2k} \quad (k = 2, 3, 4, \dots)$$

zwischen Bernoullischen Zahlen.

Sei jetzt auch noch $d \not\equiv 0 \pmod{c}$ angenommen. Dann besteht für die höheren Dedekindschen Summen die Darstellung

$$(2.7) \quad \operatorname{sgn} c S_{2k}^{(m)}(d, c) = \frac{B_{2k-m} B_m}{c^{2k-1}} + \frac{(2k-m)m}{c^{2k-1}} \sum_{\substack{|\sigma|=1 \\ \sigma \neq 1}} e^{1-d} \frac{R_{2k-m-1}(\sigma^{-d}) R_{m-1}(\sigma)}{(\sigma^{-d}-1)^{2k-m} (\sigma-1)^m}$$

durch $|\sigma|$ -te Einheitswurzeln [3], [9]. Hierbei ist über alle von 1 verschiedenen $|\sigma|$ -ten Einheitswurzeln zu summieren, und es bedeuten $R_{m-1}(x)$ die von G. Frobenius [4] eingeführten *Eulerschen Polynome*. Diese besitzen ganz-rationale Koeffizienten, so daß es sich bei $R_{2k-m-1}(\sigma^{-d})$ und $R_{m-1}(\sigma)$ um ganze Zahlen aus dem $|\sigma|$ -ten Kreiskörper handelt.

Nun ist

$$\frac{|\sigma| \sigma}{1 - \sigma} = \sum_{r=1}^{|\sigma|-1} r \sigma^{-r}$$

eine ganz-algebraische Zahl. Daher folgt für jede zu c teilerfremde ganz-rationale Zahl t :

$$(2.8) \quad \operatorname{sgn} c S_{2k}^{(m)}(d, c) - \frac{B_{2k-m} B_m}{c^{2k-1}} \text{ ist ganz für } t \quad ((t, c) = 1).$$

Diese Aussage gilt wegen (2.4) auch noch für $d \equiv 0 \pmod{c}$. Denn in diesem Fall kommt nur $c = \pm 1$ in Frage, da c und d voraussetzungsgemäß prim zueinander sind.

Schreibt man allgemein $r \equiv s \pmod{t^0}$, wenn die Differenz $r - s$ der rationalen Zahlen r und s ganz für t ist, so kann man die Aussage (2.8) auch durch

$$(2.9) \quad \operatorname{sgn} c S_{2k}^{(m)}(d, c) \equiv \frac{B_{2k-m} B_m}{c^{2k-1}} \pmod{t^0}, \quad \text{falls } t \text{ teilerfremd zu } c \text{ ist,}$$

ausdrücken.

III. Die Zahlen $B(k|\mathfrak{A}_k)$. Sei \mathfrak{A} eine absolute Idealklasse des reell-quadratischen Zahlkörpers Ω mit der Diskriminante $d_\Omega > 0$, und sei \mathfrak{g} ein ganzes Ideal aus der inversen Klasse \mathfrak{A}^{-1} von \mathfrak{A} . Die Basis γ_1, γ_2 von \mathfrak{g} sei in der kanonischen Form [5], p. 373,

$$(3.1) \quad \gamma_1 = g_1 \frac{g_0 + \sqrt{d_\Omega}}{2}, \quad \gamma_2 = g_1 g_2$$

Es gilt der Satz von v. Staudt und Clausen:

$$(3.10) \quad -B_{2m} \equiv \sum_{\substack{p-1|2m \\ p \text{ Primzahl}}} \frac{1}{p} \pmod{1}.$$

Daher geht eine Primzahl p höchstens quadratisch im reduzierten Nenner von $B_{2k-2m} B_{2m}$ auf, wenn $p-1|2m$, $p-1|2k-2m$ und $p \leq k+1$ gilt. Das kann aber nur eintreten, falls $p-1|2k$ und $p \leq k+1$ zutrifft. Ist $k+1 = q$ selbst eine Primzahl, so ist offenbar q ein Teiler von $\binom{2k}{k}$. Für eine beliebige Primzahl p hat man daher:

$$(3.11) \quad \begin{aligned} \binom{2k}{2m} B_{2k-2m} B_{2m} & \text{ ist ganz für } p, \text{ falls } p > 2k+1 \text{ ist,} \\ p \binom{2k}{2m} B_{2k-2m} B_{2m} & \text{ ist ganz für } p, \text{ falls } p > k \text{ oder } p-1 \nmid 2k \text{ ist,} \\ p^2 \binom{2k}{2m} B_{2k-2m} B_{2m} & \text{ ist ganz für } p. \end{aligned}$$

Für $\varepsilon_+ = \frac{1}{2}(u+v\sqrt{d_\Omega})$ prüft man leicht nach:

$$(3.12) \quad S_p(\varepsilon_+^{2r+1-2m}) \equiv 0 \pmod{\frac{u}{2}}.$$

Das Ideal \mathfrak{g} aus \mathfrak{A}_k^{-1} läßt sich so wählen, daß \mathfrak{g} prim zu uvd_Ω und damit auch $\mathfrak{N}(\mathfrak{g}) = g_1^2 g_2$ prim zu uvd_Ω ist. Beachtet man noch, daß auf Grund der Pellschen Gleichung

$$(3.13) \quad u^2 - v^2 d_\Omega = 4$$

u und v nur 2 als gemeinsamen Teiler haben können sowie daß sich gemäß (3.7) $\mathfrak{B}(k|\mathfrak{A}_k)$ und $B(k|\mathfrak{A}_k)$ höchstens um den Faktor 2 unterscheiden, so erhält man aus (3.9) und (3.11) den

Satz I. *Ist $p \neq 2$ ein Primteiler der Komponente u der normpositiven Grundeinheit $\varepsilon_+ = \frac{1}{2}(u+v\sqrt{d_\Omega}) > 1$ von Ω , so ist $B(k|\mathfrak{A}_k)$ ganz für p , falls eine der drei Bedingungen*

$$p-1 \nmid 2k, \quad p^2 | u \quad \text{oder} \quad p > k$$

erfüllt ist. Anderenfalls ist $pB(k|\mathfrak{A}_k)$ eine für p ganze rationale Zahl.

Es besteht die Formel

$$(3.14) \quad \binom{2k-2}{k-1} = \sum_{r=0}^{k-1} \binom{n-1}{r} \binom{2k-1-n}{k-1-r} \quad \text{für } n = 0, 1, 2, \dots, 2k.$$

Die darin auftretende Summe ist invariant bei Vertauschung von n und $2k-n$. Daher braucht diese Formel (3.14) nur für $0 \leq n \leq k$ bewiesen zu werden. Im Fall $n = 0$ besagt sie:

$$\binom{2k-2}{k-1} = \sum_{r=0}^{k-1} (-1)^r \binom{2k-1}{k-1-r}.$$

Es gilt aber sogar allgemeiner

$$\binom{2k-2}{n} = \sum_{r=0}^n (-1)^r \binom{2k-1}{n-r},$$

wie man durch vollständige Induktion nach n erkennt.

Für $1 \leq n \leq k$ ersieht man die Gültigkeit von (3.14) durch Koeffizientenvergleich von

$$\begin{aligned} \binom{2k-2}{k-1} \frac{(k-1)!^2}{(2k-1-n)!} x^{2k-1-n} &= \frac{d^{n-1}}{dx^{n-1}} x^{2k-2} \\ &= \sum_{r=0}^{n-1} \binom{n-1}{r} \frac{d^r}{dx^r} x^{k-1} \frac{d^{n-1-r}}{dx^{n-1-r}} x^{k-1} \\ &= \sum_{r=0}^{n-1} \binom{n-1}{r} \binom{k-1}{r} \binom{k-1}{n-1-r} r! (n-1-r)! x^{2k-1-n} \\ &= \frac{(k-1)!^2}{(2k-1-n)!} \sum_{r=0}^{n-1} \binom{n-1}{r} \binom{2k-1-n}{k-1-r} x^{2k-1-n}. \end{aligned}$$

Sei nun $p > k$ ein ungerader Primteiler der Diskriminante d_Ω . Mit Hilfe der Pellschen Gleichung (3.13) findet man dann

$$S_p(\varepsilon_+^{2r+1-2m}) \equiv u \pmod{p}.$$

Ist diese Primzahl p nicht gleichzeitig ein Teiler von v , und ist wieder g prim zu uvd_Ω gewählt, so folgt aus (3.9), (3.14) sowie der Eulerschen Formel (2.6):

$$(3.15) \quad \mathfrak{B}(k|\mathfrak{A}_k) \equiv \frac{-u}{v^{2k-1} g_2^k} \binom{2k-2}{k-1} (2k-1) B_{2k} \pmod{p^0}$$

$$(p|d_\Omega, p > k, (p, v) = 1).$$

Nach dem Satz von v. Staudt und Clausen (3.10) handelt es sich also um eine für p ganze Zahl, wenn nicht $p-1|2k$ gilt. Im Fall $p-1|2k$ hat man nach dem kleinen Fermatschen Satze $v^{2k} \equiv 1 \pmod{p}$, so daß man für (3.15) auch schreiben kann:

$$(3.16) \quad \mathfrak{B}(k|\mathfrak{A}_k) \equiv \frac{-uv}{g_2^k} \binom{2k-2}{k-1} (2k-1) B_{2k} \pmod{p^0}$$

$$(p|d_\Omega, p > k, (p, v) = 1).$$

Es zeigt sich nun, daß für die Gültigkeit von (3.16) die Bedingung $(p, v) = 1$ überflüssig ist. Um dies einzusehen, muß allerdings weiter ausgeholt werden.

Für die durch (3.4) gegebene Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ kann wegen $ad - bc = 1$ der Fall $d = 0$ nur für $c = \pm 1$ eintreten. Nach (3.8) ist dann aber $c = vg_2 = 1$, und daher auch $v = 1$, so daß in diesem Fall die Bedingung $(p, v) = (p, 1) = 1$ keine Einschränkung bedeutet.

Sei jetzt $d \neq 0$. In [9] ist mit Hilfe von allgemeinen Reziprozitätsgesetzen für die höheren Dedekindschen Summen $S_{2k}^{(m)}(d, c)$ gezeigt worden, daß für $\mathfrak{B}(k|\mathfrak{A}_k)$ auch die folgende Darstellung besteht⁽¹⁾:

$$(3.17) \quad \mathfrak{B}(k|\mathfrak{A}_k) = \frac{-2}{\mathfrak{N}(\mathfrak{g})^{k-1}} \left\{ \sum_{m=0}^{2k} \binom{2k}{m} (-1)^m S_{2k}^{(m)}(c, d) \times \right. \\ \times \sum_{r=0}^{k-1} \binom{m-1}{r} \binom{2k-1-m}{k-1-r} (\varepsilon_+ \gamma_2)^{k-m+r} \gamma_1^{m-1-r} (\varepsilon'_+ \gamma_2')^{k-1-r} \gamma_1'^r - \\ \left. - \sum_{m=0}^{2k} \binom{2k}{m} (-1)^m B_{2k-m} B_m \sum_{r=0}^{k-1} \binom{m-1}{r} \binom{2k-1-m}{k-1-r} \gamma_2^{k-m+r} \gamma_1^{m-1-r} \gamma_2'^{k-1-r} \gamma_1'^r \right\}.$$

Hierin bedeutet der Strich ' die Anwendung des nicht identischen Automorphismus von Ω . Im Gegensatz zur Darstellung (3.6) treten hier die höheren Dedekindschen Summen $S_{2k}^{(m)}(c, d)$ auf, deren Nenner gemäß (2.8) bzw. (2.9) im Wesentlichen durch die zu $c = vg_2$ teilerfremde Zahl d bestimmt wird.

Oben war schon das Ideal \mathfrak{g} aus \mathfrak{A}_k^{-1} prim zu uvd_Ω gewählt. Sei $p \neq 2$ ein Primteiler von v . Dann ist $\mathfrak{N}(\mathfrak{g}) = g_1^2 g_2$ und damit auch $\gamma_2 = g_1 g_2$ teilerfremd zu p . Es kann erreicht werden, daß das Basiselement γ_1 ebenfalls prim zu p ist. Hat man schon $(\gamma_1, p) = 1$, so ist nichts zu zeigen. Ist dagegen $(\gamma_1, p) \neq 1$, so sind die beiden folgenden Fälle zu unterscheiden:

a) p ist träge in Ω . Dann ist (p) ein Primideal, und es folgt aus $(\gamma_1, p) \neq 1$ notwendig $p|\gamma_1$ und daraus wegen $p \nmid \gamma_2$, daß $\gamma_1 + \gamma_2$ prim zu p ist. Man ersetze daher γ_1 durch $\gamma_1 + \gamma_2 = \frac{1}{2} g_1 (g_0^* + \sqrt{d_\Omega})$ mit $g_0^* = g_0 + 2g_2$.

b) p ist nicht träge in Ω . Dann ist $(p) = pp'$ das Produkt zweier Primideale p und p' von Ω (mit $p = p'$ für $p|d_\Omega$). Sei etwa $p|\gamma_1$. Aus $p \neq 2$ und $p \nmid \gamma_2$ folgt, daß $\gamma_1 + \gamma_2$ und $\gamma_1 + 2\gamma_2$ prim zu p sind. Hat man schon $p \nmid \gamma_1 + \gamma_2$, so ist $\gamma_1 + \gamma_2$ auch prim zu $(p) = pp'$, und man ersetze

⁽¹⁾ Der Beweis für diese Darstellung ist in [9] allerdings nur für gerades k erbracht worden. Er läßt sich aber ohne Schwierigkeiten auch auf den Fall $k \equiv 1 \pmod 2$ übertragen.

γ_1 durch $\gamma_1 + \gamma_2$. Gilt dagegen $p'|\gamma_1 + \gamma_2$, so ist wegen $p' \nmid \gamma_2$ sicher p' kein Teiler von $\gamma_1 + 2\gamma_2$. Es ist also $\gamma_1 + 2\gamma_2$ prim zu $(p) = pp'$, und man ersetze jetzt γ_1 durch $\gamma_1 + 2\gamma_2 = \frac{1}{2} g_1 (g_0^* + \sqrt{d_\Omega})$ mit $g_0^* = g_0 + 4g_2$.

Es kann also ohne Einschränkung angenommen werden, daß γ_1 und γ_2 prim zu p sind und in der Form (3.1) dargestellt werden.

Der Primteiler p von v geht nicht in der Komponente d der durch (3.4) bzw. (3.8) gegebenen Matrix auf, da d teilerfremd zu $c = vg_2$ ist. Mit (2.5) und (2.9) bekommt man daher aus (3.17):

$$(3.18) \quad \mathfrak{B}(k|\mathfrak{A}_k) = \frac{-2g_2^k g_1}{d^{2k-1}} \sum_{m=0}^k \binom{2k}{2m} \frac{1}{(g_1 g_2)^{2m}} B_{2k-2m} B_{2m} \times \\ \times \sum_{r=0}^{k-1} \binom{2m-1}{r} \binom{2k-1-2m}{k-1-r} \gamma_1^{2m-1-r} \gamma_1'^r (\varepsilon_+^{2r+1-2m} - d^{2k-1}) \pmod{p^0}.$$

Nach (3.8) gilt $d = \frac{1}{2}(u - vg_0)$. Es ist also wegen $\varepsilon_+ \varepsilon'_+ = 1$

$$\varepsilon_+^{2r-1-2m} - d^{2k-1} = \left(\frac{u + v\sqrt{d_\Omega}}{2} \right)^{2r+1} \left(\frac{u - v\sqrt{d_\Omega}}{2} \right)^{2m} - \left(\frac{u - vg_0}{2} \right)^{2k-1} \\ = \left(\frac{u}{2} \right)^{2r+1+2m} - \left(\frac{u}{2} \right)^{2k-1} \equiv 0 \pmod{p^e},$$

wenn die Potenz p^e von p in v aufgeht. Hierbei wurde ausgenutzt, daß auf Grund der Pellischen Gleichung (3.13) gilt: $\frac{1}{4}u^2 \equiv 1 \pmod{p^e}$ für $p^e|v$. Mit (3.18) und der Folgerung (3.11) aus dem Satz von v. Staudt und Clausen erhält man wie oben den zu Satz I analogen

Satz II. Ist $p \neq 2$ ein Primteiler der Komponente v der normpositiven Grundeinheit $\varepsilon_+ = \frac{1}{2}(u + v\sqrt{d_\Omega}) > 1$ von Ω , so ist $B(k|\mathfrak{A}_k)$ ganz für p , falls eine der drei Bedingungen

$$p-1 \nmid 2k, \quad p^2|v \quad \text{oder} \quad p > k$$

erfüllt ist. Anderenfalls ist $pB(k|\mathfrak{A}_k)$ eine für p ganze rationale Zahl.

Mit dem Beweis dieses Satzes II ist auch die oben aufgestellte Frage beantwortet, ob die Bedingung $(p, v) = 1$ für die Gültigkeit der Kongruenz (3.16) notwendig ist. Geht nämlich der Primteiler $p > k$ von d_Ω in v auf, so ist nach dem Satz von v. Staudt und Clausen sicher vB_{2k} eine für p ganze rationale Zahl. Für diese Primzahl p besagt (3.16) also gerade, daß $\mathfrak{B}(k|\mathfrak{A}_k)$ eine für p ganze Zahl sei. Das ist aber nach Satz II richtig; denn es ist $p > k \geq 2$ und es gilt (3.7).

Ist $k < p \leq 2k-1$, so ist die Primzahl p offenbar Teiler von $\binom{2k-2}{k-1} \times (2k-1)$. Mit der Partialbruchzerlegung (3.10) der Bernoullischen Zahlen folgt daher aus (3.16) und dem Satz II der

SATZ III. Ist $p > k$ eine in d_Ω aufgehende Primzahl, so ist $B(k|\mathfrak{A}_k)$ ganz für p , falls $p \neq 2k+1$ gilt. Ist dagegen $2k+1 = p$ ein Primteiler von d_Ω , so ist $pB(k|\mathfrak{A}_k)$ eine für p ganze rationale Zahl.

Sei nun der Fall, daß $2k+1 = p$ eine Primzahl sei, weiter verfolgt. Ist dann p ein Teiler der Diskriminante d_Ω , so hat man gemäß (3.10) und (3.16):

$$(3.19) \quad \mathfrak{B}(k|\mathfrak{A}_k) \equiv \frac{wv}{g_2^k} \binom{2k-2}{k-1} (2k-1) \frac{1}{p} \pmod{p^0}.$$

Nach dem Satz von Wilson ist dabei

$$(3.20) \quad \binom{2k-2}{k-1} (2k-1) = \frac{(2k-1)!}{(k-1)!^2} \equiv -\frac{(-1)^k}{4} \pmod{p}.$$

Außerdem folgt mit (3.2) aus dem kleinen Fermatschen Satz und dem Eulerschen Kriterium für das Legendresche Symbol

$$(3.21) \quad \frac{1}{g_2^k} \equiv g_1^{2k} g_2^k \equiv \mathfrak{N}(g) \frac{p-1}{2} \equiv \left(\frac{\mathfrak{N}(g)}{p}\right) \pmod{p} \quad (p = 2k+1).$$

Wählt man das Ideal g aus \mathfrak{A}_k^{-1} auch noch prim zu 2, so gilt nach dem quadratischen Reziprozitätsgesetz und dem ersten Ergänzungssatz

$$(3.22) \quad \left(\frac{\mathfrak{N}(g)}{p}\right) = \left(\frac{p}{\mathfrak{N}(g)}\right) (-1)^{\frac{p-1}{2} \frac{\mathfrak{N}(g)-1}{2}} = \left(\frac{p}{\mathfrak{N}(g)}\right) \left(\frac{(-1)^{\frac{p-1}{2}}}{\mathfrak{N}(g)}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{\mathfrak{N}(g)}\right).$$

Aus (3.19) bis (3.22) resultiert dann

$$(3.23) \quad \mathfrak{B}(k|\mathfrak{A}_k) \equiv -(-1)^{\frac{p-1}{2}} \frac{wv}{4} \left(\frac{(-1)^{\frac{p-1}{2}}}{\mathfrak{N}(g)}\right) \frac{1}{p} \pmod{p^0}.$$

Ist $k = \frac{p-1}{2}$ ungerade und $p|d_\Omega$, so ist die Norm $N(\varepsilon)$ der Grundeinheit

$\varepsilon = \frac{1}{2}(u_0 + v_0\sqrt{d_\Omega}) > 1$ positiv [5], p. 303. Es gilt dann also $\varepsilon_+ = \varepsilon$ und somit

$$(3.24) \quad wv = N(\varepsilon)u_0v_0 \quad (k \equiv 1 \pmod{2}).$$

Ist dagegen $k = \frac{p-1}{2}$ gerade, so sind zwei Fälle zu unterscheiden:

Entweder hat man auch hier $N(\varepsilon) = 1$ und $\varepsilon_+ = \varepsilon$, also ebenfalls

$$(3.25) \quad wv = N(\varepsilon)u_0v_0 \quad (k \equiv 0 \pmod{2}, \varepsilon_+ = \varepsilon),$$

oder es ist $N(\varepsilon) = -1$ und $\varepsilon_+ = \varepsilon^2$. Dann gilt $\frac{1}{2}(u + v\sqrt{d_\Omega}) = \frac{1}{2}(u_0 + v_0\sqrt{d_\Omega})^2$. Mit Hilfe der Pellischen Gleichung $u_0^2 - v_0^2 d_\Omega = 4N(\varepsilon)$ bekommt man wegen $p|d_\Omega$ daraus

$$(3.26) \quad wv \equiv \frac{1}{2}(u_0^2 + v_0^2 d_\Omega)u_0v_0 \equiv 2N(\varepsilon)u_0v_0 \pmod{p} \quad (k \equiv 0 \pmod{2}, \varepsilon_+ = \varepsilon^2).$$

Aus (3.7), (3.23), (3.24), (3.25) und (3.26) erhält man endlich

$$(3.27) \quad B(k|\mathfrak{A}_k) \equiv -(-1)^{\frac{p-1}{2}} \frac{N(\varepsilon)u_0v_0}{4} \left(\frac{(-1)^{\frac{p-1}{2}}}{\mathfrak{N}(g)}\right) \frac{1}{p} \pmod{p^0} \\ (2k+1 = p|d_\Omega).$$

Das Ideal g liegt in \mathfrak{A}_k^{-1} . Da $(\mathfrak{N}(g)) = gg'$ gilt, liegt das zu g konjugierte Ideal g' in der Klasse \mathfrak{A}_k selber. Daher kann man für das in (3.27) auftretende Ideal g annehmen, daß es selbst schon in \mathfrak{A}_k liegt. $(-1)^{\frac{p-1}{2}} p$ ist eine Primdiskriminante und Teiler von d_Ω . Setzt man $d_\Omega = (-1)^{\frac{p-1}{2}} p\Delta$, so wird bekanntlich durch die allgemeine Zuordnung

$$(3.28) \quad g \rightarrow \chi_p(g) = \begin{cases} \left(\frac{(-1)^{\frac{p-1}{2}} p}{\mathfrak{N}(g)}\right), & \text{falls } p \nmid \mathfrak{N}(g), \\ \left(\frac{\Delta}{\mathfrak{N}(g)}\right), & \text{falls } p | \mathfrak{N}(g) \end{cases}$$

ein Geschlechtscharakter definiert. Im Fall $p \equiv 1 \pmod{4}$ hängt dieser Charakter $\chi_p(g)$ nur von der absoluten Klasseneinteilung der Ideale von Ω ab. Denn $1 + \sqrt{d_\Omega}$ besitzt offenbar negative Norm, und man hat unter der Voraussetzung $p \equiv 1 \pmod{4}$:

$$\chi_p(1 + \sqrt{d_\Omega}) = \left(\frac{p}{d_\Omega - 1}\right) = \left(\frac{d_\Omega - 1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Daher kann man festsetzen:

$$(3.29) \quad \chi_p(\mathfrak{A}_{\frac{p-1}{2}}) = \chi_p(g), \quad \text{falls } g \text{ aus } \mathfrak{A}_{\frac{p-1}{2}} \text{ ist,}$$

und man erhält den

SATZ IV. Sei $p > 3$ eine Primzahl und Teiler der Diskriminante d_Ω des reell-quadratischen Zahlkörpers Ω , und es bezeichne $\varepsilon = \frac{1}{2}(u_0 + v_0\sqrt{d_\Omega}) > 1$ die Grundeinheit von Ω . Dann besteht für diese Primzahl die Partialbruchzerlegung

$$B\left(\frac{p-1}{2} | \mathfrak{A}_{\frac{p-1}{2}}\right) \equiv -(-1)^{\frac{p-1}{2}} \frac{N(\varepsilon)u_0v_0}{4} \chi_p(\mathfrak{A}_{\frac{p-1}{2}}) \frac{1}{p} \pmod{p^0} \quad (p|d_\Omega).$$

Dieses Ergebnis läßt sich noch erweitern, und zwar soll jetzt gezeigt werden, daß $B\left(\frac{p-1}{2} \mid \mathfrak{A}_{\frac{p-1}{2}}\right)$ ganz für die Primzahl $p > 3$ ist, wenn diese nicht in der Diskriminante d_Ω aufgeht. Dazu wird von der Kongruenz (3.9) ausgegangen. Mit dem Satz von v. Staudt und Clausen (3.10) bekommt man für nicht in $c = vg_2$ aufgehende Primzahlen $p = 2k+1$:

$$(3.30) \quad \mathfrak{B}(k \mid \mathfrak{A}_k) \equiv \frac{-1}{p v^{2k-1} g_2^k} \left\{ \sum_{r=0}^{k-1} \binom{-1}{r} \binom{2k-1}{k-1-r} S(\varepsilon_+^{2r+1}) + \sum_{r=0}^{k-1} \binom{2k-1}{r} \binom{-1}{k-1-r} S(\varepsilon_+^{2r+1-2k}) \right\} \\ \equiv \frac{-2}{p v^{2k-1} g_2^k} \sum_{r=0}^{k-1} (-1)^r \binom{2k-1}{k-1-r} S(\varepsilon_+^{2r+1}) \pmod{p^0}.$$

Die hierin auftretende Summe läßt sich als polinomischer Ausdruck in $\frac{1}{2}S(\varepsilon_+) = u/2$ schreiben. Man setze für den Quotienten der Basis (3.1) $\omega = \gamma_1/\gamma_2$. Durch mehrfache Anwendung der partiellen Integration findet man

$$(3.31) \quad \int (x-\omega)^{k-1} (x-\omega')^{k-1} dx \\ = \frac{(k-1)!^2}{(2k-1)!} \sum_{r=0}^{k-1} (-1)^r \binom{2k-1}{k-1-r} (x-\omega)^{k-1-r} (x-\omega')^{k+r}.$$

Aus (3.4) bekommt man leicht

$$\varepsilon_+^{-1} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix}.$$

Zusammen mit (3.4) erhält man daraus:

$$(3.32) \quad \varepsilon_+ = c\omega + d, \quad \varepsilon_+' = \varepsilon_+^{-1} = c\omega' + d, \\ \varepsilon_+ = -c\omega' + a, \quad \varepsilon_+' = \varepsilon_+^{-1} = -c\omega + a. \quad (\omega = \gamma_1/\gamma_2)$$

Daher folgt aus (3.31):

$$(3.33) \quad \int_{-d/c}^{a/c} (x-\omega)^{k-1} (x-\omega')^{k-1} dx \\ = \frac{(k-1)!^2}{(2k-1)! c^{2k-1}} \sum_{r=0}^{k-1} (-1)^r \binom{2k-1}{k-1-r} (\varepsilon_+^{2r+1} + \varepsilon_+'^{2r+1}) \\ = \frac{(k-1)!^2}{(2k-1)! c^{2k-1}} \sum_{r=0}^{k-1} (-1)^r \binom{2k-1}{k-1-r} S(\varepsilon_+^{2r+1}).$$

Andererseits gilt

$$\int (x-\omega)^{k-1} (x-\omega')^{k-1} dx = \int \left(\left(x - \frac{\omega + \omega'}{2} \right)^2 - \left(\frac{\omega - \omega'}{2} \right)^2 \right)^{k-1} dx \\ = \sum_{r=0}^{k-1} \binom{k-1}{r} \frac{1}{2r+1} \left(x - \frac{\omega + \omega'}{2} \right)^{2r+1} \left(- \left(\frac{\omega - \omega'}{2} \right)^2 \right)^{k-1-r},$$

woraus mit den aus (3.32) unmittelbar einzusehenden Gleichungen

$$2a - c(\omega + \omega') = \varepsilon_+ + \varepsilon_+' = u, \quad 2d + c(\omega + \omega') = \varepsilon_+ + \varepsilon_+' = u$$

und

$$-c^2(\omega - \omega')^2 = -(\varepsilon_+ - \varepsilon_+')^2 = -v^2 d_\Omega = 4 - u^2$$

die Darstellung

$$(3.34) \quad \int_{-d/c}^{a/c} (x-\omega)^{k-1} (x-\omega')^{k-1} dx \\ = \frac{2}{c^{2k-1}} \sum_{r=0}^{k-1} \binom{k-1}{r} \frac{1}{2r+1} \left(\frac{u}{2} \right)^{2r+1} \left(1 - \frac{u^2}{4} \right)^{k-1-r}$$

für das Integral (3.33) resultiert.

Führt man das Polynom

$$(3.35) \quad F_k(x) = \sum_{r=0}^{k-1} \binom{k-1}{r} \frac{1}{2r+1} x^r (1-x)^{k-r}$$

ein, so ist gemäß (3.30), (3.33), (3.34) und (3.35):

$$(3.36) \quad \mathfrak{B}(k \mid \mathfrak{A}_k) \equiv \frac{16(2k-1)!}{(k-1)!^2 v^{2k+1} d_\Omega g_2^k} \frac{\frac{u}{2} F_k\left(\frac{u^2}{4}\right)}{p} \pmod{p^0} \quad (p = 2k+1).$$

Für das Polynom (3.35) hat C. L. Siegel [13] bewiesen:

$$F_k(x) \equiv 1 - x^k \pmod{p} \quad \text{für } p = 2k+1.$$

Nach dem kleinen Fermatschen Satz ist daher

$$(3.37) \quad \frac{u}{2} F_k\left(\frac{u^2}{4}\right) \equiv 0 \pmod{p} \quad (p = 2k+1).$$

$\mathfrak{B}(k \mid \mathfrak{A}_k)$ ist also ganz für die Primzahl $p = 2k+1$, wenn diese nicht in $v d_\Omega g_2$ aufgeht. Wählt man nun das in die Darstellung (3.6) für $\mathfrak{B}(k \mid \mathfrak{A}_k)$ eingehende Ideal \mathfrak{g} auch noch prim zur vorgegebenen Primzahl p , so ist $\mathfrak{N}(\mathfrak{g}) = g_1^2 g_2$ und dann erst recht g_2 zu p teilerfremd.

Aus (3.7), (3.36), (3.37) und dem Satz II erhält man daher schließlich den

SATZ V. Ist $p > 3$ eine nicht in der Diskriminante d_Ω aufgehende Primzahl, so stellt $B\left(\frac{p-1}{2} | \mathfrak{A}_{\frac{p-1}{2}}\right)$ eine für p ganze rationale Zahl dar.

IV. Beispiele. Der im Satz IV ausgesprochene Sachverhalt sei nun an einigen Beispielen illustriert. Sei dazu $\Omega = P(\sqrt{65})$ der reell-quadratische Zahlkörper mit der Diskriminante $65 = 5 \cdot 13$. Seine Grundeinheit ist $\varepsilon = \frac{1}{2}(16 + 2\sqrt{65}) > 1$ mit $N(\varepsilon) = -1$. Ω besitzt die absolute Klassenzahl 2. Die Einheitsklasse \mathfrak{E} werde durch das Einheitsideal $\mathfrak{n} = \{\frac{1}{2}(1 + \sqrt{65}), 1\}$ vertreten. Ein Repräsentant der anderen Klasse \mathfrak{A} ist $\mathfrak{g} = \{\frac{1}{2}(5 + \sqrt{65}), 5\}$ mit $\mathfrak{N}(\mathfrak{g}) = 5$. Dann ist $\chi_5(\mathfrak{E}) = \chi_{13}(\mathfrak{E}) = 1$, und gemäß (3.28) und (3.29) hat man $\chi_5(\mathfrak{A}) = \chi_{13}(\mathfrak{A}) = \left(\frac{13}{5}\right) = -1$. Nach Satz IV

hat man:

$$(4.1) \quad \begin{aligned} B(2 | \mathfrak{E}) &\equiv \frac{3}{5} \pmod{5^0}, & B(2 | \mathfrak{A}) &\equiv -\frac{3}{5} \pmod{5^0}, \\ B(6 | \mathfrak{E}) &\equiv \frac{8}{13} \pmod{13^0}, & B(6 | \mathfrak{A}) &\equiv -\frac{8}{13} \pmod{13^0}. \end{aligned}$$

Die genauen Werte dieser hier aufgeführten Zahlen $B(k | \mathfrak{A}_k)$ sind bekannt. Sie wurden mit Hilfe der Barnerschen Formel (3.3) auf einer elektronischen Rechenanlage bestimmt. In Übereinstimmung mit (4.1) entnimmt man aus [8]:

$$B(2 | \mathfrak{E}) = \frac{208}{5} = \frac{3}{5} + 41, \quad B(2 | \mathfrak{A}) = \frac{112}{5} = -\frac{3}{5} + 23.$$

Die Werte $B(6 | \mathfrak{E})$ und $B(6 | \mathfrak{A})$ sind aus einer unveröffentlichten Tabelle entnommen, die M. Pohst [12] anlässlich einer Diplomarbeit aufgestellt hat, und zwar gilt:

$$B(6 | \mathfrak{E}) = \frac{307960755168}{5 \cdot 13} = \frac{8}{13} + \frac{23689288856}{5}$$

und

$$B(6 | \mathfrak{A}) = \frac{9646408992}{5 \cdot 13} = -\frac{8}{13} + \frac{742031464}{5}.$$

Literaturverzeichnis

- [1] T. M. Apostol, *Generalized Dedekind sums and transformation formulae of certain Lambert series*, Duke Math. J. 17 (1950), S. 217–220.
 [2] K. Barner, *Über die Werte der Ringklassen-L-Funktionen reell-quadratischer Zahlkörper an natürlichen Argumentstellen*, J. Number Theory, 1, (1) (1969), S. 28–64.

- [3] L. Carlitz, *Some theorems on generalized Dedekind sums*, Pacific J. Math. 3 (1953), S. 513–522.
 [4] G. Frobenius, *Über die Bernoullischen Zahlen und die Eulerschen Polynome*, Sitzungsber. Preuss. Akad. Wissenschaften (1910), S. 809–847; Mathematische Werke, Bd. III, Berlin–Heidelberg–New York 1968, S. 440–478.
 [5] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin–Göttingen–Heidelberg–New York 1964.
 [6] E. Hecke, *Analytische Funktionen und algebraische Zahlen*, Teil 2. Abh. Math. Sem. Univ. Hamburg 3 (1924), S. 213–236; Mathematische Werke, Göttingen 1959, S. 381–404.
 [7] H. Klingen, *Über die Werte der Dedekindschen Zetafunktion*, Math. Annalen 145 (1962), S. 265–272.
 [8] H. Lang, *Über eine Gattung elementar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper*, J. Reine Angew. Math. 233 (1968), S. 123–175.
 [9] — *Über Anwendungen höherer Dedekindscher Summen auf die Struktur elementar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper*, J. Reine Angew. Math. 254 (1972), S. 17–32.
 [10] C. Meyer, *Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern*, Berlin 1957.
 [11] — *Über die Bildung von elementar-arithmetischen Klasseninvarianten in reell-quadratischen Zahlkörpern*. Algebraische Zahlentheorie, Mathematisches Forschungsinstitut Oberwolfach, Berichte, Heft 2 (1966), S. 165–215.
 [12] M. Pohst, *Über die Werte der Zetafunktion an geraden Argumenten in reell-quadratischen und total reellen kubischen Zahlkörpern*, Diplomarbeit, Köln 1971.
 [13] C. L. Siegel, *Bernoullische Polynome und quadratische Zahlkörper*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. (1968), S. 7–38.
 [14] — *Berechnung von Zetafunktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. (1969), S. 87–102.

MATHEMATISCHES INSTITUT
 DER UNIVERSITÄT ZU KÖLN

Eingegangen 11. 2. 1972

(263)